# DOP-C02 Knowledge Points - Your Reliable Support to Pass AWS Certified DevOps Engineer - Professional


What's more, part of that ExamsLabs DOP-C02 dumps now are free: https://drive.google.com/open?id=1RPxhJk_G3tHtga7Rb5m_MTizTzybue8W

Thus, it will allow you to examine the Amazon DOP-C02 Dumps before purchasing it. ExamsLabs proudly presents the exceptional Amazon DOP-C02 material that will meet your expectations. Beware that the sections of the exam change from time to time. Therefore, be alert by checking the updates frequently. It will prevent you from wasting time, material expenses, and inner peace.

The Amazon DOP-C02 Exam covers a wide range of topics, including provisioning and managing infrastructure using AWS services like EC2, RDS, and Elastic Beanstalk, designing and implementing scalable, fault-tolerant systems, and implementing and managing continuous integration and continuous delivery pipelines using tools like CodePipeline and CodeDeploy. Candidates are also tested on their ability to monitor and troubleshoot applications and infrastructure using AWS tools like CloudWatch and CloudTrail.

**>> DOP-C02 Knowledge Points <<**

## How ExamsLabs Can Help You in Amazon DOP-C02 Exam Preparation?

In a knowledge-based job market, learning is your quickest pathway, your best investment. Knowledge is wealth. Modern society needs solid foundation, broad knowledge, and comprehensive quality of compound talents. Our DOP-C02 certification materials can help you transfer into a versatile talent. Many job seekers have successfully realized financial freedom with the assistance of our DOP-C02 test training. All your dreams will be fully realized after you have obtained the DOP-C02 certificate. Finding a good paying job is available for you. Good chances are few. Please follow your heart.

## Amazon AWS Certified DevOps Engineer - Professional Sample Questions (Q128-Q133):

**NEW QUESTION # 128**
An ecommerce company has chosen AWS to host its new platform. The company's DevOps team has started building an AWS Control Tower landing zone. The DevOps team has set the identity store within AWS IAM Identity Center (AWS Single Sign-On) to external identity provider (IdP) and has configured SAML 2.0.
The DevOps team wants a robust permission model that applies the principle of least privilege. The model must allow the team to build and manage only the team's own resources.
Which combination of steps will meet these requirements? (Choose three.)

- A. Create IAM policies that include the required permissions. Include the aws:PrincipalTag condition key.
- B. Create a group in the IdP. Place users in the group. Assign the group to accounts and the permission sets in IAM Identity Center.
- C. Create a group in the IdP. Place users in the group. Assign the group to OUs and IAM policies.
- D. Create permission sets. Attach an inline policy that includes the required permissions and uses the aws:PrincipalTag condition key to scope the permissions.
- E. Enable attributes for access control in IAM Identity Center. Map attributes from the IdP as key-value pairs.

- F. Enable attributes for access control in IAM Identity Center. Apply tags to users. Map the tags as key-value pairs.

**Answer: B,D,E**

Explanation:
Explanation
Using the principalTag in the Permission Set inline policy a logged in user belonging to a specific AD group in the IDP can be permitted access to perform operations on certain resources if their group matches the group used in the PrincipleTag. Basically you are narrowing the scope of privileges assigned via Permission policies conditionally based on whether the logged in user belongs to a specific AD Group in IDP. The mapping of the AD group to the request attributes can be done using SSO attributes where we can pass other attributes like the SAML token as well.
https://docs.aws.amazon.com/singlesignon/latest/userguide/abac.html

**NEW QUESTION # 129**
A company runs its container workloads in AWS App Runner. A DevOps engineer manages the company's container repository in Amazon Elastic Container Registry (Amazon ECR).
The DevOps engineer must implement a solution that continuously monitors the container repository. The solution must create a new container image when the solution detects an operating system vulnerability or language package vulnerability.
Which solution will meet these requirements?

- A. Use EC2 Image Builder to create a container image pipeline. Use Amazon ECR as the target repository. Enable Amazon GuardDuty Malware Protection on the container workload. Create an Amazon EventBridge rule to capture a GuardDuty finding event. Use the event to invoke the image pipeline.
- B. Create an AWS CodeBuild project to create a container image. Use Amazon ECR as the target repository. Turn on basic scanning on the repository. Create an Amazon EventBridge rule to capture an ECR image action event. Use the event to invoke the CodeBuild project. Re-upload the container to the repository.
- C. Use EC2 Image Builder to create a container image pipeline. Use Amazon ECR as the target repository. Turn on enhanced scanning on the ECR repository. Create an Amazon EventBridge rule to capture an Inspector2 finding event. Use the event to invoke the image pipeline. Re-upload the container to the repository.
- D. Create an AWS CodeBuild project to create a container image. Use Amazon ECR as the target repository. Configure AWS Systems Manager Compliance to scan all managed nodes. Create an Amazon EventBridge rule to capture a configuration compliance state change event. Use the event to invoke the CodeBuild project.

**Answer: C**

Explanation:
The solution that meets the requirements is to use EC2 Image Builder to create a container image pipeline, use Amazon ECR as the target repository, turn on enhanced scanning on the ECR repository, create an Amazon EventBridge rule to capture an Inspector2 finding event, and use the event to invoke the image pipeline. Re-upload the container to the repository.
This solution will continuously monitor the container repository for vulnerabilities using enhanced scanning, which is a feature of Amazon ECR that provides detailed information and guidance on how to fix security issues found in your container images. Enhanced scanning uses Inspector2, a security assessment service that integrates with Amazon ECR and generates findings for any vulnerabilities detected in your images. You can use Amazon EventBridge to create a rule that triggers an action when an Inspector2 finding event occurs. The action can be to invoke an EC2 Image Builder pipeline, which is a service that automates the creation of container images. The pipeline can use the latest patches and updates to build a new container image and upload it to the same ECR repository, replacing the vulnerable image.
The other options are not correct because they do not meet all the requirements or use services that are not relevant for the scenario.
Option B is not correct because it uses Amazon GuardDuty Malware Protection, which is a feature of GuardDuty that detects malicious activity and unauthorized behavior on your AWS accounts and resources. GuardDuty does not scan container images for vulnerabilities, nor does it integrate with Amazon ECR or EC2 Image Builder.
Option C is not correct because it uses basic scanning on the ECR repository, which only provides a summary of the vulnerabilities found in your container images. Basic scanning does not use Inspector2 or generate findings that can be captured by Amazon EventBridge. Moreover, basic scanning does not provide guidance on how to fix the vulnerabilities.
Option D is not correct because it uses AWS Systems Manager Compliance, which is a feature of Systems Manager that helps you monitor and manage the compliance status of your AWS resources based on AWS Config rules and AWS Security Hub standards. Systems Manager Compliance does not scan container images for vulnerabilities, nor does it integrate with Amazon ECR or EC2 Image Builder.

**NEW QUESTION # 130**

A company has a fleet of Amazon EC2 instances that run Linux in a single AWS account. The company is using an AWS Systems Manager Automation task across the EC2 instances.
During the most recent patch cycle, several EC2 instances went into an error state because of insufficient available disk space. A DevOps engineer needs to ensure that the EC2 instances have sufficient available disk space during the patching process in the future.
Which combination of steps will meet these requirements? {Select TWO.)

- A. Ensure that the Amazon CloudWatch agent is installed on all EC2 instances
- B. Create a cron job that is installed on each EC2 instance to periodically delete temporary files.
- C. Create an AWS Lambda function to periodically check for sufficient available disk space on all EC2 instances by evaluating each EC2 instance's respective Amazon CloudWatch log stream.
- D. Create an Amazon CloudWatch alarm to monitor available disk space on all EC2 instances Add the alarm as a safety control to the Systems Manager Automation task.
- E. Create an Amazon CloudWatch log group for the EC2 instances. Configure a cron job that is installed on each EC2 instance to write the available disk space to a CloudWatch log stream for the relevant EC2 instance.

**Answer: A,D**

Explanation:
* Ensure that the Amazon CloudWatch agent is installed on all EC2 instances:
The Amazon CloudWatch agent collects and logs metrics and sends them to Amazon CloudWatch.
To install the CloudWatch agent:
Download the CloudWatch agent package.
Install the agent on your EC2 instances.
Configure the agent to collect disk space metrics.
* Create an Amazon CloudWatch alarm to monitor available disk space on all EC2 instances Add the alarm as a safety control to the Systems Manager Automation task:
Create CloudWatch alarms to monitor the available disk space and trigger notifications or actions when the disk space falls below a defined threshold.
Add the CloudWatch alarm to the Systems Manager Automation task to halt or fail the task if disk space is insufficient.
To create the alarm:
Navigate to the CloudWatch console and create a new alarm.
Set the metric to monitor (e.g., disk space utilization).
Define the threshold and notification actions.
Reference:
Amazon CloudWatch agent
Creating Amazon CloudWatch alarms

**NEW QUESTION # 131**
A company has multiple AWS accounts. The company uses AWS IAM Identity Center (AWS Single Sign-On) that is integrated with AWS Toolkit for Microsoft Azure DevOps. The attributes for access control feature is enabled in IAM Identity Center.
The attribute mapping list contains two entries. The department key is mapped to ${path:enterprise.department}. The costCenter key is mapped to ${path:enterprise.costCenter}.
All existing Amazon EC2 instances have a department tag that corresponds to three company departments (d1, d2, d3). A DevOps engineer must create policies based on the matching attributes. The policies must minimize administrative effort and must grant each Azure AD user access to only the EC2 instances that are tagged with the user's respective department name.
Which condition key should the DevOps engineer include in the custom permissions policies to meet these requirements?

- A.
- B.
- C.
- D.

**Answer: D**

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

**NEW QUESTION # 132**
A DevOps engineer must implement a solution that immediately terminates Amazon EC2 instances in Auto Scaling groups when cryptocurrency mining activity is detected.
Which solution will meet these requirements with the LEAST development effort?

- A. Configure Amazon Route 53 to send query logs directly to Amazon CloudWatch Logs. Create an AWS Lambda function that runs every 5 minutes and checks the query logs for domains related to cryptocurrency activity. If the domains are found, terminate the identified EC2 instances.
- B. Enable AWS Security Hub. Monitor EC2 findings. Create an Amazon EventBridge rule with Security Hub as the event source. Create an AWS Lambda function that is triggered by the EventBridge rule.Configure the Lambda function to parse the event and terminate the identified EC2 instances.
- C. Configure VPC Flow Logs to send flow logs to an Amazon S3 bucket. Create an AWS Lambda function that runs every 5 minutes and invokes an Amazon Athena query to find IP addresses associated with cryptocurrency activity. If the IP addresses are found, terminate the identified EC2 instances.
- D. Enable Amazon GuardDuty. Monitor EC2 findings. Create an Amazon EventBridge rule with GuardDuty as the event source. Create an AWS Lambda function that is triggered by the EventBridge rule. Configure the Lambda function to parse the event and terminate the identified EC2 instances.

**Answer: D**

Explanation:
The requirement is to immediately detect and terminate EC2 instances involved in cryptocurrency mining with the least development effort. Amazon GuardDuty is the AWS-native service specifically designed to detect malicious activities such as crypto-mining by continuously analyzing CloudTrail events, VPC Flow Logs, and DNS logs. GuardDuty includes managed threat intelligence and predefined findings like CryptoCurrency:EC2/BitcoinTool.B!DNS and CryptoCurrency:EC2/BitcoinTool.B!IP, which directly identify mining behavior without custom detection logic.
Option C leverages this built-in capability. Once GuardDuty is enabled, findings are automatically generated when mining activity is detected. These findings are sent to Amazon EventBridge in near real time. An EventBridge rule can filter for cryptocurrency-related findings and trigger an AWS Lambda function. The Lambda function can then identify the affected EC2 instance and terminate it or adjust the Auto Scaling group to replace it. This approach requires minimal custom code and no log parsing, scheduled jobs, or analytics pipelines.
Options A and B rely on custom log analysis, periodic execution, and maintaining lists of mining domains or IPs, which significantly increases complexity and response time. Option D uses AWS Security Hub, which aggregates findings from GuardDuty and other services but is not intended for immediate, low-latency remediation.
Therefore, Option C provides the fastest detection, immediate response, and lowest development overhead using AWS-managed threat detection services.

**NEW QUESTION # 133**
.....

Search for 「 DOP-C02 」 and download it for free on 「 www.pdfvce.com 」 website □Reliable DOP-C02 Exam Cost

- Amazon DOP-C02 AWS Certified DevOps Engineer - Professional Exam Questions Get Excellent Scores □ Download ▸ DOP-C02 ◂ for free by simply searching on ➽ www.torrentvce.com □ □DOP-C02 Updated Demo
- Latest DOP-C02 Test Simulator □ DOP-C02 Frenquent Update □ Simulation DOP-C02 Questions □ Copy URL { www.pdfvce.com } open and search for ▸ DOP-C02 ◂ to download for free □DOP-C02 Latest Test Format
- Pass Guaranteed Quiz 2026 High Hit-Rate Amazon DOP-C02 Knowledge Points □ Open ➽ www.verifieddumps.com □ □ and search for ➡ DOP-C02 □□□ to download exam materials for free □DOP-C02 Reliable Exam Question
- DOP-C02 Frenquent Update □ DOP-C02 Updated Demo □ Vce DOP-C02 Free □ Search for ☀ DOP-C02 □☀□ and easily obtain a free download on ➥ www.pdfvce.com □ □Simulation DOP-C02 Questions
- DOP-C02 Updated Demo □ Vce DOP-C02 Free □ DOP-C02 Exam Pattern □ Search for 【 DOP-C02 】 and download it for free on " www.dumpsmaterials.com " website □New DOP-C02 Test Objectives
- jimewub506801.izrablog.com, lexieypxu142944.tokka-blog.com, janicemgjy519800.wikinarration.com, anitavncc947360.qodsblog.com, shaunacxit021995.blog-mall.com, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, bookmarkpagerank.com, zaynlonb723793.wikifrontier.com, lorifzjd459300.bloggerswise.com, Disposable vapes

2026 Latest ExamsLabs DOP-C02 PDF Dumps and DOP-C02 Exam Engine Free Share: https://drive.google.com/open?id=1RPxhJk_G3tHtga7Rb5m_MTizTzybue8W