 The AutoScaling launch configuration does not incur any charges.

--

You can control network traffic in AWS by configuring security groups, network access control lists, and route tables.

1- Security groups: Act as a firewall for associated Amazon EC2 instances, controlling both inbound and outbound traffic at the instance level.

2- Network access control lists (ACLs): Act as a firewall for associated subnets, controlling both inbound and outbound traffic at the subnet level.

3- Route Tables: A route table contains a set of rules, called routes, that are used to determine where network traffic is directed.

* + Security groups are stateful so if you allow traffic to pass through, the return traffic is automatically allowed even if no rule matches the traffic
  + A Security Group only supports allow rules
  + Network ACLs are stateless so you must create rules in both directions to allow traffic through
  + A Network ACL supports allow and deny rules. You can create a deny rule specifying a specific IP address that you would like to block

--

AWS Transit Gateway is a network transit hub that customers can use to interconnect their virtual private clouds (VPCs) and their on-premises networks.  AWS Transit Gateway is a network transit hub that simplifies how customers interconnect all of their VPCs, across thousands of AWS accounts and into their on-premises networks. Customers can easily and quickly connect into a single centrally-managed gateway, and rapidly growing the size of their network. **With**[**AWS Transit Gateway**](https://aws.amazon.com/transit-gateway/)**, each VPC only has to connect to the Transit Gateway and not to every other VPC. Customers simply connect each Amazon VPC to the AWS Transit Gateway, and the Gateway will route traffic to and from each VPC.**

--

Trusted Advisor is an online resource that helps to reduce cost, increase performance and improve security by optimizing your AWS environment

AWS Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS

AWS Shield is a managed Distributed Denial of Service (DDoS) protection service

A VPC peering connection is a networking connection between **two** VPCs that enables customers to route traffic between them using private IPv4 addresses or IPv6 addresses. Instances in either VPC can communicate with each other as if they are within the same network. Using VPC peering to connect hundreds of VPCs is very complex and time consuming because customers need to peer each Amazon VPC to each other manually.

Amazon Virtual Private Cloud (Amazon VPC) lets you provision a logically isolated section of the AWS Cloud where you can launch AWS resources in a virtual network that you define. You have complete control over your virtual networking environment, including selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways.

AWS Key Management Service (AWS KMS) is a managed service that enables customers to easily create and control the keys used for cryptographic operations. The service provides a highly available key generation, storage, management, and auditing solution for customers to encrypt or digitally sign data within their applications or to control the encryption of data across AWS services.

Amazon Simple Workflow Service (SWF) is a web service that makes it easy to coordinate work across distributed application components. SWF enables applications for a range of use cases, including media processing, web application back-ends, business process workflows, and analytics pipelines, to be designed as a coordination of tasks

Amazon Security Token Service (STS) is used for requesting temporary credentials

AWS WAF is a web application firewall that lets customers monitor the HTTP and HTTPS requests that are forwarded to Amazon CloudFront or an Application Load Balancer. AWS WAF also lets customers control access to their content by defining customizable web security rules.

Amazon S3 Transfer Acceleration enables fast transfers of files over long distances between your client and an S3 bucket. Transfer Acceleration takes advantage of Amazon CloudFront’s globally distributed edge locations.

AWS Snowball is a data transport solution that accelerates moving terabytes to petabytes of data into and out of AWS using storage devices designed to be secure for physical transport. Customers can transfer up to 80 Terabytes per Snowball.

AWS Snowmobile is an Exabyte-scale data transfer service used to move extremely large amounts of data to AWS. You can transfer up to 100 Petabytes (PB) per Snowmobile, a 45-foot long ruggedized shipping container, pulled by a semi-trailer truck.

Amazon CloudWatch is a monitoring service for AWS cloud resources and the applications you run on AWS. Amazon CloudWatch is the AWS service that allows you to monitor the usage of your AWS resources. CloudWatch collects metrics, and allows you to create alarms based on those metrics.  You can use CloudWatch to monitor your estimated AWS charges. You can use Amazon CloudWatch to gain system-wide visibility into resource utilization, application performance, and operational health. You can use these insights to react and keep your application running smoothly.

AWS Glue is a fully managed extract, transform, and load (ETL) service that makes it easy for customers to prepare and load their data for analytics.

AWS Certificate Manager (AWS ACM) is a service that lets you easily provision, manage, and deploy public and private Secure Sockets Layer/Transport Layer Security (SSL/TLS) certificates for use with AWS services and your internal connected resources.

AnAmazon Machine Image is used to launch Amazon EC2 instances.

 Amazon Aurora is a fully-managed, MySQL and PostgreSQL-compatible relational database engine. It combines the speed and reliability of high-end commercial databases with the simplicity and cost-effectiveness of open-source databases. It delivers up to five times the throughput of MySQL and up to three times the throughput of PostgreSQL without requiring changes to most of your existing applications.

Amazon Redshift is a data warehousing service.

Amazon SimpleDB is a NoSQL data store.

AmazonDynamoDB is a NoSQL database engine. AWS DynamoDB does not use or support any other NoSQL database engines such as MongoDB. You only have access to DynamoDB's built-in engine.

Amazon EBS Snapshots are copies (backups) of EBS volumes.

Amazon ECS is used to run elastic containerized applications on AWS.

AWS marketplace is the service that allows you to search for software solutions on AWS.

Amazon Athena is an interactive query service that makes it easy to analyze data in Amazon S3 using standard SQL.

AWS Migration Hub provides a single location to track the progress of application migrations across multiple AWS and partner solutions.

AWS Database Migration Service (DMS) is used to migrate your data to and from most widely used commercial and open-source databases. AWS DMS supports homogeneous migrations such as Oracle to Oracle, as well as heterogeneous migrations between different database platforms, such as Oracle or Microsoft SQL Server to Amazon Aurora.

Amazon Route 53 can be used for registering domain names, routing end users to Internet applications, configuring DNS health checks to route traffic to healthy endpoints, managing traffic globally through a variety of routing types etc. Route 53 also simplifies the hybrid cloud by providing recursive DNS for your Amazon VPC and on-premises networks over AWS Direct Connect or AWS VPN. Route 53 features include domain registration, DNS, traffic flow, health checking, and failover. Route 53 routing policies include Simple, Weighted, Latency based, Failover, Geo-location, Geo-Proximity, Multi-Value and Traffic Flow

AWS Direct Connect allows you to establish a dedicated network connection from your premises to AWS.

Amazon Connect is a cloud-based contact center solution. Amazon Connect makes it easy to set up and manage a customer contact center and provide reliable customer engagement at any scale. You can set up a contact center in just a few steps, add agents from anywhere, and start to engage with your customers right away.

AWS Data Pipeline is a web service that helps you reliably process and move data between different AWS compute and storage services, as well as on-premises data sources. AWS Data Pipeline integrates with on-premise and cloud-based storage systems to allow developers to use their data when they need it, where they want it, and in the required format.

AWS DataSync makes it simple and fast to move large amounts of data online between on-premises storage and Amazon S3, Amazon Elastic File System (Amazon EFS), or Amazon FSx for Windows File Server.

An AWS managed VPN can be used to quickly connect from an office to an Amazon VPC.

An Internet Gateway is used to connect a public subnet to the Internet (egress)

AWS TCO (Total Cost of Ownership) Calculator is a free tool that provides directional guidance on possible realized savings when deploying AWS. It helps you evaluate the savings from using AWS and compare an AWS Cloud environment to on-premises and co-location environments. This tool considers all the costs to run a solution, including physical facilities, power, and cooling, to provide a realistic, end-to-end comparison of your costs. The Total Cost of Ownership (TCO) is often the financial metric used to estimate and compare direct and indirect costs of a product or a service. Cooling and power consumption, data center space, data center real estate and Labor IT cost are examples of the indirect costs of a physical data center and should be included in TCO analysis.

AWS Simple Monthly Calculator helps customers **estimate** their monthly AWS bill based on their expected usage.

AWS Cost & Usage Report contains the most comprehensive set of AWS cost and usage data available, including additional metadata about AWS services, pricing, and reservations (e.g., Amazon EC2 Reserved Instances (RIs)). The AWS Cost and Usage Report tracks your AWS usage and provides information about your use of AWS resources and estimated costs for that usage. You can configure this report to present the data hourly or daily. AWS Cost & Usage Report provides more granular data about your AWS costs and usage than what the AWS Cost Explorer provides.  the most detailed information available about your AWS costs and usage.

AWS Cost Explorer is used to view and analyze your costs and usage. Cost Explorer is a tool that enables you to view and analyze your current AWS costs and usage. Using the AWS Cost Explorer, the company can view trends and use them to understand their spending and to predict future costs.

 AWS Cost Explorer can also be used to estimate AWS services costs, but it calculates these estimates based on your previous AWS consumption (meaning AWS Cost Explorer is suitable for **existing projects only**). In the above scenario, AWS Simple Monthly Calculator it can be used to estimate the costs of **both existing and new projects.**Forecasting capabilities have been enhanced to support twelve month forecasts. The AWS Cost Explorer is a free tool that allows you to view charts of your costs. You can view cost data for the past 13 months and forecast how much you are likely to spend over the next three months. Cost Explorer can be used to discover patterns in how much you spend on AWS resources over time and to identify cost problem area.

AWS Budgets gives you the ability to set custom budgets that alert you when your costs or usage exceed (or are forecasted to exceed) your budgeted amount.

Consolidated billing is a feature in AWS Organizations that you can use to consolidate billing and payment for multiple AWS accounts.

AWS Storage Gateway is a hybrid storage service that enables your on-premises applications to seamlessly use AWS cloud storage.

AWS X-Ray can be used to analyze and debug your production applications and helps you understand how your application and its underlying services are performing to identify and troubleshoot the root cause of performance issues and errors.  AWS X-Ray helps you identify performance bottlenecks. X-Ray’s service maps let you see relationships between services and resources in your application in real time. You can easily detect where high latencies are occurring, visualize node and edge latency distribution for services, and then drill down into the specific services and paths impacting application performance.

 AWS Trusted Advisor is an application that draws upon best practices learned from AWS’ aggregated operational history of serving hundreds of thousands of AWS customers. Trusted Advisor inspects your AWS environment and makes recommendations that can potentially save you money by highlighting unused resources and opportunities to reduce your bill. AWS Trusted Advisor also provide recommendations to improve system performance, and close SQS gaps. AWS Trusted Advisor is an online tool that provides customers with real time guidance to help them provision their resources following AWS best practices.

AWS Shield is a managed Distributed Denial of Service (DDoS) protection service that safeguards applications running on AWS. AWS Shield Standard is automatically enabled to all AWS customers and provides always-on detection and automatic inline mitigations that minimize application downtime and latency.

AWS Certificate Manager is a service that lets you provision, manage, and deploy (SSL/TLS) certificates for use with AWS services and your internal connected resources.

AWS CloudHSM is a cloud-based hardware security module (HSM) that enables customers to easily generate and use their own encryption keys on the AWS Cloud. It is a cloud-based hardware security module (HSM) that enables you to easily generate and use your own encryption keys on the AWS Cloud.

AWS DMS is used to migrate databases to AWS. AWS Database Migration Service helps you migrate databases to AWS quickly and securely.

Amazon GuardDuty is a threat detection service that continuously monitors for malicious activity and unauthorized behavior to protect your AWS accounts and workloads.

AWS CloudTrail is the service that can be used to track API calls in your AWS account. AWS CloudTrail is a web service that records AWS API calls for your account and delivers log files to you.

AWS Batch is a compute service that allows you to run hundreds of thousands of batch computing jobs on AWS.

AWS Application Discovery Service helps systems integrators quickly and reliably plan application migration projects by automatically identifying applications running in on-premises data centers, their associated dependencies, and their performance profiles.

AWS Config is used to monitor and audit changes in AWS resources and allow you to automate the evaluation of recorded configurations of a specific resource against desired configurations.

AWS Config records point-in-time configuration details for your AWS resources as Configuration Items (CIs). You can use a CI to answer “What did my AWS resource look like?” at a point in time. You can use AWS CloudTrail to answer “Who made an API call to modify this resource?”  With AWS Config, you can discover existing and deleted AWS resources, determine your overall compliance against rules, and dive into configuration details of a resource at any point in time. These capabilities enable compliance auditing, security analysis, resource change tracking, and troubleshooting.

AWS CloudFormation is a service that allows you to use a simple text file to model and provision, in an automated and secure manner, all the resources needed for your applications across all regions and accounts. You can also use AWS CloudFormation to create new RDS instances using the CloudFormation template language.  AWS CloudFormation automates and simplifies the task of repeatedly and predictably creating groups of related resources that power your applications. AWS CloudFormation is a service that helps customers model and set up their Amazon Web Services resources

Amazon PinPoint is used to engage your customers by sending them targeted and transactional email, SMS, push notifications, and voice messages.

AWS Artifact is a no cost, self-service portal for on-demand access to AWS’ compliance reports. AWS Artifact provides on-demand downloads of AWS security and compliance documents, such as AWS ISO certifications, Payment Card Industry (PCI), and Service Organization Control (SOC) reports.

Amazon Cloud Directory is a cloud-native, highly scalable, high-performance directory service that provides web-based directories to make it easy for you to organize and manage all your application resources such as users, groups, locations, devices, and policies, and the rich relationships between them. Unlike existing traditional directory systems, Cloud Directory does not limit organizing directory objects in a single fixed hierarchy. In Cloud Directory, you can organize directory objects into multiple hierarchies to support multiple organizational pivots and relationships across directory information.

AWS Directory Service is a managed Microsoft Active Directory in the AWS Cloud. Customers can use it to manage users and groups, provide single sign-on (SSO) to applications and services, as well as create and apply group policies. AWS Directory Service is the service that provides single sign-on (SSO) to applications and services on AWS. AWS Directory Service uses secure Windows trusts to enable users to sign in to the AWS Management Console and the AWS Command Line Interface (CLI) using their existing corporate Microsoft Active Directory credentials.

Quick Starts are built by AWS solutions architects and partners to help you deploy popular technologies on AWS, based on AWS best practices for security and high availability. These accelerators reduce hundreds of manual procedures into just a few steps, so you can build your production environment quickly and start using it immediately.

Amazon Simple Queue Service (SQS) is a fully managed message queuing service that enables you to decouple and scale microservices, distributed systems, and serverless applications

AWS CodeDeploy is a fully managed deployment service that automates software deployments to a variety of compute services such as Amazon EC2, AWS Fargate, AWS Lambda, and your on-premises servers. AWS CodeDeploy is a service that automates application code deployments to Amazon EC2 instances and instances running on-premises.

AWS Fargate is a compute engine for Amazon Elastic Container Service (ECS) that allows customers to run containers without having to manage servers or clusters.

AWS uses the Service Health Dashboard to publish most up-to-the-minute information on AWS service availability. You can get information about the current status and availability of any AWS service any time using the AWS Service Health Dashboard

Amazon Macie uses machine learning to automatically discover, classify, and protect sensitive data in AWS. Amazon Macie uses machine learning to automatically discover, classify, and protect sensitive data in AWS. Amazon Macie recognizes sensitive data such as personally identifiable information (PII) or intellectual property, and provides you with dashboards and alerts that give visibility into how this data is being accessed or moved. The fully managed service continuously monitors data access activity for anomalies, and generates detailed alerts when it detects risk of unauthorized access or inadvertent data leaks. Today, Amazon Macie is available to protect data stored in Amazon S3, with support for additional AWS data stores coming later this year.

 AWS Service Catalog allows organizations to create and manage catalogs of IT services that are approved for use on AWS. These IT services can include everything from virtual machine images, servers, software, and databases to complete multi-tier application architectures.

AWS Elastic Beanstalk makes it easier for developers to quickly deploy and manage applications in the AWS Cloud. Developers simply upload their application, and Elastic Beanstalk automatically handles the deployment details of capacity provisioning, load balancing, auto-scaling, and application health monitoring.

Amazon Chime is a communications service for online meetings.

AWS Config is a fully-managed service that provides you with an AWS resource inventory, configuration history, and configuration change notifications to enable security and regulatory compliance.

AWS Systems Manager gives you visibility and control of your infrastructure on AWS. Systems Manager provides a unified user interface so you can view operational data from multiple AWS services and allows you to automate operational tasks across your AWS resources.

Amazon Elastic Transcoder is a media transcoding service. It is designed to be a highly scalable, easy-to-use, and cost-effective way to convert (or transcode) media files from their source format into versions that will play back on devices like smartphones, tablets, and PCs.

AWS CloudFront is a global content delivery network (CDN) service. Amazon CloudFront is the service that is used to cache the most recent responses at global edge locations to provide faster performance for global users.  CloudFront is a content delivery network (CDN) that allows you to store (cache) your content at “edge locations” located around the world.  This allows customers to access content more quickly and provides security against DDoS attacks. CloudFront can be used for data, videos, applications, and APIs

* + Benefits include:
  + - Cache content at Edge Location for fast distribution to customers
  + - Built-in Distributed Denial of Service (DDoS) attack protection
  + - Integrates with many AWS services (S3, EC2, ELB, Route 53, Lambda)

The use cases of Amazon CloudFront include:

1- Accelerate static website content delivery: CloudFront can speed up the delivery of your static content (for example, images, style sheets, JavaScript, and so on) to viewers across the globe. By using CloudFront, you can take advantage of the AWS backbone network and CloudFront edge servers to give your viewers a fast, safe, and reliable experience when they visit your website.

2- Live & on-demand video streaming:The Amazon CloudFront CDN offers multiple options for streaming your media – both pre-recorded files and live events – at sustained, high throughput required for 4K delivery to global viewers.

 3- Security: CloudFront integrates seamlessly with AWS Shield for Layer 3/4 DDoS mitigation and AWS WAF for Layer 7 protection.

4- Customizable content delivery with Lambda@Edge: Lambda@Edge is a feature of Amazon CloudFront that lets you run code closer to users of your application, which improves performance and reduces latency.

Amazon Cognito scales to millions of users and supports sign-in with social identity providers, such as Facebook, Google, and Amazon, and enterprise identity providers via SAML 2.0.

AWS Cloud9 is a cloud-based integrated development environment (IDE) that lets customers write, run, and debug code with just a browser.

AWS Direct Connect is an AWS offering that facilitates the establishment of a dedicated network connection from your premises to AWS.

AWS Application Load Balancer (ALB) is part of the AWS Elastic Load Balancing family that is specifically designed to handle HTTP and HTTPS traffic. An ALB automatically distributes incoming application traffic across multiple targets, such as Amazon EC2 instances, containers, and IP addresses. Application Load Balancer (ALB) – layer 7 load balancer that routes connections based on the content of the request

Network Load Balancer (NLB) – layer 4 load balancer that routes connections based on IP protocol data

A transit Virtual Private Cloud (VPC) is a common strategy for connecting multiple, geographically disperse VPCs and remote networks in order to create a global network transit center.

AWS Global Accelerator uses the AWS global network to improve the availability and performance of the applications that you offer to your global users. AWS Global Accelerator does not perform load balancing functions.

The AWS Professional Services organization is a global team of experts that helps customers realize their desired business outcomes when using AWS.

AWS Systems Manager allows customers to centralize operational data from multiple AWS services and automate tasks across their AWS resources.

Services like **AWS Config, Amazon Inspector, and AWS Trusted Advisor**continually monitor for compliance or vulnerabilities giving you a clear overview of which IT resources are in compliance, and which are not.

AWS RDS  ACID (Atomicity, Consistency, Isolation, and Durability) is a set of properties of database transactions intended to guarantee validity even in the event of errors, power failures, etc. Amazon RDS is a fully-managed relational database service. It is a highly available and highly consistent database that supports ACID transactions.

Amazon QuickSight is a fast business **analytics** service that can be used to deliver insights quickly to everyone in your organization.

Amazon ElastiCache for Redis is a blazing fast in-memory data store that provides sub-millisecond latency to power internet-scale real-time applications.

AWS Server Migration Service (SMS) is an agentless service which makes it easier and faster for you to migrate thousands of on-premises workloads to AWS. AWS SMS allows you to automate, schedule, and track incremental replications of live server volumes, making it easier for you to coordinate large-scale server migrations.

With Federation, you can use single sign-on (SSO) to access your AWS accounts using credentials from your corporate directory. Federation enables users to access and use AWS resources using their existing corporate credentials.

Amazon Cognito lets you add user sign-up, sign-in, and access control to web and mobile apps quickly and easily. Amazon Cognito scales to millions of users and supports sign-in with social identity providers, such as Facebook, Google, and Amazon, and enterprise identity providers via SAML 2.0.

AWS Infrastructure Event Management is a short-term engagement with AWS Support, included in the Enterprise-level Support product offering, and available for additional purchase for Business-level Support subscribers. AWS Infrastructure Event Management partners with your technical and project resources to gain a deep understanding of your use case and provide architectural and scaling guidance for an event. Common use-case examples for AWS Event Management include advertising launches, new product launches, and infrastructure migrations to AWS.

Security Groups act as a firewall for associated Amazon EC2 instances, controlling both inbound and outbound traffic at the instance level.

A network access control list (NACL) 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. NACLs act at the subnet level, but security groups act at the instance level.

A Technical Account Manager (TAM) is your designated technical point of contact who provides advocacy and guidance to help plan and build solutions using best practices and proactively keep your AWS environment operationally healthy.

AWS Professional Services organization is a global team of experts that helps customers realize their desired business outcomes when using AWS.

Concierge Team are AWS billing and account experts that work with you to implement billing and account best practices.

AWS Lightsail provides developers compute, storage, and networking capacity and capabilities to deploy and manage websites, web applications, and databases in the cloud. Lightsail provides preconfigured virtual private servers (instances) that include everything required to deploy and application or create a database

If you work with multiple resources in multiple stages, you might find it useful to manage all the resources in each stage as a group rather than move from one AWS service to another for each task. Resource Groups help you do just that.

AWS CodeCommit is a fully-managed source control service that hosts secure Git-based repositiories. It makes it easy for teams to collaborate on code in a secure and highly scalable ecosystem

AWS CodeStar enables you to quickly develop, build, and deploy applications on AWS. AWS CodeStar provides a unified user interface, enabling you to easily manage your software development activities in one place

AWS Storage Gateway Volume Gateway represents the family of gateways that support block-based volumes, previously referred to as gateway-cached and gateway-stored mode. AWS Storage Gateway Volume Gateway operates in 2 modes:

- Stored Volume mode – the entire dataset is stored on-site and is asynchronously backed up to S3 (EBS point-in-time snapshots). Snapshots are incremental and compressed

- Cached Volume mode – the entire dataset is stored on S3 and a cache of the most frequently accessed data is cached on-site

Amazon WorkSpaces is a managed desktop computing service running on the AWS cloud.

AWS Personal Health Dashboard provides alerts and remediation guidance when AWS is experiencing events that may impact you

-----

AWS Service Health Dashboard [http://status.aws.amazon.com](http://status.aws.amazon.com/)

Penetration testing is the practice of testing a network or web application to find security vulnerabilities that an attacker could exploit. Penetration testing is the responsibility of the customer.

If you don't already have an access key for your AWS account root user, don't create one unless you absolutely need to. If you do have an access key for your AWS account root user, delete it. If you must keep it, rotate (change) the access key regularly.

A pilot light scenario is a disaster recover / business continuity scenario wherein a minimal amount of services are kept running in a failover location to enable the business to meet their Recovery Time Objective (RTO) and Recovery Point Objective (RPO) in the event of a disaster.

Recovery time objective (RTO) and recovery point objective (RPO) are two key metrics to consider when developing a disaster recover (DR) plan. RTO represents how many hours it takes customers to return to a working state after a disaster. RPO, which is also expressed in hours, represents how much data customers could lose when a disaster happens. For example, an RPO of 1 hour means that customers could lose up to 1 hour’s worth of data when a disaster occurs.

There are many services on AWS to use for auditing and compliance such as AWS CloudTrail, AWS Config  and Amazon Inspector. However, these services must be configured by the customer

AWS Customer is responsible for encrypting their data either in transit or at rest.

Amazon EC2 Reserved Instances (RI) provide a significant discount (up to 75%) compared to On-Demand instance pricing.

ELB --> Elastic Load Balancer

Read Replicas are special types of database instances that are part of Amazon RDS. The purpose of Read Replicas on Amazon RDS is to enhance database performance and increase database availability.

AWS Software Development Kit (AWS SDK) can simplify using AWS services in your applications with an API tailored to your programming language or platform. Programming languages supported include Java, .NET, Node.js, PHP, Python, Ruby, Go, and C++.

Databases and dynamic websites require block-level storage (such as EBS) not object storage S3.

Amazon Elastic File System (Amazon EFS) is not a cost effective solution for data archiving. Amazon EFS is a **file** level storage service.

 Amazon EBS provides **block** level storage volumes. Amazon EBS volumes offer consistent and low-latency performance compared to other storage options. You can use EBS volumes as primary storage for data that requires frequent updates, such as the system drive for an instance or storage for a database application.

Amazon S3 **object** level storage. Amazon S3 is well suited for storing static assets such as photos and videos, backups, and log files.

AWS Professional Services created the AWS Cloud Adoption Framework (AWS CAF) to help organizations design and travel an accelerated path to successful cloud adoption.

Amazon  Workflow Service (SWF) is a web service that makes it easy to coordinate work across distributed application components. Amazon SWF enables applications for a range of use cases, including media processing, web application back-ends, business process workflows, and analytics pipelines, to be designed as a coordination of tasks. You can think of Amazon SWF as a fully-managed state tracker and task coordinator in the cloud. If your application’s steps take more than 500 milliseconds to complete, you need to track the state of processing. If you need to recover or retry if a task fails, Amazon SWF can help you.

Reserved instances are not suitable for periodic workloads. You should use On-Demand instances instead.

Technical support is not free in AWS. Technical Support requires subscription to an AWS Support Plan.

 Amazon Relational Database Service (Amazon RDS) makes it easy to set up, operate, and scale a relational database in the cloud. It provides cost-efficient and resizable Compute (and\or Storage) capacity while automating time-consuming administration tasks such as hardware provisioning, operating system maintenance, database setup, patching and backups. It frees you to focus on your applications so you can give them the fast performance, high availability, security and compatibility they need. Amazon RDS provides you with six widely-used database engines to choose from, including Amazon Aurora, PostgreSQL, MySQL, MariaDB, Oracle Database, and SQL Server. The only RDS database that can scale instances automatically is Amazon Aurora.

For RDS databases other than Aurora, RDS only supports storage auto-scaling, NOT instance auto-scaling. If you want to scale Amazon RDS instances (other than Aurora), you have two options:

1- Manual horizontal scaling (by adding read replicas)

2- Manual vertical scaling (by upgrading/downgrading an existing instance).

--

AWS service limits are region-specific NOT AZ-specific.

Shared Controls are controls which apply to both the infrastructure layer and customer layers:

\*\* Patch Management – AWS is responsible for patching the underlying hosts and fixing flaws within the infrastructure, but customers are responsible for patching their guest OS and applications.

\*\* Configuration Management – AWS maintains the configuration of its infrastructure devices, but a customer is responsible for configuring their own guest operating systems, databases, and applications.

\*\* Awareness & Training - AWS trains AWS employees, but a customer must train their own employees.

AWS is responsible for items such as the physical security of its data centers, creating hypervisors, replacement of old disk drives, and patch management of the infrastructure.

 The customers are responsible for items such as building application schema, analyzing network performance, configuring security groups and network ACLs and encrypting their data.

--

The technical support is not available for the Basic support plan. Developer support plan provides business hours access to technical support associates via email only. Each of the Business and Enterprise support plans provide 24x7 access to technical support engineers via phone, email, and chat.

--

The factors that have the greatest impact on cost include: Compute, Storage  and Data Transfer Out.

--

There are five design principles for performance efficiency in the cloud:

1- Democratize advanced technologies: Technologies that are difficult to implement can become easier to consume by pushing that knowledge and complexity into the cloud vendor's domain. Rather than having your IT team learns how to host and run a new technology, they can simply consume it as a service. For example, NoSQL databases, media transcoding, and machine learning are all technologies that require expertise that is not evenly dispersed across the technical community. In the cloud, these technologies become services that your team can consume while focusing on product development rather than resource provisioning and management.

2- Go global in minutes: Easily deploy your system in multiple Regions around the world with just a few clicks. This allows you to provide lower latency and a better experience for your customers at minimal cost.

3- Use serverless architectures: In the cloud, serverless architectures remove the need for you to run and maintain servers to carry out traditional compute activities. For example, storage services can act as static websites, removing the need for web servers, and event services can host your code for you. This not only removes the operational burden of managing these servers, but also can lower transactional costs because these managed services operate at cloud scale.

4- Experiment more often: With virtual and automatable resources, you can quickly carry out comparative testing using different types of instances, storage, or configurations.

5- Mechanical sympathy: Use the technology approach that aligns best to what you are trying to achieve. For example, consider data access patterns when selecting database or storage approaches.

--

To enable HTTPS connections to your website or application in AWS, you need an SSL/TLS server certificate. You can use a server certificate provided by AWS Certificate Manager (ACM) or one that you obtained from an external provider. You can use ACM or IAM to store and deploy server certificates.

The AWS Key pair cryptography enables you to securely access your Amazon EC2 instances using a private key instead of a password.

Access keys are long-term credentials for an IAM user or the AWS account root user. You can use access keys to sign programmatic requests to the AWS CLI or AWS API (directly or using the AWS SDK).

Amazon S3 provides a number of security features for the protection of data at rest, which you can use or not depending on your threat profile:

1- Permissions: Use bucket-level or object-level permissions alongside IAM policies to protect resources from unauthorized access and to prevent information disclosure, data integrity compromise or deletion.

2- Versioning: Amazon S3 supports object versions. Versioning is disabled by default. Enable versioning to store a new version for every modified or deleted object from which you can restore compromised objects if necessary.

3- Replication: Amazon S3 replicates each object across all Availability Zones within the respective region. Replication can provide data and service availability in the case of system failure, but provides no protection against accidental deletion or data integrity compromise – it replicates changes across all Availability Zones where it stores copies.

4- Backup: You can use application-level technologies to manually back up data stored in Amazon S3 to other AWS regions or to on-premises backup systems.

5- Encryption – server side: Amazon S3 supports server-side encryption of user data. Server-side encryption is transparent to the end user. AWS generates a unique encryption key for each object, and then encrypts the object using AES-256.

6- Encryption – client side: With client-side encryption you create and manage your own encryption keys. Keys you create are not exported to AWS in clear text. Your applications encrypt data before submitting it to Amazon S3, and decrypt data after receiving it from Amazon S3. Data is stored in an encrypted form, with keys and algorithms only known to you.

--

AWS S3 and Lambda scale automatically

--

 AWS Organizations helps customers centrally govern their environments as they grow and scale their workloads on AWS. Whether customers are a growing startup or a large enterprise, Organizations helps them to centrally manage billing; control access, compliance, and security; and share resources across their AWS accounts.

AWS Organizations has five main benefits:

1) Centrally manage access polices across multiple AWS accounts.

2) Automate AWS account creation and management.

3) Control access to AWS services.

4) Consolidate billing across multiple AWS accounts.

5) Configure AWS services across multiple accounts.

--

Amazon Route 53  and Elastic Load Balancing service also performs health checks on Amazon EC2 instances and distribute traffic only to the healthy ones.

--

AWS supports several MFA device options including **Virtual MFA devices, Universal 2nd Factor**(**U2F) security key, and Hardware MFA devices.**

**--**

In the cloud, you can apply the same engineering discipline that you use for application code to your entire environment. You can define your entire workload (applications, infrastructure) as code and update it with code. You can implement your operations procedures as code and automate their execution by triggering them in response to events. By performing operations as code, you limit human error and enable consistent responses to events.

--

AWS continues to lower the cost of cloud computing for its customers, making everything from web apps to big data on AWS even more cost-effective and widening the TCO (Total Cost of Ownership)  gap with traditional infrastructure.