IAM-With AWS Identity and Access Management (IAM), you can specify who or what can access services and resources in AWS, centrally manage fine-grained permissions, and analyze access to refine permissions across AWS.

1.Set and manage guardrails and fine-grained access controls for your workforce and workloads.

2.Manage identities across single AWS accounts or centrally connect identities to multiple AWS accounts.

3.Grant temporary security credentials for workloads that access your AWS resources.

4.Continually analyze access to right-size permissions on the journey to least privilege.

AWS STS-AWS provides AWS Security Token Service (AWS STS) as a web service that enables you to request temporary, limited-privilege credentials for AWS Identity and Access Management (IAM) users or for users you authenticate (federated users). This guide describes the AWS STS API. For more information, see [Temporary Security Credentials](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_temp.html) in the IAM User Guide.

MFA TOKEN-[AWS multi-factor authentication](https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#enable-mfa-for-privileged-users) (MFA) is an [AWS Identity and Access Management (IAM)](https://aws.amazon.com/iam/) best practice that requires a second authentication factor in addition to user name and password sign-in credentials. You can enable MFA at the AWS account level and for root and IAM users you have created in your account.  
*AWS is expanding eligibility for its free MFA security key program. Verify your eligibility and order your*[*free MFA key*](https://aws.amazon.com/security/amazon-security-initiatives/free-mfa-security-key/)*.*

*AWS ORGANIZATION-*AWS Organizations helps you centrally manage and govern your environment as you grow and scale your AWS resources. Using AWS Organizations, you can programmatically create new AWS accounts and allocate resources, group accounts to organize your workflows, apply policies to accounts or groups for governance, and simplify billing by using a single payment method for all of your accounts.

AWS CONFIG-AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources. Config continuously monitors and records your AWS resource configurations and allows you to automate the evaluation of recorded configurations against desired configurations. With Config, you can review changes in configurations and relationships between AWS resources, dive into detailed resource configuration histories, and determine your overall compliance against the configurations specified in your internal guidelines. This enables you to simplify compliance auditing, security analysis, change management, and operational troubleshooting.

AWS CLOUD TRAIL-AWS CloudTrail is an AWS service that helps you enable operational and risk auditing, governance, and compliance of your AWS account. Actions taken by a user, role, or an AWS service are recorded as events in CloudTrail. Events include actions taken in the AWS Management Console, AWS Command Line Interface, and AWS SDKs and APIs.

AWS CLOUD WATCH-Amazon CloudWatch is a monitoring and observability service built for DevOps engineers, developers, site reliability engineers (SREs), IT managers, and product owners. CloudWatch provides you with data and actionable insights to monitor your applications, respond to system-wide performance changes, and optimize resource utilization. CloudWatch collects monitoring and operational data in the form of logs, metrics, and events. You get a unified view of operational health and gain complete visibility of your AWS resources, applications, and services running on AWS and on-premises. You can use CloudWatch to detect anomalous behavior in your environments, set alarms, visualize logs and metrics side by side, take automated actions, troubleshoot issues, and discover insights to keep your applications running smoothly.

AWS CLOUD FRONT-Reduce latency by delivering data through 410+ globally dispersed Points of Presence (PoPs) with automated network mapping and intelligent routing.

Improve security with traffic encryption and access controls, and use AWS Shield Standard to defend against DDoS attacks at no additional charge.

Cut costs with consolidated requests, customizable pricing options, and zero fees for data transfer out from AWS origins.

Customize the code you run at the AWS content delivery network (CDN) edge using serverless compute features to balance cost, performance, and security.

AWS VPC-Amazon Virtual Private Cloud (Amazon VPC) gives you full control over your virtual networking environment, including resource placement, connectivity, and security. Get started by setting up your VPC in the AWS service console. Next, add resources to it such as Amazon Elastic Compute Cloud (EC2) and Amazon Relational Database Service (RDS) instances. Finally, define how your VPCs communicate with each other across accounts, Availability Zones, or AWS Regions. In the example below, network traffic is being shared between two VPCs within each Region.

AWS SHIELD-AWS Shield is a managed Distributed Denial of Service (DDoS) protection service that safeguards applications running on AWS. AWS Shield provides always-on detection and automatic inline mitigations that minimize application downtime and latency, so there is no need to engage AWS Support to benefit from DDoS protection. There are two tiers of AWS Shield - Standard and Advanced

AWS WAF-AWS WAF is a web application firewall that helps protect your web applications or APIs against common web exploits and bots that may affect availability, compromise security, or consume excessive resources. AWS WAF gives you control over how traffic reaches your applications by enabling you to create security rules that control bot traffic and block common attack patterns, such as SQL injection or cross-site scripting.

AWS INSPECTOR-Amazon Inspector is an automated vulnerability management service that continually scans AWS workloads for software vulnerabilities and unintended network exposure.Immediately discover and scan AWS workloads for software vulnerabilities and unintended network exposure with a single click.Consolidate your vulnerability management solutions for both Amazon EC2 and ECR into one fully managed service.

Use the highly accurate Inspector risk score to efficiently prioritize your remediation.

Reduce mean time to remediate (MTTR) vulnerabilities and streamline workflow with Amazon EventBridge and AWS Security Hub integrations.

AWS KMS-AWS Key Management Service (AWS KMS) lets you create, manage, and control cryptographic keys across your applications and more than 100 AWS services.

Centrally manage keys and define policies across integrated services and applications from a single point.

Encrypt data within your applications with the AWS Encryption SDK data encryption library.

Perform signing operations using asymmetric key pairs to validate digital signatures.

Securely generate hash-based message authentication codes (HMACs) that ensure message integrity and authenticity.

AWS S3-Amazon Simple Storage Service (Amazon S3) is an object storage service offering industry-leading scalability, data availability, security, and performance.

• Amazon S3 holds trillions of objects and regularly peaks at millions of requests per second.• By default, none of your data is shared publicly. You can also encrypt your data in transit and choose to enable server-side encryption on your objects.• By default, data in Amazon S3 is stored redundantly across multiple facilities and multiple devices in each facility.• Amazon S3 also provides low-latency access to the data over the internet by Hypertext Transfer Protocol (HTTP) or Secure HTTP (HTTPS), so you can retrieve data anytime from anywhere.• Bucket names are universal and must be unique across all existing bucket names in Amazon S3.

• Amazon S3 is a fully managed cloud storage service • You store data in Amazon S3 as an object inside a bucket • You can store a virtually unlimited number of objects • You pay for only what you use • You can access Amazon S3 at any time from anywhere through a URL

AWS ELASTIC LOAD BALANCING(ELB)- Elastic Load Balancing (ELB) automatically distributes incoming application traffic across multiple targets and virtual appliances in one or more Availability Zones (AZs).

Secure your applications with integrated certificate management, user-authentication, and SSL/TLS decryption.

Deliver applications with high availability and automatic scaling.

Monitor the health and performance of your applications in real time, uncover bottlenecks, and maintain SLA compliance.

AMAZON EBS-Amazon Elastic Block Store (Amazon EBS) is an easy-to-use, scalable, high-performance block-storage service designed for Amazon Elastic Compute Cloud (Amazon EC2).

Scale fast for your most demanding, high-performance workloads, including mission-critical applications such as SAP, Oracle, and Microsoft products.

Protect against failures with 99.999% availability, including replication within Availablity Zone (AZs), and 99.999% durability with io2 Block Express volumes.

Select the storage that best fits your workload. Volumes range from cost-effective dollar-per-GB to high performance with the fastest IOPS and throughp

AMAZON RDS-Remove inefficient and time-consuming database administrative tasks without needing to provision infrastructure or maintain software.Deploy and scale the relational database engines of your choice in the cloud or on-premises.Achieve high availability with Amazon RDS Multi-AZ deployments.Benefit from over a decade of proven operational expertise, security best practices, and innovation in databases born in the cloud.

Amazon Relational Database Service (Amazon RDS) is a collection of managed services that makes it simple to set up, operate, and scale databases in the cloud. Choose from seven popular engines — [Amazon Aurora with MySQL compatibility](https://aws.amazon.com/rds/aurora/?pg=ln&sec=hiw), [Amazon Aurora with PostgreSQL compatibility](https://aws.amazon.com/rds/aurora/?pg=ln&sec=hiw), [MySQL](https://aws.amazon.com/rds/mysql/?pg=ln&sec=hiw), [MariaDB](https://aws.amazon.com/rds/mariadb/?pg=ln&sec=hiw), [PostgreSQL](https://aws.amazon.com/rds/postgresql/?pg=ln&sec=hiw), [Oracle](https://aws.amazon.com/rds/oracle/?pg=ln&sec=hiw), and [SQL Server](https://aws.amazon.com/rds/sqlserver/?pg=ln&sec=hiw) — and deploy on-premises with [Amazon RDS on AWS Outposts](https://aws.amazon.com/rds/outposts/?pg=ln&sec=hiw).

* Amazon RDS

* Amazon RDS Custom

* Amazon RDS on AWS Outposts

AWS CLOUD FORMATION-AWS CloudFormation is a service that helps you model and set up your AWS resources so that you can spend less time managing those resources and more time focusing on your applications that run in AWS.

AWS CLOUDWATCH EVENT-Amazon CloudWatch Events delivers a near real-time stream of system events that describe changes in Amazon Web Services (AWS) resources. Using simple rules that you can quickly set up, you can match events and route them to one or more target functions or streams. CloudWatch Events becomes aware of operational changes as they occur. CloudWatch Events responds to these operational changes and takes corrective action as necessary, by sending messages to respond to the environment, activating functions, making changes, and capturing state information.