Establishing a Harbor Container Registry Integrated with Trivy for Comprehensive Vulnerability Assessment

In this tutorial, we'll walk you through setting up Harbor as your image registry and integrating it with Trivy for thorough vulnerability scanning. By following these steps, you'll enhance the security of your container images effectively.

**Prerequisites**

- Docker

- Docker Compose

1. **Install Harbor**

Installation Steps

1. **Download Harbor Installer**

Fetch the latest Harbor installer:

>> curl -s [https://api.github.com/repos/goharbor/harbor/releases/latest \](https://api.github.com/repos/goharbor/harbor/releases/latest%20\)

| grep browser\_download\_url \

| cut -d '"' -f 4 \

| grep '.tgz$' \

| xargs wget

1. **Extract and Configure Harbor**

Navigate to the Harbor directory:

>> cd harbor

Edit the `harbor.yml` configuration file to suit your environment. Update the hostname, port, and other settings as per your requirements.

**For HTTPS Configuration:**

If using HTTPS, install Certbot and obtain a certificate:

>> sudo apt install certbot -y

>> sudo certbot certonly --standalone -d "harbor.xyz.com" --preferred-challenges http --agree-tos -n -m "abc@xyz.com" --keep-until-expiring

Certificates will be located at `/etc/letsencrypt/live/harbor.xyz.com/`.

**For Self-Signed Certificate:**

If you're using a self-signed certificate, create it as follows:

>> mkdir -p certs

openssl req \

-newkey rsa:4096 -nodes -sha256 -keyout certs/harbor.key \

-addext "subjectAltName = DNS:harbor.xyz.com" \

-x509 -days 365 -out certs/harbor.crt

sudo cp certs/harbor.\* /etc/ssl/certs/

**Update the `harbor.yml.tmpl` configuration file:**

hostname: harbor.xyz.com

harbor\_admin\_password: your\_admin\_password

database:

password: your\_database\_password

https:

port: 443

certificate: /etc/ssl/certs/harbor.crt

private\_key: /etc/ssl/certs/harbor.key

Save this file as `harbor.yml`.

**3. Verify Configurations**

Check your configurations with:

cat harbor.yml

1. **Install Harbor**

Run the installation script with Trivy integration:

>> ./install.sh --with-trivy

Verify the installation by listing Docker images and containers:

>> docker image ls

>> docker container ls

1. **Test Harbor Web Access**

Access Harbor via your web browser:

>> https://harborxyz.local

Update your local hosts file to resolve `harborxyz.local` to your server IP:

>> Your\_Server\_IP harborxyz.local

**B. Integrate Trivy for Vulnerability Scanning**

**1. Push and Scan an Image**

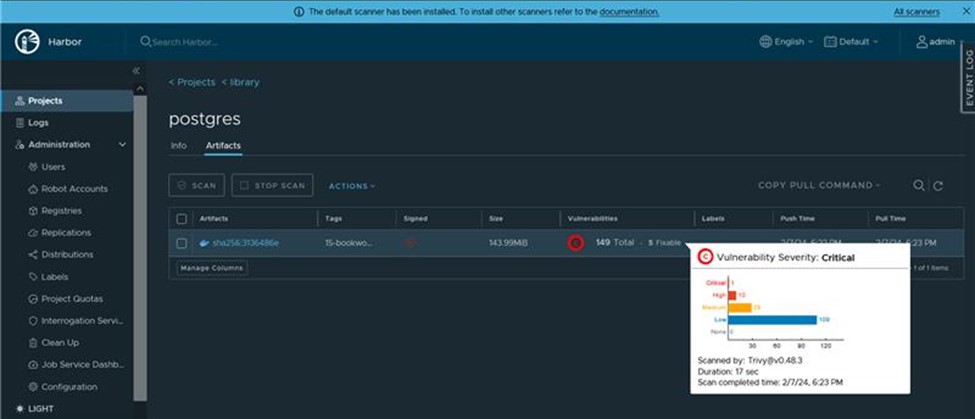
For testing, push an image to Harbor:

>> docker tag postgres:15-bookworm harborxyz.local/library/postgres:15-bookworm

>> docker push harborxyz.local/library/postgres:15-bookworm

**Scan the image with Trivy:**

trivy image harborxyz.local/library/postgres:15-bookworm



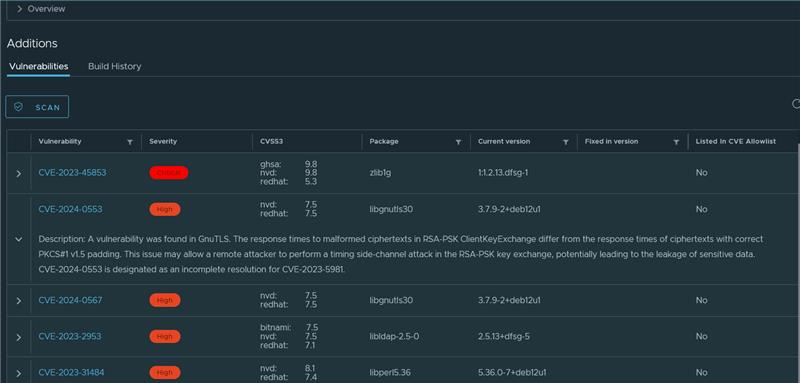
**Similarly, you can test with a `busybox` image:**

>> docker tag busybox:latest harborxyz.local/library/busybox:latest

>> docker push harborxyz.local/library/busybox:latest

**Scan the `busybox` image:**

>> trivy image harborxyz.local/library/busybox:latest



Also, we tried with a busybox image with the latest tag >> and checked for vulnerabilities >> It shows no vulnerabilities found