AWS Security
https://squasta.github.io
Updated : 13 nov 2026

How to manage an AWS Compromised account
- Change passwords for AWS root account and/or IAM users
- Delete or rotate AWS access keys
- Review/confirm recent user activities
- AWSCompromisedKeyQuarantineV2
  - an AWS-managed policy automatically attached by AWS to IAM user, group, or role when its credentials are suspected of being compromised or exposed publicly
  - It does not delete or revoke the access key itself

How to Handle an AWS Abuse Report
- Check the abuse notice for the specific logs, target IP addresses, timestamps, and reporter details
- Review the Notice
- Secure Your Resources
- Isolate and remediate the compromised resources
- Reply to AWS (trustandsafety@support.aws.com)
- **Within 24 hours** explaining the preventive and corrective actions you implemented
- Monitor via AWS Health

AWS Fault Injection Simulator (FIS)
- Chaos Engineering as a service
- To inject fault experiments
- Available in AWS Resilience Hub

AWS Security Hub & Security Hub CSPM
- **Central Security Command center in AWS**
  - Provides a comprehensive view of the security state and compliance status of AWS resources
    - Cross Region
    - AWS Organization integration
  - Consolidate
    - Across accounts & workloads
    - Security alerts
    - Compliance checks
  - Findings are deleted after 90 days
  - Findings are set in AWS Security Finding Format (ASFF)
- **Must be first enabled**
- Analyze findings from
  - AWS Config
  - AWS GuardDuty
  - AWS Inspector
  - AWS Macie
  - AWS Firewall Manager
  - IAM Access Analyzer
  - Third-party security tools
- Controls for AWS Services
  - AWS Certificate Manager
  - Findings are stored for at least 90 days
- Conducts Security standards checks
  - AWS Foundational Security Best Practices
  - CIS AWS Foundations Benchmark
  - PCI DSS
  - Others...
- Insights
  - Built in Managed
  - Custom

Amazon Security Lake
- **Fully managed security data lake service**
- Centralizes security data from
  - AWS Services
    - AWS Logs sources
      - AWS CloudTrail
      - AWS VPC Logs
      - AWS WAF Logs
      - Amazon Route 53 Resolver query logs
      - AWS Security Hub findings
      - EKS audit logs
  - SaaS solutions
    - Possible from multiple AWS accounts
  - On-premises
  - 3rd parties sources
- Automatically normalises data to Open Cybersecurity Schema Framework (OCSF) format
- Store data in Amazon S3
  - With optimised Parquet format
  - Lifecycle management
    - Security Lake doesn't support S3 Object Lock
    - Default storage class is **S3 Standard**
    - If needed specify retention settings at the Region level
      - Ex: moving data to S3 Standard-IA
- Analytics
  - Enables querying with Amazon Athena
  - Search and visualization with Amazon OpenSearch
  - Dashboards with Amazon Quick (ex QuickSight)
  - 3rd party SIEM tools
    - Splunk, Datadog, IBM Radar...

Amazon Detective
- To identify the root cause of security findings
- Streamlines investigation of suspicious activities & potential threats
- **Security Analysis Service**
- Aggregate & process data from multiple sources
  - VPC Flow logs
  - CloudTrail logs
  - GuardDuty findings
- Unified behavioral graph that maps relationship between AWS resources
- IAM Investigation

AWS Inspector
- Create findings
- Automated continuous Vulnerability Assessment
- Identity deviation from security best practices
- Detect unintended network exposure
- Discovers and scans
  - EC2 instances
    - Leverage AWS SSM agent
    - Type of scanning
      - Basic
        - Basic scanning is included in AWS ECR
          - Scan
            - OS
          - Scan Frequencies
            - Manual
            - On Push
      - **Enhanced Scanning**
        - Provided by **AWS Inspector**
          - Scan
            - OS
            - Programming languages package vulnerabilities
          - Scan Frequencies
            - On Push
            - Continuous
  - Machine images
  - Container images in ECR
  - Lambda functions (standard + code)
    - Code security
      - Inclusion rules to control which resources are targetted and scanned

AWS GuardDuty
- **Intelligent agentless threat detection service**
- Regional service
- But supports Centralised management of multi-account and multi-region through AWS Organization & a delegated administrator AWS account
- Use threat intelligence
  - Intelligence feeds
    - AWS Threat Intelligence
    - Leading 3rd party
      - Crowdstrike
      - Proofpoint
    - Custom
      - S3 URL configured as a ThreatIntelSet
- Continuously monitor Logs
  - **VPC Flow Logs**
  - **DNS Query logs**
    - Route 53 resolver DNS query logs
    - Cannot access & process Custom DNS Resolver
  - **AWS CloudTrail logs (management / data events)**
  - EKS Audit Logs
  - RDS login activities
  - Lambda Network activity
  - Runtime monitoring
    - EC2 instances
    - ECS tasks
      - Including Fargate
    - EKS pods
- Protection Plans
  - S3 protection
  - EKS protection
  - Runtime monitoring
    - Incurs additional costs (EBS snapshots)
  - EBS Malware protection
  - RDS protection (RDS & Aurora)
  - Lambda protection
  - AI Protection
  - Malware protection for AWS backup
- Generates Findings
  - Severity
    - 1.0 = Low
    - 10.0 Critical
    - A potential security issue discovered by GuardDuty
  - Type of findings
    - Backdoor, Cryptocurrency, PenTest, Persistence, Trojan, Unauthorized access...
    - Compromised Instances
    - Anomalous network traffic
    - Compromised AWS account
- Alert destinations
  - AWS User notifications
  - Amazon SNS
    - AWS Lambda
    - AWS Security Hub
    - Amazon S3
    - AWS Step Functions
  - Tired-party SIEM solutions
    - Splunk, Datadog...
- Suppression Rules
  - Criteria to automatically filter and archive new finding
- Trusted entity or IP Lists
  - Treat Lists
    - Entity lists IP
    - IP address lists
      - To avoid triggering findings that are false positives
      - Only one trusted entity list and one trusted IP address list per AWS account per Region
  - Stored in Amazon S3
    - **Trusted IP list takes priority and overrides the Threat List**
  - Format
    - Plaintext
    - Structured Threat Information Expression (STIX)
    - Open Threat Exchange (OTX) CSV
    - FireEye iSIGHT Threat Intelligence CSV
    - Proofpoint ET Intelligence Feed CSV
    - AlienVault Reputation Feed

AWS Macie
- A fully managed **data security & data privacy service**
- Multi account strategy
- Focuses primarily on identifying and safeguarding
  - Within Amazon S3
    - Personally Identifiable Information (PII)
    - Protected Health Information (PHI)
    - Financial data
    - Intellectual Property
- Data Identifiers
  - Managed Data Indentifiers
  - Custom Data Identifiers
- Allow Lists
  - To define text pattern to ignore
- Findings
  - Report of potential issue or sensitive data found
- Suppression Rules
  - For automatic archiving based on filter criteria
- Policy findings
- Data findings
- 2 types

Data backup & replication
- To protect against accidental deletion, corruption or ransomware
- **Fully Managed backup service**
- Support cross-region & cross-account backup copies
- Supported services
  - Compute (EC2+EBS, EKS)
  - Storage (EBS, EFS, FSx)
  - Database (RDS, Aurora, DynamoDB, Neptune, DocumentDB)
  - Hybrid (Storage Gateway Volumes, VMware)
- Backup Plans
- Backup Vault
  - Logical container for organizing & securing backups
  - Vault lock for immutable backups
  - Point in Time Recovery (PITR)
  - Continuous backup for RDS, Aurora & DynamoDB
  - Cold storage after X days (min 60 days)
  - Lifecycle management / Tiering
  - Encryption by default (at rest & in transit)
  - WORM (Write One Read Many)
    - Governance mode
    - Compliance mode
      - True immutability
      - Nobody can delete (including root)
      - Can not be disabled
- **AWS Backup**
- Integration with AWS Config
- AWS Backup Audit Manager
- Integration with AWS Organisation
- Centrally manage backup policies across all accounts
- Backup policies deployed via Service Control Policies (SCP)
- Cross-account Snapshot copies for Ransomware Protection
- Support snapshot encryption
- Cross-account snapshot copies
- **Amazon Data Lifecycle Manager (DLM)**
- Automate creation/retention/deletion of EBS Snapshots & EBS-backed AMIs
- Uses resources tag to identify the resources
- Fast Snapshot Restore (FSR)
  - Keeps snapshots ready for instant volume creation in selected Availability Zones
  - Critical for RTO in Disaster Recovery
  - Higher cost
  - Snapshots are stored in Amazon S3 (behind the scenes)

Core network security components
- **Route 53**
  - DNSSEC Signing
    - Works only on Public Hosted Zones
    - DNS Security Extensions (DNSSEC)
  - Public DNS query logging
    - Logs are sent to CloudWatch Logs only
    - Public DNS queries to Public Hosted Zones
  - Amazon Route 53 Resolver Query Logs
    - Help security team
    - Provide visibility into DNS Queries
    - Logs destinations
      - AWS CloudWatch Logs
      - Amazon S3
      - Amazon Data Firehose
    - Does not capture DNS-over-HTTPS (DoH) or DNS-over-SSL traffic
  - Route 53 Resolver DNS Firewall
    - To filter & regulate outbound DNS traffic for a VPC
    - To inspect and block DNS Tunneling
- **AWS CloudFront**
  - Using Lambda@Edge
    - Adding Security headers on the flying
  - To Secure Amazon S3 access (Restrict View Access)
    - To restrict access to **individual** file originating from an S3 Bucket
      - Signed URLs
    - To restrict access to **multiple** files originating from an S3 Bucket
      - Signed Cookies
  - Origin Access Control (OAC)
    - Used to restrict access only from CloudFront
  - Restrict the geographic distribution (geo blocking) of content
    - Allowlist
    - Denylist
- Integrates with
- **AWS Firewall Manager**
  - **Centrally manage & enforce security policies across and resources**
  - Integrate with
    - AWS Network Firewall
    - AWS WAF
    - AWS Shield
    - Security Groups
    - AWS Route 53 Resolver DNS Firewall
- **AWS WAF**
  - **Help to protect Web Applications from attacks**
  - Inspect L7 traffic
  - Is attached to
    - Application Load Balancer, Cloud Front, API Gateway...
  - WAF Web ACL (Protection Pack)
    - Contains 1 or many
  - WAF Rules
    - Has a unique numerical **priority**
    - Rules are evaluated in ascending numerical order (lowest number first)
  - IP match conditions
    - To allow or block web requests based on the IP addresses that the requests originate from
  - Regular rules
  - Custom rules
    - Rate-based rules
  - WAF Managed Rules
    - Pre-configured rules
      - Automatically updated by AWS Marketplace security sellers
        - AWS
        - F5
        - Fortinet
        - GeoGuard
        - Imperva
        - Cyber Security Cloud Inc
    - To protect from common web threats
      - AWS WAF Fraud Control Account Takeover Prevention (ATP)
- **AWS Network Firewall**
  - Managed network firewall services for VPCs
  - Usage
    - Inspect VPC to VPC traffic or TransitGW traffic
    - Filtering outbound traffic
    - Securing DirectConnect / VPN traffic
    - Filtering Internet traffic
  - MultiAZ
    - One IP in a subnet in each AZ
  - 3 components
    - Firewall
      - /!\ Contains only one
    - IPS / IDS
    - TLS inspection
  - Firewall Policy
    - Deep Packet Inspection (DPI)
  - Is a collection of
    - Rule Groups
      - Collection of Stateless rules
      - Collection of Stateful rules
    - Rules
      - Support Suricate compatible IPS rule syntax
      - A rule is a 5 tuple network values & domain filtering
        - Source IP
        - Source Port
        - Destination IP
        - Destination port
        - Protocol
  - Needs to update VPC table route to go through AWS Network Firewall
- **AWS Shield**
  - **DDoS protection**
    - EC2 Instances
    - ELB
    - CloudFront
    - Route53
    - AWS Global Accelerator
    - Elastic IP
  - SKU
    - By default, free & always on
      - Standard
    - Enhanced
      - AWS Shield Response Team (SRT)
        - 24/7 access
        - Requires Business or Enterprise Support Plan
        - Granting access to the SRT
      - Cost protection opportunities
      - AWS WAF integration
        - Associated a Route 53 health check with the protected resource
        - 2 prerequisites
          - Proactive engagement
          - Authorise the Shield Response Team via an IAM Role to modify rules on your behalf
- **Security Groups**
  - Allow rules only
  - Stateful
    - Automatic application layer (L7) DDoS mitigation
    - Modifying SG rule **never** disrupts its tracked connections
    - Use NACLs to interrupt/block connection immediately
  - **At the instance level**
    - AWS-managed
    - Customer managed
      - Managed Prefix List
- **Network ACLs (NACLs)**
  - Network ACL rules are evaluated when traffic enters & leaves the subnet
  - allows or denies specific inbound or outbound traffic **at the subnet level**
    - Each rule has a number from 1 to 32766
    - Rules are evaluated in order, starting with the lowest numbered rule, when deciding whether allow or deny traffic
    - If the traffic matches a rule, the rule is applied and there is no evaluation of any additional rules
  - Stateless Rules
    - Need incoming & outgoing rules
      - Incoming traffic (request from client) on defined port(s)
      - Outcoming traffic (response) on ephemereral port
  - Default Network ACLs

Data Protection in Transit
- Transport Layer Security (TLS/HTTPS)
  - All public AWS service REST API endpoints enforce HTTPS over TLS
- Private Network Connectivity
  - VPC Gateway Endpoints
    - S3
    - DynamoDB
  - VPC Interface Endpoints (AWS Private Links)
    - Can be accessed from on premises (VPN or DirectConnect)
- Interconnexion with on-premises (or other Clouds)
  - Site to Site IPSec Tunnels
    - Can be used as a backup connection if DirectConnect fails
  - Direct Connect
    - By default data is not encrypted in transit
    - Encrypt data in transit
      - Using IPSec VPN Tunnel (OSI Layer 3)
      - Using MACsec encryption (OSI Layer 2)
        - Encryption modes
          - must_encrypt
          - should_encrypt
        - Keys
          - Connectivity Association Key Name (CKN)
          - Connectivity Association Key (CAK)
          - Secure association key (SAK) = MACsec key
            - not pre-shared, but automatically derived from the CKN/CAK pair
- Nitro System Encryption - VPC encryption in Transit
  - Modern Nitro-based EC2 instance types (ex M7g, C5n..)
  - Hardware-accelerated AES-256 encryption for network traffic between instances within the same Region and VPC/peered VP
    - Bypassed if TransitGW is used
  - Extends the native hardware-layer encryption beyond the modern Nitro instances to other AWS services
- Amazon EKS
  - To complete VPC encryption, service Meshes can be used to encrypt traffic with mutual TLS authentication
    - VPC Lattice
    - Istio
    - LinkerD
  - CNI like Cilium with Wireguard can be used for transparent node to node encryption

Basics
- AWS Shared responsibility
  - AWS manages security of the cloud
  - Customer are responsible for security in the cloud
- Deny statement in IAM policies do not affect the root account
- Separation of duties
- Principle of Least Privilege
- MFA
  - Virtual MFA device
    - Google Authenticator
    - Authy
  - Universal 2nd Factor (U2F) Security Key
    - Yubikey by Yubico
  - Hardware key fob
    - Ex: Gemalto, SurePassID
- Encryption
  - Server Side Encryption
  - Client Side Encryption
    - Data is encrypted locally before reaching AWS
- AWS Prescriptive guidance
- Penetration testing
  - Is allowed on customer AWS infrastructure
    - Without prior approval for a list of services
  - Some activities are prohibited
- DDoS testing
  - DDoS attacks must be performed by an approved DDoS test Partner

Global Security Standards Certification Industry Standards
- Customer can inherit many compliance controls directly from AWS
- SOC
- ISO
- PCI DSS
- FedRamp

IAM
- Cf. specific mindmap

AWS KMS
- Key Managed service
  - FIPS 140-3 security level 3 valid HSMs
- Key types
  - Symmetric keys (AES-256)
  - Asymmetric keys (RSA & ECC key pairs)
- **Create and control encryption keys**
  - For storage encryption
    - S3
    - EBS
    - RDS
    - DynamoDB
  - For variable encryption
    - AWS Lambda...
  - Encryption in applications
    - AWS Encryption SDK
  - For OS Encryption
    - Windows Bitlocker
    - Integration with AWS SSM
      - LUKS on Linux
- Key rotation
  - Automatic
    - 90 days to 7 years
    - Default : 365 days
  - Manual
- KMS Keys are regional
- Multi-Region Keys
  - Useful for multiple scenarios
    - Disaster Recovery
    - Global Data Management
    - Distributed signing applications
    - Active-active applications that span multiple Regions
  - Opt in to replication by creating a **Multi-Region key**
    - Key policy, grant, aliases, tags and CloudWatch alarms are independent between region
      - Arn is different (different regions)
      - Same KMS key
- KMS Alias
  - An alias is an independent AWS resource
  - To hide the change of key for the application
    - Alias ARN
      - arn:aws:kms:us-west-2:111122223333:alias/<alias-name>
    - Alias name
      - alias/<alias-name>
- Envelope Encryption
  - Practice of encrypting plaintext data with a data key, and then encrypting the data key under another key
  - Key hierarchy
    - **KMS Key** (**KEK**: Key Encryption Key)
      - Encrypt
      - Data Encryption Key (**DEK**)
        - Used to encrypt
        - Data local to AWS Services
  - KMS Encrypt API call has a limit of 4K
    - To encrypt more than 4K, use Envelope encryption
      - Use GenerateDataKey API
- Types of KMS Keys
  - AWS-owned keys
    - Internals key managed by AWS
  - AWS managed keys
    - For use across multiple accounts
    - Prefixed with aws/
    - Automatic key rotation every 1 year
  - Customer-managed keys
    - Created & Controlled by user
- KMS Key Policy
  - Default KMS Key Policy
    - Gives the AWS account that owns the KMS key, full access to KMS key (programmatically)
    - **BUT** the KMS Key policy does not automatically give permissions to account or any of its users
  - Custom Key Policy
    - Allow users to directly use the KMS key
      - Not necessary if KMS key is in the same account
    - Who can use and manage keys
      - Default KMS Key + IAM Policy
- KMS grant
  - Often used for temporary permissions
    - Grant on behalf of a user
  - For 1 KMS key
  - For 1 or more IAM Principal
  - Does not expire automatically
    - Delete it after usage
- Key material (Used to encrypt/decrypt data)
  - AWS-generated key material (AWS_KMS)
    - Default option
      - Generated inside AWS's Hardware Security Modules
        - Replicated across multiple HSMs within the same region
      - Automatic key rotation
      - No exportable
      - Symmetric key or the private half of an asymmetric key pair never leaves AWS KMS unencrypted (plaintext)
  - Imported key material (EXTERNAL)
    - BYOK to KMS
      - To meet compliance requirements
      - Customer control key generation process and source of key material
        - Root of trust outside AWS
        - Customer is responsible
      - No automatic rotation
  - Custom Key Store (AWS_CLOUDHSM)
    - Allows KMS to delegate cryptographic operations to single-tenant
      - Externally hosted key management systems (External Key Stores / XKS) - on prem HSM
      - Dedicated AWS Cloud HSM
- Key deletion
  - Generated keys cannot be deleted immediately
    - Waiting period of 7 to **30 days**
  - ScheduleKeyDeletion waiting period
  - You can cancel deletion during waiting period (pending deletion status)
  - For multi-region key
    - 1- delete replica key
    - 2- delete primary key
- Integration with CloudTrail

AWS CloudHSM
- **Dedicated (single tenant) HSM in the cloud**
  - AWS
    - Manages the hardware
    - Cannot access customer keys
  - Customer complete and exclusive control over
    - Managed by customer
      - Using AWS CloudHSM client
  - FIPS 140-2 Level 3 validated HSMs (hsm1.medium)
  - FIPS 140-3 Level 3 validated HSMs (hsm2m.medium)
- Supports
  - Multiple HSMs are spread across Multi AZ for HA
  - Built-in backup and recovery capabilities
- Handles
  - Key generation
  - Encryption / Decryption
  - Digital Signing
  - Secure Key Storage
- Cryptographic Acceleration (Integration with third party services)
  - SSL/TLS Offload
    - Windows Server CA
    - Oracle TDE...

Service-Level Encryption at Rest
- Encryption Context
- Amazon S3
  - S3-managed keys (**SSE-S3** using AES-256)
    - Key managed by AWS
    - **Enabled by default**
  - KMS keys (**SSE-KMS**)
  - KMS Key Dual-Layer (**DSSE-KMS**)
  - **Server-Side Encryption**
    - Object are encrypted twice
      - Layer 1 : KMS Key
      - Layer 2 : S3 Managed Key
    - AWS does not store the encryption key
      - HTTPS must be used
    - Customer-provided keys (**SSE-C**)
      - Customer is responsible for key management
        - Can use CloudHSM
  - Client-Side Encryption
    - Customer manages its keys
    - Data encryption and decryption are done by client
- Block & File Storage (EBS & EFS)
  - EBS
    - Volume encryption transparently encrypts data at rest inside the volume, disk I/O, snapshot backups & derived volumes using KMS keys
      - An **account-level settings** can be enforced **per-region** to encrypt automatically new EBS volumes / snapshots
  - EFS
    - Supports filesystem encryption at rest using KMS
      - Customer specifies KMS key
      - 1- Create a new encrypted EFS
      - You can not encrypt an existing EFS
        - 2- migrate files using AWS DataSync
- Databases
  - RDS
    - Transparent storage encryption for DB instances, automated backups, read replicas & snapshots via KMS
    - Amazon RDS uses an AWS Key Management Service key to encrypt these resources
  - DynamoDB
    - Encryption at rest integrates with AWS Key Management Service (AWS KMS) for managing the encryption keys that are used to encrypt your tables

AWS Secret Manager
- Managed service for storing secrets
  - Secrets are encrypted using KMS
    - With symmetric KMS Keys (DEK)
  - Secrets can be replicate across multiple regions
    - Primary
    - Replica
      - A read replica can be promote standalone secret
- Integration especially with Amazon RDS, DocumentDB...
- Secrets rotation
  - Automated for integrated databases
  - Can force rotation of secrets every X days
  - Is done using Lambda function
- Resource Policy
  - Who can access a Secret
  - What actions an IAM identity can do

AWS Systems Manager
- Helps to manage EC2 & on-premises systems
  - Linux or Windows OS or MacOS
  - Works with a SSM Agent
    - Defines the actions that Systems Manager performs on managed instances
  - Documents (JSON or YAML)
    - Are associated to resources
- Node tools
  - Inventory
    - Collect metadata from managed instances
  - Run Command
    - No need for SSH
  - Patch Manager
    - Using Maintenance Windows
  - State Manager
    - Keeping managed instances to a defined state
  - Session Manager
    - Allows to start a secure shell to an EC2 or on-premises servers
      - **Doesn't need SSH access, bastion hosts or SSH Keys**
- Change management
  - Automation
    - To simplify common maintenance and deployment tasks
- Application tools
  - Parameter Store
    - Provides key-value parameter management with KMS encryption support (SecureString)
      - Free (compare to Secret Manager that has associated costs)
      - Secret Manager is better with automatic rotation and cross region replications
- Operation tools
  - OpsCenter

AWS Certificate Manager (ACM)
- Regional service
  - Can NOT copy certificates across regions
- To host public SSL Certificates
  - Can do automatic renewal
    - Notice 45 days before expiration (in EventBridge)
- Can create public or private Certificates
- Can loads SSL certificates in
  - Load Balancers
  - CloudFront distributions
  - APIs on API Gateways

AWS Private Certificate Authority
- Managed service
  - To create of private certificate authority (CA) hierarchies, including root & subordinate CAs
- Can issue end-entity X.509 certificates
  - Certificates are trust only by your Organization
- Regional resource
- Support OSCP responder

Amazon Verified Permissions
- Managed Authorization Service
- A scalable, fine-grained permissions management and authorization service for custom applications built by you

AWS Config
- Helps with auditing & recording of compliance of AWS account
  - Detailed reports and customisable dashboards
    - View of compliance posture
  - Provides a detailed inventory and history of your AWS resources
- Regional Service
  - Records details about configuration
- Config Rules
  - Managed
  - Custom
    - Remediation
      - Using SSM Automation Documents
- Conformance Pack
  - Collection of AWS Config Rules
    - Apply to AWS Accounts & AWS Organization
- Organisational Rules
  - One rule
    - Apply to AWS Organization
- Aggregator is create in one central aggregator account

Data Protection
- CloudWatch Logs Data Protection
  - Helps to discover & protect sensitive data within logs streams
  - Data protection policies
- SNS Message Data Protection
  - no longer available to new customers after April 30, 2026
  - SNS Data protection policies
- Amazon S3
  - MFA Delete
    - Need Versioning enabled on bucket
    - Can be enabled or disabled only by bucket owner / root account
  - S3 Object Lock
    - WORM Model
      - Retention period
        - Governance
        - Compliance
      - Legal Hold
  - Authorization
    - User Context
    - Bucket Context
      - Bucket level permissions
    - Object Context
      - Object level permissions
        - Arn:aws:s3::mybucket/*
  - Canned ACL
    - a predefined, standard set of access permissions that you can easily apply to an Amazon S3 bucket or object using a single request header (x-amz-acl)
  - S3 Glacier Vault Lock
    - WORM (Write Once Read Many) model
    - Has 1 Vault Lock Policy