Monday, 3 February 2025

Docker image validation

Docker images are validated in different ways to ensure **integrity, authenticity, and security** before being used.

🔷 1. Checksum Validation (Image Integrity)

✅ When pulling an image, Docker validates its **checksum (SHA256 digest)** to ensure the image hasn't been corrupted.

🔍 **Check an image's digest:**

```
docker pull ubuntu
docker images --digests
```

✅ The output will show the **SHA256 digest**, which uniquely identifies the image.

🔍 **Manually verify the image hash:**

```
docker inspect --format='{{.RepoDigests}}' ubuntu
```

✅ If the digest doesn't match, the image may be **tampered with or incomplete**.

🔷 2. Content Trust (Image Authenticity) – Docker Notary

✅ Docker **Content Trust (DCT)** ensures that images are signed and verified before pulling.

🔍 **Enable DCT before pulling images:**

```
export DOCKER_CONTENT_TRUST=1
docker pull myregistry.com/myimage:latest
```

✅ If the image is not **signed by a trusted source**, Docker will reject it.

🔷 3. Image Signature Verification (Secure Supply Chain)

🔷 **Docker Notary & Cosign** allow image publishers to sign images and users to verify them.

🔍 **Verify a signed image using Cosign (Sigstore):**

```
cosign verify myimage:latest
```

✅ Ensures the image was **not modified** after signing.

🔷 4. Security Scanning (Vulnerability Check)

✅ Docker Hub & private registries provide **built-in security scanning** to check images for vulnerabilities.

🔍 **Scan an image for security issues using Trivy:**

```
trivy image ubuntu
```

✅ Detects **CVEs** (security vulnerabilities) in installed packages.

🔷 5. Image Provenance (SBOM - Software Bill of Materials)

✅ **Tools like Syft** generate an **SBOM** to track components inside an image.

🔍 **Generate an SBOM for an image:**

syft ubuntu:latest

✅ Helps **audit dependencies** to prevent security risks.

🔷 6. Manual Inspection (Dockerfile & History Check)

✅ Check how an image was built **before using it**.

🔍 **View the full history of an image:**

docker history ubuntu

✅ If you see suspicious layers or curl downloads from unknown sources, **do not use the image**.

🔷 Summary

Validation Method	Purpose
🔷 **Checksum Digest (`SHA256`)**	Ensures image integrity after pulling.
🔷 **Docker Content Trust (DCT)**	Prevents pulling unsigned images.
🔷 **Signature Verification (Cosign/ Notary)**	Confirms the image source is trusted.
🔷 **Security Scanning (Trivy, Clair)**	Detects vulnerabilities in the image.
🔷 **SBOM Analysis (Syft, Grype)**	Tracks dependencies inside the image.
🔷 **History Check (`docker history`)**	Reviews build steps for security risks.

Would you like an example of **signing your own images** for extra security? 🚀