Tomcat 7

Mark Thomas

November 2009

Content

- Servlet 3.0 / JSP 2.2
- Manager application security
- Alias support
- Embedded improvements
- Valves & Filters
- Logging
- Miscellaneous
- Other plans

Servlet 3.0

- Specification isn't final yet
- Based on latest draft from expert group (not the latest public draft)
- Things are going to change
  - So complete == complete (for now)

Servlet 3.0

- API
  - Complete
- Asynchronous processing
  - Work in progress
  - Filip is up next
  - He will give you all the details

Servlet 3.0

- Web fragments
  - Work in progress
- Annotations
  - Will follow after web fragments
- Dynamic configuration
  - Complete
- Session tracking
  - Complete

Servlet 3.0

- Programmatic login
  - To do
- Servlet Container Profile of The Java Authentication SPI for Containers
  - To do (JSR 196 - optional)
- File upload
  - To do (Commons File Upload)

JSP 2.2

- Java EE 6
  - Servlet 3.0
  - JSP 2.2
- No sign of a JSR for JSP 2.2
- There is JSR 245 MR2 (JSP 2.1)
  - Will this become JSP 2.2?

Manager App Security

- The Manager lets you deploy apps
- Have been attacks via the Manager
- Single role for access control
  - Can add new roles and/or per command constraints
- Cross Site Request Forgery
  - Risky user behaviour can enable successful attacks

Manager App Security

- Move text interface
  - From /manager to /manager/text
- Add new roles
  - manager (HTML GUI)
  - manager-scripts (Ant, other tools)
  - manager-jmx (JMX proxy)
  - manager-status (just the status page)
- Can still add per command constraints

Manager App Security

- Use POST for non-idempotent commands
- Any POST request requires a nonce
  - Stored in the session
  - Changes on every request
  - Hidden form parameter or added to URL

Alias Support

- New <Context ... /> attribute
- aliases
  - "/aliasPath1=docBase1, /aliasPath2=docBase2“
- docBaseN can be WAR or dir
  - Must be absolute paths
- Contents NOT deleted on un-deploy

Embedded Improvements

- Based on work by Costin
- org.apache.catalina.startup.Tomcat
  - Easy to embed
  - Basis for a number of new unit tests
- Can be ‘bare bones’ or usual defaults
- Easy to configure programmatically
- Optionally, can access internals

EMBEDDED DEMONSTRATION

Valves & Filters

- GSOC 2009 project
- Replace Valves with Filters
  - I'd like to remove Valves entirely
  - Might not be possible
- Made progress
  - Some Valves replaced
  - Some Valves have equivalent Filters
  - Some Valves not addressed

Valves & Filters

- Ordering can be important
  - Valves always processed before Filters
- Engine level valves have a single instance
- Global filters (conf/web.xml) have an instance per web application

Logging

- AsyncFileHandler
  - Log events placed in a queue
  - Separate thread writes them to disk
- OneLineFormatter
  - One line per log event rather than two
- VerbatimFormatter
  - Just the message, no stack traces, no other elements

Miscellaneaous

- Use Generics throughout
- Reduce connector code duplication

Other Plans

- JMX: Align MBeans with code
  - Add missing attributes & methods
  - Remove obsolete attributes & methods
  - Correct mark attributes as read/write or read-only
- Session fixation protection
  - Change session ID on authentication

Other Plans

- More clean-up
  - Remove old code
  - Replace StringBuffer with StringBuilder
  - Loggers and StringManagers to be static final where possible

Other Plans

- Reduce configuration by system property
- Break up STRICT_SERVLET_COMPLIANCE
- Additional options for Cookie handling
  - Some for stricter compliance
  - Some for less strict compliance

QUESTIONS