# Free Questions for PCCSE by braindumpscollection

## Shared by Daniels on 24-05-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

# Question 1

## Question Type: MultipleChoice

Which command correctly outputs scan results to stdout in tabular format and writes scan results to a JSON file while still sending the results to Console?

A)

Image not found or type unknown

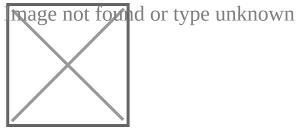
B)

Image not found or type unknown

C)

Image not found or type unknown

D)



## Options:

**A)** Option A

**B)** Option B

**C)** Option C

**D)** Option D

## Answer:

A

## Explanation:

The commands presented in the image are used to scan images with the twistcli command-line tool, which is part of the Prisma Cloud suite. To determine the correct command, we need to identify the one that specifies output to stdout in a tabular format and writes the scan results to a JSON file.

Option A uses the --stdout flag, which is the correct way to output to stdout, and --output-file with the .json format for the file. The --address flag is correctly used to specify the Console address. Thus, Option A is the correct command fulfilling the requirement.

# Question 2

**Question Type:** **MultipleChoice**

Which RQL query will help create a custom identity and access management (1AM) policy to alert on Lambda functions that have permission to terminate FP9 instances?

## Options:

**A)** config from iam where dest.cloud.type = 'AWS' AND source.cloud.service.name = 'lambda1 AND source.cloud.resource.type = 'function1 AND dest.cloud.service.name = 'ec2' AND action.name = 'ec2:TerminateInstances'

**B)** config from iam where dest.cloud.type = 'AWS' AND source.cloud.service.name = 'ec2' AND source.cloud.resource.type = 'instance' AND dest.cloud.service.name = 'lamda' AND action.name = 'ec2:TerminateInstances'

**C)** iam from cloud.resource where dest.cloud.type = 'AWS' AND source.cloud.service.name = 'lambda' AND source.cloud.resource.type = 'function' AND dest.cloud.service.name = 'ec2' AND action.name = 'ec2:TerminateInstances'

**D)** iam from cloud.resource where cloud.type equals 'AWS' AND cloud.resource.type equals 'lambda function' AND cloud.service.name = 'ec2' AND action.name equals 'ec2:TerminateInstances'

## Answer:

A

### Explanation:

To create a custom Identity and Access Management (IAM) policy that alerts on Lambda functions with permissions to terminate EC2 instances, the correct RQL query structure involves specifying the source service (Lambda), the destination service (EC2), and the specific action of interest ('ec2:TerminateInstances'). The query should identify configurations where a Lambda function ('source.cloud.service.name = 'lambda' and 'source.cloud.resource.type = 'function') has been granted permissions that allow it to perform the 'ec2:TerminateInstances' action on EC2 instances ('dest.cloud.service.name = 'ec2'). This query helps in identifying and mitigating potential risks associated with overly permissive functions that could inadvertently or maliciously impact the availability of EC2 resources.

## Question 3

**Question Type: MultipleChoice**

A customer is interested in PCI requirements and needs to ensure that no privilege containers can start in the environment. Which action needs to be set for "do not use privileged containers?

### Options:

**A)** Alert

**B)** Prevent

**C)** Fail

**D)** Block

### Answer:

A

# Question 4

**Question Type:** **MultipleChoice**

An administrator has deployed Console into a Kubernetes cluster running in AWS. The administrator also has configured a load balancer in TCP passthrough mode to listen on the same ports as the default Prisma Compute Console configuration

In the build pipeline, the administrator wants twistcli to talk to Console over HTTPS

Which port will twistcli need to use to access the Prisma Compute APIs?

### Options:

**A)** 8081

**B)** 443

**C)** 8084

**D)** 8083
https://docs.paloaltonetworks.com/prisma/prisma-cloud/20-12/prisma-cloud-compute-edition-admin/howto/configure_eks_loadbalancer.html

## Answer:

C

# Question 5

**Question Type: MultipleChoice**

Which statement is true about obtaining Console images for Prisma Cloud Compute Edition'?

To retrieve Prisma Cloud Console images using URL auth;

## Options:

**A)** 1 Access registry-urt-auth twistlock com, and authenticate using the user certificate

2. Retrieve the Prisma Cloud Console images using 'docker pull'

To retrieve Prisma Cloud Console images using basic auth:

**B)** 1. Access registry twistlock com. and authenticate using 'docker login'

2 Retrieve the Prisma Cloud Console images using 'docker pull'

To retrieve Prisma Cloud Console images using URL auth

**C)** 1 Access registry-auth.twistlock com and authenticate using the user certificate

2. Retrieve the Prisma Cloud Console images using 'docker pull'

To retrieve Prisma Cloud Console images using basic auth

**D)** 1 Access registry paloaltonetworks com. and authenticate using 'docker login'

2 Retrieve the Prisma Cloud Console images using 'docker pull'

### Answer:

C

# Question 6

**Question Type:** **MultipleChoice**

Given this information:

The password is: password123

The image to scan is: myimage:latest

Which twistcli command should be used to scan a Container for vulnerabilities and display the details about each vulnerability?

## Options:

**A)** twistcli images scan --console-address https://prisma-console.mydomain.local -u cluster -p password123 -- details myimage:latest

**B)** twistcli images scan --console-address prisma-console.mydomain.local -u cluster -p password123 -- vulnerability-details myimage:latest

**C)** twistcli images scan --address prisma-console.mydomain.local -u cluster -p password123 --vulnerability- details myimage:latest

**D)** twistcli images scan --address https://prisma-console.mydomain.local -u cluster -p password123 --details myimage:latest

## Answer:

D

# Question 7

**Question Type:** **MultipleChoice**

The development team wants to block Cross Site Scripting attacks from pods its environment

How should the team construct the CNAF policy to protect against this attack?

## Options:

**A)** create a Container CNAF policy, targeted at a specific resource, check the box for XSS attack protection and set the action to alert

**B)** create a Host CNAF policy targeted at a specific resource, check the box for XSS attack protection and set the action to 'prevent'

**C)** create a Container CNAF policy, targeted at a specific resource, check the box for XSS attack protection and set the action to prevent

**D)** create a Container CNAF policy, targeted at a specific resource, and they should set 'Explicitly allowed inbound IP sources' to the IP address of the pod.

## Answer:

B

# Question 8

**Question Type:** **MultipleChoice**

The Unusual protocol activity (Internal) network anomaly is generating too many alerts An administrator has been asked to tune it to the option that will generate the least number of events without disabling it entirely.

Which strategy should the administrator use to achieve this goal?

## Options:

**A)** Change the Training Threshold to Low

**B)** Disable the policy

**C)** Set the Alert Disposition to Conservative

**D)** Set Alert Disposition to Aggressive

## Answer:

A

# Question 9

**Question Type:** **MultipleChoice**

A customer has Prisma Cloud Enterprise and host Defenders deployed

What are two options that allow an administrator to upgrade Defenders'? (Choose two )

## Options:

**A)** generate a new DaemonSet file

**B)** auto deploy the Lambda Defender

**C)** click the update button in the web-interface

**D)** with auto-upgrade, the host Defender will auto-upgrade.

## Answer:

A, D

20%
DISCOUNT