New !

New and upcoming features in Apache Tomcat ™

Rémy Maucherat

Software engineer at Red Hat

Working on Red Hat JBoss Web Server

Apache Tomcat committer since 2000

ASF member

Contents

SSL configuration

OpenSSL

NIO 2

HTTP/2

Reactive IO

Cloud clustering

Others

SSL configuration updates

SSL configuration overhaul

SNI support with per host configuration

Multiple certificates

Configuration beautifying

Better handling of both OpenSSL and JSSE options

SSL configuration reloading

SSL Host configuration reloading

Allows updating SSL configuration without a restart

Great solution for many use cases

Use the Tomcat manager webapp for SSL management

Configuration example

See HTTP/2 and SSL/TLS State of Art in Our Servers presentation for additional details

```
<Connector SSLEnabled="true" scheme="https" secure="true" ... >
        <SSLHostConfig>
                <Certificate  certificateKeystoreFile="conf/localhost-rsa.jks" type="RSA" />
        </SSLHostConfig>
</Connector>
```

OpenSSL updates

New features

Now also supports JSSE keystores and truststores

No crash report for a while following further robustness improvements

Access to full OpenSSL configuration capabilities from server.xml:

- Use OpenSSLConf/OpenSSLConfCmd elements in SSLHostConfig
- See OpenSSL documentation for more details: https://www.openssl.org/docs/man1.1.0/ssl/SSL_CONF_cmd.html

Configuration

Install tomcat-native

Configure SSL on the connector

Done !

See HTTP/2 and SSL/TLS State of Art in Our Servers presentation for more details

Future directions

Removal of APR dependency

Support of OpenSSL clones

Modernization of native code

NIO 2 connector updates

New features

New proprietary async IO API introduced in Tomcat 9.0

Attend Improving NIO 2 (and Tomcat) presentation for more details

Configuration

```
<Connector protocol="org.apache.coyote.http11.Http11Nio2Protocol " ... />
```

Or

```
<Connector protocol="org.apache.coyote.ajp.AjpNio2Protocol " ... />
```

All configuration identical to default NIO connector

HTTP/2 protocol handler

New features

Java 9+ JSSE is ALPN ready

tomcat-native enables OpenSSL with NIOx connectors, ALPN ready

NIO 2 specific improvements with async IO:

- Gather semi blocking frame writes
- Scatter async frame reads
- Memory mapping with gather writes for static files

Caveats

ALPN and TLS configuration is demanding

Lower performance with JSSE SSL

Very high GC

Higher resource use than HTTP/1.1

Implement and expose more HTTP/2 features as needed

Configuration

HTTP/1.1 upgrade or direct HTTP/2 connect

```
<Connector protocol="HTTP/1.1" ...>
        <UpgradeProtocol className="org.apache.coyote.http2.Http2Protocol" />
</Connector>
```

Add SSL if needed

Additional HTTP/2 configuration on UpgradeProtocol: compression, performance tuning

Quickstart

Install Java 9+ to get ALPN support

… Or tomcat-native and OpenSSL

Add SSL configuration to the connector

… Or use a proxy and unencrypted direct h2c

… Or connect through HTTP/1.1 and upgrade

Reactive IO

What is it ?

Ability to pause input

Not included in event API from Servlet 3.1

Useful if the backend cannot process IO events quickly enough

Implementation and future

Suspend / resume included for Websockets

Allows suspending and resuming Servlet 3.1 input IO events

Taken advantage of by frameworks like Spring

Possible inclusion in Servlet.next specification

See Reactive IO in Tomcat presentation from Apache EU Roadshow 2018

Websockets support

Suspend / resume methods on WsSession

WsSession.suspend()

WsFrame now filters out the Servlet 3.1 onDataAvailable events

Until WsSession.resume()

Cloud clustering

Cloud clustering

Multicast needed for cluster member discovery

Static membership is not flexible

Need something ready to use

Need to support as many cloud providers as possible

Kubernetes support

Uses Kubernetes API, now supported by most major providers

JSON list of members

Processed using a special implementation of the cluster membership service

Integration in core Tomcat is a goal, until then: web-servers/tomcat-in-the-cloud in github.com

Attend Tomcat: From a cluster to the cloud presentation for more details

Password obfuscation

Password obfuscation

Warning: Obfuscation only, not real security

Uses an extension hook in Tomcat's Digester to process server.xml values and system properties

Either secure storage of values in a secure vault …

… Or straight encryption of values

External component

Configuration

In $CATALINA_BASE/conf/catalina.properties add

```
org.apache.tomcat.util.digester.PROPERTY_SOURCE=org.apache.tomcat.vault.util.PropertySourceVault
```

Store values in vault as documented, or use encryption

Use special replacement markups in server.xml such as ${VAULT::...} and ${CRYPT::...}

See full documentation at web-servers/tomcat-vault in github.com

And more !

More new features

Improved error page processing

HTTPS plaintext error message

Improved JTA readiness with full Commons DBCP 2

/WEB-INF/tomcat-web.xml override for web.xml

LoadBalancerDrainingValve allows easier cluster node updating

Even more new features

ExtractingRoot improves performance for packed WAR files

AuthenticatedUserRealm for flexible client-cert authentication

Inherited channel support for the NIO connector

Static membership cluster with easier configuration

Java 11 support

Future

Possible future major features

Jakarta EE at Eclipse and Apache Tomcat in 2019

- Servlets.next
- Websockets.next
- Reactive streams API
- Access to improved Servlet, JSP, Websockets TCKs

APR connector removal, AJP removal, streamlined and improved Tomcat native ...

Better cleaner Tomcat configuration

Better embedded Tomcat

And more ... That slide is too small, stay tuned !