Security & Compliance Section

• AWS Shared Responsibility Model

① AWS responsibility - Security of the cloud
- Protecting infrastructure (hardware, software, facilities, & networking) that runs all the AWS services.

② Customer responsibility - Security in the Cloud
- For EC2 instance, customer is responsible for management of the guest OS (including patches & updates), firewall & n/w configuration, IAM
- Encryption appl^n data

③ Shared controls:-
Patch Management, Configuration Management, Awareness & Training.

Example for RDS :-

AWS Responsibility :-

1. Manage the underlying EC2 instance, disable SSH access
2. Automated DB Patching
3. Automated OS Patching
4. Audit the underlying instance & disks & guarantee it functions

Your Responsibility :-

1. Check the ports / IP / Security group inbound rules in DB's SG.
2. In-databases user creation & permissions
3. Creating a database with or without public access.
4. Ensure parameter groups or DB is configured to only allow SSL connection
5. Database encryption setting.

Example, for S3 :-

① AWS Responsibility :-

① Guarantee you get unlimited storage
② Guarantee you get encryption
③ Ensure seperation of the data between different customers
④ Ensure AWS employees can't access your data

Your Responsibility :-

① Bucket Configuration
② Bucket Policy / Public Setting
③ IAM Users and roles
④ Enabling encryption

Example, for S3 :-

① AWS Responsibility :-

① Guarantee you get unlimited storage
② Guarantee you get encryption
③ Ensure seperation of the data between different customers
④ Ensure AWS employees can't access your data

Your Responsibility :-

① Bucket Configuration
② Bucket Policy / Public setting
③ IAM Users and roles
④ Enabling encryption

What is a DDOS* Attack?
(Distributed Denial-of-Service)

→ Attacker will have masters(⌛) which will create multiple bots requesting application server with APIcalls which to extend that server will be overwhelmed with requests & will not be able process.
Due to which normal users will not be able to access API's and it will not be responsive anymore

To protect this attack AWS came up with DDOS Protection on AWS.

DDOS Protection on AWS

① AWS Shield Standard: protects against DDOS attack for your website & applications, for all customers at no additional costs.

② AWS Shield Advanced: 24/7 premium DDOS protection

③ AWS WAF :- Filter specific requests based on rules.
(WAF : Web Appl^n Firewall)

④ Cloudfront & 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.

* AWS Shield

① AWS Shield Standard:

① Free service that is activated for every AWS customer

② Provides protection from attack such as SYN / UDP floods, Reflection attacks & other layer 3/layer 4 attacks

② AWS shield advanced:

① Optional DDoS mitigation service ($3,000 per month per organization)

② Protect against more sophisticated attack on Amazon EC2, Elastic Load balancing (ELB), Amazon Cloudfront, AWS Global Accelerator, & Route 53

③ 24/7 access to AWS DDoS response team (DRP)

④ Protect against higher fees during usage spikes due to DDoS.

AWS WAF - Web Application Firewall

① Protects your web applications from common web exploits (Layer 7)

② Layer 7 is HTTP (vs Layer 4 is TCP)

③ Deploy on application load Balancer, API Gateway, Cloudfront

* Define Web ACL (Web Access Control List):

① Rules can include IP addresses, HTTP headers, HTTP body, or URI strings

② Protects from common attack - SQL injection & Cross-site scripting (XSS)

③ Size contraints, geo-match (block countries)

④ Rate-based rules (to count occurences of events) - for DDOS protection

AWS Network Firewall

① Protect your entire Amazon VPC
② From Layer 3 to Layer 7 protection
③ Any direction, you can inspect
- VPC to VPC traffic
- Outbound to internet
- Inbound from internet
- To / from Direct connect & Site-to-site VPN

AWS Firewall Manager

* Manage security rules in all accounts of an AWS organization

* Security Policy: Common set of security rul.
  - VPC security groups for EC2, Application load balancer, etc...
  - WAF rules
  - AWS Shield Advanced
  - AWS Network firewall

* Rules are applied to new resources as they are created (good for compliance) across all & future accounts in your Organization.

Penetration Testing on AWS Cloud

AWS Customers are welcome to carry out security assessment or penetration tests against their AWS infrastructure without prior approval for 8 services:

1. Amazon EC2 instances, NAT gateways, & Elastic load balanced
2. Amazon RDS
3. Amazon Cloud Front
4. Amazon Aurora
5. Amazon API Gateways
6. Amazon Lambda & Lambda Edge fun^ns
7. Amazon Lightsail resources
8. Amazon Elastic Beanstalk environments

Prohibited Actives for Penetration Testing

① DNS zone walking via Amazon Route 53 Hosted zone
② Denial of service (DOS), distributed Denial of service (DDOS), simulated DOS & simulated DDOS
③ Port flooding
④ Protocol flooding
⑤ Request flooding (login req. flooding, API req. flooding)

Encryption with KMS & Cloud HSM

#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 Archieve, etc.

- In Transit (in motion): data being moved from one location to another.
  - means data tranferred on the nw.

- 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 :-
  1. EBS Volumes: encrypt volumes
  2. S3 buckets: Server-side encryption of objects
  3. Redshift database: encryption of data
  4. RDS database: encryption of data
  5. EFS drives: encryption of data.

* Encryption Automatically Enabled:
  1. Cloudtrail logs
  2. S3 Glacier
  3. storage gateway

Cloud HSM

① KMS ⇒ AWS manages software for encryption

② Cloud HSM ⇒ AWS provisions encryption Hardware

③ Dedicated Hardware (HSM = Hardware Security Module)

④ You manage your own encryption keys entirely (not AWS)

⑤ HSM device is tamper resistant, FIPS 140-2 level-3 compliance

Types of KMS keys

① Customer Managed key:

+ Create, manage & 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

② AWS Managed key:

+ Created, managed & used on customer's behalf by AWS
+ Used by AWS services (aws/s3, aws/ebs, aws/redshift)

③ AWS Owned key:

+ Collection of CMKs that an AWS service owns & manages to use in multiple accounts.
+ AWS can use those to protect resources in your account (but you can't view the keys)

(4) Cloud HSM keys (Custom keystore) :-

+ keys generated from own cloudHSM Hardware device
+ Cryptographic operations are performed within the cloudHSM cluster.

AWS Certificate Manager (ACM)

→ Let's you easily provision, manage & deploy SSL/TLS certificates.

→ ~~Used to provide in-flight & private TLS certificates.~~

→ Used to provide in-flight encryption for websites (HTTPS)

→ Supports both public & 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

AWS Secrets Manager

① Newer service, meant for storing secrets.

② Capability to force rotation of secrets every x days

③ Automate generation of secrets on rotation (uses Lambda)

④ Integration with Amazon RDS (MYSQL, Postgresql, Aurora)

⑤ Secrets are encrypted using KMS.

AWS Artifact (not really a service)

Portal that provides customers with on-demand access to AWS compliance documentation & AWS agreements

* **Artifact Reports:** Allows you to download AWS security & compliance documents from third-party auditors, like AWS ISO certifications, Payment Card Industry (PCI) & system & Organization Control (SOC) reports.

* **Artifact Agreements:** Allows you to review accept, & track the status of AWS agreements such as the business Associate Addendum (BAA) or the Health insurance Portability & Accountabili Act (HIPAA) for an individual account or in your organizations.

* Can be used to support internal audit or compliance

Amazon GuardDuty

→ Intelligent Threat discovery to protect your AWS Account

→ Uses machine learning algorithms, anamoly detection, 3rd party data

→ One click to enable (30 days trial), no need to install software

→ Input data includes:

① Cloud Trail Event logs - unusual API calls, unauthorized deployments

- CloudTrail Management events :- Create VPC, subnet, Create trail...
- CloudTrail S3 Data Events - get objects list objects, delete object.....

② VPC Flow logs :- unusal internal traffic, unusal IP address

③ DNS Logs :- Compramised EC2 instances sending encoded data within DNS queries

④ Optional features - EKS audit logs, RDS & Aurora, EBS, Lambda, S3 data events ...

Amazon GuardDuty

- 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).

VPC Flow logs

Cloudtrail Logs

DNS Logs (AWS DNS)

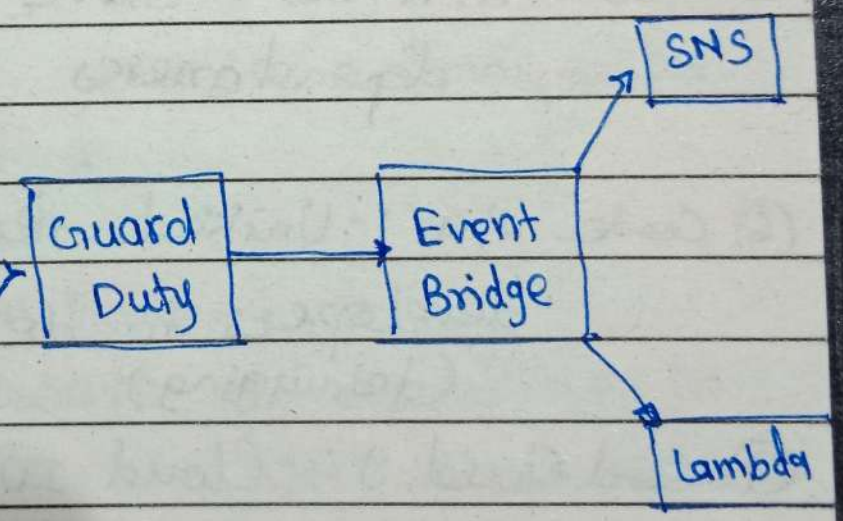
Optional features:

S3 logs, EBS Vol.

Lambda N/W Activity,

RDS & Aurora login Activity,

EKS Audit logs



Amazon Inspector

+ Automated Security Assessment

+ For EC2 instances -

① Leveraging the AWS System Managen (SSM) agent.

② Analyze against unintended network accessibilities.

③ Analyze the running OS against known vulnerabilities.

+ For Container Images push to Amazon ECR -

① Assessment of container Images as they are pushed

+ For Lambda functions -

① Identifies software vulnerabilities in function code & package dependencies.

② 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, Contain 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.

Aud

AWS Config

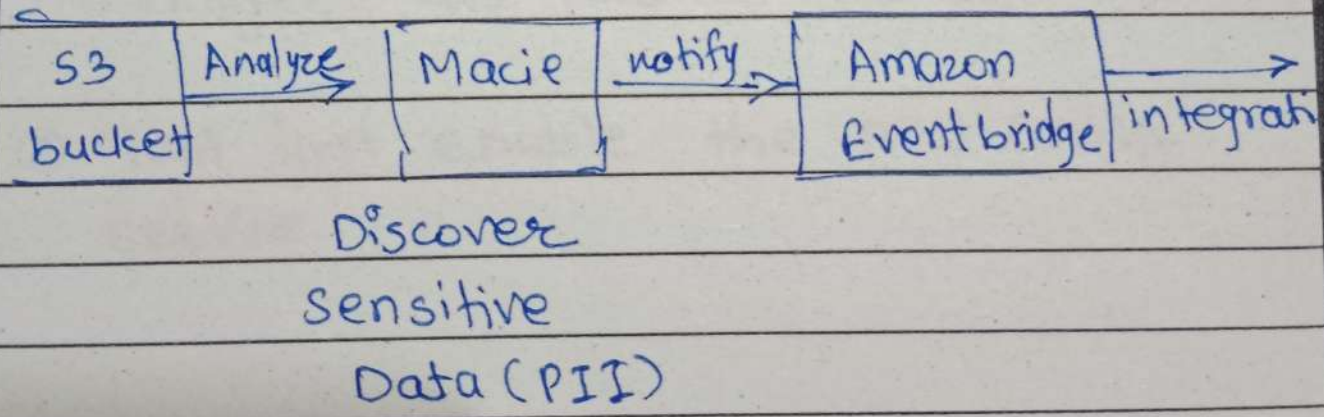
* Helps with auditing & recording compliance of your AWS resources
* Helps record configurations & changes over time.
* Possibility of storing the configuration data into S3 (analyzed by Athena)
* Questions that can be solved by AWS Config:-
  1. Is there unrestricted SSH access to my security groups?
  2. Do my buckets have any public access?
  3. 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 & accounts.

Pallavi Wattamwar

Amazon Macie :-

* Amazon Macie is a fully managed data security & data privacy service that uses machine learning & pattern matching to discover & protect your sensitive data in AWS.

* Macie helps identify & Alert you to sensitive data, such as personally identifiable information (PII)



AWS Security Hub

① Central security tool to manage security across several AWS accounts & automate security checks

② Integrated dashboards showing current security & compliance status to quickly take actions.

③ Automatically aggregates alerts in predefined or personal findings formats from various AWS services & AWS partner tools: Config, Guardduty, Inspector, Macie, IAM Access Analyzer, AWS Health, AWS systems Manager, AWS Firewall ~~Analy~~ Manager, AWS Partner N/w solutions

③ Must first enable the AWS Config service.

Amazon Detective

① GuardDuty, Macie & Security Hub are used to identify potential security issues or findings.

② Sometimes security findings require deeper analysis to isolate the root cause & take action - it's complex process

③ Amazon detective analyzes, investigates, & quickly identifies the root cause of security issues or suspicious activities (using ML & graphs)

④ Automatically collects & processes events from VPC Flow logs, Cloud trail, GuardDuty & create a unified view.

⑤ Produces visualizations with details & context to get to the root cause.

AWS Abuse

① Report suspected AWS resources used for abusive or illegal purposes.

② Abuse & Prohibited behaviours are:

① Spam - receiving undesired emails from AWS-owned IP address, websites & forums spammed by AWS resources.

② Port Scanning - sending packets to your ports to discover the unsecured ones

③ DoS or DDoS attacks - AWS owned IP addresses attempting to overwhlem or crash your servers / software

④ Intrusion attempts - logging in on your resources.

⑤ Hosting objectionable or copyrighted content - distributing illegal or copyrighted content without consent.

⑥ Distributing malware - AWS resources distributing softwares to harsh computers ~~to~~ or machines.

* Contact abuse team :- AWS abuse form or abuse@amazonaws.com

Root User Privileges

* Root User = Account owner (created when the account is created)

② Has complete access all AWS services & resources

③ Lock away your AWS account root user access keys!

④ Do not use the root account for everyday tasks, even administrative tasks.

⑤ Actions that can be performed only by root user:-

① Change account settings (account name, email address, root user pass, root user access keys)

② View certain invoices

③ Close your AWS account

④ Restore IAM user permissions

⑤ Change or cancel your AWS Support plan

⑥ Register as a seller in the reserved instance marketplace

⑦ Edit or delete an Amazon S3 bucket policy that includes an invalid VPC ID or VPC endpoint ID.

⑧ Configure Amazon S3 bucket to enable MFA.

⑨ Sign up for GorCloud.

IAM Access Analyzer

① Findout which resources are shared eseternally

- S3 buckets
- IAM Roles
- IAM Roles
- KMS keys
- Lambda functions & layers
- SQS quesies
- Secrets Manager secrets

② Define Zone of trust ⇒ AWS Account or AWS organization

③ Access outside zone of Trusts ⇒ findings

IAM access Analyzer is free to enable

Section Summary : Security & Complice

① Shared Responsibility on AWS

② Shield : Automatic DDOS Protection + 24/7 support for advanced

③ WAF : Firewall to filter incoming requests based on rules.

④ KMS : Encryption key managed by AWS.

⑤ CloudHSM : Hardware encryption, we manage encryption keys

⑥ AWS Certificate Manager : Provision, manage & deploy SSL/TLS certificates

⑦ Artifacts : Get access to compliance reports such as PCI, ISO, etc.

⑧ GuardDuty : find malicious behaviour of VPC, DNS & Cloudtrail Logs (Threat detection service)

⑨ Inspector : find software vulnerabilities in EC2, ECR Images, & Lambda funⁿs

(10) Network Firewall: Protect VPC against network attacks

(11) Config: Tracks config changes & compliance against rules

(12) Macie: Find sensitive data (ex: PII data) in Amazon S3 buckets

(13) CloudTrail: Track API calls made by users within account

(14) AWS Security Hub: gather security findings from multiple AWS accounts

(15) Amazon Detective: find the root cause of security issues or suspicious activities

(16) Amazon Abuse: Report AWS resources used for abusive or illegal purposes.

(17) IAM Access Analyzer: Identify which resources are shared externally.

(18) Root User Privileges:

1. Change account settings
2. Close your AWS account
3. Change or cancel you AWS support plan
4. Register as a setter in Reserved Instance Marketplace

(19) Firewall Manager: manage security rules accross an organization (WAF, Shield.....)