100% Money Back Guarantee

Vendor: Amazon

Exam Code:SAP-C02

Exam Name:AWS Certified Solutions Architect - Professional

Version: Demo

QUESTION 1

A company uses AWS Cloud Formation to deploy applications within multiple VPCs that are all attached to a transit gateway. Each VPC that sends traffic to the public internet must send the traffic through a shared services VPC. Each subnet within a VPC uses the default VPC route table, and the traffic is routed to the transit gateway. The transit gateway uses its default route table for any VPC attachment.

A security audit reveals that an Amazon EC2 instance that is deployed within a VPC can communicate with an EC2 instance that is deployed in any of the company\\'s other VPCs. A solutions architect needs to limit the traffic between the VPCs. Each VPC must be able to communicate only with a predefined, limited set of authorized VPCs.

What should the solutions architect do to meet these requirements?

A. Update the network ACL of each subnet within a VPC to allow outbound traffic only to the authorized VPCs. Remove all deny rules except the default deny rule.

B. Update all the security groups that are used within a VPC to deny outbound traffic to security groups that are used within the unauthorized VPCs

C. Create a dedicated transit gateway route table for each VPC attachment. Route traffic only to the authorized VPCs.

D. Update the main route table of each VPC to route traffic only to the authorized VPCs through the transit gateway.

Correct Answer: C

You can segment your network by creating multiple route tables in an AWS Transit Gateway and associate Amazon VPCs and VPNs to them. This will allow you to create isolated networks inside an AWS Transit Gateway similar to virtual

routing and forwarding (VRFs) in traditional networks. The AWS Transit Gateway will have a default route table.

The use of multiple route tables is optional.

QUESTION 2

A solutions architect is designing a multi-account structure that has 10 existing accounts. The design must meet the following requirements

Consolidate all accounts into one organization Allow full access to the Amazon EC2 service from the management account and the secondary accounts Minimize the effort required to add additional secondary accounts

Which combination of steps should be included in the solution? (Select TWO)

A. Create an organization from the management account Send invitations to the secondary accounts from the management account Accept the invitations and create an OU

B. Create an organization from the management account. Send a join request to the management account from each secondary account Accept the requests and create an OU

C. Create a VPC peering connection between the management account and the secondary accounts Accept the request for the VPC peering connection

D. Create a service control policy (SCP) that enables full EC2 access, and attach the policy to the OU

E. Create a full EC2 access policy and map the policy to a role in each account Trust every other account to assume the role

Correct Answer: AE

QUESTION 3

A company has AWS accounts that are in an organization in AWS Organizations. The company wants to track Amazon EC2 usage as a metric.

The company\\'s architecture team must receive a daily alert if the EC2 usage is more than 10% higher than the average EC2 usage from the last 30 days.

Which solution will meet these requirements?

A. Configure AWS Budgets in the organization\\'s management account. Specify a usage type of EC2 running hours. Specify a daily period. Set the budget amount to be 10% more than the reported average usage for the last 30 days from AWS Cost Explorer. Configure an alert to notify the architecture team if the usage threshold is met.

B. Configure AWS Cost Anomaly Detection in the organization\\'s management account. Configure a monitor type of AWS Service. Apply a filter of Amazon EC2. Configure an alert subscription to notify the architecture team if the usage is 10% more than the average usage for the last 30 days.

C. Enable AWS Trusted Advisor in the organization\\'s management account. Configure a cost optimization advisory alert to notify the architecture team if the EC2 usage is 10% more than the reported average usage for the last 30 days.

D. Configure Amazon Detective in the organization\\'s management account. Configure an EC2 usage anomaly alert to notify the architecture team if Detective identifies a usage anomaly of more than 10%.

Correct Answer: B

This solution meets the requirements because it uses AWS Cost Anomaly Detection, which is a feature of AWS Cost Management that uses machine learning to identify and alert on anomalous spend and usage patterns. By configuring a monitor type of AWS Service and applying a filter of Amazon EC2, the solution can track the EC2 usage as a metric across the organization\\'s accounts. By configuring an alert subscription with a threshold of 10%, the solution can notify the architecture team via email or Amazon SNS if the EC2 usage is more than 10% higher than the average usage for the last 30 days12 A. This solution is incorrect because it uses AWS Budgets, which is a feature of AWS Cost Management that helps to plan and track costs and usage. However, AWS Budgets does not support usage type of EC2 running hours as a budget type. The only supported usage types are Amazon S3 storage, Amazon EC2 RI utilization, and Amazon EC2 RI coverage. Moreover, AWS Budgets does not support setting the budget amount based on the reported average usage from AWS Cost Explorer. The budget amount has to be a fixed or variable value34 C. This solution is incorrect because it uses AWS Trusted Advisor, which is a feature of AWS Premium Support that provides recommendations to follow best practices for cost optimization, security, performance, and fault tolerance. However, AWS Trusted Advisor does not support configuring custom alerts based on EC2 usage or average usage for the last 30 days. The only supported alerts are based on predefined checks and thresholds that are applied to all services and resources in the account56 D. This solution is incorrect because it uses Amazon Detective, which is a service that helps to analyze and visualize security data to investigate potential security issues. However, Amazon Detective does not support configuring EC2 usage anomaly alerts based on average usage for the last 30 days. The only supported alerts are based on GuardDuty findings and other security-related events that are detected by machine learning models78

References:

1: AWS Cost Anomaly Detection - Amazon Web Services

2: Getting started with AWS Cost Anomaly Detection

3: Set Custom Cost and Usage Budgets - AWS Budgets - Amazon Web Services

4: Creating a budget - AWS Cost Management

5: AWS Trusted Advisor

6: AWS Trusted Advisor - AWS Support

7: Security Investigation Visualization - Amazon Detective - AWS

8: What is Amazon Detective - Amazon Detective

QUESTION 4

A company is running a containerized application in the AWS Cloud. The application is running by using Amazon Elastic Container Service (Amazon ECS) on a set Amazon EC2 instances. The EC2 instances run in an Auto Scaling group.

The company uses Amazon Elastic Container Registry (Amazon ECRJ to store its container images When a new image version is uploaded, the new image version receives a unique tag

The company needs a solution that inspects new image versions for common vulnerabilities and exposures The solution must automatically delete new image tags that have Critical or High severity findings The solution also must notify the development team when such a deletion occurs

Which solution meets these requirements?

A. Configure scan on push on the repository. Use Amazon EventBridge (Amazon CloudWatch Events) to invoke an AWS Step Functions state machine when a scan is complete for images that have Critical or High severity findings Use the Step Functions state machine to delete the image tag for those images and to notify the development team through Amazon Simple Notification Service (Amazon SNS)

B. Configure scan on push on the repository Configure scan results to be pushed to an Amazon Simple Queue Service (Amazon SQS) queue Invoke an AWS Lambda function when a new message is added to the SOS queue Use the Lambda function to delete the image tag for images that have Critical or High seventy findings. Notify the development team by using Amazon Simple Email Service (Amazon SES).

C. Schedule an AWS Lambda function to start a manual image scan every hour Configure Amazon EventBridge (Amazon CloudWatch Events) to invoke another Lambda function when a scan is complete. Use the second Lambda function to delete the image tag for images that have Cnocal or High severity findings. Notify the development team by using Amazon Simple Notification Service (Amazon SNS)

D. Configure periodic image scan on the repository Configure scan results to be added to an Amazon Simple Queue Service (Amazon SQS) queue Invoke an AWS Step Functions state machine when a new message is added to the SQS queue Use the Step Functions state machine to delete the image tag for images that have Critical or High severity findings. Notify the development team by using Amazon Simple Email Service (Amazon SES).

Correct Answer: C

QUESTION 5

A company requires that all internal application connectivity use private IP addresses. To facilitate this policy, a solutions architect has created interface endpoints to connect to AWS public services. Upon testing, the solutions architect notices that the service names are resolving to public IP addresses, and that internal services cannot connect to the interface endpoints.

Which step should the solutions architect take to resolve this issue?

A. Update the subnet route table with a route to the interface endpoint.

B. Enable the private DNS option on the VPC attributes.

C. Configure the security group on the interface endpoint to allow connectivity to the AWS services.

D. Configure an Amazon Route 53 private hosted zone with a conditional forwarder for the internal application.

Correct Answer: C

https://docs.aws.amazon.com/vpc/latest/privatelink/vpce-interface.html

---

QUESTION 6

A financial company is planning to migrate its web application from on premises to AWS. The company uses a third-party security tool to monitor the inbound traffic to the application. The company has used the security tool for the last 15 years, and the tool has no cloud solutions available from its vendor. The company\\'s security team is concerned about how to integrate the security tool with AWS technology.

The company plans to deploy the application migration to AWS on Amazon EC2 instances. The EC2 instances will run in an Auto Scaling group in a dedicated VPC. The company needs to use the security tool to inspect all packets that come in and out of the VPC. This inspection must occur in real time and must not affect the application\\'s performance. A solutions architect must design a target architecture on AWS that is highly available within an AWS Region.

Which combination of steps should the solutions architect take to meet these requirements? (Select TWO.)

A. Deploy the security tool on EC2 instances in a new Auto Scaling group in the existing VPC.

B. Deploy the web application behind a Network Load Balancer.

C. Deploy an Application Load Balancer in front of the security tool instances.

D. Provision a Gateway Load Balancer for each Availability Zone to redirect the traffic to the security tool.

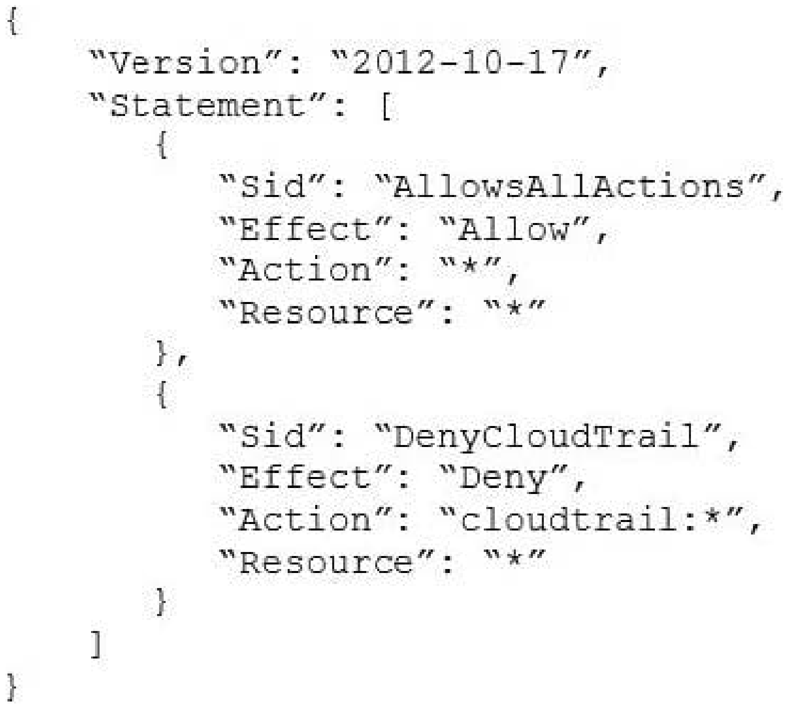
E. Provision a transit gateway to facilitate communication between VPCs.

Correct Answer: AD

Option A, Deploy the security tool on EC2 instances in a new Auto Scaling group in the existing VPC, allows the company to use its existing security tool while still running it within the AWS environment. This ensures that all packets coming in and out of the VPC are inspected by the security tool in real time. Option D, Provision a Gateway Load Balancer for each Availability Zone to redirect the traffic to the security tool, allows for high availability within an AWS Region. By provisioning a Gateway Load Balancer for each Availability Zone, the traffic is redirected to the security tool in the event of any failures or outages. This ensures that the security tool is always available to inspect the traffic, even in the event of a failure.

QUESTION 7

A company with several AWS accounts is using AWS Organizations and service control policies (SCPs). An Administrator created the following SCP and has attached it to an organizational unit (OU) that contains AWS account 1111-11111111: Developers working in account 1111-1111-1111 complain that they cannot create Amazon S3 buckets. How should the Administrator address this problem?



```
{
    “Version”: “2012-10-17”,
    “Statement”: [
        {
            “Sid”: “AllowsAllActions”,
            “Effect”: “Allow”,
            “Action”: “*”,
            “Resource”: “*”
        },
        {
            “Sid”: “DenyCloudTrail”,
            “Effect”: “Deny”,
            “Action”: “cloudtrail:*”,
            “Resource”: “*”
        }
    ]
}
```

A. Add s3:CreateBucket withAllow effect to the SCP.

B. Remove the account from the OU, and attach the SCP directly to account 1111-1111- 1111.

C. Instruct the Developers to add Amazon S3 permissions to their IAM entities.

D. Remove the SCP from account 1111-1111-1111.

Correct Answer: C

However A\\'s is incorrect - https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps.

html

"SCPs are similar to AWS Identity and Access Management (IAM) permission policies and use almost the same syntax. However, an SCP never grants permissions."

SCPs alone are not sufficient to granting permissions to the accounts in your organization. No permissions are granted by an SCP. An SCP defines a guardrail, or sets limits, on the actions that the account\\'s administrator can delegate to the

IAM users and roles in the affected accounts. The administrator must still attach identity-based or resource-based policies to IAM users or roles, or to the resources in your accounts to actually grant permissions. The effective permissions are

the logical intersection between what is allowed by the SCP and what is allowed by the IAM and resource-based policies.

QUESTION 8

A company that tracks medical devices in hospitals wants to migrate its existing storage solution to the AWS Cloud. The company equips all of its devices with sensors that collect location and usage information. This sensor data is sent in unpredictable patterns with large spikes. The data is stored in a MySQL database running on premises at each hospital. The company wants the cloud storage solution to scale with usage.

The company\\'s analytics team uses the sensor data to calculate usage by device type and hospital. The team needs to keep analysis tools running locally while fetching data from the cloud. The team also needs to use existing Java application and SQL queries with as few changes as possible.

How should a solutions architect meet these requirements while ensuring the sensor data is secure?

A. Store the data in an Amazon Aurora Serverless database. Serve the data through a Network Load Balancer (NLB). Authenticate users using the NLB with credentials stored in AWS Secrets Manager.

B. Store the data in an Amazon S3 bucket. Serve the data through Amazon QuickSight using an IAM user authorized with AWS Identity and Access Management (IAM) with the S3 bucket as the data source.

C. Store the data in an Amazon Aurora Serverless database. Serve the data through the Aurora Data API using an IAM user authorized with AWS Identity and Access Management (IAM) and the AWS Secrets Manager ARN.

D. Store the data in an Amazon S3 bucket. Serve the data through Amazon Athena using AWS PrivateLink to secure the data in transit.

Correct Answer: C

https://aws.amazon.com/blogs/aws/new-data-api-for-amazon-aurora- serverless/
https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/data-api.html

https://aws.amazon.com/blogs/aws/aws-privatelink-for-amazon-s3-now-available/

https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/data-api.html#data- api.access The data is currently stored in a MySQL database running on-prem. Storing MySQL data in S3 doesn\\'t sound good so B and D are out. Aurora Data API "enables the SQL HTTP endpoint, a connectionless Web Service API for running SQL queries against this database. When the SQL HTTP endpoint is enabled, you can also query your database from inside the RDS console (these features are free to use)."

QUESTION 9

A solutions architect has developed a web application that uses an Amazon API Gateway Regional endpoint and an AWS Lambda function. The consumers of the web application are all close to the AWS Region where the application will be deployed. The Lambda function only queries an Amazon Aurora MySQL database. The solutions architect has configured the database to have three read replicas. During testing, the application does not meet performance requirements. Under high load, the application opens a large number of database connections. The solutions architect must improve the application\\'s performance.

Which actions should the solutions architect take to meet these requirements? (Choose two.)

A. Use the cluster endpoint of the Aurora database.

B. Use RDS Proxy to set up a connection pool to the reader endpoint of the Aurora database.

C. Use the Lambda Provisioned Concurrency feature.

D. Move the code for opening the database connection in the Lambda function outside of the event handler.

E. Change the API Gateway endpoint to an edge-optimized endpoint.

Correct Answer: BD

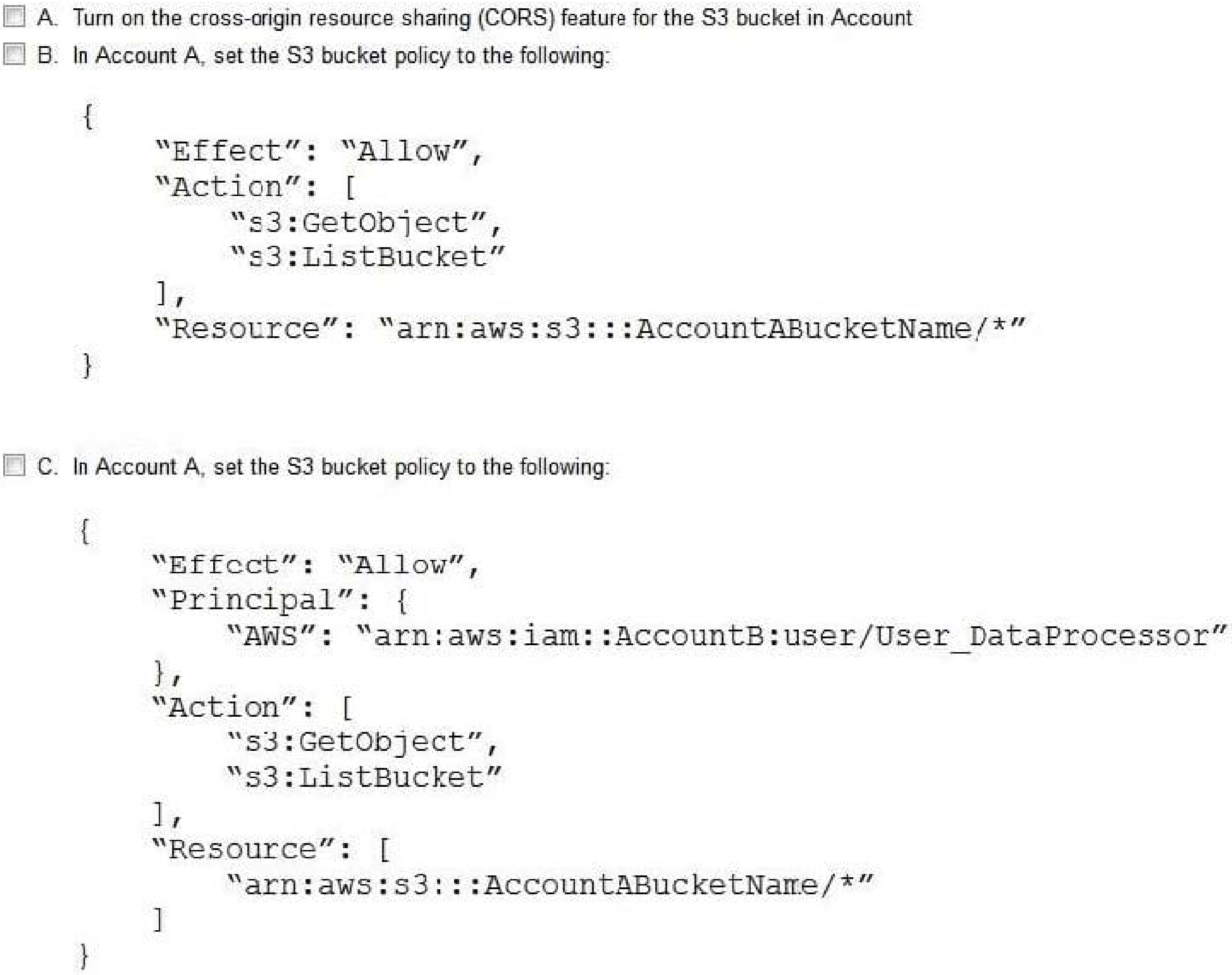
Connect to RDS outside of Lambda handler method to improve performancehttps://awstut.com/en/2022/04/30/connect-to-rds-outside-of-lambda-handler- method-to-improve-performance-en/ Using RDS Proxy, you can handle unpredictable surges in database traffic. Otherwise, these surges might cause issues due to oversubscribing connections or creating new connections at a fast rate. RDS Proxy establishes a database connection pool and reuses connections in this pool. This approach avoids the memory and CPU overhead of opening a new database connection each time. To protect the database against oversubscription, you can control the number of database connections that are created.
https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/rds-proxy.html

---

QUESTION 10

A retail company needs to provide a series of data files to another company. which is its business partner. These files are saved in an Amazon S3 bucket under Account A. which belongs to the retail company. The business partner company wants one of its IAM users User_DataProcessor to access the files from its own AWS account (Account B)

Which combination of steps must the companies take so that User_DataProcessor can access the S3 bucket successfully? (Select TWO.)



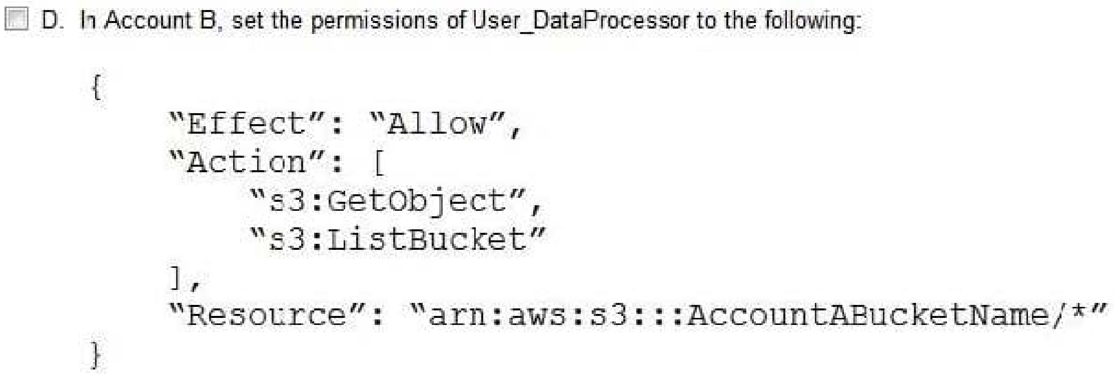
□ A. Turn on the cross-origin resource sharing (CORS) feature for the S3 bucket in Account

□ B. In Account A, set the S3 bucket policy to the following:

```
{
     “Effect”: “Allow”,
     “Action”: [
          “s3:GetObject”,
          “s3:ListBucket”
     ],
     “Resource”: “arn:aws:s3:::AccountABucketName/*”
}
```

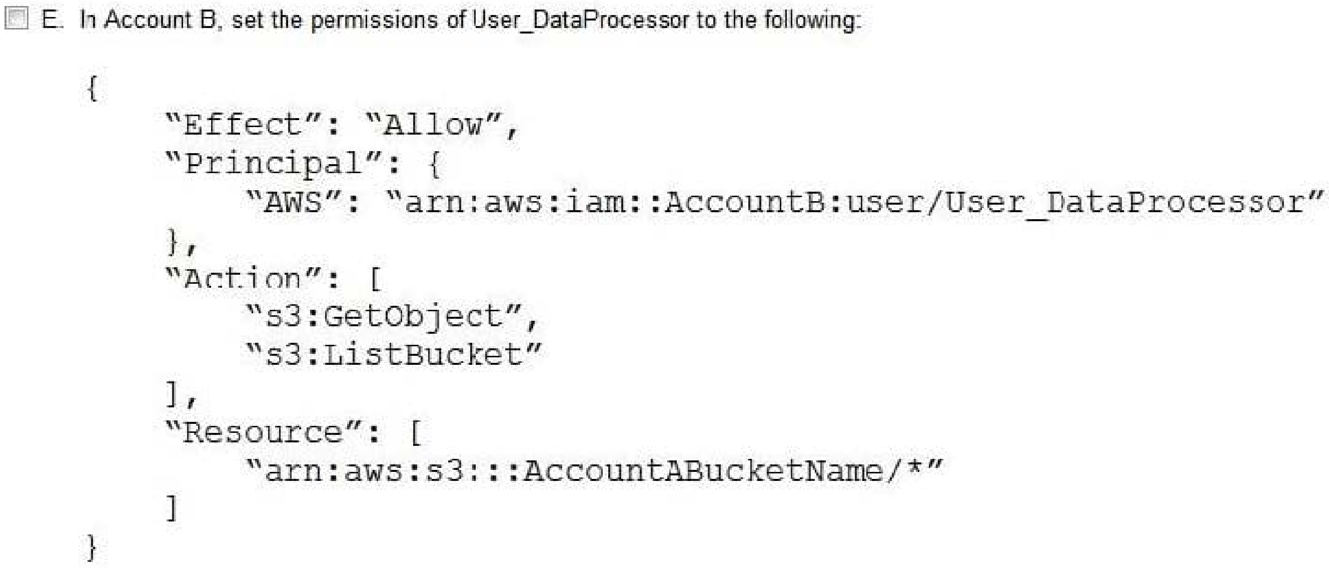
□ C. In Account A, set the S3 bucket policy to the following:

```
{
     “Effcct”: “Allow”,
     “Principal”: {
          “AWS”: “arn:aws:iam::AccountB:user/User_DataProcessor”
     },
     “Action”: [
          “s3:GetObject”,
          “s3:ListBucket”
     ],
     “Resource”: [
          “arn:aws:s3:::AccountABucketName/*”
     ]
}
```



□ D. In Account B, set the permissions of User_DataProcessor to the following:

```
{
    "Effect": "Allow",
    "Action": [
        "s3:GetObject",
        "s3:ListBucket"
    ],
    "Resource": "arn:aws:s3:::AccountABucketName/*"
}
```



□ E. In Account B, set the permissions of User_DataProcessor to the following:

```
{
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::AccountB:user/User_DataProcessor"
    },
    "Action": [
        "s3:GetObject",
        "s3:ListBucket"
    ],
    "Resource": [
        "arn:aws:s3:::AccountABucketName/*"
    ]
}
```

A. Option A

B. Option B

C. Option C

D. Option D

E. Option E

Correct Answer: CD

https://aws.amazon.com/premiumsupport/knowledge-center/cross-account- access-s3/

QUESTION 11

A company has an Amazon VPC that is divided into a public subnet and a pnvate subnet. A web application runs in Amazon VPC. and each subnet has its own NACL The public subnet has a CIDR of 10.0.0 0/24 An Application Load Balancer is deployed to the public subnet The private subnet has a CIDR of 10.0.1.0/24. Amazon EC2 instances that run a web server on port 80 are launched into the private subnet

Onty network traffic that is required for the Application Load Balancer to access the web application can be allowed to travel between the public and private subnets

What collection of rules should be written to ensure that the private subnet\\'s NACL meets the requirement? (Select TWO.)

A. An inbound rule for port 80 from source 0.0 0.0/0

B. An inbound rule for port 80 from source 10.0 0 0/24

C. An outbound rule for port 80 to destination 0.0.0.0/0

D. An outbound rule for port 80 to destination 10.0.0.0/24

E. An outbound rule for ports 1024 through 65535 to destination 10.0.0.0/24

Correct Answer: BE

Ephemeral ports are not covered in the syllabus so be careful that you don\\'t confuse day to day best practise with what is required for the exam. Link to an on Ephemeral ports here.https://acloud.guru/forums/aws-certified-solutions-architectassociate/discussion/-KUbcwo4lXefMl7janaK/network-acls-ephemeral-ports

---

QUESTION 12

A company is planning to migrate an Amazon RDS for Oracle database to an RDS for PostgreSQL DB instance in another AWS account A solutions architect needs to design a migration strategy that will require no downtime and that will minimize the amount of time necessary to complete the migration The migration strategy must replicate all existing data and any new data that is created during the migration The target database must be identical to the source database at completion of the migration process

All applications currently use an Amazon Route 53 CNAME record as their endpoint for communication with the RDS for Oracle DB instance The RDS for Oracle DB instance is in a private subnet

Which combination of steps should the solutions architect take to meet these requirements? (Select THREE)

A. Create a new RDS for PostgreSQL DB instance in the target account Use the AWS Schema Conversion Tool (AWS SCT) to migrate the database schema from the source database to the target database.

B. Use the AWS Schema Conversion Tool (AWS SCT) to create a new RDS for PostgreSQL DB instance in the target account with the schema and initial data from the source database

C. Configure VPC peering between the VPCs in the two AWS accounts to provide connectivity to both DB instances from the target account. Configure the security groups that are attached to each DB instance to allow traffic on the database port from the VPC in the target account

D. Temporarily allow the source DB instance to be publicly accessible to provide connectivity from the VPC in the target account Configure the security groups that are attached to each DB instance to allow traffic on the database port from the VPC in the target account.

E. Use AWS Database Migration Service (AWS DMS) in the target account to perform a full load plus change data capture (CDC) migration from the source database to the target database When the migration is complete, change the CNAME record to point to the target DB instance endpoint

F. Use AWS Database Migration Service (AWS DMS) in the target account to perform a change data capture (CDC) migration from the source database to the target database When the migration is complete change the CNAME record to point to the target DB instance endpoint

Correct Answer: ACE