**Objective**

The main objective of this POC was to find the suitable docker image and container scanning. The findings were based on the criteria that the tools must be open source and should be efficient enough to detect bugs and vulnerabilities in docker images and containers that are stored and run inside our infrastructure. The overall finding result, the one that is generated from successful scanning of images and containers, would help in minimizing threats and risks in our products.

**Methodology**

To perform the possible POC, we needed to look for the tool which was open-source, and which could suffice our needs. To attain this, a number of approaches were initiated to find the tools. With through search we landed on a number of tools and “Docker Bench for security” is one of them.

The Docker Bench for Security is a script that checks for dozens of common best-practices around deploying Docker containers in production. The tests are all automated and are inspired by the CIS Docker Benchmark v1.2.0. It is open source so the Docker community can have an easy way to self-assess their hosts and docker containers against this benchmark.

**Running Docker Bench for Security**

Docker bench comes in as a small container, but it is to keep in mind that the container is being run with a lot of privilege –sharing the host’s filesystem, pid and network namespaces due to portions of the benchmark applying to the running host.

Easiest way to run Docker-Bench will be by running pre-built container:

docker run -it --net host --pid host --userns host --cap-add audit\_control \

-e DOCKER\_CONTENT\_TRUST=$DOCKER\_CONTENT\_TRUST \

-v /etc:/etc:ro \

-v /usr/bin/docker-containerd:/usr/bin/docker-containerd:ro \

-v /usr/bin/docker-runc:/usr/bin/docker-runc:ro \

-v /usr/lib/systemd:/usr/lib/systemd:ro \

-v /var/lib:/var/lib:ro \

-v /var/run/docker.sock:/var/run/docker.sock:ro \

--label docker\_bench\_security \

docker/docker-bench-security

Run container in mac:

docker run -it --net host --pid host --userns host --cap-add audit\_control \

-e DOCKER\_CONTENT\_TRUST=$DOCKER\_CONTENT\_TRUST \

-v /etc:/etc \

-v usr/local/bin/

-v /var/lib:/var/lib:ro \

-v /var/run/docker.sock:/var/run/docker.sock:ro \

--label docker\_bench\_security \

docker/docker-bench-security

**Result: After running in my local,**

**# ------------------------------------------------------------------------------**

**# Docker Bench for Security v1.3.4**

**#**

**# Docker, Inc. (c) 2015-**

**#**

**# Checks for dozens of common best-practices around deploying Docker containers in production.**

**# Inspired by the CIS Docker Community Edition Benchmark v1.1.0.**

**# ------------------------------------------------------------------------------**

Initializing Fri Apr 10 14:56:23 UTC 2020

**[INFO]** 1 - Host Configuration

**[WARN]** 1.1 - Ensure a separate partition for containers has been created

**[NOTE]** 1.2 - Ensure the container host has been Hardened

**[INFO]** 1.3 - Ensure Docker is up to date

**[INFO]** \* Using 19.03.5, verify is it up to date as deemed necessary

**[INFO]** \* Your operating system vendor may provide support and security maintenance for Docker

**[INFO]** 1.4 - Ensure only trusted users are allowed to control Docker daemon

**[WARN]** 1.5 - Ensure auditing is configured for the Docker daemon

**[WARN]** 1.6 - Ensure auditing is configured for Docker files and directories - /var/lib/docker

**[WARN]** 1.7 - Ensure auditing is configured for Docker files and directories - /etc/docker

**[INFO]** 1.8 - Ensure auditing is configured for Docker files and directories - docker.service

**[INFO]** \* File not found

**[INFO]** 1.9 - Ensure auditing is configured for Docker files and directories - docker.socket

**[INFO]** \* File not found

**[INFO]** 1.10 - Ensure auditing is configured for Docker files and directories - /etc/default/docker

**[INFO]** \* File not found

**[INFO]** 1.11 - Ensure auditing is configured for Docker files and directories - /etc/docker/daemon.json

**[INFO]** \* File not found

**[INFO]** 1.12 - Ensure auditing is configured for Docker files and directories - /usr/bin/docker-containerd

**[INFO]** \* File not found

**[INFO]** 1.13 - Ensure auditing is configured for Docker files and directories - /usr/bin/docker-runc

**[INFO]** \* File not found

**[INFO]** 2 - Docker daemon configuration

**[WARN]** 2.1 - Ensure network traffic is restricted between containers on the default bridge

**[PASS]** 2.2 - Ensure the logging level is set to 'info'

**[PASS]** 2.3 - Ensure Docker is allowed to make changes to iptables

**[PASS]** 2.4 - Ensure insecure registries are not used

**[PASS]** 2.5 - Ensure aufs storage driver is not used

**[INFO]** 2.6 - Ensure TLS authentication for Docker daemon is configured

**[INFO]** \* Docker daemon not listening on TCP

**[INFO]** 2.7 - Ensure the default ulimit is configured appropriately

**[INFO]** \* Default ulimit doesn't appear to be set

**[WARN]** 2.8 - Enable user namespace support

**[PASS]** 2.9 - Ensure the default cgroup usage has been confirmed

**[PASS]** 2.10 - Ensure base device size is not changed until needed

**[WARN]** 2.11 - Ensure that authorization for Docker client commands is enabled

**[WARN]** 2.12 - Ensure centralized and remote logging is configured

**[INFO]** 2.13 - Ensure operations on legacy registry (v1) are Disabled (Deprecated)

**[WARN]** 2.14 - Ensure live restore is Enabled

**[WARN]** 2.15 - Ensure Userland Proxy is Disabled

**[PASS]** 2.16 - Ensure daemon-wide custom seccomp profile is applied, if needed

**[PASS]** 2.17 - Ensure experimental features are avoided in production

**[WARN]** 2.18 - Ensure containers are restricted from acquiring new privileges

**[INFO]** 3 - Docker daemon configuration files

**[INFO]** 3.1 - Ensure that docker.service file ownership is set to root:root

**[INFO]** \* File not found

**[INFO]** 3.2 - Ensure that docker.service file permissions are set to 644 or more restrictive

**[INFO]** \* File not found

**[INFO]** 3.3 - Ensure that docker.socket file ownership is set to root:root

**[INFO]** \* File not found

**[INFO]** 3.4 - Ensure that docker.socket file permissions are set to 644 or more restrictive

**[INFO]** \* File not found

**[PASS]** 3.5 - Ensure that /etc/docker directory ownership is set to root:root

**[PASS]** 3.6 - Ensure that /etc/docker directory permissions are set to 755 or more restrictive

**[INFO]** 3.7 - Ensure that registry certificate file ownership is set to root:root

**[INFO]** \* Directory not found

**[INFO]** 3.8 - Ensure that registry certificate file permissions are set to 444 or more restrictive

**[INFO]** \* Directory not found

**[INFO]** 3.9 - Ensure that TLS CA certificate file ownership is set to root:root

**[INFO]** \* No TLS CA certificate found

**[INFO]** 3.10 - Ensure that TLS CA certificate file permissions are set to 444 or more restrictive

**[INFO]** \* No TLS CA certificate found

**[INFO]** 3.11 - Ensure that Docker server certificate file ownership is set to root:root

**[INFO]** \* No TLS Server certificate found

**[INFO]** 3.12 - Ensure that Docker server certificate file permissions are set to 444 or more restrictive

**[INFO]** \* No TLS Server certificate found

**[INFO]** 3.13 - Ensure that Docker server certificate key file ownership is set to root:root

**[INFO]** \* No TLS Key found

**[INFO]** 3.14 - Ensure that Docker server certificate key file permissions are set to 400

**[INFO]** \* No TLS Key found

**[WARN]** 3.15 - Ensure that Docker socket file ownership is set to root:docker

**[WARN]** \* Wrong ownership for /var/run/docker.sock

**[PASS]** 3.16 - Ensure that Docker socket file permissions are set to 660 or more restrictive

**[INFO]** 3.17 - Ensure that daemon.json file ownership is set to root:root

**[INFO]** \* File not found

**[INFO]** 3.18 - Ensure that daemon.json file permissions are set to 644 or more restrictive

**[INFO]** \* File not found

**[INFO]** 3.19 - Ensure that /etc/default/docker file ownership is set to root:root

**[INFO]** \* File not found

**[INFO]** 3.20 - Ensure that /etc/default/docker file permissions are set to 644 or more restrictive

**[INFO]** \* File not found

**[INFO]** 4 - Container Images and Build File

**[WARN]** 4.1 - Ensure a user for the container has been created

**[WARN]** \* Running as root: claimcenter\_home\_1

**[WARN]** \* Running as root: aevolume\_anchore-db\_1

**[WARN]** \* Running as root: migclaimcenter-try101

**[NOTE]** 4.2 - Ensure that containers use trusted base images

**[NOTE]** 4.3 - Ensure unnecessary packages are not installed in the container

**[NOTE]** 4.4 - Ensure images are scanned and rebuilt to include security patches

**[WARN]** 4.5 - Ensure Content trust for Docker is Enabled

**[WARN]** 4.6 - Ensure HEALTHCHECK instructions have been added to the container image

**[WARN]** \* No Healthcheck found: [docker-bench-test\_docker-bench-test:latest]

**[WARN]** \* No Healthcheck found: [abc:latest]

**[WARN]** \* No Healthcheck found: [export2:latest]

**[WARN]** \* No Healthcheck found: [export:latest]

**[WARN]** \* No Healthcheck found: [anchore/engine-db-preload:v0.7.0]

**[WARN]** \* No Healthcheck found: [ubuntu:latest]

**[WARN]** \* No Healthcheck found: [python:latest]

**[WARN]** \* No Healthcheck found: [contactmanger:latest]

**[WARN]** \* No Healthcheck found: [jenkins/jenkins:latest]

**[WARN]** \* No Healthcheck found: [docker:dind]

**[WARN]** \* No Healthcheck found: [alpine:3.11]

**[WARN]** \* No Healthcheck found: [a1:latest]

**[WARN]** \* No Healthcheck found: [try2:latest]

**[WARN]** \* No Healthcheck found: [please-work:latest try1:latest]

**[WARN]** \* No Healthcheck found: [please-work:latest try1:latest]

**[WARN]** \* No Healthcheck found: [pleasework:latest]

**[WARN]** \* No Healthcheck found: [docker-compose-secret\_flask-app-service:latest]

**[WARN]** \* No Healthcheck found: [vault:latest]

**[WARN]** \* No Healthcheck found: [wordpress:latest]

**[WARN]** \* No Healthcheck found: [demo\_home:latest]

**[WARN]** \* No Healthcheck found: [nexus3.mmi.mig.corp:5000/migclaimcenter:try101]

**[WARN]** \* No Healthcheck found: [moving-env:latest]

**[WARN]** \* No Healthcheck found: [nexus3.mmi.mig.corp:5000/migclaimcenter-updated:latest]

**[WARN]** \* No Healthcheck found: [nexus3.mmi.mig.corp:5000/migclaimcenter:latest]

**[WARN]** \* No Healthcheck found: [busybox:1.31.1]

**[WARN]** \* No Healthcheck found: [mysql:5.7]

**[WARN]** \* No Healthcheck found: [mysql:latest]

**[WARN]** \* No Healthcheck found: [postgres:9.4]

**[WARN]** \* No Healthcheck found: [nexus3.mmi.mig.corp:5000/migtomcat7:7.0.99]

**[WARN]** \* No Healthcheck found: [alpine:latest]

**[WARN]** \* No Healthcheck found: [mariadb:10.4.8-bionic]

**[WARN]** \* No Healthcheck found: [alpine:3.7]

**[WARN]** \* No Healthcheck found: [alpine:3.3]

**[WARN]** \* No Healthcheck found: [nexus3.mmi.mig.corp:5000/migant:1.8.2-7]

**[WARN]** \* No Healthcheck found: [jenkins/jenkins:2.121.2]

**[WARN]** \* No Healthcheck found: [python:3-onbuild]

**[INFO]** 4.7 - Ensure update instructions are not use alone in the Dockerfile

**[INFO]** \* Update instruction found: [docker-bench-test\_docker-bench-test:latest]

**[INFO]** \* Update instruction found: [anchore/engine-db-preload:v0.7.0]

**[INFO]** \* Update instruction found: [python:latest]

**[INFO]** \* Update instruction found: [contactmanger:latest]

**[INFO]** \* Update instruction found: [jenkins/jenkins:latest]

**[INFO]** \* Update instruction found: [docker-compose-secret\_flask-app-service:latest]

**[INFO]** \* Update instruction found: [wordpress:latest]

**[INFO]** \* Update instruction found: [nexus3.mmi.mig.corp:5000/migclaimcenter:try101]

**[INFO]** \* Update instruction found: [nexus3.mmi.mig.corp:5000/migclaimcenter-updated:latest]

**[INFO]** \* Update instruction found: [nexus3.mmi.mig.corp:5000/migclaimcenter:latest]

**[INFO]** \* Update instruction found: [mysql:5.7]

**[INFO]** \* Update instruction found: [mysql:latest]

**[INFO]** \* Update instruction found: [postgres:9.4]

**[INFO]** \* Update instruction found: [nexus3.mmi.mig.corp:5000/migtomcat7:7.0.99]

**[INFO]** \* Update instruction found: [mariadb:10.4.8-bionic]

**[INFO]** \* Update instruction found: [nexus3.mmi.mig.corp:5000/migant:1.8.2-7]

**[INFO]** \* Update instruction found: [jenkins/jenkins:2.121.2]

**[INFO]** \* Update instruction found: [python:3-onbuild]

**[NOTE]** 4.8 - Ensure setuid and setgid permissions are removed in the images

**[INFO]** 4.9 - Ensure COPY is used instead of ADD in Dockerfile

**[INFO]** \* ADD in image history: [docker-bench-test\_docker-bench-test:latest]

**[INFO]** \* ADD in image history: [abc:latest]

**[INFO]** \* ADD in image history: [export2:latest]

**[INFO]** \* ADD in image history: [export:latest]

**[INFO]** \* ADD in image history: [docker-bench-security\_docker-bench-security:latest]

**[INFO]** \* ADD in image history: [anchore/engine-db-preload:v0.7.0]

**[INFO]** \* ADD in image history: [ubuntu:latest]

**[INFO]** \* ADD in image history: [python:latest]

**[INFO]** \* ADD in image history: [contactmanger:latest]

**[INFO]** \* ADD in image history: [jenkins/jenkins:latest]

**[INFO]** \* ADD in image history: [docker:dind]

**[INFO]** \* ADD in image history: [alpine:3.11]

**[INFO]** \* ADD in image history: [a1:latest]

**[INFO]** \* ADD in image history: [try2:latest]

**[INFO]** \* ADD in image history: [please-work:latest try1:latest]

**[INFO]** \* ADD in image history: [please-work:latest try1:latest]

**[INFO]** \* ADD in image history: [pleasework:latest]

**[INFO]** \* ADD in image history: [docker-compose-secret\_flask-app-service:latest]

**[INFO]** \* ADD in image history: [vault:latest]

**[INFO]** \* ADD in image history: [wordpress:latest]

**[INFO]** \* ADD in image history: [demo\_home:latest]

**[INFO]** \* ADD in image history: [nexus3.mmi.mig.corp:5000/migclaimcenter:try101]

**[INFO]** \* ADD in image history: [moving-env:latest]

**[INFO]** \* ADD in image history: [nexus3.mmi.mig.corp:5000/migclaimcenter-updated:latest]

**[INFO]** \* ADD in image history: [nexus3.mmi.mig.corp:5000/migclaimcenter:latest]

**[INFO]** \* ADD in image history: [busybox:1.31.1]

**[INFO]** \* ADD in image history: [mysql:5.7]

**[INFO]** \* ADD in image history: [mysql:latest]

**[INFO]** \* ADD in image history: [postgres:9.4]

**[INFO]** \* ADD in image history: [nexus3.mmi.mig.corp:5000/migtomcat7:7.0.99]

**[INFO]** \* ADD in image history: [alpine:latest]

**[INFO]** \* ADD in image history: [mariadb:10.4.8-bionic]

**[INFO]** \* ADD in image history: [alpine:3.7]

**[INFO]** \* ADD in image history: [alpine:3.3]

**[INFO]** \* ADD in image history: [docker/docker-bench-security:latest]

**[INFO]** \* ADD in image history: [nexus3.mmi.mig.corp:5000/migant:1.8.2-7]

**[INFO]** \* ADD in image history: [jenkins/jenkins:2.121.2]

**[INFO]** \* ADD in image history: [python:3-onbuild]

**[NOTE]** 4.10 - Ensure secrets are not stored in Dockerfiles

**[NOTE]** 4.11 - Ensure verified packages are only Installed

**[INFO]** 5 - Container Runtime

**[WARN]** 5.1 - Ensure AppArmor Profile is Enabled

**[WARN]** \* No AppArmorProfile Found: claimcenter\_home\_1

**[WARN]** \* No AppArmorProfile Found: aevolume\_engine-simpleq\_1

**[WARN]** \* No AppArmorProfile Found: aevolume\_engine-analyzer\_1

**[WARN]** \* No AppArmorProfile Found: aevolume\_engine-api\_1

**[WARN]** \* No AppArmorProfile Found: aevolume\_engine-policy-engine\_1

**[WARN]** \* No AppArmorProfile Found: aevolume\_engine-catalog\_1

**[WARN]** \* No AppArmorProfile Found: aevolume\_anchore-db\_1

**[WARN]** \* No AppArmorProfile Found: migclaimcenter-try101

**[WARN]** 5.2 - Ensure SELinux security options are set, if applicable

**[WARN]** \* No SecurityOptions Found: claimcenter\_home\_1

**[WARN]** \* No SecurityOptions Found: aevolume\_engine-simpleq\_1

**[WARN]** \* No SecurityOptions Found: aevolume\_engine-analyzer\_1

**[WARN]** \* No SecurityOptions Found: aevolume\_engine-api\_1

**[WARN]** \* No SecurityOptions Found: aevolume\_engine-policy-engine\_1

**[WARN]** \* No SecurityOptions Found: aevolume\_engine-catalog\_1

**[WARN]** \* No SecurityOptions Found: aevolume\_anchore-db\_1

**[WARN]** \* No SecurityOptions Found: migclaimcenter-try101

**[PASS]** 5.3 - Ensure Linux Kernel Capabilities are restricted within containers

**[PASS]** 5.4 - Ensure privileged containers are not used

**[PASS]** 5.5 - Ensure sensitive host system directories are not mounted on containers

**[PASS]** 5.6 - Ensure ssh is not run within containers

**[PASS]** 5.7 - Ensure privileged ports are not mapped within containers

**[NOTE]** 5.8 - Ensure only needed ports are open on the container

**[PASS]** 5.9 - Ensure the host's network namespace is not shared

**[WARN]** 5.10 - Ensure memory usage for container is limited

**[WARN]** \* Container running without memory restrictions: claimcenter\_home\_1

**[WARN]** \* Container running without memory restrictions: aevolume\_engine-simpleq\_1

**[WARN]** \* Container running without memory restrictions: aevolume\_engine-analyzer\_1

**[WARN]** \* Container running without memory restrictions: aevolume\_engine-api\_1

**[WARN]** \* Container running without memory restrictions: aevolume\_engine-policy-engine\_1

**[WARN]** \* Container running without memory restrictions: aevolume\_engine-catalog\_1

**[WARN]** \* Container running without memory restrictions: aevolume\_anchore-db\_1

**[WARN]** \* Container running without memory restrictions: migclaimcenter-try101

**[WARN]** 5.11 - Ensure CPU priority is set appropriately on the container

**[WARN]** \* Container running without CPU restrictions: claimcenter\_home\_1

**[WARN]** \* Container running without CPU restrictions: aevolume\_engine-simpleq\_1

**[WARN]** \* Container running without CPU restrictions: aevolume\_engine-analyzer\_1

**[WARN]** \* Container running without CPU restrictions: aevolume\_engine-api\_1

**[WARN]** \* Container running without CPU restrictions: aevolume\_engine-policy-engine\_1

**[WARN]** \* Container running without CPU restrictions: aevolume\_engine-catalog\_1

**[WARN]** \* Container running without CPU restrictions: aevolume\_anchore-db\_1

**[WARN]** \* Container running without CPU restrictions: migclaimcenter-try101

**[WARN]** 5.12 - Ensure the container's root filesystem is mounted as read only

**[WARN]** \* Container running with root FS mounted R/W: claimcenter\_home\_1

**[WARN]** \* Container running with root FS mounted R/W: aevolume\_engine-simpleq\_1

**[WARN]** \* Container running with root FS mounted R/W: aevolume\_engine-analyzer\_1

**[WARN]** \* Container running with root FS mounted R/W: aevolume\_engine-api\_1

**[WARN]** \* Container running with root FS mounted R/W: aevolume\_engine-policy-engine\_1

**[WARN]** \* Container running with root FS mounted R/W: aevolume\_engine-catalog\_1

**[WARN]** \* Container running with root FS mounted R/W: aevolume\_anchore-db\_1

**[WARN]** \* Container running with root FS mounted R/W: migclaimcenter-try101

**[WARN]** 5.13 - Ensure incoming container traffic is binded to a specific host interface

**[WARN]** \* Port being bound to wildcard IP: 0.0.0.0 in aevolume\_engine-api\_1

**[WARN]** \* Port being bound to wildcard IP: 0.0.0.0 in migclaimcenter-try101

**[WARN]** 5.14 - Ensure 'on-failure' container restart policy is set to '5'

**[WARN]** \* MaximumRetryCount is not set to 5: claimcenter\_home\_1

**[WARN]** \* MaximumRetryCount is not set to 5: aevolume\_engine-simpleq\_1

**[WARN]** \* MaximumRetryCount is not set to 5: aevolume\_engine-analyzer\_1

**[WARN]** \* MaximumRetryCount is not set to 5: aevolume\_engine-api\_1

**[WARN]** \* MaximumRetryCount is not set to 5: aevolume\_engine-policy-engine\_1

**[WARN]** \* MaximumRetryCount is not set to 5: aevolume\_engine-catalog\_1

**[WARN]** \* MaximumRetryCount is not set to 5: aevolume\_anchore-db\_1

**[WARN]** \* MaximumRetryCount is not set to 5: migclaimcenter-try101

**[PASS]** 5.15 - Ensure the host's process namespace is not shared

**[PASS]** 5.16 - Ensure the host's IPC namespace is not shared

**[PASS]** 5.17 - Ensure host devices are not directly exposed to containers

**[INFO]** 5.18 - Ensure the default ulimit is overwritten at runtime, only if needed

**[INFO]** \* Container no default ulimit override: claimcenter\_home\_1

**[INFO]** \* Container no default ulimit override: aevolume\_engine-simpleq\_1

**[INFO]** \* Container no default ulimit override: aevolume\_engine-analyzer\_1

**[INFO]** \* Container no default ulimit override: aevolume\_engine-api\_1

**[INFO]** \* Container no default ulimit override: aevolume\_engine-policy-engine\_1

**[INFO]** \* Container no default ulimit override: aevolume\_engine-catalog\_1

**[INFO]** \* Container no default ulimit override: aevolume\_anchore-db\_1

**[INFO]** \* Container no default ulimit override: migclaimcenter-try101

**[PASS]** 5.19 - Ensure mount propagation mode is not set to shared

**[PASS]** 5.20 - Ensure the host's UTS namespace is not shared

**[PASS]** 5.21 - Ensure the default seccomp profile is not Disabled

**[NOTE]** 5.22 - Ensure docker exec commands are not used with privileged option

**[NOTE]** 5.23 - Ensure docker exec commands are not used with user option

**[PASS]** 5.24 - Ensure cgroup usage is confirmed

**[WARN]** 5.25 - Ensure the container is restricted from acquiring additional privileges

**[WARN]** \* Privileges not restricted: claimcenter\_home\_1

**[WARN]** \* Privileges not restricted: aevolume\_engine-simpleq\_1

**[WARN]** \* Privileges not restricted: aevolume\_engine-analyzer\_1

**[WARN]** \* Privileges not restricted: aevolume\_engine-api\_1

**[WARN]** \* Privileges not restricted: aevolume\_engine-policy-engine\_1

**[WARN]** \* Privileges not restricted: aevolume\_engine-catalog\_1

**[WARN]** \* Privileges not restricted: aevolume\_anchore-db\_1

**[WARN]** \* Privileges not restricted: migclaimcenter-try101

**[WARN]** 5.26 - Ensure container health is checked at runtime

**[WARN]** \* Health check not set: claimcenter\_home\_1

**[WARN]** \* Health check not set: aevolume\_anchore-db\_1

**[WARN]** \* Health check not set: migclaimcenter-try101

**[INFO]** 5.27 - Ensure docker commands always get the latest version of the image

**[WARN]** 5.28 - Ensure PIDs cgroup limit is used

**[WARN]** \* PIDs limit not set: claimcenter\_home\_1

**[WARN]** \* PIDs limit not set: aevolume\_engine-simpleq\_1

**[WARN]** \* PIDs limit not set: aevolume\_engine-analyzer\_1

**[WARN]** \* PIDs limit not set: aevolume\_engine-api\_1

**[WARN]** \* PIDs limit not set: aevolume\_engine-policy-engine\_1

**[WARN]** \* PIDs limit not set: aevolume\_engine-catalog\_1

**[WARN]** \* PIDs limit not set: aevolume\_anchore-db\_1

**[WARN]** \* PIDs limit not set: migclaimcenter-try101

**[INFO]** 5.29 - Ensure Docker's default bridge docker0 is not used

**[INFO]** \* Container in docker0 network: migclaimcenter-try101

**[PASS]** 5.30 - Ensure the host's user namespaces is not shared

**[PASS]** 5.31 - Ensure the Docker socket is not mounted inside any containers

**[INFO]** 6 - Docker Security Operations

**[INFO]** 6.1 - Avoid image sprawl

**[INFO]** \* There are currently: 41 images

**[INFO]** \* Only 15 out of 41 are in use

**[INFO]** 6.2 - Avoid container sprawl

**[INFO]** \* There are currently a total of 15 containers, with 9 of them currently running

**[INFO]** 7 - Docker Swarm Configuration

**[PASS]** 7.1 - Ensure swarm mode is not Enabled, if not needed

**[PASS]** 7.2 - Ensure the minimum number of manager nodes have been created in a swarm (Swarm mode not enabled)

**[PASS]** 7.3 - Ensure swarm services are binded to a specific host interface (Swarm mode not enabled)

**[PASS]** 7.4 - Ensure data exchanged between containers are encrypted on different nodes on the overlay network

**[PASS]** 7.5 - Ensure Docker's secret management commands are used for managing secrets in a Swarm cluster (Swarm mode not enabled)

**[PASS]** 7.6 - Ensure swarm manager is run in auto-lock mode (Swarm mode not enabled)

**[PASS]** 7.7 - Ensure swarm manager auto-lock key is rotated periodically (Swarm mode not enabled)

**[PASS]** 7.8 - Ensure node certificates are rotated as appropriate (Swarm mode not enabled)

**[PASS]** 7.9 - Ensure CA certificates are rotated as appropriate (Swarm mode not enabled)

**[PASS]** 7.10 - Ensure management plane traffic has been separated from data plane traffic (Swarm mode not enabled)

**[INFO]** Checks: 105

**[INFO]** Score: 10

**Understanding Errors/Warnings**

After running the script successfully, we will see the output similar to the content above. Scripts results in INFO, WARNING and PASS notes for each of the configuration recommendations which are grouped into 7 sections

1. Host Configuration
2. Docker Daemon Configuration
3. Docker Daemon Configuration Files
4. Container Images and Build Files
5. Container Runtime
6. Docker Security Operations
7. Docker Swarm Configuration

With the results of these findings, you can leverage the original benchmark document to remediate them. Which each recommendation (5.14, for example) there is a Remediation heading in the document which details the steps required to bring the configuration into compliance.