Practical - 4

Name: Shivam Tawari
Roll no: A - 58

Aim: Explore AWS Cloud Based Infrastructure as Service (EC2, S3)

Theory:

Amazon EC2 Instance:
An EC2 instance is nothing but a virtual server in Amazon Web Services terminology. It stands for Elastic Compute Cloud. It is a web service where an AWS subscriber can request and provision a compute server in AWS cloud.

An on-demand EC2 instance is an offering from AWS where the subscriber / user can rent the virtual server per hour and use it to deploy his / her own applications.

The instance will be charged per hour with different rates based on the type of the instance chosen. AWS provides multiple instance types for the respective business needs of the user.

Thus, you can rent an instance based on your own CPU and memory requirements and use it as long as you want

Steps to Create EC2 Instance:

1. Login and access to AWS services
2. Choose AMI
3. Choose EC2 Instance Types
4. Configure Instance
5. Configure Security groups
6. Review Instances
7. Create a EIP and connect to your instance.

AWS S3 Storage:

Amazon Simple Storage Service (S3) is a storage for the internet.

It is designed for large - capacity, low-cost storage provision across multiple geographical regions. Amazon S3 provides developers and IT teams with secure, durable and highly scalable object storage.

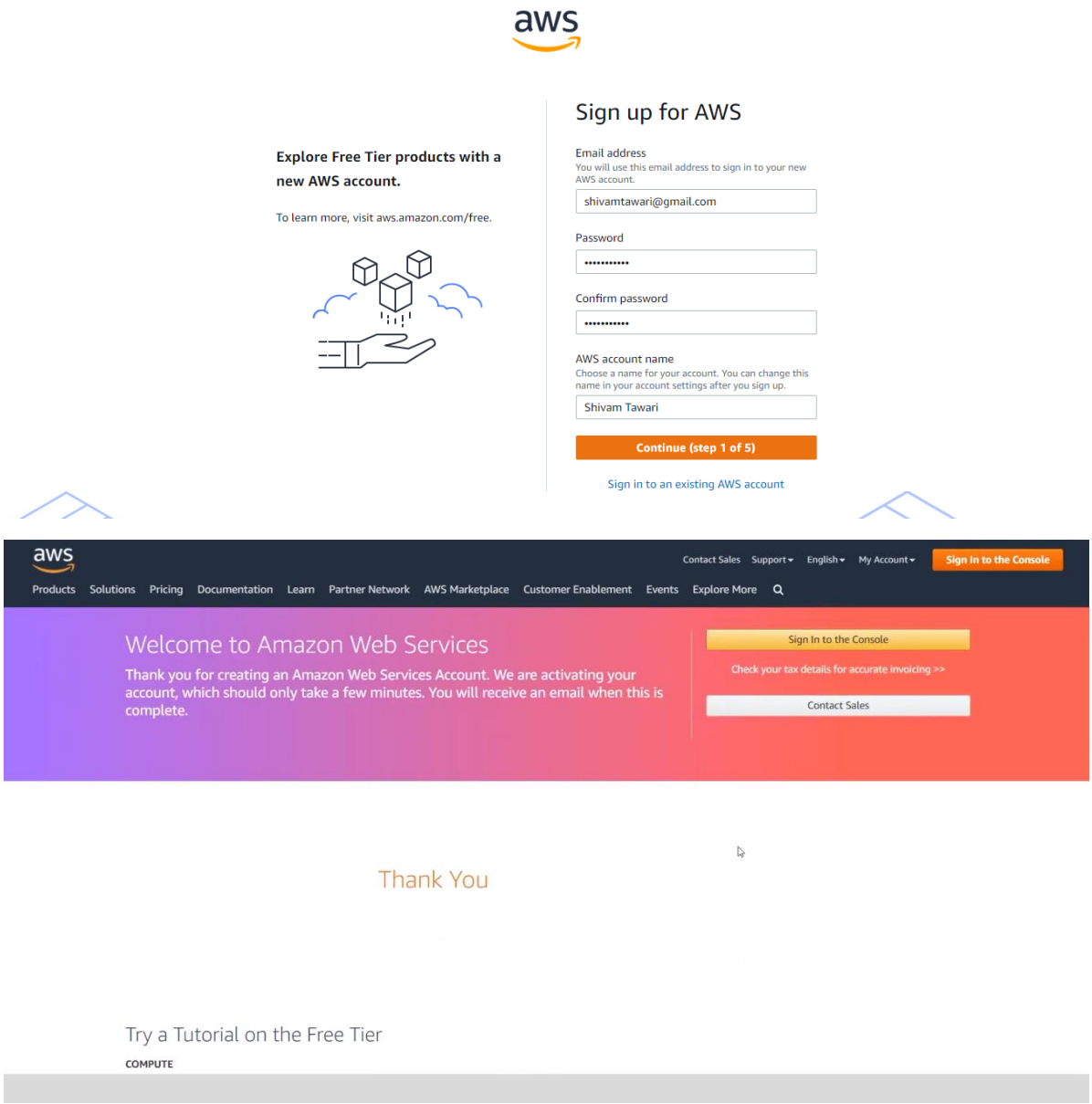
Conclusion: Hence, we have successfully performed exploring AWS services of EC2 instance and S3 storage.

Practical – 4

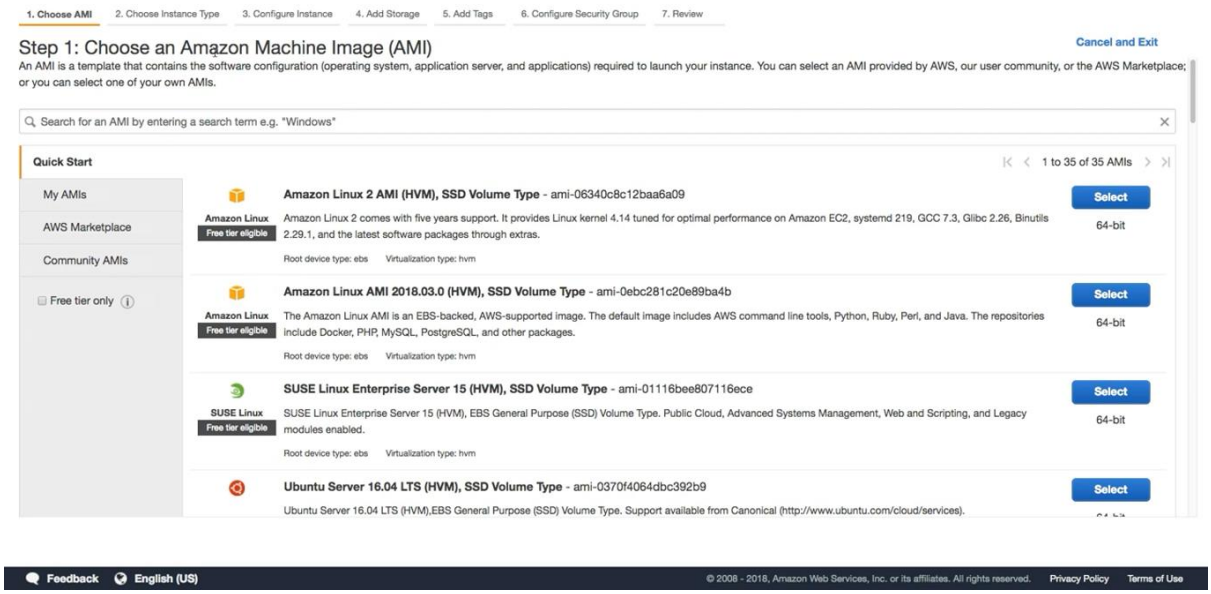
Name: Shivam Tawari

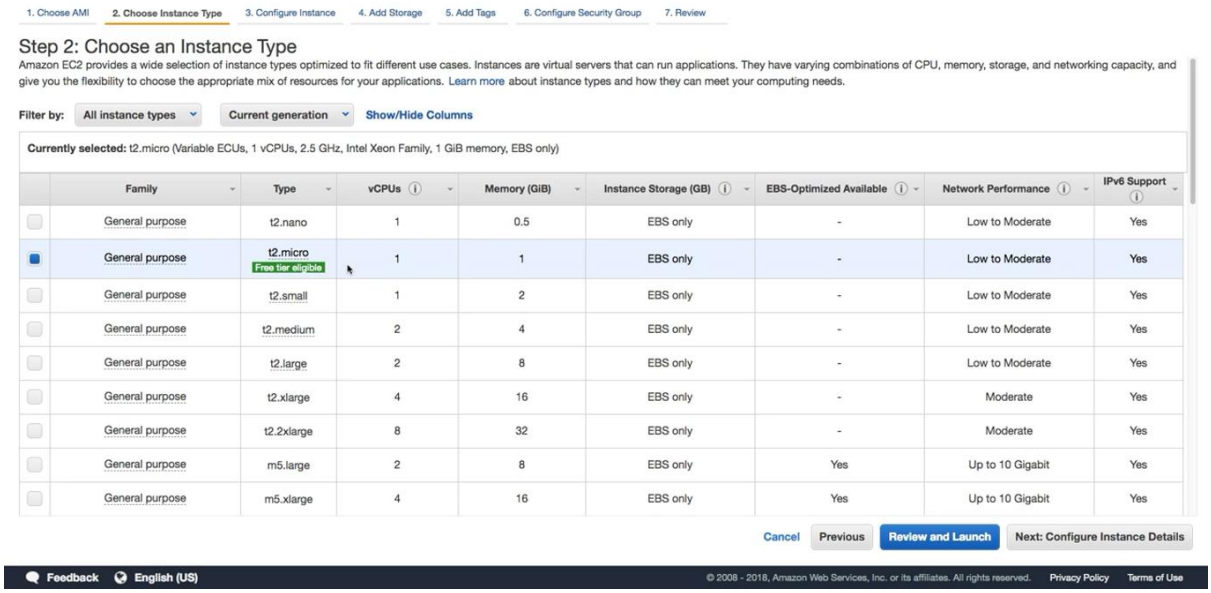
Roll no: A – 58

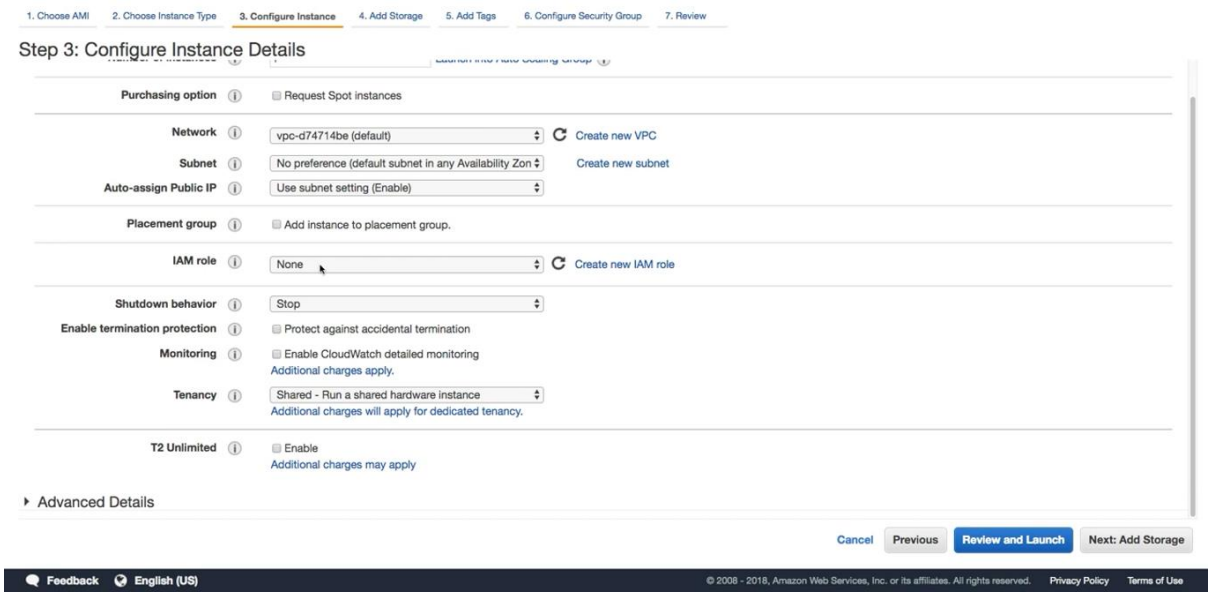
AWS Account Creation:

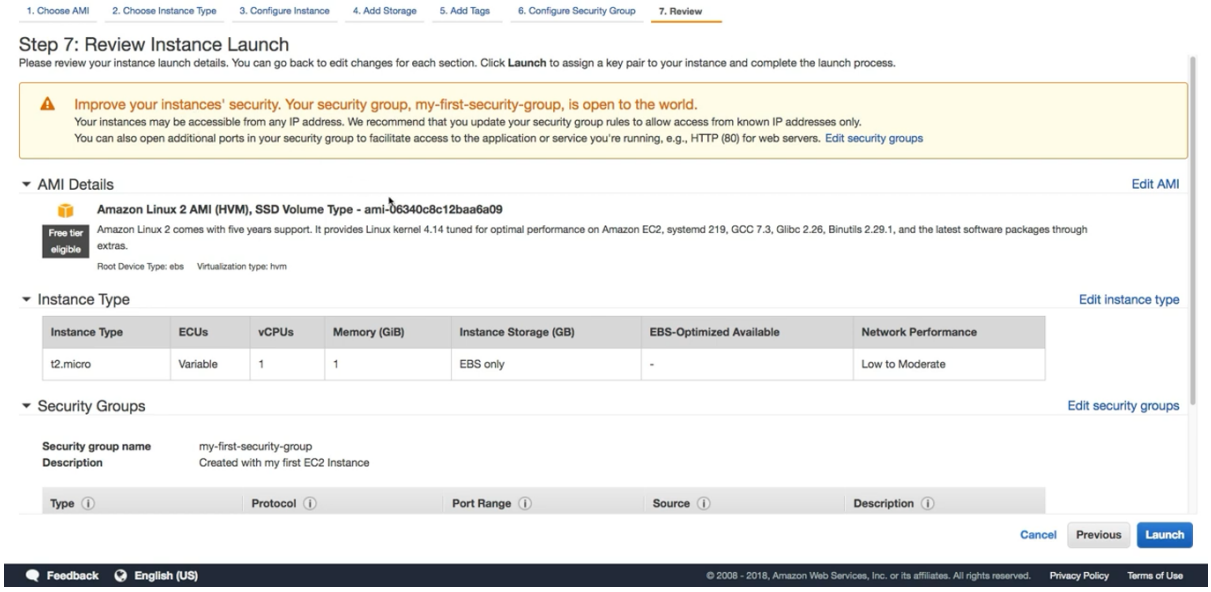


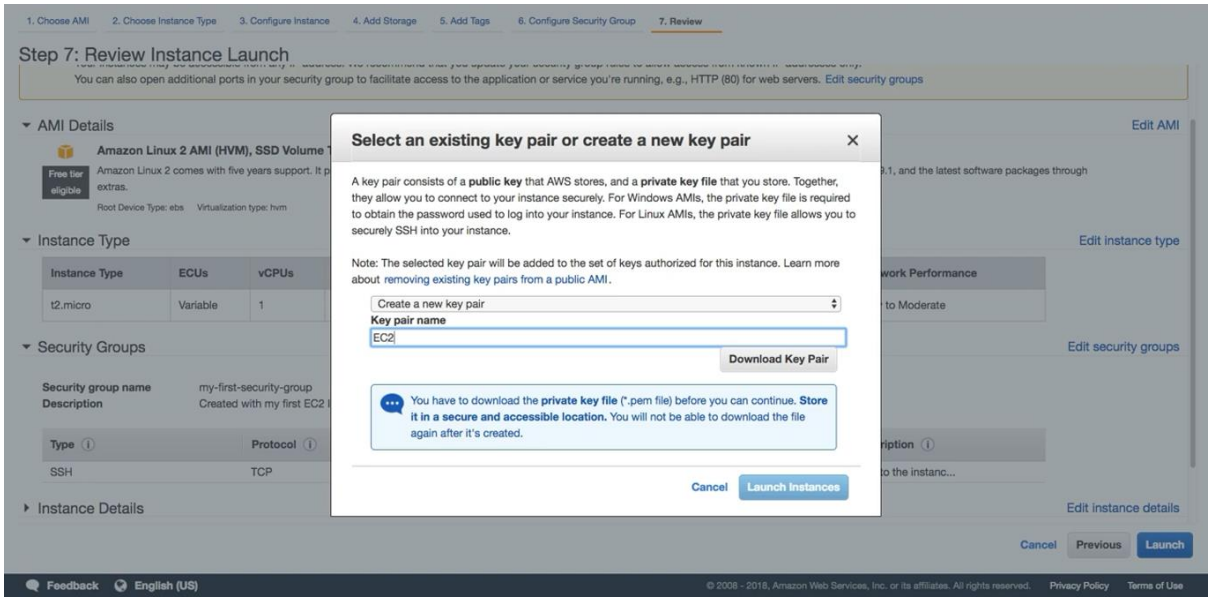
EC2 Instance:



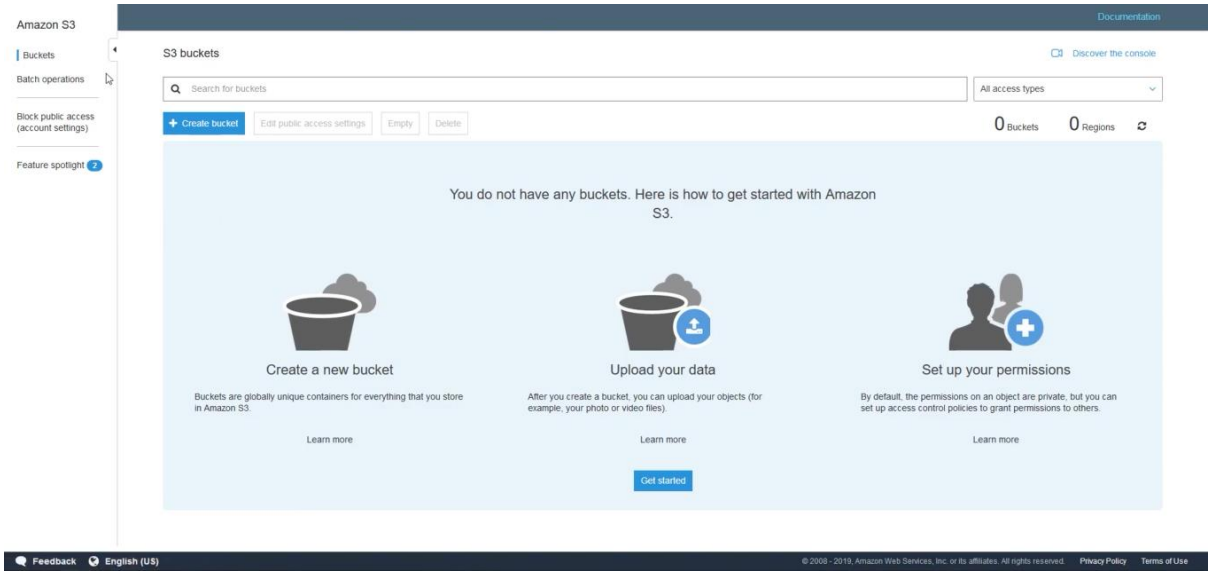


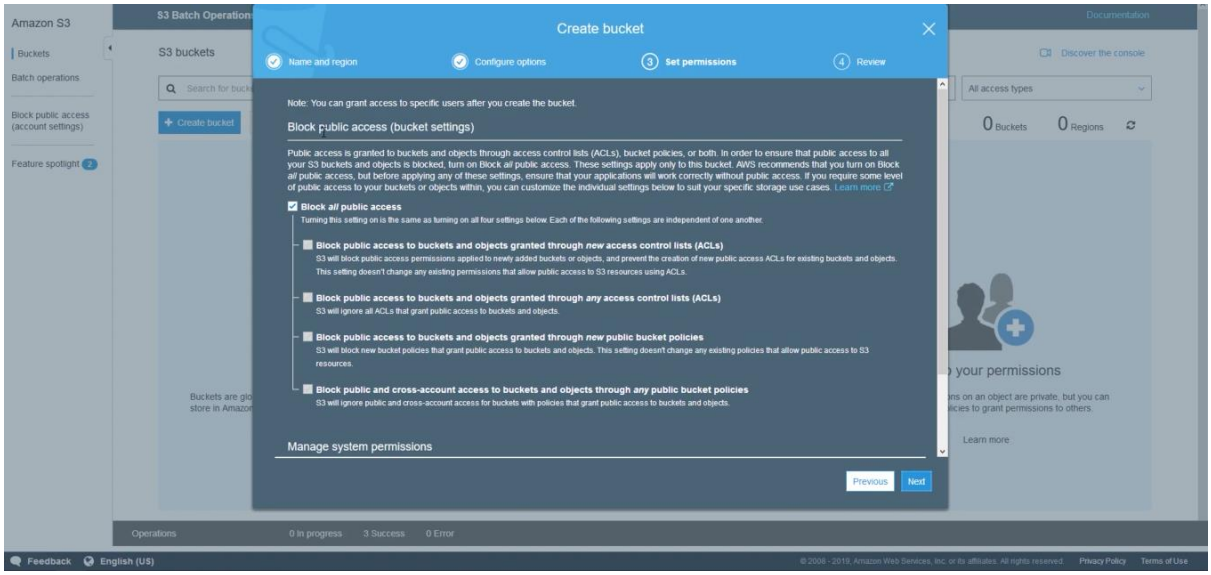

1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Add Tags
6. Configure Security Group
7. Review
Step 3: Configure Instance Details
Purchasing option
Request Spot instances
Network
vpc-d74714be (default)
Create new VPC
Subnet
No preference (default subnet in any Availability Zon
Create new subnet
Auto-assign Public IP
Use subnet setting (Enable)
Placement group
Add instance to placement group.
IAM role
None
Create new IAM role
Shutdown behavior
Stop
Enable termination protection
Protect against accidental termination
Monitoring
Enable CloudWatch detailed monitoring
Additional charges apply.
Tenancy
Shared - Run a shared hardware instance
Additional charges will apply for dedicated tenancy.
T2 Unlimited
Enable
Additional charges may apply
Advanced Details
Cancel
Previous
Review and Launch
Next: Add Storage
Feedback
English (US)
© 2008 - 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use


1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Add Tags
6. Configure Security Group
7. Review
Step 7: Review Instance Launch
Please review your instance launch details. You can go back to edit changes for each section. Click Launch to assign a key pair to your instance and complete the launch process.
Improve your instances' security. Your security group, my-first-security-group, is open to the world.
Your instances may be accessible from any IP address. We recommend that you update your security group rules to allow access from known IP addresses only.
You can also open additional ports in your security group to facilitate access to the application or service you're running, e.g., HTTP (80) for web servers. Edit security groups
AMI Details
Edit AMI
Amazon Linux 2 AMI (HVM), SSD Volume Type - ami-06340c8c12baa6a09
Free tier eligible
Amazon Linux 2 comes with five years support. It provides Linux kernel 4.14 tuned for optimal performance on Amazon EC2, systemd 219, GCC 7.3, Glibc 2.26, Binutils 2.29.1, and the latest software packages through extras.
Root Device Type: ebs
Virtualization type: hvm
Instance Type
Edit instance type
Instance Type
ECUs
vCPUs
Memory (GiB)
Instance Storage (GB)
EBS-Optimized Available
Network Performance
t2.micro
Variable
1
1
EBS only
-
Low to Moderate
Security Groups
Edit security groups
Security group name
my-first-security-group
Description
Created with my first EC2 Instance
Type
Protocol
Port Range
Source
Description
Cancel
Previous
Launch
Feedback
English (US)
© 2008 - 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use


1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Add Tags
6. Configure Security Group
7. Review
Step 7: Review Instance Launch
You can also open additional ports in your security group to facilitate access to the application or service you're running, e.g., HTTP (80) for web servers. Edit security groups
AMI Details
Edit AMI
Amazon Linux 2 AMI (HVM), SSD Volume
Free tier eligible
Amazon Linux 2 comes with five years support.
extras.
Root Device Type: ebs
Virtualization type: hvm
Instance Type
Edit instance type
Instance Type
ECUs
vCPUs
t2.micro
Variable
1
to Moderate
Security Groups
Edit security groups
Security group name
my-first-security-group
Description
Created with my first EC2
Type
Protocol
SSH
TCP
Instance Details
Edit instance details
Cancel
Previous
Launch
Feedback
English (US)
© 2008 - 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Select an existing key pair or create a new key pair
A key pair consists of a public key that AWS stores, and a private key file that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.
Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about removing existing key pairs from a public AMI.
Create a new key pair
Key pair name
EC2
Download Key Pair
You have to download the private key file (*.pem file) before you can continue. Store it in a secure and accessible location. You will not be able to download the file again after it's created.
Cancel
Launch Instances

S3 Bucket:


Amazon S3
Documentation
Buckets
Batch operations
Block public access (account settings)
Feature spotlight
S3 buckets
Discover the console
Search for buckets
All access types
Create bucket
Edit public access settings
Empty
Delete
0 Buckets
0 Regions
You do not have any buckets. Here is how to get started with Amazon S3.
Create a new bucket
Buckets are globally unique containers for everything that you store in Amazon S3.
Learn more
Upload your data
After you create a bucket, you can upload your objects (for example, your photo or video files).
Learn more
Set up your permissions
By default, the permissions on an object are private, but you can set up access control policies to grant permissions to others.
Learn more
Get started
Feedback
English (US)
© 2008 - 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use


Amazon S3
S3 Batch Operations
Buckets
Batch operations
Block public access (account settings)
Feature spotlight
S3 buckets
Search for buckets
Create bucket
Documentation
Discover the console
All access types
0 Buckets
0 Regions
Create bucket
Name and region
Configure options
3 Set permissions
4 Review
Note: You can grant access to specific users after you create the bucket.
Block public access (bucket settings)
Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, or both. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. Learn more
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 policies
S3 will block new bucket 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 policies
S3 will ignore public and cross-account access for buckets with policies that grant public access to buckets and objects.
Manage system permissions
Previous
Next
your permissions
Learn more
Operations
0 In progress
3 Success
0 Error
Feedback
English (US)
Privacy Policy
Terms of Use