**A solid Plan in Implementing Anchore and Docker-Bench in The CI-CD pipeline**

1. Both Anchore and Docker-Bench can be put together in CI Pipeline.

A screenshot of a cell phone

Description automatically generated

**Looking at Our CI steps**

* Build- does create a image from Dockerfile stored in a remote repo.
* StartUp App -🡪 looks for latest version of compose files, update it and start up an application… [ docker-compose up policycenter ]
* Server Ping Test -🡪 A script that checks if the application is up or not.
* Store Image -🡪 Push the image to the nexus artifactory.
* Clean Up Docker Environment -> Cleans the unused images and containers…

**Whole Build stage depends on other 4 jobs here;**

* In general, the CI steps is taking around 50 mins to complete…..

**How is CI triggered?**

* Every time the developers push the new code in remote repository, a new build is triggered. Every new build has new build number and hence new images are created and pushed to the nexus artifactory.

**Advantages of Anchore in CI steps?**

* Anchore is an image scanning tool that helps us to scan the docker images and look for any vulnerabilities.
* It looks for common vulnerabilities present in OS or the package level of the image.
* Anchore has a built in plugin in the Jenkins which makes it more easier for us to imply it in CI build.
* With proper memory , anchore can scan images very fast. The heaviest image of our environment policycenter tooks less than 5 minutes to complete.
* With that we can have it as a step in CI once after the image is pushed to the nexus .

After the image is stored in nexus ------ > Anchore is triggered to scan the image

* Anchore pulls the image from the nexus
* Following command in execute shell will help us attain the image to scan.

TAG=$(date "+%H%M%S%d%m%Y")

IMAGENAME=nexus3.mmi.mig.corp:5000/migoraclejava7:80

echo "$IMAGENAME" > anchore\_images

* Anchore plugin allows us to select the configuration :

A screenshot of a cell phone

Description automatically generated

The configuration that we get are :

1. Fail or Pass the build if the image scanning is failed by anchore.

* If failed, email can be triggered to the default recipents so that they can be notified.

1. We can have anchore engine installed in the Jenkins server or have a different server just for anchore.

**Part 2 : Docker-Bench Security:**

Docker-bench security is a script created by a team of docker which scans the docker containers , host configurations and container at the runtime. Docker-bench is very helpful when it comes to securing the docker.

Where does docker-bench security fit in our environment?

:

**I have two general ideas when it comes to docker-bench security:**

1. We can keep it as a part of CI , run alongside the anchore engine. Because, docker-bench script won’t take more than 5 minutes to scan it. Anchore and Docker-bench are not dependent one another. So, these two jobs can be run parallel to one another.

Note: Current build time : approx.: 50 minutes

Add : 5 more minutes to it for docker security ?

* 55 mins : I belive it should be okay for us to add 5 more minutes to the build.   
  It is not taking huge time . ?

Docker-bench doesn’t require any thing to install ? It is simply a script which can be run by pulling docker-bench image. The image is 82.9 mb around . So, it is a small image and given our server power and memory, it will be very fast.

1. Have docker-bench run in test and pre-prod environments.

* How?

---🡪 Jenkins job integration : ssh into the server

---🡪 pull docker-bench image

--🡪 run the script from the image

A screenshot of a cell phone

Description automatically generated

**What is the configuration we can control with docker bench?**

* There are many scans docker-bench does when we run the script. Every check is not important for us. It doesn’t mean that every check is important to pass . Since there are more than 100+ checks and scans, we can select the scans we want to run.

sh docker-bench-security.sh -l /tmp/docker-bench-security.sh.log -c check\_2\_2

This command will only scan for check 2.2 . Similarly, we can select the scans we feel are important for our environment and configure it.