# AWS Lightsail

### Overview

Amazon Lightsail is the easiest way to get started with AWS for developers who just need virtual private servers. Lightsail includes everything you need to launch your project quickly – a virtual machine, SSD-based storage, data transfer, DNS management, and a static IP – for a low, predictable price

# AWS EC2

### Overview

Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides resizable computing capacity—literally, servers in Amazon's data centers—that you use to build and host your software systems

### Features of Amazon EC2

Amazon EC2 provides the following features:

* Virtual computing environments, known as instances
* Preconfigured templates for your instances, known as Amazon Machine Images (AMIs), that package the bits you need for your server (including the operating system and additional software)
* Various configurations of CPU, memory, storage, and networking capacity for your instances, known as instance types
* Secure login information for your instances using key pairs (AWS stores the public key, and you store the private key in a secure place)
* Storage volumes for temporary data that's deleted when you stop or terminate your instance, known as instance store volumes
* Persistent storage volumes for your data using Amazon Elastic Block Store (Amazon EBS), known as Amazon EBS volumes
* Multiple physical locations for your resources, such as instances and Amazon EBS volumes, known as Regions and Availability Zones
* A firewall that enables you to specify the protocols, ports, and source IP ranges that can reach your instances using security groups
* Static IPv4 addresses for dynamic cloud computing, known as Elastic IP addresses
* Metadata, known as tags that you can create and assign to your Amazon EC2 resources
* Virtual networks you can create that are logically isolated from the rest of the AWS cloud, and that you can optionally connect to your own network, known as virtual private clouds (VPCs)

### Amazon Machine Images (AMI)

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

### Amazon Elastic Block Store (Amazon EBS

* Amazon Elastic Block Store (Amazon EBS) provides block level storage volumes for use with EC2 instances.
* EBS volumes behave like raw, unformatted block devices. You can mount these volumes as devices on your instances.
* You can mount multiple volumes on the same instance, and you can mount a volume to multiple instances at a time.
* You can create a file system on top of these volumes, or use them in any way you would use a block device (like a hard drive). You can dynamically change the configuration of a volume attached to an instance.
* EBS volumes are highly available and reliable storage volumes that can be attached to any running instance that is in the same Availability Zone.
* EBS volumes that are attached to an EC2 instance are exposed as storage volumes that persist independently from the life of the instance. With Amazon EBS, you pay only for what you use

### Amazon EC2 Auto Scaling

* Amazon EC2 Auto Scaling helps you ensure that you have the correct number of Amazon EC2 instances available to handle the load for your application. You create collections of EC2 instances, called Auto Scaling groups.
* You can specify the minimum number of instances in each Auto Scaling group, and Amazon EC2 Auto Scaling ensures that your group never goes below this size. You can specify the maximum number of instances in each Auto Scaling group, and Amazon EC2 Auto Scaling ensures that your group never goes above this size
* If you specify the desired capacity, either when you create the group or at any time thereafter, Amazon EC2 Auto Scaling ensures that your group has this many instances.
* If you specify scaling policies, then Amazon EC2 Auto Scaling can launch or terminate instances as demand on your application increases or decreases.

For example, the following Auto Scaling group has a minimum size of one instance, a desired capacity of two instances, and a maximum size of four instances. The scaling policies that you define adjust the number of instances, within your minimum and maximum number of instances, based on the criteria that you specify.


   An illustration of a basic Auto Scaling group.
  

# AWS Batch

### Overview

AWS Batch enables you to run batch computing workloads on the AWS Cloud. Batch computing is a common way for developers, scientists, and engineers to access large amounts of compute resources. AWS Batch removes the undifferentiated heavy lifting of configuring and managing the required infrastructure.

AWS Batch enables you to run batch computing workloads on the AWS Cloud. Batch computing is a common way for developers, scientists, and engineers to access large amounts of compute resources, and AWS Batch removes the undifferentiated heavy lifting of configuring and managing the required infrastructure, similar to traditional batch computing software. This service can efficiently provision resources in response to jobs submitted in order to eliminate capacity constraints, reduce compute costs, and deliver results quickly.

As a fully managed service, AWS Batch enables you to run batch computing workloads of any scale. AWS Batch automatically provisions compute resources and optimizes the workload distribution based on the quantity and scale of the workloads. With AWS Batch, there is no need to install or manage batch computing software, which allows you to focus on analyzing results and solving problems.

### Components of AWS Batch

AWS Batch is a regional service that simplifies running batch jobs across multiple Availability Zones within a region. You can create AWS Batch compute environments within a new or existing VPC. After a compute environment is up and associated with a job queue, you can define job definitions that specify which Docker container images to run your jobs. Container images are stored in and pulled from container registries, which may exist within or outside of your AWS infrastructure.

### Jobs

A unit of work (such as a shell script, a Linux executable, or a Docker container image) that you submit to AWS Batch. It has a name, and runs as a containerized application on an Amazon EC2 instance in your compute environment, using parameters that you specify in a job definition. Jobs can reference other jobs by name or by ID, and can be dependent on the successful completion of other jobs. For more information, see Jobs.

### Job Definitions

A job definition specifies how jobs are to be run; you can think of it as a blueprint for the resources in your job. You can supply your job with an IAM role to provide programmatic access to other AWS resources, and you specify both memory and CPU requirements. The job definition can also control container properties, environment variables, and mount points for persistent storage. Many of the specifications in a job definition can be overridden by specifying new values when submitting individual Jobs. For more information, see Job Definitions

### Job Queues

When you submit an AWS Batch job, you submit it to a particular job queue, where it resides until it is scheduled onto a compute environment. You associate one or more compute environments with a job queue, and you can assign priority values for these compute environments and even across job queues themselves. For example, you could have a high priority queue that you submit time-sensitive jobs to, and a low priority queue for jobs that can run anytime when compute resources are cheaper.

### Compute Environment

A compute environment is a set of managed or unmanaged compute resources that are used to run jobs. Managed compute environments allow you to specify desired instance types at several levels of detail. You can set up compute environments that use a particular type of instance, a particular model such as c4.2xlarge or m4.10xlarge, or simply specify that you want to use the newest instance types. You can also specify the minimum, desired, and maximum number of vCPUs for the environment, along with the amount you are willing to pay for a Spot Instance as a percentage of the On-Demand Instance price and a target set of VPC subnets. AWS Batch will efficiently launch, manage, and terminate EC2 instances as needed. You can also manage your own compute environments. In this case you are responsible for setting up and scaling the instances in an Amazon ECS cluster that AWS Batch creates for you

# AWS Organizations

### Overview

AWS Organizations is an account management service that lets you consolidate multiple AWS accounts into an organization that you create and centrally manage. With AWS Organizations, you can create member accounts and invite existing accounts to join your organization. You can organize those accounts and manage them as a group.

AWS Organizations includes account management and consolidated billing capabilities that enable you to better meet the budgetary, security, and compliance needs of your business. As an administrator of an organization, you can create accounts in your organization and invite existing accounts to join the organization.

AWS Organizations offers the following features:

### Centralized management of all of your AWS accounts

You can combine your existing accounts into an organization that enables you to manage the accounts centrally. You can create accounts that automatically are a part of your organization, and you can invite other accounts to join your organization. You also can attach policies that affect some or all of your accounts.

### Consolidated billing for all member accounts

Consolidated billing is a feature of AWS Organizations. You can use the master account of your organization to consolidate and pay for all member accounts. In consolidated billing, master accounts can also access the billing information, account information, and account activity of member accounts in their organization. This information may be used for services such as Cost Explorer, which can help master accounts improve their organization’s cost performance.

### Hierarchical grouping of your accounts to meet your budgetary, security, or compliance needs

You can group your accounts into organizational units (OUs) and attach different access policies to each OU. For example, if you have accounts that must access only the AWS services that meet certain regulatory requirements, you can put those accounts into one OU. You then can attach a policy to that OU that blocks access to services that do not meet those regulatory requirements. You can nest OUs within other OUs to a depth of five levels, providing flexibility in how you structure your account groups.

### Control over the AWS services and API actions that each account can access

As an administrator of the master account of an organization, you can use service control policies (SCPs) to specify the maximum permissions for member accounts in the organization. In SCPs, you can restrict which AWS services, resources, and individual API actions the users and roles in each member account can access. You can also define conditions for when to restrict access to AWS services, resources, and API actions. These restrictions even override the administrators of member accounts in the organization. When AWS Organizations blocks access to a service, resource, or API action for a member account, a user or role in that account can't access it. This block remains in effect even if an administrator of a member account explicitly grants such permissions in an IAM policy.

# AWS CloudWatch

Amazon CloudWatch is a monitoring and observability service built for DevOps engineers, developers, site reliability engineers (SREs), and IT managers. CloudWatch provides you with data and actionable insights to monitor your applications, respond to system-wide performance changes, optimize resource utilization, and get a unified view of operational health.

CloudWatch collects monitoring and operational data in the form of logs, metrics, and events, providing you with a unified view of AWS resources, applications, and services that run on AWS and on-premises servers.

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.

### Easiest way to collect metrics in AWS and on-premises

Monitoring your AWS resources and applications is easy with CloudWatch. It natively integrates with more than 70 AWS services such as Amazon EC2, Amazon DynamoDB, Amazon S3, Amazon ECS, Amazon EKS, and AWS Lambda, and automatically publishes detailed 1-minute metrics and custom metrics with up to 1-second granularity so you can dive deep into your logs for additional context. You can also use CloudWatch in hybrid cloud architectures by using the CloudWatch Agent or API to monitor your on-premises resources.

Amazon CloudWatch is a monitoring and management service that provides data and actionable insights for AWS, hybrid, and on-premises applications and infrastructure resources. With CloudWatch, you can collect and access all your performance and operational data in form of logs and metrics from a single platform. This allows you to overcome the challenge of monitoring individual systems and applications in silos (server, network, database, etc.). CloudWatch enables you to monitor your complete stack (applications, infrastructure, and services) and leverage alarms, logs, and events data to take automated actions and reduce Mean Time to Resolution (MTTR). This frees up important resources and allows you to focus on building applications and business value.

CloudWatch gives you actionable insights that help you optimize application performance, manage resource utilization, and understand system-wide operational health. CloudWatch provides up to 1-second visibility of metrics and logs data, 15 months of data retention (metrics), and the ability to perform calculations on metrics. This allows you to perform historical analysis for cost optimization and derive real-time insights into optimizing applications and infrastructure resources.

### Container Insights

To monitor, troubleshoot, and alarm on your containerized applications and microservices. CloudWatch collects, aggregates, and summarizes compute utilization information like CPU, memory, disk, and network data, as well as diagnostic information like container restart failures, to help DevOps engineers isolate issues and resolve them quickly. Container Insights gives you insights from container management services such as Amazon ECS for Kubernetes (EKS), Amazon’s Elastic Container Service (ECS), AWS Fargate, and standalone Kubernetes (k8s).

### ServiceLens

You can use Amazon CloudWatch ServiceLens to visualize and analyze the health, performance, and availability of your applications in a single place. CloudWatch ServiceLens ties together CloudWatch metrics and logs as well as traces from AWS X-Ray to give you a complete view of your applications and their dependencies. This enables you to quickly pinpoint performance bottlenecks, isolate root causes of application issues, and determine users impacted. CloudWatch ServiceLens enables you to gain visibility into your applications in three main areas: Infrastructure monitoring (using metrics and logs to understand the resources supporting your applications), transaction monitoring (using traces to understand dependencies between your resources), and end user monitoring (using canaries to monitor your endpoints and notify you when your end user experience has degraded). CloudWatch ServiceLens provides a Service Map that visualizes the contextual linking of all your resources, along with an intuitive interface so you can dive deep into correlated monitoring data.

### Synthetics

Amazon CloudWatch Synthetics allows you to monitor application endpoints more easily. It runs tests on your endpoints every minute, 24x7, and alerts you as soon as your application endpoints don’t behave as expected. These tests can be customized to check for availability, latency, transactions, broken or dead links, step by step task completions, page load errors, load latencies for UI assets, complex wizard flows, or checkout flows in your applications. You can also use CloudWatch Synthetics to isolate alarming application endpoints and map them back to underlying infrastructure issues to reduce mean time to resolution. With this new feature, CloudWatch now collects canary traffic, which can continually verify your customer experience even when you don’t have any customer traffic on your applications, enabling you to discover issues before your customers do. CloudWatch Synthetics supports monitoring of your REST APIs, URLs, and website content, checking for unauthorized changes from phishing, code injection and cross-site scripting.

# AWS CloudFormation

### Overview

AWS AWS CloudFormation enables you to create and provision AWS infrastructure deployments predictably and repeatedly. It helps you leverage AWS products such as Amazon EC2, Amazon Elastic Block Store, Amazon SNS, Elastic Load Balancing, and Auto Scaling to build highly reliable, highly scalable, cost-effective applications in the cloud without worrying about creating and configuring the underlying AWS infrastructure. AWS CloudFormation enables you to use a template file to create and delete a collection of resources together as a single unit (a stack).

AWS CloudFormation is a service that helps you model and set up your Amazon Web Services resources so that you can spend less time managing those resources and more time focusing on your applications that run in AWS. You create a template that describes all the AWS resources that you want (like Amazon EC2 instances or Amazon RDS DB instances), and AWS CloudFormation takes care of provisioning and configuring those resources for you. You don't need to individually create and configure AWS resources and figure out what's dependent on what; AWS CloudFormation handles all of that. The following scenarios demonstrate how AWS CloudFormation can help

### Simplify Infrastructure Management

For a scalable web application that also includes a back-end database, you might use an Auto Scaling group, an Elastic Load Balancing load balancer, and an Amazon Relational Database Service database instance. Normally, you might use each individual service to provision these resources. And after you create the resources, you would have to configure them to work together. All these tasks can add complexity and time before you even get your application up and running.

Instead, you can create or modify an existing AWS CloudFormation template. A template describes all of your resources and their properties. When you use that template to create an AWS CloudFormation stack, AWS CloudFormation provisions the Auto Scaling group, load balancer, and database for you. After the stack has been successfully created, your AWS resources are up and running. You can delete the stack just as easily, which deletes all the resources in the stack. By using AWS CloudFormation, you easily manage a collection of resources as a single unit.

### Quickly Replicate Your Infrastructure

If your application requires additional availability, you might replicate it in multiple regions so that if one region becomes unavailable, your users can still use your application in other regions. The challenge in replicating your application is that it also requires you to replicate your resources. Not only do you need to record all the resources that your application requires, but you must also provision and configure those resources in each region.

When you use AWS CloudFormation, you can reuse your template to set up your resources consistently and repeatedly. Just describe your resources once and then provision the same resources over and over in multiple regions.

### Easily Control and Track Changes to Your Infrastructure

In some cases, you might have underlying resources that you want to upgrade incrementally. For example, you might change to a higher performing instance type in your Auto Scaling launch configuration so that you can reduce the maximum number of instances in your Auto Scaling group. If problems occur after you complete the update, you might need to roll back your infrastructure to the original settings. To do this manually, you not only have to remember which resources were changed, you also have to know what the original settings were.

When you provision your infrastructure with AWS CloudFormation, the AWS CloudFormation template describes exactly what resources are provisioned and their settings. Because these templates are text files, you simply track differences in your templates to track changes to your infrastructure, similar to the way developers control revisions to source code. For example, you can use a version control system with your templates so that you know exactly what changes were made, who made them, and when. If at any point you need to reverse changes to your infrastructure, you can use a previous version of your template.

# AWS CloudTrail

### Overview

AWS CloudTrail is an AWS service that helps you enable governance, compliance, and operational and risk auditing 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.

CloudTrail is enabled on your AWS account when you create it. When activity occurs in your AWS account, that activity is recorded in a CloudTrail event. You can easily view recent events in the CloudTrail console by going to Event history

Visibility into your AWS account activity is a key aspect of security and operational best practices. You can use CloudTrail to view, search, download, archive, analyze, and respond to account activity across your AWS infrastructure. You can identify who or what took which action, what resources were acted upon, when the event occurred, and other details to help you analyze and respond to activity in your AWS account. Optionally, you can enable AWS CloudTrail Insights on a trail to help you identify and respond to unusual activity.

You can integrate CloudTrail into applications using the API, automate trail creation for your organization, check the status of trails you create, and control how users view CloudTrail events.

### View event history for your AWS account

You can troubleshoot operational and security incidents over the past 90 days in the CloudTrail console by viewing Event history. You can look up events related to creation, modification, or deletion of resources (such as IAM users or Amazon EC2 instances) in your AWS account on a per-region basis.

Events can be viewed and downloaded by using the AWS CloudTrail console. You can customize the view of event history in the console by selecting which columns are displayed and which are hidden. You can programmatically look up events by using the AWS SDKs or AWS Command Line Interface.

# AWS Command Line Interface

### Overview

AWS Command Line Interface (AWS CLI) is a unified tool that provides a consistent interface for interacting with all parts of AWS. AWS CLI commands for different services are covered in the accompanying user guide, including descriptions, syntax, and usage examples.

The AWS Command Line Interface (AWS CLI) is an open source tool that enables you to interact with AWS services using commands in your command-line shell. With minimal configuration, the AWS CLI enables you to start running commands that implement functionality equivalent to that provided by the browser-based AWS Management Console from the command prompt in your favorite terminal program

# Global Infrastructure

The AWS Global Cloud Infrastructure is the most secure, extensive, and reliable cloud platform, offering over 175 fully featured services from data centers globally. Whether you need to deploy your application workloads across the globe in a single click, or you want to build and deploy specific applications closer to your end-users with single-digit millisecond latency, AWS provides you the cloud infrastructure where and when you need it.

### Security

* Our infrastructure is monitored 24/7 to help ensure the confidentiality, integrity, and availability of your data.
* All data flowing across the AWS global network that interconnects our data centers and Regions is automatically encrypted at the physical layer before it leaves our secured facilities.
* You can build on the most secure global infrastructure, knowing you always control your data, including the ability to encrypt it, move it, and manage retention at any time.

### Availability

* AWS delivers the highest network availability of any cloud provider, with 7x fewer down time hours than the next largest cloud provider.
* Each region is fully isolated and comprised of multiple AZ’s, which are fully isolated partitions of our infrastructure. To better isolate any issues and achieve high availability, you can partition applications across multiple AZ’s in the same region.
* In addition, AWS control planes and the AWS management console are distributed across regions, and include regional API endpoints, which are designed to operate securely for at least 24 hours if isolated from the global control plane functions without requiring customers to access the region or its API endpoints via external networks during any isolation.

### Performance

* The AWS Global Infrastructure is built for performance. AWS Regions offer low latency, low packet loss, and high overall network quality.
* This is achieved with a fully redundant 100 GbE fiber network backbone, often providing many terabits of capacity between Regions.
* AWS Local Zones and AWS Wavelength, with our telco providers, provide performance for applications that require single-digit millisecond latencies by delivering AWS infrastructure and services closer to end-users and 5G connected devices.

### Flexibility

* If you need to run your applications with single-digit millisecond latencies to mobile devices and end-users you can choose AWS Local Zones or AWS Wavelength
* Or if you would like to run your applications on-premises you can choose AWS Outposts.

# AWS Local Zones

### Overview

Run latency sensitive applications closer to end-users. With AWS Local Zones, you can easily build and deploy latency-sensitive applications closer to your end-users using a consistent set of AWS services, scale up or scale down, and pay only for the resources that you use

### Brain Dump

AWS Local Zones are a new type of AWS infrastructure deployment that places AWS compute, storage, database, and other select services closer to large population, industry, and IT centers **where no AWS Region exists today**.

With AWS Local Zones, you can easily run latency-sensitive portions of applications local to end-users and resources in a specific geography, delivering single-digit millisecond latency for use cases such as media & entertainment content creation, real-time gaming, reservoir simulations, electronic design automation, and machine learning.

# AWS Wavelength

### Overview

Deliver ultra-low latency applications for 5G devices

### Brain Dump

AWS Wavelength enables developers to build applications that deliver single-digit millisecond latencies to mobile devices and end-users. AWS developers can deploy their applications to Wavelength Zones, AWS infrastructure deployments that embed AWS compute and storage services within the telecommunications providers’ datacenters at the edge of the 5G networks, and seamlessly access the breadth of AWS services in the region. This enables developers to deliver applications that require single-digit millisecond latencies such as game and live video streaming, machine learning inference at the edge, and augmented and virtual reality (AR/VR).

AWS Wavelength brings AWS services to the edge of the 5G network, minimizing the latency to connect to an application from a mobile device. Application traffic can reach application servers running in Wavelength Zones without leaving the mobile provider’s network. This reduces the extra network hops to the Internet that can result in latencies of more than 100 milliseconds, preventing customers from taking full advantage of the bandwidth and latency advancements of 5G.

Wavelength delivers a consistent developer experience across multiple 5G networks around the world, allowing you to build the next generation of ultra-low latency applications using familiar AWS services, APIs, and tools.

You can simply extend your Amazon Virtual Private Cloud (VPC) to one or more Wavelength Zones and then use AWS resources like Amazon Elastic Compute Cloud (EC2) instances, Amazon Elastic Block Storage (EBS) volumes, AWS Elastic Container Service (ECS), Amazon Elastic Kubernetes Services (EKS), AWS Identity and Access Management (IAM), AWS CloudFormation, and AWS Autoscaling to build, run, secure, manage, and scale your applications.

With just an AWS account, you can deploy your 5G applications in Wavelength Zones and seamlessly connect to applications and services in AWS Regions. Wavelength offers you the flexibility to scale up or scale down, and pay only for the resources that you use.

# AWS Outposts

### Overview

Run AWS infrastructure and services on premises for a truly consistent hybrid experience.

### Brain Dump

AWS Outposts is a fully managed service that extends AWS infrastructure, AWS services, APIs, and tools to virtually any datacenter, co-location space, or on-premises facility for a truly consistent hybrid experience. AWS Outposts is ideal for workloads that require low latency access to on-premises systems, local data processing, or local data storage.

# AWS Ground Station

### Overview

AWS Ground Station is a fully managed service that lets you control satellite communications, process data, and scale your operations without having to worry about building or managing your own ground station infrastructure.

### Brain Dump

* Satellites are used for a wide variety of use cases, including weather forecasting, surface imaging, communications, and video broadcasts. Ground stations form the core of global satellite networks.
* With AWS Ground Station, you have direct access to AWS services and the AWS Global Infrastructure including a low-latency global fiber network. For example, you can use Amazon S3 to store the downloaded data, Amazon Kinesis Data Streams for managing data ingestion from satellites, Amazon SageMaker for building custom machine learning applications that apply to your data sets.
* You can save up to 80% on the cost of your ground station operations by paying only for the actual antenna time used, and relying on the global footprint of ground stations to download data when and where you need it.
* There are no long-term commitments, and you gain the ability to rapidly scale your satellite communications on-demand when your business needs it.

# AWS Simple Notification Service

Amazon Simple Notification Service (SNS) is a highly available, durable, secure, fully managed pub/sub messaging service that enables you to decouple micro services, distributed systems, and server-less application. Amazon SNS provides topics for high-throughput, push-based, many-to-many messaging. Using Amazon SNS topics, your publisher systems can fan out messages to a large number of subscriber endpoints for parallel processing, including [Amazon SQS](https://aws.amazon.com/sqs/) queues, [AWS Lambda](https://aws.amazon.com/lambda/) functions, and HTTP/S webhooks. Additionally, SNS can be used to fan out notifications to end users using mobile push, SMS, and email.

# Amazon CloudFront

### Overview

Fast, highly secure and programmable content delivery network (CDN)

### Brain Dump

Amazon CloudFront is a fast content delivery network (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 is integrated with AWS – both physical locations that are directly connected to the AWS global infrastructure, as well as other AWS services. CloudFront works seamlessly with services including AWS Shield for DDoS mitigation, Amazon S3, Elastic Load Balancing or Amazon EC2 as origins for your applications, and Lambda@Edge to run custom code closer to customers’ users and to customize the user experience

Lastly, if you use AWS origins such as Amazon S3, Amazon EC2 or Elastic Load Balancing, you don’t pay for any data transferred between these services and CloudFront.

### Fast & global

The Amazon CloudFront content delivery network (CDN) is massively scaled and globally distributed. The CloudFront network has 216 points of presence (PoPs), and leverages the highly-resilient Amazon backbone network for superior performance and availability for your end users.

### Security at the Edge

Amazon CloudFront is a highly-secure CDN that provides both network and application level protection. Your traffic and applications benefit through a variety of built-in protections such as AWS Shield Standard, at no additional cost. You can also use configurable features such as AWS Certificate Manager (ACM) to create and manage custom SSL certificates at no extra cost.

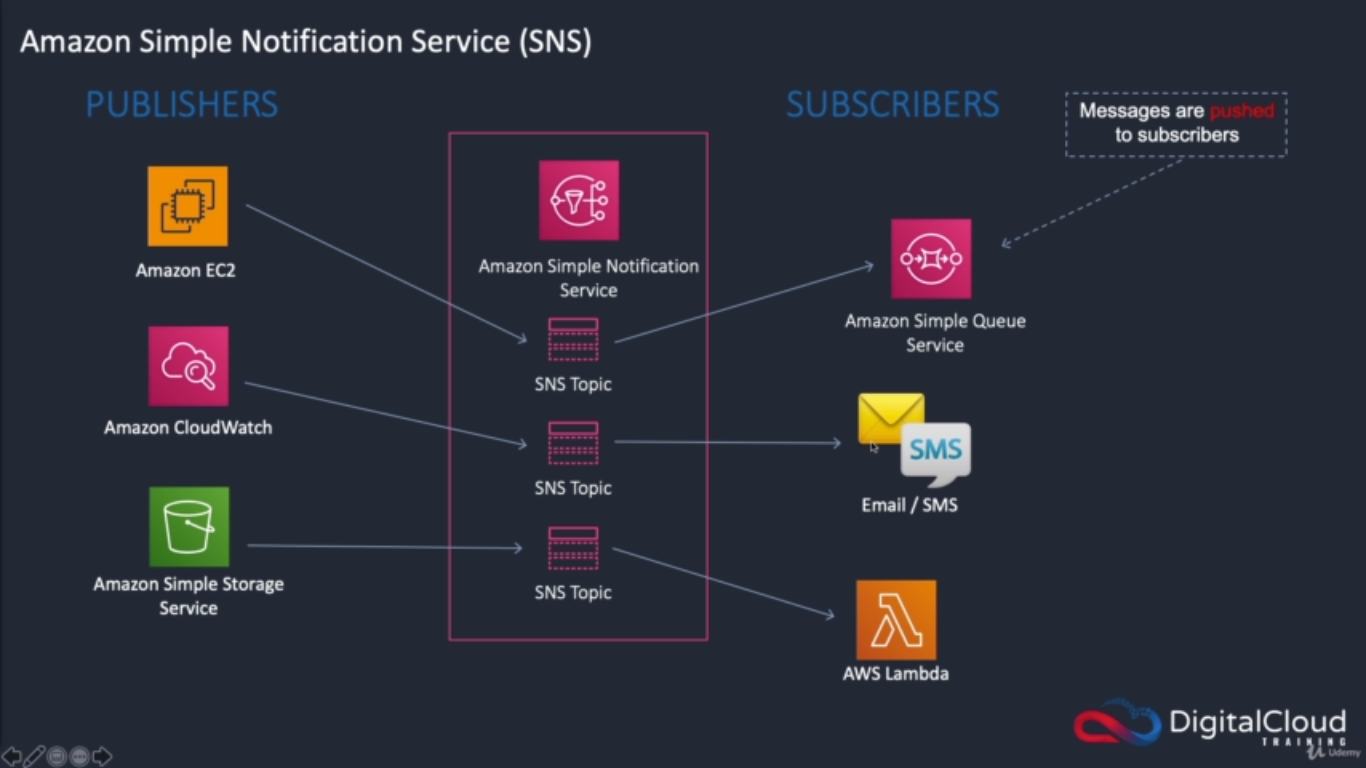
# AWS WAF

AWS WAF (Web Application Firewall) helps protect your web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources. You can use AWS WAF to create custom rules that block common attack patterns, such as SQL injection or cross-site scripting, and rules that are designed for your specific application.

# AWS SNS

### Overview

Amazon SNS - Fully managed pub/sub messaging for microservices, distributed systems, and serverless applications. Using Amazon SNS topics, your publisher systems can fan out messages to a large number of subscriber endpoints for parallel processing



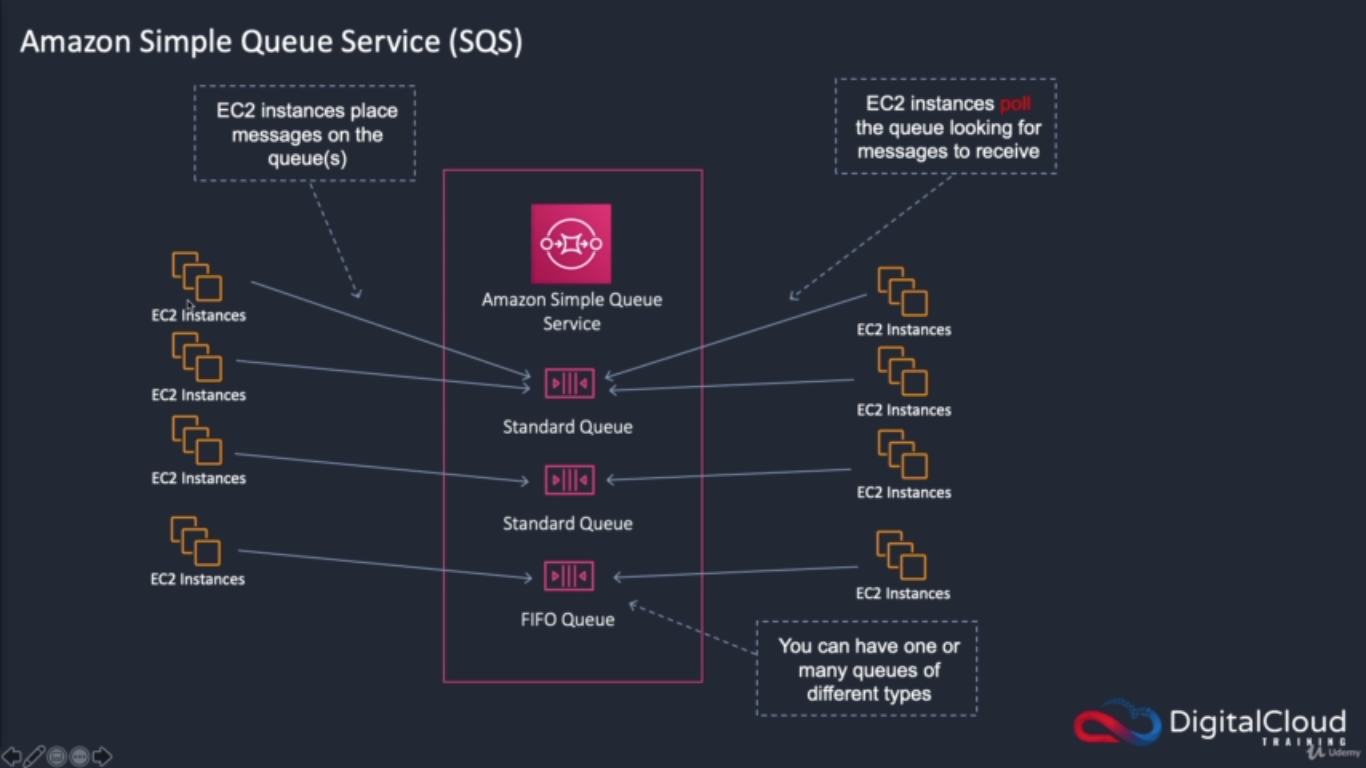


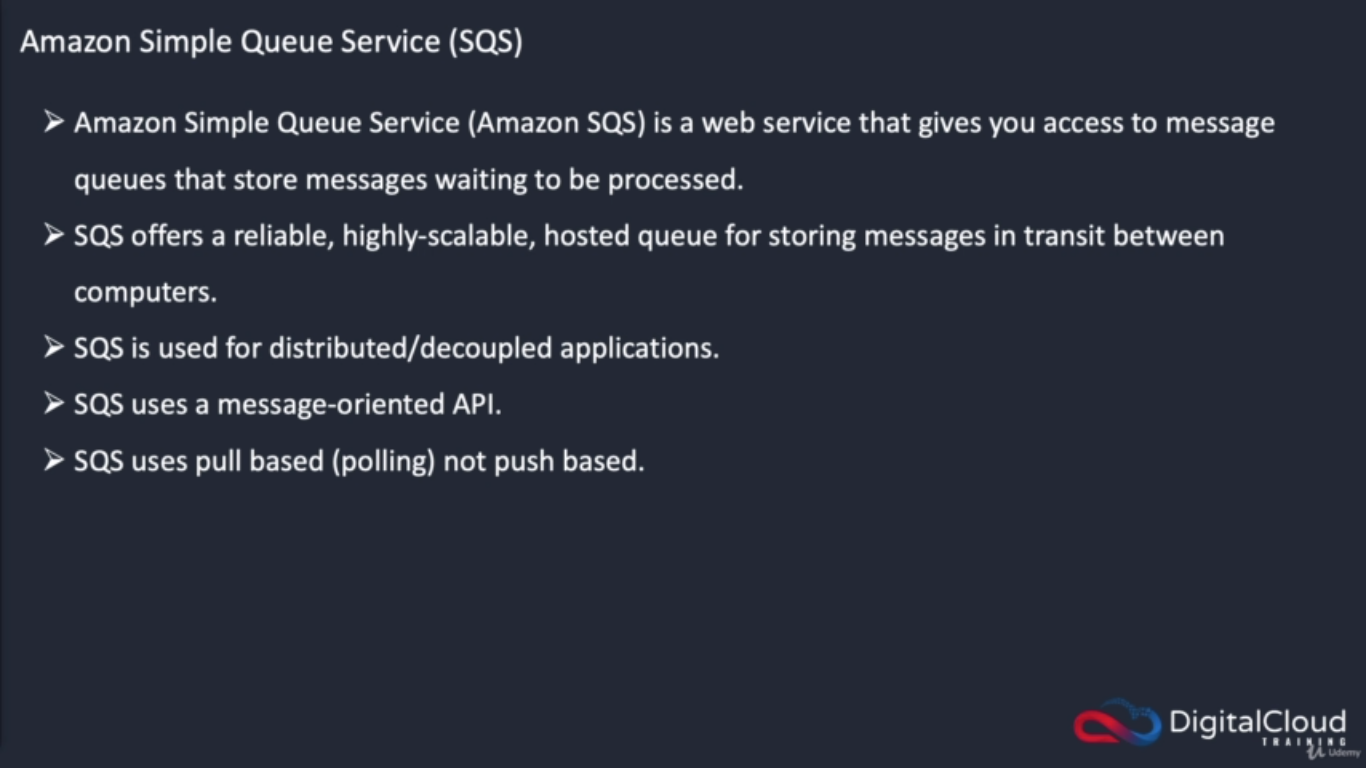
# AWS SQS

### Overview

Amazon SQS - Fully managed message queues for microservices, distributed systems, and serverless applications. 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.





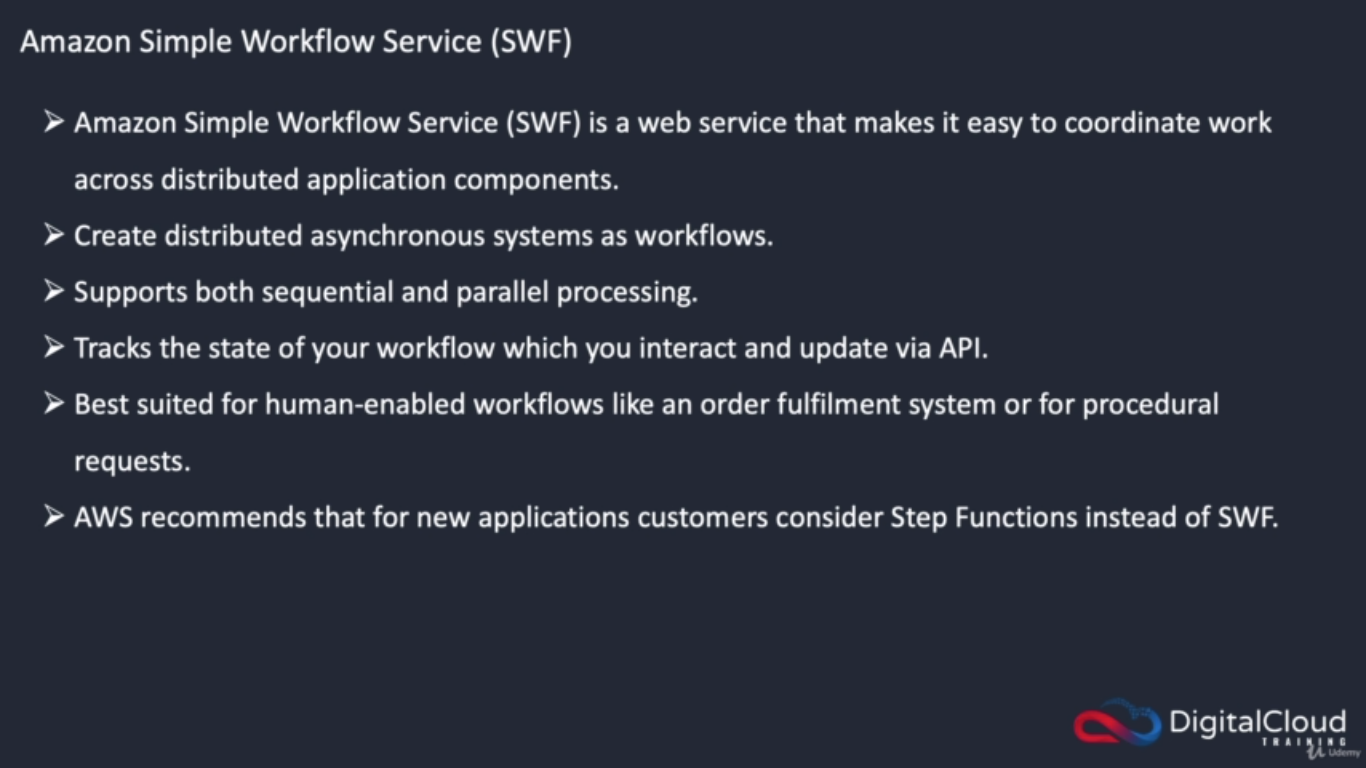
# AWS SWF

### Overview

Amazon Simple Workflow Service (SWF)

Amazon SWF helps developers build, run, and scale background jobs that have parallel or sequential steps. You can think of Amazon SWF as a fully-managed state tracker and task coordinator in the Cloud.

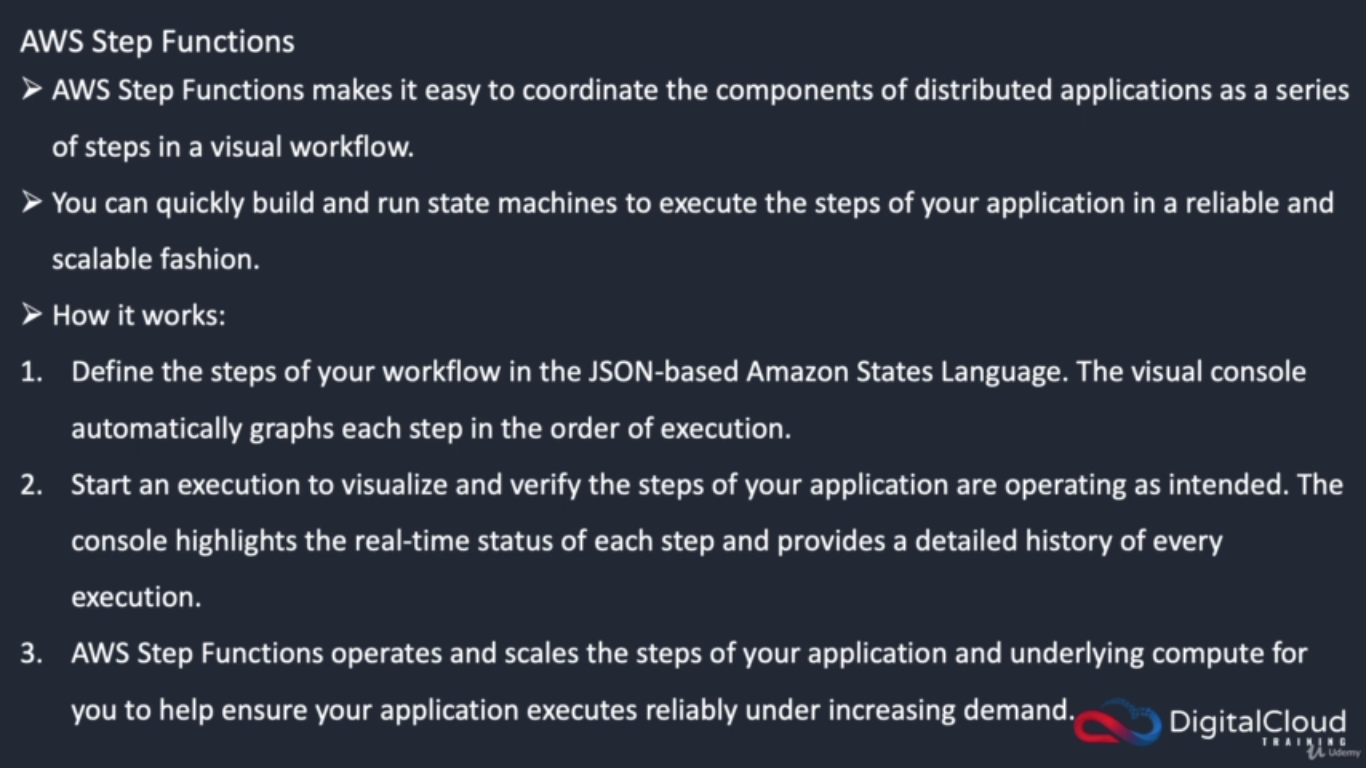
If your app's steps take more than 500 milliseconds to complete, you need to track the state of processing, and you need to recover or retry if a task fails, Amazon SWF can help you.



# AWS Step Functions

### Overview

AWS Step Functions lets you coordinate multiple AWS services into serverless workflows so you can build and update apps quickly. Using Step Functions, you can design and run workflows that stitch together services, such as AWS Lambda, AWS Fargate, and Amazon SageMaker, into feature-rich applications. Workflows are made up of a series of steps, with the output of one step acting as input into the next. Application development is simpler and more intuitive using Step Functions, because it translates your workflow into a state machine diagram that is easy to understand, easy to explain to others, and easy to change. Step Functions automatically triggers and tracks each step, and retries when there are errors, so your application executes in order and as expected. With Step Functions, you can craft long-running workflows such as machine learning model training, report generation, and IT automation. You can also build high volume, short duration workflows such as IoT data ingestion, and streaming data processing.

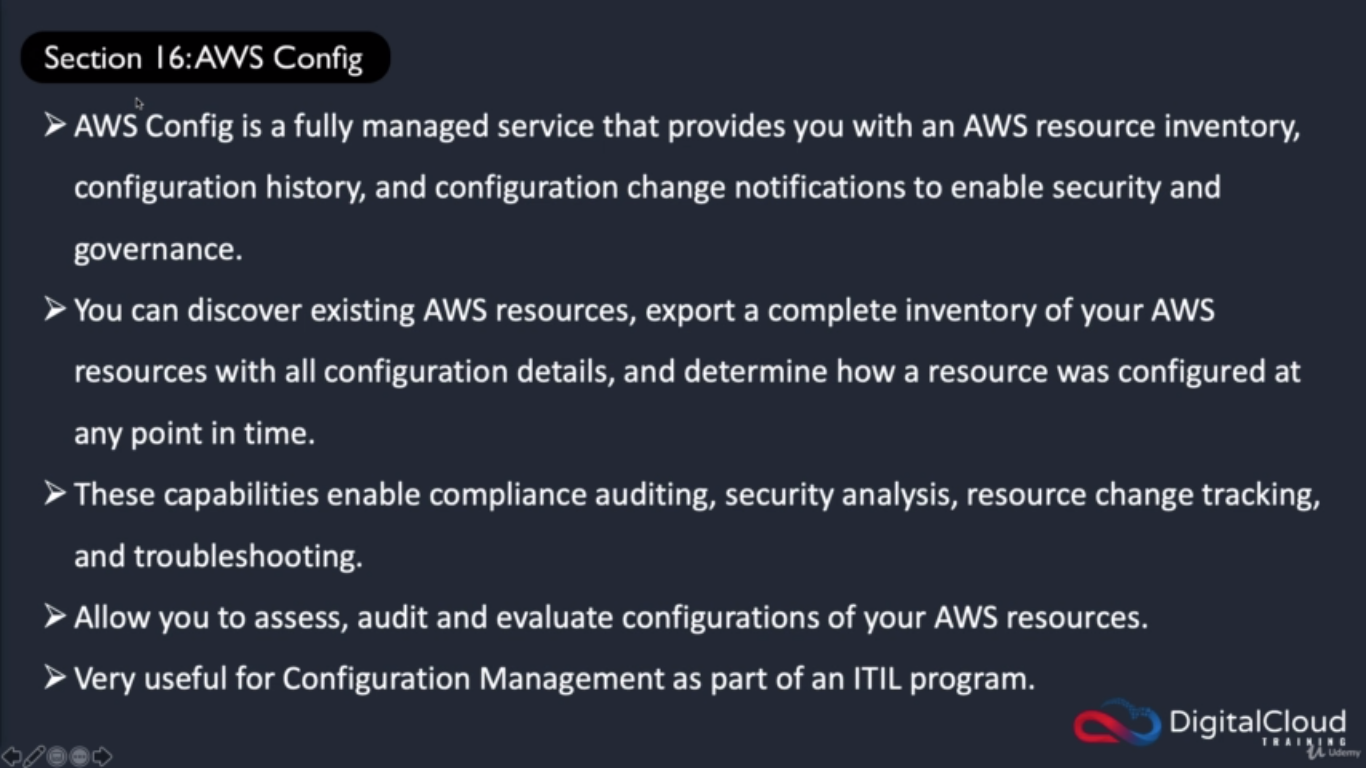


# AWS Config

### Overview

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



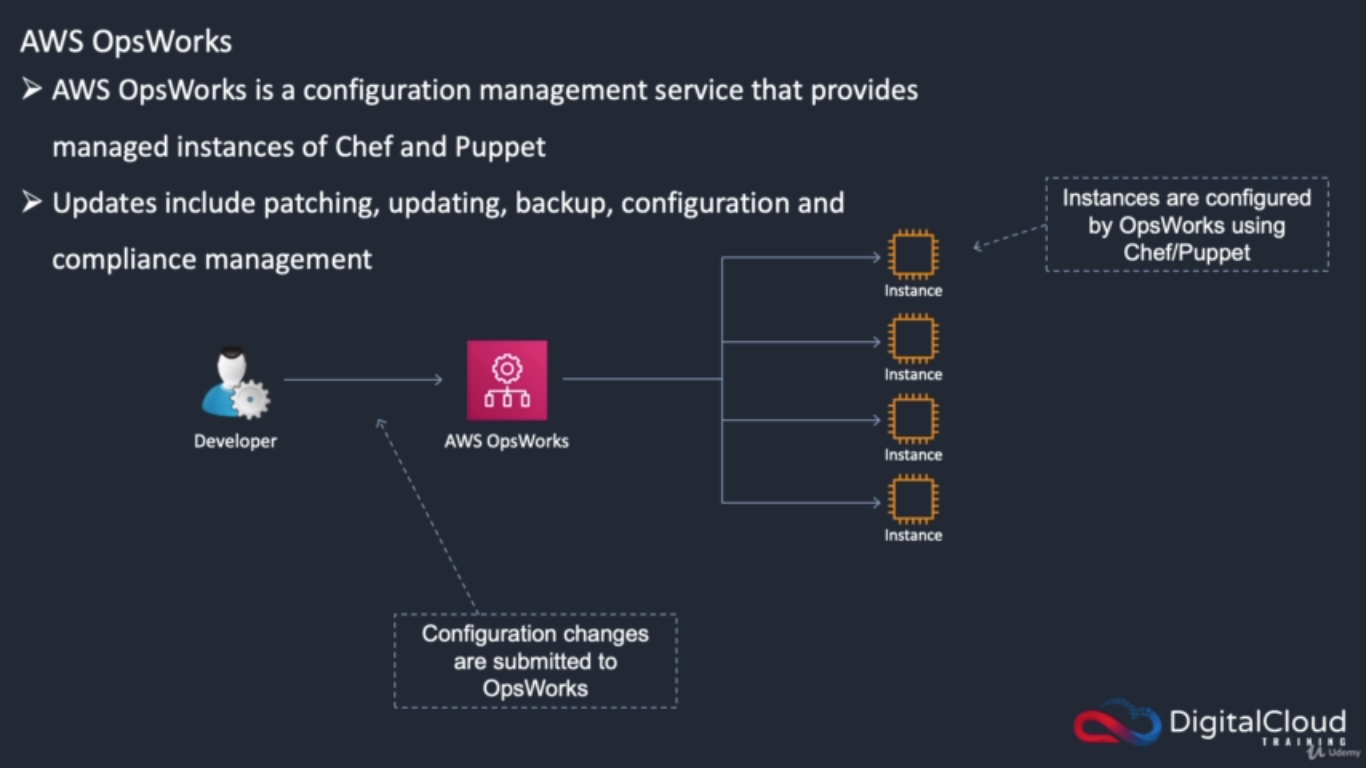


# AWS OpsWorks

### Overview

AWS 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.



# AWS Systems Manager

### Overview

Gain operational insights and take action on AWS resources. 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.

With Systems Manager, you can group resources, like Amazon EC2 instances, Amazon S3 buckets, or Amazon RDS instances, by application, view operational data for monitoring and troubleshooting, and take action on your groups of resources. Systems Manager simplifies resource and application management, shortens the time to detect and resolve operational problems, and makes it easy to operate and manage your infrastructure securely at scale.

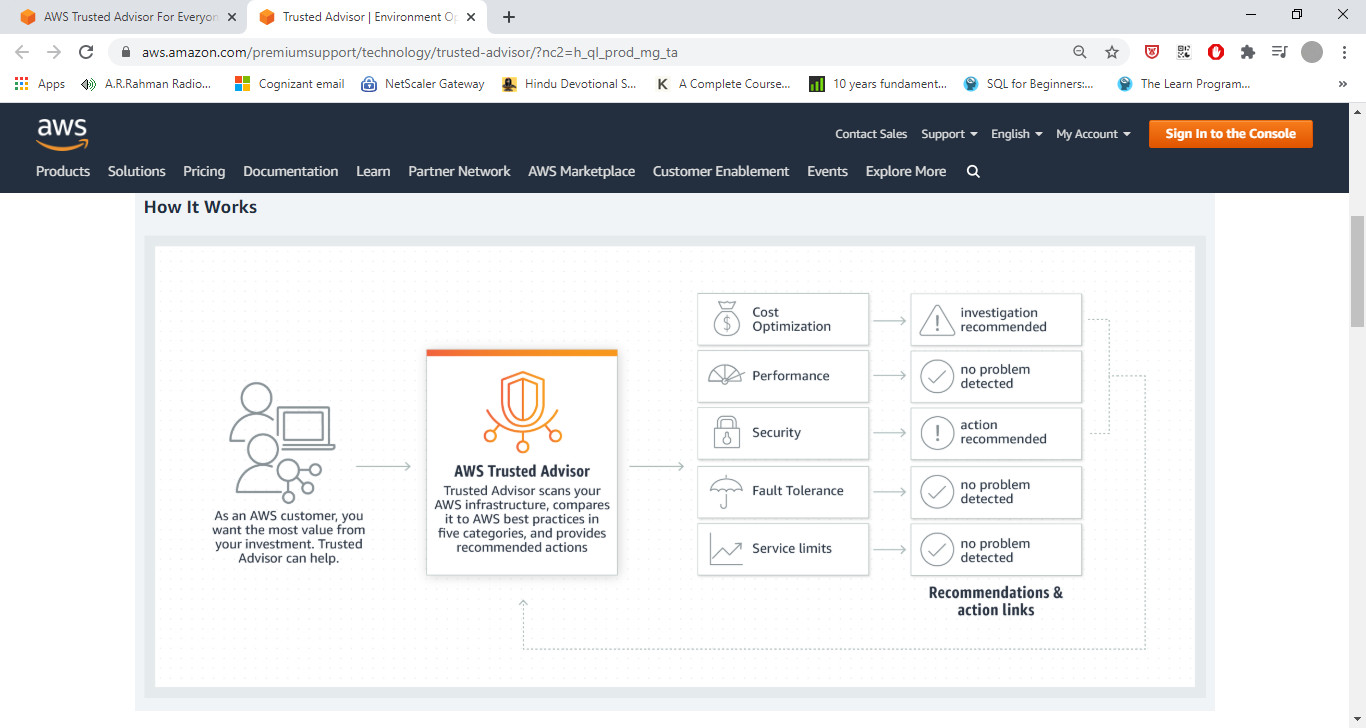


# AWS Trusted Advisor

### Overview

AWS Trusted Advisor is an online tool that provides you real time guidance to help you provision your resources following AWS best practices.

Whether establishing new workflows, developing applications, or as part of ongoing improvement, take advantage of the recommendations provided by Trusted Advisor on a regular basis to help keep your solutions provisioned optimally.



# AWS Service Catelog

### Overview

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 commonly deployed IT services, and helps you achieve consistent governance and meet your compliance requirements, while enabling users to quickly deploy only the approved IT services they need.

### Benefits:

**Ensure compliance with corporate standards**

AWS Service Catalog provides a single location where organizations can centrally manage catalogs of IT services. With AWS Service Catalog you can control which IT services and versions are available, the configuration of the available services, and permission access by individual, group, department, or cost center.

**Centrally manage IT service lifecycle**

AWS Service Catalog enables you to add new versions of IT services as necessary, and end users are notified so they can easily keep abreast of the latest updates. With AWS Service Catalog you can control the use of IT services by specifying constraints, such as the AWS region in which a product can be launched or allowed IP ranges.

**Help employees quickly find and deploy approved IT services**

With AWS Service Catalog, you define your own catalog of AWS services and AWS Marketplace software, and make them available for your organization. Then, end users can quickly discover and deploy IT services using a self-service portal.

# AWS Personal Health Dashboard

### Overview

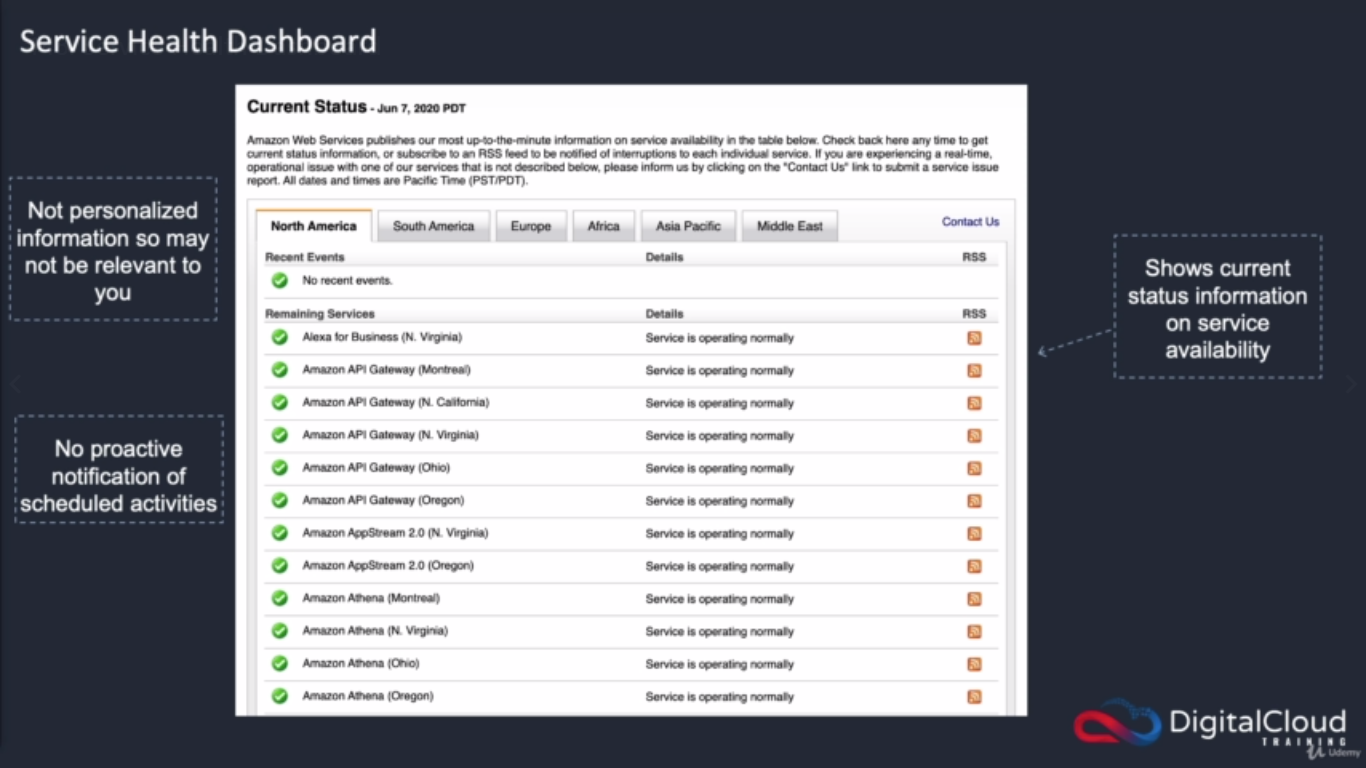
AWS Personal Health Dashboard provides alerts and remediation guidance when AWS is experiencing events that may impact you. While the Service Health Dashboard displays the general status of AWS services, Personal Health Dashboard gives you a personalized view into the performance and availability of 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.

# AWS Service Health Dashboard

### Overview

AWS Amazon Web Services publishes our most up-to-the-minute information on service availability in the table below. Check back here any time to get current status information, or subscribe to an RSS feed to be notified of interruptions to each individual service. If you are experiencing a real-time, operational issue with one of our service.



# AWS Shared Responsibility

### Overview

Need to Add

# AWS Cloud compliance and AWS Artifact

### Overview

Need to Add

# AWS Organizations Service Control Policies(SCP)

### Overview

Need to Add

# AWS Inspector

### Overview

Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS. Amazon Inspector automatically assesses applications for exposure, vulnerabilities, and deviations from best practices. After performing an assessment, Amazon Inspector produces a detailed list of security findings prioritized by level of severity. These findings can be reviewed directly or as part of detailed assessment reports which are available via the Amazon Inspector console or API.

Amazon Inspector security assessments help you check for unintended network accessibility of your Amazon EC2 instances and for vulnerabilities on those EC2 instances. Amazon Inspector assessments are offered to you as pre-defined rules packages mapped to common security best practices and vulnerability definitions. Examples of built-in rules include checking for access to your EC2 instances from the internet, remote root login being enabled, or vulnerable software versions installed. These rules are regularly updated by AWS security researchers.What is an assessment template?

An assessment template is a configuration that you create in Amazon Inspector to define your assessment run. This assessment template includes a rules package against which you want Amazon Inspector to evaluate your assessment target, the duration of the assessment run, Amazon Simple Notification Service (SNS) topics to which you want Amazon Inspector to send notifications about assessment run states and findings, and Amazon Inspector-specific attributes (key/value pairs) that you can assign to findings generated by the assessment run.

# AWS Managed Services

As enterprise customers move towards adopting the cloud at scale, some find their people need help and time to gain AWS skills and experience. AWS Managed Services (AMS) operates AWS on your behalf, providing a secure and compliant AWS Landing Zone, a proven enterprise operating model, on-going cost optimization, and day-to-day infrastructure management. By implementing best practices to maintain your infrastructure, AWS Managed Services helps to reduce your operational overhead and risk.

AWS Managed Services automates common activities, such as change requests, monitoring, patch management, security, and backup services, and provides full-lifecycle services to provision, run, and support your infrastructure. AWS Managed Services unburdens you from infrastructure operations so you can direct resources toward differentiating your business.

# AWS EMR

Amazon EMR is the industry-leading cloud big data platform for processing vast amounts of data using open source tools such as Apache Spark, Apache Hive, Apache HBase, Apache Flink, Apache Hudi, and Presto. With EMR you can run Petabyte-scale analysis at less than half of the cost of traditional on-premises solutions and over 3x faster than standard Apache Spark.

For short-running jobs, you can spin up and spin down clusters and pay per second for the instances used. For long-running workloads, you can create highly available clusters that automatically scale to meet demand. If you have existing on-premises deployments of open source tools such as Apache Spark and Apache Hive, you can also run EMR clusters

AWS Outposts

AWS Outposts offers you the same AWS hardware infrastructure, services, APIs, and tools to build and run your applications on premises and in the cloud for a truly consistent hybrid experience. AWS compute, storage, database, and other services run locally on Outposts, and you can access the full range of AWS services available in the Region to build, manage, and scale your on-premises applications using familiar AWS services and tools.

Outposts are connected to the nearest AWS Region to provide the same management and control plane services on premises for a truly consistent operational experience across your on-premises and cloud environments. Your Outposts infrastructure and AWS services are managed, monitored, and updated by AWS just like in the cloud.

# AWS Transit Gateway

AWS Transit Gateway connects VPCs and on-premises networks through a central hub. This simplifies your network and puts an end to complex peering relationships. It acts as a cloud router – each new connection is only made once.

# AWS WAF & Shield

### Overview

Amazon WAF (Web Application Firewall)

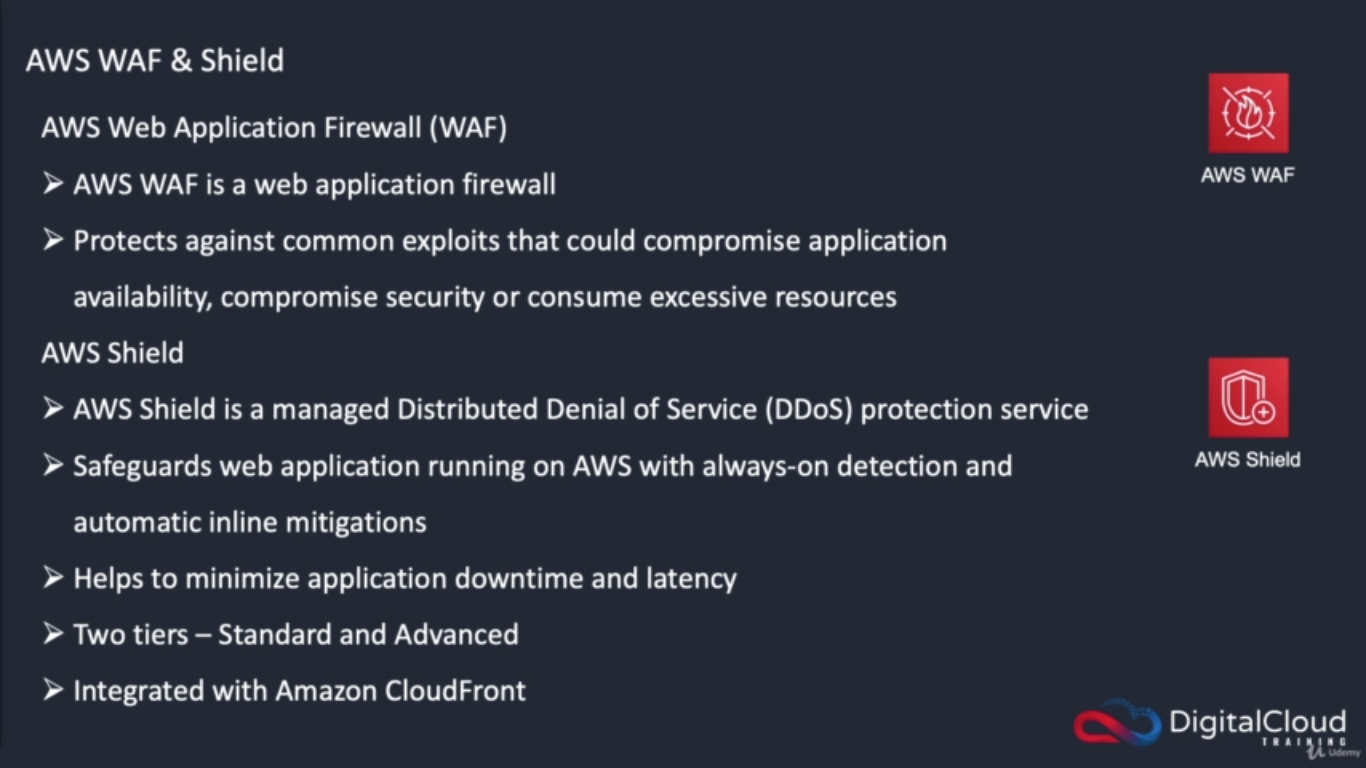
AWS WAF protects your web applications from common web exploits. AWS WAF is a web application firewall service that lets you monitor web requests that are forwarded to an Amazon API Gateway API, an Amazon CloudFront distribution, or an Application Load Balancer. You can protect those resources based on conditions that you specify, such as the IP addresses that the requests originate from.

AWS Sheild

As an AWS customer, you automatically have basic DDoS protection with the AWS Shield Standard plan, at no additional cost beyond what you already pay for AWS WAF and your other AWS services. For an additional cost, you can get advanced DDoS protection by activating the AWS Shield Advanced plan

Standard (Free and activated to all accounts)

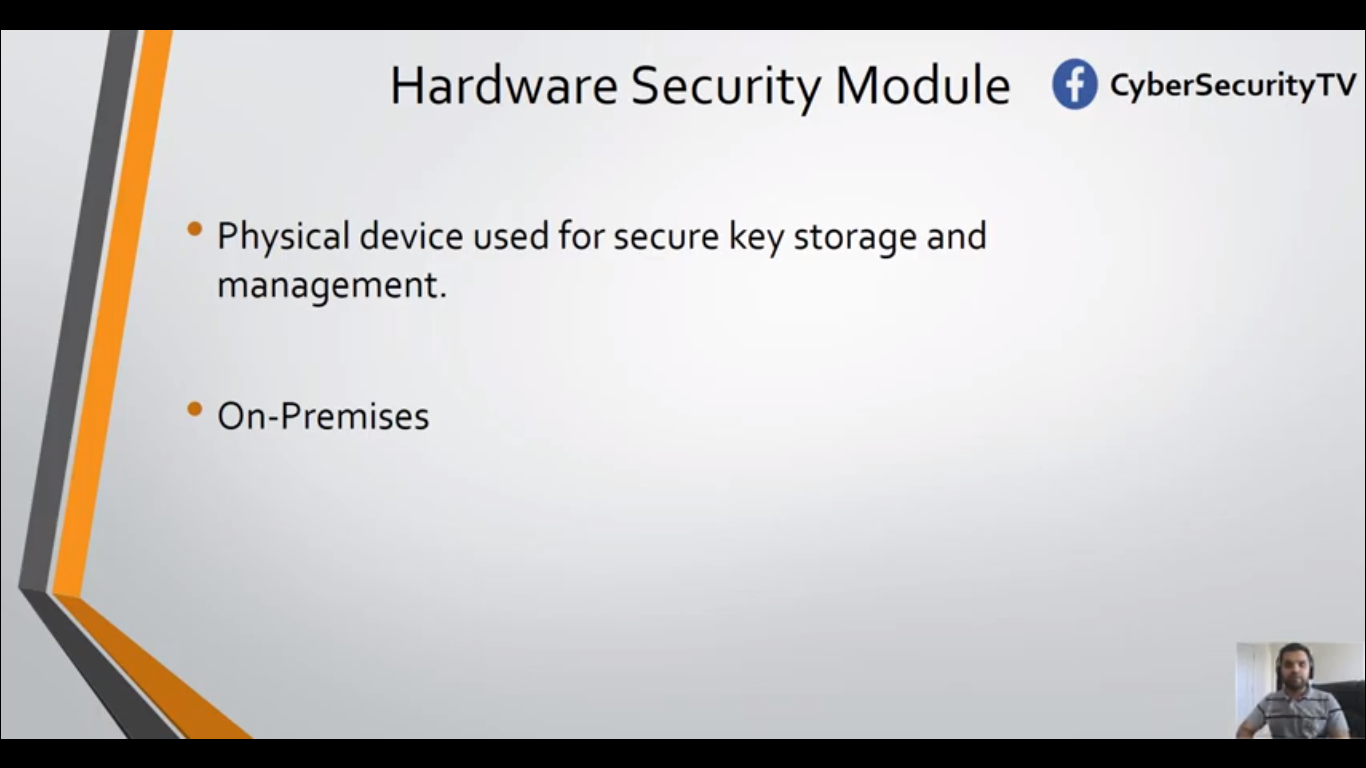
Advanced

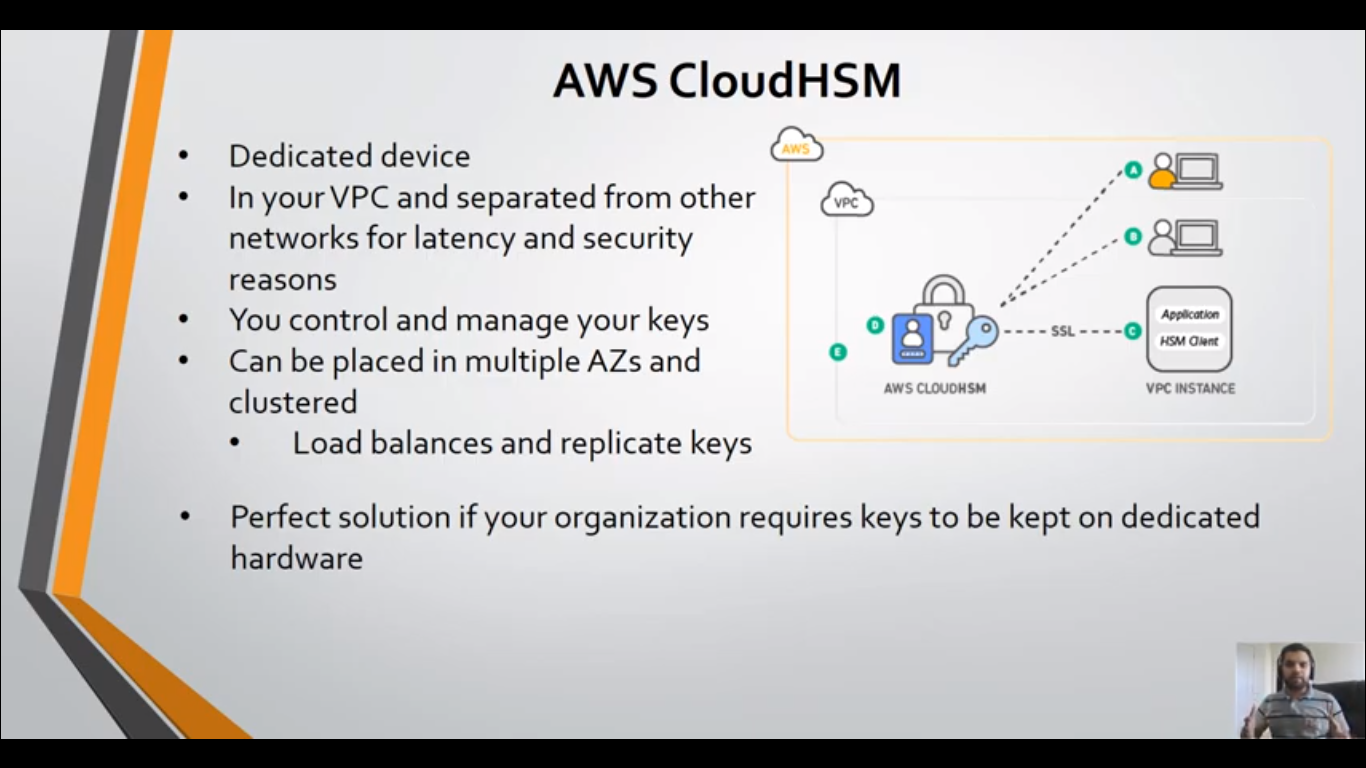


# AWS HSM (Hardware Security Module)

### Overview

Amazon HSM (Hardware security Module) is a dedicated device to store the keys.





# AWS Athena

### Overview

Amazon Athena is an interactive query service that makes it easy to analyze data directly in Amazon Simple Storage Service (Amazon S3) using standard SQL. With a few actions in the AWS Management Console, you can point Athena at your data stored in Amazon S3 and begin using standard SQL to run ad-hoc queries and get results in seconds.

Athena is serverless, so there is no infrastructure to set up or manage, and you pay only for the queries you run. Athena scales automatically—executing queries in parallel—so results are fast, even with large datasets and complex queries.

# Amazon QuickSight

### Overview

Amazon QuickSight is a fast business analytics service to build visualizations, perform ad hoc analysis, and quickly get business insights from your data. Amazon QuickSight seamlessly discovers AWS data sources, enables organizations to scale to hundreds of thousands of users, and delivers fast and responsive query performance by using a robust in-memory engine (SPICE).

# Amazon Kinesis

### Overview

Amazon Kinesis makes it easy to collect, process, and analyze video and data streams in real time.

### Video Streams

Capture, process, and store video streams for analytics and machine learning.

### Data Streams

Build custom applications that analyze data streams using popular stream-processing frameworks.

### Data Firehose

Load data streams into AWS data stores

### Data Analytics

Process and analyze streaming data using SQL or Java.

# Amazon Data Pipeline

### Overview

AWS Data Pipeline is a web service that you can use to automate the movement and transformation of data. With AWS Data Pipeline, you can define data-driven workflows, so that tasks can be dependent on the successful completion of previous tasks.

# Amazon Glue

### Overview

AWS Glue is a fully managed ETL (extract, transform, and load) service that makes it simple and cost-effective to categorize your data, clean it, enrich it, and move it reliably between various data stores. AWS Glue consists of a central data repository known as the AWS Glue Data Catalog, an ETL engine that automatically generates Python code, and a flexible scheduler that handles dependency resolution, job monitoring, and retries. AWS Glue is serverless, so there's no infrastructure to set up or manage. Use the AWS Glue console to discover your data, transform it, and make it available for search and querying. You can also use the AWS Glue API operations to interface with AWS Glue

# Amazon Elastic Beanstalk

WS Elastic Beanstalk is an easy-to-use service for deploying and scaling web applications and services developed with Java, .NET, PHP, Node.js, Python, Ruby, Go, and Docker on familiar servers such as Apache, Nginx, Passenger, and IIS.

You can simply upload your code and Elastic Beanstalk automatically handles the deployment, from capacity provisioning, load balancing, auto-scaling to application health monitoring. At the same time, you retain full control over the AWS resources powering your application and can access the underlying resources at any time.There is no additional charge for Elastic Beanstalk - you pay only for the AWS resources needed to store and run your applications.

# Scope of AWS Services

* IAM
  + Users, Groups, Roles, Accounts – **Global**
    - Same AWS accounts, users, groups and roles can be used in all regions
  + Key Pairs – **Global** or Regional
    - Amazon EC2 created key pairs are specific to the region
    - RSA key pair can be created and uploaded that can be used in all regions
* Virtual Private Cloud
  + VPC – Regional
    - VPC are created within a region
  + Subnet – **Availability Zone**
    - Subnet can span only a single Availability Zone
  + Security groups – Regional
    - A security group is tied to a region and can be assigned only to instances in the same region.
  + VPC Endpoints – Regional
    - You cannot create an endpoint between a VPC and an AWS service in a different region.
  + VPC Peering –
    - VPC Peering can be performed across VPC in the same account of different AWS accounts
    - VPC Peering can now span inter-region
  + Elastic IP Address – Regional
    - Elastic IP address created within the region can be assigned to instances within the region only
* EC2
  + Resource Identifiers – Regional
    - Each resource identifier, such as an AMI ID, instance ID, EBS volume ID, or EBS snapshot ID, is tied to its region and can be used only in the region where you created the resource.
  + Instances – **Availability Zone**
    - An instance is tied to the Availability Zones in which you launched it. However, note that its instance ID is tied to the region.
  + EBS Volumes – **Availability Zone**
    - Amazon EBS volume is tied to its Availability Zone and can be attached only to instances in the same Availability Zone.
  + EBS Snapshot – Regional
    - An EBS snapshot is tied to its region and can only be used to create volumes in the same region and has to be copied from One region to other if needed
  + AMIs – Regional
    - AMI provides templates to launch EC2 instances
    - AMI is tied to the Region where its files are located with Amazon S3. For using AMI in different regions, the AMI can be copied to other regions
  + Auto Scaling – Regional
    - Auto Scaling spans across multiple Availability Zones within the same region but cannot span across regions
  + Elastic Load Balancer – Regional
    - Elastic Load Balancer distributes traffic across instances in multiple Availability Zones in the same region
  + Cluster Placement Groups – **Availability Zone**
    - Cluster Placement groups can be span across Instances within the same Availability Zones
* S3 – Global but Data is Regional
  + S3 buckets are created within the selected region
  + Objects stored are replicated across Availability Zones to provide high durability but are not cross region replicated unless done explicitly
* Route53 – **Global**
  + Route53 services are offered at AWS edge locations and are global
* DynamoDb – Regional
  + All data objects are stored within the same region and replicated across multiple Availability Zones in the same region
  + Data objects can be explicitly replicated across regions using cross-region replication
* WAF – **Global**
  + Web Application Firewall (WAF) services protects web applications from common web exploits are offered at AWS edge locations and are global
* CloudFront – **Global**
  + CloudFront is the global content delivery network (CDN) services are offered at AWS edge locations
* Storage Gateway – Regional
  + AWS Storage Gateway stores volume, snapshot, and tape data in the AWS region in which the gateway is activated

AWS S3:

Block public Access

Query in place

S3 Select

Amazon Athena

Amazon Redshift Spectrum

**Hybrid cloud storage: AWS Storage Gateway**

**Online data transfer:**

[AWS DataSync](https://aws.amazon.com/datasync/) makes it easy and efficient to transfer hundreds of terabytes and millions of files into Amazon S3, up to 10x faster than open-source tools. DataSync automatically handles or eliminates many manual tasks, including scripting copy jobs, scheduling and monitoring transfers, validating data, and optimizing network utilization.

The [AWS Transfer Family](https://aws.amazon.com/aws-transfer-family/) provides fully managed, simple, and seamless file transfer to Amazon S3 using SFTP, FTPS, and FTP.

[Amazon S3 Transfer Acceleration](https://aws.amazon.com/s3/transfer-acceleration/) enables fast transfers of files over long distances between your client and your Amazon S3 bucket

**Offline data transfer:**

The [AWS Snow Family](https://aws.amazon.com/snow/) is purpose-built for use in edge locations where network capacity is constrained or nonexistent and provides storage and computing capabilities in harsh environments.

The [AWS Snowball](https://aws.amazon.com/snowball/) service uses ruggedized, portable storage and edge computing devices for data collection, processing, and migration. Customers can ship the physical Snowball device for offline data migration to AWS.

[AWS Snowmobile](https://aws.amazon.com/snowmobile/) is an exabyte-scale data transfer service used to move massive volumes of data to the cloud, including video libraries, image repositories, or even a complete data center migration..

<https://aws.amazon.com/s3/features/#Storage_management_and_monitoring>