**Technical Questions - Cloud Engineer**

**(Time limit: 30 mins)**

1. A media company runs its business on Amazon EC2 instances backed by Amazon S3 storage. The company is apprehensive about the consistent increase in costs incurred from S3 buckets. The company wants to make some decisions regarding data retention, storage, and deletion based on S3 usage and cost reports. You have been hired to develop a solution to track the costs incurred by each S3 bucket in the AWS account. How will you configure this requirement?
2. Configure AWS Budgets to see the cost against each S3 bucket in the AWS account
3. Use AWS Simple Monthly Calculator to check the cost against each S3 bucket in your AWS account
4. Use AWS Trusted Advisor's rich set of best practice checks to configure cost utilization for individual S3 buckets. Trusted Advisor also provides recommendations based on the findings derived from analyzing your AWS cloud architecture
5. **Add a common tag to each bucket. Activate the tag as a cost allocation tag. Use the AWS Cost Explorer to create a cost report for the tag**
6. A startup uses Amazon S3 buckets for storing their customer data. The company has defined different retention periods for different objects present in their Amazon S3 buckets, based on the compliance requirements. But, the retention rules do not seem to work as expected. Which of the following points are important to remember when configuring retention periods for objects in Amazon S3 buckets (Select two)?
7. **When you apply a retention period to an object version explicitly, you specify a Retain Until Date for the object version**
8. You cannot place a retention period on an object version through a bucket default setting
9. When you use bucket default settings, you specify a Retain Until Date for the object version
10. **Different versions of a single object can have different retention modes and periods**
11. The bucket default settings will override any explicit retention mode or period you request on an object version
12. After a developer had mistakenly shutdown a test instance, the Team Lead has decided to configure termination protection on all the instances. As a systems administrator, you have been tasked to review the termination policy and check its viability for the given requirements. Which of the following choices are correct about Amazon EC2 instance's termination policy (Select two)?
13. The DisableApiTermination attribute prevents you from terminating an instance by initiating shutdown from the instance
14. **The DisableApiTermination attribute does not prevent you from terminating an instance by initiating shutdown from Amazon EC2 console**
15. You can't enable termination protection for Spot Instances
16. **To prevent instances that are part of an Auto Scaling group from terminating on scale in, use instance protection**
17. The DisableApiTermination attribute prevents Amazon EC2 Auto Scaling from terminating an instance
18. A company is moving their on-premises technology infrastructure to AWS Cloud. Compliance rules and regulatory guidelines mandate the company to use its own software that needs socket level configurations. As the company is new to AWS Cloud, they have reached out to you for guidance on this requirement. As an AWS Certified SysOps Administrator, which option will you suggest for the given requirement?
19. Opt for On-Demand instances that are highly available and require no prior planning
20. Opt for Reserved Instances that allow you to plan and help install the necessary software
21. **Opt for Amazon EC2 Dedicated Host**
22. Opt for Amazon EC2 Dedicated Instance
23. Security and Compliance is a Shared Responsibility between AWS and the customer. As part of this Shared Responsibility, the customer is also responsible for securing the resources that he has procured under his AWS account. Which of the following is the responsibility of the customer?
24. For Amazon S3 service, managing the operating system and platform is customer responsibility
25. AWS is responsible for patching and fixing flaws within the infrastructure, for patching the guest Operating Systems and applications of the customers
26. AWS is responsible for training their customers and their employees as part of Customer Specific training
27. **For Amazon EC2 service, managing guest operating system (including updates and security patches), application software and Security Groups is the responsibility of the customer**
28. As a SysOps Administrator, you have been tasked to generate a report on all API calls made for Elastic Load Balancer from the AWS Management Console. Which feature/service will you use to fetch this data?
29. CloudWatch metrics
30. Load Balancer Access logs
31. **CloudTrail logs**
32. Load Balancer Request tracing
33. A Systems Administrator has just configured an internet facing Load Balancer for traffic distribution across the EC2 instances placed in different Availability Zones. The clients, however, are unable to connect to the Load Balancer. What is the most plausible reason for this issue?
34. It is an internal server error
35. **A security group or network ACL is not allowing traffic from the client**
36. The target returned the error code of 200 indicating an error on the server side
37. The target was incorrectly configured as a Lambda function and not an EC2 instance
38. A Systems Administrator is configuring an Application Load Balancer (ALB) that fronts Amazon EC2 instances. Which of the following options would you identify as correct for configuring the ALB? (Select two)
39. The targets of a target group in an ALB should all belong to the same Availability Zone
40. **Before you start using your Application Load Balancer, you must add one or more listeners**
41. A target can be registered with only one target group at any given time
42. When you create a listener, you define actions and conditions for the default rule
43. You configure target groups of an ALB by attaching them to the listeners
44. A company wants to migrate a part of its on-premises infrastructure to AWS Cloud. As a starting point, the company is looking at moving their daily workflow files to AWS Cloud, such that the files are accessible from the on-premises systems as well as AWS Cloud. To reduce the management overhead, the company wants a fully managed service. Which service / tool is the right choice for this requirement?
45. **File Gateway of AWS Storage Gateway**
46. Volume Gateway of AWS Storage Gateway
47. Amazon Simple Storage Service (Amazon S3)
48. Amazon Elastic Block Store (Amazon EBS)
49. A SysOps Administrator was asked to enable versioning on an Amazon S3 bucket after a few objects were accidentally deleted by the development team. Which of the following represent valid scenarios when a developer deletes an object in the versioning-enabled bucket? (Select two)
50. **A delete marker is set on the deleted object, but the actual object is not deleted**
51. GET requests can retrieve delete marker objects
52. A delete marker has a key, version ID and Access Control List (ACL) associated with it
53. GET requests do not retrieve delete marker objects
54. The delete marker has the same data associated with it, as the actual object
55. An analytics company generates reports for various client applications, some of which have critical data. As per the company's compliance guidelines, data has to be encrypted during data exchange, for all channels of communication. An Amazon S3 bucket is configured as a website endpoint and this is now being added as a custom origin for CloudFront. How will you secure this channel, as per the company's requirements?
56. **Configure CloudFront that mandates viewers to use HTTPS to request objects from S3. Configure S3 bucket to support HTTPS communication only. This will force CloudFront to use HTTPS for communication between CloudFront and S3**
57. Configure CloudFront to mandate viewers to use HTTPS to request objects from S3. However, CloudFront and S3 will use HTTP to communicate with each other
58. Communication between CloudFront and Amazon S3 is always on HTTP protocol since the network used for communication is internal to AWS and is inherently secure
59. CloudFront always forwards requests to S3 by using the protocol that viewers used to submit the requests. So, we only need to configure CloudFront to mandate the use of HTTPS for users
60. A junior developer is tasked with creating necessary configurations for AWS CloudFormation that is extensively used in a project. After declaring the necessary stack policy, the developer realized that the users still do not have access to stack resources. The stack policy created by the developer looks like so:

{

"Statement" : [

{

"Effect" : "Allow",

"Action" : "Update:\*",

"Principal": "\*",

"Resource" : "\*"

},

{

"Effect" : "Deny",

"Action" : "Update:\*",

"Principal": "\*",

"Resource" : "LogicalResourceId/ProductionDatabase"

}

]

}

Why are the users unable to access the stack resources even after giving access permissions to all?

1. A stack policy applies only during stack updates; it doesn't provide access controls. The developer needs to provide access through IAM policies
2. The stack policy is invalid and hence the users are not granted any permissions. The developer needs to fix the syntactical errors in the policy
3. Stack policies do not allow wildcard character value (\*) for the Principal element of the policy
4. **Stack policies are associated with a particular IAM role or an IAM user. Hence, they only work for the users you have explicitly attached the policy to**
5. A large IT company uses several AWS accounts for the different lines of business. Quite often, the systems administrator is faced with the problem of sharing Customer Master Keys (CMKs) across multiple AWS accounts for accessing AWS resources spread across these accounts. How will you implement a solution to address this issue?
6. **The key policy for the CMK must give the external account (or users and roles in the external account) permission to use the CMK. IAM policies in the external account must delegate the key policy permissions to its users and roles**
7. Use AWS KMS service-linked roles to share access across AWS accounts
8. AWS Owned CMK can be used across AWS accounts. Configure an AWS Owned CMK and use it across accounts that need to share the key material
9. Declare a key policy for the CMK to give the external account permission to use the CMK. This key policy should be embedded with the first request of every transaction
10. An e-commerce company is running its server infrastructure on Amazon EC2 instance store-backed instances. For better performance, the company has decided to move their applications to another Amazon EC2 instance store-backed instance with a different instance type. How will you configure a solution for this requirement?
11. You can't resize an instance store-backed instance. Instead, you choose a new compatible instance and move your application to the new instance
12. You can't resize an instance store-backed instance. Instead, configure an EBS volume to be the root device for the instance and migrate using the EBS volume
13. **Create an image of your instance, and then launch a new instance from this image with the instance type that you need. Take any Elastic IP address that you've associated with your original instance and associate it with the new instance for uninterrupted service to your application**
14. Create an image of your instance, and then launch a new instance from this image with the instance type that you need. Any public IP address associated with the instance can be moved with the instance for uninterrupted access of services
15. A developer is tasked with cleaning up obsolete resources. When he tried to delete an AWS CloudFormation stack, the stack deletion process returned without any error or a success message. The stack was not deleted either. What is the reason for this behavior and how will you fix it?
16. The AWS user who initiated the stack deletion does not have enough permissions
17. **Some resources must be empty before they can be deleted. Such resources will not be deleted if they are not empty and stack deletion fails without any error**
18. If you attempt to delete a stack with termination protection enabled, the deletion fails and the stack - including its status - remains unchanged
19. Dependent resources should be deleted first, before deleting the rest of the resources in the stack. If this order is not followed, then stack deletion fails without an error
20. An organization that started as a single AWS account, gradually moved to a multi-account setup. The organization also has multiple AWS environments in each account, that were being managed at the account level. Backups are a big part of this management task. The organization is looking at moving to a centralized backup management process that consolidates and automates Cross-Region backup tasks across AWS accounts. Which of the solutions below is the right choice for this requirement?
21. Configure AWS Systems Manager Maintenance Windows to schedule backup tasks as per company's policies. Tag the resources to help identify them by the AWS environment they run in. Amazon CloudWatch dashboards hosted by Systems Manager to get an overall view of the status of all resources under the AWS account
22. Use Amazon EventBridge to create a workflow for scheduled backup of all AWS resources under an account. Amazon S3 lifecycle policies, Amazon EC2 instance backups, and Amazon RDS backups can be used to create the events for the EventBridge. The same workflow can be scheduled to work on production and non-production environments, based on the tags created
23. **Create a backup plan in AWS Backup. Assign tags to resources based on the environment ( Production, Development, Testing). Create one backup policy for production environments and one backup policy for non-production environments. Schedule the backup plan based on the organization's backup policies**
24. Use Amazon Data Lifecycle Manager to manage creation, deletion, and managing of all the AWS resources under an account. Tag all the resources that need to be backed up and use lifecycle policies to customize the backup management to cater to the needs of the organization
25. The development team at an IT company is looking at moving its web applications to Amazon EC2 instances. The team is weighing its options for EBS volumes and instance store-backed instances for these applications with varied workloads. Which of the following would you identify as correct regarding instance store and EBS volumes? (Select three)

Use separate Amazon EBS volumes for the operating system and your data, even though root volume persistence feature is available

1. **Data stored in the instance store is preserved when you stop or terminate your instance. However, data is lost when you hibernate the instance. Configure EBS volumes or have a backup plan to avoid using critical data to this behavior**
2. **EBS snapshots only capture data that has been written to your Amazon EBS volume, which might exclude any data that has been locally cached by your application or operating system**
3. **By default, data on a non-root EBS volume is preserved even if the instance is shutdown or terminated**
4. EBS encryption does not support boot volumes
5. Snapshots of EBS volumes, stored on Amazon S3, can be accessed using Amazon S3 APIs
6. A retail company has complex AWS VPC architecture that is getting difficult to maintain. The company has decided to configure VPC flow logs to track the network traffic to analyze various traffic flow scenarios. The systems administration team has configured VPC flow logs for one of the VPCs, but it's not able to see any logs. After initial analysis, the team has been able to track the error. It says Access error and the administrator of the team wants to change the IAM Role defined in the flow log definition. What is the correct way of configuration a solution for this issue so that the VPC flow logs can be operational?
7. **The error indicates that the IAM role does not have a trust relationship with the flow logs service. Change the trust relationship from flow log configuration**
8. The flow log is still in the process of being created. It sometimes takes almost 10 minutes to start the logs
9. The error indicates IAM role is not correctly configured. After you've created a flow log, you cannot change its configuration. Instead, you need to delete the flow log and create a new one with the required configuration
10. The error indicates an internal error has occurred in the flow logs service. Raise a service request with AWS
11. A data analytics company runs its technology operations on AWS Cloud using different VPC configurations for each of its applications. A systems administrator wants to configure the Network Access Control List (ACL) and Security Group (SG) of VPC1 to allow access for AWS resources in VPC2. Which is the best way of configuring this requirement?
12. Network ACLs and Security Groups share a parent-child relationship. If resources in VPC2 are given inbound and outbound permissions on Network ACLs of VPC1, the resources will get necessary permissions on the associated security groups too
13. By default, Security Groups allow outbound traffic. Hence, only the inbound traffic configuration of the security groups have to be changed to allow requests from resources in VPC2 to access instances in VPC1. If the subnet is not associated with any Network ACL, you will not need any configuration changes
14. Based on the inbound and outbound traffic configurations on Network ACL of VPC1, you can create a similar deny rules on Security Groups of the instances in VPC1 to deny all traffic, other than the one originating from resources in VPC2
15. **The Security Groups of instances on VPC1 should be configured to allow inbound traffic from resources in VPC2. By default, Network ACLs allow all inbound and outbound traffic. So, a default Network ACLs on VPC1 will not need any configuration changes**
16. A banking service uses Amazon EC2 instances and Amazon RDS databases to run its core business functionalities. The Chief Technology Officer (CTO) of the company has requested granular OS level metrics from the database service for benchmarking. As a SysOps Administrator, how will you provide this information?
17. Enable Enhanced Monitoring for your RDS DB instance
18. Subscribe to Amazon RDS events to be notified when changes occur with a DB instance and its connected resources
19. Subscribe to CloudWatch metrics that track CPU utilization of the instances the RDS is hosted on
20. **Enable Performance Insights to expand on the existing Amazon RDS monitoring features to illustrate your database's performance**