

ACloudGuru Certification Course path for AWS Solutions Architect:

AWS Solutions Architect Associate – SAA-CO2

1. Designing resilient Architecture for Solutions Architects  
   Source: <https://learn.acloud.guru/course/2f2f600d-5ffe-4bd7-8406-fd04d29de611/dashboard>
2. Networking and Compute for Associate Solutions Architects  
   Source: <https://learn.acloud.guru/course/1ea506a0-9e59-461f-840b-d9ba1ce98d8d/dashboard>
3. Storage, Database, & Migration for Solutions Architects  
   Source: <https://acloud.guru/overview/cab21320-af77-4089-905b-cd91842b2998?_ga=2.188325743.697153314.1612792517-1559496533.1597531996>
4. High Availability & Scalability for Solutions Architects  
   Source: <https://acloud.guru/overview/59d0a824-d6b4-44aa-b37f-d8e32810b970?_ga=2.92000349.697153314.1612792517-1559496533.1597531996>
5. Application services for Associate AWS Solutions Architects  
   Source: <https://acloud.guru/overview/3cccfd2f-3a1a-434d-a1bf-f5312697f73a?_ga=2.150649841.697153314.1612792517-1559496533.1597531996>
6. Logging & Security for Associate Solutions Architects  
   Source: <https://acloud.guru/overview/af59ec1e-7cbf-4e2f-b13a-06ace26f9f0f?_ga=2.150649841.697153314.1612792517-1559496533.1597531996>

Supplemental course:

1. Architect Learning Plan  
   Source: https://explore.skillbuilder.aws/learn/learning\_plan/view/78/architect-learning-plan

# Read / Review / Practice

1. AWS Certified Solutions Architect - Associate Exam Guide
2. AWS Certified Solutions Architect - Associate Sample Questions
3. AWS Certified Solutions Architect - Associate Official Practice Question Set
4. Exam Readiness: AWS Certified Solutions Architect – Associate
5. Exam Readiness: AWS Certified Solutions Architect – Associate

## AWS Training for Solutions Architects

1. AWS Technical Essentials
2. AWS Power Hour: Architecting on-demand
3. Architecting on AWS

## AWS White Papers

1. AWS Well-Architected Framework

## FAQs

1. Amazon EC2
2. Amazon S3
3. Amazon VPC
4. Amazon Route 53
5. Amazon RDS
6. Amazon SQS

Source: <https://aws.amazon.com/faqs/>

# Graphical user interface, application, Teams Description automatically generated

# Designing resilient Architecture for Solutions Architects

## Course and Scenario Introduction

The organization you are working for, Scuba Syndrome, has decided to start moving to the cloud for all the benefits cloud computing offers. Scuba Syndrome particularly likes that AWS features a pay-as-you-go model, as they are tired of the wasted expense of over-provisioned resources and are interested in a more resilient and elastic architectural design.

As a solutions architect, you have been tasked to build out a new AWS environment for your organization with detailed requirements:

## Requirements

1. Create [principle of least privilege for all needed permissions].
2. Add an additional AWS security account – total of 3 different AWS accounts,
   1. a development account
   2. a production account
   3. a security account
3. build a multi-tiered VPC with a scalable, resilient design, and that's going to include our EC2 instances, database instances, et cetera
4. create a VPC peering connection between 2 of our AWS accounts.
5. create a WordPress blog for articles, our certification classes, and also to add highlights of our trips, and new equipment, et cetera.
6. Review possible connectivity options between our new AWS organization and our Scuba Syndromes on-premise data center.
7. review different storage options for our new AWS environment, along with data migration options that we could use to potentially move from our Scuba Syndromes on-premise data center into our new AWS environment.
8. add detailed logging and monitoring for our environment, so that costs and usage can be tracked.
9. add security - And this is going to be based on the principle of least privilege for AWS accounts and also the organization
10. use cost-effective options to make sure that AWS environment being designed and built is done with cost optimization.

## Cloud Computing Criteria

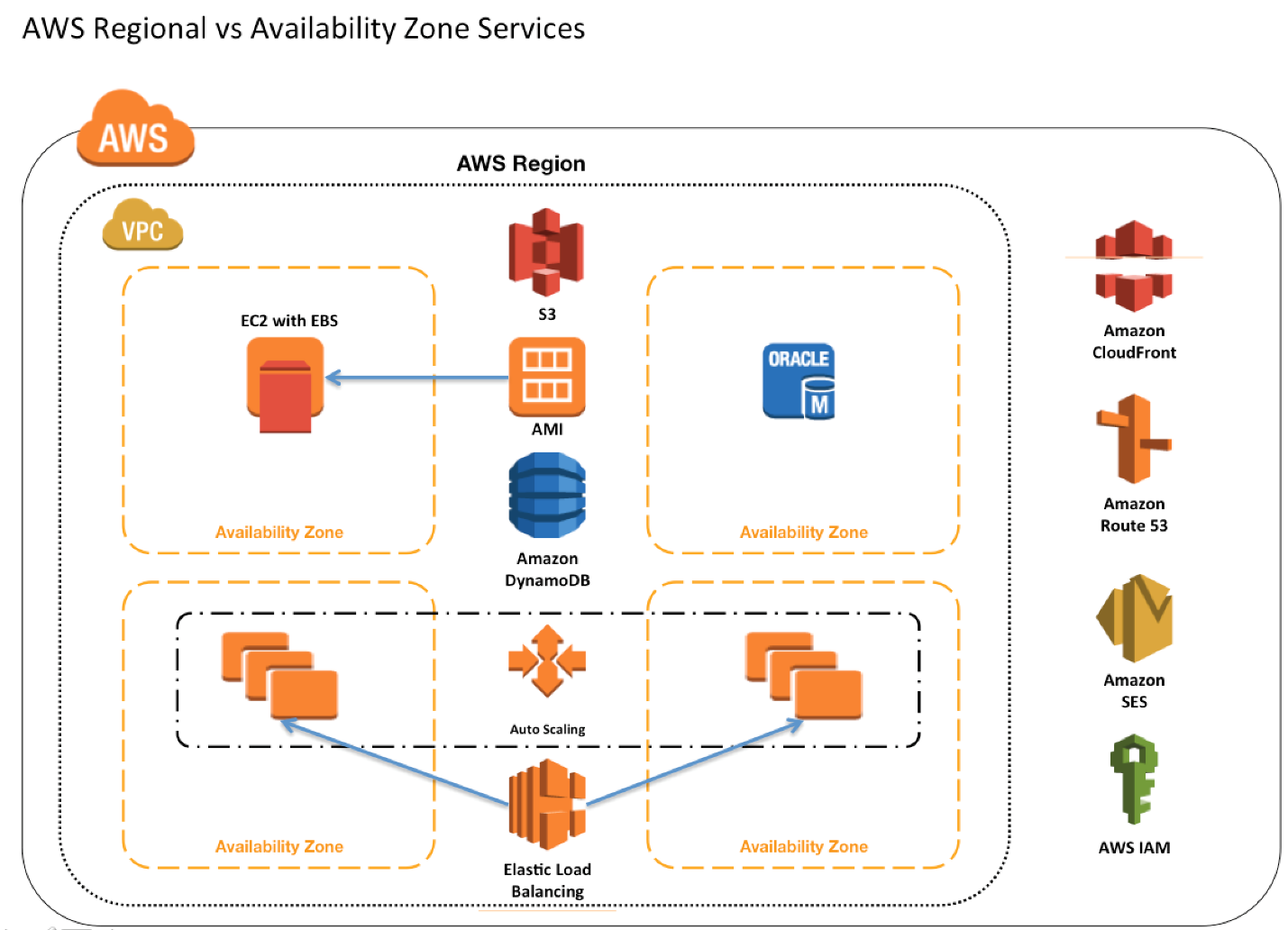
1. On-Demand Self Service  
   Provision and terminate services using the console or CLI with no human interaction
2. Network Access  
   Access services over any network and any device while using the standard methods and protocols
3. Resource Pooling  
   AWS economies of scale mean cheaper services
4. Elasticity  
   Scale up and down automatically in response to the demand or system load
5. Measure Service  
   Usage is measured, and you pay for what you use.

## Global Services - Scope

What AWS services have a global scope?

**AWS Certification Exam Practice Questions**

* IAM
* Amazon DynamoDB (already replicates across AZs)
* Amazon Elastic Compute Cloud (EC2)
* Amazon Elastic Load Balancing.
* Amazon Simple Notification Service (SNS) (Global Managed Service)
* Amazon Simple Storage Service (S3) (Global Managed Service)

[](https://www.google.com/search?rlz=1C1ONGR_enUS975US976&sxsrf=APq-WBt0V3wU9jCcUmHtRW4pZzjyhCbxvQ:1645243555238&q=What+AWS+services+have+a+global+scope?&tbm=isch&source=iu&ictx=1&vet=1&fir=WvSaY9k9WDZAnM%252CUhMQl-nMUtH4mM%252C_&usg=AI4_-kTAt-AFlglfDVutNwiPOI9rzuUkkA&sa=X&ved=2ahUKEwjJ27bt8Yr2AhWVFTQIHW_lA7wQ9QF6BAgtEAE" \l "imgrc=WvSaY9k9WDZAnM)

## Shared Responsibility Model and the AWS Well-Architected Framework

Graphical user interface

Description automatically generated

Source: <https://aws.amazon.com/compliance/shared-responsibility-model/>

Timeline

Description automatically generated

AWS responsibility “Security of the Cloud” - AWS is responsible for protecting the infrastructure that runs all of the services offered in the AWS Cloud. This infrastructure is composed of the hardware, software, networking, and facilities that run AWS Cloud services.

Customer responsibility “Security in the Cloud” – Customer responsibility will be determined by the AWS Cloud services that a customer selects. This determines the amount of configuration work the customer must perform as part of their security responsibilities. For example, a service such as Amazon Elastic Compute Cloud (Amazon EC2) is categorized as Infrastructure as a Service (IaaS) and, as such, requires the customer to perform all of the necessary security configuration and management tasks. Customers that deploy an Amazon EC2 instance are responsible for management of the guest operating system (including updates and security patches), any application software or utilities installed by the customer on the instances, and the configuration of the AWS-provided firewall (called a security group) on each instance. For abstracted services, such as Amazon S3 and Amazon DynamoDB, AWS operates the infrastructure layer, the operating system, and platforms, and customers access the endpoints to store and retrieve data. Customers are responsible for managing their data (including encryption options), classifying their assets, and using IAM tools to apply the appropriate permissions.

## AWS Well-Architected and the Six Pillars

1. Operational Excellence Pillar

The operational excellence pillar focuses on running and monitoring systems, and continually improving processes and procedures. Key topics include automating changes, responding to events, and defining standards to manage daily operations.

1. Security Pillar

The security pillar focuses on protecting information and systems. Key topics include confidentiality and integrity of data, managing user permissions, and establishing controls to detect security events.

1. Reliability Pillar

The reliability pillar focuses on workloads performing their intended functions and how to recover quickly from failure to meet demands. Key topics include distributed system design, recovery planning, and adapting to changing requirements.

1. Performance Efficiency Pillar

The performance efficiency pillar focuses on structured and streamlined allocation of IT and computing resources. Key topics include selecting resource types and sizes optimized for workload requirements, monitoring performance, and maintaining efficiency as business needs evolve.

1. Cost Optimization Pillar

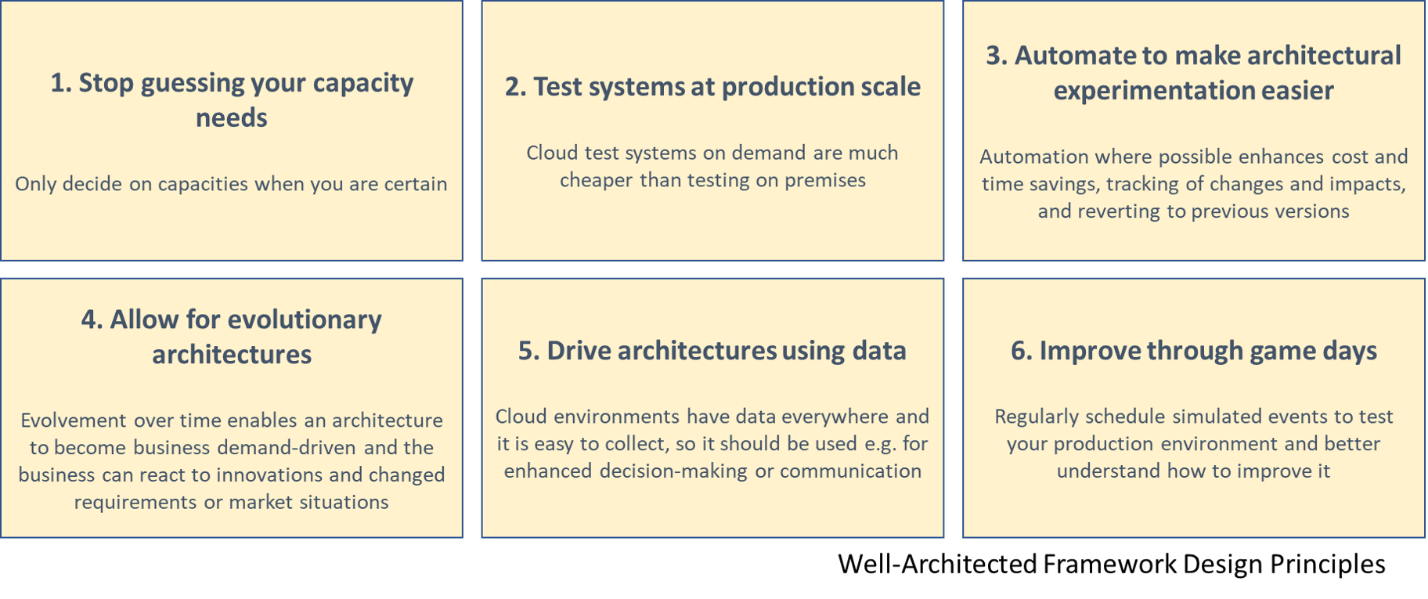
The cost optimization pillar focuses on avoiding unnecessary costs. Key topics include understanding spending over time and controlling fund allocation, selecting resources of the right type and quantity, and scaling to meet business needs without overspending.

1. Sustainability Pillar

The sustainability pillar focuses on minimizing the environmental impacts of running cloud workloads. Key topics include a shared responsibility model for sustainability, understanding impact, and maximizing utilization to minimize required resources and reduce downstream impacts.

Diagram

Description automatically generated



Diagram

Description automatically generatedDiagram

Description automatically generated