Security & Compliance

Shared Responsibility Model Reminder (2 to 3 Q's in the exam)

AWS Shared Responsibility Model

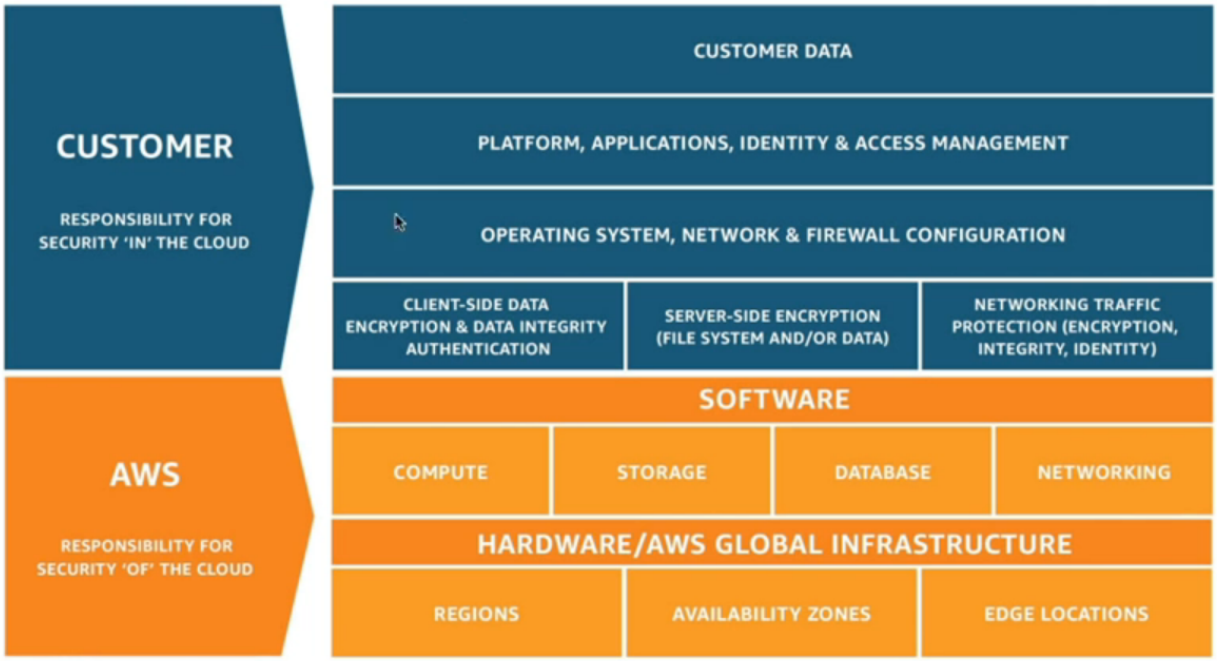
- AWS responsibility - Security of the Cloud
  - Protecting infrastructure (hardware, software, facilities, and networking) that runs all the AWS services
  - Managed services like S3, DynamoDB, RDS, etc.
- Customer responsibility - Security in the Cloud
  - For EC2 instance, customer is responsible for management of the guest OS (including security patches and updates), firewall & network configuration, IAM
  - Encrypting application data
- Shared controls:
  - Patch Management, Configuration Management, Awareness & Training

Example, for RDS

- AWS responsibility:
  - Manage the underlying EC2 instance, disable SSH access
  - Automated DB patching
  - Automated OS patching
  - Audit the underlying instance and disks & guarantee it functions
- Your responsibility:
  - Check the ports / IP / security group inbound rules in DB's SG
  - In-database user creation and permissions
  - Creating a database with or without public access
  - Ensure parameter groups or DB is configured to only allow SSL connections
  - Database encryption setting

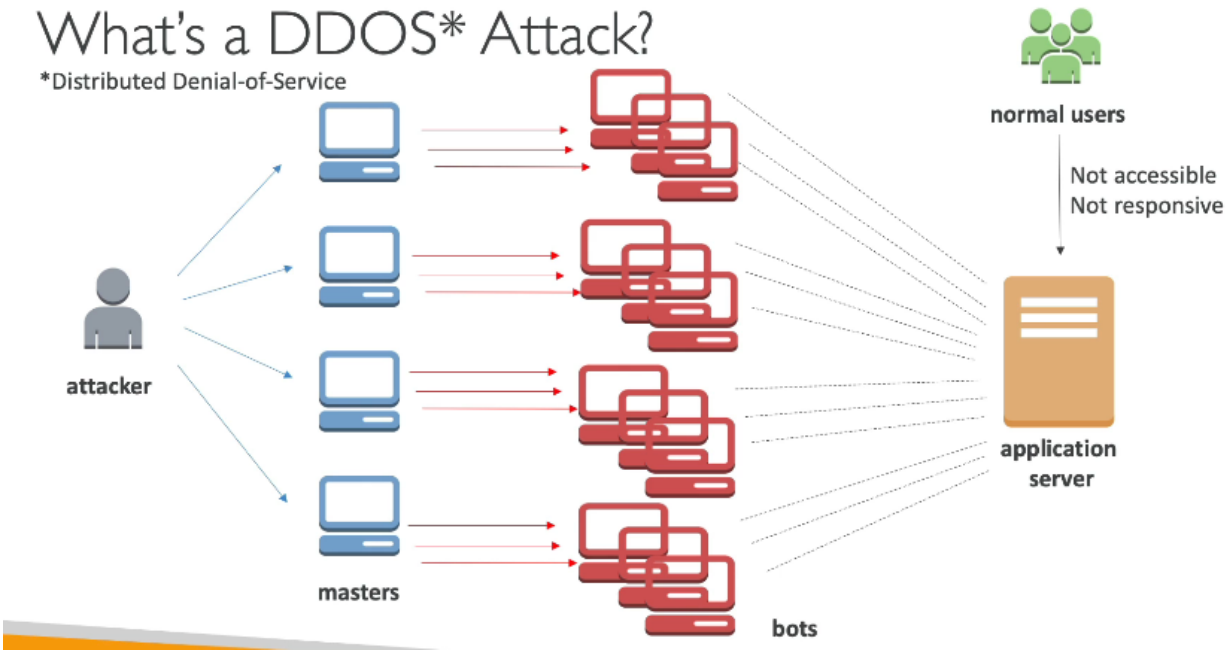
Example, for S3

- AWS responsibility:
  - Guarantee you get unlimited storage
  - Guarantee you get encryption
  - Ensure separation of the data between different customers
  - Ensure AWS employees can't access your data
- Your responsibility:
  - Bucket configuration
  - Bucket policy / public setting
  - IAM user and roles
  - Enabling encryption



DDoS Attack

- Distributed Denial of Service
- The purpose of a DDoS attack is to flood a website or online service with more traffic than it can handle. This flood of traffic isn't real people trying to use the service; instead, it's like a virtual mob created by the attacker. As a result, the website or service becomes slow or completely unavailable to real users because it's too busy dealing with the fake traffic.



DDoS Protection on AWS

- **AWS Shield Standard** - this protects your website and applications from DDoS attacks, it is enabled by default for all customers at no additional cost. It's designed to protect against the most common types of attacks that many applications might face.

  - Free service that is activated for every AWS customer
  - Provides protection from attacks such as SYN/UDP Floods, Reflection attacks and other layer 3/layer 4 attacks

- **AWS Shield Advanced** - 24/7 premium DDoS protection - This is a subscription-based, premium DDoS protection service. It has more advanced DDoS protection capabilities. It provides enhanced protection against sophisticated and larger-scale DDoS attacks.

  - Optional DDoS mitigation service ($3,000 per month per organization)
  - Protect against more sophisticated attack on Amazon EC2, Elastic Load Balancing (ELB), Amazon CloudFront, AWS Global Accelerator, and Route 53
  - 24/7 access to AWS DDoS response team (DRP)
  - Protect against higher fees during usage spikes due to DDoS

- **AWS WAF** (Web Application Firewall) - lets you filter specific requests based on rules.

  ChatGPT

  AWS WAF (Web Application Firewall) is a service that helps protect web applications from common web exploits and harmful traffic. While it's not a dedicated DDoS protection service like AWS Shield, AWS WAF can contribute to DDoS mitigation by allowing you to create rules that block or allow traffic based on defined criteria. For example, you can set up rules to block requests from specific IP addresses or patterns commonly associated with DDoS attacks. By integrating AWS WAF with other AWS services, such as CloudFront or Application Load Balancers, you can enhance your overall DDoS protection strategy and safeguard your web applications from various threats.

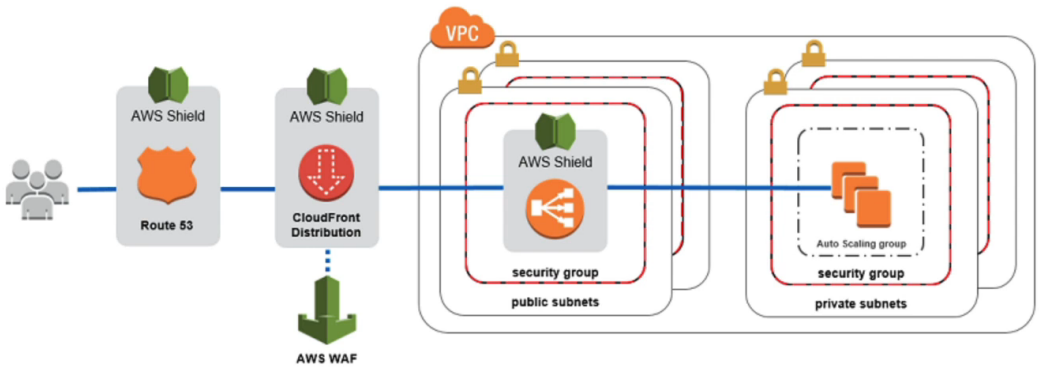
- Protects your web applications from common web exploits (Layer 7)
- Layer 7 is HTTP (vs Layer 4 is TCP)
- Deploy on Application Load Balancer, API Gateway, CloudFront

- Define Web ACL (Web Access Control List):
  - Rules can include IP addresses, HTTP headers, HTTP body, or URI strings
  - Protects from common attack - SQL injection and Cross-Site Scripting (XSS)
  - Size constraints, geo-match (block countries)
  - Rate-based rules (to count occurrences of events) – for DDoS protection

- **CloudFront and Route 53** - when using the global edge network, it must be combined with AWS Shield to allow protection against DDos attacks at edge locations.
- Always be ready to scale in case of such attacks - **leverage ASGs.**

DDoS Protection Architecture

Sample Reference Architecture for DDoS Protection



- My understanding of this diagram:

Users request to access a web application using the DSN generated through the Route 53 service. So, Route 53 is protected by AWS Shield and then that request goes to the user's nearest edge location where the web application content is cached, so that also needs to be protected by AWS Shield and AWS WAF which will filter the incoming requests based on the defined rules.

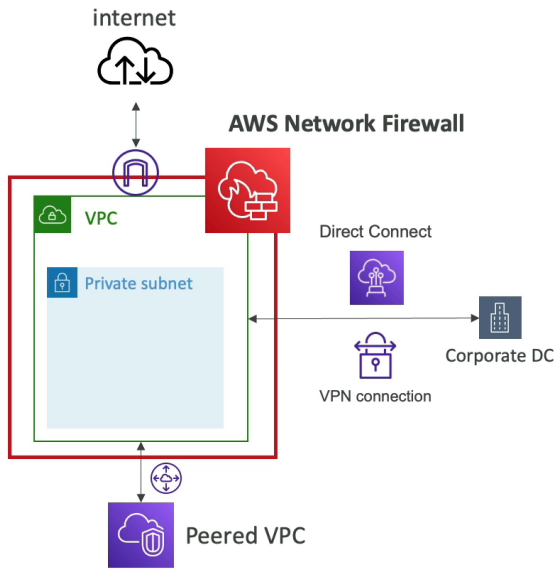
The traffic permitted to send the request to the server hits the EC2 instance which is situated inside of a public subnet within a VPC. This instance must be protected by a security group to again filter the inbound traffic and AWS Shield ofc.

Lastly, the EC2 instance is connected to an ASG so that, in the worst case scenario, even if the attacker is able to get to the instance, the application can auto scale (horizontally - launching new instances) to handle the sudden traffic spike.

I also think there should be an ELB in this architecture to distribute the incoming traffic to multiple different servers such that no server is overwhelmed.

AWS Network Firewall

- Protect your entire Amazon VPC
- From Layer 3 to Layer 7 protection
- Any direction, you can inspect
  - VPC to VPC traffic
  - Outbound to internet
  - Inbound from internet
  - To / from Direct Connect & Site-to-Site VPN



Penetration Testing on AWS

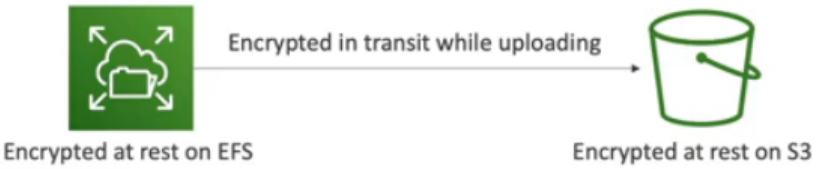
- Penetration testing on AWS involves simulating cyberattacks on your cloud infrastructure to identify and address security vulnerabilities.
- The goal is to uncover potential security risks, misconfigurations, or vulnerabilities that malicious actors could exploit. Penetration testing helps organizations assess and strengthen their security posture.

- AWS customers are welcome to carry out security assessments or penetration tests against their AWS infrastructure without prior approval for 8 services:
  - Amazon EC2 instances, NAT Gateways, and Elastic Load Balancers
  - Amazon RDS
  - Amazon CloudFront
  - Amazon Aurora
  - Amazon API Gateways
  - AWS Lambda and Lambda Edge functions
  - Amazon Lightsail resources
  - Amazon Elastic Beanstalk environments
- List can increase over time (you won't be tested on that at the exam)

- 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)

Encryption with KMS & CloudHSM

Data at rest vs. Data in transit



- At rest: data stored or archived on a device
  - On a hard disk, on a RDS instance, in S3 Glacier Deep Archive, etc.
- In transit (in motion): data being moved from one location to another
  - Transfer from on-premises to AWS, EC2 to DynamoDB, etc
  - Means data transferred on the network
- We want to encrypt data in both states to protect it!
- For this we leverage encryption keys

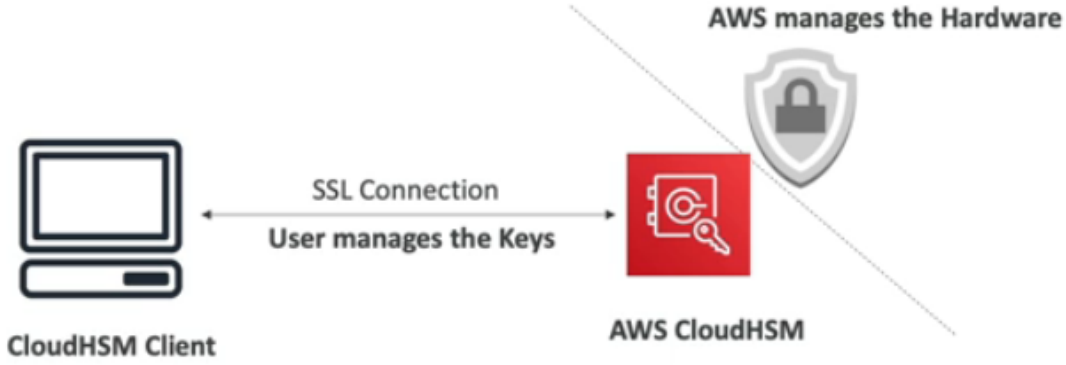
- **AWS KMS (Key Management Service)**

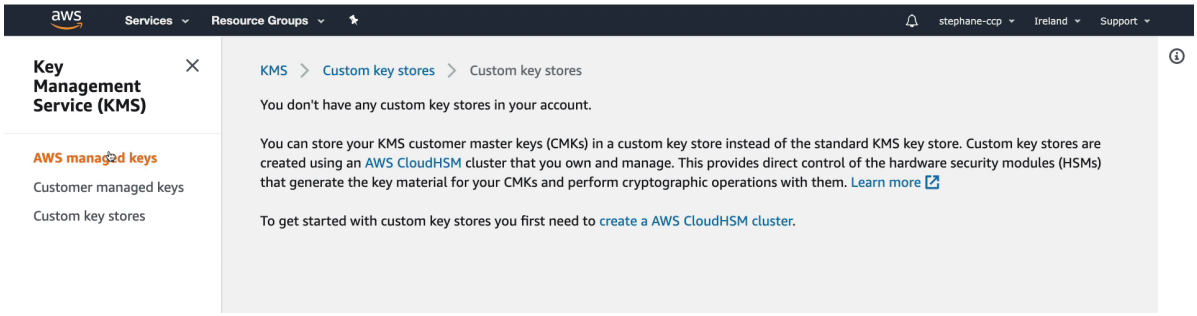
  - Anytime you hear "encryption" for an AWS service, it's most likely KMS
  - KMS = AWS manages the encryption keys for us
  - Encryption Opt-in:
    - EBS volumes: encrypt volumes
    - S3 buckets: Server-side encryption of objects
    - Redshift database: encryption of data
    - RDS database: encryption of data
    - EFS drives: encryption of data
  - Encryption Automatically enabled:
    - CloudTrail Logs
    - S3 Glacier

Types of KMS Keys

- Customer Managed Key:
  - Create, manage and used by the customer, can enable or disable
  - Possibility of rotation policy (new key generated every year, old key preserved)
  - Possibility to bring-your-own-key
- AWS Managed Key:
  - Created, managed and used on the customer's behalf by AWS
  - Used by AWS services (aws/s3, aws/ebs, aws/redshift)
- AWS Owned Key:
  - Collection of CMKs that an AWS service owns and manages to use in multiple accounts
  - AWS can use those to protect resources in your account (but you can't view the keys)
- CloudHSM Keys (custom keystore):
  - Keys generated from your own CloudHSM hardware device
  - Cryptographic operations are performed within the CloudHSM cluster

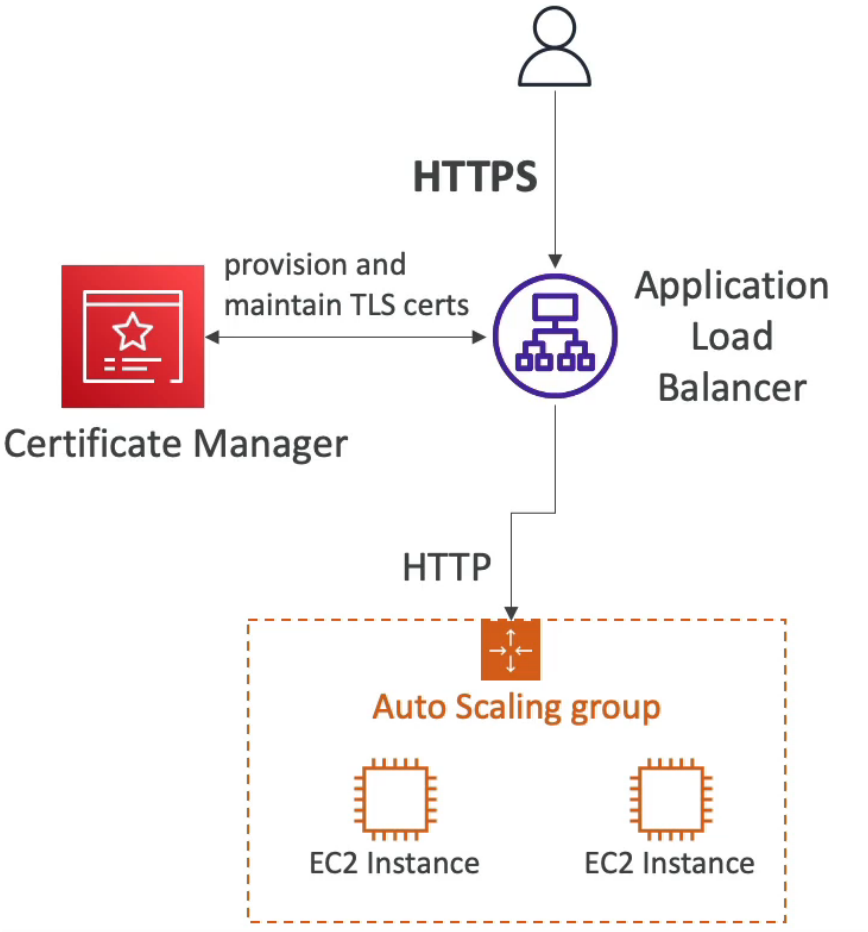
- **CloudHSM (Hardware Security Module)**
  - With HSM, aws provisions a dedicated hardware encryption device.
  - In this case, you manage your own encryption keys and not AWS.
  - HSM device is tamper resistant, FIPS 1 40-2 level 3 compliance (a security standard)





AWS Certificate Manager (ACM)

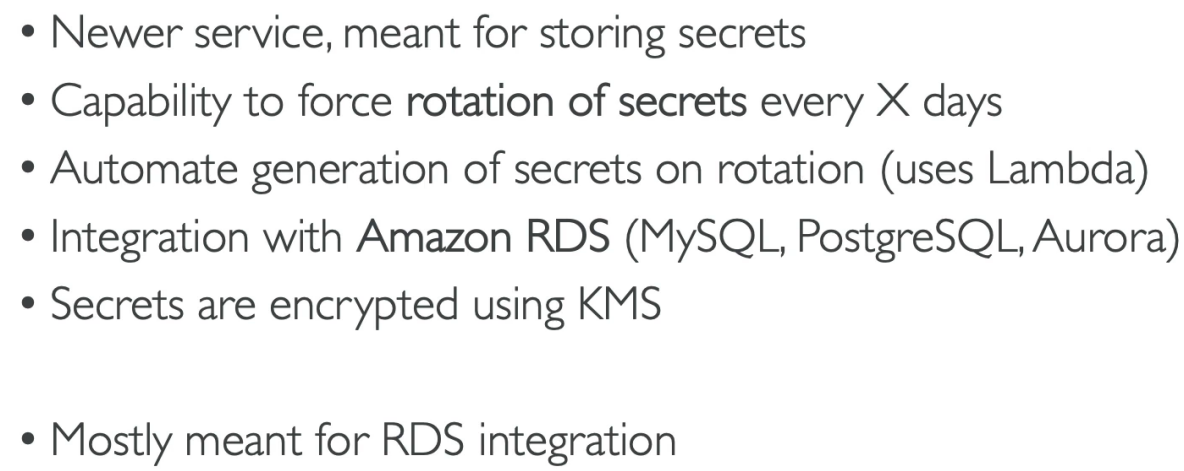
- ACM lets you easily provision, manage and deploy SSL/TLS certificates.
- These certificates are used to provide in-flight encryption for websites and enable HTTPS endpoints.
- Supports both public (free of cost) and private TLS certificates.
- Also allows automatic TLS certificate renewal feature.
- Exam: automatic infinite encryption certificate renewal = ACM.
- This service can be integrated with ELB, CloudFront Distributions, APIs or API Gateways so that it can load TLS certificates onto the user's endpoints making it secure (HTTPS).



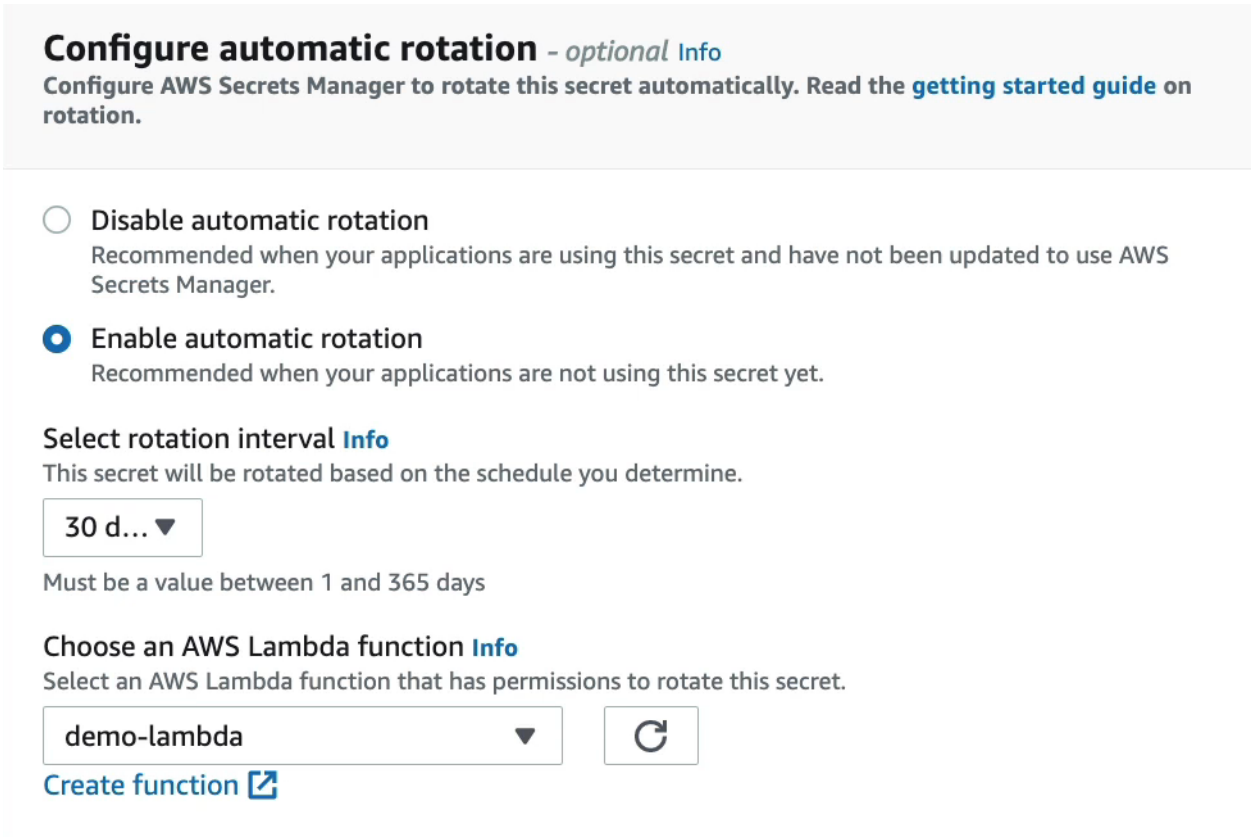
AWS Secrets Manager

- AWS Secrets Manager helps you protect sensitive information such as API keys, passwords, and database credentials.
- Allows you to securely store and manage sensitive information in a centralized and scalable manner. Instead of storing passwords and other secrets in your application code or configuration files, you can use Secrets Manager to store and retrieve them securely.
- Secrets Manager provides a simple API that your applications can use to retrieve the secrets they need during runtime.

- Seamlessly integrates with other AWS services. For instance, if you are running an AWS Lambda function that requires access to a database, you can configure it to retrieve the necessary credentials from Secrets Manager.



- One notable feature of AWS Secrets Manager is its ability to **automatically rotate secrets**. For example, if you store a database password, Secrets Manager can periodically update it without manual intervention.
- This dynamic rotation enhances security by minimizing the risk associated with long-lived static credentials.



AWS Artifact (not a service)

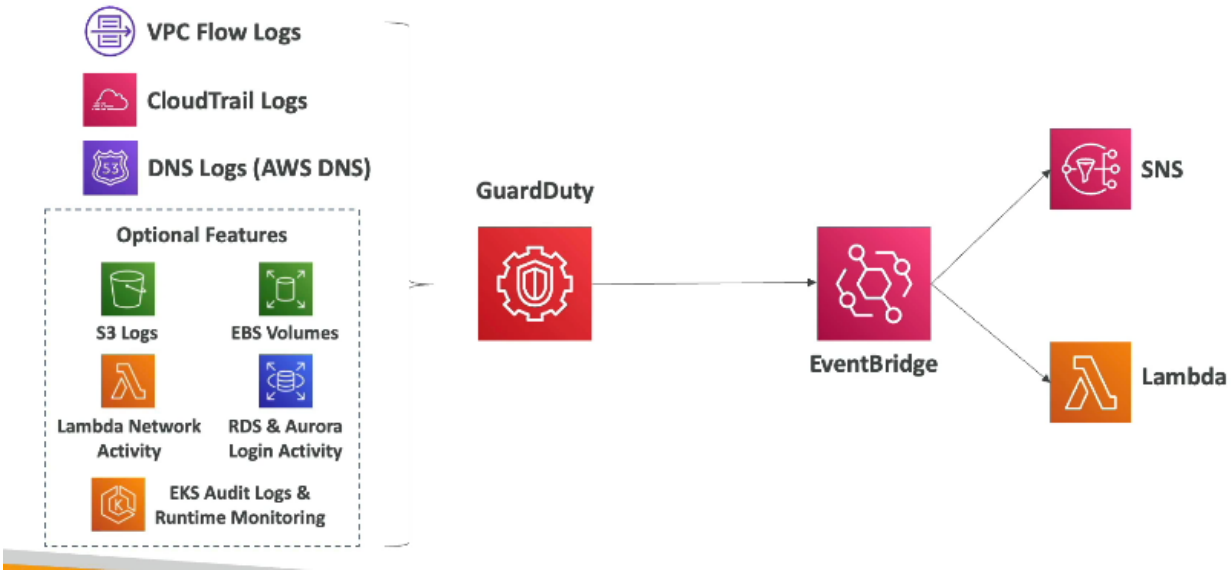
- Download compliance documents = artifact
- Check if you are in compliance with AWS laws = artifact

- Portal that provides customers with on-demand access to AWS compliance documentation and AWS agreements
- Artifact Reports - Allows you to download AWS security and compliance documents from third-party auditors, like AWS ISO certifications, Payment Card Industry (PCI), and System and Organization Control (SOC) reports
- Artifact Agreements - Allows you to review, accept, and track the status of AWS agreements such as the Business Associate Addendum (BAA) or the Health Insurance Portability and Accountability Act (HIPAA) for an individual account or in your organization

- Can be used to support internal audit or compliance

Amazon GuardDuty

- Intelligent Threat discovery to protect your AWS Account
- Uses Machine Learning algorithms, anomaly detection, 3rd party data
- One click to enable (30 days trial), no need to install software
- Input data includes:
  - CloudTrail Events Logs – unusual API calls, unauthorized deployments
    - CloudTrail Management Events – create VPC subnet, create trail, …
    - CloudTrail S3 Data Events – get object, list objects, delete object, …
  - VPC Flow Logs – unusual internal traffic, unusual IP address
  - DNS Logs – compromised EC2 instances sending encoded data within DNS queries
  - Optional Features – EKS Audit Logs, RDS & Aurora, EBS, Lambda, S3 Data Events…
- Can setup EventBridge rules to be notified in case of findings
- EventBridge rules can target AWS Lambda or SNS
- Can protect against CryptoCurrency attacks (has a dedicated "finding" for it)



Amazon Inspector

- Automated Security Assessments
- For EC2 instances
  - Leveraging the AWS System Manager (SSM) agent
  - Analyze against unintended network accessibility
  - Analyze the running OS against known vulnerabilities
- For Container Images push to Amazon ECR
  - Assessment of Container Images as they are pushed
- For Lambda Functions
  - Identifies software vulnerabilities in function code and package dependencies
  - Assessment of functions as they are deployed
- Reporting & integration with AWS Security Hub
- Send findings to Amazon Event Bridge

What does Amazon Inspector evaluate?

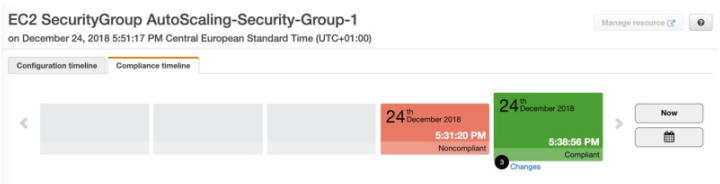
- Remember: only for EC2 instances, Container Images & Lambda functions
- Continuous scanning of the infrastructure, only when needed
- Package vulnerabilities (EC2, ECR & Lambda) – database of CVE
- Network reachability (EC2)
- A risk score is associated with all vulnerabilities for prioritization

AWS Config

- AWS Config helps you assess, audit, and evaluate the configurations of your AWS resources.
- It allows you to track changes to your resources over time, monitor compliance with your organization's policies, and troubleshoot potential security and configuration issues.
- This data can then be stored into S3 which can be analysed by Athena.
- You can receive alerts in case of any changes through SNS notifications.
- Config is a per-region service but you can aggregate it across multiple regions and accounts.
- AWS Config is about tracking and managing resource configurations, whereas AWS CloudTrail is about logging and auditing API-level activities in your AWS account. These services are often used together to provide a comprehensive view of both resource configurations and API-level actions.

- Questions that can be solved by AWS Config:
  - Is there unrestricted SSH access to my security groups?
  - Do my buckets have any public access?
  - How has my ALB configuration changed over time?

- View compliance of a resource over time

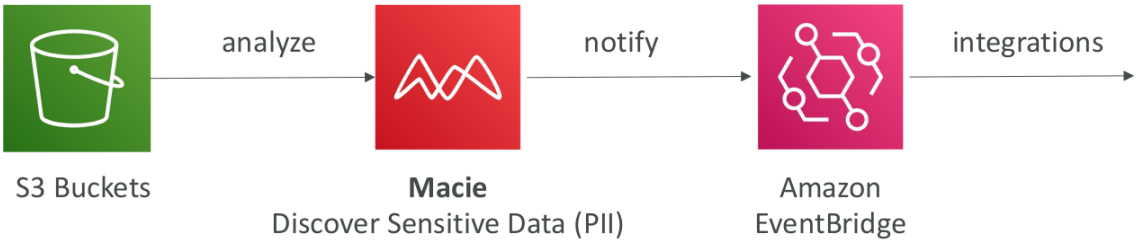


- View configuration of a resource over time

- View CloudTrail API calls if enabled

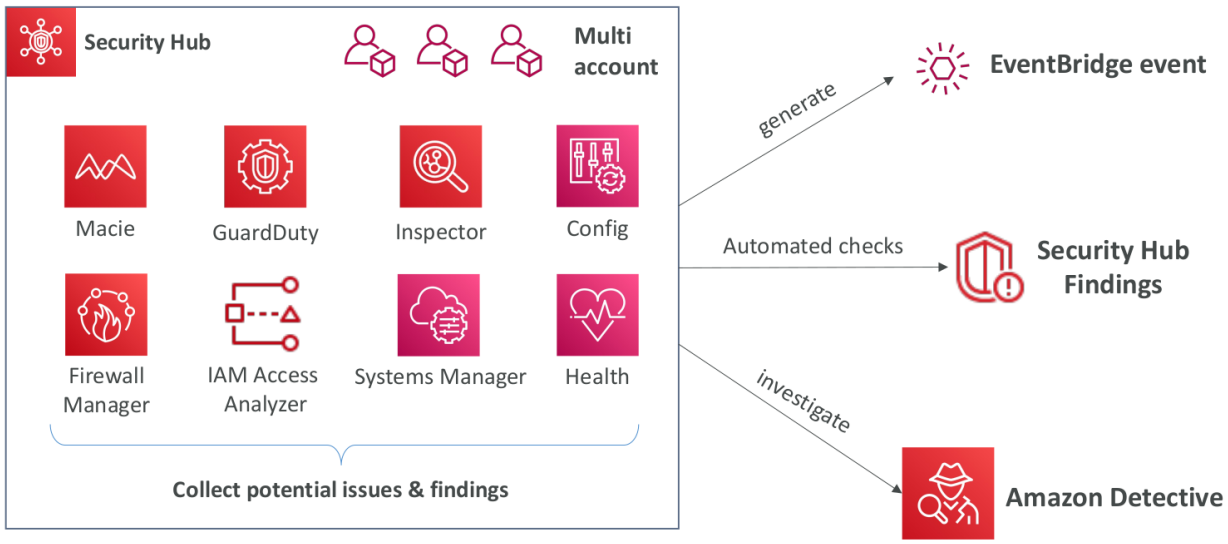
Amazon Macie

- Amazon Macie is a fully managed security service by AWS that uses machine learning to automatically discover, classify, and protect sensitive data, such as **personally identifiable information (PII)**, within your AWS environment.
- Can be enabled with one click and you just need to specify which s3 bucket you want it on.
- It helps organizations maintain data privacy and comply with regulations.



Security Hub

- Central security tool to manage security across several AWS accounts and automate security checks
- Integrated dashboards showing current security and compliance status to quickly take actions
- For security hub to work, you must enable AWS Config first.
- Automatically gathers alerts in standard or custom formats from different AWS services and partner tools:
  - Config
  - GuardDuty
  - Inspector
  - Macie
  - IAM Access Analyzer
  - AWS Systems Manager
  - AWS Firewall Manager
  - AWS Health
  - AWS Partner Network Solutions



Amazon Detective

- GuardDuty, Macie, and Security Hub are used to identify potential security issues, or findings
- Sometimes security findings require deeper analysis to isolate the root cause and take action – it's a complex process
- Amazon Detective **analyzes, investigates, and quickly identifies the root cause of security issues or suspicious activities (using ML and graphs)**
- **Automatically collects and processes events** from VPC Flow Logs, CloudTrail, GuardDuty and create a unified view
- Produces visualizations with details and context to get to the root cause

AWS Abuse

- Report suspected AWS resources used for abusive or illegal purposes
- Abusive & prohibited behaviors are:
  - **Spam** – receving undesired emails from AWS-owned IP address, websites & forums spammed by AWS resources
  - **Port scanning** – sending packets to your ports to discover the unsecured ones
  - **DoS or DDoS attacks** – AWS-owned IP addresses attempting to overwhlem or crash your servers/softwares
  - **Intrusion attempts** – logging in on your resources
  - **Hosting objectionable or copyrighted content** – distributing illegal or copyrighted content without consent
  - **Distributing malware** – AWS resources distributing softwares to harm computers or machines
- Contact the AWS Abuse team: AWS abuse form, or abuse@amazonaws.com

Root User Privileges

- Root user = account owner (the user created when the account is created)
- The root user has complete access to all AWS services and resources and it can perform some actions that even the most privileged created user within your account cannot do.
- So, the root user account should not be used for everyday tasks and must be locked away with access keys.
- Even administrative tasks are not recommended to be performed through the root user account, instead, create a different admin user account.
- **Actions that can be performed only by the root user: (imp for exam)**

- **Change account settings** (account name, email address, root user password, root user access keys)
- View certain tax invoices
- **Close your AWS account**
- Restore IAM user permissions
- **Change or cancel your AWS Support plan**
- **Register as a seller in the Reserved Instance Marketplace**
- Configure an Amazon S3 bucket to enable MFA
- Edit or delete an Amazon S3 bucket policy that includes an invalid VPC ID or VPC endpoint ID
- Sign up for GovCloud

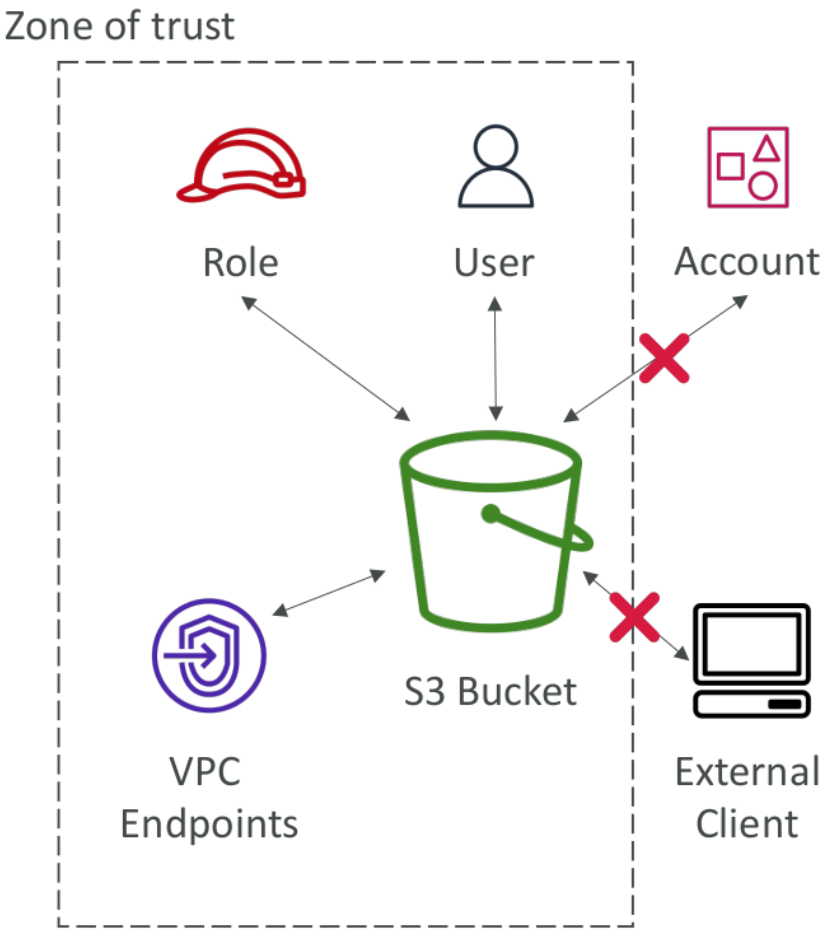
IAM Access Analyzer

- AWS IAM Access Analyzer is your security assistant, helping you keep an eye on who can do what in your AWS account and alerting you to any potential issues so you can fix them and keep your AWS environment secure.

Here's how it works:

1. **Policy Analysis:**
   - Access Analyzer looks at the policies attached to your resources. Policies are like sets of rules that say who can do what with a resource (e.g., who can read a file or modify a database).
2. **Identifying Risks:**
   - It analyzes these policies and tells you if there are any potential security risks. For example, it might highlight if someone has more access than necessary or if there's a chance of unintended sharing.
3. **Actionable Insights:**
   - Access Analyzer provides insights in a simple way, showing you what's okay and what needs attention. It helps you understand and fix potential security issues before they become problems.
4. **Security and Compliance:**
   - By using Access Analyzer, you can better ensure that your AWS environment follows security best practices and complies with your organization's policies.

- IAM Access Analyzer defines a **zone of trust** which refers to a set of AWS accounts and trusted entities within which you expect your resources to be accessed.
- Within this zone, certain access permissions are expected and considered normal.
- Enhances the accuracy and relevance of security analysis by focusing on potentially risky access patterns that fall outside the defined trusted zone.
- Any access outside of your zone of trust is reported as **findings.**
- Works especially for S3, IAM Roles, KMS Keys, Lambda functions, SQS queues, Secrets Manager.



SUMMARY

- Shared Responsibility on AWS
- **Shield:** Automatic DDoS Protection + 24/7 support for advanced
- **WAF:** Firewall to filter incoming requests based on rules
- **KMS:** Encryption keys managed by AWS
- **CloudHSM:** Hardware encryption, we manage encryption keys
- **AWS Certificate Manager:** provision, manage, and deploy SSL/TLS Certificates
- **Artifact:** Get access to compliance reports such as PCI, ISO, etc…
- **GuardDuty:** Find malicious behavior with VPC, DNS & CloudTrail Logs
- **Inspector:** find software vulnerabilities in EC2, ECR Images, and Lambda functions
- **Network Firewall:** Protect VPC against network attacks

- **Config:** Track config changes and compliance against rules
- **Macie:** Find sensitive data (ex: PII data) in Amazon S3 buckets
- **CloudTrail:** Track API calls made by users within account
- **AWS Security Hub:** gather security findings from multiple AWS accounts
- **Amazon Detective:** find the root cause of security issues or suspicious activities
- **AWS Abuse:** Report AWS resources used for abusive or illegal purposes
- **Root user privileges:**
  - Change account settings
  - Close your AWS account
  - Change or cancel your AWS Support plan
  - Register as a seller in the Reserved Instance Marketplace
- **IAM Access Analyzer:** identify which resources are shared externally

Good job!
The customer is responsible for firewall and network configuration. Customers are responsible for "Security IN the Cloud". It also includes server-side encryption, client-side data protection, customer data protection, etc.

Question 2:

According to the Shared Responsibility Model, who is responsible for firewall and network configuration for EC2 Instances?

- ○ AWS
- ◉ **The customer**
- ○ AWS and the customer

Good job!
Amazon Macie is a security service that uses machine learning to automatically discover, classify, and protect sensitive data in AWS, such as personally identifiable information (PII) or intellectual property.

Question 3:

Which of the following services can you use to discover and protect your sensitive data in AWS?

- ◉ **Macie**
- ○ Shield
- ○ Artifact
- ○ X-Ray

Good job!
AWS WAF is a web application firewall that helps protect your web applications or APIs against common web exploits that may affect availability, compromise security, or consume excessive resources.

This was discussed in Lecture 183: **DDoS Protection: WAF & Shield** >

Question 5:

A company would like to protect its web applications from common web exploits that may affect availability, compromise security, or consume excessive resources. Which AWS service should they use?

- Auto Scaling Groups (ASG)
- Shield
- CloudHSM
- **Web Application Firewall (WAF)**

Good job!
Penetration Testing is allowed without prior approval on 8 services. DDoS, port flooding and protocol flooding are examples of prohibited activities.

Question 7:

You can perform any kind of penetration testing on any AWS service without prior approval.

- True
- **False**

Good job!
AWS Certificate Manager is a service that lets you easily provision, manage, and deploy public and private Secure Sockets Layer/Transport Layer Security (SSL/TLS) certificates for use with AWS services and your internal connected resources.

Question 9:

A company would like to secure network communications using SSL & TLS certificates. Which AWS service can it use?

- (●) **Certificate Manager (ACM)**
- ( ) Secrets Manager
- ( ) Macie
- ( ) WAF

Incorrect answer. Please try again.
Customers are responsible for patching their guest OS and applications, but that's not the only patching on AWS.

This was discussed in Lecture 182: **Shared Responsibility Model: Reminders & Examples** >

Question 10:

According to the Shared Responsibility Model, who is responsible for Patch Management?

- ( ) **AWS**
- ( ) The customer
- ( ) **AWS and the customer**

Good job!
AWS is responsible for patching and fixing flaws within the infrastructure, but customers are responsible for patching their guest OS and applications. Shared Controls also includes Configuration Management, and Awareness and Training.

This was discussed in Lecture 182: **Shared Responsibility Model: Reminders & Examples** >

Question 10:

According to the Shared Responsibility Model, who is responsible for Patch Management?

- ○ AWS
- ○ The customer
- ◉ **AWS and the customer**

Good job!
Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS. It helps you test the network accessibility of your Amazon EC2 instances and the security state of your applications running on the instances.

Question 13:

A company would like to automate security on EC2 instances to assess security and vulnerabilities in these instances. Which AWS service should it use?

- ○ Config
- ○ Trusted Advisor
- ◉ **Inspector**
- ○ Systems Manager

Good job!
Shield is only used to safeguard running applications from DDoS attacks.

Question 16:

Which AWS service's ONLY role is to safeguard running applications from DDoS attacks?

- WAF
- **Shield**
- CloudFront
- KMS

Good job!
This is not a situation where you should contact the AWS Abuse team. The situations where you should contact the AWS Abuse team are: Spam, Port scanning, DoS or DDoS attacks, Intrusion attempts, Hosting objectionable or copyrighted content, Distributing malware.

Question 18:

Which of the following options is NOT a situation where you should contact the AWS Abuse team?

- DDoS attack from AWS-owned IP addresses
- Spam from AWS-owned IP addresses or AWS resources
- Hosting objectionable or copyrighted content on AWS
- **Losing your MFA device**