

# AWS

## Introduction to AWS for Non-Engineers

### All Study Breaks & Exam Tips

#### Module 1 – Cloud Concepts

##### **Study break: Reviewing cloud computing**

Welcome to the Study Break for cloud computing concepts that will come up in the AWS Certified Cloud Practitioner Exam.

The major concepts to remember are, the advantages of cloud computing over legacy on-premises IT infrastructure, cloud computing models, types of cloud computing deployments, and design principles of cloud computing, such as the as the Well-Architected Framework of a solid cloud computing IT infrastructure.

Let's start with the advantages of cloud computing over legacy on-premises IT infrastructure.

AWS calls these the six advantages of cloud computing. The advantages are:

1. trade capital expense for variable expense,
2. benefit from massive economies of scale,
3. stop guessing about capacity,
4. increase speed and agility,
5. stop spending money running and maintaining data centers, and
6. go global in minutes.

There are three cloud computing models and there are three cloud computing deployments.

The cloud computing models are:

1. Software as a Service, SaaS,
2. Infrastructure as a Service, IaaS, and
3. Platform as a Service, PaaS.

The cloud computing deployments are:

1. public cloud,
2. hybrid cloud, and
3. private cloud, otherwise known as on-premises cloud.

Finally, the Well-Architected Framework of cloud computing provides best practices framework for designing a stable, robust, and secure IT infrastructure on the cloud.

The five pillars of a Well-Architected Framework are,

1. cost optimization,
2. reliability,
3. operational excellence,
4. performance efficiency, and
5. security.

Knowing these concepts and models could mean a few extra points on the exam which could go a long way in securing you the certification. Most importantly, the six advantages of cloud computing comes up again and again in the exam, so it's well worth your time to make sure you know what these phrases mean in layman's terms.

## **Study break: Exam tips and resources**

We began this course with what even is the cloud? Since then, we've come a long way. Let's get prepped for the exam. We've learned about the cloud, cloud computing, Amazon Web Services, and various but essential cloud computing concepts to help begin the preparation process for the AWS Certified Cloud Practitioner Exam. We will review major concepts you should know about for the AWS Certified Cloud Practitioner Exam's Cloud Concepts domain. These topics are, what is AWS, six advantages of cloud computing, three cloud computing models, three cloud computing deployments, and five pillars of a Well-Architected Framework. We will also throw in some study tips for memorizing certain concepts in preparation for the exam. Let's get started.

The AWS Certified Cloud Practitioner Exam is the most fundamental certification exam that AWS offers to help validate the candidate's overall fundamental understanding of the AWS Cloud. It includes four domains which are:

1. Cloud Concepts,
2. Security,
3. Technology, and
4. Billing and Pricing.

We began with Cloud Computing and then went over to the Cloud Concepts domain. For the Cloud Concepts domain part of the exam, AWS wants you to *define* the AWS Cloud and its value proposition, *identify* aspects of AWS Cloud economics, and *list* the different cloud architecture design principles.

AWS, or Amazon Web Services, is a cloud computing platform created by Amazon and currently holds the world's highest market share in the cloud computing sphere. It provides

many different IT services on the cloud and helps to make it easier, faster and cheaper to run your IT infrastructure compared with legacy on-premises IT infrastructure.

According to AWS, there are six distinct advantages of utilizing cloud computing over on-premises IT infrastructure. The advantages are:

1. trade capital expense for variable expense,
2. benefit from massive economies of scale,
3. stop guessing about capacity,
4. increase speed and agility,
5. stop spending money running and maintaining data centers, and
6. go global in minutes.

Basically, utilizing cloud computing is faster, cheaper, and more agile than utilizing your own data centers.

There are three types of cloud computing models and three types of cloud computing deployments. The three types of cloud computing models are:

1. Software as a Service, SaaS,
2. Infrastructure as a Service, IaaS, and
3. Platform as a Service, PaaS.

The three types of cloud computing deployments are:

1. Public Cloud,
2. Hybrid Cloud, and
3. Private or On-Premises Cloud.

Want the way to memorize them? Try out my silly memorization method, SIP PHO.

SIP is an acronym for the three cloud computing models, Software as a Service, Infrastructure as a Service, and Platform as a Service.

PHO stands for the cloud computing deployment models, Public, Hybrid, and On-Premises or Private Cloud.

There are five pillars of a Well-Architected Framework. They provide best practices for specific areas of running an AWS Cloud IT infrastructure. To help me memorize these five pillars, I created the acronym CROPS.

The pillars are, Cost Optimization, Reliability, Operational Excellence, Performance Efficiency, and Security, CROPS.

## Module 2 – Security

### Study break: Security domain

What are the differences between security in the Cloud and security in an on-premises data center? Security in the Cloud may look a little different, and include some added benefits. Let's review the security domain of the AWS Certified Cloud Practitioner Exam together. Some topics we'll be covering are the security in the Cloud, Shared Responsibility Model, security pillar of the Well-Architected Framework, Principle of Least Privilege, and AWS Cloud Compliance. Let's go.

One of the biggest benefits of utilizing Cloud computing is that you no longer have to purchase equipment and maintain your own data center to run IT resources. Cloud computing providers like AWS manage the data centers so you can focus on other aspects of IT infrastructure management. When you deploy to the AWS Cloud, you benefit from the global network of data centers and architecture built with security in mind. There are dozens of compliance programs embedded into AWS to help you meet your industry's compliance requirements. AWS is designed to keep your data safe, no matter how big or small your Cloud usage is, so you are free to scale your business as quickly as you want.

There are three major concepts that outline AWS' recommended security practices.

These are:

1. the Shared Responsibility Model,
2. the Security Pillar of a Well-Architected Framework, and
3. Principle of Least Privilege.

In addition, we will review how AWS accounts for compliance requirements for data and resources stored in the Cloud. The first concept addresses the question who is responsible for security? The answer is slightly complex. You, as the consumer, are responsible for security in the Cloud. AWS, as the Cloud computing service provider, is responsible for security of the Cloud. This concept is called the Shared Responsibility Model, and it asserts that the security of the data and resources in the Cloud is a shared responsibility between the Cloud computing service provider and the customer. While the customer no longer has to worry about certain aspects of IT infrastructure, like securing the physical data center or hardware, there are other aspects that they are still responsible for, including patching virtual service regularly, and utilizing proper permission sets so only people who should be accessing certain resources, do access them.

Next, AWS addresses how can you best protect your AWS Cloud infrastructure from both internal and external security threats? AWS has the five pillars of a Well-Architected Framework to help it's customers build the most secure, fault resilient, efficient, and high performing IT infrastructure possible.

Within the five pillars, there is the security pillar, which outlines how you can secure your infrastructure adhering to best practices.

Security in the Cloud is composed of five areas:

1. Identity and Access Management,
2. Detective Controls,
3. Infrastructure Protection,
4. Data Protection, and
5. Incident Response.

Architecting a Well-Architected Framework can go a long way to making your IT infrastructure stable and secure.

Next is Principle of Least Privilege. What resources should you provide access to? The Principle of Least Privilege states that you should only be providing access to resources that an entity requires to do its job. Every role has a set of access permissions necessary to effectively execute its job, and the resources and individuals should have no more or no less than the optimal level of access.

In AWS, you would make this happen by using a service called Identity and Access Management, or IAM, providing granular access permissions. Providing the minimum amount of access to entities to complete their work is a vital way to keep your IT infrastructure secure. The Principle of Least Privilege coincides with the Shared Responsibility Model, where the customer, you, are responsible for security in the Cloud by making sure access is provided responsibly.

Lastly, here are many AWS Cloud Compliance programs available to help you determine if your industry allows you to store data on AWS. Many industries have compliance requirements for storing your data, such as HIPAA for medical organizations. You can learn more about the various compliance programs AWS offers by visiting [aws.amazon.com/compliance](https://aws.amazon.com/compliance). In the security domain of the AWS Certified Cloud Practitioner Exam, AWS wants you to be able to explain what concepts like the Shared Responsibility Model and Principle of Least Privilege may mean in real life scenarios.

## **Study break: Reviewing security services**

Let's review the security related services that may be relevant to the AWS Certified Cloud Practitioner exam. The security services we will be reviewing in this video are:

- AWS Identity and Access Management or IAM,
- AWS Web Application Firewall or WAF,

- AWS Shield,
- Amazon Inspector,
- AWS Trusted Advisor, and
- Amazon GuardDuty.

First, AWS Identity and Access Management, more commonly referred simply as IAM, is a free service that enables you to securely manage access to services and resources in the AWS cloud. The permission sets are extremely granular, helping you allow or deny access by users or other services to various resources. You can set access by using IAM to manage users utilizing granular permission sets. You could also create and manage IAM roles which has specific permission sets. You can allow entities to assume a role to do specific actions in your AWS cloud instance. In this way, you don't have to manually set up every entities permission sets, which could result in human errors and inconsistencies. Finally, you can enable identity Federation, which will allow existing identities in your enterprise accounts. Many organizations allow identity Federation for their Microsoft active directory. Allowing employees to access their AWS cloud instance without having to create a new IAM user for every single employee. IAM allows you to have enhanced security, granular control over permission sets, ability to provide temporary credentials, flexible security credential management, inability to utilize identity Federation.

Second, the AWS Web Application Firewall of WAF, is as it sounds. A firewall service for web applications running on AWS cloud. It protects web apps from common web exploits as well as potential compromises that could force your apps to consume excessive AWS resources, which could be detrimental to your finances. It improves web traffic visibility, provides cost-effective web application protection and delivers increased security against web attacks. It's an affordable protection for your web applications that can be deployed within minutes.

Another security service is AWS Shield, which can protect your web applications from a distributed denial of service or DDoS attack. It provides detection and automatic mitigation of DDoS attacks to applications, helping you minimize the negative consequences and application downtime. There are two tiers available for customers. The standard tier is automatic, free and protects web apps against majority of common DDoS attacks. The shield Advanced tier provides 24/7 access to AWS DDoS response team and detects and mitigates sophisticated DDoS attacks with near real time visibility into events. And even provides financial protection against DDoS-related spikes in AWS resource usages. You can receive comprehensive DDoS protection catered around your budget and needs with AWS shield.

Next, the Amazon Inspector is an automated security assessment service for your AWS applications, which helps you improve security and compliance. It inspects your applications automatically assessing them for exposure, vulnerabilities, and derivations from best practices. After an assessment is completed, it generates detailed reports to help you check for vulnerabilities. Utilizing Amazon Inspector helps to reduce the risk of introducing security issues by proactively identifying potential security vulnerabilities that do not align with

best practices and policies. You can define your own standards to check against and create reports that validate that specific tests were performed. You can continue enforcing best practices within your AWS cloud infrastructure. What the help of AWS has constantly updated standards made available through inspector.

Another crucial security service is the AWS Trusted Advisor, AWS trusted advisor guides provisioning of resources to AWS cloud. So you're following AWS best practices. As the name suggests, it advises you on how your infrastructure is or is not following AWS best practices based on five categories; Optimization, Performance, Security, Fault tolerance and Service limits. It then offers recommendations to bring your infrastructure closer to standards. The Seven core Trusted Advisor checks are free and those with Business Support plans and above have access to Full Trusted Advisor checks. AWS trusted advisor provides customized recommendations based on proactive monitoring to make sure your AWS cloud deployments are aligned with best practices.

Lastly, Amazon GuardDuty is a threat detection service that monitors for malicious activity and unauthorized behavior 24/7. Utilizing machine learning, anomaly detection and integrated threat intelligence. GuardDuty identifies and prioritizes potential threats that may impact your AWS infrastructure. It's deployable with just a few clicks and helps you take action immediately against the threat. It works as a 24/7 monitoring solution to help your human infrastructure team get a good night's rest. So, this was a quick study break review of the security related services AWS offers to help protect your cloud infrastructure.

## **Study break: Exam tips and resources**

We will be going over contents that will be relevant to the security domain of the AWS Certified Cloud Practitioner exam. We will go over the shared responsibility model, principle of least privilege, security pillar of a Well-Architected Framework, and the security services. Let's get started.

The security domain is concerned with how to make sure your IT infrastructure hosted on AWS Cloud, is safe from both internal and external security threats. There are a few concepts related to this, such as the shared responsibility model, the security pillar of the Well-Architected Framework, and the principle of least privilege.

In the shared responsibility model, the most important concept to understand is that you as the customer, and AWS as the cloud computing service provider, share the responsibility of keeping AWS Cloud secure. Customers are responsible for security in the cloud and AWS is responsible for security of the cloud. How do you make sure you're keeping the information in the cloud secure? You should only provide the least amount of access possible for any entity to make sure

that no one has access to resources they are not entitled to. This concept is called the principle of least privilege.

Finally, the security pillar of the Well-Architected Framework states that the security of the cloud is composed of identity and access management, detective controls, infrastructure protection, data protection, and incident response. We also went over a few core security related AWS services such as AWS Identity and Access Management, or IAM, AWS Web Application Firewall, or WAF, AWS Shield, Amazon Inspector, AWS Trusted Advisor, and Amazon GuardDuty. You should be familiar with what each of these services do and how they contribute to helping keep AWS Cloud secure. A few extra minutes making sure you have the services or concepts straightened out could mean a few extra points on the certification exam.

## Module 3 – Core Services

### Study break: Reviewing compute services

In this chapter, we went over five of the major compute services in AWS:

1. Amazon Elastic Compute Cloud, or EC2,
2. Amazon Elastic Beanstalk,
3. Elastic Load Balancing,
4. AWS Lambda and
5. Amazon Lightsail.

Let's quickly review all of them to make sure we've got the fundamental concepts down before moving on.

Amazon Elastic Compute Cloud, more commonly referred to as Amazon EC2, is a virtual server hosted on AWS cloud. You can instantly launch applications and servers wherever you want with an extremely versatile range of capabilities. It is one of the most widely used services in AWS and you can spin up an instance with no upfront financial commitments.

AWS Elastic Beanstalk helps you deploy and scale web applications by simply uploading your code. It handles the deployment process like capacity provisioning, load balancing, auto-scaling, and application health monitoring so you and your team can focus on coding. You can upload code in many of the popular programming languages like PHP, Node.js, and python. And you can retain full control over the underlying resources at all times. Better yet, it's free. You only pay for the AWS resources utilized as a result of deploying the code.

Elastic Load Balancing helps your application achieve fault tolerance by ensuring scalability, performance, and security. They can monitor the health of your servers, and if one goes down, it can reroute incoming web traffic to healthy servers. Elastic Load Balancers are highly available, secure, flexible, and monitorable which means you can feel confident that your



applications are up at all times and even get insightful information about web traffic going to your applications.

AWS Lambda runs code called a lambda function in response to an event. An event could be someone uploading an image into your application, or someone visiting a specific web page. When an event happens, your code runs. Instead of having to spin up and maintain servers to take care of set events, lambda allows you to deploy the lambda function and only charges you for the time your code spends running in each event trigger. No servers to provision, manage, or scale. Lambda functions can be up and running with just a few clicks, saving you tons of time.

You can think about Amazon Lightsail as a EC2 on bumper bowling mode. AWS provides many preconfigured and ready to use operating systems, web applications, and development stacks to help you get your applications or websites up and running with minimal configurations. When you want to focus on launching and creating instead of configuring and managing your virtual servers, Amazon Lightsail might be the better option to you over Amazon EC2. It's a snap to spin up a virtual server, but the servers are still designed to scale with you with cost effective monthly fees. Some popular resources available to you are Word Press, Windows OS, Ubuntu, and Node.js. With a one click to launch service like Amazon Lightsail, there's no real excuse to not get your project up and running on the cloud.

Of the services we went over, AWS Elastic Beanstalk and AWS Lambda are what we consider infrastructure as code because they allow us to deploy resources to the cloud using code. There are three ways to deploy to the AWS cloud:

1. The AWS Management Console,
2. AWS Command-Line Interface, or CLI, and
3. AWS Software Development Kits, or SDKs.

Finally, AWS has a global infrastructure. They have independent data centers called Availability Zones. Two or more Availability Zones make up a Region. Your AWS cloud infrastructure is generally hosted in a Region closest to your organization's physical location. By creating redundancy by replicating your resources in multiple Availability Zones or Regions, you can create an infrastructure that is resilient to natural disasters and highly available.

## Study break: Reviewing storage services

In this chapter, we run over four of the major storage services in AWS:

1. Amazon Simple Storage Service or S3,
2. Amazon Elastic Block Store or EBS,
3. AWS Snowball, and
4. AWS Storage Gateway.

Let's quickly review all of them to make sure we've got the fundamental concepts down before moving on.

Amazon Simple Storage, more commonly known as Amazon S3, is an object storage service, which you can conceptualize like storing each file as an individual object, like you would in your My Documents folder. It's designed for scalability, data availability, security, and performance, and is used in industries of all sizes. There are many storage classes available to fit every organizations budget and needs. You can even set up S3 lifecycle policies which will automatically transfer files from one storage class to a cheaper one after a certain number of days. You can use S3 for a variety of needs whether it's for hosting images your users upload to your web app as your as inexpensive backup solutions.

In contrast, Amazon Elastic Block Store or EBS is a block storage service while S3 stores files individually as objects, Amazon EBS stores them as blocks. They're not a 100% accurate representation, you can think of it like making a zip file of your Christmas holiday photos and sharing that zip file with a friend. They can't just download a portion of the zip file, they have to download the whole thing to unzip it and see your individual photos. Amazon EBS behaves like raw, unformatted block devices, which can be attached to your EC2 instances to expand your server storage. Think about an external hard drive that helps you up your laptop storage capacity. Amazon EBS is scalable, durable, and reliable storage option to make sure you always have enough storage available for all of your applications and servers.

AWS Snowball is one of the very few hardware services AWS offers. It's a data migration tool that can also function as a storage service. When you begin using AWS Snowball, AWS will actually ship you a physical Snowball to move your data onto. Once you finish moving the data onto Snowball, you mail it back and AWS will migrate the data onto Amazon S3 for you. The amount of data you can transfer to AWS cloud at one time using this service ranges from 50 gigabytes with a regular Snowball to up to 100 petabytes with a Snowmobile, a 45 foot long shipping container pulled by a semi-trailer truck. Why bother with a physical device? Because transferring such large amounts of data over the internet will take a lot of time. By moving the data to a physical device and then shipping it to AWS to upload to S3 on their end, you can save a lot of time, bandwidth and even money.

AWS Storage Gateway is a hybrid storage solution for your IT infrastructure providing both low latency for file access and benefit of cost and time saving with cloud computing. It is a gate that

connects your onsite users and devices to resources stored in the AWS cloud with minimal latency, and offers three types of storage solutions to fit your needs, file gateway, tape gateway, and volume gateway, all addressing different kinds of needs. In the most fundamental sense, the difference in the three gateways is where you want to keep the complete copy of your data, onsite or on the cloud. There was a lot to unpack with the storage services. They all store things for you in the cloud, but they all have different uses in different ways of getting your data there.

## **Study break: Reviewing database services**

In this chapter, we went over four of the major database services in AWS.

1. Amazon DynamoDB,
2. Amazon Relational Database Service, or RDS.
3. Amazon Aurora, and
4. Amazon Redshift.

Let's quickly review all of them to make sure we've got the fundamental concepts down before moving on.

Amazon DynamoDB is a fast, flexible, fully managed and secure non relational, or NoSQL. Database, that can handle more than 10 trillion requests per day, and support peaks of more than 20 million requests per second. It's serverless, so you don't have to provision, patch or manage any servers, and it automatically scales up or down, to adjust for capacity. Instead of worrying about managing your database, you can just worry about scaling your application.

Amazon relational database service, or Amazon RDS is a fully managed relational database, because it's fully managed, like Amazon DynamoDb. You don't have to provision, or manage any servers. Instead of spending your time doing administrative tasks, you can devote your time to working on your products. You have six database engines to choose from. Amazon Aurora, PostgreSQL, MySQL, MariaDB, Oracle database, and SQL Server.

We just mentioned Amazon Aurora, as one of the database engines you can use with Amazon RDS. Amazon Aurora is fully managed by Amazon RDS, and it's MySQL and PostgreSQL compatible. You can get the same security, availability and reliability of commercial databases, but for faster and cheaper.

Amazon Redshift is a cloud based, fully managed, petabyte-scale data warehouse service, that's faster and cheaper than other data warehouse providers. Data warehouses store extremely large amount of data, collected from a wide range of sources to analyze. It is quick to set up, and easy to scale, and its encryption, is compliant with many industry regulations.

Databases, databases. You may not be very familiar with databases, which could make trying to decipher these options a little more difficult.

Amazon DynamoDB, is a non relational or NoSQL database.

Whereas Amazon RDS, and Amazon Aurora, are relational databases.

Amazon Redshift, is a data warehouse for lots and lots of data.

All are scalable, secure, and less expensive than industry alternatives. If you want to review any of the databases, feel free to take a few minutes, going over to videos.

## **Study break: Network and content delivery**

In this chapter, we went over three of the major network and content delivery services in AWS. Amazon Virtual Private Cloud or VPC, Amazon CloudFront and Amazon Route 53. Let's quickly review all of them to make sure we've got the fundamental concepts down, before moving on.

Amazon Virtual Private Cloud or VPC is an isolated corner of AWS Cloud made just for you. You can provision your AWS resources into a virtual network that you define with complete control over your virtual networking environment. From IP address range, to configurational route tables, and network gateways. It's free, and it's automatically created for you when you create your AWS account. Inside your very own Amazon VPC, you can create and scale your AWS Cloud resources to your heart's content.

Amazon CloudFront is a content delivery network or CDN. The main purpose of CDNs is to make websites and applications load faster. Amazon CloudFront achieves this by using Edge Locations all around the world to cache files and resources for quicker retrieval. By caching, say a video, at an Edge Location in Sydney Australia, someone who lives in Australia can stream the video much quicker than if there was no content delivery networks. Because they would have to download the video all the way from the content origin, which could be anywhere in the world. Amazon CloudFront sees where you're based and routes your traffic to the closest cache location. So you can enjoy the content without having to wait. It's scalable, and you only pay for content delivered using the service.

Amazon Route 53 sounds like a highway, and in a sense, it is kind of like a highway. If highways help take you from here to there, it is a highly scalable domain name system or DNS. It allows you to route your users to your internal applications. This could be in form of your users accessing infrastructure running on AWS, like an EC2 instance. It's basic functions are: domain registration, Domain Name System or DNS, health checking of web applications' accessibility, and auto-naming for service discovery. It helps route your users to the appropriate resources you want them to access.

AWS's networking content delivery services mainly occupy themselves with helping you create secure networks for your resources to live within, and to route traffic to proper services.

## **Study break: Reviewing management tools**

In this chapter, we went over three of the major management tools in AWS. [AWS CloudFormation](#), [AWS CloudTrail](#), and [Amazon CloudWatch](#). Let's quickly review all of them to make sure we've got the fundamental concepts down before moving on.

AWS CloudFormation allows you to create a recipe for spinning up identical setups for a collection of resources and services for your IT infrastructure. It's free to use and you only pay for the resources you utilize by building a project on CloudFormation. It utilizes infrastructure as code, and you can deploy IT infrastructure based on a text file filled with code that specifies configurations for all of your services and resources. Once that's created, CloudFormation does the actual configurations and deployment for you. You can continue to build out your resources without having to worry about human error and configurations.

AWS CloudTrail can log monitor account activities, provide event history of account activities, simplify compliance audits, discover and troubleshoot security and operational issues, provide visibility into user and resource activities and track and automatically respond to security threats within your AWS infrastructure. And in that show, it's an event tracker and security analysis tool that helps keep your AWS cloud infrastructure compliant and secure.

Amazon CloudWatch helps you gain system wide visibility into resource utilization, application performance and operational health. It collects monitoring and operational data as logs, metrics and events and provides insight into your application performance. You can even set up CloudWatch alarms to automatically make changes using predefined triggers to automatically solve common issues. It's integrated with nearly 70 AWS services helping your team keep comprehensive monitoring data 24 seven.

Now you might be thinking CloudTrail, CloudWatch, what's the difference?

AWS CloudTrail audits logs.

Amazon CloudWatch monitors and can react to changes.

Need access logs because someone did something they shouldn't have, CloudTrail.

Need to know how much CPU on EC2 instance is using, CloudWatch.

Imagine a detective trailing a trail of footprints for CloudTrail.

CloudWatch is watching or monitoring to make sure your resources are functioning as they should be.

AWS's management tools help you build and manage your AWS cloud infrastructure.

## Study break: Exam tips and resources

We went over quite a lot of information in a very short period of time. We'll be reviewing compute, storage, database, network and content delivery and management tools and services.

And we'll also be reviewing concepts like infrastructure as code, deploying on the AWS cloud and availability zones and regions. As mentioned, we covered a lot of services in this course and many of their names are pretty confusing. I'm going to help you create a study cheat sheet so you can refer to it as you study for the exam.

Having a couple words that describe each service will make it easier for you to jog your memory when you're a little unsure about what the specific service does. Here we go.

Let's begin with compute services.

Amazon EC2 or elastic compute cloud is a virtual server.

Amazon Elastic Beanstalk helps you automatically grow your applications to meet demands, like Jack's beanstalk growing and growing.

Elastic Load Balancing balances incoming traffic loads.

AWS Lambda allows you to run serverless code.

AWS Lightsail provides preconfigured virtual servers.

Let's move on to storage services.

Amazon S3 or simple storage service provides object storage. Think of objects like individual files.

Amazon Elastic Block Store provides block storage. Think of them like external hard-drives you'd attach to your computer. Block storage is, quote unquote, opposite of object storage like a zip file instead of a single image file.

Amazon Snowball transfers huge amounts of data to AWS with a physical storage device.

Amazon Storage Gateway provides gateways to connect on-premises resources with the cloud.

Next, let's go over the database services.

Amazon Dynamo DB is a non-relational or no SQL database.

Amazon RDS or relational database service is a relational database.

Amazon Aurora is a relational database and can be run on amazon RDS.

Amazon Redshift is a data warehouse for a lot of data. Now, to the network and content delivery services.

Amazon VPC or virtual private cloud is a virtual network. Think of it as your corner of the AWS cloud.

Amazon CloudFront helps you have speedy websites using edge locations.

Amazon Route 53 routes domains to services and IP addresses.

Finally, let's go over the AWS management tools.

Amazon CloudFormation helps you create templates to form cloud services.

AWS CloudTrail helps you track trails of action, think of audit logs.

Amazon CloudWatch monitors or watches your AWS cloud instance for you.

Just as a note, sometimes other services come up in the exam. However, if you know what these core services are and what they do, then you'll be able to filter through the ones you're unsure of to come to the correct answer. Thankfully it's a process of elimination because the exam is all multiple choice. So don't get distracted by a service you've never heard about and utilize your process of elimination skills.

Next, let's discuss infrastructure as code. The concept of infrastructure as code is that you can write code that describes the configurations for specific AWS cloud services and they can be deployed for you by AWS. It helps speed up the deployment process and removes the risk of human error when spinning up new resources.

Some AWS cloud services that utilize infrastructure as code are:

- Elastic Beanstalk,
- AWS Lambda, and
- AWS CloudFormation.

Some ways to deploy and manage resources on the AWS cloud are by utilizing AWS Management Console with AWS Command-Line Interface or CLI, and with AWS Software Deployment Kits, or SDKs.

Finally, let's review AWS as global infrastructure. AWS has data centers around the world called availability zones. Each availability zone is independent from each other in network and power source and there are currently almost six dozen availability zones or AZs around the world. A region is made up of two or more availability zones and there are currently two dozen AWS regions around the world. You should strive to create a highly available, resilient and redundant IT infrastructure by replicating your AWS cloud resources across multiple availability zones and potentially, even regions.

## Module 4 – Billing & Pricing

### Study Break: Billing and Pricing domain

Welcome to the billing and pricing study break. Let's review some of the concepts we learned about that will be good to know for the AWS Certified Cloud Practitioner Exam. The AWS billing and cost management console is the go to a place to plan your AWS spending, simplify your accounts or consolidated billing and receive alerts for service uses this thresholds.

Cost explorer lets you get granular information about your AWS usage and generate billing reports with a breakdown of costs and usage.

The AWS billing and cost management console is an important part of making sure your AWS bills are expected and paid.

Additionally, the AWS pricing calculator and the AWS total cost of ownership calculator help you to evaluate how much running or migrating your it resources onto AWS Cloud could cost.

We just covered how to manage your billing. Now, let's cover the charges options provided by AWS.

The pay-as-you-go model of Cloud computing includes the different ways AWS charges you for your AWS Cloud resource usage.

The three fundamental ways you can be charged are:

- compute,
- storage, and
- outbound data transfer.

Different services have different ways of charging and pricing. And in general, the more you do something compute store or transfer data, the cheaper per unit the action becomes. There are more ways that AWS services charge its users, but these are the three most common charges. You should always check the way service usage is charged before spinning up any resources in AWS Cloud that you have never used before, so that you aren't hit with surprised bills at the end of the month.

All of these charges, you may wonder, is there any way that I can save money? Yes, there is. Consolidated billing is one way of saving money, while making the administrative work of managing multiple AWS accounts within one organization much easier. Instead of manually logging into each account owned by an organization to check usage and pay bills. The organization can create a billing only payer account that views and pays combined billing charges for all linked AWS accounts. One huge advantage of consolidated billing is that all resources used within the linked accounts are considered part of one large organization. This



means that the organization as a whole maybe eligible for volume discounts for the combined usage instead of by account basis.

## **Study break: Reviewing AWS support plans**

For this study break, let's review the four different support plans available for AWS Cloud. Questions about the AWS Support Plans appear in the AWS Certified Cloud Practitioner exam. So it's important to understand the differences and similarities between the four options, if you're looking into taking the exam.

Organizations can choose a support plan based on their budget, level of engagement with AWS, and support requirements. One important thing to remember when considering support plans in real use case scenarios, is that it is a separate charge from your usage cost.

The four different support plans are

- Basic,
- Developer,
- Business, and
- Enterprise Support Plans.

The Basic Support Plan has no monthly fees and is a great way for both organizations and users to test out and learn about the AWS Cloud and to evaluate the different services and functions. With this plan, you will not be able to receive any tech support aside from access to the AWS Community Forums, or you can pose questions for other users. You can receive customer service for account and billing questions directly from AWS. The Basic Support Plan is best for organizations without any mission critical resources hosted on AWS Cloud.

The Developer Support Plans starts at \$29 a month and scales with use. You will be charged either \$29 a month or 3% of your AWS monthly usage cost, whichever is larger. So if 3% of your monthly AWS cost is less than \$29, you'll receive a flat \$29 bill. If it's larger than \$29, you'll pay the larger fee. This plan is great for organizations that are experimenting with AWS in a more serious way for potential mission critical usage, and require more technical assistance than what the community forum can offer with the Basic Support Plan. However, the technical support is not immediate, so this plan is not ideal for production or mission critical use of AWS, where service failures could lead to business disruption.

The Business Support Plan starts at \$100 a month and scales with use. As with the Developer Support Plan, AWS will charge you the higher value of either \$100 a month, or between 3% to 10% of your monthly AWS bill. You can receive 24/7 tech support and for a fee could receive additional services like infrastructure event management. The Billing Support Plan is often considered the best bang for buck in terms of monthly cost versus the level of support compared with other support plans.

Finally, the Enterprise Support Plan. It comes with a hefty price tag starting at \$15,000 a month and scaling with use. As with the Business Support Plan AWS charges the higher of the static fee, or 3% to 10% of monthly AWS usage bill. This plan comes with all the bells and whistles, including a technical account manager, support concierge, proactive programs, well architected reviews and training, along with 24/7 tech support with a service level agreement or SLA of 15 minutes for emergencies. The Enterprise Support Plan is great for large organizations with substantial mission critical usage of AWS that cannot afford to have long standing downtime of their infrastructure. Remember, the support plan cost of \$15,000 and up is an addition to the AWS usage bill. Aside from the costs and AWS use cases, there are more nitty gritty features and options with each support plan. Some options include number of contacts that can open support cases, and what the service level agreements or SLAs are for number of tickets. Most of the questions about support plans are evaluating your ability to pick an appropriate support plan.

## **Study break: Exam tips and resources**

Of the four domains in the AWS Certified Cloud Practitioner Exam, the Billing and Pricing domain has the smallest amount of content at 12% of the exam. However, the multiple choice questions on the exam require you to know the concepts inside and out. Especially important is the ability to compare and contrast the different support plans.

The first thing you need to be able to do is compare and contrast the various pricing models for AWS. The questions could ask about the different ways AWS charges for resource usage, with the most fundamental ones being compute, storage, and data transfer out. It may also require you to realize that for many AWS services, the more you do something, such as storage or compute, the cheaper per unit the action becomes. So, transferring 50 gigabytes of data may be cheaper per kilobyte of transfer than transferring just 400 megabytes of data.

Another component of this domain is to recognize the various account structures in relation to AWS billing and pricing. Questions about this section could be asking about consolidated billing, which helps lower organizational cost as a whole by creating a billing-only account that links all AWS accounts together within the organization. By doing so, the organization may be eligible for volume discounts by combining their resource usage from all the accounts.

The questions could also ask about different support plans and ask you to identify the most suitable support plan for a certain situation. There are four support plans available from AWS ranging in monthly fees from free to starting at \$15,000 a month. The monthly fees do not include the monthly AWS usage costs, which are billed separately. The basic support plan is free and goes very well with the AWS free tier offer, which is 12 months of free service usage offered for new customers. And for the three plans that have monthly fees, AWS bills you

for the higher of the monthly flat fee or somewhere between three to 10% of monthly AWS usage.

Are you thinking, "well, which is more expensive, "the business support plan or developer support plan?"

A silly memory aid that I came up with to memorize the four support plans in order of monthly cost was BDBE.

B for Basic, D for Developer, B for Business, and E for Enterprise.

The monthly prices and features provided go up in that order.

Finally, you need to be able to identify resources available for billing support. These could be in the form of white papers, knowledge bases, contacting AWS Billing Support, or utilizing calculators like the AWS Cost Explorer, AWS Total Cost of Ownership Calculator, or the AWS Simple Monthly Calculator to find out how much you can expect to pay by running your resources on the AWS cloud.

How do you feel about your support plan compare and contrast skills? Or the different ways that you can be charged by AWS? If you have a few minutes, I highly recommend that you pick out a service like Amazon EC2, and search around the official AWS website for ways they bill for service usage and find out how you can reduce the cost of running that service. The best way to digest information is by testing it out, and you'll learn a lot from going out and trying to find the information yourself for future use.