DOP-C02 Q&As

AWS Certified DevOps Engineer - Professional

QUESTION 1

A growing company manages more than 50 accounts in an organization in AWS Organizations. The company has configured its applications to send logs to Amazon CloudWatch Logs.

A DevOps engineer needs to aggregate logs so that the company can quickly search the logs to respond to future security incidents. The DevOps engineer has created a new AWS account for centralized monitoring.

Which combination of steps should the DevOps engineer take to make the application logs searchable from the monitoring account? (Select THREE.)

A. In the monitoring account, download an AWS CloudFormation template from CloudWatch to use in Organizations. Use CloudFormation StackSets in the organization\\'s management account to deploy the CloudFormation template to the entire organization.

B. Create an AWS CloudFormation template that defines an IAM role. Configure the role to allow logs-amazonaws.com to perform the logs:Link action if the aws:ResourceAccount property is equal to the monitoring account ID. Use CloudFormation StackSets in the organization\\'s management account to deploy the CloudFormation template to the entire organization.

C. Create an IAM role in the monitoring account. Attach a trust policy that allows logs.amazonaws.com to perform the iam:CreateSink action if the aws:PrincipalOrgld property is equal to the organization ID.

D. In the organization\\'s management account, enable the logging policies for the organization.

E. use CloudWatch Observability Access Manager in the monitoring account to create a sink. Allow logs to be shared with the monitoring account. Configure the monitoring account data selection to view the Observability data from the organization ID.

F. In the monitoring account, attach the CloudWatchLogsReadOnlyAccess AWS managed policy to an IAM role that can be assumed to search the logs.

Correct Answer: BCF

To aggregate logs from multiple accounts in an organization, the DevOps engineer needs to create a cross-account subscription that allows the monitoring account to receive log events from the sharing accounts.

To enable cross-account subscription, the DevOps engineer needs to create an IAM role in each sharing account that grants permission to CloudWatch Logs to link the log groups to the destination in the monitoring account. This can be done

using a CloudFormation template and StackSets to deploy the role to all accounts in the organization.

The DevOps engineer also needs to create an IAM role in the monitoring account that allows CloudWatch Logs to create a sink for receiving log events from other accounts. The role must have a trust policy that specifies the organization ID

as a condition.

Finally, the DevOps engineer needs to attach the CloudWatchLogsReadOnlyAccess policy to an IAM role in the monitoring account that can be used to search the logs from the cross-account subscription.

References:

1: Cross-account log data sharing with subscriptions

2: Create an IAM role for CloudWatch Logs in each sharing account

3: AWS CloudFormation StackSets

4: Create an IAM role for CloudWatch Logs in your monitoring account

5: CloudWatchLogsReadOnlyAccess policy

QUESTION 2

What flag would you use to limit a Docker container\\'s memory usage to 128 megabytes?

A. -memory 128m

B. -m 128m

C. --memory-reservation 128m

D. -m 128MB

Correct Answer: B

Docker can enforce hard memory limits, which allow the container to use no more than a given amount of user or system memory, or soft limits, which allow the container to use as much memory as it needs unless certain conditions are met,

such as when the kernel detects low memory or contention on the host machine. Some of these options have different effects when used alone or when more than one option is set. Most of these options take a positive integer, followed by a

suffix of b, k, m, g, to indicate bytes, kilobytes, megabytes, or gigabytes.

Option -m or --memory=

Description The maximum amount of memory the container can use. If you set this option, the minimum allowed value is 4m (4 megabyte).

Reference:

https://docs.docker.com/engine/admin/resource_constraints/#memory

QUESTION 3

Which services can be used as optional components of setting up a new Trail in CloudTrail?

A. KMS, SNS and SES

B. CloudWatch, S3 and SNS

C. KMS, Cloudwatch and SNS

D. KMS, S3 and CloudWatch

Correct Answer: C

Key Management Service: The use of AWS KMS is an optional element of CloudTrail, but it allows additional encryption to be added to your Log files when stored on S3 Simple Notification Service: Amazon SNS is also an optional component for CloudTrail, but it allows for you to create notifications, for example when a new log file is delivered to S3 SNS could notify someone or a team via an e-mail. Or it could be used in conjunction with CloudWatch when metric thresholds have been reached. CloudWatch Logs: Again, this is another optional component, but AWS CloudTrail allows you to deliver its logs to AWS Cloudwatch Logs as well as S3 for specific monitoring metrics to take place.

Reference: https://cloudacademy.com/amazon-web-services/aws-cloudtrail-introduction-course/how-doesaws-cloudtrail-work.html

QUESTION 4

Which answer is the proper syntax for specifying two target hosts on the command line when running an Ansible Playbook?

A. ansible-playbook -h host1.example.com -i all playbook.yml

B. ansible-playbook -i host1.example.com playbook.yml

C. ansible-playbook -h host1.example.com,host2.example.com playbook.yml

D. ansible-playbook -i host1.example.com,host2.example.com playbook.yml

Correct Answer: D

Ansible uses the `-i\\' flag for accepting an inventory file or host. To allow Ansible to determine if you are passing a host list versus an inventory file the list must be comma separated. If a single host is specified, a trailing comma must be present.

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

QUESTION 5

A company plans to use Amazon CloudWatch to monitor its Amazon EC2 instances. The company needs to stop EC2 instances when the average of the NetworkPacketsIn metric is less than 5 for at least 3 hours in a 12-hour time window. The company must evaluate the metric every hour. The EC2 instances must continue to run if there is missing data for the NetworkPacketsIn metric during the evaluation period.

A DevOps engineer creates a CloudWatch alarm for the NetworkPacketsIn metric. The DevOps engineer configures a threshold value of 5 and an evaluation period of 1 hour.

Which set of additional actions should the DevOps engineer take to meet these requirements?

A. Configure the Datapoints to Alarm value to be 3 out of 12. Configure the alarm to treat missing data as breaching the threshold. Add an AWS Systems Manager action to stop the instance when the alarm enters the ALARM state.

B. Configure the Datapoints to Alarm value to be 3 out of 12. Configure the alarm to treat missing data as not breaching the threshold. Add an EC2 action to stop the instance when the alarm enters the ALARM state.

C. Configure the Datapoints to Alarm value to be 9 out of 12. Configure the alarm to treat missing data as breaching the threshold. Add an EC2 action to stop the instance when the alarm enters the ALARM state.

D. Configure the Datapoints to Alarm value to be 9 out of 12. Configure the alarm to treat missing data as not breaching the threshold. Add an AWS Systems Manager action to stop the instance when the alarm enters the ALARM state.

Correct Answer: B

To meet the requirements, the DevOps engineer needs to configure the CloudWatch alarm to stop the EC2 instances when the average of the NetworkPacketsIn metric is less than 5 for at least 3 hours in a 12-hour time window. This means that the alarm should trigger when 3 out of 12 datapoints are below the threshold of 5. The alarm should also treat missing data as not breaching the threshold, so that the EC2 instances continue to run if there is no data for the metric during the evaluation period. The DevOps engineer can add an EC2 action to stop the instance when the alarm enters the ALARM state, which is a built-in action type for CloudWatch alarms.

DOP-C02 VCE Dumps DOP-C02 Practice Test DOP-C02 Study Guide