FDA Validation

FDA (21 CFR Part 11) Validation

Permalink to this page: https://cwiki.apache.org/confluence/x/BSolBg

Preface

This page discusses using Tomcat in an FDA validated environment, i.e. one where 21 CFR Part 11 regulations apply.

Please note that although this page mentions specific companies, we do not explicitly endorse or sell anyone's services. Tomcat and Apache are not-for-profit organizations. This page is also far from a complete listing of vendors and support options. It is meant as a demonstration showing that these options do exist and that running Tomcat in a validated environment is both feasible and reasonable.

Questions

Answers

Can Tomcat be used in a validated environment?

Yes. There's nothing in Tomcat's design or implementation that prevent it from being used in a validated environment. The same validation procedures and guidelines that apply to most software packages apply to Tomcat as well. Being an open-source application does not preclude Tomcat validation. In fact, it helps in at least one key aspect: the source code itself can be audited, as can the commit and change logs for the software.

Has anyone actually done it?

Yes. As shown in this user mailing list archive, Merck and other large companies are using Tomcat in a validated environment. In addition, there is at least one application provider (Interchange Digital) whose application runs on Tomcat that has deployed said package in numerous pharma data centers.

Is Tomcat itself validated?

Yes. Tomcat itself is validated to the extent it can be. Tomcat implements several Java EE Specifications, most important of them are the Servlet Specification and the Java Server Pages (JSP) Specification. Each of these specifications has a Technology Compatibility Kit (TCK), which is a collection of tests to certify a given product meets the Specification fully and accurately.

The Apache Software Foundation is licensed to run these TCKs. They are run against every major Tomcat release. **No Tomcat release is pronounced stable unless it has passed both of these TCKs with 100% compliance**. Therefore, every stable Tomcat release is validated to the extent of Tomcat's core functionality.

Furthermore, any company of individual may apply to obtains and use these TCKs themselves. That way, you can re-validated Tomcat including any custom patches you have implemented.

However, we cannot validate your application's use of Tomcat. You're on your own there.

What kind of support is there around validating Tomcat?

Several kinds. They include:

- There are numerous smaller vendors and several large ones, including IBM, HP, Sun, and Novell, who offer Tomcat consulting and support services, including application auditing, environment assessments, and risk analysis.
- There are numerous vendors in addition to the above consultants, like SpringSource (formerly Covalent) and JBoss, who offer 24/7/365 enterprise-level support for Tomcat.
- The Tomcat mailing lists are extremely active and contain members of many of the above organizations, including contractors available for hire.

How do I know I have a validated release? How do I know no one has tampered with the release package?

All Tomcat releases are signed using the Release Manager's PGP key. The key is also available in the KEYS file that ships with every Tomcat release. The same KEYS file is also available in the Tomcat Git repository (here). The PGP signatures are available on all the Tomcat download pages, and can (and should!) be used to verify the release really is the signed distribution.

As for tampering: every Tomcat release is also digested using the SHA-512 algorithm as specified in RFC6234. The SHA-512 digest is included in all the download pages. Users run `sha512sum` on their local machine to verify that the digest of what they downloaded is the same as that published in the Apache download pages. That way, users are assured the distribution has not been modified since the Release Manager signed it.

What about security? I'm concerned about attacks.

There's no need to be. See the security page of this FAQ for more information.