K21Academy
Learn Cloud from Experts

amazon web services

AWS Certified Solutions Architect Associate [SAA-C03]

25 SAMPLE EXAM QUESTIONS

[EDITION 01]

Contents

1 DESIGN RESILIENT ARCHITECTURES

Q1. Your company is planning on the following architecture for their application.

- A set of EC2 Instances hosting the web part of the application.
- A relational database for the backend.
- A Load balancer for distribution of traffic.
- A NAT gateway for routing traffic from the database server to the Internet.

Which of the following architecture ensures high availability across all components?

A. A Load balancer with one public subnet, one private subnet. The EC2 Instances placed in one Availability Zone. RDS with Multi-AZ Enabled. NAT Gateway in one availability zone.
B. A Load balancer with 2 public subnets, 2 private subnets. The EC2 Instances placed across 2 Availability Zones. RDS with Multi-AZ Enabled. NAT Gateways in each availability zone.
C. A Load balancer with 2 public subnets, 2 private subnets. The EC2 Instances placed in 2 Availability Zones. RDS with MultiAZ Enabled. NAT Gateway in one availability zone.
D. A Load balancer with 2 public subnets, 2 private subnets. The EC2 Instances placed in one Availability Zone. RDS with MultiAZ Enabled. NAT Gateway in one availability zone.

Answer: B

In a Multi-AZ deployment, Amazon RDS automatically provisions and maintains a synchronous standby replica in a different Availability Zone. The primary DB instance is synchronously replicated across Availability Zones to a standby replica to provide data redundancy, eliminate I/O freezes, and minimize latency spikes during system backups. Running a DB instance with high availability can enhance availability during planned system maintenance and help protect your databases against DB instance failure and Availability Zone disruption.

Let's try to understand the scenario using a few use cases:

Depending upon your risk appetite, you might configure things differently.

Use Case 1: A load balancer, one public subnet, one private subnet in same AZ, one NAT Gateway, and RDS with Multi-AZ

- The NAT Gateway goes into the public subnet.
- The EC2 Instances go into the private subnet.
- The Route Table for the private subnet points to the NAT Gateway in the public subnet.

Use Case 2: A load balancer, two public subnets, two private subnets, one NAT Gateway, RDS with Multi-AZ

- The NAT Gateway goes into one public subnet (Public-Subnet-A)
- The EC2 instances are launched in private subnets across two AZs (Private-Subnet-A, Private-Subnet-B) or the same AZ (Private-Subnet-A/Private-Subnet-B)

- The Route Table for both of the private subnets point to the NAT Gateway.

However, if there is a failure with Availability Zone A (rare, but can happen), then the NAT Gateway is not reachable from Private-Subnet-B. Thus, the system may be impacted even though it runs across two AZs or a single AZ.

Use Case 3: A load balancer, two public subnets, two private subnets, two NAT Gateways, RDS with Multi-AZ

- The NAT Gateway goes into both public subnets (Public-Subnet-A, Public-Subnet-B)
- The EC2 instances are launched in private subnets across two AZs (Private-Subnet-A, Private-Subnet-B)
- The Route Table Private-Subnet-A points to the NAT Gateway in Public-Subnet-A
- The Route Table Private-Subnet-B points to the NAT Gateway in Public-Subnet-B

If one of the AZs should fail, then the EC2 instances in the remaining private subnet will still be able to communicate with the Internet because they have their own NAT Gateway in the same AZ.

Option A) is incorrect because, according to Use Case 1, High Availability is not ensured.
When you enable an Availability Zone for your load balancer, Elastic Load Balancing creates a load balancer node in the Availability Zone. If you register targets in an Availability Zone but do not enable the Availability Zone, these registered targets do not receive traffic. Note that your load balancer is most effective if you ensure that each enabled Availability Zone has at least one registered target.
We recommend that you enable multiple Availability Zones. (Note that with an Application Load Balancer, we require you to enable multiple Availability Zones.) With this configuration, if one Availability Zone becomes unavailable or has no healthy targets, the load balancer can continue to route traffic to the healthy targets in another Availability Zone.

Option B) is Correct because according to Use Case 3, High Availability is ensured.

Option C) and D) are incorrect because according to Use Case 2, High Availability is not ensured as either if we have EC2 in single AZ or multiple AZ. We have NAT Gateway in single AZ is a cause for not ensuring High Availability.

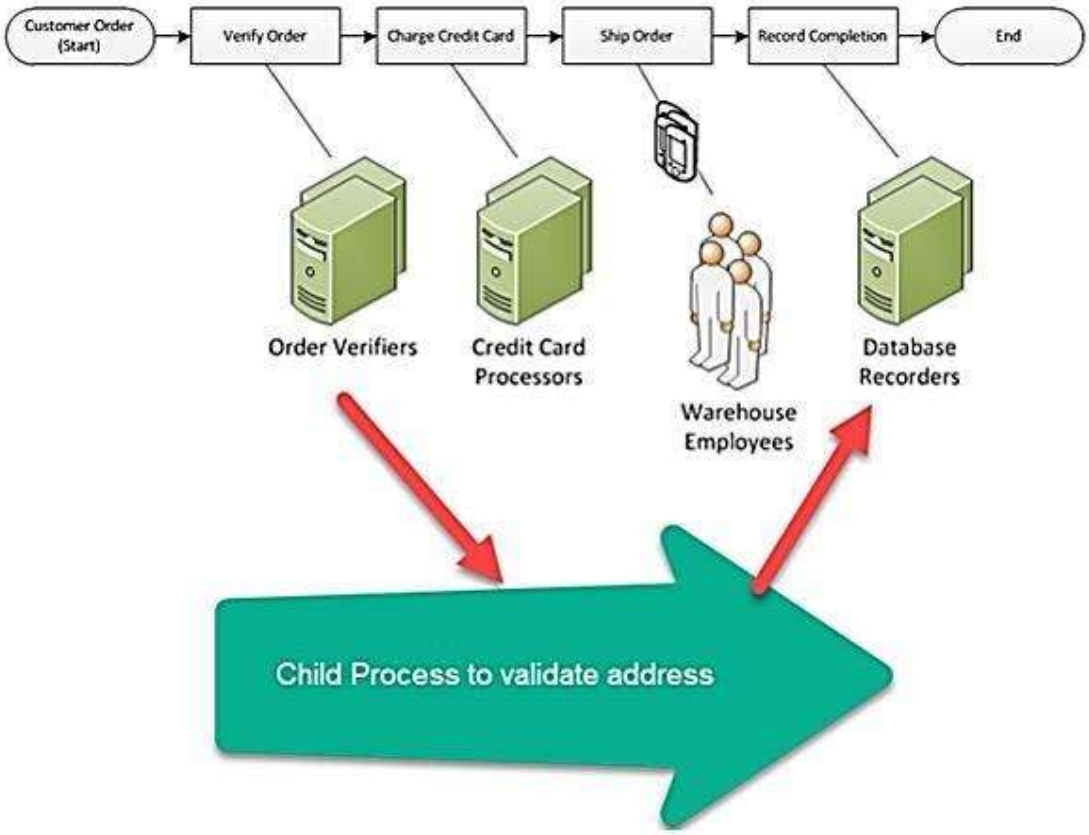
For more information on Elastic Load Balancing, Multi-AZ and NAT gateway, please refer to the below URL's:

https://k21academy.com/awssa20
https://docs.aws.amazon.com/elasticloadbalancing/latest/userguide/how-elastic-load-balancing-works.html
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.MultiAZ.html

Q2. A Solutions architect has been asked to design an order processing e-commerce application on AWS where synchronous transaction processing is not required. Some of the order processing tasks might take a long time and require integrations with external applications. How can this be achieved?

- **A.** Use AWS Simple Workflow Service to design activities coordination between different components of the application.
- **B.** Use Step functions to design activities coordination between different components of the application.
- **C.** Use API Gateway and Lambda to design the application.
- **D.** Use SQS to coordinate the activities of the application.

Answer: A



Different between Steps function and SWF

Step Functions	SWF
Good for any new serverless application where coordination is required between various components using visual workflow	Need external signals to intervene in processes, OR Good if there are child processes and those require passing signals to parents.
Easy to use while developing application	More complex while developing application but complete control of orchestration logic
Uses declarative JAON to write state machine	Need to write decider program (programing of your choice) to separate activities between steps or use AWS flow framework
Serverless, lower admin overhead	Uses servers
Short running workflows	Long-running workflows,
Mostly used for synchronous tasks	Mostly used for asynchronous tasks
New AWS Service, less complex applications	Legacy application, Complex decisions (custom decide application)
	Integrate with AWS Mechanical Turk

The main point is to design an application where some tasks can take longer than expected. For example, address validation. Also, this application should support integration with other AWS services.

- Option A is CORRECT since this SWF is the right fit for long-running tasks. SWF can manage activities in an async way and support integration with other AWS services. See

the difference table for more details. SWF helps manage tasks sequentially or in a parallel way, and this is a must require for an order processing application.

- Option B is incorrect because the Step function is not good for long-running activities. See the difference table for more details.
- Option C is incorrect because managing workflow with Lambda and API gateway would not be the right solution.
- Option D is incorrect because SQS is queue management. SQL enables decoupling applications.

References:

https://k21academy.com/awssa37
https://k21academy.com/awsdev16

Q3. A company is planning to host an application with the below architecture.

- A lambda function that reads the metadata of objects from an S3 bucket.
- The Lambda function then stores the metadata in DynamoDB and AWS RDS - MySQL.

Which of the following needs to be in place to ensure the above architecture is high available?

A. Enable Cross Region Replication for the S3 bucket.
B. Enable Lambda functions in Multiple Availability Zones.
C. Enable Multi-AZ for the MySQL database.
D. Enable Auto-Scaling for the DynamoDB table

Answer – C

Option C is correct because, in a Multi-AZ deployment, Amazon RDS automatically provisions and maintains a synchronous standby replica in a different Availability Zone. The primary DB instance is synchronously replicated across Availability Zones to a standby replica to provide data redundancy, eliminate I/O freezes, and minimize latency spikes during system backups. Running a DB instance with high availability can enhance availability during planned system maintenance and help protect your databases against DB instance failure and Availability Zone disruption.

Option A is invalid because the S3 service is already a highly available service within a particular region. Also, Amazon S3 gives any developer access to the same highly scalable, highly available, fast, inexpensive data storage infrastructure that Amazon uses to run its own global network of web sites. The S3 Standard storage class is designed for 99.99% availability, the S3 Standard-IA storage class is designed for 99.9% availability, the S3 One Zone-IA storage class is designed for 99.5% availability, and the S3 Glacier and S3 Glacier Deep Archive class are designed for 99.99% availability and SLA of 99.9%. All of these storage classes are backed by the Amazon S3 Service Level Agreement.

Options B is invalid because AWS Lambda is already a highly available service in AWS.

Option D is invalid because High Availability is about availability; AS is about performance (usually throughput), also DynamoDB is high available by default. High Availability focuses on maintaining the liveness of the system in the presence of server or network failures. At the same time, Auto Scaling means adding more resources when demand increases. Refer to the below document for DynamoDB reliability.

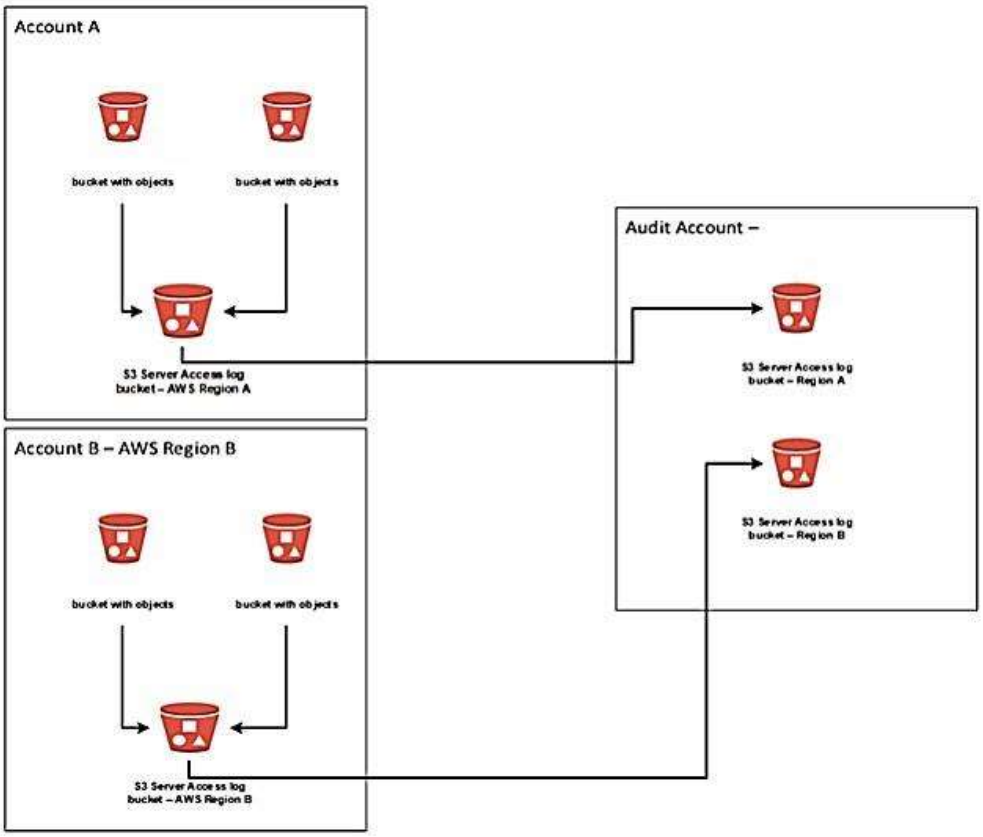
References:

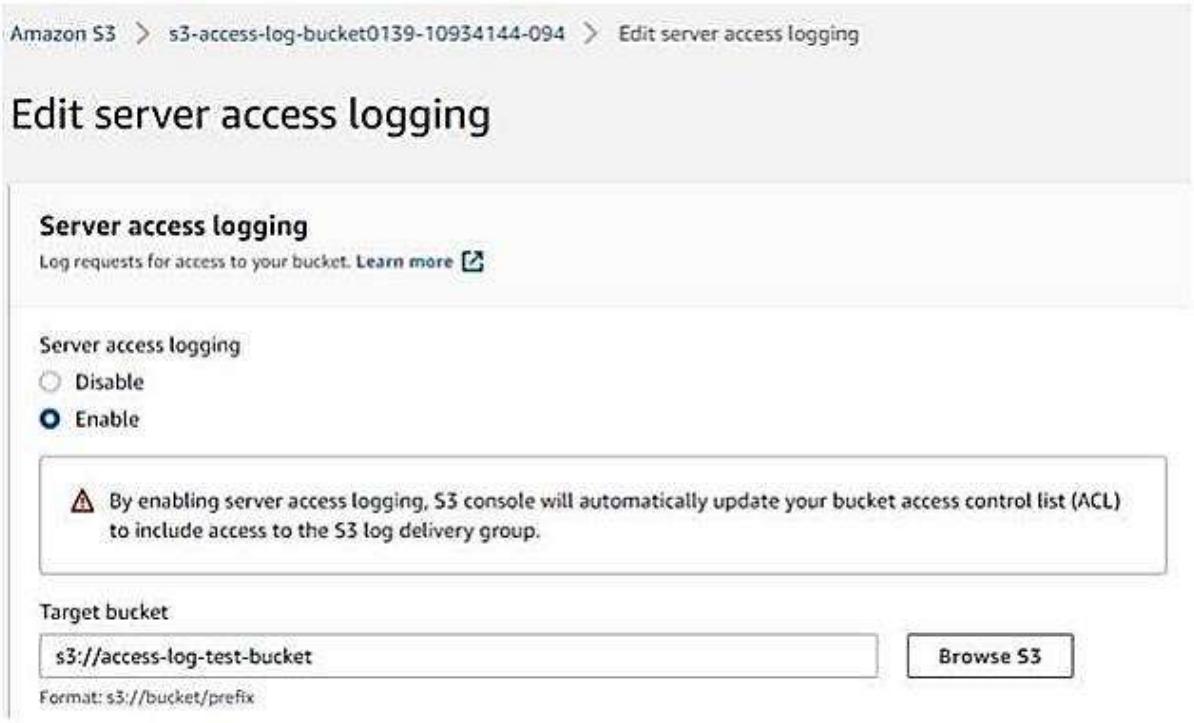
https://k21academy.com/awsdev16
https://k21academy.com/awssa32
https://aws.amazon.com/lambda/features/

Q4. A company has many Amazon S3 buckets across many different AWS accounts. A company has a new compliance and audit requirement where all the S3 buckets server access log should be collected and centralized into an Audit AWS account. How would you design this solution?

- **A.** Collect all S3 buckets server access logs in separate S3 buckets per account. Enable replication in the S3 server access log buckets to copy the logs to a centralized destination S3 bucket in the Audit account.
- **B.** Directly enable the server access logs for the S3 buckets in all the AWS accounts to a centralized destination S3 bucket in the Audit account.
- **C.** Collect all S3 buckets server access logs in one S3 bucket per account. Enable replication in the S3 server access log buckets to copy the logs to a centralized destination S3 bucket in the Audit account.
- **D.** Collect all S3 buckets server access logs in one S3 bucket per account. In the Audit AWS account, create a Lambda function to get the new logs from these S3 buckets and save the files in a centralized S3 bucket.

Answer: C





- Option A is incorrect because in each AWS account, you only need an S3 bucket to save the server access logs.
- Option B is incorrect because for the server access logs, you can only configure the target S3 bucket in the same AWS account.
- Option C is CORRECT because it meets all the requirements for the solution. All the S3 server access logs from each AWS account have been replicated to the audit account.
- Option D is incorrect because the Lambda function is not required. You can directly enable replication to copy the logs to the S3 bucket in the Audit account.

References

http://k21academy.com/awssa16
https://k21academy.com/awssa22

Q5. Your company has just started using the AWS RDS service. They have an application making requests to a MySQL instance on this service. Due to the sudden surge of high requests, you need to ensure that the backup activities on the database do not interfere with the database's normal operation. Which of the following would help in this requirement?

A. Ensure that the underlying instance type RDS instance is using General Purpose SSD storage. This type of storage will have minimal impact on such operations.
B. Ensure that the underlying instance type RDS instance is using Enhanced Networking. This type of setting will have minimal impact on such operations.
C. Ensure that the Multi-AZ feature has been enabled for the underlying RDS Instance.
D. Ensure that cross-region replication is enabled for the underlying RDS Instance.

Answer: C

Option C is correct because, in a Multi-AZ deployment, Amazon RDS automatically provisions and maintains a synchronous standby replica in a different Availability Zone. The primary DB instance is synchronously replicated across Availability Zones to a standby replica to provide data redundancy, eliminate I/O freezes, and minimize latency spikes during system backups. Running a DB instance with high availability can enhance availability during planned system maintenance and help protect your databases against DB instance failure and Availability Zone disruption.

We know that during the backups, for instance, taking snapshots, there is usually an I/O consumption that takes place. To avoid this when using a multi-AZ enabled RDS database engine, create a backup on the standby instance. With automated backups, I/O activity is no longer suspended on your primary during your preferred backup window since backups are taken from the standby.

Options A and B are incorrect because, using General Purpose SSD Storage or using Enhanced networking, our backup activities will interfere with normal database operation.

Option D is incorrect, Cross-region replication is not required as it is Asynchronous replication.

References

https://k21academy.com/awssa32
https://k21academy.com/awsdev14

Q6. Your company is planning on the following architecture for their application.

- A set of EC2 Instances hosting the web part of the application.
- A relational database for the backend
- A Load balancer for distribution of traffic

There is critical nature of the data stored on the underlying EBS volumes attached to the EC2 Instances. As a Solutions Architect of the Company, your supervisor has asked you to follow best backup practices to ensure data is available in another region for disaster recovery purposes. Which of the following would you consider complying with this requirement?

A. Create a copy of the volume in another region.
B. Create a snapshot of the volume in another region.
C. Create a snapshot. Copy the snapshot to the new region.
D. Create a copy of the volume. Copy the volume to the new region.

Answer – C

The AWS Documentation showcases the use cases of EBS snapshots.

Use Cases

- Geographic expansion: Launch your applications in a new region.
- Migration: Move an application to a new region, to enable better availability and to minimize cost.
- Disaster recovery: Back up your data and logs across different geographical locations at regular intervals. In case of disaster, you can restore your applications using point-in-time backups stored in the secondary region. This minimizes data loss and recovery time.
- Encryption: Encrypt a previously unencrypted snapshot, change the key with which the snapshot is encrypted, or, for encrypted snapshots that have been shared with you, create a copy that you own to restore a volume from it.
- Data retention and auditing requirements: Copy your encrypted EBS snapshots from one AWS account to another to preserve data logs or other files for auditing or data retention. Using a different account helps prevent accidental snapshot deletions and protects you if your main AWS account is compromised.

Options A and D are incorrect since you need to create a snapshot.

Option B is incorrect since you cannot directly create a snapshot in another region.

References

https://k21academy.com/awsdevops12
https://k21academy.com/awssa31

Q7. An application consists of a fleet of EC2 Instances. These Instances are launched in the Oregon (us-west-2) region which consists of 3 availability zones. This application needs 6 Instances running at all times. As an architect, you need to distribute the instances so that the application could still maintain its capacity if any availability zone goes down. Also, you need to ensure that the cost is kept to a minimum. Which of the following configurations would you consider?

- **A.** 6 Instances running in us-west-2a, 6 Instances running in us-west-2b, 6 Instances running in us-west-2c.
- **B.** 3 Instances running in us-west-2a, 3 Instances running in us-west-2c
- **C.** 6 Instances running in us-west-2a, 3 Instances running in us-west-2b, 3 Instances running in us-west-2c.
- **D.** 3 Instances running in us-west-2a, 3 Instances running in us-west-2b, 3 Instances running in us-west-2c.

Answer – D

So now, let's look at Option A.

If any availability zone goes down, we will have a total of 12 instances running. This is an additional 6 over the requirement of the question and will result in a higher cost.

So now, let's look at Option B.
If the availability zone us-west-2a goes down, then you will have only 3 instances running. Because the other 3 instances are running in the useast-2c region.

So now, let's look at Option C.
If either of us-west-2b or us-west-2c availability zone goes down, we will have a total of 9 instances running. This is an additional 3 over the requirement of the question and will result in a higher cost.

So now, let's look at Option D.
If either of us-east-2a or us-west-2b or us-west-2c availability zone goes down, there will be a total of 6 instances running, which is what we need.

References

https://k21academy.com/awssa31
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/

Q 8. A startup has recently moved its monolithic web application to AWS Cloud. The application runs on a single EC2 instance. Currently, the user base is small and the startup does not want to spend effort on elaborate disaster recovery strategies or Auto Scaling Group. The application can afford a maximum downtime of 10 minutes.

In case of a failure, which of these options would you suggest as a cost-effective and automatic recovery procedure for the instance?

A. Configure Amazon CloudWatch events that can trigger the recovery of the EC2 instance, in case the instance or the application fails
B. Configure an Amazon CloudWatch alarm that triggers the recovery of the EC2 instance, in case the instance fails. The instance, however, should only be configured with an EBS volume
C. Configure AWS Trusted Advisor to monitor the health check of EC2 instance and provide a remedial action in case an unhealthy flag is detected
D. Configure an Amazon CloudWatch alarm that triggers the recovery of the EC2 instance, in case the instance fails. The instance can be configured with EBS volume or with instance store volumes

Correct option: B

Explanation:

Configure an Amazon CloudWatch alarm that triggers the recovery of the EC2 instance, in case the instance fails. The instance, however, should only be configured with an EBS volume – If your instance fails a system status check, you can use CloudWatch alarm actions to automatically recover it. The recover option is available for over 90% of deployed customer EC2 instances. The CloudWatch recovery option works only for system check failures, not for instance status check failures. Also, if you terminate your instance, then it can't be recovered.

You can create an Amazon CloudWatch alarm that monitors an Amazon EC2 instance and automatically recovers the instance if it becomes impaired due to an underlying hardware failure or a problem that requires AWS involvement to repair. Terminated instances cannot be recovered. A recovered instance is identical to the original instance, including the instance ID, private IP addresses, Elastic IP addresses, and all instance metadata. If the impaired instance is in a placement group, the recovered instance runs in the placement group.

The automatic recovery process attempts to recover your instance for up to three separate failures per day. Your instance may subsequently be retired if automatic recovery fails and a hardware degradation is determined to be the root cause for the original system status check failure.

Incorrect options:

Configure Amazon CloudWatch events that can trigger the recovery of the EC2 instance, in case the instance or the application fails – You cannot use CloudWatch events to directly trigger the recovery of the EC2 instance.

Configure an Amazon CloudWatch alarm that triggers the recovery of the EC2 instance, in case the instance fails. The instance can be configured with EBS volume or with instance store volumes – The recover action is supported only on instances that have EBS volumes configured on them, instance store volumes are not supported for automatic recovery by CloudWatch alarms.

Configure AWS Trusted Advisor to monitor the health check of EC2 instance and provide a remedial action in case an unhealthy flag is detected – You can use Amazon CloudWatch Events to detect and react to changes in the status of Trusted Advisor checks. This support is only available with AWS Business Support and AWS Enterprise Support. Trusted Advisor by itself does not support health checks of EC2 instances or their recovery.

Reference:

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-recover.html

2 DESIGN SECURE ARCHITECTURES

Q1. Your company has an AWS account and a lot of resources defined in the Frankfurt region. They want to use an API monitoring service to track the changes to the resources in their account. Which of the following should be used for this purpose?

A. AWS Config
B. AWS CloudTrail
C. AWS CloudWatch
D. AWS Opswork

Answer: B

Option A is incorrect because AWS Config is a fully managed service that provides you with a resource inventory, configuration history, and configuration change notifications to enable security and governance. You can also discover existing AWS resources, export a complete inventory of your AWS resources with all configuration details, and determine how a resource was configured at any point in time.

Option B is correct because this is an API monitoring service and using 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. Besides, you can use CloudTrail to detect unusual activity in your AWS accounts.

Also, CloudTrail records the changes made to AWS Config, including who made the change, vice versa may not true.

Option C is invalid because this is a metric and logging service.

Option D is invalid because it is used to deploy stacks of resources.

CloudWatch and Config serve distinct use cases for monitoring and complements each other from the AWS ecosystem.

Config is typically used for auditing and compliance purposes across organizations to verify whether AWS resource changes being made are per compliance rules.

CloudWatch is designed to provide performance information about AWS resources such as EC2, Lambda, etc. Developers can use information from CloudWatch to identify bottlenecks in applications or workflows.

CloudWatch will help you send alerts when CPU /Memory utilization reaches a certain threshold and browse metrics associated with CPU/Network to identify operational and security issues.

References

https://k21academy.com/awssa35
https://aws.amazon.com/cloudtrail/

Q2. A company has a set of EC2 Instances hosted in a VPC. The IT Security department has specified that they need to ensure they get a list of IP addresses for all sources making requests to the EC2 Instances. Which one of the following could help achieve this requirement?

A. AWS VPC Flow Logs
B. AWS Cloudwatch
C. AWS CloudFormation
D. AWS Trusted Advisor

Answer – A

The AWS Documentation mentions the following.

VPC Flow Logs is a feature that enables you to capture information about the IP traffic going to and from network interfaces in your VPC. Flow log data can be published to Amazon CloudWatch Logs and Amazon S3. After you've created a flow log, you can retrieve and view its data in the chosen destination.

Option B is invalid since this is a monitoring service that can only give metrics and not the detailed IP address tracing for traffic flowing into EC2 Instances.

Option C is invalid since 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.

Option D is invalid since this is only used as a recommendation service.

References

https://k21academy.com/awssa35
https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs.html
https://k21academy.com/awsdevops13

Q3. Your company is planning on the following architecture for their application.

- A set of EC2 Instances hosting the web part of the application.
- A relational database for the backend using the AWS RDS MySQL service
- A Load balancer for distribution of traffic

There is a requirement to ensure that all data hosted in the database service is encrypted at rest. How can you achieve this requirement in the easiest manner? (Select 2)

A. Encrypt the underlying EBS volumes for the database.
B. Use the Encryption feature for RDS.
C. Use S3 server-side encryption.
D. Use AWS Key Management Service

Answer – B and D

The AWS Documentation mentions the following.

Option B is correct because, With RDS-encrypted resources, data is encrypted at rest, including the underlying storage for a database (DB) instance, its automated backups, read replicas, and snapshots. This capability uses the open standard AES-256 encryption algorithm to encrypt your data, transparent to your database engine.

This encryption option protects against physical exfiltration or access to your data bypassing the DB instances. Therefore, it is critical to complement encrypted resources with an effective encryption key management and database credential management practice to mitigate any unauthorized access. Otherwise, compromised credentials or insufficiently protected keys might allow unauthorized users to access the plaintext data directly through the database engine.

Encryption key management is provided using the AWS KMS.

Option D is correct because Amazon RDS encrypts your databases using keys you manage with the AWS Key Management Service (KMS). On a database instance running with Amazon RDS encryption, data stored at rest in the underlying storage is encrypted, as are its automated backups, read replicas, and snapshots. RDS encryption uses the industry-standard AES-256 encryption algorithm to encrypt your data on the server that hosts your RDS instance.

Options C is incorrect because this is used for the encryption of objects in S3.

Option A is incorrect since this can be easily achieved using the encryption at rest feature for AWS RDS.

The term 'rest' means when data is resting (not in transition-while data is traveling to the database.

References

https://k21academy.com/awssa27
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.Encryption.html

Q4. Your company has an application that has been developed and needs to be hosted on an EC2 Instance. The EC2 Instance is located in a private subnet and needs to access AWS Kinesis streams without passing into the Internet. How can you achieve this in the best manner possible?

A. Attach a NAT gateway to the VPC.
B. Attach an Internet gateway to the VPC.
C. Create a VPC Gateway Endpoint that would allow access to Kinesis Streams.
D. Create a VPC Interface Endpoint that would allow access to Kinesis Streams.

Answer – D

The AWS Documentation mentions the following. You can use an interface VPC endpoint to keep traffic between your Amazon VPC and Kinesis Data Streams from leaving the Amazon network. Interface VPC endpoints don't require an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. Interface VPC endpoints are powered by AWS PrivateLink, an AWS technology that enables private communication between AWS services using an elastic network interface with private IPs in your Amazon VPC.

Options A and B are incorrect since it is mentioned in the question that traffic should not go via the Internet.

Option C is incorrect since this is mostly used for S3 and DynamoDB access from Instances in the private subnet.

References

https://k21academy.com/awssa28
https://docs.aws.amazon.com/streams/latest/dev/vpc.html

Q5. A company is planning to store sensitive documents in an S3 bucket. They want to ensure that documents are encrypted at rest. They want to ensure they manage the underlying keys used for encryption but not the encryption/decryption process. Which of the following can be used for this purpose?

A. Use S3 server-side encryption with Customer keys.
B. Use S3 client-side encryption.
C. Use S3 server-side encryption with AWS managed keys.
D. Use S3 server-side encryption with AWS KMS keys with Key policy document of size 40kb.
E. Use S3 server-side encryption with an AWS CloudHSM key uploaded by the company.

Answer – A

AWS Documentation mentions the following.

Server-side encryption is about protecting data at rest. Using server-side encryption with customer-provided encryption keys (SSE-C) allows you to set your own encryption keys. With the encryption key you provide as part of your request, Amazon S3 manages both the encryption, as it writes to disks, and decryption, when you access your objects. Therefore, you don't need to maintain any code to perform data encryption and decryption. The only thing you do is manage the encryption keys you provide.

In short,

- SSE-S3 requires that Amazon S3 manage the data and master encryption keys.
- SSE-C requires that you manage the encryption key.
- SSE-KMS requires that AWS manage the data key, but you manage the master key in AWS KMS.

Option B is incorrect because when you do client-side encryption, data goes to s3 in an encrypted format. Again when you download, it is the client who has to decrypt the data. But question specifies customer should not manage the encryption/decryption process.

Option C is incorrect since you will still not manage the complete lifecycle of the keys.

Option D is incorrect because the maximum key policy document size is 32kb.

Option E is incorrect because CloudHSM is not cost-efficient and cannot be used in S3 server-side encryption.

References

https://k21academy.com/awssa27
https://k21academy.com/awssa22
https://docs.aws.amazon.com/kms/latest/developerguide/services-s3.html

Q6. Your team is planning to develop and deploy an application onto AWS with the following architecture.

- A set of EC2 Instances in a VPC hosting the web tier
- A database hosted using the AWS RDS MySQL instance

Which of the following should ideally be set so that only HTTPS users can access the web application and for the web application to access the database? (Choose 2)

A. An Inbound Security group rule for the web EC2 Instances allowing traffic from the source of 0.0.0.0/0 and port 443.
B. An Inbound Security group rule for the database layer allowing traffic from the source of 0.0.0.0/0 and port 443.
C. An Inbound Security group rule for the web EC2 Instances allowing traffic from the source of the database on port 3306.
D. An Inbound Security group rule for the database layer allowing traffic from the source of the web layer on port 3306.

Answer – A and D

Option A is correct because port 443 will allow only HTTPS traffic from all sources.

Option D is correct because the Database server Security Group must allow traffic from the source Web server on port 3306.

WebServerSG: Recommended Rules

Inbound			
Source	**Protocol**	**Port Range**	**Comments**
0.0.0.0/0	TCP	80	Allow inbound HTTP access to the web servers from any IPv4 address.
0.0.0.0/0	TCP	443	Allow inbound HTTPS access to the web servers from any IPv4 address.

DBServerSG: Recommended Rules

Inbound			
Source	**Protocol**	**Port Range**	**Comments**
The ID of your WebServerSG security group	TCP	1433	Allow inbound Microsoft SQL Server access from the web servers associated with the WebServerSG security group.
The ID of your WebServerSG security group	TCP	3306	Allow inbound MySQL Server access from the web servers associated with the WebServerSG security group.

Option B is invalid since the database should not be exposed to the Internet.

Option C is invalid since the database security group should allow incoming traffic on port 3306.

References

https://k21academy.com/awssa22
https://k21academy.com/awssa31

Q7. A financial services company wants a single log processing model for all the log files (consisting of system logs, application logs, database logs, etc) that can be processed in a serverless fashion and then durably stored for downstream analytics. The company wants to use an AWS-managed service that automatically scales to match the throughput of the log data and requires no ongoing administration. As a solutions architect, which of the following AWS services would you recommend for solving this problem?

A. Kinesis Data Firehose
B. Amazon EMR
C. AWS Lambda
D. Kinesis Data Streams

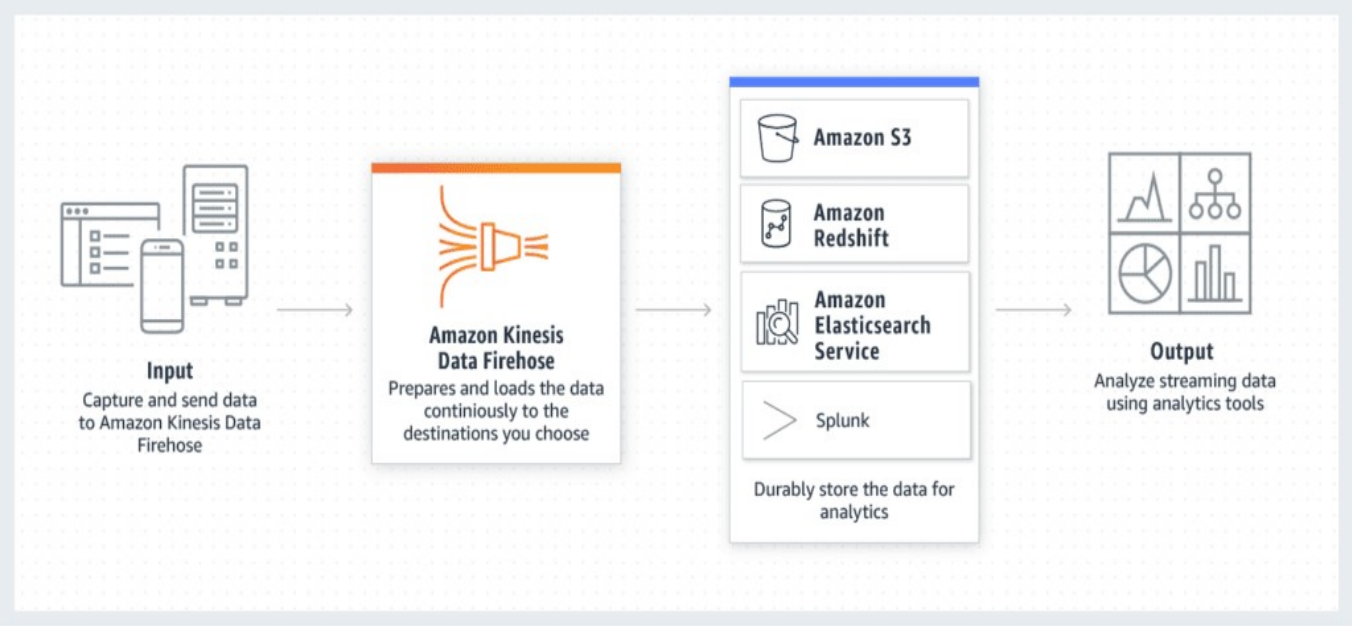
Correct Answer: A

Explanation:

Kinesis Data Firehose

Amazon Kinesis Data Firehose is the easiest way to reliably load streaming data into data lakes, data stores, and analytics tools. It can capture, transform, and load streaming data into Amazon S3, Amazon Redshift, Amazon Elasticsearch Service, and Splunk, enabling near real-time analytics with existing business intelligence tools and dashboards you're already using today. It is a fully managed service that automatically scales to match the throughput of your data and requires no ongoing administration. Therefore, this is the correct option.

Please see this overview of how Kinesis Firehose works:



via – https://aws.amazon.com/kinesis/data-firehose/
Incorrect options:

Kinesis Data Streams – Amazon Kinesis Data Streams (KDS) is a massively scalable and durable real-time data streaming service. The throughput of an Amazon Kinesis data stream is designed to scale without limits via increasing the number of shards within a data stream. With Amazon Kinesis Data Streams, you can scale up to a sufficient number of shards (note, however, that you'll need to provision enough shards ahead of time). As it requires manual administration of shards, it's not the correct choice for the given use-case.

Amazon EMR – Amazon EMR is the industry-leading cloud big data platform for processing vast amounts of data using open source tools such as Apache Spark, Apache Hive, Apache HBase, Apache Flink, Apache Hudi, and Presto. With EMR you can run Petabyte-scale analysis at less than half of the cost of traditional on-premises solutions and over 3x faster than standard Apache Spark. Amazon EMR uses Hadoop, an open-source framework, to distribute your data and processing across a resizable cluster of Amazon EC2 instances.

Using an EMR cluster would imply managing the underlying infrastructure so it's ruled out.

AWS Lambda – AWS Lambda lets you run code without provisioning or managing servers. It cannot be used for production-grade serverless log analytics.

Reference:

https://aws.amazon.com/kinesis/data-firehose/

Q8. You have been hired as a Solutions Architect to advise a company on the various authentication/authorization mechanisms that AWS offers to authorize an API call within the API Gateway. The company would prefer a solution that offers built-in user management. Which of the following solutions would you suggest as the best fit for the given use-case?

A. Use AWS_IAM authorization
B. Use Amazon Cognito User Pools
C. Use API Gateway Lambda authorizer
D. Use Amazon Cognito Identity Pools

Correct Answer: B

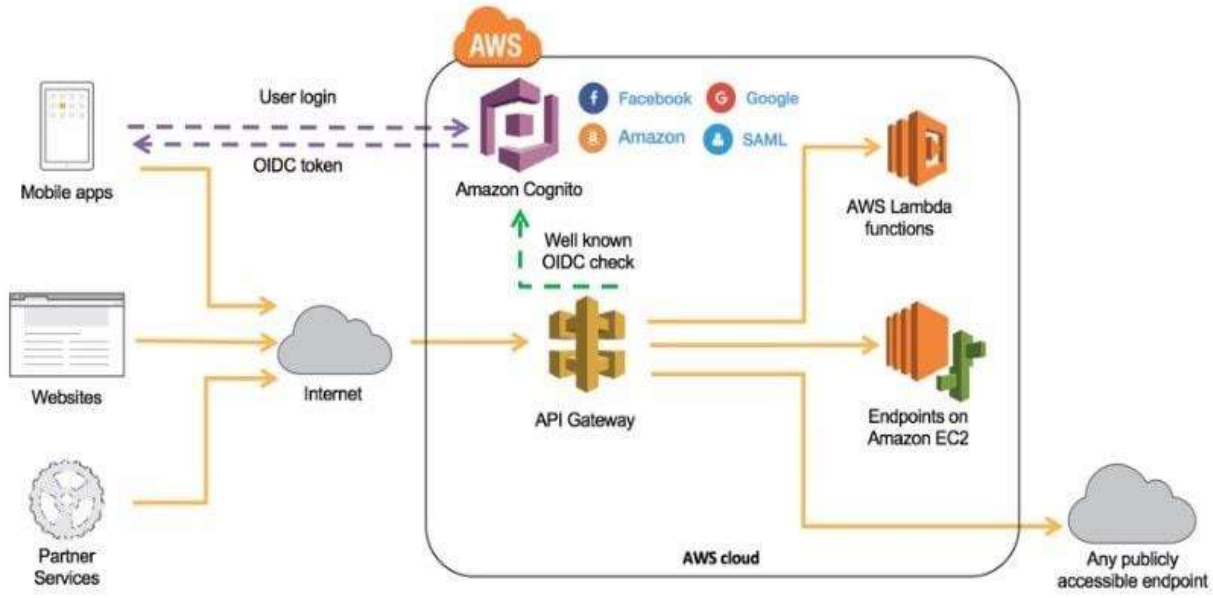
Explanation:

Use Amazon Cognito User Pools – A user pool is a user directory in Amazon Cognito. You can leverage Amazon Cognito User Pools to either provide built-in user management or integrate with external identity providers, such as Facebook, Twitter, Google+, and Amazon. Whether your users sign-in directly or through a third party, all members of the user pool have a directory profile that you can access through a Software Development Kit (SDK).

User pools provide: 1. Sign-up and sign-in services. 2. A built-in, customizable web UI to sign in users. 3. Social sign-in with Facebook, Google, Login with Amazon, and Sign in with Apple, as well as sign-in with SAML identity providers from your user pool. 4. User directory management and user profiles. 5. Security features such as multi-factor authentication (MFA), checks for compromised credentials, account takeover protection, and phone and email verification. 6. Customized workflows and user migration through AWS Lambda triggers.

After creating an Amazon Cognito user pool, in API Gateway, you must then create a COGNITO_USER_POOLS authorizer that uses the user pool.

Amazon Cognito User Pools:



via – https://docs.aws.amazon.com/wellarchitected/latest/serverless-applications-lens/identity-and-access-management.html

Incorrect options:

Use AWS_IAM authorization – For consumers who currently are located within your AWS environment or have the means to retrieve AWS Identity and Access Management (IAM) temporary credentials to access your environment, you can use AWS_IAM authorization and add least-privileged permissions to the respective IAM role to securely invoke your API. API Gateway API Keys is not a security mechanism and should not be used for authorization unless it's a public API. It should be used primarily to track a consumer's usage across your API.

Use API Gateway Lambda authorizer – If you have an existing Identity Provider (IdP), you can use an API Gateway Lambda authorizer to invoke a Lambda function to authenticate/validate a given user against your IdP. You can use a Lambda authorizer for custom validation logic based on identity metadata.

A Lambda authorizer can send additional information derived from a bearer token or request context values to your backend service. For example, the authorizer can return a map containing user IDs, user names, and scope. By using Lambda authorizers, your backend does not need to map authorization tokens to user-centric data, allowing you to limit the exposure of such information to just the authorization function.

When using Lambda authorizers, AWS strictly advises against passing credentials or any sort of sensitive data via query string parameters or headers, so this is not as secure as using Cognito User Pools.

In addition, both these options do not offer built-in user management.

Use Amazon Cognito Identity Pools – The two main components of Amazon Cognito are user pools and identity pools. Identity pools provide AWS credentials to grant your users access to other AWS services. To enable users in your user pool to access AWS resources, you can configure an identity pool to exchange user pool tokens for AWS credentials. So, identity pools aren't an authentication mechanism in themselves and hence aren't a choice for this use case.

References:

https://docs.aws.amazon.com/wellarchitected/latest/serverless-applications-lens/identity-and-access-management.html
https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-enable-cognito-user-pool.html
https://docs.aws.amazon.com/cognito/latest/developerguide/cognito-user-identity-pools.html

Q 9. A development team has noticed that one of the EC2 instances has been incorrectly configured with the 'DeleteOnTermination' attribute set to True for its root EBS volume. As a Solution Architect, can you suggest a way to disable this flag while the instance is still running?

A. Set the DisableApiTermination attribute of the instance using the API
B. Set the DeleteOnTermination attribute to False using the command line
C. The attribute cannot be updated when the instance is running. Stop the instance from Amazon EC2 console and then update the flag
D. Update the attribute using AWS management console. Select the EC2 instance and then uncheck the Delete On Termination check box for the root EBS volume

Correct Answer: B

Explanation:

When an instance terminates, the value of the DeleteOnTermination attribute for each attached EBS volume determines whether to preserve or delete the volume. By default, the DeleteOnTermination attribute is set to True for the root volume and is set to False for all other volume types.

Set the DeleteOnTermination attribute to False using the command line – If the instance is already running, you can set DeleteOnTermination to False using the command line.

Incorrect options:

Update the attribute using AWS management console. Select the EC2 instance and then uncheck the Delete On Termination check box for the root EBS volume – You can set the DeleteOnTermination attribute to False when you launch a new instance. It is not possible to update this attribute of a running instance from the AWS console.

Set the DisableApiTermination attribute of the instance using the API – By default, you can terminate your instance using the Amazon EC2 console, command-line interface, or API. To prevent your instance from being accidentally terminated using Amazon EC2, you can enable termination protection for the instance. The DisableApiTermination attribute controls whether the instance can be terminated using the console, CLI, or API. This option cannot be used to control the delete status for the EBS volume when the instance terminates.

The attribute cannot be updated when the instance is running. Stop the instance from Amazon EC2 console and then update the flag – This statement is wrong and given only as a distractor.

References:

https://aws.amazon.com/premiumsupport/knowledge-center/deleteontermination-ebs/

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/terminating-instances.html#delete-on-termination-running-instance

3 DESIGN COST-OPTIMISED ARCHITECTURES

Q1. A company has an application that needs to be hosted on an EC2 Instance. The general amount of throughput data per volume will be in the range of 400-500 MiB/s from the application. Which of the following should be used as the storage type for the underlying EC2 Instance in a Cost-effective manner?

A. EBS - General Purpose SSD
B. EBS - Provisioned IOPS SSD
C. EBS - Throughput Optimized HDD
D. EBS - Cold HDD

Answer – C

When you want high throughput, you should choose using the Throughput Optimized EBS volume. The below snapshot from the AWS Documentation shows the features of the different types of volumes.

Volume Type	EBS Provisioned IOPS SSD (io1)	EBS General Purpose SSD (gp2)*	Throughput Optimized HDD (st1)	Cold HDD (sc1)
Short Description	Highest performance SSD volume designed for latency-sensitive transactional workloads	General Purpose SSD volume that balances price performance for a wide variety of transactional workloads	Low cost HDD volume designed for frequently accessed, throughput intensive workloads	Lowest cost HDD volume designed for less frequently accessed workloac
Use Cases	I/O-intensive NoSQL and relational databases	Boot volumes, low-latency interactive apps, dev & test	Big data, data warehouses, log processing	Colder data requiring fewer scans per day
API Name	io1	gp2	st1	sc1
Volume Size	4 GB - 16 TB	1 GB - 16 TB	500 GB - 16 TB	500 GB - 16 TB
Max IOPS**/Volume	64,000	16,000	500	250
Max Throughput***/Volume	1,000 MB/s	250 MB/s	500 MB/s	250 MB/s

As per the above document, Option A, B and D stands invalid.

References

https://k21academy.com/awsdevops12
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumeTypes.html
https://k21academy.com/awssa31

Q2. Your company is currently hosting a long-running heavy load application on its On-premise environment. The company has developed this application in-house. Consulting companies then use this application via API calls, and each API call may take half an hour to finish. You now need to consider moving this application to AWS. Which of the following services would be best suited in the architecture design, which would also help deliver a cost-effective solution? Choose 2 answers from the options given below.

A. AWS Lambda
B. AWS API Gateway
C. AWS Config
D. AWS EC2

Answer – B and D

Option A might be a valid choice, but the question specifies heavy load application, leading to a need for time-out of API greater than 15min. As per AWS documentation, AWS Lambda can handle a max time-out of up to 15 minutes. In this case, the application may take more time to run.

Option B is correct because 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. With a few clicks in the AWS Management Console, you can create an API that acts as a "front door" for applications to access data, business logic, or functionality from your back-end services, such as workloads running on Amazon Elastic Compute Cloud (Amazon EC2), code running on AWS Lambda, or any web application.

Option C is incorrect since this is a configuration service available from AWS.

Option D is correct because EC2 would fit for using API calls for the application.

References

https://k21academy.com/awssa31
https://k21academy.com/awsdev16
https://k21academy.com/awssa38

Q3. You launched 9 spot instances for a specific workload in your AWS Account. Your bid price was $0.07 per hour, and the spot price at the time of launch was $0.06 per hour. After 1.5 hours, the spot price rises to $0.08 an hour. What is the cost incurred?

A. $0.54
B. $0.24
C. $0.00
D. $0.44

Answer: A

Spot instances are those instances for which a user has to place a bid on the AWS portal. If the bid price is greater than the amazon price (i.e., spot price), then the spot instances are automatically granted. The user would be charged based on the 'spot' price instead of the 'bid' price.

If the bid price is lower than the amazon price (i.e., spot price), then the spot instances are cancelled.

Now, if a user has got a spot instance running and if suddenly the spot price goes up, then amazon automatically cancels the instance, and the user is not charged for the extra minutes (rounded to one hour). This is called as amazon's termination of the spot instance.

In a second case, if a user has got a spot instance running (when the bid price is greater than the spot price and the user is granted the 'spot instance' on the 'spot' price) and the user by himself voluntarily terminates the spot instance, then the user is charged till the minute he has used the spot instance. This is called the user's voluntary termination of the spot instance.

With the above introduction, we can proceed with the below calculation.

In the first hour,

Bid price = $0.07

Spot price = $0.06

Therefore, the user is granted the spot instance. Now the price for '9' instances for the first hour would be = $0.06 * 9 = $0.54

In the second hour (i.e., for 0.5 hour)

Bid price = $0.07

Spot price = $0.08

Now the spot price is greater than the bid price which will end up in the spot instance being terminated by amazon, and the user is not charged any amount for the instances for the 0.5 hours that the instances ran.

Therefore, the total payable amount by the user for '9' instances is = $0.54.

Therefore Option 'A' is the correct answer.

Option 'B' is incorrect because the total cost is $0.24 which is lesser than $0.54

Option 'C' is incorrect because the total cost is $0.00 which is lesser than $0.54

Option 'D' is incorrect because the total cost is $0.44 which is lesser than $0.54

References

https://k21academy.com/awssa31
https://aws.amazon.com/ec2/spot/pricing/

Q4. A mid-sized Fintech company is using AWS Organization to manage multiple AWS accounts created for each department. Each of the accounts has purchased a Reserved Instance & is running web applications on a mix of On-Demand & Reserved Instance pool. A default IAM policy is configured for all accounts. Due to high recurring costs, Management has appointed you as an AWS consultant to suggest recommendations to reduce costs. Post analysis, you suggested purchasing more Reserved Instance as compared to using On-Demand EC2 instance. How would you justify your recommendations to the management?

- **A.** Use organization master account to create RI coverage budgets for all the accounts in an organization and receive SNS alert once the threshold is below 50%.
- **B.** Use Organization member account owners to create RI coverage budgets for their individual accounts in an organization & receive SNS alert once the threshold is below 50%.
- **C.** Use Organization member account owners to create RI utilization budgets for their individual accounts in an organization and receive SNS alert once the threshold is below 50%.
- **D.** Use Organization master account to create RI utilization budgets for all the accounts in an organization and receive SNS alert once the threshold is below 50%.

Answer – B

The Reserved Instance Utilization and Coverage reports are not the same.

EC2 RI Utilization % offers relevant data to identify and act on opportunities to increase your Reserved Instance usage efficiency. It's calculated by dividing the Reserved Instance used hours by total Reserved Instance purchased hours.

EC2 RI Coverage % shows how much of your overall instance usage is covered by Reserved Instances. This lets you make informed decisions about when to purchase or modify a Reserved Instance to ensure maximum coverage. It's calculated by dividing the Reserved Instance used hours by total EC2 On-Demand and Reserved Instance hours.

RI Coverage Budget reports the number of instances that are part of the Reserved Instance. This helps you get an alert when the number of instances covered by reservation falls below 50% of the number of instances launched. This report can identify the instance which is consistently running using On-Demand instance & can be converted to Reserved Instance for cost savings. AWS Organization member accounts' owners can create a budget for individual accounts. AWS Organization master account pays for usage incurred by all accounts in the organization.

Option A is incorrect since the company uses a default IAM policy. Each member account owner needs to create a budget policy for individual accounts & not by master account.

Option C is incorrect as RI utilization Budget reports the utilization of your RI instance. You need an RI Coverage report to check when the number of instances covered by reservation falls below 50% of the number of instances launched.

Option D is incorrect since the company uses a default IAM policy. Each member account owner needs to create a budget policy for individual accounts & not by master account. Also, you need an RI Coverage report to check when the number of instances covered by reservation falls below 50% of the total number of instances launched.

References

https://k21academy.com/awssa19
https://k21academy.com/awssa18
https://aws.amazon.com/aws-cost-management/reserved-instance-reporting/

Q5. A global software company is using Amazon EC2 Reserved and On-Demand Instance for all project-related work. They have different accounts created for each vertical like Finance, Project, HR, which are managed individually by account owners in each vertical. Management is looking for options to decrease these recurring charges. How could the management save monthly billing charges without impacting the performance? [Choose TWO]

A. Each account should launch a Spot Instance instead of using On-Demand Instance.
B. Each account should share Reserved Instance which they have purchased with other accounts.
C. create AWS organization and leverage consolidated billing feature to get the discounts on Amazon EC2.
D. Use Budgets to limit the charges incurred for using Amazon EC2.

Answer – B and C

Consolidated Billing combines usage from all the accounts & billing is generated based on the total usage. Services like Amazon EC2, Amazon S3, etc. have volume pricing tiers where the overall charges decrease with more usage volume.

Option A is incorrect. However, this will save the cost but will impact the performance.

Spot Instance and On-demand Instance are very similar in nature. The main difference between these is commitment. In Spot Instance, there is no commitment. As soon as the Bid price exceeds the Spot price, a user gets the Instance. In an On-demand Instance, a user has to pay the On demand rate specified by Amazon. Once they have bought the Instance, they have to use it by paying that rate.

In Spot Instance, once the Spot price exceeds the Bid price, Amazon will shut the instance. The benefit to users is that they will not be charged for the partial hour in which the Instance was taken back from them.

Spot instances are not always cheaper than on-demand. They can and do sometimes fluctuate wildly, even to very high per hour amounts, higher than the on-demand price at times.

Option B is correct as Reserved Instance discounts can be applied to accounts in an organization, but Reserved Instance sharing has to be turned on or off for the account.

Option D is incorrect as the Budget will limit charges but will not provide discounts on services being used by various accounts.

References

https://k21academy.com/awssa18
http://k21academy.com/awssa17
https://aws.amazon.com/premiumsupport/knowledge-center/ec2-ri-consolidated-billing/

Q6. A media firm uses the Amazon S3 bucket to save all videos shared by reporters across the globe. Operation Team has instructed all reporters to use only Multipart Uploads while uploading these large-sized videos to Amazon S3 bucket in each region. Most of the reporters are working from remote areas & face challenges in uploading videos. The Finance Team is concerned about high costs incurred by saving data in the Amazon S3 bucket & seeking your guidance. Post verification, you observe a large number of incomplete uploads in Amazon S3 buckets in each region. The uncompleted uploads can be deleted after a certain period of time. Which of the following actions can minimize charges for saving video files in the Amazon S3 bucket?

A. Reporter's need to compress video files locally before uploading to Amazon S3 bucket.
B. Reporter's need to upload Videos to Amazon S3 Glacier to save additional charges.
C. Create a Lifecycle Policy to move all incomplete Multipart uploads to Amazon S3 Glacier after weeks' time from initiation.
D. Create a Lifecycle Policy to delete all incomplete Multipart uploads after weeks' time from initiation.

Correct Answer: D

Incomplete Multipart Uploads incur storage charges on the Amazon S3 bucket. Lifecycle rules can be used to abort the uploading of multipart uploads that are incomplete since a specific time frame & also deletes these parts to free up storage, reducing costs for this storage.

Option A & B are incorrect as Incomplete Multipart Uploads incur charges. These charges can be stopped by stopping multipart uploads.

Option C is incorrect as Moving all incomplete Multipart uploads to Amazon S3 Glacier would not completely reduce the cost for storing data. As data in Amazon S3 Glacier would incur cost, it would be less than data storing the Amazon S3 bucket. Also, incomplete Multipart uploads would not be used until fully uploaded.

References

http://k21academy.com/awssa17
Uploading and copying objects using multipart upload - Amazon Simple Storage Service
http://k21academy.com/awssa16

Q 7. A Big Data company wants to optimize its daily Extract-Transform-Load (ETL) process that migrates and transforms data from its S3 based data lake to a Redshift cluster. The team wants to manage this daily job in a serverless environment.
Which AWS service is the best fit to manage this process without the need to configure or manage the underlying compute resources?

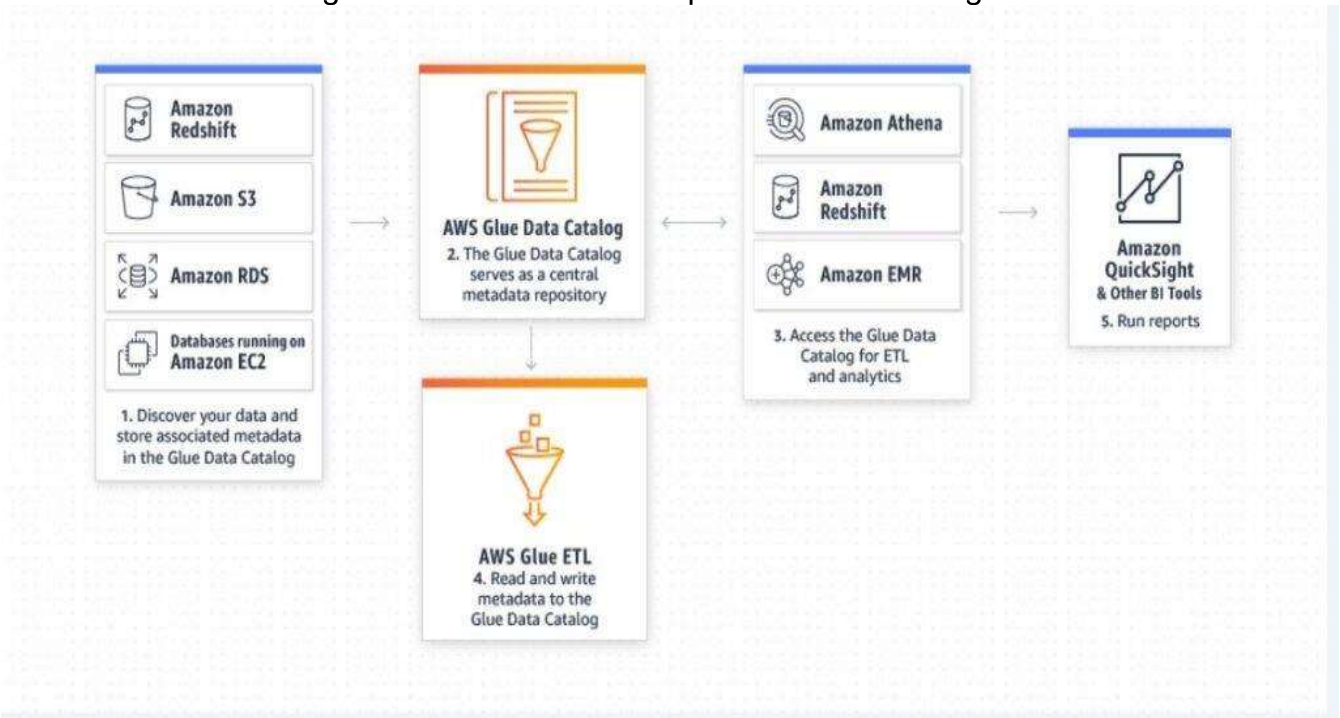
A. Amazon EMR
B. AWS Data Pipeline
C. AWS Database Migration Service (DMS)
D. AWS Glue

Correct Answer: D

Explanation:

AWS Glue – AWS Glue provides a managed ETL service that runs on a serverless Apache Spark environment. This allows you to focus on your ETL job and not worry about configuring and managing the underlying compute resources. AWS Glue takes a data-first approach and allows you to focus on the data properties and data manipulation to transform the data to a form where you can derive business insights. It provides an integrated data catalog that makes metadata available for ETL as well as querying via Amazon Athena and Amazon Redshift Spectrum.

Create a unified catalog to find data across multiple data stores using Glue:

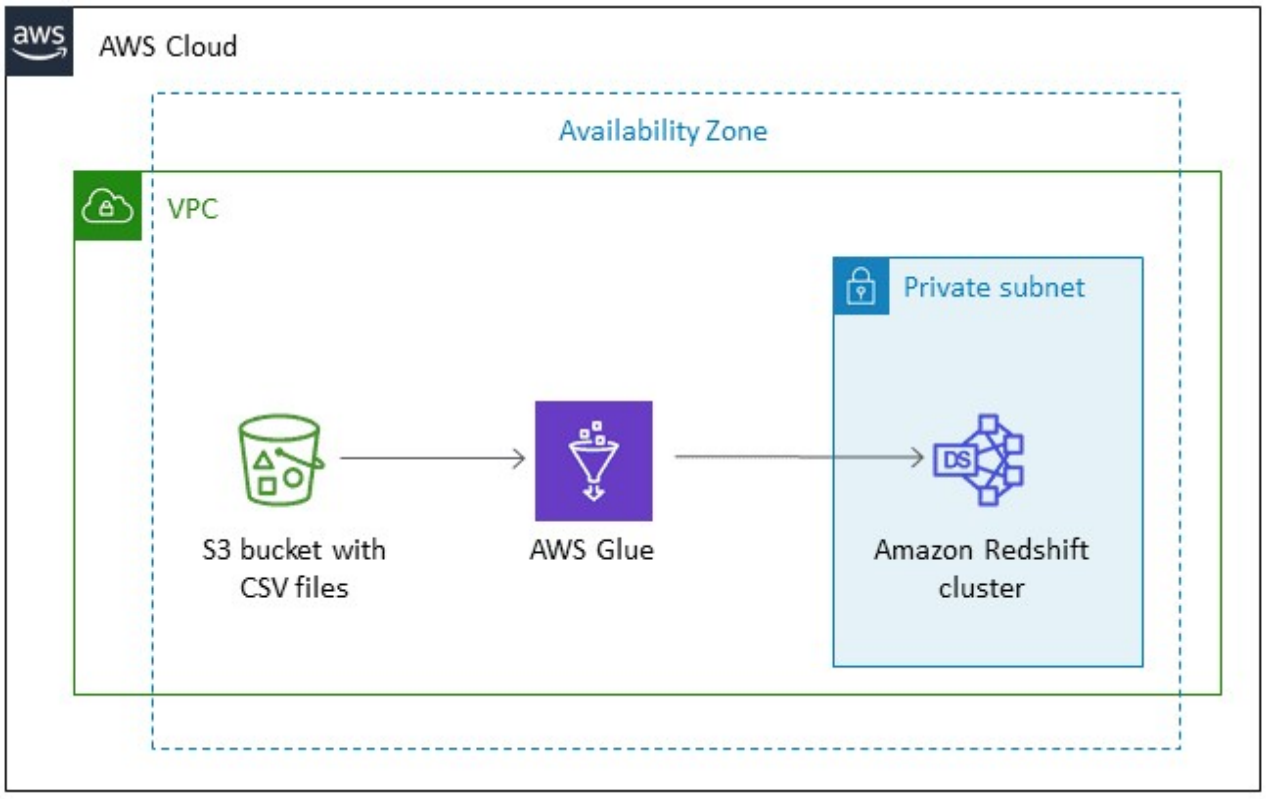


via – https://aws.amazon.com/glue/

AWS Glue automates much of the effort required for data integration. AWS Glue crawls your data sources, identifies data formats, and suggests schemas to store your data. It automatically generates the code to run your data transformations and loading processes. You can use AWS Glue to easily run and manage thousands of ETL jobs or to combine and replicate data across multiple data stores using SQL.

AWS Glue runs in a serverless environment. There is no infrastructure to manage, and AWS Glue provisions, configures, and scales the resources required to run your data integration jobs. You pay only for the resources your jobs use while running.

AWS Glue is the right fit since the company is looking at a managed ETL service without having the overhead of configuring, maintaining, or managing any servers.



via – https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/load-data-from-amazon-s3-to-amazon-redshift-using-aws-glue.html

Incorrect options:

AWS Data Pipeline – AWS Data Pipeline provides a managed orchestration service that gives you greater flexibility in terms of the execution environment, access and control over the compute resources that run your code, as well as the code itself that does data processing. AWS Data Pipeline launches compute resources in your account allowing you direct access to the Amazon EC2 instances or Amazon EMR clusters. As this option provides access to the underlying EC2 instances so it's not a serverless solution. Therefore, this option is incorrect for the given use case.

Amazon EMR – EMR is a web service to easily and cost-effectively process vast amounts of data. EMR utilizes a hosted Hadoop framework running on the web-scale infrastructure of Amazon Elastic Compute Cloud (Amazon EC2) and Amazon Simple Storage Service (Amazon S3). As this option provides access to the underlying EC2 instances so it's not a serverless solution. Therefore this option is incorrect for the given use case.

AWS Database Migration Service (DMS) – AWS Database Migration Service (DMS) helps you migrate databases to AWS easily and securely. For use cases that require a database migration from on-premises to AWS or database replication between on-premises sources and sources on AWS, AWS recommends you use AWS DMS. Once your data is in AWS, you can use AWS Glue to move, combine, replicate, and transform data from your data source into another database or data warehouse, such as Amazon Redshift. As the use-case talks about data migration and transformation between AWS services, so AWS Glue is a better fit than DMS.

References:

https://aws.amazon.com/glue/faqs/

https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/load-data-from-amazon-s3-to-amazon-redshift-using-aws-glue.html

4 DESIGN HIGH-PERFORMING ARCHITECTURES

Q1. A company has set up its application in AWS. It consists of a web tier hosted on a set of EC2 Instances. These instances interact with a MongoDB database server located in a private subnet. The web tier also interacts with many service-based applications in the private subnet. A NAT Instance is being used to route traffic from the instances in the private subnet to the Internet. The IT Administrative team is now getting CloudWatch alerts that the NAT Instance is going beyond its threshold value for Network Activity. Which of the following would you advise to increase the performance of this architecture?

A. Place the database server and application servers in the public subnet.
B. Place the NAT instance closer to the database servers by placing them in the private subnet.
C. Use the NAT gateway service instead of the NAT Instance.
D. Use a VPN connection for the Instances in the private subnet.

Answer – C

The below snapshot from the AWS Documentation shows a partial comparison of the NAT Instance and NAT Gateway. You should consider using the NAT gateway for higher bandwidth requirements.

Comparison of NAT Instances and NAT Gateways

The following is a high-level summary of the differences between NAT instances and NAT gateways.

Attribute	NAT gateway	NAT instance
Availability	Highly available. NAT gateways in each Availability Zone are implemented with redundancy. Create a NAT gateway in each Availability Zone to ensure zone-independent architecture.	Use a script to manage failover between instances.
Bandwidth	Can scale up to 45 Gbps.	Depends on the bandwidth of the instance type.

Option A is incorrect since you should not change the database or application servers' architecture since this would result in security issues.

Option B is incorrect since this would still alleviate the current network issue.

Option D is incorrect since the NAT instance should be used to route traffic to the Internet from the Instances in the private subnet.

References

https://k21academy.com/awssa28
https://k21academy.com/awssa18
https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-comparison.html

Q2. You have a set of EC2 Instances in a custom VPC. You have installed a web application and need to ensure that only HTTP and HTTPS traffic is allowed into the instance. Which of the following would you consider for this requirement?

A. Add a security group rule to allow HTTP and HTTPS Traffic.
B. Add a security group rule to an explicit DENY all traffic and a default allow on HTTP and HTTPS Traffic.
C. Add a security group rule to deny explicit traffic on HTTP and HTTPS Traffic.
D. Add a security group rule to allow all traffic.

Answer – A

Option A is correct because we need to specify the allowed traffic in the security group, i.e., HTTP and HTTPS Traffic must be allowed from all sources. No inbound traffic is allowed by default. By adding security group rules, you can specify which traffic you want to allow. This is essentially a whitelist.

Options B is incorrect since, by default, nothing is allowed, and in the Security group, we can't specify what is denied. We don't have any deny option in Security Groups.

Option C is incorrect because we can specify what is allowed in the security group but not what is denied. If you want to deny explicitly, you should use the Network Access control list.

Option D is incorrect since this would be a security issue.

Refrences

https://k21academy.com/awssa28
https://k21academy.com/awssa18
https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html

Q3. A company has an application defined with the following architecture.

- A fleet of EC2 Instances which are used to accept video uploads from users.
- A fleet of EC2 Instances which are used to process the video uploads.

Which of the following would help architect an operationally excellent architecture?

A. Create an SQS queue to store the information for Video uploads. Spin up the processing servers via an Autoscaling Group. Ensure the Group scales based on the Memory utilization of the underlying processing servers.
B. Create an SQS queue to store the information for Video uploads. Spin up the processing servers via an Autoscaling Group. Ensure the Group scales based on the size of the queue.

C. Create an SNS topic to store the information for Video uploads. Spin up the processing servers via an Autoscaling Group. Ensure the Group scales based on the Memory utilization of the underlying processing servers.

D. Create an SNS topic to store the information for Video uploads. Spin up the processing servers via an Autoscaling Group. Ensure the Group scales based on the size of the queue messages.

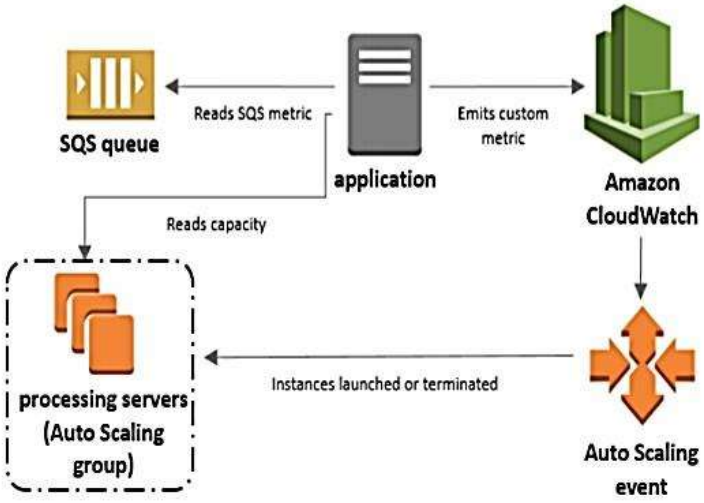
Answer – B

This architecture is also given in the AWS Documentation.

There are three main parts to this configuration:

- An Auto Scaling group to manage EC2 instances for the purposes of processing messages from an SQS queue.
- A custom metric to send to Amazon CloudWatch that measures the number of messages in the queue per EC2 instance in the Auto Scaling group.
- A target tracking policy that configures your Auto Scaling group to scale based on the custom metric and a set target value. CloudWatch alarms invoke the scaling policy.

The following diagram illustrates the architecture of this configuration.



Option A is incorrect. The ideal approach is to scale the instances based on the size of the queue.

Options C and D are incorrect since you should be using SQS queues. SNS topics are used for notification purposes.

As per AWS,

You can use the number of messages stored in an SQS queue as an indicator of the amount of work waiting in line for eventual processing within an Auto Scaling Group comprised of a variable

number of EC2 instances. Each SQS queue reports a number of metrics to CloudWatch at five-minute intervals, including ApproximateNumberOfMessagesVisible. If your workload is spikey in nature, you may want to build an application that can respond more quickly to changes in the size of the queue.

Memory utilization metrics are custom metrics. For this, you need to install a Cloudwatch agent on the EC2 instances and need to aggregate the dimensions.
However, AWS already has a well-defined architecture based on SQS Queuelength being used for Autoscaling EC2 instances.

References

https://k21academy.com/awssa35
https://k21academy.com/awssa46
https://aws.amazon.com/blogs/aws/auto-scaling-with-sqs/

Q4. An organization has branches across the world, and there are many applications deployed across AWS regions. As per organization compliance requirements, data in an S3 bucket should be copied to another S3 bucket in a different region in 24 hrs period. How can this be achieved with minimal cost?

- **A.** Use the S3 cp command to copy the data from one AWS region to another AWS region.
- **B.** Use Amazon S3 select to copy the data from one AWS region to another AWS region.
- **C.** Enable S3 versioning on source and destination buckets and copy the data using cross-region replication.
- **D.** Create a Lambda function in each AWS region to run AWS CLI "s3 sync" periodically to replicate data from one region to another region.

Answer – C

Option A is incorrect as S3 cp is an AWS CLI command where a custom program is required. S3 CP can copy data from one bucket to another, but this won't be a cost-effective solution.

Option B incorrect because S3 Select uses SQL-like statements where objects are filtered at the S3 end (service side) for an end-user application and cannot be used to copy data to another bucket in another region.

Option C is CORRECT because versioning on source and destination buckers should be enabled. Using Cross-region replication rules, data from bucket in one region to bucket in another region can be copied in 24 hrs. This replication is not sensitive to latency.

Option D is incorrect because this option needs a Lambda function in each region to execute the AWS CLI command. This method takes more efforts and is not cost-efficient.

Reference

https://k21academy.com/awssa42
https://k21academy.com/awssa22

Q5. A company has an Amazon Aurora cluster setup, and it needs to invoke a Lambda function. Which of the following need to be in place for this setup to work? Choose 2 answers from the options given below

A. Ensure that the Lambda function has an IAM Role assigned to it which can be used to invoke functions on Amazon Aurora.
B. Ensure that the Amazon Aurora cluster has an IAM Role which allows it to invoke Lambda functions.
C. Allow the Lambda function to allow outbound communication to Amazon Aurora.
D. Allow the Amazon Aurora cluster to allow outbound communication to the Lambda function.

Answer – B and D

The below snapshot from the AWS Documentation shows the different steps required to ensure that the Lambda function can access Amazon Aurora.

Giving Aurora Access to Lambda

Before you can invoke Lambda functions from an Aurora MySQL, you must first give your Aurora MySQL DB cluster permission to access Lambda.

To give Aurora MySQL access to Lambda

1. Create an AWS Identity and Access Management (IAM) policy that provides the permissions that allow your Aurora MySQL DB cluster to invoke Lambda functions. For instructions, see Creating an IAM Policy to Access AWS Lambda Resources.
2. Create an IAM role, and attach the IAM policy you created in Creating an IAM Policy to Access AWS Lambda Resources to the new IAM role. For instructions, see Creating an IAM Role to Allow Amazon Aurora to Access AWS Services.
3. Set the `aws_default_lambda_role` DB cluster parameter to the Amazon Resource Name (ARN) of the new IAM role.

   For more information about DB cluster parameters, see Amazon Aurora DB Cluster and DB Instance Parameters.
4. To permit database users in an Aurora MySQL DB cluster to invoke Lambda functions, associate the role that you created in Creating an IAM Role to Allow Amazon Aurora to Access AWS Services with the DB cluster. For information about associating an IAM role with a DB cluster, see Associating an IAM Role with an Amazon Aurora MySQL DB Cluster.
5. Configure your Aurora MySQL DB cluster to allow outbound connections to Lambda. For instructions, see Enabling Network Communication from Amazon Aurora MySQL to Other AWS Services.

Options A and C are incorrect since the configurations need to be the other way around.

References

https://k21academy.com/awsdev16
https://k21academy.com/awssa32
https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/AuroraMySQL.Integrating.Lambda.html

Q6. Your application consists of a set of EC2 Instances spun up as part of an Auto scaling group. These Instances need to access objects in an S3 bucket. Which of the following is the ideal approach to ensure this access is set in place?

- **A.** Ensure that the Access Keys are picked up from another S3 bucket. Access Keys can be embedded in the User data during Instance Launch.
- **B.** Ensure that the launch configurations in Auto scaling group have an IAM Role to access S3 Objects.
- **C.** Ensure that an IAM policy is attached to the S3 bucket which allows access to the S3 buckets.
- **D.** Ensure that the launch configurations in Auto scaling group have an IAM user to access S3 Objects.

Answer – B

Applications must sign their API requests with AWS credentials. Therefore, if you are an application developer, you need a strategy for managing credentials for your applications that run on EC2 instances. For example, you can securely distribute your AWS credentials to the instances, enabling the applications on those instances to use your credentials to sign requests while protecting your credentials from other users. However, it's challenging to securely distribute credentials to each instance, especially those that AWS creates on your behalf, such as Spot Instances or instances in Auto Scaling groups. You must also be able to update the credentials on each instance when you rotate your AWS credentials.

We designed IAM roles so that your applications can securely make API requests from your instances without requiring you to manage the security credentials that the applications use.

A launch configuration is an instance configuration template that an Auto Scaling group uses to launch EC2 instances.

For details about launch configurations, please refer to the below URL
https://docs.aws.amazon.com/autoscaling/ec2/userguide/create-launch-config.html

Option A is incorrect since using Access keys is the least secure option.

Option C is incorrect since the IAM policy is not the right option. You have to use IAM Roles instead. Also, attaching the IAM role should be a part of Launch Configurations.

Option D is incorrect since you need to use IAM Roles and not IAM Users.

To understand the basic difference between IAM Roles and Users:

IAM controls: Who can do What in your AWS account. Who (Authentication) in IAM is defined using users/groups and roles means what (Authorization) defined by policies.

User - End-user think about people.

Groups- a set of users under one set of permission(policies).

Roles - are used to grant specific permission to specific users for a set of duration of time.

References

https://k21academy.com/awssa27
https://k21academy.com/awssa19
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/iam-roles-for-amazon-ec2.html

FREE CLASS

Register for our FREE Class To know about What is AWS Solution Architect role, most important AWS services you will master Like - Why & Who Should Learn AWS?, Cloud Service, Deployment Models, and AWS Services, Demo: Creating S3 Bucket & Make a Data available to the Entire world, IAM, Compute, Storage, Networking, HA & DR Architecture and what to study Including Hands-On labs you must perform to clear **[AWS SAA-C03]** Amazon AWS Solution Architect Certification, so that you can stay ahead in your career and earn a lot more

https://k21academy.com/awssa02

contact@k21academy.com