**SUMMARY**

**Amazon EBS Volume Types**

There are two categories of volume types:

* **SSD-Backed volume** optimized for transactional workloads involving frequent read/write operations with small I/O size, where the dominant performance attribute is IOPS
* **HDD-Backed volume** optimized for large streaming workload were throughput (measure in MiB/s is better performance measure than IOPS.

There are several factors than can affect the performance of EBS volume such as i**nstance configurations, I/O characteristics,** and **workload demand.**

**SSD** is a default volume type which is General purpose SSD (gp2).it provides higher performance, or performance consistency than other generation volumes.

**Amazon EC2 Auto Scalling**

Amazon EC2 Auto scaling helps you ensure that you have the correct number of Amazon instances available to handle the load for your application. You can specify the minimum number of instances in each auto scaling group. Amazon EC2 Auto scaling ensure that your group never goes below this size.

**Auto scaling components are:**

* **Groups:** The EC2 instances are organize into groups so that they can be treated as a logical unit for the scaling purpose and management. When you created a group, you specify its minimum, maximum, and desired number of instances.
* **Configuration template:**  You can specify information such as the AMI ID, instance type, key pair, security group, and block device mapping for your instances.
* **Scalling options:**  you can configure a group to scale based on the occurrence of specified conditions (dynamic scaling) or on a schedule.

**Accessing Amazon EC2 Auto scaling**

You can access auto scaling form amazon console by choosing **Auto Scaling Groups** from the navigation panel, you can also access it using the **Amazon EC2 Auto Scalling API** request that you use HTTP verbs **GET** or **POST** and a query parameter named **Action**.

**Amazon Machine Image (AMI)**

Amazon Machine Image (AMI) provides the information required to launch an instance. You must specify an AMI when you launch an instance. You can launch multiples instances from the same AMI when you need multiples instance with the same configuration. You can use different AMI to launch instances when you need instances with different configurations.

An AMI includes:

* **One or more EBS Snapshots,** or for instance-store-backed AMI, a template for the root volume of the instance (for example an operating system, an application server, and application).
* **Launch permission** that controls which AWS account can use the AMI instances.
* **A Block device** mapping that specify the volume to attach to the instance when it’s launched.

After creating an AMI, you can keep it private so that only you can use it, or you can share it with a specified list of AWS accounts. Yu can deregister an AMI when you have finished with it. After deregistered it, it can’t be used to launch new instances.

**Security Groups**

A security group acts as a virtual firewall for your EC2 instance to control incoming and outgoing traffic. When you launch an instance, you can specify one or more security groups. If you don’t specify the security groups Amazon use the default security group.

**Security group rules**

You can add rules to each security group. You can modify the rules for a security group at any time. The rule of security group controls the inbound traffic that allowed to reach the instances that are associated with the security group. The rule also controls the outbound traffic allowed to leave them.

**The characteristics of security groups**

* By default, security group allow all outbound traffic
* Security group rules are always permissive; you can’t create rules that deny access.
* Security groups are stateful. If you send a request from your instance, the response traffic for that request is allowed to flow in regardless of inbound security group rules.
* You can add and remove rules at any time.
* When you associate multiple security groups with an instance, the rule from each security group are effectively aggregated to create one set of rules.

**For each rule you specify the following:**

* **Name:** the name for the security group (for example, my-security-group).
* **Protocol:** most common 6(TCP), 17(UDP), and 1(ICMP).
* **Port Range** for example (7000-8000).
* **ICMP type and code** for ICMP, the ICMP type and code.
* **Source destination:** the source (inbound rules) destination (outbound rules) for traffic.
* **Description(optional):** you can add a description for the rule which can help you identify it later.