**DATABASE**

instance store – temporary block-level storage for EC2 instance

object storage – each object consists of data, metadata, and a key

file storage – multiple clients can access data stored in shared file folders

Elastic Block Store (EBS) – provides block-level storage volumes to be used with EC2 instances. stores data within a single Availability Zone (same AZ that the EC2 instance uses)

EBS snapshot – an incremental backup that saves only the updated blocks of data

Simple Storage Service (S3) – stores data as objects in buckets

Elastic File System – scalable file system used with AWS Cloud services. uses multiple AZs

**Relational Database Service** (RDS) – managed rd that automates tasks such as hardware provisioning, db setup, patching, and backups.

relational database – data stored in a way it relates to other pieces of data

structured query language (SQL) – language to store and query data from RDS

Amazon RDS provides a number of different security options. ex encryption at rest (protecting data while it is stored) and encryption in transit (protecting data while being sent and received)

6 db engines available – Aurora, PostgresSQL, MySQL, MariaDB, Oracle Database, Microsoft SQL Server

Amazon Aurora – enterprise-class relational db. 5x faster than standard MySQL, 3x faster than Postgres. reduces unnecessary i/o operations. is highly reliable and available

Amazon DynamoDB – serverless, scaling, key-value db service

nonrelational database – use tables and key-value pairs. data is organized into items (keys) and each item has attributes (values)

Amazon Redshift – data warehousing service for big data analytics. collects data from many sources and helps to understand relationships and trends across data

AWS Database Migration Service (AWS DMS) – enables the migration of all dbs. move data between a source db and a target db.

used for Development and test db migrations, db consolidation, continuous replication

ElastiCache and DynamoDB Accelerator = caching solutions to speed up db reads. they add caching layers on top of the db to improve the read times of common requests

**SECURITY**

AWS shared responsibility model – AWS controls security of the cloud (data centers, services, etc) and customers control security in the cloud

Security In the Cloud – customers responsible for everything they create and put *IN* the cloud. manage security requirements for

* content – which you choose to store, which service you use, who has access
* access rights – how they are granted, managed, and revoked
* selecting, configuring, and patching the OS
* configuring security groups
* managing user accounts

Security Of the Cloud – AWS responsible for operation, management, and control of the components at all layers of infrastructure – host operating system, virtualization layer, physical security of data centers

* physical security of data centers
* hardware and software infrastructure (AWS Regions, Availability Zones, edge locations)
* network infrastructure
* virtualization infrastructure

AWS Identity and Access Management (IAM) - enables you to manage access to AWS services and resources securely in a flexible way via

* IAM users, groups, and roles
* IAM policies
* Multi-factor Authentication (MFA)

AWS account root user – first identity for creating AWS account. has complete access to all the AWS services and resources in the account. (shouldn’t be used for every day tasks)

IAM users – identity you create in AWS that represents the person/app that interacts with AWS services and resources. it consists of a name and credentials. It has no permissions by default. Should create individual IAM users for each person who needs to access AWS.

1. create an AWS account (root user)
2. create a IAM user and give it permissions to create other users
3. log in as the new IAM user and continue to create other users
4. only access the root user for a limited number of tasks

IAM policies – document that allows or denies permissions to AWS services. Enables the customization of users level of access to various resources. Follow the security of ‘least privilige’. Example – IAM policy allows ListObject and GetObject for bucket example-bucket-aws. (and owner attaches this policy to the

IAM groups – collection of IAM users. When you assign an IAM policy to a group, all users in the group are granted permissions specified by the policy.

IAM roles – identity you assume to gain temporary access to permissions. First the IAM user, app, or service must be granted permissions to switch to the role. Then after the switch, they abandon all previous permissions that had in their prior role. IAM roles are ideal for temporary access (not long term)

Multi-factor authentication – extra layer of security, requires 2 mores of authentication such as a phone

1. when a user signs in to AWS, they first enter IAM user ID and password
2. user is then prompted for authentication response from their AWS MFA device
3. user responds on cell phone or other device
4. user has been successfully authenticated and are able to access AWS services

AWS Organizations – to consolidate and manager multiple AWS accounts within a central location. It comes with a ***root***, aka the parent container for all accounts in the organization. also allows for consolidated billing

Service Control Policies (SCPs) – enable you to place restrictions on AWS services, resources, and individual API actions that users and roles in each account can access. For central control of permissions for all accounts in the AWS organization

Organizational Units (OU) - grouped accounts in AWS Orgs. Usually by similar business or security requirements. When a policy is applied to OU, all the accounts in the OU automatically inherit the permissions specified

AWS Artifact – service that provides on-demand access to AWS security and compliance reports and select online agreements. consists of

* AWS Artifact Agreements – agreement with AWS regarding use of certain types of information throughout AWS services. review, accept, and manage agreements for an individual account and for all accounts in an AWS organization (like HIPAA)
* AWS Artifact Reports – provides compliance reports from third-party auditors which test and verify that AWS is compliant with a variety of security standards and regulations.

Customer Compliance Center = contains resources to help learn about AWS compliance and how companies in regulated industries have solved various compliance, governance, or audit challenges. topis include AWS answers to key compliance questions, overview of AWS risk and compliance, and an auditing security checklist

DoS = denial-of-service attak. deliberate attempt to make an app unavailable to users

DDoS = distributed denial-of-service. An attack on the enterprise’s infrastructure with an army of zombie bots or multiple hackers. it shuts down the application’s ability to function by overwhelming the system.

AWS Shield – service that protects apps against DDoS attacks.

* AWS Shield Standard – automatically protects all AWS customers at no cost. protects against most common, frequently occurring types of DDoS attacks
* AWS Shield Advanced – paid service that pvodies detailed attack diagnostics and the ability ot detect and mitigate sophisticated DDoS attacks. Integrates with other services such as CloudFront, Route 53, and Elastic Load Balancing

AWS Key Management Service (KMS) – to perform encryption operations through the user of cryptographic keys. can control the use of keys across a wide range of services. You can choose the specific levels of access control that you need for your keys (like which IAM users and roles can manage keys). Also, you can temporarily disable keys

cryptographic key – random string of digits used for locking (encrypting) and unlocking (decrypting) data

AWS Web Application Firewall (WAF) – web application firewall that lets you monitor network requests that come into your web applications. Works together with CloudFront and a load balancer. Uses a web access control list (ACL) to protect resources. the web access control blocks specific IP addresses

Amazon Inspector – for performing automated security assessments. Improves security and compliance via checking applications for security vulnerabilities and deviations from security best practices. After an assessment, Inspector provides a list of security findings, prioritized by severity level, including a detailed description of each security issue and a recommendation on how to fix it.

Amazon GuardDuty – service that provides intelligent threat detection for your AWS infrastructure and resources. It identifies threats by continuously monitoring the network activity and account behavior. Detailed findings available in AWS Management Console including recommended steps for remediation. (Lambdas can be configured to automatically take remediation steps)

**MONITORING and ANALYTICS**

Amazon CloudWatch – web service that enables you to monitor and manage various metrics and configure alarms based on data from those metrics. CloudWatch uses metrics to represent the data points for your resources. AWS services send metrics to CloudWatch which uses them to create graphs displaying their performance. aka – CloudWatch allows you to monitor your AWS infrastructure and applications in real time.

CloudWatch alarms – automatically perform actions if the value of your metrics go above/below a predefined threshold. ex – create CloudWatch automatically stops unused EC2 instances

CloudWatch dashboard – enables you to access all the metrics for your resources in a single location. ie monitor CPU ulization of EC2 instance, requests made to S3 bucket, etc

AWS CloudTrail – records API calls for your account. a ‘trail’ of information like identity and IP address of API caller, time of the call, etc. Can filter the events to find a CloudTrail event

CloudTrail Insights – optional feature that automatically detects unusual API activities in AWS account

AWS Trusted Advisor – web service that inspects your AWS environment and provides real-time recommendations in accordance with AWS best practices. Checks 5 categories – cost optimization, performance, security, fault tolerance, and service limits. Trusted Advisor offers a list of recommended action in AWS management console. green check = no problems. orange triangle = number of recommended investigations. red circle = number of recommended actions.

**Billing**

consolidated billing = combine usage across accounts to receive volume pricing discounts

AWS Budgets = review how much cost your predicted AWS usage will incur for the month. set custom alerts when your usage exceeds (or will exceed) the budgeted amount

AWS Pricing calculator = create an estimate for the cost of your use cases on AWS

AWS Cost Explorer = visualize and manage your AWS costs and usage over time includes a default report of the costs and usage for your top 5 cost-accruing AWS services. can apply custom filters and groups to analyze your data like hourly resource usage levels

AWS Free Tier = program that consists of 3 types of offers that allow customers to use AWS services for free. Always free, 12 months free, and Trials

AWS Marketplace = digital catalog for software listings from independent software vendors. can use Marketplace to find, test, and buy software that runs on AWS

**MIGRATION AND INNOVATION**

AWS Cloud Adoption Framework (AWS CAF) - organizes guidance into six perspectives. each perspective (aka area of focus) addresses distinct responsibilities.

* Business – ensures IT aligns with business needs and that IT investments link to business results
* People – supports development of an organization-wide change management strategy for successful cloud adoption. used to evaluate organization structures and roles, new skill requirements, etc
* Governance – focuses on the skills and processes to align IT strategy with business strategy. maximize business value and minimize risks
* Platform – principles and patterns for implementing new solutions on the cloud and migrating on-premise workloads to the cloud
* Security – ensures that the organization meets security objectives for visibility, auditability, control and agility
* Operations – helps to enable, run, use, operate, and recover IT workloads to the level agreed upon. Define how day-to-day, quarter-to-quarter, business is conducted

6 Strategies for Migration

* rehosting – moves app without changes
* replatforming – moves app and make a few cloud optimizations
* refactoring/re-architecting – redo an app’s architecture and development using cloud-native features. used if business needs to add features, scale, or performance
* repurchasing – move from traditional license to software-as-a-service model
* retaining – keep critical apps in the source environment. maybe for apps that need to be refactored before they can be migrated
* retiring – remove apps that are no longer needed

AWS Snow Family – collection of physical devices that help to physically transport exabytes of data in and out of AWS. small to big – AWS Snowcone, AWS Snowball, AWS Snowmobile

serverless applications – apps that don’t need to be provisioned or maintained like AWS Lambda

artificial intelligence –

* Amazon Transcribe – convert speech to text
* Amazon Comprehend – discover patterns in text
* Amazon Fraud Detector – identify potentially fraudulent online activities
* Amazon Lex – build voice and text chatbots

machine learning – used to analyze data, solve complex problems, and predict outcomes. Amazon SageMaker can be used to build, train, and deploy ML models

AWS Well-Architected Framework – helps show how to design and operate reliable, secure, efficient, cost-effective, systems in AWS. provides a way to consistently measure your architecture against best practices and design principles and identify areas of improvement. Based on 5 pillars-

* *Operational Excellence* – ability to run and monitor systems to deliver business value. Design principles include performing operations as code, annotating documentation, anticipating failure, and frequently making small, reversible changes
* *Security* – ability to protect information systems and assets. Follows these best practices – automate security best practices, apply security at all layers, protect data in transit and at rest
* *Reliability* – ability of a system to recover from infrastructure or service disruptions, dynamically acquire computing resources to meet demand, and mitigate disruptions such as misconfigurations or transient network issues. includes testing recovery procedures, scaling horizontally to increase aggregate system availability, and auto recovery from failures
* *Performance Efficiency* – ability to use computing resources efficiently to meet system requirements. Includes experimenting more often, using serverless architecture, and designing systems to be able to go global in minutes
* *Cost Optimization* – ability to run systems to deliver business value at the lowest price point. Includes adopting a consumption model, analyzing and attributing expenditure, and using managed services to reduce the cost of ownership

Six Advantages of Cloud Computing

* trade upfront expense for variable expense
* benefit from massive economies of scale
* stop guessing capacity
* increase speed and agility
* stop spending money running and maintaining data centers
* go global in minutes

QUIZ

AWS Command Line Interface – tool to automate actions for AWS services through scripts

AWS GuardDuty – service that provides intelligent threat detection for AWS infrastructure

Amazon Augmented AI – provides built-in human review workflows for common machine learning use cases. Can also create own workflows for machine learnings models built on Amazon SageMaker

AWS Elastic Beanstalk – automatically handles the deployment details of capacity provisioning, load balancing, auto-scaling, and app health monitoring

check for TEKSystems

Anderson Contracting

Café Del Rio and Posados