AMAZON ASSIGNMENT 3

1. What do you mean by VPC? What do you mean by VPC?

## Ans:-

A virtual private cloud (VPC) is a secure, isolated [private cloud](https://www.cloudflare.com/learning/cloud/what-is-a-private-cloud/) hosted within a [public cloud](https://www.cloudflare.com/learning/cloud/what-is-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. (Not all private clouds are hosted in this fashion.) VPCs combine the scalability and convenience of public cloud computing with the data isolation of private cloud computing.

Imagine a public cloud as a crowded restaurant, and a virtual private cloud as a reserved table in that crowded restaurant. Even though the restaurant is full of people, a table with a "Reserved" sign on it can only be accessed by the party who made the reservation. Similarly, a public cloud is crowded with various cloud customers accessing computing resources – but a VPC reserves some of those resources for use by only one customer

A VPC isolates computing resources from the other computing resources available in the public cloud. The key technologies for isolating a VPC from the rest of the public cloud are:

**Subnets:** A subnet is a range of [IP addresses](https://www.cloudflare.com/learning/dns/glossary/what-is-my-ip-address/) within a network that are reserved so that they're not available to everyone within the network, essentially dividing part of the network for private use. In a VPC these are private IP addresses that are not accessible via the public Internet, unlike typical IP addresses, which are publicly visible.

**VLAN:** A LAN is a local area network, or a group of computing devices that are all connected to each other without the use of the Internet. A VLAN is a virtual LAN. Like a subnet, a VLAN is a way of partitioning a network, but the partitioning takes place at a different layer within the [OSI model](https://www.cloudflare.com/learning/ddos/glossary/open-systems-interconnection-model-osi/) (layer 2 instead of layer 3).

**VPN:** A [virtual private network (VPN)](https://www.cloudflare.com/learning/vpn/what-is-a-vpn/) uses [encryption](https://www.cloudflare.com/learning/ssl/what-is-encryption/) to create a private network over the top of a public network. VPN traffic passes through publicly shared Internet infrastructure – routers, switches, etc. – but the traffic is scrambled and not visible to anyone.

A VPC will have a dedicated subnet and VLAN that are only accessible by the VPC customer. This prevents anyone else within the public cloud from accessing computing resources within the VPC – effectively placing the "Reserved" sign on the table. The VPC customer connects via VPN to their VPC, so that data passing into and out of the VPC is not visible to other public cloud users.

Some VPC providers offer additional customization with:

* **Network Address Translation (NAT):** This feature matches private IP addresses to a public IP address for connections with the public Internet. With NAT, a public-facing website or application could run in a VPC.
* **BGP route configuration:** Some providers allow customers to customize BGP routing tables for connecting their VPC with their other infrastructure. ([Learn how BGP works.](https://www.cloudflare.com/learning/security/glossary/what-is-bgp/))

1. What are the various types of cloud services?

Ans:- loud computing is a broad term which refers to a collection of services that offer businesses a cost-effective solution to increase their IT capacity and functionality.

Depending on their specific requirements, businesses can choose where, when and how they use cloud computing to ensure an efficient and reliable IT solution.

Below we explore the different types of cloud computing, including the three main deployment models and the cloud services that can be hosted within these environments.

## Cloud Deployment Models

There are three main types of cloud environment, also known as cloud deployment models. Businesses can choose to run applications on public, private or hybrid clouds – depending on their specific requirements.

## Public Cloud

A public cloud environment is owned by an outsourced cloud provider and is accessible to many businesses through the internet on a pay-per-use model. This deployment model provides services and infrastructure to businesses who want to save money on IT operational costs, but it’s the cloud provider who is responsible for the creation and maintenance of the resources.

Public clouds are ideal for small and medium sized businesses with a tight budget requiring a quick and easy platform in which to deploy IT resources.

**Pros of a public cloud**

* Easy scalability
* No geographical restrictions
* Cost effective
* Highly reliable
* Easy to manage

**Cons of a public cloud**

* Not considered the safest option for sensitive data

## Private Cloud

This cloud deployment model is a bespoke infrastructure owned by a single business. It offers a more controlled environment in which access to IT resources is more centralised within the business. This model can be externally hosted or can be managed in-house. Although private cloud hosting can be expensive, for larger businesses it can offer a higher level of security and more autonomy to customise the storage, networking and compute components to suit their IT requirements.

**Pros of a private cloud**

* Improved level of security
* Greater control over the server
* Customisable

**Cons of a private cloud**

* Harder to access data from remote locations
* Requires IT expertise

## Hybrid Cloud

For businesses seeking the benefits of both private and public cloud deployment models, a hybrid cloud environment is a good option. By combining the two models, a hybrid cloud model provides a more tailored IT solution that meets specific business requirements.

**Pros of a hybrid cloud**

* Highly flexible and scalable
* Cost effective
* Enhanced security

**Cons of a hybrid cloud**

* Communication in network level may be conflicted as it’s used in both private and public clouds.

## Cloud Services

There are three main service models of cloud computing – Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). There are clear differences between the three and what they can offer a business in terms of storage and resource pooling, but they can also interact with each other to form one comprehensive model of cloud computing.

#### **IaaS (Infrastructure as Service)**

This is the most common service model of cloud computing as it offers the fundamental infrastructure of virtual servers, network, operating systems and data storage drives. It allows for the flexibility, reliability and scalability that many businesses seek with the cloud, and removes the need for hardware in the office. This makes it ideal for small and medium sized organisations looking for a cost-effective IT solution to support business growth. IaaS is a fully outsourced pay-for-use service and is available as a public, private or hybrid infrastructure.

#### **PaaS (Platform-as-a-Service)**

This is where cloud computing providers deploy the infrastructure and software framework, but businesses can develop and run their own applications. Web applications can be created quickly and easily via PaaS, and the service is flexible and robust enough to support them. PaaS solutions are scalable and ideal for business environments where multiple developers are working on a single project. It is also handy for situations where an existing data source (such as CRM tool) needs to be leveraged.

#### **SaaS (Software as a Service)**

This cloud computing solution involves the deployment of software over the internet to variousbusinesses who pay via subscription or a pay-per-use model. It is a valuable tool for CRM and for applications that need a lot of web or mobile access – such as mobile sales management software. SaaS is managed from a central location so businesses don’t have to worry about maintaining it themselves, and is ideal for short-term projects.

##### **If you’re considering cloud computing for your business, take a look at our**[Cloud Computing](https://www.leadingedgetech.co.uk/it-consultancy-services/cloud-computing/)**page to find out how we can help.**

3) What do you mean by S3 bucket?

Ans:- Amazon Simple Storage Service (Amazon S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance. Customers of all sizes and industries can use Amazon S3 to store and protect any amount of data for a range of use cases, such as data lakes, websites, mobile applications, backup and restore, archive, enterprise applications, IoT devices, and big data analytics. Amazon S3 provides management features so that you can optimize, organize, and configure access to your data to meet your specific business, organizational, and compliance requirements.

**Topics**

* [Features of Amazon S3](https://docs.aws.amazon.com/AmazonS3/latest/userguide/Welcome.html#S3Features)
* [How Amazon S3 works](https://docs.aws.amazon.com/AmazonS3/latest/userguide/Welcome.html#CoreConcepts)
* [Amazon S3 data consistency model](https://docs.aws.amazon.com/AmazonS3/latest/userguide/Welcome.html#ConsistencyModel)
* [Related services](https://docs.aws.amazon.com/AmazonS3/latest/userguide/Welcome.html#RelatedAmazonWebServices)
* [Accessing Amazon S3](https://docs.aws.amazon.com/AmazonS3/latest/userguide/Welcome.html#API)
* [Paying for Amazon S3](https://docs.aws.amazon.com/AmazonS3/latest/userguide/Welcome.html#PayingforStorage)
* [PCI DSS compliance](https://docs.aws.amazon.com/AmazonS3/latest/userguide/Welcome.html#pci-dss-compliance)

## Features of Amazon S3

### Storage classes

Amazon S3 offers a range of storage classes designed for different use cases. For example, you can store mission-critical production data in S3 Standard for frequent access, save costs by storing infrequently accessed data in S3 Standard-IA or S3 One Zone-IA, and archive data at the lowest costs in S3 Glacier Instant Retrieval, S3 Glacier Flexible Retrieval, and S3 Glacier Deep Archive.

You can store data with changing or unknown access patterns in S3 Intelligent-Tiering, which optimizes storage costs by automatically moving your data between four access tiers when your access patterns change. These four access tiers include two low-latency access tiers optimized for frequent and infrequent access, and two opt-in archive access tiers designed for asynchronous access for rarely accessed data.

For more information, see [Using Amazon S3 storage classes](https://docs.aws.amazon.com/AmazonS3/latest/userguide/storage-class-intro.html). For more information about S3 Glacier Flexible Retrieval, see the [Amazon S3 Glacier Developer Guide](https://docs.aws.amazon.com/amazonglacier/latest/dev/introduction.html).

### Storage management

Amazon S3 has storage management features that you can use to manage costs, meet regulatory requirements, reduce latency, and save multiple distinct copies of your data for compliance requirements.

* [S3 Lifecycle](https://docs.aws.amazon.com/AmazonS3/latest/userguide/object-lifecycle-mgmt.html) – Configure a lifecycle policy to manage your objects and store them cost effectively throughout their lifecycle. You can transition objects to other S3 storage classes or expire objects that reach the end of their lifetimes.
* [S3 Object Lock](https://docs.aws.amazon.com/AmazonS3/latest/userguide/object-lock.html) – Prevent Amazon S3 objects from being deleted or overwritten for a fixed amount of time or indefinitely. You can use Object Lock to help meet regulatory requirements that require write-once-read-many (WORM) storage or to simply add another layer of protection against object changes and deletions.
* [S3 Replication](https://docs.aws.amazon.com/AmazonS3/latest/userguide/replication.html) – Replicate objects and their respective metadata and object tags to one or more destination buckets in the same or different AWS Regions for reduced latency, compliance, security, and other use cases.
* [S3 Batch Operations](https://docs.aws.amazon.com/AmazonS3/latest/userguide/batch-ops.html) – Manage billions of objects at scale with a single S3 API request or a few clicks in the Amazon S3 console. You can use Batch Operations to perform operations such as **Copy**, **Invoke AWS Lambda function**, and **Restore** on millions or billions of objects.

### Access management

Amazon S3 provides features for auditing and managing access to your buckets and objects. By default, S3 buckets and the objects in them are private. You have access only to the S3 resources that you create. To grant granular resource permissions that support your specific use case or to audit the permissions of your Amazon S3 resources, you can use the following features.

* [S3 Block Public Access](https://docs.aws.amazon.com/AmazonS3/latest/userguide/access-control-block-public-access.html) – Block public access to S3 buckets and objects. By default, Block Public Access settings are turned on at the account and bucket level.
* [AWS Identity and Access Management (IAM)](https://docs.aws.amazon.com/AmazonS3/latest/userguide/s3-access-control.html) – Create IAM users for your AWS account to manage access to your Amazon S3 resources. For example, you can use IAM with Amazon S3 to control the type of access a user or group of users has to an S3 bucket that your AWS account owns.
* [Bucket policies](https://docs.aws.amazon.com/AmazonS3/latest/userguide/bucket-policies.html) – Use IAM-based policy language to configure resource-based permissions for your S3 buckets and the objects in them.
* [Amazon S3 access points](https://docs.aws.amazon.com/AmazonS3/latest/userguide/access-points.html) – Configure named network endpoints with dedicated access policies to manage data access at scale for shared datasets in Amazon S3.
* [Access control lists (ACLs)](https://docs.aws.amazon.com/AmazonS3/latest/userguide/acls.html) – Grant read and write permissions for individual buckets and objects to authorized users. As a general rule, we recommend using S3 resource-based policies (bucket policies and access point policies) or IAM policies for access control instead of ACLs. ACLs are an access control mechanism that predates resource-based policies and IAM. For more information about when you'd use ACLs instead of resource-based policies or IAM policies, see [Access policy guidelines](https://docs.aws.amazon.com/AmazonS3/latest/userguide/access-policy-alternatives-guidelines.html).
* [S3 Object Ownership](https://docs.aws.amazon.com/AmazonS3/latest/userguide/about-object-ownership.html) – Disable ACLs and take ownership of every object in your bucket, simplifying access management for data stored in Amazon S3. You, as the bucket owner, automatically own and have full control over every object in your bucket, and access control for your data is based on policies.
* [Access Analyzer for S3](https://docs.aws.amazon.com/AmazonS3/latest/userguide/access-analyzer.html) – Evaluate and monitor your S3 bucket access policies, ensuring that the policies provide only the intended access to your S3 resources.

### Data processing

To transform data and trigger workflows to automate a variety of other processing activities at scale, you can use the following features.

* [S3 Object Lambda](https://docs.aws.amazon.com/AmazonS3/latest/userguide/transforming-objects.html) – Add your own code to S3 GET requests to modify and process data as it is returned to an application. Filter rows, dynamically resize images, redact confidential data, and much more.
* [Event notifications](https://docs.aws.amazon.com/AmazonS3/latest/userguide/NotificationHowTo.html) – Trigger workflows that use Amazon Simple Notification Service (Amazon SNS), Amazon Simple Queue Service (Amazon SQS), and AWS Lambda when a change is made to your S3 resources.

### Storage logging and monitoring

Amazon S3 provides logging and monitoring tools that you can use to monitor and control how your Amazon S3 resources are being used. For more information, see [Monitoring tools](https://docs.aws.amazon.com/AmazonS3/latest/userguide/monitoring-automated-manual.html).

**Automated monitoring tools**

* [Amazon CloudWatch metrics for Amazon S3](https://docs.aws.amazon.com/AmazonS3/latest/userguide/cloudwatch-monitoring.html)– Track the operational health of your S3 resources and configure billing alerts when estimated charges reach a user-defined threshold.
* [AWS CloudTrail](https://docs.aws.amazon.com/AmazonS3/latest/userguide/cloudtrail-logging.html) – Record actions taken by a user, a role, or an AWS service in Amazon S3. CloudTrail logs provide you with detailed API tracking for S3 bucket-level and object-level operations.

**Manual monitoring tools**

* [Server access logging](https://docs.aws.amazon.com/AmazonS3/latest/userguide/ServerLogs.html) – Get detailed records for the requests that are made to a bucket. You can use server access logs for many use cases, such as conducting security and access audits, learning about your customer base, and understanding your Amazon S3 bill.
* [AWS Trusted Advisor](https://docs.aws.amazon.com/awssupport/latest/user/trusted-advisor.html) – Evaluate your account by using AWS best practice checks to identify ways to optimize your AWS infrastructure, improve security and performance, reduce costs, and monitor service quotas. You can then follow the recommendations to optimize your services and resources.

### Analytics and insights

Amazon S3 offers features to help you gain visibility into your storage usage, which empowers you to better understand, analyze, and optimize your storage at scale.

* [Amazon S3 Storage Lens](https://docs.aws.amazon.com/AmazonS3/latest/userguide/storage_lens.html) – Understand, analyze, and optimize your storage. S3 Storage Lens provides 29+ usage and activity metrics and interactive dashboards to aggregate data for your entire organization, specific accounts, AWS Regions, buckets, or prefixes.
* [Storage Class Analysis](https://docs.aws.amazon.com/AmazonS3/latest/userguide/analytics-storage-class.html) – Analyze storage access patterns to decide when it's time to move data to a more cost-effective storage class.
* [S3 Inventory with Inventory reports](https://docs.aws.amazon.com/AmazonS3/latest/userguide/storage-inventory.html) – Audit and report on objects and their corresponding metadata and configure other Amazon S3 features to take action in Inventory reports. For example, you can report on the replication and encryption status of your objects. For a list of all the metadata available for each object in Inventory reports, see [Amazon S3 Inventory list](https://docs.aws.amazon.com/AmazonS3/latest/userguide/storage-inventory.html#storage-inventory-contents).

### Strong consistency

Amazon S3 provides strong read-after-write consistency for PUT and DELETE requests of objects in your Amazon S3 bucket in all AWS Regions. This behavior applies to both writes of new objects as well as PUT requests that overwrite existing objects and DELETE requests. In addition, read operations on Amazon S3 Select, Amazon S3 access control lists (ACLs), Amazon S3 Object Tags, and object metadata (for example, the HEAD object) are strongly consistent. For more information, see [Amazon S3 data consistency model](https://docs.aws.amazon.com/AmazonS3/latest/userguide/Welcome.html#ConsistencyModel).

## How Amazon S3 works

Amazon S3 is an object storage service that stores data as objects within buckets. An object is a file and any metadata that describes the file. A bucket is a container for objects.

To store your data in Amazon S3, you first create a bucket and specify a bucket name and AWS Region. Then, you upload your data to that bucket as objects in Amazon S3. Each object has a key (or key name), which is the unique identifier for the object within the bucket.

S3 provides features that you can configure to support your specific use case. For example, you can use S3 Versioning to keep multiple versions of an object in the same bucket, which allows you to restore objects that are accidentally deleted or overwritten.

Buckets and the objects in them are private and can be accessed only if you explicitly grant access permissions. You can use bucket policies, AWS Identity and Access Management (IAM) policies, access control lists (ACLs), and S3 Access Points to manage access.

4)List the different types of Instances.

Ans:- **The instance types can be broadly classified into five different categories as follows.**

* General Purpose.
* Compute-Optimized.
* Memory-Optimized.
* Storage-Optimized.
* Accelerated Computing.

When you launch an instance, the instance type that you specify determines the hardware of the host computer used for your instance. Each instance type offers different compute, memory, and storage capabilities, and is grouped in an instance family based on these capabilities. Select an instance type based on the requirements of the application or software that you plan to run on your instance.

Amazon EC2 provides each instance with a consistent and predictable amount of CPU capacity, regardless of its underlying hardware.

Amazon EC2 dedicates some resources of the host computer, such as CPU, memory, and instance storage, to a particular instance. Amazon EC2 shares other resources of the host computer, such as the network and the disk subsystem, among instances. If each instance on a host computer tries to use as much of one of these shared resources as possible, each receives an equal share of that resource. However, when a resource is underused, an instance can consume a higher share of that resource while it's available.

Each instance type provides higher or lower minimum performance from a shared resource. For example, instance types with high I/O performance have a larger allocation of shared resources. Allocating a larger share of shared resources also reduces the variance of I/O performance. For most applications, moderate I/O performance is more than enough. However, for applications that require greater or more consistent I/O performance, consider an instance type with higher I/O performance.

**Contents**

* [Available instance types](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/instance-types.html#AvailableInstanceTypes)
* [Hardware specifications](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/instance-types.html#instance-hardware-specs)
* [AMI virtualization types](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/instance-types.html#instance-virtualization-type)
* [Instances built on the Nitro System](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/instance-types.html#ec2-nitro-instances)
* [Networking and storage features](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/instance-types.html#instance-networking-storage)
* [Instance limits](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/instance-types.html#instance-type-limits)
* [General purpose instances](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/general-purpose-instances.html)
* [Compute optimized instances](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/compute-optimized-instances.html)
* [Memory optimized instances](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/memory-optimized-instances.html)
* [Storage optimized instances](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/storage-optimized-instances.html)
* [Linux accelerated computing instances](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/accelerated-computing-instances.html)
* [Find an Amazon EC2 instance type](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/instance-discovery.html)
* [Get recommendations for an instance type](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-recommendations.html)
* [Change the instance type](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-resize.html)

## Available instance types

Amazon EC2 provides a wide selection of instance types optimized for different use cases. To determine which instance types meet your requirements, such as supported Regions, compute resources, or storage resources, see [Find an Amazon EC2 instance type](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/instance-discovery.html).

### Current generation instances

For the best performance, we recommend that you use the following instance types when you launch new instances. For more information, see [Amazon EC2 Instance Types](http://aws.amazon.com/ec2/instance-types/).

| **Type** | **Sizes** | **Use case** |
| --- | --- | --- |
| C4 | c4.large | c4.xlarge | c4.2xlarge | c4.4xlarge | c4.8xlarge | [Compute optimized](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/compute-optimized-instances.html) |
| C5 | c5.large | c5.xlarge | c5.2xlarge | c5.4xlarge | c5.9xlarge | c5.12xlarge | c5.18xlarge | c5.24xlarge | c5.metal | [Compute optimized](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/compute-optimized-instances.html) |
| C5a | c5a.large | c5a.xlarge | c5a.2xlarge | c5a.4xlarge | c5a.8xlarge | c5a.12xlarge | c5a.16xlarge | c5a.24xlarge | [Compute optimized](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/compute-optimized-instances.html) |
| C5ad | c5ad.large | c5ad.xlarge | c5ad.2xlarge | c5ad.4xlarge | c5ad.8xlarge | c5ad.12xlarge | c5ad.16xlarge | c5ad.24xlarge | [Compute optimized](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/compute-optimized-instances.html) |
| C5d | c5d.large | c5d.xlarge | c5d.2xlarge | c5d.4xlarge | c5d.9xlarge | c5d.12xlarge | c5d.18xlarge | c5d.24xlarge | c5d.metal | [Compute optimized](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/compute-optimized-instances.html) |
| C5n | c5n.large | c5n.xlarge | c5n.2xlarge | c5n.4xlarge | c5n.9xlarge | c5n.18xlarge | c5n.metal | [Compute optimized](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/compute-optimized-instances.html) |
| C6a | c6a.large | c6a.xlarge | c6a.2xlarge | c6a.4xlarge | c6a.8xlarge | c6a.12xlarge | c6a.16xlarge | c6a.24xlarge | c6a.32xlarge | c6a.48xlarge | c6a.metal | [Compute optimized](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/compute-optimized-instances.html) |
| C6g | c6g.medium | c6g.large | c6g.xlarge | c6g.2xlarge | c6g.4xlarge | c6g.8xlarge | c6g.12xlarge | c6g.16xlarge | c6g.metal | [Compute optimized](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/compute-optimized-instances.html) |
| C6gd | c6gd.medium | c6gd.large | c6gd.xlarge | c6gd.2xlarge | c6gd.4xlarge | c6gd.8xlarge | c6gd.12xlarge | c6gd.16xlarge | c6gd.metal | [Compute optimized](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/compute-optimized-instances.html) |
| C6gn | c6gn.medium | c6gn.large | c6gn.xlarge | c6gn.2xlarge | c6gn.4xlarge | c6gn.8xlarge | c6gn.12xlarge | c6gn.16xlarge | [Compute optimized](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/compute-optimized-instances.html) |
| C6i | c6i.large | c6i.xlarge | c6i.2xlarge | c6i.4xlarge | c6i.8xlarge | c6i.12xlarge | c6i.16xlarge | c6i.24xlarge | c6i.32xlarge | c6i.metal | [Compute optimized](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/compute-optimized-instances.html) |
| C6id | c6id.large | c6id.xlarge | c6id.2xlarge | c6id.4xlarge | c6id.8xlarge | c6id.12xlarge | c6id.16xlarge | c6id.24xlarge | c6id.32xlarge | c6id.metal | [Compute optimized](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/compute-optimized-instances.html) |
| C7g | c7g.medium | c7g.large | c7g.xlarge | c7g.2xlarge | c7g.4xlarge | c7g.8xlarge | c7g.12xlarge | c7g.16xlarge | [Compute optimized](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/compute-optimized-instances.html) |
| D2 | d2.xlarge | d2.2xlarge | d2.4xlarge | d2.8xlarge | [Storage optimized](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/storage-optimized-instances.html) |
| D3 | d3.xlarge | d3.2xlarge | d3.4xlarge | d3.8xlarge | [Storage optimized](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/storage-optimized-instances.html) |
| D3en | d3en.large | d3en.xlarge | d3en.2xlarge | d3en.4xlarge | d3en.6xlarge | d3en.8xlarge | d3en.12xlarge | [Storage optimized](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/storage-optimized-instances.html) |
| DL1 | dl1.24xlarge | [Accelerated computing](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/accelerated-computing-instances.html) |
| F1 | f1.2xlarge | f1.4xlarge | f1.16xlarge | [Accelerated computing](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/accelerated-computing-instances.html) |
| G3 | g3s.xlarge | g3.4xlarge | g3.8xlarge | g3.16xlarge | [Accelerated computing](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/accelerated-computing-instances.html) |
| G4ad | g4ad.xlarge | g4ad.2xlarge | g4ad.4xlarge | g4ad.8xlarge | g4ad.16xlarge | [Accelerated computing](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/accelerated-computing-instances.html) |
| G4dn | g4dn.xlarge | g4dn.2xlarge | g4dn.4xlarge | g4dn.8xlarge | g4dn.12xlarge | g4dn.16xlarge | g4dn.metal | [Accelerated computing](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/accelerated-computing-instances.html) |
| G5 | g5.xlarge | g5.2xlarge | g5.4xlarge | g5.8xlarge | g5.12xlarge | g5.16xlarge | g5.24xlarge | g5.48xlarge | [Accelerated computing](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/accelerated-computing-instances.html) |
| G5g | g5g.xlarge | g5g.2xlarge | g5g.4xlarge | g5g.8xlarge | g5g.16xlarge | g5g.metal | [Accelerated computing](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/accelerated-computing-instances.html) |
| H1 | h1.2xlarge | h1.4xlarge | h1.8xlarge | h1.16xlarge | [Storage optimized](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/storage-optimized-instances.html) |
| Hpc6a | hpc6a.48xlarge | [Compute optimized](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/compute-optimized-instances.html) |
| I3 | i3.large | i3.xlarge | i3.2xlarge | i3.4xlarge | i3.8xlarge | i3.16xlarge | i3.metal | [Storage optimized](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/storage-optimized-instances.html) |
| I3en | i3en.large | i3en.xlarge | i3en.2xlarge | i3en.3xlarge | i3en.6xlarge | i3en.12xlarge | i3en.24xlarge | i3en.metal | [Storage optimized](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/storage-optimized-instances.html) |
| I4i | i4i.large | i4i.xlarge | i4i.2xlarge | i4i.4xlarge | i4i.8xlarge | i4i.16xlarge | i4i.32xlarge | i4i.metal | [Storage optimized](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/storage-optimized-instances.html) |
| Im4gn | im4gn.large | im4gn.xlarge | im4gn.2xlarge | im4gn.4xlarge | im4gn.8xlarge | im4gn.16xlarge | [Storage optimized](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/storage-optimized-instances.html) |
| Inf1 | inf1.xlarge | inf1.2xlarge | inf1.6xlarge | inf1.24xlarge | [Accelerated computing](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/accelerated-computing-instances.html) |
| Is4gen | is4gen.medium | is4gen.large | is4gen.xlarge | is4gen.2xlarge | is4gen.4xlarge | is4gen.8xlarge | [Storage optimized](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/storage-optimized-instances.html) |
| M4 | m4.large | m4.xlarge | m4.2xlarge | m4.4xlarge | m4.10xlarge | m4.16xlarge | [General purpose](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/general-purpose-instances.html) |
| M5 | m5.large | m5.xlarge | m5.2xlarge | m5.4xlarge | m5.8xlarge | m5.12xlarge | m5.16xlarge | m5.24xlarge | m5.metal | [General purpose](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/general-purpose-instances.html) |
| M5a | m5a.large | m5a.xlarge | m5a.2xlarge | m5a.4xlarge | m5a.8xlarge | m5a.12xlarge | m5a.16xlarge | m5a.24xlarge | [General purpose](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/general-purpose-instances.html) |
| M5ad | m5ad.large | m5ad.xlarge | m5ad.2xlarge | m5ad.4xlarge | m5ad.8xlarge | m5ad.12xlarge | m5ad.16xlarge | m5ad.24xlarge | [General purpose](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/general-purpose-instances.html) |
| M5d | m5d.large | m5d.xlarge | m5d.2xlarge | m5d.4xlarge | m5d.8xlarge | m5d.12xlarge | m5d.16xlarge | m5d.24xlarge | m5d.metal | [General purpose](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/general-purpose-instances.html) |
| M5dn | m5dn.large | m5dn.xlarge | m5dn.2xlarge | m5dn.4xlarge | m5dn.8xlarge | m5dn.12xlarge | m5dn.16xlarge | m5dn.24xlarge | m5dn.metal | [General purpose](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/general-purpose-instances.html) |
| M5n | m5n.large | m5n.xlarge | m5n.2xlarge | m5n.4xlarge | m5n.8xlarge | m5n.12xlarge | m5n.16xlarge | m5n.24xlarge | m5n.metal | [General purpose](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/general-purpose-instances.html) |
| M5zn | m5zn.large | m5zn.xlarge | m5zn.2xlarge | m5zn.3xlarge | m5zn.6xlarge | m5zn.12xlarge | m5zn.metal | [General purpose](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/general-purpose-instances.html) |
| M6a | m6a.large | m6a.xlarge | m6a.2xlarge | m6a.4xlarge | m6a.8xlarge | m6a.12xlarge | m6a.16xlarge | m6a.24xlarge | m6a.32xlarge | m6a.48xlarge | m6a.metal | [General purpose](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/general-purpose-instances.html) |
| M6g | m6g.medium | m6g.large | m6g.xlarge | m6g.2xlarge | m6g.4xlarge | m6g.8xlarge | m6g.12xlarge | m6g.16xlarge | m6g.metal | [General purpose](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/general-purpose-instances.html) |
| M6gd | m6gd.medium | m6gd.large | m6gd.xlarge | m6gd.2xlarge | m6gd.4xlarge | m6gd.8xlarge | m6gd.12xlarge | m6gd.16xlarge | m6gd.metal | [General purpose](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/general-purpose-instances.html) |
| M6i | m6i.large | m6i.xlarge | m6i.2xlarge | m6i.4xlarge | m6i.8xlarge | m6i.12xlarge | m6i.16xlarge | m6i.24xlarge | m6i.32xlarge | m6i.metal | [General purpose](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/general-purpose-instances.html) |
| M6id | m6id.large | m6id.xlarge | m6id.2xlarge | m6id.4xlarge | m6id.8xlarge | m6id.12xlarge | m6id.16xlarge | m6id.24xlarge | m6id.32xlarge | m6id.metal | [General purpose](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/general-purpose-instances.html) |
| Mac1 | mac1.metal | [General purpose](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/general-purpose-instances.html) |
| P2 | p2.xlarge | p2.8xlarge | p2.16xlarge | [Accelerated computing](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/accelerated-computing-instances.html) |
| P3 | p3.2xlarge | p3.8xlarge | p3.16xlarge | [Accelerated computing](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/accelerated-computing-instances.html) |
| P3dn | p3dn.24xlarge | [Accelerated computing](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/accelerated-computing-instances.html) |
| P4d | p4d.24xlarge | [Accelerated computing](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/accelerated-computing-instances.html) |
| P4de | p4de.24xlarge | [Accelerated computing](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/accelerated-computing-instances.html) |
| R4 | r4.large | r4.xlarge | r4.2xlarge | r4.4xlarge | r4.8xlarge | r4.16xlarge | [Memory optimized](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/memory-optimized-instances.html) |
| R5 | r5.large | r5.xlarge | r5.2xlarge | r5.4xlarge | r5.8xlarge | r5.12xlarge | r5.16xlarge | r5.24xlarge | r5.metal | [Memory optimized](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/memory-optimized-instances.html) |
| R5a | r5a.large | r5a.xlarge | r5a.2xlarge | r5a.4xlarge | r5a.8xlarge | r5a.12xlarge | r5a.16xlarge | r5a.24xlarge | [Memory optimized](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/memory-optimized-instances.html) |
| R5ad | r5ad.large | r5ad.xlarge | r5ad.2xlarge | r5ad.4xlarge | r5ad.8xlarge | r5ad.12xlarge | r5ad.16xlarge | r5ad.24xlarge | [Memory optimized](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/memory-optimized-instances.html) |
| R5b | r5b.large | r5b.xlarge | r5b.2xlarge | r5b.4xlarge | r5b.8xlarge | r5b.12xlarge | r5b.16xlarge | r5b.24xlarge | r5b.metal | [Memory optimized](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/memory-optimized-instances.html) |
| R5d | r5d.large | r5d.xlarge | r5d.2xlarge | r5d.4xlarge | r5d.8xlarge | r5d.12xlarge | r5d.16xlarge | r5d.24xlarge | r5d.metal | [Memory optimized](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/memory-optimized-instances.html) |
| R5dn | r5dn.large | r5dn.xlarge | r5dn.2xlarge | r5dn.4xlarge | r5dn.8xlarge | r5dn.12xlarge | r5dn.16xlarge | r5dn.24xlarge | r5dn.metal | [Memory optimized](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/memory-optimized-instances.html) |
| R5n | r5n.large | r5n.xlarge | r5n.2xlarge | r5n.4xlarge | r5n.8xlarge | r5n.12xlarge | r5n.16xlarge | r5n.24xlarge | r5n.metal | [Memory optimized](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/memory-optimized-instances.html) |
| R6g | r6g.medium | r6g.large | r6g.xlarge | r6g.2xlarge | r6g.4xlarge | r6g.8xlarge | r6g.12xlarge | r6g.16xlarge | r6g.metal | [Memory optimized](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/memory-optimized-instances.html) |
| R6gd | r6gd.medium | r6gd.large | r6gd.xlarge | r6gd.2xlarge | r6gd.4xlarge | r6gd.8xlarge | r6gd.12xlarge | r6gd.16xlarge | r6gd.metal | [Memory optimized](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/memory-optimized-instances.html) |
| R6i | r6i.large | r6i.xlarge | r6i.2xlarge | r6i.4xlarge | r6i.8xlarge | r6i.12xlarge | r6i.16xlarge | r6i.24xlarge | r6i.32xlarge | r6i.metal | [Memory optimized](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/memory-optimized-instances.html) |
| T2 | t2.nano | t2.micro | t2.small | t2.medium | t2.large | t2.xlarge | t2.2xlarge | [General purpose](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/general-purpose-instances.html) |
| T3 | t3.nano | t3.micro | t3.small | t3.medium | t3.large | t3.xlarge | t3.2xlarge | [General purpose](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/general-purpose-instances.html) |
| T3a | t3a.nano | t3a.micro | t3a.small | t3a.medium | t3a.large | t3a.xlarge | t3a.2xlarge | [General purpose](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/general-purpose-instances.html) |
| T4g | t4g.nano | t4g.micro | t4g.small | t4g.medium | t4g.large | t4g.xlarge | t4g.2xlarge | [General purpose](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/general-purpose-instances.html) |
| High memory (u-\*) | u-3tb1.56xlarge | u-6tb1.56xlarge | u-6tb1.112xlarge | u-6tb1.metal | u-9tb1.112xlarge | u-9tb1.metal | u-12tb1.112xlarge | u-12tb1.metal | u-18tb1.metal | u-24tb1.metal | [Memory optimized](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/memory-optimized-instances.html) |
| VT1 | vt1.3xlarge | vt1.6xlarge | vt1.24xlarge | [Accelerated computing](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/accelerated-computing-instances.html) |
| X1 | x1.16xlarge | x1.32xlarge | [Memory optimized](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/memory-optimized-instances.html) |
| X1e | x1e.xlarge | x1e.2xlarge | x1e.4xlarge | x1e.8xlarge | x1e.16xlarge | x1e.32xlarge | [Memory optimized](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/memory-optimized-instances.html) |
| X2gd | x2gd.medium | x2gd.large | x2gd.xlarge | x2gd.2xlarge | x2gd.4xlarge | x2gd.8xlarge | x2gd.12xlarge | x2gd.16xlarge | x2gd.metal | [Memory optimized](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/memory-optimized-instances.html) |
| X2idn | x2idn.16xlarge | x2idn.24xlarge | x2idn.32xlarge | x2idn.metal | [Memory optimized](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/memory-optimized-instances.html) |
| X2iedn | x2iedn.xlarge | x2iedn.2xlarge | x2iedn.4xlarge | x2iedn.8xlarge | x2iedn.16xlarge | x2iedn.24xlarge | x2iedn.32xlarge | x2iedn.metal | [Memory optimized](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/memory-optimized-instances.html) |
| X2iezn | x2iezn.2xlarge | x2iezn.4xlarge | x2iezn.6xlarge | x2iezn.8xlarge | x2iezn.12xlarge | x2iezn.metal | [Memory optimized](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/memory-optimized-instances.html) |
| z1d | z1d.large | z1d.xlarge | z1d.2xlarge | z1d.3xlarge | z1d.6xlarge | z1d.12xlarge | z1d.metal | [Memory optimized](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/memory-optimized-instances.html) |

### Previous generation instances

Amazon Web Services offers previous generation instance types for users who have optimized their applications around them and have yet to upgrade. We encourage you to use current generation instance types to get the best performance, but we continue to support the following previous generation instance types. For more information about which current generation instance type would be a suitable upgrade, see [Previous Generation Instances](https://aws.amazon.com/ec2/previous-generation/).

| **Type** | **Sizes** |
| --- | --- |
| A1 | a1.medium | a1.large | a1.xlarge | a1.2xlarge | a1.4xlarge | a1.metal |
| C1 | c1.medium | c1.xlarge |
| C3 | c3.large | c3.xlarge | c3.2xlarge | c3.4xlarge | c3.8xlarge |
| G2 | g2.2xlarge | g2.8xlarge |
| I2 | i2.xlarge | i2.2xlarge | i2.4xlarge | i2.8xlarge |
| M1 | m1.small | m1.medium | m1.large | m1.xlarge |
| M2 | m2.xlarge | m2.2xlarge | m2.4xlarge |
| M3 | m3.medium | m3.large | m3.xlarge | m3.2xlarge |
| R3 | r3.large | r3.xlarge | r3.2xlarge | r3.4xlarge | r3.8xlarge |
| T1 | t1.micro |

5) What do you mean by security group?

#### Ans:- **Introduction to AWS Security Groups**

Amazon web services provide a wide range of IT infrastructure, on-demand, and scalable cloud computing services. As such, many clients will tend to trust the platform if it allows for some level of security regarding cloud workloads and projects — and where network traffic can be filtered appropriately.

To maintain and provide this level of security, AWS is built with security groups that support some degree of control of network traffic associated with EC2 instances.

A security group is an AWS firewall solution that performs one primary function: to filter incoming and outgoing traffic from an EC2 instance. It accomplishes this filtering function at the TCP and IP layers, via their respective ports, and source/destination IP addresses.

#### **The Function of Security Groups**

Every Security Group works in a similar fashion to a firewall as it carries a set of rules that filter traffic entering and leaving the EC2 instances. As said earlier, security groups are associated with the EC2 instances and offer protection at the ports and protocol access level. Typically, the firewall possesses a ‘Deny rule,’ but the SG has a “Deny All” that allows data packets to be dropped if no rule is assigned to them from the source IP.

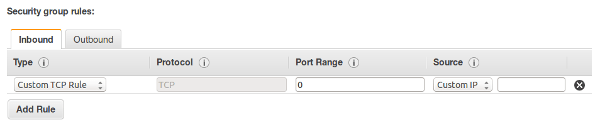
Also, when compared to a Network Access Control List (NACL), security groups form the first layer of defense at the instance level in a cloud computing environment whereas NACLs provides a second layer of protection at the subnet level.

When creating a security group, each group will be assigned to a particular virtual private cloud VPC. It’s also an excellent approach to give each group a name and description for easy access from the account menus. It’s also important to note that when creating a security group, you should ensure that it is assigned to the VPC it’s meant to protect to avoid errors.

#### **Rules guiding AWS Security Groups**

AWS Security Groups have a set of rules that filter traffic in two ways: inbound and outbound. Since AWS security groups are assigned differently, you won’t be needing the same rules for both inbound and outbound traffic. Thus, any provision that permits traffic into the EC2 instance will ultimately filter outbound traffic.

To further break this down each rule is made up of four principal components: Type, Protocol, Port Range, and Source. There is also a space for a description as well.



**The rule** allows for selection of the common type of protocols such as HTTP, SSH, etc., and it opens a drop-down menu were all the protocols are listed.

**Protocols** are automatically selected to be the TCP. However, it can be changed to UDP, ICMP as well as assigns a corresponding association to IPv4 or IPv6.

**Port Range** is also pre-filled, but you can decide to choose the port range of your choice depending on the protocol. Nonetheless, there will be times when you will have to use the custom port range number. A selection of ICMP will grey out the port selection option as it is not a layer 4 protocol.

**Source (custom IP)** this can be a particular IP address or a subnet range. However, you can grant access using the anywhere source IP (0.0.0.0/0) value. Allowing access through the anywhere source can turn out to be a mistake every AWS user should avoid. It will be a discussion in the best practices section below.

#### **Some Tips on Configuring Security Groups:**

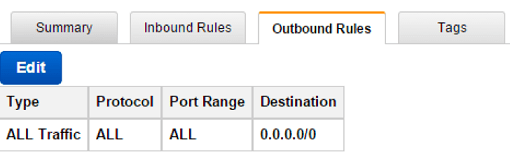
##### **1. Avoid incoming traffic through (0.0.0.0/0).**

One common mistake is to allow inbound traffic from (0.0.0.0/0). It could end up exposing sensitive cloud information to outside threats. Though the security group performs its initial layer filtering when all inbound traffic is allowed but ultimately allows for many risks during the process.



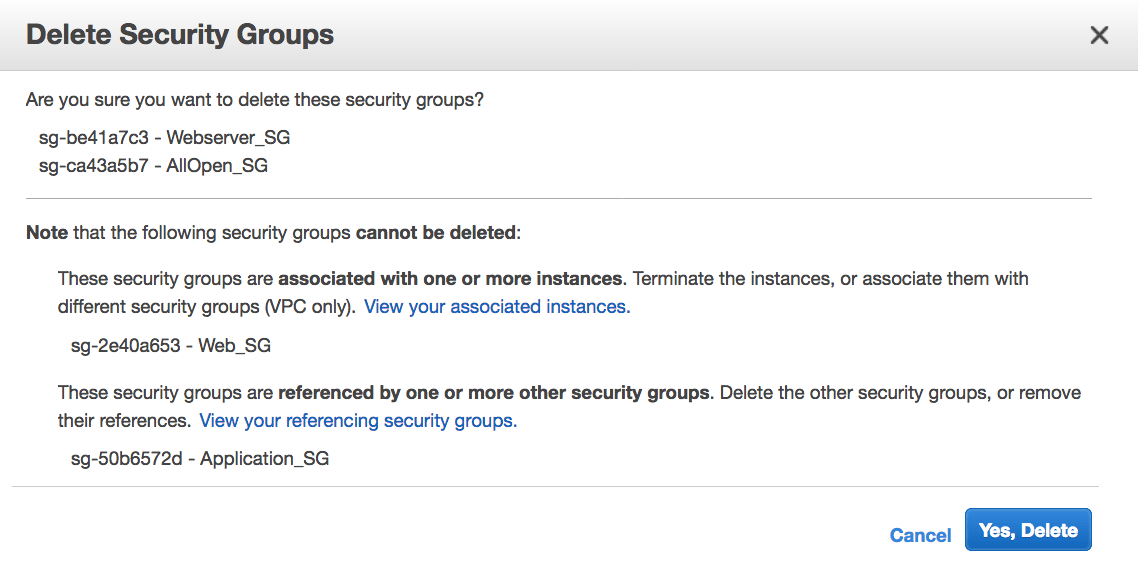
Avoid opening the floodgates to the entire internet

The best thing to do is permit only necessary IP ranges and their respective ports to send incoming traffic, and all other connection attempts will be dropped. When working with EC2 instances, all workloads are only exposed based on the implemented rules of the Security Group applied to that instance.



##### **2. Delete unused security groups**

There is no need to keep a security group not assigned to an EC2 instance. Ensure that all unused SG’s are deleted to keep the working environment clean and less at risk to link the AWS to the outside world.



##### **3. Enable Tracking and Alerting**

AWS comes with some unique set of tools that allows its user to keep track of working information. The [AWS Cloudtrail](https://aws.amazon.com/cloudtrail/) is a cloud tool that enforces the compliance of AWS.

It’s apparent that the right deployment of Security Groups and Network access control lists will go a long way in providing first and second layer form of security for an AWS  account.