AWS Services Overview

Kiran

Table of Contents

AWS Key Services

Management and Governance:

AWS offers a suite of tools to help customers run their workloads on cloud and to ease the process of deployment and access control.

These include a wide range of tools from Monitoring & auditing solutions, dashboards , programmatic management tools and various configuration utilities.

CloudFormation

Cloudformation is AWS Infrastructure as Code tool. CloudFormation gives you an easy way to model a collection of related AWS and third-party resources, provision them quickly and consistently, and manage them throughout their lifecycles, by treating infrastructure as code. A CloudFormation template describes your desired resources and their dependencies so you can launch and configure them together as a stack. You can use a template to create, update, and delete an entire stack as a single unit, as often as you need to, instead of managing resources individually. You can manage and provision stacks across multiple AWS accounts and AWS Regions.

CloudFormation Documentation

CloudWatch

Cloudwatch is aws' native monitoring tool. It lets users Monitor resources and applications and also create alerts when a metric reaches a threshold.

CloudWatch Documentation

AWS Chatbot

AWS Chatbot is an interactive agent that makes it easy to monitor and interact with your AWS resources in your Slack channels and Amazon Chime chat rooms. With AWS Chatbot you can receive alerts, run commands to return diagnostic information, invoke AWS Lambda functions, and create AWS support cases.

AWS Chatbot manages the integration between AWS services and your Slack channels or Amazon Chime chat rooms helping you to get started with ChatOps fast.

With just a few clicks you can start receiving notifications and issuing commands in your chosen channels or chat rooms, so your team doesn't have to switch contexts to collaborate.

AWS Chatbot makes helps your teams easily stay updated, collaborate, and respond faster to operational events, security findings, CI/CD workflows, budget, and other alerts for applications running in your AWS accounts.

ChatBot Documentation

CloudTrail

CloudTrail is an auditing tool that enables governance, compliance, operational auditing, and risk auditing of AWS accounts.

CloudTrail helps customers log, continuously monitor, and retain account activity related to actions across performed on your account.

CloudTrail provides event history of your AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command line tools, and other AWS services. In simple terms, CloudTrail logs every activity performed through various channels so customers can track changes.

This event history simplifies security analysis, resource change tracking, and troubleshooting. In addition, you can use CloudTrail to detect unusual activity in your AWS accounts. These capabilities help simplify operational analysis and troubleshooting.

Cloud Trail Documentation

License Manager

AWS License Manager makes it easier to manage your software licenses from vendors such as Microsoft, SAP, Oracle, and IBM across AWS and on-premises environments. AWS License Manager lets administrators create customized licensing rules that mirror the terms of their licensing agreements. Administrators can use these rules to help prevent licensing violations, such as using more licenses than an agreement stipulates. Rules in AWS License Manager help prevent a licensing breach by stopping the instance from launching or by notifying administrators about the infringement. Administrators gain control and visibility of all their licenses with the AWS License Manager dashboard and reduce the risk of non-compliance, misreporting, and additional costs due to licensing overages. Independent software vendors (ISVs) can also use AWS License Manager to easily distribute and track licenses.

AWS License Manager also simplifies the management of your software licenses that require Amazon EC2 Dedicated Hosts. In AWS License Manager, administrators can specify their Dedicated Host management preferences for host allocation and host capacity utilization. Once set up, AWS License Manager takes care of these administrative tasks on your behalf, so that you can seamlessly launch instances just like you would launch an EC2 instance with AWS-provided

licenses.

AWS License Manager is offered at no additional charge. You only pay for AWS resources you use to run your applications. Visit the AWS License Manager console to start managing your licenses.

License Manager Documentation

AWS OpsWorks

AWS OpsWorks is a configuration management service that provides managed instances of Chef and Puppet. Chef and Puppet are automation platforms that allow you to use code to automate the configurations of your servers. OpsWorks lets you use Chef and Puppet to automate how servers are configured, deployed, and managed across your Amazon EC2 instances or on-premises compute environments. OpsWorks has three offerings, AWS Opsworks for Chef Automate, AWS OpsWorks for Puppet Enterprise, and AWS OpsWorks Stacks.

OpsWorks Documentation

Trusted Advisor

AWS Trusted Advisor is a fully managed service that provides you guidance to follow AWS best practices. Trusted Advisor helps optimize your AWS infrastructure, improve security and performance, reduce the overall costs, and monitor service limits. Whether establishing new workflows, developing applications, or as part of ongoing improvement, take advantage of the recommendations provided by Trusted Advisor regularly to help keep your solutions provisioned optimally.

AWS Basic Support and AWS Developer Support customers get access to core security checks and service limit checks. AWS Business Support and AWS Enterprise Support customers get access to all Trusted Advisor checks and recommendations, including cost optimization, security, fault tolerance, performance, and service limits. For a complete list of checks and descriptions, explore Trusted Advisor Best Practices .

Trusted Advisor Documentation

Systems Manager

Managing large infrastructure at scale poses many operational challanges.Customers need a centralized mechanism to run the operational tasks.

Systems Manager is the operations hub for AWS. Systems Manager provides a unified user interface so you can track and resolve operational issues across your AWS applications and resources from a central place. With Systems Manager, you can automate operational tasks for Amazon EC2 instances or Amazon RDS instances. You can also group resources by application, view operational data for monitoring and troubleshooting, implement pre-approved change work flows, and audit operational changes for your groups of resources. Systems Manager simplifies resource and application management, shortens the time to detect and resolve operational problems, and makes it easier to operate and manage your infrastructure at scale.

SSM Documentation

AWS Personal Health Dashboard

AWS Personal Health Dashboard provides alerts and remediation guidance when AWS is experiencing events that may impact you. While the Service Health Dashboard displays the general

status of AWS services, Personal Health Dashboard gives you a personalized view into the performance and availability of the AWS services underlying your AWS resources.

The dashboard displays relevant and timely information to help you manage events in progress, and provides proactive notification to help you plan for scheduled activities. With Personal Health Dashboard, alerts are triggered by changes in the health of AWS resources, giving you event visibility, and guidance to help quickly diagnose and resolve issues.

For example, in the event of a lost Amazon Elastic Block Store (EBS) volume associated with one of your Amazon EC2 instances, you would gain quick visibility into the status of the specific service you are using, helping save precious time troubleshooting to determine root cause.

If you use AWS Organizations, AWS Health allows you to aggregate notifications from all accounts in your organization. This provides centralized and real-time access to all AWS Health events posted to individual accounts in your organization, including operational issues, scheduled maintenance, and account notifications.

AWS Service Catalog

You are responsible for managining aws for a large organization and you want to ensure your team members only create approved services and do not provision services that are not approved, then Service Catalog is the answer.

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 Service Catalog allows you to centrally manage deployed IT services and your applications, resources, and metadata. This helps you achieve consistent governance and meet your compliance requirements, while enabling users to quickly deploy only the approved IT services they need. With AWS Service Catalog AppRegistry, organizations can understand the application context of their AWS resources. You can define and manage your applications and their metadata, to keep track of cost, performance, security, compliance and operational status at the application level.

AWS Service Catalog AppRegistry provides a single repository for collecting and managing your application resources on AWS. You define your application metadata, which may include information from your internal systems, other AWS services, and software vendors. Builders can include a reference to their application within the infrastructure code, and business stakeholders have up-to-date information on application contents and metadata, such as organizational ownership, data sensitivity, and cost center.

Service Catalog Documentation

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.

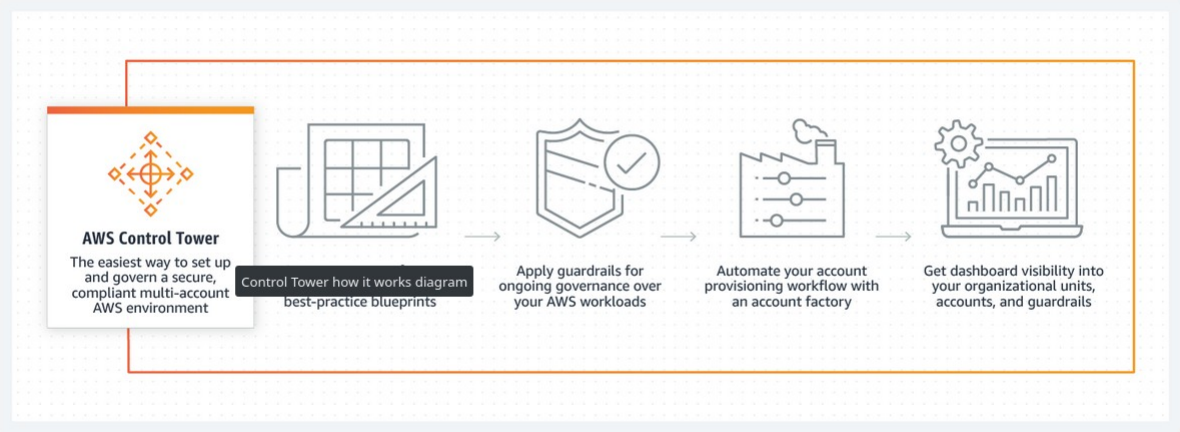
AWS Config Documentation

AWS Control Tower

f you're a customer with multiple AWS accounts and teams, cloud setup and governance can be complex and time consuming, slowing down the very innovation you're trying to speed up. AWS Control Tower provides the easiest way to set up and govern a secure, multi-account AWS environment, called a landing zone. AWS Control Tower creates your landing zone using AWS Organizations, bringing ongoing account management and governance as well as implementation best practices based on AWS's experience working with thousands of customers as they move to the cloud.

With AWS Control Tower, builders can provision new AWS accounts in a few clicks, while you have peace of mind knowing that your accounts conform to company-wide policies. AWS customers can implement AWS Control Tower, extend governance into new or existing accounts, and gain visibility into their compliance status quickly. If you are building a new AWS environment, starting out on your journey to AWS or starting a new cloud initiative, Control Tower will help you get started quickly with governance and best practices built-in.

How it works



Networking & Content Delivery

CloudFront

CDN: Content Delivery Network or Content Distribution Network is a geographically distributed network of proxy servers. The aim is to improve page loads and increase global availability of content by creating Edge Locations in various geographic locations.

CloudFront is a fast CDN service that securely delivers data, videos, applications, and APIs to customers globally with low latency, high transfer speeds, all within a developer-friendly environment.

CloudFront offers the most advanced security capabilities, including field level encryption and HTTPS support, seamlessly integrated with AWS Shield, AWS Web Application Firewall and Amazon Route 53 to protect against multiple types of attacks including network and application layer DDoS attacks.

These services co-reside at edge networking locations - globally scaled and connected via the AWS network backbone - providing a more secure, performant, and available experience for your users.

CloudFront works seamlessly with any AWS origin, such as Amazon S3, Amazon EC2, Elastic Load Balancing, or with any custom HTTP origin.

You can customize your content delivery through CloudFront using the secure and programmable edge computing features CloudFront Functions and AWS Lambda@Edge .

Use Cases:

Website Delivery and Security

Dynamic Content & API Acceleration

Live & On-Demand Video Streaming

Software Distribution, Game Delivery and IoT OTA

CloudFront Documentation

Amazon API Gateway

API: Application Programming Interface is an interface that defines interactions between multiple software applications.

It defines the kinds of calls or requests that can be made, how to make them, the data formats that should be used, the conventions to follow, etc.

It can also provide extension mechanisms so that users can extend existing functionality in various ways and to varying degrees.

An API can be entirely custom, specific to a component, or designed based on an industry-standard to ensure interoperability.

Through information hiding, APIs enable modular programming, allowing users to use the interface independently of the implementation.

APIs act as the "front door" for applications to access data, business logic, or functionality from your backend services.

API Gateway is a fully managed service that makes it easy for developers to create, publish, maintain, monitor, and secure APIs at any scale.

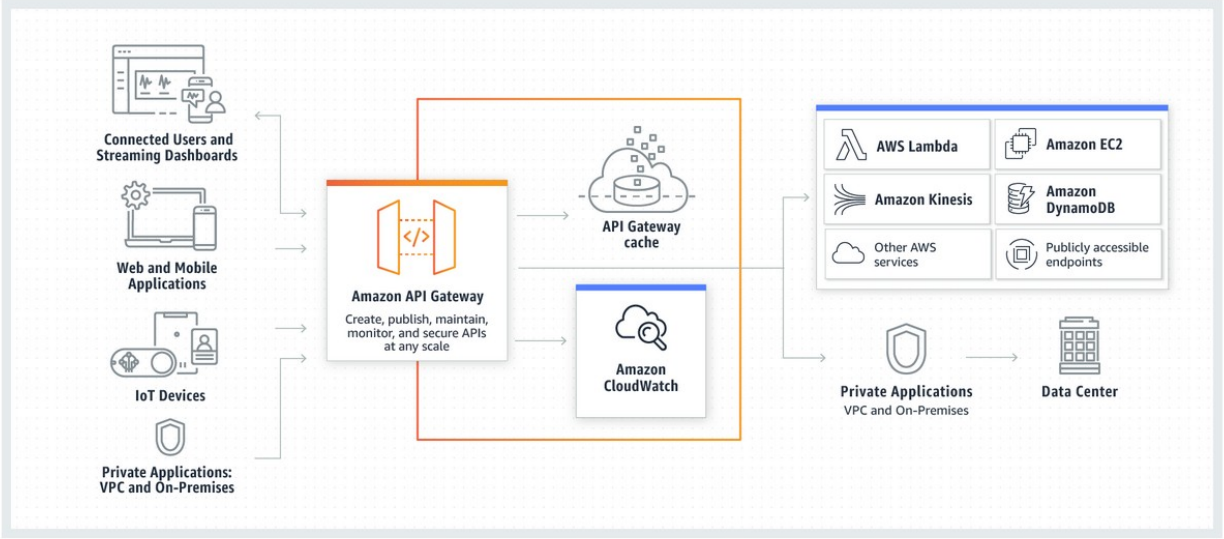
Using API Gateway, you can create RESTful APIs and WebSocket APIs that enable real-time two-way communication applications.

API Gateway supports containerized and serverless workloads, as well as web applications.

API Gateway handles all the tasks involved in accepting and processing up to hundreds of thousands of concurrent API calls, including traffic management, CORS support, authorization and access control, throttling, monitoring, and API version management.

API Gateway has no minimum fees or startup costs. You pay for the API calls you receive and the amount of data transferred out and, with the API Gateway tiered pricing model, you can reduce your cost as your API usage scales.

How API Gateway Works



Benefits:

1. Efficient API development.
2. Performance at any scale.
3. Cost Savings.
4. Easy Monitoring.
5. Flexible Security Controls.
6. RESTful API options.

PrivateLink

AWS PrivateLink provides private connectivity between VPCs, AWS services, and your on-premises networks, without exposing your traffic to the public internet.

AWS PrivateLink makes it easy to connect services across different accounts and VPCs to significantly simplify your network architecture.

Interface VPC endpoints, powered by AWS PrivateLink, connect you to services hosted by AWS Partners and supported solutions available in AWS Marketplace. By powering Gateway Load Balancer endpoints, AWS PrivateLink brings the same level of security and performance to your virtual network appliances or custom traffic inspection logic.

PrivateLink Use Cases:

1. Securely Access SaaS Applications.
2. Maintain Regulatory Compliance.
3. Migrate to Hybrid Cloud.

PrivateLink Benefits:

1. Secure Traffic.

2. Simplify Network Management.
3. Accelerate Cloud Migration.
4. Cost Savings

Development Services

AWS CodeCommit

Source Control: Source Control or Version control is the practice of tracking and managing changes to code. Source Code Management System provide a running history of cdoe development and enable parallel development with branching and merging features.

Git: Git is an open-source distributed source code management system. Git allows you to create a copy of your repository known as a branch. Using this branch, you can then work on your code independently from the stable version of your codebase. Once you are ready with your changes, you can store them as a set of differences, known as a commit. You can pull in commits from other contributors to your repository, push your commits to others, and merge your commits back into the main version of the repository.

Source Code Repository: Source Code repository is a central location where developers working on a project check-in (save) their code which is typically available over the web and can be managed through Version Control Software such as Git.

`AWS CodeCommit` is a fully-managed source control service that hosts secure Git-based repositories. It makes it easy for teams to collaborate on code in a secure and highly scalable ecosystem. CodeCommit eliminates the need to operate your own source control system or worry about scaling its infrastructure. You can use CodeCommit to securely store anything from source code to binaries, and it works seamlessly with your existing Git tools.

Benefits:

1. Fully Managed.
2. High Availability
3. Integrate with existing tools.
4. Faster development Lifecycle.

Alternatives:

1. GitHub: A Fully managed (SaaS) Source Code Management service. Available for Free and Enterprise Tiers.
2. Gitlab: Gitlab is available as SaaS offering. It is also open-source and can be installed on the on-premise servers.
3. BitBucket: SaaS offering by Atlassian.
4. Azure DevOps Repos: A SaaS product by Microsoft.

AWS CodeBuild

_Continuous Integration$_{(CI)}$: Continuous Integration is the process of developers checking their code into Source code repository several times a day followed by running build (compiling) and run tests.

Continuous Integration ensures the changes to the code are validated and avoids integration hell.

The compiled object(s)/file(s) that is generated after the build process is generally referred as `Artifact(s)`

`CodeBuild` is a fully managed continuous integration service that compiles source code, runs tests, and produces software packages that are ready to deploy.

With CodeBuild, you don't need to provision, manage, and scale your own build servers.

CodeBuild scales continuously and processes multiple builds concurrently, so your builds are not left waiting in a queue.

You can get started quickly by using prepackaged build environments, or you can create custom build environments that use your own build tools.

The charges are per minute for the compute resources you use.

Alternatives:

1. Jenkins: Opensource CI tool that has to be installed on your ownservers.
2. JenkinsX: Jenkins SaaS offering.
3. GitlabCI: is offered both as SaaS offering or can be managed on your own infra.
4. Azure DevOps Piplelines: SaaS offering by Microsoft.
5. GitHub Actions.

AWS CodeDeploy

Continuous Deployment(CD): Continuous Deployment is the process of delivering software functionalities/features through automated deployments. CD complements CI and CD is often a follow up step for CI.

`CodeDeploy` is a fully managed deployment service that automates software deployments to a variety of compute services such as Amazon EC2, AWS Fargate, AWS ambda, and your on-premises servers. AWS CodeDeploy makes it easier for you to rapidly release new features, helps you avoid downtime during application deployment, and handles the complexity of updating your applications. You can use AWS CodeDeploy to automate software deployments, eliminating the need for error-prone manual operations. The service scales to match your deployment needs.

Alternatives:

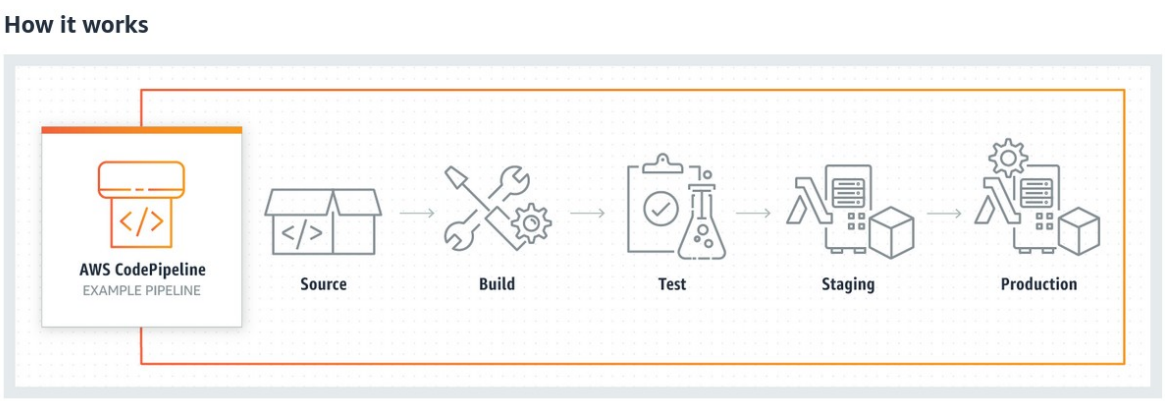
1. Jenkins
2. Azure DevOps releases.
3. GitlabCI.
4. GitHub Actions.
5. Ansible.

AWS CodePipeline

`CodePipeline` is a fully managed continuous delivery service that helps you automate your release pipelines for fast and reliable application and infrastructure updates.

`CodePipeline` automates the build, test, and deploy phases of your release process every time there is a code change, based on the release model you define. This enables you to rapidly and reliably deliver features and updates.

`CodePipeline` can be easily integrated with third-party services such as GitHub or with your own custom plugin. With AWS CodePipeline, you only pay for what you use. There are no upfront fees or long-term commitments.



Alternatives:

1. Jenkins: Opensource CI tool that has to be installed on your ownservers.
2. JenkinsX: Jenkins SaaS offering.
3. GitlabCI: is offered both as SaaS offering or can be managed on your own infra.
4. Azure DevOps Piplelines: SaaS offering by Microsoft.
5. GitHub Actions.

AWS Codestar *

`CodeStar` enables you to quickly develop, build, and deploy applications on AWS.

It offers Templates for various applications such as web application or web serivce to be deployed from a platform of your choice.

`CodeStar` provides a unified user interface, enabling you to easily manage your software development activities in one place.

`CodeStar` let's you set up your entire continuous delivery toolchain in minutes, allowing you to start releasing code faster.

`CodeStar` makes it easy for your whole team to work together securely, allowing you to easily manage access and add owners, contributors, and viewers to your projects. Each AWS CodeStar project comes with a project management dashboard, including an integrated issue tracking capability powered by Atlassian JIRA Software. With the AWS CodeStar project dashboard, you can easily track progress across your entire software development process, from your backlog of work items to teams' recent code deployments. Visit here to learn more.

There is no additional charge for using AWS CodeStar.

You only pay for the AWS resources that you provision for developing and running your application (for example, Amazon EC2 instances).

More information can be found here

AWS CodeGuru

`CodeGuru` is a developer tool that provides intelligent recommendations to improve code quality and identify an application's most expensive lines of code.

Integrate `CodeGuru` into your existing software development workflow to automate code reviews during application development, continuously monitor application performance in production, provide recommendations and visual clues for improving code quality and application performance, and reduce overall cost.

`CodeGuru` Reviewer uses machine learning and automated reasoning to identify critical issues, security vulnerabilities, and hard-to-find bugs during application development and provides recommendations to improve code quality.

Similar Products:

1. SonarQube.
2. Embold.
3. Codacy

Security Identity & Compliance

Amazoon Cognito

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

Amazon Detective

Amazon Detective makes it easy to analyze, investigate, and quickly identify the root cause of potential security issues or suspicious activities. Amazon Detective automatically collects log data from your AWS resources and uses machine learning, statistical analysis, and graph theory to build a linked set of data that enables you to easily conduct faster and more efficient security investigations.

AWS security services like Amazon GuardDuty, Amazon Macie, and AWS Security Hub as well as partner security products can be used to identify potential security issues, or findings. These services are really helpful in alerting you when something is wrong and pointing out where to go to fix it. But sometimes there might be a security finding where you need to dig a lot deeper and analyze more information to isolate the root cause and take action. Determining the root cause of security findings can be a complex process that often involves collecting and combining logs from many separate data sources, using extract, transform, and load (ETL) tools or custom scripting to organize the data, and then security analysts having to analyze the data and conduct lengthy investigations.

Amazon Guard-Duty

GuardDuty is a threat detection service that continuously monitors for malicious activity and unauthorized behavior to protect your AWS accounts, workloads, and data stored in Amazon S3. With the cloud, the collection and aggregation of account and network activities is simplified, but it

can be time consuming for security teams to continuously analyze event log data for potential threats. With GuardDuty, you now have an intelligent and cost-effective option for continuous threat detection in AWS. The service uses machine learning, anomaly detection, and integrated threat intelligence to identify and prioritize potential threats. GuardDuty analyzes tens of billions of events across multiple AWS data sources, such as AWS CloudTrail event logs, Amazon VPC Flow Logs, and DNS logs. With a few clicks in the AWS Management Console, GuardDuty can be enabled with no software or hardware to deploy or maintain. By integrating with Amazon CloudWatch Events, GuardDuty alerts are actionable, easy to aggregate across multiple accounts, and straightforward to push into existing event management and workflow systems.

Amazon Macie

Amazon Macie is a fully managed data security and data privacy service that uses machine learning and pattern matching to discover and protect your sensitive data in AWS.

As organizations manage growing volumes of data, identifying and protecting their sensitive data at scale can become increasingly complex, expensive, and time-consuming. Amazon Macie automates the discovery of sensitive data at scale and lowers the cost of protecting your data. Macie automatically provides an inventory of Amazon S3 buckets including a list of unencrypted buckets, publicly accessible buckets, and buckets shared with AWS accounts outside those you have defined in AWS Organizations. Then, Macie applies machine learning and pattern matching techniques to the buckets you select to identify and alert you to sensitive data, such as personally identifiable information (PII).

Macie's alerts, or findings, can be searched and filtered in the AWS Management Console and sent to Amazon EventBridge, formerly called Amazon CloudWatch Events, for easy integration with existing workflow or event management systems, or to be used in combination with AWS services, such as AWS Step Functions to take automated remediation actions. This can help you meet regulations, such as the Health Insurance Portability and Accountability Act (HIPAA) and General Data Privacy Regulation (GDPR). You can get started with Amazon Macie by leveraging the 30-day free trial for bucket evaluation. The trial includes 30-days of Amazon S3 bucket inventory and bucket-level security and access control assessment at no cost. Note that sensitive data discovery is not included in the 30-day free trial for bucket evaluation.

AWS Audit Manager

AWS Audit Manager helps you continuously audit your AWS usage to simplify how you assess risk and compliance with regulations and industry standards. Audit Manager automates evidence collection to reduce the -all hands on deck- manual effort that often happens for audits and enable you to scale your audit capability in the cloud as your business grows. With Audit Manager, it is easy to assess if your policies, procedures, and activities - also known as controls - are operating effectively. When it is time for an audit, AWS Audit Manager helps you manage stakeholder reviews of your controls and enables you to build audit-ready reports with much less manual effort.

AWS Audit Manager's prebuilt frameworks help translate evidence from cloud services into auditor-friendly reports by mapping your AWS resources to the requirements in industry standards or regulations, such as CIS AWS Foundations Benchmark, the General Data Protection Regulation (GDPR), and the Payment Card Industry Data Security Standard (PCI DSS). You can also fully customize a framework and its controls for your unique business requirements.

Based on the framework you select, Audit Manager launches an assessment that continuously collects and organizes relevant evidence from your AWS accounts and resources, such as resource configuration snapshots, user activity, and compliance check results.

You can get started quickly in the AWS Management Console. Just select a prebuilt framework to launch an assessment and begin automatically collecting and organizing evidence.

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.

Serverless

Simple Queue Service

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. SQS eliminates the complexity and overhead associated with managing and operating message oriented middleware, and empowers developers to focus on differentiating work. Using SQS, you can send, store, and receive messages between software components at any volume, without losing messages or requiring other services to be available. Get started with SQS in minutes using the AWS console, Command Line Interface or SDK of your choice, and three simple commands.

SQS offers two types of message queues. Standard queues offer maximum throughput, best-effort ordering, and at-least-once delivery. SQS FIFO queues are designed to guarantee that messages are processed exactly once, in the exact order that they are sent.

Simple Notification Service

Amazon Simple Notification Service (Amazon SNS) is a fully managed messaging service for both application-to-application (A2A) and application-to-person (A2P) communication.

The A2A pub/sub functionality provides topics for high-throughput, push-based, many-to-many messaging between distributed systems, microservices, and event-driven serverless applications. Using Amazon SNS topics, your publisher systems can fanout messages to a large number of subscriber systems including Amazon SQS queues, AWS Lambda functions and HTTPS endpoints, for parallel processing, and Amazon Kinesis Data Firehose. The A2P functionality enables you to send messages to users at scale via SMS, mobile push, and email.

AWS AppSync

Organizations choose to build APIs with GraphQL because it helps them develop applications faster, by giving front-end developers the ability to query multiple databases, microservices, and APIs with a single GraphQL endpoint.

AWS AppSync is a fully managed service that makes it easy to develop GraphQL APIs by handling the heavy lifting of securely connecting to data sources like AWS DynamoDB, Lambda, and more. Adding caches to improve performance, subscriptions to support real-time updates, and client-side data stores that keep off-line clients in sync are just as easy. Once deployed, AWS AppSync automatically scales your GraphQL API execution engine up and down to meet API request volu

Fargate

AWS Fargate is a serverless compute engine for containers that works with both Amazon Elastic Container Service (ECS) and Amazon Elastic Kubernetes Service (EKS). Fargate makes it easy for you to focus on building your applications. Fargate removes the need to provision and manage servers, lets you specify and pay for resources per application, and improves security through application isolation by design.

Fargate allocates the right amount of compute, eliminating the need to choose instances and scale cluster capacity. You only pay for the resources required to run your containers, so there is no over-provisioning and paying for additional servers. Fargate runs each task or pod in its own kernel providing the tasks and pods their own isolated compute environment. This enables your application to have workload isolation and improved security by design. This is why customers such as Vanguard, Accenture, Foursquare, and Ancestry have chosen to run their mission critical applications on Fargate.

Container Services

Elastic Container Registry (ECR)

Amazon Elastic Container Registry (ECR) is a fully managed container registry that makes it easy to store, manage, share, and deploy your container images and artifacts anywhere. Amazon ECR eliminates the need to operate your own container repositories or worry about scaling the underlying infrastructure. Amazon ECR hosts your images in a highly available and high-performance architecture, allowing you to reliably deploy images for your container applications. You can share container software privately within your organization or publicly worldwide for anyone to discover and download. For example, developers can search the ECR public gallery for an operating system image that is geo-replicated for high availability and faster downloads. Amazon ECR works with Amazon Elastic Kubernetes Service (EKS), Amazon Elastic Container Service (ECS), and AWS Lambda, simplifying your development to production workflow, and AWS Fargate for one-click deployments. Or you can use ECR with your own containers environment. Integration with AWS Identity and Access Management (IAM) provides resource-level control of each repository. With ECR, there are no upfront fees or commitments. You pay only for the amount of data you store in your repositories and data transferred to the Internet.

Alternatives :

1. DockerHub: SaaS and predominantly used container registry.
2. ACR: Azure Container Registry.
3. Self-hosted Registry.

ECS

Amazon Elastic Container Service (Amazon ECS) is a fully managed container orchestration service. Customers such as Duolingo, Samsung, GE, and Cookpad use ECS to run their most sensitive and mission critical applications because of its security, reliability, and scalability.

ECS is a great choice to run containers for several reasons. First, you can choose to run your ECS clusters using AWS Fargate, which is serverless compute for containers. Fargate removes the need to provision and manage servers, lets you specify and pay for resources per application, and improves security through application isolation by design. Second, ECS is used extensively within Amazon to power services such as Amazon SageMaker, AWS Batch, Amazon Lex, and

Amazon.com's recommendation engine, ensuring ECS is tested extensively for security, reliability, and availability.

Additionally, because ECS has been a foundational pillar for key Amazon services, it can natively integrate with other services such as Amazon Route 53, Secrets Manager, AWS Identity and Access Management (IAM), and Amazon CloudWatch providing you a familiar experience to deploy and scale your containers. ECS is also able to quickly integrate with other AWS services to bring new capabilities to ECS. For example, ECS allows your applications the flexibility to use a mix of Amazon EC2 and AWS Fargate with Spot and On-Demand pricing options. ECS also integrates with AWS App Mesh, which is a service mesh, to bring rich observability, traffic controls and security features to your applications. ECS has grown rapidly since launch and is currently launching 5X more containers every hour than EC2 launches instances.

EKS

Amazon Elastic Kubernetes Service (Amazon EKS) gives you the flexibility to start, run, and scale Kubernetes applications in the AWS cloud or on-premises. Amazon EKS helps you provide highly-available and secure clusters and automates key tasks such as patching, node provisioning, and updates. Customers such as Intel, Snap, Intuit, GoDaddy, and Autodesk trust EKS to run their most sensitive and mission critical applications.

EKS runs upstream Kubernetes and is certified Kubernetes conformant for a predictable experience. You can easily migrate any standard Kubernetes application to EKS without needing to refactor your code.

EKS makes it easy to standardize operations across every environment. You can run fully managed EKS clusters on AWS. You can have an open source, proven distribution of Kubernetes wherever you want for consistent operations with Amazon EKS Distro. You can host and operate your Kubernetes clusters on-premises and at the edge with AWS Outposts and AWS Wavelength, and have a consistent cluster management experience with Amazon EKS Anywhere (coming in 2021.)