DOP-C02$^{Q\&As}$

AWS Certified DevOps Engineer - Professional

Pass Amazon DOP-C02 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/dop-c02.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Amazon Official Exam Center

QUESTION 1

A company is using an organization in AWS Organizations to manage multiple AWS accounts. The company\\'s development team wants to use AWS Lambda functions to meet resiliency requirements and is rewriting all applications to work with Lambda functions that are deployed in a VPC. The development team is using Amazon Elastic Pile System (Amazon EFS) as shared storage in Account A in the organization.

The company wants to continue to use Amazon EPS with Lambda Company policy requires all serverless projects to be deployed in Account B.

A DevOps engineer needs to reconfigure an existing EFS file system to allow Lambda functions to access the data through an existing EPS access point.

Which combination of steps should the DevOps engineer take to meet these requirements? (Select THREE.)

A. Update the EFS file system policy to provide Account B with access to mount and write to the EFS file system in Account A.

B. Create SCPs to set permission guardrails with fine-grained control for Amazon EFS.

C. Create a new EFS file system in Account B Use AWS Database Migration Service (AWS DMS) to keep data from Account A and Account B synchronized.

D. Update the Lambda execution roles with permission to access the VPC and the EFS file system.

E. Create a VPC peering connection to connect Account A to Account B.

F. Configure the Lambda functions in Account B to assume an existing IAM role in Account A

Correct Answer: AEF

A Lambda function in one account can mount a file system in a different account. For this scenario, you configure VPC peering between the function VPC and the file system VPC. https://docs.aws.amazon.com/lambda/latest/dg/servicesefs.html https://aws.amazon.com/ru/blogs/storage/mount-amazon-efs-file-systems-cross-account-from-amazon-eks/

1.

Need to update the file system policy on EFS to allow mounting the file system into Account B. ## File System Policy $ cat file-system-policy.json { "Statement": [{ "Effect": "Allow", "Action": ["elasticfilesystem:ClientMount", "elasticfilesystem:ClientWrite"], "Principal": { "AWS": "arn:aws:iam:::root" # Replace with AWS account ID of EKS cluster } }] }

2.

Need VPC peering between Account A and Account B as the pre-requisite

3.

Need to assume cross-account IAM role to describe the mounts so that a specific mount can be chosen.

QUESTION 2

If Erin has three clusters of server types that are all managed by Ansible and she needs to provision each cluster so that they are configured with their appropriate NTP server addresses. What is the best method Erin should use in Ansible for managing this?

A. Write a task that scans the network in the target hosts\\' region for the NTP server, register the resulting address so that the next task can write the NTP configuration.

B. Break down the hosts by region in the Ansible inventory file and assign an inventory group variable the NTP address value for the respective region. The playbook can contain just the single play referencing the NTP variable from the inventory.

C. Create a playbook for each different region and store the NTP address in a variable in the play in the event the NTP server changes.

D. Create three plays, each one has the hosts for their respective regions and set the NTP server address in each task.

Correct Answer: B

While all four answers provided are correct, only B is the best choice. Ansible offers the ability to assign variables to groups of hosts in the inventory file. When the playbook is ran it will use the variables assigned to the group, even all the groups are specified in a single playbook run. The respective variables will be available to the play. This is easiest method to run, maintain and write.

Reference: http://docs.ansible.com/ansible/intro_inventory.html#group-variables

QUESTION 3

A company runs applications in AWS accounts that are in an organization in AWS Organizations The applications use Amazon EC2 instances and Amazon S3.

The company wants to detect potentially compromised EC2 instances suspicious network activity and unusual API activity in its existing AWS accounts and in any AWS accounts that the company creates in the future When the company detects one to these events the company wants to use an existing Amazon Simple Notification Service (Amazon SNS) topic to send a notification to its operational support team for investigation and remediation.

Which solution will meet these requirements in accordance with AWS best practices?

A. In the organization\\'s management account configure an AWS account as the Amazon GuardDuty administrator account. In the GuardDuty administrator account add the company\\'s existing AWS accounts to GuardDuty as members In the GuardDuty administrator account create an Amazon EventBridge rule with an event pattern to match GuardDuty events and to forward matching events to the SNS topic.

B. In the organization\\'s management account configure Amazon GuardDuty to add newly created AWS accounts by invitation and to send invitations to the existing AWS accounts Create an AWS Cloud Formation stack set that accepts the GuardDuty invitation and creates an Amazon EventBridge rule Configure the rule with an event pattern to match. GuardDuty events and to forward matching events to the SNS topic. Configure the Cloud Formation stack set to deploy into all AWS accounts in the organization.

C. In the organization\\'s management account. create an AWS CloudTrail organization trail Activate the organization trail in all AWS accounts in the organization. Create an SCP that enables VPC Flow Logs in each account in the organization. Configure AWS Security Hub for the organization Create an Amazon EventBridge rule with an even pattern to match Security Hub events and to forward matching events to the SNS topic.

D. In the organization\\'s management account configure an AWS account as the AWS CloudTrail administrator account in the CloudTrail administrator account create a CloudTrail organization trail. Add the company\\'s existing AWS accounts to the organization trail Create an SCP that enables VPC Flow Logs in each account in the organization. Configure AWS Security Hub for the organization. Create an Amazon EventBridge rule with an event pattern to match Security Hub events and to forward matching events to the SNS topic.

Correct Answer: B

It allows the company to detect potentially compromised EC2 instances, suspicious network activity, and unusual API activity in its existing AWS accounts and in any AWS accounts that the company creates in the future using Amazon GuardDuty. It also provides a solution for automatically adding future AWS accounts to GuardDuty by configuring GuardDuty to add newly created AWS accounts by invitation and to send invitations to the existing AWS accounts.

QUESTION 4

A company\\'s developers use Amazon EC2 instances as remote workstations. The company is concerned that users can create or modify EC2 security groups to allow unrestricted inbound access.

A DevOps engineer needs to develop a solution to detect when users create unrestricted security group rules. The solution must detect changes to security group rules in near real time, remove unrestricted rules, and send email notifications to the security team. The DevOps engineer has created an AWS Lambda function that checks for security group ID from input, removes rules that grant unrestricted access, and sends notifications through Amazon Simple Notification Service (Amazon SNS).

What should the DevOps engineer do next to meet the requirements?

A. Configure the Lambda function to be invoked by the SNS topic. Create an AWS CloudTrail subscription for the SNS topic. Configure a subscription filter for security group modification events.

B. Create an Amazon EventBridge scheduled rule to invoke the Lambda function. Define a schedule pattern that runs the Lambda function every hour.

C. Create an Amazon EventBridge event rule that has the default event bus as the source. Define the rule\\'s event pattern to match EC2 security group creation and modification events. Configure the rule to invoke the Lambda function.

D. Create an Amazon EventBridge custom event bus that subscribes to events from all AWS services. Configure the Lambda function to be invoked by the custom event bus.

Correct Answer: C

To meet the requirements, the DevOps engineer should create an Amazon EventBridge event rule that has the default event bus as the source. The rule\\'s event pattern should match EC2 security group creation and modification events, and it should be configured to invoke the Lambda function. This solution will allow for near real-time detection of security group rule changes and will trigger the Lambda function to remove any unrestricted rules and send email notifications to the security team. https://repost.aws/knowledge-center/monitor-security-group-changes-ec2

QUESTION 5

The Ansible Inventory system allows many attributes to be defined within it. Which item below is not one of these?

A. Group variables

B. Host groups

C. Include vars

D. Children groups

Correct Answer: C

Ansible inventory files cannot reference other files for additional data. If this functionality is needed, it must be done in as a script to create a dynamic inventory.

Reference: http://docs.ansible.com/ansible/intro_inventory.html