Maintaining Supported Software

Recommended Practice

- Appropriate staff monitor "security" and/or "announce" mailing lists for critical software.
- Software versions are reasonably current and upgraded ahead of "End of Life" dates.

Federation software relies on an extensive technology stack. As with all web-based software, vulnerabilities can be introduced in many places, and a security flaw on one site can lead to the exposure of another. This is particularly true when web authentication software is involved.

In addition, as a still-evolving and expanding technology, federation is not yet an area for "install and forget" technology management. New use cases and new best practices continue to emerge, and federation software, if viable, will continue to evolve to address these new requirements.

Carefully consider strategies for maintaining currency in your:

- Operating Systems
- Web Servers
- Java or other Application Servers (if applicable)
- Federation Software

Avoid big-bang upgrades crossing multiple significant versions. Ensure staff are monitoring the appropriate mailing lists to stay abreast of security issues and patches. In general, treat your environment the way you would treat any mission-critical system.