SECURITY, IDENTITY, AND COMPLIANCE IN AWS

AWS Secrets Manager

AWS Secrets Manager is a service that helps securely store, manage, and retrieve **database credentials** and other secrets. It allows automatic rotation of credentials, reducing the risk of exposure and ensuring robust security. By integrating with AWS services, Secrets Manager simplifies managing access to sensitive information, enhancing security for your applications and databases.

Watch Out For: When storing credentials in AWS Secrets Manager, there's no such thing as a secure string parameter, that only exists in parameter store.

IAM Roles

AWS Identity and Access Management (IAM) is a key service that enhances security and access control within the Amazon Web Services ecosystem. It allows administrators to manage users and groups, and set fine-grained permissions to securely control access to AWS resources. IAM ensures that only authorized users can perform specific actions, maintaining robust security and compliance.

Key features of IAM include multi-factor authentication (MFA), integration with identity providers for federated access, and the use of IAM roles for secure cross-account and service-to-service communication. IAM policies enable precise access control, supporting the principle of least privilege to minimize unauthorized access risks and strengthen overall security.

IAM Roles allow you to give permissions to Amazon Services to access other services/perform operations on your behalf.

Ex. Give EC2 instances an IAM Role that grants permission to access S3.

IAM Roles when using AD

Active Directory (AD) is a directory service developed by Microsoft for Windows domain networks. AD enables organizations to enforce security policies, manage access to resources, and maintain a hierarchical structure of the network in a centralized way.

When using Active Directory, IAM roles play a crucial role in determining what permissions users have regarding various AWS services. By integrating AD with IAM roles, organizations can assign specific permissions to users or groups based on their roles within the company.

So in other words, **for giving permissions to AWS Services when using External Active Directory connectors, IAM Roles are used.**

IAM Administration best practice

Quick Tip:

It is accepted as an IAM best practice for system administrators to utilize MFA (Multi-Factor Authentication) for more secure access to AWS Services.

KMS and multi-region keys

AWS Key Management Service (KMS) is a vital service for managing cryptographic keys and controlling their use across a wide range of AWS services and applications. It provides centralized management of encryption keys, enhancing data security both at rest and in transit. By integrating with various AWS services, KMS ensures seamless encryption and decryption processes, facilitating strong security measures without adding operational complexity.

KMS supports several types of keys, including:

- **Customer Managed Keys (CMKs)**: Created and managed by the user, offering full control over permissions and lifecycle.
- **AWS Managed Keys**: Automatically created and managed by AWS services such as S3, RDS, and EBS, providing ease of use without manual key management.
- **AWS Owned Keys**: Managed entirely by AWS and used across multiple AWS accounts, offering a simplified, cost-effective solution for less sensitive data.

Important tip for the exams:

When dealing with info stored in multiple regions, use the multi-region KMS key.

Certificate Authority (CA)

A
Certificate Authority (CA) is a trusted entity that issues digital certificates used to verify the identity of individuals, organizations, and servers over the internet or within a private network. CAs play a crucial role in establishing secure communication channels by encrypting data and confirming the authenticity of parties involved in online transactions and communications.

Note:

CAs can be used to both import and issue an SSL/TLS certificate but imported certificates need to be rotated manually.

AWS Config Certificates

Quick tip:

AWS Config has a managed rule
named acm-certificate-expiration-check
to check for expiring certificates
(configurable number of days)

AWS CloudHSM

AWS CloudHSM

- **Purpose**: AWS CloudHSM provides hardware security modules in the cloud, allowing you to generate and use your own encryption keys within a highly secure, dedicated hardware device. It gives you complete control over your key management, including key creation, management, and use for cryptographic operations.
- **Independence from CloudTrail**: While AWS CloudHSM can be integrated with other AWS services, its primary function is to secure cryptographic keys and perform cryptographic operations. Auditing in the context of CloudHSM typically refers to its ability to log and report on cryptographic operations that occur within the HSM itself, which is separate from the kind of API call logging provided by AWS CloudTrail.

Service Control Policies (SCPs)

Service control policies (SCPs) are one type of policy that you can use to manage your organization. SCPs offer central control over the maximum available permissions for all accounts in your organization, allowing you to ensure your accounts stay within your organization's access control guidelines.

AWS Shield Advanced

AWS Shield is a managed Distributed Denial of Service (DDoS) protection service that safeguards applications running on AWS and can be assigned to load balancers and other AWS networking resources.

For more sophisticated and larger-scale attacks, **AWS Shield Advanced** offers enhanced detection and mitigation, cost protection against scaling charges during attacks, and detailed attack diagnostics. Thereby making AWS Shield a robust solution for maintaining the availability and performance of your applications in the face of DDoS threats.

AWS WAF

Short for Web Application Firewall, used to fight against SQL injection attacks and other common attacks as well as restrict access to the website to certain countries only.

Basically, just a firewall.

AWS Firewall manager however has to be used when managing firewalls across AWS accounts.

Shield vs WAF, When to use what:

Shield ⇒ Load Balancer, CloudFront, Route53
WAF ⇒ CloudFront, ALB, API Gateway

GuardDuty

GuardDuty is an Amazon-managed continuous threat detection service for detection of malicious activity in your AWS Accounts and services.

It uses machine learning, anomaly detection, and integrated threat intelligence to identify potential security threats, such as unusual API calls or unauthorized access attempts.

AWS Network Firewall

AWS Network Firewall is a managed service that provides scalable network protection for Amazon Virtual Private Cloud (VPC) environments.

It allows you to filter and inspect traffic at the network level using customizable rulesets based on IP addresses, protocols, and ports. Network Firewall integrates with AWS Firewall Manager for centralized management and provides real-time visibility into network traffic patterns and threats.

Basically. AWS Network Firewall is a very extensive service, used for **traffic inspection and filtering**. An important consideration, when protecting VPCs.