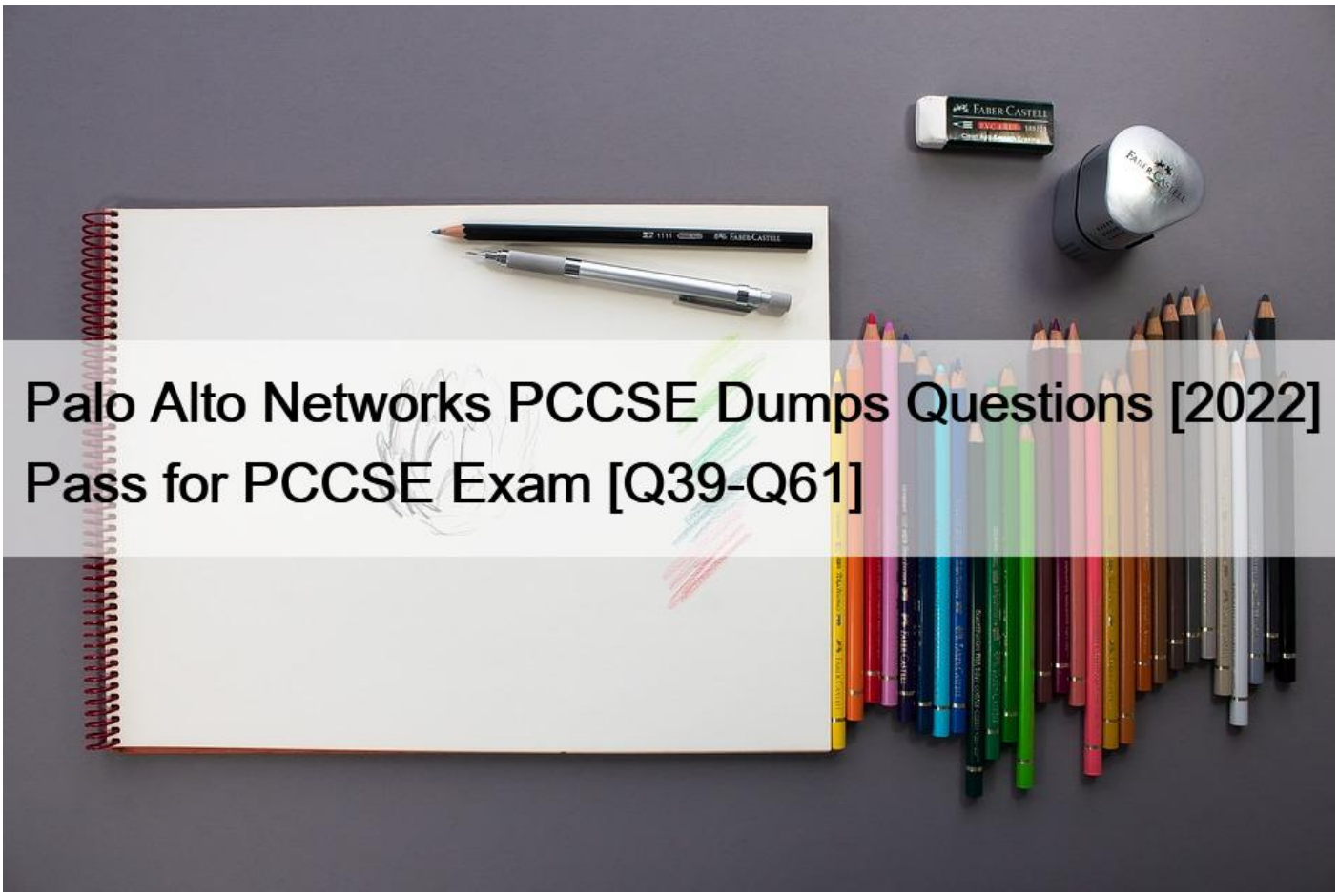
Palo Alto Networks PCCSE Dumps Questions [2022 Pass for PCCSE Exam [Q39-Q61



Palo Alto Networks PCCSE Dumps Questions [2022] Pass for PCCSE Exam
Updated Palo Alto Networks Study Guide PCCSE Dumps Questions

Q39. An administrator has a requirement to ingest all Console and Defender logs to Splunk.

Which option will satisfy this requirement in Prisma Cloud Compute?
* Enable the API settings for logging.
* Enable the CSV export in the Console.
* Enable the syslog option in the Console
* Enable the Splunk option in the Console.

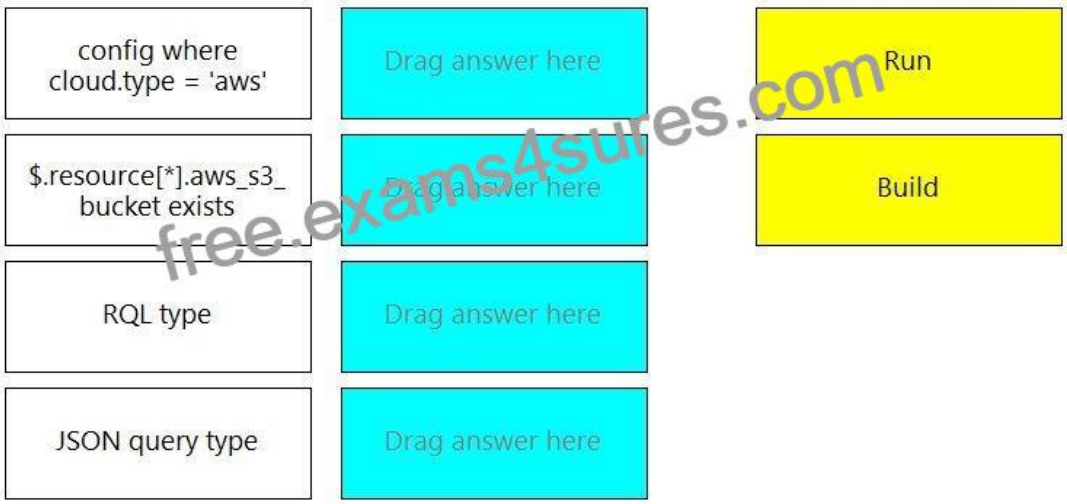
Q40. A security team has a requirement to ensure the environment is scanned for vulnerabilities. What are three options for configuring vulnerability policies? (Choose three.)
* individual actions based on package type
* output verbosity for blocked requests
* apply policy only when vendor fix is available
* individual grace periods for each severity level

* customize message on blocked requests

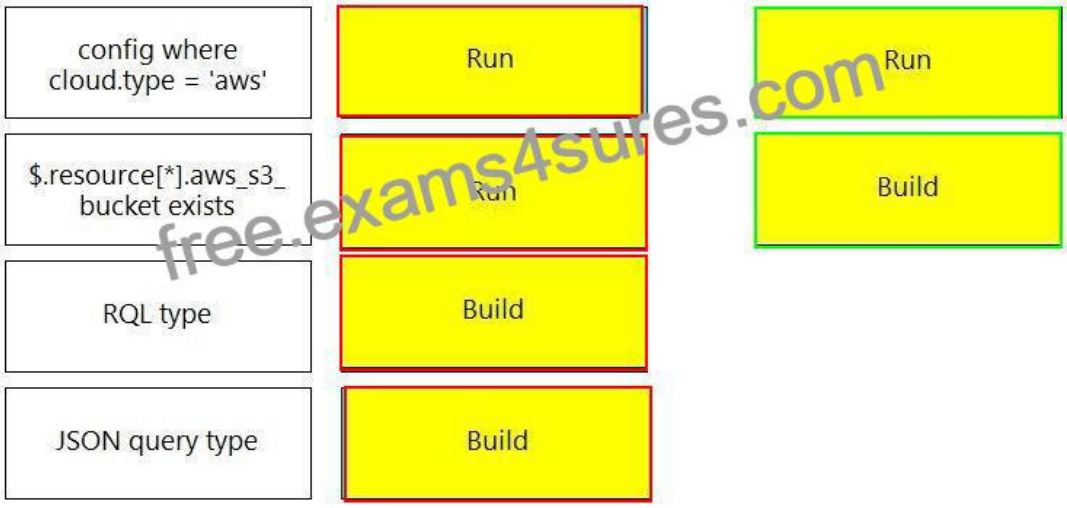
Q41. You wish to create a custom policy with build and run subtypes. Match the query types for each example.

(Select your answer from the pull-down list. Answers may be used more than once or not at all.)

Answer Area



Answer Area



Reference:

https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud-policies/create-a- policy.html

Q42. A customer has a requirement to terminate any Container from image topSecret:latest when a process named ransomWare is executed.

How should the administrator configure Prisma Cloud Compute to satisfy this requirement?
* set the Container model to manual relearn and set the default runtime rule to block for process protection.
* set the Container model to relearn and set the default runtime rule to prevent for process protection.

* add a new runtime policy targeted at a specific Container name, add ransomWare process into the denied process list, and set the action to “prevent”.
* choose “copy into rule” for the Container, add a ransomWare process into the denied process list, and set the action to “block”.

Q43. A customer has a requirement to restrict any container from resolving the name www.evil-url.com.

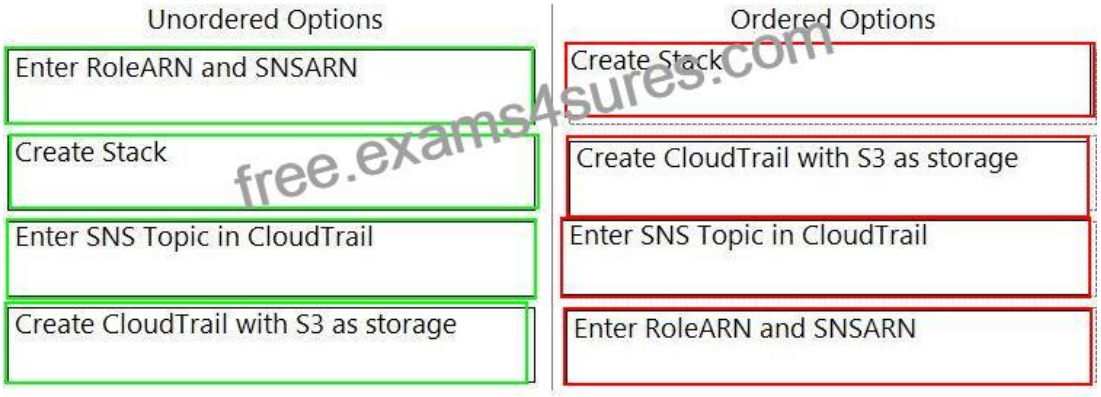
How should the administrator configure Prisma Cloud Compute to satisfy this requirement?
* Choose “copy into rule” for any Container, set www.evil-url.com as a blocklisted DNS name in the Container policy and set the policy effect to alert.
* Set www.evil-url.com as a blocklisted DNS name in the default Container runtime policy, and set the effect to block.
* Choose “copy into rule” for any Container, set www.evil-url.com as a blocklisted DNS name, and set the effect to prevent.
* Set www.evil-url.com as a blocklisted DNS name in the default Container policy and set the effect to prevent.

Q44. Which two attributes of policies can be fetched using API? (Choose two.)
* policy label
* policy signature
* policy mode
* policy violation

Q45. Order the steps involved in onboarding an AWS Account for use with Data Security feature.

Answer Area

Answer Area



Q46. A security team has a requirement to ensure the environment is scanned for vulnerabilities. What are three options for configuring vulnerability policies? (Choose three.)
* customize message on blocked requests
* individual actions based on package type
* output verbosity for blocked requests
* apply policy only when vendor fix is available
* individual grace periods for each severity level

Q47. Which method should be used to authenticate to Prisma Cloud Enterprise programmatically?
* single sign-on
* SAML
* basic authentication
* access key

Q48. Which statement accurately characterizes SSO Integration on Prisma Cloud?
* Prisma Cloud supports IdP initiated SSO, and its SAML endpoint supports the POST and GET methods.
* Okta, Azure Active Directory, PingID, and others are supported via SAML.
* An administrator can configure different Identity Providers (IdP) for all the cloud accounts that Prisma Cloud monitors.
* An administrator who needs to access the Prisma Cloud API can use SSO after configuration.

Q49. Which options show the steps required to upgrade Console when using projects?
* Upgrade all Supervisor Consoles Upgrade Central Console
* Upgrade Central Console

Upgrade Central Console Defenders
* Upgrade Defender Upgrade Central Console

Upgrade Supervisor Consoles
* Upgrade Central Console Upgrade all Supervisor Consoles

Q50. Which order of steps map a policy to a custom compliance standard?

(Drag the steps into the correct order of occurrence, from the first step to the last.)

Answer Area

Unordered Options	Ordered Options
Add the custom compliance standard from the drop-down menu	
Create the custom compliance standard	
Edit the Policy	
Click on Compliance Standards	

Answer Area

Unordered Options	Ordered Options
Add the custom compliance standard from the drop-down menu	Click on Compliance Standards
Create the custom compliance standard	Edit the Policy
Edit the Policy	Add the custom compliance standard from the drop-down menu
Click on Compliance Standards	Create the custom compliance standard

Q51. Which three types of classifications are available in the Data Security module? (Choose three.)
* Malicious IP
* Compliance standard
* Financial information
* Malware
* Personally identifiable information

Q52. Which three types of classifications are available in the Data Security module? (Choose three.)
* Compliance standard
* Financial information
* Malware
* Malicious IP
* Personally identifiable information

Q53. Which intensity setting for anomaly alerts is used for the measurement of 100 events over 30 days?
* High
* Medium
* Low
* Very High

Q54. A customer is interested in PCI requirements and needs to ensure that no privilege containers can start in the environment.

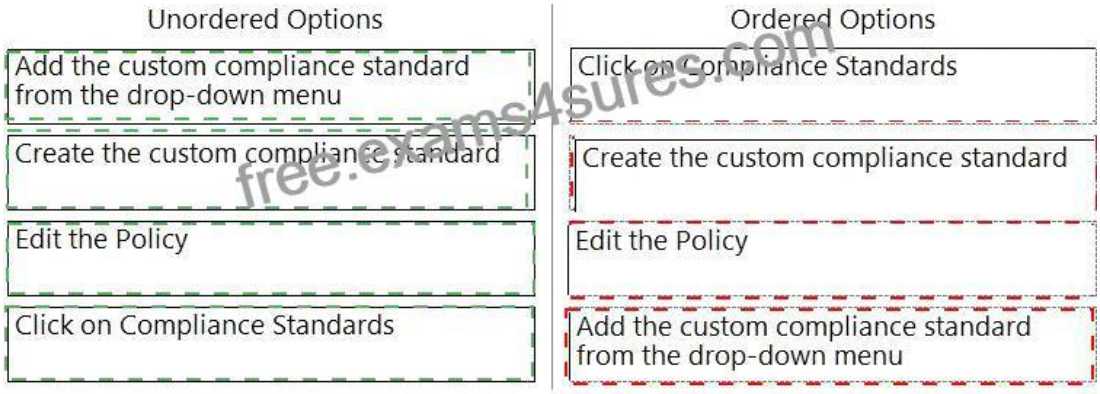
Which action needs to be set for “do not use privileged containers”?
* Prevent
* Alert
* Block
* Fail

Q55. Which order of steps map a policy to a custom compliance standard?

(Drag the steps into the correct order of occurrence, from the first step to the last.)

Answer Area

Answer Area



Explanation

1. click on compliance standard.

2. add custom compliance standard.

3. edit policies.

4. add compliance standard from drop-down menu

https://docs.prismacloudcompute.com/docs/enterprise_edition/compliance/custom_compliance_checks.html#cre

Q56. 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?

* 8084
* 443
* 8083
* 8081

Explanation

https://docs.prismacloudcompute.com/docs/compute_edition_21_04/tools/twistcli.html#connectivity-to-console

Q57. The security team wants to protect a web application container from an SQLi attack? Which type of policy should the administrator create to protect the container?
* Compliance
* Runtime
* CNAF
* CNNF

Q58. The development team wants to fail CI jobs where a specific CVE is contained within the image. How should the development team configure the pipeline or policy to produce this outcome?
* Set the specific CVE exception as an option in Jenkins or twistcli.
* Set the specific CVE exception as an option in Defender running the scan.
* Set the specific CVE exception as an option using the magic string in the Console.
* Set the specific CVE exception in Console’s CI policy.

Explanation

Reference tech docs:

https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/continuous_integration/se Vulnerability rules that target the build tool can allow specific vulnerabilities by creating an exception and setting the effect to ‘ignore’. Block them by creating an exception and setting hte effect to ‘fail’. For example, you could create a vulnerability rule that explicitly allows CVE-2018-1234 to suppress warnings in the scan results.

Q59. Which three Options are selectable in a CI policy for image scanning with Jenkins or twistcli? (Choose three.)
* Scope – Scans run on a particular host
* Grace Period
* Failure threshold
* Credential
* Apply rule only when vendor fixes are available

Q60. An administrator wants to install the Defenders to a Kubernetes cluster. This cluster is running the console on the default service endpoint and will be exporting to YAML Console Address SCONSOLE_ADDRESS Websocket Address SWEBSOCKHT_ADDRESS User: SADMIN USER Which command generates the YAML file for Defender install?

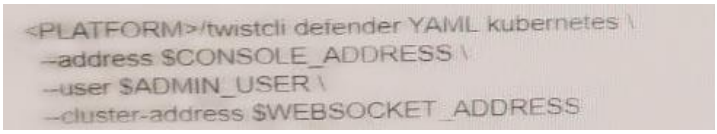
A)

```
<PLATFORM>/twistcli defender export kubernetes \
  --address $CONSOLE_ADDRESS \
  --user $ADMIN_USER \
  --cluster-address $WEBSOCKET_ADDRESS
```

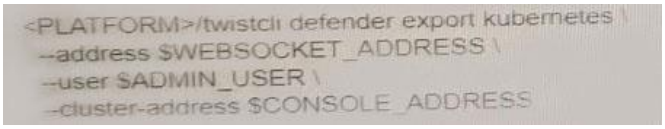
B)

```
<PLATFORM>/twistcli defender \
  --address $CONSOLE_ADDRESS \
  --user $ADMIN_USER \
  --cluster-address $CONSOLE_ADDRESS
```

C)



D)



* Option A
* Option B
* Option C
* Option D

Q61. What is the maximum number of access keys a user can generate in Prisma Cloud with a System Admin role?
* 1
* 2
* 3
* 4

Achieve Success in Actual PCCSE Exam PCCSE Exam Dumps:
https://www.exams4sures.com/Palo-Alto-Networks/PCCSE-practice-exam-dumps.html]