The Java Web Server Documentation Pages

Servlet Sandbox

Goal

Jeeves is a dynamically configurable and dynamically extensible Web Server. *Servlets* are used to extend the Web Server, similar to the way that *Applets* extend a Web Browser. Jeeves will provide a controlled execution environment, a *Servlet Sandbox* analagous to the *Applet Sandbox* used by Web Browsers to control applets.

Use of the upcoming code signing facility will allow a new level of policy flexibility to be granted to the web site adminstrator. A new mode of operation will be supported, so that servlets will come in four flavors:

- *Jeeves-Internal Servlets* ... Some parts of Jeeves itself are implemented using servlets, which are granted full access since they are trusted as much as Jeeves itself.
- *Local Servlets* ... Jeeves may be configured with local servlets. Local servlets are normally granted full access, just as if they were Jeeves-internal servlets.
- *Signed Network Servlets* ... All network servlets execute in the **server sandbox**. If the servlet was signed by one of a set of signers who are trusted by the website administrator, the sandbox allows full access. (It can access the file system, remote hosts, and so on.) Servlets which were signed, but not by entities trusted by the website administrator, will be treated like unsigned network servlets.
- *Unsigned Network Servlets* ... Unsigned network servlets will be constrained by the sandbox so that they execute without privilege to access the file system, network and so on.

In the future, the control granted by the sandbox should be made even more flexible. Specifically, an ACL associated with a given web server will define what basic privileges are extended to which signers, and ACL entries used to control access to web resources will be appropriately applied to requests coming through servlets. For example, on a given host the web server operating on port 80 might use a different ACL than one running on port 8080, and if the host uses multihoming, each web server on port 80 could have a different ACL.

Servlet Sandbox Functionality

The servlet sandbox, to be provided in a later release, will protect access to Jeeves resources such as these:

1. Files, including
   - Web pages served by Jeeves
   - Data used to operate each servlet
   - Other files on the file system
2. Runtime state, including
   - Threads controlled by other servlets
   - Security context of other servlets
   - Private Keys used to authenticate this server
3. Administrative state, including
   - Users and groups
   - ACL entries (including ones controlling the sandbox!)
4. Network Servers
5. Other resources controlled by *SecurityManager* objects