Security 101

Security Basics

CIA
AAA
Non-repudiation } The Triad

#CIA

Confidentiality, Integrity, Availability

MFA, IAM
Bucket policies

ACM

Autoscaling
multi-AZ

AAA

Authentication, Authorization, Accounting

Cloudtrail

Non-repudiation

cant deny you did something

Security of AWS

Physical & Environmental Security

- Fire Detection & Suppression
- Power
- Climate & Temperature
- Management
- Storage Device Decommissioning

Business Continuity Management

- Availibility
- Incident Response
- Company-Wide Executive Review
- Communication

Network Security

- Secure Network Architecture
- Secure Access Points
- Transmission Protection
- Amazon Corporate Segregation
- Fault-Tolerant Design
- Network Monitoring & Protection

AWS Access

- Account Review & Audit
- Background Checks
- Credentials Policy

Secure Design Principles

Change Management

- Software
- Infrastructure

Shared Responsibility Model

AWS responsibility

security OF / IN the cloud

your responsibility

AWS Responsibilities

- global infrastructure
- hardware, software, networking & facilities
- "managed services"

Customer Responsibilities

- IaaS
- updates & security patches
- Configuration of AWS firewall

The model changes for:

- Infrastructure
  → Compute services
    [EC2, EBS, Auto Scaling, VPC]
- Container
  → RDS, EMR & Elastic Beanstalk
- Abstracted
  → S3, Glacier, DynamoDB, SQS, SES

Security in AWS

Cloud Controls

- Visibility
  What assets you have?
  AWS Config
- Auditability
  AWS CloudTrail
- Controllability
  AWS KMS, AWS Cloud HSM
  {multitenant} {DEDICATED, FIPS 140-2}
- Agility
  CloudFormation, Elastic Beanstalk
- Automation
  OpsWorks, CodeDeploy

IAM, CloudWatch, Trusted Advisor

Identity Access Management, S3 & Security Policies

IAM Recap

"manage users & level of access"

- Centralised control
- Shared access
- Granular Permissions
- Identity Federation
- MFA
- Temporary access
- Rotation Policy
- PCI DSS compliance
- Other service integrations

Terms:

- Users
- Groups
- Roles

} Principal Entities

- Policies

IAM Root Users

"secure root users"

IAM Policies Overview

- what you're allowed to do with any AWS resource, IAM is global

3 types

→ AWS Managed
→ Customer managed
→ inline policies

S3 Bucket Policies

"attached only to S3 buckets"

READ, PUT, DELETE

cross account access enabling

S3 ACL's

legacy access control mechanisms
object level permissions

Conflicting Policies - Exam Essential

IAM Policy conflicts S3 policy conflicts S3 ACL

least-privilege ALWAYS default to DENY

DENY | ALLOW | DENY

Forcing Encryption Using S3

- Using bucket policy

  aws: SecureTransport

Cross Region Replication and S3

- replicates objects from one region to another
- default done using SSL

- one-to-one relationship
- must have versioning enabled
- object owner must grant READ & READ_ACP permission
- works across accounts

What is replicated?

- all new objects [even SSE-S3 & SSE-KMS]
- Object metadata
- delete markers

Forcing S3 to use CloudFront

"force users to use CloudFront instead of S3 bucket url"

Origin Access Identity

Custom SSL Certificates with CloudFront

custom SSL certificate → to use your own domain

ACM, cert must be in us-east-1 region

S3 Pre-signed URLs

aws s3 presign s3://bucket-name/object
--expires-in seconds

Security Token Service with Active Directory

Users can come from:

- Federation (usually AD)
  - → SAML
  - → SSO
  - → temp access
- Mobile Apps Federation
  - → OpenID

- Cross Account Access

Key terms
- Federation
- Identity Broker
- Identity Store
- Identities

Web Identity Federation

to federate users from Facebook, Google, etc

Amazon Cognito
→ seamless app web identity federation
→ Identity Broker

Cognito

User Pools
Identity Pools

Glacier Vault Lock

extremely low cost archival storage service

Vault lock Policy

→ Similar to IAM Policy

→ Configure WORM (write once read many) arch
Create data retention policy

After 24 hrs Vault lock policies are immutable

AWS Organisations & Service Control Policies

AWS Organisation → acc. management service

OUs → have accounts

Permissions Boundary using SCP

IAM Credential Report

lists all users & status of credentials

```
aws iam generate-credential-report
aws iam get-credential-report
```

Logging and Monitoring

CloudTrail - Turning It On

"logs API calls"

- incident investigation
- intrusion provision
- Industry & regulatory compliance

CloudTrail - Protecting Your Logs

- logs can have sensitive information.

CloudWatch 101

"monitoring service"

→ CW,
→ CW Logs
→ CW Events

Log aggregation, resource utilizations, op perform monitoring

Hooks to event triggers

AWS Config 101

"assess, audit & evaluate"

records & normalizes the changes
Config APIs can be used for accessing

- Compliance auditing
- Security analysis
- Resource tracking

AWS Managed Rules
Customer Managed Rules

Set Up An Alert If The Root User Logs In

"proactive alerting for root user"

go to CloudTrail & configure CW Logs
then,
create Metric Filter & assign metric
then,
Create an alarm

Cloud HSM

"helps you meet regulatory requirements using dedicated HSM"

Inspector & Trusted Advisor

- Amazon Inspector is an automated assessment service
- Trusted Advisor advises on optimization metrics
  - Cost Optimization, Security, Performance Fault Tolerance

Logging With AWS

- AWS CloudTrail
- AWS Config
- VPC Flow Logs
- AWS CloudWatch Logs

Infrastructure Security

KMS

"AWS Key Management Service
- managed service
- create & control enc keys
- uses HSM to protect keys"

- KMS is region based

Key Rotation Options

- Rotate keys regularly
- Method depends on type of keys

AWS managed
- auto rotates every 3 yrs

CMK
- auto once a yr → disabled default
- On-demand manual rotation

Using KMS with EBS

- KMS → create key → symmetric key (cust. managed)
- create snapshot of root volume & copy it to encrypt a root device volume
- Can't copy keys from region to region but volumes can be. (using snapshots)

EC2 & Key Pairs

view public key under ~/.ssh/authorized_keys
EC2 can have multiple public keys
curl http://192.254.192.254/latest/meta-data/public-keys/0/openssh-key/

AWS Marketplace - Security Products

- Can purchase security products from 3rd party vendors

AWS WAF & AWS Shield

- Shield → $3000 for enterprise support
  WAF - monitor HTTP & HTTPs requests
  Shield → DDoS protection at layer 7

WAF three behaviors - Allow all, block all, count reqs (monitor)

Dedicated Instances vs Dedicated Hosts

Dedicated Instances	Dedicated Hosts
EC2 run in a VPC on hardware dedicated to you	same as ded. instances but additional visibility & control
On-demand, Reserved or Spot	charged by host
charged by instance	

AWS Hypervisors

hypervisor → creates & runs virtual machines
Choose HVM over PV where possible

KMS Grants

grants are alternate access control mechanisms
- → only allow, not deny
- → temporary access given programmatically
- → create-grant, list-grants, revoke-grant
- → grant token is created & can be passed using API

KMS Via Service

Policy conditions used to specify conditions within key or IAM policy

predefined Condition Keys

kms:ViaService ← condition key which can allow or denys access to CMK based on originating service.

Cross Account Access To KMS CMKs

- Access is controlled using:
  - The Key Policy → add root user
  - IAM Policies

Introduction To Microservices

traditionally monolithic

microservice → software with small independent services communicating over APIs

Serviceability, Flexibility, Scalability

Run in containers
Does one thing Only
Easy to support & maintain

Introduction to Containers

"virtual operating environment"

ECS, EKS | Fargate (serverless) preferred option

Container Security

Best Practices:

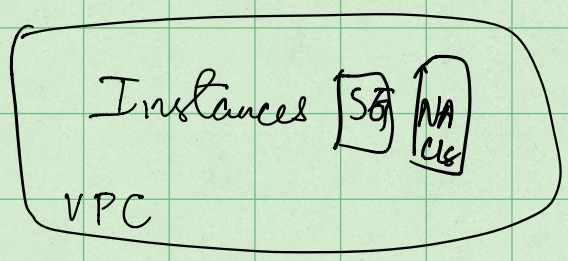
- Don't store secrets & passwords
- One Service per container
- Trusted Images Only

Image Scanning, Protect Infrastructure

Use IAM rules, Secrets Manager, ACM
Avoid unnecessary libraries
Avoid public internet, use ECS Service Endpoints
Use TLS (use ACM to store certs)

Data Protection With VPCs

VPC Introduction



Default VPC immediate deployment of EC2
NO TRANSITIVE PEERING

NAT Instances & NAT Gateways

NAT Instance
Disable Source/Destin Checks
Bottlenecking increase size
Behind a SG

NGW
Preferred
Scale automatically upto 10 Gbps
No need to patch

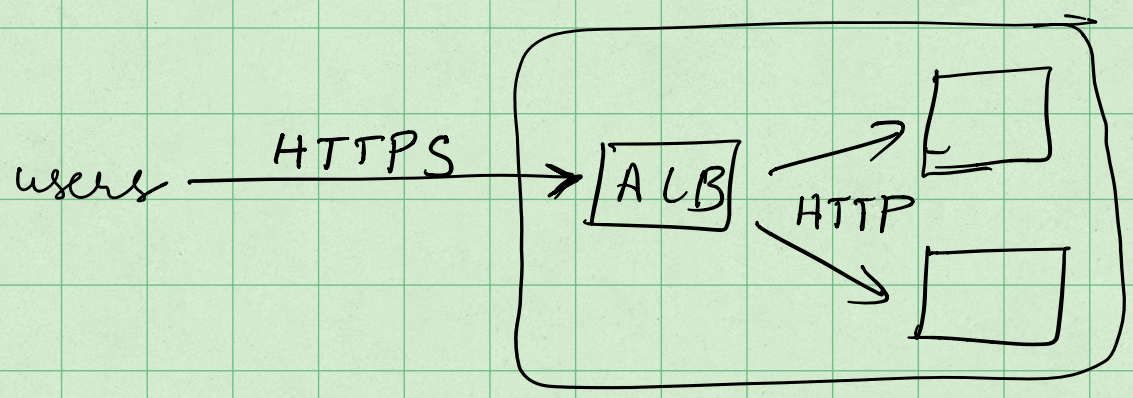
NACLs vs Security Groups

NACL rules are evaluated numerical order
↳ used to block specific IP addresses
VPC comes with default NACL
stateless
Ephemeral ports on outbound rules only

ALBs

Thru types of LBs:
- ALB
- NLB
- Classic

Elastic Load Balancer TLS/SSL Termination



ALB only supports TLS/SSL termination on the load Balancer

Classic & NLB for termination on EC2

VPC Flow Logs

capture IP traffic to & from ENIs

created at three levels:

- → VPC
- → Subnet
- → Network Interface Levels

NATs vs Bastion

Harden bastion

NAT instance is always behind SG, but not NGW

Session Manager

- Enables secure remote login
- alternative to SSH & RDP
- browser based
- Single Solution
- No keys, no bastion host needed.

VPC Endpoints

Two varieties
→ Interface
→ Gateway

Cloud HSM - Introduction

single tenancy
symmetric & assymmetric
FIPS 140-2 & EAL-4

4 types of users:
- PRECO admin: password

- CO User management
- CU key management
- AU cloning & syncing

Anyone can zeroize your cluster even unauthenticated user

Amazon DNS

10.0.0.0 → network address
10.0.0.1 → VPC router
10.0.0.2 → DNS server
10.0.0.3 } Reserved
10.0.0.255 }

Transit Gateway

communicate between multiple VPCs
Highly Scalable
Hub & Spoke
Secure
Centralized connectivity

Incident Response & AWS irl

DDOS Overview

attack that makes your website unavailable to end users

→ Amplification / Reflection Attacks
→ Slowloris Attacks

- Minimize surface area
  → Use bastion / jump box
- Scale to absorb attacks
- Safeguard Exposed Resources
  → Georestriction
  → Origin Access Identity
  → Alias Record Sets
  → Private DNS
- Learn Normal Behaviour
- Create a plan for attacks

WAF Integration

"integrate with ALB & CloudFront"

EC2 Has Been Hacked!

Stop → snapshot → isolated deploy → setup

Read through logs ← Access using forensic workstation ← VPC flow logs

Keys Leaked On Github

make Inactive → then delete it

Reading CloudTrail Logs

It's all json

AWS Certificate Manager

Route 53 → register a domain
ACM makes it easy to manage certificates
Automatically renews

Perfect Forward Secrecy & ALBs

compromise of long term keys won't allow decryption of previous data

API Gateway Throttling

steady state → 10,000 in one second
burst limit → 5000 / second

account-level limits can be increased upon requests

API caching, default TTL is 300 secs

AWS Systems Manager Parameter Store

store & reference data

AWS Systems Manager Run Command

setup & run

Compliance in AWS

PCI-DSS, HIPAA

↑

12 different requirements

Updates

Introduction to Athena

Interactive query service
SQL, Serverless, data stored in S3
Analyse log data

Macie

protect sensitive data in S3
PII protection
Security service which uses ML & NLP

GuardDuty

threat detection service, uses ML to continuous monitor AWS infrastructure

7 - 14 days → create a baseline

30 days free

Secrets Manager

securely store, encrypts & rotates credentials

RDS credentials

Simple Email Service

cloud based email service which supports both sending & recieving emails

Port 25, but to avoid port throttling, port 587 or 2587

Security Hub

Central Hub for Alerts
Automated Checks
Ongoing security audit

integrates with most AWS security services

Network Packet Inspection

inspect network packets headers
&
data content

VPC Flow Logs ✗ doesn't provide packet inspection
AWS WAF

Use 3rd party software from AWS marketplace

Active Directory Federation with AWS

AWS allows federated sign-in
provide SSO for users

ADFS
SAML

AWS Artifact

demonstrate compliance to auditors