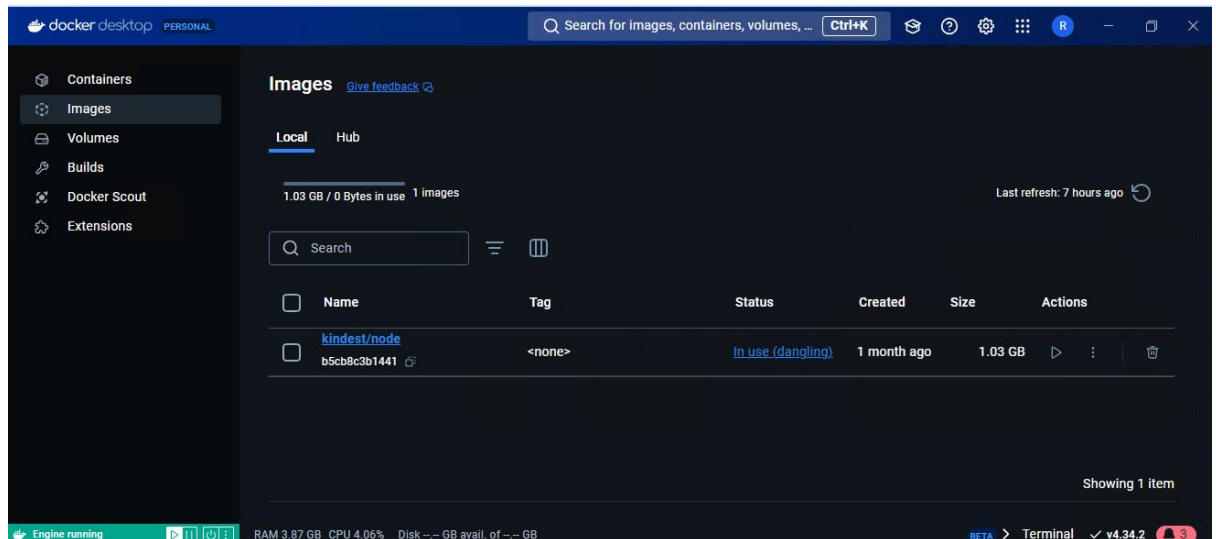


Kubernetes Security Scan

Process followed:

- ➔ The whole process is performed in a Windows environment
- ➔ Docker-Desktop is installed and set up.



- ➔ Now Kubernetes needs to be installed for which kubectl is installed from the official page.
- ➔ Once Kubernetes is running kind(Kubernetes in docker) is installed.

```
PS C:\Users\sRamu\Documents> .\kubectl.exe get nodes
NAME                                STATUS    ROLES    AGE    VERSION
ramu-cluster-control-plane         Ready    control-plane    30m    v1.31.0
PS C:\Users\sRamu\Documents> |
```

- ➔ Using kind a new cluster is created and nodes from Kubernetes are added to the cluster.

```
PS C:\Users\sRamu\Documents> .\kind-windows-amd64.exe get clusters
ramu-cluster
PS C:\Users\sRamu\Documents> |
```

➔ Now kubescape is installed and the new cluster created by using kind is scanned.

```
PS C:\Users\sRamu\Documents> kubescape scan --format json --output results.json
[✓] Initialized scanner
[✓] Loaded policies
[✓] Loaded exceptions
[✓] Loaded account configurations
[✓] Accessed Kubernetes objects
Control: C-0063 100% | ████████████████████████████████████████████████████████████████████████████████ (47/47, 48 it/s)
[✓] Done scanning. Cluster: kind-ramu-cluster
[✓] Done aggregating results

Security posture overview for cluster: 'kind-ramu-cluster'

In this overview, Kubescape shows you a summary of your cluster security posture, including the number of users who can perform administrative actions. For each result greater than 0, you should evaluate its need, and then define an exception to allow it. This baseline can be used to detect drift in future.
```

```
Control plane
```

	Control name	Docs
[✓]	API server insecure port is enabled	https://hub.armosec.io/docs/c-0005
[✗]	Anonymous access enabled	https://hub.armosec.io/docs/c-0262
[✗]	Audit logs enabled	https://hub.armosec.io/docs/c-0067
[✓]	RBAC enabled	https://hub.armosec.io/docs/c-0088

➔ The output format is provided to be json.

```
C:\> Users > sRamu > Documents > {} results.json > {} summaryDetails > {} controls > {} C-0265 > {} name
1  {"generationTime":"0001-01-01T00:00:00Z","clusterAPIServerInfo":{"major":"1","minor":"31","gitVersion":"v1.31.0",
"gitCommit":"9edcfcde5595e8a5b1a35f88c421764e575afce","gitTreeState":"clean","buildDate":"2024-08-13T22:44:37Z",
"goVersion":"go1.22.5","compiler":"gc","platform":"linux/amd64"},"clusterCloudProvider":"","customerGUID":"","
"clusterName":"","reportGUID":"","jobID":"","summaryDetails":{"controls":{"C-0002":{"statusInfo":
{"status":"failed"},"controlID":"C-0002","name":"Prevent containers from allowing command execution",
"status":"failed","resourceIDs":{"},"ResourceCounters":{"passedResources":72,"failedResources":1,
"skippedResources":0,"excludedResources":0},"subStatusCounters":{"ignoredResources":1},"score":1.369863,
"complianceScore":98.630135,"scoreFactor":5,"category":{"name":"Access control","id":"Cat-2"}},
{"statusInfo":{"status":"passed"},"controlID":"C-0005","name":"API server insecure port is enabled",
"status":"passed","resourceIDs":{"},"ResourceCounters":{"passedResources":1,"failedResources":0,"skippedResources":0,
"excludedResources":0},"subStatusCounters":{"ignoredResources":0},"score":0,"complianceScore":100,"scoreFactor":9,
"category":{"name":"Control plane","id":"Cat-1"}},
{"statusInfo":{"status":"failed"},"controlID":"C-0007",
"name":"Roles with delete capabilities","status":"failed","resourceIDs":{"},"ResourceCounters":{"passedResources":70,
"failedResources":3,"skippedResources":0,"excludedResources":0},"subStatusCounters":{"ignoredResources":17},
"score":4.109589,"complianceScore":95.89041,"scoreFactor":5,"category":{"name":"Access control","id":"Cat-2"}},
{"statusInfo":{"status":"failed"},"controlID":"C-0012","name":"Applications credentials in configuration
files","status":"failed","resourceIDs":{"},"ResourceCounters":{"passedResources":19,"failedResources":2,
"skippedResources":0,"excludedResources":0},"subStatusCounters":{"ignoredResources":5},"score":9.009008,
"complianceScore":90.47619,"scoreFactor":8,"category":{"name":"Secrets","id":"Cat-3"}},
{"statusInfo":{"status":"failed"},"controlID":"C-0013","name":"Non-root containers","status":"failed","resourceIDs":{"},
"ResourceCounters":{"passedResources":6,"failedResources":2,"skippedResources":0,"excludedResources":0},
```