TomcatSecurityPolicy

Using the Security Manager in Tomcat

The Java SecurityManager protects a Web application from other servlets JSPs and the like.

The easiest way to run lenya in Tomcat is to switch the Security Manager off, by removing the option `-security` from the Tomcat startup options.

If you want to run Lenya in Tomcat with the security manager enabled, you need to write a suitable policy. The appended code is a starting point, but it is incomplete.

Put these lines into, e.g.

`/etc/tomcat5/policy.d/50lenya.policy`

(or whereever your policy files are located).

```
 numbers=off
// You can assign additional permissions to particular web applications by
// adding additional "grant" entries here, based on the code base for that
// application, /WEB-INF/classes/, or /WEB-INF/lib/ jar files.
//
// Different permissions can be granted to JSP pages, classes loaded from
// the /WEB-INF/classes/ directory, all jar files in the /WEB-INF/lib/
// directory, or even to individual jar files in the /WEB-INF/lib/ directory.
//
// For instance, assume that the standard "examples" application
// included a JDBC driver that needed to establish a network connection to the
// corresponding database and used the scrape taglib to get the weather from
// the NOAA web server.  You might create a "grant" entries like this:
//
// The permissions granted to the context root directory apply to JSP pages.
// grant codeBase "file:${catalina.home}/webapps/examples/-" {
//      permission java.net.SocketPermission "dbhost.mycompany.com:5432", "connect";
//      permission java.net.SocketPermission "*.noaa.gov:80", "connect";
// };
//
// The permissions granted to the context WEB-INF/classes directory
// grant codeBase "file:${catalina.home}/webapps/examples/WEB-INF/classes/-" {
// };
//
// The permission granted to your JDBC driver
// grant codeBase "file:${catalina.home}/webapps/examples/WEB-INF/lib/driver.jar!/-" {
//      permission java.net.SocketPermission "dbhost.mycompany.com:5432", "connect";
// };
// The permission granted to the scrape taglib
// grant codeBase "file:${catalina.home}/webapps/examples/WEB-INF/lib/scrape.jar!/-" {
//      permission java.net.SocketPermission "*.noaa.gov:80", "connect";
// };

grant codeBase "file:/var/lib/tomcat5/webapps/lenya/WEB-INF/classes/-" {
 // OS Specific properties to allow read access
  permission java.util.PropertyPermission "java.*", "read";
  permission java.util.PropertyPermission "awt.toolkit", "read";
  permission java.util.PropertyPermission "file.encoding", "read";
  permission java.util.PropertyPermission "user.*", "read";
  permission java.util.PropertyPermission "org.xml.sax.driver", "read";
  permission java.util.PropertyPermission "javax.xml.parsers.*", "read";
  permission java.util.PropertyPermission "org.quartz.properties", "read";
  permission java.util.PropertyPermission "org.xml.sax.driver", "write";
  permission java.io.FilePermission "quartz.properties", "read";
  permission java.util.PropertyPermission "*", "read, write";
  permission java.lang.RuntimePermission "setContextClassLoader";
  permission java.lang.RuntimePermission "shutdownHooks";
  permission java.io.FilePermission "/usr/lib/j2sdk1.5-sun/jre/lib/-", "read";
};

grant codeBase "file:/var/lib/tomcat5/webapps/lenya/WEB-INF/lib/-" {
  permission java.util.PropertyPermission "org.apache.cocoon.*", "read";
  permission java.util.PropertyPermission "context-root", "read";
```

```
  permission java.util.PropertyPermission "log4j.*", "read";
  permission java.util.PropertyPermission "*", "read, write";
  permission java.io.FilePermission "/var/lib/tomcat5/webapps/lenya/WEB-INF/logs/-", "write";
  permission java.io.FilePermission "/usr/share/tomcat5/.cocoon/settings.properties", "read";
  permission java.io.FilePermission "/usr/lib/j2sdk1.5-sun/jre/lib/-", "read";
  permission java.lang.RuntimePermission "shutdownHooks";
  permission java.lang.RuntimePermission "createClassLoader";
  permission java.lang.RuntimePermission "createSecurityManager";
  permission java.lang.RuntimePermission "setContextClassLoader";
  permission java.lang.RuntimePermission "getClassLoader";
  permission java.lang.RuntimePermission "accessDeclaredMembers";
};

grant codebase "file:/var/cache/tomcat5/Catalina/localhost/lenya/cocoon-files/-" {
  permission java.util.PropertyPermission "user.*", "read";

  permission java.io.FilePermission "/var/lib/tomcat5/webapps/lenya", "read";
  permission java.io.FilePermission "/var/lib/tomcat5/webapps/lenya/-", "read";
};

grant {
  permission java.io.FilePermission "quartz.properties", "read";
  permission java.net.SocketPermission "*", "resolve";
  permission java.lang.RuntimePermission "getClassLoader";

};

grant codeBase "file:/var/lib/tomcat5/webapps/cocoon/WEB-INF/classes/-" {
  permission java.util.PropertyPermission "javax.xml.parsers.*", "read";
  permission java.util.PropertyPermission "awt.toolkit", "read";
  permission java.util.PropertyPermission "file.encoding", "read";
  permission java.util.PropertyPermission "java.*", "read";
  permission java.util.PropertyPermission "user.*", "read";
  permission java.util.PropertyPermission "org.xml.sax.driver", "read, write";
  permission java.util.PropertyPermission "javax.xml.parsers.*", "read";
};

grant codeBase "file:/var/lib/tomcat5/webapps/cocoon/WEB-INF/lib/-" {
  permission java.util.PropertyPermission "org.apache.cocoon.*", "read";
  permission java.util.PropertyPermission "context-root", "read";
  permission java.util.PropertyPermission "log4j.*", "read";
  permission java.util.PropertyPermission "org.xml.sax.driver", "read, write";
  permission java.util.PropertyPermission "javax.xml.parsers.*", "read";
  permission java.util.PropertyPermission "awt.toolkit", "read";
  permission java.util.PropertyPermission "file.encoding", "read";
  permission java.util.PropertyPermission "java.*", "read";
  permission java.util.PropertyPermission "user.*", "read";
  permission java.util.PropertyPermission "*", "read, write";

  permission java.lang.RuntimePermission "shutdownHooks";
  permission java.lang.RuntimePermission "createClassLoader";
  permission java.lang.RuntimePermission "createSecurityManager";
  permission java.lang.RuntimePermission "setContextClassLoader";

  permission java.io.FilePermission "/var/lib/tomcat5/webapps/cocoon/WEB-INF/logs/-", "write";
  permission java.io.FilePermission "/usr/share/tomcat5/.cocoon/settings.properties", "read";
  permission java.io.FilePermission "/usr/lib/j2sdk1.5-sun/jre/lib/-", "read";

};
```