Docker Best Practice

**TABLE OF CONTENTS**

[Best Practices 1](#_Toc1720439405)

[Naming 1](#_Toc563187559)

[General conventions 1](#_Toc1140858885)

[Service Users 1](#_Toc218798029)

[Resource and data source arguments 1](#_Toc896516024)

[Variables 2](#_Toc8454459)

[Outputs 2](#_Toc852868051)

[Resources: 2](#_Toc9478135)

# Best Security Practice

* NEVER run EXEC or ENTRYPOINT commands as root  
  hint : <https://medium.com/@mccode/processes-in-containers-should-not-run-as-root-2feae3f0df3b>
* SHOULD delete caches for npm/pip/apt-get to reduce image size
* NEVER have move than 2 entrypoints
* NEVER embed secrets into directly an the image, mount secrets from volumes or secret services
* use small base images from official sources
* ALWAYS scan your image using trivy or similar SAST tool to check for known vulnerabilities
* ALWAYS define a USER with limited access to docker image, else most base images default to ROOT  
  <https://en.wikipedia.org/wiki/Principle_of_least_privilege>

# Best DockerfilePractice

<https://docs.docker.com/develop/develop-images/dockerfile_best-practices/>

# Further Reading

## Official Getting Started

* <https://docs.docker.com/get-started/>

## Snyk top 10

* <https://snyk.io/blog/10-best-practices-to-containerize-nodejs-web-applications-with-docker/>