**What is AWS Artifact?**

**AWS Artifact**

* **Compliance Repository:** Provides on-demand access to AWS compliance reports, certifications, and audit documents.
* **Centralized Agreements:** Lets organizations review, accept, and manage legal agreements with AWS across multiple accounts.
* **Audit Enablement:** Acts as a single source for third‑party attestations and industry‐standard certifications.
* **Streamlined Compliance:** Simplifies your compliance processes by offering self‑service access to security and compliance documentation.

**What is AWS Certificate Manager (ACM)?**

### ****AWS Certificate Manager (ACM)****

* **Certificate Provisioning:** Automates the creation, deployment, and renewal of SSL/TLS certificates.
* **Secure Communication:** Ensures encrypted data transmission for websites and applications on AWS.
* **Public & Private Support:** Manages both publicly trusted and private certificates from your own certificate authority.
* **Service Integration:** Seamlessly integrates with AWS services such as CloudFront, Elastic Load Balancing, and API Gateway.

**What is AWS CloudHSM?**

### ****AWS CloudHSM****

* **Dedicated Hardware:** Offers single‑tenant hardware security modules (HSMs) for secure cryptographic processing.
* **Key Management Control:** Provides full control over the generation, storage, and lifecycle of cryptographic keys.
* **Regulatory Compliance:** Meets stringent FIPS 140‑2/140‑3 standards for organizations with high compliance needs.
* **Direct API Access:** Allows integration into your applications via standard cryptographic APIs and SDKs.

**What is Amazon Cognito?**

### ****Amazon Cognito****

* **User Authentication:** Manages sign‑up, sign‑in, and user authentication for web and mobile applications.
* **User Pools & Identity Pools:** Separates user directory management from AWS credential provisioning for authenticated access.
* **Social and Enterprise Integration:** Supports login via social identity providers (Google, Facebook) as well as enterprise directories.
* **Scalable and Secure:** Scales to millions of users while simplifying access control and synchronization across devices.

**What is AWS Directory Service?**

### ****AWS Directory Service****

* **Multiple Directory Options:** Provides choices like AWS Managed Microsoft AD, AD Connector, and Simple AD.
* **Active Directory Integration:** Allows you to run Microsoft Active Directory in the cloud or connect to your on‑premises AD.
* **Centralized Management:** Enables centralized identity management for AWS resources, simplifying access control.
* **Support for Applications:** Facilitates the integration of directory‑based applications (such as file sharing or single sign‑on) within AWS.

**What is AWS Firewall Manager?**

### ****AWS Firewall Manager****

* **Centralized Security Policies:** Allows you to deploy and manage firewall rules across multiple AWS accounts and resources.
* **Multi‑Service Integration:** Works jointly with AWS WAF, Shield Advanced, and VPC security groups to enforce policies.
* **Automation:** Automatically applies security configurations to newly provisioned resources.
* **Consistent Compliance:** Ensures that your organization follows a consistent security posture across accounts.

**What is Amazon GuardDuty?**

### ****Amazon GuardDuty****

* **Threat Detection:** Continuously monitors AWS accounts, networks, and logs for security threats using machine learning.
* **Log Analysis:** Integrates with CloudTrail logs, VPC flow logs, and DNS logs to detect anomalous activity.
* **Actionable Findings:** Generates detailed findings with prioritized recommendations for remediation.
* **Fully Managed Service:** Scales effortlessly, providing automated protection without the need for manual configuration.

**What is AWS Identity and Access Management (IAM)?**

### ****AWS Identity and Access Management (IAM)****

* **Granular Access Control:** Enables creation and management of users, groups, and roles with fine‑grained permissions.
* **Secure Authentication:** Provides mechanisms for identity verification and secure sign‑in to AWS resources.
* **Policy-Based Permissions:** Uses policies to enforce least privilege access and secure resource interactions.
* **Integration with AWS:** Interfaces seamlessly with most AWS services to control and audit API requests.

**What is AWS IAM Identity Center (AWS Single Sign-On)?**

### ****AWS IAM Identity Center (AWS Single Sign‑On)****

* **Streamlined Access:** Offers a unified SSO experience across multiple AWS accounts and third‑party applications.
* **Centralized User Management:** Simplifies workforce identity management by integrating with existing directories or using its built‑in user store.
* **Permission Assignment:** Allows centralized assignment of roles and permissions for a multi‑account environment.
* **Federation Support:** Integrates with external identity providers (like Active Directory, Okta, or Azure AD) for streamlined authentication.

**What is Amazon Inspector?**

### ****Amazon Inspector****

* **Automated Vulnerability Assessment:** Scans AWS workloads (EC2 instances, container images, Lambda functions) for security vulnerabilities.
* **Continuous Monitoring:** Automatically detects changes such as new vulnerabilities or unintended network exposures.
* **Detailed Findings:** Provides comprehensive reports with prioritized remediation actions.
* **DevOps Integration:** Easily integrates into CI/CD pipelines for continuous security assessment throughout the development lifecycle.

**What is AWS Key Management Service (AWS KMS)?**

### ****AWS Key Management Service (AWS KMS)****

* **Managed Key Infrastructure:** Simplifies the creation, storage, and administration of cryptographic keys.
* **Hardware Security Integration:** Leverages FIPS‑validated HSMs to protect keys in a secure and compliant manner.
* **Granular Control:** Provides fine‑grained permissions to determine who can use or manage your keys.
* **Service Interoperability:** Natively integrates with many AWS services for encryption and decryption tasks across your environment.

**What is Amazon Macie?**

### ****Amazon Macie****

* **Sensitive Data Discovery:** Uses machine learning to automatically identify and classify sensitive data in Amazon S3.
* **Risk Visibility:** Offers dashboards and reports that highlight security risks and exposure of sensitive information.
* **Compliance Support:** Helps organizations meet regulatory requirements by monitoring data access and usage.
* **Customizable Analysis:** Provides options to tailor detection criteria based on your organizational needs and data sensitivity.

**What is AWS Resource Access Manager (AWS RAM)?**

### ****AWS Resource Access Manager (AWS RAM)****

* **Resource Sharing Made Easy:** Lets you share AWS resources (such as subnets or Transit Gateways) with other AWS accounts.
* **Simplified Administration:** Reduces duplication by allowing a single resource instance to be shared across multiple accounts.
* **Flexible Sharing Options:** Supports sharing within AWS Organizations, specified account groups, or even to individual IAM roles and users.
* **Audit and Visibility:** Integrates with AWS CloudTrail and CloudWatch for monitoring resource usage and tracking sharing changes.

**What is AWS Secrets Manager?**

### ****AWS Secrets Manager****

* **Secure Secret Storage:** Safely stores sensitive information such as passwords, API keys, and database credentials.
* **Automated Rotation:** Supports automatic, scheduled rotation of secrets to enhance security posture.
* **Dynamic Retrieval:** Eliminates hard‑coded credentials by enabling applications to retrieve secrets programmatically at runtime.
* **Fine‑Grained Access:** Integrates with IAM to control who or what can read and manage your secrets.

**What is AWS Shield?**

### ****AWS Shield****

* **DDoS Protection:** Provides managed Distributed Denial of Service (DDoS) protection to safeguard AWS applications.
* **Two Tiers of Service:** Includes AWS Shield Standard (built‑in at no extra cost) and Shield Advanced for enhanced protection.
* **Always‑On Monitoring:** Automatically detects and mitigates DDoS attacks to minimize downtime and latency.
* **Integration with Other Services:** Works with AWS WAF and Firewall Manager to provide a layered security defense.

**What is AWS WAF?**

### ****AWS Web Application Firewall (WAF)****

* **Traffic Filtering:** Protects web applications by filtering HTTP/HTTPS traffic based on rules you define.
* **Customizable Rules:** Allows creation of custom rules targeting SQL injections, cross‑site scripting (XSS), and other common exploits.
* **Bot Control and Rate Limiting:** Provides features like CAPTCHA challenges and rate‑limiting to control malicious bot traffic.
* **Service Compatibility:** Integrates smoothly with Amazon CloudFront, API Gateway, Application Load Balancer, and more to safeguard web endpoints.