**Answer Sheet**

**Q1) Which of the following AWS services uses tiered pricing?**

✅ S3
**Explanation:-**This option is correct. For S3 storage and data transfer OUT from EC2, AWS follows a tiered pricing model. Tiered pricing means that you pay less per unit when you use more. For example the more GBs you use in S3, the more you save.
⚪ AWS Cost Explorer
**Explanation:-**This option is incorrect.
⚪ lightsail
**Explanation:-**This option is incorrect.
⚪ VPC
**Explanation:-**This option is incorrect.

---

**Q2) For mobile applications, which of the following allows client devices access to AWS resources?**

⚪ None of these
**Explanation:-**This option is incorrect.
✅ Amazon Cognito
**Explanation:-**This option is correct. Amazon Cognito provides solutions to control access to backend resources from your app. You can define roles and map users to different roles so your app can access only the resources that are authorized for each user.
⚪ Amazon Inspector
**Explanation:-**this option is not correct. Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS.
⚪ Amazon GuardDuty
**Explanation:-**This option is not correct. Amazon GuardDuty is a threat detection service that continuously monitors for malicious activity and unauthorized behavior to protect your AWS accounts and workloads.

---

**Q3)**

**You need to improve the security of your AWS service APIs against unauthorized access.**

**What activity best achieves this goal?**

⚪ Set up two login passwords
**Explanation:-**This option is incorrect.
✅ Apply Multi-Factor Authentication (MFA)
**Explanation:-**This option is correct. AWS Multi-Factor Authentication (MFA) is a simple best practice that adds an extra layer of protection on top of your user name and password.
⚪ Use only one private e-mail address to access the console
**Explanation:-**This option is incorrect.
⚪ Download root access privileges to your device
**Explanation:-**This option is incorrect.

---

**Q4)**

**A company is using EC2 Instances to run their e-commerce site on the AWS platform.**

**A busy e-commerce site could lose thousands of dollars every minute it is unavailable.**

**Which of the principles below should they adopt to ensure that even if some of their EC2 Instances stop working, their site will continue to run as usual?**

✅ Use a fault tolerant system.
**Explanation:-**This option is correct. A system that is designed to be fault tolerant can recover gracefully from EC2 instance failures. Amazon Web Services gives you access to a vast amount of IT infrastructure–compute, storage, and communications–that you can allocate automatically (or nearly automatically) to account for almost any kind of failure.
⚪ Use an adaptive system.
**Explanation:-**This option is incorrect.
⚪ Use an elastic system.
**Explanation:-**This option is incorrect.
⚪ Use a scalable system.
**Explanation:-**This option is incorrect.

---

**Q5) You decide to buy one reserved instance for one year. Which of the following options provides the largest discount?**

⚪ None of these
**Explanation:-**This option is incorrect.
✅ All up-front.
**Explanation:-**This option is correct. You can choose between three payment options when you purchase a Standard or Convertible Reserved Instance.
1- No up-front
2- Partial up-front
3- All up-front.
The general rule is: “the more you spend upfront, the more discounts you get.
With the All Upfront option, you pay for the entire Reserved Instance term with one upfront payment. This option provides you with the largest discount compared to On-Demand instance pricing.

Partial up-front.

**Explanation:-**This option is not correct. With the Partial Upfront option, you make a low upfront payment and are then charged a discounted hourly rate for the instance for the duration of the Reserved Instance term. The price of the instance will be less than the price of the instance purchased using the “No Upfront option” because you do make some type of upfront payment.

No up-front.

**Explanation:-**This option is not correct. The No Upfront option does not require any upfront payment and provides a discounted hourly rate for the duration of the term. But the price will be much higher compared to other options because you didn’t pay anything upfront.

---

**Q6)**

**You need to select an EC2 Instance type to service your workloads. If you have flexibility about the availability of the Amazon EC2 Instances, which of the following EC2 Instances would be most cost-effective?**

Dedicated instances

**Explanation:-**This option is not correct. Dedicated instances are used when you need your instances to be isolated at the host hardware level from instances that belong to other AWS accounts.

On-demand instances

**Explanation:-**This option is not correct. On-demand instances are used when you need a consistent compute capacity that cannot be interrupted.

Reserved Instances.

**Explanation:-**This option is not correct. Spot instances provide more discounts than Reserved instances. Also, you are committed to a one or three year term when procuring Reserved Instances.

Spot instances

**Explanation:-**This option is correct. Spot Instances are a cost-effective choice if you can be flexible about when your applications run and if your applications can be interrupted. For example, Spot Instances are well-suited for data analysis, batch jobs, background processing, and optional tasks, but are not suitable for always-on e-commerce front-end platforms.

---

**Q7)**

**Your organization heavily uses Chef to operate their configuration management systems.**

**Which AWS Cloud service provides integration with Chef recipes to automate the configuration of servers across Amazon EC2 Instances?**

AutoScaling

**Explanation:-**This option B is not correct. AutoScaling is used to increase or decrease capacity based on demand.

AWS OpsWorks

**Explanation:-**This option is correct. 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 Config

**Explanation:-**This option is not correct. AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources.

AWS CloudFormation

**Explanation:-**This option is not correct. AWS CloudFormation allows you to provision your resources using code.

---

**Q8)**

**You want to monitor the CPU utilization of an EC2 resource in AWS.**

**Which of the below services can help in this regard?**

AWS Inspector

**Explanation:-**This option is not correct. Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS.

AWS Cloudwatch

**Explanation:-**This option is correct. Amazon CloudWatch is a service that monitors AWS cloud resources and the applications you run on AWS. You can use Amazon CloudWatch to collect and track metrics, collect and monitor log files, set alarms, and automatically react to changes in your AWS resources. 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/

AWS Trusted Advisor

**Explanation:-**This option is not correct. AWS Trusted Advisor is an online tool that provides real time guidance to help you provision your resources following AWS best practices.

AWS Config

**Explanation:-**This option is not correct. AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources.

---

**Q9)**

**A company wants to reduce their overall AWS costs but they don’t know where the high costs come from.**

**What should they do? (Choose two)**

Use the AWS Price List API.

**Explanation:-**This option is not correct. The AWS Price List API is used to know the prices of the AWS services.

Activate cost allocation tags to categorize and track their costs.

**Explanation:-**A tag is a label that you or AWS assigns to an AWS resource. Each tag consists of a key and a value. A key can have more than one value. You can use tags to organize your resources, and cost allocation tags to track your AWS costs on a detailed level. After you activate cost allocation tags, AWS uses the cost allocation tags to organize your resource costs on your cost allocation report, to make it easier for you to

categorize and track your AWS costs.
Enabling billing alerts using CloudWatc
Use the Budget Explorer to estimate and plan their AWS costs.
**Explanation:-**This Option is not correct. There is nothing called Budget Explorer.
Use CloudWatch to create billing alerts that notify them when their usage of their services exceeds thresholds that they define.
**Explanation:-**A tag is a label that you or AWS assigns to an AWS resource. Each tag consists of a key and a value. A key can have more than one value. You can use tags to organize your resources, and cost allocation tags to track your AWS costs on a detailed level. After you activate cost allocation tags, AWS uses the cost allocation tags to organize your resource costs on your cost allocation report, to make it easier for you to categorize and track your AWS costs.
Enabling billing alerts using CloudWatc

---

**Q10) Which of the following can be used to control access to your Amazon EC2 instances?**

None of these
**Explanation:-**This option is incorrect.
EC2 security groups
**Explanation:-**This option is correct. Security groups are used to define and control the way you want your instances to be accessed, and whether or not certain kind of communications is allowed. AWS security groups provide security at the protocol and port access level. You can add rules to each security group that allow traffic to or from its associated instances.
IAM policies
**Explanation:-**This option is not correct.IAM policies are used to grant users permissions to perform specific actions on EC2. A user can only access the instance and perform these actions if his IP address is allowed in the security group that is attached to the instance. In brief, security groups are used to control who can access the instance. IAM policies are used to control what actions can a specific user perform after accessing the instance.
DB security groups
**Explanation:-**This option is not correct. DB security groups are used to control access to the databases.

---

**Q11)**

**You have 2 accounts in AWS. One for Dev and the other for QA. All are part of consolidated billing.**

**The master account has purchased 4 reserved instances. The Dev department is currently using 2 reserved instances.**

**The QA team is planning on using 3 instances, which are of the same instance type.**

**What is the pricing tier of the instances that can be used by the QA Team?**

Two Reserved and 1 on-demand
**Explanation:-**This option is correct. For billing purposes, the consolidated billing feature of AWS Organizations treats all the accounts in the organization as one account. This means that all accounts in the organization can receive the hourly cost benefit of Reserved Instances that are purchased by any other account. Since 2 reserved instances are already used by the Dev team , then there are another 2 instances that can be used by the QA team. The rest of the instances can be on-demand instances.
Three Reserved and one on-demand
**Explanation:-**This option is incorrect.
One Reserved and 2 on-demand
**Explanation:-**This option is incorrect.
No Reserved and 3 on-demand
**Explanation:-**This option is incorrect.

---

**Q12)**

**AWS allows users to manage their resources using a web based user interface.**

**What is the name of this interface?**

AWS API
**Explanation:-**This option is not correct. AWS API refers to the AWS application programming interface.
AWS Management Console
**Explanation:-**This option is correct. The AWS Management Console allows you to access and manage Amazon Web Services through a simple and intuitive web-based user interface. You can also use the AWS Console mobile app to quickly view resources on the go.
AWS CLI
**Explanation:-**This option is not correct. The AWS Command Line Interface (CLI) is a unified tool to manage your AWS services. With just one tool to download and configure, you can control multiple AWS services from the command line and automate them through scripts.
AWS SDK
**Explanation:-**This option is not correct. The AWS SDK (Software Development Kit) allows you to interact with AWS services using your preferred programming language.

---

**Q13) Which of the following should an IAM user provide to interact with AWS services using the AWS CLI?**

User ID
**Explanation:-**This option is incorrect.
Secret token
**Explanation:-**This option is incorrect.
Access keys
**Explanation:-**This option is correct. Access keys consist of an access key ID and secret access key, which are used to sign programmatic requests to AWS using the CLI or the SDK.
User name and password
**Explanation:-**This option is incorrect.

---

**Q14)**

**A company has a DevOps team in its organizational structure. They are looking forward to moving to the AWS Cloud.**

**They are wondering if there is an AWS service that can help them manage infrastructure as code.**

**Which of the following would you suggest for them?**

✅ AWS CloudFormation
**Explanation:-**This option is correct. AWS CloudFormation is a service that helps you model and set up your Amazon Web Services resources so that you can spend less time managing those resources and more time focusing on your applications that run in AWS. You create a template that describes all the AWS resources that you want (like Amazon EC2 instances or Amazon RDS DB instances), and AWS CloudFormation takes care of provisioning and configuring those resources for you.
⚪ AWS Inspector
**Explanation:-**This option is not correct. Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS.
⚪ Amazon EMR
**Explanation:-**This option is not correct. Amazon EMR is used to run and scale Apache Spark, Hadoop, HBase, Presto, Hive, and other Big Data Frameworks.
⚪ AWS Config
**Explanation:-**This option is not correct. AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources.

---

**Q15)**

**An organization has 500 employees. The organization wants to set up AWS access for each department.**

**Which of the below-mentioned options is a possible solution?**

⚪ It is not possible to manage more than 100 IAM users with AWS
**Explanation:-**This option is not correct. The current limit of users in an AWS account is 5000.
✅ Create an IAM group for each department and assign IAM users to the groups.
**Explanation:-**This option is correct. An IAM group is a collection of IAM users that are managed as a unit. Groups let you specify permissions for multiple users, which can make it easier to manage the permissions for those users. For example, you could have a group called Admins and give that group the types of permissions that administrators typically need. Any user in that group automatically has the permissions that are assigned to the group.
⚪ Create IAM roles based on the permission and assign users to each role.
**Explanation:-**This option is not correct. An IAM role is very similar to a user, in that it is an identity with permission policies that determine what the identity can and cannot do in AWS. However, a role does not have any credentials (password or access keys) associated with it. Instead of being uniquely associated with one person, a role is intended to be assumable by anyone who needs it (Note: we mean by anyone: any user who has permission to assume the role).
⚪ Create IAM users and provide individual permission for each one of them.
**Explanation:-**This option is not correct. It is not an effective solution and waste of time.

---

**Q16)**

**A company has decided to migrate to AWS.**

**What design principles should they consider to facilitate good design in the cloud?**

⚪ Spend more time and effort when architecting your environment, it is not easy to change your decisions later.
**Explanation:-**This option is not correct. In AWS, you can test and provision your resources on-demand and pay only for what you use with no long term contracts. This enables you to make any changes you want in your architecture design at any time without any risks.
⚪ Analyze your on-premises usage to guess your capacity needs on AWS.
**Explanation:-**This option is not correct. Pay-as-you-go pricing eliminates the need to guess your capacity needs.
⚪ Use AWS reservations to reduce costs when testing your production environment.
**Explanation:-**This option is not correct. Reservations in AWS are not an appropriate choice when you need to test your AWS environment since it requires you to pay for at least one year.
✅ Automate to make architectural experimentation easier.
**Explanation:-**This option is correct. The Well-Architected Framework identifies a set of general design principles to facilitate good design in the cloud:
1- Stop guessing your capacity needs: Eliminate guessing about your infrastructure capacity needs. When you make a capacity decision before you deploy a system, you might end up sitting on expensive idle resources or dealing with the performance implications of limited capacity. With cloud computing, these problems can go away.

---

**Q17)**

**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.**

**What should you do?**

⚪ Contact the AWS Customer Service team.
**Explanation:-**This option is not correct. The AWS Customer Service team is at the forefront of this transformational technology assisting a global list of customers that are taking advantage of a growing set of services and features to run their mission-critical applications. The team helps AWS customers understand what Cloud Computing is all about, and whether it can be useful for their business needs.
⚪ Contact the AWS Security team.
**Explanation:-**This option is not correct. The AWS Security team is responsible for the security of services offered by AWS.
⚪ Contact the AWS Concierge team.
**Explanation:-**This option is not correct. The AWS Concierge team can assist you with the issues that are related to your billing and account management.
✅ Contact the AWS Abuse team.

**Explanation:-**This option is correct.

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

This option is correct.

The AWS Abuse team can assist you when AWS resources are being used to engage in the following types of abusive behavior:
I. Spam: You are receiving unwanted emails from an AWS-owned IP address, or AWS resources are being used to spam websites or forums.
II. 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.
III. 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.
IV. Intrusion attempts: Your logs show that one or more AWS-owned IP addresses are used to attempt to log in to your resources.
V. 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.
VI. 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.

---

**Q18)**

**One of the most important AWS best practices to follow is the cloud architecture principle of elasticity.**

**How does following this principle improve your architecture's design?**

○ None of these
**Explanation:-**This option is not correct. It is not possible to scale on-premises resources automatically. When deploying on-premises, you have to guess on your infrastructure capacity needs.
○ By reducing interdependencies between application components wherever possible
**Explanation:-**This option is not correct. Reducing interdependencies between application components is much more related to the concept of "Loose Coupling". Loose coupling is an approach that involves interconnecting the components in a system or network so that those components depend on each other to the least extent practical. Engineers should architect their system or application such that failure in one component does not negatively affect other components.
○ By automatically scaling your on-premises resources based on changes in demand
**Explanation:-**This option is not correct. It is not possible to scale on-premises resources automatically. When deploying on-premises, you have to guess on your infrastructure capacity needs.
✓ By automatically provisioning the required AWS resources based on changes in demand.
**Explanation:-**This option is correct. The concept of Elasticity involves the ability of a service to automatically scale its resources up or down based on changes in demand. For example, Amazon EC2 Autoscaling can help automate the process of adding or removing Amazon EC2 instances as demand increases or decreases.

---

**Q19) Which of the following allows you to carve out a portion of the AWS Cloud?**

○ AWS Subnets
**Explanation:-**This option is not correct. A subnet is a range of IP addresses in your VPC.
○ AWS Regions
**Explanation:-**This option is not correct. An AWS Region is a physical location in the world. Each Amazon Region is designed to be completely isolated from the other Amazon Regions. This achieves the greatest possible fault tolerance and stability.
✓ AWS VPC
**Explanation:-**This option is correct. Amazon Virtual Private Cloud (Amazon VPC) enables you to launch AWS resources into a virtual network that you've defined. This virtual network closely resembles a traditional network that you'd operate in your own data center, with the benefits of using the scalable infrastructure of AWS.
○ AWS Availability Zones
**Explanation:-**This option is not correct. Each region has multiple, isolated locations known as Availability Zones. Availability Zones consist of one or more discrete data centers, each with redundant power, networking, and connectivity, housed in separate facilities. These Availability Zones offer you the ability to operate production applications and databases that are more highly available, fault tolerant, and scalable than would be possible to operate out of a single data center.

---

**Q20)**

**You have just set up a brand-new AWS account. You want to keep monthly billing under $100, but you are worried about going over that limit.**

**What can you use in order to be notified when the monthly bill approaches $100?**

✓ A CloudWatch billing alarm that triggers an SNS notification to your email address.
**Explanation:-**This option is correct. In CloudWatch, you can set up a billing alarm that triggers if your costs exceed a threshold that you set. This CloudWatch alarm can also be configured to trigger an SNS notification to your email address.
○ A CloudWatch billing alarm that triggers a CloudTrail notification to your email address.
**Explanation:-**This option is not correct. CloudTrail cannot be used to send email notifications.
○ A CloudTrail billing alarm that triggers an SNS notification to your email address.
**Explanation:-**This option is not correct. AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. You cannot use it to setup billing alarms.
○ A SNS billing alarm that triggers a CloudWatch notification to your email address.
**Explanation:-**This option is not correct. SNS is the service that is used to send email notifications.

---

**Q21) Which of the following helps you by collecting important metrics from AWS RDS and EC2 Instances?**

✓ Amazon CloudWatch
**Explanation:-**This option is correct. Amazon CloudWatch is a monitoring service for AWS cloud resources and the applications you run on AWS. You can use Amazon CloudWatch to collect and track metrics, collect and monitor log files, set alarms, and automatically react to changes in your AWS resources.

Amazon CloudTrail logs

**Explanation:-**This option is not correct. CloudTrail logs include details about any API calls made to your AWS services.

Amazon CloudFormation

**Explanation:-**This option is not correct. Amazon CloudFormation allows you to use a simple text file to model and provision, in an automated and secure manner, all the resources needed for your applications across all regions and accounts.

Amazon Config

**Explanation:-**This option is not correct. Amazon Config is used to record and evaluate configurations of your AWS resources.

---

**Q22)**

**Your application requirements for CPU and RAM change rapidly these days.**

**Which service can be used to dynamically adjust those resources based on demand?**

Amazon Elastic Container Service

**Explanation:-**This option is not correct. Amazon Elastic Container Service is used to run containerized applications in AWS.

Auto Scaling

**Explanation:-**This option is correct. The AWS Auto Scaling service allows you to automatically provision new resources to meet demand and maintain performance. When demand decreases Auto Scaling shuts down unused resources to reduce costs.

Amazon Route53

**Explanation:-**This option is not correct. Route53 is provides the Domain Name System (DNS) in the cloud.

ELB

**Explanation:-**This option is not correct. Elastic Load Balancing (ELB) is used to distribute traffic automatically across multiple targets, such as Amazon EC2 instances, containers, IP addresses, and Lambda functions.

---

**Q23) Which of the following aspects of security are managed by AWS? (Choose two)**

Securing global physical infrastructure

**Explanation:-**AWS is continuously innovating the design and systems of its data centers to protect them from man-made and natural risks. For example, at the first layer of security, AWS provides a number of security features depending on the location, such as security guards, fencing, security feeds, intrusion detection technology, and other security measures.
According to the Shared Responsibility model, patching of the underlying hardware is the AWSâ€™ responsibility. AWS is responsible for patching and fixing flaws within the infrastructure, but customers are responsible for patching their guest OS and applications.

Access permissions

Hardware patching

**Explanation:-**AWS is continuously innovating the design and systems of its data centers to protect them from man-made and natural risks. For example, at the first layer of security, AWS provides a number of security features depending on the location, such as security guards, fencing, security feeds, intrusion detection technology, and other security measures.
According to the Shared Responsibility model, patching of the underlying hardware is the AWSâ€™ responsibility. AWS is responsible for patching and fixing flaws within the infrastructure, but customers are responsible for patching their guest OS and applications.

VPC security

Encryption of EBS volumes

---

**Q24) Using Amazon RDS falls under the shared responsibility model. Which of the following are customer responsibilities? (Choose two)**

Patching the database software

Managing the database settings

**Explanation:-**Amazon RDS manages the work involved in setting up a relational database, from provisioning the infrastructure capacity you request to installing the database software. Once your database is up and running, Amazon RDS automates common administrative tasks such as performing backups and patching the software that powers your database. With optional Multi-AZ deployments, Amazon RDS also manages synchronous data replication across Availability Zones with automatic failover. Since Amazon RDS provides native database access, you interact with the relational database software as you normally would. This means you're still responsible for managing the database settings that are specific to your application. You'll need to build the relational schema that best fits your use case and are responsible for any performance tuning to optimize your database for your applicationâ€™s workflow.

Performing backups

Building the relational database schema

**Explanation:-**Amazon RDS manages the work involved in setting up a relational database, from provisioning the infrastructure capacity you request to installing the database software. Once your database is up and running, Amazon RDS automates common administrative tasks such as performing backups and patching the software that powers your database. With optional Multi-AZ deployments, Amazon RDS also manages synchronous data replication across Availability Zones with automatic failover. Since Amazon RDS provides native database access, you interact with the relational database software as you normally would. This means you're still responsible for managing the database settings that are specific to your application. You'll need to build the relational schema that best fits your use case and are responsible for any performance tuning to optimize your database for your applicationâ€™s workflow.

Installing the database software

---

**Q25) Based on the AWS Shared Responsibility Model, which of the following are the sole responsibility of AWS? (Choose two)**

Installing software on EC2 instances

Creating hypervisors

**Explanation:-**AWS is responsible for items such as the physical security of its data centers, creating hypervisors, replacement of old disk drives, and patch management of the infrastructure.
The customers are responsible for items such as building application schema, analyzing network performance, configuring security groups and network ACLs and encrypting their data.

Configuring Access Control Lists (ACLs)

Monitoring network performance

Hardware maintenance

**Explanation:-**AWS is responsible for items such as the physical security of its data centers, creating hypervisors, replacement of old disk drives,

and patch management of the infrastructure.
The customers are responsible for items such as building application schema, analyzing network performance, configuring security groups and network ACLs and encrypting their data.

---

**Q26) When running a workload in AWS, the customer is NOT responsible for: (Select two)**

- Reserving capacity
- Auditing and regulatory compliance
- Running penetration tests
- ✅ Data center operations

**Explanation:-**AWS is responsible for the infrastructure security and all data center operations such as racking, stacking, and powering servers, so customers can focus on revenue generating activities rather than on IT infrastructure.

- ✅ Infrastructure security

**Explanation:-**AWS is responsible for the infrastructure security and all data center operations such as racking, stacking, and powering servers, so customers can focus on revenue generating activities rather than on IT infrastructure.

---

**Q27) What are AWS shared controls?**

- ✅ Controls that apply to both the infrastructure layer and customer layers

**Explanation:-**Shared Controls are controls which apply to both the infrastructure layer and customer layers, but in completely separate contexts or perspectives. In a shared control, AWS provides the requirements for the infrastructure and the customer must provide their own control implementation within their use of AWS services. Examples include:
** Patch Management – AWS is responsible for patching the underlying hosts and fixing flaws within the infrastructure, but customers are responsible for patching their guest OS and applications.
** Configuration Management – AWS maintains the configuration of its infrastructure devices, but a customer is responsible for configuring their own guest operating systems, databases, and applications.
** Awareness & Training - AWS trains AWS employees, but a customer must train their own employees.

- Controls that are solely the responsibility of the customer based on the application they are deploying within AWS services
- Controls that a customer inherits from AWS
- Controls that the customer and AWS collaborate together upon to secure the infrastructure

---

**Q28) For managed services like Amazon DynamoDB, which of the below is AWS responsible for? (Choose two)**

- Protecting Credentials
- Creating access policies
- Logging access activity
- ✅ Operating system maintenance

**Explanation:-**AWS has increased responsibilities for its managed services. Examples of managed services include Amazon DynamoDB, Amazon RDS, Amazon Redshift, Amazon Elastic MapReduce, and Amazon WorkSpaces. These services provide the scalability and flexibility of cloud-based resources with less operational overhead because AWS handle basic security tasks like guest operating system (OS) and database patching, installing antivirus software, backup, and disaster recovery. For most managed services, you only configure logical access controls and protect account credentials, while maintaining control and responsibility of any personal data.

- ✅ Patching the database software

**Explanation:-**AWS has increased responsibilities for its managed services. Examples of managed services include Amazon DynamoDB, Amazon RDS, Amazon Redshift, Amazon Elastic MapReduce, and Amazon WorkSpaces. These services provide the scalability and flexibility of cloud-based resources with less operational overhead because AWS handle basic security tasks like guest operating system (OS) and database patching, installing antivirus software, backup, and disaster recovery. For most managed services, you only configure logical access controls and protect account credentials, while maintaining control and responsibility of any personal data.

---

**Q29) Which of the below are responsibilities of the customer when using Amazon EC2? (Choose TWO)**

- Maintaining consistent hardware components
- ✅ Installing and configuring third-party software

**Explanation:-**Amazon EC2 requires the customer to perform all of the necessary security configuration and management tasks. When customers deploy Amazon EC2 instances, they are responsible for management of custom Amazon Machine Images, management of the guest operating systems (including updates and security patches), securing application access and data, installing and configuring third-party applications or utilities, and the configuration of the AWS-provided firewall (called a security group) on each instance.

- ✅ Protecting sensitive data

**Explanation:-**Amazon EC2 requires the customer to perform all of the necessary security configuration and management tasks. When customers deploy Amazon EC2 instances, they are responsible for management of custom Amazon Machine Images, management of the guest operating systems (including updates and security patches), securing application access and data, installing and configuring third-party applications or utilities, and the configuration of the AWS-provided firewall (called a security group) on each instance.

- Setup and operation of managed databases
- Patching of the underlying infrastructure

---

**Q30) Which of the following are examples of the customer's responsibility to implement "security in the cloud"? (Choose TWO)**

- Patch management of the underlying infrastructure
- Replacing physical hardware
- Creating a new hypervisor
- ✅ File system encryption

**Explanation:-**"Security in the Cloud" refers to the Customer's responsibility in the Shared Responsibility Model. Customers are responsible for items such as building application schema, monitoring server and application performance, configuring security groups and network ACLs, and encrypting their data.
"Security of the Cloud" refers to the AWS' responsibility in the Shared Responsibility Model. AWS is responsible for items such as the physical security of the DC (data center), creating hypervisors, replacement of old disk drives, and patch management of the infrastructure.

- ✅ Building a schema for an application

**Explanation:-**"Security in the Cloud" refers to the Customer's responsibility in the Shared Responsibility Model. Customers are responsible for items such as building application schema, monitoring server and application performance, configuring security groups and network ACLs, and encrypting their data.
"Security of the Cloud" refers to the AWS' responsibility in the Shared Responsibility Model. AWS is responsible for items such as the physical security of the DC (data center), creating hypervisors, replacement of old disk drives, and patch management of the infrastructure.

---

**Q31) Which of the following are use cases for Amazon S3? (Choose two)**

- Cost-effective database and log storage
- Hosting websites that require sustained high CPU utilization
- Processing data streams at any scale
- ✅ A media store for the CloudFront service

**Explanation:-**You can host a static website on Amazon Simple Storage Service (Amazon S3). On a static website, individual webpages include static content. They might also contain client-side scripts. To host a static website, you configure an Amazon S3 bucket for website hosting, allow public read access, and then upload your website content to the bucket. By contrast, a dynamic website relies on server-side processing, including server-side scripts such as PHP, JSP, or ASP.NET. Amazon S3 does not support server-side scripting. Amazon Web Services (AWS) also has resources for hosting dynamic websites such as Amazon EC2.
Amazon S3 is an excellent storage facility for your media assets. It is infinitely scalable, has built-in redundancy, and is available to you on a pay-as-you-go basis. For example, if you want to deliver or stream video files to your global users, all you need to do is to put your content in an S3 bucket and create a CloudFront distribution that points to the bucket. Your user's video player will use CloudFront URLs to request the video file. The request will be directed to the best edge location, based on the user's location. The Amazon Cloudfront Content Delivery Network (CDN) will serve the video from its cache, fetching it from the S3 bucket if it has not already been cached. The CDN caches content at the edge locations for consistent, low-latency, high-throughput video delivery.

- ✅ Hosting static websites

**Explanation:-**You can host a static website on Amazon Simple Storage Service (Amazon S3). On a static website, individual webpages include static content. They might also contain client-side scripts. To host a static website, you configure an Amazon S3 bucket for website hosting, allow public read access, and then upload your website content to the bucket. By contrast, a dynamic website relies on server-side processing, including server-side scripts such as PHP, JSP, or ASP.NET. Amazon S3 does not support server-side scripting. Amazon Web Services (AWS) also has resources for hosting dynamic websites such as Amazon EC2.
Amazon S3 is an excellent storage facility for your media assets. It is infinitely scalable, has built-in redundancy, and is available to you on a pay-as-you-go basis. For example, if you want to deliver or stream video files to your global users, all you need to do is to put your content in an S3 bucket and create a CloudFront distribution that points to the bucket. Your user's video player will use CloudFront URLs to request the video file. The request will be directed to the best edge location, based on the user's location. The Amazon Cloudfront Content Delivery Network (CDN) will serve the video from its cache, fetching it from the S3 bucket if it has not already been cached. The CDN caches content at the edge locations for consistent, low-latency, high-throughput video delivery.

---

**Q32)**

**A company decides to migrate its Oracle database to AWS.**

**Which AWS service can help achieve this without negatively impacting the functionality of the source database?**

- RDS Multi-AZ

**Explanation:-**This option is not correct. RDS Multi-AZ is a feature of Amazon RDS that is used to increase the availability of the database.

- AWS Server Migration Service

**Explanation:-**This option is not correct. AWS Server Migration Service (SMS) is used to migrate your on-premises workloads to AWS.

- AWS Application Discovery Service

**Explanation:-**This option is not correct. AWS Application Discovery Service helps enterprise customers plan migration projects by gathering information about their on-premises data centers.

- ✅ AWS Database Migration Service

**Explanation:-**This option is correct. AWS Database Migration Service (DMS) helps you migrate databases to AWS easily and securely. The source database remains fully operational during the migration, minimizing downtime to applications that rely on the database. The AWS Database Migration Service can migrate your data to and from most widely used commercial and open-source databases. The service supports homogeneous migrations such as Oracle to Oracle, as well as heterogeneous migrations between different data

---

**Q33) According to the AWS Acceptable Use Policy, penetration testing of EC2 instances:**

- May be performed by the customer on their own instances with prior authorization from AWS.

**Explanation:-**This option is incorrect.

- Are expressly prohibited under all circumstances.

**Explanation:-**This option is incorrect.

- ✅ May be performed by the customer on their own instances without prior authorization from AWS.

**Explanation:-**This option is correct. AWS customers are welcome to carry out security assessments and penetration tests against their AWS infrastructure without prior approval for 8 services
1- Amazon EC2 instances, NAT Gateways, and Elastic Load Balancers.
2- Amazon RDS.
3- Amazon CloudFront.
4- Amazon Aurora.
5- Amazon API Gateways.
6- AWS Lambda and Lambda Edge functions.
7- Amazon Lightsail resources.
8- Amazon Elastic Beanstalk environments.

- Will be performed by AWS upon customer request.

**Explanation:-**This option is incorrect.

---

**Q34) What best describes the "Principle of Least Privilege"?**

- Users should always have a little more permissions granted to them, just in case they end up needed them in the future.

**Explanation:-**This option is incorrect.

Users should submit all access request in written so that there is a paper trail of who needs access to different AWS resources.

**Explanation:-**This option is incorrect.

Users should be granted permissions to access only the resources they need to do their assigned job.

**Explanation:-**This option is correct. The principle of least privilege is one of the most important security practices and it means granting users the required permissions to perform the tasks entrusted to them and nothing more. The security administrator determines what tasks users need to perform and then attach the policies that allow them to perform only those tasks. You should start with a minimum set of permissions and grant additional permissions when necessary. Doing so is more secure than starting wi

All users should have the same baseline permissions granted to them to use basic AWS services.

**Explanation:-**This option is incorrect.

---

**Q35)**

**You noticed that several critical Amazon Elastic Compute Cloud (Amazon EC2) instances have been terminated.**

**Which of the following AWS services would help you determine who took this action?**

AWS Trusted Advisor

**Explanation:-**This option is not correct. AWS Trusted Advisor is an online tool that provides real time guidance to help provision resources following AWS best practices.

AWS CloudTrail

**Explanation:-**This option is correct. 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 an

Amazon CloudWatch

**Explanation:-**This option is not correct. Amazon CloudWatch is used to monitor AWS resources. For example you can use it to monitor the performance of your EBS volumes.

Amazon EC2 Instance Usage report

**Explanation:-**This option is not correct. The report provides a preconfigured view, based on fixed filter settings, that displays information about your usage and cost trends.

---

**Q36)**

**A company is planning to develop an application consisting of hundreds of microservices. They decide to host the application on the AWS Cloud.**

**Since there are a large number of services produced by the application, it needs a powerful tool for analysis and debugging.**

**Which of the following services can best meet this requirement?**

AWS CloudWatch

**Explanation:-**This option is not correct. The main purpose of the AWS CloudWatch is to monitor the utilization of your AWS resources.

Amazon Aurora

**Explanation:-**This option is not correct. Amazon Aurora is a database service.

AWS X-Ray

**Explanation:-**This option is correct. 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.

AWS OpsWorks

**Explanation:-**This option is not correct. AWS OpsWorks is a configuration management service that provides managed instances of Chef and Puppet.

---

**Q37) Which of the following can be used to provide an additional level of security above your username and password when logging into the AWS Console?**

Multi-Factor Authentication (MFA)

**Explanation:-**This option is correct. AWS Multi-Factor Authentication (MFA) is a simple best practice that adds an extra layer of protection on top of using just your user name and password to authenticate.

Encrypted keys.

**Explanation:-**This option is not correct. Logging to the AWS management console doesn't require encrypted keys.

Email verification.

**Explanation:-**This option is not correct. Email verification is the process of verifying your ownership of an account's e-mail address.

Root access privileges.

**Explanation:-**This option is not correct. Root access privileges are used by the account owner to perform certain actions on AWS that cannot be performed using user credentials.

---

**Q38)**

**Your company is developing a critical application and the security of the application is one of the top priorities.**

**Which of the following AWS services will provide infrastructure security optimization recommendations?**

AWS Shield

**Explanation:-**This option is not correct. AWS Shield is a managed Distributed Denial of Service (DDoS) protection service that safeguards applications running on AWS.

AWS Management Console

**Explanation:-**This option is not correct. The AWS Management Console is used to access and manage Amazon Web Services through a simple and intuitive web-based user interface. The console itself doesn't provide any recommendations.

Amazon Aurora

**Explanation:-**This option is not correct. Amazon Aurora is a database service.

AWS Trusted Advisor

**Explanation:-**This option is correct. AWS Trusted Advisor is an online resource to help you reduce cost, increase performance, and improve security by optimizing your AWS environment. Trusted Advisor provides real time guidance to help you provision your resources following AWS best practices.

---

**Q39)**

**You are trying to organize and import gigabytes of data into AWS that are currently structured in JSON-like, name-value documents.**

**Which AWS service would best fit your needs?**

DynamoDB

**Explanation:-**This option is correct. DynamoDB is AWS' NoSQL database offering. NoSQL databases are used for non-structured data that are typically stored in JSON-like, name-value documents.

Lambda

**Explanation:-**This option is not correct. Lambda is a serverless compute service.

Aurora

**Explanation:-**This option is not correct. Aurora is a MySQL and PostgreSQL-compatible relational database NOT a key-value database.

RDS

**Explanation:-**This option is not correct. RDS is a relational database NOT a key-value database.

---

**Q40)**

**You are going to create snapshots from EBS volumes in another geographical location using the console.**

**Where would you create the snapshots?**

In another Edge location

**Explanation:-**This option is incorrect.

In another data center

**Explanation:-**This option is incorrect.

In another Availability Zone

**Explanation:-**This option is incorrect.

In another Region

**Explanation:-**This option is correct. Since you are going to create snapshots in another geographical location then you will create them in another AWS Region.

---

**Q41)**

**Your web application is generating digital policy files for verifying users. Once the files are verified, they may not be required in the future unless there are some compliance issues.**

**If you want to save them in a cost-effective way, what is the best possible solution?**

S3 Intelligent-Tiering

**Explanation:-**This option is not correct. S3 Intelligent-Tiering is ideal for data with unknown or changing access patterns. S3 Intelligent-Tiering is the first cloud object storage class that delivers automatic cost savings by moving data between two access tiers — frequent access and infrequent access — when access patterns change.

AWS RDS

**Explanation:-**This option is not correct. AWS RDS is a database service.

AWS EBS

**Explanation:-**This option is not correct. AWS EBS is a block level storage that provides storage volumes for use with Amazon EC2 and Amazon RDS.

AWS Glacier

**Explanation:-**This option is correct. Amazon Glacier is an extremely low-cost storage service that provides secure, durable, and flexible storage for long-term data backup and archival. With Amazon Glacier, customers can reliably store their data for as little as $0.004 per gigabyte per month. Amazon Glacier enables customers to offload the administrative burdens of operating and scaling storage to AWS, so that they don't have to worry about capacity planning, hardware provisioning, data replication, hardware.

---

**Q42)**

**Your company has a microservices data store that requires access to a NoSQL database.**

**Your IT department has no desire to manage the NoSQL servers.**

**Which Amazon service provides a fully-managed and highly available NoSQL service?**

SimpleDB

**Explanation:-**This option is not correct. SimpleDB doesn't stand out against other database platforms by performance, computing capacity or storage facilities. Nevertheless, it's beneficial to use it as an auxiliary service for other AWS products or as a simple database for non-complex needs. SimpleDB is not suitable for the Microservices Data Store application.

Amazon RDS

**Explanation:-**This option is not correct. Amazon RDS doesn't support NoSQL databases.

ElasticMap Reduce

**Explanation:-**This option is not correct. Amazon EMR provides a managed Hadoop framework.

DynamoDB

**Explanation:-**This option is correct. Amazon DynamoDB is a fast and flexible NoSQL database service for all applications that need consistent,

single-digit millisecond latency at any scale. It is a fully managed cloud database and supports both document and key-value store models. Its flexible data model, reliable performance, and automatic scaling of throughput capacity, makes it a great fit for mobile, web, gaming, ad tech, IoT, and many other applications.

---

**Q43) What is the main benefit of decoupling an application?**

- Optimize costs

**Explanation:-**This option is incorrect.

- Increase the integrity of the application's components

**Explanation:-**This option is incorrect.

- ✅ Reduce inter-dependencies so failures do not impact other components of the application.

**Explanation:-**This option is correct. As application complexity increases, a desirable attribute of an IT system is that it can be broken into smaller, loosely coupled components. This means that IT systems should be designed in a way that reduces interdependencies—a change or a failure in one component should not cascade to other components. On the other hand if the components of an application are tightly coupled and one component fails, the entire application will also fail. Therefore when designing your a

- Make updates quickly and easily.

**Explanation:-**This option is incorrect.

---

**Q44) Which of the following needs a username and password to access AWS resources?**

- AWS Software Development Kit (SDK)

**Explanation:-**This option is not correct. To make programmatic requests to AWS services using SDKs you must provide valid credentials (Access key ID and secret access key) when setting up your SDK and must also have the IAM permissions that allow you to interact with these services.
Note: SDKs are used to simplify using AWS services in your applications with an API tailored to your programming language or platform. AWS SDKs in AWS include Java SDK, .NET SDK, Node.js SDK and many others.

- AWS CLI

**Explanation:-**This option is not correct. Just like the AWS SDKs you must provide valid credentials (Access key ID and secret access key) when configuring your CLI NOT a user name or password. To interact with AWS services using CLI you must also have the required IAM permissions to use these services.

- AWS Application Programming Interface (API)

**Explanation:-**This option is not correct. To make an API call you need an IAM Permission NOT a user name or password.
Note: AWS Application Programming Interface (AWS API) is the sole way that external users interact with AWS resources, and there's literally no way to use AWS resources without the API being involved. In fact, if you access AWS through the AWS Management Console or the command line tools, you are actually using tools that make calls to the AWS API.

- ✅ AWS Management Console

**Explanation:-**This option is correct. The AWS Management console allows you to access and manage Amazon Web Services through a simple and intuitive web-based user interface. You can also use the AWS Console mobile app to quickly view resources on the go.

---

**Q45) Which AWS service uses Edge Locations to cache content?**

- ✅ AWS CloudFront

**Explanation:-**This option is correct. CloudFront is a content caching service provided by AWS that uses Edge Locations (which are AWS data centers located all around the world) to reduce network latency when delivering content to end users.

- AWS KMS

**Explanation:-**This option is not correct. AWS KMS is a key management service.

- AWS Glacier

**Explanation:-**This option is not correct. AWS Glacier is an Amazon S3 storage class.

- AWS Inspector

**Explanation:-**This option is not correct. AWS Inspector is a security assessment service.

---

**Q46) What service helps you to aggregate log files from your EC2 instances?**

- SQS
- S3
- CloudTrail
- ✅ CloudWatch Logs

---

**Q47) Which of the following is required to connect to Amazon EC2 instances?**

- ✅ Key pairs

**Explanation:-**This option is correct. During the creation process of the Amazon EC2 instances you can create and download your key pair. This key pair is required when you want to connect to your Amazon EC2 instances.
Note:
You can't connect to your instance unless you launched it with a security group that allows SSH access from your IP.

- MFA

**Explanation:-**This option is not correct. MFA is an additional security layer that can be used to secure your AWS console. MFA can also be used to control access to AWS service APIs.

- Route Tables

**Explanation:-**This option is not correct. A route table contains a set of rules, called routes, that are used to determine where network traffic is directed.

- Instance Password

**Explanation:-**This option is not correct. There are no passwords related to the EC2 instances.

---

**Q48)**

**A company needs to host a database for at least 1 year.**

**Which of the following options would be the most cost-effective solution?**

On-Demand
**Explanation:-**This option is not correct. On-Demand is not a cost effective solution.
No Upfront - Reserved
**Explanation:-**This option is not correct. The No Upfront option does not require any upfront payment and provides a discounted hourly rate for the duration of the term. With the Partial Upfront option provides more discounts than the No Upfront option because you spend more upfront.
Partial Upfront - Reserved
**Explanation:-**This option is correct. Since the database server will be hosted for a period of at least one year then it is better to use the RDS Reserved Instances as it provides you with a significant discount compared to the On-Demand Instance pricing for the DB instance.
With the Partial Upfront option, you make a low upfront payment and are then charged a discounted hourly rate for the instance for the duration of the Reserved Instance term. The Partial Upfront option is more cost effective than th
Spot Instances
**Explanation:-**This option is not correct. Spot is an option for paying for EC2 not RDS.

---

**Q49)**

**An organization has an on-premises application that serves users from all around the world.**

**If instead the application was deployed in AWS, what is the AWS characteristic that could help reduce latency to their users?**

Fault tolerance
**Explanation:-**This option is not correct. Fault tolerance has a different purpose. You should build your architecture to be fault tolerant to protect from infrastructure or system disruptions.
High Availability
**Explanation:-**This option is not correct. High Availability can be achieved by deploying your application in multiple availability zones within a single region. This may not reduce latency to your international users.
Elasticity
**Explanation:-**This option is not correct. AWS Elasticity allows you to reduce costs by scaling your resources down when demand decreases and maintain performance by scaling your resources up when demand increases.
Global reach
**Explanation:-**This option is correct. If you deliver applications to your global users from an on-premises datacenters, your users might face inconsistent availability and performance. AWS solved this problem by providing the ability to deploy your application in multiple regions around the world. The user will be redirected to the region that provides the lowest possible latency and the highest performance. You can also use the CloudFront service that uses edge locations (which are located in most of the maj

---

**Q50) For managed services like Amazon DynamoDB, what are the security-related tasks that AWS is responsible for? (Choose two)**

Create the required access policies
**Explanation:-**This Option is not correct. The customer is responsible for creating the required access policies for all users using the Identity and Access Management service.
Protect Credentials
**Explanation:-**This Option is not correct. All IAM users are responsible for protecting their credentials.
Logging DynamoDB operations
**Explanation:-**This Option is not correct. The AWS customer can use the CloudTrail service to record all DynamoDB events from all Regions.
Install antivirus software
**Explanation:-**AWS has increased responsibilities for its managed services. Examples of managed services include Amazon DynamoDB, Amazon RDS, Amazon Redshift, Amazon Elastic MapReduce, and Amazon WorkSpaces. These services provide the scalability and flexibility of cloud-based resources with less operational overhead because AWS handle basic security tasks like guest operating system (OS) and database patching, installing antivirus software, and disaster recovery.
Disaster recovery
**Explanation:-**AWS has increased responsibilities for its managed services. Examples of managed services include Amazon DynamoDB, Amazon RDS, Amazon Redshift, Amazon Elastic MapReduce, and Amazon WorkSpaces. These services provide the scalability and flexibility of cloud-based resources with less operational overhead because AWS handle basic security tasks like guest operating system (OS) and database patching, installing antivirus software, and disaster recovery.

---