

Shared Responsibility Model : Remainder

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

- 1.
2. So for example, as a customer, you are responsible for the security in the cloud. So in the instance of EC2 instance as a customer of aws we are responsible for the management of all the operating system that includes patching the operating system and making updates to it.
3. We have to configure firewalls for our ec2 instance..like NACL..and also you need to make sure that your EC2 instance has the correct IAM information through the use of, IAM instance role.

-
- 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

- 4.
5. For example, for awareness and training, AWS has to train their employees to use their facilities correctly, and to make sure they adhere to their security guidelines. And you have to make sure to train your employees correctly, to use the cloud, and doing this training is one of these ways, obviously.
- 6.

Shared controls in AWS are security controls that are jointly managed by AWS and its customers. These controls apply to both the infrastructure layer and the customer layer, but in completely separate contexts or perspectives.

For example, AWS is responsible for patching and fixing flaws within the infrastructure, but customers are responsible for patching their guest operating system and applications. AWS maintains the configuration of its infrastructure devices, but customers are responsible for configuring their own guest operating systems, databases, and applications.

Shared controls can be a source of confusion for customers, as it can be difficult to determine which party is responsible for implementing and maintaining a particular control. However, AWS provides documentation and guidance on shared controls to help customers understand their responsibilities.

Here are some examples of shared controls in AWS:

- **Patch management:** AWS is responsible for patching and fixing flaws within the infrastructure, but customers are responsible for patching their guest operating system and applications.
7.
8. Lets take example of RDS
9.

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

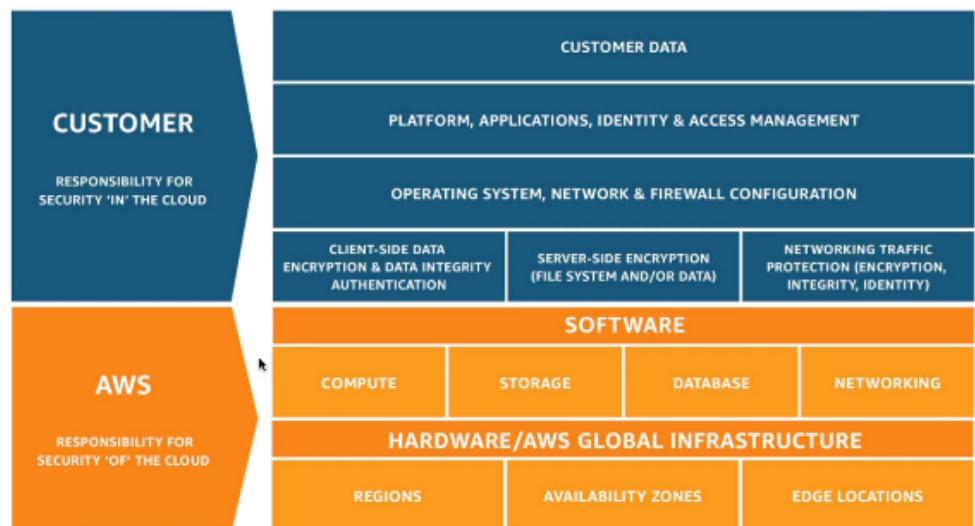
10. Example of s3

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

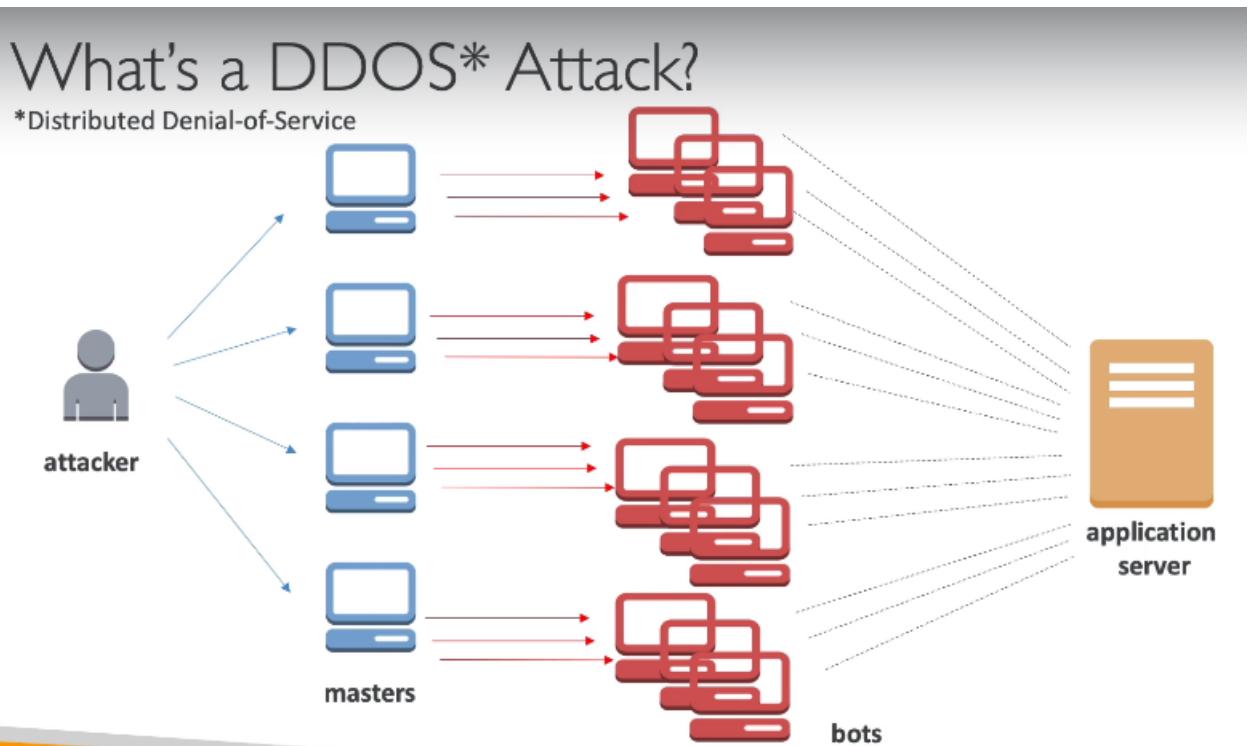
11.

Shared Responsibility Model diagram

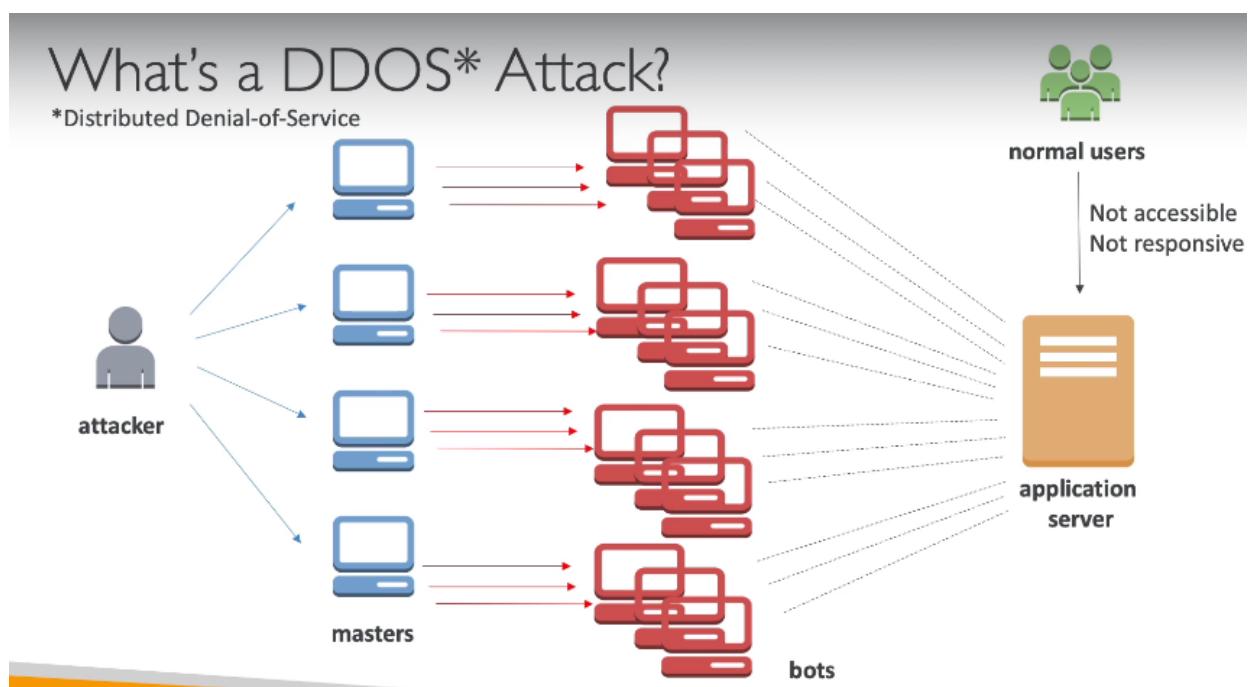


12.

DDoS Protection:WAF & shield



1.



2.

3. and therefore any normal user trying to connect to our application server, will see that our server is not accessible or not responsive,effectively making our application down.

DDOS Protection on AWS

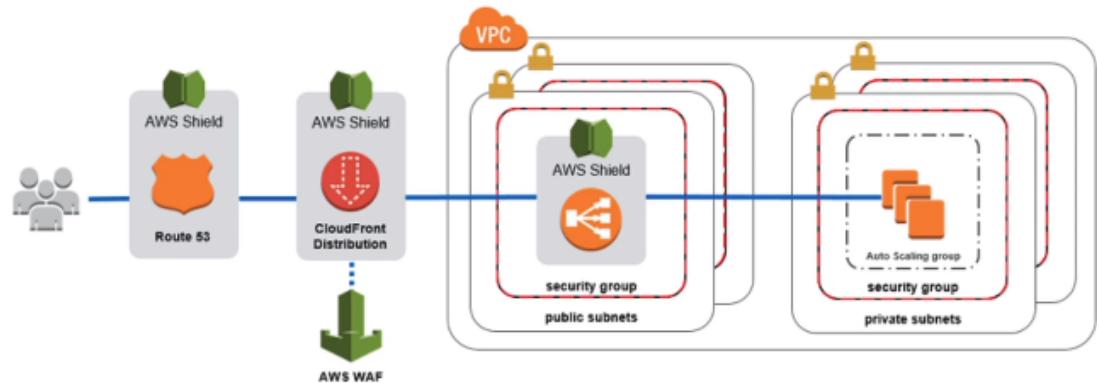
- AWS Shield Standard: protects against DDOS attack for your website and applications, for all customers at no additional costs
 - AWS Shield Advanced: 24/7 premium DDoS protection
 - AWS WAF: Filter specific requests based on rules
 - CloudFront and Route 53:
 - Availability protection using global edge network
 - Combined with AWS Shield, provides attack mitigation at the edge
 - Be ready to scale – leverage AWS Auto Scaling
- 4.
 5. Even if we getting attacked.... we need to be ready to scale..to avoid crashing and giving users to access our application

AWS offers a variety of services to help protect against DDoS attacks, including:

- **AWS Shield Standard:** This is a free service that provides basic DDoS protection for all AWS customers. Shield Standard uses a combination of network flow monitoring, signature-based detection, and anomaly detection to identify and mitigate DDoS attacks.
- **AWS Shield Advanced:** This is a paid service that provides more comprehensive DDoS protection than Shield Standard. Shield Advanced includes all of the features of Shield Standard, as well as additional features such as:
 - Application layer DDoS protection
 - Custom detection rules
 - 24/7 support from AWS experts
- **AWS WAF:** This is a web application firewall (WAF) that can be used to protect web applications from a variety of attacks, including DDoS attacks. WAF can be used to block malicious traffic, filter traffic, and rate limit traffic.
- **AWS CloudFront:** This is a content delivery network (CDN) that can be used to distribute your content to users around the world. CloudFront can help to protect your content from DDoS attacks by caching your content in multiple locations and by using a variety of techniques to mitigate DDoS attacks.

6.

Sample Reference Architecture for DDoS Protection



7.

8. So we have our users
9. and they will be routed through the DNS on Route 53 which is protected by shield so your DNS is safe from DDoS attack, then you should use a CloudFront distribution to make sure your content is cached at the edge and then it is also protected by shield
10. and in case you need to filter and protect from an attack, you can use the web application firewall, then to serve that application you can use a load balancer in the public subnet that will scale for you
11. and finally behind the load balancer you should use EC2 instances in an auto scaling group to be able to scale to the higher demand.
12. AWS Shield



- AWS Shield Standard:
 - 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:
 - 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

13.

AWS WAF – Web Application Firewall



- 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

14.

Sure. AWS WAF (Web Application Firewall) is a web application firewall that helps protect web applications from a variety of attacks, including common web exploits and bots that can affect availability, compromise security, or consume excessive resources. AWS WAF can be used to block malicious traffic, filter traffic, and rate limit traffic.

Here is a practical example of how AWS WAF can be used to protect a web application from a DDoS attack. Let's say you have a web application that is hosted on Amazon Elastic Compute Cloud (EC2) instances. You can use AWS WAF to create a rule that blocks traffic from any IP address that sends more than 100 requests per second to your web application. This will help to protect your web application from a DDoS attack that is trying to overwhelm your EC2 instances with traffic.

15.

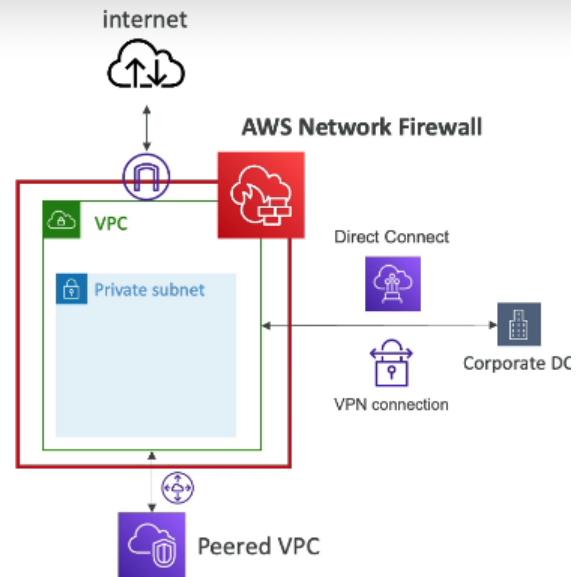
Sure. A web access control list (Web ACL) is a collection of rules that you define to control the HTTP(S) traffic that your web application receives. AWS WAF uses Web ACLs to inspect and filter web requests before they reach your application.

16.

AWS Network FireWall

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



1.

Penetration testing

Penetration Testing on AWS Cloud



- 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)

1.

Penetration Testing on your AWS Cloud



• 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 any other simulated events, contact aws-security-simulated-event@amazon.com
- Read more: <https://aws.amazon.com/security/penetration-testing/>

2.

DNS zone walking is a type of attack that attempts to retrieve all of the records in a DNS zone. This can be done by issuing a series of DNS queries, starting with the zone apex (the domain name itself) and then recursively querying for all of the subdomains.

In AWS, DNS zone walking can be performed using the Route 53 API or the Route 53 console. To perform a zone walk using the API, you would use the following command:

Code snippet

```
aws route53 list-resource-record-sets --hosted-zone-id Z123ABCDE890ABCDE
```

Use code with caution. [Learn more](#)



This command will return a list of all of the resource record sets in the specified hosted zone.

To perform a zone walk using the console, you would go to the Route 53 console and select the hosted zone that you want to walk. Then, you would click on the "Resource record sets" tab. This will display a list of all of the resource record sets in the hosted zone.

3.

Encryption with KMS and cloudHSM

1. Here we have two types of encryption...which is data at rest & data in transit

Data at rest vs. Data in transit



Encrypted at rest on EFS



Encrypted at rest on S3

- **At rest:** data stored or archived on a device
 - On a hard disk, on a RDS instance, in S3 Glacier Deep Archive, etc.

2.

3. Here we can see data is encrypted and stores in EFS and S3

Data at rest vs. Data in transit



Encrypted at rest on EFS



Encrypted at rest on S3

- **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!

4. For this we leverage encryption keys

5.

Leveraging encryption keys in AWS allows you to protect your data by encrypting it with a key that is stored in AWS Key Management Service (KMS). This ensures that your data is only accessible to authorized users and that it cannot be decrypted without the key.

Here are some of the benefits of leveraging encryption keys in AWS:

- **Data security:** Encryption keys help to protect your data from unauthorized access, even if your data is stored in the cloud.
- **Compliance:** Encryption keys can help you to comply with data security regulations, such as HIPAA and PCI DSS.
- **Auditability:** Encryption keys can help you to track who has access to your data and when they accessed it.
- **Scalability:** Encryption keys can be used to encrypt data stored in any AWS service, so you can easily scale your security as your needs grow.

Sure. Here is an example of how you can leverage encryption keys in AWS to protect your data:

Let's say you have a database of customer records that you need to store in the cloud. You can use AWS KMS to create an encryption key and then use that key to encrypt the data in your database. This will ensure that your data is only accessible to authorized users and that it cannot be decrypted without the key.

To do this, you would first need to create an encryption key in AWS KMS. You can do this using the AWS KMS console or the AWS KMS API. Once you have created an encryption key, you can then use it to encrypt your data.

6.

7. AWS KMS

8. So the encryption service at the center of AWS is called KMS, key management service. So anytime you hear encryption for a service it's most likely going to be KMS.
9. And so with KMS we don't have access to the keys. AWS will manage the keys for us and we just define who can access these 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
 - Storage Gateway

10.

11. We have an option to choose the encryption for like EBS,S3 etc..

12. CloudHSM

CloudHSM



- KMS => AWS manages the software for encryption
- CloudHSM => AWS provisions encryption hardware
- Dedicated Hardware (HSM = Hardware Security Module)
- You manage your own encryption keys entirely (not AWS)
- HSM device is tamper resistant, FIPS 140-2 Level 3 compliance



Sample HSM device

13.

Sure. Here is a practical example of how you can use CloudHSM in AWS:

Let's say you have a web application that stores customer credit card information. You want to store this information in a secure way, so you decide to use CloudHSM.

You would first need to create a CloudHSM cluster. You can do this using the AWS Management Console or the AWS CLI. Once you have created a CloudHSM cluster, you would need to create a Customer Master Key (CMK) in AWS KMS. You can do this using the AWS Management Console or the AWS CLI.

Once you have created a CMK, you would need to use the CloudHSM client to encrypt the customer credit card information. You can do this using the CloudHSM API or the CloudHSM CLI.

Once the customer credit card information is encrypted, you would need to store it in your web application. You can store the encrypted data in any AWS service that supports encryption, such as Amazon S3 or Amazon RDS.

14. To access the customer credit card information, you would need to use the CloudHSM client to decrypt the data. You can do this using the CloudHSM API or the CloudHSM CLI.

A customer master key (CMK) is a cryptographic key that you create and manage in AWS Key Management Service (KMS). You can use a CMK to encrypt your data and to perform cryptographic operations on your data.

CMKs are stored in AWS KMS, which is a highly secure service that uses FIPS 140-2 Level 3 validated hardware and software to protect your keys. AWS KMS also provides detailed audit logs that you can use to track who has accessed your keys and when they accessed them.

There are two types of CMKs:

- **Customer managed CMKs:** These are CMKs that you create and manage in AWS KMS. You have full control over these CMKs, including their key policies, IAM policies, and grants.
 - **AWS managed CMKs:** These are CMKs that are created and managed by AWS. AWS managed CMKs are used by AWS services to encrypt your data. You cannot directly use AWS managed CMKs, but you can use them indirectly by using the AWS services that use them.
- 15.

Types of Customer Master Keys: CMK

- **Customer Managed CMK:**
 - 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 CMK:**
 - Created, managed and used on the customer's behalf by AWS
 - Used by AWS services (aws/s3, aws/ebs, aws/redshift)
- **AWS owned CMK:**
 - 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

16.

17. So this customer managed CMK are the keys that we create, manage and use ourselves, AWS users.

18. And we can create them, enable them or disable them. We can define a rotation policy for these keys, for example a new key generated every year while the old keys of course preserved. And we can bring our own key.

AWS KMS & cloudHSM hands on

1. Here first we have create a volume for our ec2 instance and have to opt in encryption and gave protection to it using aws/ebs

Volumes > Create Volume

Create Volume

Volume Type: General Purpose SSD (gp2) i

Size (GiB): 1 (Min: 1 GiB, Max: 16384 GiB) i

IOPS: 300 / 3000 (Baseline of 3 IOPS per GiB with a minimum of 100 IOPS, burstable to 3000 IOPS) i

Availability Zone*: eu-west-1a i

Throughput (MB/s): Not applicable i

Snapshot ID: Select a snapshot C i

Encryption: Encrypt this volume

Key (128 characters maximum) i

Value (256 characters) i

2.

Master Key (default) avs/ebs C

KMS Key Description Default master key that protects my EBS volumes when no other key is defined

KMS Key Account This account (855174697623)

KMS Key ID 640b56a8-94cf-4911-9923-0a90fb41eac4

KMS Key ARN arn:aws:kms:eu-west-1:855174697623:key/640b56a8-94cf-4911-9923-0a90fb41eac4

Volumes that are created from encrypted snapshots are automatically encrypted, and volumes that are created from unencrypted snapshots are automatically unencrypted. If no snapshot is selected, you can choose to encrypt the volume and specify your own key. [Learn more about KMS keys](#)

- 3.
4. Then click on create volume
5. And now we have created an encrypted volume. So it is properly protected against for example, attacks if they're trying to decrypt it.
6. where this is a voluntary opt-in for the encryption. But if you remember, I said that for example, for CloudTrail or for Glacier S3 encryption was enabled by default.

CloudTrail > Dashboard > arn:aws:cloudtrail:eu-west-1:855174697623:trail/demo-trail

demo-trail Delete Stop logging

General details			
Trail logging Logging	Trail log location clouptrail-demo-stephane-ccp/AWSLogs/855174697623	Log file validation Disabled	SNS notification delivery Disabled
Trail name demo-trail	Last file validation delivered -	Last SNS notification -	
Apply trail to my organization Not enabled	Last log file delivered June 02, 2020, 19:18 (UTC+01:00)		
	Log file SSE-KMS encryption Disabled		

7.

- 8.
9. even though it said disabled here for the encryption, it actually was enabled in Amazon S3.
10. In customer managed keys

- 11.
12. If we create a CMS..then we get an option to choose encryption for our volume

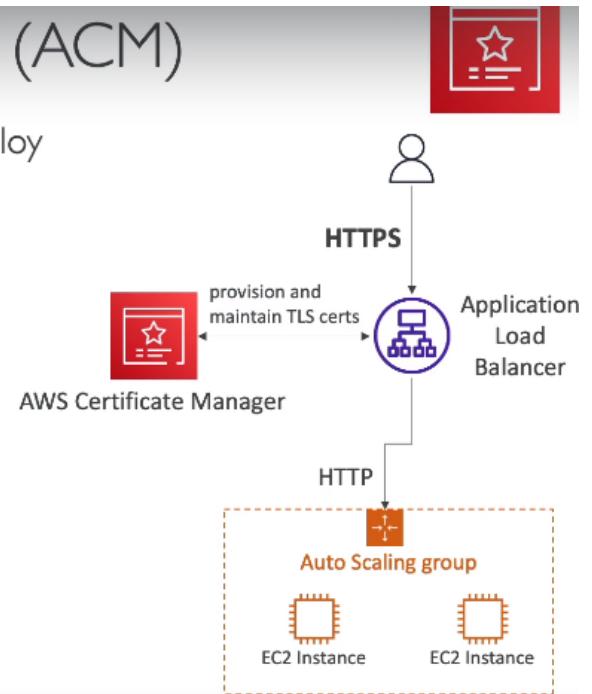
Availability Zone	State	Alarm Status	Attachment Information	Monitoring	Volume Status	Encryption	KMS Key ID	KMS Key Alias	Multi-Attach Enabled
eu-west-1a	available	None			Okay	Encrypted	d9630b4-d7a...	demokey	No
eu-west-1a	available	None			Okay	Encrypted	640b56a6-84cf...	sjsebs	No

- 13.
14. Here we have created 2 volumes with diff types of encryptions ..

AWS Certificate Manager(ACM)

AWS Certificate Manager (ACM)

- Let's you easily provision, manage, and deploy SSL/TLS Certificates
- Used to provide in-flight encryption for websites (HTTPS)
- Supports both public and private TLS certificates
- Free of charge for public TLS certificates
- Automatic TLS certificate renewal
- Integrations with (load TLS certificates on)
 - Elastic Load Balancers
 - CloudFront Distributions
 - APIs on API Gateway



1.

Sure. AWS Certificate Manager (ACM) is a fully managed service that makes it easy to request, deploy, and manage SSL/TLS certificates for your website or application. ACM can be used to provision certificates for a wide variety of use cases, including:

- **Ecommerce websites:** ACM can be used to provision certificates for ecommerce websites, which helps to protect sensitive data, such as credit card numbers, from being intercepted by unauthorized third parties.
 - **Banking websites:** ACM can also be used to provision certificates for banking websites, which helps to protect customers' financial information from being intercepted by unauthorized third parties.
 - **Email:** ACM can also be used to provision certificates for email servers, which helps to protect the confidentiality of email messages.
 - **Remote access:** ACM can also be used to provision certificates for remote access servers, which helps to protect sensitive data from being accessed by unauthorized users.
- 2.
3. So anytime you see what service can help us do in-flight encryption and generates these certificates then think ACM, that's it.

Inflight encryption in AWS Certificate Manager (ACM) is a feature that encrypts all traffic between your website or application and your users' browsers. This helps to protect sensitive data, such as credit card numbers and passwords, from being intercepted by unauthorized third parties.

Inflight encryption works by using a technique called Transport Layer Security (TLS). TLS is a cryptographic protocol that encrypts data in transit. When a user visits your website or application, their browser will request a TLS connection from your server. Your server will then send back a TLS certificate, which contains the public key for your website or application. The user's browser will then use the public key to encrypt data that it sends to your server. Your server will then decrypt the data using its private key.

4. This process ensures that all traffic between your website or application and your users' browsers is encrypted and cannot be intercepted by unauthorized third parties.

AWS Secrets Manager

AWS Secrets Manager

- Newer service, meant for storing secrets
 - Capability to force rotation of secrets every X days
 - Automate generation of secrets on rotation (uses Lambda)
 - Integration with Amazon RDS (MySQL, PostgreSQL, Aurora)
1. And it has an integration with Amazon RDS. So using the Secrets Manager, we can create the passwords for Amazon RDS automatically.
 2. The secrets are going to be encrypted using KMS, that we just saw from before, automatically.
 3. And so from an exam perspective, anytime you see a secret to be managing in RDS and to be rotated, you have to think about Secrets Manager.

- Secrets are encrypted using KMS

- Mostly meant for RDS integration

5.

The screenshot shows a user interface titled "Store a new secret". Below it, a section titled "Select secret type" includes a link "Info". There are five options, each with a radio button:

- Credentials for RDS database
- Credentials for DocumentDB database
- Credentials for Redshift cluster
- Credentials for other database
- Other type of secrets (e.g. API key)

6.

AWS ArtiFact

AWS Artifact (not really a service)



- 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
 - 1.
 2. Can be used to download reports regarding security and compliances etc
 3. It's not really a service. It's a way for you to download compliance documents,

Amazon GuardDuty

1.

Amazon GuardDuty



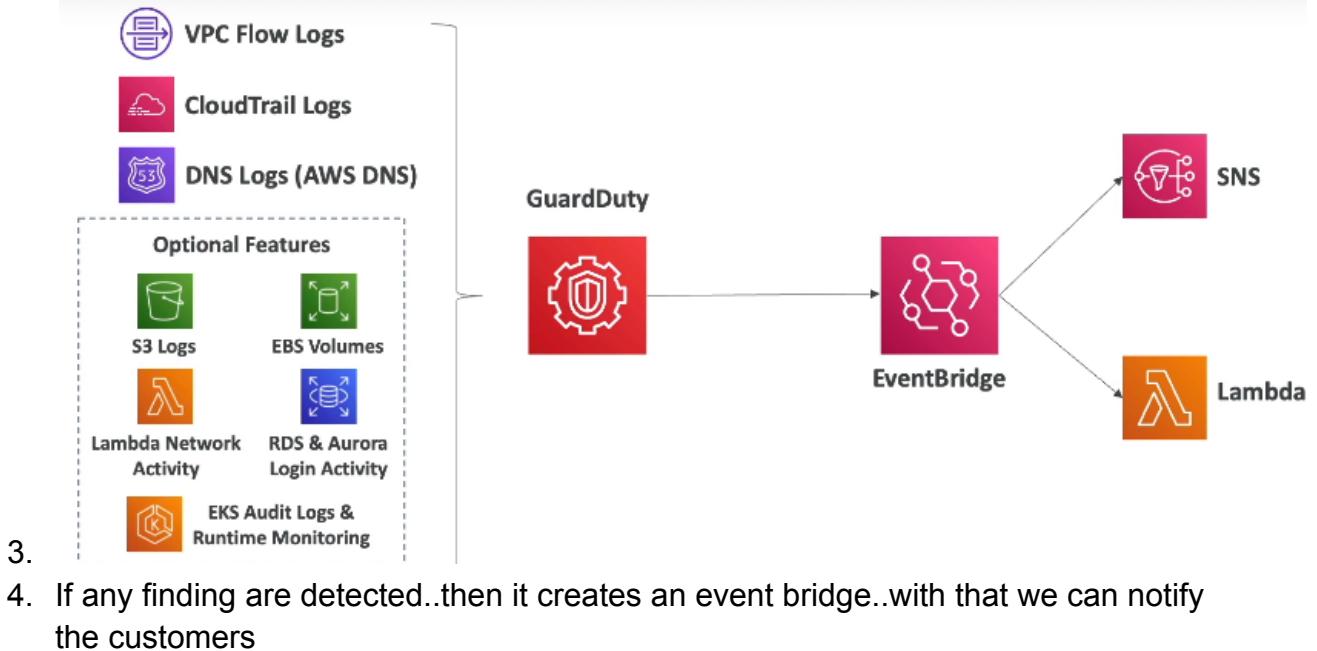
- Intelligent Threat discovery to protect your AWS Account
- Uses Machine Learning algorithms, anomaly detection, 3rd party data
- One click to enable (30 days trial), no need to install software
- Input data includes:
 - CloudTrail Events Logs – unusual API calls, unauthorized deployments
 - CloudTrail 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)

Sure. Amazon GuardDuty is a continuous security monitoring service that helps to identify and investigate potential security threats to your AWS resources. GuardDuty uses machine learning and anomaly detection to identify unusual activity in your AWS environment, and it can alert you to potential threats even before they cause damage.

Here is an example of how you can use GuardDuty to protect your AWS resources:

2.
 - Let's say you have an EC2 instance that is running a web server. GuardDuty can monitor the instance for unusual activity, such as a large number of failed login attempts or a sudden increase in network traffic. If GuardDuty detects any unusual activity, it will alert you so that you can investigate the issue.
 - GuardDuty can also monitor your VPC for unauthorized access. If GuardDuty detects any unauthorized access, it will alert you so that you can take action to block the unauthorized access.
 - GuardDuty can also monitor your AWS CloudTrail logs for suspicious activity. If GuardDuty detects any suspicious activity, it will alert you so that you can investigate the issue.

Amazon GuardDuty

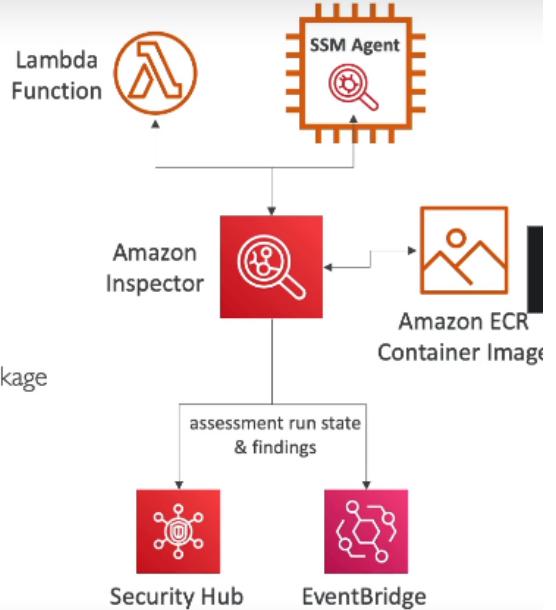


Amazon Inspector

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

1.



What does Amazon Inspector evaluate?

2.

- 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 with auditing and recording compliance of your AWS resources
- Helps record configurations and changes over time

1.

2. So any time we've been doing some manual changes of the configuration in AWS, we did not have a list of all the changes that happened, but we can have this using Config.

AWS Config



- Helps with auditing and recording compliance of your AWS resources
- Helps record configurations and changes over time
- Possibility of storing the configuration data into S3 (analyzed by Athena)
- 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?
- You can receive alerts (SNS notifications) for any changes
- AWS Config is a per-region service
- Can be aggregated across regions and accounts

3.

AWS Config Resource

- View compliance of a resource over time



- View configuration of a resource over time



- View CloudTrail API calls if enabled

- 4.
5. And finally, you can view who made these changes to the resources based on CloudTrail if you have enabled CloudTrail in your accounts.
- 6.

Sure. AWS Config is a service that helps you to track and manage the configurations of your AWS resources. You can use AWS Config to:

- **Record the current configuration of your AWS resources:** AWS Config records the current configuration of your AWS resources in a central repository. This allows you to track changes to your configurations over time and to restore your resources to a previous configuration if necessary.
- **Identify misconfigurations:** AWS Config can identify misconfigurations in your AWS resources. This can help you to improve the security and compliance of your AWS environment.
- **Audit your AWS environment:** AWS Config can be used to audit your AWS environment to ensure that your resources are configured in accordance with your security policies and procedures.

Here is an example of how you can use AWS Config to track and manage the configurations of your AWS resources:

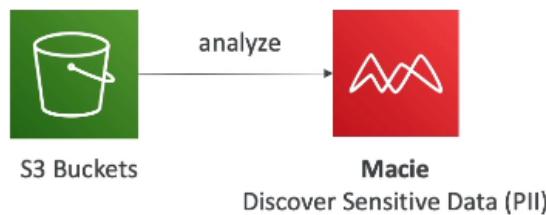
- Let's say you have an EC2 instance that is running a web server. You can use AWS Config to record the current configuration of the EC2 instance, including the ports that are open, the permissions that are granted to users, and the software that is installed.
 - If you make a change to the configuration of the EC2 instance, AWS Config will record the change. This allows you to track changes to the configuration of the EC2 instance over time and to restore the EC2 instance to a previous configuration if necessary.
 - AWS Config can also identify misconfigurations in the EC2 instance. For example, if you open a port that should not be open, AWS Config will identify the misconfiguration. This can help you to improve the security of the EC2 instance.
 - You can also use AWS Config to audit your AWS environment to ensure that your resources are configured in accordance with your security policies and procedures. For example, you can use AWS Config to ensure that all of your EC2 instances have strong passwords and that all of your software is up to date.
- 7.

AWS Macie

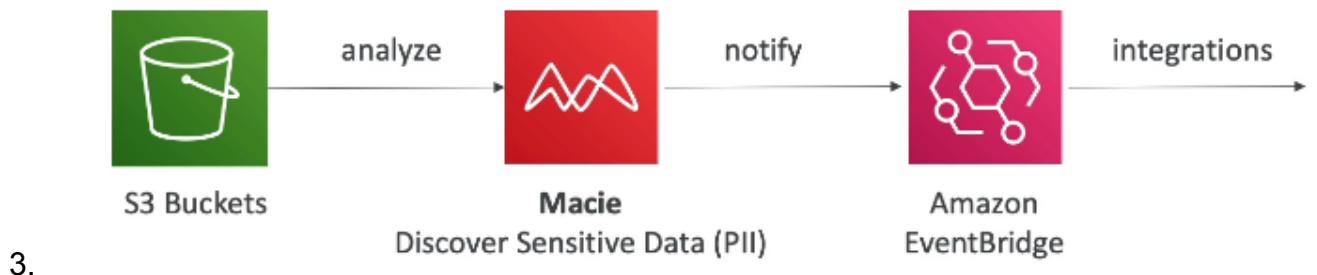
Amazon Macie



- Amazon Macie is a fully managed data security and data privacy service that uses machine learning and pattern matching to discover and protect your sensitive data in AWS.
- Macie helps identify and alert you to sensitive data, such as personally identifiable information (PII)



- 1.
2. So very simply, your PII data will be in your S3 buckets and it will be analyzed by Macie which will discover what data can be classified as PII.



Sure. Amazon Macie is a fully managed data security and compliance service that uses machine learning to discover, classify, and protect sensitive data in AWS. Macie can be used to:

- **Discover sensitive data:** Macie uses machine learning to discover sensitive data in your AWS environment, including personal identifiable information (PII), financial data, and intellectual property.
- **Classify sensitive data:** Macie classifies sensitive data according to a variety of classification schemes, such as industry standards and regulatory requirements.
- **Protect sensitive data:** Macie can be used to protect sensitive data by encrypting it, tagging it, and setting access controls.
- **Audit your AWS environment:** Macie can be used to audit your AWS environment to ensure that your sensitive data is properly classified and protected.

4.

Here is an example of how you can use Amazon Macie to protect sensitive data:

- Let's say you have a database that contains PII data. You can use Macie to discover the database and classify the PII data. Macie can then be used to encrypt the PII data and set access controls to restrict access to the data.
- Macie can also be used to audit the database to ensure that the PII data is properly classified and protected. For example, Macie can be used to check if the PII data is encrypted and if access to the data is restricted to authorized users.

5.

AWS Security Hub

AWS 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
- Automatically aggregates alerts in predefined or personal findings formats from various AWS services & AWS partner tools:
 - Config
 - GuardDuty
 - Inspector
 - Macie
 - IAM Access Analyzer
 - AWS Systems Manager
 - AWS Firewall Manager
 - AWS Health
 - AWS Partner Network Solutions

1.

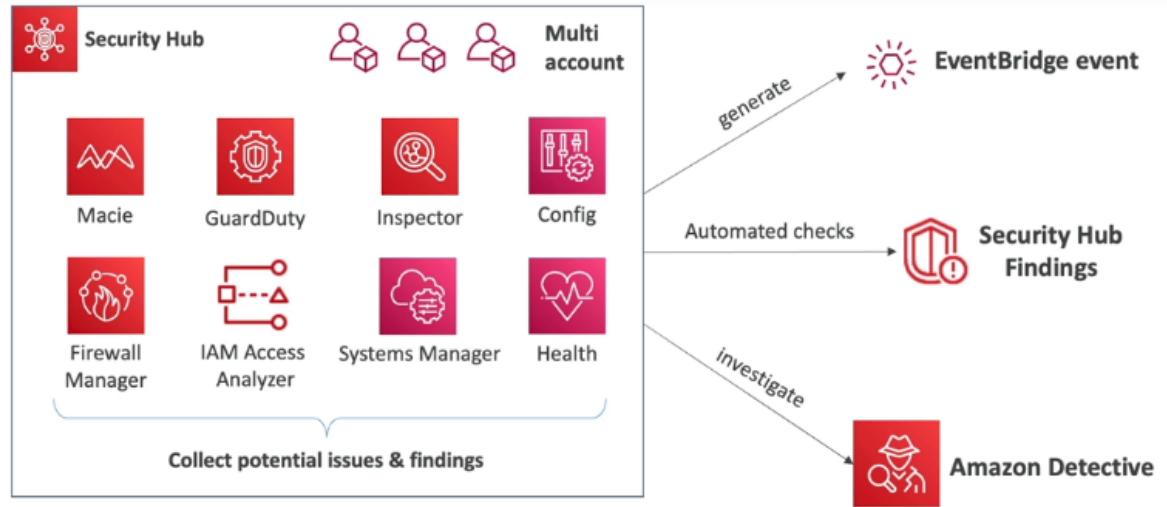
Sure. AWS Security Hub is a centralized security management and compliance service that helps you to monitor your AWS environment for security best practices, compliance with regulations, and operational issues. Security Hub provides a single view of your security posture across AWS accounts, regions, and services. It can be used to:

- **Identify security best practices and compliance controls:** Security Hub identifies security best practices and compliance controls that are applicable to your AWS environment. It can also identify gaps in your security posture and help you to prioritize remediation efforts.
- **Receive security alerts and notifications:** Security Hub receives security alerts and notifications from AWS services, such as Amazon GuardDuty and Amazon Inspector. It can also receive security alerts from third-party security services.
- **Investigate security events:** Security Hub helps you to investigate security events by providing you with a centralized view of the events, including the affected resources, the severity of the events, and the recommended remediation steps.

2.

- Must first enable the AWS Config Service
- 3.
4. And so for Security Hub to work, first of all, you must enable the AWS Config service.

AWS Security Hub



5.

Amazon Detective

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
- 1.

AWS Abuse

1.

AWS Abuse



- Report suspected AWS resources used for abusive or illegal purposes
- Abusive & prohibited behaviors are:
 - Spam – receiving 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 overwhelm 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 privileges



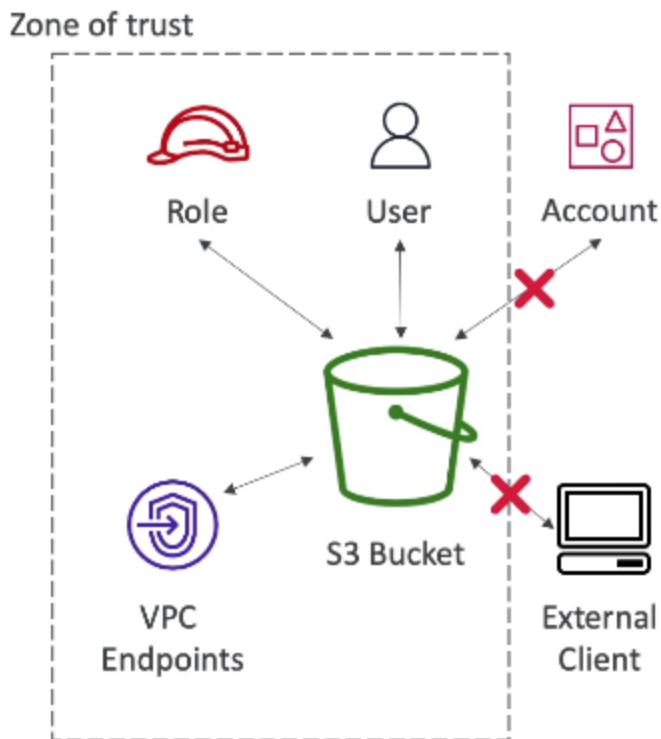
- Root user = Account Owner (created when the account is created)
- Has complete access to all AWS services and resources
- **Lock away your AWS account root user access keys!**
- Do not use the root account for everyday tasks, even administrative tasks
- Actions that can be performed only by the root user:
 - 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

1.

IAM Access Analyzer

IAM Access Analyzer

- Find out which resources are shared externally
 - S3 Buckets
 - IAM Roles
 - KMS Keys
 - Lambda Functions and Layers
 - SQS queues
 - Secrets Manager Secrets
- Define Zone of Trust = AWS Account or AWS Organization
- Access outside zone of trusts => findings
 - 1.
 2. and then anything outside your zone of trust that has access to the resources said above are going to be reported as findings.



- 3.
4. Here the account and an external client can access the s3 bucket...and if Account and external client will try to access it..then access analyzer will notify us

Summary

Section Summary: Security & Compliance

- 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
- 1. **Network Firewall:** Protect VPC against network attacks

Section Summary: Security & Compliance

- 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
- 2. **IAM Access Analyzer:** identify which resources are shared externally