

Prismacloud Workflow



1

Navigate to console.cloud.google.com/kubernetes/clusters/details

2

Click here.

Backup for GKE	Release channel	Regular channel
Security Posture	Version	1.24.8-gke.2000
Marketplace	Total size	3
Release Notes	External endpoint	34.70.202.111 Show cluster certificate
	Internal endpoint	10.128.0.5 Show cluster certificate

CLOUD SHELL

Terminal (valued-base-377112) X + ▾

```
Cloud Shell! Type "help" to get started.
Cloud Platform project in this session is set to valued-base-377112.
cloud config set project [PROJECT_ID] to change to a different project.
doyinsola@cloudshell:~ (valued-base-377112)$ █
```

- 3 Click "akanfedoyinsola@cloudshell:~ (valued-base-377112)\$ if [[! -f ./twistcli || \$(./twistcli --version) != *"22.12.427"*]]; then curl --progress-bar..."

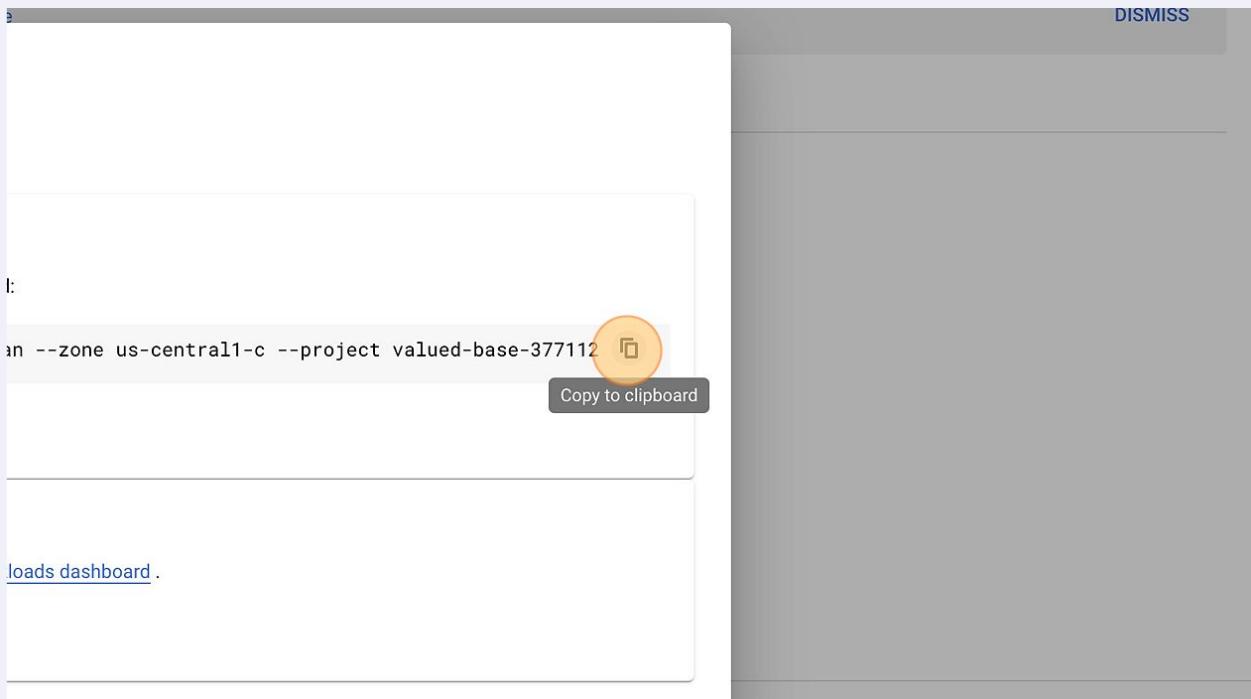
The screenshot shows the Cloud Shell interface with a terminal window titled '(valued-base-377112)'. The terminal displays the following output:

```
Welcome to Cloud Shell! Type "help" to get started.
Your Cloud Platform project in this session is set to valued-base-377112.
Use "gcloud config set project [PROJECT_ID]" to change to a different project.
akanfedoyinsola@cloudshell:~ (valued-base-377112)$ if [[ ! -f ./twistcli || $(./twistcli --version) != *"22.12.427"* ]]; then curl --progress-bar..."
```

- 4 Click "CONNECT"

The screenshot shows the GKE Cluster Overview page for 'cluster-1stan'. At the top, there are buttons for 'DELETE', 'ADD NODE POOL', 'DEPLOY', 'CONNECT' (which is highlighted with a yellow circle), and 'DUPLICATE'. Below the buttons, a note says 'Protect your workloads by enabling Backup for GKE. [Learn more](#)'. The main section shows the cluster status: 'CONNECTED' to the cluster, 'Cloud Shell' access, and 'Logs'. A note says 'Connect to your cluster via command-line or using a dashboard.' Below this, there's a 'Command-line access' section with instructions to run 'kubectl' commands to get credentials for 'us-central1-c'. At the bottom, it shows 'Regular channel' and 'UPGRADE AVAILABLE'.

5 Click here.



6 Click here.

RUN IN CLOUD SHELL

Cloud Console dashboard

You can view the workloads running in your cluster in the Cloud Console [Workloads dashboard](#).

[OPEN WORKLOADS DASHBOARD](#)

```
(optional flags)
gion | --zone
```

```
, run:
```

- 7 Click "akanfedoyinsola@cloudshell:~ (valued-base-377112)\$"

The screenshot shows the Cloud Shell interface. At the top, there's a navigation bar with 'Regular channel' and 'UPGRADE AVAILABLE'. Below it is a table with cluster information:

1.24.8-gke.2000	3	34.70.202.111	Show cluster certificate
10.128.0.5		10.128.0.5	Show cluster certificate

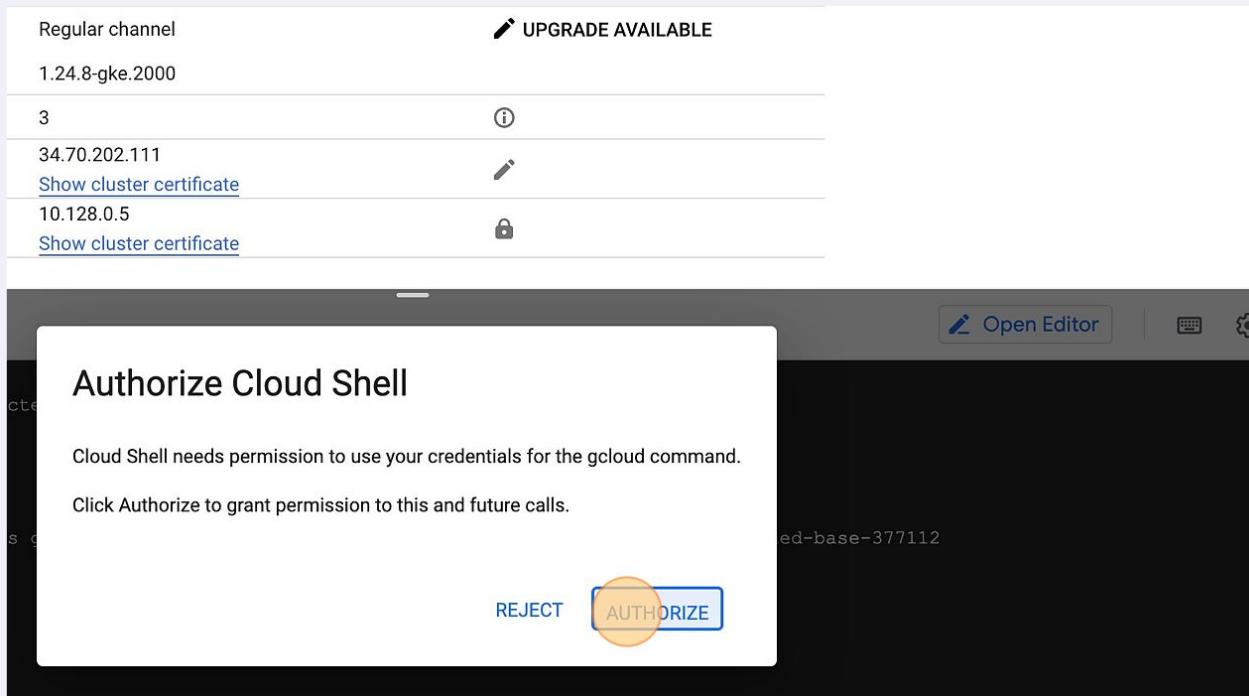
Below the table is a large black terminal window containing the following text:

```
argument --project: expected one argument
AME [optional flags]
--region | --zone

lags, run:
```

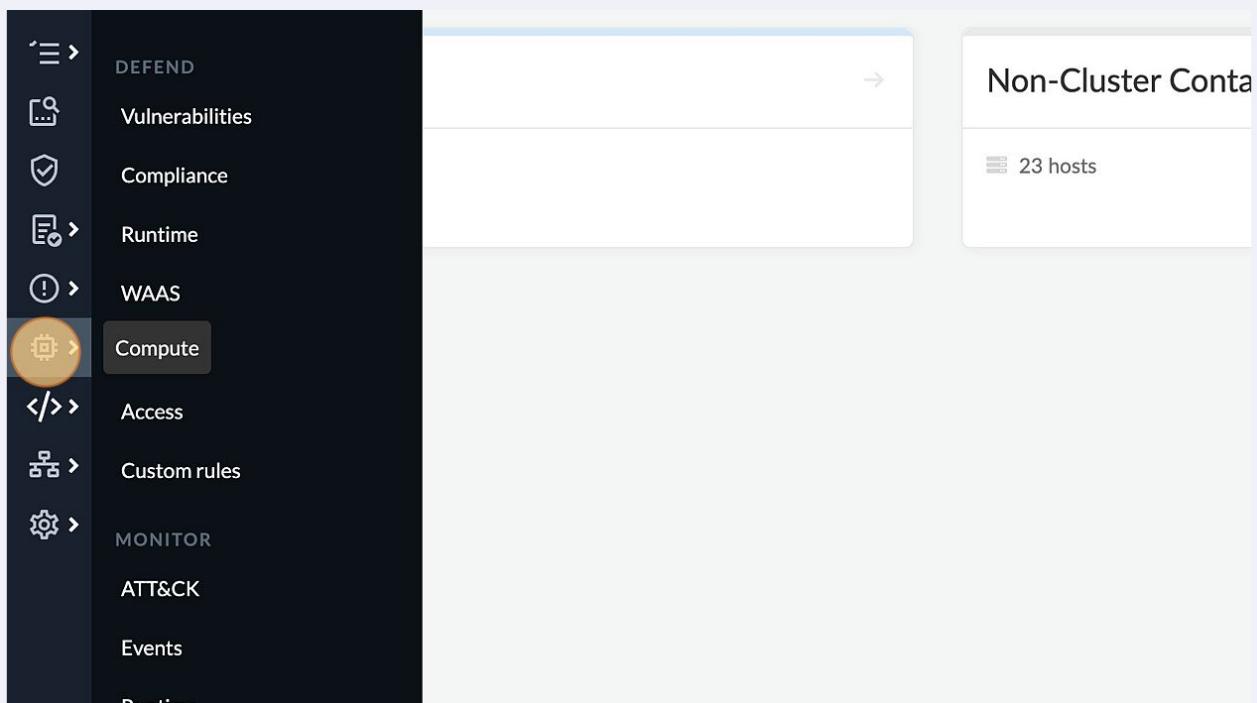
A small orange circle is overlaid on the terminal window.

- 8 Click "AUTHORIZE"



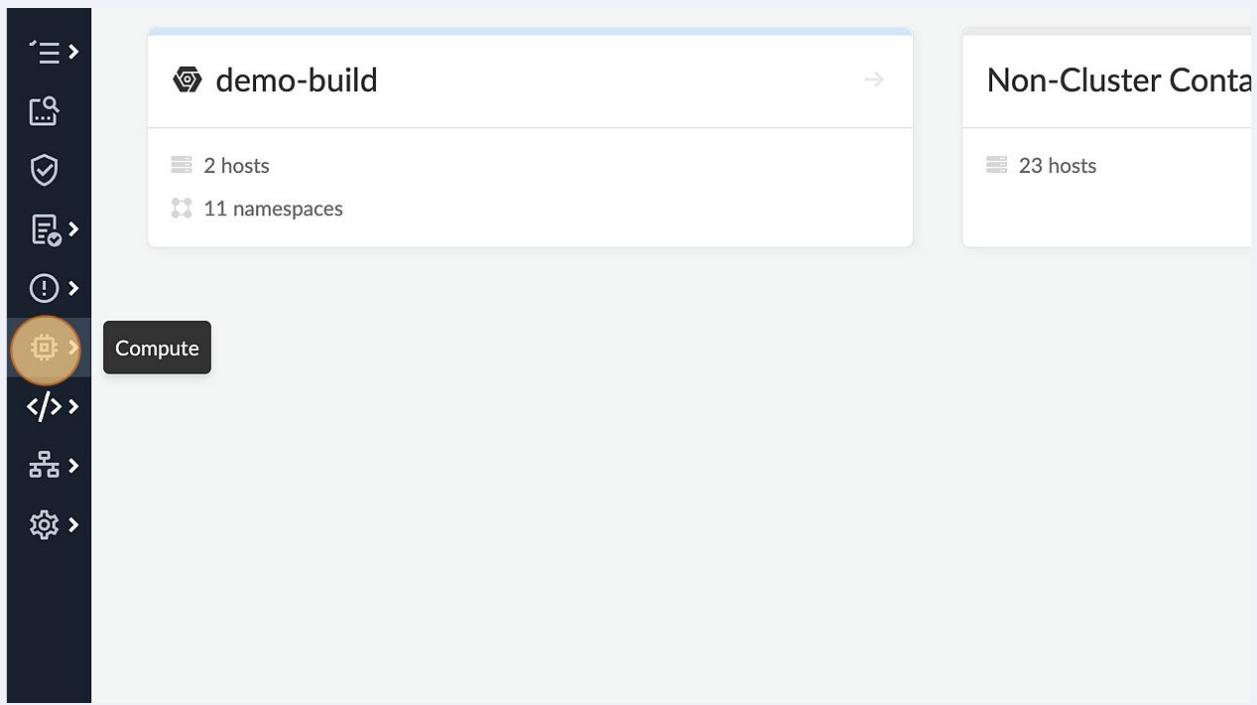
9 Switch to tab "Prisma Cloud | Compute"

10 Click this icon.



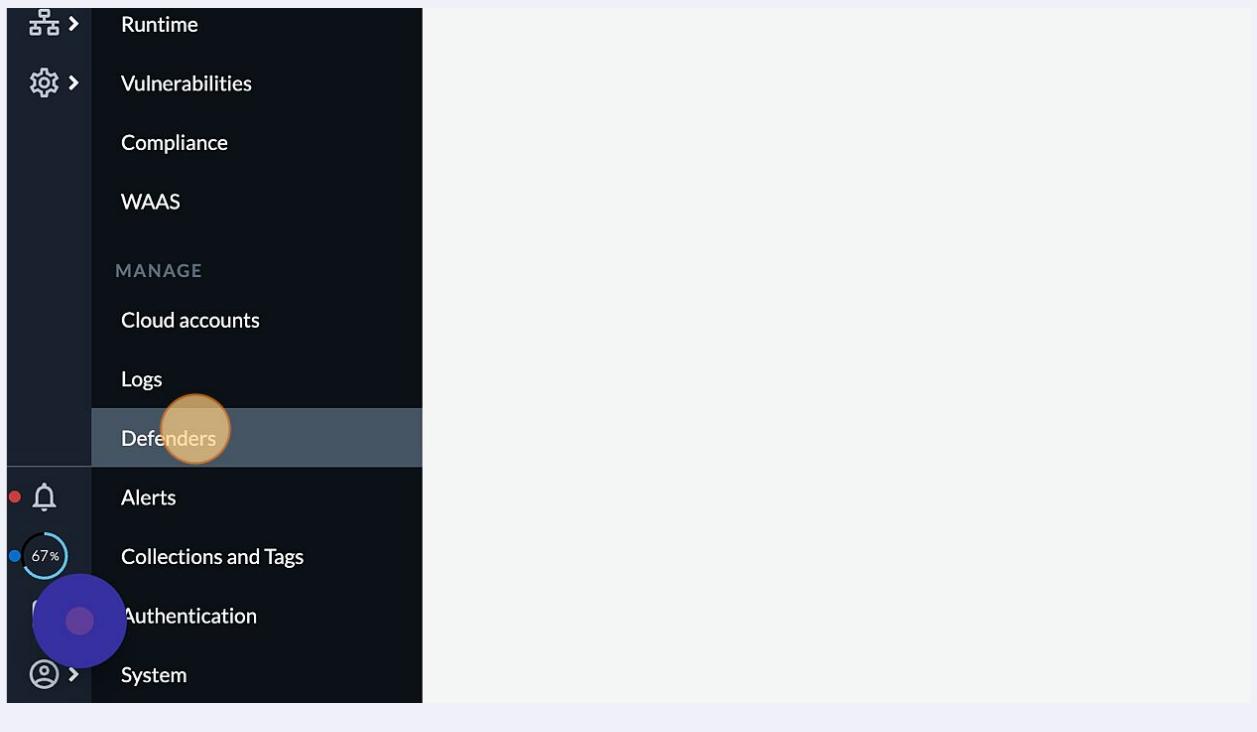
11

Click this icon.



12

Click "Defenders"



13 Click "Manual deploy"

The screenshot shows the 'Defenders' section of the Prisma Cloud console. It includes tabs for 'Auto-defend' and 'Defenders'. Below these are two buttons: 'Manual deploy' (highlighted with a yellow circle) and 'Auto-deploy'. A table lists various defenders with columns for Version, Cluster, and Type. The table shows entries like 'c.cto-demos-245420.internal' (Version 22.06.228, Host Defender - Linux) and 'demo-twistlock.com' (Version 22.12.427, DaemonSet CRI on Linux).

	Version	Cluster	Type
c.cto-demos-245420.internal	22.06.228		Host Defender - Linux
demo-twistlock.com	22.12.427	demo-build	DaemonSet CRI on Linux

14 Click this icon.

The screenshot shows the 'Orchestrator' tab selected in the 'Defender' configuration interface. It displays fields for 'Workstation platform' (Linux x86_64), 'Download file' (YAML and Helm chart download links), and 'Installation scripts' (Install and Uninstall scripts). The 'Install' script is shown in a code block and has a 'Copy' icon next to it, which is highlighted with a yellow circle.

```
if [[ ! -f ./twistcli || $(./twistcli --version) != *"22.12.427"* ]]; then
curl --progress-bar -L -k --header "authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyljoiYW9ndW5s
```

15 Click here.

Backup for GKE

Release channel	Regular channel
Version	1.24.8-gke.2000
Total size	3
External endpoint	34.70.202.111 Show cluster certificate
Internal endpoint	10.128.0.5 Show cluster certificate

CLOUD SHELL

Terminal (valued-base-377112) X + ▾

```
(gcloud.container.clusters.get-credentials) argument --project: expected one argument
gcloud container clusters get-credentials NAME [optional flags]
optional flags may be --help | --internal-ip | --region | --zone

Detailed information on this command and its flags, run:
gcloud container clusters get-credentials --help
doyinsola@cloudshell:~ (valued-base-377112)$ gcloud container clusters get-credentials cluster-1stan --zone
  Using cluster endpoint and auth data.
  A config entry generated for cluster-1stan.
doyinsola@cloudshell:~ (valued-base-377112)$ █
```

16 Click here.

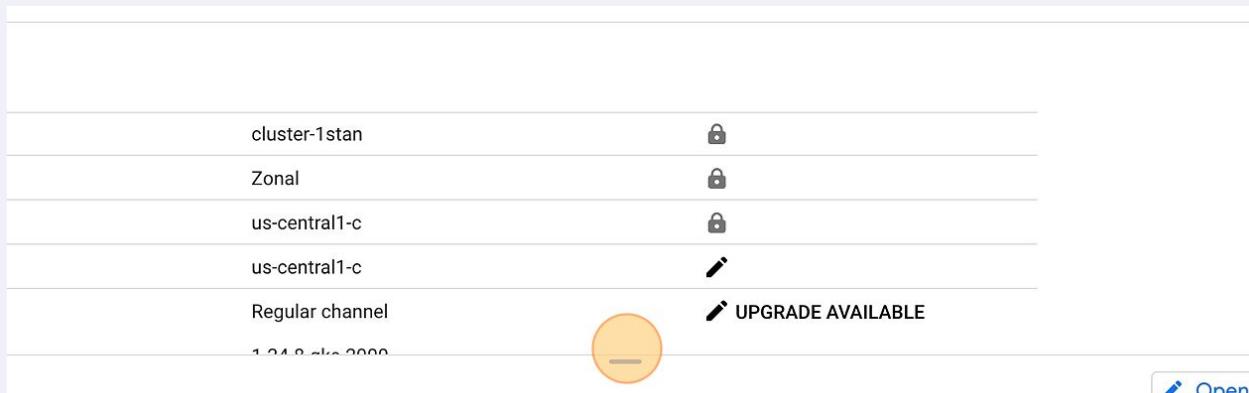
us-central1-c

Regular channel	UPGRADE AVAILABLE
1.24.8-gke.2000	ⓘ
3	ⓘ
34.70.202.111 Show cluster certificate	ⓘ
10.128.0.5 Show cluster certificate	ⓘ

Open

```
Vkhsd1pVbGtJam94TENKelpXeGxZM1JsWkVOMWMzUnZiV1Z5VG1GdFpTSTZJbE5YVhOdFlVTnNiM1ZrTW1Jc0luTmxjM05wYjI1VWFXMWxi
m9ZWB5FW1dabGJtUmxjbEJsY20xcGMzTnbimjV6SwPwMGNuVmxBQ0psZUhBaU9qRTJ0e1u0T0Rnek5qWXNJBwxcZENJNk1UWTNOVGc0Tnpjm
lKUWNtbHpiV0VnUTJ4dmRXUWdVMFVnVkdWaGJTSjkuYklvWGJuXzF6QWtPeHF1VzFncXFSMGFwdDFLWl1CaExvdz13dUFpSuphcyIsImV4cC
.twistlock.com/pandemoapp2-1234/api/v1/util/twistcli > twistcli; chmod +x twistcli; fi; ./twistcli defender
W5szWtlQHBhbG9hbHRvbmV0d29ya3MuY29tIiwiZ9sZSI6ImFkbWluIiwiZ3JvdXBzIjpudWxsLCJyb2x1UGVybXMiOltbMjU1LDI1NSwyN
oiZX1KaGJHY21PaUpjVXpJMU5pSjkuZX1KemRXSWlPaUpoYjJkMWJteGxhM1ZBY0dGc2TyRnNRz11WlhSM2IzSnJjeTVqYjIwaUxDSpaWE
NVGd5TRnME9UWLMQ0pwY0VGAlpISmxjM01pT2lJek5DNDNOQ20TkMOMU1TSXNbWx6Y31JNK1taDBkSEJ6T2k4d1LYQnBNaTV3Y21semJ
alpYTnpJanBtWVd4elpYMHNJblZ6WlhKU2IyeGxWSGx3WlU1aGJXWVlPaUpUZVhOMFpXMGdRV1J0YVc0aUxDsNbJMU5UVDFObGMzTnBiMjRp
0ZqYkc5MvpDNXBieUlzSW5We1pYS1NiMnhsVkhsd1pVbGtJam94TENKelpXeGxZM1JsWkVOMWMzUnZiV1Z5VG1GdFpTSTZJbE5YVhOdFlVT
1UZG1OaTaB5TW1VMV16UXdZV05oTm1NaUxZn9ZWE5FW1dabGJtUmxjbEJsY20xcGMzTnBiMjV6SwPwMGNuVmxBQ0psZUhBaU9qRTJ0e1u0T0
qYjIwaUxDs1FjM1Z5W05c1pVNWhiV1VpT2lKUWNtbHpiV0VnUTJ4dmRXUWdVMFVnVkdWaGJTSjkuYklvWGJuXzF6QWtPeHF1VzFncXFSMGF
XG-M442iZx4 --address https://us-east1.cloud.twistlock.com/pandemoapp2-1234 --cluster-address us-east1.cloud
```

17 Click here.



```
i container clusters get-credentials cluster-1stan --zone us-central1-c --project valued-base-377112
```

```
! -f ./twistcli || $(./twistcli --version) != *"22.12.427"* ]]; then curl --progress-bar -L -k --header "aut
Iiwicm9sZSI6ImFkbWluIiwicZ3JvdXBzIjpudWxsLCJyb2xlUGVybXMiOltbMjU1LDI1NSwyNTUsMjU1LDI1NSwxMjcsMV0sWzI1NSwyNTUsN
nRXSWlPaUpoYjKmWJteGxhM1ZBY0dGc2IyRnNkRz1lWhSM2IzSnjeTVqYjIwaUxDsnpaWeoyYVdObFZYTmhaM1ZQYm14NU1qcDBjbzstP
t2IJe5DNDNOQzQ0Tkm0Mu1TSXNjbWx6Y3lJNkltadBkSEJ6T2k4d1lYQnBNatv3Y21semJXRmpirRzkxWkM1cGJ5SXNbdkpsYzNSeWFXTjF
veGxWSGx3WlU1aGJXVWlPaUpUzVhOMFpXMGdRV1J0YVc0aUxDsnpBjM5UVDFobGMzTnBiMjRpT25SeWRXVNjBxhoYzNSTWiYzHB1bFJwYldV
Vkhds1pVbJtJam94TENkelpXeGxM1JsWkVOMWMzUnZiV1Z5VG1GdFpTSTZJbE5YVhOdFlVTnNiM1ZrTWlJc0luTmxjM05wYjI1VWFXMWxiM
n9ZWE5FWldabGJtUmxbEJyS20xcGMzTnBiMjV6SpwMNgNuVmxBM0QpsZuhBaU9qRTJoelU0TORek5qWXNjBwXoZENJNk1UWTNOVGc0Tnpjm
lKUWNtbHpiV0VnUTJ4dmRXUwdVMFVnVkdWaGJTSjkuYklvWGJuXzF60WtPeHF1VzFncXFSMGEWdFLWllCaExvdz13dUFoSUphcyIsimV4cC
```

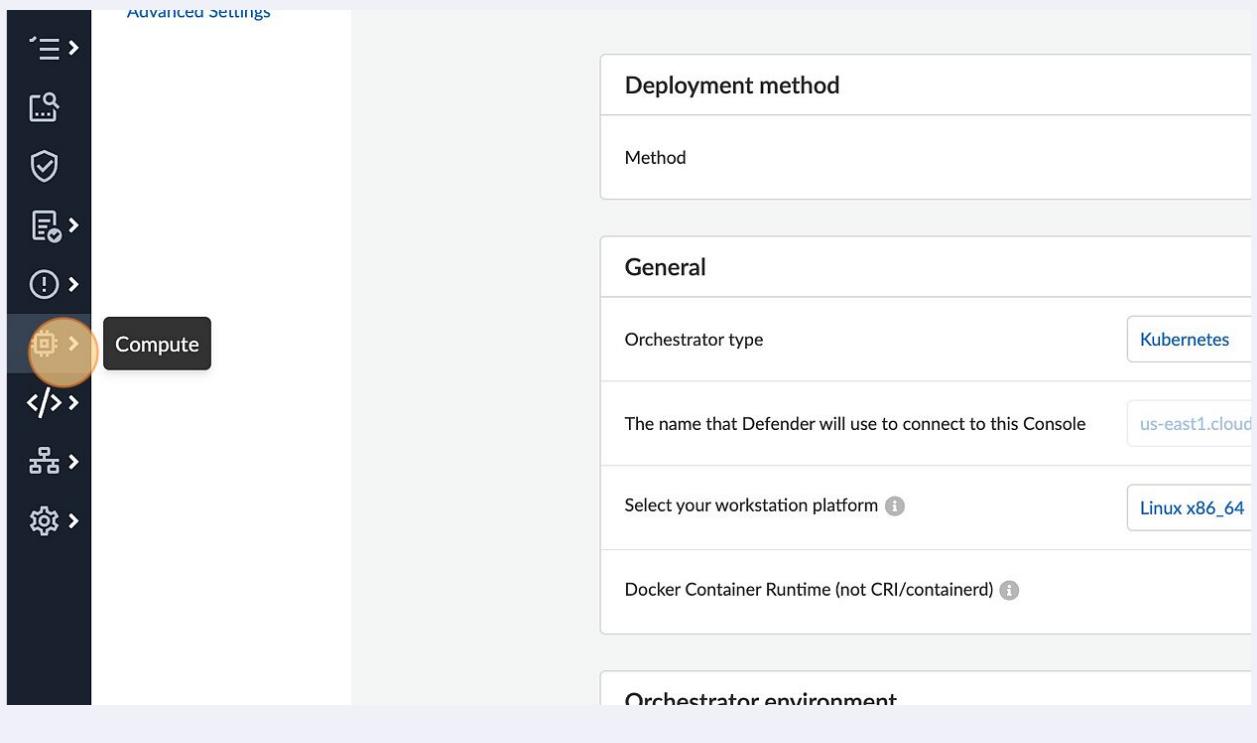
18 Click "Defender daemonset installation completed"

```
optional flags may be --help | --internal-ip | --region | --zone

For detailed information on this command and its flags, run:
  gcloud container clusters get-credentials --help
akanfedoyinsola@cloudshell:~ (valued-base-377112)$ gcloud container clusters get-credentials cluster-1stan -
Fetching cluster endpoint and auth data.
kubeconfig entry generated for cluster-1stan.
akanfedoyinsola@cloudshell:~ (valued-base-377112)$ if [[ ! -f ./twistcli || $(./twistcli --version) != *"22.
CJ9.eyJ1c2VyIjoiYW9ndW5sZwtlQHbhg9hbHRvbmv0d29ya3MuY29tIiwicm9sZSI6ImFkbWluIiwicZ3JvdXBzIjpudWxsLCJyb2xlUGV
yjQ5Nywic2Fhc1Rva2VuIjoiZX1KaGJHY21pAUpJVXpJMUSpSjkuZX1KemRXSWlPaUpoYjKmWJteGxhM1ZBY0dGc2IyRnNkRz1lWhSM2IzS
9pSTRNRFkzTnpVME9UUTTRNvGd5TVRnME9UWW1lMQ0pwY0VGAlpISmxjM01pT2lJek5DNDNOQzQ0Tkm0Mu1TSXNjbWx6Y3lJNkltadBkSEJ6T2
oYzA5dWJ1bFnNaV0ZrUVd0alpYTnpJanBtWVd4elpYMHNjb1Z6WhlKU2IyeGxWSGx3WlU1aGJXVWlPaUpUzVhOMFpXMGdRV1J0YVc0aUxDsN
OHZZWEjwTWk1d2NtbHpiV0ZgYkc5MvpDNXBieUlzSw5We1pYS1NiMhsVkhds1pVbGtJam94TENkelpXeGxZM1jsWkVOMWMzUnZiV1Z5VG1G
1MweE9HUTFMVFjtWlRrdFlUZG10aTB5TW1VMV16UXdZv05oTm1NaUxDsM9ZWE5FWldabGJtUmxbEJyS20xcGMzTnBiMjV6SpwMNgNuVmxBM
NkRz1lWhSM2IzSnjeTVqYjIwaUxDsFjM1Z5VW05c1pVNWHiV1VpT21KUWNtbHpiV0VnUTJ4dmRXUwdVMFVnVkdWaGJTSjkuYklvWGJuXz
_7xxZpcYp-f28-nw4Hmt-XG-M442izx4 --address https://us-east1.cloud.twistlock.com/pandemoapp-1234/api/v1/util/twistcli
n eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXCVJ9.eyJ1c2VyIjoiYW9ndW5sZwtlQHbhg9hbHRvbmv0d29ya3MuY29tIiwicm9sZSI6ImFkb
I3LDfxSwic2Vzc2lvblRpBwVvdXRTZWM0jQ5Nywic2Fhc1Rva2VuIjoiZX1KaGJHY21pAUpJVXpJMUSpSjkuZX1KemRXSWlPaUpoYjKmW
sdU1qcG1ZV3h6WlN3aWNISnBjMjFoU1dRaU9pSTRNRFkzTnpVME9UUTTRNvGd5TVRnME9UWW1lMQ0pwY0VGAlpISmxjM01pT2lJek5DNDNOQzQ
bTlzw1lSNWNHvkVaWFJ0YVd4eklqcDdJbWhoYzA5dWJ1bFnNaV0ZrUVd0alpYTnpJanBtWVd4elpYMHNjb1Z6WhlKU2IyeGxWSGx3WlU1aGJX
05UQTFNak1zSw1GMVpDSTZjBwgwZEhCek9pOHZZWEjwTWk1d2NtbHpiV0ZgYkc5MvpDNXBieUlzSw5We1pYS1NiMhsVkhds1pVbGtJam94T
Z6WhlKU2IyeGxTV1FpT2lJMV1XRTR2bUpqWLMweE9HUTFMVFjtWlRrdFlUZG10aTB5TW1VMV16UXdZv05oTm1NaUxDsM9ZWE5FWldabGJtUm
XVWlPaUpoYjKmWJteGxhM1ZBY0dGc2IyRnNkRz1lWhSM2IzSnjeTVqYjIwaUxDsFjM1Z5VW05c1pVNWHiV1VpT21KUWNtbHpiV0VnUTJ
aXNzIjoidHdpC3Rsb2NrIn0.MLAjBPYUZcZ_7xxZpcYp-f28-nw4Hmt-XG-M442izx4 --address https://us-east1.cloud.twistlock
defender daemonset written successfully to /home/akanfedoyinsola/defender.yaml
Defender daemonset installation completed
akanfedoyinsola@cloudshell:~ (valued-base-377112)$
```

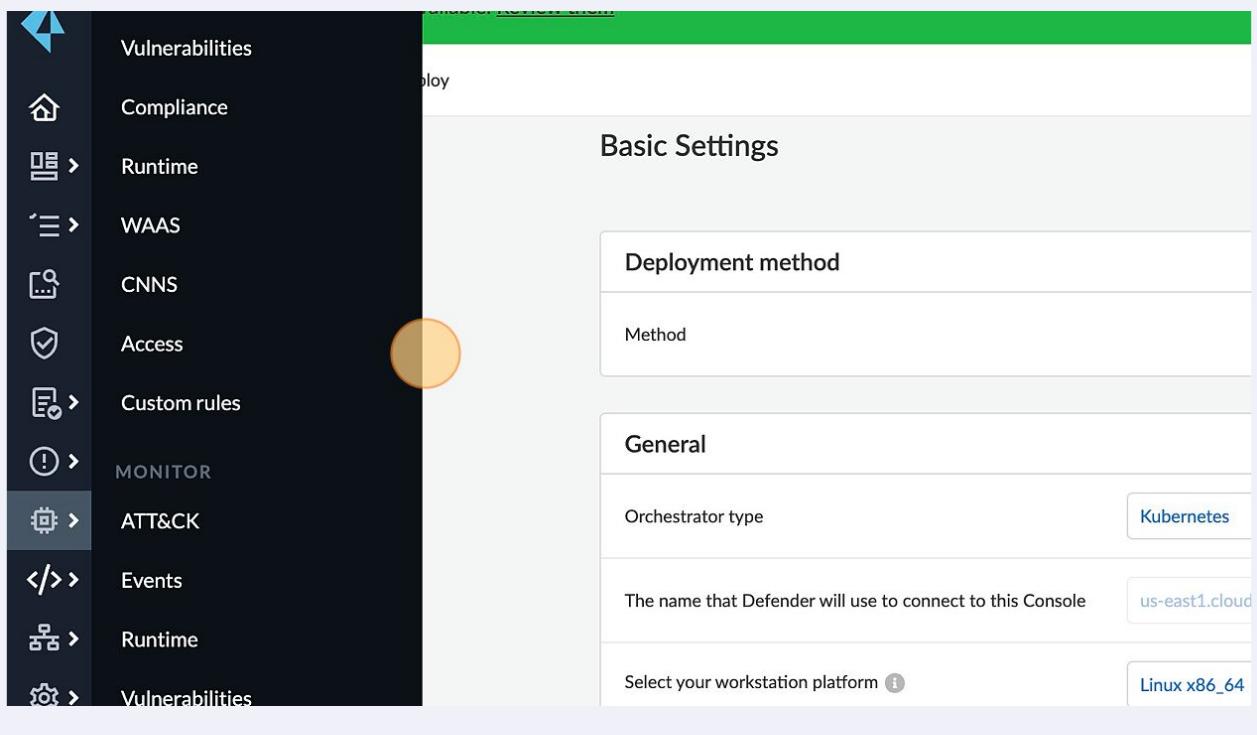
19

Click this link.



20

Click here.



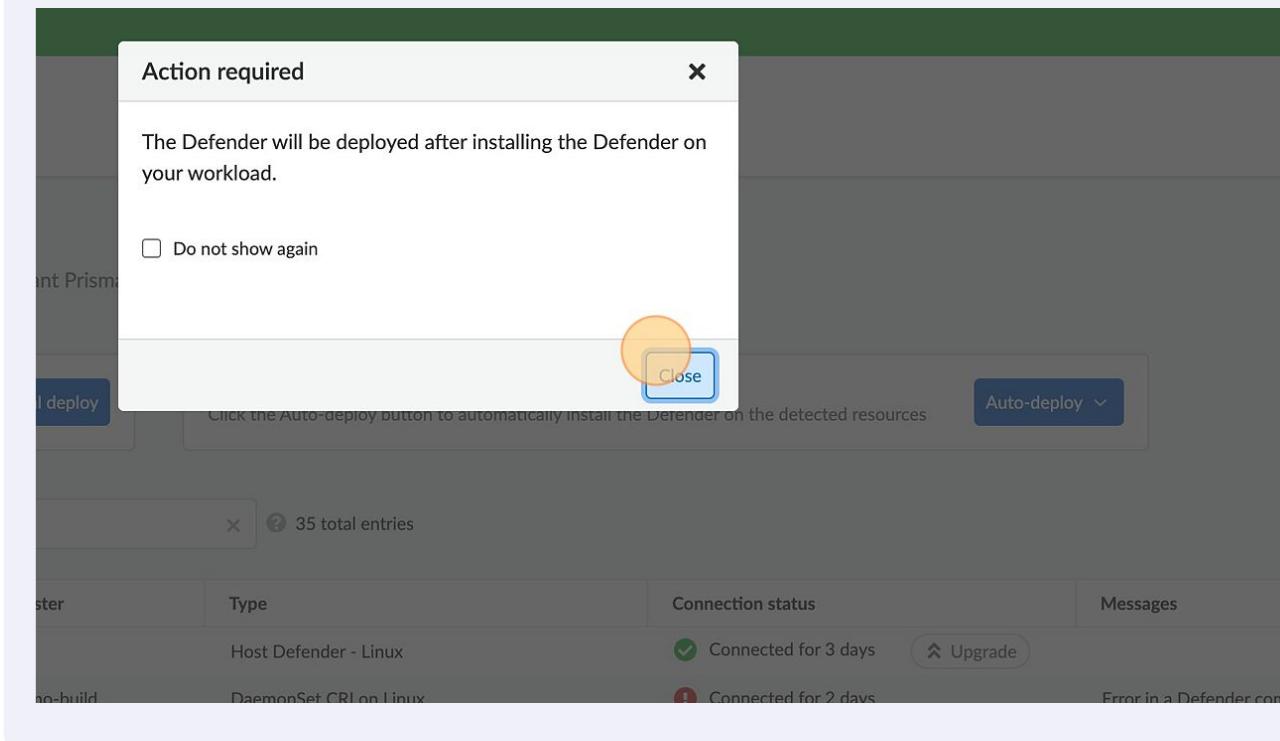
21 Click "Defenders"

The screenshot shows the Cloud Defender navigation bar on the left with various options like Runtime, Vulnerabilities, Compliance, WAAS, etc. The 'Defenders' option is highlighted with a blue selection bar and has a yellow circle around it. The main panel on the right shows configuration sections for 'Orchestrator environment' and 'Defender and Console communication', with platform selection (Linux x86_64) and deployment-related settings.

22 Click "Deployed Defenders"

The screenshot shows the 'Deployed Defenders' settings page. A yellow circle highlights the 'Basic Settings' tab. The 'Basic Settings' section includes fields for 'Deployment method' (Method), 'General' (Orchestrator type set to Kubernetes), and 'Console connection' (Name set to us-east1.cloud). A green banner at the top indicates new WAAS virtual patches available.

23 Click "Close"



24 Click "20"

Linux	Disconnected for 28 days	
	Disconnected for 3 days	
Linux	Disconnected for 28 days	
Linux	Disconnected for 14 days	
Linux	Disconnected for 15 days	
Linux	Disconnected for 13 days	
Linux	Disconnected for 13 days	
Linux	Disconnected for 13 days	
Linux	Disconnected for 10 days	
Linux	Disconnected for 9 days	
Linux	Disconnected for 8 days	
Linux	Disconnected for 7 days	

Rows **20** Page **1** of 2 < >

25 Click "50"

Linux	✖ Disconnected for 28 days	
	✖ Disconnected for 3 days	
Linux	✖ Disconnected for 28 days	
Linux	✖ Disconnected for 14 days	
Linux	✖ Disconnected for 15 days	
Linux	✖ Disconnected for 13 days	
Linux	✖ Disconnected for 13 days	
Linux	✖ Disconnected for 10 days	
Linux	✖ Disconnected for 10 days	
Linux	✖ Disconnected for 9 days	
Linux	✖ Disconnected for 8 days	
Linux	✖ Disconnected for 7 days	

Rows **50 ↴** Page **1 ▾** of 1 < >

26 Click this icon.

	ip-10-11-0-20/	22.06.229	Container Defen
	ip-10-11-0-254	22.06.229	Container Defen
	ip-10-11-0-35	22.06.229	Container Defen
	ip-10-11-0-14	22.06.229	Container Defen
	ip-10-11-0-232	22.06.229	Container Defen
	ip-10-11-0-179	22.06.229	Container Defen
	ip-10-11-0-230	22.06.229	Container Defen
	ip-10-11-0-80	22.06.229	Container Defen
	gk3-autopilot-cluster-1-default-pool-7e84588d-68c5	22.06.229	autopilot-cluster-1 DaemonSet on L
	gk3-autopilot-cluster-1-default-pool-78cd0d80-jlcw	22.06.229	autopilot-cluster-1 DaemonSet on L
	ip-10-11-0-137	22.06.229	Container Defen
	ip-10-11-0-115	22.06.229	Container Defen
	ip-10-11-0-198	22.06.229	Container Defen
	ip-10-11-0-36	22.06.229	Container Defen
	ip-10-11-0-199	22.12.427	Container Defen

27

Click "Vulnerabilities"

The screenshot shows the Prisma Cloud interface. On the left is a dark sidebar with various icons and sections: DEFEND, Compliance, Runtime, WAAS, CNNS, Access, Custom rules, MONITOR, ATT&CK, and Events. The 'Vulnerabilities' section under DEFEND is highlighted with a yellow circle. The main area has a green header bar with the text 'New vulnerabilities available. Review them'. Below the header is a table titled 'Vulnerabilities to defend' with the following data:

Vulnerability	Last updated	Scope	Type
pool-7e84588d-68c5	22.06.229	autopilot-cluster-1	DaemonSet on Local
pool-78cd0d80-jlcw	22.06.229	autopilot-cluster-1	DaemonSet on Local
	22.06.229		Container Defense

28

Click "Registry settings"

The screenshot shows the Prisma Cloud interface. The sidebar includes icons for Home, Defend, Compliance, Runtime, WAAS, CNNS, Access, Custom rules, MONITOR, ATT&CK, and Events. The 'Defend / Vulnerabilities' section is active. Below it, tabs for 'Code repositories', 'Images' (which is selected and highlighted with a yellow circle), 'Hosts', 'Functions', and 'VMware Tanzu blobstore' are visible. Under the 'Images' tab, there are tabs for 'Deployed', 'Registry settings' (which is highlighted with a yellow circle), 'CI', and 'Base images'. The main content area is titled 'Registry settings' and contains the following text:

Prisma Cloud lets you scan your registries for vulnerabilities.
Rules are evaluated at scan-time against all registries in scope, where scope is specified by the table under registry scan scop

Webhooks

29 Click "Add registry"

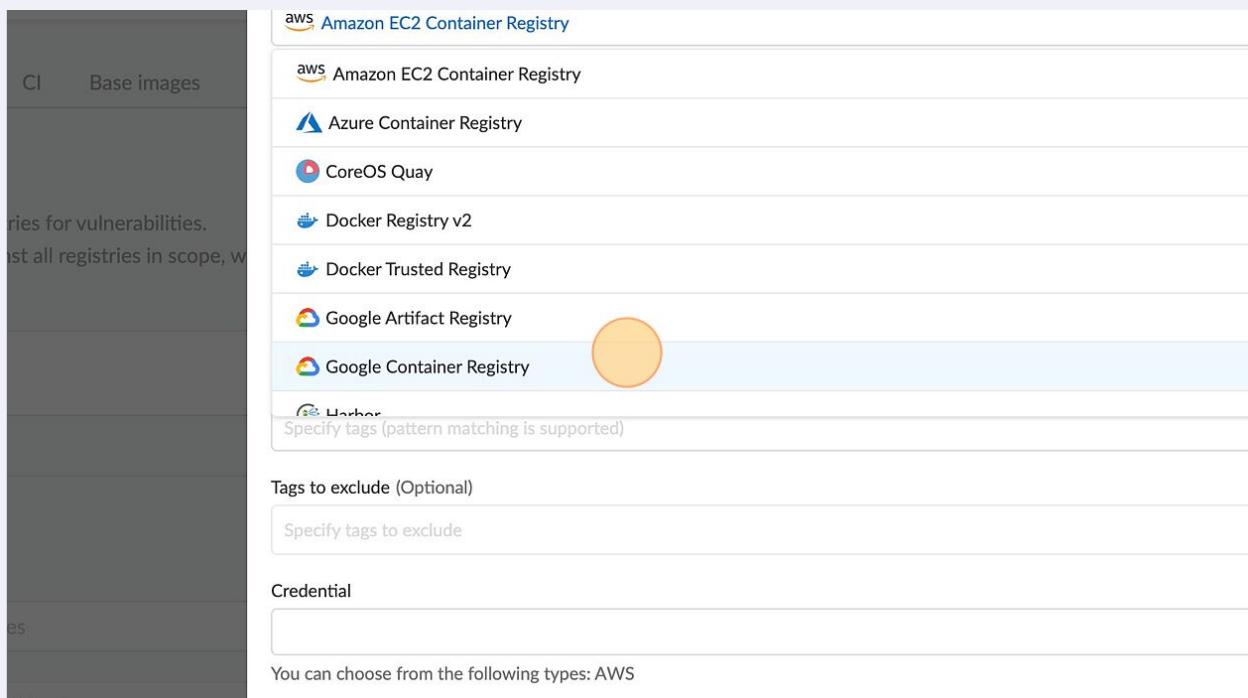
A screenshot of a web-based interface for managing registries. At the top right, there is a blue button with a white plus sign and the text 'Add registry'. This button is highlighted with a yellow circle. Below the button is a table with the following columns: Credential, OS type, Scanner scope, Scanners, Cap, Details, and Actions. The table contains five rows, each representing a different registry entry. The entries are: Prisma (Linux x86_64), Prisma (Linux x86_64), GCP Service Acco... (Linux x86_64), mbarker-se-custo... (Linux x86_64), and another entry for Linux x86_64. Each row includes a 'View details' link and edit/delete icons.

Credential	OS type	Scanner scope	Scanners	Cap	Details	Actions
Prisma	Linux x86_64	■	2	5	View details	
Prisma	Linux x86_64	■	2	5	View details	
GCP Service Acco...	Linux x86_64	■	2	5	View details	
mbarker-se-custo...	Linux x86_64	■	2	5	View details	
	Linux x86_64	■	2	5	View details	

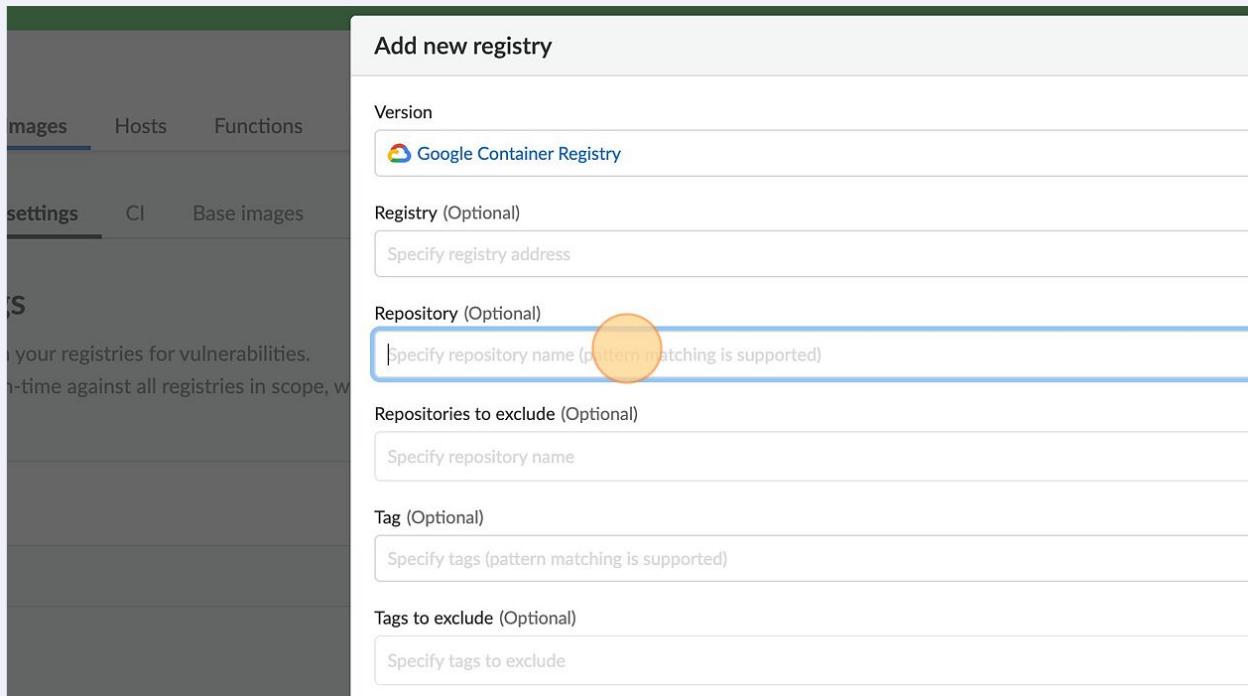
30 Click "Amazon EC2 Container Registry"

A screenshot of a 'Add new registry' dialog box. On the left, there is a sidebar with options: Functions, Base images, and Harbor. The 'Functions' option is currently selected. The main area is titled 'Add new registry' and has a section for 'Version'. A dropdown menu shows several options: aws Amazon EC2 Container Registry (which is highlighted with a yellow circle), aws Amazon EC2 Container Registry, Azure Container Registry, CoreOS Quay, Docker Registry v2, Docker Trusted Registry, Google Artifact Registry, Google Container Registry, and Harbor. Below the dropdown is a placeholder text 'Specify tags (pattern matching is supported)'. At the bottom, there is a field for 'Tags to exclude (Optional)'.

31 Click "Google Container Registry"



32 Click the "Repository(Optional)" field.



33 Click this button.

The screenshot shows a configuration page with the following sections:

- Repositories to exclude (Optional)**: A text input field labeled "Specify repository name".
- Tag (Optional)**: A text input field labeled "Specify tags (pattern matching is supported)".
- Tags to exclude (Optional)**: A text input field labeled "Specify tags to exclude".
- Credential**: A section with a blue background and a yellow circle highlighting the "Credential" tab. Below it, a message says "You can choose from the following types: GCP".
- OS type**: A dropdown menu set to "Linux x86_64".
- Scanners scope**: A section with a "All" button and a link "Click to select collection".
- Number of scanners**: A text input field with a help icon.

On the left, there is a sidebar with the heading "Keywords and attributes" and a table titled "Registry" showing the following data:

	Registry
Registry	us-central1-docker.pkg.dev
Registry	us-central1-docker.pkg.dev
er Registry	gcr.io
er Registry	gcr.io

34 Click "abej GCP cred01"

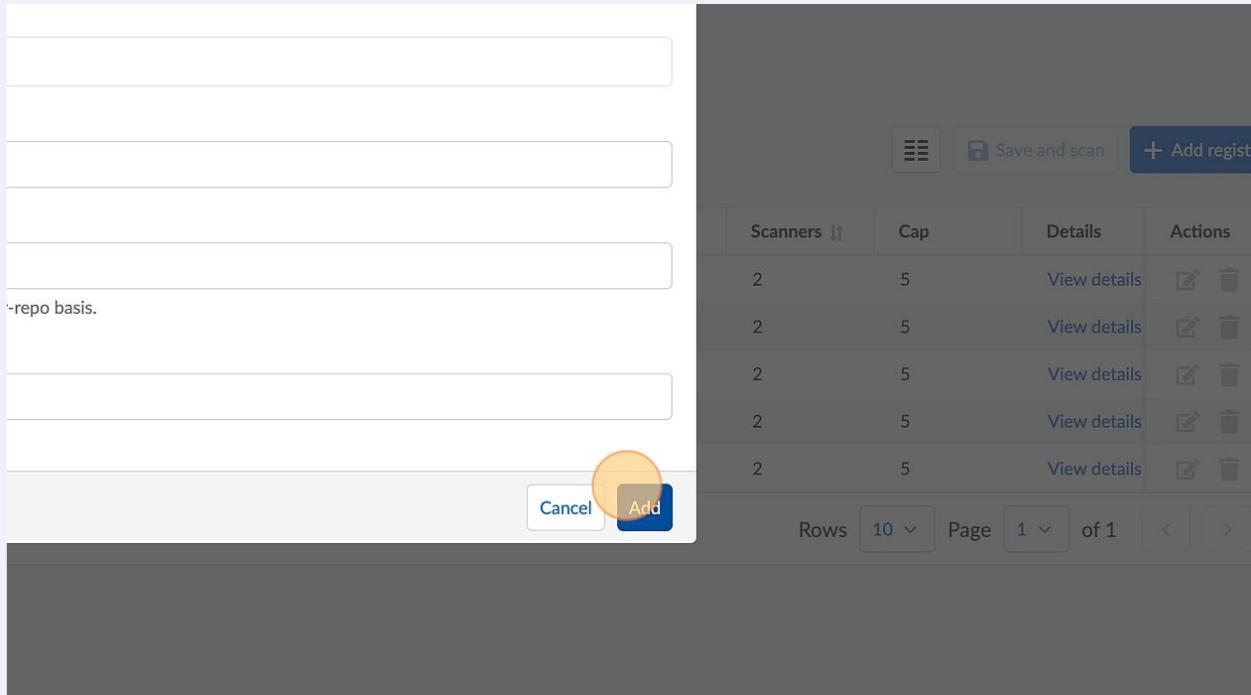
The screenshot shows a search interface for credentials:

- Specify tags (pattern matching is supported)**: A text input field.
- Tags to exclude (Optional)**: A text input field labeled "Specify tags to exclude".
- Credential**: A section with a blue background and a yellow circle highlighting the "Credential" tab. Below it, a search bar labeled "Search".
- Search results**: A list of credentials:
 - abej GCP cred01 (highlighted with a yellow circle)
 - cto-demos
 - GCP Org1
 - GCP Service Account
 - GCP: RedLock Demo Account
 - Host Project - 884318314730
 - Host Project - 91283809440
 - mbarker.co.customer-facing

On the left, there is a sidebar with the heading "Keywords and attributes" and a table titled "Registry" showing the following data:

	Registry
stry	us-central1-docker.pkg.dev
stry	us-central1-docker.pkg.dev
gistry	gcr.io
gistry	gcr.io

35 Click "Add"



36 Click "Google Container Registry"

A screenshot of a software interface titled 'Registries'. On the left, there is a vertical sidebar with several icons: a gear, a bell, a circular progress bar (67%), a document, and a user profile. The main area shows a table of registries. The first row, 'Google Container Registry', is highlighted with a yellow circle. The table has four columns: 'Version', 'Registry', 'Repository', and 'Tag'. The data for the highlighted row is: Version: Google Container Registry, Registry: gcr.io, Repository: aaaaaaaaaa, Tag: . The table also lists other registries like Google Artifact Registry and Docker Registry v2. A yellow banner at the top of the main area says: '⚠ You have unsaved changes. Click the Save and scan button to keep the changes.' Below the table, it says 'Displaying 1 - 6 of 6'.

37

Click here.

You have unsaved changes. Click the **Save and scan** button to keep the changes.

Filter by keywords and attributes

x ⓘ 6 total entries

	Registry ↓↑	Repository ↓↑	Tag ↓↑	Credential ↓↑
Registry		aaaaaaaaaa		abej GCP cred01
Registry	us-central1-docker.pkg.dev			Prisma
Registry	us-central1-docker.pkg.dev			Prisma
Registry	gcr.io		cto-sandbox/...	GCP Service Acco...
Registry	gcr.io			mbarker-se-custo...

2

notemaker*

:6

38

Click this link.



Deployed

Registry settings

CI

Base images

Registry settings

Prisma Cloud lets you scan your registries for vulnerabilities.

Rules are evaluated at scan-time against all registries in scope, where scope is specified by the table under registry scan scope.

Compute books

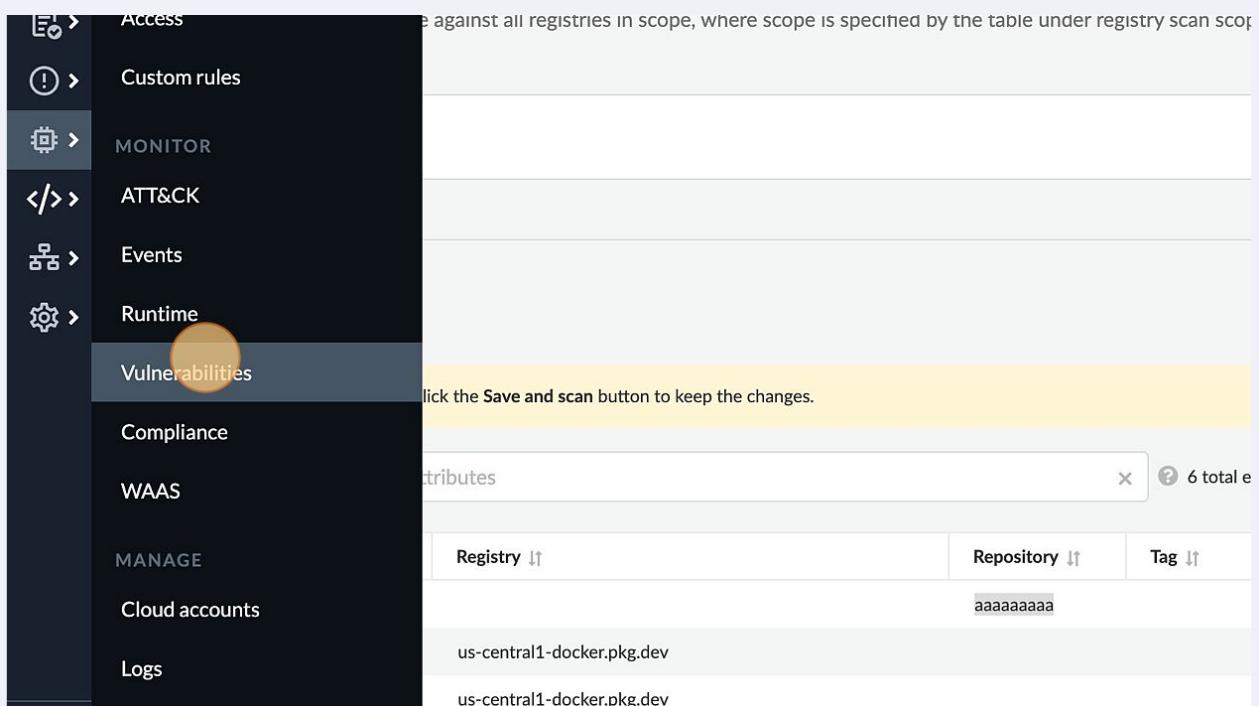
Registries ⓘ

⚠ You have unsaved changes. Click the **Save and scan button to keep the changes.**

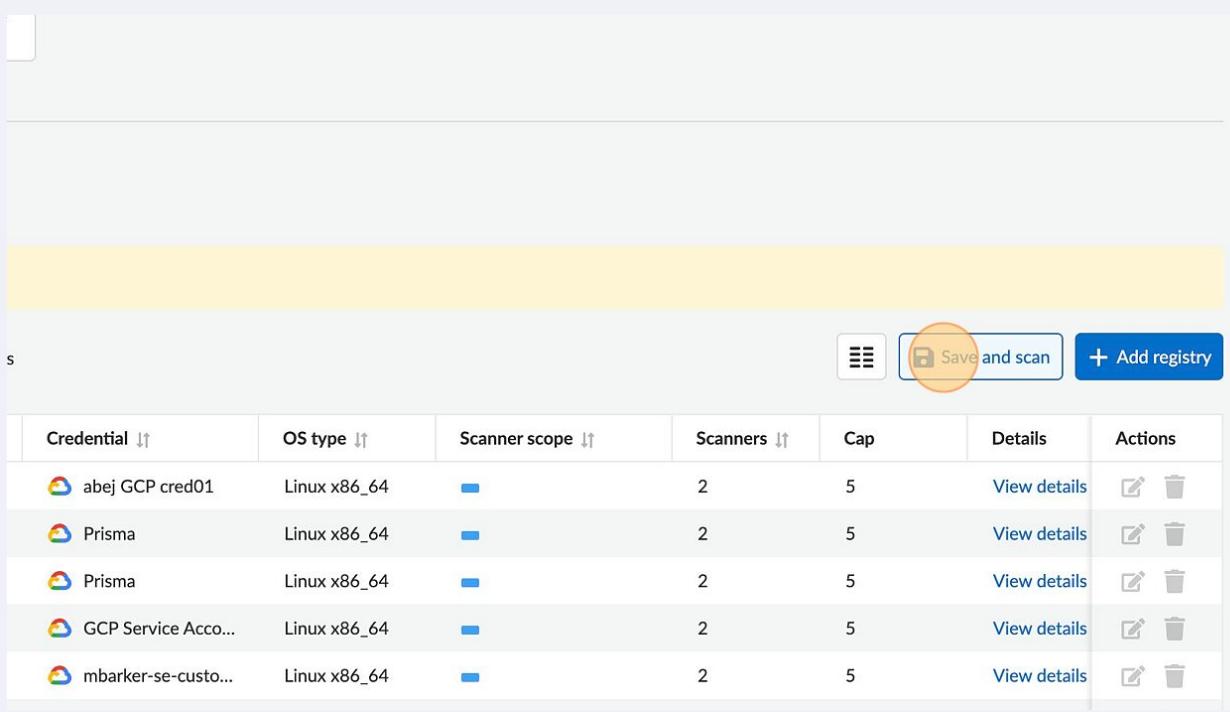
Filter by keywords and attributes

x ⓘ 6 total e

39 Click "Vulnerabilities"



40 Click "Save and scan"



41

Click "Failed to retrieve repository aaaaaaaaa tags, error Get "https://registry-1.docker.io/v2/aaaaaaaa/tags/list": proxyconnect tcp: dial tcp: lookup..."

The screenshot shows the Prisma Cloud interface with a sidebar containing icons for monitoring, logs, metrics, and configuration. The main area displays a 'Webhooks' section and a 'Registries' section. In the 'Registries' section, there is a prominent red error message: 'Failed to retrieve repository aaaaaaaaa tags, error Get "https://registry-1.docker.io/v2/aaaaaaaa/tags/list": proxyconnect tcp: dial tcp: lookup..."' followed by a yellow circular highlight. Below this, a search bar says 'Filter by keywords and attributes' and shows '6 total e'. A table lists registry entries:

Version	Registry	Repository	Tag
Google Container Registry		aaaaaaaaaa	
Google Artifact Registry	us-central1-docker.pkg.dev		
Google Artifact Registry	us-central1-docker.pkg.dev		
Google Container Registry	eu-west1-docker.pkg.dev	sts-sandbox	/

42

Click here.

The screenshot shows the 'Registry settings' tab of the Prisma Cloud interface. The sidebar includes icons for monitoring, logs, metrics, and configuration. The main content area features a 'Registries' section with a red error message: 'Failed to retrieve repository aaaaaaaaa tags, error Get "https://registry-1.docker.io/v2/aaaaaaaa/tags/list": proxyconnect tcp: dial tcp: lookup...' followed by a yellow circular highlight. Below this is a search bar with 'Filter by keywords and attributes' and '6 total e' results. The 'Deployed' tab is also visible at the top.

43 Click "Vulnerabilities"

The screenshot shows a software interface with a dark sidebar menu on the left. The menu items are: Custom rules, MONITOR, ATT&CK, Events, Runtime, Vulnerabilities, Compliance, WAAS, MANAGE, Cloud accounts, and Logs. The 'Vulnerabilities' item is highlighted with a blue selection bar and has a yellow circle around it. To the right of the sidebar is a table with the following data:

Registry	Repository	Tag
aaaaaaa tags, error Get "https://registry-1.docker.io/v2/aaaaaaaaa/tags/list": proxyconnect tcp: dial tcp: lo	aaaaaaaaa	aaaaaaaaa
us-central1-docker.pkg.dev	aaaaaaaaa	aaaaaaaaa

44 Click this link.

The screenshot shows a software interface with a dark sidebar menu on the left. The menu items are: Deployed, Registries, CI, and Compute. The 'Compute' item is highlighted with a blue selection bar and has a yellow circle around it. To the right of the sidebar is a table with the following data:

Compute	Repository	Tag	Hosts	Cluster
	weaveworksdemos/qu...	0.3.1	master-demo2-tlbuild-...	demo-
	tl_demo/struts2_demo	2.3.12_build	master-demo2-tlbuild-...	demo-
	weaveworksdemos/shi...	0.4.8	master-demo2-tlbuild-...	demo-
	weaveworksdemos/or...	0.4.7	master-demo2-tlbuild-...	demo-
	weaveworksdemos/car...	0.4.8	node-demo2-tlbuild-d...	demo-

45 Click "Vulnerability scan reports for deployed images"

The screenshot shows a user interface for a security platform. On the left is a dark sidebar with various icons and labels: 'DEFEND' (Vulnerabilities, Compliance, Runtime, WAAS, CNNS, Access, Custom rules), 'MONITOR' (ATT&CK, Events, Runtime), and other sections like Compute, Vulnerabilities, Compliance, and NAAS. The 'Images' tab is highlighted in blue at the top of the main content area. Below it, there's a table with columns for Repository, Tag, Hosts, and Cluster. One row is selected, showing 'javeworksdemos/qu...' with tag '0.3.1'. A yellow circle is drawn around the 'Deployed images' link under the Runtime section in the sidebar.

Repository	Tag	Hosts	Cluster
javeworksdemos/qu...	0.3.1	master-demo2-tlbuild...	demo-
javeworksdemos/struts2_demo	2.3.12_build	master-demo2-tlbuild...	demo-
javeworksdemos/shi...	0.4.8	master-demo2-tlbuild...	demo-

46 Click this image.

This screenshot shows the same interface as the previous one, but with a different focus. The 'Compute' icon in the sidebar is highlighted with a yellow circle. The 'Vulnerabilities' link in the sidebar is also highlighted with a blue bar. The main content area remains the same, showing the 'Images' tab selected and the table of deployed images.

47

Click "Registries"

New WAAS virtual patches available. [Review them](#)

Monitor / Vulnerabilities

Vulnerability Explorer Code repositories **Images** Hosts Functions CVE viewer VMware Tanzu

Deployed **Registries** CI

Deployed images

Vulnerability scan reports for deployed images

Filter images by keywords and attributes

Registry	Repository	Tag	Hosts	Cluster
	weaveworksdemos/qu...	0.3.1	master-demo2-tlbuild-...	demo-
	tl_demo/struts2_demo	2.3.12_build	master-demo2-tlbuild-...	demo-

48

Click "Deployed"

New WAAS virtual patches available. [Review them](#)

Monitor / Vulnerabilities

Vulnerability Explorer Code repositories **Images** Hosts Functions CVE viewer VMware Tanzu

Deployed Registries CI

Registry images

Vulnerability scan reports for registry images

Filter registries by keywords and attributes

Registry	Repository	Tag

49

Click "Registries"

New WAAS virtual patches available. [Review them](#)

Monitor / Vulnerabilities

Vulnerability Explorer Code repositories **Images** Hosts Functions CVE viewer VMware Tanzu

Deployed **Registries** CI

Deployed images

Vulnerability scan reports for deployed images

Filter images by keywords and attributes

Registry	Repository	Tag	Hosts	Cluster
	weaveworksdemos/qu...	0.3.1	master-demo2-tlbuild-...	demo-
	tl_demo/struts2_demo	2.3.12_build	master-demo2-tlbuild-...	demo-

50

Click here.

Deployed **Registries** CI

Registry images

Vulnerability scan reports for registry images

Filter registries by keywords and attributes

Compute	Repository	Tag

51 Click "Vulnerabilities"

The screenshot shows the VMware Tanzu interface. On the left is a sidebar with various icons and sections: Settings, DEFEND (with Vulnerabilities highlighted and circled in orange), Compliance, Runtime, WAAS, CNNS, Access, Custom rules, MONITOR, ATT&CK, and Events. The main content area has a green header bar with the text 'available. Review them'. Below the header, there are tabs for Code repositories, Images (which is selected and highlighted in blue), Hosts, Functions, CVE viewer, and VMware Tanzu. The 'Images' tab displays a table with columns for Repository, Tag, and a search bar. The table contains several rows of registry images.

52 Click this button.

The screenshot shows the VMware Tanzu interface with a table titled 'Credentials'. The table has columns: Credential, OS type, Scanner scope, Scanners, Cap, Details, and Actions. The 'Actions' column contains icons for View details, Edit, and Delete. The 'Delete' icon in the last row is circled in orange. At the top right of the table are buttons for Save and scan and Add registry. Below the table are buttons for Rows (10), Page (1 of 1), and navigation arrows.

Credential	OS type	Scanner scope	Scanners	Cap	Details	Actions
abej GCP cred01	Linux x86_64	■	2	5	View details	
Prisma	Linux x86_64	■	2	5	View details	
Prisma	Linux x86_64	■	2	5	View details	
GCP Service Acco...	Linux x86_64	■	2	5	View details	
mbarker-se-custo...	Linux x86_64	■	2	5	View details	
	Linux x86_64	■	2	5	View details	

53 Click "Save and scan"

The screenshot shows a list of credentials in a table. The columns are: Credential, OS type, Scanner scope, Scanners, Cap, Details, and Actions. There are six rows of data. A yellow circle highlights the 'Save and scan' button in the top right corner of the table header.

Credential	OS type	Scanner scope	Scanners	Cap	Details	Actions
Prisma	Linux x86_64	■	2	5	View details	
Prisma	Linux x86_64	■	2	5	View details	
GCP Service Acco...	Linux x86_64	■	2	5	View details	
mbarker-se-custo...	Linux x86_64	■	2	5	View details	
	Linux x86_64	■	2	5	View details	

54 Click this icon.

The screenshot shows a dark-themed dashboard. On the left is a sidebar with several icons: a shield, a checkmark, a document, an exclamation mark, a gear, and a server icon (which is highlighted with a yellow circle). The main panel has a heading 'Review the urgent risks and incidents detected in the last 24 hours.' Below it is a section titled 'Compute' with a sub-section 'Recommended Workflows'. It lists two items: 'ASSET INVENTORY' and 'COMPLIANCE OVERVIEW'.

Review the urgent risks and incidents detected in the last 24 hours.

Compute

Recommended Workflows

ASSET INVENTORY

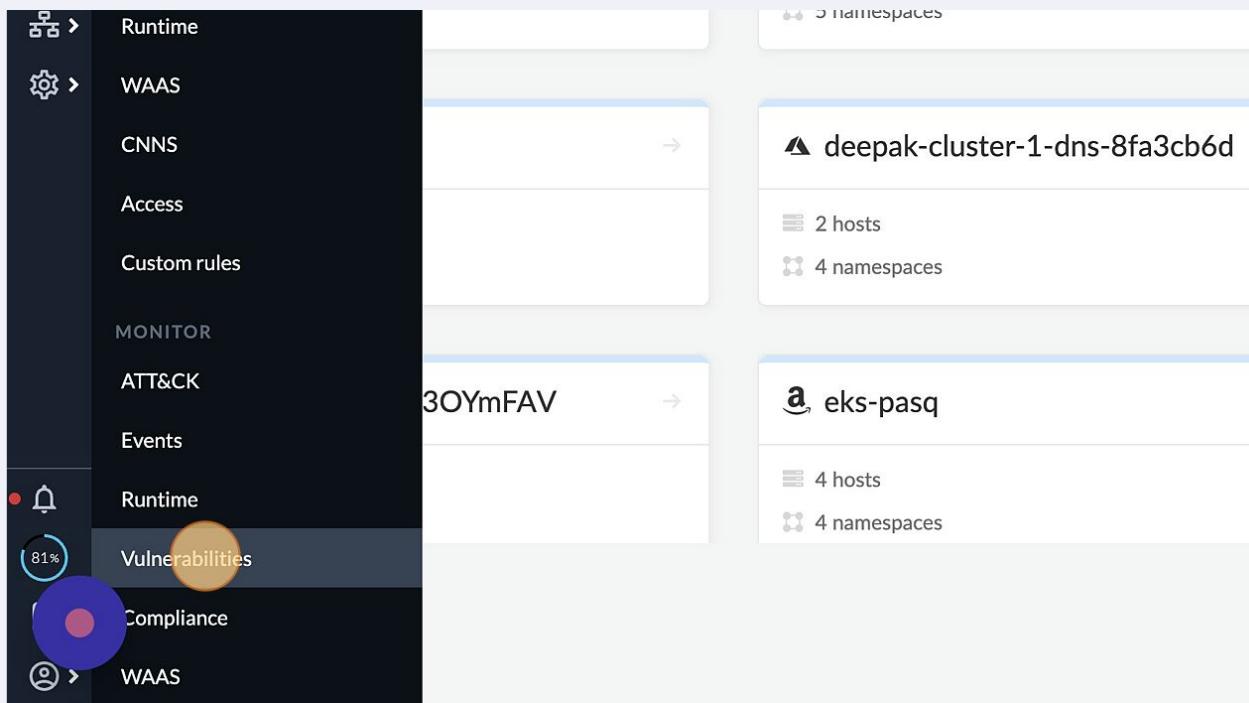
Get visibility into your cloud assets from a unified inventory.

COMPLIANCE OVERVIEW

Monitor your cloud infrastructure health and compliance posture.

55

Click "Vulnerabilities"



56

Click "zwaqaracr.azurecr.io"

The screenshot shows the 'Registry images' page. On the left is a sidebar with various icons. The main area displays a table of registry images. A yellow circle highlights the 'zwaqaracr.azurecr.io' entry in the 'Registry' column. The table has columns for Registry, Repository, Tag, and a small icon. The data is as follows:

Registry	Repository	Tag
zwaqaracr.azurecr.io	voting/azure-vote-front	v1
	cgray413/colexcuse	23
	cgray413/colexcuse	21
	cgray413/colexcuse	24
anrchcontainerregistry.azurecr.io	anrchclusterprisma	dfe126acd2
499040555397.dkr.ecr.eu-west-2.amazonaws.com	medium	latest

57 Click "Compliance"

The screenshot shows the 'Registry images' page with the 'Compliance' tab highlighted. The page displays details about a registry entry, including its ID, OS distribution, OS release, Digest, Scanner, and Scanned by information. Below this, there is a table of vulnerabilities categorized by type (python, OS) and severity (medium). A yellow circle highlights the 'Compliance' tab.

Type	Highest severity	Description
python	medium	click version 7.1.2 has 1 vulnerability
OS	medium	unzip version 6.0-23+deb10u1 has 1 vulnerability
OS	medium	libcurl version 7.61.1 has 1 vulnerability

58 Click "Layers"

The screenshot shows the 'try images' page with the 'Layers' tab highlighted. The page displays details about a registry entry, including its ID, OS distribution, OS release, Digest, Scanner, and Scanned by information. Below this, there is a table of compliance results categorized by ID, category, severity, and result. A yellow circle highlights the 'Layers' tab.

ID	Category	Severity	Result	Description
9010	Custom	high	Pass	check for open ports with
9009	Custom	high	Pass	check for endpoints

59 Click "Process info"

The screenshot shows a Docker image details page. At the top, there is a table with various metadata fields:

registry	zwaqaracr.azurecr.io/voting/azure-vote-front:v1
ID	sha256:9d26e987625b7925d03c0fbcc151c9a2d15648dad267a2d11c887130288b9169b
OS distribution	Debian GNU/Linux 10 (buster)
OS release	buster
Digest	sha256:98638c0da34e9a75710d0f76a4e3a0a63e565fb75b77482095e42def685a5328
Scanner	⚠️ aks-agentpool-29918397-vmss00000-MC_anrch-prisma-rg_anrch_cluster_prisma_eastus-16dfdbcc-e407-4fbe-9
Scanned by	Defender

Below the table, there is a navigation bar with tabs: Vulnerabilities, Compliance, Layers, Process info (which is highlighted with a yellow circle), General info, Package info, and Labels.

A message below the tabs indicates: "57 Layers, Image Size: 968.4 MB".

There is also a search bar labeled "Filter layers by keywords and attributes".

On the right side, there is a detailed view of one layer, showing its "Details", "Size" (119.2 MB), and "Vulnerabilities" count (42, 14, 20, 10). The layer's content is partially visible as a command script.

60 Click "General info"

The screenshot shows a Docker image details page. At the top, there is a table with various metadata fields, identical to the one in step 59.

Below the table, there is a navigation bar with tabs: Vulnerabilities, Compliance, Layers, Process info (which is highlighted with a yellow circle), General info (which is highlighted with a blue circle), Package info, and Labels.

A message below the tabs indicates: "Filter processes by keywords".

On the right side, there is a table showing a list of processes with columns: Name, Path, and Md5. The data is as follows:

Name	Path	Md5
rm	/bin/rm	e596d7fc985d161f68b2:
gpg	/usr/bin/gpg	cba5c0286db0098322af
grep	/bin/grep	c70403dc8cea610520c8

61 Click "Package info"

```
zwaqaracr.azurecr.io/voting/azure-vote-front:v1  
sha256:9d26e987625b7925d03c0fbcc151c9a2d15648dad267a2d11c887130288b9169b  
Debian GNU/Linux 10 (buster)  
buster  
sha256:98638c0da34e9a75710d0f76a4e3a0a63e565fb75b77482095e42def685a5328  
⚠️ aks-agentpool-29918397-vmss00000-MC_anrch-prisma-rg_anrch_cluster_prisma_eastus-16dfdbcc-e407-4fbe-9096-e7a97ee  
Defender
```

The screenshot shows a container details interface. At the top, there are tabs for 'Compliance', 'Layers', 'Process info', 'General info' (which is highlighted with a yellow circle), and 'Labels'. Below the tabs, there is a timestamp section with two entries: 'Jan 13, 2023 9:40:10 PM' and 'Jun 30, 2021 3:06:07 PM'. A large black redaction bar covers the majority of the content below this section.

62 Click "Package info"

```
acr.azurecr.io/voting/azure-vote-front:v1  
sha256:9d26e987625b7925d03c0fbcc151c9a2d15648dad267a2d11c887130288b9169b  
Debian GNU/Linux 10 (buster)  
sha256:98638c0da34e9a75710d0f76a4e3a0a63e565fb75b77482095e42def685a5328  
aks-agentpool-29918397-vmss00000-MC_anrch-prisma-rg_anrch_cluster_prisma_eastus-16dfdbcc-e407-4fbe-9096-e7a97ee  
Defender
```

The screenshot shows a container details interface. At the top, there are tabs for 'Compliance', 'Layers', 'Process info', 'General info' (which is highlighted with a yellow circle), and 'Labels'. Below the tabs, there is a search bar containing 'ds and attributes' and a note '228 total entries'. A table is displayed with columns: 'Source package' (with an upward arrow icon), 'Path', 'Version' (with a downward/upward arrow icon), 'All known CVEs' (with a downward/upward arrow icon), and 'Binaries'. The table has two rows. The first row shows '3.118' in the Version column and '0' in the All known CVEs column. The second row shows '1.2.1' in the Version column and '0' in the All known CVEs column.

Source package	Path	Version	All known CVEs	Binaries
		3.118	0	
		1.2.1	0	

63 Click "Defender"

The screenshot shows the Azure Container Registry interface. On the left, there's a sidebar with tabs for 'Deployed' and 'Registries'. The 'Registries' tab is selected, showing a list of registries. The first registry listed is 'zwaqaracr.azurecr.io'. On the right, the main panel displays details for an image in this registry. At the top, a yellow warning icon with the text 'Please note' and 'Report data might not be fully up-to-date while registry scans are in progress' is visible. Below this, the image details are shown:

registry	zwaqaracr.azurecr.io/voting/azure-vote-front:v1
ID	sha256:9d26e987625b7925d03c0fbcc151c9a2d15648dad267a2d11c8871302
OS distribution	Debian GNU/Linux 10 (buster)
OS release	buster
Digest	sha256:98638c0da34e9a75710d0f76a4e3a0a63e565fb75b77482095e42def
Scanner	⚠️ aks-agentpool-29918397-vmss00000-MC_anrch-prisma-rg_anrch_cluster
Scanned by	Defender

Below the image details, there are tabs for 'Vulnerabilities', 'Compliance', 'Layers', 'Process info', 'General info', and 'Package info'. The 'Package info' tab is selected. A table below shows the package details:

Type	Names	Source package	Path
package	adduser		

At the bottom of the main panel, there's a search bar labeled 'Filter packages by keywords and attributes'.