

14.7 Container Logs

[Go To Top](#)

[Return to Containerisation](#)

Containers should expose logs in a way that supports troubleshooting, review, and acceptance [Evidence](#). Logs should not remain trapped inside transient containers that disappear when the runtime stops.

The team should define how each container produces and exposes logs. Container logs may appear through:

1. Standard output.
2. Standard error.
3. Mounted log directories.
4. Runtime log files.
5. Container runtime logging commands.
6. Evidence export scripts.

Container logs should include enough context to identify the Node or service, [Lifecycle](#) state changes, [Configuration](#) source, [DDS](#) participation, command handling, publication or subscription events where relevant, warnings, errors, and shutdown results.

Containers should not log secrets, credentials, private keys, tokens, or sensitive local values. If runtime Configuration includes sensitive values, the Node or container entry point should mask them in logs.

Acceptance Evidence may include container logs, Node logs, [Control Plane](#) status captures, script output, and test results. The team should store Evidence in the approved Evidence location rather than relying only on live terminal output.

© 2026 Dido Solutions, Inc. and Jackrabbit Consulting, Inc.

From:

<https://wiki.didosolutions.com/> - **Dido Solutions, Inc Wiki**

Permanent link:

<https://wiki.didosolutions.com/fxdemo/05-part/14-containerisation/14-7-container-logs/start>

Last update: **2026/08/10 15:34**

