

AtomicWP Workload Security for Docker Getting Started Pre-

launch:

1. Ensure that traffic is allowed on ports 22 and 30001 for either this instance or all instances. Go to the GCP VPC network section and then to firewall rules. Select create a firewall rule and create an ingress/allow rule for tcp ports 22 and 30001.

Example:

VPC network

VPC networks

External IP addresses

Firewall

Routes

VPC network peering

Shared VPC

Serverless VPC access

Packet mirroring

CREATE FIREWALL RULE

REFRESH

CONFIGURE LOGS

DELETE

Filter table

<input type="checkbox"/>	Name	Type	Targets	Filters	Protocols / ports	Action	Priority	Network	↑	Logs	Hit count
<input type="checkbox"/>	aeo-outbound-rule	Egress	Apply to all	IP ranges: 0.0.0.0/0	all	Allow	1	default		Off	
<input type="checkbox"/>	aeo-v6-outbound	Egress	Apply to all	IP ranges: 0.0.0.0/0	tcp:22,30001	Allow	11	default		Off	
<input type="checkbox"/>	cluster-port-outbound	Egress	Apply to all	IP ranges: 0.0.0.0/0	tcp:8443	Allow	11	default		Off	
<input type="checkbox"/>	port-6443-outbound	Egress	Apply to all	IP ranges: 0.0.0.0/0	tcp:6443 udp:6443	Allow	12	default		Off	
<input type="checkbox"/>	aeo-inbound-rule	Ingress	Apply to all	IP ranges: 0.0.0.0/0	tcp:22,80,443,30000,1515 udp:1514,514	Allow	1	default		Off	
<input type="checkbox"/>	awp-firewall-rule2	Ingress	Apply to all	IP ranges: 0.0.0.0/0	tcp:22,30000	Allow	1	default		Off	
<input type="checkbox"/>	all-ports-inbound	Ingress	Apply to all	IP ranges: 0.0.0.0/0	all	Allow	4	default		Off	
<input type="checkbox"/>	aeo-v6-inbound	Ingress	Apply to all	IP ranges: 0.0.0.0/0	tcp:22,30001	Allow	10	default		Off	

Post-launch:

1. Upon starting the instance, wait approximately 30 minutes for background updates and scans to finish. If you have connected to the instance via ssh, you'll a line that says AtomicWP Workload Security: Scan complete when it is finished. You may not see this if you wait till the scan is finished before connecting. Once this is done, note the

onscreen instructions. Example:

```
ssh.cloud.google.com/projects/atomicorp-public/zones/us-east4-c/instances/awp-docker-v6-build-attempt2?us
agencies, both domestic and foreign.

By using this system, the user consents to such interception, monitoring,
recording, copying, auditing, inspection, and disclosure at the
discretion of such personnel or officials. Unauthorized or improper use
of this system may result in civil and criminal penalties and
administrative or disciplinary action, as appropriate. By continuing to
use this system you indicate your awareness of and consent to these terms
and conditions of use. LOG OFF IMMEDIATELY if you do not agree to the
conditions stated in this warning.
*****

Connected, host fingerprint: ssh-rsa 0 7D:03:B8:3A:02:61:A0:81:88:E5:2A:A3:2B:48
:1E:28:65:EB:18:4B:E9:90:C0:A2:89:E8:BB:53:8B:96:19:43
Last login: Thu Jul 23 13:37:48 2020 from 35.235.241.33
#####
# AtomicWP Workload Protection #
#####
To access the ui for this instance, go to https://<IP>:30001 and login with the
username and password in /var/awp/etc/config.

To use docker on this machine, please run gcloud auth login and then reboot this
instance.
[mdavis@awp-docker-v6-build-attempt2 ~]$
```

2. In order to enable docker on your instance, once the instance is finished with background tasks run `gcloud auth login` and follow the given prompts. Then reboot your instance. If you do not follow this step you will likely see an error concerning docker being unable to create an endpoint. Example:

```
[root@awp-docker-prep-check ~]# gcloud auth login

You are running on a Google Compute Engine virtual machine.
It is recommended that you use service accounts for authentication.

You can run:

    $ gcloud config set account 'ACCOUNT'

to switch accounts if necessary.

Your credentials may be visible to others with access to this
virtual machine. Are you sure you want to authenticate with
your personal account?

Do you want to continue (Y/n)? Y

Go to the following link in your browser:

    https://accounts.google.com/o/oauth2/auth?redirect_uri=urn%3Aietf%3Awg%3Aoauth%3A2.0%3Aacob&prompt=select_account&response_type=code&client_id=32555940559.apps.googleusercontent.com&scope=https%3A%2F%2Fwww.googleapis.com%2Fauth%2Fuserinfo.email+https%3A%2F%2Fwww.googleapis.com%2Fauth%2Fcloud-platform+https%3A%2F%2Fwww.googleapis.com%2Fauth%2Fappengine.admin+https%3A%2F%2Fwww.googleapis.com%2Fauth%2Fcompute+https%3A%2F%2Fwww.googleapis.com%2Fauth%2Faccounts.reauth&access_type=offline

Enter verification code: 4/sgE1JU6ofWuUnflxg-zcfYC_2ccfDUA0W_V1ClLmmSQttY8K0zEYNFA
WARNING: 'gcloud auth login' no longer writes application default credentials.
If you need to use ADC, see:
    gcloud auth application-default --help

You are now logged in as [mdavis@atomicorp.com].
Your current project is [atomicorp-public]. You can change this setting by running:
    $ gcloud config set project PROJECT_ID
[root@awp-docker-prep-check ~]#
```