
aws
certified
Security
Specialty

IAM

Define permissions for an action

Policies

New IAM Users have no privileges by default

Privileges are specified by an IAM policy

IAM policy can be attached to

User, Groups

Resources

Roles

Policy Doc

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
        "Sid": "<Statement identifier>",
        "Effect": "<Allow or Deny>",
        "Action": [   "<Some Action>" ],
        "Resource": [ "<Some AWS Resource>" ],
        "Condition": [ "<Some condition>" ]
        }
{
```

mandatory, optional

By default, all requests are implicitly denied

An explicit allow overrides this default

An explicit deny in any policy overrides any allows

explicit & implicit effects

Identity-based Policies

Identity-based policies are JSON permissions policy documents that you can attach to an identity (user, group of users, or role).

Resource-based Policies

Resource-based policies are JSON policy documents that you attach to a resource such as an Amazon S3 bucket.

Resource-based policies are inline policies. There are no managed resource-based policies.

Session Policies

Session policies are advanced policies that you pass in a parameter when you programmatically create a temporary session for a role or federated user.

USER vs ROLE

AWS IAM User	AWS IAM Role
IAM identity with specific permission	IAM identity with specific permission
A user is a fixed identity	A role can be assumed by entities
User has static credentials (password, Access Key, Secret Access key)	Role has temporary credentials (Access Key, Secret Access key, Session Token)

ROLE USE CASES

Intra-account scenario

User is granted temporary permission to do something

Cross-account scenario

AWS users is granted access to resources on different account

Service Role scenario

Provide access for services offered by AWS to AWS resources

Identity Federation Scenario

Provide access for external users (Identity Federation)

Summary

AWS IAM Policies provides:

- granular access to resources
- perfect coupling with AWS resources

AWS IAM Policies offer proper tools to successfully cover all possible scenarios.

Securing Data & Secrets

KMS

Create and manage Customer Master Keys (CMKs)	Integrate with AWS services	Enable and disable CMKs
Schedule CMK deletion	Configure key policies and grants	Configure account and API-level permissions

Key Rotation Options

Key rotation is accomplished by updating the backing key material
Old key material is retained to decrypt previously encrypted data

AWS-managed
Always rotated automatically every 3 years

AWS-generated
Can optionally be rotated automatically every year

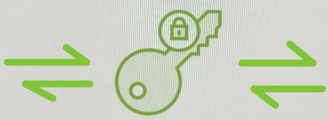
Imported key material
Cannot be automatically rotated, only manually
Can use any rotation schedule

Envelope Encryption

Encrypting Data Using CMKs

CMKs can only directly encrypt/decrypt 4 KB of data
Must use envelope encryption technique for larger data

Master key (CMK)
Used to generate data key



Data key
Used to encrypt data

Data
Encrypted data key is stored alongside the encrypted data

Cloud HSM

Cloud-based Hardware Security Module

Single-tenant

Cluster for high availability

Secure Parameter Storage

Applications use variables as key-value parameters

Never store application secrets directly in code

Store parameter values separately from code

AWS Systems Manager Parameter Store and AWS Secrets Manager

	Secrets Manager	Parameter Store
Centralized management of secrets	✓	✓
Always encrypted	✓	✓
Can share secrets between accounts	✓	
Per-parameter cost	✓	
Encrypted or unencrypted		✓
Within a single account		✓
10,000 free parameters (standard tier)		✓

Secrets Mgr CRED Rotation

Automatic credential rotation

Customer-defined schedule

Applied automatically to RDS databases

Lambda for non-RDS credentials

Assign new CRED prior to rotation

S3 cross region replication (CRR)

Copies data between S3 buckets

Data encrypted in transit

Meet compliance requirements

Can copy across AWS accounts

IAM role for replication

Bucket policy for cross-account

EBS & RDS SNAPSHOTS

Backup and disaster recovery	Encrypt copies of an unencrypted snapshot
Add encryption to a resource after it is created	Encrypted snapshot copies remain encrypted

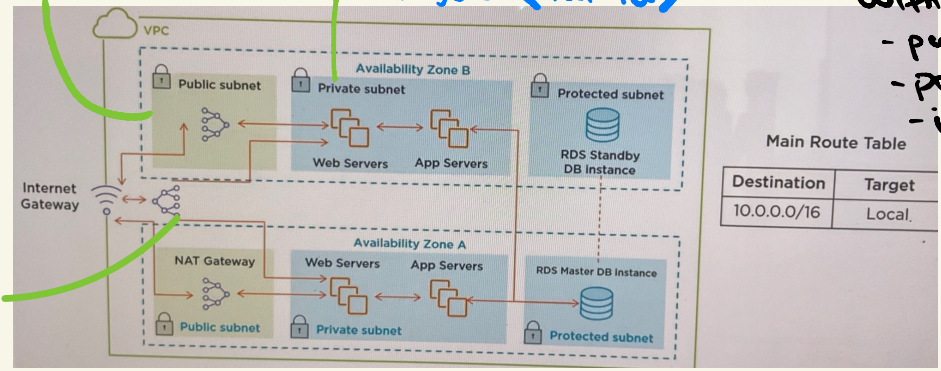
only with snapshot /copy

VPC BEST PRACTICES

Public Route table targets <igw-id>

Private RT targets <nat-id>

Layer Def with subnets
- public
- private
- isolated private



Main Route Table

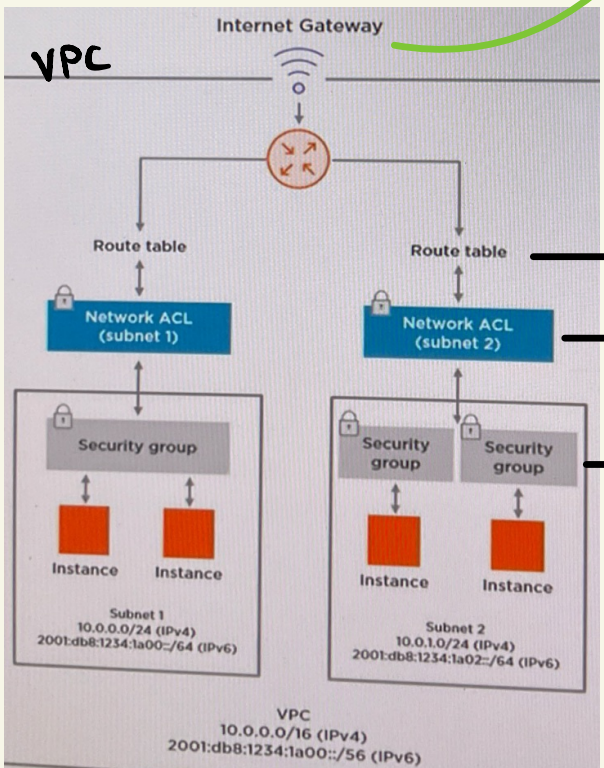
Destination	Target
10.0.0.0/16	Local

ELB

Security Group	Network ACL
Associated to an EC2 instance via their network interface card (ENI)	Associated to a subnet and implemented in the network
Supports Allow rules only because it blocks traffic by default	Supports Allow rules and Deny rules
Stateful	Stateless
All rules are evaluated before deciding whether to allow traffic	All rules are processed by their sequence number

An IG is not attatched to an A2, it is attached to a VPC

Introduce security at different layers of the Infra



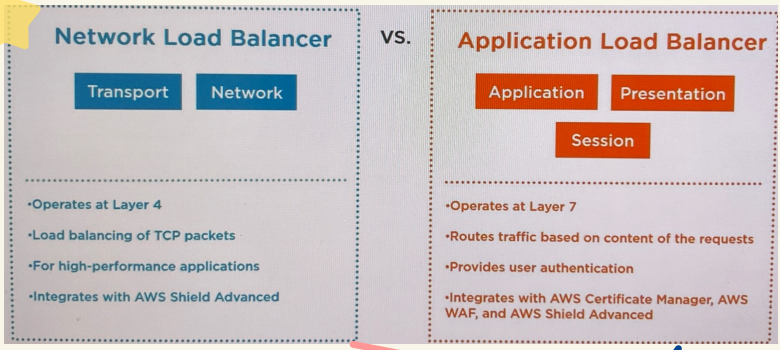
LAYERED DEF

1 RT

2 NACL

3 SG

ELB



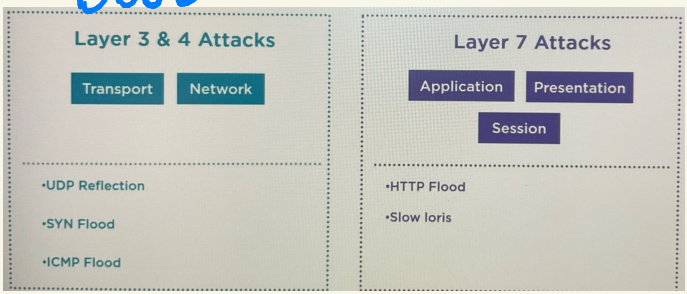
L4

OLD, ALL Ls

L7

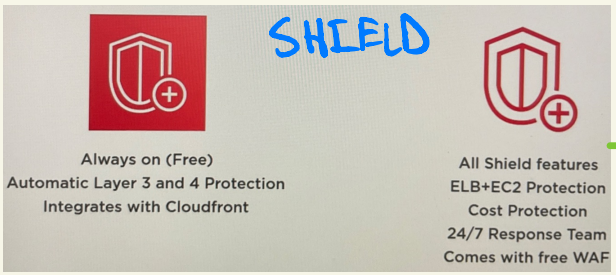
	Application Load Balancer	Network Load Balancer	Classic Load Balancer
Protocols	HTTP, HTTPS	TCP, UDP, TLS	TCP, TLS/SSL, HTTP, HTTPS
Platforms	VPC	VPC	EC2-Classic, VPC
Logging	✓	✓	✓
Health checks	✓	✓	✓
TLS offloading	✓	✓	✓
Path-based routing	✓		
Static/elastic IPs		✓	
User authentication	✓		

DDoS



CAN USE ELB to minimize the attack surface, scale & absorb the attack

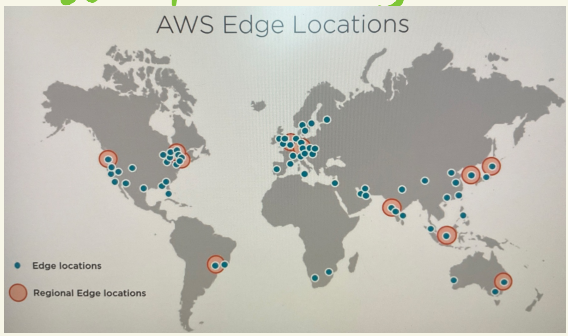
SHIELD



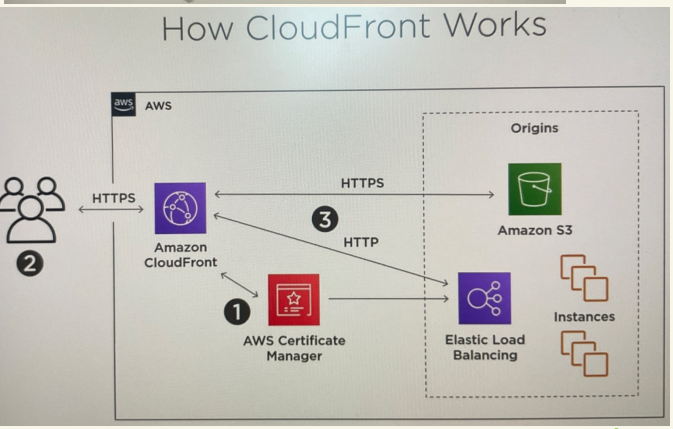
Pair with shield for layered DEF

"Security at the Edge" **CloudFront**

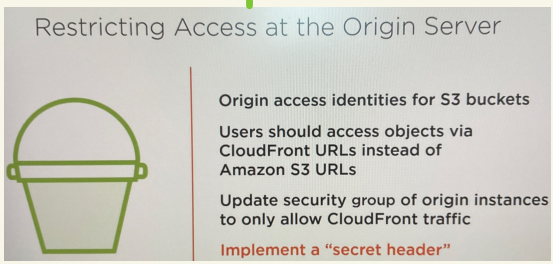
CDN that securely delivers data, videos, Apps, and APIs



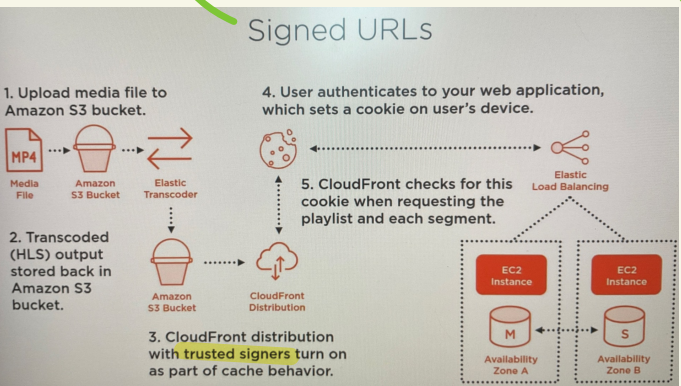
Sits in front of infra, integrate with ACM for SSL/TLS



USE OAI to secure S3



Signed URLs or signed cookies for selective file download/streaming or access control of multiple files



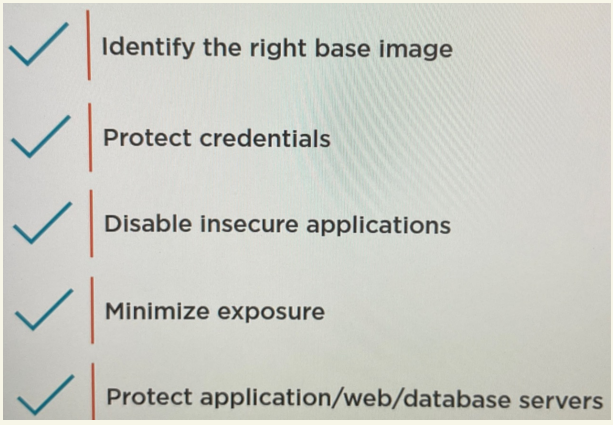
CF can do field-level encryption end-to-end

HARDENING AMIs

AMI core components
- EBS snapshots
- Access Control
- Device Mapping

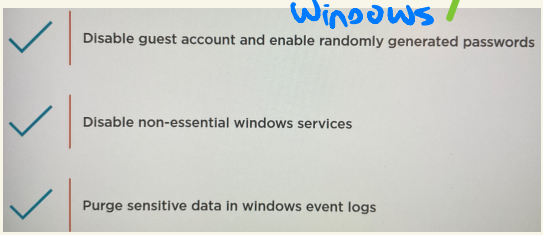
Industry Standards
- CIS
- ISO
- NIST
- SANS

Common Bootstrapping APIs
- Puppet
- Chef
- Capistrano
- Cloud-init
- CFN-init

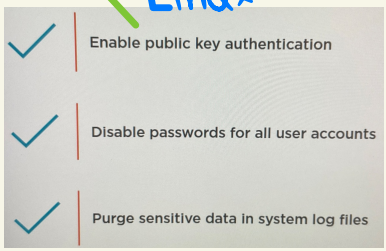


AMI Hardening Process

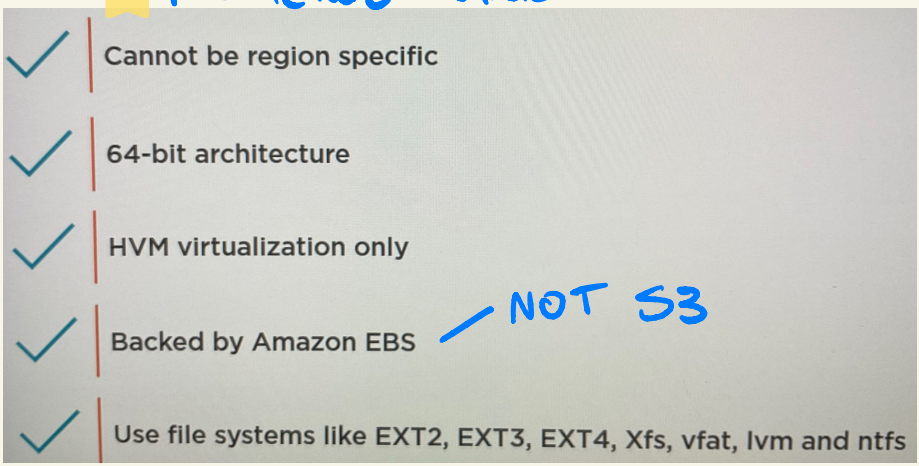
Windows



Linux



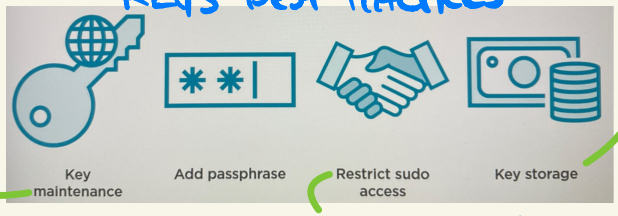
Architecture Policies



EC2 Access Control

Keys Best Practices

1 SSH key per person, rotate keys consistently

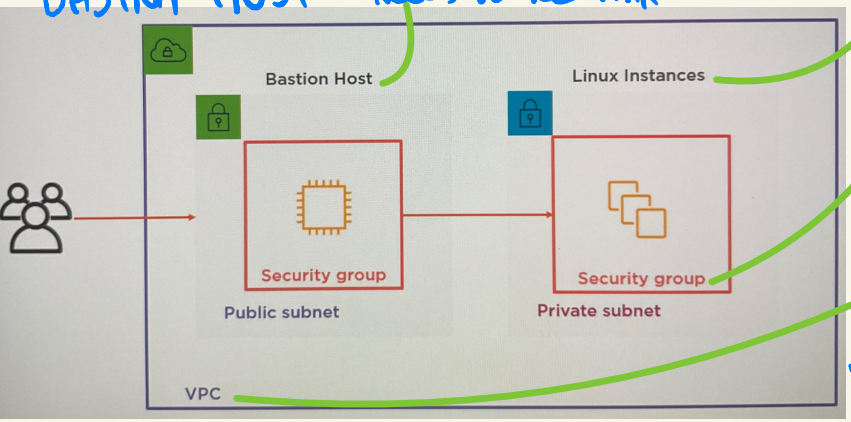


Never store private keys in tmp or home directories, keep in hidden only known by need

Give by case-by-case basis only

Bastion Host

needs to be HARDENED well

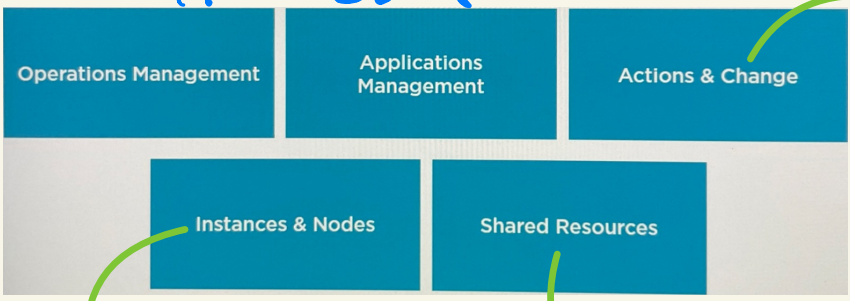


Accessible only through SSH from Bastion Host

Sec groups can be configured to block all other requests

CAN be placed in separate VPC, use VPC peering to setup connection

AWS SSM

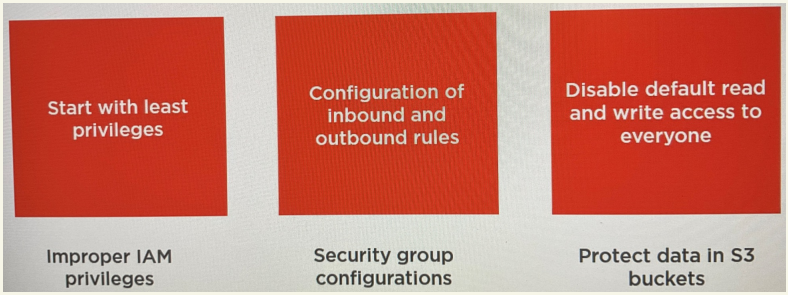


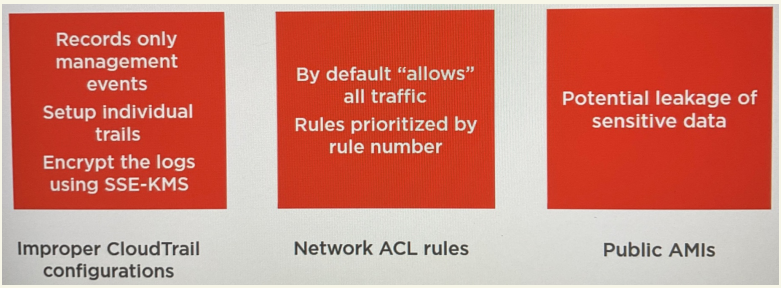
Automate maintenance tasks: patches, resetting SSH keys & passwds

manage on-prem servers, VM's, & EC2 instances

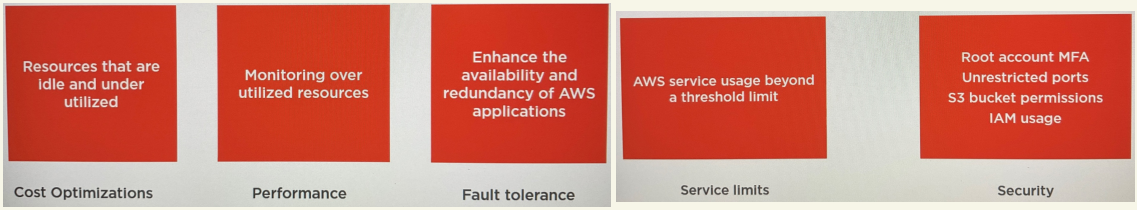
maintains all docs for config & running AWS resources

Common Threats





Trusted Advisor



Architecture Decision

Amazon Inspector	AWS Trusted Advisor
Applies to EC2 instances	Applies to AWS account
An agent needs to be installed for inspection	No additional software required
Free for first 250 instance assessments	Only security and service limits checks are free

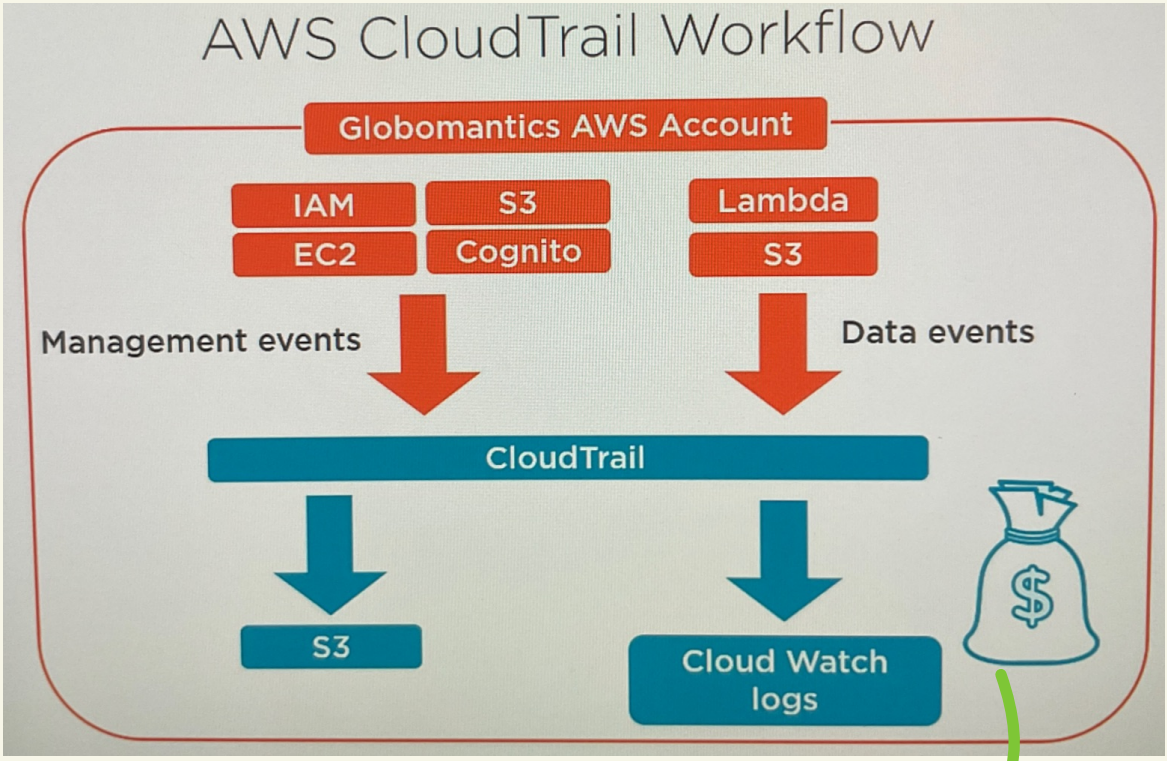
Cloud Trail

AWS CloudTrail

AWS CloudTrail is an AWS service that helps you enable governance, compliance, and operational and risk auditing of your AWS account.

Actions taken by a user, role, or an AWS service are recorded as events in CloudTrail.

Events include actions taken in the AWS Management Console, AWS Command Line Interface, and AWS SDKs and APIs.



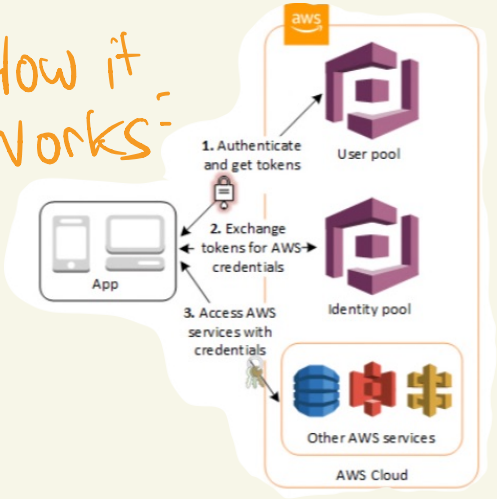
Streaming CT to CW logs will cost $$

COGNITO

- A user Mgmt auth service for web or mobile apps.
- auth through external IDP, provides temp security creeds.

- ID is represented as a JSON web token (JWT)

How it Works:



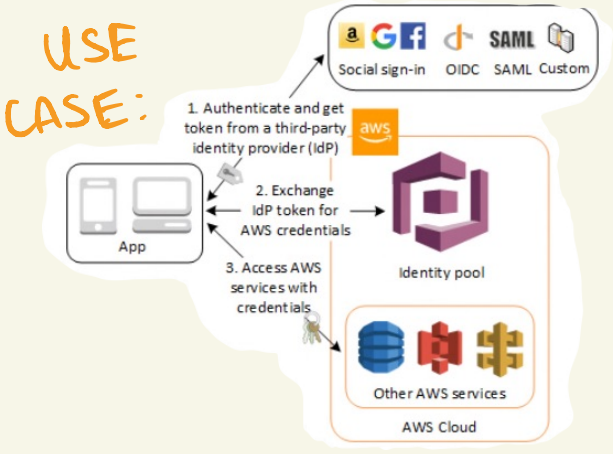
- USER POOLS: directories that provide sign-up & sign-in options

- Identity Pools: use to federate users. Grant temp creds to Access AWS services

Pricing:

- user pool, pay based on MAUs
- SNS costs

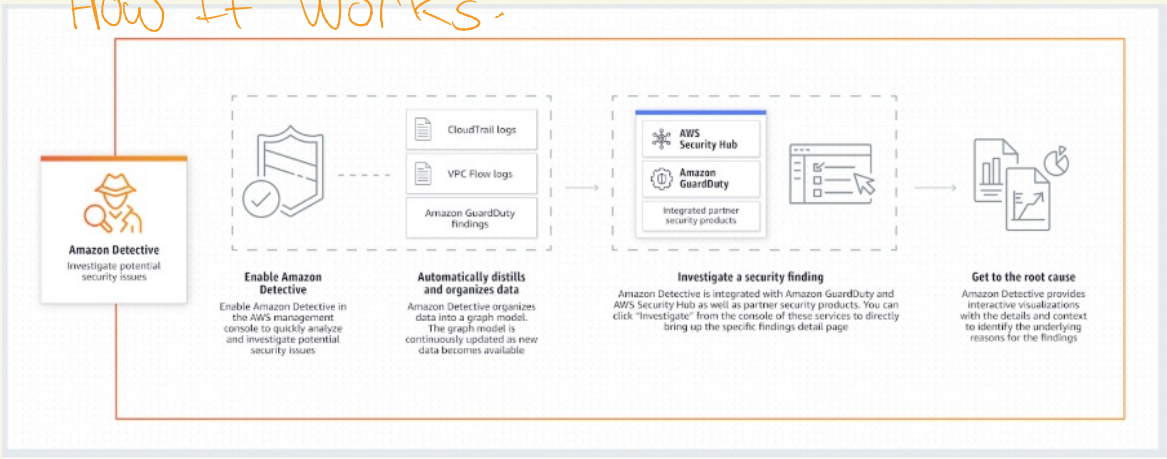
USE CASE:



DETECTIVE

The service automatically collects log data from your AWS resources and uses machine learning, statistical analysis, and graph theory to build a linked set of data that enables you to easily conduct faster and more efficient security investigations.

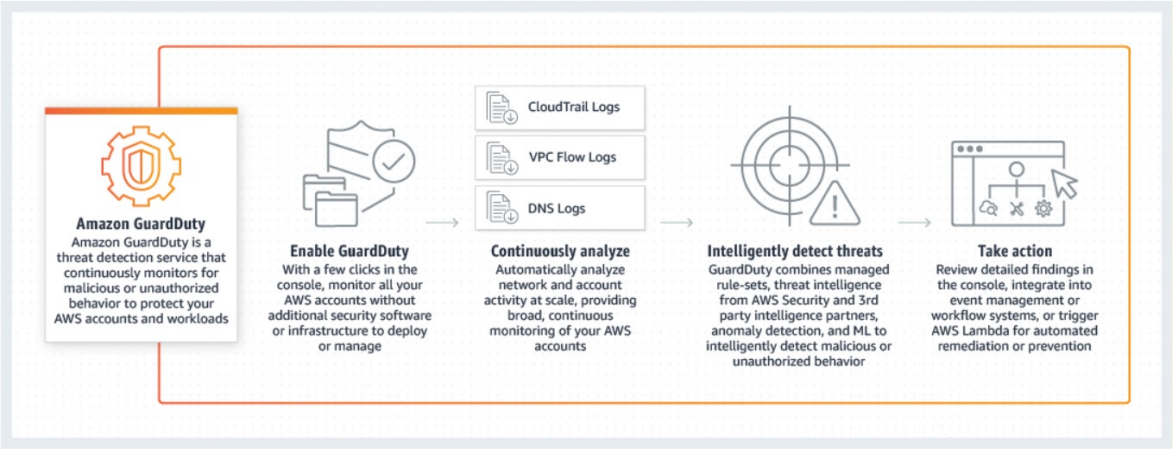
How It works:



- per region basis
- multi account service
- maintain up to A yr of aggregated findings
- USE cases:
  - triage security findings
  - incident investigation
  - hunting for hidden security threats

GuaRD DuTY

An intelligent threat detection service. It analyzes billions of events across your AWS accounts from AWS CloudTrail (AWS user and API activity in your accounts), Amazon VPC Flow Logs (network traffic data), and DNS Logs (name query patterns).



Pricing: Based on the quantity of AWS CloudTrail Events, volume of VPC flow log & DNS log data analyzed

Threat Detection Categories

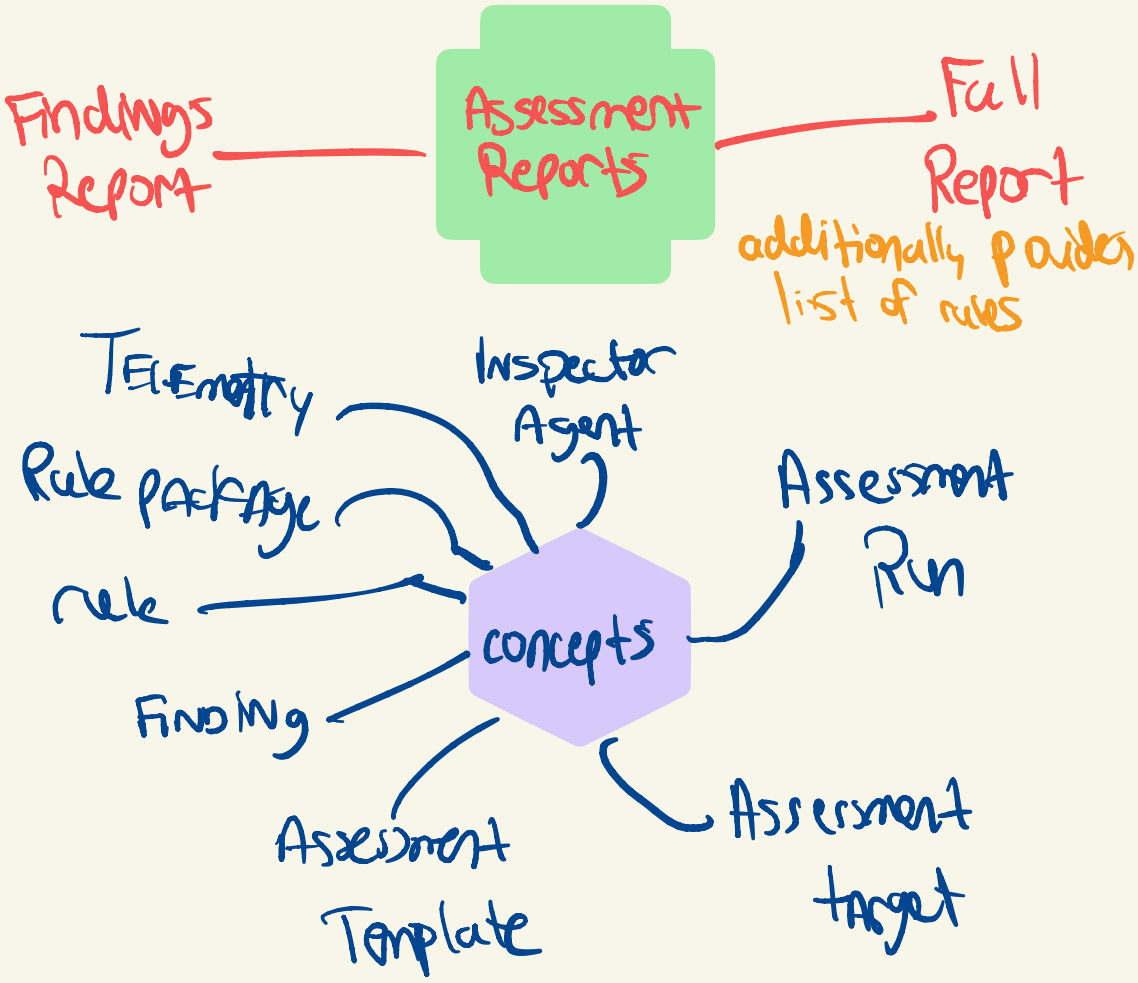
- Reconnaissance
- Account compromise
- instance compromise

- Trusted IP lists
- Threat lists

Inspector

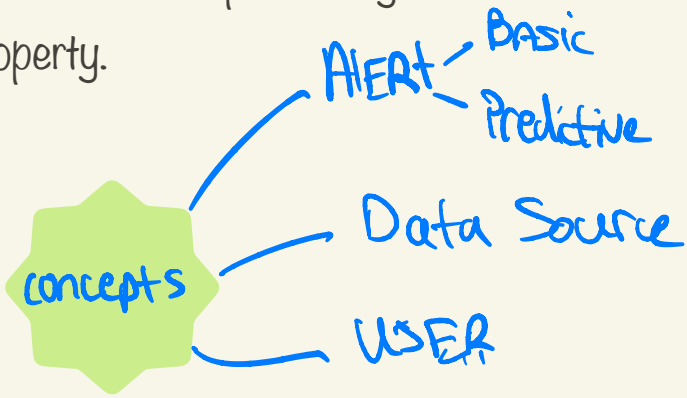
- An automated security assessment service that helps you test the network accessibility of your EC2 instances and the security state of your applications running on the instances.
- Inspector uses IAM service-linked roles..

Pricing: # of EC2 instances in each assessment
- type of rules package you select



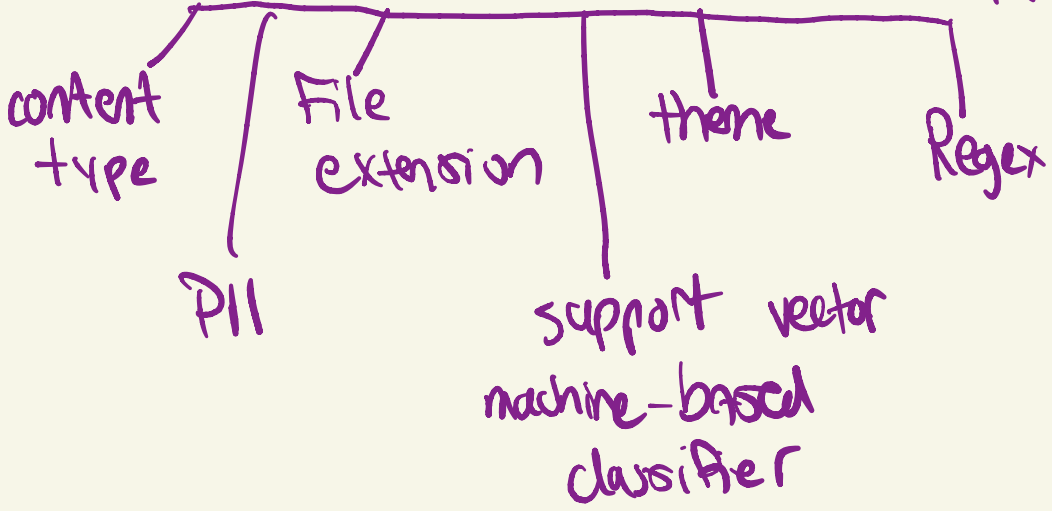
Macie

A security service that ' uses machine learning to automatically discover, classify, and protect sensitive data in AWS. Macie recognizes sensitive data such as personally identifiable information (PII) or intellectual property.



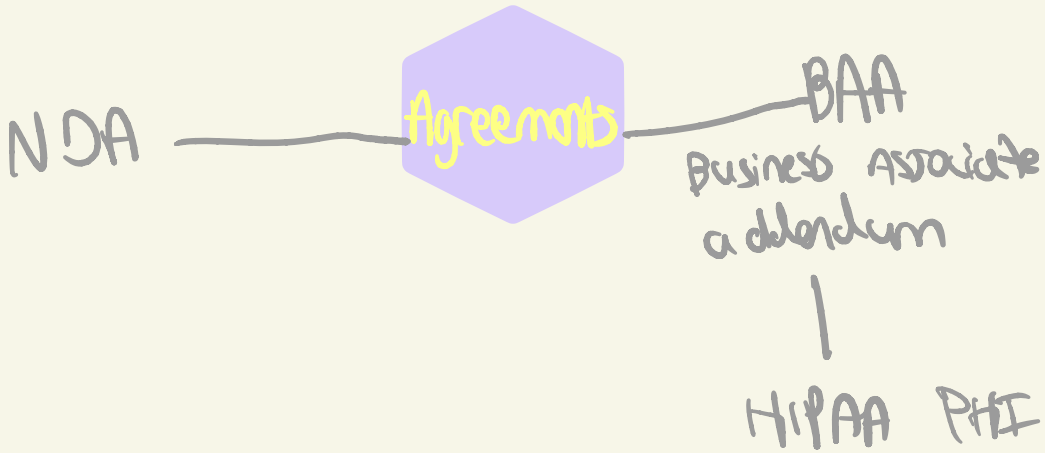
Pricing: amount of content classified + CloudTrail events

- Uses several auto content classification methods



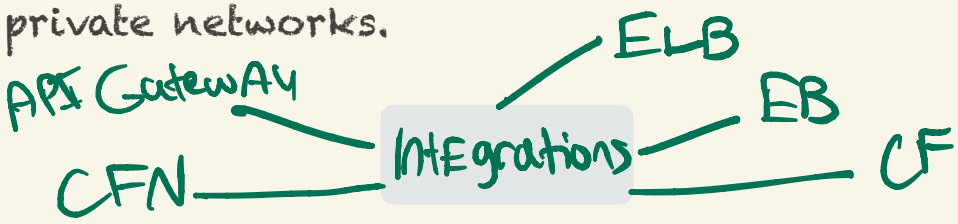
ARTIFACT

- A self-service central repository of AWS' security and compliance reports and select online agreements.
- An audit artifact is a piece of evidence that demonstrates that an organization is following a documented process or meeting a specific requirement (business compliant).



ACM

A service that lets you easily provision, manage, and deploy public and private SSL/TLS certificates for use with AWS services and your internal connected resources. SSL/TLS certificates are used to secure network communications and establish the identity of websites over the Internet as well as resources on private networks.



Concepts: - X.509 v3 certs, valid 13 months
- each cert needs FQDN
- public cert
- private cert
- imported cert

Pricing: billed for each Active ACM Private CA /month

Directory Service

- Also known as AWS Managed Microsoft AD, the service enables your directory-aware workloads and AWS resources to use managed Active Directory in the AWS Cloud.
- The service is built on actual Microsoft Active Directory and powered by Windows Server 2012 R2.

Firewall Manager

Simplifies your AWS WAF administration and maintenance tasks across multiple accounts and resources. You set up you'r firewall rules just once, and the service automatically applies your rules across your accounts and resources.

SHIELD

A managed Distributed Denial of Service (DDoS) protection service that safeguards applications running on AWS. '

Advanced : Layer 3, 4, 7

Pricing : standard = Free (L3 & L4)

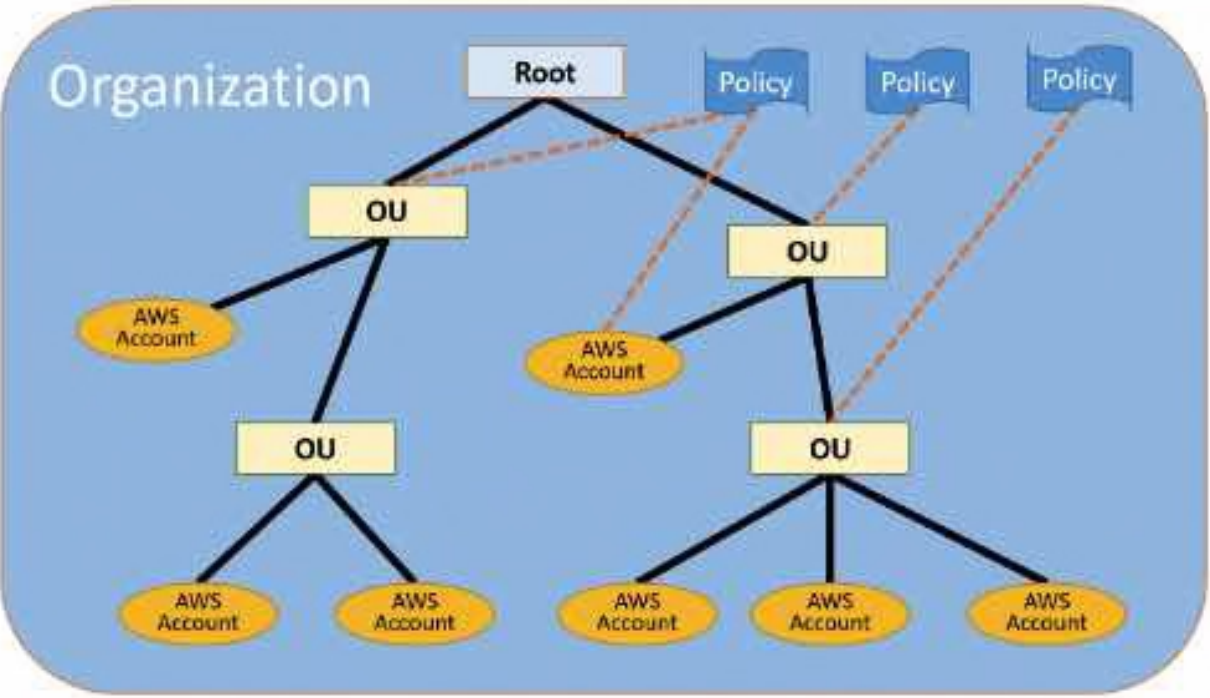
advanced = 1 yr subscription

WAF

A web application firewall that helps protect web applications from attacks by allowing you to configure rules that allow, block, or monitor (count) web requests based on conditions that you define.

ORGANIZATIONS

It offers policy-based management for multiple AWS accounts.



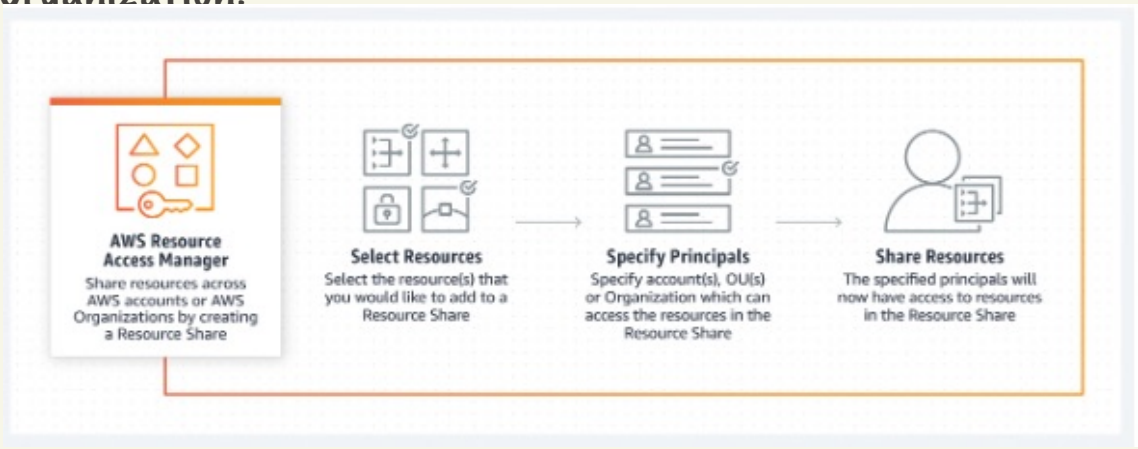
Pricing: FREE

A management account is the AWS account you use to create your organization. You cannot change which account in your organization is the management account.

Service control policy (SCP) is a policy that specifies the services and actions that users and roles can use in the accounts that the SCP affects. SCPs are similar to IAM permission policies except that they don't grant any permissions. Instead, SCPs are filters that allow only the specified services and actions to be used in affected accounts.

Resource Access Mgr (RAM)

A service that enables you to easily and securely share AWS resources with any AWS account or, if you are part of AWS Organizations, with Organizational Units (OUs) or your entire Organization.



Service	Resource
Amazon Aurora	DB Clusters
AWS CodeBuild	Projects,Report Groups
Amazon EC2	Capacity Reservations, Dedicated Hosts, Subnets, Traffic mirror targets, Transit gateways
Amazon EC2 Image Builder	Components, Images (AMI), Image recipes
AWS License Manager	License configurations
AWS Resource Groups	Resource groups
Amazon Route 53	Forwarding rules

Sharable Services

SECRETS MGR

A secret management service that enables you to easily rotate, manage, and retrieve database credentials, API keys, and other secrets throughout their lifecycle.

- contains metadata, can contain versions

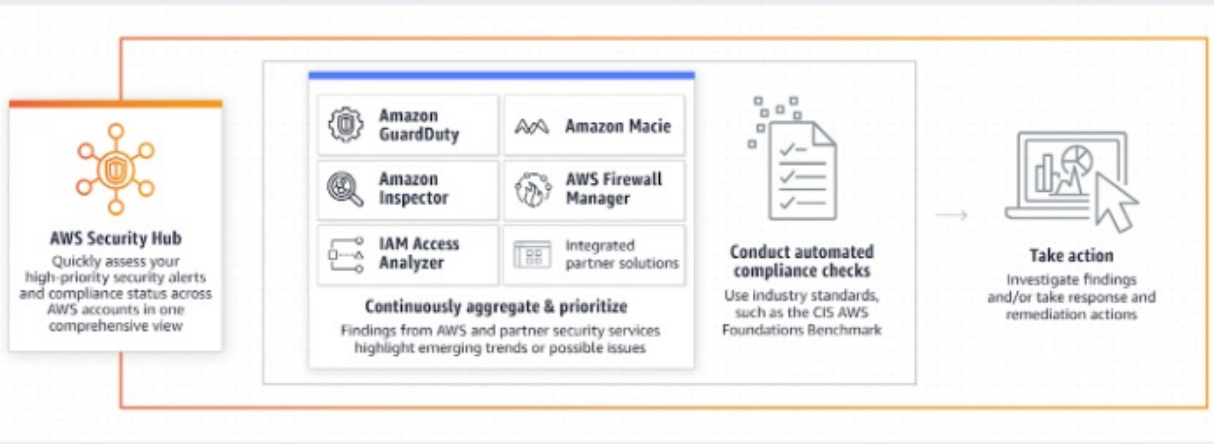
SUPPORTED SECRETS:
- Database credentials, on-premises resource credentials, SaaS application credentials, third-party API keys, and SSH keys.
- You can also store JSON documents.

- Does NOT immediately delete secrets, makes inaccessible - deletes in 7 days

SECURITY HUB

AWS Security Hub provides a comprehensive view of your security state within AWS and your compliance with security industry standards and best practices.

You now have a single place that aggregates, organizes, and prioritizes your security alerts, or findings, across multiple accounts, AWS partner tools, and AWS services such as Amazon GuardDuty, Amazon Inspector, Amazon Macie, AWS IAM Access Analyzer, AWS Firewall Manager, and AWS Audit Manager.



IAM

Control who is authenticated (signed in) and authorized (has permissions) to use resources.

Best Practice

- Lock Away Your AWS Account Root User Access Keys
- Create Individual IAM Users
- Use Groups to Assign Permissions to IAM Users
- Use AWS Defined Policies to Assign Permissions Whenever Possible
- Grant Least Privilege
- Use Access Levels to Review IAM Permissions
- Configure a Strong Password Policy for Your Users
- Enable MFA for Privileged Users
- Use Roles for Applications That Run on Amazon EC2 Instances
- Use Roles to Delegate Permissions
- Do Not Share Access Keys
- Rotate Credentials Regularly
- Remove Unnecessary Credentials
- Use Policy Conditions for Extra Security
- Monitor Activity in Your AWS Account

IAM Access Analyzer

Provides policy checks that help you proactively validate policies when creating them. These checks analyze your policy and report errors, warnings, and suggestions with actionable recommendations that help you set secure and functional permissions.

STS

. Create and provide trusted users with temporary security credentials that can control access to your AWS resources.

When to Create IAM User	When to Create an IAM Role
You created an AWS account and you're the only person who works in your account.	You're creating an application that runs on an Amazon EC2 instance and that application makes requests to AWS.
Other people in your group need to work in your AWS account, and your group is using no other identity mechanism.	You're creating an app that runs on a mobile phone and that makes requests to AWS.
You want to use the command-line interface to work with AWS.	Users in your company are authenticated in your corporate network and want to be able to use AWS without having no sign in again (federate into AWS)

KMS

A managed service that enables you to easily encrypt your data. KMS provides a highly available key storage, management, and auditing solution for you to encrypt data within your own applications and control the encryption of stored data across AWS services.

CMKs

Customer Master Keys (CMKs) – You can use a CMK to encrypt and decrypt up to 4 KB of data. Typically, you use CMKs to generate, encrypt, and decrypt the data keys that you use outside of KMS to encrypt your data. Master keys are 256-bits in length.

Type of CMK	Can view	Can manage	Used only for my AWS account
Customer managed CMK	Yes	Yes	Yes
AWS managed CMK	Yes	No	Yes
AWS owned CMK	No	No	No