Vessel: Reproducible Container Builds

IS YOUR ORGANIZATION WORKING TO IMPLEMENT ZERO-TRUST INITIATIVES? Are you trying to find a way to ensure that you can trust the software supply chain and that the software you build is free from malicious tampering?

Build reproducibility—a method of compiling software that ensures it can be exactly reproduced by any party—is an essential method that can provide guarantees that software builds are safe. Reproducible builds ensure that software comes from trusted source code and that no malicious code was inserted into it during the build process.

However, most software builds today are not reproducible, often because of factors like changes in build environments involving timestamps or external dependencies. Builds that aren't reproducible are less trustworthy, and they can lead to other problems as well, such as generating software with differing behavior and even builds that fail.

Because there were no solutions on the market that fully addressed reproducibility, the SEI created the Vessel tool to detect and correct reproducibility issues in container builds.

Vessel: Ensuring Trustworthiness and Reliable Deployment

As the Department of Defense (DoD) increasingly uses containers to support its DevSecOps processes and deploy its software, it must consider the security and reliability implications of using containers. Container builds often suffer from lack of reproducibility, which can result in a lack of trust, changes in software behavior, or build failures. To ensure that the DoD can deploy mission capabilities securely and reliably, the SEI's Vessel tool advances the state of the art in container reproducibility to achieve the following goals:

- **Detect reproducibility failures.** Vessel is a tool that detects reproducibility failures (i.e., when two images are built from the same Dockerfile but are not identical).
- **Identify container build reproducibility issues.** There are several tools on the market that can identify some reproducibility issues, but they lack a holistic view of container reproducibility. Vessel checks for issues others can't, such as detecting reliance on external volatile sources and nondeterminism from timestamps; it then categorizes issues based on its reproducibility model.
- **Repair reproducibility issues in software builds.** Vessel automates repair of reproducibility issues. When automated repair isn't possible, Vessel provides detailed and actionable guidance for developers to repair any issues that remain.
- **Enhance reproducibility of open source and DoD software pipelines.** By releasing Vessel, the SEI aims to raise awareness among organizations about container reproducibility and to provide them with the tools to add reproducibility to their own container build pipelines.

Figure 1 shows how Vessel fits into a container build pipeline to ensure reproducible builds.

Get Started Today

By adopting the Vessel tool, you can improve your software processes and zero-trust initiatives and achieve the following goals:

- assess the reproducibility of your current containers
- increase the reproducibility of your container builds
- secure your CI pipelines against malicious tampering

The SEI can help you improve the trust and reliability of your build processes by instantiating Vessel in your organizations and integrating it into your container build pipelines.

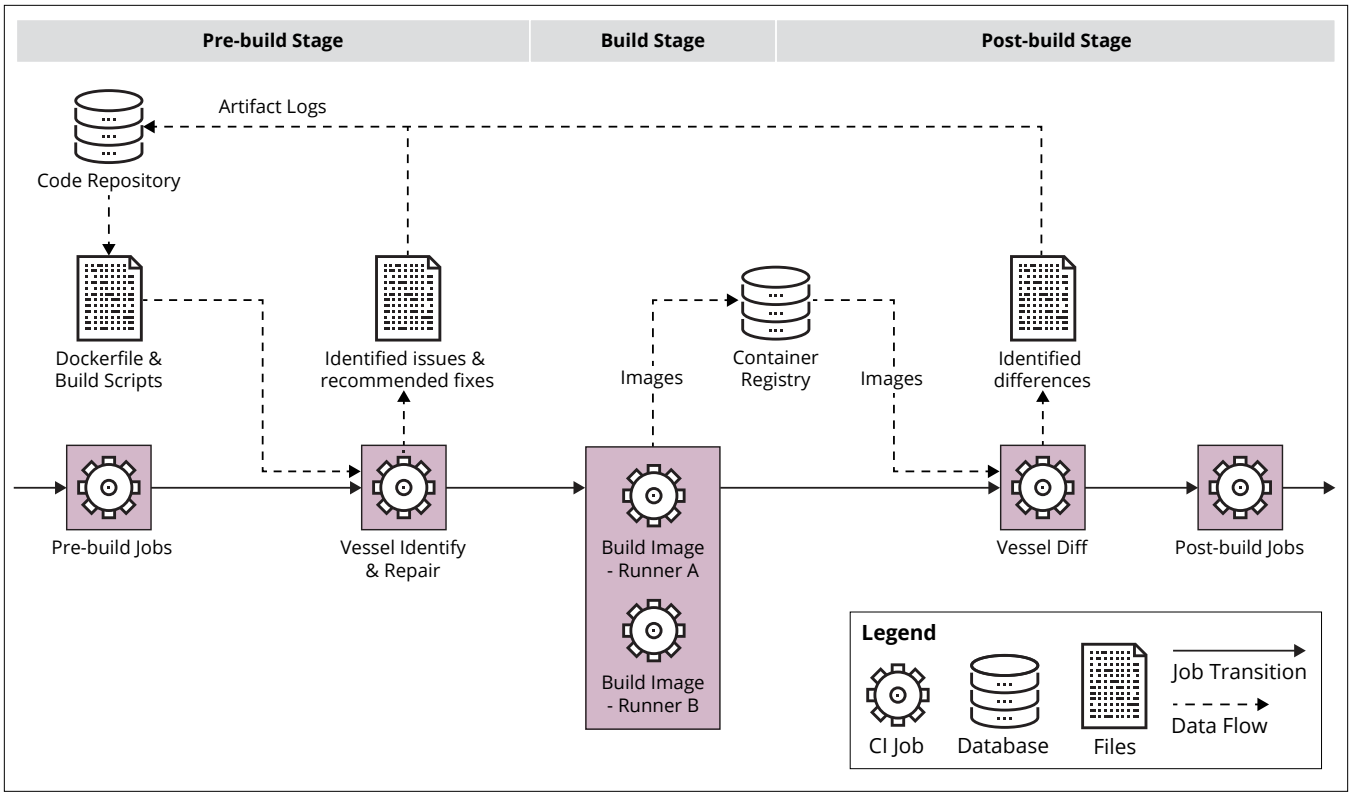

Figure 1: Vessel Workflow

About the SEI

Always focused on the future, the Software Engineering Institute (SEI) advances software as a strategic advantage for national security. We lead research and direct transition of software engineering, cybersecurity, and artificial intelligence technologies at the intersection of academia, industry, and government. We serve the nation as a federally funded research and development center (FFRDC) sponsored by the U.S. Department of Defense (DoD) and are based at Carnegie Mellon University, a global research university annually rated among the best for its programs in computer science and engineering.

Contact Us

CARNEGIE MELLON UNIVERSITY
SOFTWARE ENGINEERING INSTITUTE
4500 FIFTH AVENUE; PITTSBURGH, PA 15213-2612

sei.cmu.edu
412.268.5800 | 888.201.4479
info@sei.cmu.edu