Grype Database Docker Image Build

This tool provides a simple way to build a custom Grype image containing only the CVE sources you wish to use.

Overview

For enterprise administrators it may be desirable to create a standardized vulnerability database to use as part of the SDLC. The files in this directory provide a sample for building a Grype database using a specific configuration and set of sources.

Note that as created this repository uses the official Grype and Grype-db binaries. It is possible to use a custom binary (for example, if you are using a custom Vunnel provider) by adjusting the Dockerfile to build/copy the custom binary into place.

Existing Documentation

Please see the CVE Scans with BuildX and Grype for more information, and a more detailed explanation of the Grype and GrypeDB tooling.

Important Notes

The speed at which a database can be generated using this process is heavily dependent on the speed that the various providers are able to be downloaded. In order to provide some insight into what is happening, the Dockerfile invokes the Grype build commands with the `-vv` flags; this can be changed if desired.

Usage

1. Update the Grype and GrypeDB configuration files as desired. The default is to only use the Alpine provider.
2. Build the image using `docker build -t <yourtag>:<yourversion> .`
3. Run the image normally `docker run -it --rm <yourtag>:<yourversion> <namespace>/<image>:<version>`

Example Output

Image Build

```
$ docker build  . -t grype

[+] Building 0.9s (18/18) FINISHED
docker:desktop-linux
 => [internal] load build definition from Dockerfile
0.0s
 => => transferring dockerfile: 964B
0.0s
 => [internal] load .dockerignore
0.0s
 => => transferring context: 2B
0.0s
 => [internal] load metadata for docker.io/library/debian:bullseye-slim
0.8s
 => [auth] library/debian:pull token for registry-1.docker.io
0.0s
```

```
 => [ 1/12] FROM docker.io/library/debian:bullseye-
slim@sha256:3bc5e94a0e8329c102203c3f5f26fd67835f0c81633dd6949de0557867a87fac
0.0s
 => => resolve docker.io/library/debian:bullseye-
slim@sha256:3bc5e94a0e8329c102203c3f5f26fd67835f0c81633dd6949de0557867a87fac
0.0s
 => [internal] load build context
0.0s
 => => transferring context: 141B
0.0s
 => CACHED [ 2/12] RUN apt-get update &&     apt-get install -y curl bash jq python3-pip &&     rm -rf
/var/lib/apt/lists/*
0.0s
 => CACHED [ 3/12] RUN curl -sSfL https://raw.githubusercontent.com/anchore/grype/main/install.sh | sh -s
-- -b /usr/local/bin
0.0s
 => CACHED [ 4/12] RUN curl -sSfL https://raw.githubusercontent.com/anchore/grype-db/main/install.sh | sh
-s -- -b /usr/local/bin
0.0s
 => CACHED [ 5/12] RUN pip install vunnel
0.0s
 => CACHED [ 6/12] RUN mkdir -p ./grype/db
0.0s
 => CACHED [ 7/12] COPY .grype.yaml /root/
0.0s
 => CACHED [ 8/12] COPY .grype-db.yaml /root/
0.0s
 => CACHED [ 9/12] WORKDIR /root
0.0s
 => CACHED [10/12] RUN grype-db -vv -g -p alpine
0.0s
 => CACHED [11/12] RUN grype-db -vv -g -p alpine build
0.0s
 => CACHED [12/12] RUN grype db import ./build/*.tar.gz
0.0s
 => exporting to image
0.0s
 => => exporting layers
0.0s
 => => exporting manifest sha256:a7f951869c9843037c93cf2e74b2c90173de0cf348f0dbbba4d19752fda40ca8
0.0s
 => => exporting config sha256:bbd6b09d8961d1676c9ba29f0a45b6266b6b6b75611629188c25d0ea5f3696b9
0.0s
 => => exporting attestation manifest
sha256:8f51a468294e020644a8bd727a41aa7c5685d5e9665c3881e5935c4997c56086
0.0s
 => => exporting manifest list sha256:85226fb4790fac468857e300fa9f30fb6a07246ce04632c67e3410018c166898
0.0s
 => => naming to docker.io/library/grype:latest
0.0s
 => => unpacking to docker.io/library/grype:latest
0.0s

View build details: docker-desktop://dashboard/build/desktop-linux/desktop-
linux/oj6ktivq757b4kqcrhcp6ypyy

What's Next?
  View a summary of image vulnerabilities and recommendations → docker scout quickview
```

Sample Run

```
$ docker run -it --rm  grype "felipecruz/alpine-tar-zstd"
 ✔ Vulnerability DB                [no update available]
 ✔ Scanned for vulnerabilities     [19 vulnerability matches]
   ├── by severity: 0 critical, 0 high, 0 medium, 0 low, 0 negligible (19 unknown)
   └── by status:   19 fixed, 0 not-fixed, 0 ignored
NAME          INSTALLED  FIXED-IN   TYPE  VULNERABILITY   SEVERITY
libcrypto1.1  1.1.1q-r0  1.1.1v-r0  apk   CVE-2023-3817   Unknown
libcrypto1.1  1.1.1q-r0  1.1.1u-r2  apk   CVE-2023-3446   Unknown
libcrypto1.1  1.1.1q-r0  1.1.1u-r0  apk   CVE-2023-2650   Unknown
libcrypto1.1  1.1.1q-r0  1.1.1t-r2  apk   CVE-2023-0465   Unknown
libcrypto1.1  1.1.1q-r0  1.1.1t-r1  apk   CVE-2023-0464   Unknown
libcrypto1.1  1.1.1q-r0  1.1.1t-r0  apk   CVE-2023-0286   Unknown
libcrypto1.1  1.1.1q-r0  1.1.1t-r0  apk   CVE-2023-0215   Unknown
libcrypto1.1  1.1.1q-r0  1.1.1t-r0  apk   CVE-2022-4450   Unknown
libcrypto1.1  1.1.1q-r0  1.1.1t-r0  apk   CVE-2022-4304   Unknown
libssl1.1     1.1.1q-r0  1.1.1v-r0  apk   CVE-2023-3817   Unknown
libssl1.1     1.1.1q-r0  1.1.1u-r2  apk   CVE-2023-3446   Unknown
libssl1.1     1.1.1q-r0  1.1.1u-r0  apk   CVE-2023-2650   Unknown
libssl1.1     1.1.1q-r0  1.1.1t-r2  apk   CVE-2023-0465   Unknown
libssl1.1     1.1.1q-r0  1.1.1t-r1  apk   CVE-2023-0464   Unknown
libssl1.1     1.1.1q-r0  1.1.1t-r0  apk   CVE-2023-0286   Unknown
libssl1.1     1.1.1q-r0  1.1.1t-r0  apk   CVE-2023-0215   Unknown
libssl1.1     1.1.1q-r0  1.1.1t-r0  apk   CVE-2022-4450   Unknown
libssl1.1     1.1.1q-r0  1.1.1t-r0  apk   CVE-2022-4304   Unknown
tar           1.34-r0    1.34-r1    apk   CVE-2022-48303  Unknown
```

SOFTWARE DISCLAIMER

This software is provided as a "Proof of Concept" (PoC) and is not intended for production use.

NO WARRANTIES: The author expressly disclaims any warranty for this software. The software and any related documentation is provided "as is" without warranty of any kind, either express or implied, including, without limitation, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement. The entire risk arising out of use or performance of the software remains with the user.

NO LIABILITY FOR DAMAGES: In no event shall the author be liable for any damages whatsoever (including, without limitation, damages for loss of business profits, business interruption, loss of business information, or any other pecuniary loss) arising out of the use or inability to use this product, even if the author has been advised of the possibility of such damages.

USE AT YOUR OWN RISK: This software is intended for educational or demonstration purposes only. Users are strongly cautioned against using it in production or mission-critical environments. If you choose to use the software, it is at your own discretion and responsibility to ensure that it does not cause any harm or issues to your systems or data.

MODIFICATIONS: Users are free to modify the software for their own use, but redistribution should include this disclaimer.

Always take a backup of your data and test any software in a controlled environment before any widespread use.

Citations and Helpful Information

- Grype

- Grype-db
- Vunnel
- CVE Scans with BuildX and Grype