**ASSIGNMENT**

**To launch the EC2 instance in AWS**

1. Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.
2. Choose **Launch Instance**.
3. In **Step 1: Choose an Amazon Machine Image (AMI)**, find an Amazon Linux 2 AMI at the top of the list and choose **Select**.
4. In **Step 2: Choose an Instance Type**, choose **Next: Configure Instance Details**.
5. In **Step 3: Configure Instance Details**, provide the following information:
   * Leave **Number of instances** at one.
   * Leave **Purchasing option** at the default setting.
   * For **Network**, choose the entry for the same VPC that you noted when you created your EFS file system in [Step 1: Create your Amazon EFS file system](https://docs.aws.amazon.com/efs/latest/ug/gs-step-two-create-efs-resources.html).
   * For **Subnet**, choose a default subnet in any Availability Zone.
   * For **File systems**, make sure that the EFS file system that you created in [Step 1: Create your Amazon EFS file system](https://docs.aws.amazon.com/efs/latest/ug/gs-step-two-create-efs-resources.html) is selected. The path shown next to the file system ID is the mount point that the EC2 instance will use, which you can change.
   * The **User data** automatically includes the commands for mounting your Amazon EFS file system.
6. Choose **Next: Add Storage**.
7. Choose **Next: Add Tags**.
8. Name your instance and choose **Next: Configure Security Group**.
9. In **Step 6: Configure Security Group**, set **Assign a security group** to **Select an existing security group**. Choose the default security group to make sure that it can access your EFS file system.
10. Choose **Review and Launch**.
11. Choose **Launch**.
12. Select the check box for the key pair that you created, and then choose **Launch Instances**.

Once the EC2 instance is created and becomes available, it will be mounted to your EFS file system. At this point, you will be able to transfer files to your EFS file system

--------------------------------------------------------------------------------------------------------------------------------------

**12th may 2022**

**What is lifecycle rule.**

What is lifecycle rule in AWS?

Lifecycle Rules  
  
**A lifecycle configuration consists of a number of rules, with each rule specifying the objects it acts on and the actions to take**. Rules specify which objects they act on by defining a prefix. A rule can archive an object to Amazon Glacier, delete an object, or both.

**Write the steps with screen shots.(Any one like transition from one class to other)**

**What is S3 Object lock?**

Amazon S3 Object Lock is **an Amazon S3 feature that allows you to store objects using a write once, read many (WORM) model**. You can use WORM protection for scenarios where it is imperative that data is not changed or deleted after it has been written

**What is S3 Glacier Vault Lock?**

S3 Glacier Vault Lock **allows you to easily deploy and enforce compliance controls for individual S3 Glacier vaults with a vault lock policy**. You can specify controls such as “write once read many” (WORM) in a vault lock policy and lock the policy from future edits. Once locked, the policy can no longer be changed.

**What is SRR? Explain**

**What is SRR in AWS?**

Amazon S3 SRR is **an S3 feature that automatically replicates data between buckets within the same AWS Region**. With SRR, you can set up replication at a bucket level, a shared prefix level, or an object level using S3 object tags. You can use SRR to make one or more copies of your data in the same AWS Region.

**What CRR?**

Amazon S3 Cross-Region Replication (CRR)

Amazon S3 CRR **automatically replicates data between buckets across different AWS Regions**. With CRR, you can set up replication at a bucket level, a shared prefix level, or an object level using S3 object tags.

----------------------------------------------------------------------------------------------------------------------------------

14th may 2022

**What is DNS? Explain**

……….DNS, or **the Domain Name System**, translates human readable domain names (for example, www.amazon.com) to machine readable IP addresses (for example, 192.0. 2.44).

**What is Route 53**

……….Amazon Route 53 is a scalable and highly available Domain Name System service. Released on December 5, 2010, it is part of Amazon.com's cloud computing platform, Amazon Web Services.

**. What is hosted zone**

A hosted zone is **a container for records**, and records contain information about how you want to route traffic for a specific domain, such as example.com, and its subdomains (acme.example.com, zenith.example.com). A hosted zone and the corresponding domain have the same name.

**What is sub domain**

A **subdomain** is an additional part to your main domain name. Subdomains are created to organize and navigate to different sections of your website.

**. What are the features of route 53**

Route 53 is an “**authoritative DNS**” system. An authoritative DNS system provides an update mechanism that developers use to manage their public DNS names. It then answers DNS queries, translating domain names into IP address so computers can communicate with each other.

**Do hands on, create domain name, create hosted zone in aws for ec2 instance and check whether its working**

**What is single point of failure**

A single point of failure is a part of a system that, if it fails, will stop the entire system from working. SPOFs are undesirable in any system with a goal of high availability or reliability, be it a business practice, software application, or other industrial system.

**What is the drawback of vertical scaling?**

Disadvantages of Vertical Scaling:

**Limited Scaling**. The risk for downtime is much higher than horizontal scaling. Greater risk of outages and hardware failures. Finite scope of upgradeability in the future.

**What is Auto-Scaling**

Autoscaling, also spelled auto scaling or auto-scaling, and sometimes also called automatic scaling, is a method used in cloud computing that dynamically adjusts the amount of computational resources in a server farm - typically measured by the number of active servers - automatically based on the load on

**What is Load Balancing**

**Load balancing** refers to efficiently distributing incoming network traffic across a group of backend servers, also known as a server farm or server pool.

**What is High Availability and Fault tolerance**

The difference between fault tolerance and high availability, is this: **A fault tolerant environment has no service interruption but a significantly higher cost, while a highly available environment has a minimal service interruption**.

**What are the different types of Load Balancers?**

* ) Network Load Balancer / Layer 4 (L4) Load Balancer: ...
* b.) Application Load Balancer / Layer 7 (L7) Load Balancer: ...
* c.) Global Server Load Balancer/Multi-site Load Balancer: ...
* a.) Hardware Load Balancers: ...

**16th may 2022**

**What is lifecycle rule?**

**A rule can archive an object to Amazon Glacier, delete an object, or both**. The action associated with a rule specifies a time constraint on it, acting on the objects that are either older than a specific number of days, or after a particular date

**What is S3 Object lock**

Amazon S3 Object Lock is **an Amazon S3 feature that allows you to store objects using a write once, read many (WORM) model**. You can use WORM protection for scenarios where it is imperative that data is not changed or deleted after it has been written.

**What is S3 Glacier Vault Lock?**

S3 Glacier Vault Lock **allows you to easily deploy and enforce compliance controls for individual S3 Glacier vaults with a vault lock policy**. You can specify controls such as “write once read many” (WORM) in a vault lock policy and lock the policy from future edits. Once locked, the policy can no longer be changed.

**What is SRR?**

SRR **helps you address data sovereignty and compliance requirements by keeping a copy of your objects in the same AWS Region as the original**. When an S3 object is replicated using SRR, the metadata, Access Control Lists (ACL), and object tags associated with the object are also part of the replication.

**What CRR?**

Amazon S3 Cross-Region Replication (CRR)

Amazon S3 CRR **automatically replicates data between buckets across different AWS Regions**. With CRR, you can set up replication at a bucket level, a shared prefix level, or an object level using S3 object tags.

Assignment-17-May-22

**What is VPC**

A virtual private cloud (VPC) is a secure, isolated private cloud hosted within a public cloud. VPC customers can **run code, store data, host websites, and do anything else they could do in an ordinary private cloud**, but the private cloud is hosted remotely by a public cloud provider.

**What is Subnet**

A subnetwork or subnet is a logical subdivision of an IP network. The practice of dividing a network into two or more networks is called subnetting. Computers that belong to the same subnet are addressed with an identical most-significant bit-group in their IP

**What is Internet Gateway?**

**A computer that sits between different networks or applications**. The gateway converts information, data or other communications from one protocol or format to another. A router may perform some of the functions of a gateway. An Internet gateway can transfer communications between an enterprise network and the Internet.

**What is Router**

A router is **a device that connects two or more packet-switched networks or subnetworks**. It serves two primary functions: managing traffic between these networks by forwarding data packets to their intended IP addresses, and allowing multiple devices to use the same Internet connection.

**What is Peering Connection**

Peering is **a method that allows two networks to connect and exchange traffic directly without having to pay a third party to carry traffic across the Internet**.

**What is VPC endpoints?**

A VPC endpoint is a virtual device which is horizontally scaled, redundant and highly available, that provides communication between EC2 instances within your Virtual Private Cloud and other supported AWS services without introducing availability risks or bandwidth constraints on your network traffic.

**What is NAT instance**

A NAT (Network Address Translation) instance is, like a bastion host, **an EC2 instance that lives in your public subnet**. A NAT instance, however, allows your private instances outgoing connectivity to the internet while at the same time blocking inbound traffic from the internet.

**What is NAT gateway**

NAT Gateway is **a highly available AWS managed service that makes it easy to connect to the Internet from instances within a private subnet in an Amazon Virtual Private Cloud (Amazon VPC)**. Previously, you needed to launch a NAT instance to enable NAT for instances in a private subnet.

**. What is Virtual Private Gateway?**

A virtual private gateway is **a logical, fully redundant distributed edge routing function that sits at the edge of your VPC**. As it is capable of terminating VPN connections from your on-prem or customer environments, the VPG is the VPN concentrator on the Amazon side of the Site-to-Site VPN connection.

**. What is Customer Gateway?**

A customer gateway is **a resource that you create in AWS that represents the customer gateway device in your on-premises network**. When you create a customer gateway, you provide information about your device to AWS. For more information, see Customer gateway options for your Site-to-Site VPN connection.

**What is AWS direct Connect**

AWS Direct Connect is **a network service that provides an alternative to using the Internet to utilize AWS cloud services**. AWS Direct Connect enables customers to have low latency, secure and private connections to AWS for workloads which require higher speed or lower latency than the internet.

**What is Security Group**

A security group **acts as a virtual firewall, controlling the traffic that is allowed to reach and leave the resources that it is associated with**. For example, after you associate a security group with an EC2 instance, it controls the inbound and outbound traffic for the instance.

**. What is Network ACL**

A network access control list (ACL) is **an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets**. You might set up network ACLs with rules similar to your security groups in order to add an additional layer of security to your VPC.

**. What is CIDR?**

CIDR (Classless Inter-Domain Routing) -- also known as supernetting -- is **a method of assigning Internet Protocol (IP) addresses that improves the efficiency of address distribution and replaces the previous system based on Class A, Class B and Class C networks**.

Assignment-19-May-2022

**What is the difference between NAT Gateway and NAT instance?**

When a connection times out, a NAT gateway returns an RST packet to any resources behind the NAT gateway that attempt to continue the connection (it does not send a FIN packet). When a connection times out, a NAT instance sends a FIN packet to resources behind the NAT instance to close the connection.

**What is the difference between Security group and NACLs**

As we mentioned earlier, **security groups work at the instance level while NACLs work at the subnet level**. Security groups are a required form of defense for instances, because an instance must be associated with at least one security group.

**What is a public IP address?**

A public IP address is **an IP address that can be accessed directly over the internet and is assigned to your network router by your internet service provider (ISP)**. Your personal device also has a private IP that remains hidden when you connect to the internet through your router's public IP.

**What is a private IP address?**

In Internet networking, a private network is a computer network that uses a private address space of IP addresses. These addresses are commonly used for local area networks in residential, office, and enterprise environments. Both the IPv4 and the IPv6 specifications define private IP address ranges.

**. What is an elastic IP address**

An Elastic IP address is **a reserved public IP address that you can assign to any EC2 instance in a particular region, until you choose to release it**. To allocate an Elastic IP address to your account in a particular region, see Allocate an Elastic IP address

**What is Direct connect?**

Direct Connect is **a network service that allows a customer to establish a dedicated network connection between one of Amazon's Direct Connect locations and the customer's data center or colocation environment**.

**What is VPN?**

A virtual private network extends a private network across a public network and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.

**What is VPN? And its different types**

Virtual Private Network (VPN) services fall into four main types: **personal VPNs, remote access VPNs, mobile VPNs, and site-to-site VPNs**. In this guide, we explain how each of these VPN types work and when to use them. A VPN is a service that creates a private tunnel within a public connection (e.g. the internet)

**What is AWS transit Gateway**

AWS Transit Gateway **connects your Amazon Virtual Private Clouds (VPCs) and on-premises networks through a central hub**. This simplifies your network and puts an end to complex peering relationships. It acts as a cloud router – each new connection is only made once.