COMMAND: 5.1 Change the directory to execute the benchmark (CIS)

```
clus
```

OR

COMMAND: 5.2 - Change the directory to execute the benchmark (CIS)

```
cd /home/cluser1/clus19-audit/cis_benchmark/docker-bench-security
```

OUTPUT: 5.1 and 5.2

```
[cluser1@clus2019-management docker-bench-security]$
```

OR

```
[cluser1@clus2019-management docker-bench-security]$
```

COMMAND: 5.3 Execute the benchmark (CIS) in the Management Node of CVIM

```
sudo sh docker-bench-security.sh
```

OUTPUT: 5.3

```
[cluser1@clus2019-management docker-bench-security]$ sudo sh docker-bench-security.sh
# ------------------------------------------------------------------------------
# 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 Sat Jun  8 02:00:09 UTC 2019

****************** Section 1 ****************************
[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 1.13.1, 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
[WARN] 1.8  - Ensure auditing is configured for Docker files and directories - docker.service
```

```
[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
[WARN] 1.11  - Ensure auditing is configured for Docker files and directories -
/etc/docker/daemon.json
[WARN] 1.12  - Ensure auditing is configured for Docker files and directories - /usr/bin/docker-
containerd
[INFO] 1.13  - Ensure auditing is configured for Docker files and directories - /usr/bin/docker-runc
[INFO]      * File not found


***************** Section 2 **************************
[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

[WARN] 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
[PASS] 2.11  - Ensure that authorization for Docker client commands is enabled
[PASS] 2.12  - Ensure centralized and remote logging is configured

[WARN] 2.13  - Ensure operations on legacy registry (v1) are Disabled
[WARN] 2.14  - Ensure live restore is Enabled
[WARN] 2.15  - Ensure Userland Proxy is Disabled
[INFO] 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


***************** Section 3 **************************

[INFO] 3 - Docker daemon configuration files
[PASS] 3.1  - Ensure that docker.service file ownership is set to root:root
```

```
[PASS] 3.2  - Ensure that docker.service file permissions are set to 644 or more restrictive
[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
[PASS] 3.7  - Ensure that registry certificate file ownership is set to root:root
[PASS] 3.8  - Ensure that registry certificate file permissions are set to 444 or more restrictive
[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
[PASS] 3.17  - Ensure that daemon.json file ownership is set to root:root
[PASS] 3.18  - Ensure that daemon.json file permissions are set to 644 or more restrictive
[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

***************** Section 4 ***************************

[INFO] 4 - Container Images and Build File
[WARN] 4.1  - Ensure a user for the container has been created
[WARN]      * Running as root: container_registry
[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: [dockbler-keys:latest]
[WARN]      * No Healthcheck found: [192.168.20.105:5000/cvim-rhel7-osp13/elasticsearch:16550]
[WARN]      * No Healthcheck found: [192.168.20.105:5000/cvim-rhel7-osp13/vmtp:16550]
[WARN]      * No Healthcheck found: [192.168.20.105:5000/cvim-rhel7-osp13/vim-config:16550]
[WARN]      * No Healthcheck found: [192.168.20.105:5000/cvim-rhel7-osp13/curator:16550]
[WARN]      * No Healthcheck found: [192.168.20.105:5000/cvim-rhel7-osp13/dockbler-web:16550]
```

```
[WARN]      * No Healthcheck found: [192.168.20.105:5000/cvim-rhel7-osp13/dockbler-rhel-7-server-optional-rpms:16550]
[WARN]      * No Healthcheck found: [192.168.20.105:5000/cvim-rhel7-osp13/fluentd-aggr:16550]
[WARN]      * No Healthcheck found: [192.168.20.105:5000/cvim-rhel7-osp13/dockbler-rhel-7-server-openstack-13-devtools-rpms:16550]
[WARN]      * No Healthcheck found: [192.168.20.105:5000/cvim-rhel7-osp13/dockbler-app:16550]
[WARN]      * No Healthcheck found: [192.168.20.105:5000/cvim-rhel7-osp13/dockbler-mercury-cloudpulse-rpms:16550]
[WARN]      * No Healthcheck found: [192.168.20.105:5000/cvim-rhel7-osp13/dockbler-mercury-buildnode-rpms:16550]
[WARN]      * No Healthcheck found: [192.168.20.105:5000/cvim-rhel7-osp13/dockbler-rhel-7-server-rpms:16550]
[WARN]      * No Healthcheck found: [192.168.20.105:5000/cvim-rhel7-osp13/dockbler-rhel-7-server-openstack-13-optools-rpms:16550]
[WARN]      * No Healthcheck found: [192.168.20.105:5000/cvim-rhel7-osp13/dockbler-rhel-7-server-extras-rpms:16550]
[WARN]      * No Healthcheck found: [192.168.20.105:5000/cvim-rhel7-osp13/dockbler-rhel-7-server-rh-common-rpms:16550]
[WARN]      * No Healthcheck found: [192.168.20.105:5000/cvim-rhel7-osp13/dockbler-mercury-thirdparty-hw-binary-utilities-rpms:16550]
[WARN]      * No Healthcheck found: [192.168.20.105:5000/cvim-rhel7-osp13/dockbler-rhel-7-server-openstack-13-rpms:16550]
[WARN]      * No Healthcheck found: [192.168.20.105:5000/cvim-rhel7-osp13/dockbler-rhel-7-server-rhceph-3-osd-rpms:16550]
[WARN]      * No Healthcheck found: [192.168.20.105:5000/cvim-rhel7-osp13/dockbler-rhel-7-server-openstack-13-tools-rpms:16550]
[WARN]      * No Healthcheck found: [192.168.20.105:5000/cvim-rhel7-osp13/kibana:16550]
[WARN]      * No Healthcheck found: [192.168.20.105:5000/cvim-rhel7-osp13/dockbler-cisco-rhel-server-7-openstack-13-hotfix-rpms:16550]
[WARN]      * No Healthcheck found: [192.168.20.105:5000/cvim-rhel7-osp13/dockbler-rhel-ha-for-rhel-7-server-rpms:16550]
[WARN]      * No Healthcheck found: [192.168.20.105:5000/cvim-rhel7-osp13/dockbler-mercury-common-rpms:16550]
[WARN]      * No Healthcheck found: [192.168.20.105:5000/cvim-rhel7-osp13/dockbler-tftp:16550]
[WARN]      * No Healthcheck found: [192.168.20.105:5000/cvim-rhel7-osp13/dockbler-rhel-boot:16550]
[WARN]      * No Healthcheck found: [192.168.20.105:5000/cvim-rhel7-osp13/dockbler-repofiles:16550]
[WARN]      * No Healthcheck found: [cloud-docker.cisco.com:8443/redstone/registry-2.6.2:16550]
[INFO] 4.7  - Ensure update instructions are not use alone in the Dockerfile
[INFO]      * Update instruction found: [dockbler-keys:latest]
[INFO]      * Update instruction found: [192.168.20.105:5000/cvim-rhel7-osp13/elasticsearch:16550]
[INFO]      * Update instruction found: [192.168.20.105:5000/cvim-rhel7-osp13/vmtp:16550]
[INFO]      * Update instruction found: [192.168.20.105:5000/cvim-rhel7-osp13/vim-config:16550]
[INFO]      * Update instruction found: [192.168.20.105:5000/cvim-rhel7-osp13/curator:16550]
[INFO]      * Update instruction found: [192.168.20.105:5000/cvim-rhel7-osp13/dockbler-web:16550]
[INFO]      * Update instruction found: [192.168.20.105:5000/cvim-rhel7-osp13/dockbler-rhel-7-server-optional-rpms:16550]
```

```
[INFO]      * Update instruction found: [192.168.20.105:5000/cvim-rhel7-osp13/fluentd-aggr:16550]
[INFO]      * Update instruction found: [192.168.20.105:5000/cvim-rhel7-osp13/dockbler-rhel-7-server-openstack-13-devtools-rpms:16550]
[INFO]      * Update instruction found: [192.168.20.105:5000/cvim-rhel7-osp13/dockbler-app:16550]
[INFO]      * Update instruction found: [192.168.20.105:5000/cvim-rhel7-osp13/dockbler-mercury-cloudpulse-rpms:16550]
[INFO]      * Update instruction found: [192.168.20.105:5000/cvim-rhel7-osp13/dockbler-mercury-buildnode-rpms:16550]
[INFO]      * Update instruction found: [192.168.20.105:5000/cvim-rhel7-osp13/dockbler-rhel-7-server-rpms:16550]
[INFO]      * Update instruction found: [192.168.20.105:5000/cvim-rhel7-osp13/dockbler-rhel-7-server-openstack-13-optools-rpms:16550]
[INFO]      * Update instruction found: [192.168.20.105:5000/cvim-rhel7-osp13/dockbler-rhel-7-server-extras-rpms:16550]
[INFO]      * Update instruction found: [192.168.20.105:5000/cvim-rhel7-osp13/dockbler-rhel-7-server-rh-common-rpms:16550]
[INFO]      * Update instruction found: [192.168.20.105:5000/cvim-rhel7-osp13/dockbler-mercury-thirdparty-hw-binary-utilities-rpms:16550]
[INFO]      * Update instruction found: [192.168.20.105:5000/cvim-rhel7-osp13/dockbler-rhel-7-server-openstack-13-rpms:16550]
[INFO]      * Update instruction found: [192.168.20.105:5000/cvim-rhel7-osp13/dockbler-rhel-7-server-rhceph-3-osd-rpms:16550]
[INFO]      * Update instruction found: [192.168.20.105:5000/cvim-rhel7-osp13/dockbler-rhel-7-server-openstack-13-tools-rpms:16550]
[INFO]      * Update instruction found: [192.168.20.105:5000/cvim-rhel7-osp13/kibana:16550]
[INFO]      * Update instruction found: [192.168.20.105:5000/cvim-rhel7-osp13/dockbler-cisco-rhel-server-7-openstack-13-hotfix-rpms:16550]
[INFO]      * Update instruction found: [192.168.20.105:5000/cvim-rhel7-osp13/dockbler-rhel-ha-for-rhel-7-server-rpms:16550]
[INFO]      * Update instruction found: [192.168.20.105:5000/cvim-rhel7-osp13/dockbler-mercury-common-rpms:16550]
[INFO]      * Update instruction found: [192.168.20.105:5000/cvim-rhel7-osp13/dockbler-tftp:16550]
[INFO]      * Update instruction found: [192.168.20.105:5000/cvim-rhel7-osp13/dockbler-rhel-boot:16550]
[INFO]      * Update instruction found: [192.168.20.105:5000/cvim-rhel7-osp13/dockbler-repofiles:16550]
[NOTE] 4.8  - Ensure setuid and setgid permissions are removed in the images
unknown flag: --format
See 'docker history --help'.
 [PASS] 4.9  - Ensure COPY is used instead of ADD in Dockerfile
[NOTE] 4.10  - Ensure secrets are not stored in Dockerfiles
[NOTE] 4.11  - Ensure verified packages are only Installed

***************** Section 5 ***************************

[INFO] 5 - Container Runtime
[WARN] 5.1  - Ensure AppArmor Profile is Enabled
[WARN]      * No AppArmorProfile Found: vmtp_16550
```

```
[WARN]      * No AppArmorProfile Found: vimconfig_16550
[WARN]      * No AppArmorProfile Found: fluentd_aggr_16550
[WARN]      * No AppArmorProfile Found: curator_16550
[WARN]      * No AppArmorProfile Found: kibana_16550
[WARN]      * No AppArmorProfile Found: elasticsearch_16550
[WARN]      * No AppArmorProfile Found: tftp_server_16550
[WARN]      * No AppArmorProfile Found: my_cobbler_16550
[WARN]      * No AppArmorProfile Found: repo_mirror_16550
[WARN]      * No AppArmorProfile Found: container_registry
[WARN] 5.2  - Ensure SELinux security options are set, if applicable
[WARN]      * No SecurityOptions Found: vimconfig_16550
[WARN]      * No SecurityOptions Found: curator_16550
[WARN]      * No SecurityOptions Found: kibana_16550
[WARN]      * No SecurityOptions Found: tftp_server_16550
[WARN]      * No SecurityOptions Found: my_cobbler_16550
[PASS] 5.3  - Ensure Linux Kernel Capabilities are restricted within containers
[WARN] 5.4  - Ensure privileged containers are not used
[WARN]      * Container running in Privileged mode: vmtp_16550
[WARN]      * Container running in Privileged mode: fluentd_aggr_16550
[WARN]      * Container running in Privileged mode: elasticsearch_16550
[WARN]      * Container running in Privileged mode: repo_mirror_16550
[WARN]      * Container running in Privileged mode: container_registry
[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
[WARN] 5.9  - Ensure the host's network namespace is not shared
[WARN]      * Container running with networking mode 'host': vmtp_16550
[WARN]      * Container running with networking mode 'host': vimconfig_16550
[WARN]      * Container running with networking mode 'host': fluentd_aggr_16550
[WARN]      * Container running with networking mode 'host': curator_16550
[WARN]      * Container running with networking mode 'host': kibana_16550
[WARN]      * Container running with networking mode 'host': elasticsearch_16550
[WARN]      * Container running with networking mode 'host': tftp_server_16550
[WARN]      * Container running with networking mode 'host': my_cobbler_16550
[WARN]      * Container running with networking mode 'host': repo_mirror_16550
[WARN]      * Container running with networking mode 'host': container_registry
[WARN] 5.10  - Ensure memory usage for container is limited
[WARN]      * Container running without memory restrictions: vmtp_16550
[WARN]      * Container running without memory restrictions: vimconfig_16550
[WARN]      * Container running without memory restrictions: fluentd_aggr_16550
[WARN]      * Container running without memory restrictions: curator_16550
[WARN]      * Container running without memory restrictions: kibana_16550
[WARN]      * Container running without memory restrictions: elasticsearch_16550
[WARN]      * Container running without memory restrictions: tftp_server_16550
[WARN]      * Container running without memory restrictions: my_cobbler_16550
[WARN]      * Container running without memory restrictions: repo_mirror_16550
[WARN]      * Container running without memory restrictions: container_registry
```

```
[WARN] 5.11  - Ensure CPU priority is set appropriately on the container
[WARN]      * Container running without CPU restrictions: vmtp_16550
[WARN]      * Container running without CPU restrictions: vimconfig_16550
[WARN]      * Container running without CPU restrictions: fluentd_aggr_16550
[WARN]      * Container running without CPU restrictions: curator_16550
[WARN]      * Container running without CPU restrictions: kibana_16550
[WARN]      * Container running without CPU restrictions: elasticsearch_16550
[WARN]      * Container running without CPU restrictions: tftp_server_16550
[WARN]      * Container running without CPU restrictions: my_cobbler_16550
[WARN]      * Container running without CPU restrictions: repo_mirror_16550
[WARN]      * Container running without CPU restrictions: container_registry
[WARN] 5.12  - Ensure the container's root filesystem is mounted as read only
[WARN]      * Container running with root FS mounted R/W: vmtp_16550
[WARN]      * Container running with root FS mounted R/W: vimconfig_16550
[WARN]      * Container running with root FS mounted R/W: fluentd_aggr_16550
[WARN]      * Container running with root FS mounted R/W: curator_16550
[WARN]      * Container running with root FS mounted R/W: kibana_16550
[WARN]      * Container running with root FS mounted R/W: elasticsearch_16550
[WARN]      * Container running with root FS mounted R/W: tftp_server_16550
[WARN]      * Container running with root FS mounted R/W: my_cobbler_16550
[WARN]      * Container running with root FS mounted R/W: repo_mirror_16550
[WARN]      * Container running with root FS mounted R/W: container_registry
[PASS] 5.13  - Ensure incoming container traffic is binded to a specific host interface
[WARN] 5.14  - Ensure 'on-failure' container restart policy is set to '5'
[WARN]      * MaximumRetryCount is not set to 5: vmtp_16550
[WARN]      * MaximumRetryCount is not set to 5: vimconfig_16550
[WARN]      * MaximumRetryCount is not set to 5: fluentd_aggr_16550
[WARN]      * MaximumRetryCount is not set to 5: curator_16550
[WARN]      * MaximumRetryCount is not set to 5: kibana_16550
[WARN]      * MaximumRetryCount is not set to 5: elasticsearch_16550
[WARN]      * MaximumRetryCount is not set to 5: tftp_server_16550
[WARN]      * MaximumRetryCount is not set to 5: my_cobbler_16550
[WARN]      * MaximumRetryCount is not set to 5: repo_mirror_16550
[WARN]      * MaximumRetryCount is not set to 5: container_registry
[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: vmtp_16550
[INFO]      * Container no default ulimit override: vimconfig_16550
[INFO]      * Container no default ulimit override: fluentd_aggr_16550
[INFO]      * Container no default ulimit override: curator_16550
[INFO]      * Container no default ulimit override: kibana_16550
[INFO]      * Container no default ulimit override: elasticsearch_16550
[INFO]      * Container no default ulimit override: tftp_server_16550
[INFO]      * Container no default ulimit override: my_cobbler_16550
[INFO]      * Container no default ulimit override: repo_mirror_16550
[INFO]      * Container no default ulimit override: container_registry
```

```
[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: vmtp_16550
[WARN]      * Privileges not restricted: vimconfig_16550
[WARN]      * Privileges not restricted: fluentd_aggr_16550
[WARN]      * Privileges not restricted: curator_16550
[WARN]      * Privileges not restricted: kibana_16550
[WARN]      * Privileges not restricted: elasticsearch_16550
[WARN]      * Privileges not restricted: tftp_server_16550
[WARN]      * Privileges not restricted: my_cobbler_16550
[WARN]      * Privileges not restricted: repo_mirror_16550
[WARN]      * Privileges not restricted: container_registry
[WARN] 5.26  - Ensure container health is checked at runtime
[WARN]      * Health check not set: vmtp_16550
[WARN]      * Health check not set: vimconfig_16550
[WARN]      * Health check not set: fluentd_aggr_16550
[WARN]      * Health check not set: curator_16550
[WARN]      * Health check not set: kibana_16550
[WARN]      * Health check not set: elasticsearch_16550
[WARN]      * Health check not set: tftp_server_16550
[WARN]      * Health check not set: my_cobbler_16550
[WARN]      * Health check not set: repo_mirror_16550
[WARN]      * Health check not set: container_registry
[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: vmtp_16550
[WARN]      * PIDs limit not set: vimconfig_16550
[WARN]      * PIDs limit not set: fluentd_aggr_16550
[WARN]      * PIDs limit not set: curator_16550
[WARN]      * PIDs limit not set: kibana_16550
[WARN]      * PIDs limit not set: elasticsearch_16550
[WARN]      * PIDs limit not set: tftp_server_16550
[WARN]      * PIDs limit not set: my_cobbler_16550
[WARN]      * PIDs limit not set: repo_mirror_16550
[WARN]      * PIDs limit not set: container_registry
[PASS] 5.29  - Ensure Docker's default bridge docker0 is not used
[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: 28 images
```

```
[INFO] 6.2  - Avoid container sprawl
[INFO]      * There are currently a total of 28 containers, with 10 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: 13
```

Compare OpenStack with VM running Docker

Switch to the VM with IP 10.201.36.76

COMMANDS:5.4 – Log into the VM running in CVIM management node

```
ssh <username>@10.201.36.76
cd sec_audit/cisc_benchmark/docker-bench-security
```

COMMAND:5.5 Execute the benchmark (CIS)

```
sudo sh docker-bench-security.sh
```

OUTPUT: 5.5

```
[cluser1@clus-1-vm1 docker-bench-security]$ sudo sh docker-bench-security.sh

We trust you have received the usual lecture from the local System Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
```

```
   #2) Think before you type.
   #3) With great power comes great responsibility.

[sudo] password for cluser1:
# ------------------------------------------------------------------------------
# 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 Sat Jun  8 14:24:51 UTC 2019


[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 1.13.1, 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
[INFO]      * docker:x:994:
[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
[WARN] 1.8  - Ensure auditing is configured for Docker files and directories -
docker.service
[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
[WARN] 1.11  - Ensure auditing is configured for Docker files and directories -
/etc/docker/daemon.json
[WARN] 1.12  - Ensure auditing is configured for Docker files and directories -
/usr/bin/docker-containerd
[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] 2.3  - Ensure Docker is allowed to make changes to iptables


[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
[PASS] 2.12  - Ensure centralized and remote logging is configured
[WARN] 2.13  - Ensure operations on legacy registry (v1) are Disabled
[WARN] 2.14  - Ensure live restore is Enabled
[WARN] 2.15  - Ensure Userland Proxy is Disabled
[INFO] 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
[PASS] 3.1  - Ensure that docker.service file ownership is set to root:root
[PASS] 3.2  - Ensure that docker.service file permissions are set to 644 or
more restrictive
[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
[PASS] 3.7  - Ensure that registry certificate file ownership is set to root:root
[PASS] 3.8  - Ensure that registry certificate file permissions are set to 444 or
more restrictive
[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
[PASS] 3.15  - Ensure that Docker socket file ownership is set to root:docker
[PASS] 3.16  - Ensure that Docker socket file permissions are set to 660 or
more restrictive
[PASS] 3.17  - Ensure that daemon.json file ownership is set to root:root
[PASS] 3.18  - Ensure that daemon.json file permissions are set to 644 or
more restrictive
[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: infallible_albattani
[WARN]      * Running as root: romantic_noether
[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.io/ubuntu:latest]
[WARN]      * No Healthcheck found: [docker.io/busybox:latest]
[WARN]      * No Healthcheck found: [docker.io/hello-world:latest]
[PASS] 4.7  - Ensure update instructions are not use alone in the Dockerfile
[NOTE] 4.8  - Ensure setuid and setgid permissions are removed in the images
unknown flag: --format
See 'docker history --help'.
unknown flag: --format
See 'docker history --help'.
unknown flag: --format
See 'docker history --help'.
unknown flag: --format
```

```
See 'docker history --help'.
[PASS] 4.9  - Ensure COPY is used instead of ADD in Dockerfile
[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: infallible_albattani
[WARN]      * No AppArmorProfile Found: romantic_noether
[WARN] 5.2  - Ensure SELinux security options are set, if applicable
[WARN]      * No SecurityOptions Found: infallible_albattani
[WARN]      * No SecurityOptions Found: romantic_noether
[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: infallible_albattani
[WARN]      * Container running without memory restrictions: romantic_noether
[WARN] 5.11  - Ensure CPU priority is set appropriately on the container
[WARN]      * Container running without CPU restrictions: infallible_albattani
[WARN]      * Container running without CPU restrictions: romantic_noether
[WARN] 5.12  - Ensure the container's root filesystem is mounted as read only
[WARN]      * Container running with root FS mounted R/W: infallible_albattani
[WARN]      * Container running with root FS mounted R/W: romantic_noether
[PASS] 5.13  - Ensure incoming container traffic is binded to a specific host interface
[WARN] 5.14  - Ensure 'on-failure' container restart policy is set to '5'
[WARN]      * MaximumRetryCount is not set to 5: infallible_albattani
[WARN]      * MaximumRetryCount is not set to 5: romantic_noether
[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: infallible_albattani
[INFO]      * Container no default ulimit override: romantic_noether
[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: infallible_albattani
[WARN]      * Privileges not restricted: romantic_noether
[WARN] 5.26  - Ensure container health is checked at runtime
[WARN]      * Health check not set: infallible_albattani
[WARN]      * Health check not set: romantic_noether
[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: infallible_albattani
[WARN]      * PIDs limit not set: romantic_noether
[INFO] 5.29  - Ensure Docker's default bridge docker0 is not used
[INFO]      * Container in docker0 network: romantic_noether
[INFO]      * Container in docker0 network: infallible_albattani
[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: 4 images
[INFO] 6.2  - Avoid container sprawl
[INFO]      * There are currently a total of 21 containers, with 2 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: 17
```