



- Expert Verified, Online, **Free**.



## **CERTIFICATION TEST**

- [CertificationTest.net](https://CertificationTest.net) - Cheap & Quality Resources With Best Support

Given a default deployment of Console, a customer needs to identify the alerted compliance checks that are set by default.  
Where should the customer navigate in Console?

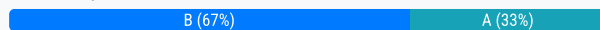
- A. Monitor > Compliance
- B. Defend > Compliance
- C. Manage > Compliance
- D. Custom > Compliance

**Suggested Answer: B**

Reference:

[https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/compliance/manage\\_compliance.html](https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/compliance/manage_compliance.html)

Community vote distribution



🗳️ 👤 **Iyan\_w** 6 months, 4 weeks ago

**Selected Answer: B**

If default set is done, you can check compliance set in Defend > Compliance.

Monitor section is for scanned result.

upvoted 1 times

🗳️ 👤 **JohnOrtiz** 1 year, 1 month ago

**Selected Answer: B**

This is B

upvoted 2 times

🗳️ 👤 **FS9** 1 year, 3 months ago

**Selected Answer: B**

It's asking for checks(rules) not for alerts against those checks.

upvoted 3 times

🗳️ 👤 **Chiquitabandita** 1 year, 3 months ago

B <https://docs.prismacloud.io/en/enterprise-edition/assets/pdf/prisma-cloud-compute-edition-admin-22-06.pdf>

upvoted 2 times

🗳️ 👤 **JohnFo17** 1 year, 4 months ago

**Selected Answer: A**

Answer is A

upvoted 1 times

🗳️ 👤 **Mozak** 2 years ago

Answer is A

upvoted 1 times

🗳️ 👤 **Spippolo** 2 years ago

**Selected Answer: A**

I Think A.

A. Monitor > Compliance

upvoted 1 times

🗳️ 👤 **kumar\_57** 2 years, 3 months ago

It's asking for checks(rules) not for alerts against those checks.

upvoted 1 times

🗳️ 👤 **SpanwEvil** 2 years, 6 months ago

**Selected Answer: B**

[https://docs.paloaltonetworks.com/prisma/prisma-cloud/22-06/prisma-cloud-compute-edition-admin/compliance/manage\\_compliance](https://docs.paloaltonetworks.com/prisma/prisma-cloud/22-06/prisma-cloud-compute-edition-admin/compliance/manage_compliance)

upvoted 2 times

🗨️ 👤 **damc** 2 years, 11 months ago

**Selected Answer: B**

[https://docs.paloaltonetworks.com/prisma/prisma-cloud/22-06/prisma-cloud-compute-edition-admin/compliance/manage\\_compliance](https://docs.paloaltonetworks.com/prisma/prisma-cloud/22-06/prisma-cloud-compute-edition-admin/compliance/manage_compliance)

upvoted 2 times

🗨️ 👤 **oscarbest** 3 years, 3 months ago

**Selected Answer: A**

If you want to check the alerted compliance checks, you should go to Monitor > Compliance

upvoted 2 times

🗨️ 👤 **piipo** 3 years, 3 months ago

B

The question is that you want to see the default settings, not the alerts you are getting.

upvoted 3 times

Which container scan is constructed correctly?

- A. `twistcli images scan -u api -p api --address https://us-west1.cloud.twistlock.com/us-3-123456789 --container myimage/latest`
- B. `twistcli images scan --docker-address https://us-west1.cloud.twistlock.com/us-3-123456789 myimage/latest`
- C. `twistcli images scan -u api -p api --address https://us-west1.cloud.twistlock.com/us-3-123456789 --details myimage/latest`
- D. `twistcli images scan -u api -p api --docker-address https://us-west1.cloud.twistlock.com/us-3-123456789 myimage/latest`

**Suggested Answer: B**

Community vote distribution

C (100%)

🗳️ **[Removed]** **Highly Voted** 👍 3 years, 4 months ago

Correct answer is C. --docker-address is a path not a url.  
upvoted 10 times

🗳️ **JohnOrtiz** **Most Recent** 🕒 7 months, 1 week ago

**Selected Answer: C**

<https://docs.prismacloud.io/en/classic/compute-admin-guide/tools/twistcli-scan-images>  
upvoted 1 times

🗳️ **JohnOrtiz** 7 months, 1 week ago

The correct is C  
upvoted 1 times

🗳️ **FS9** 9 months, 1 week ago

**Selected Answer: C**

Correct answer is C. --docker-address is a path not a url.  
upvoted 1 times

🗳️ **Spippolo** 1 year, 6 months ago

**Selected Answer: C**

C.

[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)  
upvoted 2 times

🗳️ **Spippolo** 1 year, 6 months ago

C.

[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)  
upvoted 2 times

🗳️ **kumar\_57** 1 year, 9 months ago

C is correct option. If your Docker socket isn't in the default location then use the --docker-address option to tell twistcli where to find it:  
upvoted 1 times

🗳️ **SpanwEvil** 2 years ago

**Selected Answer: C**

[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)

--docker-address cannot point to Prisma Cloud Console and (B and D) --containers doesn't exist in the command line (A).  
upvoted 1 times

🗳️ **walala** 2 years, 1 month ago

The correct is C  
upvoted 1 times

🗳️ **[Removed]** 3 years, 4 months ago

[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)  
upvoted 2 times

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?

- A. Set the specific CVE exception as an option in Jenkins or twistcli.
- B. Set the specific CVE exception as an option in Defender running the scan.
- C. Set the specific CVE exception as an option using the magic string in the Console.
- D. Set the specific CVE exception in Console's CI policy.

**Suggested Answer: C**

Community vote distribution

D (100%)

🗳️ **wandc** Highly Voted 2 years, 11 months ago

Answer is D

upvoted 12 times

🗳️ **JohnOrtiz** Most Recent 7 months, 1 week ago

**Selected Answer: D**

The Correct Option is D

upvoted 2 times

🗳️ **JohnFo17** 10 months ago

**Selected Answer: D**

[https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?](https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u000000oMkpCAE&lang=en_US%E2%80%A9&refURL=http%3A%2F%2Fknowledgebase.paloaltonetworks.com%2FKCSArticleDetail)

[id=kA14u000000oMkpCAE&lang=en\\_US%E2%80%A9&refURL=http%3A%2F%2Fknowledgebase.paloaltonetworks.com%2FKCSArticleDetail](https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u000000oMkpCAE&lang=en_US%E2%80%A9&refURL=http%3A%2F%2Fknowledgebase.paloaltonetworks.com%2FKCSArticleDetail)

upvoted 1 times

🗳️ **assadhashmi** 1 year, 4 months ago

**Selected Answer: D**

Answer is D

upvoted 1 times

🗳️ **Spippolo** 1 year, 6 months ago

**Selected Answer: D**

D.

By configuring the CI policy in Palo Alto Networks' Console, the development team can define rules and conditions for the CI (Continuous Integration) process.

upvoted 2 times

🗳️ **kumar\_57** 1 year, 9 months ago

The correct option is D

upvoted 1 times

🗳️ **vimal1206** 2 years, 2 months ago

Answer is clearly D

upvoted 2 times

🗳️ **deeee** 3 years, 3 months ago

which answer is correct?

upvoted 1 times

🗳️ **[Removed]** 3 years, 4 months ago

Reference tech docs: [https://docs.paloaltonetworks.com/prisma-cloud/prisma-cloud-admin-compute/continuous\\_integration/set\\_policy\\_ci\\_plugins.html](https://docs.paloaltonetworks.com/prisma-cloud/prisma-cloud-admin-compute/continuous_integration/set_policy_ci_plugins.html)

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 the effect to 'fail'. For example, you could create a vulnerability rule that explicitly allows CVE-2018-1234 to suppress warnings in the scan results.

upvoted 1 times

Which three types of classifications are available in the Data Security module? (Choose three.)

- A. Personally identifiable information
- B. Malicious IP
- C. Compliance standard
- D. Financial information
- E. Malware

**Suggested Answer:** CDE

Community vote distribution

ADE (100%)

 **waewae** Highly Voted 3 years, 1 month ago

Think it's A,D and E.

<https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud-data-security.html>

upvoted 9 times

 **JohnOrtiz** Most Recent 7 months, 1 week ago

Selected Answer: ADE

This is the correct Option

upvoted 2 times

 **JohnFo17** 10 months ago

Selected Answer: ADE

<https://docs.prismacloud.io/en/classic/cspm-admin-guide/prisma-cloud-data-security/monitor-data-security-scan-prisma-cloud/data-security-settings#data-security-settings> Step 6

upvoted 1 times

 **Spippolo** 1 year, 6 months ago

Selected Answer: ADE

Palo Alto Networks' Enterprise DLP service and provides data classification that includes built-in data profiles with data patterns that match sensitive information such as PII, health care, financial information and Intellectual Property. In addition to protecting your confidential and sensitive data, your data is also protected against threats—known and unknown (zero-day) malware—using the Palo Alto Networks' WildFire service.

upvoted 4 times

 **kumar\_57** 1 year, 9 months ago

The correct answer is A,D and E

upvoted 1 times

 **peqwilber** 2 years, 10 months ago

ADE, correct

PII (A), health care, financial information (D) and Intellectual Property. In addition to protecting your confidential and sensitive data, your data is also protected against threats—known and unknown (zero-day) malware(E)—using the Palo Alto Networks' WildFire service.

upvoted 3 times



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?

- A. set the Container model to manual relearn and set the default runtime rule to block for process protection.
- B. set the Container model to relearn and set the default runtime rule to prevent for process protection.
- C. 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.
- D. choose copy into rule for the Container, add a ransomWare process into the denied process list, and set the action to block.

**Suggested Answer: C**

Community vote distribution

D (100%)

🗳️ 👤 **[Removed]** Highly Voted 3 years, 9 months ago

Correct answer is D. Block terminate container. Prevent only terminate process.  
upvoted 11 times

🗳️ 👤 **Phoenix** 2 years, 10 months ago

Bro have you given this exam ? Did you passed ? Any link for Dump and study  
upvoted 1 times

🗳️ 👤 **elzm** Most Recent 11 months, 4 weeks ago

Prevent – Defender stops the process (and just the process) that violates your policy from executing.

Block – Defender stops the entire container if a process that violates your policy attempts to run.

D.

<https://docs.prismacloud.io/en/classic/compute-admin-guide/runtime-defense/runtime-defense-containers#effect>  
upvoted 1 times

🗳️ 👤 **JohnOrtiz** 1 year, 1 month ago

Selected Answer: D

Option D is the correct answer  
upvoted 1 times

🗳️ 👤 **steven\_xie2** 1 year, 7 months ago

Correct answer is D  
upvoted 1 times

🗳️ 👤 **Spippolo** 2 years ago

Selected Answer: D

D. Block terminate container  
upvoted 1 times

🗳️ 👤 **kumar\_57** 2 years, 3 months ago

The correct option is D because 'prevent' just tells you that operation is not permitted but on enabling 'block', it will terminate your container.  
upvoted 1 times

🗳️ 👤 **Shivam\_ayir** 2 years, 3 months ago

D is the right option. Prevent only blocks containers from running processes, whereas the requirement is to terminate the container, which is only possible by Block. [https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/runtime\\_defense/runtime\\_defense\\_containers](https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/runtime_defense/runtime_defense_containers)  
upvoted 1 times

🗳️ 👤 **NodummyIQ** 2 years, 4 months ago

Option C is the correct answer. The administrator should add a new runtime policy targeted at a specific Container name, add the ransomWare process into the denied process list, and set the action to "prevent". This will prevent the ransomWare process from being executed in the Container image topSecret:latest.

upvoted 2 times

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

- A. To retrieve Prisma Cloud Console images using basic auth: 1. Access registry.paloaltonetworks.com, and authenticate using 'docker login'. 2. Retrieve the Prisma Cloud Console images using 'docker pull'.
- B. To retrieve Prisma Cloud Console images using basic auth: 1. Access registry.twistlock.com, and authenticate using 'docker login'. 2. Retrieve the Prisma Cloud Console images using 'docker pull'.
- C. To retrieve Prisma Cloud Console images using URL auth: 1. Access registry-url-auth.twistlock.com, and authenticate using the user certificate. 2. Retrieve the Prisma Cloud Console images using 'docker pull'.
- D. To retrieve Prisma Cloud Console images using URL auth: 1. Access registry-auth.twistlock.com, and authenticate using the user certificate. 2. Retrieve the Prisma Cloud Console images using 'docker pull'.


**Suggested Answer: B**

Reference:

[https://docs.twistlock.com/docs/compute\\_edition/install/twistlock\\_container\\_images.html#retrieving-prisma-cloud-images-using-basic-auth](https://docs.twistlock.com/docs/compute_edition/install/twistlock_container_images.html#retrieving-prisma-cloud-images-using-basic-auth)

Community vote distribution

B (100%)

 **Spippolo** 6 months, 3 weeks ago

**Selected Answer: B**

B.

Authenticate using docker login or podman login, then retrieve the Prisma Cloud images using docker pull or podman pull. For basic authorization, the registry is accessible at registry.twistlock.com.

upvoted 2 times

 **PRANAVMHATRE** 8 months, 3 weeks ago

Retrieve Prisma Cloud images with a single command by embedding your access token into the registry URL. For URL authorization, the registry is accessible at registry-auth.twistlock.com.


By embedding your access token into the registry URL, you only need to run docker pull or podman pull. The docker login or podman login command isn't required.

As per above line User cert is not available however access token can be used.

So answer should be B only.

Kindly confirm who has cleared the exam.

upvoted 1 times

 **kumar\_57** 9 months, 1 week ago

The correct option is B. It supports token-based authorization not certificate based while using url-authorization method for accessing images in the cloud registry.

upvoted 1 times

 **Ravi221** 1 year, 1 month ago

Answer D

please ignore my earlier comment

[https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/install/twistlock\\_container\\_images](https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/install/twistlock_container_images)

upvoted 1 times

 **Ravi221** 1 year, 3 months ago

Answer D,

[https://docs.twistlock.com/docs/compute\\_edition/install/twistlock\\_container\\_images.html#retrieving-prisma-cloud-images-using-basic-auth](https://docs.twistlock.com/docs/compute_edition/install/twistlock_container_images.html#retrieving-prisma-cloud-images-using-basic-auth)

upvoted 1 times


Which two statements are true about the differences between build and run config policies? (Choose two.)

- A. Run and Network policies belong to the configuration policy set.
- B. Build and Audit Events policies belong to the configuration policy set.
- C. Run policies monitor resources, and check for potential issues after these cloud resources are deployed.
- D. Build policies enable you to check for security misconfigurations in the IaC templates and ensure that these issues do not get into production.
- E. Run policies monitor network activities in your environment, and check for potential issues during runtime.

**Suggested Answer: BE**

Community vote distribution

CD (100%)

 **SakeBomb** Highly Voted 1 year, 11 months ago

Answer is C and D

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

upvoted 11 times

 **peqwilber** Highly Voted 1 year, 10 months ago

Config—Configuration policies monitor your resource configurations for potential policy violations. Configuration policies on Prisma Cloud can be of two sub-types—Build and Run—to enable a layered approach. Build policies enable you to check for security misconfigurations in the IaC templates and ensure that these issues do not make their way into production (D). The Run policies monitor resources and check for potential issues once these cloud resources are deployed (C). See Create a Configuration Policy.

upvoted 5 times

 **Spippolo** Most Recent 6 months, 3 weeks ago

**Selected Answer: CD**

Options C and D are the correct statements about the differences between build and run config policies.

upvoted 1 times

A security team notices a number of anomalies under Monitor > Events. The incident response team works with the developers to determine that these anomalies are false positives.

What will be the effect if the security team chooses to Relearn on this image?

- A. The model is deleted, and Defender will relearn for 24 hours.
- B. The anomalies detected will automatically be added to the model.
- C. The model is deleted and returns to the initial learning state.
- D. The model is retained, and any new behavior observed during the new learning period will be added to the existing model.


**Suggested Answer: B**

Reference:

<https://digitalguardian.com/blog/five-steps-incident-response>

Community vote distribution

D (100%)

 **[Removed]** Highly Voted 3 years, 3 months ago

Correct is D.

[https://docs.prismacloudcompute.com/docs/compute\\_edition\\_21\\_04/runtime\\_defense/runtime\\_defense\\_containers.html#learning-mode](https://docs.prismacloudcompute.com/docs/compute_edition_21_04/runtime_defense/runtime_defense_containers.html#learning-mode)  
upvoted 7 times

 **df1** Highly Voted 3 years, 2 months ago

According to the reference, I think correct answer is D.  
upvoted 5 times

 **JohnOrtiz** Most Recent 7 months, 1 week ago

**Selected Answer: D**

You can relearn an existing model by clicking the Relearn button in the Actions menu. This is an additive process, so any existing static and behavioral modeling remain in place.  
upvoted 1 times

 **Spippolo** 1 year, 6 months ago

**Selected Answer: D**

Extend Learning: You can relearn an existing model by clicking the Extend Learning button in the Actions menu. This is an additive process, so any existing static and behavioral modeling remain in place.

Manual Learning: You can manually alter the duration of learning at any time by starting and stopping the Manual Learning option in the Actions menu. This should be done with discretion because the model may or may not complete within the time-period due to manual interruption. There is no time limit for manual learning. It depends on the user's selection.


upvoted 1 times

 **kumar\_57** 1 year, 9 months ago

The correct option is D. Relearn: You can relearn an existing model by clicking the Relearn button in the Actions menu. This is an additive process, so any existing static and behavioral modeling remain in place.  
upvoted 1 times


 **TheIronSheik** 1 year, 9 months ago

Another study guide I'm looking at has this same question and their answer is A. just wanted to share.  
upvoted 1 times

 **vaisat** 2 years, 1 month ago

I would say C.

D is for "Extend learning" option. The keyword in this question is "relearn" hence answer C.  
upvoted 1 times

 **vaisat** 2 years, 1 month ago

DISREGARD my above message ^^^

D is correct.

upvoted 1 times

🗨️ 👤 **Ravi221** 2 years, 3 months ago

Correct answer is D,

[https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/runtime\\_defense/runtime\\_defense\\_containers](https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/runtime_defense/runtime_defense_containers)

upvoted 2 times

🗨️ 👤 **ssukum** 2 years, 3 months ago

Correct answer is D

upvoted 1 times

🗨️ 👤 **j1518** 2 years, 4 months ago

**Selected Answer: D**

Correct answer is D

upvoted 1 times

A customer does not want alerts to be generated from network traffic that originates from trusted internal networks. Which setting should you use to meet this customer's request?

- A. Trusted Login IP Addresses
- B. Anomaly Trusted List
- C. Trusted Alert IP Addresses
- D. Enterprise Alert Disposition

**Suggested Answer: C**

Reference:

<https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/manage-prisma-cloud-alerts/trusted-ip-addresses-on-prisma-cloud.html>

Community vote distribution

C (100%)

 **ominator** Highly Voted 1 year, 9 months ago

**Selected Answer: C**

Trusted Alert IP Addresses—If you have internal networks that connect to your public cloud infrastructure, you can add these IP address ranges (or CIDR blocks) as trusted on Prisma Cloud. When you add IP addresses to this list, you can create a label to identify your internal networks that are not in the private IP address space to make alert analysis easier.

Key words in the above is internal networks.

upvoted 6 times

 **Spippolo** Most Recent 6 months, 3 weeks ago

**Selected Answer: C**

B --> Anomaly Trusted List—Exclude trusted IP addresses when conducting tests for PCI compliance or penetration testing on your network. Any addresses included in this list do not generate alerts against the Prisma Cloud Anomaly Policies that detect unusual network activity such as the policies that detect internal port scan and port sweep activity, which are enabled by default.

C --> Trusted Alert IP Addresses—If you have internal networks that connect to your public cloud infrastructure, you can add these IP address ranges (or CIDR blocks) as trusted ...

Prisma Cloud default network policies that look for internet exposed instances also do not generate alerts when the source IP address is included in the trusted IP address list and the account hijacking anomaly policy filters out activities from known IP addresses. Also, when you use RQL to query network traffic, you can filter out traffic from known networks that are included in the trusted IP address list.

upvoted 1 times

 **kumar\_57** 9 months, 1 week ago

C is the correct answer. Anomaly Trusted List is used for penetration testing which is within the system not at the customer-end.

<https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/manage-prisma-cloud-alerts/trusted-ip-addresses-on-prisma-cloud>

upvoted 1 times

 **SakeBomb** 1 year, 11 months ago

Correct answer is Anomaly Trusted List.

<https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/manage-prisma-cloud-alerts/trusted-ip-addresses-on-prisma-cloud.html>

upvoted 4 times

A DevOps lead reviewed some system logs and notices some odd behavior that could be a data exfiltration attempt. The DevOps lead only has access to vulnerability data in Prisma Cloud Compute, so the DevOps lead passes this information to SecOps. Which pages in Prisma Cloud Compute can the SecOps lead use to investigate the runtime aspects of this attack?

- A. The SecOps lead should investigate the attack using Vulnerability Explorer and Runtime Radar.
- B. The SecOps lead should use Incident Explorer and Compliance Explorer.
- C. The SecOps lead should use the Incident Explorer page and Monitor > Events > Container Audits.
- D. The SecOps lead should review the vulnerability scans in the CI/CD process to determine blame.

**Suggested Answer: B**

Reference:

[https://docs.paloaltonetworks.com/prisma/prisma-cloud/19-11/prisma-cloud-compute-edition-admin/runtime\\_defense/incident\\_explorer.html](https://docs.paloaltonetworks.com/prisma/prisma-cloud/19-11/prisma-cloud-compute-edition-admin/runtime_defense/incident_explorer.html)

Community vote distribution

C (100%)

🗳️ 👤 **JohnOrtiz** 7 months, 1 week ago

**Selected Answer: C**

option C is the correct

upvoted 1 times

🗳️ 👤 **Spippolo** 1 year, 6 months ago

**Selected Answer: C**

option C is the correct choice for the SecOps lead to investigate the runtime aspects of the attack in Prisma Cloud Compute.

upvoted 1 times

🗳️ 👤 **kumar\_57** 1 year, 9 months ago

C is the correct option. DevOps team has noticed a runtime incident (odd behavior) which you can explore either through Incident Explorer or Container audits.

upvoted 2 times

🗳️ 👤 **vaisat** 2 years, 1 month ago

C container audits under events)

upvoted 1 times

🗳️ 👤 **piipo** 2 years, 9 months ago

**Selected Answer: C**

Compliance vulnerabilities should already be seen by DevOps. SecOps should see Audits.

upvoted 3 times



A customer finds that an open alert from the previous day has been resolved. No auto-remediation was configured.

Which two reasons explain this change in alert status? (Choose two.)

- A. user manually changed the alert status.
- B. policy was changed.
- C. resource was deleted.
- D. alert was sent to an external integration.

**Suggested Answer:** CD

Reference:

<https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/manage-prisma-cloud-alerts/prisma-cloud-alert-resolution-reasons.html>

Community vote distribution

BC (100%)

 **SakeBomb** Highly Voted 3 years, 5 months ago

Answer is B and C.


upvoted 11 times

 **Mig\_MAM** Most Recent 1 year ago

The two reasons that could explain the change in alert status are:

A. User manually changed the alert status. Even without auto-remediation configured, a user with the appropriate permissions can manually change the status of an alert.

C. Resource was deleted. If the resource related to the alert was deleted, the alert would be resolved because the issue no longer exists.  
upvoted 2 times

 **JohnOrtiz** 1 year, 1 month ago

Selected Answer: BC

<https://docs.prismacloud.io/en/classic/cspm-admin-guide/manage-prisma-cloud-alerts/prisma-cloud-alert-resolution-reasons>

upvoted 1 times

 **Spippolo** 2 years ago

Selected Answer: BC

Tricky Question. I think B and C.

RESOURCE\_DELETED

Resource was deleted.

USER\_DISMISSED

Alert was dismissed or snoozed by the Prisma Cloud administrator with role of System admin, Account Group Admin, or Account and Cloud Provisioning Admin.

POLICY\_UPDATED

Policy was updated. This status indicates a change in the policy RQL that results in a resource not being in scope for the policy evaluation.

upvoted 1 times

 **kumar\_57** 2 years, 3 months ago

Yes, B and C are correct options.

<https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/manage-prisma-cloud-alerts/prisma-cloud-alert-resolution-reasons>

upvoted 1 times

 **Ravi221** 2 years, 9 months ago

Correct Answer is B and C,

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u00000040Q2CAM>

upvoted 2 times

  **SakeBomb** 3 years, 5 months ago



\*resolved

upvoted 1 times

  **SakeBomb** 3 years, 5 months ago

users cannot manually set an alert as remediated, they can only dismiss or snooze it.

upvoted 2 times

  **[Removed]** 3 years, 9 months ago

correct anser should be A & C.

based on the reference provided. No external services listed in the reference list.

upvoted 1 times

Which three steps are involved in onboarding an account for Data Security? (Choose three.)

- A. Create a read-only role with in-line policies
- B. Create a Cloudtrail with SNS Topic
- C. Enable Flow Logs
- D. Enter the RoleARN and SNSARN
- E. Create a S3 bucket

**Suggested Answer:** BCE

Community vote distribution

BDE (100%)

🗳️ 👤 **Spippolo** 6 months, 3 weeks ago

**Selected Answer:** BDE

- B. Create a CloudTrail with SNS Topic
- D. Enter the RoleARN and SNSARN
- E. Create an S3 bucket

<https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud-data-security/enable-data-security-module/add-a-new-aws-account>

upvoted 1 times

🗳️ 👤 **Spippolo** 6 months, 3 weeks ago

OR

- A. Create a read-only role with in-line policies
- D. Enter the RoleARN and SNSARN
- E. Create an S3 bucket

upvoted 1 times

🗳️ 👤 **kumar\_57** 9 months, 1 week ago

ABD is the correct answer.

<https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud-data-security/enable-data-security-module/add-a-new-aws-account>

upvoted 2 times

🗳️ 👤 **gekvprasad** 1 year, 7 months ago

DBE is the correct answer as per documentation

upvoted 2 times

🗳️ 👤 **piipo** 1 year, 9 months ago

**Selected Answer:** BDE

<https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud-data-security/enable-data-security-module/add-a-new-aws-account.html>

upvoted 4 times

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?

- A. 8084
- B. 443
- C. 8083
- D. 8081

**Suggested Answer: A**

Reference:

[https://docs.paloaltonetworks.com/prisma/prisma-cloud/19-11/prisma-cloud-compute-edition-admin/install/install\\_kubernetes.html](https://docs.paloaltonetworks.com/prisma/prisma-cloud/19-11/prisma-cloud-compute-edition-admin/install/install_kubernetes.html)

Community vote distribution

 C (100%)

 **[Removed]**  3 years, 3 months ago

C is correct.

[https://docs.prismacloudcompute.com/docs/compute\\_edition\\_21\\_04/tools/twistcli.html#connectivity-to-console](https://docs.prismacloudcompute.com/docs/compute_edition_21_04/tools/twistcli.html#connectivity-to-console)

upvoted 6 times

 **JohnOrtiz**  7 months, 1 week ago

**Selected Answer: C**<https://docs.prismacloud.io/en/compute-edition/32/admin-guide/install/deploy-console/console-on-kubernetes>

upvoted 1 times

 **Spippolo** 1 year, 6 months ago

**Selected Answer: C**

C --&gt; By default Prisma Cloud listens on:

8083 HTTPS management port for access to Console.

8084 WSS port for Defender to Console communication.

upvoted 1 times

 **Chichi23** 1 year, 8 months ago

Port 8083, as per docs "Open a browser window, and navigate to Console. By default, Console is served on HTTPS on port 8083. For example, go to <https://yourconsole.example.com:8083>."

[https://docs.paloaltonetworks.com/prisma/prisma-cloud/19-11/prisma-cloud-compute-edition-admin/install/install\\_kubernetes](https://docs.paloaltonetworks.com/prisma/prisma-cloud/19-11/prisma-cloud-compute-edition-admin/install/install_kubernetes)

upvoted 2 times

 **kumar\_57** 1 year, 9 months ago

Yes, C is the correct option.

[https://docs.paloaltonetworks.com/prisma/prisma-cloud/19-11/prisma-cloud-compute-edition-admin/install/install\\_kubernetes](https://docs.paloaltonetworks.com/prisma/prisma-cloud/19-11/prisma-cloud-compute-edition-admin/install/install_kubernetes)

upvoted 1 times

 **SakeBomb** 2 years, 11 months ago

C

port 8084 is reserved for communication between console and defender. 8083 is for HTTPS

upvoted 4 times

A customer is reviewing Container audits, and an audit has identified a cryptominer attack. Which three options could have generated this audit? (Choose three.)

- A. The value of the mined currency exceeds \$100.
- B. High CPU usage over time for the container is detected.
- C. Common cryptominer process name was found.
- D. The mined currency is associated with a user token.
- E. Common cryptominer port usage was found.

**Suggested Answer:** BCD

Community vote distribution

BCE (100%)

🗲️ 👤 **[Removed]** Highly Voted 👍 2 years, 3 months ago

BCE. Prisma cloud is unable to detect D.  
upvoted 12 times

🗲️ 👤 **Spippolo** Most Recent 🕒 6 months, 3 weeks ago

Selected Answer: BCE

B. High CPU usage over time for the container is a common indicator of a cryptominer attack. Cryptominers utilize the computational resources of a system to mine cryptocurrencies, which often leads to increased CPU usage.

C. Detection of a common cryptominer process name can trigger an audit. Cryptominers typically run specific processes or executables with recognizable names that indicate their presence.

E. Discovery of common cryptominer port usage can also generate an audit. Cryptominers often communicate with mining pools or other components using specific ports associated with cryptocurrency mining.  
upvoted 3 times

🗲️ 👤 **kumar\_57** 9 months ago

BCD is correct option  
upvoted 1 times

Which step is included when configuring Kubernetes to use Prisma Cloud Compute as an admission controller?

- A. copy the Console address and set the config map for the default namespace.
- B. create a new namespace in Kubernetes called admission-controller.
- C. enable Kubernetes auditing from the Defend > Access > Kubernetes page in the Console.
- D. copy the admission controller configuration from the Console and apply it to Kubernetes.

**Suggested Answer: B**

Reference:

<https://thenewstack.io/kubernetes-security-best-practices-to-keep-you-out-of-the-news/>

Community vote distribution

D (100%)

🗳️ 👤 [Removed] Highly Voted 👍 3 years, 9 months ago

D is correct.

[https://docs.paloaltonetworks.com/prisma/prisma-cloud/20-04/prisma-cloud-compute-edition-admin/access\\_control/open\\_policy\\_agent.html](https://docs.paloaltonetworks.com/prisma/prisma-cloud/20-04/prisma-cloud-compute-edition-admin/access_control/open_policy_agent.html)  
step 2

upvoted 5 times

🗳️ 👤 7a9e5e5 Most Recent 🕒 8 months ago

D is the correct response. Since we are talking about Prisma Compute, according to the PCCSE guide to Prisma Cloud, the step-by-step instructions are as follows:

Step 1: Go to Defend > Access > Admission.

Step 2: Enable admission control.

Step 3: Click Go to settings.

- Copy the configuration provided to a file named webhook.yaml.

Step 4: Click Save.

Step 5: Create the webhook configuration object.

```
$ kubectl apply -f webhook.yaml
```

After creating the object, the Kubernetes API server directs AdmissionReview requests to Defender.

upvoted 2 times

🗳️ 👤 Spippolo 2 years ago

Selected Answer: D

D --> The correct step to configure Kubernetes to use Prisma Cloud Compute as an admission controller is to copy the admission controller configuration from the Console and apply it to Kubernetes.

upvoted 1 times

🗳️ 👤 kumar\_57 2 years, 3 months ago

The correct answer is D.

<https://www.paloaltonetworks.com/blog/prisma-cloud/prisma-cloud-compute-open-policy-agent/#:~:text=To%20use%20the%20admission%20controller%2C%20enable%20it%20within,control%20in%20Prisma%20Cloud%20Compute%20Deploy%20a>

upvoted 1 times

🗳️ 👤 [Removed] 3 years, 9 months ago

namespace created by prismacloud is 'twistlock'

upvoted 2 times

A Prisma Cloud administrator is onboarding a single GCP project to Prisma Cloud.

Which two steps can be performed by the Terraform script? (Choose two.)

- A. enable flow logs for Prisma Cloud.
- B. create the Prisma Cloud role.
- C. enable the required APIs for Prisma Cloud.
- D. publish the flow log to a storage bucket.

**Suggested Answer:** AC

Community vote distribution


BC (100%)

 **piipo** Highly Voted 1 year, 9 months ago

**Selected Answer:** BC

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

upvoted 7 times

 **Spippolo** Most Recent 6 months, 3 weeks ago

**Selected Answer:** BC

When onboarding a single GCP project to Prisma Cloud using a Terraform script, the two steps that can be performed are:

- B. Create the Prisma Cloud role.
- C. Enable the required APIs for Prisma Cloud.

upvoted 2 times

 **kumar\_57** 9 months ago

Yes, B and C are correct options.

upvoted 2 times

Which statement about build and run policies is true?

- A. Build policies enable you to check for security misconfigurations in the IaC templates.
- B. Every type of policy has auto-remediation enabled by default.
- C. The four main types of policies are: Audit Events, Build, Network, and Run.
- D. Run policies monitor network activities in the environment and check for potential issues during runtime.

**Suggested Answer: A**

🗨️ 👤 **Spippolo** 6 months, 3 weeks ago

A --> Build policies are used to validate Infrastructure-as-Code (IaC) templates, such as those written in Terraform or AWS CloudFormation, for security misconfigurations.

upvoted 2 times

🗨️ 👤 **kumar\_57** 9 months ago

Only option A is correct.

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

upvoted 2 times



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

The audit message is:

`Service postfix attempted to obtain capability SHELL by executing /bin/sh /usr/libexec/postfix/postfix-script.stop. Low severity audit, event is automatically added to the runtime model`

Which runtime host policy rule is the root cause for this runtime audit?

- A. Custom rule with specific configuration for file integrity
- B. Custom rule with specific configuration for networking
- C. Default rule that alerts on capabilities
- D. Default rule that alerts on suspicious runtime behavior

**Suggested Answer:** D

Community vote distribution

D (100%)

🗨️ 👤 **Spippolo** 6 months, 3 weeks ago

**Selected Answer: D**

For exclusion D.

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

upvoted 2 times

🗨️ 👤 **kumar\_57** 9 months ago

Yes, D is the correct answer.

upvoted 1 times

Which option identifies the Prisma Cloud Compute Edition?

- A. Package installed with APT
- B. Downloadable, self-hosted software
- C. Software-as-a-Service (SaaS)
- D. Plugin to Prisma Cloud

**Suggested Answer:** B

Reference:

[https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/welcome/pcee\\_vs\\_pcce.html](https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/welcome/pcee_vs_pcce.html)

*Community vote distribution*

B (100%)

🗳️ 👤 **Spippolo** 6 months, 3 weeks ago

**Selected Answer: B**

B.

Prisma Cloud Compute Edition is a downloadable, self-hosted software solution. It is installed and deployed within an organization's infrastructure to provide visibility, security, and compliance for cloud native applications and infrastructure.

upvoted 1 times

🗳️ 👤 **kumar\_57** 9 months ago

Yes, B is correct option.

[https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/welcome/pcee\\_vs\\_pcce](https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/welcome/pcee_vs_pcce)

upvoted 1 times

🗳️ 👤 **vaisat** 1 year, 1 month ago

B makes most sense.

upvoted 2 times

Which type of compliance check is available for rules under Defend > Compliance > Containers and Images > CI?

- A. Host
- B. Container
- C. Functions
- D. Image

**Suggested Answer: B**

Reference:

[https://docs.twistlock.com/docs/enterprise\\_edition/compliance/manage\\_compliance.html](https://docs.twistlock.com/docs/enterprise_edition/compliance/manage_compliance.html)

Community vote distribution

D (100%)

🗲️ 👤 **[Removed]** Highly Voted 👍 3 years, 3 months ago

Correct answer is D.

Concerns CI images compliance policy.

upvoted 10 times

🗲️ 👤 **FS9** Most Recent ⌚ 9 months ago

Selected Answer: D

D Image

upvoted 2 times

🗲️ 👤 **Spippolo** 1 year, 6 months ago

Selected Answer: D

D --> CI images compliance policy. Compliance rules let you monitor, audit, and enforce security and configuration settings for your CI images.

upvoted 2 times

🗲️ 👤 **Jihe** 1 year, 7 months ago

D

[https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/compliance/manage\\_compliance](https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/compliance/manage_compliance)

upvoted 1 times

🗲️ 👤 **kumar\_57** 1 year, 9 months ago

Yes, correct option is D.

Compliance rules let you monitor, audit, and enforce security and configuration settings for your CI images.

upvoted 2 times

🗲️ 👤 **gekvprasad** 2 years, 7 months ago

Correct Answer id D

upvoted 2 times

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?

- A. CNAF
- B. Runtime
- C. Compliance
- D. CNNF

**Suggested Answer: A**

Reference:

<https://docs.paloaltonetworks.com/prisma/prisma-cloud/20-09/prisma-cloud-compute-edition-admin/firewalls/waas>

*Community vote distribution*

A (100%)

🗳️ 👤 **Spippolo** 6 months, 3 weeks ago

**Selected Answer: A**

A --> WAAS (Web-Application and API Security, formerly known as CNAF, Cloud Native Application Firewall).

[https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/waas/waas\\_app\\_firewall](https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/waas/waas_app_firewall)

upvoted 2 times

🗳️ 👤 **kumar\_57** 9 months ago

The correct option is A.

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

upvoted 2 times

🗳️ 👤 **gekvprasad** 1 year, 7 months ago

WAAS (Web-Application and API Security, formerly known as CNAF

upvoted 4 times

An S3 bucket within AWS has generated an alert by violating the Prisma Cloud Default policy `AWS S3 buckets are accessible to public`. The policy definition follows: config where cloud.type = 'aws' AND api.name='aws-s3api-get-bucket-acl' AND json.rule="((((acl.grants[? (@.grantee=='AllUsers')] size > 0) or policyStatus.isPublic is true) and publicAccessBlockConfiguration does not exist) or ((acl.grants[? (@.grantee=='AllUsers')] size > 0) and publicAccessBlockConfiguration.ignorePublicAcls is false) or (policyStatus.isPublic is true and publicAccessBlockConfiguration.restrictPublicBuckets is false)) and websiteConfiguration does not exist"

Why did this alert get generated?

- A. an event within the cloud account
- B. network traffic to the S3 bucket
- C. configuration of the S3 bucket
- D. anomalous behaviors

**Suggested Answer: B**

Community vote distribution

C (100%)

🗳️ 👤 **[Removed]** Highly Voted 👍 2 years, 9 months ago

websiteConfiguration does not exist concerns about config not traffic. Therefore correct answer is C  
upvoted 9 times

🗳️ 👤 **assadhashmi** Most Recent 🕒 10 months ago

Selected Answer: C

Correct option is C  
upvoted 1 times

🗳️ 👤 **Spippolo** 1 year ago

Selected Answer: C

For exclusion "C".  
upvoted 1 times

🗳️ 👤 **kumar\_57** 1 year, 3 months ago

Yes, correct option is C.  
upvoted 1 times

DRAG DROP -

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.)

Select and Place:

### 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
Suggested Answer:	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

**[Removed]** Highly Voted 3 years, 3 months ago

1. click on compliance standard.
  2. add custom compliance standard.
  3. edit policies.
  4. add compliance standard from drop-down menu
- upvoted 9 times

**vaisat** 2 years, 1 month ago

This right here ^^^  
upvoted 3 times

**Bubbleman** Most Recent 8 months, 2 weeks ago

The question ask about step mapping policy with Compliance Standard. So I tested on my lab and the correct should like this.

1. Create the custom compliance standard
  2. Edit the Policy
  3. Click on Compliance Standard
  4. Add compliance standard from drop-down menu
- upvoted 3 times

**Spippolo** 1 year, 6 months ago

<https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud-compliance/create-a-custom-compliance-standard>

- 1) On Prisma Cloud, select Compliance > Standards
- 2) Create a compliance standard from scratch.

- 3) Edit policies
  - 4) Add policies to your custom compliance standard.
- upvoted 3 times

🗨️ 👤 **Chichi23** 1 year, 8 months ago

1. click on compliance standard. \*\*
  2. create custom compliance standard. <<<
  3. edit policies. < 3rd
  4. add compliance standard from drop-down menu
- upvoted 2 times

🗨️ 👤 **kumar\_57** 1 year, 9 months ago

1. click on compliance standard.
2. add custom compliance standard.
3. edit policies.
4. add compliance standard from drop-down menu

<https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud-compliance/create-a-custom-compliance-standard>

upvoted 2 times

🗨️ 👤 **ducanhcbbn** 2 years, 2 months ago

Correct answer should be:

1. add custom compliance standard.
2. edit policies.
3. click on compliance standard.
4. add compliance standard from drop-down menu

<https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud-compliance/create-a-custom-compliance-standard>

upvoted 3 times

🗨️ 👤 **[Removed]** 3 years, 3 months ago

incorrect order.

[https://docs.prismacloudcompute.com/docs/enterprise\\_edition/compliance/custom\\_compliance\\_checks.html#creating-a-new-custom-check](https://docs.prismacloudcompute.com/docs/enterprise_edition/compliance/custom_compliance_checks.html#creating-a-new-custom-check)

upvoted 1 times

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`?

- A. Prevent
- B. Alert
- C. Block
- D. Fail

**Suggested Answer:** (133)A

Reference:

[https://docs.paloaltonetworks.com/content/dam/techdocs/en\\_US/pdf/prisma/prisma-cloud/prisma-cloud-policy-reference/prisma-cloud-policy-reference.pdf](https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/prisma/prisma-cloud/prisma-cloud-policy-reference/prisma-cloud-policy-reference.pdf)

Community vote distribution

C (100%)

 **[Removed]** Highly Voted 3 years, 3 months ago

Correct anser is Block.

Block – Defender stops the entire container if a process that violates your policy attempts to run.

[https://docs.prismacloudcompute.com/docs/enterprise\\_edition/runtime\\_defense/runtime\\_defense\\_containers.html#\\_effect](https://docs.prismacloudcompute.com/docs/enterprise_edition/runtime_defense/runtime_defense_containers.html#_effect)  
upvoted 7 times

 **JohnOrtiz** Most Recent 7 months, 1 week ago

Selected Answer: C

ID: 5054

Type: container

Severity: critical

Action: Ignore, Alert or Bolock

Description: Do not use privileged containers

upvoted 1 times

 **David2606** 1 year, 6 months ago

Selected Answer: C

CORRECT ANSWER IS C

upvoted 1 times

 **Spippolo** 1 year, 6 months ago

Selected Answer: C

C

Prevent – Defender stops the process (and just the process) that violates your policy from executing. This is known as discrete blocking.

Block – Defender stops the entire container if a process that violates your policy attempts to run.

upvoted 2 times

 **kumar\_57** 1 year, 9 months ago

Option c IS CORRECT.

[https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/compliance/manage\\_compliance#:~:text=The%20flow%20for%20blocking%20such%20a%20container%20is%3A,deploy%20a%20container%20to%2](https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/compliance/manage_compliance#:~:text=The%20flow%20for%20blocking%20such%20a%20container%20is%3A,deploy%20a%20container%20to%2)

upvoted 1 times



Given an existing ECS Cluster, which option shows the steps required to install the Console in Amazon ECS?

- A. The console cannot natively run in an ECS cluster. A onebox deployment should be used.
- B. Download and extract the release tarball Ensure that each node has its own storage for Console data Create the Console task definition Deploy the task definition
- C. Download and extract release tarball Download task from AWS Create the Console task definition Deploy the task definition
- D. Download and extract the release tarball Create an EFS file system and mount to each node in the cluster Create the Console task definition Deploy the task definition

**Suggested Answer: D**

Reference:

[https://docs.paloaltonetworks.com/prisma/prisma-cloud/19-11/prisma-cloud-compute-edition-admin/install/install\\_amazon\\_ecs.html](https://docs.paloaltonetworks.com/prisma/prisma-cloud/19-11/prisma-cloud-compute-edition-admin/install/install_amazon_ecs.html)

Community vote distribution

D (100%)

🗳️ 👤 **JohnOrtiz** 7 months, 1 week ago

**Selected Answer: D**

<https://docs.prismacloud.io/en/compute-edition/30/admin-guide/install/deploy-console/console-on-amazon-ecs>

upvoted 1 times

🗳️ 👤 **Spippolo** 1 year, 6 months ago

**Selected Answer: D**

The correct answer is:

D. Download and extract the release tarball, create an EFS (Elastic File System) file system and mount it to each node in the cluster, create the Console task definition, and deploy the task definition.

upvoted 1 times

🗳️ 👤 **kumar\_57** 1 year, 9 months ago

Yes, option is correct.

[https://docs.paloaltonetworks.com/prisma/prisma-cloud/21-08/prisma-cloud-compute-edition-admin/install/install\\_amazon\\_ecs](https://docs.paloaltonetworks.com/prisma/prisma-cloud/21-08/prisma-cloud-compute-edition-admin/install/install_amazon_ecs)

upvoted 1 times

🗳️ 👤 **kumar\_57** 1 year, 9 months ago

option D\*

upvoted 2 times

🗳️ 👤 **Redrum702** 1 year, 10 months ago

D

[https://docs.paloaltonetworks.com/prisma/prisma-cloud/21-08/prisma-cloud-compute-edition-admin/install/install\\_amazon\\_ecs](https://docs.paloaltonetworks.com/prisma/prisma-cloud/21-08/prisma-cloud-compute-edition-admin/install/install_amazon_ecs)

upvoted 2 times

Which options show the steps required to upgrade Console when using projects?

- A. Upgrade all Supervisor Consoles Upgrade Central Console
- B. Upgrade Central Console Upgrade Central Console Defenders
- C. Upgrade Defender Upgrade Central Console Upgrade Supervisor Consoles
- D. Upgrade Central Console Upgrade all Supervisor Consoles

**Suggested Answer: A**

Reference:

[https://docs.paloaltonetworks.com/prisma/prisma-cloud/20-09/prisma-cloud-compute-edition-admin/upgrade/upgrade\\_process.html](https://docs.paloaltonetworks.com/prisma/prisma-cloud/20-09/prisma-cloud-compute-edition-admin/upgrade/upgrade_process.html)

*Community vote distribution*

A (100%)

🗳️ 👤 **Spippolo** 6 months, 3 weeks ago

**Selected Answer: A**

When you have one or more tenant or scale Projects, upgrade all Supervisors before upgrading the Central Console.

[https://docs.paloaltonetworks.com/prisma/prisma-cloud/20-09/prisma-cloud-compute-edition-admin/upgrade/upgrade\\_process](https://docs.paloaltonetworks.com/prisma/prisma-cloud/20-09/prisma-cloud-compute-edition-admin/upgrade/upgrade_process)  
upvoted 2 times

🗳️ 👤 **kumar\_57** 9 months ago

The correct is A.

[https://docs.paloaltonetworks.com/prisma/prisma-cloud/20-09/prisma-cloud-compute-edition-admin/upgrade/upgrade\\_process](https://docs.paloaltonetworks.com/prisma/prisma-cloud/20-09/prisma-cloud-compute-edition-admin/upgrade/upgrade_process)  
upvoted 1 times

🗳️ 👤 **Redrum702** 10 months, 3 weeks ago

A

[https://docs.paloaltonetworks.com/prisma/prisma-cloud/21-08/prisma-cloud-compute-edition-admin/upgrade/upgrade\\_process\\_self\\_hosted](https://docs.paloaltonetworks.com/prisma/prisma-cloud/21-08/prisma-cloud-compute-edition-admin/upgrade/upgrade_process_self_hosted)  
upvoted 1 times

🗳️ 👤 **gekvprasad** 1 year, 7 months ago

When you have one or more tenant or scale Projects, upgrade all Supervisors before upgrading the Central Console

upvoted 2 times

A customer has Prisma Cloud Enterprise and host Defenders deployed.

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

- A. with auto-upgrade, the host Defender will auto-upgrade.
- B. auto deploy the Lambda Defender.
- C. click the update button in the web-interface.
- D. generate a new DaemonSet file.

**Suggested Answer:** AD

Community vote distribution

AC (100%)

 **piipo** Highly Voted 1 year, 9 months ago

**Selected Answer:** AC

host Defenders

upvoted 6 times

 **Spippolo** Most Recent 6 months, 3 weeks ago

**Selected Answer:** AC

If Defender auto-upgrade is enabled – Console will upgrade deployed Defenders for you. If Console fails to upgrade one or more Defenders, it displays a banner at the top of the UI. If you've created an alert for Defender health events, Console emits a message on the alert channel for any Defender it fails to upgrade. Manually upgrade any Defenders that Console could not auto-upgrade.

If Defender auto-upgrade is disabled – Manually upgrade all deployed Defenders.

upvoted 1 times

 **kumar\_57** 9 months ago

AC is correct.

[https://docs.paloaltonetworks.com/prisma/prisma-cloud/20-09/prisma-cloud-compute-edition-admin/upgrade/upgrade\\_process](https://docs.paloaltonetworks.com/prisma/prisma-cloud/20-09/prisma-cloud-compute-edition-admin/upgrade/upgrade_process)

upvoted 1 times

Which intensity setting for anomaly alerts is used for the measurement of 100 events over 30 days?

- A. High
- B. Medium
- C. Low
- D. Very High

**Suggested Answer:** B

Reference:

<https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/manage-prisma-cloud-administrators/define-prisma-cloud-enterprise-settings.html>

*Community vote distribution*

B (100%)

🗳️ 👤 **Spippolo** 6 months, 3 weeks ago

**Selected Answer: B**

For unusual user activity:

Medium: The behavioral models are based on observing at least 100 events over 30 days.

upvoted 1 times

🗳️ 👤 **kumar\_57** 9 months ago

B is the correct option.

<https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/manage-prisma-cloud-administrators/define-prisma-cloud-enterprise-settings>

upvoted 1 times

🗳️ 👤 **Redrum702** 10 months, 3 weeks ago

B

<https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/manage-prisma-cloud-administrators/define-prisma-cloud-enterprise-settings>

upvoted 1 times

Given this information:

- ⇒ The Console is located at `https://prisma-console.mydomain.local`
- ⇒ The username is: `cluster`
- ⇒ 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?

- 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`

**Suggested Answer:** C

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)

Community vote distribution

D (100%)

🗳️ 👤 [Removed] **Highly Voted** 👍 2 years, 3 months ago

Correct answer is D.

--details --

Show all vulnerability details.

upvoted 10 times

🗳️ 👤 **Spippolo** **Most Recent** 🕒 6 months, 3 weeks ago

**Selected Answer: D**

D.

This command specifies the Console address using the `--address` flag with the provided URL, and includes the username and password using the `-u` and `-p` flags respectively. The `--details` flag is used to display the details about each vulnerability. Finally, the image to scan is specified as `myimage:latest`.

upvoted 2 times

🗳️ 👤 **kumar\_57** 9 months ago

The correct answer is D.

[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)

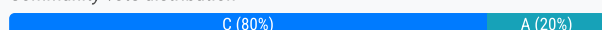
upvoted 1 times

The development team wants to block Cross Site Scripting attacks from pods in its environment.  
How should the team construct the CNAF policy to protect against this attack?

- A. create a Host CNAF policy, targeted at a specific resource, check the box for XSS attack protection, and set the action to prevent.
- B. create a Container CNAF policy, targeted at a specific resource, check the box for XSS attack protection, and set the action to alert.
- C. create a Container CNAF policy, targeted at a specific resource, check the box for XSS 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.

**Suggested Answer: A**

Community vote distribution



🗳️ 👤 **[Removed]** Highly Voted 👍 2 years, 3 months ago

Correct anser is C. pods run in k8s.  
upvoted 7 times

🗳️ 👤 **Spippolo** Most Recent 🕒 6 months, 3 weeks ago

Selected Answer: C

C.

Prevent - The request is denied from reaching the protected application, an audit is generated and WAAS responds with an HTML page indicating the request was blocked.

Supported only in WAAS Inline proxy setup.

upvoted 2 times

🗳️ 👤 **Jihe** 7 months ago

C

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

upvoted 1 times

🗳️ 👤 **kumar\_57** 9 months ago

A is correct answer since pods are specified WAAS policy must be created for hosts where these pods might be running in your k8s environment.

upvoted 1 times

🗳️ 👤 **tipzzz** 11 months, 2 weeks ago

Containers are in pod,

Pods are in host.

If you want to protect pods, you have to protect host.

A

upvoted 1 times

🗳️ 👤 **piipo** 1 year, 9 months ago

Selected Answer: C

Pod is a container, not a Host

upvoted 3 times

🗳️ 👤 **SakeBomb** 1 year, 11 months ago

Unlike other systems you may have used in the past, Kubernetes doesn't run containers directly; instead it wraps one or more containers into a higher-level structure called a pod. Any containers in the same pod will share the same resources and local network. Pods are used as the unit of replication in Kubernetes.

upvoted 1 times

🗳️ 👤 **SakeBomb** 1 year, 11 months ago

Selected Answer: A

The "one-container-per-Pod" model is the most common Kubernetes use case; in this case, you can think of a Pod as a wrapper around a single container; Kubernetes manages Pods rather than managing the containers directly.

upvoted 1 times

The Prisma Cloud administrator has configured a new policy.  
Which steps should be used to assign this policy to a compliance standard?

- A. Edit the policy, go to step 3 (Compliance Standards), click + at the bottom, select the compliance standard, fill in the other boxes, and then click Confirm.
- B. Create the Compliance Standard from Compliance tab, and then select Add to Policy.
- C. Open the Compliance Standards section of the policy, and then save.
- D. Custom policies cannot be added to existing standards.

**Suggested Answer: B**

Reference:

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

Community vote distribution

A (100%)



  **kemalgoklen** Highly Voted 1 year, 12 months ago

The point is user created a new policy, you can't modify existing policies that were created by Prisma (default) but you can modify your own custom policies.

Answer A is correct.

Edit the policy, go to step 3 (Compliance Standards), click + at the bottom, select the compliance standard, fill in the other boxes, and then click Confirm.

upvoted 6 times

  **ubersys** Most Recent 6 months, 3 weeks ago

Selected Answer: A

There's no add to policy in compliance standard section

upvoted 1 times

  **Spippolo** 1 year ago

Selected Answer: A

A.

Tested the solution.

upvoted 2 times

  **Jihe** 1 year, 1 month ago

A



To Add policies to your custom compliance standard: Select the policy rule to edit, on 3 Compliance Standards click + and associate the policy with the custom compliance standard. (<https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud-compliance/create-a-custom-compliance-standard>)

upvoted 2 times

  **kumar\_57** 1 year, 3 months ago

Compliance Standard can be associated to a policy, but reverse is not true hence option A is correct.

upvoted 1 times

  **gekvprasad** 2 years, 1 month ago

You can not add policy from compliance section. Option 1 is correct

upvoted 1 times



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: \$CONSOLE\_ADDRESS
- ⇒ Websocket Address: \$WEBSOCKET\_ADDRESS
- ⇒ User: \$ADMIN\_USER

Which command generates the YAML file for Defender install?

- A. <PLATFORM>/twistcli defender \ --address \$CONSOLE\_ADDRESS \ --user \$ADMIN\_USER \ --cluster-address \$CONSOLE\_ADDRESS
- B. <PLATFORM>/twistcli defender export kubernetes \ --address \$WEBSOCKET\_ADDRESS \ --user \$ADMIN\_USER \ --cluster-address \$CONSOLE\_ADDRESS
- C. <PLATFORM>/twistcli defender YAML kubernetes \ --address \$CONSOLE\_ADDRESS \ --user \$ADMIN\_USER \ --cluster-address \$WEBSOCKET\_ADDRESS
- D. <PLATFORM>/twistcli defender export kubernetes \ --address \$CONSOLE\_ADDRESS \ --user \$ADMIN\_USER \ --cluster-address \$WEBSOCKET\_ADDRESS

**Suggested Answer: D**

Reference:

[https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/install/install\\_kubernetes.html](https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/install/install_kubernetes.html)

Community vote distribution

D (100%)

🗳️ 👤 **Spippolo** 6 months, 3 weeks ago

**Selected Answer: D**

D.

```
$ <PLATFORM>/twistcli defender export kubernetes \
--user <ADMIN_USER> \
--address <PRISMA_CLOUD_COMPUTE_CONSOLE_URL> \
--cluster-address <PRISMA_CLOUD_COMPUTE_HOSTNAME>
--cri
```

[https://docs.paloaltonetworks.com/prisma/prisma-cloud/22-06/prisma-cloud-compute-edition-admin/install/install\\_kubernetes](https://docs.paloaltonetworks.com/prisma/prisma-cloud/22-06/prisma-cloud-compute-edition-admin/install/install_kubernetes)  
upvoted 1 times

🗳️ 👤 **kumar\_57** 9 months ago

The correct answer is option D.

[https://medium.com/@sureshthivanka/cloud-native-security-devsecops-3e263df2a06c#:~:text=Use%20twistcli%20to%20generate%20a%20YAML%20configuration%20file,YAML%20file.%20%24%20%3CPLATFORM%3E%2Ftwistcli%](https://medium.com/@sureshthivanka/cloud-native-security-devsecops-3e263df2a06c#:~:text=Use%20twistcli%20to%20generate%20a%20YAML%20configuration%20file,YAML%20file.%20%24%20%3CPLATFORM%3E%2Ftwistcli%20)

upvoted 2 times

🗳️ 👤 **Redrum702** 10 months, 3 weeks ago

A

[https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/install/install\\_kubernetes](https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/install/install_kubernetes)  
upvoted 1 times



Which options show the steps required after upgrade of Console?

- A. Uninstall Defenders Upgrade Jenkins Plugin Upgrade twistcli where applicable Allow the Console to redeploy the Defender
- B. Update the Console image in the Twistlock hosted registry Update the Defender image in the Twistlock hosted registry Uninstall Defenders
- C. Upgrade Defenders Upgrade Jenkins Plugin Upgrade twistcli where applicable
- D. Update the Console image in the Twistlock hosted registry Update the Defender image in the Twistlock hosted registry Redeploy Console

**Suggested Answer:** C

Community vote distribution

C (100%)

  **Spippolo** 6 months, 3 weeks ago

**Selected Answer:** C

After the Console has been upgraded, check and upgrade any of the Defenders that have reached the end of their support lifecycle (Defenders are backward compatible for N-2 releases). The Defender release image is built from the UBI8-minimal base image and on upgrade it is a full container image upgrade, which means that the old Defender container is replaced with a new container. Then, upgrade all other Prisma Cloud components, such as the Jenkins plugin.

[https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/upgrade/upgrade\\_process\\_saas](https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/upgrade/upgrade_process_saas)

upvoted 2 times

  **Redrum702** 11 months, 3 weeks ago

C

[https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/upgrade/upgrade\\_process\\_saas](https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/upgrade/upgrade_process_saas)

upvoted 2 times

An organization wants to be notified immediately to any `High Severity` alerts for the account group `Clinical Trials` via Slack. Which option shows the steps the organization can use to achieve this goal?

- A. 1. Configure Slack Integration 2. Create an alert rule and select `Clinical Trials` as the account group 3. Under the `Select Policies` tab, filter on severity and select `High` 4. Under the Set Alert Notification tab, choose Slack and populate the channel 5. Set Frequency to `As it Happens`
- B. 1. Create an alert rule and select `Clinical Trials` as the account group 2. Under the `Select Policies` tab, filter on severity and select `High` 3. Under the Set Alert Notification tab, choose Slack and populate the channel 4. Set Frequency to `As it Happens` 5. Set up the Slack Integration to complete the configuration
- C. 1. Configure Slack Integration 2. Create an alert rule 3. Under the `Select Policies` tab, filter on severity and select `High` 4. Under the Set Alert Notification tab, choose Slack and populate the channel 5. Set Frequency to `As it Happens`
- D. 1. Under the `Select Policies` tab, filter on severity and select `High` 2. Under the Set Alert Notification tab, choose Slack and populate the channel 3. Set Frequency to `As it Happens` 4. Configure Slack Integration 5. Create an Alert rule

**Suggested Answer: B**

Community vote distribution

A (100%)

 **piipo** Highly Voted 1 year, 9 months ago

**Selected Answer: A**

<https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/alerts/slack.html>

upvoted 8 times

 **Spippolo** Most Recent 6 months, 3 weeks ago

**Selected Answer: A**

A.

Configure Slack Integration.

Create an alert rule and select "Clinical Trials" as the account group.

Under the "Select Policies" tab, filter on severity and select "High".

Under the "Set Alert Notification" tab, choose Slack and populate the channel.

Set the frequency to "As it Happens".

upvoted 2 times

A business unit has acquired a company that has a very large AWS account footprint. The plan is to immediately start onboarding the new company's AWS accounts into Prisma Cloud Enterprise tenant immediately. The current company is currently not using AWS Organizations and will require each account to be onboarded individually.

The business unit has decided to cover the scope of this action and determined that a script should be written to onboard each of these accounts with general settings to gain immediate posture visibility across the accounts.

Which API endpoint will specifically add these accounts into the Prisma Cloud Enterprise tenant?

- A. <https://api.prismacloud.io/cloud/>
- B. <https://api.prismacloud.io/account/aws>
- C. <https://api.prismacloud.io/cloud/aws>
- D. <https://api.prismacloud.io/accountgroup/aws>

**Suggested Answer: B**

Community vote distribution

C (100%)

🗨️ 👤 **Joe27** Highly Voted 👍 1 year, 8 months ago

**Selected Answer: C**

<https://prisma.pan.dev/api/cloud/cspm/cloud-accounts#operation/add-cloud-account>  
upvoted 9 times

🗨️ 👤 **Spippolo** Most Recent 🕒 6 months, 3 weeks ago

**Selected Answer: C**

Should be C.

<https://pan.dev/prisma-cloud/docs/cspm/aws-cloud-account-onboarding/>  
upvoted 1 times

A security team has a requirement to ensure the environment is scanned for vulnerabilities.

What are three options for configuring vulnerability policies? (Choose three.)

- A. individual actions based on package type
- B. output verbosity for blocked requests
- C. apply policy only when vendor fix is available
- D. individual grace periods for each severity level
- E. customize message on blocked requests

**Suggested Answer:** BCD

Reference:

[https://docs.paloaltonetworks.com/prisma/prisma-cloud/19-11/prisma-cloud-compute-edition-admin/vulnerability\\_management/vuln\\_management\\_rules.html](https://docs.paloaltonetworks.com/prisma/prisma-cloud/19-11/prisma-cloud-compute-edition-admin/vulnerability_management/vuln_management_rules.html)

Community vote distribution



🗳️ 👤 **vaisat** Highly Voted 2 years, 1 month ago

Everything but A seems correct

upvoted 5 times

🗳️ 👤 **f69ea9c** Most Recent 2 months, 1 week ago

Selected Answer: BCE

BCDE are all valid options when configuring a Vulnerability Management Policy

<https://docs.prismacloud.io/en/enterprise-edition/content-collections/runtime-security/vulnerability-management/vulnerability-management-policies>

upvoted 1 times

🗳️ 👤 **FS9** 9 months ago

Selected Answer: ACD

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

upvoted 1 times

🗳️ 👤 **Spippolo** 1 year, 6 months ago

Selected Answer: BCD

BCD

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

upvoted 1 times

🗳️ 👤 **bersus96** 1 year, 10 months ago

ACD, check it out on Prisma

upvoted 2 times

🗳️ 👤 **Redrum702** 1 year, 10 months ago

BCD

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

upvoted 2 times

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?

- A. Disable the policy
- B. Set the Alert Disposition to Conservative
- C. Change the Training Threshold to Low
- D. Set Alert Disposition to Aggressive

**Suggested Answer: C**

Reference:

<https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud-policies/anomaly-policies.html>

Community vote distribution

B (100%)

 **SakeBomb** Highly Voted 1 year, 11 months ago

Answer is B

<https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/manage-prisma-cloud-administrators/define-prisma-cloud-enterprise-settings>

upvoted 7 times

 **Spippolo** Most Recent 6 months, 3 weeks ago

**Selected Answer: B**

B.

Set the Alert Disposition to Conservative to reduce false positives.

upvoted 1 times

 **vimal1206** 1 year, 2 months ago

Answer is B. Set alert disposition to conservative.

<https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/manage-prisma-cloud-administrators/define-prisma-cloud-enterprise-settings>

upvoted 1 times

What is the behavior of Defenders when the Console is unreachable during upgrades?

- A. Defenders continue to alert, but not enforce, using the policies and settings most recently cached before upgrading the Console.
- B. Defenders will fail closed until the web-socket can be re-established.
- C. Defenders will fail open until the web-socket can be re-established.
- D. Defenders continue to alert and enforce using the policies and settings most recently cached before upgrading the Console.

**Suggested Answer:** D

Reference:

[https://docs.paloaltonetworks.com/prisma/prisma-cloud/20-09/prisma-cloud-compute-edition-admin/upgrade/upgrade\\_process.html](https://docs.paloaltonetworks.com/prisma/prisma-cloud/20-09/prisma-cloud-compute-edition-admin/upgrade/upgrade_process.html)

Community vote distribution

D (100%)

🗳️ 👤 **Spippolo** 6 months, 3 weeks ago

Selected Answer: D

D.

Although older Defenders can interoperate with newer Consoles, their operation is restricted. Older Defenders fully protect your nodes using the policies and settings most recently cached before upgrading Console. They can emit audits to Console and local logs, including syslog. However, they cannot access any API endpoint other than the upgrade endpoint, and they cannot share any new data with Console. No new policies or settings can be pushed from Console to older Defenders. When Defender is in this state, its status is shown as 'Upgrade needed' in Manage > Defenders > Manage. To restore older Defenders to a fully operation state, upgrade them so that their versions match Console's version.

upvoted 1 times

🗳️ 👤 **Spippolo** 6 months, 3 weeks ago

In the event of a communications failure with Console, Defender continues running and enforcing the active policy that was last pushed by the management point. Events that would be pushed back to Console are cached locally until it is once again reachable.

[https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/technology\\_overviews/defender\\_architecture](https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/technology_overviews/defender_architecture)

upvoted 1 times

🗳️ 👤 **Jihe** 7 months ago

D

When version mismatches, Older Defenders fully protect your nodes using the policies and settings most recently cached before upgrading Console. ([https://docs.paloaltonetworks.com/prisma/prisma-cloud/20-09/prisma-cloud-compute-edition-admin/upgrade/upgrade\\_process](https://docs.paloaltonetworks.com/prisma/prisma-cloud/20-09/prisma-cloud-compute-edition-admin/upgrade/upgrade_process) )

upvoted 1 times

How are the following categorized?

- ⇒ Backdoor account access
- ⇒ Hijacked processes
- ⇒ Lateral movement
- ⇒ Port scanning

- A. audits
- B. incidents
- C. admission controllers
- D. models

**Suggested Answer:** B

Community vote distribution

B (100%)

FS9 9 months ago

**Selected Answer: B**

Palo Alto Docs.

upvoted 1 times

Spippolo 1 year, 6 months ago

B.

[https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/runtime\\_defense/incident\\_types](https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/runtime_defense/incident_types)

upvoted 1 times

Spippolo 1 year, 6 months ago

Palo Alto Docs.

upvoted 1 times

Redrum702 1 year, 11 months ago

B

[https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/runtime\\_defense/incident\\_types](https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/runtime_defense/incident_types)

upvoted 3 times



## DRAG DROP -

An administrator needs to write a script that automatically deactivates access keys that have not been used for 30 days.

In which order should the API calls be used to accomplish this task?

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

Select and Place:

**Answer Area**

## Unordered Options

POST https://api.prismacloud.io/login

GET  
https://api.prismacloud.io/access\_keys

PATCH  
https://api.prismacloud.io/access\_keys/  
<id>/status/<status>

## Ordered Options


**Answer Area**

## Unordered Options

POST https://api.prismacloud.io/login

GET  
https://api.prismacloud.io/access\_keys

PATCH  
https://api.prismacloud.io/access\_keys/  
<id>/status/<status>

## Ordered Options

GET  
https://api.prismacloud.io/access\_keys

PATCH  
https://api.prismacloud.io/access\_keys/  
<id>/status/<status>

POST https://api.prismacloud.io/login

Suggested Answer:

 Jihe 1 year ago

The correct order seems to be:

POST > GET > PATCH

1) POST as shown in Step 1 (doc below) Authenticate to obtain a JWT:

--request POST \

'https://api.prismacloud.io/login'

2) GET (access keys)

3) PATCH (Update or Patch access\_keys/status)

<https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/get-started-with-prisma-cloud/access-the-prisma-cloud-api>  
upvoted 3 times

Which method should be used to authenticate to Prisma Cloud Enterprise programmatically?

- A. single sign-on
- B. SAML
- C. basic authentication
- D. access key

**Suggested Answer:** D

Reference:

<https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/get-started-with-prisma-cloud/access-the-prisma-cloud-api.html>

*Community vote distribution*

D (100%)

🗲️ 👤 **Spippolo** 6 months, 3 weeks ago

**Selected Answer: D**

D --> Prisma Cloud requires an API access key to enable programmatic access to the REST API.

upvoted 1 times

🗲️ 👤 **Redrum702** 10 months, 3 weeks ago

D

<https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/get-started-with-prisma-cloud/access-the-prisma-cloud-api.html>

upvoted 1 times



Which option shows the steps to install the Console in a Kubernetes Cluster?

- A. Download the Console and Defender image Generate YAML for Defender Deploy Defender YAML using kubectl
- B. Download and extract release tarball Generate YAML for Console Deploy Console YAML using kubectl
- C. Download the Console and Defender image Download YAML for Defender from the document site Deploy Defender YAML using kubectl
- D. Download and extract release tarball Download the YAML for Console Deploy Console YAML using kubectl

**Suggested Answer: B**

*Community vote distribution*

B (100%)

  **Spippolo** 6 months, 3 weeks ago

**Selected Answer: B**

Download and extract the release tarball of Prisma Cloud Console.

Generate the YAML configuration file for the Console.

Deploy the Console YAML configuration file using kubectl command to apply the configuration to the Kubernetes cluster.

upvoted 2 times

  **Jihe** 7 months ago

B

[https://docs.paloaltonetworks.com/prisma/prisma-cloud/22-06/prisma-cloud-compute-edition-admin/install/install\\_kubernetes](https://docs.paloaltonetworks.com/prisma/prisma-cloud/22-06/prisma-cloud-compute-edition-admin/install/install_kubernetes)

upvoted 1 times

A customer has a requirement to automatically protect all Lambda functions with runtime protection.  
What is the process to automatically protect all the Lambda functions?

- A. Configure a function scan policy from the Defend/Vulnerabilities/Functions page.
- B. Configure serverless radar from the Defend/Compliance/Cloud Platforms page.
- C. Configure a manually embedded Lambda Defender.
- D. Configure a serverless auto-protect rule for the functions.

**Suggested Answer:** D

Reference:

<https://blog.paloaltonetworks.com/prisma-cloud/protect-serverless-functions/>

*Community vote distribution*

D (100%)

🗨️ 👤 **Spippolo** 6 months, 3 weeks ago

**Selected Answer: D**

D.

[https://docs.paloaltonetworks.com/prisma/prisma-cloud/30/prisma-cloud-compute-edition-admin/install/deploy-defender/serverless/auto\\_defend\\_serverless](https://docs.paloaltonetworks.com/prisma/prisma-cloud/30/prisma-cloud-compute-edition-admin/install/deploy-defender/serverless/auto_defend_serverless)

upvoted 1 times

🗨️ 👤 **kemalgoklen** 1 year, 5 months ago

Based on the demo and resource, D is correct.

upvoted 2 times

Which statement accurately characterizes SSO Integration on Prisma Cloud?

- A. Prisma Cloud supports IdP initiated SSO, and its SAML endpoint supports the POST and GET methods.
- B. Okta, Azure Active Directory, PingID, and others are supported via SAML.
- C. An administrator can configure different Identity Providers (IdP) for all the cloud accounts that Prisma Cloud monitors.
- D. An administrator who needs to access the Prisma Cloud API can use SSO after configuration.

**Suggested Answer: A**

Reference:

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

Community vote distribution

B (100%)

🗳️ 👤 **Spippolo** 6 months, 3 weeks ago

For Exclusion B (Tricky question about A).

On Prisma Cloud, you can enable single sign-on (SSO) using an Identity Provider (IdP) that supports Security Assertion Markup Language (SAML), such as Okta, Microsoft Active Directory Federation Services (AD FS), Azure Active Directory (AD), Google, or OneLogin. You can configure only one IdP for all the cloud accounts that Prisma Cloud monitors.

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

upvoted 1 times

🗳️ 👤 **Joe27** 1 year, 8 months ago

**Selected Answer: B**

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

'Prisma Cloud supports IdP initiated SSO, and it's SAML endpoint supports the POST method only.'

upvoted 4 times

🗳️ 👤 **piipo** 1 year, 9 months ago

**Selected Answer: B**

SAML endpoint supports the POST method only

upvoted 1 times

## DRAG DROP -

Match the service on the right that evaluates each exposure type on the left.

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

Select and Place:

**Answer Area**

Financial Information	Drag answer here	Data Security Service
Malware	Drag answer here	Wildfire Service
Health Information	Drag answer here	
Intellectual Property	Drag answer here	


**Answer Area**

Suggested Answer:

Financial Information	Data Security Service	Data Security Service
Malware	Wildfire Service	Wildfire Service
Health Information	Data Security Service	
Intellectual Property	Data Security Service	

Reference:

<https://www.paloaltonetworks.com/prisma/cloud/cloud-data-security>

 **goofball** 11 months, 3 weeks ago

The Data Security capabilities on Prisma Cloud enable you to discover and classify data stored in AWS S3 buckets and protect accidental exposure, misuse, or sharing of sensitive data. To identify and detect confidential and sensitive data, Prisma Cloud Data Security integrates with Palo Alto Networks Enterprise DLP service and provides built-in data profiles. These profiles include data patterns that match sensitive information such as PII, health care, financial information, and intellectual property. In addition to protecting your confidential and sensitive data, the data profiles protect against known and unknown (zero-day) malware threats, using the Palo Alto Networks WildFire service.

upvoted 1 times

What are two ways to scan container images in Jenkins pipelines? (Choose two.)

- A. twistcli
- B. Jenkins Docker plugin
- C. Compute Jenkins plugin
- D. Compute Azure DevOps plugin
- E. Prisma Cloud Visual Studio Code plugin with Jenkins integration

**Suggested Answer:** BE

Community vote distribution

AC (100%)

🗳️ 👤 **Spippolo** 6 months, 3 weeks ago

**Selected Answer:** AC

A --> [https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/continuous\\_integration/jenkins\\_plugin.html](https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/continuous_integration/jenkins_plugin.html)

C --> [https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/continuous\\_integration/jenkins\\_pipeline\\_project](https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/continuous_integration/jenkins_pipeline_project)  
upvoted 1 times

🗳️ 👤 **Chichi23** 8 months ago

What is the correct answer?

The link shared by piipo just give and answer, we are missing the 2nd one...  
upvoted 1 times

🗳️ 👤 **piipo** 1 year, 9 months ago

**Selected Answer:** AC

[https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/continuous\\_integration/jenkins\\_plugin.html](https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/continuous_integration/jenkins_plugin.html)  
upvoted 4 times

A customer wants to harden its environment from misconfiguration.

Prisma Cloud Compute Compliance enforcement for hosts covers which three options? (Choose three.)

- A. Docker daemon configuration files
- B. Docker daemon configuration
- C. Host cloud provider tags
- D. Host configuration
- E. Hosts without Defender agents

**Suggested Answer:** BCD

Community vote distribution

ABD (100%)

🗨️ 👤 **Spippolo** 6 months, 3 weeks ago

**Selected Answer:** ABD

[https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/compliance/host\\_scanning](https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/compliance/host_scanning)

Host configuration: Compliance issues in the host setup.

Docker daemon configuration: Compliance issues that stem from misconfiguring your Docker daemons. Docker daemon derives its configuration from various files, including /etc/sysconfig/docker or /etc/default/docker. Misconfigured daemons affect all container instances on a host.

Docker daemon configuration files: Compliance issues that arise from improperly securing critical configuration files with the correct permissions.

upvoted 3 times

🗨️ 👤 **Jihe** 7 months ago

ABD

[https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/compliance/host\\_scanning](https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/compliance/host_scanning)

upvoted 1 times

🗨️ 👤 **Joe27** 1 year, 8 months ago

**Selected Answer:** ABD

You can e.g. select 'host config', 'daemon config' and 'daemon config files' as types in the compliance rule.

upvoted 2 times



A Prisma Cloud administrator is tasked with pulling a report via API. The Prisma Cloud tenant is located on app2.prismacloud.io. What is the correct API endpoint?

- A. <https://api.prismacloud.io>
- B. <https://api2.eu.prismacloud.io>
- C. <https://api.prismacloud.cn>
- D. <https://api2.prismacloud.io>

**Suggested Answer: A**

Community vote distribution

D (100%)

  **backup\_HM**  2 years, 3 months ago

<https://prisma.pan.dev/api/cloud/api-urls/>

should be D

upvoted 8 times

  **Spippolo**  6 months, 3 weeks ago

**Selected Answer: D**

D.

<https://pan.dev/prisma-cloud/api/cspm/api-urls/>

upvoted 1 times

  **Chichi23** 8 months ago

Backup\_HM is right, the correct one is D

<https://api2.prismacloud.io>

<https://prisma.pan.dev/api/cloud/api-urls/>

upvoted 1 times

A customer has Defenders connected to Prisma Cloud Enterprise. The Defenders are deployed as a DaemonSet in OpenShift. How should the administrator get a report of vulnerabilities on hosts?

- A. Navigate to Monitor > Vulnerabilities > CVE Viewer
- B. Navigate to Defend > Vulnerabilities > VM Images
- C. Navigate to Defend > Vulnerabilities > Hosts
- D. Navigate to Monitor > Vulnerabilities > Hosts

**Suggested Answer:** D

*Community vote distribution*

D (100%)

🗲️ 👤 **Spippolo** 6 months, 3 weeks ago

**Selected Answer: D**

D --> Prisma Cloud also scans your hosts and VM images for vulnerabilities. To see the scan report for your hosts and VM images, go to Monitor > Vulnerabilities > Hosts.

upvoted 1 times

🗲️ 👤 **Redrum702** 10 months, 3 weeks ago

D

[https://github.com/PaloAltoNetworks/prisma-cloud-docs/blob/master/compute/admin\\_guide/vulnerability\\_management/scan\\_reports.adoc](https://github.com/PaloAltoNetworks/prisma-cloud-docs/blob/master/compute/admin_guide/vulnerability_management/scan_reports.adoc)

upvoted 1 times

🗲️ 👤 **vaisat** 1 year, 1 month ago

D correct

upvoted 2 times

DRAG DROP -

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

Select and Place:

**Answer Area**

Unordered Options

Enter RoleARN and SNSARN

Create Stack

Enter SNS Topic in CloudTrail

Create CloudTrail with S3 as storage

Ordered Options


**Answer Area**

Unordered Options

Enter RoleARN and SNSARN

Create Stack

Enter SNS Topic in CloudTrail

Create CloudTrail with S3 as storage

Ordered Options


Create Stack

Create CloudTrail with S3 as storage

Enter SNS Topic in CloudTrail

Enter RoleARN and SNSARN

Suggested Answer:

  **FS9** 9 months ago

- 1 -Create Stack
- 2 - Ener SNS Topic in Cloudtrail
- 3 - Create Cloudtrail with S3 as Storage
- 4 - Enter RoleARN and SNSARN

<https://docs.prismacloud.io/en/classic/cspm-admin-guide/prisma-cloud-data-security/enable-data-security-module/enable-data-security-for-aws-org-account>

upvoted 1 times

  **stock28\_CA** 1 year, 1 month ago

- create stack
  - enter role
  - create cloudtrail
  - enter sns in cloudtrail
- upvoted 4 times

A customer has a requirement to scan serverless functions for vulnerabilities.

Which three settings are required to configure serverless scanning? (Choose three.)

- A. Defender Name
- B. Region
- C. Credential
- D. Console Address
- E. Provider

**Suggested Answer:** BCE

Reference:

[https://docs.paloaltonetworks.com/prisma/prisma-cloud/21-04/prisma-cloud-compute-edition-admin/vulnerability\\_management/serverless\\_functions.html](https://docs.paloaltonetworks.com/prisma/prisma-cloud/21-04/prisma-cloud-compute-edition-admin/vulnerability_management/serverless_functions.html)

Community vote distribution

BCE (100%)

🗉 👤 **Spippolo** 6 months, 3 weeks ago

**Selected Answer: BCE**

B --> Specify which regions to scan in AWS Scanning scope

C --> Select the accounts to scan by credential. If you wish to add an account, click on Add credential.

E --> Provider

[https://docs.paloaltonetworks.com/prisma/prisma-cloud/22-12/prisma-cloud-compute-edition-admin/vulnerability\\_management/serverless\\_functions](https://docs.paloaltonetworks.com/prisma/prisma-cloud/22-12/prisma-cloud-compute-edition-admin/vulnerability_management/serverless_functions)  
upvoted 1 times

🗉 👤 **Jihe** 7 months ago

BCD

[https://docs.paloaltonetworks.com/prisma/prisma-cloud/22-12/prisma-cloud-compute-edition-admin/vulnerability\\_management/serverless\\_functions](https://docs.paloaltonetworks.com/prisma/prisma-cloud/22-12/prisma-cloud-compute-edition-admin/vulnerability_management/serverless_functions)  
upvoted 1 times

🗉 👤 **Redrum702** 10 months, 3 weeks ago

BCE

[https://docs.paloaltonetworks.com/prisma/prisma-cloud/22-12/prisma-cloud-compute-edition-admin/vulnerability\\_management/serverless\\_functions](https://docs.paloaltonetworks.com/prisma/prisma-cloud/22-12/prisma-cloud-compute-edition-admin/vulnerability_management/serverless_functions)  
upvoted 3 times

You are tasked with configuring a Prisma Cloud build policy for Terraform.  
What type of query is necessary to complete this policy?

- A. YAML
- B. JSON
- C. CloudFormation
- D. Terraform

**Suggested Answer: B**

Reference:

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

Community vote distribution



🗨️ 👤 **RJ002** 8 months, 2 weeks ago

**Selected Answer: B**

Build Policies in Prisma Cloud

Prisma Cloud IaC Build policies identify insecure configurations in your IaC templates, including:

AWS CloudFormation Templates (JSON or YAML format).

HashiCorp Terraform templates (HCL or JSON format).

Kubernetes App manifests (JSON or YAML format).

upvoted 1 times

🗨️ 👤 **Leonel01** 1 year, 4 months ago

**Selected Answer: B**

"you can also create configuration policies to scan your Infrastructure as Code (IaC) templates that are used to deploy cloud resources. The policies used for scanning IaC templates use a JSON query instead of RQL."

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

upvoted 2 times

🗨️ 👤 **Jihe** 1 year, 6 months ago

B (JSON)

Build Policies in Prisma Cloud identify insecure configurations in your IaC templates, including:

HashiCorp Terraform templates (HCL or JSON format).

<https://www.paloaltonetworks.com/blog/prisma-cloud/cloud-iac-build-policies/>

upvoted 1 times

🗨️ 👤 **Spippolo** 1 year, 6 months ago

**Selected Answer: D**

D.

You can create custom build policies for the following formats:

Terraform - Policies written using Terraform attributes will apply for Terraform (.tf and plan files).

CloudFormation - Policies written using CloudFormation attributes will apply for CloudFormation, AWS Serverless Application Model (SAM), and Cloud Development Kit (CDK).

<https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-code-security/scan-monitor/custom-build-policies>

upvoted 1 times

🗨️ 👤 **HARRY** 1 year, 10 months ago

**Selected Answer: A**

<https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-code-security/scan-monitor/custom-build-policies>

upvoted 4 times

You have onboarded a public cloud account into Prisma Cloud Enterprise. Configuration Resource ingestion is visible in the Asset Inventory for the onboarded account, but no alerts are being generated for the configuration assets in the account.

Config policies are enabled in the Prisma Cloud Enterprise tenant, with those policies associated to existing alert rules. ROL statements on the investigate matching those policies return config resource results successfully.

Why are no alerts being generated?

- A. The public cloud account is not associated with an alert notification.
- B. The public cloud account does not have audit trail ingestion enabled.
- C. The public cloud account does not access to configuration resources.
- D. The public cloud account is not associated with an alert rule.

**Suggested Answer: A**

Community vote distribution

D (100%)

🗲️ 👤 **Spippolo** 6 months, 3 weeks ago

**Selected Answer: D**

D --> create an alert rule that associates all of the cloud accounts in an account group with the set of policies for which you want Prisma Cloud to generate alerts.

<https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/manage-prisma-cloud-alerts/prisma-cloud-alert-notifications>  
upvoted 1 times

🗲️ 👤 **Jihe** 7 months ago

D

<https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/manage-prisma-cloud-alerts/prisma-cloud-alert-notifications>  
upvoted 1 times

🗲️ 👤 **Joe27** 1 year, 8 months ago

**Selected Answer: D**

The account is not selected in the alert rule.

upvoted 4 times

The security team wants to target a CNAF policy for specific running Containers.  
How should the administrator scope the policy to target the Containers?

- A. scope the policy to Image names.
- B. scope the policy to namespaces.
- C. scope the policy to Defender names.
- D. scope the policy to Host names.

**Suggested Answer: B**

*Community vote distribution*

A (100%)

🗳️ 👤 **Spippolo** 6 months, 3 weeks ago

**Selected Answer: A**

Maybe A for exclusion.  
upvoted 2 times

🗳️ 👤 **marcosvporto** 7 months, 2 weeks ago

**Selected Answer: A**

A  
WAAS is the former CNAF  
[https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/waas/deploy\\_waas/deployment\\_containers](https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/waas/deploy_waas/deployment_containers)  
upvoted 2 times

🗳️ 👤 **marcosvporto** 7 months, 2 weeks ago

A  
WAAS is the former CNAF  
[https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/waas/deploy\\_waas/deployment\\_containers](https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/waas/deploy_waas/deployment_containers)  
upvoted 2 times

🗳️ 👤 **Redrum702** 10 months, 3 weeks ago

B  
[https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/runtime\\_defense/runtime\\_defense\\_containers](https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/runtime_defense/runtime_defense_containers)  
upvoted 1 times



The InfoSec team wants to be notified via email each time a Security Group is misconfigured.  
Which Prisma Cloud tab should you choose to complete this request?

- A. Notifications
- B. Policies
- C. Alert Rules
- D. Events

**Suggested Answer: B**

Reference:

<https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/manage-prisma-cloud-alerts/configure-prisma-cloud-to-automatically-remediate-alerts.html>

Community vote distribution

C (100%)

🗳️ 👤 **SakeBomb** Highly Voted 👍 1 year, 11 months ago

Selected Answer: C

<https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/manage-prisma-cloud-alerts/create-an-alert-rule-for-build-time-checks.html>

upvoted 5 times

🗳️ 👤 **Spippolo** Most Recent 🕒 6 months, 3 weeks ago

Selected Answer: C

C

To send email notifications for alerts triggered by an alert rule, Prisma Cloud provides a default email notification template. You can customize the message in the template using the in-app rich text editor and attach the template to an alert rule. In the alert notification, you can configure Prisma Cloud to send the alert details as an uncompressed CSV file or as a compressed zip file, of 9 MB maximum attachment.

<https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/manage-prisma-cloud-alerts/send-prisma-cloud-alert-notifications-to-third-party-tools>

upvoted 1 times

🗳️ 👤 **Spippolo** 6 months, 3 weeks ago

Tricky question. Inside an "Alert rules" you can configure an "Configure Notifications"

upvoted 3 times

🗳️ 👤 **Jihe** 7 months ago

A

1. Alert Rules, you can enable the optional Auto-Actions, Alert Notifications, and Auto-Remediation
  2. Assign Targets- select Account Groups
  3. Select the policies for which you want this alert rule to trigger alert
  4. Configure Notifications to enable alert Notifications (email)
- (<https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/manage-prisma-cloud-alerts/create-an-alert-rule>)

upvoted 1 times

🗳️ 👤 **Chichi23** 8 months ago

C... alert rules is correct.

To complete the request of notifying the InfoSec team via email each time a Security Group is misconfigured, you should use the "Alerts" tab in Prisma Cloud Enterprise.

You can create an alert rule for misconfigured Security Groups by configuring a policy that checks for Security Group misconfigurations and then associating that policy with an alert rule. In the alert rule, you can specify the email addresses of the InfoSec team to receive the alerts when a Security Group is misconfigured.

To create an alert rule in Prisma Cloud Enterprise:

Go to the "Alerts" tab in the Prisma Cloud Enterprise console.

Click on "Create Rule" button.

Select the policy you want to use to generate alerts for Security Group misconfigurations.

Specify the alert details, such as severity level, notification method, and recipient email addresses.

Save the alert rule.

Once the alert rule is created, the InfoSec team will receive an email notification each time a Security Group is misconfigured, as per the defined policy.

upvoted 1 times

An administrator has access to a Prisma Cloud Enterprise.

What are the steps to deploy a single container Defender on an ec2 node?

- A. Pull the Defender image to the ec2 node, copy and execute the curl | bash script, and start the Defender to ensure it is running.
- B. Execute the curl | bash script on the ec2 node.
- C. Configure the cloud credential in the console and allow cloud discovery to auto-protect the ec2 node.
- D. Generate DaemonSet file and apply DaemonSet to the twistlock namespace.



**Suggested Answer: D**

Reference:

[https://docs.twistlock.com/docs/compute\\_edition/install/install\\_kubernetes.html](https://docs.twistlock.com/docs/compute_edition/install/install_kubernetes.html)

Community vote distribution

B (100%)

  **FS9** 9 months ago

**Selected Answer: B**

Because this in Palo Docs: Run the script to download and run the Defender container image.

This excludes A. The script downloads the image

upvoted 2 times

  **Spippolo** 1 year, 6 months ago

**Selected Answer: B**

B is correct.

[https://docs.paloaltonetworks.com/prisma/prisma-cloud/22-06/prisma-cloud-compute-edition-admin/install/install\\_defender/install\\_host\\_defender](https://docs.paloaltonetworks.com/prisma/prisma-cloud/22-06/prisma-cloud-compute-edition-admin/install/install_defender/install_host_defender)  
upvoted 1 times

  **Chichi23** 1 year, 8 months ago

I would say option A:

To deploy a single container Defender on an EC2 node, you can follow these steps:

Log in to the Prisma Cloud Enterprise console and navigate to the "Defenders" tab.

Click on the "Add Defender" button in the top right corner of the page.

Select "Single Container" from the list of Defender types.

Configure the Defender settings as follows:

Enter a name for the Defender.

Choose the appropriate OS type for the EC2 instance.

Select the "Download Script" option to generate a script that will download and run the Defender container image.

Choose the runtime environment for the container (Docker or Kubernetes).

Copy the script that is generated.


SSH into the EC2 instance where you want to deploy the Defender.

Run the script to download and run the Defender container image.

Verify that the Defender is running by going back to the "Defenders" tab in the Prisma Cloud Enterprise console and checking the status of the Defender you just deployed.

That's it! The single container Defender should now be deployed and protecting your EC2 instance.

upvoted 4 times

  **Joe27** 2 years, 8 months ago

**Selected Answer: B**

[https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/install/install\\_defender/install\\_single\\_container\\_defender](https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/install/install_defender/install_single_container_defender)

upvoted 3 times

A customer wants to turn on Auto Remediation.

Which policy type has the built-in CLI command for remediation?

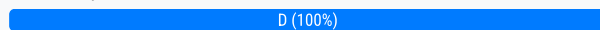
- A. Anomaly
- B. Audit Event
- C. Network
- D. Config

**Suggested Answer:** D

Reference:

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

*Community vote distribution*



🗲️ 👤 **Spippolo** 6 months, 3 weeks ago

**Selected Answer: D**

D.

CLI remediation is available for config from queries only.

upvoted 1 times

🗲️ 👤 **Redrum702** 11 months, 2 weeks ago

D

<https://live.paloaltonetworks.com/t5/blogs/auto-remediation-in-prisma-cloud/ba-p/445343>

upvoted 2 times

A customer is deploying Defenders to a Fargate environment. It wants to understand the vulnerabilities in the image it is deploying. How should the customer automate vulnerability scanning for images deployed to Fargate?

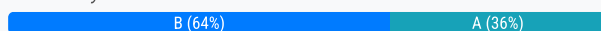
- A. Set up a vulnerability scanner on the registry
- B. Embed a Fargate Defender to automatically scan for vulnerabilities
- C. Designate a Fargate Defender to serve a dedicated image scanner
- D. Use Cloud Compliance to identify misconfigured AWS accounts

**Suggested Answer: A**

Reference:

<https://blog.paloaltonetworks.com/prisma-cloud/securing-aws-fargate-tasks/>

Community vote distribution



🗳️ 👤 **Cosmonauta** 11 months, 3 weeks ago

**Selected Answer: A**

Actually both A and B seem to be correct, I vote for B, because it is more specific.  
upvoted 1 times

🗳️ 👤 **Leonel01** 1 year ago

**Selected Answer: B**

If you use services providing containers on demand, you can run containers, but the service abstracts away the underlying cluster, host, operating system, and software modules. Without access to those hooks, container Defenders can't monitor and protect resources in those environments. Instead, embed an app-embedded Defender directly inside your workload running in the container to establish a point of control. You can manually embed the Defenders or use automated workflows to embed Defenders using Fargate or Dockerfile.

Using Dockerfile, you deploy one app-embedded Defender per container. Using Fargate, you deploy one app-embedded Defender per task.  
upvoted 1 times

🗳️ 👤 **FS9** 1 year, 3 months ago

**Selected Answer: B**

<https://www.paloaltonetworks.com/blog/prisma-cloud/securing-aws-fargate-tasks/>  
upvoted 2 times

🗳️ 👤 **FS9** 1 year, 3 months ago

**Selected Answer: A**

This is about vulnerabilities, not defend runtime.

<https://docs.prismacloud.io/en/classic/compute-admin-guide/vulnerability-management/registry-scanning/configure-registry-scanning>  
upvoted 1 times

🗳️ 👤 **Spippolo** 2 years ago

**Selected Answer: B**

Should be B.

App-Embedded Defenders for Fargate monitor and protect your Fargate tasks to ensure they execute as designed.  
upvoted 1 times

🗳️ 👤 **Redrum702** 2 years, 4 months ago

B:



[https://docs.paloaltonetworks.com/prisma/prisma-cloud/22-06/prisma-cloud-compute-edition-admin/install/install\\_defender/install\\_app\\_embedded\\_defender\\_fargate](https://docs.paloaltonetworks.com/prisma/prisma-cloud/22-06/prisma-cloud-compute-edition-admin/install/install_defender/install_app_embedded_defender_fargate)  
upvoted 1 times

🗳️ 👤 **HARRY** 2 years, 4 months ago

**Selected Answer: B**

[https://docs.paloaltonetworks.com/prisma/prisma-cloud/22-06/prisma-cloud-compute-edition-admin/install/install\\_defender/install\\_app\\_embedded\\_defender\\_fargate](https://docs.paloaltonetworks.com/prisma/prisma-cloud/22-06/prisma-cloud-compute-edition-admin/install/install_defender/install_app_embedded_defender_fargate)

upvoted 3 times

  **Joe27** 3 years, 2 months ago

**Selected Answer: A**

[https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/install/defender\\_types](https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/install/defender_types)

upvoted 2 times

Which container image scan is constructed correctly?

- A. `twistcli images scan --docker-address https://us-west1.cloud.twistlock.com/us-3-123456789 myimage/latest`
- B. `twistcli images scan --address https://us-west1.cloud.twistlock.com/us-3-123456789 myimage/latest`
- C. `twistcli images scan --address https://us-west1.cloud.twistlock.com/us-3-123456789 --container myimage/latest`
- D. `twistcli images scan --address https://us-west1.cloud.twistlock.com/us-3-123456789 --container myimage/latest --details`




**Suggested Answer: C**

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)

Community vote distribution

B (100%)

  **ominator**  2 years, 3 months ago

**Selected Answer: B**

--container is not a flag. Correct answer is B  
upvoted 7 times

  **David2606**  12 months ago

ChiChi23 do not use gpt chat for these questions will give you a wrong answer. the correct answer is B --container is not a flag  
upvoted 1 times



  **Spippolo** 1 year ago

**Selected Answer: B**

B for exclusion. Container sin't a flag.

[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)

upvoted 1 times

  **Chichi23** 1 year, 2 months ago

D.

D. `twistcli images scan --address https://us-west1.cloud.twistlock.com/us-3-123456789 --container myimage/latest --details`

Explanation:

The "--address" flag specifies the address of the Prisma Cloud Console to which Twistcli should connect for image scanning.

The "--container" flag specifies the container image that needs to be scanned.

The "--details" flag provides additional details about the scan results.

upvoted 1 times

  **ominator** 2 years, 3 months ago

--container is not a flag. Correct answer is B  
upvoted 2 times



## DRAG DROP -

An administrator has been tasked with creating a custom service that will download any existing compliance report from a Prisma Cloud Enterprise tenant.

In which order will the APIs be executed for this service?

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

Select and Place:

**Answer Area**

## Unordered Options

POST https://api.prismacloud.io/login

GET  
https://api.prismacloud.io/report

GET  
https://api.prismacloud.io/report/id/  
download

## Ordered Options

**Answer Area**

## Unordered Options

POST https://api.prismacloud.io/login

GET  
https://api.prismacloud.io/report

GET  
https://api.prismacloud.io/report/id/  
download

## Ordered Options

GET  
https://api.prismacloud.io/report

GET  
https://api.prismacloud.io/report/id/  
download

POST https://api.prismacloud.io/login

Suggested Answer:

 **HARRY** Highly Voted 10 months, 3 weeks ago

1. Post /Login
  2. Get /report
  3. Get report/id/download
- upvoted 7 times

 **Spippolo** Most Recent 6 months, 3 weeks ago

- 1 - login
  - 2 - report
  - 3 - download
- upvoted 3 times

Which two processes ensure that builds can function after a Console upgrade? (Choose two.)

- A. allowing Jenkins to automatically update the plugin
- B. updating any build environments that have twistcli included to use the latest version
- C. configuring build pipelines to download twistcli at the start of each build
- D. creating a new policy that allows older versions of twistcli to connect the Console

**Suggested Answer:** AB

*Community vote distribution*

BC (100%)

🗉 👤 **Spippolo** 6 months, 3 weeks ago

**Selected Answer: BC**

BC for exclusion.

upvoted 1 times

🗉 👤 **Chichi23** 8 months ago

BC correct option

upvoted 1 times

🗉 👤 **HARRY** 10 months, 3 weeks ago

**Selected Answer: BC**

A is wrong. Jenkins Plugin can not be upgraded automatically

upvoted 3 times

🗉 👤 **Redrum702** 10 months, 4 weeks ago

A/B:

[https://docs.paloaltonetworks.com/prisma/prisma-cloud/21-08/prisma-cloud-compute-edition-admin/upgrade/upgrade\\_process\\_self\\_hosted](https://docs.paloaltonetworks.com/prisma/prisma-cloud/21-08/prisma-cloud-compute-edition-admin/upgrade/upgrade_process_self_hosted)

upvoted 1 times

The compliance team needs to associate Prisma Cloud policies with compliance frameworks.  
Which option should the team select to perform this task?

- A. Custom Compliance
- B. Policies
- C. Compliance
- D. Alert Rules

**Suggested Answer: B**

Reference:

<https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud-compliance/compliance-dashboard.html>

*Community vote distribution*

B (100%)

🗲️ 👤 **Spippolo** 6 months, 3 weeks ago

**Selected Answer: B**

B --> Compliance Standards in under Policies.

upvoted 1 times

🗲️ 👤 **Jihe** 6 months, 4 weeks ago

B

1) Select Policies

2) Select the policy rule to edit, on 3 Compliance Standards click + and associate the policy with the compliance standard

(<https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud-compliance/create-a-custom-compliance-standard>)

upvoted 1 times

🗲️ 👤 **Chichi23** 8 months ago

Option C.

<https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud-compliance/create-a-custom-compliance-standard>

upvoted 1 times

🗲️ 👤 **Redrum702** 10 months, 4 weeks ago

B

<https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud-compliance/create-a-custom-compliance-standard>

upvoted 2 times

Review this admission control policy:

```
match[{"msg": msg}] {  
  input.request.operation == "CREATE"  
  input.request.kind.kind == "Pod"  
  input.request.resource.resource == "pods"  
  input.request.object.spec.containers[_].securityContext.privileged msg := "Privileged"  
}
```

Which response to this policy will be achieved when the effect is set to `block`?

- A. The policy will block all pods on a Privileged host.
- B. The policy will replace Defender with a privileged Defender.
- C. The policy will alert only the administrator when a privileged pod is created.
- D. The policy will block the creation of a privileged pod.

**Suggested Answer:** C

Community vote distribution

D (100%)

🗳️ 👤 **Spippolo** 6 months, 3 weeks ago

**Selected Answer: D**

D for exclusion.

upvoted 1 times

🗳️ 👤 **Chichi23** 8 months ago

D is correct

upvoted 1 times

🗳️ 👤 **kemalgoklen** 1 year, 5 months ago

**Selected Answer: D**

The question is mentioning about if the effect is set to "block"

Which response to this policy will be achieved when the effect is set to `block`?

Prevent will only terminates related process in container, otherwise block will block the resource creation.

Answer is D

upvoted 4 times

🗳️ 👤 **kemalgoklen** 1 year, 5 months ago

The question is mentioning about if the effect is set to "block"

Which response to this policy will be achieved when the effect is set to `block`?

Prevent will only terminates related process in container, otherwise block will block the resource creation.

Answer is D

upvoted 1 times

Per security requirements, an administrator needs to provide a list of people who are receiving e-mails for Prisma Cloud alerts. Where can the administrator locate this list of e-mail recipients?

- A. Target section within an Alert Rule.
- B. Notification Template section within Alerts.
- C. Users section within Settings.
- D. Set Alert Notification section within an Alert Rule.

**Suggested Answer: A**

*Community vote distribution*

D (100%)

🗲️ 👤 **ominator** Highly Voted 1 year, 9 months ago

Selected Answer: D

<https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/manage-prisma-cloud-alerts/send-prisma-cloud-alert-notifications-to-third-party-tools.html>

upvoted 5 times

🗲️ 👤 **Spippolo** Most Recent 6 months, 3 weeks ago

Selected Answer: D

D --> The new Voice is "Configure Notifications" within an Alert Rule.

upvoted 1 times

🗲️ 👤 **Chichi23** 8 months ago

Selected Answer: D

upvoted 1 times

A customer wants to scan a serverless function as part of a build process.

Which twistcli command can be used to scan serverless functions?

- A. twistcli function scan <SERVERLESS\_FUNCTION.ZIP>
- B. twistcli scan serverless <SERVERLESS\_FUNCTION.ZIP>
- C. twistcli serverless AWS <SERVERLESS\_FUNCTION.ZIP>
- D. twistcli serverless scan <SERVERLESS\_FUNCTION.ZIP>



**Suggested Answer: D**

Reference:

[https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/vulnerability\\_management/serverless\\_functions](https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/vulnerability_management/serverless_functions)

Community vote distribution

D (100%)

  **Spippolo** 6 months, 3 weeks ago

**Selected Answer: D**


D.

[https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/vulnerability\\_management/serverless\\_functions](https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/vulnerability_management/serverless_functions)

You can also use the twistcli command line utility to scan your serverless functions. First download your serverless function as a ZIP file, then run:

```
$ twistcli serverless scan <SERVERLESS_FUNCTION.ZIP>
```

upvoted 2 times

  **Chichi23** 8 months ago

A is correct.

twistcli function scan <SERVERLESS\_FUNCTION.ZIP>

Option D has a typo in the "twistcli " it is missing a T "twisTcli "

twiscli function scan <SERVERLESS\_FUNCTION.ZIP>

upvoted 1 times

  **Redrum702** 10 months, 4 weeks ago

D:

Scanning functions at build time with twistcli

You can also use the twistcli command line utility to scan your serverless functions. First download your serverless function as a ZIP file, then run:

```
$ twistcli serverless scan <SERVERLESS_FUNCTION.ZIP>
```

upvoted 1 times

  **HARRY** 11 months ago

**Selected Answer: D**

<https://docs.paloaltonetworks.com/prisma/prisma-cloud/22-12/prisma-cloud-compute-edition-admin/tools/twistcli>

upvoted 1 times

  **Redrum702** 11 months, 1 week ago

B

The twistcli scan serverless command can be used to scan serverless functions.

upvoted 1 times

A customer has a development environment with 50 connected Defenders. A maintenance window is set for Monday to upgrade 30 stand-alone Defenders in the development environment, but there is no maintenance window available until Sunday to upgrade the remaining 20 stand-alone Defenders.



Which recommended action manages this situation?

- A. Go to Manage > Defender > Manage, then click Defenders, and use the Scheduler to choose which Defenders will be automatically upgraded during the maintenance window.
- B. Find a maintenance window that is suitable to upgrade all stand-alone Defenders in the development environment.
- C. Upgrade a subset of the Defenders by clicking the individual Actions > Upgrade button in the row that corresponds to the Defender that should be upgraded during the maintenance window.
- D. Open a support case with Palo Alto Networks to arrange an automatic upgrade.

**Suggested Answer: A**

*Community vote distribution*


C (100%)

  **Spippolo** 6 months, 3 weeks ago

C.

Alternatively, you can select which Defenders to upgrade. Use this method when you have different maintenance windows for different deployments. For example, you might have an open window on Tuesday to upgrade thirty Defenders in your development environment, but no available window until Saturday to upgrade the remaining twenty Defenders in your production environment. In order to give you sufficient time to upgrade your environment, older versions of Defender can coexist with the latest version of Defender and the latest version of Console.

[https://docs.paloaltonetworks.com/prisma/prisma-cloud/22-12/prisma-cloud-compute-edition-admin/upgrade/upgrade\\_defender\\_single\\_container](https://docs.paloaltonetworks.com/prisma/prisma-cloud/22-12/prisma-cloud-compute-edition-admin/upgrade/upgrade_defender_single_container)  
upvoted 1 times

  **Chichi23** 8 months ago

A.

Go to Manage > Defender > Manage, then click Defenders, and use the Scheduler to choose which Defenders will be automatically upgraded during the maintenance window.  
upvoted 2 times

  **HARRY** 11 months ago

**Selected Answer: C**

[https://docs.paloaltonetworks.com/prisma/prisma-cloud/22-12/prisma-cloud-compute-edition-admin/upgrade/upgrade\\_defender\\_single\\_container](https://docs.paloaltonetworks.com/prisma/prisma-cloud/22-12/prisma-cloud-compute-edition-admin/upgrade/upgrade_defender_single_container)  
upvoted 2 times

What is an example of an outbound notification within Prisma Cloud?

- A. AWS Inspector
- B. Qualys
- C. Tenable
- D. PagerDuty

**Suggested Answer:** D

*Community vote distribution*

D (100%)

🗨️ 👤 **Spippolo** 6 months, 3 weeks ago

**Selected Answer: D**

D is correct. Tested.

upvoted 1 times

🗨️ 👤 **Jihe** 6 months, 4 weeks ago

D

<https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/configure-external-integrations-on-prisma-cloud/prisma-cloud-integrations>

upvoted 1 times

🗨️ 👤 **Chichi23** 8 months ago

Option D.

PagerDuty

upvoted 1 times



A security team has been asked to create a custom policy.

Which two methods can the team use to accomplish this goal? (Choose two.)

- A. add a new policy
- B. clone an existing policy
- C. disable an out-of-the-box policy
- D. edit the query in the out-of-the-box policy

**Suggested Answer:** AB

Reference:

<https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud-policies/manage-prisma-cloud-policies>

*Community vote distribution*

AB (100%)

🗳️ 👤 **Spippolo** 6 months, 3 weeks ago

**Selected Answer: AB**

A and B.

upvoted 1 times

🗳️ 👤 **Chichi23** 8 months ago

AB options

upvoted 1 times

The security auditors need to ensure that given compliance checks are being run on the host.  
Which option is a valid host compliance policy?

- A. Ensure functions are not overly permissive.
- B. Ensure host devices are not directly exposed to containers.
- C. Ensure images are created with a non-root user.
- D. Ensure compliant Docker daemon configuration.

**Suggested Answer: C**

*Community vote distribution*

D (100%)

🗨️ 👤 **stock28\_CA** 7 months ago

<https://docs.prismacloud.io/en/enterprise-edition/content-collections/runtime-security/compliance/operations/host-scanning>

D

upvoted 1 times

🗨️ 👤 **Chichi23** 1 year, 2 months ago

Selected Answer: D

upvoted 1 times

🗨️ 👤 **Joe27** 2 years, 2 months ago

**Selected Answer: D**

There are compliance rules for Docker (CIS v1.3.1) which cover the daemon configuration

upvoted 4 times

A customer wants to be notified about port scanning network activities in their environment.  
Which policy type detects this behavior?

- A. Network
- B. Port Scan
- C. Anomaly
- D. Config

**Suggested Answer: A**

*Community vote distribution*

C (100%)

🗳️ 👤 **Spippolo** 6 months, 3 weeks ago

**Selected Answer: C**

Tested the solution --> C.

<https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud-policies/anomaly-policies>  
upvoted 1 times

🗳️ 👤 **Chichi23** 8 months ago

B. Port Scan

upvoted 1 times

🗳️ 👤 **HARRY** 10 months, 3 weeks ago

**Selected Answer: C**

<https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud-policies/anomaly-policies>  
upvoted 4 times

🗳️ 👤 **Redrum702** 12 months ago

A: Network

<https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud-policies/create-a-policy>  
upvoted 1 times

A security team is deploying Cloud Native Application Firewall (CNAF) on a containerized web application. The application is running an NGINX container. The container is listening on port 8080 and is mapped to host port 80. Which port should the team specify in the CNAF rule to protect the application?

- A. 443
- B. 80
- C. 8080
- D. 8888

**Suggested Answer:** C

Reference:

[https://docs.paloaltonetworks.com/prisma/prisma-cloud/19-11/prisma-cloud-compute-edition-admin/firewalls/deploy\\_cnaf.html](https://docs.paloaltonetworks.com/prisma/prisma-cloud/19-11/prisma-cloud-compute-edition-admin/firewalls/deploy_cnaf.html)

Community vote distribution

C (100%)

🗳️ 👤 **stock28\_CA** 7 months, 2 weeks ago

Port (Required) - For containerized applications, the internal port on which the application is listening. For all other types, the externally facing port.

C

upvoted 1 times

🗳️ 👤 **Spippolo** 1 year ago

**Selected Answer: C**

Should be C --> Specify the ports where the container listens for web traffic.

[https://docs.paloaltonetworks.com/prisma/prisma-cloud/19-11/prisma-cloud-compute-edition-admin/firewalls/deploy\\_cnaf](https://docs.paloaltonetworks.com/prisma/prisma-cloud/19-11/prisma-cloud-compute-edition-admin/firewalls/deploy_cnaf)

upvoted 2 times

🗳️ 👤 **Chichi23** 1 year, 2 months ago

port 80 is correct

upvoted 2 times

Which three types of buckets exposure are available in the Data Security module? (Choose three.)

- A. Public
- B. Private
- C. International
- D. Differential
- E. Conditional

**Suggested Answer:** CDE

Community vote distribution

ABE (100%)

🗳️ 👤 **SakeBomb** Highly Voted 3 years, 5 months ago

Answer is A, B, E.

<https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud-data-security/monitor-data-security-scan-prisma-cloud/exposure-evaluation.html#exposure-evaluation>

upvoted 6 times

🗳️ 👤 **ominator** Highly Voted 3 years, 3 months ago

Selected Answer: ABE

Previous commentor is correct - A, B, E

upvoted 5 times

🗳️ 👤 **Zubair2131** Most Recent 10 months, 2 weeks ago

Answer A,B, and E is correct

upvoted 1 times

🗳️ 👤 **Cosmonauta** 11 months, 3 weeks ago

Selected Answer: ABE

<https://docs.prismacloud.io/en/classic/cspm-admin-guide/prisma-cloud-data-security/monitor-data-security-scan-prisma-cloud/exposure-evaluation>

upvoted 1 times

🗳️ 👤 **Spippolo** 2 years ago

Selected Answer: ABE

A. Public

B. Private

E. Conditional

<https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud-data-security/monitor-data-security-scan-prisma-cloud/exposure-evaluation#exposure-evaluation>

upvoted 1 times

🗳️ 👤 **Chichi23** 2 years, 2 months ago

A. Public Most Voted

B. Private Most Voted

E. Conditional Most Voted

upvoted 1 times

The administrator wants to review the Console audit logs from within the Console.

Which page in the Console should the administrator use to review this data, if it can be reviewed at all?

- A. Navigate to Monitor > Events > Host Log Inspection
- B. The audit logs can be viewed only externally to the Console
- C. Navigate to Manage > Defenders > View Logs
- D. Navigate to Manage > View Logs > History

**Suggested Answer:** D

Reference:

[https://docs.twistlock.com/docs/compute\\_edition/howto/review\\_debug\\_logs.html](https://docs.twistlock.com/docs/compute_edition/howto/review_debug_logs.html)

*Community vote distribution*

D (100%)

🗲️ 👤 **Spippolo** 6 months, 3 weeks ago

**Selected Answer: D**

D --> Manage > View Logs > History

upvoted 1 times

🗲️ 👤 **Chichi23** 8 months ago

D. Navigate to Manage > View Logs > History

upvoted 1 times

🗲️ 👤 **Redrum702** 10 months, 4 weeks ago

D

[https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/audit/audit\\_admin\\_activity](https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/audit/audit_admin_activity)

upvoted 2 times

DRAG DROP -

What is the order of steps in a Jenkins pipeline scan?

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

Select and Place:

**Answer Area**

Unordered Options

Scan Image

Publish Scan Details

Build Image

Commit to Registry

Ordered Options

**Answer Area**

Unordered Options

Scan Image

Publish Scan Details

Build Image

Commit to Registry

Ordered Options

Scan Image

Publish Scan Details

Build Image

Commit to Registry

Suggested Answer:

 **Joe27** Highly Voted 1 year, 8 months ago

It should be:

Build Image, Scan Image, Publish Scan, Commit to Registry (if scan result is passed)

upvoted 9 times

 **Chichi23** Most Recent 8 months ago

BSPC.

Build, Scan, Publish, Commit

upvoted 2 times

DRAG DROP -

What is the order of steps to create a custom network policy?

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

Select and Place:

### Answer Area

#### Unordered Options

Build your Query → New Search or Saved Search

Select Compliance Standards

From Policies tab → Add Policy → Network

Click Confirm

#### Ordered Options

### Answer Area

#### Unordered Options

Build your Query → New Search or Saved Search

Select Compliance Standards

From Policies tab → Add Policy → Network

Click Confirm

#### Ordered Options

From Policies tab → Add Policy → Network

Build your Query → New Search or Saved Search


Select Compliance Standards

Click Confirm

Suggested Answer:

Reference:

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

 **Spippolo** 6 months, 3 weeks ago

Select Policies and click Add Policy

Build the query

Add the compliance standards

Click Submit.

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

upvoted 2 times

 **Redrum702** 10 months, 4 weeks ago

Policies/Build/Compliance and Confirm:

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



upvoted 2 times

DRAG DROP -

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.)

Select and Place:

### Answer Area

config where cloud.type = 'aws'	Drag answer here	Run
\$.resource[*].aws_s3_ bucket exists	Drag answer here	Build
RQL type	Drag answer here	
JSON query type	Drag answer here	

### Answer Area

Suggested Answer:	config where cloud.type = 'aws'	Run	Run
	\$.resource[*].aws_s3_ bucket exists	Run	Build
	RQL type	Build	
	JSON query type	Build	

Reference:

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

 **stock28\_CA** 7 months, 2 weeks ago

Run subtype enables you to scan cloud resources that are already deployed on a supported cloud platform.

Build subtype enables you to scan code repositories and IaC templates that are used to deploy cloud resources.

upvoted 1 times

 **SakeBomb** 2 years, 5 months ago

config where cloud.type='aws' is run

\$.resource[\*].aws\_s3\_bucket exists is build

because

RQL type is run

JSON query type is build

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

build-policy.html

Section 5.2 in the link below

[https://www.paloaltonetworks.com/content/dam/pan/en\\_US/assets/pdf/datasheets/education/pccse-study-guide.pdf](https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/datasheets/education/pccse-study-guide.pdf)

upvoted 4 times


Which statement is true regarding CloudFormation templates?

- A. Scan support does not currently exist for nested references, macros, or intrinsic functions.
- B. A single template or a zip archive of template files cannot be scanned with a single API request.
- C. Request-Header-Field 'cloudformation-version' is required to request a scan.
- D. Scan support is provided for JSON, HTML and YAML formats.

**Suggested Answer: A**

Reference:

<https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud-devops-security/use-the-prisma-cloud-iac-scan-rest-api.html>

  **Chichi23** 8 months ago

I would say:

B. A single template or a zip archive of template files cannot be scanned with a single API request.

upvoted 3 times

A customer has a large environment that needs to upgrade Console without upgrading all Defenders at one time.

What are two prerequisites prior to performing a rolling upgrade of Defenders? (Choose two.)

- A. manual installation of the latest twistcli tool prior to the rolling upgrade
- B. all Defenders set in read-only mode before execution of the rolling upgrade
- C. a second location where you can install the Console
- D. additional workload licenses are required to perform the rolling upgrade
- E. an existing Console at version n-1

**Suggested Answer: BE**

Community vote distribution

AE (100%)

🗳️ 👤 **Spippolo** 6 months, 3 weeks ago

**Selected Answer: AE**

For exclusion.

[https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/upgrade/upgrade\\_process\\_saas](https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/upgrade/upgrade_process_saas)

After the Console has been upgraded, check and upgrade any of the Defenders that have reached the end of their support lifecycle (Defenders are backward compatible for N-2 releases). The Defender release image is built from the UBI8-minimal base image and on upgrade it is a full container image upgrade, which means that the old Defender container is replaced with a new container. Then, upgrade all other Prisma Cloud components, such as the Jenkins plugin.

upvoted 1 times

🗳️ 👤 **Chichi23** 8 months ago

A. manual installation of the latest twistcli tool prior to the rolling upgrade

E. an existing Console at version n-1

upvoted 1 times

🗳️ 👤 **HARRY** 10 months, 3 weeks ago

CE is correct

upvoted 3 times

🗳️ 👤 **Redrum702** 10 months, 3 weeks ago

A/E

[https://github.com/PaloAltoNetworks/prisma-cloud-docs/blob/master/compute/admin\\_guide/upgrade/upgrade\\_process\\_self\\_hosted.adoc](https://github.com/PaloAltoNetworks/prisma-cloud-docs/blob/master/compute/admin_guide/upgrade/upgrade_process_self_hosted.adoc)

upvoted 3 times

An administrator sees that a runtime audit has been generated for a Container. The audit message is `DNS resolution of suspicious name wikipedia.com. type A`.

Why would this message appear as an audit?

- A. The DNS was not learned as part of the Container model or added to the DNS allow list.
- B. This is a DNS known to be a source of malware.
- C. The process calling out to this domain was not part of the Container model.
- D. The Layer7 firewall detected this as anomalous behavior.

**Suggested Answer: A**

*Community vote distribution*

A (100%)

🗲️ 👤 **Spippolo** 6 months, 3 weeks ago

**Selected Answer: A**

A --> To avoid getting such an event for a known and allowed domain, add the domain name to the Runtime rule's Domains list under Allowed in the Networking tab.

upvoted 1 times

🗲️ 👤 **Chichi23** 8 months ago

A. The DNS was not learned as part of the Container model or added to the DNS allow list.

upvoted 1 times

🗲️ 👤 **Redrum702** 10 months, 3 weeks ago

A

[https://docs.paloaltonetworks.com/prisma/prisma-cloud/21-08/prisma-cloud-compute-edition-admin/runtime\\_defense/runtime\\_audits](https://docs.paloaltonetworks.com/prisma/prisma-cloud/21-08/prisma-cloud-compute-edition-admin/runtime_defense/runtime_audits)

upvoted 2 times

Which 'kind' of Kubernetes object is configured to ensure that Defender is acting as the admission controller?

- A. MutatingWebhookConfiguration
- B. DestinationRules
- C. ValidatingWebhookConfiguration
- D. PodSecurityPolicies

**Suggested Answer:** C

Reference:

[https://docs.paloaltonetworks.com/prisma/prisma-cloud/21-04/prisma-cloud-compute-edition-admin/access\\_control/open\\_policy\\_agent.html](https://docs.paloaltonetworks.com/prisma/prisma-cloud/21-04/prisma-cloud-compute-edition-admin/access_control/open_policy_agent.html)

*Community vote distribution*

C (100%)

🗳️ 👤 **Spippolo** 6 months, 3 weeks ago

**Selected Answer: C**

C --> Prisma Cloud provides a dynamic admission controller for Kubernetes and OpenShift that is built on the Open Policy Agent (OPA). In Console, you can manage and compose rules in Rego, which is OPA's native query language. Rules can allow or deny (alert or block) pods. Console pushes your policies to Defender, which enforces them. Decisions made by the system are logged .... In Kubernetes terms, these are known as validating admission webhooks.

upvoted 1 times

🗳️ 👤 **Chichi23** 8 months ago

C. ValidatingWebhookConfiguration

upvoted 1 times

🗳️ 👤 **Redrum702** 10 months, 3 weeks ago

C

[https://docs.paloaltonetworks.com/prisma/prisma-cloud/21-08/prisma-cloud-compute-edition-admin/access\\_control/open\\_policy\\_agent](https://docs.paloaltonetworks.com/prisma/prisma-cloud/21-08/prisma-cloud-compute-edition-admin/access_control/open_policy_agent)

upvoted 1 times

Which three options are selectable in a CI policy for image scanning with Jenkins or twistcli? (Choose three.)

- A. Scope - Scans run on a particular host
- B. Credential
- C. Apply rule only when vendor fixes are available
- D. Failure threshold
- E. Grace Period

**Suggested Answer:** BDE

Community vote distribution



FS9 9 months ago

Selected Answer: ACD

A C D

[https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/continuous\\_integration/set\\_policy\\_ci\\_plugins](https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/continuous_integration/set_policy_ci_plugins)

upvoted 1 times

nede514 1 year, 4 months ago

Selected Answer: ADE

In Prisma: Compute > Defend > Vulnerabilities > Images > CI

Docs: [https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/continuous\\_integration/set\\_policy\\_ci\\_plugins](https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/continuous_integration/set_policy_ci_plugins)

It's shown in step 3, add rule: Scope, failure threshold, and grace period.

upvoted 3 times

Spippolo 1 year, 6 months ago

Selected Answer: ACD

A C D

[https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/continuous\\_integration/set\\_policy\\_ci\\_plugins](https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/continuous_integration/set_policy_ci_plugins)

upvoted 2 times

Chichi23 1 year, 8 months ago

- B. Credential
- D. Failure threshold
- E. Grace Period

upvoted 1 times

Joe27 2 years, 8 months ago

Selected Answer: CDE

Scope is not applicable if you scan with twistcli or Jenkins.

upvoted 3 times





Which component(s), if any, will Palo Alto Networks host and run when a customer purchases Prisma Cloud Enterprise Edition?

- A. Defenders
- B. Console
- C. Jenkins
- D. twistcli

**Suggested Answer:** B

*Community vote distribution*



B (100%)

  **Spippolo** 6 months, 3 weeks ago

**Selected Answer: B**

B --> SaaS solution

upvoted 1 times

  **Chichi23** 8 months ago

A and B comes with Prisma Cloud Ent Edition, hosted and run by PAN

upvoted 1 times

Which port should a security team use to pull data from Console's API?

- A. 53
- B. 25
- C. 8084
- D. 8083

**Suggested Answer:** D

*Community vote distribution*

D (100%)

🗳️ 👤 **Spippolo** 6 months, 3 weeks ago

**Selected Answer: D**

D

Both Console's API and web interfaces, served on port 8083 (HTTPS), require authentication over a different channel with different credentials (e.g. username and password, access key, and so on), none of which Defender holds.

[https://docs.paloaltonetworks.com/prisma/prisma-cloud/22-06/prisma-cloud-compute-edition-admin/technology\\_overviews/defender\\_architecture](https://docs.paloaltonetworks.com/prisma/prisma-cloud/22-06/prisma-cloud-compute-edition-admin/technology_overviews/defender_architecture)  
upvoted 2 times

🗳️ 👤 **Chichi23** 8 months ago

D. 8083

upvoted 1 times

🗳️ 👤 **Redrum702** 10 months, 3 weeks ago

D

<https://prisma.pan.dev/docs/cloud/cwpp/access-api-self-hosted/>  
upvoted 1 times

You are an existing customer of Prisma Cloud Enterprise. You want to onboard a public cloud account and immediately see all of the alerts associated with this account based off ALL of your tenant's existing enabled policies. There is no requirement to send alerts from this account to a downstream application at this time.

Which option shows the steps required during the alert rule creation process to achieve this objective?

- A. Ensure the public cloud account is assigned to an account group Assign the confirmed account group to alert rule Select ☒select all policies☐ checkbox as part of the alert rule Confirm the alert rule
- B. Ensure the public cloud account is assigned to an account group Assign the confirmed account group to alert rule Select one or more policies checkbox as part of the alert rule Confirm the alert rule
- C. Ensure the public cloud account is assigned to an account group Assign the confirmed account group to alert rule Select one or more policies as part of the alert rule Add alert notifications Confirm the alert rule
- D. Ensure the public cloud account is assigned to an account group Assign the confirmed account group to alert rule Select ☒select all policies☐ checkbox as part of the alert rule Add alert notifications Confirm the alert rule

**Suggested Answer: C**

Community vote distribution

A (86%)

14%

 **Joe27** Highly Voted 3 years, 2 months ago

**Selected Answer: A**

A because you want to see alerts for ALL policies and downstream notifications are not required  
upvoted 5 times

 **mridul4c** Most Recent 6 months, 3 weeks ago

**Selected Answer: A**

to ensure all cloud accounts are assigned similar privileges and alerts  
upvoted 1 times

 **Spippolo** 2 years ago

**Selected Answer: A**

A --> I agree with Joe27, "There is no requirement to send alerts from this account to a downstream application at this time", so, the "alert notifications" is useless.  
upvoted 1 times

 **Chichi23** 2 years, 2 months ago

D. Ensure the public cloud account is assigned to an account group Assign the confirmed account group to alert rule Select ☒select all policies☐ checkbox as part of the alert rule Add alert notifications Confirm the alert rule  
upvoted 1 times

 **SakeBomb** 3 years, 5 months ago

**Selected Answer: D**

D because you want to see all of the alerts associated with this account based off ALL of your tenant's existing enabled policies  
upvoted 1 times

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:

**Saml 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.

**Suggested Answer: A**

*Community vote distribution*

A (100%)

FS9 9 months ago

**Selected Answer: A**

Error 4: <https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u000000oMYeCAM>  
upvoted 1 times

Jihe 1 year, 6 months ago

A

See "Error -4" in this KB: <https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u000000oMYeCAM>  
upvoted 3 times

Spippolo 1 year, 6 months ago

D for exclusion.  
upvoted 1 times

Redrum702 1 year, 10 months ago

D  
<https://docs.paloaltonetworks.com/prisma/prisma-sd-wan/prisma-sd-wan-admin/prisma-sd-wan-administrator-authorization-and-authentication/single-sign-on-access-using-saml/saml-setup-errors>  
upvoted 2 times

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

**Suggested Answer:** *BD*

*Community vote distribution*

BD (100%)

🗳️ 👤 **Spippolo** 6 months, 3 weeks ago

**Selected Answer:** BD

BD --> I have tested the solution.

Images

Labels

upvoted 1 times

🗳️ 👤 **Chichi23** 8 months ago

I would say

A. container name

B. image name

upvoted 1 times

🗳️ 👤 **Redrum702** 11 months, 2 weeks ago

BD

[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)

upvoted 2 times



Which policy type in Prisma Cloud can protect against malware?

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

**Suggested Answer: A**

*Community vote distribution*

A (100%)


  **Spippolo** 6 months, 3 weeks ago

**Selected Answer: A**

A --> Use Data Policies to Scan for Data Exposure or Malware

<https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud-data-security/monitor-data-security-scan-prisma-cloud/data-policies>

upvoted 1 times

  **Chichi23** 8 months ago

A. Data

upvoted 1 times

  **Redrum702** 11 months, 2 weeks ago

A

<https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud-data-security/monitor-data-security-scan-prisma-cloud/data-policies>

upvoted 1 times

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

**Suggested Answer: B**

*Community vote distribution*

B (100%)

🗨️ 👤 **Spippolo** 6 months, 3 weeks ago

**Selected Answer: B**

B --> Prisma Cloud Compute Edition is for air-gapped environment too.

upvoted 1 times

🗨️ 👤 **Chichi23** 8 months ago

B. Prisma Cloud Compute Edition

upvoted 1 times

🗨️ 👤 **poiuytr** 11 months, 3 weeks ago

**Selected Answer: B**

Answer B

upvoted 1 times

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

**Suggested Answer:** *B*

  **Jihe** 1 year ago

B

By default, only the System Admin has API access and can enable API access for other administrators. If you have API access, you can create up to two access keys.

<https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/manage-prisma-cloud-administrators/create-access-keys>  
upvoted 1 times

  **Spippolo** 1 year ago

B --> "1 of 2 total available access keys has been successfully generated"

<https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/manage-prisma-cloud-administrators/create-access-keys>  
upvoted 1 times

  **Chichi23** 1 year, 2 months ago

Did not find answer for this quest.

upvoted 1 times



DRAG DROP

-

Put the steps involved to configure and scan using the IntelliJ plugin in the correct order.

Scan using the Prisma Cloud plugin

Add Prisma Cloud plugin

Install IntelliJ IDE

Configure the Prisma Cloud plugin

**Answer Area****Suggested Answer:**

Scan using the Prisma Cloud plugin

Add Prisma Cloud plugin

Install IntelliJ IDE

Configure the Prisma Cloud plugin

**Answer Area**

Add Prisma Cloud plugin

Configure the Prisma Cloud plugin

Scan using the Prisma Cloud plugin

Install IntelliJ IDE

 **HARRY** Highly Voted 10 months, 3 weeks ago

Install, Add, Config, Scan

upvoted 6 times

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

**Suggested Answer: C**

*Community vote distribution*

D (100%)

🗳️ 👤 **Leonel01** 1 year ago

D - It should be with event type RQL, but I did it with config-run policy type as well, in AWS can be done with that type of policy  
upvoted 1 times

🗳️ 👤 **Spippolo** 2 years ago

**Selected Answer: D**

D --> Audit Event—A set of RQL based policies that monitors audit events in your environment for potential policy violations. You create audit policies to flag sensitive events such as root activities or configuration changes that may potentially put your cloud environment at risk. To view all of the audit event policies available, apply a filter for Policy Type and select Audit Event. Refer to Create a Network or Audit Event Policy to learn how to create custom audit event policies.  
upvoted 1 times

🗳️ 👤 **Chichi23** 2 years, 2 months ago

D. audit event  
upvoted 1 times

🗳️ 👤 **poiuytr** 2 years, 5 months ago

**Selected Answer: D**

D  
<https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud-policies/prisma-cloud-threat-detection>  
upvoted 2 times

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 X; config from cloud.resource where api.name = 'aws-ecs-cluster' AND json.rule = status equals ACTIVE and registeredContainerInstancesCount equals 0 as Y; filter '$.X.clusterArn equals $.Y.clusterArn'; show Y;`
- 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[*] contains 0.0.0.0/0 or ipv6Ranges[*].cidrIpv6 contains ::/0))] exists)`

#### Suggested Answer: B

Community vote distribution

B (100%)

 **assadhashmi** 9 months, 4 weeks ago

**Selected Answer: B**

B is the correct answer. Verified in the console on the investigate tab.

upvoted 1 times

 **Spippolo** 1 year ago

**Selected Answer: B**

B is correct.

`config from cloud.resource where api.name = 'aws-iam-get-credential-report' AND json.rule = '(access_key_1_active is true and access_key_1_last_rotated != and _DateTime.ageInDays(access_key_1_last_rotated) > 90) or (access_key_2_active is true and access_key_2_last_rotated != and _DateTime.ageInDays(access_key_2_last_rotated) > 90)'`

upvoted 1 times

 **Jihe** 1 year, 4 months ago

B is correct

As the RQL Lists resource names where access keys are not rotated for 90 days.

(<https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-rql-reference/rql-reference/operators>)

upvoted 2 times

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

**Suggested Answer: A**

*Community vote distribution*

D (100%)

🗳️ 👤 **Spippolo** 6 months, 3 weeks ago

**Selected Answer: D**

D for exclusion.

The Compliance section in Prisma Cloud Console provides visibility into compliance violations and allows administrators to manage and remediate them.

upvoted 2 times

🗳️ 👤 **Chichi23** 8 months ago

D. Compliance

upvoted 2 times

🗳️ 👤 **Redrum702** 10 months, 3 weeks ago

D

<https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud-compliance/compliance-dashboard>

upvoted 1 times

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

**Suggested Answer: C**

*Community vote distribution*

C (100%)

🗳️ 👤 **Spippolo** 6 months, 3 weeks ago

**Selected Answer: C**

C --> Prisma Cloud Labs has developed compliance checks for serverless functions. Currently, only AWS Lambda is supported.

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

upvoted 1 times

🗳️ 👤 **Chichi23** 8 months ago

C. AWS

upvoted 1 times

🗳️ 👤 **Redrum702** 10 months, 3 weeks ago

C

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

upvoted 1 times

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.

**Suggested Answer: A**

*Community vote distribution*

D (100%)

🗳️ 👤 **Spippolo** 6 months, 3 weeks ago

**Selected Answer: D**

D --> I think D, because we have to restrict any container from resolving, we don't need to block the container; so, the correct answer should be "prevent" by default.

upvoted 2 times

🗳️ 👤 **marcosvporto** 7 months, 1 week ago

The question does not refer to delete the container, just to restrict the container from resolving the DNS name. So I would go with D.

upvoted 2 times

🗳️ 👤 **Chichi23** 8 months ago

B. Set `www.evil-url.com` as a blocklisted DNS name in the default Container runtime policy, and set the effect to block.

upvoted 1 times

🗳️ 👤 **HARRY** 10 months, 3 weeks ago

**Selected Answer: D**

D is Correct

upvoted 1 times

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

A. \$ twistcli images scan \

--address \

--user \

--password \

--verbose \

myimage: latest

B. \$ twistcli images scan \

--address \

--user \

--password \

--details \

myimage: latest

C. \$ twistcli images scan \

--address \

--user \

--password \

myimage: latest

D. \$ twistcli images scan \

--address \

--user \

--password \



--console \

myimage: latest

**Suggested Answer: B**

*Community vote distribution*

B (100%)

  **Spippolo** 6 months, 3 weeks ago

**Selected Answer: B**

B --> You can have twistcli generate a detailed report for each scan. The following procedure shows you how to scan an image with twistcli, and then retrieve the results from Console.

[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)

upvoted 1 times

  **Redrum702** 10 months, 3 weeks ago

B

Scan an image named myimage:latest.

\$ twistcli images scan \

--address <COMPUTE\_CONSOLE> \

--user <COMPUTE\_CONSOLE\_USER> \

--password <COMPUTE\_CONSOLE\_PASSWD> \

--details \

myimage:latest

upvoted 2 times

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" },`

**Suggested Answer: A**

*Community vote distribution*

D (100%)

🗳️ 👤 **Spippolo** 6 months, 3 weeks ago

**Selected Answer: D**

Should be D --> List all events with sensitive user actions on GCP.

<https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-rql-reference/rql-reference/event-query/event-query-examples>  
upvoted 2 times

🗳️ 👤 **kalapka** 8 months, 1 week ago

**Selected Answer: D**

Answer D

upvoted 2 times

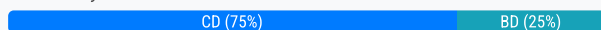


Which two of the following are required to be entered on the IdP side when setting up SSO in Prisma Cloud? (Choose two.)

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

**Suggested Answer:** BD

Community vote distribution



FS9 9 months ago

**Selected Answer:** CD

C. Assertion Consumer Service (ACS) URL

This URL specifies the location where the IdP should send the SAML assertion after authentication. Prisma Cloud needs to know this URL to properly process the SAML response from the IdP.

D. SP (Service Provider) Entity ID

The Service Provider Entity ID uniquely identifies Prisma Cloud as a service provider within the SSO setup. The IdP typically needs to be configured with this ID to establish trust between the IdP and Prisma Cloud.

So, the correct options are C and D.

upvoted 1 times

goofball 1 year, 5 months ago

**Selected Answer:** BD

<https://docs.paloaltonetworks.com/prisma/prisma-access/prisma-access-panorama-integration/authenticate-mobile-users/saml-authentication-using-okta-as-idp-for-users>

upvoted 1 times

Spippolo 1 year, 6 months ago

**Selected Answer:** CD

CD

<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-okta>

upvoted 2 times

Chichi23 1 year, 8 months ago

C. Assertion Consumer Service (ACS) URL

D. SP (Service Provider) Entity ID

upvoted 2 times

Redrum702 1 year, 10 months ago

BD

<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-okta>

upvoted 4 times

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

**Suggested Answer: D**

Community vote distribution

C (100%)

🗳️ 👤 **HARRY** Highly Voted 👍 11 months ago

**Selected Answer: C**

Processes is correct  
upvoted 5 times

🗳️ 👤 **Spippolo** Most Recent 🕒 6 months, 3 weeks ago

**Selected Answer: C**

Should be C.  
upvoted 1 times

🗳️ 👤 **Chichi23** 8 months ago

C is correct  
upvoted 1 times

🗳️ 👤 **Jihe** 10 months ago

C is correct  
([https://docs.paloaltonetworks.com/prisma/prisma-cloud/22-12/prisma-cloud-compute-edition-admin/runtime\\_defense/runtime\\_audits](https://docs.paloaltonetworks.com/prisma/prisma-cloud/22-12/prisma-cloud-compute-edition-admin/runtime_defense/runtime_audits))  
upvoted 2 times

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

**Suggested Answer: A**

Community vote distribution

C (100%)

🗳️ 👤 **Spippolo** 6 months, 3 weeks ago

**Selected Answer: C**

C --> Tested inside console.

Policy name: Objects containing Malware

Description: This policy scans for objects containing Malware using Wildfire as a Service.

upvoted 1 times

🗳️ 👤 **Chichi23** 8 months ago

I would say, option A

upvoted 1 times

🗳️ 👤 **kalapka** 8 months, 1 week ago

C

"Prisma Cloud includes default data policies to help you start scanning. These data policies include predefined data profiles and data patterns that enable you to detect malware and prevent inadvertent or malicious exposure of sensitive data."

upvoted 1 times

🗳️ 👤 **tipzzz** 11 months, 2 weeks ago

**Selected Answer: C**

This policy scans for objects containing Malware using Wildfire as a Service.

upvoted 3 times

🗳️ 👤 **Redrum702** 11 months, 2 weeks ago

Should be A:

Prisma Cloud ships with a simple default vulnerability policy for containers, hosts, and serverless functions. These policies have a rule named Default - alert all components, which sets the alert threshold to low. With this rule, all vulnerabilities in images, hosts, and functions are reported.

upvoted 2 times

🗳️ 👤 **poiuytr** 11 months, 2 weeks ago

**Selected Answer: C**

C

Only: "Objects containing Malware" is default data policy. Class: Vulnerabilities.

upvoted 1 times

🗳️ 👤 **Redrum702** 11 months, 3 weeks ago

A

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

upvoted 1 times

Given the following audit event activity snippet:

```
{
  "payload": {
    "requestMetadata": {
      "callerSuppliedUserAgent": "google-loud-sdk gcloud/274.0.1 command/gcloud.compute.firewall-rules.delete invocation-id/edda7aa325264545a4322f516ec15791 environment/None environment-version/None interactive/False from-script/False python/2.7.15 term/ (Linux 4.14.186-146.268.amzn2.x86_64),gzip(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', 'AuthorizeSecurityGroupIngress', 'CreateVpc', 'DeleteFlowLogs', 'DeleteVpc', 'ModifyVpcAttribute', 'RevokeSecurityGroupIngress')
- D. event from cloud.audit\_logs where operation IN ('v1.compute.networks.delete', 'beta.compute.networks.insert', 'v1.compute.routes.delete', 'v1.compute.firewalls.insert', 'v1.compute.firewalls.delete')

**Suggested Answer: B**

Community vote distribution

D (100%)

🗳️ 👤 **Spippolo** 6 months, 3 weeks ago

**Selected Answer: D**

D for the request "compute.firewalls.delete"

upvoted 2 times

🗳️ 👤 **poiuytr** 11 months, 2 weeks ago

**Selected Answer: D**

Code try to invoke action "compute.firewalls.delete"

upvoted 4 times

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

**Suggested Answer:** ABD

Community vote distribution

ABD (100%)

 **Redrum702** Highly Voted 11 months, 4 weeks ago

ABD

<https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-code-security/get-started/connect-your-repositories/connect-intellij>  
upvoted 5 times

 **Spippolo** Most Recent 6 months, 3 weeks ago


**Selected Answer:** ABD

Access Key.

Secret Key.

Prisma Cloud API URL.

<https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-code-security/get-started/connect-your-repositories/connect-intellij>  
upvoted 1 times

 **Chichi23** 8 months ago

- A. Secret Key
  - B. Prisma Cloud API URL
  - D. Access Key
- upvoted 1 times

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

**Suggested Answer:** BC

Community vote distribution

BD (100%)

  **tipzzz** Highly Voted 1 year, 11 months ago

**Selected Answer:** BD

A sys admin can't create Access Key for others, he can give the right to do it  
upvoted 5 times

  **FS9** Most Recent 9 months ago

**Selected Answer:** BD

A sys admin can't create Access Key for others, he can give the right to do it  
upvoted 1 times

  **Spippolo** 1 year, 6 months ago

**Selected Answer:** BD


When we create an Access Key, we cannot create it for other user.  
We are limited up to 2.

- B. Up to two access keys can be active at any time
  - D. Access keys are used for API calls
- upvoted 3 times


  **Spippolo** 1 year, 6 months ago

When you create an access key, the key is tied to the role with which you logged in and if you delete the role, the access key is automatically deleted.

<https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/manage-prisma-cloud-administrators/create-access-keys>  
upvoted 1 times



  **Chichi23** 1 year, 8 months ago

- C. System Admin can create access key for all users
  - D. Access keys are used for API calls
- upvoted 1 times

  **Redrum702** 1 year, 11 months ago

CD looks to be the better answer:

If you have API access, you can create up to two access keys per role for most roles; some roles such as the Build and Deploy Security role can generate one access key only.  
upvoted 2 times

  **poiuytr** 1 year, 11 months ago

I would say: CD

<https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/get-started-with-prisma-cloud/access-the-prisma-cloud-api>

"Prisma Cloud requires an API access key to enable programmatic access to the REST API" -D

"By default, only the System Admin has API access and can enable API access for other administrators." - C

"If you have API access, you can create up to two access keys per role for most roles" - PER ROLE, so more than two can be active at any time. That's

why I think B is incorrect.

<https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/manage-prisma-cloud-administrators/create-access-keys>  
upvoted 3 times

  **Redrum702** 1 year, 11 months ago

BC

<https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/manage-prisma-cloud-administrators/create-access-keys>  
upvoted 1 times

Given the following RQL:

```
event from cloud.audit_logs where operation IN ('v1.compute.urlMaps.update', 'v1.compute.urlMaps.delete',
'v1.compute.backendServices.delete', 'v1.compute.backendBuckets.delete', 'v1.compute.backendServices.update',
'v1.compute.globalForwardingRules.delete', 'v1.compute.urlMaps.delete', 'v1.compute.targetHttpsProxies.delete',
'v1.compute.targetHttpsProxies.setSslPolicy', 'v1.compute.targetHttpsProxies.setSslCertificates')
```

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,gzip(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": ""

**Suggested Answer: D**

Community vote distribution

B (100%)

🗳️ 👤 **assadhashmi** 9 months, 4 weeks ago

**Selected Answer: B**

Answer is B. See bankendServices.delete

upvoted 1 times

🗳️ 👤 **Spippolo** 1 year ago

**Selected Answer: B**

Should be B. --> Audit event request "backendServices.delete"

upvoted 1 times

🗳️ 👤 **poiuytr** 1 year, 5 months ago

**Selected Answer: B**

"backendServices.delete"

upvoted 4 times



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.

**Suggested Answer: B**

*Community vote distribution*

D (100%)

🗳️ 👤 **Chichi23** 8 months ago

D. The development team should create a WAAS rule targeted at the image name of the pods.  
upvoted 1 times

🗳️ 👤 **HARRY** 11 months ago

**Selected Answer: D**

Image is the correct way of scoping the rule. Although host and image can be used to scope the rule. but the host can have other application pods which can be none web apps. scoping based on Image will make sure the rule only applies to the containers created from the web image.

[https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/waas/deploy\\_waas](https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/waas/deploy_waas)

upvoted 4 times

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.

**Suggested Answer: D**

Community vote distribution



🗳️ 👤 **Leonel01** 1 year ago

**Selected Answer: B**

B - D answer doesn't say anything about production environment. True that D includes all environments meaning includes production but you're doing more than required causing issues in other environments.

upvoted 1 times

🗳️ 👤 **Spippolo** 2 years ago

**Selected Answer: D**

D --> To enable automated remediation, identify the set of policies that you want to remediate automatically and verify that Prisma Cloud has the required permissions in the associated cloud environments. Then Create an Alert Rule for Run-Time Checks that enables automated remediation for the set of policies you identified.

upvoted 1 times

🗳️ 👤 **Jihe** 2 years ago

D

<https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/manage-prisma-cloud-alerts/configure-prisma-cloud-to-automatically-remediate-alerts>

upvoted 1 times

🗳️ 👤 **Chichi23** 2 years, 2 months ago

D. Enable "AWS RDS database instance is publicly accessible" policy and add policy to an auto-remediation alert rule.

upvoted 1 times

🗳️ 👤 **Redrum702** 2 years, 5 months ago

D

<https://live.paloaltonetworks.com/t5/prisma-cloud-articles/prisma-cloud-release-notes-for-july-14-2020/ta-p/340499>

upvoted 2 times

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 CNNF
- 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 CNNF

**Suggested Answer: C**

*Community vote distribution*

C (100%)

🗳️ 👤 **Spippolo** 6 months, 3 weeks ago

**Selected Answer: C**

C --> WAAS is able to enforce rate limit on IPs or sessions to protect against high-rate and "low and slow" application layer DoS attacks.

[https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/waas/waas\\_dos\\_protection](https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/waas/waas_dos_protection)

upvoted 1 times

🗳️ 👤 **Redrum702** 11 months, 4 weeks ago

C

[https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/waas/waas\\_dos\\_protection](https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/waas/waas_dos_protection)

upvoted 4 times

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

**Suggested Answer: B**

*Community vote distribution*

B (100%)

🗨️ 👤 **Spippolo** 6 months, 3 weeks ago

**Selected Answer: B**

Should be B --> Incident Explorer automatically correlates individual events generated by the firewall and runtime sensors to identify unfolding attacks.

upvoted 1 times

🗨️ 👤 **Chichi23** 8 months ago

B. incident

upvoted 1 times

🗨️ 👤 **Redrum702** 10 months, 3 weeks ago

B

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

upvoted 3 times

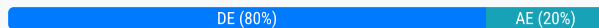
A customer wants to monitor the company's AWS accounts via Prisma Cloud, but only needs the resource configuration to be monitored for now.

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

**Suggested Answer: AE**

*Community vote distribution*



🗳️ 👤 **pooh82** 1 year ago

has anyone passed the exam recently? are these questions valid  
upvoted 3 times

🗳️ 👤 **Spippolo** 1 year ago

**Selected Answer: AE**

A E

To automate the process of creating the Prisma Cloud role that is trusted and has the permissions required to retrieve data on your AWS deployment, Prisma Cloud uses a CFT. The CFT enables the ingestion of configuration data, Amazon S3 flow logs, and AWS CloudTrail logs (audit events) only, and it does not support the ability to enable VPC flow logs for your AWS account.

upvoted 2 times

🗳️ 👤 **Chichi23** 1 year, 2 months ago

- A. Cloudtrail
- E. Role ARN

upvoted 1 times

🗳️ 👤 **Jihe** 1 year, 3 months ago

DE

<https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/connect-your-cloud-platform-to-prisma-cloud/onboard-your-aws-account/set-up-your-prisma-cloud-role-for-aws-manual>

upvoted 1 times

🗳️ 👤 **tipzzz** 1 year, 5 months ago

**Selected Answer: DE**

@Redrum702 Cloudtrail is for API; configuration is About AWS Config

upvoted 4 times

🗳️ 👤 **Redrum702** 1 year, 5 months ago

AE

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

upvoted 2 times

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

**Suggested Answer:** *D*

*Community vote distribution*

D (100%)

🗳️ 👤 **Spippolo** 6 months, 3 weeks ago

**Selected Answer: D**

For exclusion D.

[https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/technology\\_overviews/radar](https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/technology_overviews/radar)  
upvoted 1 times

🗳️ 👤 **Chichi23** 8 months ago

D. Cloud Native Network Firewall  
upvoted 1 times

🗳️ 👤 **Redrum702** 10 months, 3 weeks ago

D  
[https://docs.paloaltonetworks.com/prisma/prisma-cloud/22-06/prisma-cloud-compute-edition-admin/firewalls/cnnf\\_self\\_hosted](https://docs.paloaltonetworks.com/prisma/prisma-cloud/22-06/prisma-cloud-compute-edition-admin/firewalls/cnnf_self_hosted)  
upvoted 2 times

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

**Suggested Answer:** AB

*Community vote distribution*

BC (100%)

  **Redrum702**  11 months, 4 weeks ago

BC

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u000000oMYeCAM>



upvoted 6 times

  **Jobejara7**  4 months, 1 week ago

**Selected Answer:** BC

Per documentation: <https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u000000oMYeCAM>

upvoted 1 times

  **Spippolo** 6 months, 3 weeks ago

**Selected Answer:** BC

- B. Identity Provider Issuer
- C. Certificate

The others one are optionals.

upvoted 1 times

  **Chichi23** 8 months ago

- A. Prisma Cloud Access SAML URL
- B. Identity Provider Issuer

upvoted 2 times

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

**Suggested Answer:** AC

Community vote distribution

BD (100%)

🗳️ 👤 **Redrum702** Highly Voted 👍 1 year, 5 months ago

BD

<https://live.paloaltonetworks.com/t5/blogs/what-is-changing-for-ci-cd-plugins/ba-p/461676>

upvoted 5 times

🗳️ 👤 **Meh057** 9 months, 2 weeks ago

I am going with AC based on the same article. IntelliJ and vsCode are IDEs and the CircleCI and BitBucket CI/CD integration is provided by plugins to those IDEs.

upvoted 1 times

🗳️ 👤 **Meh057** 9 months, 2 weeks ago

never mind that. Based on the next question in the list, I think I misinterpreted this.

upvoted 1 times

🗳️ 👤 **Spippolo** Most Recent 🔄 1 year ago

Selected Answer: BD

BD

<https://live.paloaltonetworks.com/t5/blogs/what-is-changing-for-ci-cd-plugins/ba-p/461676>

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

upvoted 1 times

🗳️ 👤 **Chichi23** 1 year, 2 months ago

B. Visual Studio Code

D. IntelliJ

upvoted 1 times

🗳️ 👤 **Jihe** 1 year, 3 months ago

BD

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

upvoted 2 times



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

**Suggested Answer:** *CD*

*Community vote distribution*

AC (100%)

  **poiuytr** Highly Voted 11 months, 2 weeks ago

**Selected Answer:** AC

AC - category CI/CD

<https://live.paloaltonetworks.com/t5/blogs/what-is-changing-for-ci-cd-plugins/ba-p/461676>

upvoted 5 times

  **Spippolo** Most Recent 6 months, 3 weeks ago

**Selected Answer:** AC

AC



<https://live.paloaltonetworks.com/t5/blogs/what-is-changing-for-ci-cd-plugins/ba-p/461676>

upvoted 1 times

  **Redrum702** 11 months, 2 weeks ago

I agree with AC

upvoted 4 times

  **Redrum702** 11 months, 3 weeks ago

Disregard the BC - It should be AD

upvoted 2 times

  **Redrum702** 11 months, 4 weeks ago

BC

<https://live.paloaltonetworks.com/t5/blogs/what-is-changing-for-ci-cd-plugins/ba-p/461676>

upvoted 1 times

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)

**Suggested Answer: C**

Community vote distribution

E (100%)

 **tipzzz** Highly Voted 1 year, 5 months ago

**Selected Answer: E**

E --> Check question 77

upvoted 5 times

 **goofball** Most Recent 11 months ago

D

You can choose one or both the policy subtypes options:

Run subtype enables you to scan cloud resources that are already deployed on a supported cloud platform.

Build subtype enables you to scan code repositories and IaC templates that are used to deploy cloud resources.

upvoted 1 times

 **goofball** 11 months ago

Correction E\* JSON query is employed when scanning an IAC .. hence policy type would be Build.

upvoted 1 times

 **Spippolo** 1 year ago

**Selected Answer: E**

E --> The correct place to add the JSON query when creating a Config policy is in the "Build Your Rule (Build tab)" of the Config policy creation. In the Build Your Rule section, you can define the conditions and rules using JSON-based queries to specify the desired policy criteria.

RQL type is run

JSON query type is build --> The policies used for scanning IaC templates use a JSON query instead of RQL.

upvoted 1 times

 **Jihe** 1 year ago

D

The doc below shows: in Step 3 select Subtype

Select Run or Build

in Step 5 Under Run tab


Build the query to define the match criteria for your policy.

2) Add a rule for the Build phase.

\*Build phase policies do not support remediation CLI; however add the instructions for manually fixing the issue.

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

upvoted 1 times

 **Chichi23** 1 year, 2 months ago

E. Build Your Rule (Build tab)

upvoted 1 times

  **Redrum702** 1 year, 5 months ago

C

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


upvoted 1 times

  **Redrum702** 1 year, 5 months ago

Correct is D

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

upvoted 4 times

  **poiuytr** 1 year, 5 months ago

Agree:

config from cloud.resource where json.rule = \$.resource[\*].aws\_s3\_bucket exists

is OK

upvoted 3 times

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

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

**Suggested Answer:** AD

Community vote distribution

AC (100%)

🗳️ 👤 **Spippolo** 6 months, 3 weeks ago

**Selected Answer:** AC

A --> policy.class

C --> policy.policyMode

<https://pan.dev/prisma-cloud/api/cspm/get-policy-filters-and-options/>

upvoted 1 times

🗳️ 👤 **Spippolo** 6 months, 3 weeks ago

A --> policy.label

C --> policy.policyMode

upvoted 1 times

🗳️ 👤 **Redrum702** 11 months, 3 weeks ago

AC

<https://prisma.pan.dev/api/cloud/cspm/policy/>

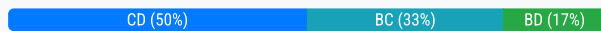
upvoted 4 times

Which two options may be used to upgrade the Defenders with a Console v20.04 and Kubernetes deployment? (Choose two.)

- A. Run the provided curl | bash script from Console to remove Defenders, and then use Cloud Discovery to automatically redeploy Defenders.
- B. Remove Defenders DaemonSet, and then use Cloud Discovery to automatically redeploy the Defenders.
- C. Remove Defenders, and then deploy the new DaemonSet so Defenders do not have to automatically update on each deployment.
- D. Let Defenders automatically upgrade.

**Suggested Answer:** AB

*Community vote distribution*



FS9 9 months ago

**Selected Answer:** BD

A is excluded, does not makes sense.

Defenders are deployed via daemon set. Remove Defenders without removing deamon set will recreate agin. So C is excluded.

upvoted 1 times

Spippolo 1 year, 6 months ago

**Selected Answer:** BC

C --> Delete the Defender DaemonSet. Generate a defender.yaml file. Deploy the Defender DaemonSet.

B --> For excluson

[https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/upgrade/upgrade\\_defender\\_daemonset](https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/upgrade/upgrade_defender_daemonset)

upvoted 2 times

kalapka 1 year, 8 months ago

**Selected Answer:** CD

C, D - Correct!

upvoted 3 times