

# Introduction to Security & Architecture

## Guided Notes

I am excited that you are on the journey to get your AWS Certified Cloud Practitioner certification. This guided outline is meant to complement the video course. Here are a few tips to help you get the most out of these resources:

1. Print this out before you start the video course.
2. Follow along with the course and fill out areas in this document as you watch the course. You'll notice that the module names in the course are the bold headings here in these notes. In addition, clips in the module have their titles in this document too. Not all clips have notes.
3. Review your notes against the completed notes that can be found in the exercise files.
4. Keep this document after you finish the course as a part of the materials you will use to study for the exam.

Remember, this course is just the first step in your journey to achieve this certification. Follow along with the remainder of courses in this path, and then register for the exam.

Don't forget to reach out on [Twitter](#) and [LinkedIn](#) to let me know how you are doing along the way.

## AWS Architecture Core Concepts

### Learning Outcomes

- Policies and Models
  - Acceptable Use Policy
    - You should know what this policy covers and the types of things it doesn't allow
  - Shared Responsibility Model
    - You should be able to know what kind of areas are the responsibility of the custom and which are for AWS
- Well-architected Framework
  - Know the type of information included in the framework and how it could be useful
  - Know the different pillars of the framework
- High-availability and Fault Tolerance
  - Understand the difference between these terms
  - Know the services that can help enable these

### Helpful Links

- [AWS Acceptable Use Policy](#)
- [AWS Shared Responsibility Model](#)
- [Well-architected Framework](#)
- Services
  - [AWS Config](#)
  - [AWS Artifact](#)
  - [Amazon GuardDuty](#)

### Security and Architecture Overview

\_\_\_\_\_ AWS's policy for acceptable and unacceptable uses of their cloud platform. All users must agree with this policy to have an account on the platform.

Shared Responsibility Model

“\_\_\_\_\_ and \_\_\_\_\_ is a shared responsibility between AWS and the customer.” -- Amazon Web Services

AWS Responsibility	Customer Responsibility
Global data centers and underlying network	
	Operating system, network, and firewall configuration
Patching cloud infrastructure and services	

AWS Well-architected Framework

Pillars of the Well-architected Framework

1. \_\_\_\_\_ - Running and monitoring systems for business value
2. \_\_\_\_\_ - Protecting information and business assets
3. \_\_\_\_\_ - Enabling infrastructure to recover from

disruptions

4. \_\_\_\_\_ - Using resources efficiently to achieve business

value

5. \_\_\_\_\_ - Achieving minimal costs for the desired value

6. \_\_\_\_\_ - Minimizing environmental impacts for cloud

workloads

## High-availability and Fault Tolerance

Some services that support fault tolerance:

1. \_\_\_\_\_

## Compliance

Services that support compliance:

1. \_\_\_\_\_ - Continually monitor AWS resources and provides conformance packs for specific compliance standards
2. \_\_\_\_\_ - Portal that provides self-service access to compliance reports
3. \_\_\_\_\_ - Provides intelligent threat detection



## Scenarios

*The following scenarios are presented in the course as a way to explore your understanding of the module. Include your answer here in this outline, as well as your notes on the solution to each scenario.*

### SCENARIO 1

- Jane's company is building an application to process credit cards
- They will be processing cards directly and not through a service
- Their bank needs a PCI DSS compliance report for AWS
- Where would Jane go to get the information?

What's Your Answer: \_\_\_\_\_

Why did you pick this answer:

If you didn't get this one right, what insight did you gain from the explanation:

### SCENARIO 2

- Tim's company is considering a transition to the cloud
- They store personal information securely in their system
- Tim's CTO has asked what the company's responsibility is for security
- What would you tell Tim's CTO?

What's Your Answer: \_\_\_\_\_

Why did you pick this answer:

If you didn't get this one right, what insight did you gain from the explanation:

## SCENARIO 3

- Ellen is a solutions architect at a startup
- They are building a new tool for digital asset management
- Ellen is curious how to best leverage the capabilities of AWS in this application
- What resources would you recommend for Ellen and her team?

What's Your Answer: \_\_\_\_\_

Why did you pick this answer:

If you didn't get this one right, what insight did you gain from the explanation:

## Module Wrap Up

Take a minute to write down any areas from this module that you don't fully understand or where you still have questions:

## AWS Identities and User Management

### Learning Outcomes

- AWS Identity & Access Management (IAM)
  - Understand the purpose of the service
  - Know about the three different IAM identity types and know when you would use each one
  - Know about identity federation for IAM
  - Know about IAM best practices
    - Multi-factor Authentication
    - Least Privilege Access
- Amazon Cognito
  - Know about why you would use the service
  - Know about social logins with Cognito and supported identity providers

### Helpful Links

- [AWS Identity and Access Management](#)
- [Amazon Cognito](#)

### Summary

\_\_\_\_\_ When granting permission for a user to access AWS resources, you should grant them the minimum permissions needed to complete their tasks and no more.

## Introduction to AWS IAM

### AWS IAM Identities

*Please fill in the correct identities for the following descriptions:*



---

**Account for a single individual to access AWS resources**



---

**Allows you to manage permissions for a group of IAM users**



---

**Enables a user or AWS service to assume permissions for a task**

## Amazon Cognito

List the supported Cognito identity providers:

- 1.
- 2.
- 3.
- 4.
- 5.





## Scenarios

*The following scenarios are presented in the course as a way to explore your understanding of the module. Include your answer here in this outline, as well as your notes on the solution to each scenario.*

### SCENARIO 1

- Sylvia manages a team of DevOps engineers for her company
- Each member of her team needs to have the same access to cloud systems
- It is taking her a long time to attach permissions to each user for access
- What approach would help Sylvia manage the team's permissions?

What's Your Answer: \_\_\_\_\_

Why did you pick this answer:

If you didn't get this one right, what insight did you gain from the explanation:

### SCENARIO 2

- Edward works for a startup that is building a mapping visualization tool
- Their EC2 servers need to access data stored within S3 buckets
- Edward created a user in IAM for these servers and uploaded keys to the server
- Is Edward following best practices for this approach? If not, what should he do?

What's Your Answer: \_\_\_\_\_



Why did you pick this answer:

If you didn't get this one right, what insight did you gain from the explanation:

## SCENARIO 3

- William is leading the effort to transition his organization to the cloud
- His CIO is concerned about securing access to AWS resources with a password
- He asks William to research approaches for additional security
- What approach would you recommend to William for this additional security?

What's Your Answer: \_\_\_\_\_

Why did you pick this answer:

If you didn't get this one right, what insight did you gain from the explanation:

## Module Wrap Up

Take a minute to write down any areas from this module that you don't fully understand or where you still have questions:

## Data Architecture on AWS

### Learning Outcomes

- On-premise Data Services
  - Understand when you would use each of these
    - [AWS Storage Gateway](#)
    - [AWS DataSync](#)
- Be able to explain the different data processing services
  - [AWS Glue](#)
  - [Amazon EMR](#)
  - [AWS Data Pipeline](#)
- Be able to define and explain the different data analysis services
  - [Amazon Athena](#)
  - [Amazon Quicksight](#)
  - [Amazon CloudSearch](#)
- Be able to explain each of the following AI / ML services and its use
  - [Amazon Rekognition](#)
  - [Amazon Translate](#)
  - [Amazon Transcribe](#)

### Integrating On-premise Data

\_\_\_\_\_ - Hybrid-cloud storage service that integrates cloud storage into your local network.

#### AWS Storage Gateway Volume Types

*Please enter the name and brief definition of each volume type for AWS Storage Gateway:*

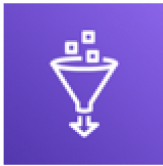
1.

2.

3.

\_\_\_\_\_ - Automated data transfer service that uses an optimized protocol for high-speed synchronization to the cloud

## Processing Data



**Managed Extract, Transform, and Load (ETL) Service**



**Big-data cloud processing using popular tools**



**Data workflow orchestration service across AWS services**

AWS Glue supports data in \_\_\_\_\_, \_\_\_\_\_, \_\_\_\_\_, and \_\_\_\_\_.

## Supported EMR Tools

*Enter the different open-source tools supported in Amazon EMR:*

- 1.
- 2.
- 3.
- 4.
- 5.
- 6.

AWS Data Pipeline integrates with \_\_\_\_\_,  
\_\_\_\_\_, \_\_\_\_\_,  
and \_\_\_\_\_.

Analyzing Data

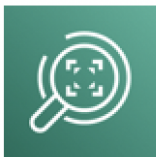
Data Analysis Services

Please enter the service name for each description:

Service Name	Description
	Service that enables serverless querying of data stored within Amazon S3 using standard SQL queries
	Fully managed Business Intelligence (BI) service enabling self-service data dashboards for data stored in the cloud
	Managed search service for custom applications

Integrating AI and Machine Learning

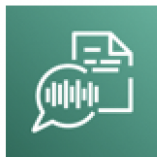
Enter the service names for the following ML services on AWS:



Computer vision  
service powered by  
Machine Learning



Text translation  
service powered by  
Machine Learning



Speech to text  
solution using  
Machine Learning



## Scenarios

*The following scenarios are presented in the course as a way to explore your understanding of the module. Include your answer here in this outline, as well as your notes on the solution to each scenario.*

### SCENARIO 1

- Ruth is a data scientist for a financial services company
- Large-scale data set needs to be processed before analysis
- Ruth doesn't want to manage servers but just wants to define processing
- What service would you recommend to Ruth?

What's Your Answer: \_\_\_\_\_

Why did you pick this answer:

If you didn't get this one right, what insight did you gain from the explanation:

### SCENARIO 2

- Jessi is a member of the IT team for a biotech company
- She is currently working to identify an approach for controlled lab access
- She wants leverage AI to determine access based on facial imaging
- Is there an AWS service that can help with this approach?

What's Your Answer: \_\_\_\_\_

Why did you pick this answer:

If you didn't get this one right, what insight did you gain from the explanation:

## SCENARIO 3

- Roger's company sells custom services around machine learning
- His head of sales is trying to find a great way to visualize their sales data
- This data is currently stored in Redshift as their data warehouse
- What AWS service would allow this access to the data by non-technical resources?

What's Your Answer: \_\_\_\_\_

Why did you pick this answer:

If you didn't get this one right, what insight did you gain from the explanation:

## Module Wrap Up

Take a minute to write down any areas from this module that you don't fully understand or where you still have questions:

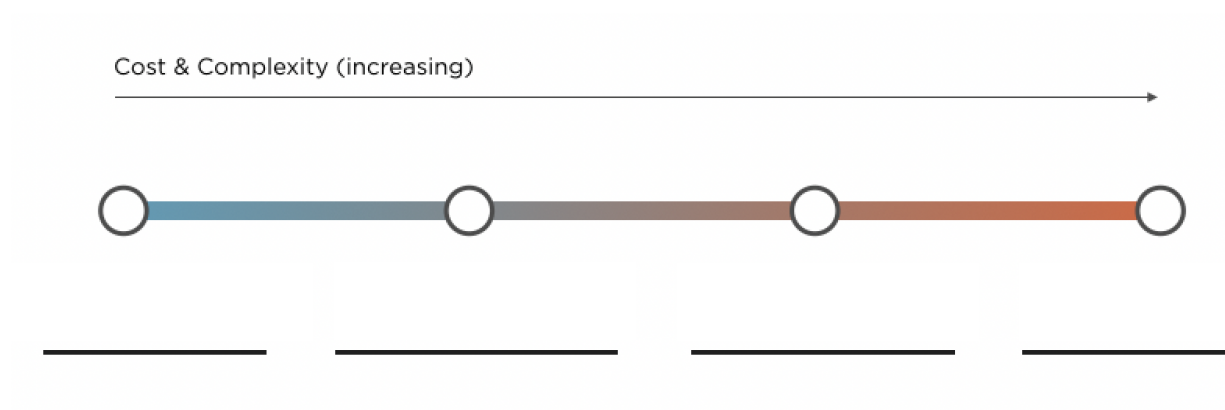
## Disaster Recovery on AWS

### Learning Outcomes

- Understand the four different recommended architectures for disaster recovery (DR)
  - Backup and Restore
  - Pilot Light
  - Warm Standby
  - Multi-site
- Be able to determine which approach makes sense for an organization based on RTO and RPO

### Disaster Recovery Architectures

Enter the correct names for each disaster recovery architecture:



### Selecting a Disaster Recovery Architecture

\_\_\_\_\_ - The time it takes to get your systems back up and running to the ideal business state after a disaster recovery event.

\_\_\_\_\_ - The amount of data loss (in terms of time) for a production system during a disaster recovery event.





## Scenarios

*The following scenarios are presented in the course as a way to explore your understanding of the module. Include your answer here in this outline, as well as your notes on the solution to each scenario.*

### SCENARIO 1

- Roger's company runs several production workloads in AWS
- Roger is tasked with architecting the disaster recovering approach
- His organization wants there to be a seamless transition during an event
- Which disaster recovery approach would Roger's company use for this?

What's Your Answer: \_\_\_\_\_

Why did you pick this answer:

If you didn't get this one right, what insight did you gain from the explanation:

### SCENARIO 2

- Jennifer's company is a startup
- They do not currently have a disaster recovery approach
- In this case, minimizing cost is more critical than minimizing RTO
- What disaster recovery approach would you recommend to Jennifer?

What's Your Answer: \_\_\_\_\_

Why did you pick this answer:

If you didn't get this one right, what insight did you gain from the explanation:

## SCENARIO 3

- Eliza is documenting her company's disaster recovery approach
- They keep a few key servers up and running in AWS in case of an event
- These servers have smaller instance types than what production would need
- Which disaster recovery approach most closely matches this scenario?

What's Your Answer: \_\_\_\_\_

Why did you pick this answer:

If you didn't get this one right, what insight did you gain from the explanation:

## Module Wrap Up

Take a minute to write down any areas from this module that you don't fully understand or where you still have questions:



## Architecting Applications on Amazon EC2

### Learning Outcomes

- Scaling EC2
  - Understand the difference between horizontal and vertical scaling
  - Explain services that support scaling
    - Auto-scaling groups
    - [Elastic Load Balancing](#)
- Limiting Access to EC2 Instances
  - Understand the different approaches for controlling access
    - Security Groups
    - ACL's
    - [AWS VPN](#)
- Know the AWS services that provide protection from hacks and attacks
  - [AWS Shield](#)
  - [Amazon Macie](#)
  - [Amazon Inspector](#)
- Understand the different ways to launch pre-existing experiences on EC2
  - [AWS Service Catalog](#)
  - [AWS Marketplace](#)
- Be able to define the different services in the suite of developer tools on AWS
  - [AWS CodeCommit](#)
  - [AWS CodeBuild](#)
  - [AWS CodeDeploy](#)
  - [AWS CodePipeline](#)
  - [AWS CodeStar](#)

### Scaling EC2 Infrastructure

\_\_\_\_\_ - You “scale up” your instance type to a larger instance type with additional resources

\_\_\_\_\_ - You “scale out” and add additional instances to handle the demand of your application

Fill in the notes on Auto-scaling Groups for EC2:

Amazon EC2 Auto-scaling Groups
Defines the minimum, maximum, and desired number of instances

\_\_\_\_\_ - Service that manages secrets (such as passwords, keys, tokens, etc...) used in your custom applications on AWS. It also supports auto-rotation of credentials on supported AWS services.

## Controlling Access to EC2 Instances

Fill in the solutions for limiting access to EC2 instances based on the included descriptions:

Solution	Description
	Enables firewall-like controls for resources within the VPC
	Controls inbound and outbound traffic for subnets within the VPC

	Secure access to an entire VPC using an encrypted tunnel
--	--

Indicate which of the following are characteristics of Security Groups and which are Network ACL's:

Security Group, ACL, or both	Characteristic
	Operates at the instance level
	Works for an entire subnet
	Multiple can be assigned to an EC2 instance
	Can be used to allow or deny traffic
	Controls inbound and outbound traffic

Protecting Infrastructure from Attacks

Fill in the names for the following security services:



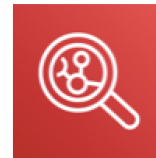
---

**Managed DDoS  
protection service for  
apps on AWS**



---

**Data protection  
service powered by  
machine learning**



---

**Automated security  
assessment service for  
EC2 instances**

## Deploying Pre-defined Solutions

\_\_\_\_\_ - Targeted to serve as an organizational service  
catalog for the cloud

\_\_\_\_\_ - Enables third-party ISV's to offer configurations  
for the cloud that can be launched in your account

## Developer Tools

*Fill in the following service names based on the description:*

Service Name	Description
	Fully managed source control service using Git

	Fully managed build and continuous integration service on AWS
	Fully managed deployment service for applications running on Amazon EC2, AWS Fargate, AWS Lambda, and on-premise servers
	Fully managed continuous delivery service on AWS for automating building, deploying, and testing. Integrates with other developer services
	Workflow tool for automatic creation of a continuous delivery pipeline for a custom application using the other developer services



## Scenarios

*The following scenarios are presented in the course as a way to explore your understanding of the module. Include your answer here in this outline, as well as your notes on the solution to each scenario.*

### SCENARIO 1

- Ellen is a solutions architect at a traditional financial services company
- They recently transitioned to AWS
- They want to be sure each department follows best practices
- They want to create compliant IT services that other departments can use
- What service would you recommend for Ellen and her team?

What's Your Answer: \_\_\_\_\_

Why did you pick this answer:

If you didn't get this one right, what insight did you gain from the explanation:

### SCENARIO 2

- Tim's company leverages AWS for multiple production workloads
- Recently they have had downtime due to one of their applications failing on EC2
- Tim is looking to avoid downtime if an instance stops responding
- What approach would you recommend for Tim to solve this issue?

What's Your Answer: \_\_\_\_\_





Why did you pick this answer:

If you didn't get this one right, what insight did you gain from the explanation:

## SCENARIO 3

- Jane's company deals with sensitive information from its users
- They have put reasonable policies in place for data stored in S3
- Jane is worried if some of those policies accidentally get changed
- She is also worried of a breach going unnoticed
- What service would you recommend to Jane and her company?

What's Your Answer: \_\_\_\_\_

Why did you pick this answer:

If you didn't get this one right, what insight did you gain from the explanation:

## Module Wrap Up

Take a minute to write down any areas from this module that you don't fully understand or where you still have questions:

## The Exam

Complete all of the courses in this path to prepare for your AWS Certified Cloud Practitioner exam. Once you are ready, follow the links below to register for the exam:

### Exam Links

- [Certified Cloud Practitioner - Exam Information](#)
- [Schedule an Exam](#)

### Stay in Touch

If you have questions along the way, feel free to reach out to **David Tucker** on Twitter ([@davidtucker](#)) or through [his website](#). Also, feel free to connect on [LinkedIn](#).

### For More Information

As a part of creating this course, the pages for each included service were referenced. For additional information, follow the links in this document to each service.