Crafting Killer Containers By Following Best Practices

By Akshay Ithape - DevOps Engineer

$whoami

Akshay Ithape, CKA/AD,AWS(2x),RedHat(2x),Terraform,Azure

DevOps Engineer @ Eastern Enterprise , Pune
empowering your software

Passionate About & DEVOPS

Writer @ OpenSource For U .com
The complete portal on open source

I truly believes in Open Source so I like to share my knowledge with community in as many ways possible and helping people.

akshayithape

https://www.akshayithape.in/

akshayithape-devops

Session Agenda

- Overview about dockerfile best practices
- Multi-stage dockerfile
- Buildx & Buildkit
- Vulnerabilities Scanner - Trivy

Overview About Dockerfile Best Practices

- Choose Official or Verified Base Image
- Prefer Minimal Base Images
- Use Tags for Immutability
- Use Labels for Metadata
- Use COPY instead of ADD
- Use Multi-Stage Builds for Small Secure Images
- Use a Static Code Analysis
- Verify and Sign Images to Mitigate MITM Attacks

Overview About Dockerfile Best Practices

- Scan Images for Vulnerabilities
- Create Multi-Arch Supported Images
- Use BuildKit with Docker Build
- Limit the Number of Layers
- Remove Unnecessary Files

Multi-Stage Dockerfile

- Smaller Image Sizes
- Improved Security
- Faster Build Times

```
# Build Stage
FROM golang:1.16 AS build
WORKDIR /app
COPY go.mod go.sum ./
RUN go mod download
COPY . .
RUN CGO_ENABLED=0 GOOS=linux go build -a -installsuffix cgo -o app .

# Production Stage
FROM alpine:latest AS production
RUN apk --no-cache add ca-certificates
WORKDIR /root/
COPY --from=build /app/app .
CMD ["./app"]
```

Multi-Stage Dockerfile Demo

Buildkit

- BuildKit is a modern and efficient tool for building Docker images, developed by Docker Inc. It is designed to improve the build process by providing faster and more secure builds, as well as more flexibility and control over the build process.
- BuildKit is a backend for the Docker Build command.
- BuildKit is now integrated into the Docker Build command and is enabled by default in Docker versions 18.09 and later.
- Key features of BuildKit :
    - Parallel Builds
    - Efficient Caching
    - Secure Build Process
    - Multi-Platform Support

Buildx

- Buildx is a Docker CLI plugin that extends the functionality of Docker build to support multiple platforms and build contexts. It is designed to make it easier to build, test, and deploy Docker images for multiple architectures and platforms.
- Buildx supports a variety of advanced features, such as multi-platform builds, build caching, and buildkit-based builds. These features can help you optimize your build process and reduce build times.
- Buildx is still in experimental mode and is not yet fully supported by all Docker versions

Buildx Demo

Vulnerabilities Scanner - Trivy

- Trivy is a popular open-source vulnerability scanner for containers and other artifacts.
- Trivy supports scanning for vulnerabilities in a variety of package managers.
- Trivy's vulnerability database is regularly updated to include the latest CVEs and security advisories.
- One of the benefits of Trivy is that it's easy to use and can be integrated into various tools and workflows.

Trivy Demo

Thank You EveryOne

Be In Touch

Linkedin : https://www.linkedin.com/in/akshayithape/

GitHub : https://github.com/akshayithape-devops

Website : https://www.akshayithape.in/

Youtube : https://www.youtube.com/@akshayithape-devops

Subscribe Now @akshayithape-devops on YouTube