

Practice Test #6 - AWS Certified Cloud Practitioner - Results

Return to review

Chart

Pie chart with 4 slices.

End of interactive chart.

Attempt 2

All knowledge areas

All questions

Question 1: **Correct**

Which of the following are the security best practices suggested by AWS for Identity and Access Management (IAM)? (Select two)

- **When you create IAM policies, grant the least privileges required to perform a task**

(Correct)

- **Do not change passwords and access keys once created. This results in failure of connectivity in the application logic**
- **Share your AWS account root user credentials only if absolutely necessary for performing an important billing operation**
- **Enable AWS Multi-Factor Authentication (AWS MFA) on your AWS root user account. MFA helps give root access to multiple users without actually sharing the root user login credentials**
- **Do not share security credentials between accounts, use IAM roles instead**

(Correct)

Explanation

Correct options:

When you create IAM policies, grant the least privileges required to perform a task

When you create IAM policies, follow the standard security advice of granting the least privileges, or granting only the permissions required to perform a task. Determine what users (and roles) need to do and then craft policies that allow them to perform only those tasks.

Start with a minimum set of permissions and grant additional permissions as necessary. Doing so is more secure than starting with permissions that are too lenient and then trying to tighten them later.

Do not share security credentials between accounts, use IAM roles instead

Don't share security credentials between accounts to allow users from another AWS account to access resources in your AWS account. Instead, use IAM roles. You can define a role that specifies what permissions the IAM users in the other account are

allowed. You can also designate which AWS accounts have the IAM users that are allowed to assume the role.

Incorrect options:

Share your AWS account root user credentials only if absolutely necessary for performing an important billing operation - Never share your AWS account root user password or access keys with anyone. Don't use your AWS account root user credentials to access AWS, and don't give your credentials to anyone else. Instead, create individual users for anyone who needs access to your AWS account. Create an IAM user for yourself as well, give that user administrative permissions, and use that IAM user for all your work.

Enable AWS Multi-Factor Authentication (AWS MFA) on your AWS root user account. MFA helps give root access to multiple users without actually sharing the root user login credentials - The given option just acts as a distractor. For extra security, AWS recommends that you use multi-factor authentication (MFA) for the root user in your account. With MFA, users have a device that generates a response to an authentication challenge. Both the user's credentials and the device-generated response are required to complete the sign-in process. If a user's password or access keys are compromised, your account resources are still secure because of the additional authentication requirement.

Do not change passwords and access keys once created. This results in failure of connectivity in the application logic - The given option just acts as a distractor. You should change your own passwords and access keys regularly, and make sure that all IAM users in your account do as well. That way, if a password or access key is compromised without your knowledge, you limit how long the credentials can be used to access your resources. You can apply a custom password policy to your account to require all your IAM users to rotate their AWS Management Console passwords. You can also choose how often they must do so.

Reference:

<https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html>

Question 2: **Correct**

Which of the following statements are true about AWS Shared Responsibility Model? (Select two)

- **AWS maintains the configuration of its infrastructure devices and is responsible for configuring the guest operating systems, databases, and applications**
- **For abstracted services, such as Amazon S3, AWS operates the infrastructure layer, the operating system, platforms, encryption options, and appropriate permissions for accessing the S3 resources**
- **AWS trains AWS employees, but a customer must train their own employees**

(Correct)

- **Amazon Elastic Compute Cloud (Amazon EC2) is categorized as Infrastructure as a Service (IaaS) and hence AWS will perform all of the necessary security configuration and management tasks**
- **AWS is responsible for patching and fixing flaws within the infrastructure, but customers are responsible for patching their guest operating system and applications**

(Correct)

Explanation

Correct options:

AWS is responsible for patching and fixing flaws within the infrastructure, but customers are responsible for patching their guest operating system and applications

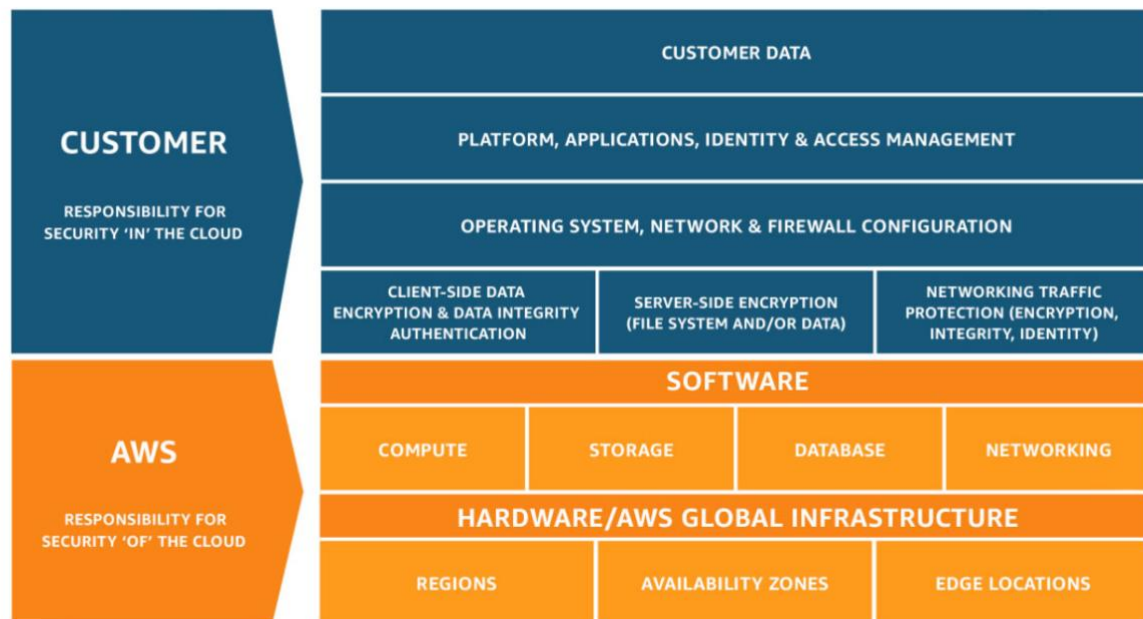
AWS trains AWS employees, but a customer must train their own employees

“Security of the Cloud” is the responsibility of AWS - 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. As part of Patch Management, a Shared Control responsibility of AWS Shared Responsibility Model, AWS is responsible for patching and fixing flaws within the infrastructure, but customers are responsible for patching their guest OS and applications.

“Security in the Cloud” is the responsibility of the customer. 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.

As part of Awareness & Training, a Shared Control responsibility of the AWS Shared Responsibility Model, AWS trains AWS employees, but a customer must train their own employees.

AWS Shared Responsibility
Model:



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

Incorrect options:

AWS maintains the configuration of its infrastructure devices and is responsible for configuring the guest operating systems, databases, and applications - As part of Configuration Management, a Shared Control responsibility of the AWS Shared Responsibility Model, AWS maintains the configuration of its infrastructure devices, but a customer is responsible for configuring their own guest operating systems, databases, and applications.

Amazon Elastic Compute Cloud (Amazon EC2) is categorized as Infrastructure as a Service (IaaS) and hence AWS will perform all of the necessary security configuration and management tasks - 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 the 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, AWS operates the infrastructure layer, the operating system, platforms, encryption options, and appropriate permissions for accessing the S3 resources - 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.

Reference:

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

Question 3: **Correct**

Which of the following AWS services will help provision a logically isolated network for your AWS resources?

- **AWS PrivateLink**
- **Amazon Route 53**
- **Amazon Virtual Private Cloud (Amazon VPC)**

(Correct)

- **AWS Firewall Manager**

Explanation

Correct option:

Amazon Virtual Private Cloud (Amazon VPC)

Amazon Virtual Private Cloud (Amazon VPC) is a service that lets you launch AWS resources in a logically isolated virtual network that you define. You have complete control over your virtual networking environment, including the selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways. You can use both IPv4 and IPv6 for most resources in your virtual private cloud, helping to ensure secure and easy access to resources and applications.

As one of AWS's foundational services, Amazon VPC makes it easy to customize your VPC's network configuration. You can create a public-facing subnet for your web servers that have access to the internet. It also lets you place your backend systems, such as databases or application servers, in a private-facing subnet with no internet access. Amazon VPC lets you use multiple layers of security, including security groups and network access control lists, to help control access to Amazon EC2 instances in each subnet.

Incorrect options:

AWS PrivateLink - AWS PrivateLink provides private connectivity between Amazon VPCs and services hosted on AWS or on-premises, securely on the Amazon network. By providing a private endpoint to access your services, AWS PrivateLink ensures your traffic is not exposed to the public internet.

Amazon Route 53 - Amazon Route 53 is a highly available and scalable cloud Domain Name System (DNS) web service. It is designed to give developers and businesses an extremely reliable and cost-effective way to route end users to Internet applications by translating names like `www.example.com` into the numeric IP addresses like `192.0.2.1` that computers use to connect to each other. Amazon Route 53 is fully compliant with IPv6 as well.

AWS Firewall Manager - AWS Firewall Manager is a security management service that allows you to centrally configure and manage firewall rules across your accounts and applications in AWS Organizations. As new applications are created,

Firewall Manager makes it easy to bring new applications and resources into compliance by enforcing a common set of security rules.

Reference:

<https://aws.amazon.com/vpc/>

Question 4: **Correct**

AWS Support plans are designed to give the right mix of tools and access to expertise for successfully running a business using AWS.

Which support plan(s) offers the full set of checks for AWS Trusted Advisor best practices and also provides support for programmatic case management?

- **AWS Business Support, AWS Enterprise On-Ramp, and AWS Enterprise Support plans**

(Correct)

- **Only AWS Enterprise Support plan**
- **AWS Enterprise On-Ramp Support plan after paying an additional fee and AWS Enterprise Support plan**
- **AWS Developer Support, AWS Business Support and AWS Enterprise Support plans**

Explanation

Correct option:

AWS Business Support, AWS Enterprise On-Ramp, and AWS Enterprise Support plans

AWS Trusted Advisor provides you with real-time guidance to help you provision your resources following AWS best practices.

The full set of AWS Trusted Advisor checks are included with Business and Enterprise Support plans. These checks can help optimize your AWS infrastructure, increase security and performance, reduce your overall costs, and monitor service limits.

AWS Support API provides programmatic access to AWS Support Center features to create, manage, and close your support cases, and operationally manage your Trusted Advisor check requests and status. AWS Support API is available for Business, Enterprise On-Ramp and Enterprise Support plans.

Comparing AWS Support Plans:

	Developer	Business	Enterprise On-Ramp	Enterprise
	Recommended if you are experimenting or testing in AWS.	Minimum recommended tier if you have production workloads in AWS	Recommended if you have production and/or business critical workloads in AWS.	Recommended if you have business and/or mission critical workloads in AWS.
AWS Trusted Advisor Best Practice Checks	Service Quota and basic Security checks	Full set of checks	Full set of checks	Full set of checks
AWS Trusted Advisor Priority				Prioritized recommendations curated by your AWS account team
Enhanced Technical Support	Business hours** web access to Cloud Support Associates Unlimited cases with 1 primary contact Prioritized responses on AWS re:Post	24/7 phone, web, and chat access to Cloud Support Engineers Unlimited cases and unlimited contacts (IAM supported) Prioritized responses on AWS re:Post Access to AWS Support App in Slack	24/7 phone, web, and chat access to Cloud Support Engineers Unlimited cases and unlimited contacts (IAM supported) Prioritized responses on AWS re:Post Access to AWS Support App in Slack	24/7 phone, web, and chat access to Cloud Support Engineers Unlimited cases and unlimited contacts (IAM supported) Prioritized responses on AWS re:Post Access to AWS Support App in Slack
Case Severity / Response Times*	General guidance: < 24 hours** System impaired: < 12 hours**	General guidance: < 24 hours System impaired: < 12 hours Production system impaired: < 4 hours Production system down: < 1 hour	General guidance: < 24 hours System impaired: < 12 hours Production system impaired: < 4 hours Production system down: < 1 hour Business-critical system down: < 30 minutes	General guidance: < 24 hours System impaired: < 12 hours Production system impaired: < 4 hours Production system down: < 1 hour Business/Mission-critical system down: < 15 minutes
Architectural Guidance	General	Contextual to your use-cases	Consultative review and guidance based on your applications (one-per-year)	Consultative review and guidance based on your applications
Programmatic Case Management		AWS Support API	AWS Support API	AWS Support API

via - <https://aws.amazon.com/premiumsupport/plans/>

Incorrect options:

Only AWS Enterprise Support plan

AWS Developer Support, AWS Business Support and AWS Enterprise Support plans

AWS Enterprise On-Ramp Support plan after paying an additional fee and AWS Enterprise Support plan

These three options contradict the explanation provided above, so these options are incorrect.

Reference:

<https://aws.amazon.com/premiumsupport/plans/>

Question 5: **Correct**

A team lead is reviewing the AWS services that can be used in the development workflow for his company. Which of the following statements are correct regarding the capabilities of these AWS services? (Select three)

- **AWS CodePipeline uses Amazon CloudWatch Events to detect changes in CodeCommit repositories used as a source for a pipeline**

(Correct)

- **Each AWS CodeStar project includes development tools, including AWS CodePipeline, AWS CodeCommit, AWS CodeBuild, and AWS CodeDeploy, that can be used on their own and with existing AWS applications**

(Correct)

- **AWS CodeCommit allows you to run builds and tests as part of your AWS CodePipeline**
- **AWS CodeStar is a cloud-based integrated development environment that lets you write, run, and debug your code with just a browser**
- **You can use AWS CodeStar and AWS Cloud9 to develop, build, and deploy a serverless web application**

(Correct)

- **AWS CodeBuild is directly integrated with both AWS CodePipeline and AWS CodeCommit**

Explanation

Correct options:

Each AWS CodeStar project includes development tools, including AWS CodePipeline, AWS CodeCommit, AWS CodeBuild, and AWS CodeDeploy, that can be used on their own and with existing AWS applications

AWS CodeStar accelerates software release with the help of AWS CodePipeline, a continuous integration and continuous delivery (CI/CD) service. Each project comes pre-configured with an automated pipeline that continuously builds, tests, and deploys your code with each commit. AWS CodeStar integrates with AWS CodeDeploy and AWS CloudFormation so that you can easily update your application code and deploy to Amazon EC2 and AWS Lambda.

More information on AWS
CodeStar:

Automated continuous delivery pipeline

AWS CodeStar accelerates software release with the help of [AWS CodePipeline](#), a continuous integration and continuous delivery (CI/CD) service. Each project comes pre-configured with an automated pipeline that continuously builds, tests, and deploys your code with each commit.

AWS CodeStar > Create project

Select template Set up tools Start coding

Project name: SF Summit Project ID: sf-summit

AWS CodeStar includes all of the tools and services you need for a development project. This project includes an AWS CodePipeline connected with the following tools:

Source Build Test Deploy Monitoring

AWS CodeCommit AWS CodeBuild AWS CloudFormation Amazon CloudWatch

☒ AWS CodeStar would like permission to administer AWS resources on your behalf. [Learn more](#)

Previous Create Project

via - <https://aws.amazon.com/codestar/features/>

AWS CodePipeline uses Amazon CloudWatch Events to detect changes in CodeCommit repositories used as a source for a pipeline

AWS CodePipeline uses Amazon CloudWatch Events to detect changes in CodeCommit repositories used as a source for a pipeline. Each source action has a corresponding event rule. This event rule starts your pipeline when a change occurs in the repository.

AWS CodePipeline integration with AWS CodeCommit:

CodeCommit source actions

CodeCommit	<p>CodeCommit is a version control service that you can use to privately store and manage assets (such as documents, source code, and binary files) in the cloud. You can configure CodePipeline to use a branch in a CodeCommit repository as the source for your code. Create the repository and associate it with a working directory on your local machine. Then you can create a pipeline that uses the branch as part of a source action in a stage. You can connect to the CodeCommit repository by either creating a pipeline or editing an existing one.</p> <p>You can use the Full clone option for this action to reference the repository Git metadata so that downstream actions can perform Git commands directly. This option can only be used by CodeBuild downstream actions.</p> <p>Learn more:</p> <ul style="list-style-type: none">• To view configuration parameters and an example JSON/YAML snippet, see CodeCommit.• Tutorial: Create a simple pipeline (CodeCommit repository)• CodePipeline uses Amazon CloudWatch Events to detect changes in CodeCommit repositories used as a source for a pipeline. Each source action has a corresponding event rule. This event rule starts your pipeline when a change occurs in the repository. See General integrations with CodePipeline.
-------------------	---

via - <https://docs.aws.amazon.com/codepipeline/latest/userguide/integrations-action-type.html>

You can use AWS CodeStar and AWS Cloud9 to develop, build, and deploy a serverless web application

AWS CodeStar is a cloud-based development service that provides the tools you need to quickly develop, build, and deploy applications on AWS. AWS Cloud9 is a cloud-based integrated development environment (IDE) that lets you write, run, and debug your code with just a browser. Together, the two services can be used to build serverless applications in very little time.

Incorrect options:

AWS CodeBuild is directly integrated with both AWS CodePipeline and AWS CodeCommit - AWS CodeCommit can trigger a Lambda function that in turns invokes a CodeBuild job, therefore CodeBuild has an indirect integration with CodeCommit. However, AWS CodePipeline is directly integrated with both AWS CodeBuild and AWS CodeCommit because CodePipeline can use source action integrations with CodeCommit and build action integrations with CodeBuild.

AWS CodeCommit allows you to run builds and tests as part of your AWS CodePipeline - AWS CodeCommit is a version control service that you can use to privately store and manage assets (such as documents, source code, and binary files) in the cloud. AWS CodeBuild is a fully managed continuous integration service that compiles source code, runs tests, and produces software packages that are ready to deploy. AWS CodeBuild allows you to run builds and tests as part of your pipeline.

AWS CodeStar is a cloud-based integrated development environment that lets you write, run, and debug your code with just a browser - AWS CodeStar is a

cloud-based development service that provides the tools you need to quickly develop, build, and deploy applications on AWS. AWS Cloud9 is a cloud-based integrated development environment (IDE) that lets you write, run, and debug your code with just a browser.

Here is an example to explain the collaboration between these services - You can use AWS CodeStar to build a new AWS Lambda based Node.js serverless web application. You will use AWS CodeStar to set up a continuous delivery mechanism using AWS CodeCommit for source control and AWS CodePipeline to automate your release process. You can then change some code in the Node.js project using Cloud9 and commit the change to trigger your continuous pipeline and redeploy your project.

Build a Serverless Application using AWS CodeStar and AWS Cloud9:

In this tutorial you will learn how to use AWS CodeStar and AWS Cloud9 to develop, build, and deploy a Node.js serverless web application. As a developer, setting up an automated software development workflow can be a time-intensive, detailed task. AWS CodeStar is a software development tool that enables you to quickly develop, build, and deploy applications on AWS. With CodeStar, you can setup your continuous delivery toolchain in minutes, allowing you to start releasing code faster.

Cloud9 is a cloud IDE for writing, running, and debugging code. Cloud9 comes prepackaged with essential tools for many popular programming languages (JavaScript, Python, PHP, etc.) so you don't have to tinker with installing various compilers and toolchains.

In the next several minutes, you'll use AWS CodeStar to build a new AWS Lambda based Node.js serverless web application. You will use AWS CodeStar to set up a continuous delivery toolchain using AWS CodeCommit for source control and AWS CodePipeline to automate your release process. You will then change some code in the Node.js project using Cloud9 and commit the change to trigger your continuous pipeline and redeploy your project.

via - <https://aws.amazon.com/getting-started/hands-on/build-serverless-app-codestar-cloud9/>

References:

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

<https://aws.amazon.com/codebuild/>

<https://aws.amazon.com/cloud9/>

Question 6: **Correct**

An e-learning company wants to build a knowledge graph by leveraging a fully managed database. Which of the following is the best fit for this requirement?

- **Amazon DocumentDB**
- **Amazon DynamoDB**
- **Amazon Neptune**

(Correct)

- **Amazon Relational Database Service (Amazon RDS)**

Explanation

Correct option:

Amazon Neptune

Amazon Neptune is a fast, reliable, fully-managed graph database service that makes it easy to build and run applications that work with highly connected datasets. The core of Amazon Neptune is a purpose-built, high-performance graph database engine optimized for storing billions of relationships and querying the graph with milliseconds latency. Amazon Neptune is tailor-built for use cases like Knowledge Graphs, Identity Graphs, Fraud Detection, Recommendation Engines, Social Networking, Life Sciences, and so on.

Amazon Neptune supports popular graph models Property Graph and W3C's RDF, and their respective query languages Apache TinkerPop Gremlin and SPARQL, allowing you to easily build queries that efficiently navigate highly connected datasets. Neptune powers graph use cases such as recommendation engines, fraud detection, knowledge graphs, drug discovery, and network security.

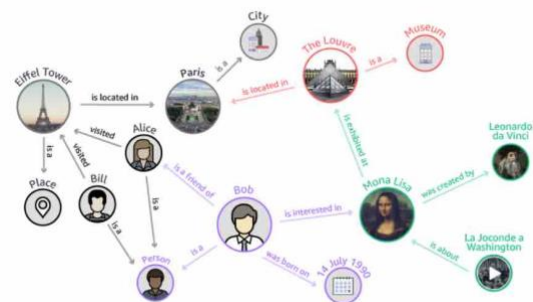
Amazon Neptune is highly available, with read-replicas, point-in-time recovery, continuous backup to Amazon S3, and replication across Availability Zones. Neptune is secure with support for HTTPS encrypted client connections and encryption at rest. Neptune is fully managed, so you no longer need to worry about database management tasks such as hardware provisioning, software patching, setup, configuration, or backups.

Fraud Detection with Amazon Neptune:

Knowledge Graphs

Amazon Neptune helps you build knowledge graph applications. A knowledge graph allows you to store information in a graph model and use graph queries to enable your users to easily navigate highly connected datasets. Neptune supports open source and open standard APIs to allow you to quickly leverage existing information resources to build your knowledge graphs and host them on a fully managed service. For example, if a user is interested in The Mona Lisa, you can also help them discover other works of art by Leonardo da Vinci, or other works of art located in The Louvre. Using a knowledge graph, you can add topical information to product catalogs, build and query complex models of regulatory rules, or model general information, like [Wikidata](#).

Learn more about [Knowledge Graphs on AWS](#).



via - <https://aws.amazon.com/neptune/>

Incorrect options:

Amazon DocumentDB - Amazon DocumentDB (with MongoDB compatibility) is a fast, scalable, highly available, and fully managed document database service that supports MongoDB workloads. As a document database, Amazon DocumentDB makes it easy to store, query, and index JSON data.

Amazon DocumentDB is a non-relational database service designed from the ground-up to give you the performance, scalability, and availability you need when operating mission-critical MongoDB workloads at scale. In Amazon DocumentDB, the storage and compute are decoupled, allowing each to scale independently, and you can increase the read capacity to millions of requests per second by adding up to 15 low latency read replicas in minutes, regardless of the size of your data.

Amazon DynamoDB - Amazon DynamoDB is a key-value and document database that delivers single-digit millisecond performance at any scale. It's a fully managed, multi-region, multi-active, durable database with built-in security, backup and restores, and in-memory caching for internet-scale applications. DynamoDB can handle more than 10 trillion requests per day and can support peaks of more than 20 million requests per second. For highly connected datasets Amazon Neptune is a better choice.

Amazon Relational Database Service (Amazon RDS) - Amazon Relational Database Service (Amazon RDS) makes it easy to set up, operate, and scale a relational database in the cloud. It provides cost-efficient and resizable capacity while automating time-consuming administration tasks such as hardware provisioning, database setup, patching, and backups. It frees you to focus on your applications so you can give them the fast performance, high availability, security, and compatibility they need. Amazon RDS is available on several database instance types - optimized for memory, performance, or I/O - and provides you with six familiar database engines to choose from, including Amazon Aurora, PostgreSQL, MySQL, MariaDB, Oracle Database, and SQL Server.

Reference:

<https://aws.amazon.com/neptune/>

Question 7: **Correct**

A team manager needs data about the changes that have taken place for AWS resources in his account during the past two weeks. Which AWS service can help get this data?

- **AWS CloudTrail**
- **Amazon CloudWatch**
- **Amazon Inspector**
- **AWS Config**

(Correct)

Explanation

Correct option:

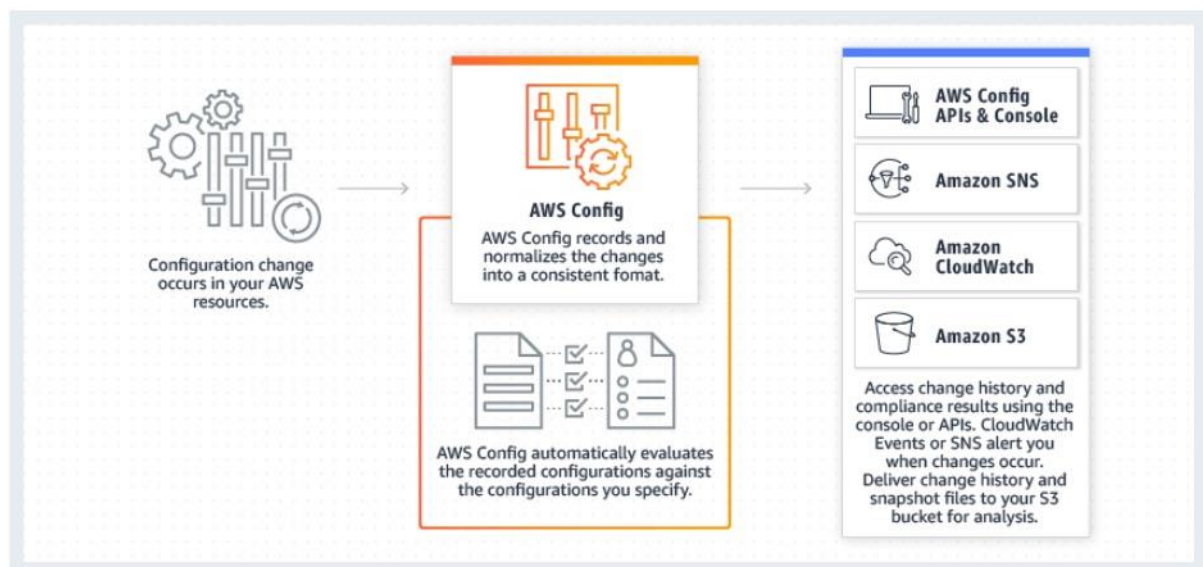
AWS Config

AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources. Config continuously monitors and records your AWS resource configurations and allows you to automate the evaluation of

recorded configurations against desired configurations. With Config, you can review changes in configurations and relationships between AWS resources, dive into detailed resource configuration histories, and determine your overall compliance against the configurations specified in your internal guidelines. This enables you to simplify compliance auditing, security analysis, change management, and operational troubleshooting.

While AWS Config helps you answer questions like - “What did my AWS resource look like?” at a point in time. You can use AWS CloudTrail to answer “Who made an API call to modify this resource?”

Diagrammatic representation of how AWS Config works:



via - <https://aws.amazon.com/config/>

Incorrect options:

Amazon CloudWatch - You can use Amazon CloudWatch to collect and track metrics, collect and monitor log files, and set alarms. Amazon CloudWatch can monitor AWS resources such as Amazon EC2 instances, Amazon DynamoDB tables, and Amazon RDS DB instances, as well as custom metrics generated by your applications and services, and any log files your applications generate. You can use Amazon CloudWatch to gain system-wide visibility into resource utilization, application performance, and operational health. You can use these insights to react and keep your application running smoothly. CloudWatch cannot however tell if the configuration of the resource has changed and what exactly changed.

Amazon Inspector - Amazon Inspector is an automated security assessment service that helps you test the network accessibility of your Amazon EC2 instances and the security state of your applications running on the instances. Amazon Inspector allows you to automate security vulnerability assessments throughout your development and deployment pipeline or against static production systems. This

allows you to make security testing a more regular occurrence as part of the development and IT operations.

AWS CloudTrail - AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. With CloudTrail, you can log, continuously monitor, and retain account activity related to actions across your AWS infrastructure. CloudTrail provides event history of your AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command-line tools, and other AWS services. This event history simplifies security analysis, resource change tracking, and troubleshooting. In addition, you can use CloudTrail to detect unusual activity in your AWS accounts. These capabilities help simplify operational analysis and troubleshooting.

Reference:

<https://aws.amazon.com/config/>

Question 8: **Correct**

Which AWS service allows you to connect any number of IoT devices to the cloud without requiring you to provision or manage servers?

- **Amazon Connect**
- **AWS IoT Core**

(Correct)

- **AWS Control Tower**
- **AWS IoT Gateway**

Explanation

Correct option:

AWS IoT Core

AWS IoT Core lets you connect IoT devices to the AWS cloud without the need to provision or manage servers. AWS IoT Core can support billions of devices and trillions of messages and can process and route those messages to AWS endpoints and to other devices reliably and securely. With AWS IoT Core, your applications can keep track of and communicate with all your devices, all the time, even when they aren't connected.

AWS IoT Core also makes it easy to use AWS and Amazon services like AWS Lambda, Amazon Kinesis, Amazon S3, Amazon SageMaker, Amazon DynamoDB, Amazon CloudWatch, AWS CloudTrail, Amazon QuickSight, and Alexa Voice Service to build IoT applications that gather, process, analyze and act on data generated by connected devices, without having to manage any infrastructure.

AWS IoT Core lets you select the communication protocol most appropriate for your use case to connect and manage IoT devices. AWS IoT Core supports MQTT (Message Queuing and Telemetry Transport), HTTPS (Hypertext Transfer Protocol -

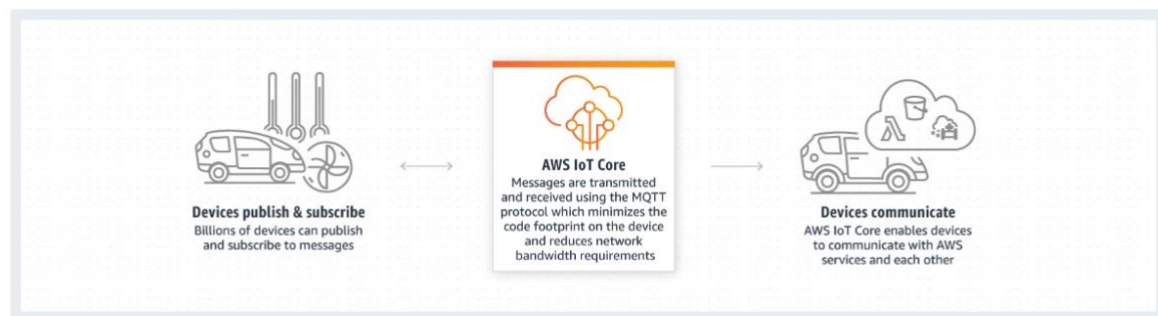
Secure), MQTT over WSS (WebSockets Secure), and LoRaWAN (low-power long-range wide-area network).

AWS IoT Core provides automated configuration and authentication upon a device's first connection to AWS IoT Core, as well as end-to-end encryption throughout all points of connection, so that data is never exchanged between devices and AWS IoT Core without proven identity. In addition, you can secure access to your devices and applications by applying policies with granular permissions.

AWS IoT Core capabilities:

Publish and subscribe to messages with message broker

The Message Broker is a high throughput publish/subscribe (pub/sub) message broker that securely transmits messages to and from all of your IoT devices and applications with low latency. AWS IoT Core supports devices and clients that use the MQTT and the MQTT over WSS protocols to pub/sub to messages, and devices and clients that use the HTTPS protocol to publish messages.



via - <https://aws.amazon.com/iot-core/>

Incorrect options:

Amazon Connect - Amazon Connect is an easy to use omnichannel cloud contact center that helps you provide superior customer service at a lower cost. Designed from the ground up to be omnichannel, Amazon Connect provides a seamless experience across voice and chat for your customers and agents. This includes one set of tools for skills-based routing, task management, powerful real-time and historical analytics, and intuitive management tools – all with pay-as-you-go pricing, which means Amazon Connect simplifies contact center operations, improves agent efficiency, and lowers costs.

AWS IoT Gateway - This is a made-up option and has been added as a distractor.

AWS Control Tower - AWS Control Tower provides the easiest way to set up and govern a new, secure, multi-account AWS environment based on best practices established through AWS' experience working with thousands of enterprises as they move to the cloud. Control Tower provides mandatory and strongly recommended high-level rules, called guardrails, that help enforce your policies using service control policies (SCPs), or detect policy violations using AWS Config rules.

References:

<https://docs.aws.amazon.com/iot/latest/developerguide/what-is-aws-iot.html>

<https://aws.amazon.com/connect/>

<https://aws.amazon.com/transit-gateway/>

<https://aws.amazon.com/controltower/>

Question 9: **Correct**

A university provides access to AWS services for its students to submit their research data for analysis. The university is looking at the most cost-effective approach for recovering from disasters and it can tolerate data loss of a few hours.

Which disaster recovery strategy is well-suited for this use case?

- **Pilot light strategy**
- **Multi-site active/active strategy**
- **Backup and restore strategy**

(Correct)

- **Warm standby strategy**

Explanation

Correct option:

Backup and restore strategy

When selecting your DR strategy, you must weigh the benefits of lower recovery time objective (RTO) and recovery point objective (RPO) vs the costs of implementing and operating a strategy. The Backup and restore strategy offers a good balance of benefits and cost for the current use case. This is the cheapest of all the disaster recovery options available with AWS.

Backup and restore is the most suitable approach for the given use case as the university can tolerate data loss of a few hours. This approach can be used to mitigate against a regional disaster by replicating data to other AWS Regions or to mitigate the lack of redundancy for workloads deployed to a single Availability Zone. In addition to data, you must redeploy the infrastructure, configuration, and application code in the recovery Region.

Comparing different disaster recovery strategies:

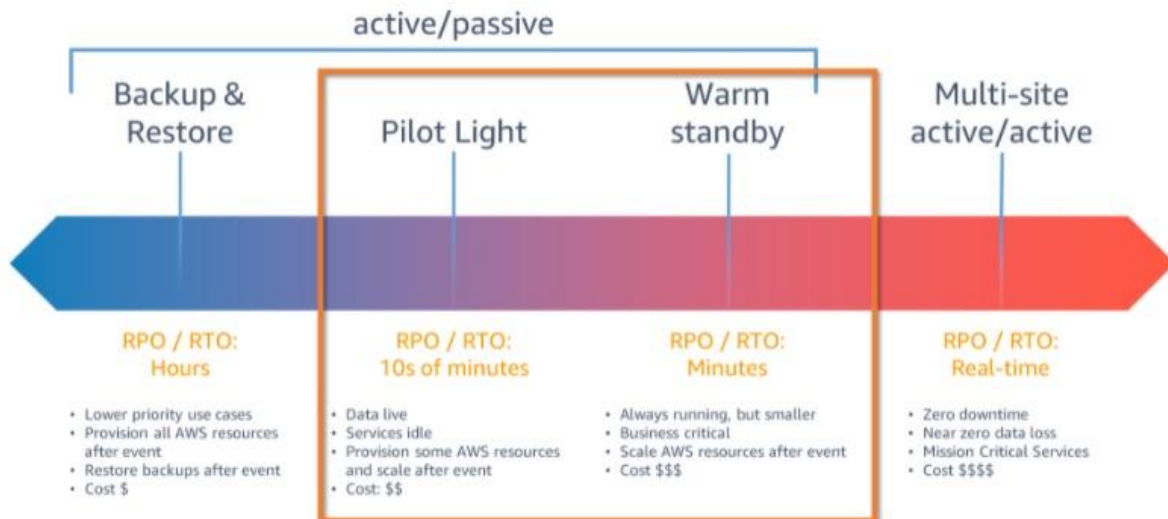


Figure 1. DR strategies

via - <https://aws.amazon.com/blogs/architecture/disaster-recovery-dr-architecture-on-aws-part-iii-pilot-light-and-warm-standby/>

Incorrect options:

Pilot light strategy - With the pilot light approach, you replicate your data from one Region to another and provision a copy of your core workload infrastructure. Resources required to support data replication and backup, such as databases and object storage, are always on. Other elements, such as application servers, are loaded with application code and configurations but are switched off and are only used during testing or when disaster recovery failover is invoked. Unlike the backup and restore approach, your core infrastructure is always available and you always have the option to quickly provision a full-scale production environment by switching on and scaling out your application servers. This also implies that the cost incurred is higher than what it is for the backup and restore approach.

Multi-site active/active strategy - You can run your workload simultaneously in multiple AWS Regions as part of a multi-site active/active strategy. Multi-site active/active serves traffic from all regions to which it is deployed. With a multi-site active/active approach, users can access the workload in any of the Regions in which it is deployed. This approach is the most complex and costliest for disaster recovery.

Warm standby strategy - The warm standby approach involves ensuring that there is a scaled-down but fully functional copy of your production environment in another AWS Region. This approach extends the pilot light concept and decreases the time to recovery because your workload is always-on in another Region. This approach also allows you to more easily perform testing or implement continuous testing to increase confidence in your ability to recover from a disaster. This strategy is costly and is used only for business-critical applications.

Reference:

<https://docs.aws.amazon.com/whitepapers/latest/disaster-recovery-workloads-on-aws/disaster-recovery-options-in-the-cloud.html>

Question 10: **Correct**

As part of log analysis, you have realized that one or more AWS-owned IP addresses are being used for port scanning your on-premises server. Which service/team should you connect to resolve this issue?

- **Reach out to Werner Vogels, the CTO of Amazon, with the details of the incident**
- **Use AWS Trusted Advisor to log a complaint with AWS**
- **Contact AWS Abuse team**

(Correct)

- **Contact AWS Support**

Explanation

Correct option:

Contact AWS Abuse team

If you suspect that AWS resources are being used for abusive purposes, you need to contact the AWS Abuse team using the Report Amazon AWS abuse form, or by contacting abuse@amazonaws.com.

The AWS Abuse team can assist you when AWS resources are used to engage in the following types of abusive behavior: spam from AWS-owned IP addresses or AWS resources, port scanning, Denial-of-service (DoS) or DDoS from AWS-owned IP addresses, intrusion attempts, hosting objectionable or copyrighted content, distributing malware.

List of activities that fall under abusive behavior:

The AWS Abuse team can assist you when AWS resources are used to engage in the following types of abusive behavior:

- **Spam:** You are receiving unwanted emails from an AWS-owned IP address, or AWS resources are used to spam websites or forums.
- **Port scanning:** Your logs show that one or more AWS-owned IP addresses are sending packets to multiple ports on your server, and you believe this is an attempt to discover unsecured ports.
- **Denial-of-service (DoS) attacks:** Your logs show that one or more AWS-owned IP addresses are used to flood ports on your resources with packets, and you believe that this is an attempt to overwhelm or crash your server or the software running on your server.
- **Intrusion attempts:** Your logs show that one or more AWS-owned IP addresses are used to attempt to log in to your resources.
- **Hosting objectionable or copyrighted content:** You have evidence that AWS resources are used to host or distribute illegal content or distribute copyrighted content without the consent of the copyright holder.
- **Distributing malware:** You have evidence that AWS resources are used to distribute software that was knowingly created to compromise or cause harm to computers or machines on which it is installed.

via - <https://aws.amazon.com/premiumsupport/knowledge-center/report-aws-abuse/>

Incorrect options:

Contact AWS Support - AWS Support can't assist with reports of abuse or questions about notifications from the AWS Abuse team. AWS Abuse team is the right contact point for raising voice on abusive behavior using AWS resources.

Use AWS Trusted Advisor to log a complaint with AWS - AWS Trusted Advisor is an online tool that provides you real-time guidance to help you provision your resources following AWS best practices. Trusted Advisor checks help optimize your AWS infrastructure, increase security and performance, reduce your overall costs, and monitor service limits. Whether establishing new workflows, developing applications, or as part of ongoing improvement, take advantage of the recommendations provided by Trusted Advisor on a regular basis to help keep your solutions provisioned optimally.

Reach out to Werner Vogels, the CTO of Amazon, with the details of the incident - This has been added as a distractor. For the record, please let us know if you do get a shout out from Mr. Vogels.

Reference:

<https://aws.amazon.com/premiumsupport/knowledge-center/report-aws-abuse/>

Question 11: **Correct**

Which of the following AWS services can be used to continuously monitor both malicious activities as well as unauthorized behavior to protect your AWS accounts and workloads?

- **Amazon GuardDuty**

(Correct)

- **Amazon Detective**
- **Amazon Inspector**
- **AWS Security Hub**

Explanation

Correct option:

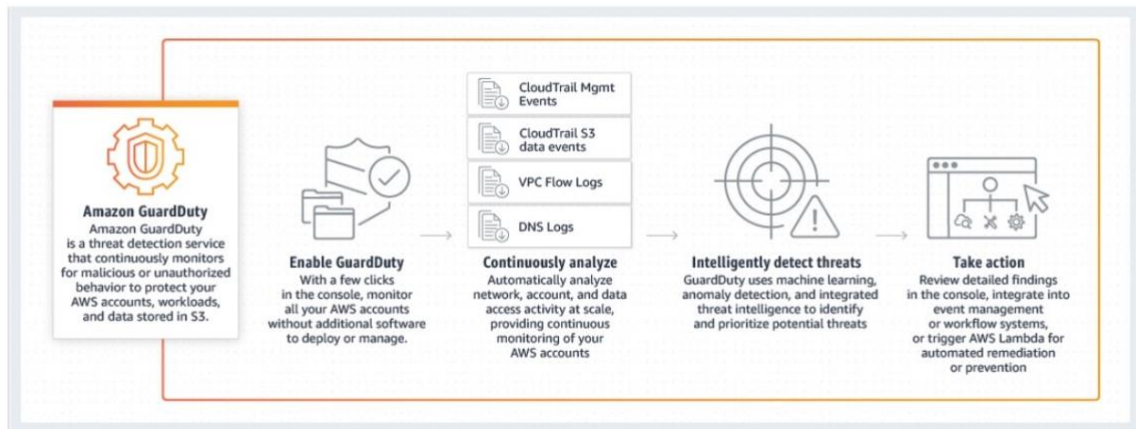
Amazon GuardDuty

Amazon GuardDuty is a threat detection service that continuously monitors for malicious activity and unauthorized behavior to protect your AWS accounts, workloads, and data stored in Amazon Simple Storage Service (Amazon S3). With the cloud, the collection and aggregation of account and network activities are simplified, but it can be time-consuming for security teams to continuously analyze event log data for potential threats. With Amazon GuardDuty, you now have an intelligent and cost-effective option for continuous threat detection in AWS.

The service uses machine learning, anomaly detection, and integrated threat intelligence to identify and prioritize potential threats. GuardDuty analyzes tens of billions of events across multiple AWS data sources, such as AWS CloudTrail event logs, Amazon VPC Flow Logs, and DNS logs. With a few clicks in the AWS Management Console, GuardDuty can be enabled with no software or hardware to deploy or maintain.

Amazon GuardDuty makes it easy for you to enable continuous monitoring of your AWS accounts, workloads, and data stored in Amazon S3. It operates completely independently from your resources so there is no risk of performance or availability impacts to your workloads. It's fully managed with integrated threat intelligence, anomaly detection, and machine learning. Amazon GuardDuty delivers detailed and actionable alerts that are easy to integrate with existing event management and workflow systems. There are no upfront costs and you pay only for the events analyzed, with no additional software to deploy or subscriptions to threat intelligence feeds required.

How Amazon GuardDuty
Works:



via - <https://aws.amazon.com/guardduty/>

Incorrect options:

AWS Security Hub - AWS Security Hub gives you a comprehensive view of your security alerts and security posture across your AWS accounts. There is a range of powerful security tools at your disposal, from firewalls and endpoint protection to vulnerability and compliance scanners. With Security Hub, you have a single place that aggregates, organizes, and prioritizes your security alerts, or findings, from multiple AWS services, such as Amazon GuardDuty, Amazon Inspector, and Amazon Macie, as well as from AWS Partner solutions.

Amazon Detective - Amazon Detective simplifies the process of investigating security findings and identifying the root cause. Amazon Detective analyzes trillions of events from multiple data sources such as VPC Flow Logs, AWS CloudTrail logs, and Amazon GuardDuty findings and automatically creates a graph model that provides you with a unified, interactive view of your resources, users, and the interactions between them over time.

Amazon Inspector - Amazon Inspector is an automated security assessment service that helps you test the network accessibility of your Amazon EC2 instances and the security state of your applications running on the instances. Amazon Inspector allows you to automate security vulnerability assessments throughout your development and deployment pipeline or against static production systems. This allows you to make security testing a more regular occurrence as part of the development and IT operations.

References:

<https://aws.amazon.com/guardduty/>

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

Question 12: **Correct**

Which of the following are NoSQL database services from AWS? (Select two)

- **Amazon DocumentDB**

(Correct)

- **AWS Storage Gateway**
- **Amazon Aurora**
- **Amazon Neptune**

(Correct)

- **Amazon Relational Database Service (Amazon RDS)**

Explanation

Correct options:

Amazon Neptune

A graph database's purpose is to make it easy to build and run applications that work with highly connected datasets. Typical use cases for a graph database include social networking, recommendation engines, fraud detection, and knowledge graphs. Amazon Neptune is a fully-managed graph database service and it's also considered as a type of NoSQL database.

Amazon DocumentDB

In application code, data is represented often as an object or JSON-like document because it is an efficient and intuitive data model for developers. Document databases make it easier for developers to store and query data in a database by using the same document model format that they use in their application code. Amazon DocumentDB (with MongoDB compatibility) and MongoDB are popular document databases that provide powerful and intuitive APIs for flexible and iterative development.

Incorrect options:

Amazon Relational Database Service (Amazon RDS) - Amazon Relational Database Service (Amazon RDS) makes it easy to set up, operate, and scale a relational database in the cloud. It provides cost-efficient and resizable capacity while automating time-consuming administration tasks such as hardware provisioning, database setup, patching and backups. It frees you to focus on your applications so you can give them the fast performance, high availability, security and compatibility they need.

Amazon Aurora - Amazon Aurora is a MySQL and PostgreSQL-compatible relational database built for the cloud, that combines the performance and availability of traditional enterprise databases with the simplicity and cost-effectiveness of open source databases. Amazon Aurora is fully managed by Amazon Relational Database Service (RDS), which automates time-consuming administration tasks like hardware provisioning, database setup, patching, and backups.

AWS Storage Gateway - AWS Storage Gateway is a hybrid cloud storage service that gives you on-premises access to virtually unlimited cloud storage. Customers use

Storage Gateway to simplify storage management and reduce costs for key hybrid cloud storage use cases. These include moving backups to the cloud, using on-premises file shares backed by cloud storage, and providing low latency access to data in AWS for on-premises applications. It is not a database service.

Reference:

<https://aws.amazon.com/nosql/>

Question 13: **Correct**

An e-commerce company needs to generate custom reports and graphs every week for analyzing the product sales data. The company is looking at a tool/service that will help them analyze this data using interactive dashboards with minimal effort. The dashboards also need to be accessible from any device.

Which AWS tool/service will you recommend for this use-case?

- **Amazon Quicksight**

(Correct)

- Amazon Athena
- Amazon SageMaker
- AWS Glue

Explanation

Correct option:

Amazon Quicksight

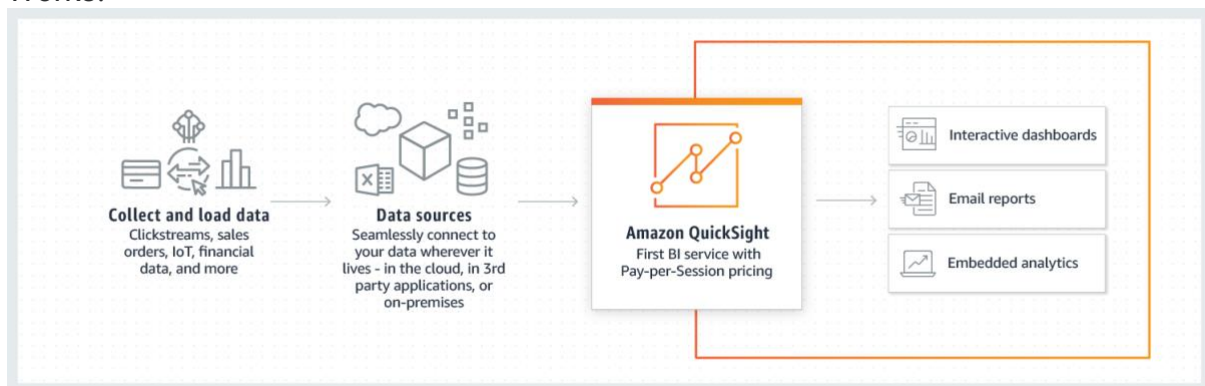
Amazon QuickSight is a scalable, serverless, embeddable, machine learning-powered business intelligence (BI) service built for the cloud. QuickSight lets you easily create and publish interactive BI dashboards that include Machine Learning-powered insights. QuickSight dashboards can be accessed from any device, and seamlessly embedded into your applications, portals, and websites.

With Amazon QuickSight, you can quickly embed interactive dashboards into your applications, websites, and portals. QuickSight provides a rich set of APIs and SDKs that allow you to easily customize the look and feel of the dashboards to match applications. With Amazon QuickSight, you can manage your dashboard versions, grant dashboard authoring privileges, and share usage reports with your end-customers. If your application is used by customers that belong to different teams or organizations, QuickSight ensures that their data is always siloed and secure.

Amazon QuickSight has a serverless architecture that automatically scales to tens of thousands of users without the need to set up, configure, or manage your own servers. It also ensures that your users don't have to deal with slow dashboards during peak-hours when multiple BI users are accessing the same dashboards or datasets. And with pay-per-session pricing, you only pay when your users access the

dashboards or reports, which makes it cost-effective for deployments with lots of users. There are no upfront costs or annual commitments for using QuickSight.

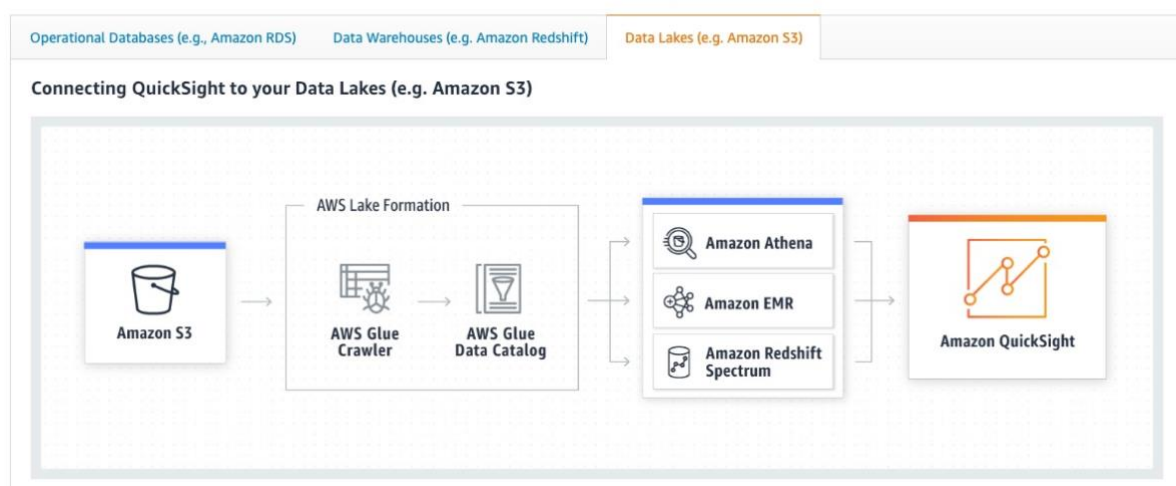
How Amazon QuickSight Works:



via - <https://aws.amazon.com/quicksight/>

Connecting QuickSight to your Data Lakes (e.g. Amazon S3):

Use cases



via - <https://aws.amazon.com/quicksight/>

Incorrect options:

AWS Glue - AWS Glue is a serverless data integration service that makes it easy to discover, prepare, and combine data for analytics, machine learning, and application development. AWS Glue provides all of the capabilities needed for data integration, so you can start analyzing your data and putting it to use in minutes instead of months. You should use AWS Glue to discover properties of the data you own, transform it, and prepare it for analytics. Glue can automatically discover both structured and semi-structured data stored in your data lake on Amazon S3, data warehouse in Amazon Redshift, and various databases running on AWS.

Amazon SageMaker - Amazon SageMaker is a fully managed service that provides every developer and data scientist with the ability to build, train, and deploy machine

learning (ML) models quickly. SageMaker removes the heavy lifting from each step of the machine learning process to make it easier to develop high-quality models. Amazon SageMaker ensures that ML model artifacts and other system artifacts are encrypted in transit and at rest.

Amazon Athena - Amazon Athena is an interactive query service that makes it easy to analyze data in Amazon S3 using standard SQL. Athena is serverless, so there is no infrastructure to manage, and you pay only for the queries that you run. Athena is easy to use. Simply point to your data in Amazon S3, define the schema, and start querying using standard SQL. Most results are delivered within seconds. With Athena, there's no need for complex ETL jobs to prepare your data for analysis. This makes it easy for anyone with SQL skills to quickly analyze large-scale datasets.

Athena is integrated out-of-the-box with AWS Glue Data Catalog, allowing you to create a unified metadata repository across various services, crawl data sources to discover schemas, and populate your Catalog with new and modified table and partition definitions, and maintain schema versioning.

As discussed in the example above, Athena can be used to analyze data, while QuickSight can be used to visualize this data via advanced interactive dashboards.

References:

<https://aws.amazon.com/quicksight/>

<https://aws.amazon.com/athena/>

<https://aws.amazon.com/glue/>

Question 14: **Correct**

Which tool/service will help you get a forecast of your spending for the next 12 months?

- **Consolidated Billing of AWS Organizations**
- **AWS Cost Explorer**

(Correct)

- **AWS Pricing Calculator**
- **AWS Marketplace**

Explanation

Correct option:

AWS Cost Explorer

AWS Cost Explorer lets you explore your AWS costs and usage at both a high level and at a detailed level of analysis, and empowering you to dive deeper using a number of filtering dimensions (e.g., AWS Service, Region, Member Account, etc.) AWS Cost Explorer also gives you access to a set of default reports to help you get started, while also allowing you to create custom reports from scratch.

You can explore your usage and costs using the main graph, the Cost Explorer cost, and usage reports, or the Cost Explorer RI report. You can view data for up to the last 12 months, forecast how much you're likely to spend for the next 12 months, and get recommendations for what Reserved Instances to purchase. You can use Cost Explorer to identify areas that need further inquiry and see trends that you can use to understand your costs.

You can view your costs and usage using the Cost Explorer user interface free of charge. You can also access your data programmatically using the Cost Explorer API.

When you first sign up for Cost Explorer, AWS prepares the data about your costs for the current month and the last 12 months and then calculates the forecast for the next 12 months. The current month's data is available for viewing in about 24 hours. The rest of your data takes a few days longer. Cost Explorer updates your cost data at least once every 24 hours. After you sign up, Cost Explorer can display up to 12 months of historical data (if you have that much), the current month, and the forecasted costs for the next 12 months.

Incorrect options:

Consolidated Billing of AWS Organizations - AWS products and services are designed to accommodate every size of the company, from small start-ups to enterprises. If your company is large or likely to grow, you might want to set up multiple AWS accounts that reflect your company's structure. If you create multiple accounts, you can use the Consolidated Billing feature of AWS Organizations to combine all member accounts under a management account and receive a single bill.

AWS Pricing Calculator - AWS Pricing Calculator lets you explore AWS services and create an estimate for the cost of your use cases on AWS. You can model your solutions before building them, explore the price points and calculations behind your estimate, and find the available instance types and contract terms that meet your needs. This enables you to make informed decisions about using AWS. You cannot use this service to get a forecast of your spending for the next 12 months.

AWS Marketplace - AWS Marketplace is a digital catalog with thousands of software listings from independent software vendors that make it easy to find, test, buy, and deploy software that runs on AWS.

References:

<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/ce-what-is.html>

<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/billing-what-is.html>

<https://aws.amazon.com/aws-cost-management/>

Question 15: **Correct**

A media company uses Amazon Simple Storage Service (Amazon S3) for storing all its data. Which storage class should it consider for cost-optimal storage of the data that has random access patterns?

- **Amazon S3 Standard (S3 Standard)**
- **Amazon S3 Intelligent-Tiering (S3 Intelligent-Tiering)**

(Correct)

- **Amazon S3 Random Access (S3 Random-Access)**
- **Amazon S3 Standard-Infrequent Access (S3 Standard-IA)**

Explanation

Correct option:

Amazon S3 Intelligent-Tiering (S3 Intelligent-Tiering)

Amazon S3 Intelligent-Tiering (S3 Intelligent-Tiering) is the only cloud storage class that delivers automatic cost savings by moving objects between four access tiers when access patterns change. The S3 Intelligent-Tiering storage class is designed to optimize costs by automatically moving data to the most cost-effective access tier, without operational overhead. It works by storing objects in four access tiers: two low latency access tiers optimized for frequent and infrequent access, and two optional archive access tiers designed for asynchronous access that are optimized for rare access.

Amazon S3 Intelligent-Tiering works by storing objects in four access tiers: two low latency access tiers optimized for frequent and infrequent access, and two opt-in archive access tiers designed for asynchronous access that are optimized for rare access. Objects uploaded or transitioned to S3 Intelligent-Tiering are automatically stored in the Frequent Access tier. S3 Intelligent-Tiering works by monitoring access patterns and then moving the objects that have not been accessed in 30 consecutive days to the Infrequent Access tier. Once you have activated one or both of the archive access tiers, Amazon S3 Intelligent-Tiering will automatically move objects that haven't been accessed for 90 consecutive days to the Archive Access tier and then after 180 consecutive days of no access to the Deep Archive Access tier. If the objects are accessed later, S3 Intelligent-Tiering moves the objects back to the Frequent Access tier.

There are no retrieval fees when using the S3 Intelligent-Tiering storage class, and no additional tiering fees when objects are moved between access tiers within S3 Intelligent-Tiering. It is the ideal storage class for data sets with unknown storage access patterns, like new applications, or unpredictable access patterns, like data lakes.

Incorrect options:

Amazon S3 Standard (S3 Standard) - Amazon S3 Standard offers high durability, availability, and performance object storage for frequently accessed data. Because it delivers low latency and high throughput, S3 Standard is appropriate for a wide

variety of use cases, including cloud applications, dynamic websites, content distribution, mobile and gaming applications, and big data analytics.

Amazon S3 Standard-Infrequent Access (S3 Standard-IA) - Amazon S3 Standard-Infrequent Access (S3 Standard-IA) is for data that is accessed less frequently but requires rapid access when needed. S3 Standard-IA offers the high durability, high throughput, and low latency of S3 Standard, with a low per GB storage price and per GB retrieval fee. This combination of low cost and high performance makes S3 Standard-IA ideal for long-term storage, backups, and as a data store for disaster recovery files.

Amazon S3 Random Access (S3 Random-Access) - This is a made-up option, given only as a distractor.

Reference:

<https://aws.amazon.com/s3/storage-classes/>

Question 16: **Correct**

Which member of the AWS Snow Family is used by the Edge computing applications for IoT use cases for facilitating the collection and processing of data to gain immediate insights and then transfer the data to AWS?

- **AWS Snowposts**
- **AWS Snowmobile**
- **AWS Snowball Edge Storage Optimized**
- **AWS Snowcone**

(Correct)

Explanation

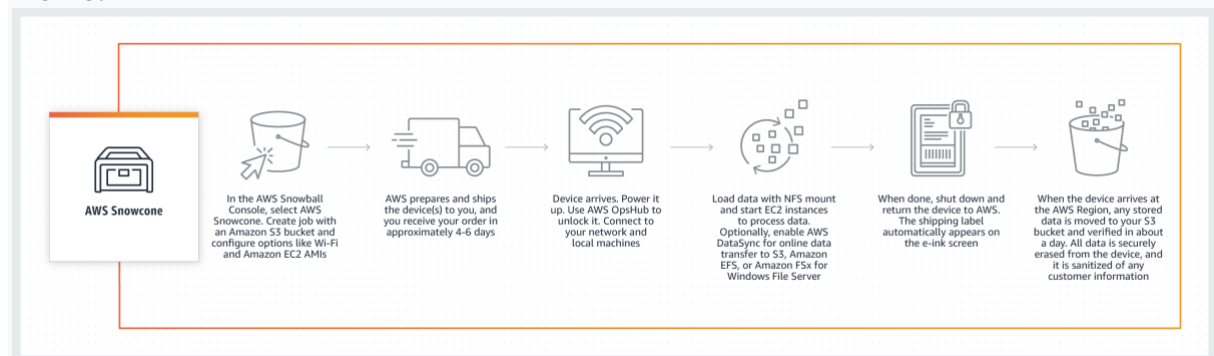
Correct option:

AWS Snowcone

AWS Snowcone is the smallest member of the AWS Snow Family of edge computing, edge storage, and data transfer devices, weighing in at 4.5 pounds (2.1 kg) with 8 terabytes of usable storage. Snowcone is ruggedized, secure, and purpose-built for use outside of a traditional data center. Its small form factor makes it a perfect fit for tight spaces or where portability is a necessity and network connectivity is unreliable. You can use Snowcone in backpacks on first responders, or for IoT, vehicular, and drone use cases. You can execute compute applications on the edge, and you can ship the device with data to AWS for offline data transfer, or you can transfer data online with AWS DataSync from edge locations.

Like AWS Snowball, Snowcone has multiple layers of security and encryption. You can use either of these services to run edge computing workloads, or to collect, process, and transfer data to AWS. Snowcone is designed for data migration needs up to 8 terabytes per device and from space-constrained environments where AWS Snowball devices will not fit.

How AWS Snowcone works:



via - <https://aws.amazon.com/snowcone/>

Feature comparison in members of Snow Family:

Feature comparison

	AWS Snowcone	AWS Snowball Edge Storage Optimized	AWS Snowball Edge Compute Optimized	AWS Snowmobile
Usage Scenario	Edge computing, Data transfer, Edge storage	Data transfer, Edge storage	Edge computing, Data transfer	Data transfer
Usable HDD Storage	8 TB	80 TB	42 TB	100 PB
Usable SSD Storage	No	1 TB	7.68 TB	No
Usable vCPUs	2 vCPUs	40 vCPUs	52 vCPUs	N/A
Usable Memory	4 GB	80 GB	208 GB	N/A
GPU	No	No	nVidia V100 (optional)	No
Onboard Computing Options	AWS IoT Greengrass Amazon EC2 AMIs	AWS IoT Greengrass Amazon EC2 AMIs	AWS IoT Greengrass Amazon EC2 AMIs	N/A
DataSync	Yes	No	No	No
Transfers via NFS	Yes	Yes	Yes	Yes
Transfers via S3 API	No	Yes	Yes	No
Network Interfaces	2x 1/10 Gbit - RJ45	2x 10 Gbit - RJ45 1x 25 Gbit - SFP+ 1x 100 Gbit - QSFP28	2x 10 Gbit - RJ45 1x 25 Gbit - SFP+ 1x 100 Gbit - QSFP28	6x 40 Gbit
Device Size	9 inches long, 6 inches wide, and 3 inches tall (227 mm x 148.6 mm x 82.65 mm)	28.3 inches long, 10.6 inches wide, and 15.5 inches tall (548 mm x 320 mm x 501 mm)	28.3 inches long, 10.6 inches wide, and 15.5 inches tall (548 mm x 320 mm x 501 mm)	N/A
Device Weight	4.5 lbs. (2.1 kg)	49.7 lbs. (22.3 kg)	49.7 lbs. (22.3 kg)	N/A
Encryption	Yes, 256-bit	Yes, 256-bit	Yes, 256-bit	Yes, 256-bit
Portability	Battery-based Operation	No	No	No
Wireless	Wi-Fi	No	No	No
Storage Clustering	No	Yes, 5-10 nodes	Yes, 5-10 nodes	N/A
HIPAA Compliant	Yes, eligible	Yes, eligible	Yes, eligible	No
Typical Job Lifetime	Offline or Online Data Transfer: Days-Weeks Edge Compute: Weeks-Years	Offline Data Transfer: Days-Weeks	Edge Compute: Weeks-Years	Data Migration: Months

via - https://aws.amazon.com/snow/#Feature_comparison

Incorrect options:

AWS Snowball Edge Storage Optimized - AWS Snowball, a part of the AWS Snow Family, is an edge computing, data migration, and edge storage device that comes in two options. Snowball Edge Storage Optimized devices provide both block storage and Amazon S3-compatible object storage, and 40 vCPUs. They are well suited for local storage and large scale data transfer.

AWS Snowball Edge Compute Optimized devices provide 52 vCPUs, block and object storage, and an optional GPU for use cases like advanced machine learning and full-motion video analysis in disconnected environments. You can use these devices for data collection, machine learning and processing, and storage in environments with intermittent connectivity or in extremely remote locations before shipping them back to AWS.

AWS Snowposts - This is a made-up option, used only as a distractor.

AWS Snowmobile- AWS Snowmobile is an Exabyte-scale data transfer service used to move extremely large amounts of data to AWS. You can transfer up to 100PB per Snowmobile, a 45-foot long ruggedized shipping container, pulled by a semi-trailer truck. Snowmobile makes it easy to move massive volumes of data to the cloud, including video libraries, image repositories, or even a complete data center migration. Transferring data with Snowmobile is more secure, fast and cost effective.

Reference:

<https://aws.amazon.com/snowcone/>

Question 17: **Correct**

Due to regulatory guidelines, a company needs to encrypt data as it passes through the different layers of its AWS architecture. The company is reviewing the capabilities of the various AWS services and their encryption options.

Which of the below services are encrypted by default and need no user intervention to enable encryption?

- **AWS Storage Gateway, Application Load Balancer (ALB), Amazon CloudFront**
- **AWS CloudTrail Logs, Amazon S3 Glacier, AWS Storage Gateway**

(Correct)

- **AWS Organizations, Amazon EC2, AWS CloudTrail Logs**
- **Amazon CloudWatch logs, Application Load Balancer (ALB), Amazon S3 Glacier**

Explanation

Correct option:

AWS CloudTrail Logs, Amazon S3 Glacier, AWS Storage Gateway

By default, all data stored by AWS Storage Gateway in S3 is encrypted server-side with Amazon S3-Managed Encryption Keys (SSE-S3). Also, you can optionally configure different gateway types to encrypt stored data with AWS Key Management Service (KMS) via the Storage Gateway API.

Data at rest stored in S3 Glacier is automatically server-side encrypted using 256-bit Advanced Encryption Standard (AES-256) with keys maintained by AWS. If you prefer to manage your own keys, you can also use client-side encryption before storing data in S3 Glacier.

By default, the log files delivered by AWS CloudTrail to your bucket are encrypted by Amazon server-side encryption with Amazon S3-managed encryption keys (SSE-S3). To provide a security layer that is directly manageable, you can instead use server-side encryption with AWS KMS-managed keys (SSE-KMS) for your CloudTrail log files. To use SSE-KMS with CloudTrail, you create and manage a KMS key, also known as a customer master key (CMK).

Incorrect options:

Amazon CloudWatch logs, Application Load Balancer (ALB), Amazon S3 Glacier - Encryption at rest and Encryption in transit is a configurable feature in Application Load Balancer.

Data protection in Elastic Load Balancing:

Encryption at rest

If you enable server-side encryption with Amazon S3-managed encryption keys (SSE-S3) for your S3 bucket for Elastic Load Balancing access logs, Elastic Load Balancing automatically encrypts each access log file before it is stored in your S3 bucket. Elastic Load Balancing also decrypts the access log files when you access them. Each log file is encrypted with a unique key, which is itself encrypted with a master key that is regularly rotated.

Encryption in transit

Elastic Load Balancing simplifies the process of building secure web applications by terminating HTTPS and TLS traffic from clients at the load balancer. The load balancer performs the work of encrypting and decrypting the traffic, instead of requiring each EC2 instance to handle the work for TLS termination. When you configure a secure listener, you specify the cipher suites and protocol versions that are supported by your application, and a server certificate to install on your load balancer. You can use AWS Certificate Manager (ACM) or AWS Identity and Access Management (IAM) to manage your server certificates. Application Load Balancers support HTTPS listeners. Network Load Balancers support TLS listeners. Classic Load Balancers support both HTTPS and TLS listeners.

via - <https://docs.aws.amazon.com/elasticloadbalancing/latest/userguide/data-protection.html>

AWS Organizations, Amazon EC2, AWS CloudTrail Logs - AWS Organizations helps you centrally manage and govern your environment as you grow and scale your AWS resources.

Instance storage provides temporary block-level storage for Amazon EC2 instances. This storage is located on disks attached physically to a host computer. By default, files stored on these disks are not encrypted. Amazon Elastic Block Store (Amazon EBS) volumes attached to EC2 instances are not encrypted by default either.

AWS Storage Gateway, Application Load Balancer (ALB), Amazon CloudFront - Amazon CloudFront does not encrypt data by default. But, encryption can be enabled if needed, by configuring encryption in transit and encryption at rest, for your distributions.

More information on data protection in Amazon CloudFront:

Encryption in Transit

To encrypt your data during transit, you configure Amazon CloudFront to require that viewers use HTTPS to request your files, so that connections are encrypted when CloudFront communicates with viewers. You also can configure CloudFront to use HTTPS to get files from your origin, so that connections are encrypted when CloudFront communicates with your origin.

For more information, see [Using HTTPS with CloudFront](#).

Field-level encryption adds an additional layer of security along with HTTPS that lets you protect specific data throughout system processing so that only certain applications can see it. By configuring field-level encryption in CloudFront, you can securely upload user-submitted sensitive information to your web servers. The sensitive information provided by your clients is encrypted at the edge closer to the user. It remains encrypted throughout your entire application stack, ensuring that only applications that need the data—and have the credentials to decrypt it—are able to do so.

For more information, see [Using Field-Level Encryption to Help Protect Sensitive Data](#).

Encryption at Rest

CloudFront uses SSDs which are encrypted for edge location points of presence (POPs), and encrypted EBS volumes for Regional Edge Caches (RECs).

via
- <https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/data-protection-summary.html>

References:

<https://docs.aws.amazon.com/awsccloudtrail/latest/userguide/best-practices-security.html>

<https://docs.aws.amazon.com/amazonglacier/latest/dev/DataEncryption.html>

<https://aws.amazon.com/storagegateway/features/>

Question 18: **Correct**

Which of the following statements are correct regarding Amazon API Gateway?
(Select two)

- **API Gateway can be configured to send data directly to Amazon Kinesis Data Stream**

(Correct)

- **If an API response is served by the cached data, it is not considered an API call for billing purposes**
- **Amazon API Gateway can call an AWS Lambda function to create the front door of a serverless application**

(Correct)

- **Amazon API Gateway does not yet support API result caching**
- **Amazon API Gateway creates RESTful APIs, Storage Gateway creates WebSocket APIs**

Explanation

Correct options:

Amazon API Gateway can call an AWS Lambda function to create the front door of a serverless application

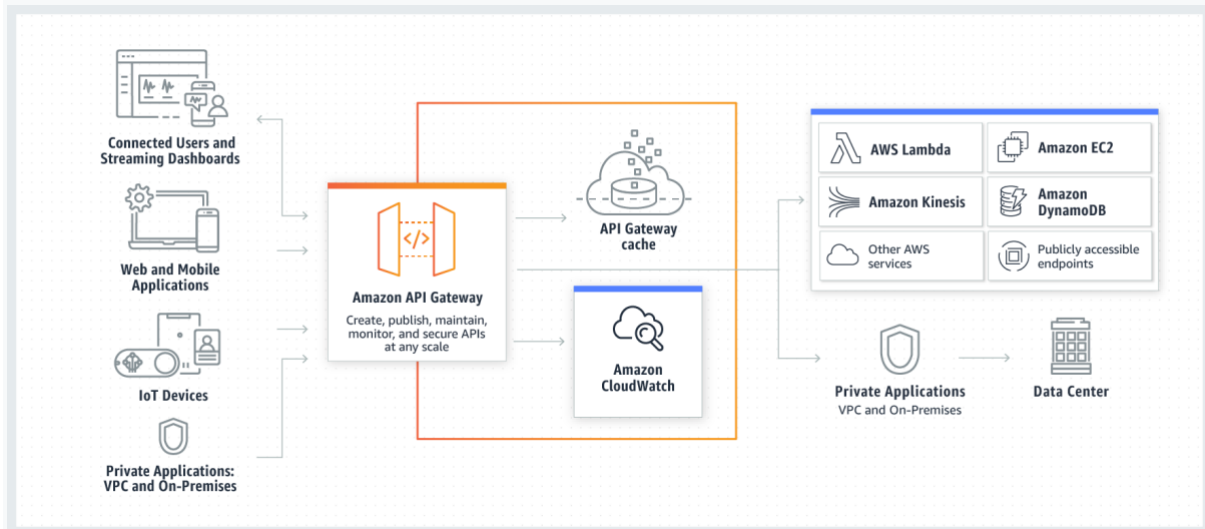
Amazon API Gateway is an AWS service for creating, publishing, maintaining, monitoring, and securing REST, HTTP, and WebSocket APIs at any scale. API developers can create APIs that access AWS or other web services, as well as data stored in the AWS Cloud.

API Gateway acts as a "front door" for applications to access data, business logic, or functionality from your backend services, such as workloads running on Amazon Elastic Compute Cloud (Amazon EC2), code running on AWS Lambda, any web application, or real-time communication applications.

API Gateway can be configured to send data directly to Amazon Kinesis Data Stream

Amazon API Gateway can execute AWS Lambda functions in your account, start AWS Step Functions state machines, or call HTTP endpoints hosted on AWS Elastic Beanstalk, Amazon EC2, and also non-AWS hosted HTTP based operations that are accessible via the public Internet. API Gateway also allows you to specify a mapping template to generate static content to be returned, helping you mock your APIs before the backend is ready. You can also integrate API Gateway with other AWS services directly – for example, you could expose an API method in API Gateway that sends data directly to Amazon Kinesis.

How Amazon API Gateway Works:



via - <https://aws.amazon.com/api-gateway/>

Incorrect options:

Amazon API Gateway creates RESTful APIs, Storage Gateway creates WebSocket APIs - Amazon API Gateway is an AWS service for creating, publishing, maintaining, monitoring, and securing REST, HTTP, and WebSocket APIs. AWS Storage Gateway is a hybrid storage solution offered by AWS.

Amazon API Gateway does not yet support API result caching - API Gateway supports result caching. You can add caching to API calls by provisioning an API Gateway cache and specifying its size in gigabytes.

If an API response is served by the cached data, it is not considered an API call for billing purposes - API calls are counted equally for billing purposes whether the response is handled by your backend operations or by the Amazon API Gateway caching operation.

References:

<https://aws.amazon.com/api-gateway/>

<https://aws.amazon.com/api-gateway/faqs/>

Question 19: **Correct**

Which of the following data sources are used by Amazon Detective to analyze events and identify potential security issues?

- **AWS CloudTrail logs, Amazon VPC Flow Logs, and Amazon GuardDuty findings**

(Correct)

- **Amazon CloudWatch Logs, AWS CloudTrail logs and Amazon Simple Storage Service (Amazon S3) Access Logs**
- **Amazon CloudWatch Logs, AWS CloudTrail logs and Amazon Inspector logs**
- **Amazon CloudWatch Logs, Amazon VPC Flow Logs and Amazon GuardDuty findings**

Explanation

Correct option:

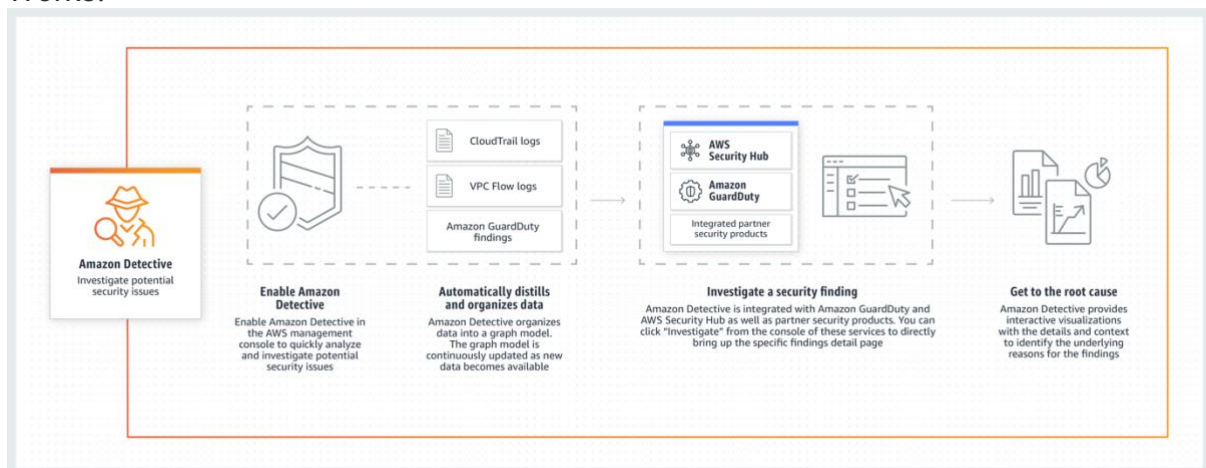
AWS CloudTrail logs, Amazon VPC Flow Logs, and Amazon GuardDuty findings

Amazon Detective can analyze trillions of events from multiple data sources such as Virtual Private Cloud (VPC) Flow Logs, AWS CloudTrail, and Amazon GuardDuty, and automatically creates a unified, interactive view of your resources, users, and the interactions between them over time.

Amazon Detective conforms to the AWS shared responsibility model, which includes regulations and guidelines for data protection. Once enabled, Amazon Detective will process data from AWS CloudTrail logs, VPC Flow Logs, and Amazon GuardDuty findings for any accounts where it has been turned on.

Amazon Detective requires that you have Amazon GuardDuty enabled on your accounts for at least 48 hours before you enable Detective on those accounts. However, you can use Detective to investigate more than just your GuardDuty findings. Amazon Detective provides detailed summaries, analyses, and visualizations of the behaviors and interactions amongst your AWS accounts, EC2 instances, AWS users, roles, and IP addresses. This information can be very useful in understanding security issues or operational account activity.

How Amazon Detective Works:



via - <https://aws.amazon.com/detective/>

Incorrect options:

Amazon CloudWatch Logs, Amazon VPC Flow Logs and Amazon GuardDuty findings

Amazon CloudWatch Logs, AWS CloudTrail logs and Amazon Simple Storage Service (Amazon S3) Access Logs

Amazon CloudWatch Logs, AWS CloudTrail logs and Amazon Inspector logs

These three options contradict the explanation provided above, so these options are incorrect.

Reference:

<https://aws.amazon.com/detective/>

Question 20: **Correct**

A company wants to establish a private, dedicated connection between AWS and its on-premises data center. Which AWS service is the right choice for this requirement?

- **Amazon API Gateway**
- **AWS Direct Connect**

(Correct)

- **AWS Site-to-Site VPN**
- **Amazon CloudFront**

Explanation

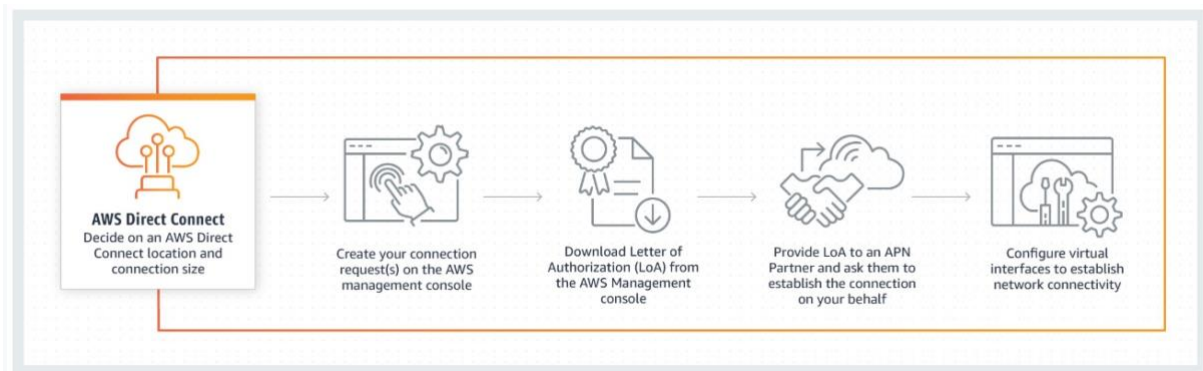
Correct option:

AWS Direct Connect

AWS Direct Connect is a cloud service solution that makes it easy to establish a dedicated network connection from your premises to AWS. Using AWS Direct Connect, you can establish private connectivity between AWS and your datacenter, office, or colocation environment, which in many cases can reduce your network costs, increase bandwidth throughput, and provide a more consistent network experience than Internet-based connections. AWS Direct Connect does not encrypt your traffic that is in transit.

AWS Direct Connect lets you establish a dedicated network connection between your network and one of the AWS Direct Connect locations. Using industry-standard 802.1q VLANs, this dedicated connection can be partitioned into multiple virtual interfaces. This allows you to use the same connection to access public resources such as objects stored in Amazon S3 using public IP address space, and private resources such as Amazon EC2 instances running within an Amazon Virtual Private Cloud (VPC) using private IP space while maintaining network separation between the public and private environments. Virtual interfaces can be reconfigured at any time to meet your changing needs.

How AWS Direct Connect works:



via - <https://aws.amazon.com/directconnect/>

Incorrect options:

AWS Site-to-Site VPN - AWS virtual private network (VPN) solutions establish secure connections between your on-premises networks, remote offices, client devices, and the AWS global network. AWS VPN is comprised of two services: AWS Site-to-Site VPN and AWS Client VPN. AWS Site-to-Site VPN creates encrypted tunnels between your network and your Amazon Virtual Private Clouds or AWS Transit Gateway(s).

Amazon CloudFront - Amazon CloudFront is a fast content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to customers globally with low latency, high transfer speeds, all within a developer-friendly environment. Amazon CloudFront offers the most advanced security capabilities, including field-level encryption and HTTPS support, seamlessly integrated with AWS Shield, AWS web application firewall (AWS WAF), and Amazon Route 53 to protect against multiple types of attacks including network and application layer DDoS attacks.

Amazon API Gateway - Amazon API Gateway is a fully managed service that makes it easy for developers to create, publish, maintain, monitor, and secure APIs at any scale. APIs act as the "front door" for applications to access data, business logic, or functionality from your backend services. Using API Gateway, you can create RESTful APIs and WebSocket APIs that enable real-time two-way communication applications. API Gateway supports containerized and serverless workloads, as well as web applications.

References:

<https://aws.amazon.com/directconnect/>

<https://aws.amazon.com/vpn/>

Question 21: **Correct**

A gaming company needs compute and storage services close to edge locations in order to ensure ultra-low latency for end-users and devices that connect through mobile networks. Which AWS service is the best fit for this requirement?

- **AWS Snowball Edge**

- **AWS Wavelength**

(Correct)

- **AWS Snowmobile**
- **AWS Outposts**

Explanation

Correct option:

AWS Wavelength

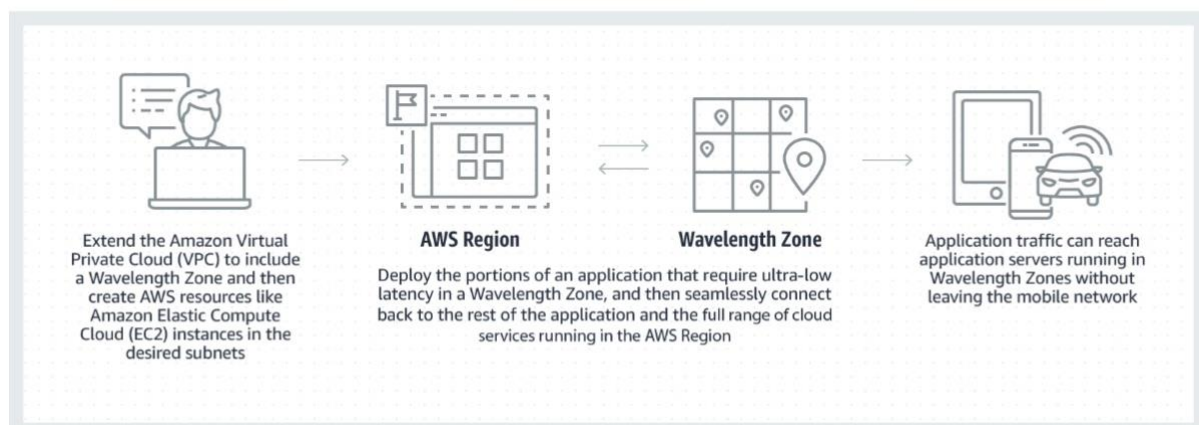
AWS Wavelength is an AWS Infrastructure offering optimized for mobile edge computing applications. Wavelength Zones are AWS infrastructure deployments that embed AWS compute and storage services within cloud service provider (CSP) data centers at the edge of the 5G network, so application traffic from 5G devices can reach application servers running in Wavelength Zones without leaving the telecommunications network. This avoids the latency that would result from application traffic having to traverse multiple hops across the Internet to reach their destination, enabling customers to take full advantage of the latency and bandwidth benefits offered by modern 5G networks.

AWS enterprise customers that build applications to serve their own use-cases such as IoT, live media production, and industrial automation can use Wavelength to deliver low-latency solutions. Customers with edge data processing needs such as image and video recognition, inference, data aggregation, and responsive analytics can use Wavelength to perform low-latency operations and processing right where their data is generated, reducing the need to move large amounts of data to be processed in centralized locations.

How AWS Wavelength works:

How it works

Getting started is easy, you simply log-in to the AWS Management Console and enable the Wavelength Zones you want to use for your account.



via - <https://aws.amazon.com/wavelength/>

Incorrect options:

AWS Outposts - AWS Outposts is designed for workloads that need to remain on-premises due to latency requirements, where customers want that workload to run seamlessly with the rest of their other workloads in AWS. AWS Outposts are fully managed and configurable compute and storage racks built with AWS-designed hardware that allow customers to run compute and storage on-premises, while seamlessly connecting to AWS's broad array of services in the cloud.

You should also note another service called AWS Local Zones, which is a new type of AWS infrastructure designed to run workloads that require single-digit millisecond latency in more locations, like video rendering and graphics intensive, virtual desktop applications. Not every customer wants to operate their own on-premises data center, while others may be interested in getting rid of their local data center entirely. Local Zones allow customers to gain all the benefits of having compute and storage resources closer to end-users, without the need to own and operate their own data center infrastructure.

AWS Snowball Edge - AWS Snowball Edge is a type of Snowball device with on-board storage and compute power for select AWS capabilities. Snowball Edge can do local processing and edge-computing workloads in addition to transferring data between your local environment and the AWS Cloud. Snowball edge cannot be used to optimize connections through mobile networks.

AWS Snowmobile - AWS Snowmobile is an Exabyte-scale data transfer service used to move extremely large amounts of data to AWS. You can transfer up to 100PB per Snowmobile, a 45-foot long ruggedized shipping container, pulled by a semi-trailer truck. Snowmobile makes it easy to move massive volumes of data to the cloud, including video libraries, image repositories, or even a complete data center migration. Transferring data with Snowmobile is more secure, fast and cost effective. Snowmobile cannot be used to optimize connections through mobile networks.

Reference:

<https://aws.amazon.com/wavelength/>

Question 22: **Correct**

Which of the following is a repository service that helps in maintaining application dependencies via integration with commonly used package managers and build tools like Maven, Gradle, npm, etc?

- **AWS CodeStar**
- **AWS CodeArtifact**

(Correct)

- **AWS CodeCommit**
- **AWS CodeBuild**

Explanation

Correct option:

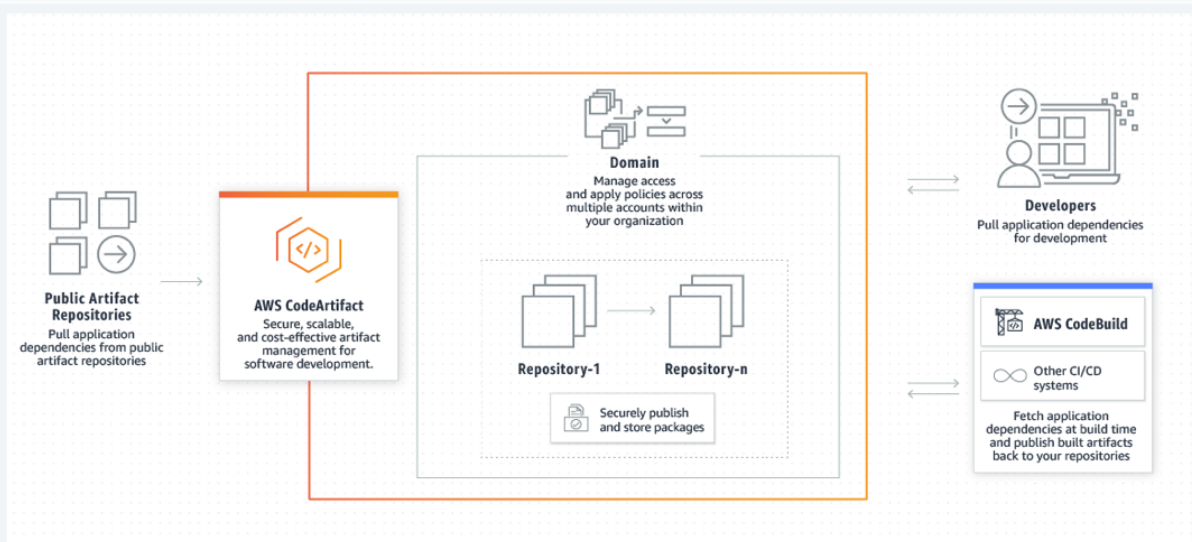
AWS CodeArtifact

AWS CodeArtifact is a fully managed artifact repository service that makes it easy for organizations of any size to securely store, publish, and share software packages used in their software development process. CodeArtifact can be configured to automatically fetch software packages and dependencies from public artifact repositories so developers have access to the latest versions. CodeArtifact works with commonly used package managers and build tools like Maven, Gradle, npm, yarn, twine, pip, and NuGet making it easy to integrate into existing development workflows.

Development teams often rely on both open-source software packages and those packages built within their organization. IT leaders need to be able to control access to and validate the safety of these software packages. Teams need a way to find up-to-date packages that have been approved for use by their IT leaders. To address these challenges, IT leaders turn to central artifact repository services to store and share packages. However, existing solutions often require teams to purchase licenses for software solutions that are complex to set up, scale, and operate.

AWS CodeArtifact is a pay-as-you-go artifact repository service that scales based on the needs of the organization. With CodeArtifact, there is no software to update or servers to manage. In just a few clicks, IT leaders can set up central repositories that make it easy for development teams to find and use the software packages they need. IT leaders can also approve packages and control distribution across the organization, ensuring development teams consume software packages that are safe for use.

How AWS CodeArtifact works:



via - <https://aws.amazon.com/codeartifact/>

Incorrect options:

AWS CodeCommit - AWS CodeCommit is a fully-managed source control service that hosts secure Git-based repositories. It makes it easy for teams to collaborate on code in a secure and highly scalable ecosystem. CodeCommit eliminates the need to operate your own source control system or worry about scaling its infrastructure. You can use CodeCommit to securely store anything from source code to binaries, and it works seamlessly with your existing Git tools.

AWS CodeBuild - AWS CodeBuild is a fully managed continuous integration service that compiles source code, runs tests, and produces software packages that are ready to deploy. With CodeBuild, you don't need to provision, manage, and scale your own build servers. CodeBuild scales continuously and processes multiple builds concurrently, so your builds are not left waiting in a queue. You can get started quickly by using prepackaged build environments, or you can create custom build environments that use your own build tools.

AWS CodeStar - AWS CodeStar is a cloud-based development service that provides the tools you need to quickly develop, build, and deploy applications on AWS. With AWS CodeStar, you can set up your entire continuous delivery toolchain in minutes, allowing you to start releasing code faster. AWS CodeStar makes it easy for your whole team to work together securely, with built-in role-based policies that allow you to easily manage access and add owners, contributors, and viewers to your projects.

Each CodeStar project includes development tools, including AWS CodePipeline, AWS CodeCommit, AWS CodeBuild, and AWS CodeDeploy, that can be used on their own and with existing AWS applications.

Reference:

<https://aws.amazon.com/codeartifact/>

Question 23: **Correct**

Which of the following statements are correct regarding the AWS Support Plans?
(Select two)

- **A designated Technical Account Manager is available only for AWS Enterprise Support plan**

(Correct)

- **Contextual guidance based on customer use-case, is available only for the AWS Enterprise support plan**
- **Infrastructure Event Management is included for free for AWS Business Support and AWS Enterprise Support plans and can be extended to AWS Developer Support plan for an additional fee**
- **AWS Concierge service is available for the AWS Business Support and AWS Enterprise Support plans**
- **Both Basic and AWS Developer Support plans have access to the core Trusted Advisor checks only**

(Correct)

Explanation

Correct options:

A designated Technical Account Manager is available only for AWS Enterprise Support plan

A designated Technical Account Manager (TAM) is the primary point of contact who provides guidance, architectural review, and ongoing communication to keep the customer informed and well prepared as they plan, deploy, and proactively optimize their AWS solutions. As the cornerstone of the Enterprise Support plan, your TAM serves as your guide and advocate, focused on delivering the right resources to support the success and ongoing operational health of your AWS infrastructure.

Both Basic and AWS Developer Support plans have access to the core Trusted Advisor checks only

AWS Trusted Advisor draws upon best practices learned from the aggregated operational history of serving hundreds of thousands of AWS customers. Trusted Advisor inspects your AWS environment and alerts you to opportunities to save money, improve system availability and performance, or help close security gaps. Access to the core Trusted Advisor checks, and guidance to provision your resources following best practices to increase performance and improve security are only part of the Basic and Developer support plans.

Incorrect options:

AWS Concierge service is available for the AWS Business Support and AWS Enterprise Support plans - AWS Concierge is a senior customer service agent who is assigned to your account when you subscribe to an Enterprise or qualified Reseller Support plan. This Concierge agent is your primary point of contact for billing or account inquiries; when you don't know whom to call, they will find the right people to help. In most cases, the AWS Concierge is available during regular business hours in your headquarters' geography.

Contextual guidance based on customer use-case, is available only for the AWS Enterprise support plan - Contextual guidance on how services fit together to meet your specific use-case, workload, or application is part of the Business support plan.

Infrastructure Event Management is included for free for AWS Business Support and AWS Enterprise Support plans and can be extended to AWS Developer Support plan for an additional fee - AWS Infrastructure Event Management is a short-term engagement with AWS Support, available as part of the Enterprise-level Support product offering (also available to the AWS Enterprise On-Ramp Support plan subject to a cap of one per year), and available for additional purchase for AWS Business Support plan users. AWS Infrastructure Event Management partners with your technical and project resources to gain a deep understanding of your use case and provide architectural and scaling guidance for an event. Common use-case examples for AWS Event Management include advertising launches, new product

launches, and infrastructure migrations to AWS. Infrastructure Event Management cannot be extended to a AWS Developer Support plan for an additional fee.

Reference:

<https://aws.amazon.com/premiumsupport/plans/>

Question 24: **Correct**

A company is looking at a service/tool to automate and minimize the time spent on keeping the server images up-to-date. These server images are used by Amazon Elastic Compute Cloud (Amazon EC2) instances as well as the on-premises systems.

Which AWS service will help achieve the company's need?

- **Amazon EC2 Amazon Machine Image (AMI)**
- **AWS Systems Manager (Amazon Simple Systems Manager (SSM))**
- **Amazon EC2 Image Builder**

(Correct)

- **AWS CloudFormation templates**

Explanation

Correct option:

Amazon EC2 Image Builder

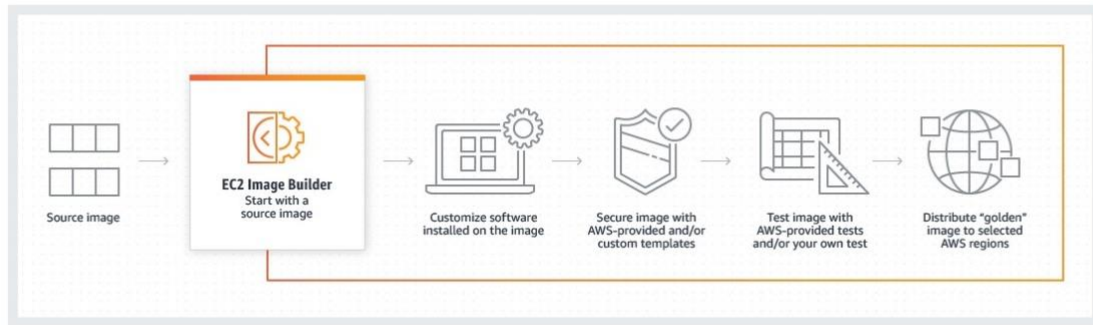
Amazon EC2 Image Builder simplifies the building, testing, and deployment of Virtual Machine and container images for use on AWS or on-premises.

Keeping Virtual Machine (VM) and container images up-to-date can be time-consuming, resource-intensive, and error-prone. Currently, customers either manually update and snapshot VMs or have teams that build automation scripts to maintain images.

Amazon EC2 Image Builder significantly reduces the effort of keeping images up-to-date and secure by providing a simple graphical interface, built-in automation, and AWS-provided security settings. With Image Builder, there are no manual steps for updating an image nor do you have to build your own automation pipeline.

How to use Amazon EC2 Image Builder to automate server image creation:

Image Builder provides a one-stop-shop to automate image management processes. Customers can generate an automated pipeline with an intuitive wizard in the AWS console to produce compliant Linux and Windows Server images for use on AWS and on-premises. When software updates become available, Image Builder automatically produces a new image and distributes it to stipulated AWS regions after running tests on it.



Examples of **customize software installed on the image** includes: 1/ Applications (build environments, business productivity tools, and databases) 2/ OS Updates 3/ Security patches.

Examples of **secure image with AWS-provided and/or custom templates** includes: 1/ Ensure security patches are applied, 2/ Enforce strong passwords, 3/ Turn on full disk encryption, 4/ Close all non-essential open ports, 5/ Enable software firewall, 6/ Enable logging/audit controls.

Examples of **test image with AWS-provided test and/or your own test** includes: 1/ Test that AMI can boot, 2/ Test that sample application can be run, 3/ Test specific patch has been applied, 5/ Test security policy.

via - <https://aws.amazon.com/image-builder/>

Incorrect options:

Amazon EC2 Amazon Machine Image (AMI) - An Amazon Machine Image (AMI) provides the information required to launch an instance. You must specify an AMI when you launch an EC2 instance. An Amazon Machine Image (AMI) is the basic unit of deployment in Amazon EC2 and is one of the types of images you can create with Image Builder.

AWS CloudFormation templates - AWS CloudFormation simplifies provisioning and management on AWS. You can create templates for the service or application architectures you want and have AWS CloudFormation use those templates for quick and reliable provisioning of the services or applications.

AWS Systems Manager (Amazon Simple Systems Manager (SSM)) - AWS Systems Manager (formerly known as SSM) is an AWS service that you can use to view and control your infrastructure on AWS. Using the Systems Manager console, you can view operational data from multiple AWS services and automate operational tasks across your AWS resources.

Instances used to build images and run tests using Image Builder must have access to the Systems Manager service. All build activity is orchestrated by SSM Automation. The SSM Agent will be installed on the source image if it is not already present, and it will be removed before the image is created.

References:

<https://aws.amazon.com/image-builder/>

<https://docs.aws.amazon.com/imagebuilder/latest/userguide/image-builder-setting-up.html>

Question 25: **Correct**

A company provides you with a completed product that is run and managed by the company itself. As a customer, you only use the product without worrying about maintaining or managing the product.

Which cloud computing model does this kind of product belong to?

- **Infrastructure as a Service (IaaS)**
- **Product as a Service (Paas)**
- **Platform as a Service (PaaS)**
- **Software as a Service (SaaS)**

(Correct)

Explanation

Correct option:

Software as a Service (SaaS)

Software as a Service provides you with a completed product that is run and managed by the service provider. In most cases, people referring to Software as a Service are referring to end-user applications. With a SaaS offering, you do not have to think about how the service is maintained or how the underlying infrastructure is managed; you only need to think about how you will use that particular piece of software.

A common example of a SaaS application is the web-based email where you can send and receive email without having to manage feature additions to the email product or maintaining the servers and operating systems that the email program is running on.

Incorrect options:

Infrastructure as a Service (IaaS) - Infrastructure as a service (IaaS), sometimes abbreviated as IaaS, contains the basic building blocks for cloud IT and typically provides access to networking features, computers (virtual or on dedicated hardware), and data storage space. Infrastructure as a Service provides you with the highest level of flexibility and management control over your IT resources and is most similar to existing IT resources that many IT departments and developers are familiar with today.

Platform as a Service (PaaS) - Platform as a Service (PaaS) as a service removes the need for organizations to manage the underlying infrastructure (usually hardware and operating systems) and allow you to focus on the deployment and management of your applications. This helps you be more efficient as you don't need to worry about resource procurement, capacity planning, software maintenance, patching, or any of the other undifferentiated heavy lifting involved in running your application.

Product as a Service (Paas) - This is a made-up option, given only as a distractor.

Reference:

<https://aws.amazon.com/types-of-cloud-computing/>

Question 26: **Correct**

Which of the following statements are true about AWS Elastic Beanstalk? (Select two)

- **AWS Elastic Beanstalk supports web applications built on different languages. But, AWS Elastic Beanstalk cannot be used for deploying non-web applications**
- **AWS Elastic Beanstalk supports Java, .NET, PHP, but does not support Docker web applications**
- **With AWS Elastic Beanstalk, you can quickly deploy and manage applications in the AWS Cloud without having to learn about the infrastructure that runs those applications**

(Correct)

- **There is no additional charge for AWS Elastic Beanstalk. You pay only for the underlying AWS resources that your application consumes**

(Correct)

- **AWS Elastic Beanstalk automates the details of capacity provisioning, load balancing, and application deployment, creating an environment that runs a version of your application. However, auto-scaling functionality cannot be automated using AWS Elastic Beanstalk**

Explanation

Correct options:

With AWS Elastic Beanstalk, you can quickly deploy and manage applications in the AWS Cloud without having to learn about the infrastructure that runs those applications

There is no additional charge for AWS Elastic Beanstalk. You pay only for the underlying AWS resources that your application consumes

With AWS Elastic Beanstalk, you can quickly deploy and manage applications in the AWS Cloud without having to learn about the infrastructure that runs those applications. Elastic Beanstalk reduces management complexity without restricting choice or control. You simply upload your application, and AWS Elastic Beanstalk automatically handles the details of capacity provisioning, load balancing, scaling, and application health monitoring.

AWS Elastic Beanstalk supports applications developed in Go, Java, .NET, Node.js, PHP, Python, and Ruby. When you deploy your application, AWS Elastic Beanstalk builds the selected supported platform version and provisions one or more AWS resources, such as Amazon EC2 instances, to run your application.

There is no additional charge for AWS Elastic Beanstalk. You pay only for the underlying AWS resources that your application consumes.

Incorrect options:

AWS Elastic Beanstalk supports Java, .NET, PHP, but does not support Docker web applications - AWS Elastic Beanstalk supports Java, .NET, PHP, Node.js, Python, Ruby, Go, and Docker web applications.

AWS Elastic Beanstalk automates the details of capacity provisioning, load balancing, and application deployment, creating an environment that runs a version of your application. However, auto-scaling functionality cannot be automated using AWS Elastic Beanstalk - AWS Elastic Beanstalk automates the details of capacity provisioning, load balancing, auto-scaling, and application deployment, creating an environment that runs a version of your application. You can simply upload your deployable code (e.g., WAR file), and AWS Elastic Beanstalk does the rest.

AWS Elastic Beanstalk supports web applications built on different languages. But, AWS Elastic Beanstalk cannot be used for deploying non-web applications - AWS Elastic Beanstalk supports Java, .NET, PHP, Node.js, Python, Ruby, Go, and Docker, and is ideal for web applications. However, due to Elastic Beanstalk's open architecture, non-web applications can also be deployed using AWS Elastic Beanstalk.

References:

<https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/Welcome.html>

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

Question 27: **Correct**

Which of the following represents the correct scenario where an Auto Scaling group's (ASG) predictive scaling can be effectively used to maintain the required number of AWS resources?

- To manage a fixed number of resources in the Auto Scaling group
- To help configure a scaling policy to keep the average aggregate CPU utilization of your Auto Scaling group at 40 percent
- To help configure a CloudWatch Amazon Simple Queue Service (Amazon SQS) metric like `ApproximateNumberOfMessagesVisible` for scaling the group based on the value of the metric
- To manage a workload that exhibits recurring load patterns that are specific to the day of the week or the time of day

(Correct)

Explanation

Correct option:

To manage a workload that exhibits recurring load patterns that are specific to the day of the week or the time of day

Predictive scaling uses machine learning to predict capacity requirements based on historical data from CloudWatch. The machine learning algorithm consumes the available historical data and calculates capacity that best fits the historical load pattern, and then continuously learns based on new data to make future forecasts more accurate.

Predictive scaling is well suited for situations where you have:

1. Cyclical traffic, such as high use of resources during regular business hours and low use of resources during evenings and weekends
2. Recurring on-and-off workload patterns, such as batch processing, testing, or periodic data analysis
3. Applications that take a long time to initialize, causing a noticeable latency impact on application performance during scale-out events

Incorrect options:

To help configure a scaling policy to keep the average aggregate CPU utilization of your Auto Scaling group at 40 percent - Target tracking scaling policy is the best fit for this use case. With target tracking scaling policies, you select a scaling metric and set a target value. Amazon EC2 Auto Scaling creates and manages the CloudWatch alarms that trigger the scaling policy and calculates the scaling adjustment based on the metric and the target value. The scaling policy adds or removes capacity as required to keep the metric at, or close to, the specified target value.

To help configure a CloudWatch Amazon Simple Queue Service (Amazon SQS) metric like `ApproximateNumberOfMessagesVisible` for scaling the group based on the value of the metric - Target tracking scaling policy with `backlog per instance metric` is the best fit for this use case. That's because the number of messages in your SQS queue does not solely define the number of instances needed. The number of instances in your Auto Scaling group can be driven by multiple factors, including how long it takes to process a message and the acceptable amount of latency (queue delay).

To manage a fixed number of resources in the Auto Scaling group - Maintaining current instance levels at all times to a fixed number is a basic way to configure an ASG. Predictive Scaling is not needed to maintain a fixed number of resources.

References:

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/ec2-auto-scaling-predictive-scaling.html>

https://docs.aws.amazon.com/autoscaling/ec2/userguide/scaling_plan.html

Question 28: **Correct**

A healthcare company wants to implement a continuous replication based disaster recovery mechanism and provide fast, reliable recovery of physical, virtual, and cloud-based servers into AWS Cloud. Which of the following represents the best-fit solution for this use case?

- **AWS Snowball Edge**
- **CloudCover Disaster Recovery**
- **AWS Storage Gateway**
- **CloudEndure Disaster Recovery**

(Correct)

Explanation

Correct option:

CloudEndure Disaster Recovery

CloudEndure Disaster Recovery, available from the AWS Marketplace, continuously replicates server-hosted applications and server-hosted databases from any source into AWS using block-level replication of the underlying server. CloudEndure Disaster Recovery enables you to use AWS Cloud as a disaster recovery Region for an on-premises workload and its environment. It can also be used for disaster recovery of AWS hosted workloads if they consist only of applications and databases hosted on EC2 (i.e. not RDS).

Features of CloudEndure Disaster Recovery:

1. Continuous replication: CloudEndure Disaster Recovery provides continuous, asynchronous, block-level replication of your source machines into a staging area. This allows you to achieve sub-second Recovery Point Objectives (RPOs), since up-to-date applications are always ready to be spun up on AWS if a disaster strikes.
2. Low-cost staging area: Data is continually kept in sync in a lightweight staging area in your target AWS Region. The staging area contains low-cost resources that are automatically provisioned and managed by CloudEndure Disaster Recovery. This eliminates the need for duplicate resources and significantly reduces your disaster recovery total cost of ownership (TCO).
3. Automated machine conversion and orchestration: In the event of a disaster or drill, CloudEndure Disaster Recovery triggers a highly automated machine conversion process and a scalable orchestration engine that quickly spins up thousands of machines in your target AWS Region in parallel. This enables Recovery Time Objectives (RTOs) of minutes. Unlike application-level solutions, CloudEndure Disaster Recovery replicates entire machines, including OS, system state configuration, system disks, databases, applications, and files.
4. Point-in-time recovery: Granular point-in-time recovery allows you to recover applications and IT environments that have been corrupted as a result of accidental system changes, ransomware, or other malicious attacks. In such cases, you can launch applications from a previous consistent point in time

rather than launching applications in their most up-to-date state. During the recovery, you can select either the latest state or an earlier state from a list of points in time.

5. Easy, non-disruptive drills: With CloudEndure Disaster Recovery, you can conduct disaster recovery drills without disrupting your source environment or risking data loss. During drills, CloudEndure Disaster Recovery spins up machines in your target AWS Region in complete isolation to avoid network conflicts and performance impact.
6. Wide application and infrastructure support: Because CloudEndure Disaster Recovery replicates data at the block level, you can use it for all applications and databases that run on supported versions of Windows and Linux OS.

CloudEndure Disaster Recovery:

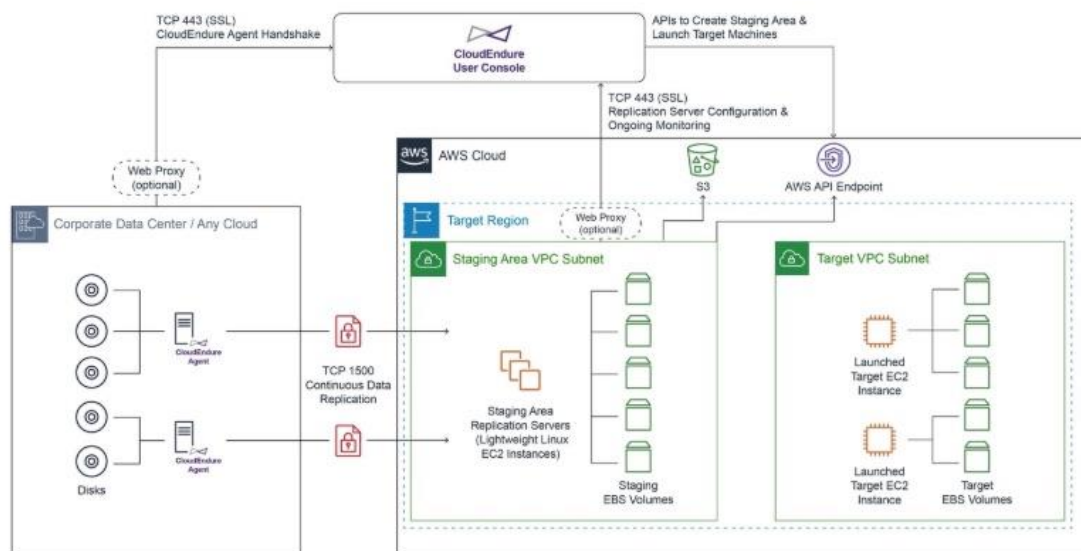


Figure 10 - CloudEndure Disaster Recovery architecture

via - <https://docs.aws.amazon.com/whitepapers/latest/disaster-recovery-workloads-on-aws/disaster-recovery-options-in-the-cloud.html>

Incorrect options:

AWS Snowball Edge - AWS Snowball Edge is a type of Snowball device with on-board storage and compute power for select AWS capabilities. Snowball Edge can do local processing and edge-computing workloads in addition to transferring data between your local environment and the AWS Cloud. AWS Snowball Edge cannot be used to optimize connections through mobile networks. It cannot be used for continuous replication based disaster recovery.

AWS Storage Gateway - AWS Storage Gateway is a hybrid cloud storage service that gives you on-premises access to virtually unlimited cloud storage. Storage Gateway provides a standard set of storage protocols such as iSCSI, SMB, and NFS, which

allow you to use AWS storage without rewriting your existing applications. You can take point-in-time snapshots of your Volume Gateway volumes in the form of Amazon EBS snapshots. Using this approach, you can easily supply data from your on-premises applications to your applications running on Amazon EC2 if you require additional on-demand compute capacity for data processing or replacement capacity for disaster recovery purposes. However, Storage Gateways cannot be used for continuous replication based disaster recovery.

CloudCover Disaster Recovery - This is a made-up option and has been added as a distractor.

References:

<https://docs.aws.amazon.com/whitepapers/latest/disaster-recovery-workloads-on-aws/disaster-recovery-options-in-the-cloud.html>

Question 29: **Correct**

Which of the following services/tools offers a user-friendly graphical user interface to manage AWS Snowball devices without a need for command-line interface or REST APIs?

- **AWS Transfer Family**
- **AppStream 2.0**
- **AWS OpsHub**

(Correct)

- **AWS OpsWorks**

Explanation

Correct option:

AWS OpsHub

AWS OpsHub is a graphical user interface you can use to manage your AWS Snowball devices, enabling you to rapidly deploy edge computing workloads and simplify data migration to the cloud. With just a few clicks in AWS OpsHub, you have the full functionality of the Snowball devices at your fingertips; you can unlock and configure devices, drag-and-drop data to devices, launch applications, and monitor device metrics.

Previously, customers operated Snowball devices by either entering commands into a command-line interface or by using REST APIs. Now with AWS OpsHub, you have an easier way to deploy and manage even large fleets of Snowball devices, all while operating without an internet connection.

AWS OpsHub takes all the existing operations available in the Snowball API and presents them as a simple graphical user interface. This interface helps you quickly and easily migrate data to the AWS Cloud and deploy edge computing applications on Snow Family Devices.

AWS OpsHub provides a unified view of AWS services that are running on Snow Family Devices and automates operational tasks through AWS Systems Manager. With AWS OpsHub, users with different levels of technical expertise can easily manage a large number of Snow Family Devices. With just a few clicks, you can unlock devices, transfer files, manage Amazon EC2 instances, and monitor device metrics.

When your Snow device arrives at your site, you download, install, and launch the AWS OpsHub application on a client machine, such as a laptop. After installation, you can unlock the device and start managing it and using supported AWS services locally. AWS OpsHub provides a dashboard that summarizes key metrics such as storage capacity and active instances on your device. It also provides a selection of the AWS services that are supported on the Snow Family Devices. Within minutes, you can begin transferring files to the device.

Incorrect options:

AppStream 2.0 - Amazon AppStream 2.0 is a fully managed non-persistent application and desktop streaming service. You centrally manage your desktop applications on AppStream 2.0 and securely deliver them to any computer. You can easily scale to any number of users across the globe without acquiring, provisioning, and operating hardware or infrastructure. AppStream 2.0 is built on AWS, so you benefit from a data center and network architecture designed for the most security-sensitive organizations. This is not a tool for AWS Snowball devices.

AWS OpsWorks - AWS OpsWorks is a configuration management service that provides managed instances of Chef and Puppet. Chef and Puppet are automation platforms that allow you to use code to automate the configurations of your servers. OpsWorks lets you use Chef and Puppet to automate how servers are configured, deployed, and managed across your Amazon EC2 instances or on-premises compute environments.

AWS Transfer Family - The AWS Transfer Family is the aggregated name of AWS Transfer for SFTP, AWS Transfer for FTPS, and AWS Transfer for FTP. The AWS Transfer Family offers fully managed support for the transfer of files over SFTP, FTPS, and FTP directly into and out of Amazon S3 or Amazon EFS.

Reference:

<https://docs.aws.amazon.com/snowball/latest/developer-guide/aws-opshub.html>

Question 30: **Correct**

A financial consulting company is looking for automated reference deployments, that will speed up the process of deploying its financial solutions on AWS Cloud. The reference deployment should be able to deploy most of the well-known functions of financial services and leave space for customizations, if necessary.

Which AWS service will help achieve this requirement?

- **Amazon Quicksight**
- **AWS Elastic Beanstalk**
- **AWS CloudFormation**
- **AWS Partner Solutions(formerly Quick Starts)**

(Correct)

Explanation

Correct option:

AWS Partner Solutions(formerly Quick Starts)

AWS Partner Solutions are automated reference deployments for key workloads on the AWS Cloud. Each Partner Solution launches, configures, and runs the AWS compute, network, storage, and other services required to deploy a specific workload on AWS, using AWS best practices for security and availability.

Partner Solutions are accelerators that condense hundreds of manual procedures into just a few steps. They are customizable and designed for production.

Partner Solutions include: 1. A reference architecture for the deployment 2. AWS CloudFormation templates (JSON or YAML scripts) that automate and configure the deployment 3. A deployment guide, which explains the architecture and implementation in detail, and provides instructions for customizing the deployment

Partner Solutions also include integrations that extend the cloud-based contact center functionality provided by Amazon Connect with key services and solutions from APN Partners—for customer relationship management (CRM), workforce optimization (WFO), analytics, unified communications (UC), and other use cases.

Incorrect options:

AWS CloudFormation - AWS CloudFormation gives you an easy way to model a collection of related AWS and third-party resources, provision them quickly and consistently, and manage them throughout their lifecycles, by treating infrastructure as code. A CloudFormation template describes your desired resources and their dependencies so you can launch and configure them together as a stack.

AWS Elastic Beanstalk - AWS Elastic Beanstalk is an easy-to-use service for deploying and scaling web applications and services developed with Java, .NET, PHP, Node.js, Python, Ruby, Go, and Docker on familiar servers such as Apache, Nginx, Passenger, and IIS. You can simply upload your code and Elastic Beanstalk automatically handles the deployment, from capacity provisioning, load balancing, auto-scaling to application health monitoring. At the same time, you retain full control over the AWS resources powering your application and can access the underlying resources at any time.

Amazon Quicksight - Amazon QuickSight is a scalable, serverless, embeddable, machine learning-powered business intelligence (BI) service built for the cloud.

QuickSight lets you easily create and publish interactive BI dashboards that include Machine Learning-powered insights. With QuickSight, you can quickly embed interactive dashboards into your applications, websites, and portals.

Reference:

<https://aws.amazon.com/solutions/partners/faq/>

Question 31: **Correct**

Which of the following use-cases can be solved using the Amazon Forecast service?

- **Predict the web traffic of a website for the next few weeks**

(Correct)

- **To recommend personalized products for users based on their previous purchases**
- **To develop and test fully functional machine learning models**
- **Document search service that can extract answers from text within documents**

Explanation

Correct option:

Predict the web traffic of a website for the next few weeks

Amazon Forecast is a fully managed service that uses machine learning to deliver highly accurate forecasts. Based on the same technology used at Amazon.com, Amazon Forecast uses machine learning to combine time series data with additional variables to build forecasts. Amazon Forecast requires no machine learning experience to get started. You only need to provide historical data, plus any additional data that you believe may impact your forecasts.

Amazon Forecast can be used to forecast any time-series data, such as retail demand, manufacturing demand, travel demand, revenue, IT capacity, logistics, and web traffic.

Incorrect options:

To develop and test fully functional machine learning models - Amazon SageMaker is the correct service for this requirement. Amazon SageMaker is a fully managed service that provides every developer and data scientist with the ability to build, train, and deploy machine learning (ML) models quickly. SageMaker removes the heavy lifting from each step of the machine learning process to make it easier to develop high-quality models.

Document search service that can extract answers from text within documents - Amazon Kendra is the best fit for this use case. Amazon Kendra is an intelligent search service powered by machine learning. Kendra reimagines enterprise search for your websites and applications so your employees and customers can easily find

the content they are looking for, even when it's scattered across multiple locations and content repositories within your organization.

To recommend personalized products for users based on their previous purchases - Amazon Personalize is useful in creating recommendations. Amazon Personalize makes it easy for developers to build applications capable of delivering a wide array of personalization experiences, including specific product recommendations, personalized product re-ranking, and customized direct marketing.

Reference:

<https://aws.amazon.com/forecast/>

Question 32: **Correct**

Historically, IT departments had to over-provision for peak demand. IT professionals may bring this legacy mindset to the table when they build their cloud infrastructure leading to over-provisioned resources and unnecessary costs. Right-sizing of resources is necessary to reduce infrastructure costs while still using cloud functionality optimally.

Which feature of the AWS Cloud refers to right-sizing the resources?

- **Resiliency**
- **Elasticity**

(Correct)

- **Horizontal scaling**
- **Reliability**

Explanation

Correct option:

Elasticity

Most people, when thinking of cloud computing, think of the ease with which they can procure resources when needed. This is only one aspect of elasticity. The other aspect is to contract when they no longer need resources. Scale-out and scale in. Scale up and scale down.

The ability to acquire resources as you need them and release resources when you no longer need them. In the cloud, you want to do this automatically.

Some AWS services do this as part of their service: Amazon Simple Storage Service (Amazon S3), Amazon Simple Queue Service (Amazon SQS), Amazon Simple Notification Service (Amazon SNS), Amazon Simple Email Service (Amazon SES), Amazon Aurora, etc. Some require vertical scaling, like Amazon Relational Database Service (Amazon RDS). Others integrate with AWS Auto Scaling, like Amazon EC2, Amazon ECS, AWS Fargate, Amazon EKS, and Amazon DynamoDB. Amazon Aurora Serverless and Amazon Athena also qualify as elastic.

Incorrect options:

Reliability - The ability of a workload to perform its intended function correctly and consistently when it's expected to. This includes the ability to operate and test the workload through its total lifecycle.

Resiliency - The ability of a workload to recover from infrastructure or service disruptions, dynamically acquire computing resources to meet demand, and mitigate disruptions, such as misconfigurations or transient network issues.

Horizontal scaling - A "horizontally scalable" system can increase capacity by adding more computers to the system. This is in contrast to a "vertically scalable" system, which is constrained to running its processes on only one computer; in such systems, the only way to increase performance is to add more resources into one computer in the form of faster (or more) CPUs, memory or storage.

References:

<https://wa.aws.amazon.com/wellarchitected/2020-07-02T19-33-23/wat.concept.elasticity.en.html>

<https://wa.aws.amazon.com/wellarchitected/2020-07-02T19-33-23/wat.concepts.wa-concepts.en.html>

Question 33: **Correct**

Which free tool helps to review the state of your workloads and compares them to the latest AWS architectural best practices after you have answered a series of questions about your workload?

- **AWS Well-Architected Framework**
- **AWS Trusted Advisor**
- **AWS Well-Architected Tool**

(Correct)

- **AWS Technical Account Manager (TAM)**

Explanation

Correct option:

AWS Well-Architected Tool

The AWS Well-Architected Tool helps you review the state of your workloads and compares them to the latest AWS architectural best practices. The tool is based on the AWS Well-Architected Framework, developed to help cloud architects build secure, high-performing, resilient, and efficient application infrastructure.

To use this free tool, available in the AWS Management Console, just define your workload and answer a set of questions regarding operational excellence, security, reliability, performance efficiency, and cost optimization. The AWS Well-Architected

Tool then provides a plan on how to architect for the cloud using established best practices.

The AWS Well-Architected Tool gives you access to knowledge and best practices used by AWS architects, whenever you need it. You answer a series of questions about your workload, and the tool delivers an action plan with step-by-step guidance on how to build better workloads for the cloud.

How AWS Well-Architected Tool works:



A. Identify the workload to document. Then answer a series of questions about your architecture.

B. Review your answers against the five pillars established by the Well-Architected Framework that are visually depicted via the icons in the column above; a) Operational excellence, b) Security, c) Reliability, d) Performance efficiency, & e) Cost optimization.

C. You can 1) get videos and documentation 2) generate a report that summarizes your workload review, & 3) see the results of reviews in a single dashboard.

via - <https://aws.amazon.com/well-architected-tool/>

Incorrect options:

AWS Well-Architected Framework - AWS Well-Architected Framework helps cloud architects build secure, high-performing, resilient, and efficient infrastructure for their applications and workloads. Based on six pillars — operational excellence, security, reliability, performance efficiency, cost optimization and sustainability — AWS Well-Architected provides a consistent approach for customers and partners to evaluate architectures, and implement designs that can scale over time. This is a framework based on which Well-Architected Tool and AWS Trusted Advisor offer guidance, suggestions and improvements.

AWS Trusted Advisor - AWS Trusted Advisor is an online tool that provides you real-time guidance to help you provision your resources following AWS best practices. Trusted Advisor checks help optimize your AWS infrastructure, increase security and performance, reduce your overall costs, and monitor service limits. Whether establishing new workflows, developing applications, or as part of ongoing improvement, take advantage of the recommendations provided by Trusted Advisor on a regular basis to help keep your solutions provisioned optimally.

While AWS Trusted advisor checks are based on the support plan the customer has. Both Basic and Developer support plans have access to the 7 core Trusted Advisor checks. Unlike documentation-based guidance (like AWS Well-Architected Tool), this

tool provides recommendations against AWS Well Architected Framework best practices and is able to track against your current AWS architecture.

AWS Technical Account Manager (TAM) - With AWS Enterprise Support, you get 24x7 technical support from high-quality engineers, tools, and technology to automatically manage the health of your environment, consultative architectural guidance delivered in the context of your applications and use-cases, and a designated Technical Account Manager (TAM).

A Technical Account Manager (TAM) is your designated technical point of contact who helps you onboard, provides advocacy and guidance to help plan and build solutions using best practices, coordinates access to subject matter experts, assists with case management, presents insights and recommendations on your AWS spend, workload optimization, and event management, and proactively keeps your AWS environment healthy.

Reference:

<https://aws.amazon.com/well-architected-tool/>

Question 34: **Correct**

Which feature/functionality will help you organize your AWS resources, manage and automate tasks on large numbers of resources at a time?

- **AWS Resource Groups**

(Correct)

- **Tags**
- **AWS Organizations**
- **Amazon WorkSpaces**

Explanation

Correct option:

AWS Resource Groups

In AWS, a resource is an entity that you can work with. Examples include an Amazon EC2 instance, an AWS CloudFormation stack, or an Amazon S3 bucket. If you work with multiple resources, you might find it useful to manage them as a group rather than move from one AWS service to another for each task. If you manage large numbers of related resources, such as EC2 instances that make up an application layer, you likely need to perform bulk actions on these resources at one time.

You can use AWS Resource Groups to organize your AWS resources. Resource groups make it easier to manage and automate tasks on large numbers of resources at a time. Resource Groups feature permissions are at the account level. As long as users who are sharing your account have the correct IAM permissions, they can work with the resource groups that you create.

Incorrect options:

AWS Organizations - AWS Organizations helps you centrally manage and govern your environment as you grow and scale your AWS resources. Using AWS Organizations, you can programmatically create new AWS accounts and allocate resources, group accounts to organize your workflows, apply policies to accounts or groups for governance, and simplify billing by using a single payment method for all of your accounts.

Tags - To help you manage your instances, images, and other Amazon EC2 resources, you can assign your own metadata to each resource in the form of tags. Tags enable you to categorize your AWS resources in different ways, for example, by purpose, owner, or environment. Tags are properties of a resource. Resource Groups allow you to easily create, maintain, and view a collection of resources that share common tags.

Amazon WorkSpaces - Amazon WorkSpaces enables you to provision virtual, cloud-based Microsoft Windows or Amazon Linux desktops for your users, known as WorkSpaces. Amazon WorkSpaces eliminates the need to procure and deploy hardware or install complex software. You can quickly add or remove users as your needs change. Users can access their virtual desktops from multiple devices or web browsers.

References:

<https://docs.aws.amazon.com/ARG/latest/userguide/welcome.html>

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Using_Tags.html

<https://aws.amazon.com/organizations/>

Question 35: **Correct**

Which of the following statements are correct regarding the health monitoring and reporting capabilities supported by AWS Elastic Beanstalk? (Select two)

- **AWS Elastic Beanstalk provides only basic health reporting system; Combined with Elastic Load Balancing (ELB), they provide advanced health check features**
- **The basic health reporting system that provides information about the health of instances in an AWS Elastic Beanstalk environment does not use health checks performed by Elastic Load Balancing (ELB)**
- **In a single instance environment, AWS Elastic Beanstalk determines the instance's health by monitoring the Elastic Load Balancing (ELB) health settings**
- **With basic health reporting, the AWS Elastic Beanstalk service does not publish any metrics to Amazon CloudWatch**

(Correct)

- **The AWS Elastic Beanstalk health monitoring can determine that the environment's Auto Scaling group is available and has a minimum of at least one instance**

(Correct)

Explanation

Correct options:

The AWS Elastic Beanstalk health monitoring can determine that the environment's Auto Scaling group is available and has a minimum of at least one instance

In addition to Elastic Load Balancing health checks, AWS Elastic Beanstalk monitors resources in your environment and changes health status to red if they fail to deploy, are not configured correctly, or become unavailable. These checks confirm that: 1. The environment's Auto Scaling group is available and has a minimum of at least one instance. 2. The environment's security group is available and is configured to allow incoming traffic on port 80. 3. The environment CNAME exists and is pointing to the right load balancer. 4. In a worker environment, the Amazon Simple Queue Service (Amazon SQS) queue is being polled at least once every three minutes.

With basic health reporting, the AWS Elastic Beanstalk service does not publish any metrics to Amazon CloudWatch

With basic health reporting, the AWS Elastic Beanstalk service does not publish any metrics to Amazon CloudWatch. The CloudWatch metrics used to produce graphs on the Monitoring page of the environment console are published by the resources in your environment.

Incorrect options:

AWS Elastic Beanstalk provides only basic health reporting system; Combined with Elastic Load Balancing (ELB), they provide advanced health check features - This option has been added as a distractor.

In a single instance environment, AWS Elastic Beanstalk determines the instance's health by monitoring the Elastic Load Balancing (ELB) health settings - In a single instance or worker tier environment, AWS Elastic Beanstalk determines the instance's health by monitoring its Amazon EC2 instance status. Elastic Load Balancing health settings, including HTTP health check URLs cannot be used in these environment types.

The basic health reporting system that provides information about the health of instances in an AWS Elastic Beanstalk environment does not use health checks performed by Elastic Load Balancing (ELB) - The basic health reporting system provides information about the health of instances in an AWS Elastic Beanstalk environment based on health checks performed by Elastic Load Balancing for load-balanced environments, or Amazon Elastic Compute Cloud (Amazon EC2) for single-instance environments.

Reference:

<https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/using-features.healthstatus.html#monitoring-basic-additionalchecks>

Question 36: **Correct**

AWS Support offers five support plans for its customers. Which of the following features are covered as part of the AWS Basic Support Plan? (Select two)

- **One-on-one responses to account and billing questions**

(Correct)

- **Use-case guidance – What AWS products, features, and services to use for best supporting your specific needs**
- **Client-side diagnostic tools**
- **Service health checks**

(Correct)

- **Infrastructure event management**

Explanation

Correct options:

One-on-one responses to account and billing questions

Service health checks

AWS Support offers five support plans: Basic support plan, AWS Developer support plan, AWS Business support plan, AWS Enterprise-On-Ramp support plan, and AWS Enterprise Support plan.

The Basic plan offers support for account and billing questions and service quota increases. The other plans offer a number of technical support cases with pay-by-the-month pricing and no long-term contracts. All AWS customers automatically have 24/7 access to these features of the Basic support plan: 1. One-on-one responses to account and billing questions 2. Support forums 3. Service health checks 4. Documentation, technical papers, and best practice guides

Features of AWS Support Plans

AWS Support offers five support plans:

- Basic
- Developer
- Business
- Enterprise On-Ramp
- Enterprise

Basic Support offers support for account and billing questions and service quota increases. The other plans offer a number of technical support cases with pay-by-the-month pricing and no long-term contracts.

All AWS customers automatically have 24x7 access to these features of Basic Support:

- One-on-one responses to account and billing questions
- Support forums
- Service health checks
- Documentation, technical papers, and best practice guides

Customers with a Developer Support plan have access to these additional features:

- Best practice guidance
- Client-side diagnostic tools
- Building-block architecture support: guidance on how to use AWS products, features, and services together
- Supports an unlimited number of support cases that can be opened by one primary contact, which is the [AWS account root user](#).

In addition, customers with a Business, Enterprise On-Ramp, or Enterprise Support plan have access to these features:

- Use-case guidance – What AWS products, features, and services to use to best support your specific needs.
- [AWS Trusted Advisor](#) – A feature of AWS Support, which inspects customer environments and identifies opportunities to save money, close security gaps, and improve system reliability and performance. You can access all Trusted Advisor checks.
- The AWS Support API to interact with Support Center and Trusted Advisor. You can use the AWS Support API to automate support case management and Trusted Advisor operations.
- Third-party software support – Help with Amazon Elastic Compute Cloud (Amazon EC2) instance operating systems and configuration. Also, help with the performance of the most popular third-party software components on AWS. Third-party software support isn't available for customers on Basic or Developer Support plans.
- Supports an unlimited number of AWS Identity and Access Management (IAM) users who can open technical support cases.

In addition, customers with an Enterprise On-Ramp or Enterprise Support plan have access to these features:

- Application architecture guidance – Consultative guidance on how services fit together to meet your specific use case, workload, or application.
- Infrastructure event management – Short-term engagement with AWS Support to get a deep understanding of your use case. After analysis, provide architectural and scaling guidance for an event.
- Technical account manager – Work with a technical account manager (TAM) for your specific use cases and applications.
- White-glove case routing.
- Management business reviews.

via - <https://docs.aws.amazon.com/awssupport/latest/user/aws-support-plans.html>

Incorrect options:

Client-side diagnostic tools - Customers with any of the Developer, Business, Enterprise-On-Ramp, Enterprise support plans have access to client-side diagnostic tools.

Use-case guidance – What AWS products, features, and services to use for best supporting your specific needs - Customers with any of the Business, Enterprise-On-Ramp, Enterprise support plans have access to use-case guidance.

Infrastructure event management - Customers with AWS Enterprise-On-Ramp or Enterprise support plan have access to infrastructure event management which is a short-term engagement with AWS Support to get a deep understanding of customer use-cases. After analysis, AWS provides architectural and scaling guidance for an event.

References:

<https://docs.aws.amazon.com/awssupport/latest/user/aws-support-plans.html>

<https://docs.aws.amazon.com/awssupport/latest/user/getting-started.html>

Question 37: **Correct**

Which pillar of AWS Well-Architected Framework focuses on using IT and computing resources efficiently, while considering the right resource types and sizes based on workload requirements?

- **Reliability Pillar**
- **Operational Excellence Pillar**
- **Performance Efficiency Pillar**

(Correct)

- **Cost Optimization Pillar**

Explanation

Correct option:

Performance Efficiency Pillar

The performance efficiency pillar focuses on using IT and computing resources efficiently. Key topics include selecting the right resource types and sizes based on workload requirements, monitoring performance, and making informed decisions to maintain efficiency as business needs evolve.

Performance Efficiency uses the following design principles to help achieve and maintain efficient workloads in the cloud: Democratize advanced technologies, Go global in minutes, Use serverless architectures, Experiment more often and Consider mechanical sympathy.

More information on the Design principles of the Performance Efficiency

pillar: via - <https://d1.awsstatic.com/whitepapers/architecture/AWS-Performance-Efficiency-Pillar.pdf>

Incorrect options:

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

Cost Optimization Pillar - The cost optimization pillar focuses on avoiding unnecessary costs. Key topics include understanding and controlling where the money is being spent, selecting the most appropriate and right number of resource types, analyzing spend over time, and scaling to meet business needs without overspending.

Reliability Pillar - The reliability pillar focuses on ensuring a workload performs its intended function correctly and consistently when it's expected to. A resilient workload quickly recovers from failures to meet business and customer demand. Key topics include distributed system design, recovery planning, and how to handle change.

Reference:

<https://aws.amazon.com/architecture/well-architected/>

Question 38: **Correct**

Per the AWS Shared Responsibility Model, management of which of the following AWS services is the responsibility of the customer?

- **Amazon Elastic Compute Cloud (Amazon EC2)**

(Correct)

- AWS Elastic Beanstalk
- Amazon DynamoDB
- Amazon Simple Storage Service (Amazon S3)

Explanation

Correct option:

Amazon Elastic Compute Cloud (Amazon EC2)

Security and Compliance is a shared responsibility between AWS and the customer. This shared model can help relieve the customer's operational burden as AWS operates, manages, and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the service operates.

"Security of the Cloud" is the responsibility of AWS - 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.

"Security in the Cloud" is the responsibility of the customer. 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 the 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.

Incorrect options:

Amazon Simple Storage Service (Amazon S3)

Amazon DynamoDB

AWS Elastic Beanstalk

For abstracted services, such as Amazon S3, Amazon DynamoDB and for managed services such as AWS Elastic Beanstalk, 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.

Reference:

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

Question 39: **Correct**

Which of the following AWS services is delivered globally rather than regionally?

- **AWS Snowmobile**
- **Amazon WorkSpaces**

(Correct)

- **Amazon Elastic File System (Amazon EFS)**
- **Amazon Simple Storage Service (Amazon S3) buckets**

Explanation

Correct option:

Amazon WorkSpaces

AWS offers a broad set of global cloud-based products including compute, storage, database, analytics, networking, machine learning and AI, mobile, developer tools, IoT, security, enterprise applications, and much more.

Due to the nature of the service, some AWS services are delivered globally rather than regionally, such as Amazon Route 53, Amazon Chime, Amazon WorkDocs, Amazon WorkMail, Amazon WorkSpaces, Amazon WorkLink.

Amazon WorkSpaces is a managed, secure Desktop-as-a-Service (DaaS) solution. You can use Amazon WorkSpaces to provision either Windows or Linux desktops in just a few minutes and quickly scale to provide thousands of desktops to workers across the globe.

Incorrect options:

Amazon Simple Storage Service (Amazon S3) buckets - You specify an AWS Region when you create your Amazon S3 bucket and hence the S3 buckets are region-specific. For S3 on AWS Outposts, your data is stored in your Outpost on-premises environment, unless you manually choose to transfer it to an AWS Region.

Amazon Elastic File System (Amazon EFS) - Amazon Elastic File System (Amazon EFS) is AWS region-based service. You can use AWS DataSync to copy files between different AWS regions.

AWS Snowmobile - AWS Snowmobile can be made available for use with AWS services in specific AWS regions and hence is a region-specific service. Once all the data is copied into Snowmobile, Snowmobile will be returned to your designated AWS region where your data will be uploaded into the AWS storage services you have selected, such as S3 or Glacier.

Reference:

https://aws.amazon.com/about-aws/global-infrastructure/regions_az/

Question 40: **Correct**

A company is looking at real-time processing of streaming big data for their ad-tech platform. Which of the following AWS services is the right choice for this requirement?

- **Amazon Redshift**
- **Amazon Kinesis Data Streams**

(Correct)

- **Amazon Simple Queue Service (Amazon SQS)**
- **Amazon EMR**

Explanation

Correct option:

Amazon Kinesis Data Streams

Amazon Kinesis Data Streams enables you to build custom applications that process or analyze streaming data for specialized needs. You can continuously add various types of data such as clickstreams, application logs, and social media to an Amazon Kinesis data stream from hundreds of thousands of sources. Within seconds, the data will be available for your Amazon Kinesis Applications to read and process from the stream.

Amazon Kinesis Data Streams is useful to rapidly move the data off data producers and then continuously process the data, be it to transform the data before emitting it to a data store, run real-time metrics and analytics, or derive more complex data streams for further processing. The following are typical scenarios for using Amazon Kinesis Data Streams: accelerated log and data feed intake, real-time metrics and reporting, real-time data analytics, complex stream processing.

How Amazon Kinesis Data Streams Work:



via - <https://aws.amazon.com/kinesis/data-streams/>

Incorrect options:

Amazon Simple Queue Service (Amazon SQS) - Amazon Simple Queue Service (Amazon SQS) offers a reliable, highly scalable hosted queue for storing messages as they travel between computers. Amazon SQS lets you easily move data between distributed application components and helps you build applications in which messages are processed independently (with message-level ack/fail semantics), such as automated workflows.

Amazon Redshift - With Amazon Redshift, you can query and combine exabytes of structured and semi-structured data across your data warehouse, operational database, and data lake using standard SQL. Redshift lets you easily save the results of your queries back to your S3 data lake using open formats, like Apache Parquet, so that you can do additional analytics from other analytics services like Amazon EMR, Amazon Athena, and Amazon SageMaker. Redshift is a data warehousing solution and not a real-time streaming service.

Amazon EMR - Amazon EMR makes it easy to set up, operate, and scale your big data environments by automating time-consuming tasks like provisioning capacity and tuning clusters. EMR is not suitable as a real-time streaming service.

Reference:

<https://aws.amazon.com/kinesis/data-streams/>

Question 41: **Correct**

By default, which of the following events are logged by AWS CloudTrail?

- **Data events and Insights events**
- **Management events**

(Correct)

- **AWS CloudTrail Insights events**

- **Data events**

Explanation

Correct option:

Management events

An event in AWS CloudTrail is the record of activity in an AWS account. This activity can be an action taken by a user, role, or service that is monitorable by CloudTrail. CloudTrail events provide a history of both API and non-API account activity made through the AWS Management Console, AWS SDKs, command line tools, and other AWS services.

There are three types of events that can be logged in CloudTrail: management events, data events, and AWS CloudTrail Insights events.

By default, AWS CloudTrail logs all management events and does not include data events or Insights events. Additional charges apply for data and Insights events. All event types use the same CloudTrail JSON log format.

Management events provide information about management operations that are performed on resources in your AWS account. These are also known as control plane operations. Examples include registering devices, configuring rules for routing data, setting up logging etc.

Incorrect options:

Data events - Data events provide information about the resource operations performed on or in a resource. These are also known as data plane operations. Data events are often high-volume activities. The following data types are recorded: Amazon S3 object-level API activity, AWS Lambda function execution activity, Amazon S3 object-level API activity on AWS Outposts.

Data events are not logged by default when you create a trail. To record AWS CloudTrail data events, you must explicitly add to a trail the supported resources or resource types for which you want to collect activity. Additional charges apply for logging data events.

AWS CloudTrail Insights events - AWS CloudTrail Insights events capture unusual activity in your AWS account. If you have Insights events enabled, and CloudTrail detects unusual activity, Insights events are logged to a different folder or prefix in the destination S3 bucket for your trail. You can also see the type of insight and the incident time period when you view Insights events on the CloudTrail console.

Insights events are disabled by default when you create a trail. To record AWS CloudTrail Insights events, you must explicitly enable Insights event collection on a new or existing trail. Additional charges apply for logging CloudTrail Insights events.

Data events and Insights events - As mentioned above, this option is incorrect.

Reference:

<https://docs.aws.amazon.com/awsccloudtrail/latest/userguide/cloudtrail-concepts.html#cloudtrail-concepts-events>

Question 42: **Correct**

A manufacturing company is looking at a service that can offer AWS infrastructure, AWS services, APIs, and tools to its on-premises data center for running low latency applications.

Which of the following service/tool is the best fit for the given requirement?

- **AWS Local Zones**
- **AWS Snow Family**
- **AWS Outposts**

(Correct)

- **AWS Wavelength**

Explanation

Correct option:

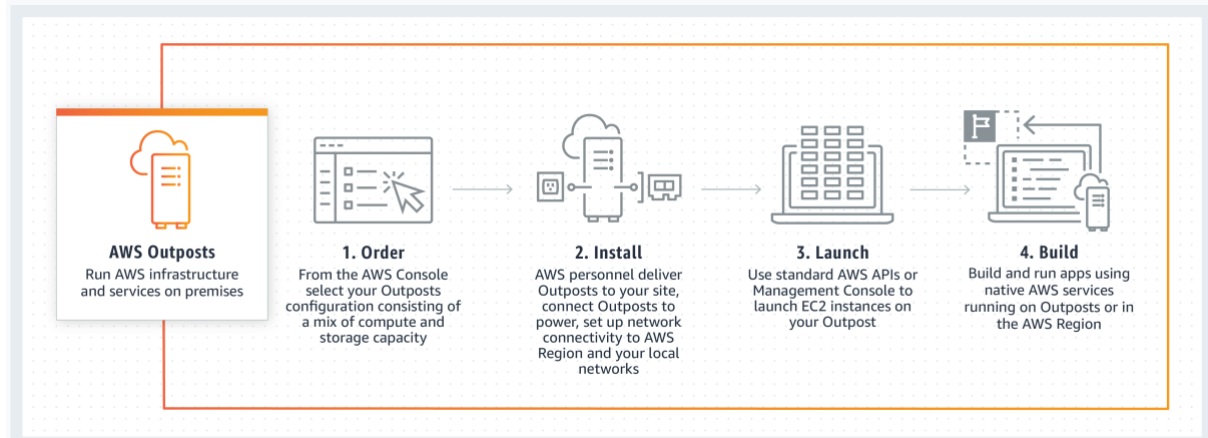
AWS Outposts

AWS Outposts is a fully managed service that offers the same AWS infrastructure, AWS services, APIs, and tools to virtually any data center, co-location space, or on-premises facility for a truly consistent hybrid experience. AWS Outposts is ideal for workloads that require low latency access to on-premises systems, local data processing, data residency, and migration of applications with local system interdependencies.

AWS compute, storage, database, and other services run locally on Outposts, and you can access the full range of AWS services available in the Region to build, manage, and scale your on-premises applications using familiar AWS services and tools.

You can use AWS Outposts to support your applications that have low latency or local data processing requirements. These applications may need to generate near real-time responses to end-user applications or need to communicate with other on-premises systems or control on-site equipment. These can include workloads running on factory floors for automated operations in manufacturing, real-time patient diagnosis or medical imaging, and content and media streaming. You can use Outposts to securely store and process customer data that needs to remain on-premises or in countries where there is no AWS region. You can run data-intensive workloads on Outposts and process data locally when transmitting data to the cloud is expensive and wasteful and for better control on data analysis, back-up, and restoration.

How AWS Outposts Works:



via - <https://aws.amazon.com/outposts/>

Incorrect options:

AWS Snow Family - The AWS Snow Family is a collection of physical devices that help migrate large amounts of data into and out of the cloud without depending on networks. This helps you apply the wide variety of AWS services for analytics, file systems, and archives to your data. You can use AWS Snow Family services for data transfer and occasional pre-processing on location. Some large data transfer examples include cloud migration, disaster recovery, data center relocation, and/or remote data collection projects. These projects typically require you to migrate large amounts of data in the shortest, and most cost-effective, amount of time.

AWS Wavelength - AWS Wavelength is an AWS Infrastructure offering optimized for mobile edge computing applications. Wavelength Zones are AWS infrastructure deployments that embed AWS compute and storage services within communications service providers' (CSP) data centers at the edge of the 5G network, so application traffic from 5G devices can reach application servers running in Wavelength Zones without leaving the telecommunications network.

AWS Local Zones - AWS Local Zones are a type of AWS infrastructure deployment that places AWS compute, storage, database, and other select services close to a large population, industry, and IT centers. With AWS Local Zones, you can easily run applications that need single-digit millisecond latency closer to end-users in a specific geography. AWS Local Zones are ideal for use cases such as media & entertainment content creation, real-time gaming, live video streaming, and machine learning inference.

Reference:

<https://aws.amazon.com/outposts/>

Question 43: **Correct**

A company has defined a baseline that mentions the number of AWS resources to be used for different stages of application testing. However, the company realized

that employees are not adhering to the guidelines and provisioning additional resources via API calls, resulting in higher testing costs.

Which AWS service will help the company raise alarms whenever the baseline resource numbers are crossed?

- **AWS X-Ray**
- **AWS CloudTrail Insights**

(Correct)

- **AWS Config**
- **Amazon Detective**

Explanation

Correct option:

AWS CloudTrail Insights

AWS CloudTrail Insights helps AWS users identify and respond to unusual activity associated with write API calls by continuously analyzing CloudTrail management events.

Insights events are logged when AWS CloudTrail detects unusual write management API activity in your account. If you have CloudTrail Insights enabled, and CloudTrail detects unusual activity, Insights events are delivered to the destination S3 bucket for your trail. You can also see the type of insight and the incident time period when you view Insights events on the CloudTrail console. Unlike other types of events captured in a CloudTrail trail, Insights events are logged only when CloudTrail detects changes in your account's API usage that differ significantly from the account's typical usage patterns.

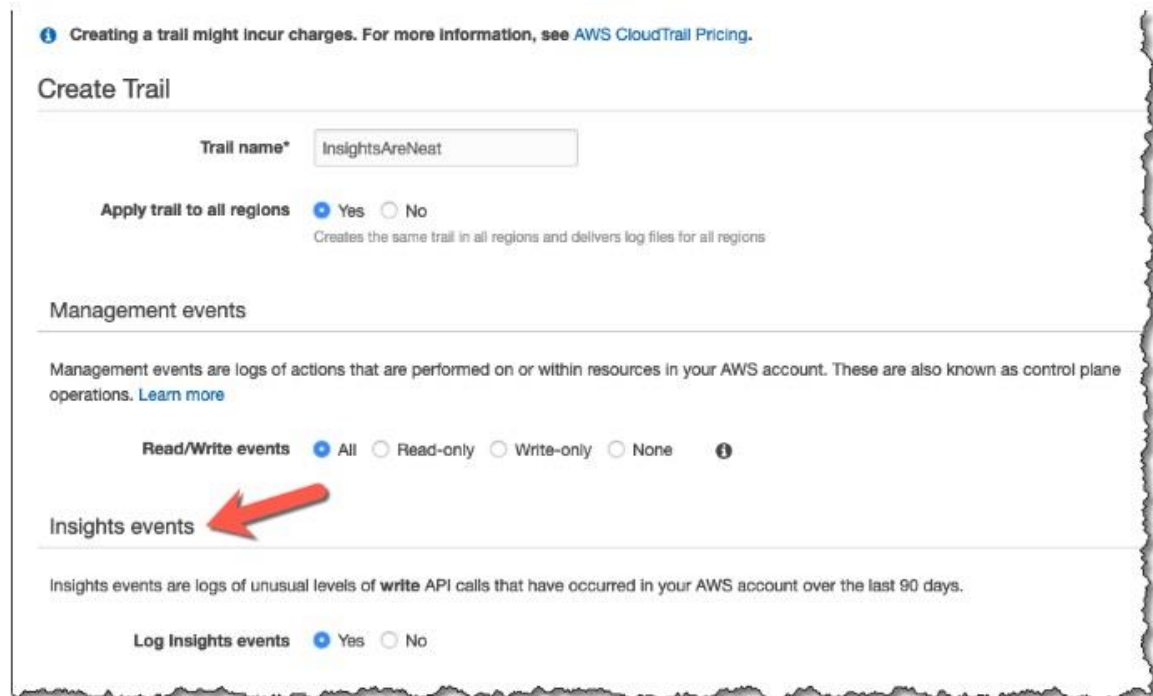
AWS CloudTrail Insights can help you detect unusual API activity in your AWS account by raising Insights events. CloudTrail Insights measures your normal patterns of API call volume, also called the baseline, and generates Insights events when the volume is outside normal patterns.

AWS CloudTrail Insights continuously monitors CloudTrail write management events, and uses mathematical models to determine the normal levels of API and service event activity for an account. CloudTrail Insights identifies behavior that is outside normal patterns, generates Insights events, and delivers those events to a /CloudTrail-Insight folder in the chosen destination S3 bucket for your trail. You can also access and view Insights events in the AWS Management Console for CloudTrail.

Identify and Respond to Unusual API Activity using AWS CloudTrail Insights:

Enabling AWS CloudTrail Insights

CloudTrail tracks user activity and API usage. It provides an event history of AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command line tools, and other AWS services. With the launch of **AWS CloudTrail Insights**, you can enable machine learning models that detect unusual activity in these logs with just a few clicks. **AWS CloudTrail Insights** will analyze historical API calls, identifying usage patterns and generating Insight Events for unusual activity.



Creating a trail might incur charges. For more information, see [AWS CloudTrail Pricing](#).

Create Trail

Trail name*

Apply trail to all regions ☒ Yes ☐ No
Creates the same trail in all regions and delivers log files for all regions

Management events

Management events are logs of actions that are performed on or within resources in your AWS account. These are also known as control plane operations. [Learn more](#)

Read/Write events ☒ All ☐ Read-only ☐ Write-only ☐ None ⓘ

Insights events

Insights events are logs of unusual levels of **write** API calls that have occurred in your AWS account over the last 90 days.

Log Insights events ☒ Yes ☐ No

via - <https://aws.amazon.com/blogs/aws/announcing-cloudtrail-insights-identify-and-respond-to-unusual-api-activity/>

Incorrect options:

AWS X-Ray - AWS X-Ray helps developers analyze and debug production, distributed applications, such as those built using a microservices architecture. With X-Ray, you can understand how your application and its underlying services are performing to identify and troubleshoot the root cause of performance issues and errors. X-Ray provides an end-to-end view of requests as they travel through your application, and shows a map of your application's underlying components. X-Ray is not for tracking user actions when interacting with the AWS systems.

Amazon Detective - Amazon Detective simplifies the process of investigating security findings and identifying the root cause. Amazon Detective analyzes trillions of events from multiple data sources such as VPC Flow Logs, AWS CloudTrail logs, and Amazon GuardDuty findings and automatically creates a graph model that provides you with a unified, interactive view of your resources, users, and the interactions between them over time.

AWS Config - AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources. Config continuously monitors and records your AWS resource configurations and allows you to automate the

evaluation of recorded configurations against desired configurations. With Config, you can review changes in configurations and relationships between AWS resources, dive into detailed resource configuration histories, and determine your overall compliance against the configurations specified in your internal guidelines. This enables you to simplify compliance auditing, security analysis, change management, and operational troubleshooting.

Reference:

<https://docs.aws.amazon.com/awscloudtrail/latest/userguide/logging-insights-events-with-cloudtrail.html>

Question 44: **Correct**

A supply chain company is looking for a database that provides a centrally verifiable history of all changes made to data residing in it. This functionality is critical for the product and needs to be available off the shelf without the need for any customizations.

Which of the following databases is the right choice for this use case?

- **Amazon Quantum Ledger Database (Amazon QLDB)**

(Correct)

- Amazon Timestream
- Amazon Neptune
- Amazon Managed Blockchain

Explanation

Correct option:

Amazon Quantum Ledger Database (Amazon QLDB)

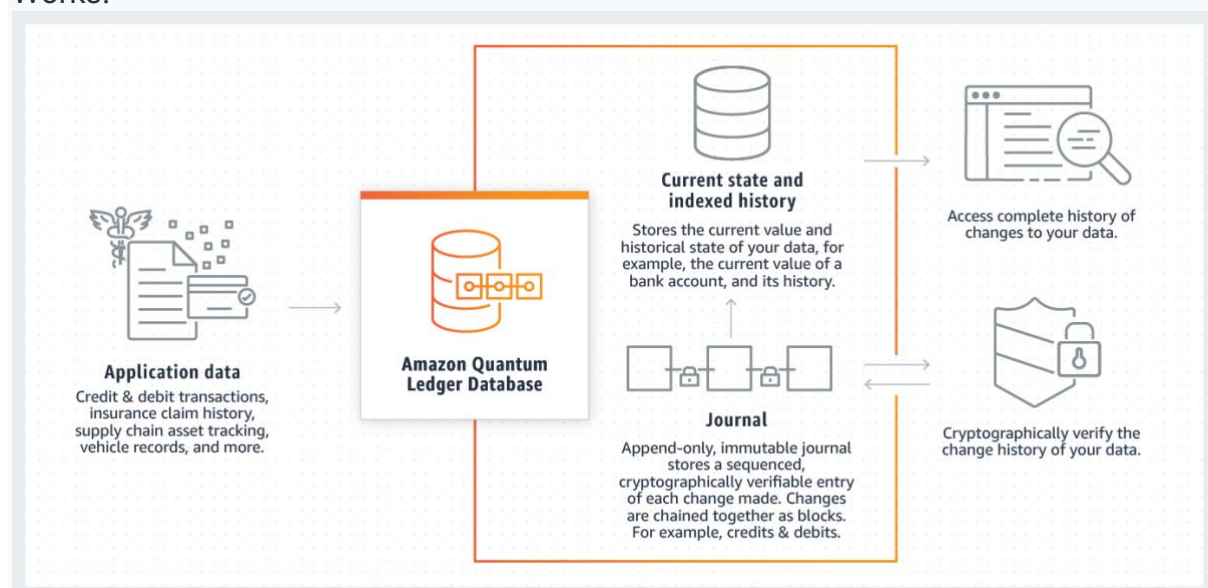
Amazon Quantum Ledger Database (Amazon QLDB) is a fully managed ledger database that provides a transparent, immutable, and cryptographically verifiable transaction log owned by a central trusted authority. Amazon QLDB can be used to track each and every application data change and maintains a complete and verifiable history of changes over time.

Ledgers are typically used to record a history of economic and financial activity in an organization. Many organizations build applications with ledger-like functionality because they want to maintain an accurate history of their applications' data, for example, tracking the history of credits and debits in banking transactions, verifying the data lineage of an insurance claim, or tracing the movement of an item in a supply chain network. Ledger applications are often implemented using custom audit tables or audit trails created in relational databases.

Amazon QLDB is a new class of databases that eliminates the need to engage in the complex development effort of building your own ledger-like applications. With QLDB, your data's change history is immutable – it cannot be altered or deleted –

and using cryptography, you can easily verify that there have been no unintended modifications to your application's data. QLDB uses an immutable transactional log, known as a journal, that tracks each application data change and maintains a complete and verifiable history of changes over time. QLDB is easy to use because it provides developers with a familiar SQL-like API, a flexible document data model, and full support for transactions. QLDB's streaming capability provides a near real-time flow of your data stored within QLDB, allowing you to develop event-driven workflows, and real-time analytics, and to replicate data to other AWS services to support advanced analytical processing. QLDB is also serverless, so it automatically scales to support the demands of your application. There are no servers to manage and no read or write limits to configure. With QLDB, you only pay for what you use.

How Amazon Quantum Ledger Database (Amazon QLDB)
Works:



via - <https://aws.amazon.com/qldb/>

Incorrect options:

Amazon Neptune - Amazon Neptune is a fast, reliable, fully-managed graph database service that makes it easy to build and run applications that work with highly connected datasets. The core of Amazon Neptune is a purpose-built, high-performance graph database engine optimized for storing billions of relationships and querying the graph with milliseconds latency. Amazon Neptune is tailor-built for use cases like Knowledge Graphs, Identity Graphs, Fraud Detection, Recommendation Engines, Social Networking, Life Sciences, and so on.

Amazon Timestream - Amazon Timestream is a fast, scalable, and serverless time series database service for IoT and operational applications that makes it easy to store and analyze trillions of events per day up to 1,000 times faster and at as little as 1/10th the cost of relational databases. Amazon Timestream saves you time and costs in managing the lifecycle of time series data by keeping recent data in memory and moving historical data to a cost-optimized storage tier based upon user-defined policies.

Amazon Managed Blockchain - Amazon Managed Blockchain is a fully managed service that allows you to join public networks or set up and manage scalable private networks using popular open-source frameworks. Amazon Managed Blockchain eliminates the overhead required to create the network or join a public network and automatically scales to meet the demands of thousands of applications running millions of transactions.

While QLDB is a ledger database purpose-built for customers who need to maintain a complete and verifiable history of data changes in an application that they own and manage in a centralized way, QLDB is not a blockchain technology. Instead, blockchain technologies focus on enabling multiple parties to transact and share data securely in a decentralized way; without a trusted, central authority. Every member in a network has an independently verifiable copy of an immutable ledger, and members can create and endorse transactions in the network.

References:

<https://aws.amazon.com/qldb/>

<https://aws.amazon.com/managed-blockchain/>

Question 45: **Correct**

Which of the following AWS services are offered free of cost? (Select two)

- **An Elastic IP address, which is chargeable as long as it is associated with an EC2 instance**
- **AWS Elastic Beanstalk**

(Correct)

- **AWS Auto Scaling**

(Correct)

- **Amazon EC2 Spot Instances**
- **Amazon CloudWatch facilitated detailed monitoring of EC2 instances**

Explanation

Correct options:

AWS Elastic Beanstalk

There is no additional charge for AWS Elastic Beanstalk. You pay for AWS resources (e.g. EC2 instances or S3 buckets) you create to store and run your application. You only pay for what you use, as you use it; there are no minimum fees and no upfront commitments.

AWS Auto Scaling

There is no additional charge for AWS Auto Scaling. You pay only for the AWS resources needed to run your applications and Amazon CloudWatch monitoring fees.

Incorrect options:

Amazon EC2 Spot Instances - Amazon EC2 Spot Instances let you take advantage of unused EC2 capacity in the AWS cloud. Spot Instances are available at up to a 90% discount compared to On-Demand prices. Spot Instances are, however, not free.

Amazon CloudWatch facilitated detailed monitoring of EC2 instances - If you enable detailed monitoring, you are charged per metric that is sent to CloudWatch. You are not charged for data storage. Data is available in 1-minute periods, as opposed to 5-minute periods at no charge, for basic monitoring.

An Elastic IP address, which is chargeable as long as it is associated with an EC2 instance - An Elastic IP address doesn't incur charges as long as all the following conditions are true: The Elastic IP address is associated with an EC2 instance, The instance associated with the Elastic IP address is running, The instance has only one Elastic IP address attached to it and the Elastic IP address is associated with an attached network interface, such as a Network Load Balancer or NAT gateway.

References:

<https://aws.amazon.com/elasticbeanstalk/pricing/>

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-cloudwatch-new.html>

<https://aws.amazon.com/premiumsupport/knowledge-center/elastic-ip-charges/>

Question 46: **Correct**

Which of the following statements are correct regarding the AWS Control Tower and Service Control Policies? (Select two)

- **Service Control Policies (SCPs) are a type of organization policy that you can use to manage permissions in your organization**

(Correct)

- **AWS Control Tower is an AWS native service providing a pre-defined set of blueprints and guardrails to help customers implement a landing zone for new AWS accounts**

(Correct)

- **AWS Control Tower helps you deploy a multi-account AWS environment and operate it with day-to-day reminders and recommendations**
- **Service Control Policies (SCPs) can help grant permissions to the accounts in your organization**

- **Service Control Policies (SCPs), by default, affect all the users in the AWS Organization. They have to be configured to effect only the member accounts, if needed**

Explanation

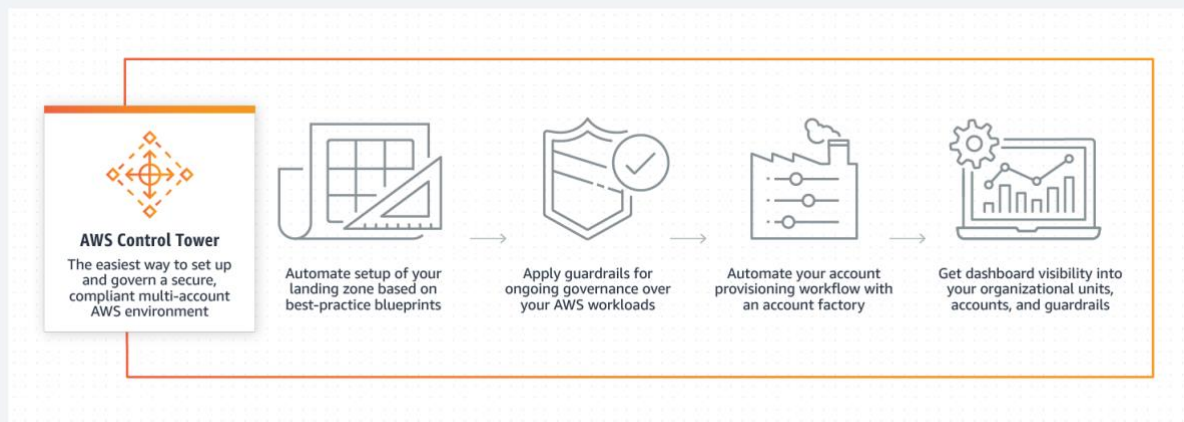
Correct options:

AWS Control Tower is an AWS native service providing a pre-defined set of blueprints and guardrails to help customers implement a landing zone for new AWS accounts

AWS Control Tower is an AWS native service providing a pre-defined set of blueprints and guardrails to help customers implement a landing zone for new AWS accounts.

AWS Control Tower is designed to provide an easy, self-service setup experience and an interactive user interface for ongoing governance with guardrails. While Control Tower automates creation of a new landing zone with pre-configured blueprints (e.g., AWS IAM Identity Center for directory and access), the AWS Landing Zone solution provides a configurable setup of a landing zone with rich customization options through custom add-ons (e.g., Active Directory, Okta Directory) and ongoing modifications through a code deployment and configuration pipeline.

How AWS Control Tower Works:



via - <https://aws.amazon.com/controltower/>

Service Control Policies (SCPs) are a type of organization policy that you can use to manage permissions in your organization

Service control policies (SCPs) are a type of organization policy that you can use to manage permissions in your organization. Service control policies (SCPs) offer central control over the maximum available permissions for all accounts in your organization. Service control policies (SCPs) help you to ensure your accounts stay within your organization's access control guidelines. SCPs are available only in an organization that has all features enabled. SCPs aren't available if your organization has enabled only the consolidated billing features.

Incorrect options:

AWS Control Tower helps you deploy a multi-account AWS environment and operate it with day-to-day reminders and recommendations - AWS Control Tower helps you deploy a multi-account AWS environment based on best practices, however, the customer is still responsible for day-to-day operations and checking compliance status. Enterprises that need help operating regulated infrastructure in the cloud should consider a certified MSP partner or AWS Managed Services (AMS).

Service Control Policies (SCPs) can help grant permissions to the accounts in your organization - SCPs alone are not sufficient to grant permissions to the accounts in your organization. No permissions are granted by an SCP. An SCP defines a guardrail, or sets limits, on the actions that the account's administrator can delegate to the IAM users and roles in the affected accounts. The administrator must still attach identity-based or resource-based policies to IAM users or roles, or to the resources in your accounts to actually grant permissions. The effective permissions are the logical intersection between what is allowed by the SCP and what is allowed by the IAM and resource-based policies.

Service Control Policies (SCPs), by default, affect all the users in the AWS Organization. They have to be configured to effect only the member accounts, if needed - SCPs don't affect users or roles in the management account. They affect only the member accounts in your organization.

References:

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps.html

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

Question 47: **Correct**

Which of the following statements are true about AWS Regions and Availability Zones (AZ)? (Select two)

- **All traffic between Availability Zones (AZ) is encrypted**

(Correct)

- **Traffic between Availability Zones (AZ) is not encrypted by default, but can be configured from AWS console**
- **An Availability Zone (AZ) is a physical location where AWS clusters the data centers**
- **AWS calls each group of logical data centers as AWS Regions**
- **Each AWS Region consists of multiple, isolated, and physically separate Availability Zones (AZ) within a geographic area**

(Correct)

Explanation

Correct options:

Each AWS Region consists of multiple, isolated, and physically separate Availability Zones (AZ) within a geographic area

AWS has the concept of a Region, which is a physical location around the world where we cluster data centers. AWS calls each group of logical data centers an Availability Zone. Each AWS Region consists of multiple, isolated, and physically separate Availability Zones (AZ) within a geographic area.

Each Availability Zone (AZ) has independent power, cooling, and physical security and is connected via redundant, ultra-low-latency networks. AWS customers focused on high availability can design their applications to run in multiple AZ's to achieve even greater fault tolerance. AWS infrastructure Regions meet the highest levels of security, compliance, and data protection.

All traffic between Availability Zones (AZ) is encrypted

All Availability Zones (AZ) in an AWS Region are interconnected with high-bandwidth, low-latency networking, over fully redundant, dedicated metro fiber providing high-throughput, low-latency networking between AZs. All traffic between Availability Zones (AZ) is encrypted.

Incorrect options:

Traffic between Availability Zones (AZ) is not encrypted by default, but can be configured from AWS console - All traffic between Availability Zones (AZ) is encrypted.

An Availability Zone (AZ) is a physical location where AWS clusters the data centers - AWS has the concept of a Region, which is a physical location around the world where AWS clusters the data centers.

AWS calls each group of logical data centers as AWS Regions - AWS has the concept of a Region, which is a physical location around the world where AWS clusters the data centers. AWS calls each group of logical data centers as an Availability Zone (AZ).

Reference:

https://aws.amazon.com/about-aws/global-infrastructure/regions_az/

Question 48: **Correct**

Which AWS service is used to store and commit code privately and also offer features for version control?

- **AWS CodeBuild**
- **AWS CodePipeline**
- **AWS CodeCommit**

(Correct)

- **AWS CodeStar**

Explanation

Correct option:

AWS CodeCommit

AWS CodeCommit is a fully-managed source control service that hosts secure Git-based repositories. It makes it easy for teams to collaborate on code in a secure and highly scalable ecosystem. CodeCommit eliminates the need to operate your own source control system or worry about scaling its infrastructure. You can use CodeCommit to securely store anything from source code to binaries, and it works seamlessly with your existing Git tools.

AWS CodeCommit eliminates the need to host, maintain, back up, and scale your own source control servers. The service automatically scales to meet the growing needs of your project. AWS CodeCommit automatically encrypts your files in transit and at rest. AWS CodeCommit is integrated with AWS Identity and Access Management (AWS IAM) allowing you to customize user-specific access to your repositories.

AWS CodeCommit supports all Git commands and works with your existing Git tools. You can keep using your preferred development environment plugins, continuous integration/continuous delivery systems, and graphical clients with CodeCommit.

Incorrect options:

AWS CodePipeline - AWS CodePipeline is a fully managed continuous delivery service that helps you automate your release pipelines for fast and reliable application and infrastructure updates. CodePipeline automates the build, test, and deploy phases of your release process every time there is a code change, based on the release model you define. This enables you to rapidly and reliably deliver features and updates.

AWS CodeBuild - AWS CodeBuild is a fully managed continuous integration service that compiles source code, runs tests, and produces software packages that are ready to deploy. With CodeBuild, you don't need to provision, manage, and scale your own build servers. CodeBuild scales continuously and processes multiple builds concurrently, so your builds are not left waiting in a queue. You can get started quickly by using prepackaged build environments, or you can create custom build environments that use your own build tools. With CodeBuild, you are charged by the minute for the compute resources you use.

AWS CodeStar - AWS CodeStar is a cloud-based development service that provides the tools you need to quickly develop, build, and deploy applications on AWS. With AWS CodeStar, you can set up your entire continuous delivery toolchain in minutes, allowing you to start releasing code faster. AWS CodeStar makes it easy for your

whole team to work together securely, with built-in role-based policies that allow you to easily manage access and add owners, contributors, and viewers to your projects.

Each CodeStar project includes development tools, including AWS CodePipeline, AWS CodeCommit, AWS CodeBuild and AWS CodeDeploy, that can be used on their own and with existing AWS applications.

References:

<https://aws.amazon.com/codecommit/>

<https://aws.amazon.com/codestar/>

Question 49: **Correct**

A financial services company needs to retain its data for 10 years to meet compliance norms. Which Amazon Simple Storage Service (Amazon S3) storage class is the best fit for this use case considering that the data has to be stored at a minimal cost?

- **Amazon S3 Intelligent-Tiering**
- **Amazon S3 Glacier Flexible Retrieval**
- **Amazon S3 Standard-Infrequent Access (S3 Standard-IA)**
- **Amazon S3 Glacier Deep Archive**

(Correct)

Explanation

Correct option:

Amazon S3 Glacier Deep Archive

Amazon S3 Glacier Deep Archive is Amazon S3's lowest-cost storage class and supports long-term retention and digital preservation for data that may be accessed once or twice a year. It is designed for customers — particularly those in highly-regulated industries, such as the Financial Services, Healthcare, and Public Sectors — that retain data sets for 7-10 years or longer to meet regulatory compliance requirements. S3 Glacier Deep Archive can also be used for backup and disaster recovery use cases, and is a cost-effective and easy-to-manage alternative to magnetic tape systems, whether they are on-premises libraries or off-premises services.

Amazon S3 Glacier Deep Archive complements Amazon S3 Glacier, which is ideal for archives where data is regularly retrieved and some of the data may be needed in minutes. All objects stored in S3 Glacier Deep Archive are replicated and stored across at least three geographically-dispersed Availability Zones, protected by 99.999999999% of durability, and can be restored within 12 hours.

Incorrect options:

Amazon S3 Glacier Flexible Retrieval - Amazon S3 Glacier Flexible Retrieval delivers low-cost storage, up to 10% lower cost (than Amazon S3 Glacier Instant Retrieval), for archive data that is accessed 1–2 times per year and is retrieved asynchronously. For archive data that does not require immediate access but needs the flexibility to retrieve large sets of data at no cost, such as backup or disaster recovery use cases, Amazon S3 Glacier Flexible Retrieval (formerly Amazon S3 Glacier) is the ideal storage class.

Amazon S3 Standard-Infrequent Access (S3 Standard-IA) - Amazon S3 Standard-Infrequent Access (S3 Standard-IA) is for data that is accessed less frequently, but requires rapid access when needed. S3 Standard-IA offers the high durability, high throughput, and low latency of S3 Standard, with a low per GB storage price and per GB retrieval fee. This combination of low cost and high performance makes S3 Standard-IA ideal for long-term storage, backups, and as a data store for disaster recovery files. S3 Storage Classes can be configured at the object level and a single bucket can contain objects stored across S3 Standard, S3 Intelligent-Tiering, S3 Standard-IA, and S3 One Zone-IA. You can also use S3 Lifecycle policies to automatically transition objects between storage classes without any application changes.

Amazon S3 Intelligent-Tiering - Amazon S3 Intelligent-Tiering (S3 Intelligent-Tiering) is the only cloud storage class that delivers automatic cost savings by moving objects between four access tiers when access patterns change. The S3 Intelligent-Tiering storage class is designed to optimize costs by automatically moving data to the most cost-effective access tier, without operational overhead. It works by storing objects in four access tiers: two low latency access tiers optimized for frequent and infrequent access, and two optional archive access tiers designed for asynchronous access that are optimized for rare access.

Reference:

<https://aws.amazon.com/s3/storage-classes/>

Question 50: **Correct**

A company stores all its media files in Amazon Simple Storage Service (Amazon S3) which is accessed by an application hosted on Amazon EC2 instances. The company wants to convert these media files into formats that users can playback on mobile devices.

Which AWS service/tool helps you achieve this requirement?

- **Amazon Transcribe**
- **Amazon Elastic Transcoder**

(Correct)

- **Amazon Comprehend**
- **AWS Glue**

Explanation

Correct option:

Amazon Elastic Transcoder

Amazon Elastic Transcoder lets you convert media files that you have stored in Amazon Simple Storage Service (Amazon S3) into media files in the formats required by consumer playback devices. For example, you can convert large, high-quality digital media files into formats that users can playback on mobile devices, tablets, web browsers, and connected televisions.

Amazon Elastic Transcoder manages all aspects of the media transcoding process for you transparently and automatically. There's no need to administer software, scale hardware, tune performance, or otherwise manage transcoding infrastructure. You simply create a transcoding "job" specifying the location of your source media file and how you want it transcoded. Amazon Elastic Transcoder also provides transcoding presets for popular output formats, which means that you don't need to guess about which settings work best on particular devices. All these features are available via service API, AWS SDKs and the AWS Management Console.

Incorrect options:

Amazon Transcribe - Amazon Transcribe makes it easy for developers to add speech to text capabilities to their applications. Audio data is virtually impossible for computers to search and analyze. Therefore, recorded speech needs to be converted to text before it can be used in applications.

Amazon Transcribe uses a deep learning process called automatic speech recognition (ASR) to convert speech to text quickly and accurately. Amazon Transcribe can be used to transcribe customer service calls, automate subtitling, and generate metadata for media assets to create a fully searchable archive.

Amazon Comprehend - Amazon Comprehend is a natural language processing (NLP) service that uses machine learning to find insights and relationships in a text. Amazon Comprehend uses machine learning to help you uncover the insights and relationships in your unstructured data. The service identifies the language of the text; extracts key phrases, places, people, brands, or events; understands how positive or negative the text is; analyzes text using tokenization and parts of speech, and automatically organizes a collection of text files by topic.

AWS Glue - AWS Glue is a serverless data integration service that makes it easy to discover, prepare, and combine data for analytics, machine learning, and application development. AWS Glue provides all of the capabilities needed for data integration, so you can start analyzing your data and putting it to use in minutes instead of months. You should use AWS Glue to discover properties of the data you own, transform it, and prepare it for analytics. Glue can automatically discover both structured and semi-structured data stored in your data lake on Amazon S3, data warehouse in Amazon Redshift, and various databases running on AWS.

References:

<https://aws.amazon.com/elastictranscoder/>

<https://aws.amazon.com/comprehend/>

<https://aws.amazon.com/transcribe/>

Question 51: **Correct**

An e-commerce company has its on-premises data storage on an NFS file system that is accessed in parallel by multiple applications. The company is looking at moving the applications and data stores to AWS Cloud.

Which storage service should the company use to move their files to AWS Cloud seamlessly if the application is hosted on Amazon Elastic Compute Cloud (Amazon EC2) instances?

- **AWS Storage Gateway**
- **Amazon Elastic File System (Amazon EFS)**

(Correct)

- **Amazon Simple Storage Service (Amazon S3)**
- **Amazon Elastic Block Store (Amazon EBS)**

Explanation

Correct option:

Amazon Elastic File System (Amazon EFS)

Amazon Elastic File System (Amazon EFS) provides a simple, scalable, fully managed elastic NFS file system for use with AWS Cloud services and on-premises resources. It is built to scale on-demand to petabytes without disrupting applications, growing and shrinking automatically as you add and remove files, eliminating the need to provision and manage capacity to accommodate growth.

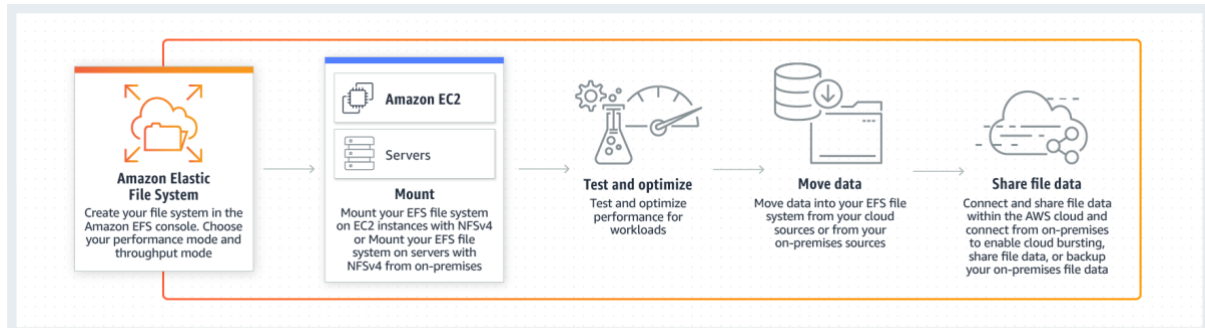
Amazon EFS is designed to provide massively parallel shared access to thousands of Amazon EC2 instances, enabling your applications to achieve high levels of aggregate throughput and input/output operations per second (IOPS) with consistently low latencies.

Amazon EFS is well suited to support a broad spectrum of use cases from home directories to business-critical applications. Customers can use EFS to lift and shift existing enterprise applications to the AWS Cloud. Other use cases include big data analytics, web serving and content management, application development, and testing, media and entertainment workflows, database backups, and container storage.

Amazon EFS offers two storage classes: the Standard storage class, and the Infrequent Access storage class (EFS IA). EFS IA provides price/performance that's cost-optimized for files not accessed every day. By simply enabling EFS Lifecycle

Management on your file system, files not accessed according to the lifecycle policy you choose will be automatically and transparently moved into EFS IA.

How Amazon EFS Works:



via - <https://aws.amazon.com/efs/>

Incorrect options:

Amazon Elastic Block Store (Amazon EBS) - Amazon Elastic Block Store (Amazon EBS) is an easy-to-use, high-performance, block-storage service designed for use with Amazon Elastic Compute Cloud (EC2) for both throughput and transaction-intensive workloads at any scale. A broad range of workloads, such as relational and non-relational databases, enterprise applications, containerized applications, big data analytics engines, file systems, and media workflows are widely deployed on Amazon EBS. EBS is a block storage service and not a file storage service like EFS.

Amazon Simple Storage Service (Amazon S3) - Amazon Simple Storage Service (Amazon S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance. This means customers of all sizes and industries can use it to store and protect any amount of data for a range of use cases, such as data lakes, websites, mobile applications, backup and restore, archive, enterprise applications, IoT devices, and big data analytics. Parallel access of NFS file systems is not a feature Amazon S3 is capable of and hence EFS is the right choice here.

AWS Storage Gateway - AWS Storage Gateway is a hybrid cloud storage service that gives you on-premises access to virtually unlimited cloud storage. Customers use Storage Gateway to simplify storage management and reduce costs for key hybrid cloud storage use cases. These include moving backups to the cloud, using on-premises file shares backed by cloud storage, and providing low latency access to data in AWS for on-premises applications.

Reference:

<https://aws.amazon.com/efs/>

Question 52: **Correct**

A Security Group has been changed in an AWS account and the manager of the account has asked you to find out the details of the user who changed it. As a Cloud Practitioner, which AWS service will you use to fetch the necessary information?

- **AWS X-Ray**
- **AWS CloudTrail**

(Correct)

- **Amazon Inspector**
- **AWS Trusted Advisor**

Explanation

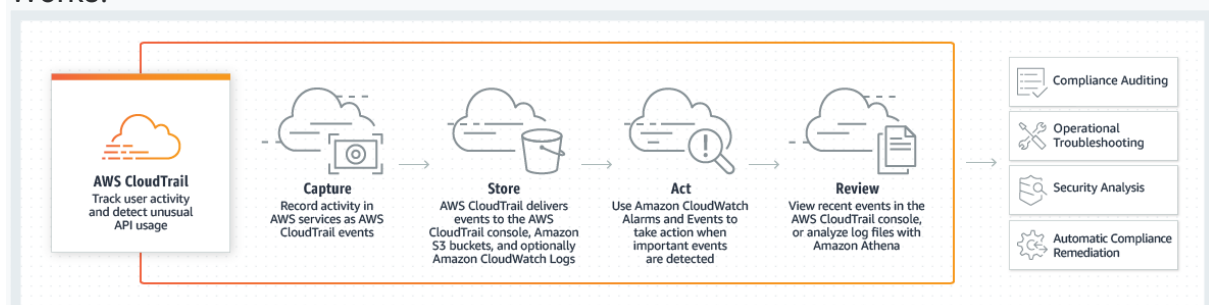
Correct option:

AWS CloudTrail

AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. With CloudTrail, you can log, continuously monitor and retain account activity related to actions across your AWS infrastructure. CloudTrail provides the event history of your AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command-line tools, and other AWS services. This event history simplifies security analysis, resource change tracking, and troubleshooting. In addition, you can use AWS CloudTrail to detect unusual activity in your AWS accounts. These capabilities help simplify operational analysis and troubleshooting.

AWS CloudTrail provides visibility into user activity by recording actions taken on your account. CloudTrail records important information about each action, including who made the request, the services used, the actions performed, parameters for the actions, and the response elements returned by the AWS service. This information helps you to track changes made to your AWS resources and to troubleshoot operational issues. CloudTrail makes it easier to ensure compliance with internal policies and regulatory standards.

How AWS CloudTrail Works:



via - <https://aws.amazon.com/cloudtrail/>

Incorrect options:

AWS X-Ray - AWS X-Ray helps developers analyze and debug production, distributed applications, such as those built using a microservices architecture. With X-Ray, you

can understand how your application and its underlying services are performing to identify and troubleshoot the root cause of performance issues and errors. X-Ray provides an end-to-end view of requests as they travel through your application, and shows a map of your application's underlying components. X-Ray is not for tracking user actions when interacting with the AWS systems.

Amazon Inspector - Amazon Inspector is an automated security assessment service that helps you test the network accessibility of your Amazon EC2 instances and the security state of your applications running on the instances. Amazon Inspector allows you to automate security vulnerability assessments throughout your development and deployment pipeline or against static production systems. This allows you to make security testing a more regular occurrence as part of the development and IT operations.

AWS Trusted Advisor - AWS Trusted Advisor is an online tool that provides you real-time guidance to help you provision your resources following AWS best practices. Trusted Advisor checks help optimize your AWS infrastructure, increase security and performance, reduce your overall costs, and monitor service limits. Whether establishing new workflows, developing applications, or as part of ongoing improvement, take advantage of the recommendations provided by Trusted Advisor on a regular basis to help keep your solutions provisioned optimally.

Reference:

<https://aws.amazon.com/cloudtrail/>

Question 53: **Correct**

A company is planning to move their traditional CRM application running on MySQL to an AWS database service. Which database service is the right fit for this requirement?

- **Amazon Neptune**
- **Amazon Aurora**

(Correct)

- **Amazon ElastiCache**
- **Amazon DynamoDB**

Explanation

Correct option:

Amazon Aurora

Amazon Aurora is a relational database engine that combines the speed and reliability of high-end commercial databases with the simplicity and cost-effectiveness of open-source databases. Amazon Aurora MySQL delivers up to five times the performance of MySQL without requiring any changes to most MySQL applications; similarly, Amazon Aurora PostgreSQL delivers up to three times the performance of PostgreSQL. Amazon RDS manages your Amazon Aurora databases, handling time-consuming tasks such as provisioning, patching, backup, recovery,

failure detection, and repair. You pay a simple monthly charge for each Amazon Aurora database instance you use. There are no upfront costs or long-term commitments required.

Amazon Aurora features a distributed, fault-tolerant, self-healing storage system that auto-scales up to 128TB per database instance. It delivers high performance and availability with up to 15 low-latency read replicas, point-in-time recovery, continuous backup to Amazon S3, and replication across three Availability Zones (AZs).

You can use the standard "mysqldump" utility to export data from MySQL and "mysqlimport" utility to import data to Amazon Aurora, and vice-versa. You can also use Amazon RDS's DB Snapshot migration feature to migrate an RDS MySQL DB Snapshot to Amazon Aurora using the AWS Management Console. Migration completes for most customers in under an hour, though the duration depends on format and data set size.

Incorrect options:

Amazon DynamoDB - Amazon DynamoDB is a key-value and document database that delivers single-digit millisecond performance at any scale. It's a fully managed, multi-region, multi-active, durable database with built-in security, backup and restore, and in-memory caching for internet-scale applications. DynamoDB can handle more than 10 trillion requests per day and can support peaks of more than 20 million requests per second. DynamoDB is not for relational databases.

Amazon Neptune - Amazon Neptune is a fast, reliable, fully-managed graph database service that makes it easy to build and run applications that work with highly connected datasets. The core of Amazon Neptune is a purpose-built, high-performance graph database engine optimized for storing billions of relationships and querying the graph with milliseconds latency. Amazon Neptune is tailor-built for use cases like Knowledge Graphs, Identity Graphs, Fraud Detection, Recommendation Engines, Social Networking, Life Sciences, and so on. Amazon Neptune is not for relational databases.

Amazon ElastiCache - Amazon ElastiCache allows you to seamlessly set up, run, and scale popular open-source compatible in-memory data stores in the cloud. Build data-intensive apps or boost the performance of your existing databases by retrieving data from high throughput and low latency in-memory data stores. ElastiCache however, is not a relational database solution.

Reference:

<https://aws.amazon.com/rds/aurora/>

Question 54: **Correct**

A weather-tracking application is built using Amazon DynamoDB. The performance of the application has been consistently good. But lately, the team has realized that during holidays and travel seasons, the load on the application is high and the read

requests consume most of the database resources, thereby drastically increasing the overall application latency.

Which feature/service will help resolve this issue?

- **Amazon DynamoDB Regulator**
- **Amazon CloudFront**
- **Amazon ElastiCache**
- **Amazon DynamoDB Accelerator**

(Correct)

Explanation

Correct option:

Amazon DynamoDB Accelerator

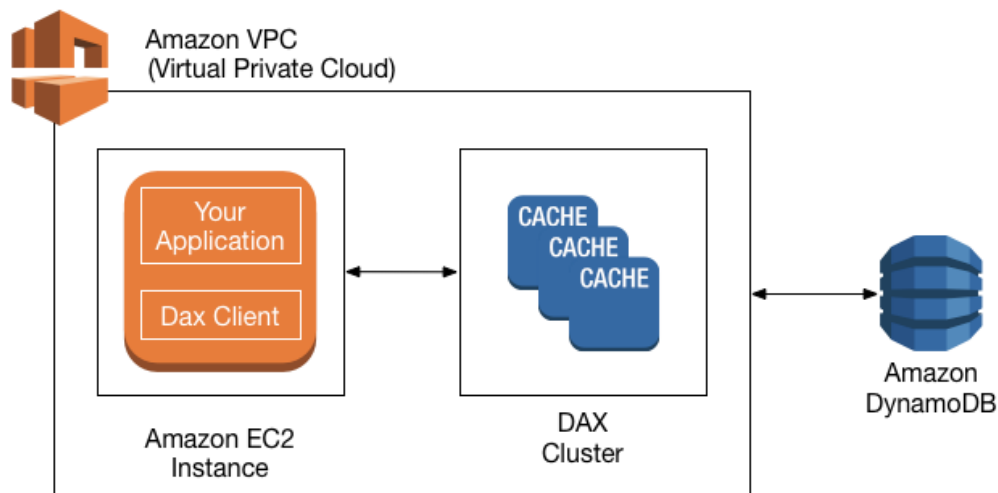
Amazon DynamoDB is designed for scale and performance. In most cases, the DynamoDB response times can be measured in single-digit milliseconds. However, there are certain use cases that require response times in microseconds. For these use cases, Amazon DynamoDB Accelerator (DAX) delivers fast response times for accessing eventually consistent data.

DAX is a DynamoDB-compatible caching service that enables you to benefit from fast in-memory performance for demanding applications. DAX addresses three core scenarios:

1. As an in-memory cache, DAX reduces the response times of eventually consistent read workloads by an order of magnitude from single-digit milliseconds to microseconds.
2. DAX reduces operational and application complexity by providing a managed service that is API-compatible with DynamoDB. Therefore, it requires only minimal functional changes to use with an existing application.
3. For read-heavy or bursty workloads, DAX provides increased throughput and potential operational cost savings by reducing the need to overprovision read capacity units. This is especially beneficial for applications that require repeated reads for individual keys.

How Amazon DynamoDB Accelerator (DAX)

Works:



via - <https://aws.amazon.com/dynamodb/dax/>

Incorrect options:

Amazon DynamoDB Regulator - This is a made-up option, used only as a distractor.

Amazon ElastiCache - Amazon ElastiCache is a web service that makes it easy to deploy, operate, and scale an in-memory data store and cache in the cloud. The service improves the performance of web applications by allowing you to retrieve information from fast, managed, in-memory data stores, instead of relying entirely on slower disk-based databases. Amazon ElastiCache supports two open-source in-memory engines: Amazon ElastiCache for Redis, and Amazon ElastiCache for Memcached. AWS recommends using Amazon DynamoDB Accelerator (DAX) for DynamoDB, which is an out-of-box caching solution for DynamoDB.

Amazon CloudFront - Amazon CloudFront is a global content delivery network (CDN) service that accelerates delivery of your websites, APIs, video content or other web assets. It integrates with other Amazon Web Services products to give developers and businesses an easy way to accelerate content to end-users with no minimum usage commitments. It is not a caching solution.

Reference:

<https://aws.amazon.com/caching/aws-caching/>

Question 55: **Correct**

A company is looking for ways to make its desktop applications available to the employees from browsers on their devices/laptops. Which AWS service will help achieve this requirement without having to procure servers or maintain infrastructure?

- **Amazon AppStream 2.0**

(Correct)

- Amazon WorkSpaces
- AWS Outposts
- AWS Snowball

Explanation

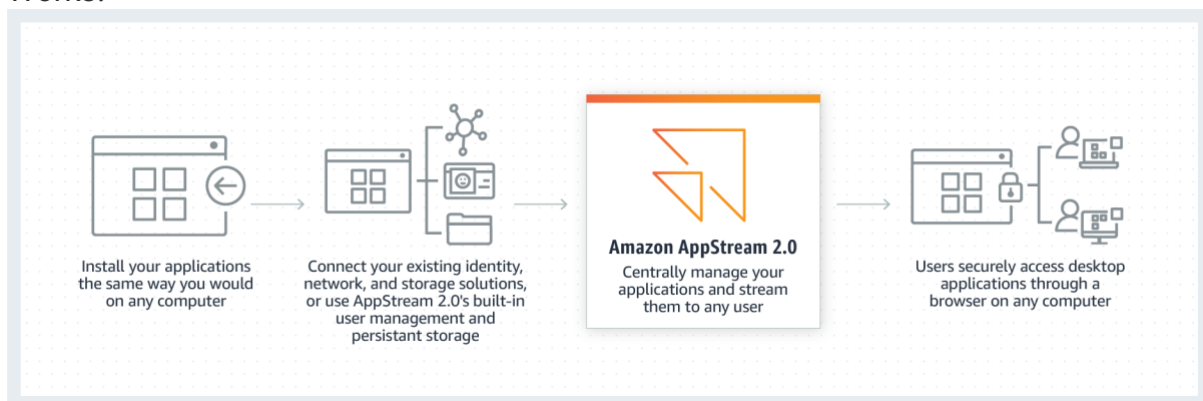
Correct option:

Amazon AppStream 2.0

Amazon AppStream 2.0 is a fully managed non-persistent application and desktop streaming service. You centrally manage your desktop applications on AppStream 2.0 and securely deliver them to any computer. You can easily scale to any number of users across the globe without acquiring, provisioning, and operating hardware or infrastructure. AppStream 2.0 is built on AWS, so you benefit from a data center and network architecture designed for the most security-sensitive organizations. Each end-user has a fluid and responsive experience because your applications run on virtual machines optimized for specific use cases and each streaming session automatically adjusts to network conditions.

Users can access the desktop applications they need at any time. AppStream 2.0 streams your applications from AWS to any computer, including Chromebooks, Macs, and PCs. AppStream 2.0 connects to your Active Directory, network, cloud storage, and file shares. Users access applications using their existing credentials and your existing security policies manage access. Extensive APIs integrate AppStream 2.0 with your IT solutions.

How Amazon AppStream 2.0 Works:



via - <https://aws.amazon.com/appstream2/>

Incorrect options:

Amazon WorkSpaces - Amazon WorkSpaces is a managed, secure Desktop-as-a-Service (DaaS) solution. You can use Amazon WorkSpaces to provision either Windows or Linux desktops in just a few minutes and quickly scale to provide thousands of desktops to workers across the globe. Amazon WorkSpaces helps you eliminate the complexity in managing hardware inventory, OS versions and patches,

and Virtual Desktop Infrastructure (VDI), which helps simplify your desktop delivery strategy. With Amazon WorkSpaces, your users get a fast, responsive desktop of their choice that they can access anywhere, anytime, from any supported device.

While Amazon AppStream 2.0 helps move desktop applications to AWS Cloud, so they can be accessed from anywhere; Workspaces provides the entire Desktop environment needed for the workforce.

AWS Outposts - AWS Outposts is a fully managed service that offers the same AWS infrastructure, AWS services, APIs, and tools to virtually any data center, co-location space, or on-premises facility for a truly consistent hybrid experience. AWS Outposts is ideal for workloads that require low latency access to on-premises systems, local data processing, data residency, and migration of applications with local system interdependencies.

AWS Snowball - AWS Snowball, a part of the AWS Snow Family, is an edge computing, data migration, and edge storage device that comes in two options. Snowball Edge Storage Optimized devices provide both block storage and Amazon S3-compatible object storage, and 40 vCPUs. They are well suited for local storage and large scale data transfer.

References:

<https://aws.amazon.com/appstream2/>

<https://aws.amazon.com/workspaces/>

Question 56: **Correct**

AWS Web Application Firewall (AWS WAF) can be deployed on which of the following services?

- **Amazon CloudFront, Amazon Elastic Compute Cloud (Amazon EC2), Amazon API Gateway, Application Load Balancer**
- **Application Load Balancer, Amazon Elastic Compute Cloud (Amazon EC2), Amazon API Gateway**
- **AWS AppSync, Amazon CloudFront, Application Load Balancer, Amazon Elastic Compute Cloud (Amazon EC2)**
- **Amazon CloudFront, Application Load Balancer, Amazon API Gateway, AWS AppSync**

(Correct)

Explanation

Correct option:

Amazon CloudFront, Application Load Balancer, Amazon API Gateway, AWS AppSync

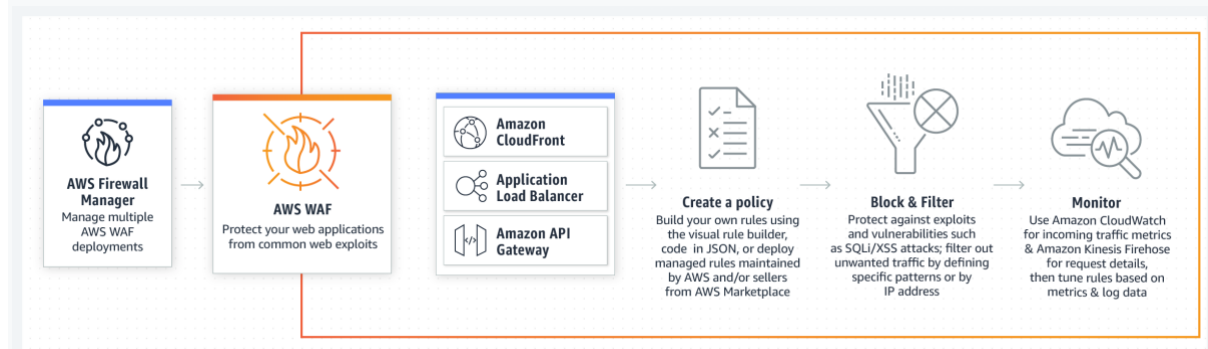
AWS Web Application Firewall (AWS WAF) is a web application firewall that helps protect your web applications or APIs against common web exploits that may affect

availability, compromise security, or consume excessive resources. AWS WAF gives you control over how traffic reaches your applications by enabling you to create security rules that block common attack patterns, such as SQL injection or cross-site scripting, and rules that filter out specific traffic patterns you define.

You can deploy AWS WAF on Amazon CloudFront as part of your CDN solution, the Application Load Balancer that fronts your web servers or origin servers running on EC2, Amazon API Gateway for your REST APIs, or AWS AppSync for your GraphQL APIs.

AWS WAF is tightly integrated with Amazon CloudFront, the Application Load Balancer, Amazon API Gateway, and AWS AppSync – services that AWS customers commonly use to deliver content for their websites and applications. When you use AWS WAF on Amazon CloudFront, your rules run in all AWS Edge Locations, located around the world close to your end-users. This means security doesn't come at the expense of performance. Blocked requests are stopped before they reach your web servers. When you use AWS WAF on regional services, such as Application Load Balancer, Amazon API Gateway, and AWS AppSync, your rules run in the region and can be used to protect internet-facing resources as well as internal resources.

How AWS WAF Works:



via - <https://aws.amazon.com/waf/>

Incorrect options:

Amazon CloudFront, Amazon Elastic Compute Cloud (Amazon EC2), Amazon API Gateway, Application Load Balancer

Application Load Balancer, Amazon Elastic Compute Cloud (Amazon EC2), Amazon API Gateway

AWS AppSync, Amazon CloudFront, Application Load Balancer, Amazon Elastic Compute Cloud (Amazon EC2)

AWS WAF cannot be deployed on Amazon EC2 instances directly, so these three options are incorrect. Application Load Balancer should be configured in front of EC2 instances to deploy AWS WAF.

Reference:

<https://aws.amazon.com/waf/>

Question 57: **Correct**

As a Cloud Practitioner, which of the following credentials would you recommend for signing in to the AWS Management Console to meet security best practices? (Select two)

- **Secret Access Key**
- **IAM Username and password**

(Correct)

- **Access Key ID**
- **Multi Factor Authentication (MFA)**

(Correct)

- **X.509 certificate**

Explanation

Correct option:

IAM Username and password

An AWS Identity and Access Management (IAM) user is an entity that you create in AWS. The IAM user represents the human user or workload who uses the IAM user to interact with AWS. A user in AWS consists of a name and credentials. You also need a password that the IAM user can type to sign in to interactive sessions using the AWS Management Console.

Multi Factor Authentication (MFA)

AWS multi-factor authentication (MFA) is an AWS Identity and Access Management (IAM) best practice that requires a second authentication factor in addition to user name and password sign-in credentials. You can enable MFA at the AWS account level and for root and IAM users you have created in your account.

Incorrect options:

Secret Access Key

Access Key ID

Access keys are long-term credentials for an IAM user or the AWS account root user. You can use access keys to sign programmatic requests to the AWS CLI or AWS API (directly or using the AWS SDK). Access keys consist of two parts: an access key ID (for example, AKIAIOSFODNN7EXAMPLE) and a secret access key (for example, wJalrXUtnFEMI/K7MDENG/bPxrFiCYEXAMPLEKEY). You must use both the access key ID and secret access key together to authenticate your requests.

X.509 certificate

X.509 certificates are used by the AWS Certificate Manager (ACM). ACM certificates are X.509 SSL/TLS certificates that bind the identity of your website and the details of your organization to the public key that is contained in the certificate. One of the keys is public and is typically made available in the X.509 certificate. The other key is private and is stored securely. The X.509 certificate binds the identity of a user, computer, or other resource (the certificate subject) to the public key.

References:

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_users.html

<https://aws.amazon.com/iam/features/mfa/>

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_access-keys.html

<https://docs.aws.amazon.com/acm/latest/userguide/acm-concepts.html>

Question 58: **Correct**

A Cloud Practitioner wants to use CIDR block notation when providing an IP address range. Which of the following AWS network services/utilities allow this feature? (Select two)

- **Network access control list (network ACL)**

(Correct)

- AWS Lambda
- Security group

(Correct)

- Amazon Simple Storage Service (Amazon S3)
- AWS Cost Explorer

Explanation

Correct option:

Security group

A security group acts as a firewall that controls the traffic allowed to and from the resources in your virtual private cloud (VPC). You can choose the ports and protocols to allow for inbound traffic and for outbound traffic. For each security group, you add separate sets of rules for inbound traffic and outbound traffic. By default, new security groups start with only an outbound rule that allows all traffic to leave the resource. You must add rules to enable any inbound traffic or to restrict the outbound traffic. Security groups allow CIDR block notation when providing an IP address range.

Network access control list (network ACL)

A network access control list (ACL) allows or denies specific inbound or outbound traffic at the subnet level. You can use the default network ACL for your VPC, or you can create a custom network ACL for your VPC with rules that are similar to the rules for your security groups in order to add an additional layer of security to your VPC. There is no additional charge for using network ACLs.

Network access control lists (ACL) allow CIDR block notation when providing an IP address range.

Incorrect options:

AWS Lambda - AWS Lambda is a serverless, event-driven compute service that lets you run code for virtually any type of application or backend service without provisioning or managing servers.

AWS Cost Explorer - AWS Cost Explorer has an easy-to-use interface that lets you visualize, understand, and manage your AWS costs and usage over time.

Amazon Simple Storage Service (Amazon S3) - Amazon Simple Storage Service (Amazon S3) is an object storage built to store and retrieve any amount of data from anywhere.

References:

<https://docs.aws.amazon.com/vpc/latest/userguide/security-groups.html>

<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html>

Question 59: **Correct**

Which of the following will help you control the incoming traffic to an Amazon EC2 instance?

- **AWS Resource Group**
- **Route Table**
- **Network access control list (network ACL)**
- **Security Group**

(Correct)

Explanation

Correct option:

Security Group

A security group acts as a virtual firewall for your Amazon EC2 instances to control incoming and outgoing traffic. Inbound rules control the incoming traffic to your instance, and outbound rules control the outgoing traffic from your instance. When you launch an instance, you can specify one or more security groups. If you don't specify a security group, Amazon EC2 uses the default security group. You can add rules to each security group that allows traffic to or from its associated instances.

You can modify the rules for a security group at any time. New and modified rules are automatically applied to all instances that are associated with the security group. When Amazon EC2 decides whether to allow traffic to reach an instance, it evaluates all of the rules from all of the security groups that are associated with the instance.

Security is a shared responsibility between AWS and you. AWS provides security groups as one of the tools for securing your instances, and you need to configure them to meet your security needs. If you have requirements that aren't fully met by security groups, you can maintain your own firewall on any of your instances in addition to using security groups.

Incorrect options:

AWS Resource Group - You can use AWS Resource Groups to organize your AWS resources. Resource groups make it easier to manage and automate tasks on large numbers of resources at one time. Resource Groups feature permissions are at the account level. As long as users who are sharing your account have the correct IAM permissions, they can work with the resource groups that you create. Resource Groups are for grouping resources for managing the resources. They do not provide access to Amazon EC2 instances.

Network access control list (network ACL) - A Network access control list (network ACL) is an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets. You might set up network ACLs with rules similar to your security groups in order to add an additional layer of security to your VPC.

Route Table - A Route table contains a set of rules, called routes, that are used to determine where network traffic from your VPC is directed. You can explicitly associate a subnet with a particular route table. Otherwise, the subnet is implicitly associated with the main route table.

Each route in a route table specifies the range of IP addresses where you want the traffic to go (the destination) and the gateway, network interface, or connection through which to send the traffic (the target).

References:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-security-groups.html>

<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html>

Question 60: **Correct**

A company is moving its on-premises application to AWS Cloud. The application uses in-memory caches for running custom workloads. Which Amazon Elastic Compute Cloud (Amazon EC2) instance type is the right choice for the given requirement?

- **Storage Optimized instance types**
- **Compute Optimized instance types**

- **Accelerated computing instance types**
- **Memory Optimized instance types**

(Correct)

Explanation

Correct option:

Memory Optimized instance types

Memory optimized instances are designed to deliver fast performance for workloads that process large data sets in memory. Memory optimized instances offer large memory size for memory intensive applications including in-memory applications, in-memory databases, in-memory analytics solutions, High Performance Computing (HPC), scientific computing, and other memory-intensive applications.

Amazon EC2 R6g instances are the next-generation of memory-optimized instances powered by Arm-based AWS Graviton2 Processors.

Incorrect options:

Compute Optimized instance types - Compute Optimized instances are designed for applications that benefit from high compute power. These applications include compute-intensive applications like high-performance web servers, high-performance computing (HPC), scientific modelling, distributed analytics, and machine learning inference.

Amazon EC2 C6g instances are the next-generation of compute-optimized instances powered by Arm-based AWS Graviton2 Processors.

Storage Optimized instance types - Dense-storage instances are designed for workloads that require high sequential read and write access to very large data sets, such as Hadoop distributed computing, massively parallel processing data warehousing, and log processing applications. The Dense-storage instances offer the best price/GB-storage and price/disk-throughput across other EC2 instances.

Accelerated computing instance types - Accelerated Computing instance family is a family of instances that use hardware accelerators, or co-processors, to perform some functions, such as floating-point number calculation and graphics processing, more efficiently than is possible in software running on CPUs. Amazon EC2 provides three types of Accelerated Computing instances – GPU compute instances for general-purpose computing, GPU graphics instances for graphics-intensive applications, and FPGA programmable hardware compute instances for advanced scientific workloads.

Reference:

<https://aws.amazon.com/ec2/faqs/>

Question 61: **Correct**

As part of a flexible pricing model, AWS offers two types of Savings Plans. Which of the following are the Savings Plans from AWS?

- **Instance Savings Plans, Storage Savings Plans**
- **Compute Savings Plans, Storage Savings Plans**
- **Compute Savings Plans, EC2 Instance Savings Plans**

(Correct)

- **Reserved Instances (RI) Savings Plans, EC2 Instance Savings Plans**

Explanation

Correct option:

Compute Savings Plans, EC2 Instance Savings Plans

Savings Plans is a flexible pricing model that provides savings of up to 72% on your AWS compute usage. This pricing model offers lower prices on Amazon EC2 instances usage, regardless of instance family, size, OS, tenancy or AWS Region, and also applies to AWS Fargate and AWS Lambda usage.

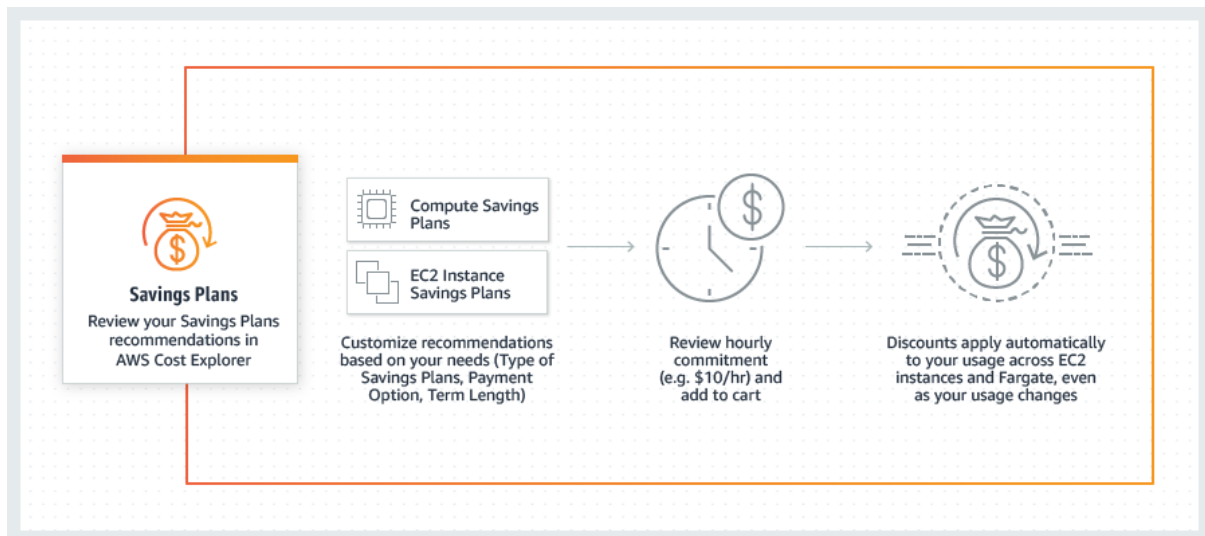
Savings Plans offer significant savings over On-Demand, just like EC2 Reserved Instances, in exchange for a commitment to use a specific amount of compute power (measured in \$/hour) for a one or three-year period. You can sign up for Savings Plans for a 1- or 3-year term and easily manage your plans by taking advantage of recommendations, performance reporting and budget alerts in the AWS Cost Explorer.

AWS offers two types of Savings Plans:

1. Compute Savings Plans provide the most flexibility and help to reduce your costs by up to 66%. These plans automatically apply to EC2 instance usage regardless of instance family, size, AZ, region, OS or tenancy, and also apply to Fargate and Lambda usage. For example, with Compute Savings Plans, you can change from C4 to M5 instances, shift a workload from EU (Ireland) to EU (London), or move a workload from EC2 to Fargate or Lambda at any time and automatically continue to pay the Savings Plans price.
2. EC2 Instance Savings Plans provide the lowest prices, offering savings up to 72% in exchange for a commitment to the usage of individual instance families in a region (e.g. M5 usage in N. Virginia). This automatically reduces your cost on the selected instance family in that region regardless of AZ, size, OS or tenancy. EC2 Instance Savings Plans give you the flexibility to change your usage between instances within a family in that region. For example, you can move from c5.xlarge running Windows to c5.2xlarge running Linux and automatically benefit from the Savings Plans prices.

How Savings Plans

Work:



via - <https://aws.amazon.com/savingsplans/>

Incorrect options:

Compute Savings Plans, Storage Savings Plans

Reserved Instances (RI) Savings Plans, EC2 Instance Savings Plans

Instance Savings Plans, Storage Savings Plans

These three options contradict the explanation above, so these options are incorrect.

References:

<https://aws.amazon.com/savingsplans/>

<https://aws.amazon.com/savingsplans/faq/>

Question 62: **Correct**

An e-commerce application sends out messages to a downstream application whenever an order is created. The downstream application processes the messages and updates its own systems. Currently, the two applications directly communicate with each other.

Which service will you use to decouple this architecture, without any communication loss between the two systems?

- AWS Lambda
- Amazon Simple Queue Service (SQS)

(Correct)

- Amazon Simple Notification Service (Amazon SNS)
- Amazon Kinesis Data Streams

Explanation

Correct option:

Amazon Simple Queue Service (SQS)

Amazon Simple Queue Service (SQS) is a fully managed message queuing service that enables you to decouple and scale microservices, distributed systems, and serverless applications. SQS eliminates the complexity and overhead associated with managing and operating message-oriented middleware and empowers developers to focus on differentiating work. Using SQS, you can send, store, and receive messages between software components at any volume, without losing messages or requiring other services to be available. Get started with SQS in minutes using the AWS console, Command Line Interface or SDK of your choice, and three simple commands.

Amazon SQS uses a pull mechanism, i.e. the messages in the queue are available till a registered process pulls the messages to process them. This decouples the architecture since the second application does not need to be available all the time to process messages coming from application one.

Incorrect options:

Amazon Simple Notification Service (Amazon SNS) - Amazon Simple Notification Service (Amazon SNS) is a fully managed messaging service for both application-to-application (A2A) and application-to-person (A2P) communication. The A2A pub/sub functionality provides topics for high-throughput, push-based, many-to-many messaging between distributed systems, microservices, and event-driven serverless applications. Amazon SNS allows applications to send time-critical messages to multiple subscribers through a “push” mechanism, which implies that the receiving applications have to be present and running to receive the messages. There is a scope for message loss in SNS and hence SQS is the right choice for this use case.

Amazon Kinesis Data Streams - Amazon Kinesis Data Streams enables you to build custom applications that process or analyze streaming data for specialized needs. You can continuously add various types of data such as clickstreams, application logs, and social media to an Amazon Kinesis data stream from hundreds of thousands of sources. Within seconds, the data will be available for your Amazon Kinesis Applications to read and process from the stream. Kinesis Data streams are overkill for this use-case since Kinesis Data Streams are meant for real-time processing of streaming big data.

AWS Lambda - AWS Lambda is a serverless compute service that lets you run code without provisioning or managing servers, creating workload-aware cluster scaling logic, maintaining event integrations, or managing runtimes. With Lambda, you can run code for virtually any type of application or backend service - all with zero administration. Just upload your code as a ZIP file or container image, and Lambda automatically and precisely allocates compute execution power and runs your code based on the incoming request or event, for any scale of traffic. Lambda functions cannot self invoke and need to be called. Also, Lambda functions cannot store data for later processing.

Reference:

<https://aws.amazon.com/sqs/>

Question 63: **Correct**

Which of the following is the least effort way to encrypt data for AWS services only in your AWS account using AWS Key Management Service (KMS)?

- **Create your own customer managed keys (CMKs) in AWS KMS**
- **Use AWS owned CMK in the service you wish to use encryption**
- **Use AWS KMS APIs to encrypt data within your own application by using the AWS Encryption SDK**
- **Use AWS managed master keys that are automatically created in your account for each service**

(Correct)

Explanation

Correct option:

Use AWS managed master keys that are automatically created in your account for each service

AWS KMS keys (KMS keys) are the primary resource in AWS KMS. You can use a KMS key to encrypt, decrypt, and re-encrypt data. It can also generate data keys that you can use outside of AWS KMS. AWS KMS is replacing the term customer master key (CMK) with AWS KMS key and KMS key.

AWS managed CMKs are CMKs in your account that are created, managed, and used on your behalf by an AWS service that is integrated with AWS KMS. Some AWS services support only an AWS managed CMK. Others use an AWS owned CMK or offer you a choice of CMKs. AWS managed CMK can be used only for your AWS account.

You can view the AWS managed CMKs in your account, view their key policies, and audit their use in AWS CloudTrail logs. However, you cannot manage these CMKs, rotate them, or change their key policies. And, you cannot use AWS managed CMKs in cryptographic operations directly; the service that creates them uses them on your behalf.

AWS managed CMKs appear on the AWS managed keys page of the AWS Management Console for AWS KMS. You can also identify most AWS managed CMKs by their aliases, which have the format `aws/service-name`, such as `aws/redshift`.

You do not pay a monthly fee for AWS managed CMKs. They can be subject to fees for use in excess of the free tier, but some AWS services cover these costs for you.

Incorrect options:

Create your own customer managed keys (CMKs) in AWS KMS - The AWS KMS keys that you create are customer managed keys. Customer managed keys are KMS keys in your AWS account that you create, own, and manage. You have full control over these KMS keys, including establishing and maintaining their key policies, IAM policies, and grants, enabling and disabling them, rotating their cryptographic material, adding tags, creating aliases that refer to the KMS keys, and scheduling the KMS keys for deletion.

customer managed key (CMK) incur a monthly fee and a fee for use in excess of the free tier. They are counted against the AWS KMS quotas for your account.

Use AWS KMS APIs to encrypt data within your own application by using the AWS Encryption SDK - AWS KMS APIs can also be accessed directly through the AWS KMS Command Line Interface or AWS SDK for programmatic access. AWS KMS APIs can also be used indirectly to encrypt data within your own applications by using the AWS Encryption SDK. This requires code changes and is not the easiest way to achieve encryption.

Use AWS owned CMK in the service you wish to use encryption - AWS owned CMKs are a collection of CMKs that an AWS service owns and manages for use in multiple AWS accounts. Although AWS owned CMKs are not in your AWS account, an AWS service can use its AWS owned CMKs to protect the resources in your account. AWS owned CMK can be used for multiple AWS accounts.

You do not need to create or manage the AWS owned CMKs. However, you cannot view, use, track, or audit them. You are not charged a monthly fee or usage fee for AWS owned CMKs and they do not count against the AWS KMS quotas for your account.

Reference:

https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html#master_keys

Question 64: **Correct**

A blogging company is looking at an easy to use solution to host WordPress blogs. The company needs a cost-effective, readily available solution without the need to manage the configurations for servers or the databases.

Which AWS service will help you achieve this functionality?

- **Amazon Elastic Compute Cloud (EC2) with Amazon S3 for storage**
- **AWS Fargate**
- **Amazon Lightsail**

(Correct)

- **Host the application directly on Amazon S3**

Explanation

Correct option:

Amazon Lightsail

Amazon Lightsail is the easiest way to get started with AWS for developers, small businesses, students, and other users who need a solution to build and host their applications on the cloud. Lightsail provides developers with compute, storage, and networking capacity and capabilities to deploy and manage websites and web applications in the cloud. Lightsail includes everything you need to launch your project quickly – virtual machines, containers, databases, CDN, load balancers, DNS management, etc. – for a low, predictable monthly price.

You can get preconfigured virtual private server (VPS) plans that include everything to easily deploy and manage your application. Amazon Lightsail is best suited to projects that require a few virtual private servers and users who prefer a simple management interface. Common use cases for Lightsail include running websites, web applications, blogs, e-commerce sites, simple software, and more.

Also referred to as a bundle, a Lightsail plan includes a virtual server with a fixed amount of memory (RAM) and compute (vCPUs), SSD-based storage (disks), and a free data transfer allowance. Amazon Lightsail plans also offer static IP addresses (5 per account) and DNS management (3 domain zones per account). Lightsail plans are charged on an hourly, on-demand basis, so you only pay for a plan when you're using it.

Amazon Lightsail offers a number of preconfigured, one-click-to-launch operating systems, development stacks, and web applications, including Linux and Windows OS, WordPress, LAMP, CentOS, and more.

Incorrect options:

AWS Fargate - AWS Fargate is a serverless compute engine for containers that work with both Amazon Elastic Container Service (ECS) and Amazon Elastic Kubernetes Service (EKS). Fargate makes it easy for you to focus on building your applications. Fargate removes the need to provision and manage servers, lets you specify and pay for resources per application, and improves security through application isolation by design. Fargate is meant for container applications that you wish to host without having to manage the servers such as EC2 instances.

Amazon Elastic Compute Cloud (EC2) with Amazon S3 for storage - Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides secure, resizable compute capacity in the cloud. It is designed to make web-scale cloud computing easier for developers. Amazon EC2's simple web service interface allows you to obtain and configure capacity with minimal friction. It provides you with complete control of your computing resources and lets you run on Amazon's proven computing environment.

Amazon EC2 instances need to be managed by the customers and hence is the wrong choice for the given scenario.

Host the application directly on Amazon S3 - Amazon S3 does not support compute capacity to generate dynamic content. Only static web applications can be hosted on Amazon S3.

References:

<https://aws.amazon.com/lightsail/>

<https://docs.aws.amazon.com/AmazonS3/latest/dev/WebsiteHosting.html>

Question 65: **Correct**

Which of the following points have to be considered when choosing an AWS Region for a service? (Select two)

- **AWS Region chosen should be geographically closer to the user base that utilizes the hosted AWS services**

(Correct)

- **The AWS Region with high availability index should be considered for your business**
- **The AWS Region should have 5G networks, to seamlessly access the breadth of AWS services in the region**
- **Compliance and Data Residency guidelines of the AWS Region should match your business requirements**

(Correct)

- **The AWS Region chosen should have all its Availability Zones (AZ) within 100 Kms radius, to keep latency low for hosted applications**

Explanation

Correct options:

Compliance and Data Residency guidelines of the AWS Region should match your business requirements

If you have data residency requirements, you can choose the AWS Region that is in close proximity to your desired location. You retain complete control and ownership over the region in which your data is physically located, making it easy to meet regional compliance and data residency requirements.

AWS Region chosen should be geographically closer to the user base that utilizes the hosted AWS services

When deploying your applications and workloads to the cloud, you have the flexibility in selecting a technology infrastructure and AWS Region that is closest to your primary target of users.

Incorrect options:

The AWS Region with high availability index should be considered for your business - AWS delivers the highest network availability of any cloud provider. Each region is fully isolated and comprised of multiple Availability Zone (AZ), which are fully isolated partitions of our infrastructure. All AWS Regions are designed to be highly available.

The AWS Region should have 5G networks, to seamlessly access the breadth of AWS services in the region - AWS Local Zones and AWS Wavelength, with telco providers, provide performance for applications that require single-digit millisecond latencies by delivering AWS infrastructure and services closer to end-users and 5G connected devices. But, having a 5G network is not a factor for a customer to decide on an AWS Region.

The AWS Region chosen should have all its Availability Zones (AZ) within 100 Kms radius, to keep latency low for hosted applications - An Availability Zone (AZ) is one or more discrete data centers with redundant power, networking, and connectivity in an AWS Region. AZ's are physically separated by a meaningful distance, many kilometers, from any other Availability Zone (AZ), although all are within 100 km (60 miles) of each other. This applies to all Availability Zones (AZ) and hence is not a criterion for choosing an AWS Region.

Reference:

https://aws.amazon.com/about-aws/global-infrastructure/regions_az/