AWS-SOLUTION ARCHITECT: Fastest Growing Public Cloud

**CERTIFICATION**:

Practitioner Tier: Certified Cloud Practitioner

Associate Tier: Certified Solutions Architect Associate, Certified Developer Associate, Certified

Sysops Admin Associate

Professional Tier: Certified Solutions Architect Professional, DevOps Professional

Specialty Tier: Advanced Networking, Big Data, Security, Machine Learning

**Exam Blue Print**:

1. 130 minutes in length
2. 60 questions (this can change)
3. Multiple choice
4. Results are between 100 – 1000 with a passing score of 720
5. Aim for 70%
6. Qualification is valid for 2 years
7. Scenario based questions

Google AWS Solution Associate Exam $150

Aws.training

Create aws certificate account

Schedule your exam

Opens psi exam website

From Surya Dai:

aws>awsguides>orionpapaer\_aws\_csa

Account & Services Layer-------------------------------------------------

The account and Services Layer represent how you create, access and

manage an AWS account and its services. From how you interact with

an AWS account and managing user rights, to how you access and use

various AWS services and features.

This layer is all about account management and managing services.

There are basically three type of users:

1. AWS Users (prod. account)

2. AWS Root Account Holder

3. AWS Users (dev. account)

These users connect to AWS INFRASTRUCTURE "CONTAINER" using ACCOUNT

CONNECTION TOOLS like AWS Console, ASW CLI AND AWS SDK. The connection

is of course via open internet.

The uses must go through IAM. There could be production account

and development account and cross account access between them.

On premises data centers can be connected to AWS INFRASTRUCTURE using

hybrid connection.

Root User:

The user created when you first create your AWS account is called root

user. Its credentials are the email and password used when signing up

your AWS account. The root user has FULL administrative rights and

access to every part of the account. Privileges cannot be revoked from

the root user.

Best practices for Root User:

You should not use the root user for daily work and AWS administration.

You should create a second user that has admin rights and sign in as

that user for daily work. You should always protect your root account

via MFA.

Customers uses web browser [front end/public access] to connect to

AWS. AWS users use Terminal (SSH, RDP) to connect (back end/private

access) to connect to AWS services. AWS services is in various regions

like us-east-1, us-west-1, ap-northeast-1, eu-central-1 and some other

Edge Location and Edge Cache.

AWS Users (prod. account):

This represents an AWS user that you may create (in IAM), who will

have varying degree of access to the "production" AWS account.

Permissions are controlled in IAM policies.

ACCOUNT CONNECTION TOOLS:-----------------------------------------

Console:

AWS Management Console generally referred as the console is the

browser interface (URL) used to interact with AWS. All the actions

done in the console are API calls.

CLI:

AWS CLI is text-based interface for accessing and adminstering AWS

resources. All commands executed using the CLI are API calls- and

require API Key Configuration.

SDK:

AWS Software Development Kits integrate AWS Services with your Custom

applications. All commands are API calls and require API Key

configuration. SKD automatically perform request signing. Some examples

of SDK are:

Xamrin, JavaScript, Java, iOS, Python(boto), .NET and many more.

AWS Well Architected Framework ---------------------------------------------------------------------------

The well architected framework is a series of best practice recommendations

And questions to ask when designing and developing cloud architectures.

Operational Excellence: Run and monitor systems to provider business value.

Design Principles: Perform operations as code, annotate documentation, make frequent,

Small, reversible changes, refine operations procedure frequently, anticipate failure

And learn from all operational failures.

Prepare, Operate, Evolve.

Amazon ElasticSearch Services: open source distributed search and analysis engine for log

Analysis, full text search and operational intelligence. Datasources: logstash, cloudwatch logs

Kinesis firehouse, kibana dashboards.

Reliability: Recover from failure and mitigate disruptions

Design Principles: test recovery procedures, automatically recover from failure, scale horizontally, stop guessing capacity, automate change

Foundations, Change Management, Failure Management.

Foundations: Key Services- IAM (Access Control), Amazon VPC (Isolated Networks),

Trusted Advisor (Service Limits), AWS Shield(DDOS Protection)

Change Management: Amazon CloudWatch (Control Access), AWS Config (Configuration

Awareness), AWS CloudTrail (Audit AWS APIS), Auto Scaling (Demand Management)

Failure Management:

AWS CloudFormation (Infrastructure as code), Amazon S3 (Durable backups), Amazon

Glacier (Durable Archives), AWS KMS (Reliable Key Management)

Recovery Time Objective: How long to recover

Recovery Point Objective: How much data is lost

Security: Protect and Monitor systems

Performance Efficiency: Use computing resources efficiently

Cost optimization: Avoid or eliminate unneeded expenses