

- **Vendor:** Palo Alto Networks
- **Exam Code:** PCCSE
- **Exam Name:** Prisma Certified Cloud Security Engineer
- **New Updated Questions from [Braindump2go](#)**
- **(Updated in [February/2022](#))**

[Visit Braindump2go and Download Full Version PCCSE Exam Dumps](#)

**QUESTION 96**

A customer has configured the JIT, and the user created by the process is trying to log in to the Prisma Cloud console. The user encounters the following error message:

```
SamI Missing Required Auto Provision Attributes
Error occurred due to unexpected value of required field 'SAML_RESPONSE'
Expected Value: 'unavailable'
Actual Value: '[ROLE=[3ed546ec-a509-4774-b872-e55cb2cfd60b]]'.
```

What is the reason for the error message?

- A. The attribute name is not set correctly in JIT settings.
- B. The user does not exist.
- C. The user entered an incorrect password
- D. The role is not assigned for the user.

**Answer:** A

**Explanation:**

Reference:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CmZ4CAK>

**QUESTION 97**

What are the two ways to scope a CI policy for image scanning? (Choose two.)

- A. container name
- B. image name
- C. hostname
- D. image labels

**Answer:** BD

**Explanation:**

Reference: <https://www.optiv.com/insights/source-zero/blog/defending-against-container-threats-palo-alto-prisma-cloud>

**QUESTION 98**

Which policy type in Prisma Cloud can protect against malware?

- A. Data

[PCCSE Exam Dumps](#) [PCCSE Exam Questions](#) [PCCSE PDF Dumps](#) [PCCSE VCE Dumps](#)

<https://www.braindump2go.com/pccse.html>

- B. Config
- C. Network
- D. Event

**Answer:** A

**QUESTION 99**

If you are required to run in an air-gapped environment, which product should you install?

- A. Prisma Cloud Jenkins Plugin
- B. Prisma Cloud Compute Edition
- C. Prisma Cloud with self-hosted plugin
- D. Prisma Cloud Enterprise Edition

**Answer:** B

**Explanation:**

Reference: <https://docs.paloaltonetworks.com/prisma/prisma-cloud.html>

**QUESTION 100**

What is the maximum number of access keys a user can generate in Prisma Cloud with a System Admin role?

- A. 1
- B. 2
- C. 3
- D. 4

**Answer:** B

**QUESTION 101**

An administrator needs to detect and alert on any activities performed by a root account. Which policy type should be used?

- A. config-run
- B. config-build
- C. network
- D. audit event

**Answer:** C

**QUESTION 102**

One of the resources on the network has triggered an alert for a Default Config policy. Given the following resource JSON snippet:

```
{
  "password_enabled": "false",
  "password_last_used": "N/A",
  "user_creation_time": "2021-02-09T06:56:33Z",
  "access_key_1_active": true,
  "access_key_2_active": false,
  "cert_1_last_rotated": "N/A",
  "cert_2_last_rotated": "N/A",
  "password_last_changed": "N/A",
  "password_next_rotation": "N/A",
  "access_key_1_last_rotated": "2021-02-09T06:57:20Z",
}
```

Which RQL detected the vulnerability?

- A. `config from cloud.resource where api.name = 'aws-ecs-service' AND json.rule = launchType equals EC2 as Xr config from cloud.resource where api.name = 'aws-ecs-cluster' AND json.rule = status equals ACTIVE and registeredContainerInstancesCount equals 0 as Y: filter '0.X.clusterArn equals 1.Y.clusterArn': show Yr`
- B. `config from cloud.resource where cloud.type = 'aws' and api.name = 'aws-iam-get-credential-report' AND json.rule = '(access_key_1_active is true and access_key_1_last_rotated != N/A and _DateTime.ageInDays(access_key_1_last_rotated) > 90) or (access_key_2_active is true and access_key_2_last_rotated != N/A and _DateTime.ageInDays(access_key_2_last_rotated) > 90)'`
- C. `config from cloud.resource where cloud.type = 'aws' AND api.name = 'aws-ec2-describe-images' AND json.rule = image.platform contains windows and image.imageId contains ami-1e542176`
- D. `config from cloud.resource where cloud.type = 'aws' AND api.name = 'aws-ec2-describe-security-groups' AND json.rule = isShared is false and (ipPermissions[*].any((ipProtocol equals tcp or ipProtocol equals icmp or ipProtocol equals icmpv6 or ipProtocol equals udp) and (ipRanges[*].cidrIpV6`

**Answer: B**

**QUESTION 103**

A customer has multiple violations in the environment including:

- User namespace is enabled
- An LDAP server is enabled
- SSH root is enabled

Which section of Console should the administrator use to review these findings?

- A. Manage
- B. Vulnerabilities
- C. Radar
- D. Compliance

**Answer: A**

**QUESTION 104**

A customer has serverless functions that are deployed in multiple clouds. Which serverless cloud provider is covered by "overly permissive service access" compliance check?

- A. Alibaba
- B. GCP
- C. AWS
- D. Azure

**Answer: C**

**Explanation:**

Reference: <https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/compliance/serverless.html>

**QUESTION 105**

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?

- A. 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.
- B. Set www.evil-url.com as a blocklisted DNS name in the default Container runtime policy, and set the effect to block.
- C. Choose "copy into rule" for any Container, set www.evil-url.com as a blocklisted DNS name, and set the effect to prevent.
- D. Set www.evil-url.com as a blocklisted DNS name in the default Container policy and set the effect to prevent.

**Answer:** A

**QUESTION 106**

Which API calls can scan an image named myimage: latest with twistcli and then retrieve the results from Console?

- A. 

```
$ twistcli images scan \  
--address <COMPUTE_CONSOLE> \  
--user <COMPUTER_CONSOLE_USER> \  
--password <COMPUTER_CONSOLE_PASSWD> \  
--verbose \  
myimage: latest
```
- B. 

```
$ twistcli images scan \  
--address <COMPUTE_CONSOLE> \  
--user <COMPUTER_CONSOLE_USER> \  
--password <COMPUTER_CONSOLE_PASSWD> \  
--details \  
myimage: latest
```
- C. 

```
$ twistcli images scan \  
--address <COMPUTE_CONSOLE> \  
--user <COMPUTER_CONSOLE_USER> \  
--password <COMPUTER_CONSOLE_PASSWD> \  
myimage: latest
```
- D. 

```
$ twistcli images scan \  
--address <COMPUTE_CONSOLE> \  
--user <COMPUTER_CONSOLE_USER> \  
--password <COMPUTER_CONSOLE_PASSWD> \  
--console \  
myimage: latest
```

**Answer:** B

**Explanation:**

Reference: [https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/tools/twistcli\\_scan\\_images](https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/tools/twistcli_scan_images)

**QUESTION 107**

Given the following RQL:

event from cloud.audit\_logs where operation IN ('CreateCryptoKey', 'DestroyCryptoKeyVersion', 'v1.compute.disks.createSnapshot')

Which audit event snippet is identified?

- A. `"request": { "resource": "604173093072", "@type": "type.googleapis.com/google.iam.v1.SetIamPolicyRequest", "policy": { "bindings": [`
- B. `], "stateTransitionReason": "", "elasticGpuAssociations": [], "capacityReservationSpecification": { "capacityReservationPreference": "open" }, "elasticInferenceAcceleratorAssociations": []`
- C. `{ "Statement": [ { "Action": "*", "Effect": "Allow", "Resource": "*" } ], "Version": "2012-10-17"`
- D. `"payload": { "requestMetadata": { "callerSuppliedUserAgent": "Terraform/0.14.0 (+https://www.terraform.io) Terraform-Plugin-SDK/2.1.0 terraform-provider-google/3.50.0, gzip(gfe)", "callerIp": "34.265.226.252" }, "request": { "@type": "type.googleapis.com/compute.disks.createSnapshot" },`

**Answer: A**

**Explanation:**

Reference: <https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-rql-reference/rql-reference/event-query/event-query-attributes.html#id192IG500ES0>

### QUESTION 108

Which two of the following are required to be entered on the IdP side when setting up SSO in Prisma Cloud? (Choose two.)

- A. Username
- B. SSO Certificate
- C. Assertion Consumer Service (ACS) URL
- D. SP (Service Provider) Entity ID

**Answer: BD**

**Explanation:**

Reference: <https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/manage-prisma-cloud-administrators/setup-sso-integration-on-prisma-cloud.html>

### QUESTION 109

An administrator sees that a runtime audit has been generated for a container.

The audit message is:

`"/bin/ls launched and is explicitly blocked in the runtime rule. Full command: ls -latr"`

Which protection in the runtime rule would cause this audit?

- A. Networking
- B. File systems
- C. Processes
- D. Container

**Answer: D**

**Explanation:**

Reference: [https://docs.paloaltonetworks.com/prisma/prisma-cloud/21-04/prisma-cloud-compute-edition-admin/runtime\\_defense/runtime\\_audits.html](https://docs.paloaltonetworks.com/prisma/prisma-cloud/21-04/prisma-cloud-compute-edition-admin/runtime_defense/runtime_audits.html)

### QUESTION 110

Which data security default policy is able to scan for vulnerabilities?

- A. Objects containing Vulnerabilities
- B. Objects containing Threats
- C. Objects containing Malware
- D. Objects containing Exploits

**Answer: A**

[PCCSE Exam Dumps](#) [PCCSE Exam Questions](#) [PCCSE PDF Dumps](#) [PCCSE VCE Dumps](#)

<https://www.braindump2go.com/pccse.html>

**Explanation:**

Reference: [https://docs.paloaltonetworks.com/prisma/prisma-cloud/21-04/prisma-cloud-compute-edition-admin/vulnerability\\_management/vuln\\_management\\_rules.html](https://docs.paloaltonetworks.com/prisma/prisma-cloud/21-04/prisma-cloud-compute-edition-admin/vulnerability_management/vuln_management_rules.html)

**QUESTION 111**

Given the following audit event activity snippet:

```
{
  "payload": {
    "requestMetadata": {
      "callerSuppliedUserAgent": "google-cloud-sdk gcloud/274.0.1 command/gcloud.compute.firewall-rules.delete invocation-
id/edda7aa325264545a4322f916ec15791 environment/None environment-version/None interactive/False from-script/False python/2.7.15
term/ (Linux 4.14.186-146.268.amzn2.x86_64).gslp(gfe)",
      "callerip": "52.87.62.40"
    },
    "request": {
      "@type": "type.googleapis.com/compute.firewalls.delete"
    }
  }
}
```

Which RQL will be triggered by the audit event?

- A. event from cloud.audit\_logs where operation IN ('cloudsql.instances.update', 'cloudsql.sslCerts.create', 'cloudsql.instances.create', 'cloudsql.instances.delete')
- B. event from cloud.audit\_logs where operation IN ('storage.buckets.create', 'storage.setIamPermissions', 'storage.buckets.delete')
- C. event from cloud.audit\_logs where operation IN ('AuthorizeSecurityGroupEgress', 'AuthorizedSecurityGroupIngress', 'CreateVpc', 'DeleteFlowLogs', 'DeleteVpc', 'ModifyVpcAttribute', 'RevokeSecurityGroupIngress')
- D. event from cloud.audit\_logs where operation IN ('vl.compute.networks.delete', 'beta.compute.networks.insert', 'vl.compute.routes.delete', 'vl.compute.firewalls.insert', 'vl.compute.firewalls.delete')

**Answer: B**

**QUESTION 112**

Which three fields are mandatory when authenticating the Prisma Cloud plugin in the IntelliJ application? (Choose three.)

- A. Secret Key
- B. Prisma Cloud API URL
- C. Tags
- D. Access Key
- E. Asset Name

**Answer: ABD**

**Explanation:**

Reference: <https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud-devops-security/use-the-prisma-cloud-plugin-for-intellij.html>

**QUESTION 113**

Which of the following are correct statements regarding the use of access keys? (Choose two.)

- A. Access keys must have an expiration date
- B. Up to two access keys can be active at any time
- C. System Admin can create access key for all users
- D. Access keys are used for API calls

**Answer: BC**

**QUESTION 114**

Given the following RQL:

```
event from cloud.audit_logs where operation IN ('vl.compute.urlMaps.update', 'vl.compute.urlMaps.delete',
'vl.compute.backendServices.delete', 'vl.compute.backendBuckets.delete', 'vl.compute.backendServices.update',
'vl.compute.globalForwardingRules.delete', 'vl.compute.urlMaps.delete', 'vl.compute.targetHttpsProxies.delete',
'vl.compute.targetHttpsProxies.setSslPolicy', 'vl.compute.targetHttpsProxies.setSslCertificates')
```

**[PCCSE Exam Dumps](#) **[PCCSE Exam Questions](#) **[PCCSE PDF Dumps](#) **[PCCSE VCE Dumps](#)********

**<https://www.braindump2go.com/pccse.html>**

Which audit event snippet is identified by the RQL?

- A. `"eventTime": "2021-05-19T14:34:08Z", "eventSource": "iam.amazonaws.com", "eventName": "AttachRolePolicy", "awsRegion": "us-east-1"`
- B. `"payload": { > "requestMetadata": { "callerSuppliedUserAgent": "Terraform/0.14.0 (+https://www.terraform.io) Terraform-Plugin-SDK/2.1.0 terraform-provider-google/3.50.0,qzip(gfe)", "callerIp": "34.235.226.252" }, "request": { "@type": "type.googleapis.com/compute.backendServices.delete"`
- C. `"resource": "projects/_/buckets/gvtest110221", "permission": "storage.buckets.setIamPolicy", "resourceAttributes": {}, "granted": true`
- D. `"userIdentity": { "type": "Root", "principalId": "6849955112A19", "arn": "arn:aws:iam::6849955112A9:root", "accountId": "689995514A219", "accessKeyId": ""`

**Answer: D**

### QUESTION 115

The development team is building pods to host a web front end, and they want to protect these pods with an application firewall.

Which type of policy should be created to protect this pod from Layer7 attacks?

- A. The development team should create a WAAS rule for the host where these pods will be running.
- B. The development team should create a WAAS rule targeted at all resources on the host.
- C. The development team should create a runtime policy with networking protections.
- D. The development team should create a WAAS rule targeted at the image name of the pods.

**Answer: B**

**Explanation:**

Reference: <https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/waas/waas-intro.html>

### QUESTION 116

A manager informs the SOC that one or more RDS instances have been compromised and the SOC needs to make sure production RDS instances are NOT publicly accessible.

Which action should the SOC take to follow security best practices?

- A. Enable "AWS S3 bucket is publicly accessible" policy and manually remediate each alert.
- B. Enable "AWS RDS database instance is publicly accessible" policy and for each alert, check that it is a production instance, and then manually remediate.
- C. Enable "AWS S3 bucket is publicly accessible" policy and add policy to an auto-remediation alert rule.
- D. Enable "AWS RDS database instance is publicly accessible" policy and add policy to an auto-remediation alert rule.

**Answer: D**

### QUESTION 117

An administrator wants to enforce a rate limit for users not being able to post five (5) .tar.gz files within five (5) seconds. What does the administrator need to configure?

- A. A ban for DoS protection with an average rate of 5 and file extensions match on .tar.gz on WAAS
- B. A ban for DoS protection with a burst rate of 5 and file extensions match on .tar.gz on CNMF
- C. A ban for DoS protection with a burst rate of 5 and file extensions match on .tar.gz on WAAS
- D. A ban for DoS protection with an average rate of 5 and file extensions match on .tar.gz on CNMF

**Answer: C**

**QUESTION 118**

What is an automatically correlated set of individual events generated by the firewall and runtime sensors to identify unfolding attacks?

- A. policy
- B. incident
- C. audit
- D. anomaly

**Answer: B**

**Explanation:**

Reference: [https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/runtime\\_defense/incident\\_explorer.html](https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/runtime_defense/incident_explorer.html)

**QUESTION 119**

A customer wants to monitor the company's AWS accounts via Prisma Cloud, but only needs the resource configuration to be monitored for now.

Which two pieces of information do you need to onboard this account? (Choose two.)

- A. Cloudtrail
- B. Subscription ID
- C. Active Directory ID
- D. External ID
- E. Role ARN

**Answer: AE**

**Explanation:**

Reference: <https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/connect-your-cloud-platform-to-prisma-cloud/onboard-your-aws-account/add-aws-organization-to-prisma-cloud.html>

**QUESTION 120**

An administrator for Prisma Cloud needs to obtain a graphical view to monitor all connections, including connections across hosts and connections to any configured network objects. Which setting does the administrator enable or configure to accomplish this task?

- A. ADEM
- B. WAAS Analytics
- C. Telemetry
- D. Cloud Native Network Firewall
- E. Host Insight

**Answer: D**

**Explanation:**

Reference: [https://docs.paloaltonetworks.com/prisma/prisma-cloud/21-04/prisma-cloud-compute-edition-admin/firewalls/cnnf\\_self\\_hosted.html](https://docs.paloaltonetworks.com/prisma/prisma-cloud/21-04/prisma-cloud-compute-edition-admin/firewalls/cnnf_self_hosted.html)

**QUESTION 121**

Which two fields are required to configure SSO in Prisma Cloud? (Choose two.)

- A. Prisma Cloud Access SAML URL
- B. Identity Provider Issuer
- C. Certificate
- D. Identity Provider Logout URL

**Answer: AB**

**Explanation:**

[PCCSE Exam Dumps](#) [PCCSE Exam Questions](#) [PCCSE PDF Dumps](#) [PCCSE VCE Dumps](#)

<https://www.braindump2go.com/pccse.html>



Reference: <https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/manage-prisma-cloud-administrators/setup-sso-integration-on-prisma-cloud/setup-sso-integration-on-prisma-cloud-for-microsoft-azure-active-directory.html>

**QUESTION 122**

Which two IDE plugins are supported by Prisma Cloud as part of its DevOps Security? (Choose two.)

- A. BitBucket
- B. Visual Studio Code
- C. CircleCI
- D. IntelliJ

**Answer:** AC

**Explanation:**

Reference: <https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud-devops-security/prisma-cloud-plugins.html>

**QUESTION 123**

Which two CI/CD plugins are supported by Prisma Cloud as part of its DevOps Security? (Choose two.)

- A. BitBucket
- B. Visual Studio Code
- C. CircleCI
- D. IntelliJ

**Answer:** CD

**Explanation:**

Reference: <https://www.paloaltonetworks.com/blog/prisma-cloud/cloud-devops-plugins/>

**QUESTION 124**

Given the following JSON query:

```
$.resource[*].aws_s3_bucket exists
```

Which tab is the correct place to add the JSON query when creating a Config policy?

- A. Details
- B. Compliance Standards
- C. Remediation
- D. Build Your Rule (Run tab)
- E. Build Your Rule (Build tab)

**Answer:** C

**Explanation:**

Reference: [https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-policy-reference/configuration-policies/configuration-policies-build-phase/amazon-web-services-configuration-policies/policy\\_630d3779-d932-4fbf-9cce-6e8d793c6916.html](https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-policy-reference/configuration-policies/configuration-policies-build-phase/amazon-web-services-configuration-policies/policy_630d3779-d932-4fbf-9cce-6e8d793c6916.html)

**QUESTION 125**

Which two attributes of policies can be fetched using API? (Choose two.)

- A. policy label
- B. policy signature
- C. policy mode
- D. policy violation

**Answer:** AD

**Explanation:**

[PCCSE Exam Dumps](#) [PCCSE Exam Questions](#) [PCCSE PDF Dumps](#) [PCCSE VCE Dumps](#)

<https://www.braindump2go.com/pccse.html>



**Braindump2go Guarantee All Exams 100% Pass**  
**One Time!**

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

[PCCSE Exam Dumps](#) [PCCSE Exam Questions](#) [PCCSE PDF Dumps](#) [PCCSE VCE Dumps](#)

<https://www.braindump2go.com/pccse.html>