WHIZLABS

AWS Security Speciality Certification

Cheat Sheet

Quick Bytes for you before the exam!

*The information provided in the cheat sheet is for educational purposes only. It was created in our efforts to help aspirants prepare for the **AWS Security Speciality certification exam**. Though references have been taken from **AWS documentation**, it's not intended as a substitute for the official documents. The document can be reused, reproduced, and printed in any form; ensure that appropriate sources are credited and required permissions are received.*

Are you Ready for

"AWS Security Speciality" Certification?

Self-assess yourself with

Whizlabs FREE TEST

800+ Hands-on-Labs and Cloud Sandbox

Hands-on Labs **Cloud Sandbox environments**

Index

—-Back to Index—

Management and Governance

AWS CloudTrail

What is AWS CloudTrail?

AWS CloudTrail is defined as a global service that permits users to enable operational and risk auditing of the AWS account.

It allows users to view, search, download, archive, analyze, and respond to account activity across the AWS infrastructure.

It records actions as an event taken by a user, role, or an AWS service in the AWS Management Console, AWS Command Line Interface, and AWS SDKs and APIs.

AWS CloudTrail mainly integrates with:

- Amazon S3 can be used to retrieve log files.
- Amazon SNS can be used to notify about log file delivery to the bucket with Amazon Simple Queue Service (SQS).
- Amazon CloudWatch for monitoring and AWS Identity and Access Management (IAM) for security.
- CloudTrail events from the past 90 days can be viewed in the console or downloaded as CSV/JSON files.
- Trail log files can be aggregated across accounts into a single bucket and shared between accounts.
- CloudTrail Insights detects and analyzes unusual API activity in management events.

There are three types of CloudTrail events:

- Management events or control plane operations
  - Example - Amazon EC2 *CreateSubnet* API operations and CreateDefaultVpc API operations
- Data events
  - Example - S3 Bucket *GetObject*, *DeleteObject*, and *PutObject* API operations
- CloudTrail Insights events (unusual activity events)
  - Example - Amazon S3 *deleteBucket* API, Amazon EC2 *AuthorizeSecurityGroupIngress* API

CloudWatch monitors and manages the activity of AWS services and resources, reporting on their health and performance. Whereas, CloudTrail resembles logs of all actions performed inside the AWS environment.

Amazon CloudWatch

What is Amazon CloudWatch?

Amazon CloudWatch is a service that helps monitor and manage services by providing data and actionable insights for AWS applications and infrastructure resources.
It monitors AWS resources such as Amazon RDS DB instances, Amazon EC2 instances, Amazon DynamoDB tables, and, as well as any log files generated by the applications.

Amazon CloudWatch can be accessed by the following methods:

- **Amazon CloudWatch console**
- AWS CLI
- CloudWatch API
- AWS SDKs

Amazon CloudWatch is used together with the following services:

- Amazon Simple Notification Service (Amazon SNS)
- Amazon EC2 Auto Scaling
- AWS CloudTrail
- AWS Identity and Access Management (IAM)

Features

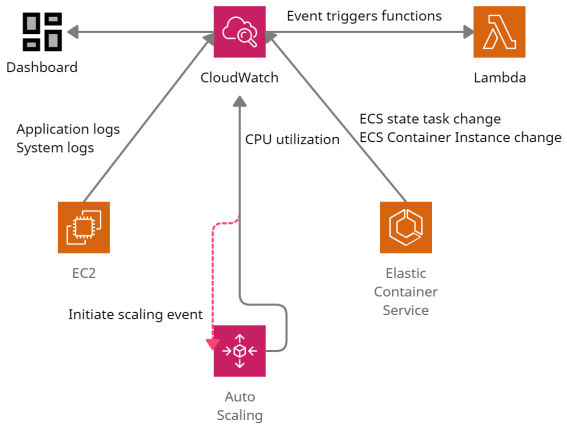
- Collects logs, metrics, and events from AWS resources, applications, and on-premises servers.
- Displays key metrics on the CloudWatch console home page and allows custom dashboards.
- Enables alarms to monitor metrics, send notifications, or automate actions when thresholds are breached.
- Supports cross-account visibility for dashboards, alarms, and metrics, especially useful with AWS Organizations.
- **Container Insights:** Summarizes metrics and logs from containerized applications on ECS, EKS, and Kubernetes.
- **Lambda Insights:** Tracks system-level metrics (CPU, memory, disk, network) for AWS Lambda serverless applications.

CloudWatch Agent Features:

- Collects system-level metrics from EC2 instances and on-premises servers across OS.
- Gathers custom metrics using **StatsD** (Linux & Windows) and **collected** (Linux only).

Metrics Handling:

- Metrics are stored in CloudWatch like standard CloudWatch metrics.
- Default namespace: **CWAgent** (configurable during setup)



Amazon CloudWatch in action

AWS Config

What is AWS Config?

Monitoring & Evaluation:

- Continuously monitors and evaluates AWS resource configurations.
- Tracks configuration changes over time via AWS Config Console or CLI.

Snapshots & Notifications:

- Captures resource configuration snapshots for a complete inventory.
- Retrieves past configurations and sends notifications for resource creation, modification, or deletion.

Config Rules:

- Evaluate resource configurations and check rule violations.
- Supports up to **150 rules per region**:
    - **Managed Rules**
    - **Custom Rules**

Integration:

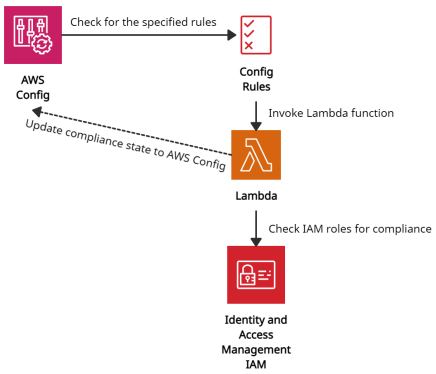
- Works with AWS IAM for permission policies, S3 for snapshots, and SNS for notifications.
- Integrated with CloudTrail to log API calls as events in AWS Config.

AWS Config provides an aggregator (a resource) to collect AWS Config configuration and compliance data from:

- Multiple accounts and multiple regions.
- Single account and multiple regions.
- An organization in AWS Organizations
- The Accounts in the organization which have AWS Config enabled.

Use Cases:

- **Custom Rules:**
    - Define custom resource configuration rules using AWS Lambda.
    - Automate resource configuration assessments for compliance and self-governance.
- **Security Monitoring:**
    - Continuously monitor configurations for security weaknesses.
    - Review configuration history after alerts to assess risk factors.



AWS Config in action

AWS Organizations

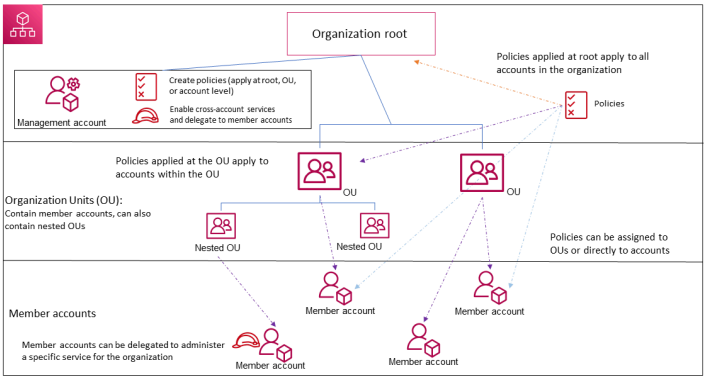
What are AWS Organizations?

AWS Organizations is a global service that enables users to consolidate and manage multiple AWS accounts into an organization.
It includes account management and combined billing capabilities that help to meet the budgetary, and security needs of the business better.

- The main account is the management account – it cannot be changed.
- Other accounts are member accounts that can only be part of a single organization.

Access Methods

- AWS Management Console
- AWS Command Line Tools and CLI
- AWS Tools for Windows PowerShell
- AWS SDKs
- AWS Organizations HTTPS Query API



AWS Organizations flow

Features

- **Security and Resource Sharing:**
  - Enforces security boundaries with multiple member accounts.
  - Shares critical resources across accounts.
- **Account Organization:**
  - Groups accounts into **Organizational Units (OUs)** for specific applications.
  - Enforces governance using **Service Control Policies (SCPs)** to meet security requirements.
- **Cost Management:**
  - Uses cost allocation tags for tracking costs by category.
  - Provides consolidated billing for all member accounts with volume discounts.
- **Integrations:**
  - **AWS CloudTrail:** Auditing and event logging.
  - **AWS Backup:** Backup monitoring.
  - **AWS Control Tower:** Cross-account security audits and policy management.
  - **Amazon GuardDuty:** Threat detection and security services.
  - **AWS RAM:** Shares resources to reduce duplication.

Member Account Migration

1. Remove the member account from the old organization.
2. Invite the member account to the new organization.
3. Accept the invitation in the member account.

Pricing

- AWS Organizations is free. Charges apply to other AWS services used.
- The management account pays for all resources used within the organization.

AWS Systems Manager

What is AWS Systems Manager?

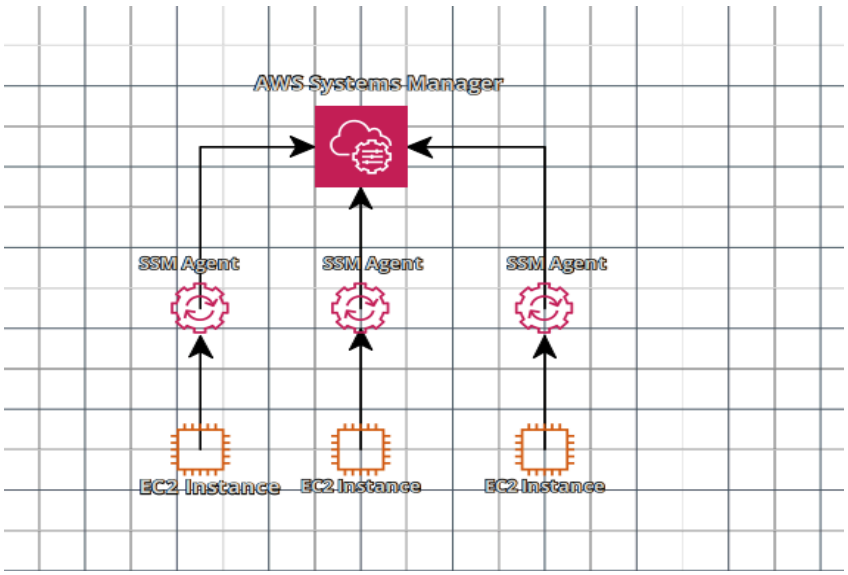
AWS Systems Manager helps manage EC2 and on-premises systems at scale, providing infrastructure insights, problem detection, and automated patching for compliance. It supports both Windows and Linux operating systems.

Key Features

- **Integration:** Works with AWS Config and CloudWatch metrics/dashboards.
- **Compliance Management:**
  - Automates patching and ensures compliance with desired states.
  - Audits installed software and detects discrepancies.
- **Resource Grouping:** Organizes over 100 resource types into applications, business units, or environments.
- **Instance Insights:**
  - Provides information on OS patch levels and installed software.
  - Distributes multiple software versions securely.
- **Security and Automation:**
  - Runs commands/scripts to increase security.
  - Automates workflows to reduce errors using configurable parameters.

How AWS Systems Manager Works

1. **SSM Agent:** Install the SSM agent on systems to enable management.
2. **IAM Role:** Ensure EC2 instances have proper IAM roles for SSM actions.
3. **Troubleshooting:** If management fails, verify the SSM agent installation and role configuration.



—-Back to Index—

AWS Trusted Advisor

What is AWS Trusted Advisor?

Trusted Advisor itself provides checks based on Best Practices in the Cost Optimization, Security, Fault Tolerance, and Performance improvement categories.

- **Cost Optimization** - Provides recommendations to Organizations for saving money on their AWS infrastructure by terminating unused & idle resources, and using Reserved capacity for continuous usage.
- **Security** - Provides recommendations to Organizations for improving the security of their applications by Restricting access using SG/ NACL, Checking permissions on S3 Buckets, and enabling various security features.
- **Fault Tolerance** - Increasing availability and redundancy of applications using Auto Scaling, Performing Health checks, configuring Multi-AZ environments, and taking backups.
- **Performance** - Provides recommendations to Organizations for improving the performance of applications by taking advantage of provisioned throughput, and monitoring over-utilized instances
- Service Limits - Notifies Organizations when their resource usage is more than 80%.

Use cases:

- **Optimization of cost & efficiency -** Trusted Advisor helps identify resources that are not used to capacity or idle resources and provides recommendations to lower costs.
- **Address Security Gaps -** Trusted Advisor performs Security checks of your AWS environment based on security best practices. It flags off errors or warnings depending on the severity of the security threat e.g. Open SG/NACL ports for unrestricted external user access, and open access permissions for S3 buckets in Accounts.
- **Performance Improvement -** Trusted Advisor checks for usage & configuration of your AWS resources and provides recommendations that can improve performance e.g. it can check for Provisioned IOPS EBS volumes on EC2 instances that are not EBS-optimized.

Networking & Content Delivery

AWS VPC

Overview

- Amazon Virtual Private Cloud (VPC) allows the launching of AWS resources in an isolated virtual network.
- Mimics traditional on-premises networks with AWS's scalability.
- Includes subnets, IP addressing, gateways, and routing for connectivity.

Features

- **Virtual Private Clouds (VPCs):** Logical, isolated virtual networks resembling on-premises setups.
- **Subnets:** IP address ranges within a VPC, tied to specific Availability Zones.
- **IP Addressing:** Supports IPv4 and IPv6, Allows bringing public IPs to AWS for allocation.
- **Routing:** Route tables manage network traffic direction.

Gateways and Endpoints

- Internet Gateway: Connects VPC to the internet.
- VPC Endpoint: Private connection to AWS services.
- **VPC Peering:** Connects multiple VPCs for resource communication.
- **Traffic Mirroring:** Captures network traffic for monitoring and inspection.
- **Transit Gateways:** Central hub for routing across VPCs, VPNs, and Direct Connect.
- **VPC Flow Logs:** Logs IP traffic for monitoring.
- **VPN Connections:** Connects VPCs to on-premises networks securely.

Interfaces for Management

- Web-based interface: **AWS Management Console**
- Command-line tool for VPC management: **AWS CLI**
- Language-specific APIs for easy integration: **AWS SDKs**
- Direct, low-level access to VPC actions: **Query API**

Pricing Highlights

- No base charges for VPC usage.
- Charges for specific components like NAT gateways and traffic mirroring.
- Public IPv4 addresses (Elastic IPs, EC2 public IPs) may incur additional costs.

Common AWS Services Using VPC

- **Compute:** EC2, Amazon ECS, Amazon EKS.
- **Database:** Amazon RDS, Amazon Redshift.
- **Networking:** Elastic Load Balancer, AWS Site-to-Site VPN.
- **Others:** AWS Global Accelerator, Amazon WorkSpaces.

AWS Security Groups

Overview

- Security groups function as virtual firewalls, managing the flow of inbound and outbound traffic to associated resources, such as EC2 instances.
- Traffic permissions are determined by rules that specify the source or destination, port range, and protocol.

Key Concepts

- Associated with resources in the same VPC.
- Stateful: Responses to allowed traffic are permitted.
- Can assign multiple security groups to a resource.

1. Rules and Naming

- Names must be unique within the VPC.
- Allowed characters: a-z, A-Z, 0-9, spaces, . _-:/()#,@[]+=&;{}!$*.
- Rules specify traffic directions, ports, protocols, and sources/destinations.

2. Exclusions

- Traffic to/from AWS services like DNS, DHCP, EC2 metadata, and reserved IPs is not filtered.

Best Practices

- Authorize specific IAM principals to create/modify security groups.
- Minimize the number of security groups and tailor them for similar resources.
- Restrict inbound rules for sensitive ports (e.g., SSH, RDP) to specific IP ranges.
- Avoid opening large port ranges.
- Use network ACLs alongside security groups for additional security layers.

Security Group Example

Scenario:

- **Subnet A:** Associated with Security Group 1 (SG1).
  - Rule 1: Allow SSH traffic from a specific address range.
  - Rule 2: Allow all internal communication.
- **Subnet B:** Associated with Security Group 2 (SG2).
  - Rule 1: Allow internal communication.
  - Rule 2: Allow SSH traffic from Subnet A.
- **Default Rule:** Both groups allow all outbound traffic.

Pricing Highlights

- **Quotas:** Limited security groups per VPC, rules per group, and groups per network interface.
- **Pricing:** No additional charges for using security groups.

VPC Endpoints

Overview

- VPC endpoints enable private connections to supported AWS services and services powered by AWS PrivateLink.
- No public IP addresses are required for communication between Amazon VPC instances and services.
- Traffic stays within the Amazon network, ensuring privacy and security.

VPC Endpoint Types

1. **Interface Endpoints**
    - Enable connectivity to services over AWS PrivateLink.
    - Support AWS-managed services, partner services, and services hosted by other AWS customers.
    - Consists of elastic network interfaces with private IP addresses for service communication.
2. **Gateway Endpoints**
    - Target specific IP routes in the VPC route table for services like DynamoDB and S3.
    - Do not use AWS PrivateLink.
    - Accessed using prefix lists within the VPC route table.

Key Features

- Interface endpoints use local IPs within the consumer VPC, without the need for public IPs.
- Gateway endpoints are reachable via prefix lists in the route table for specific AWS services.

Network Access Control Lists (ACLs)

Overview

- Network ACLs manage both inbound and outbound traffic at the subnet level.
- You can use default or custom ACLs to enhance the security of a VPC.
- There are no extra costs for utilizing network ACLs.

Key Features

1. **Traffic Control**
    - Determines allowed traffic for each subnet in a VPC.
    - Inbound and outbound rules control traffic entry and exit between subnets or from external sources.
2. **Default vs Custom Network ACLs**
    - **Default ACL**: Pre-configured to allow all inbound and outbound traffic.
    - **Custom ACLs**: Can be tailored to define specific rules for traffic control.
3. **Ephemeral Ports and Path MTU Discovery**
    - Custom ACLs can manage ephemeral ports and support Path MTU Discovery.

Use Cases

- Example: Control access to instances in a subnet based on specific traffic rules.
- Troubleshoot reachability issues by analyzing ACL rules and traffic flow.

Comparison with Security Groups

- Network ACLs are stateless and evaluate both inbound and outbound traffic, while security groups are stateful.

Network Access Analyzer

Purpose

- Identifies unintended network access to AWS resources.
- Allows you to define network access requirements and find non-compliant paths.

Use Cases

1. **Enhance Security Posture**:
    - Identifies access violations based on security and compliance requirements.
    - Helps improve network security configurations.
2. **Compliance Verification**:
    - Demonstrates that AWS networks meet compliance standards.

Example Verifications

- **Network Segmentation**: Ensure isolation between production and development VPCs or other logical networks.
- **Internet Accessibility**: Identify resources accessible from internet gateways and limit access to necessary ones.
- **Trusted Paths and Access**: Confirm network paths and access adhere to defined IP ranges, ports, and protocols.

Key Concepts

1. **Network Access Scopes**: Define access requirements with:
    - **MatchPaths**: Paths considered violations (e.g., from VPC A to VPC B).
    - **ExcludePaths**: Exceptions to findings (e.g., web server access).
2. **Findings**: Potential paths matching MatchPaths but excluded from ExcludePaths.

Interfaces for Access

- **AWS Management Console**: Web interface for managing analyses.
- **AWS CLI**: Command-line tool for automation.
- **AWS CloudFormation**: Templates for provisioning and managing resources.
- **AWS SDKs**: Language-specific APIs for simplified integration.
- **Query API**: Direct access using HTTPS requests.

Pricing

- Charged per network interface analyzed.

Security, Identity, and Compliance

AWS Certificate Manager (ACM)

What is AWS Certificate Manager?

- AWS Certificate Manager is a service that allows a user to provide, manage, renew and deploy public and private Secure Sockets Layer/Transport Layer Security (SSL/TLS) X.509 certificates.
- The certificates can be integrated with AWS services either by issuing them directly with ACM or importing third-party certificates into the ACM management system.

SSL Server Certificates:

● HTTPS transactions require server certificates X.509 that bind the public key in the certificate to provide authenticity.

● The certificates are signed by a certificate authority (CA) and contain the server's name, the validity period, the public key, the signature algorithm, and more.

The different types of SSL certificates are:

● Extended Validation Certificates (EV SSL) - most expensive SSL certificate type
● Organization Validated Certificates (OV SSL) - validate a business' creditably
● Domain Validated Certificates (DV SSL) - provide minimal encryption
● Wildcard SSL Certificate - secures base domain and subdomains
● Multi-Domain SSL Certificate (MDC) - secure up to hundreds of domain and subdomains
● Unified Communications Certificate (UCC) - single certificate secures multiple domain names.

Ways to deploy managed X.509 certificates:

AWS Certificate Manager (ACM)

- Secures web presence for large customers.
- Deploys certificates on API Gateway, Load Balancers, and CloudFront.

ACM Private CA

- Builds PKI for private use.
- Issues certificates for users, devices, and services.
- Supports variable lifetimes and resource-specific names.

Benefits:

- Automates private certificate creation and renewal for on-premises and AWS resources.
- Simplifies certificate creation via CSR submission or certificate upload.
- Ensures data-in-transit security and site identity verification with SSL/TLS certificates

AWS Secrets Manager

What is AWS Secrets Manager?

- AWS Secrets Manager replaces hardcoded credentials with API calls to retrieve secrets programmatically.
- Manages, rotates, and retrieves secrets like database passwords, API keys, and OAuth tokens.
- Ensures in-transit encryption for secure secret retrieval.
- Automates credential rotation for AWS databases without additional coding.
- Uses Lambda functions for rotating secrets in non-AWS databases or services.

Accessing Secrets Manager

- **AWS Management Console**: Supports storing binary data in secrets.
- **AWS Command Line Tools**: Includes AWS CLI and AWS Tools for Windows PowerShell.
- **AWS SDKs**
- **Secrets Manager HTTPS Query API**

Supported Databases for Secret Rotation

- MySQL, PostgreSQL, Oracle, MariaDB on Amazon RDS
- Amazon DocumentDB, Amazon Redshift
- Microsoft SQL Server on Amazon RDS
- Amazon Aurora

Features

- Rotates secrets securely without code deployment for compliance.
- IAM and resource-based policies manage permissions for secret access.
- Secures secrets using AWS KMS-managed encryption keys.
- Logs and monitors via AWS CloudTrail and CloudWatch for centralized auditing.

Use Cases

- Store sensitive data in encrypted **SecretString** or **SecretBinary** fields.
- Use open-source client components to cache and update secrets as needed.
- Handles API request throttling with retries for **ThrottlingException** errors.
- Tracks change in Secrets Manager through AWS Config integration.

Pricing

- No upfront costs or long-term contracts.
- Charges are based on stored secrets and API calls.
- AWS KMS usage incurs additional charges at current rates.

AWS Resource Access Manager

Allows resource sharing across AWS accounts or within an AWS Organization.

Supported Resources

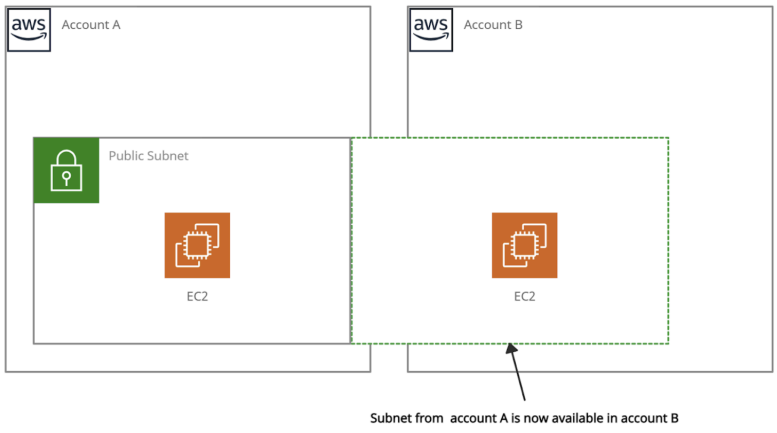
- AWS App Mesh, Amazon Aurora
- AWS Certificate Manager Private CA
- AWS CodeBuild, EC2 Image Builder
- AWS Glue, AWS License Manager
- AWS Network Firewall, AWS Outposts
- AWS Resource Groups

Benefits

- Eliminates the need for duplicate resources across accounts.
- Manages resource consumption using existing policies and permissions.
- Integrates with CloudWatch and CloudTrail for detailed visibility.
- Ensures security and governance with IAM policies and Service Control Policies (SCPs).

Pricing

- Charges vary by resource type.
- No costs for creating resource shares or sharing resources.



AWS Resource Access Manager

Amazon Detective

What is Amazon Detective?

For Amazon Detective to be enabled, GuardDuty should be enabled for your Account for at least 48 hours.

- For Amazon Detective to be enabled, Volume of data flowing into Amazon Detective's Security Behavior Graph for your account should be less than the maximum allowed by Detective.
- Amazon Detective is a Regional service and needs to be enabled for each Region.

Features:

- It is recommended to use an Administrator Account for Amazon Detective, GuardDuty & Security Hub for the following integration points to work seamlessly
- Details of GuardDuty findings can be pivoted from the finding details to Amazon Detective's finding profile.
- While investigating a GuardDuty finding in Amazon Detective, an option to archive the finding can be chosen.
- In order to reduce the amount of time it takes for Detective to receive updates of GuardDuty findings, it is recommended to update the Amazon CloudWatch notification frequency to 15 minutes in GuardDuty rather than its default frequency of 6 hours.

Use cases:

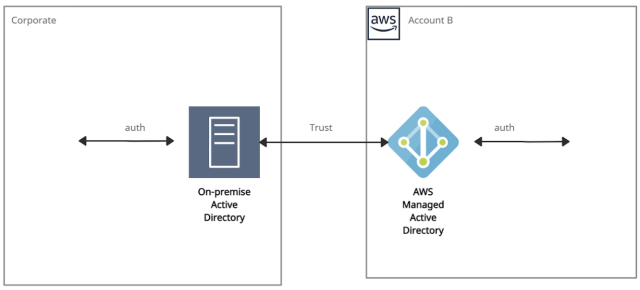
- **Triage Security findings/alerts** - Explore whether GaurdDuty findings need to be examined further. Amazon Detective helps users to see whether a finding is a concern.
- **Incident investigation** - Since Amazon Detective allows for viewing analysis & summaries going back up to a year, it can help answer questions like how long has the security issue been there, and the resources affected because of that.
- **Threat Hunting** - Access indicators like IP addresses, users to see what interactions they would have had with the environment. Detective's Security Behaviour Graph will help here.

AWS Directory Service

- Trust relationships with on-premises AD for authentication.
- Schema extensions and compatibility with SharePoint, SQL Server, and .Net apps.
- Directory availability during patching.
- Migration of AD-dependent apps and Windows workloads.
- Single sign-on (SSO) via AD trust relationships.

Directory Types

1. **Simple AD**
    - Cost-effective, AD-compatible (SAMBA 4).
    - Suitable for isolated directories with <5000 users.
    - Not compatible with on-premises AD or RDS SQL Server.
    - Features:
        - Kerberos-based SSO, group policies, user account management.
        - Domain joining for Linux and Windows EC2 instances.
    - Limitations:
        - No MFA, trust relationships, schema extensions, LDAPS communication, or PowerShell AD cmdlets.
2. **Amazon Cognito**
    - User directory for application sign-up/sign-in via Cognito User Pools.
    - Supports custom fields, federated SAML IdP users, and standard auth tokens.
3. **AD Connector**
    - Redirects requests to on-premises AD via VPN or Direct Connect.
    - Compatible with AWS services like WorkSpaces, WorkDocs, QuickSight, and EC2.
    - Supports MFA through RADIUS-based infrastructure.
    - Incompatible with RDS SQL Server.



AWS Managed AD

Use Cases

- Sign in to AWS Cloud Services using AD credentials.
- Provide directory services for AD-aware workloads.
- Enable SSO for Office 365 and cloud applications.
- Extend on-premises AD to AWS using trust relationships.

Pricing

- Varies by region. Hourly charges apply for directory sharing across accounts. Data transfer charges apply per GB for inter-region directory deployments.

Amazon GuardDuty

Overview

- Managed threat detection service that monitors AWS accounts for security threats.
- Uses machine learning, threat intelligence feeds, and log analysis to detect suspicious activities.
- Analyzes AWS CloudTrail logs, VPC Flow Logs, and DNS logs for anomalies.
- Generates actionable findings and alerts for remediation.

Features

- Ensure complete detection coverage by enabling VPC Flow logs for all regions and necessary interfaces.
- GuardDuty is Region-specific; enable it for all regions for full visibility.
- Analyze GuardDuty findings with CloudTrail to detect tampering.
- Integrate GuardDuty with EventBridge and Lambda for automated risk mitigation.

Use Cases

- Assist security analysts with investigation using GuardDuty's findings, context, and impacted resource details.
- Detect malware in EBS files or suspicious behavior on EC2 container workloads.
- Automatically enable log sources (VPC Flow logs, DNS logs) for GuardDuty—no need for manual configuration.
- Cannot add custom log sources, only the five supported by GuardDuty.

AWS IAM

- IAM is a service that helps securely control access to AWS resources.
- Allows management of user permissions without sharing passwords or access keys.
- Attach policies to users, groups, and roles for access control.

Key IAM Components

- **Principal**: Entity (user, group, or role) making requests to AWS resources. The root user is the first principal.
- **IAM User**: An entity representing a person or service with individual access.
    - Users interact with AWS without sharing passwords.
    - Permissions based on assigned policies.
- **IAM Group**: A collection of IAM users with specific permissions.
- **IAM Role**: A set of policies with permissions that can be assumed by users or external identity providers (no credentials attached).

IAM Policies

- Define access levels for users, groups, or resources.
- **Resource-Based Policies**: Attached to resources (e.g., S3 bucket) to grant permissions.
- **Identity-Based Policies**: Control user access to resources.
    - **Managed Policies**: Predefined or custom policies attached to users, groups, or roles.
    - **Inline Policies**: Directly attached to a specific user, group, or role.

IAM Security Best Practices

- Grant least privilege access.
- Enable multi-factor authentication (MFA).
- Use CloudTrail to monitor activity.
- Implement strong password policies and remove unnecessary credentials.

Pricing

- IAM is free to use; charges apply for services used by account holders.

Amazon Inspector

What is Amazon Inspector?

- Amazon Inspector is a **vulnerability management service** that scans AWS resources for **software vulnerabilities** and **network accessibility**.
- It provides a **consolidated view** of vulnerabilities across EC2 instances, container images (ECR), and Lambda functions.

Features:

- **Automated vulnerability management**: Automatically scans AWS resources like EC2, Lambda, and containers for vulnerabilities.
- **Multi-account support**: Integrates with AWS Organizations and assigns a **Delegated Administrator** to manage and configure member accounts.
- **Integration with AWS Systems Manager**: Collects software inventory and configurations from EC2 instances for vulnerability assessment.
- **Findings suppression**: Allows users to suppress findings that are considered acceptable based on predefined rules.
- **Risk scoring**: Generates a **contextual risk score** for each finding to prioritize remediation.
- **Automatic closure of findings**: Findings are automatically closed when vulnerabilities are remediated.
- **Monitoring and coverage**: Provides detailed monitoring to ensure **organization-wide coverage** without gaps.
- **Integration with AWS Security Hub and EventBridge**: Enables automation of workflows like ticketing based on findings.
- **Lambda security scans**: Scans Lambda functions for security flaws, including injection issues and missing encryption.
- **CI/CD integration**: Works with CI/CD tools like Jenkins to scan container images early in the development cycle for proactive security measures.

Use Cases:

- **Prioritize patch remediation**: Use **CVE** and network accessibility findings to prioritize patching efforts.
- **Compliance support**: Assists with **PCI DSS**, **NIST CSF**, and other regulatory compliance requirements through vulnerability scanning.

AWS Key Management Service

- **Purpose**: Secure service for creating and managing encryption keys for data protection.
- **Integration**: Works with AWS services (e.g., Amazon EBS, Amazon S3) for data encryption at rest.
- **Region-Specific**: KMS is global, but keys are region-specific and cannot be transferred outside the region.

Key Types

- **Customer Master Keys (CMKs)**: Used for encryption and decryption.
  - **Symmetric CMK**: 256-bit key for encryption/decryption.
  - **Asymmetric CMK**: RSA/ECC key pairs for encryption/decryption or signing/verification.
- **Customer-Managed CMKs**: Created, owned, and fully controlled by the user.
- **AWS Managed CMKs**: Managed and used by AWS services on the user's behalf, not for direct cryptographic operations.

Envelope Encryption

- Encrypts data with a data key and then encrypts the data key under another key, offering benefits like:
  - Protecting data keys.
  - Encrypting data under multiple master keys.
  - Combining various algorithms' strengths.

Features

- **Automatic Key Rotation**: CMKs automatically rotate yearly without needing to re-encrypt data.
- **CloudTrail Integration**: Logs all KMS requests, including details of the user, action, and key used.
- **Scalability**: Automatically scales with growing encryption needs.
- **High Availability**: Stores multiple copies of encrypted keys for resilience.

Pricing

- **Free Tier**: 20,000 requests per month across all regions.
- **Customer Managed CMK**: $1/month per key.
- **AWS Managed CMKs**: No charge for creation and storage.
- **Deletions**: Charges apply if customer-managed CMKs are canceled during the waiting period.

Amazon Cognito

What is Amazon Cognito?

- Amazon Cognito is a service for **authentication**, **authorization**, and **user management** in web and mobile applications.
- It enables user sign-ins via social (Google, Facebook) and enterprise (Microsoft Active Directory via SAML) identity providers.
- Acts as an **OpenID token provider** trusted by AWS Security Token Service (STS) for temporary AWS credentials.

Key Components:

1. **User Pools**:
    - User repository for profile management.
    - Provides **sign-up/sign-in** with a customizable web UI.
    - Includes **security features** like MFA, compromised credential checks, account takeover protection, and verification via email/phone.
    - Custom workflows and user migration through **AWS Lambda triggers**.
2. **Identity Pools**:
    - Provides **temporary AWS credentials** to users.
    - Supports identity providers like Amazon Cognito, third-party sign-ins, OpenID Connect (OIDC), and SAML.
    - Can use **user pools** and **identity pools** together or separately.

Amazon Cognito Federated Identities:

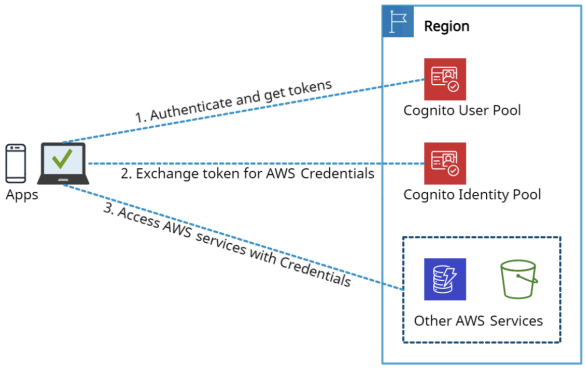
- Provides **temporary security credentials** to mobile and untrusted environments.
- Helps create **unique user identities** throughout the app's lifecycle.

Features:

- **Risk-based authentication** and protection from **compromised credentials**.
- **SDKs** available for Android, iOS, and JavaScript to add user sign-up and sign-in.
- Supports identity management standards like **OAuth 2.0**, **OpenID Connect**, and **SAML 2.0**.
- **Multi-factor authentication** via SMS or TOTP (e.g., Google Authenticator).

Pricing:

- **Volume-based pricing** for identity management and data synchronization.
- **Free tier** with additional tiers based on user sign-ins via credentials or social identity providers.



Amazon Cognito

—-Back to Index—

AWS Security Hub

- AWS Security Hub provides a comprehensive view of the **security posture** in AWS.
- Helps protect AWS environments by ensuring adherence to **security industry standards** and best practices.
- Aggregates and organizes security alerts from services like **Amazon GuardDuty**, **Amazon Inspector**, **Amazon Macie**, **AWS IAM Access Analyzer**, **AWS Firewall Manager**, and partner solutions.
- Supports compliance with standards like **PCI DSS** and **CIS AWS Foundations Benchmark**.
- Recommends **remediation steps** when issues are detected.

Key Features:

- **Automated compliance checks** using **CIS AWS Foundations Benchmark** (43 best practice checks).
- **Findings aggregation** from multiple AWS services in a **standard format**.
- Provides **integrated dashboards** to track security and compliance status.
- Can be enabled/disabled via **AWS Management Console**, **AWS CLI**, or **Infrastructure-as-Code tools** (e.g., Terraform).
- Requires enabling in each region if AWS architecture spans multiple regions.

Benefits:

- Reduces time spent on **data conversion** by using a standardized findings format.
- Offers **real-time security and compliance status** through dashboards.

Pricing:

- Charges based on the usage of **services Security Hub interacts with** (e.g., AWS Config).
- **Master account** incurs costs for all **member accounts** in a Security Hub setup.
- **Member account** incurs charges only for its own usage.
- Charges apply only in the **current region**, not across all regions where Security Hub is enabled.

AWS WAF

What is AWS WAF?

- **AWS WAF** (Web Application Firewall) is a managed service that helps protect web applications from common exploits like SQL injection, cross-site scripting (XSS), and DDoS attacks.
- It provides an **additional security layer** to safeguard application availability, security, and resource consumption.

Features:

- **Integration with AWS services**: Combine AWS WAF with services like **AWS Shield** (DDoS protection) and **Amazon CloudFront** (content delivery) for a **multi-layered security approach**.
- **Managed Rule Sets**: Keep **AWS Managed Rule Sets** up to date for protection against emerging threats.
- **Logging**: Enable logging to capture detailed information about web requests and potential threats. Use **Amazon CloudWatch** or SIEM solutions for monitoring and analysis.
- **Rate-limiting**: Implement **rate-limiting rules** to protect APIs from abuse and DDoS attacks by setting limits based on traffic patterns.
- **Web ACLs**: Customize **web access control lists (ACLs)** according to the specific needs of your application.
- **Regular rule reviews**: Periodically **review and adjust AWS WAF rules** based on changing requirements and evolving threats.

AWS Audit Manager

What is AWS WAF?

AWS Audit Manager is a service that helps automate the process of collecting evidence and managing audits to simplify compliance and risk assessments.

Key Features:

- **Free Tier Access**: Get **33,500 resource assessments** for **60 days** with the AWS Free Tier.
- **Automated Evidence Collection**: Automatically collect evidence and focus on verifying that your controls are functioning properly.
- **Collaboration**: Streamline teamwork and ensure integrity in audits with **read-only permissions**.
- **Prebuilt & Custom Frameworks**: Map AWS usage to compliance requirements using prebuilt and custom frameworks.

How It Works:

- **Mapping Compliance**: AWS Audit Manager maps your compliance requirements to AWS usage data with automated evidence collection.
- **Audit-Ready Reports**: Generate reports that are ready for audits, simplifying compliance reviews.

Use Cases:

- **Automated Evidence Collection**: Eliminate the need to manually collect and manage audit evidence.
- **Continuous Audits**: Continuously monitor your compliance posture and adjust controls proactively to reduce risk.

AWS CloudHSM

What is AWS CloudHSM?

- AWS CloudHSM is a cloud-based service for cryptographic operations and key management using Hardware Security Modules (HSMs).
- Provides enhanced data protection to meet strict corporate and regulatory compliance requirements.
- Ensures encryption keys are protected both at rest and in transit, within a secure, isolated environment.
- Uses FIPS 140-2 Level 3 validated HSMs for key management.
- Customers retain full control over their encryption keys.

Working with AWS CloudHSM

- Requires creating a **CloudHSM cluster** containing multiple HSMs across multiple Availability Zones.
- HSMs are automatically synchronized and load-balanced within a cluster.
- Each HSM is accessed in a **single-tenant** manner within an **Amazon VPC** (Virtual Private Cloud).
- Supports secure connection with EC2 instances using SSL channels, reducing network latency.

Features of AWS CloudHSM

- **Tamper Resistant:** Provides single-tenant access to tamper-resistant HSMs, compliant with FIPS 140-2 Level 3.
- **Secure Authentication:** Supports MFA and key management authentication.
- **Scalable:** Easily scale capacity by adding or removing HSMs via AWS API/CLI.
- **Open Solution:** Allows easy migration of keys to/from AWS Cloud.
- **Industry-Standard APIs:** Integrates with applications using PKCS#11, Java Cryptography Extensions (JCE), and Microsoft CryptoNG (CNG).
- **AWS Managed Infrastructure:** Automates administrative tasks like provisioning, software patching, and backups.

AWS CloudHSM Pricing

- **New customers**: No upfront costs, only pay an hourly fee per HSM launched (ranging from $1 to $3 USD depending on the region).
- **Classic customers**: $5000 USD upfront cost per instance, plus an hourly fee until termination.

Use Cases

- **Data Encryption**: Ensures high-security encryption key management.
- **Compliance**: Meets strict regulatory requirements for cryptographic operations.

AWS Firewall Manager

Overview

- Simplifies administration and maintenance across multiple accounts and resources for various protections (AWS WAF, AWS Shield Advanced, VPC security groups, network ACLs, AWS Network Firewall, Route 53 Resolver DNS Firewall).
- Protects resources by applying security configurations across accounts and resources, even when new ones are added.

Key Benefits

- Cross-account Protection: Protects resources across multiple accounts.
- Resource-based Protection: Secures all resources of a specific type (e.g., CloudFront distributions).
- Tag-based Protection: Secures resources based on specific tags.
- Automatic Protection: Automatically adds protection to new resources as they are added to your account.
- Centralized Management for Shield Advanced: Subscribes all member accounts in an AWS Organizations organization to AWS Shield Advanced and automatically subscribes new accounts.
- Security Group Management: Allows applying security group rules to all or specific subsets of accounts in an AWS Organization, and auto-applies to new accounts.
- Custom and Managed Rules: Allows using custom rules or purchasing managed rules from AWS Marketplace.

Use Cases

- Ideal for organizations protecting multiple accounts and resources or frequently adding new resources.
- Provides centralized monitoring of DDoS attacks across the organization.

AWS Shield

Overview

- **Shield Standard**: Free, automatic protection against DDoS attacks at Layer 3 & 4 (network/transport).
- **Shield Advanced**: Paid, enhanced protection including Layer 7 (application) attacks.

DDoS Attack Types

1. **Volumetric (Layer 3)**: Floods target's network or resources to deny service.
2. **Protocol (Layer 4)**: Exploits protocols like TCP SYN floods to exhaust resources.
3. **Application (Layer 7)**: Overloads applications with excessive valid requests.

AWS Shield Protection

- **Shield Standard**: Basic protection, no cost.
- **Shield Advanced**: Advanced detection, mitigation, and enhanced protections.

DDoS Detection & Mitigation

- **Layer 3 & 4**: Detects network and protocol attacks using traffic analysis.
- **Layer 7**: Detects application layer floods targeting web applications.
- **Multiple Resources**: Protects multiple resources within an application.

Mitigation Features

- **CloudFront/Route 53**: Specialized DDoS protection at edge and DNS services.
- **Regions**: Protects resources across AWS Regions.
- **Global Accelerator**: Safeguards traffic on standard accelerators.
- **Elastic IPs**: Additional protection for Elastic IPs.
- **Web Applications**: Advanced mitigation for DDoS targeting web applications.

AWS Shield Standard vs AWS Shield Advanced

- **AWS Shield Standard**:
  - Automatically provided at no additional cost.
  - Protects against common DDoS attacks.
  - Coverage for network and transport layer attacks (Layer 3 & 4).
- **AWS Shield Advanced**:
  - Subscription-based service for enhanced protection.
  - Provides additional features for proactive attack detection and mitigation.
  - Includes advanced protection for application layer attacks (Layer 7).

AWS Security Finding Format (ASFF)

Overview

AWS Security Finding Format (ASFF) is a standardized format used by AWS Security Hub to consume and aggregate findings from AWS services and third-party tools. It simplifies data processing by eliminating the need for conversion efforts.

Key Features

- **Standardized Format**: ASFF provides a consistent structure for findings, making it easier to process and analyze security data.
- **JSON-Based**: The format is derived from JSON Schema, offering a structured and machine-readable representation of findings.
- **Integration**: AWS Security Hub can ingest findings from various AWS services and third-party security products in ASFF.

Attributes of ASFF

- **Top-Level Attributes**:
    - **Required**: Essential attributes that must be included in every ASFF finding (e.g., finding ID, severity, resource).
    - **Optional**: Attributes that may be present but are not mandatory (e.g., remediation steps, additional details).

Use Case

- **Security Hub Comparison**: You can compare your findings against ASFF examples to better understand and interpret the data in your Security Hub environment.