

H1 Technology Overview

H2 Organizations & Accounts

H3 Organizations

Organizations allow you to centrally manage billing, compliance, control access, security & share resources across your AWS accounts.

- Billing
- Compliance
- Control Access
- Security
- Share resources

H3 Organization Units

Group of AWS account within an Organization which contain other organizations - creating an hierarchy.

H3 Root Account User

Its a single sign-in identity that has complete access to all services & resources in AWS account. Every account has a Root-account user.

H3 Service Control Policies

Gives central control over the allowed permission across all your AWS accounts in your organization, ensuring all your accounts stay within the organization's guidelines.

H2 AWS Networking

AWS Networking takes a recap of AWS Global Infrastructure ([aws-ccp-02.md](#) / [aws-ccp-02.pdf](#))

Name	Description
Region	Geographical Location of your network
AZ	Availability Zone - Data center of your AWS resources (us-east-1a)
VPC (Virtual Private Cloud)	Logically isolated section in your AWS cloud where you can launch AWS resources
Internet Gateway (IGW)	Enables access to the internet
Route Tables	Determine network traffic from where your subnets are redirected
NACLs	Network Access Control List - Acts as firewall 🔥 at Subnet levels
Security Group	Acts as firewall 🔥 at Instance levels
Subnets	Logically partitioning of an IP Network, into smaller network segments (Eg: Public, Private subnet)

H3 VPCs

Amazon Virtual Private Cloud (Amazon VPC) enables you to launch AWS resources into a virtual network that you've defined. This virtual network closely resembles a traditional network that you'd operate in your own data center, with the benefits of using the scalable infrastructure of AWS.

- Amazon VPC is the networking layer for Amazon EC2.

You can create, access, and manage your VPCs using any of the following interfaces:

- **AWS Management Console** — Provides a web interface that you can use to access your VPCs.
- **AWS Command Line Interface (AWS CLI)** — Provides commands for a broad set of AWS services, including Amazon VPC, and is supported on Windows, Mac, and Linux, see [AWS Command Line Interface](#) .
- **AWS SDKs** — Provides language-specific APIs and takes care of many of the connection details, such as calculating signatures, handling request retries, and error handling, see [AWS SDKs](#) .
- **Query API** — Provides low-level API actions that you call using HTTPS requests. Using the Query API is the most direct way to access Amazon VPC, see the [Amazon EC2 API Reference](#) .

H1 AWS Services

H2 Database Services

The following is a list of 8 Database services offered by AWS -

Database	Description
DynamoDB	NoSQL key/value database (eg: Cassandra / Firebase)
DocumentDB	NoSQL Document database that is MongoDB compatible
RDS	Relational Database Service that supports multiple engines (Engines - MySQL, PostgreSQL, Maria DB, Oracle, Microsoft SQL server, Aurora)
Aurora	MySQL (5x faster) & PostgreSQL (3x faster) database fully managed Relational Database - greater performance. Also more expensive. Enterprise level.
Aurora Server less	Database that only runs when you need it - just like AWS Lambda services. Most in-expensive RDS
Neptune	Managed Graph Database
Redshift	Columnar Database, Petabyte warehouse (1000 TB = 1 PB !!)
ElastiCache	Redis or Memcached database. Used for Caching solutions. Open-source

NOTE: Amazon RDS supports the following databases only - Amazon Aurora, PostgreSQL, MySQL, MariaDB, Oracle Database, and Microsoft SQL Server.

H2 Provisioning Services

Services	Description
Elastic Beanstalk	AWS service for deploying & developing Web applications & services developed using Java, Node JS. Provides an easy installation wizard. (Heroku for AWS 😊)
OpsWorks	Configuration Management service that provides managed instances of Chef & Puppet
Cloud Formation	Infrastructure as Code, JSON or YAML
AWS QuickStart	pre-made packages that can launch & configure your AWS compute, network, storage & other services required to deploy a workload on AWS
AWS Marketplace	Digital catalogue of thousands of AWS listings - from independent software vendors that you can - find, buy, test & deploy software

H2 Computing Services

The following is a list of Computing services offered by AWS

Instances	Description
EC2	Elastic Cloud Compute - Highly configurable server. consists of CPU, Memory, Network & Operating system.
ECS	Elastic Container Service - Imagine Docker as a Service - A Highly scalable, high-performance, container orchestration service that supports Docker containers, pay for EC2 instances.
Fargate	Microservices where you don't think about the infrastructure. Pay per task. It's an evolution of ECS.
EKS	Elastic Kubernetes Service - Imagine Kubernetes as a Service - easy to deploy, manage & scale containerized applications using Kubernetes.
Lambda	Lambda Server less Functions, run code without provisioning or managing servers. You pay only for the compute time you consume
Elastic Beanstalk	orchestrates various other AWS services including, EC2, S3, SNS, Cloudwatch, Autoscaling & Elastic Load Balancers
AWS Batch	plans, schedules & executes your batch computing workloads across the full range of AWS compute services, such as - EC2 & Spot instances.

H2 Storage Services

The following is a list of services offered by AWS related to Storage & data access.

Storage	Description
S3	Simple Storage Service - File system storage service provided by AWS (logical partition storage)
S3 Glacier	Low-cost storage for archiving & long-term backup
Storage Gateway	Hybrid Cloud storage with local caching 1. File gateway, 2. Volume gateway 3. Tape Gateway. Extension of on-prem storage to cloud.
EBS	Elastic Block Storage - Unlike S3, it consists of virtual Hard-drives that you attach to your EC2 instances for storage. Only attach to one EC2 instance per EBS.
EFS	Elastic File Storage - File storage solution, mountable to multiple EC2 instances at the same time.
Snowball	Physically migrate a lot of data via a computer science - 50-80 TB
Snowball Edge	A Better version of Snowball - ~100 TB
Snowmobile	Shipping container, pulled by a Semi-trailer truck - 100 PB

H2 Business Centric Services

Consists of AWS Enterprise related services

Name	Description
Amazon Connect	Cloud based call center service, you can set it up in few clicks. Record, inbound calls. Setup call workflows.
WorkSpaces	Virtual Remote Desktop - AWS service for provisioning either Windows or Linux OS. scalable upto 1000 desktops
WorkDocs	A content creation & collaboration service - AWS version of Sharepoint - CRUD content
Chime	AWS solution for Online Meetings, Video Conferencing, Business calling. Similar to Skype + Slack
WorkMail	AWS service for managed Business emails. Online GMail for AWS.
Pinpoint	Marketing Campaign Management system, send E-newsletters, Targeted emails, SMS, Push notifications.
SES	Simple Email Service - Cloud based email service designed for marketers & application developers to send marketing, notifications & email. Supports HTML content emails unlike SNS which only sends simple Unicode emails.
Quicksight	A Business Intelligence BI service. Generate & share visualizations, charts.

H2 Enterprise Integration

Enterprise Integration is all about "Going Hybrid".

- List of AWS services for bringing on-premise technologies over to cloud.

Name	Description
Direct Connect	dedicated Gigabyte network connection for your on-premise to AWS.
VPN	Setup a secure Virtual Private Network connection from on-prem to AWS. Site to site (direct on-prem to AWS) or client VPN (from clients to AWS).
Storage Gateway	AWS hybrid storage services allows your On-Premise applications to use AWS cloud storage. Useful for backup, archiving, disaster recovery.
Active Directory	AWS Directory Services for Microsoft Managed Active Directories.

H2 Logging Services

List of AWS services for Logging & Monitoring purposes.

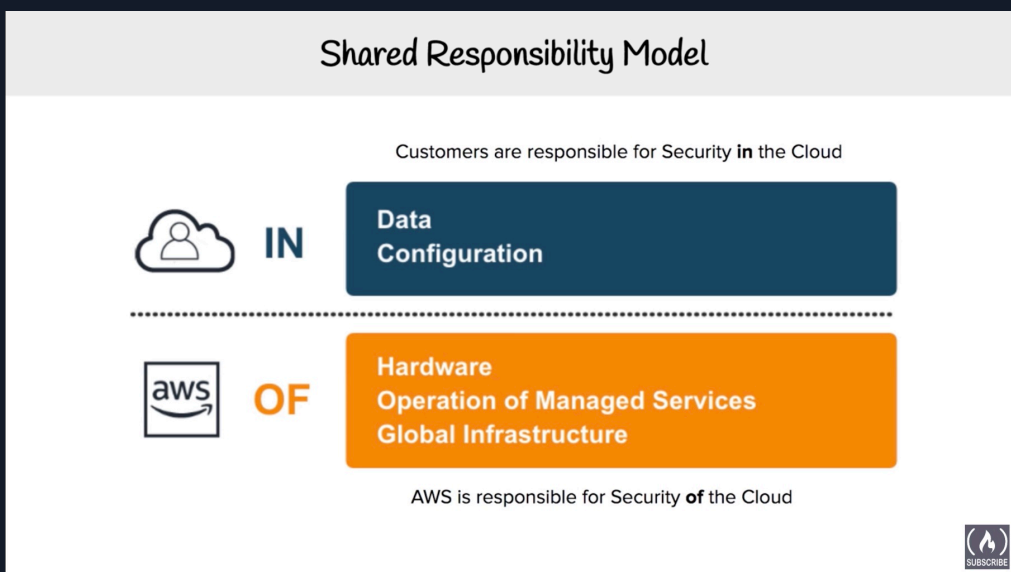
Name	Description
CloudTrail	Logs all API calls between AWS services (who is to blame for this EC2 spin up...?)
CloudWatch	is a collection of multiple services for Logging purposes
1. CloudWatch Logs	Performance data about AWS services. CPU Utilization, Memory, Network, Application Logs. Eg. Rails, Nginx, Lambda
2. CloudWatch Metrics	Represents a time-ordered set of data points. A variable to monitor
3. CloudWatch Events	Trigger an event based on a condition / situation - Exceeding Space - trigger email
4. CloudWatch Alarms	Trigger notifications based on metrics. You can specify a Threshold.
5. CloudWatch Dashboard	Create visualizations based on metrics.

H1 Security

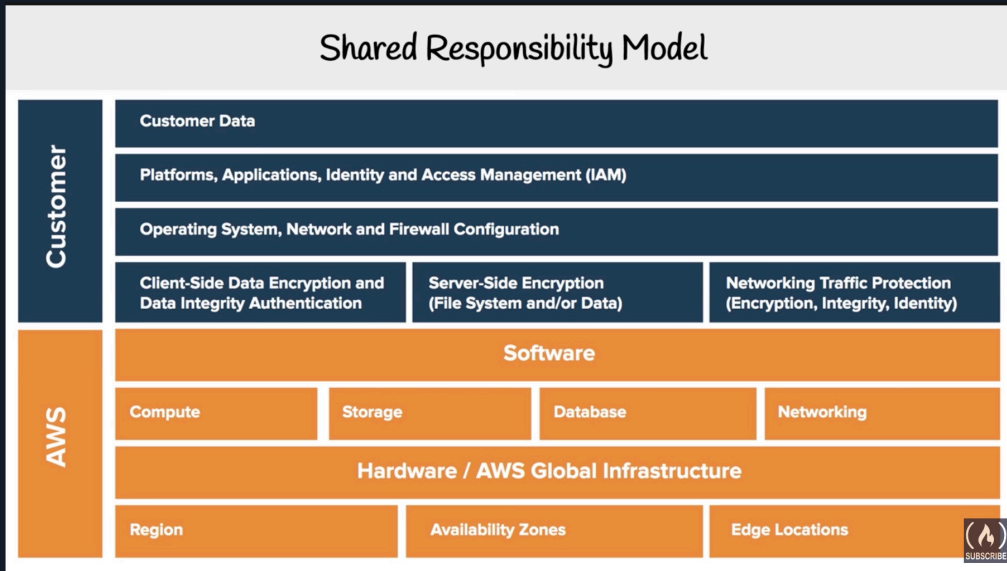
H2 Shared Responsibility Model

The following diagrams show the shared responsibility model between a AWS customer & AWS management

H3 High-level Overview



H3 Detailed Overview



H2 AWS Compliance Programs

To get the full list of compliances that AWS service provides. Click the following link - [Compliance Programs Link](#)

H3 Compliances Overview



H2 AWS Artifact

H3 How do we know AWS meets compliance ?

AWS "Artifact" is a service which provides compliance & security details -

- No cost, self-service portal
- On-demand access to AWS' compliance reports
- These checks are based on Global compliance frameworks
- Ability to report out - **PDF*** (Adobe Acrobat reader only), **XLSX**

H2 Amazon Inspector


H3 How do we prove that a EC2 instance is harden ?

"Hardening" - The act of removing as many security risks as possible

- AWS Inspector runs a **security benchmark** against specific EC2 instances. You can run a variety of security benchmarks.
- Can perform both Network & Host assessments
 - Install AWS agent on your EC2 instance
 - Run an assessment for your targets
 - Review findings & remedy security issues.

One very popular benchmark you can run is CIS which as 699 checks! CIS- Center for Internet Security

H2 AWS WAF - Web Application Firewall

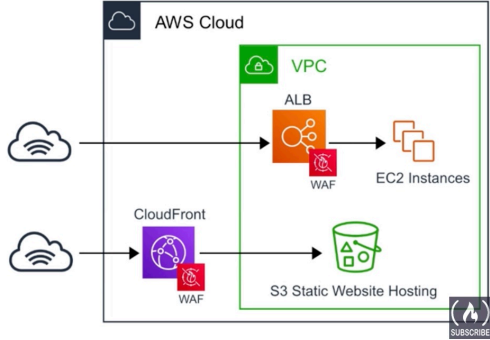


AWS WAF

AWS **Web Application Firewall** protect your web applications from common web exploits
Write your own **rules** to ALLOW or DENY traffic based on the contents of an HTTP requests
Use a **ruleset** from a trusted AWS Security Partner in the AWS WAF Rules Marketplace
WAF can be attached to either **CloudFront** or an **Application Load Balancer**

Protect web applications from attacks covered in the **OWASP Top 10** most dangerous attacks:

1. Injection
2. Broken Authentication
3. Sensitive data exposure
4. XML External Entities (XXE)
5. Broken Access control
6. Security misconfigurations
7. Cross Site Scripting (XSS)
8. Insecure Deserialization
9. Using Components with known vulnerabilities
10. Insufficient logging and monitoring



The diagram illustrates the AWS WAF architecture. It shows two paths for incoming traffic from the Internet. The top path goes through an Application Load Balancer (ALB) and then to EC2 instances. The bottom path goes through CloudFront and then to S3 Static Website Hosting. In both paths, an AWS WAF instance is positioned to filter traffic before it reaches the destination. The diagram is set within the context of an AWS Cloud VPC.

OWASP
Open Web Application Security Project

SUBSCRIBE

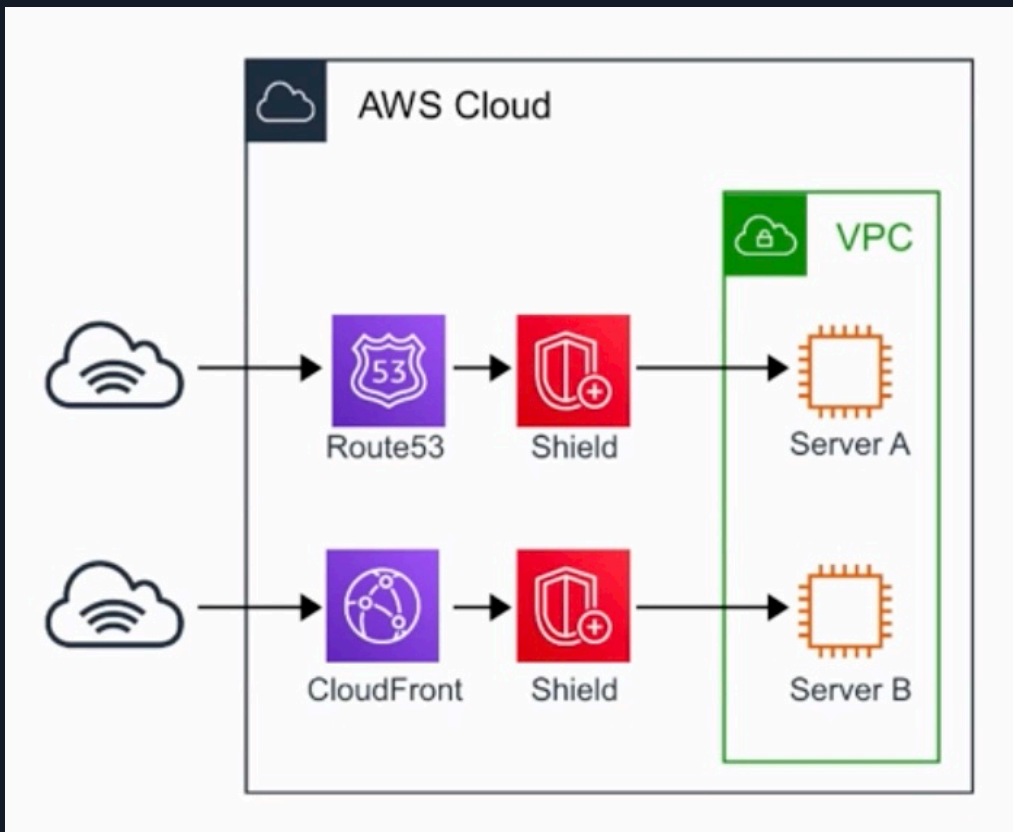
H2 AWS Shield

AWS Shield is a managed DDoS (Distributed Denial of Service) protection service that safeguards applications running on AWS

H3 What is a DDoS attack ?

A Malicious attempt to disrupt normal traffic by flooding a website with large amount of fake traffic.

- **!** When you route your traffic using **AWS Route 53** or **CloudFront**, you are using AWS Shield standard.
- All AWS customers benefit from automatic protections of AWS shield standard, at no additional cost
- Protects you against Layer 3,4,7 attacks
 - 7 - Application layer
 - 4 - Transport layer
 - 3 - Network layer



H2 Penetration Testing

Penetration Testing

What is PenTesting?

An authorized simulated cyberattack on a computer system, performed to evaluate the security of the system.

Can you perform PenTesting on AWS? Yes!

Permitted Services

1. EC2 instances, NAT Gateways, and ELB
2. RDS
3. CloudFront
4. Aurora
5. API Gateways
6. AWS Lambda and Lambda@Edge functions
7. Lightsail resources
8. Elastic Beanstalk environments

Prohibited Activities

- DNS zone walking via Amazon Route 53 Hosted Zones
- Denial of Service (DoS), Distributed Denial of Service (DDoS), Simulated DoS, Simulated DDoS
- Port flooding
- Protocol flooding
- Request flooding (login request flooding, API request flooding)

For **Other Simulated Events** you will need to submit a request to AWS. A reply could take up to 7 days.



H2 Guard Duty

Amazon Service which protects resources using IDS & IPS

H3 What is IDS / IPS ?

- Intrusion Detection System & Intrusion Protection System
- A Device or Software that monitors a network or systems for malicious activity or policy violation
- Guard duty is threat detection service
- Logs stored under Guard Duty ➡ Findings

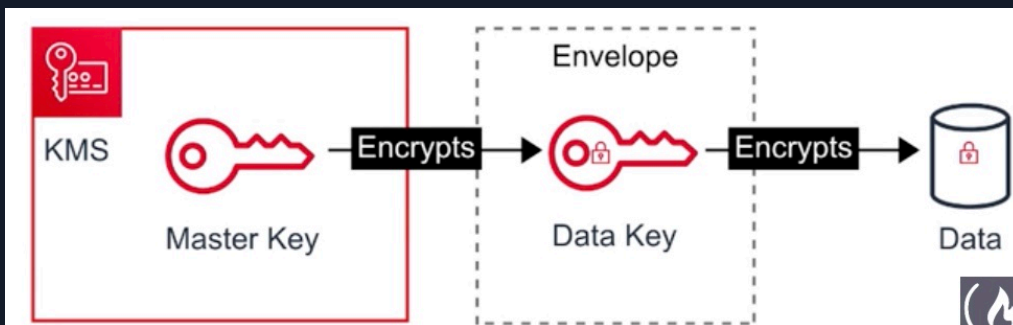
H2 Key Management Service

A managed service that makes it easy for you to create & control encrypted keys used to encrypt your data.

- KMS is a multi-tenant HSM (hardware security model)
- Encrypt your data with a simple checkbox
- KMS uses Envelope Encryption

H3 Envelope Encryption

When you encrypt your data key with a master key as an additional level of security



H2 Amazon Macie

Fully managed service that continuously monitors S3 data access activity for anomalies.

- Generates detailed alerts when it detects risks
- **!** Uses Machine learning to analyze your CloudTrail logs
- Identifies your most risk users which leads to a compromise

H2 Security Groups & NACLs

The following shows important differences between Security Groups & NACLs

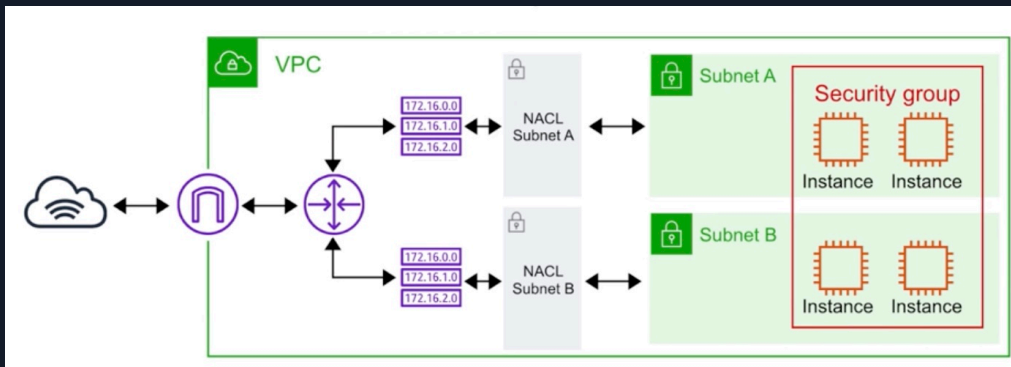
H3 Security Groups

- Act as 🔥 firewall at **instance** level
- Implicitly denies all traffic
- You control the allow rules
- Eg: Allow EC2 access on port 22 for SSH

H3 NACLs

Network Access Control Lists

- Act as 🔥 firewall at **subnet** level
- You create both allow & deny rules
- Cherry pick IP address to deny access to AWS resources
- Eg: Block a specific IP for access which might have been flagged for abuse



H2 Amazon VPN

Virtual Private Network lets you establish a secure & private tunnel from your network or device to AWS global network

- **AWS Site-to-Site VPN** : securely connect on-premises network or branch office to VPC.
- **AWS Client VPN** : securely connect users to AWS network or on-premises networks.

H1 Variation Study

H2 Cloud - Names

The following is a list of names which begin with the prefix - cloud, but have completely different meaning and responsibilities

Service	Description
CloudFormation	Infrastructure as code, setup services via temptation eg: YAML, JSON
CloudTrail	Logs API call between AWS services (who we can blame ?)
CloudFront	Content Distribution Network
CloudWatch	All about Logging, Alerts, Notification
! CloudSearch	Search Engine, You have an ecommerce website & you want to add a search bar

H2 Connect - services

Lists different services that have the word - "Connect" in them

Connect	Description
Direct Connect	Dedicated Fibre optics connection from Data Center to AWS
Amazon Connect	Call center service
Media Connect	New version of Elastic Transcoder, converts video to different video types

H2 Elastic Transcoder vs Media Convert

Both the following services are used for - Transcode videos

Elastic Transcoder	AWS Elemental Media Convert
The old way of encoding media	The new way of encoding media
Transcodes videos to streaming formats	Transcodes videos to streaming formats
	Overlays images (Watermark)
	Insert Video clips
	Extracts captions data
	Robust UI

H2 SNS vs SQS

Both the following services are used for connecting - Your Applications via Messages

SNS - Simple Notification Service	SES - Simple Email Service	SQS - Simple Queue Service
Practical & Internal	Professional, Marketing, Emails	Scheduled, Queues
Pass along messages eg: PubSub mail service	A cloud based email service Eg: Twilio SendGrid	Queue up messages, Guaranteed Delivery
Send notification to subscribers of topics via multiple protocol eg: HTTP, Email, SQS, SMS	Supports Lambda operations	Places messages into a queue. Applications pull queue using AWS SDK
SNS is generally used for sending "plain text emails". Best eg: Billing alarms	SES can send HTML email, SNS cannot	
Can retry sending in case of failure of HTTPS	<ul style="list-style-type: none"> - SES can receive inbound emails. - SES can create Email template - Custom domain name email - Monitor your email reputation 	<ul style="list-style-type: none"> - Can retain a message upto 14 days - Can send msgs in a sequential order or in parallel - Can ensure only one message is sent - Can ensure msgs delivered atleast once
Really good for web-hooks, simple internal emails, triggering lambda functions		Really good for delayed tasks, queueing up emails
Eg: Pusher, PubNub		Eg: RabbitMQ, Sidekiq

H2 Inspector vs Trusted Advisor

Both are Security tools & they both perform audits

Amazon Inspector	Trusted Advisor
Audits a single EC2 instance you've selected	Gives you a holistic view of recommendations across multiple services & best practices
Generates a report from a long list of security checks i.e., 🚨 699 checks	Doesn't generate out a PDF report
Generates PDF report	You should enable MFA on your root account when using trusted advisor.

H2 AWS Artifact vs AWS Inspector

Both Artifact & Inspector compile out PDFs

AWS Artifact	AWS Inspector
Why should an enterprise trust AWS ?	How do we know this EC2 instance is Secure ?
Generates a security report that's based on global compliance frameworks	Runs a script that analyze your EC2 instance then generates a PDF report telling you which security check has passed
Eg: Service Organization Control (SOC) & Payment Card Industry (PCI)	Audit Tool for security of EC2 instances

H2 ALB vs NLB vs CLB

All of the above deal with Load balancing when it comes to AWS Services

NOTE: can attach Amazon Certification Manager (ACM) SSL certificate

Application	Network	Classic (old)
Layer 7 Requests	Layer 4 IP protocol data	Layer 4 & Layer 7
HTTP & HTTPS traffic	TCP & TLS traffic where extreme performance is required	Intended for applications that were built within the EC2-class network
Can attach WAF	Capable of handling millions of requests per second while maintaining ultra-low-latencies	Doesn't use Target groups
	Optimized for sudden & volatile traffic patterns while using a single static IP address per availability zone.	

H1 Questions & Answers

H3 Question 01

AWS RDS supports six database engines. From the list below, choose three engines supported by Amazon RDS? (Choose 3 answers)

- Oracle ✓
- MySQL ✓
- DB2 ✗
- FoxPro ✗
- Microsoft SQL ✓

Explanation

Amazon RDS is available on several database instance types - optimized for memory, performance, or I/O - and provides you with six familiar database engines to choose from, including Amazon Aurora, PostgreSQL, MySQL, MariaDB, Oracle Database, and SQL Server.

H4

Although you can host other databases on EC2 Instances, only the above are natively supported by the Amazon Relational Database Management Service (RDS)

Ref: <https://youtu.be/eMzCI7S1P9M>

H3 Question 02

One of the seven design principals of the Security Pillar in the Well-Architected Framework refers to the concept of applying security at all layers. Which two firewall options can you configure to protect your EC2 Instances deployed in a VPC? (Choose 2 answers)

- IAM Groups ✗
- Security Groups ✓
- AWS WAF ✗
- Amazon Macie ✗
- NACLs ✓

Explanation

- NACLs are firewalls that protect the entire subnet and allow you to define both allow and deny rules for traffic that flows into and out of the subnet. This protects your EC2 Instance the Subnet.

H4

- Security Groups are firewalls that protect the individual EC2 Instance and further restrict what traffic can be allowed to the instance.
- Amazon Macie is an incorrect answer. Amazon Macie is a security service that uses machine learning to automatically discover, classify, and protect sensitive data in AWS. Amazon Macie recognizes sensitive data such as personally identifiable information (PII) or intellectual property (such as your corporate application source codes) and provides you with dashboards and alerts that give visibility into how this data is being accessed or moved. The fully managed service continuously monitors data access activity for anomalies and generates detailed alerts when it detects the risk of unauthorized access or inadvertent data leaks. Amazon Macie is available to

protect data stored in Amazon S3.

- AWS WAF is an incorrect answer. AWS WAF is a web application firewall that helps protect your web applications or APIs against common web exploits. AWS WAF can be used to control how traffic reaches your applications by enabling you to create security rules that block common attack patterns, such as SQL injection or cross-site scripting, and rules that filter out specific traffic patterns you configure.
- IAM Groups are an incorrect answer. IAM Groups are designed to club together IAM Users who share common job functions and grant IAM Policies to. These have nothing to do with protecting network traffic to EC2 instances.

H3 Question 03

Which storage solution enables you to share a common file system across multiple Linux based EC2 Instances that can be used to support applications which require access to data with very low latency connectivity?

- NTFS ❌
- S3 ❌
- EFS ✔️
- EBS ❌

Explanation

- Amazon EFS is a fully managed service providing shared file system storage for Linux workloads. It provides a simple interface allowing you to create and configure file systems quickly and manages the file storage infrastructure for you, removing the complexity of deploying, patching, and maintaining the underpinnings of a file system. You can use to provide your application that runs on multiple EC2 instances to share a common file system that offers very low latency connectivity.
- The answer, "EBS" is incorrect because although you can configure a file system on EBS Volumes, you cannot share an EBS volume across multiple EC2 Instances.
- The answer, "S3" is incorrect because it is not a file system. Also, EFS would offer much lower latency. Amazon S3 is object storage and ideally used to host assets such as documents, images, and videos which can be referenced by web applications.
- The answer, "NTFS" is incorrect because this is a file system, specifically a Windows File System and not the actual storage option.

H3 Question 04

Your organization hosts multiple AWS Accounts with multiple VPCs. You would like to connect these VPCs together and centrally manage connectivity policies. Which AWS service enables you to connect multiple VPCs configured as a hub that controls how traffic is routed among all the connected networks which act like spokes?

- AWS Transit Gateway ✔️
- AWS VPC Peering ❌

- AWS Global Accelerator ❌
- AWS Virtual Private Gateway ❌

Explanation

- H4
- AWS Transit Gateway is a service that enables customers to connect their Amazon Virtual Private Clouds (VPCs) and their on-premises networks to a single gateway. This allows you to connect your on-premise network and all your VPCs in a hub and spoke configuration which significantly simplifies management and reduces operational costs because each network only has to connect to the Transit Gateway and not to every other network.
 - The answer, 'AWS Global Accelerator', is incorrect. AWS Global Accelerator is a service that improves the availability and performance of your applications with local or global users. It provides static IP addresses that act as a fixed entry point to your application endpoints in a single or multiple AWS Regions, such as your Application Load Balancers, Network Load Balancers, or Amazon EC2 instances.
 - The answer, 'AWS VPC Peering', is incorrect. While VPC Peering allows you to connect two VPCs to each other, it does not enable you to centrally manage multiple VPCs connections centrally. You could configure all your VPCs with individual peering connections, but this becomes very difficult to manage.
 - The answer, 'AWS Virtual Private Gateway', is incorrect. AWS Virtual Private Gateway is a component of your Site to Site VPN connection that needs to be configured to build out a VPC tunnel with your on-premise network.
 - Ref: <https://aws.amazon.com/transit-gateway/>

H3 Question 05

You wish to configure a bucket that will enforce a policy that enables anonymous to access its content if they connect to the data from the Corporate and branch offices as part of your security strategy. Which S3 configuration feature will enable you to define the IP Ranges from where you will allow access to the data?

- NTFS Permissions ❌
- Bucket Policy ✔️
- NACLs ❌
- Security Groups ❌

Explanation

- H4
- S3 bucket policies specify what actions are allowed or denied for which principals on the bucket that the bucket policy is attached to. Bucket Policies enable you to also define conditional statements so that you can restrict access based on location for example. Also, note that S3 supports bucket policies of up to 20 kb.
 - Security Groups is an incorrect answer because these are used to protect EC2 Instances by enabling you to only allow traffic inbound/outbound on specific ports
 - NTFS Permissions is an incorrect answer. NTFS (NT File System) permissions are available to drives formatted with NTFS. The advantage with NTFS permissions is that they affect local users as well as network users and they are based on the permission granted to each individual user at the Windows login, regardless of where the user is

connecting.

- Network Access Control Lists (NACLs) is an incorrect answer. NACL is a VPC Firewall security services that enable you to configure which inbound and outbound ports you can open at a subnet level,
- Ref: <https://aws.amazon.com/blogs/security/iam-policies-and-bucket-policies-and-acls-oh-my-controlling-access-to-s3-resources/>

H3 Question 06

Which AWS Service enables developers to analyze and debug applications, identifying the root cause of performance issues and errors?

- AWS CloudTrail ❌
- AWS X-Ray ✔️
- Access Analyzer ❌
- AWS Trusted Advisor

Explanation

- AWS X-Ray helps developers analyze and debug production, distributed applications, such as those built using a microservices architecture. With X-Ray, you can understand how your application and its underlying services are performing to identify and troubleshoot the root cause of performance issues and errors.

H4

- The answer, 'AWS CloudTrail' is incorrect. AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. With CloudTrail, you can log, continuously monitor, and retain account activity related to actions across your AWS infrastructure.
- The answer, 'AWS Trusted Advisor' is incorrect. AWS Trusted Advisor provides real-time guidance to help you provision your resources following AWS best practices. To help you maximize utilization of Reserved Instances, AWS Trusted Advisor checks your Amazon EC2 computing-consumption history and calculates an optimal number of Partial Upfront Reserved Instances. Recommendations are based on the previous calendar month's hour-by-hour usage aggregated across all consolidated billing accounts.

H3 Question 07

Which AWS Service can be used to capture, transform, and load streaming data into Amazon S3, Amazon Redshift, Amazon Elasticsearch Service, and Splunk, enabling near real-time analytics with existing business intelligence?

- AWS Kinesis Firehose ✔️
- AWS Kinesis Video Streams ❌
- AWS S3 ❌
- AWS Athena ❌





Explanation

H4

- Amazon Kinesis Data Firehose provides a simple way to capture, transform, and load streaming data with just a few clicks in the AWS Management Console. It is integrated with Amazon S3, Amazon Redshift, and Amazon Elasticsearch Service and you can capture, transform, and load streaming data. From the AWS Management Console, you can point Kinesis Data Firehose to an Amazon S3 bucket, Amazon Redshift table, or Amazon Elasticsearch domain.
- The answer 'Kinesis Video Streams' is incorrect. Amazon Kinesis Video Streams makes it easy to securely stream video from connected devices to AWS for analytics, machine learning (ML), playback, and other processing. Kinesis Video Streams automatically provisions and elastically scales all the infrastructure needed to ingest streaming video data from millions of devices.
- The answer, 'Amazon Athena' is incorrect. Amazon Athena is an interactive query service that makes it easy to analyze data in Amazon S3 using standard SQL. Athena is serverless, so there is no infrastructure to manage, and you pay only for the queries that you run.
- The answer, 'Amazon S3' is incorrect. Amazon S3 is an Object Storage solution offered by AWS, allowing to store an unlimited amount of data in the cloud where every object is stored as a complete object. Objects contain extensive metadata and Amazon S3 is often used to store static content that can be used as digital assets for your websites or even archival data for long term retention.

H3 Question 08

Which VPC Component enables to you grant Internet access to servers in the public subnet deployed in the VPC?

- Internet Gateway 
- Security Group 
- NAT Gateway 
- VPC Peering 

Explanation

H4

An internet gateway is a horizontally scaled, redundant, and highly available VPC component that allows communication between instances in your VPC and the internet. It, therefore, imposes no availability risks or bandwidth constraints on your network traffic.

An internet gateway serves two purposes: to provide a target in your VPC route tables for internet-routable traffic and to perform network address translation (NAT) for instances that have been assigned public IPv4 addresses.

The answer, 'NAT Gateway', is incorrect as this is used to enable Internet access for servers deployed in the private subnet

The answer, 'VPC Peering', is incorrect. A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IPv4 addresses or IPv6 addresses. Instances in either VPC can communicate with each other as if they are within the same network.

The answer, 'Security Group', is incorrect. Security Groups act as virtual firewalls for your instances to control inbound and outbound traffic to them. This ensures that only the necessary traffic is permitted inbound to those servers.

Ref: https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Internet_Gateway.html

H3 Question 09

Which Amazon S3 Storage Class enables you to optimize costs by automatically moving data to the most cost-effective access tier, while ensuring that frequently access data is made available immediately?

- Amazon Glacier ❌
- Amazon S3 Standard ❌
- Amazon S3 One-Zone IA ❌
- Amazon S3 Intelligent Tiering ✅

Explanation

H4

- The S3 Intelligent-Tiering storage class is designed to optimize costs by automatically moving data to the most cost-effective access tier, without performance impact or operational overhead. It works by storing objects in two access tiers: one tier that is optimized for frequent access and another lower-cost tier that is optimized for infrequent access. For a small monthly monitoring and automation fee per object, Amazon S3 monitors access patterns of the objects in S3 Intelligent-Tiering and moves the ones that have not been accessed for 30 consecutive days to the infrequent access tier. If an object in the infrequent access tier is accessed, it is automatically moved back to the frequent access tier.
- The answer "S3 Standard" is incorrect as it does not ensure cost-efficiency to your data
- The answer "S3 One-Zone IA" is incorrect. While it is cheaper than S3 Standard, it does not ensure automatically moving data to the most cost-effective storage when not required and then moving back to a storage class that makes the data rapidly accessible.
- The answer "Amazon Glacier" is incorrect as while it is the cheapest available on the platform, it does not offer the ability to make data instantly available when required. Retrieving data from Glacier can take a bit of time depending on the retrieval option.

H3 Question 10

Which of the following AWS services enables you to quickly launch a webserver with a pre-configured WordPress installation pack, offers predictable monthly pricing, comes with integrated certificate management, and provides free SSL/TLS certificates?

- AWS Lightsail 
- AWS EC2 
- AWS EB 
- AWS RDS 

Explanation

H4

- AWS LightSail offers virtual servers that are easy to set up and manage. AWS LightSail servers offer preconfigured virtual specifications for your servers, with predictable pricing strategy. You can launch your website, web application, or project in minutes, and manage your instance from the intuitive LightSail console or API. Applications like WordPress can be launched preconfigured making it very easy to provision a website within minutes and where you do not need the complexity associated with manually configuring an EC2 server such as storage, load balancing, and certificate management.

LightSail also offers free SSL/TLS certificates that can be provisioned and added to a load balancer in just a few clicks.

- The answer, 'AWS EC2', is incorrect because EC2 offers much for configuration options and individual components such as configuring a server with WordPress and other web applications have to be managed separately or via scripts. Furthermore, you will need to configure your own Elastic Load Balancers and install SSL Certs, etc.





As your requirements become more complex, you can easily upgrade your LightSail environment and move to EC2 with a simple, guided experience.

- The answer, 'AWS RDS' is incorrect because AWS RDS is a managed database solution and not a virtual server solution to host websites and applications like WordPress
- The answer, 'Elastic Beanstalk' is incorrect as it is a platform service enabling you to automatically provision an entire infrastructure environment to support application code that you can upload.

Ref: <https://aws.amazon.com/lightsail/features/>

H3 Question 11

Which AWS service enables you to perform heterogeneous migrations between different database platforms, such as Oracle to Amazon Aurora

- AWS Database conversion service 
- AWS Database Migration service 
- AWS EKS 
- AWS Snowball 

Explanation

H4

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

The answer, AWS Snowball is incorrect. Snowball is a petabyte-scale data transport solution that uses secure appliances to transfer large amounts of data into and out of the AWS cloud. Using Snowball addresses common challenges with large-scale data transfers including high network costs, long transfer times, and security concerns.


The answer, AWS EKS is incorrect. Amazon Elastic Kubernetes Service (Amazon EKS) is a fully managed Kubernetes service.

The answer, AWS Database Conversion Service is incorrect as there is no such service.

Ref: <https://youtu.be/ouia1Sc5QGo>

H3 Question 12

Which AWS services enables you to track all API activity in your AWS account regardless of whether the activity was performed using the AWS Management Console or the Command Line Interface?

- AWS API Log
- AWS Trusted Advisor
- AWS CloudTrail 
- AWS Config

Explanation

H4

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.

The answer, 'AWS Config' is incorrect. 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.

The answer, 'Trusted Advisor' is incorrect. AWS Trusted Advisor provides real-time guidance to help you provision your resources following AWS best practices. To help you maximize utilization of Reserved Instances, AWS Trusted Advisor checks your Amazon EC2 computing-consumption history and calculates an optimal number of Partial Upfront Reserved Instances. Recommendations are

based on the previous calendar month's hour-by-hour usage aggregated across all consolidated billing accounts.

The answer, 'API Log' is incorrect as there is no such service.

Ref: <https://youtu.be/mXQSnbc9jMs>

H3 Question 13

You are building a multi-tier architecture with web servers placed in the public subnet and application servers placed in the private subnet of your VPC. You need to deploy Elastic Load Balancers to distribute traffic to both the web-server farm and the application server farm. Which type of load balancer would you choose to distribute traffic to your application servers?

- Internet-facing ❌
- Static load balancers ❌
- Internal load balancers ✅
- Dynamic load balancers ❌

Explanation

When you create a load balancer, you must choose whether to make it an internal load balancer or an internet-facing load balancer. In a multi-tier architecture, as described above, you would deploy an internal load balancer to distribute traffic from the web servers to the application servers. The nodes of an internal load balancer have only private IP addresses. The DNS name of an internal load balancer is publicly resolvable to the private IP addresses of the nodes. Therefore, internal load balancers can only route requests from clients with access to the VPC for the load balancer.

H4

The answer "Internet-facing" is incorrect as this configuration is used to support traffic the web-servers from users on the Internet

The answers "Dynamic load balancers" and "Static load balancers" are incorrect as there is no such service.

Ref: <https://docs.aws.amazon.com/elasticloadbalancing/latest/userguide/how-elastic-load-balancing-works.html#load-balancer-scheme>

H3 Question 14

You have launched a VPC in your AWS Account. You have been asked if it is possible to establish connectivity from your on-premise network to the VPC enabling your Developers with seamless access to production workloads deployed in the VPC from the on-premise network. Which connectivity strategy will enable you to establish this connection over the standard public Internet while keeping costs to a minimum?

- Setup a Direct Connect Connection between on-premise network and VPC ❌
- This cannot be done ❌

- Setup a Snowball Service ❌
 - Setup a Hardware VPC Connection between your on-premise network and the VPC
- ✅

Explanation

You can create a hardware virtual private network (VPN) connection between your corporate data center and your VPC and leverage the AWS Cloud as an extension of your corporate data center.

- H4 You can alternatively use Direct Connect to configure connectivity between the on-premise network and the cloud. However, this is the most expensive and uses private network connectivity.

Ref: <https://docs.aws.amazon.com/whitepapers/latest/aws-vpc-connectivity-options/network-to-amazon-vpc-connectivity-options.html>

H3 Question 15

Your company hosts various workloads across multiple AWS Accounts. Which AWS service can help you maximize on your total spend across all accounts by combining your accounts in a group and thus benefiting from volume discounts?

- AWS Organization ✅
- AWS Budgets ❌
- AWS Bulk Subscribe ❌
- AWS Cost Explorer ❌

Explanation

- H4 You can use the consolidated billing feature in AWS Organizations to consolidate billing and payment for multiple AWS accounts or multiple Amazon Internet Services Pvt. Ltd (AISPL) accounts. You can combine the usage across all accounts in the organization to share the volume pricing discounts, Reserved Instance discounts, and Savings Plans. This can result in a lower charge for your project, department, or company than with individual standalone accounts.

The answer, 'AWS Bulk Subscribe', is incorrect as there is no such service.

The answer, 'AWS Cost Explorer', is incorrect. AWS Cost Explorer has an easy-to-use interface that lets you visualize, understand, and manage your AWS costs and usage over time. However, using the service does not help you benefit from volume discounts.

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

Ref: <https://youtu.be/T4NK8fv8Ydl>

H3 Question 16

Which AWS Service enables companies looking to migrate to the AWS Cloud obtain copies of various compliance documents such as ISO certifications, Payment Card Industry (PCI), and Service Organization Control (SOC) reports?

- AWS Artifact 
- AWS Security Reports 
- AWS Config 
- AWS CloudWatch 

Explanation

H4 AWS Artifact provides on-demand access to AWS' security and compliance reports and select online agreements. Reports available in AWS Artifact include our Service Organization Control (SOC) reports, Payment Card Industry (PCI) reports, and certifications from accreditation bodies across geographies and compliance verticals that validate the implementation and operating effectiveness of AWS security controls.

Ref: <https://youtu.be/ILEoLqpbfXM>

H3 Question 17

Which AWS EC2 pricing option can help you reduce costs by allowing you to use your existing server-bound software licenses?

- Reserved 
- On-Demand 
- Spot 
- Dedicated Hosts 

Explanation


H4 Dedicated Hosts allow you to use your existing per-socket, per-core, or per-VM software licenses, including Microsoft Windows Server, Microsoft SQL Server, SUSE Linux Enterprise Server, Red Hat Enterprise Linux, or other software licenses that are bound to VMs, sockets, or physical cores, subject to your license terms.

When you launch instances on a Dedicated Host, the instances run on a physical server that is dedicated to your use. While Dedicated instances also run on dedicated hardware, Dedicated Hosts provide further visibility and control by allowing you to place your instances on a specific, physical server. This enables you to deploy instances using configurations that help address corporate compliance and regulatory requirements.

Ref: <https://aws.amazon.com/ec2/pricing/>

H3 Question 18

When retrieving data from Amazon Glacier, what is the typical time taken to make a Standard archive available?

- 5 minutes 

- 90 seconds ❌
- 24 hours ❌
- 3 to 5 hours ✅

Explanation

It takes 3 to 5 hours to prepare a Glacier archive to be available for download using the Standard Retrieval Option.

Ref: <https://youtu.be/EKaJENJqD8E>

H4