10.6 Deployment Artifact to Evidence

Go to Top

A Deployment Artifact traces to Evidence when recorded information supports a claim about the deployed system.

Evidence may support claims about deployment, execution, configuration, communication, health, recovery, policy enforcement, release, audit, provenance, or test results.

For example, a Kubernetes Deployment may trace to Evidence showing that a Node started, reported health, subscribed to the expected Communication Endpoint, published a status message, and produced an audit record. A ConfigMap may trace to Evidence showing which QoS profile, topic definition, or runtime configuration was active during a test.

Examples include:

Table 10.6-1: Examples of deployment artifacts traced to evidence

Deployment Artifact	**Evidence**
Kubernetes Deployment or Pod	Startup logs, status records, health reports, and captured heartbeat messages
ConfigMap or mounted configuration file	Configuration snapshot, checksum, version record, review record
Deployed Node	Node status message, audit record, provenance record, captured output
Runtime topic or endpoint configuration	Captured publication, subscription record, topic discovery output, test result
Policy release service deployment	Release decision record, redaction output, audit entry, policy-version record
Test scenario execution	Test report, captured messages, logs, screenshots, evidence bundle