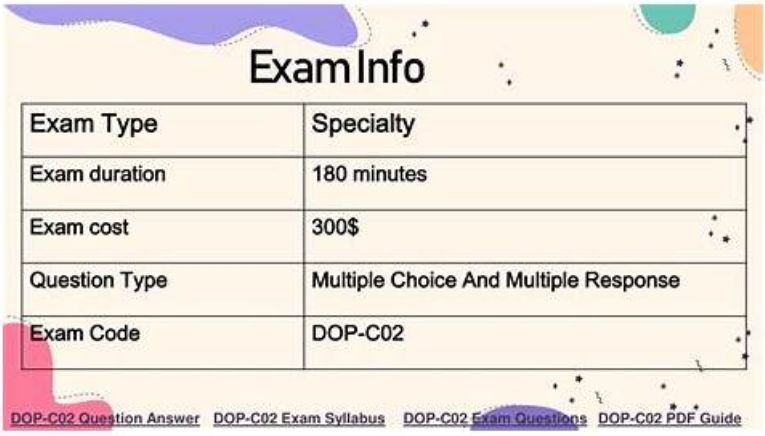
DOP-C02 Exam Questions are Available in 3 Easy-to-Understand Formats



P.S. Free 2026 Amazon DOP-C02 dumps are available on Google Drive shared by Itcertking: https://drive.google.com/open?id=1yJ5v2AZvdzS8phKXoLHWEghHEaGlAzci

The second format Itcertking also has a product support team available every time to help you out in any terms. And they will fix all of your problems on time. provides its users to study for Prepare for your AWS Certified DevOps Engineer - Professional (DOP-C02) exam is web-based practice exam. This format has all the features of desktop practice exam software for Amazon DOP-C02 exam preparation.

Amazon DOP-C02 is an advanced level certification exam offered by Amazon Web Services (AWS) for IT professionals who want to enhance their expertise in DevOps practices and technologies. AWS Certified DevOps Engineer - Professional certification is intended for individuals who have extensive experience with AWS services and have a thorough understanding of DevOps principles and practices. Passing DOP-C02 Exam validates the candidate's ability to design, deploy, and manage AWS services and infrastructure using DevOps methodologies.

>> Exam DOP-C02 Simulator Free <<

New Exam DOP-C02 Materials & Latest DOP-C02 Mock Test

Maybe life is too dull; people are willing to pursue some fresh things. If you are tired of the comfortable life, come to learn our DOP-C02 exam guide. Learning will enrich your life and change your views about the whole world. Also, lifelong learning is significant in modern society. Perhaps one day you will become a creative person through your constant learning of our DOP-C02 Study Materials. And with our DOP-C02 practice engine, your dream will come true.

Amazon AWS Certified DevOps Engineer - Professional Sample Questions (Q337-Q342):

NEW QUESTION # 337
A company has proprietary data available by using an Amazon CloudFront distribution. The company needs to ensure that the distribution is accessible by only users from the corporate office that have a known set of IP address ranges. An AWS WAF web ACL is associated with the distribution and has a default action set to Count.
Which solution will meet these requirements with the LEAST operational overhead?

- A. Create a WAF IP address set that matches the corporate office IP address range. Set the default action on the existing web ACL to Block. Add a rule that has priority 0 that allows traffic from the IP address set.
- B. Create a new regex pattern set. Add the regex pattern set to a new rule group. Create a new web ACL that has a default action set to Block. Associate the web ACL with the CloudFront distribution. Add a rule that allows traffic based on the new rule group.
- C. Create a new regex pattern set. Add the regex pattern set to a new rule group. Set the default action on the existing web ACL to Allow. Add a rule that has priority 0 that allows traffic based on the regex pattern set.
- D. Create an AWS WAF IP address set that matches the corporate office IP address range. Create a new web ACL that

has a default action set to Allow. Associate the web ACL with the CloudFront distribution. Add a rule that allows traffic from the IP address set.

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
To restrict access to CloudFront to a specific IP address range:
* Create anAWS WAF IP address setwith the corporate office IPs.
* Modify the existing WebACL'sdefault action to Block(deny all except explicitly allowed).
* Add a high-priority rule thatallows traffic from the IP address set(the corporate IPs).This way, only requests from the corporate IPs are allowed; all others are blocked.Regex pattern sets are not necessary for IP-based restrictions and add complexity. Setting default action to Allow with exceptions is less secure and more complex to manage.
References:
AWS WAF IP Set Examples
Restricting Access by IP Address

NEW QUESTION # 338
A company's web app runs on EC2 Linux instances and needs to monitor custom metrics for API response and DB query latency across instances with least overhead.
Which solution meets this?

- A. Create Lambda to poll app endpoints and DB, calculate metrics, send to CloudWatch via PutMetricData.
- B. Implement custom logging in app; use CloudWatch Logs Insights to extract and analyze metrics.
- C. Install CloudWatch agent on instances, configure it to collect custom metrics, and instrument app to send metrics to agent.
- D. Use Amazon Managed Service for Prometheus to scrape metrics, use CloudWatch agent to forward metrics to CloudWatch.

Answer: C

Explanation:
* Installing theCloudWatch agentand instrumenting the application to push custom metrics to the agent is the easiest and lowest overhead method.
* Prometheus (B) adds operational complexity.
* Lambda polling (C) introduces unnecessary complexity and latency.
* Using Logs Insights (D) requires extracting metrics from logs, which is less efficient.
References:
Custom Metrics with CloudWatch Agent
CloudWatch Agent User Guide

NEW QUESTION # 339

- A.
- B. Option A
- C. Option C
- D. Option D
- E.
- F. Option B
- G.
- H.

Answer: C,H

Explanation:
https://docs.aws.amazon.com/singlesignon/latest/userguide/configure-abac.html

NEW QUESTION # 340
A production account has a requirement that any Amazon EC2 instance that has been logged in to manually must be terminated

within 24 hours. All applications in the production account are using Auto Scaling groups with the Amazon CloudWatch Logs agent configured.
How can this process be automated?

- A. Create an Amazon CloudWatch alarm that will be invoked by the login event. Send the notification to an Amazon Simple Notification Service (Amazon SNS) topic that the operations team is subscribed to, and have them terminate the EC2 instance within 24 hours.
- B. Create a CloudWatch Logs subscription to an AWS Lambda function. Configure the function to add a tag to the EC2 instance that produced the login event and mark the instance to be decommissioned.Create an Amazon EventBridge rule to invoke a daily Lambda function that terminates all instances with this tag.
- C. Create an Amazon CloudWatch alarm that will be invoked by the login event. Configure the alarm to send to an Amazon Simple Queue Service (Amazon SQS) queue. Use a group of worker instances to process messages from the queue, which then schedules an Amazon EventBridge rule to be invoked.
- D. Create a CloudWatch Logs subscription to an AWS Step Functions application. Configure an AWS Lambda function to add a tag to the EC2 instance that produced the login event and mark the instance to be decommissioned. Create an Amazon EventBridge rule to invoke a second Lambda function once a day that will terminate all instances with this tag.

Answer: B

Explanation:
"You can use subscriptions to get access to a real-time feed of log events from CloudWatch Logs and have it delivered to other services such as an Amazon Kinesis stream, an Amazon Kinesis Data Firehose stream, or AWS Lambda for custom processing, analysis, or loading to other systems. When log events are sent to the receiving service, they are Base64 encoded and compressed with the gzip format." Seehttps://docs.aws.
amazon.com/AmazonCloudWatch/latest/logs/Subscriptions.html

NEW QUESTION # 341
AnyCompany is using AWS Organizations to create and manage multiple AWS accounts AnyCompany recently acquired a smaller company, Example Corp. During the acquisition process, Example Corp's single AWS account joined AnyCompany's management account through an Organizations invitation. AnyCompany moved the new member account under an OU that is dedicated to Example Corp.
AnyCompany's DevOps eng*neer has an IAM user that assumes a role that is named OrganizationAccountAccessRole to access member accounts. This role is configured with a full access policy When the DevOps engineer tries to use the AWS Management Console to assume the role in Example Corp's new member account, the DevOps engineer receives the following error message "Invalid information in one or more fields. Check your information or contact your administrator." Which solution will give the DevOps engineer access to the new member account?

- A. In the new member account edit the trust policy for the Organ zationAccountAccessRole IAM role.Grant the management account permission to assume the role.
- B. In the new member account, create a new IAM role that is named OrganizationAccountAccessRole.
  Attach the AdmInistratorAccess AVVS managed policy to the role. In the role's trust policy, grant the management account permission to assume the role.
- C. In the management account, grant the DevOps engineer's IAM user permission to assume the OrganzatlonAccountAccessR01e IAM role in the new member account.
- D. In the management account, create a new SCR In the SCP, grant the DevOps engineer's IAM user full access to all resources in the new member account. Attach the SCP to the OU that contains the new member account,

Answer: B

Explanation:
Explanation
The problem is that the DevOps engineer cannot assume the OrganizationAccountAccessRole IAM role in the new member account that joined AnyCompany's management account through an Organizations invitation.
The solution is to create a new IAM role with the same name and trust policy in the new member account.
Option A is incorrect, as it does not address the root cause of the error. The DevOps engineer's IAM user already has permission to assume the OrganizationAccountAccessRole IAM role in any member account, as this is the default role name that AWS Organizations creates when a new account joins an organization. The error occurs because the new member account does not have this role, as it was not created by AWS Organizations.
Option B is incorrect, as it does not address the root cause of the error. An SCP is a policy that defines the maximum permissions for account members of an organization or organizational unit (OU). An SCP does not grant permissions to IAM users or roles, but

rather limits the permissions that identity-based policies or resource-based policies grant to them. An SCP also does not affect how IAM roles are assumed by other principals.
Option C is correct, as it addresses the root cause of the error. By creating a new IAM role with the same name and trust policy as the OrganizationAccountAccessRole IAM role in the new member account, the DevOps engineer can assume this role and access the account. The new role should have the AdministratorAccess AWS managed policy attached, which grants full access to all AWS resources in the account. The trust policy should allow the management account to assume the role, which can be done by specifying the management account ID as a principal in the policy statement.
Option D is incorrect, as it assumes that the new member account already has the OrganizationAccountAccessRole IAM role, which is not true. The new member account does not have this role, as it was not created by AWS Organizations. Editing the trust policy of a non-existent role will not solve the problem.

NEW QUESTION # 342
.....