SECURITY, DEPLOYMENT & OPERATIONS

AWS Secrets Manager

AWS Secrets manager is a product which can manage secrets within AWS. There is some overlap between it and the SSM Parameter Store - but Secrets manager is specialised for secrets. EXAM - Secrets manager is capable of automatic CREDENTIAL ROTATION using LAMBDA.

- For supported services it can even adjust the credentials of the service itself.
- Secrets encrypted using KMS
- Integrates with RDS

EXAM Secrets Manager VS Parameter Store? SM is designed for SECRETS (passwords, API Keys), SM auto rotation of secrets with Lambda,

- Parameter store stores strongs, secure strings--for config info

Application Layer (L7) Firewall

L7 firewalls are capable of inspecting, filtering and even adjusting data up to Layer 7 of the OSI model. They have visibility of the data inside a L7 connection. For HTTP this means content, headers, DNS names .. for SMTP this would mean visibility of email metadata and for plaintext emails the contents.

- WAF is an L7 Firewall

Web Application Firewall (WAF), WEBACLs, Rule Groups and Rules

AWS WAF is an L7 web application firewall that helps protect your web applications or APIs against common web exploits and bots that may affect availability, compromise security, or consume excessive resources.

- cross-scripting attacks, SQL Injection, ALLOW/DENY lists, XSS, HTTP Flood, IP Reputation, bots
- Actual unit of configuration within WAF is the WEB Access Control List (ACL)
- Web ACLs use Rules/Rule Groups -- Rule components: Type, Statement, Action --- Rule types: Regular or Rate-based --- Statement: WHAT to match/count... even down to matching body (first 8192 bytes ONLY) --- Action: Allow, Block, Count, custom respon, label

AWS Shield

For DDoS protection. AWS Shield provides always-on detection and automatic inline mitigations that minimize application downtime and latency, so there is no need to engage AWS Support to benefit from DDoS protection.

You can use AWS WAF web access control lists (web ACLs) to help minimize the effects of a Distributed Denial of Service (DDoS) attack. For additional protection against DDoS attacks, AWS also provides AWS Shield Standard and AWS Shield Advanced. AWS Shield Standard is automatically included at no extra cost beyond what you already pay for AWS WAF and your other AWS services.

- Shield Standard is free. Automatically provided with CloudFront and R53

- AWS Shield Advanced (not free) provides expanded DDoS attack protection for your Amazon EC2 instances, Elastic Load Balancing load balancers, CloudFront distributions, Route 53 hosted zones, and AWS Global Accelerator standard accelerators. -- Advanced requires manual configuration, explicit enabling. Has const protection incurred from attacks --- Advanced Shield USES WAF for L7 DDoS protection

CloudHSM

CloudHSM - an AWS provided Hardware Security Module products. Similar to KMS... creates/manages/secures crypto keys

- CloudHSM is required to achieve COMPLIANCE with certain SECURITY STANDARDS such as FIPS 140-2 Level 3

When to use KMS over CloudHSM

- KMS is a SHARED service and AWS has certain level of access to it. KMS is mostly Level 2 FIPS EXAM - CloudHSM is a SINGLE TENANT HSM (hardware security module). CloudHSM is aws provisioned but fully customer managed. CloudHSM is LEVEL 3 FIPS compliant.

- EXAM - Need CloudHSM if need access by industry standard APIs (not AWS api's); JCE, PKCS#11, CryptoNG EXAM - Need to enable Transparent Data Encryption (TDE) for Oracle DBs? CloudHSM EXAM - Protect private keys for an issuing CA (cert authority)

AWS Config

AWS Config is a service which records the configuration of resources over time (configuration items) into configuration histories.

- All the information is stored regionally in an S3 config bucket.
- AWS Config is capable of checking for compliance .. and generating notifications and events based on compliance.
- Terms: config item, config history, config rules, config stream, config notifications (via eventbridge or sns)

AWS Config - Two main jobs

1. Record configuration changes over time on resources
2. Auditing of changes, compliance with standards NOTE: AWS Config DOES NOT prevent changes from happening; no protectoin, just watches

Amazon Macie

Amazon Macie is a fully managed data security and data privacy service that uses machine learning and pattern matching to discover and protect your sensitive data in AWS.

- protect personally identifiable information of stuff in S3 buckets
- Can have Managed (built in, ML\patterns) or Custom Data Identifiers (regex based)
- checks s3 buckets

Amazon Inspector

Inspect for COMPLIANCE. Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS. Amazon Inspector automatically assesses applications for exposure, vulnerabilities, and deviations from best practices

- checks EC2 instances and the instance OS, and containers
- creates security reports ordered by priority
- Does Network Reachability (with or without Agent--agent means more info)
- Packages: Host Assessments, Common Vulnerabilities/Exposures (CVE), Center for Internet Security (CIS) Benchmarks, Security Best Practices for Amazon Inspector

Amazon Guardduty

Guard Duty is an automatic threat detection service which reviews data from supported services and attempts to identify any events outside of the 'norm' for a given AWS account or Accounts.

- CONTINUOUS SECURITY MONITORING SERVICE
- Ingests Logs and Events

Inspector VS GuardDuty

If we try to describe it in a chronological fashion, you can have Inspector set up at the start when you deploy your applications, and then GuardDuty immediately after that in order to receive alerts on potential threats. Amazon Inspector provides you with security assessments of your applications’ settings and configurations while Amazon GuardDuty helps with analysing the entirety of your AWS accounts for potential threats.