AWS Certified Solutions Architect - Associate

Week 4 – Content Review

29 JULY 2021

DHAVAL SONI

infostretch

Agenda

- Week 4 content review
  - AWS Security & Encryption
  - Networking – VPC
  - Disaster Recovery & Migrations
  - Other AWS Services
- Q & A


infostretch
CONTENT REVIEW

AWS Security & Encryption : KMS

- **Why Encryption:**
  - Encryption in flight (SSL)
  - Server-side encryption at rest
  - Client-side encryption

- Fully integrated with IAM for authorization
- Seamlessly integrated into: EBS, S3, Redshift, RDS, SSM, etc.
- You can also use the CLI / SDK

KMS

KMS – Customer Master Key (CMK) Types:

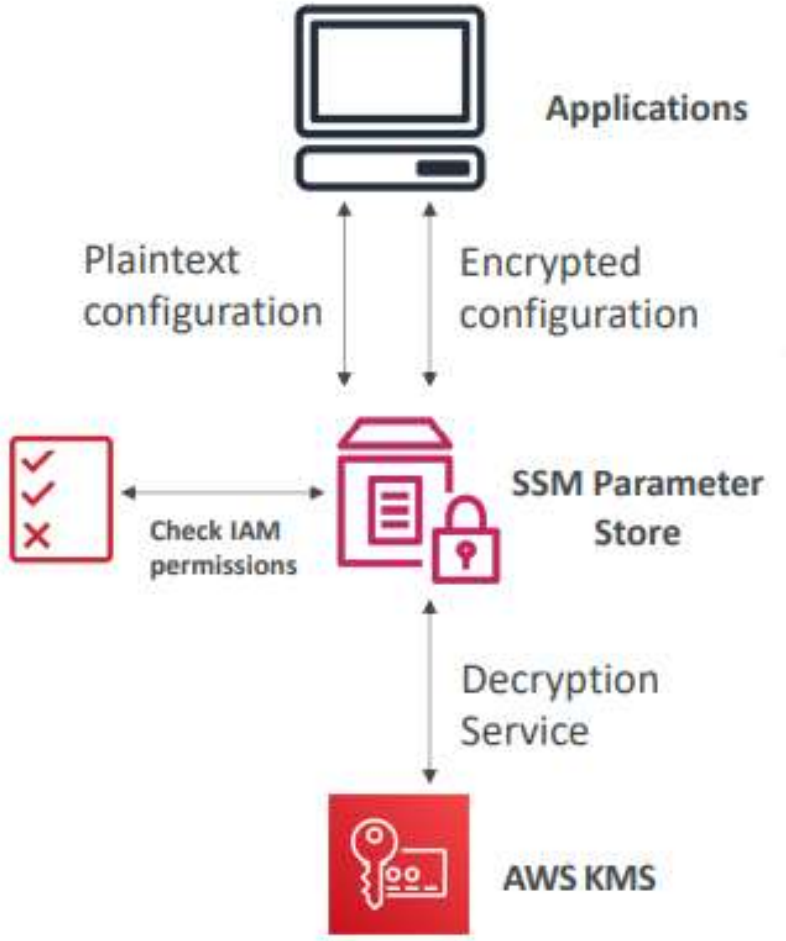
- **Symmetric (AES-256 keys)**
  - First offering of KMS, single encryption key that is used to Encrypt and Decrypt
  - AWS services that are integrated with KMS use Symmetric CMKs

- **Asymmetric (RSA & ECC key pairs)**
  - Public (Encrypt) and Private Key (Decrypt) pair
  - Used for Encrypt/Decrypt, or Sign/Verify operations

SSM Parameter Store

- Secure storage for configuration and secrets
- Optional Seamless Encryption using KMS
- Serverless, scalable, durable, easy SDK
- Version tracking of configurations / secrets
- Configuration management using path & IAM
- Notifications with CloudWatch Events
- Integration with CloudFormation

Note: Understand SSM Parameter Store Hierarchy



Security Services

AWS Secrets Manager:

- Newer service, meant for storing secrets
- Capability to force **rotation of secrets** every X days
- Automate generation of secrets on rotation (uses Lambda)
- Integration with **Amazon RDS** (MySQL, PostgreSQL, Aurora)
- Secrets are encrypted using KMS

AWS Shield:

- **AWS Shield Standard:**
  - Free service that is activated for every AWS customer
  - Provides protection from attacks such as SYN/UDP Floods, Reflection attacks and other layer 3/layer 4 attacks
- **AWS Shield Advanced:**
  - Optional DDoS mitigation service ($3,000 per month per organization)
  - Protect against more sophisticated attack on Amazon EC2, Elastic Load Balancing (ELB), Amazon CloudFront, AWS Global Accelerator, and Route 53
  - 24/7 access to AWS DDoS response team (DRP)
  - Protect against higher fees during usage spikes due to DDoS

Security Services – Contd.

CloudHSM:

- KMS => AWS manages the software for encryption
- CloudHSM => AWS provisions encryption **hardware**
- Dedicated Hardware (HSM = Hardware Security Module)
- You manage your own encryption keys entirely (not AWS)
- HSM device is tamper resistant, **FIPS 140-2 Level 3** compliance
- Supports both **symmetric** and **asymmetric** encryption (SSL/TLS keys)
- Must use the CloudHSM Client Software
- **Good option to use with SSE-C encryption**

Security Services – Contd.

AWS WAF – Web Application Firewall:

- Protects your web applications from common web exploits (Layer 7)
- **Layer 7 is HTTP** (vs Layer 4 is TCP)
- Deploy on **Application Load Balancer, API Gateway, CloudFront**
- Define Web ACL (Web Access Control List):
- Rules can include: **IP addresses**, HTTP headers, HTTP body, or URI strings
- Protects from common attack - **SQL injection** and **Cross-Site Scripting (XSS)**
- Size constraints, **geo-match (block countries)**
- **Rate-based rules** (to count occurrences of events) – **for DDoS protection**

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.**
- Macie helps identify and alert you to **sensitive data, such as PII data.**

Security Services – Contd.

infostretch

Amazon GuardDuty

- Intelligent Threat discovery to Protect AWS Account
- Uses Machine Learning algorithms, anomaly detection, 3rd party data
- Input data includes:
  - CloudTrail Logs: unusual API calls, unauthorized deployments
  - VPC Flow Logs: unusual internal traffic, unusual IP address
  - DNS Logs: compromised EC2 instances sending encoded data within DNS queries
- Can setup **CloudWatch Event rules** to be notified in case of findings
- CloudWatch Events rules can target AWS Lambda or SNS
- **Can protect against CryptoCurrency attacks (has a dedicated "finding" for it)**

Amazon Inspector

- **Automated Security Assessments for EC2 instances**
- Analyze the **running OS** against **known vulnerabilities**
- Analyze against **unintended network accessibility**
- AWS Inspector Agent must be installed on OS in EC2 instances
- After the assessment, you get a report with a list of vulnerabilities
- Possibility to send notifications to SNS

VPC Summary

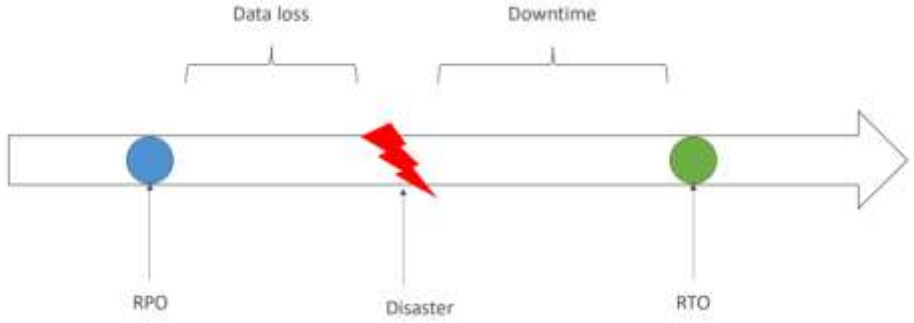
- **CIDR**: IP Range e.g., 10.0.0.16, 10.0.0.1/24
- **VPC**: Virtual Private Cloud => we define a list of IPv4 & IPv6 CIDR
- **Subnets**: Tied to an AZ, we define a CIDR
- **Internet Gateway:** at the VPC level, provide IPv4 & IPv6 Internet Access
- **Route Tables:** must be edited to add routes from subnets to the IGW, VPC Peering Connections, VPC Endpoints, etc…
- **NAT Instances**: gives internet access to instances in private subnets. Old, must be setup in a public subnet, disable Source / Destination check flag
- **NAT Gateway**: managed by AWS, provides scalable internet access to private instances, IPv4 only
- **Private DNS + Route 53:** enable DNS Resolution + DNS hostnames (VPC)
- **NACL: Stateless**, subnet rules for inbound and outbound, don’t forget ephemeral ports
- **Security Groups: Stateful**, operate at the EC2 instance level
- **VPC Peering:** Connect two VPC with non overlapping CIDR, nontransitive
- **VPC Endpoints:** Provide private access to AWS Services (S3, DynamoDB, CloudFormation, SSM) within VPC

VPC Summary

- **VPC Flow Logs:** Can be setup at the VPC / Subnet / ENI Level, for ACCEPT and REJECT traffic, helps identifying attacks, analyze using Athena or CloudWatch Log Insights
- **Bastion Host:** Public instance to SSH into, that has SSH connectivity to instances in private subnets
- **Site to Site VPN:** setup a Customer Gateway on DC, a Virtual Private Gateway on VPC, and site-to-site VPN over public internet
- **Direct Connect:** setup a Virtual Private Gateway on VPC, and establish a direct private connection to an AWS Direct Connect Location
- **Private Link / VPC Endpoint Services:**
  - connect services privately from your service VPC to customers VPC
  - Doesn’t need VPC peering, public internet, NAT gateway, route tables
  - Must be used with Network Load Balancer & ENI
- **ClassicLink**: connect EC2-Classic instances privately to your VPC
- **Transit Gateway:** AWS Transit Gateway connects VPCs and on-premises networks through a central hub

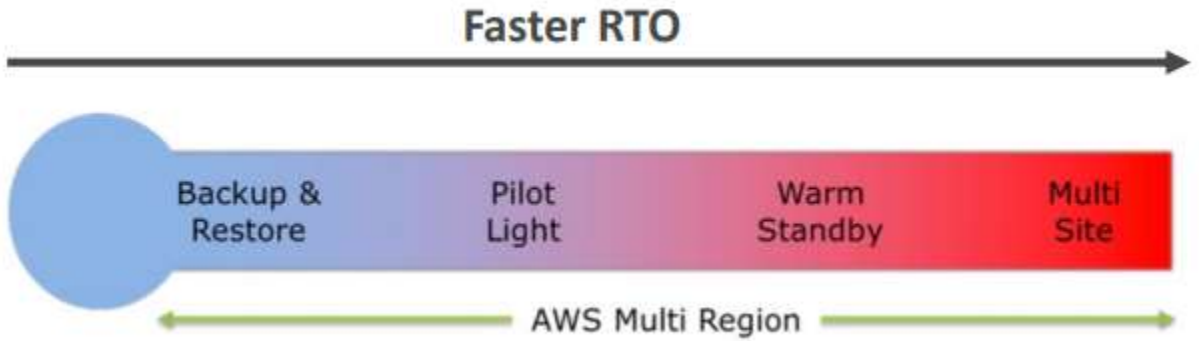
Disaster Recovery Overview

- Any event that has a negative impact on a company's business continuity or finances is a disaster
- Disaster recovery (DR) is about preparing for and recovering from a disaster
- What kind of disaster recovery?
  - On-premise => On-premise: traditional DR, and very expensive
  - On-premise => AWS Cloud: hybrid recovery
  - AWS Cloud Region A => AWS Cloud Region B
- Need to define two terms:
  - **RPO**: **Recovery Point Objective** (RPO is used for determining the frequency of data backup to recover the needed data in case of a disaster)
  - **RTO**: **Recovery Time Objective** (RTO is used to determine what kind of preparations are necessary for a disaster, in terms of money, facilities, telecommunications, automated systems, personnel, etc. The shorter the RTO, the greater the resources required.)



Disaster Recovery Strategies

- Backup and Restore
- Pilot Light
- Warm Standby
- Hot Site / Multi Site Approach



Disaster Recovery Tips

- **Backup**
  - EBS Snapshots, RDS automated backups / Snapshots, etc…
  - Regular pushes to S3 / S3 IA / Glacier, Lifecycle Policy, Cross Region Replication
  - From On-Premise: Snowball or Storage Gateway
- **High Availability**
  - Use Route53 to migrate DNS over from Region to Region
  - RDS Multi-AZ, ElastiCache Multi-AZ, EFS, S3
  - Site to Site VPN as a recovery from Direct Connect
- **Replication**
  - RDS Replication (Cross Region), AWS Aurora + Global Databases
  - Database replication from on-premise to RDS
  - Storage Gateway
- **Automation**
  - CloudFormation / Elastic Beanstalk to re-create a whole new environment
  - Recover / Reboot EC2 instances with CloudWatch if alarms fail
  - AWS Lambda functions for customized automations

Other Services

- **Technology Stack for CI/CD:**
  - CodeCommit
  - CodeBuild
  - CodeDeploy
  - CodePipeline

- **Infrastructure as Code**:
  - CloudFormation: Declarative way of outlining your AWS Infrastructure, for any resources (most of them are supported).

- **Amazon EMR:**
  - EMR stands for “Elastic MapReduce”
  - EMR helps creating Hadoop clusters (Big Data) to analyze and process vast amount of data

- **AWS Opsworks:**
  - Chef & Puppet help you perform server configuration automatically, or repetitive actions
  - They work great with EC2 & On Premise VM
  - AWS Opsworks = Managed Chef & Puppet

.

Other Services – Contd.

- **AWS Elastic Transcoder:**
  - **Convert media files (video + music)** stored in S3 into various formats for tablets, PC, Smartphone, TV, etc
  - Features: bit rate optimization, thumbnail, watermarks, captions, DRM, progressive download, encryption

- **AWS WorkSpaces:**
  - **Managed, Secure Cloud Desktop**
  - Great to eliminate management of on-premise VDI (Virtual Desktop Infrastructure)

- **AWS AppSync:**
  - Store and sync data across mobile and web apps in real-time
  - Makes use of GraphQL (mobile technology from Facebook)

- **Cost Explorer:**
  - Visualize, understand, and manage your AWS costs and usage over time
  - Create custom reports that analyze cost and usage data.
  - Analyze your data at a high level: total costs and usage across all accounts
  - Or Monthly, hourly, resource level granularity

Well Architected Framework

- 5 Pillars of AWS Well-Architected Framework Tool:
  - Operational Excellence
  - Security
  - Reliability
  - Performance Efficiency
  - Cost Optimization

- **Trusted Advisor:**
  - No need to install anything – high level AWS account assessment
  - **Analyze your AWS accounts and provides recommendation**

infostretch

Q & A

Thank you

CONNECT WITH US

EMAIL INFO@INFOSTRETCH.COM

CALL +1-408-727-1100

infostretch