26/06/2024

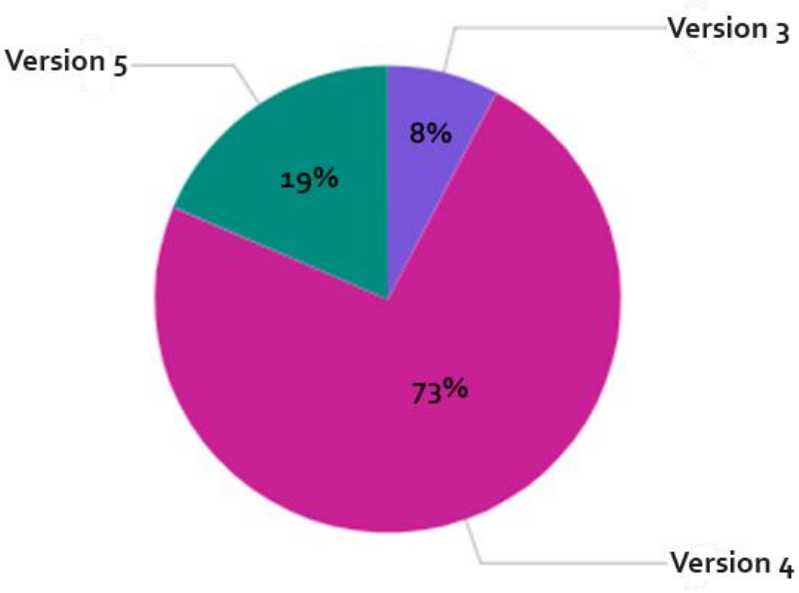
Shibboleth Version 5 Upgrade

Matt Huckson, UK Federation support team

Overview

- over 65% of IdPs in the federation use the Shibboleth Identity Provider
- IdP v5 – Released September 2023.
- IdP v4 – EOL September 2024
- IdP v3 – EOL December 2020

Breakdown of versions @ 12 June 2024

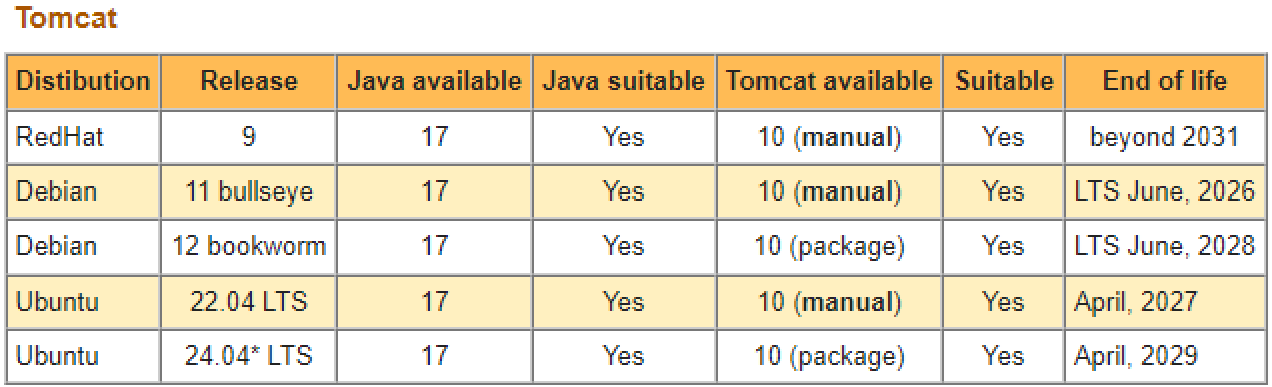


IdPv5 upgrade considerations #1

- Shibboleth IdP is a Java web app, and needs a Java Web Servlet Container.
- Two Java Servlet containers commonly used Tomcat and Jetty
- Tomcat supported in Debian12 bookworm & Ubuntu 24.04 (noble Numbat)
- Jetty manual update
- To run IdPv5 You will need Java 17 (or later) and either Tomcat 10.1 (or later) or Jetty 11 (or later)
- Deployers on a Windows platform use an installer.

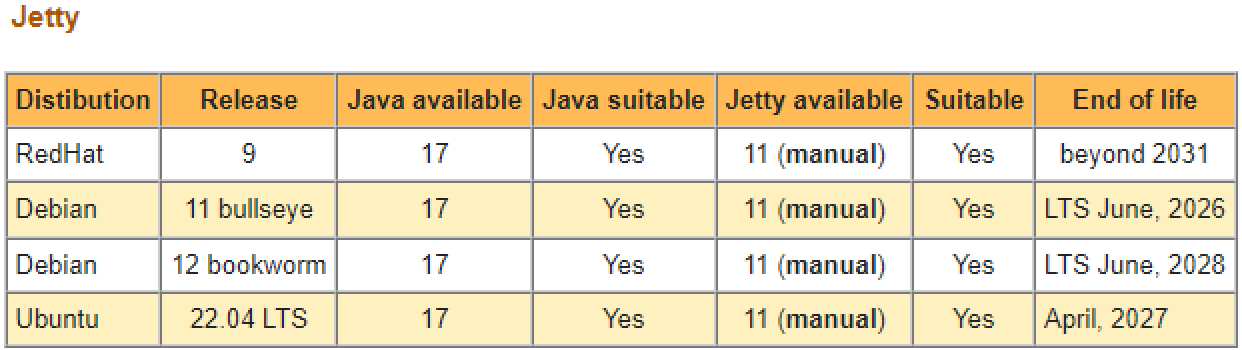
IdPv5 upgrade considerations #1

- Shibb… Web Servle…
- Two Ja… at and Jetty
- Tomcat su…
- Jetty mar…
- To run … ner Tomca…
- Deplo…



Tomcat

Distibution	Release	Java available	Java suitable	Tomcat available	Suitable	End of life
RedHat	9	17	Yes	10 (manual)	Yes	beyond 2031
Debian	11 bullseye	17	Yes	10 (manual)	Yes	LTS June, 2026
Debian	12 bookworm	17	Yes	10 (package)	Yes	LTS June, 2028
Ubuntu	22.04 LTS	17	Yes	10 (manual)	Yes	April, 2027
Ubuntu	24.04* LTS	17	Yes	10 (package)	Yes	April, 2029



Jetty

Distibution	Release	Java available	Java suitable	Jetty available	Suitable	End of life
RedHat	9	17	Yes	11 (manual)	Yes	beyond 2031
Debian	11 bullseye	17	Yes	11 (manual)	Yes	LTS June, 2026
Debian	12 bookworm	17	Yes	11 (manual)	Yes	LTS June, 2028
Ubuntu	22.04 LTS	17	Yes	11 (manual)	Yes	April, 2027

IdPv5 upgrade considerations #1

- Shibboleth IdP is a Java web app, and needs a Java Web Servlet Container.
- Two Java Servlet containers commonly used Tomcat and Jetty
- Tomcat supported in Debian12 bookworm & Ubuntu 24.04 (noble Numbat)
- Jetty manual update
- To run IdPv5 You will need Java 17 (or later) and either Tomcat 10.1 (or later) or Jetty 11 (or later)
- Deployers on a Windows platform use an installer.

IdPv5 upgrade considerations #2

- Jetty v11 end of Community Service 01 Jan 2025
- Jetty v12 not available in any supported Linux distributions. Shibboleth project have released a "jetty-base" for Jetty 12 is now recommend by Shibboleth project.
  - Backchannel support (SAML1), is not supported
- Have a good recovery plan in place.
- Staging environment.

Tips #1 - Read the guides

- Shibboleth IdP v5 upgrade guide
  - Recently updated feedback appreciated to service@ukfederation.org.uk
- Shibboleth Wiki IdP v5
- Jetty 12

Tips #2 - XML editing and linting

- Install a decent editor tool with knowledge of XML.
  - Notepad++ has an XML
  - Visual Studio Code (vscode)
  - (or use vim)
- Remember to lint your XML
  - xmllint
  - xml_pp
  - A web browser

Tips #3 - Use git

- Use git to manage your Shibboleth IdP folder git add and git commit regularly, on each change or update
- That location is commonly referred to as %{idp.home}
  - C:\Program Files (x86)\Shibboleth\IdP Windows
  - /opt/shibboleth-idp on Linux
- git is available for both Windows and Linux
- You'll need a decent .gitignore file, so you commit the right data avoid credentials folder, which should be elsewhere e.g. a password manager
- avoid logs, old-*
- You should have an upstream/copy of the git repo Gitlab, Github, Gitolite etc...
- git clone --bare on another host via SSH, create a blah.git folder

Tips #4 - Reloadable services

- Read and book mark - Reloadable services
- Common ones are
  - shibboleth.AttributeResolverService
  - shibboleth.AttributeRegistryService
  - shibboleth.AttributeFilterService
  - shibboleth.MetadataResolverService
- Remember logs can also be reloaded
  - If you were going from INFO to DEBUG (and back?)
  - shibboleth.LoggingService
- Reload services *without* breaking the IdP, whereas a full restart could be service affecting.

Tips #5 - loglevels & Log files

- Setting in %{idp.home}/conf/idp.properties and using the Reload described on the last slide.

idp.loglevel.idp=DEBUG

idp.loglevel.messages=DEBUG

idp.loglevel.encryption=DEBUG

- idp-process.log
  - First line of start-up… INFO [net.shibboleth.idp.log.LogbackLoggingService:245] - Shibboleth IdP Version 5.1.2
  - Last line of start-up INFO [net.shibboleth.idp.authn.impl.RemoteUserAuthServlet:214] - RemoteUserAuthServlet will process REMOTE_USER, along with attributes [] and headers []
  - You may need it DEBUG quite a lot if you are working with non-federation SPs or SAML proxying…
  - Investigate ERROR and WARN messages in your logs.
- idp-audit.log - For logging of user activity and attributes sent
  - Looking for SAML1 references

Tips #6 - Version of IdP

Web brower on IdP:

```
http[s]://localhost/status
```

The same thing on the command line would be:

```
$ /opt/shibboleth-idp/bin/status.sh
```

For more details (and programmatically useful) data the Metrics administrative flow should be used.

Thank you

- Getting in touch
  - service@ukfederation.org.uk

- The UK federation technical support team provides support for deployment of SAML-capable software within the UK federation. We cannot provide in-depth support for web applications which rely on that SAML software.

- The UK federation also provides in-depth technical support for Shibboleth software within the UK federation, which includes support for installation, configuration and troubleshooting.

- We recommend that you always use a supported release of your chosen software. We reserve the right not to support software designated end of life (EOL) by its authors and in such cases will only provide assistance in upgrading to a supported version.