H2 Simple Concepts in AWS I don't know

H3 Security Groups

Security Groups are firewalls that protect the individual EC2 Instance and further restrict what traffic can be allowed to the instance.

H3 NACLs

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.

H3 Amazon Macie

> ❗ *Remember MACIE is present in MACHINE LEARNING*

- 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.

H3 AWS WAF

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.

H3 EFS vs S3

EFS	S3
Shared File System	S3 is Object Storage
Common file system across multiple Linux based EC2 Instances	Used mainly for Web applications files / objects / images storage
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.	Ideally used to host assets such as documents, images, and videos which can be referenced by web applications.

H3 IAM Policies vs Bucket Policies

Distinction between IAM & S3 Bucket Policies

IAM Policies	S3 Bucket Policies
IAM policies specify what actions are allowed or denied on what AWS resources (e.g. allow ec2:TerminateInstance on the EC2 instance with instance_id=i-8b3620ec). You attach IAM policies to IAM users, groups, or roles, which are then subject to the permissions you've defined.	S3 bucket policies, on the other hand, are attached only to S3 buckets. S3 bucket policies specify what actions are allowed or denied for which principals on the bucket that the bucket policy is attached to (e.g. allow user Alice to PUT but not DELETE objects in the bucket).
AWS User account centric	AWS S3 bucket centric
What can this user do in AWS ?	Who can access this S3 bucket ?

Use IAM policies if:

- You need to control access to AWS services other than S3. IAM policies will be easier to manage since you can centrally manage all of your permissions in IAM, instead of spreading them between IAM and S3.
- You have numerous S3 buckets each with different permissions requirements. IAM policies will be easier to manage since you don't have to define a large number of S3 bucket policies and can instead rely on fewer, more detailed IAM policies.
- You prefer to keep access control policies in the IAM environment.

Use S3 bucket policies if:

- You want a simple way to grant cross-account access to your S3 environment, without using IAM roles .
- Your IAM policies bump up against the size limit (up to 2 kb for users, 5 kb for groups, and 10 kb for roles). S3 supports bucket policies of up 20 kb.

- You prefer to keep access control policies in the S3 environment.

If you're still unsure of which to use, consider which audit question is most important to you:

- If you're more interested in " **What can this user do in AWS?** " then IAM policies are probably the way to go. You can easily answer this by looking up an IAM user and then examining their IAM policies to see what rights they have.
- If you're more interested in " **Who can access this S3 bucket?** " then S3 bucket policies will likely suit you better. You can easily answer this by looking up a bucket and examining the bucket policy.

H3 AWS Transit Gateway

> ❗ *Remember Hub & Spoke configuration*

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.

> ❓ *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?*
>
> *Answer: AWS Transit Gateway*

H3 AWS Global Accelerator

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.

H3 AWS VPC Peering

VPC Peering allows you to connect 2 peer-peer VPCs together

- It does not enalbe you to centrally manage multiple VPCs connections centrally.

H3 AWS Virtual Private Gateway

Component of your site-to-site VPN connection that needs to configured to build out a VPC tunnel with your on-premise network.

H3 AWS X-Ray

> *Remember microservice architecture - enable developers to debug & analyze production distributed applications*

AWS X-Ray helps developers analyze & debug production, distributed applications, especially those build using a microserice architecture

- With X-Ray, you can understand how your application & its underlying services are performing.
- To identify & troubleshoot the root cause of performance issues & errors.

H3 AWS CloudTrail

> *Remember - Auditing across your AWS infrastructure*

H3 AWS Trusted Advisor

Provides real-time guidance following AWS best practices.

- 7 AWS Trusted advisor checks for Basic & Developer billing model
- All AWS Trusted advisor checks for Business & Enterprise billing model

H3 AWS Kinesis Firehose

> *Remember Video streaming integration with S3, Redshift, Elastic-search*

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.

H3 AWS Kinesis Video Streams

> *Remember Video streaming for analysis*

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.

H3 AWS Athena

> *Analyse S3 data using interactive SQL queries. Also serverless.*

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.

H3 NAT Gateway

'NAT Gateway', is used to enable Internet access for servers deployed in the private subnet