Contents

Preface ................................................................................................................................................... 11

1 Web Server Technologies Overview ...................................................................................................... 19
   Technologies and Enhancements in Web Server 7.0 ................................................................. 19
   Supported Standards, Protocols, and Technologies ............................................................... 20
   Tools Support ............................................................................................................................ 22
   Lifecycle Listeners and Modules ............................................................................................... 23
   Session Replication .................................................................................................................. 23
   API Changes from Web Server 6.1 to Web Server 7.0 ............................................................ 23

2 Web Applications Overview ............................................................................................................... 25
   Java Web Applications .................................................................................................................. 25
   Developing and Deploying Web Applications ............................................................................ 25
      Creating Web Applications .................................................................................................... 25
      About Securing Web Applications ...................................................................................... 26
      About Deploying Applications ............................................................................................... 27
      About Virtual Servers ........................................................................................................... 27
      About Default Web Applications ......................................................................................... 27
      Servlet Result Caching .......................................................................................................... 27
      JSP Cache Tags ...................................................................................................................... 28
      Database Connection Pooling ............................................................................................... 28
   Sample Applications in Web Server 7.0 .................................................................................... 29
      Sample Directories ................................................................................................................ 30
      Java Samples ....................................................................................................................... 30
      Building the Samples ........................................................................................................... 32
      Documentation for the Samples ............................................................................................ 32
### Contents

3 **Web Services Overview** ................................................................................................................................. 33
   Introducing Web Services ................................................................................................................................. 33
   Technologies Supported in Web Server 7.0 ......................................................................................................... 34
      Java Web Services Developer Pack 2.0 Technologies ................................................................................. 34
      Message Security (JSR-196) ....................................................................................................................... 35
   Creating Web Services ................................................................................................................................. 35
      Web Services Tools ...................................................................................................................................... 35
      ▼ To Create Web Services from a Java Source ............................................................................................ 35
      ▼ To Create Web Services from Java Classes .............................................................................................. 36
      ▼ To Create Web Services from a WSDL file .............................................................................................. 36
   Securing Web Services .................................................................................................................................. 36
      Understanding Message Security in the Web Server ..................................................................................... 37
      Securing a Web Service ............................................................................................................................... 39
      Admin Console Tasks for Message Security ............................................................................................... 40
   Deploying Web Services ................................................................................................................................ 43
   Testing Web Services .................................................................................................................................... 43
      ▼ To Invoke a Web Service Client ................................................................................................................ 43
   Web Services Samples .................................................................................................................................... 44

4 **Developing Servlets** ...................................................................................................................................... 45
   About Servlets .................................................................................................................................................. 45
   Servlet Output .................................................................................................................................................. 46
   Caching Servlet Results .................................................................................................................................. 46
      Features of Caching .................................................................................................................................... 47
      Default Cache Configuration ......................................................................................................................... 48
      CacheHelper Interface .................................................................................................................................. 48
      Caching Example ........................................................................................................................................ 49
      CacheKeyGenerator Interface ....................................................................................................................... 50
   Maximizing Servlet Performance ...................................................................................................................... 51
   Servlet Internationalization Issues .................................................................................................................. 52
      Servlet Request .......................................................................................................................................... 52
      Servlet Response ........................................................................................................................................ 52
   Migrating Legacy Servlets ............................................................................................................................... 53
      JSP file by Extension ..................................................................................................................................... 53
      Servlet by Extension of Servlet by Directory ............................................................................................. 54
Contents

Using Sessions .................................................................................................................. 77
  Creating or Accessing a Session .................................................................................. 77
  Examining Session Properties ..................................................................................... 78
  Binding Data to a Session ........................................................................................... 79
  Invalidating a Session ............................................................................................... 80
Session Managers .......................................................................................................... 81
  memory Option ............................................................................................................. 81
  file Session Manager ................................................................................................. 82
  IWS60 Session Manager ............................................................................................. 83
  mmap Session Manager (UNIX Only) ......................................................................... 89

7 Developing Lifecycle Listeners .................................................................................. 91
  Server Lifecycle Events ............................................................................................. 91
  The LifecycleListener Interface .................................................................................. 92
  The LifecycleEvent Class .......................................................................................... 92
  The Server Lifecycle Event Context .......................................................................... 92
  Deploying a Lifecycle Module .................................................................................... 93
  Considerations for Lifecycle Modules ....................................................................... 94
  Sample Lifecycle Configuration .................................................................................. 95

8 Securing Web Applications ....................................................................................... 97
  Supported Security Features ....................................................................................... 97
  Common Security Terminology ................................................................................... 98
    Authentication ........................................................................................................... 98
    Authorization ............................................................................................................ 98
    Realms ...................................................................................................................... 98
    Java EE Application Role Mapping .......................................................................... 99
  Security Features Specific to the Web Server ............................................................. 99
    Web Server Security Model ..................................................................................... 99
    Web Application and URL Authorizations ............................................................... 102
  Container Security ................................................................................................... 102
    Programmatic Security ............................................................................................ 102
    Declarative Security ................................................................................................. 102
  User Authentication by Servlets ................................................................................... 103
    HTTP Basic Authentication ..................................................................................... 103
SSL Mutual Authentication .......................................................................................................103
Form-Based Login .....................................................................................................................104
User Authentication for Single Sign-On .........................................................................................104
User Authorization by Servlets ........................................................................................................105
Defining Roles ............................................................................................................................106
Defining Servlet Authorization Constraints ...........................................................................106
Fetching the Client Certificate ....................................................................................................107
Using Web Services Message Security ............................................................................................107
Configuring the Web Server for Message Security ................................................................107
Using Message Security Provider in an Application ........................................................................115
Programmatic Login .........................................................................................................................116
Precautions ........................................................................................................................................116
Granting Programmatic Login Permission .....................................................................................116
ProgrammaticLogin Class ...............................................................................................................117
Enabling the Java Security Manager ..............................................................................................117
The server.policy File ..................................................................................................................118
Default Permissions ......................................................................................................................118
Changing Permissions for an Application ......................................................................................119
Related Information .......................................................................................................................120

9 Deploying Web Applications ...........................................................................................................121
Web Application Structure ..............................................................................................................121
Deployment Tools .............................................................................................................................122
Using Sun Java Studio Enterprise 8.1 .................................................................................................122
Using NetBeans IDE 5.5 ...................................................................................................................123
Creating Web Deployment Descriptors .............................................................................................125
Deploying Web Applications ...........................................................................................................125
▼ To Deploy Using Admin Console ...........................................................................................125
Deploying Using wadm ......................................................................................................................126
Deploying Using JSR 88 .....................................................................................................................128
Auto-Deploying Web Applications .................................................................................................128
▼ Auto-Deploying a Web Application ............................................................................................128
▼ Removing an Auto-Deployed Web Application ............................................................................129
Managing Web Applications ..........................................................................................................129
▼ To Enable or Disable a Deployed Web Application ....................................................................130
Enabling Web Applications ......................................................................................................130
▼ To Remove a Deployed Web Application ........................................................................130
Dynamic Reloading of Web Applications ...............................................................................131
▼ To Set Dynamic Reloading of Web Application ................................................................131
▼ To Load a New Servlet or Reload a Deployment Descriptor ........................................131
Classloaders ........................................................................................................................................132

10 **Debugging Web Applications** .........................................................................................135
Enabling Debugging .....................................................................................................................135
▼ To Enable Debugging Through Admin Console .................................................................135
▼ To Enable Debugging by Editing server.xml .....................................................................136
JPDA Options ....................................................................................................................................136
Using Developer Tools for Debugging ......................................................................................137
▼ To Debug using NetBeans 5.5 ..............................................................................................137
Debugging JSPs ..................................................................................................................................137
Generating a Stack Trace for Debugging ...................................................................................137
Displaying Stack Trace and Compiler Errors ............................................................................137
Using Logging for Debugging .......................................................................................................138
▼ To Change the Log Settings .....................................................................................................138
Using Profiling for Debugging ......................................................................................................139
Using the HPROF Profiler ............................................................................................................139
Using the Optimizeit Profiler .......................................................................................................141

A **Deployment Descriptor Files** ............................................................................................143
About Deployment Descriptor Files ............................................................................................143
Migration Issues ..............................................................................................................................143
Extension to Standard Descriptors ..............................................................................................144
sun-web.xml .................................................................................................................................144
default-web.xml ...........................................................................................................................144
Sun Java System Web Server Descriptors .................................................................................144
The sun-web-app_2_5-0.dtd File ...............................................................................................144
Subelements ...................................................................................................................................145
Data ...............................................................................................................................................145
Attributes ......................................................................................................................................146
Elements in the default-web.xml File .........................................................................................146
Elements in the sun-web.xml File ................................................................. 149
  General Elements ....................................................................................... 150
  Security Elements ...................................................................................... 154
  Session Elements ....................................................................................... 156
  Reference Elements .................................................................................... 162
  Caching Elements ....................................................................................... 170
  Classloader Element ................................................................................... 179
  JSP Element ............................................................................................... 180
  Internationalization Elements .................................................................... 183
  Alphabetical List of sun-web.xml Elements ................................................ 187
Sample Web Application XML Files ............................................................ 189
  Sample web.xml File .................................................................................. 189
  Sample sun-web.xml File ......................................................................... 190

Index ............................................................................................................. 191
Preface

This book explains how Web Applications are created, deployed, and supported in Sun Java™ System Web Server 7.0. The book also includes basic information about Web Services.

Who Should Use This Book

The intended audience for this guide is the person who develops and deploys web applications in a corporate enterprise. This guide assumes you are familiar with the following topics:

- Java SE
- HTML
- The Java programming language
- Software development processes, including debugging and source code control

Web Server Documentation Set

The Sun Java System Web Server documentation set describes how to install and administer the Web Server. You can access Web Server 7.0 Update 6 documentation at http://docs.sun.com/coll/1653.6.

The Sun Java System Web Server documents are now in wiki format at http://wikis.sun.com/display/WebServerdocs/Home. This wiki is intended to promote collaboration and contribution on documentation content for Web Server. You are welcome to contribute, by posting your comments or by directly editing the wiki page, as long as the content is relevant to an appropriate standard.

For an introduction to Sun Java Update 6, refer to the books in the order in which they are listed in the following table.
TABLE P-1 Books in the Web Server Documentation Set

<table>
<thead>
<tr>
<th>Documentation Title</th>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Sun Java System Web Server Documentation Wiki</strong></td>
<td>This wiki is intended to promote collaboration and contribution on documentation content for Web Server.</td>
</tr>
<tr>
<td><strong>Sun Java System Web Server 7.0 Update 6 Documentation</strong></td>
<td>Web Server documentation topics organized by tasks and subject</td>
</tr>
<tr>
<td><strong>Center</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Sun Java System Web Server 7.0 Update 6 Release Notes</strong></td>
<td>▪ Late-breaking information about the software and documentation</td>
</tr>
<tr>
<td></td>
<td>▪ Supported platforms and patch requirements for installing Web Server</td>
</tr>
<tr>
<td><strong>Sun Java System Web Server 7.0 Update 6 Installation</strong></td>
<td>Performing installation and migration tasks:</td>
</tr>
<tr>
<td><strong>and Migration Guide</strong></td>
<td>▪ Installing Web Server and its various components,</td>
</tr>
<tr>
<td></td>
<td>▪ Migrating data from Sun ONE Web Server 6.0 or 6.1 to Sun Java System Web Server 7.0</td>
</tr>
<tr>
<td><strong>Sun Java System Web Server 7.0 Update 6 Administrator’s</strong></td>
<td>Performing the following administration tasks:</td>
</tr>
<tr>
<td><strong>Guide</strong></td>
<td>▪ Using the Administration GUI and command-line interface</td>
</tr>
<tr>
<td></td>
<td>▪ Configuring server preferences</td>
</tr>
<tr>
<td></td>
<td>▪ Using server instances</td>
</tr>
<tr>
<td></td>
<td>▪ Monitoring and logging server activity</td>
</tr>
<tr>
<td></td>
<td>▪ Using certificates and public key cryptography to secure the server</td>
</tr>
<tr>
<td></td>
<td>▪ Configuring access control to secure the server</td>
</tr>
<tr>
<td></td>
<td>▪ Using Java Platform Enterprise Edition (Java EE) security features</td>
</tr>
<tr>
<td></td>
<td>▪ Deploying applications</td>
</tr>
<tr>
<td></td>
<td>▪ Managing virtual servers</td>
</tr>
<tr>
<td></td>
<td>▪ Defining server workload and sizing the system to meet performance needs</td>
</tr>
<tr>
<td></td>
<td>▪ Searching the contents and attributes of server documents, and creating a text search interface</td>
</tr>
<tr>
<td></td>
<td>▪ Configuring the server for content compression</td>
</tr>
<tr>
<td></td>
<td>▪ Configuring the server for web publishing and content authoring using WebDAV</td>
</tr>
<tr>
<td><strong>Sun Java System Web Server 7.0 Update 6 Developer’s</strong></td>
<td>Using programming technologies and APIs to do the following:</td>
</tr>
<tr>
<td><strong>Guide</strong></td>
<td>▪ Extend and modify Sun Java System Web Server</td>
</tr>
<tr>
<td></td>
<td>▪ Dynamically generate content in response to client requests and modify the content of the server</td>
</tr>
</tbody>
</table>
Related Books

The URL for all documentation about Sun Java Enterprise System (Java ES) and its components is http://docs.sun.com/coll/1286.3.

Default Paths and File Names

The following table describes the default paths and file names that are used in this book.
### Default Paths and File Names

<table>
<thead>
<tr>
<th>Placeholder</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>install-dir</strong></td>
<td>Represents the base installation directory for Sun Java</td>
<td>Sun Java Enterprise System (Java ES) installations on the Solaris™ platform: <code>/opt/SUNWwbsvr7</code>&lt;br&gt;Java ES installations on the Linux and HP-UX platform: <code>/opt/sun/webserver/</code>&lt;br&gt;Java ES installations on the Windows platform: <code>system-drive:\Program Files\Sun\JavaES5\WebServer7</code>&lt;br&gt;Other Solaris, Linux, and HP-UX installations, non-root user: <code>home-directory/sun/webserver7</code>&lt;br&gt;Other Solaris, Linux, and HP-UX installations, root user: <code>/sun/webserver7</code>&lt;br&gt;Windows, all installations: <code>system-drive:\Program Files\Sun\WebServer7</code>&lt;br&gt;For stand-alone installations, the default location for instance on Solaris: <code>/var/opt/SUNWwbsvr7</code>&lt;br&gt;For Java ES installations, the default location for instances on Linux and HP-UX: <code>/var/opt/sun/webserver7</code>&lt;br&gt;For Java ES installations, the default location for instance on Windows: <code>system-drive:\Program Files\Sun\JavaES5\WebServer7</code>&lt;br&gt;For stand-alone installations, the default location for instance on Solaris, Linux, and HP-UX: <code>install-dir</code>&lt;br&gt;For stand-alone installations, the default location for instance on Windows: <code>system-drive:\Program Files\sun\WebServer7</code></td>
</tr>
<tr>
<td><strong>instance-dir</strong></td>
<td>Directory that contains the instance-specific subdirectories.</td>
<td>For Java ES installations, the default location for instances on Solaris: <code>/var/opt/SUNWwbsvr7</code>&lt;br&gt;For Java ES installations, the default location for instances on Linux and HP-UX: <code>/var/opt/sun/webserver7</code>&lt;br&gt;For Java ES installations, the default location for instance on Windows: <code>system-drive:\Program Files\Sun\JavaES5\WebServer7</code>&lt;br&gt;For stand-alone installations, the default location for instance on Solaris, Linux, and HP-UX: <code>install-dir</code>&lt;br&gt;For stand-alone installations, the default location for instance on Windows: <code>system-drive:\Program Files\sun\WebServer7</code></td>
</tr>
</tbody>
</table>
Typographic Conventions

The following table describes the typographic changes that are used in this book.

<table>
<thead>
<tr>
<th>Typeface</th>
<th>Meaning</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>AaBbCc123</td>
<td>The names of commands, files, and directories, and onscreen computer output</td>
<td>Edit your .login file. Use <code>ls -a</code> to list all files. `machine_name% you have mail.</td>
</tr>
<tr>
<td>AaBbCc123</td>
<td>What you type, contrasted with onscreen computer output</td>
<td><code>machine_name% su</code> <code>Password:</code></td>
</tr>
<tr>
<td>AaBbCc123</td>
<td>A placeholder to be replaced with a real name or value</td>
<td>The command to remove a file is <code>rm filename</code>.</td>
</tr>
<tr>
<td>AaBbCc123</td>
<td>Book titles, new terms, and terms to be emphasized (note that some emphasized items appear bold online)</td>
<td>Read Chapter 6 in the <code>User's Guide</code>. A <code>cache</code> is a copy that is stored locally. Do not save the file.</td>
</tr>
</tbody>
</table>

Symbol Conventions

The following table explains symbols that might be used in this book.

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
<th>Example</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>[ ]</td>
<td>Contains optional arguments and command options.</td>
<td><code>ls [-l]</code></td>
<td>The <code>-l</code> option is not required.</td>
</tr>
<tr>
<td>{</td>
<td>}</td>
<td>Contains a set of choices for a required command option.</td>
<td>`-d {y</td>
</tr>
<tr>
<td>$ {</td>
<td>}</td>
<td>Indicates a variable reference.</td>
<td><code>${com.sun.javaRoot}</code></td>
</tr>
<tr>
<td>-</td>
<td>Joins simultaneous multiple keystrokes.</td>
<td>Control-A</td>
<td>Press the Control key while you press the A key.</td>
</tr>
<tr>
<td>+</td>
<td>Joins consecutive multiple keystrokes.</td>
<td>Ctrl+A+N</td>
<td>Press the Control key, release it, and then press the subsequent keys.</td>
</tr>
</tbody>
</table>
TABLE P-4  Symbol Conventions  (Continued)

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
<th>Example</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>➔</td>
<td>Indicates menu item selection in a graphical user interface.</td>
<td>File ➔ New ➔ Templates</td>
<td>From the File menu, choose New. From the New submenu, choose Templates.</td>
</tr>
</tbody>
</table>

**Accessing Sun Resources Online**

The [http://docs.sun.com](http://docs.sun.com) (docs.sun.com™) web site enables you to access Sun technical documentation online. You can browse the docs.sun.com archive or search for a specific book title or subject. Books are available as online files in PDF and HTML formats. Both formats are readable by assistive technologies for users with disabilities.

To access the following Sun resources, go to [http://www.sun.com](http://www.sun.com):

- Downloads of Sun products
- Services and solutions
- Support (including patches and updates)
- Training
- Research
- Communities (for example, Sun Developer Network)

** Searching Sun Product Documentation**

Besides searching Sun product documentation from the [docs.sun.com](http://docs.sun.com) web site, you can use a search engine by typing the following syntax in the search field:

```
search-term  site:docs.sun.com
```

For example, to search for “Web Server,” type the following:

```
Web Server  site:docs.sun.com
```

To include other Sun web sites in your search (for example, [java.sun.com](http://java.sun.com), [www.sun.com](http://www.sun.com), and [developers.sun.com](http://developers.sun.com)), use “sun.com” in place of “docs.sun.com” in the search field.
Third-Party Web Site References

Third-party URLs are referenced in this document and provide additional, related information.

**Note** – Sun is not responsible for the availability of third-party web sites mentioned in this document. Sun does not endorse and is not responsible or liable for any content, advertising, products, or other materials that are available on or through such sites or resources. Sun will not be responsible or liable for any actual or alleged damage or loss caused or alleged to be caused by or in connection with use of or reliance on any such content, goods, or services that are available on or through such sites or resources.

Sun Welcomes Your Comments

Sun is interested in improving its documentation and welcomes your comments and suggestions. To share your comments:

- Go to [http://docs.sun.com](http://docs.sun.com) and click Feedback.
- Go to [http://wikis.sun.com/display/WebServerdocs/Home](http://wikis.sun.com/display/WebServerdocs/Home) and post your comments or directly edit the wiki page.
Web Server Technologies Overview

This chapter provides a basic overview on various technologies that are supported in the Web Server.

Technologies and Enhancements in Web Server 7.0

Web Server is a major new release with significant enhancements in the administration infrastructure. This release is the first 64-bit version of Web Server supported on Solaris SPARC®, AMD64 and Linux platforms.

Web Server 7.0 provides:

- Comprehensive command-line interface support
- Consolidated configuration
- Enhanced security
- Web-based Distributed Authoring and Versioning (WDAV)
- Access control lists (ACL)
- URL rewriting
- Clustering support

This product also comes with a robust built-in migration tool that helps migrate applications and configurations from Web Server 6.0 and 6.1 to Sun Java System Web Server 7.0.

Sun Java System Web Server 7.0 introduces the following new features:

- Management infrastructure
- Java Web Services Developer Pack 2.0 support
- Session replication support
- Extensive real-time monitoring support
- Integrated reverse proxy plug-in and FastCGI plug-in support

For more features and information, see “Features and Enhancements in Update 2 Release” in Sun Java System Web Server 7.0 Update 6 Release Notes.
Supported Standards, Protocols, and Technologies

Servlet 2.5 Support
Java servlets are server-side Java programs that generate content in response to a client request. Servlets can be thought of as applets that run on the server side without a user interface. Servlets are invoked through URL invocation or by other servlets.

Sun Java System Web Server 7.0 supports the Java Servlet 2.5 specification.

Note – Java Servlet API version 2.5 is fully backward compatible with versions 2.1, 2.2, 2.3, and 2.5. Therefore, all existing servlets continue to work without modification or recompilation.

To develop servlets, use Sun’s Java Servlet API. For information about using the Java Servlet API, see the documentation provided by Sun at http://java.sun.com/products/servlet/index.html.

For the Java Servlet 2.5 specification, see http://java.sun.com/products/servlet/download.html.

For information about developing servlets in Sun Java System Web Server, see Chapter 4, “Developing Servlets”

JSP 2.1 Support
Web Server 7.0 supports the JavaServer Pages (JSP) 2.1 specification. A JSP page is, much like an HTML page, that can be viewed in a web browser. However, in addition to HTML tags, JSP can include a set of JSP tags and directives intermixed with Java code that extend the ability of the web page designer to incorporate dynamic content in a page. These additional features provide functionality such as displaying property values and using simple conditionals.

JSP pages can access full Java functionality using the following methods:

- Embedding Java code directly into scriptlets
- Using server-side tags that include Java servlets

Servlets are Java classes that must be compiled. Servlets can be defined and compiled by a Java programmer, who then publishes the interface to the servlet. The web page designer can access a precompiled servlet from a JSP page. For information about creating JSP pages, see http://java.sun.com/products/jsp/index.html

JSTL 1.2
The Java Server Pages Standard Tag Library (JSTL) encapsulates as simple tags the core functionality common to many web applications. JSTL has support for common, structural
tasks such as iteration and conditionals, tags for manipulating XML documents, internationalization tags, and SQL tags. It also provides a framework for integrating existing custom tags with JSTL tags.

For more information on JSTL 1.2, see http://java.sun.com/j2ee/1.4/docs/tutorial/doc/JSTL.html#wp74644.

Java Web Services Developer Pack 2.0 Support
Web Services uses a Web Services Description Language (WSDL) file to describe the service and a registry service to register and lookup the services. The Simple Object Access Protocol (SOAP) binding is the standard interoperable binding for accessing Web Services. Based on Java Web Services Developer Pack (Java WSDP), Web Server supports integrated Java Web Services runtime and tools, and therefore supports portable Web Services implementations. For more information, see Chapter 3, “Web Services Overview.”

JNDI Naming
Web Server 7.0 provides Java Naming and Directory Interface™ (JNDI) API support that enables web applications to look up for Java Enterprise Edition (Java EE) services such as Java Database Connectivity (JDBC™) data sources. All functional aspects of this JNDI implementation are essential. However, the web server’s implementation does not support the CosNaming service required for remote objects as well as lookup of UserTransaction, ORB, JMS resources, or the EJB references.

JDBC Connection Pooling
In Web Server, JDBCRESOURCE and JDBC CONNECTIONPOOL elements in server.xml have been merged into one element called jdbc-resource to simplify JDBC configuration. Many of the configuration parameters have been renamed. For more information on the jdbc-resource element, see Chapter 3, “Elements in server.xml,” in Sun Java System Web Server 7.0 Update 6 Administrator’s Configuration File Reference.

Using JNDI to Access the jdbc-resource Within a Web Application
Using JNDI, a web application can access a JDBC connection pool by looking up the jdbc-resource that configures it. The jdbc-resources can access the name in its web descriptor. The following web descriptors example refer to the connection pool created in the earlier example.

WEB-INF/web.xml

```xml
<web-app>
...
<resource-ref>
  <description>jdbc-resource</description>
</resource-ref>
```
In the above example, `jdbc/myJdbc` is the name by which the pool is referenced in the web application and `jdbc/MyPool` is the JNDI name of the `jdbc-resources` configuration.

The following is an example for using the pool in a web application.

```java
Context initContext = new InitialContext();
Context webContext = (Context)initContext.lookup("java:/comp/env");

DataSource ds = (DataSource) webContext.lookup("jdbc/myJdbc");
Connection dbCon = ds.getConnection();
```

## Tools Support

Web Server 7.0 provides support for the following tools:

- **Sun Java Studio Enterprise 8.1** – Java Studio Enterprise 8.1 enables you create Java, Web, and EJB projects from existing code.

- **NetBeans IDE 5.5** – NetBeans IDE 5.5 is an integrated development environment to create, deploy the Java EE based web applications.
  
  For more information, see “Using NetBeans IDE 5.5” on page 123.

- **Sun Java Studio Enterprise 8.1** – Web Server 7.0 supports Sun Java Studio Enterprise 8.1, Standard Edition. You can use Sun Java Studio to assemble and deploy web applications. For more information, see “Using Sun Java Studio Enterprise 8.1” on page 122.

Lifecycle Listeners and Modules

Sun Java System Web Server 7.0 enables you to write customized classes for the various phases of the server lifecycle. For instance, a user may have a startup code that ensures that a remote data source is available for the applications. Such classes are notified of server lifecycle events supporting Java based tasks within the Web Server environment. These tasks automatically perform actions such as starting the server and sending notification if the server shuts down. You can use this support to instantiate singletons, RMI servers, and so forth. For more information, see “List of Elements” in Sun Java System Web Server 7.0 Update 6 Administrator’s Configuration File Reference

Session Replication

The intention of session replication is to provide sufficient session failover support through in-memory-backup of HTTP sessions to another server instance of the same cluster. This feature covers most usage scenarios. For more information, see “Configuring Session Replication” in Sun Java System Web Server 7.0 Update 6 Administrator’s Guide

API Changes from Web Server 6.1 to Web Server 7.0

Sun Java System Web Server has the following core components:

- Web container implements the JSP 2.1, Servlet 2.5, and JSTL 1.2 specification which are part of Java EE 1.4.
- Monitoring and configuring interfaces.

For more information about non-Java APIs and programming technologies, see the Sun Java System Web Server 7.0 Update 6 Developer’s Guide and the Sun Java System Web Server 7.0 Update 6 NSAPI Developer’s Guide.
Chapter 2

Web Applications Overview

This chapter provides a basic overview of how web applications are supported in Web Server. This chapter includes the following sections:

- “Java Web Applications” on page 25
- “Developing and Deploying Web Applications” on page 25
- “Sample Applications in Web Server 7.0” on page 29

Java Web Applications

Web Server supports the Java™ Servlet 2.5 API specification and the JavaServer Pages™ (JSP™) 2.1 specification, which allows servlets and JSPs to be included in web applications.

A web application is a collection of servlets, JavaServer Pages, HTML documents, and other web resources that include image files, compressed archives, and other data. A web application can be packaged into a web archive (WAR) file or exist in an open directory structure.

Web Server 7.0 also supports, SHTML and CGI, which are not Java Platform, Enterprise Edition (Java EE) application components. For more information about APIs and programming technologies, see Sun Java System Web Server 7.0 Update 6 Developer’s Guide.

Developing and Deploying Web Applications

This section describes how to create, secure, and deploy web applications using Web Server.

Creating Web Applications

This section lists the general actions to create a web application, and provides pointers to more information.
1. Create a directory for all of the web application's files. This directory is the web application's document root.
2. Create any needed HTML files, image files, and other static content.
3. Place these files in the document root directory or a subdirectory where they can be accessed by other parts of the application.
4. Create any needed JSP files.
   For more information, see Chapter 5, "Developing JavaServer Pages"
5. Create any needed servlets.
   For more information, see Chapter 4, "Developing Servlets."
6. Compile the servlets.
   For details about precompiling JSPs, see “Compiling JSPs Using the Command-Line Compiler” on page 58.
7. Organize the web application as described in “Web Application Structure” on page 121.
8. Create the deployment descriptor files.
   For more information, see “Creating Web Deployment Descriptors” on page 125.
9. (Optional) Package the web application in a .war file. For example:
   
   \( \text{jar } -cvf \text{ module_name.war *} \)
10. Deploy the web application. For more information, see “Deploying Web Applications” on page 125.

You can create a web application manually or you can use Java System Enterprise Studio. For more information about developing web applications in Sun Java Enterprise Studio, see http://developers.sun.com/prodtech/javatools/jscreator/learning/tutorials/2/helloweb.html

### About Securing Web Applications

You can write secure web applications for the Sun Java System Web Server with components that perform user authentication and access authorization. You can build security into web applications using the following mechanisms:

- User authentication by servlets
- User authentication for single sign-on
- User authorization by servlets
- Requesting the client certificate

For detailed information about these mechanisms, see Chapter 8, “Securing Web Applications.”
About Deploying Applications

A web application is a collection of servlets, JSP, HTML documents, and other web resources that might include image files, compressed archives, and other data. A web application can be packaged into a Web ARchive file (a WAR file) or exist in an open directory structure. For more information, see Chapter 9, “Deploying Web Applications.”

About Virtual Servers

A virtual server is a virtual web server that uses a unique combination of IP address, port number, and host name to identify it. You might have several virtual servers all of which use the same IP address and port number but are distinguished by their unique host names.

When you first install Web Server, a default virtual server is created. You can also assign a default virtual server to each new HTTP listener you create. For details, see Sun Java System Web Server 7.0 Update 6 Administrator’s Guide.

About Default Web Applications

A web application that is deployed in a virtual server at a URL / becomes the default web application for that virtual server. To access the default web application for a virtual server, type the URL for the virtual server but do not supply a context root. For example:

http://myvirtualserver:3184/

If none of the web applications under a virtual server are deployed at the URI "/", the virtual server serves HTML or JSP content from its document root, which is usually instance_dir/docs. To access this HTML or JSP content, point your browser to the URL for the virtual server specify the target file rather than a context root. For example:

http://myvirtualserver:3184/hellothere.jsp

Servlet Result Caching

The Web Server can cache servlet or JSP results to make subsequent calls to the same servlet or JSP page faster.

For more information about response caching as it pertains to servlets, see “Caching Servlet Results” on page 46.
JSP Cache Tags

JSP cache tags enable you to cache JSP page fragments within the Java engine. Each can be cached using different cache criteria. For example, if you have page fragments to view stock quotes and weather information, you can cache the stock quote fragment for 15 minutes, and the weather report fragment for 25 minutes.

For more information about JSP caching, see “JSP Cache Tags” on page 61.

Database Connection Pooling

Database connection pooling enhances the performance of servlet or JSP database interactions. For more information about the Java™ Database Connectivity (JDBC™) software, see “Configuring JDBC Resources” in Sun Java System Web Server 7.0 Update 6 Administrator’s Guide.

The simplest connection pool can be configured by using the given. In this example, the connection pool is assigned to use the ORACLE JDBC driver.

▼ To Configure a Simple Connection Pool

In this example procedure, the connection pool uses the ORACLE JDBC driver.

1 Start wadm

    $ ./bin/wadm --user=admin
    Please enter admin-user-password>user-admin-password
    Sun Java System Web Server 7.0 08/02/2006 14:22
    wadm>

2 Verify the list of available configurations.

    wadm> list-configs

3 Create the jdbc-resource configuration.

    For more information about all possible elements, see Sun Java System Web Server 7.0 Administrator’s Configuration File Reference.

    wadm> create-jdbc-resource --config=test
    --datasource-class=oracle.jdbc.pool.OracleDataSource jdbc/MyPool

4 Add properties to jdbc-resource.

    Properties are primarily used to configure the driver’s vendor-specific properties. In the following example, the values for the properties url, user, and password are added to jdbc-resource.

    wadm> list-jdbc-resource-userprops --config=test --jndi-name=jdbc/MyPool
    password=mypassword user=myuser url=jdbcZ:oracle:thin:@hostname:1421MYSID
Enable the connection validation.

```
> wadm set-jdbc-resource-prop --config=test --jndi-name=jdbc/MyPool connection-validation-table-name=test connection-validation=table
CLI201 Command "set-jdbc-resource-prop" ran successfully.
```

Change the pool setting.

In this example, the maximum number of connections is set to 100.

```
> wadm set-jdbc-resource-prop --config=test --jndi-name=jdbc/MyPool max-connections=100
CLI201 Command "set-jdbc-resource-prop" ran successfully.
```

Deploy the configuration.

```
> wadm deploy-config test
CLI201 Command "deploy-config" ran successfully.
```

You can install a JDBC driver with Java Archive (JAR) files in one of the following ways:

- Copy the driver’s JAR file into the server’s instance library directory. JAR files in the instance library directory will automatically load and available for server.
- Modify the JVM class-path-suffix to include JDBC drivers jar file. The new value will overwrite the old value of the element. For example,

```
> wadm set-jvm-prop --config=test class-path-suffix=/export/home/lib/classes12.jar
```

Sample Applications in Web Server 7.0

Sun Java System Web Server 7.0 includes a set of sample applications, which can be found in the `install-dir/samples` directory. All the sample applications are arranged in a specific and well-defined directory structure. The sample application included as part of the Sun Java System Web Server are packaged into consistent directory structure as elaborated below:

- **NSAPI** — This directory contains examples of source code for Server Application Functions (SAFs) which helps you get started with programming your Sun Java System Web Server.
  Directory path: `install-dir/samples/nsapi`
- **Java** — This directory contains samples which help to create, deploy and run various java applications.
  Directory path: `install-dir/samples/java`
- **FastCGI** — This directory contains samples, which demonstrates the use of PHP Add-On and FastCGI plug-in on Web Server 7.0.
  Directory path: `install-dir/samples/fastcgi`
- **Administration CLI** — This directory contains scripts that one can run using the `wadm` command line utility. The utility can be found at `<install-root>/bin/wadm`. `wadm` is built on a Tc1 engine and hence supports Tcl scripting. Some of these samples demonstrate how
scripts can be used to perform common administrative tasks. They also demonstrate how new utilities can be built on top of existing commands.

- **NSACL** — This directory contains access control samples which implement the Loadable Attribute Service (LAS) APIs.

Sample Directories

All of the sample applications are arranged in a specific and well-defined directory structure. In general, the top-level directory of a sample application includes the following:

- **src**: A directory containing all the Java source files, deployment descriptors, JSPs, and HTML files. Samples that use a database provide a script to populate data in the database.
- **docs**: A directory containing all documentation for the application.
- **.WAR file**: The deployable .WAR file for the sample application.
- **build.xml**: A file for the ANT system to build the sample application

Java Samples

A complete index of Java sample applications provided as part of the Sun Java System Web Server product is listed below:

<table>
<thead>
<tr>
<th>Directory</th>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>apis</td>
<td>This directory contains source code of the extensible session manager and session store API that was published in the previous release of Web Server (6.0). These APIs have been deprecated since Sun ONE Web Server 6.1 and are provided in this directory for the purpose of backward compatibility. Directory path: install-dir/samples/java/apis</td>
</tr>
<tr>
<td>simple</td>
<td>Basic JSP and servlet examples combined into a single web application (Tomcat samples). Directory path: install-dir/samples/java/webapps/simple</td>
</tr>
<tr>
<td>caching</td>
<td>JSP and servlet examples that demonstrate how to cache results of JSP and servlet execution. Directory path: install-dir/samples/java/webapps/caching</td>
</tr>
</tbody>
</table>
### TABLE 2-1 Java Samples (Continued)

<table>
<thead>
<tr>
<th>Directory</th>
<th>Contents</th>
</tr>
</thead>
</table>
| jstl      | Basic examples that demonstrate usage of the JSP Standard Tag Library.  
            Directory path: install-dir/samples/java/webapps/jstl |
| rmi-iiop  | Basic example that demonstrates using a servlet to access a stateless EJB™ using RMI/IIOP running in Sun Java System Application Server 8.x.  
            Directory path: install-dir/samples/java/webapps/rmi-iiop |
| javamail  | A servlet that uses the Javamail API to send an email message.  
            Directory path: install-dir/samples/java/webapps/javamail |
| i18n      | A basic Java EE web application that demonstrates how to dynamically change the display language based on user preference.  
            Directory path: install-dir/samples/java/webapps/i18n |
| JSF       | Example showing how to use Java Server Faces (JSF) components to quickly build web application user interfaces. JSF examples are included in the following directories:  
            ❘ carstore: Online car store sample  
            ❘ components: JSF custom components sample  
            ❘ guessnumber: Guess number sample  
            Directory path: install-dir/samples/java/webapps/jsf |
| jdbc      | Java DataBase Connectivity examples are included in the following directories:  
            ❘ blob: A servlet that accesses BLOBs through the JDBC API  
            ❘ simple: A basic servlet that accesses an RDBMS through the JDBC API  
            ❘ transactions: A servlet that uses the transaction API with JDBC to control a local transaction  
            ❘ rowset: Demonstrates the JDBC rowset feature  
            Directory path: install-dir/samples/java/webapps/jdbc |
| jndi      | Java Naming and Directory Interface examples are in the following directories:  
            ❘ custom: Demonstrates how to use the custom resource  
            ❘ external: Demonstrates how to use the external resource  
            ❘ readenv: Demonstrates how to use the environment entries specified in the web.xml file  
            ❘ url: Demonstrates how to use the servlet with the URL resource facility to access a resource  
            Directory path: install-dir/samples/java/webapps/jndi |
### Directory Contents

**security**

Examples demonstrating how to secure Java EE web applications through standard authentication mechanisms and access controls. Security examples are included in the following directories:

- **basic-auth**: Demonstrates how to develop, configure, and exercise basic authentication
- **client-cert**: Demonstrates how to develop, configure, and exercise client certificate authentication
- **form-auth**: Demonstrates how to develop, configure, and exercise form-based authentication
- **jdbcrealm**: Demonstrates how to develop, configure, and exercise JDBC realm authentication

Directory path: `install-dir/samples/java/webapps/security`

**webservices/security**

Web services security examples are located in the following directory:

- **fromwsdl-soap12**: Demonstrates how to develop, configure, and run a simple web services security sample

Directory path: `install-dir/samples/java/webapps/webservices/security`

### Building the Samples

An ANT-based build system is used to build the individual sample application. The `build.xml` file has targets to compile the sources, to clean, and to build the war file. It also has targets to deploy and undeploy the application, using the corresponding CLI commands provided by the Web Server. Register application resources in the deployment target.

### Documentation for the Samples

Documentation is installed along with the samples during the installation. The `index.html` in the document root of the default Web Server instance contains links to the samples documentation. In addition, you can access the documentation HTML files directly in the samples directory.
This chapter focuses on web services tasks that are performed by developers. For administrator tasks, including configuration and management information, see Appendix C, "Web Services," in *Sun Java System Web Server 7.0 Update 6 Administrator’s Guide*.

### Introducing Web Services

Web Services uses a Web Services Description Language (WSDL) file to describe the service and registry service to register and look up the services. The Simple Object Access Protocol (SOAP) binding is the standard interoperable binding for accessing Web Services. Several registry protocols available, but UDDI (Universal Description, Discovery and Integration) is probably the most recognizable based on Java Web Services Developer Pack, Web Server because it supports integrated Java Web Services runtime and tools, and therefore supports portable Web Services implementations, making it interoperable with .NET clients and services using the WS-I Basic Profile. For more information on Web Services, see [http://java.sun.com/webservices/docs/2.0/tutorial/doc/index.html](http://java.sun.com/webservices/docs/2.0/tutorial/doc/index.html).

WS-Security is an OASIS proposal for adding message-layer security to SOAP messages. It defines standardized locations and syntax by which security tokens such as X.509 certificates and Kerberos tickets can be carried within SOAP Headers in order to secure the contents of the SOAP message exchanges. WS-Security leverages the existing XML Digital Signature and XML Encryption specifications for capturing the results of signing and encryption operations in XML syntax. In essence, WS-Security standardizes the XML Signature and XML Encryption data blocks that are carried with a SOAP message. Web Server supports the integrated WS-Security standard. In addition, this release supports JSR-196 as applicable to Web Services. Web Server provides the ability to bind SOAP-layer message-security providers and message-protection policies to the container. This binding allows the container to enforce the security on behalf of the applications.
Technologies Supported in Web Server 7.0

This section describes the technologies supported by Web Server 7.0. For more information, see http://java.sun.com/webservices/docs/2.0/tutorial/doc/index.html.

This section contains the following topics:
- “Java Web Services Developer Pack 2.0 Technologies” on page 34
- “Message Security (JSR-196)” on page 35

Java Web Services Developer Pack 2.0 Technologies

Java Web Services Developer Pack, provides an integrated development and test environment. The technologies included with Web Server are:

- JAX-WS 2.0 (JSR 224) - The Java API for XML-based JAX-WS 2.0 is the key specification for component-based web service development, and governs the standard mappings between WSDL/XML schema and the Java platform. It is the next generation of JAX-RPC.
- JAXB 2.0.3 – The Java architecture for XML Binding 2.0.3 (“JAXB”) defines an extensible mapping between the Java and XML schema type models and facilitates XML serialization of Java objects.
- JAXP 1.3.1: The Java API for XML Processing 1.3.1 (“JAXP”) provides a standard framework for parsing and transforming XML documents and streams using the Simple API for XML (SAX), the Document Object Model (DOM), and Extensible Stylesheets Language Transformations (XSLT).
- SOAP 1.2 – SOAP is a means for encoding remote procedure calls (RPCs) and document-style information as XML.
- WSDL 1.1 – WSDL is an XML-based standard for describing the external interface to a web service.
- SAAJ 1.3 – SOAP with Attachments API for Java (SAAJ) defines a simple object model for creating, manipulating, and sending SOAP messages.
- XWSS-XML Web Services Security (XWSS) provides a framework within which a Web service developer can secure applications. For more information, see http://java.sun.com/webservices.
- Fast Infoset- The Fast Infoset specification (ITU-T Rec. X.891 | ISO/IEC 24824-1) describes an open, standards-based binary XML format that is based on the XML Information Set. It is an efficient alternative to XML. For more information, see http://java.sun.com/webservices/docs/2.0/fastinfoset/fastinfoset1.0.1-manual.html.
Message Security (JSR-196)

In message security, security information is inserted into messages so that it travels through the networking layers and arrives with the message at the message destination. Message security differs from transport layer security. Message security can be used to decouple message protection from message transport so that the message remains protected after transmission. For more information on security, see http://java.sun.com/j2ee/1.4/docs/tutorial/doc/Security2.html#wp268799.

JSR-196, as applicable to Web Services, defines a standard service provider interface by which authentication mechanism providers may be integrated with containers. Providers integrated through this interface establish the authentication identities used in container access decisions while servicing the request.

Creating Web Services

Web Services is created in different ways, depending on whether the starting point of development is a Java source file, a Java class file, or a WSDL file.

Web Services Tools

Use different tools is used to generate JAX-WS artifacts, depending on whether the starting point of Web Services development is a Java source file, a Java class file, or a WSDL file.

- **apt** — The Annotation Processing Tool (APT) tool is part of Java SE 5. It programmatically processes the annotations and generates the JAX-WS portable artifacts from an annotated Java source file.
- **wsgen** - The wsgen tool reads a service endpoint implementation class and generates all of the portable artifacts for a JAX-WS web service.
- **wsimport** - The wsimport tool reads a WSDL and generates all the required artifacts for web service development, deployment, and invocation.

---

**Note** – After using the tools, the web.xml, sun-jaxws.xml, the implementation class, and the portable JAX-WS artifacts must be bundled into a WAR that can be deployed onto a container.

The following procedures describes how to use these methods.

▼ To Create Web Services from a Java Source

1. **Use** apt **to generate Java artifacts such as the WSDL file, and schema documents.**
2 Package the `web.xml`, `sun-jaxws.xml`, service endpoint interface and implementation class, value types, and generated classes, if any, into a WAR file.

3 Deploy the WAR file to Web Server.

▼ To Create Web Services from Java Classes

1 Use `wsgen` to generate portable artifacts.

2 Package the `web.xml`, `sun-jaxws.xml`, service endpoint interface and implementation class, value types, and generated classes, if any, into a WAR file.

3 Deploy the WAR file to Web Server.

▼ To Create Web Services from a WSDL file

1 Use `wsimport` to generate portable artifacts.

2 Implement the service endpoint.

3 Package the `WSDL` file, `schema documents`, `web.xml`, `sun-jaxws.xml`, service endpoint interface and implementation class, value types, and generated classes, if any, into a WAR file.

4 Deploy the WAR file to a web container.

Securing Web Services

Web Services Security SOAP Message Security (WS-Security) is an international standard for interoperable web services security that was developed in OASIS by a collaboration of all the major providers of web services technology (including Sun Microsystems). WS-Security is a message security mechanism that uses XML Encryption and XML Digital Signature to secure web services messages sent over SOAP. The WS-Security specification defines the use of various security tokens including X.509 certificates, SAML assertions, and username and password tokens to authenticate and encrypt SOAP Web Services messages. This section also includes the following sections:

- Understanding message security in the Web Server
- Securing a web service
- Securing a sample application
- Configuring the Web Server for message security
Admin Console tasks for message security

Understanding Message Security in the Web Server

The Web Server offers integrated support for the WS-Security standard in the server-side container. This functionality is integrated with Web Services security and enforced by the container of the Web Server on behalf of applications. Web Server can protect any web service application without requiring changes to the implementation of the application. The Web Server achieves this effect by providing facilities to bind SOAP layer message security providers and message protection policies to container and to applications deployed in container.

Assigning Message Security Roles

In the Web Server, the system administrator and application deployer roles are expected to take primary responsibility for configuring message security. In some situations, the application developer also contribute, although in the typical case either of the roles might secure an existing application without changing its implementation and therefore without involving the developer. The responsibilities of the various roles are defined in the following sections.

System Administrator Tasks

The system administrator is responsible for the following tasks:

- Configuring message security providers on the Web Server
- Managing user databases
- Managing the keystore and truststore files
- Deploying the samples program fromwsdl-soap12, which demonstrates the message layer web services security

A system administrator uses the Admin Console to manage server security settings. Web Server stores certificates and private keys in an NSS database, the administrator can manage them using certutil. For an overview of message security tasks, see “Configuring the Web Server for Message Security” on page 107.

Application Deployer Tasks

The application deployer is responsible for the following tasks:

- Specifying at application assembly any required application-specific message protection policies if such policies have not already been specified by upstream roles (the developer or assembler).
- Modifying Sun deployment descriptors to specify application-specific message protection policies information message-security-binding elements to a web service endpoint.
The application developer can setup message security but is not responsible for doing so. The system administrator can set the message security so that all Web Services are secured. The application deployer can set the message security when the provider or protection policy bound to the application must be different from that bound to the container.

**Application Developer Tasks**

The application developer or assembler is responsible for the following tasks:

- Determining whether an application-specific message protection policy is required by the application. If the policy is required, the developer or assembler works with the application deployer and ensures that the required policy is specified during application assembly.

**Security Tokens and Security Mechanisms**

The WS-Security specification provides an extensible mechanism for using security tokens to authenticate and encrypt SOAP Web Services messages. Use the SOAP-layer message security providers installed with the Web Server to employ username, password and X.509 certificate security tokens to authenticate and encrypt SOAP Web Services messages.

**Username Tokens**

The Web Server uses username tokens in the SOAP messages to establish the authentication identity of the message sender. The recipient of a message containing a Username token within an embedded password validates that the message sender is authorized to act as the user (identified in the token) by confirming that the sender knows the users secret password.

When using a Username token, a valid user database must be configured on the Web Server.

**Digital Signatures**

The Web Server uses XML Digital signatures to bind an authentication identity to the message content. Clients use digital signatures to establish their caller identity, analogous to basic authentication or SSL client certificate authentication. Digital signatures are verified by the message receiver to authenticate the source of the message content, which might be different from the sender of the message. When using digital signatures, valid keystore and truststore files must be configured on the Web Server.

**Encryption**

The purpose of encryption is to modify the data such that it can only be understood by its intended audience. This modification is accomplished by substituting an encrypted element for the original content. When predicated on public key cryptography, encryption establishes the identity of the parties who can read the message.
Message Protection Policies

Message protection policies are defined for request message processing and response message processing. These policies are expressed in terms of requirements for source or recipient authentication. A source authentication policy requires that the identity of the entity that sent a message or that defined the content of a message be established in the message so that the message receiver can authenticate it. A recipient authentication policy represents a requirement that the message be sent such that the identity of the entities that can receive the message can be established by the message sender. The providers apply specific message security mechanisms so that the message protection policies are in SOAP Web Services messages.

Request and response message protection policies are defined when a provider is configured in a container. You can also configure application-specific message protection policies at the granularity of the web service port or operation within the Sun deployment descriptors of the application or application client. Where message protection policies are defined, the request and response message protection policies of the client must match the request and response message protection policies of the server.

Securing a Web Service

Web Services deployed on the Web Server are secured by binding SOAP-layer message security providers and message protection policies to the container in which the applications are deployed or to web service endpoints served by the applications. When the Web Server is installed, SOAP-layer message security providers are configured in the server-side container of the Web Server. The container or individual applications in the container can bind to them or to individual applications in the container. During installation, the providers are configured with a simple message protection policy that, if bound to a container or to an application, would cause the source of the content in all request and response messages to be authenticated by an XML digital signature.

Use the Admin Console and CLI to perform the following tasks:

- To bind the existing providers for use by the server-side containers of the Web Server
- To modify the message protection policies enforced by the providers
- To create new provider configurations with alternative message protection policies

By default, message layer security is disabled on the Web Server. For more information about how to configure message layer security for the Web Server, see “Configuring the Web Server for Message Security” on page 107. For more information about how to use Web Services security to protect all Web Services applications deployed on the Web Server, see “Enabling Providers for Message Security” on page 42.

Once this security is established, Web Services security will be applied to all Web Services applications deployed on the Web Server.
Configuring Application-Specific Web Services Security

Configure application-specific web services during application assembly by defining message-security-binding elements in the applications Sun deployment descriptors. Use these message-security-binding elements to associate a specific provider or message protection policy with a web services endpoint or service reference. You can also qualify these elements so that they apply to a specific port or method of the corresponding endpoint or referenced service.

Admin Console Tasks for Message Security

All the steps for setting up the Web Server for using message security can be accomplished using the Admin Console or the `wadm` command-line tool. For more information on message security, see *Sun Java System Web Server 7.0 Update 6 Administrator’s Guide*.

Support for message-layer security is integrated into the Web Server in the form of pluggable authentication modules. By default, message layer security is disabled on the Web Server. The tasks in this section provide the details for enabling, creating, editing, and deleting message security configurations and providers.

- To create a message security provider
- To enable providers for message security
- To delete a message security provider
- To enable message security for stand-alone clients

In most cases, you need to restart or reconfigure the Web Server after performing these tasks, especially to apply the change to applications already deployed on Web Server.

▼ To Create a Message Security Provider

You can add or edit or modify the message protection policy. The provider type, implementation class, and provider-specific configuration properties should be modified.

1 Login to the Admin Console.

2 Select the configuration you want to modify and click Edit Configuration.

3 Click the Java tab.

4 Click the Authentication tab and scroll down to the SOAP Authentication.
   - To modify an existing provider, select the provider name and edit the values.

5 Click New to add a provider.

6 Add the new provider information
   In this page, following information is available for modification.
Note – Only Name and class Name are required. If these two fields are not specified, no authentication is applied to request or response messages. All other values are optional.

- **Name**: Identifier for this provider. You can use this identifier name to specify the default provider when using `wadm`.

- **Class Name**: The Java implementation class of the provider. Server-side providers must implement the `com.sun.enterprise.security.jauth.ServerAuthModule` interface.

The request policy defines the authentication policy requirements associated with request processing performed by the authentication provider. Type the policies in message-sender order. For example, a requirement that encryption occur after content means that the message receiver expects to decrypt the message before validating the signature.

- **Request Authentication Source**— Possible values are:
  - **sender**: Message-layer sender authentication, such as username and password
  - **content**: Content authentication, for example, digital signature
  - **null**: Source authentication of the request is not required

7 Click the Add Property button to add additional properties.

The provider shipped with the Web Server requires the server-config property. If other providers are used, refer to their documentation for more information on properties and valid values.

- **server.config**: The directory and file name of an XML file that contains the server configuration information. This file is in the following location
  `install_dir/samples/java/webapps/webservices/security/etc/wss-server-config-2.0.xml`.

8 Click OK.

**Example 3-1** To set the response policy, replace the word `request` in the following commands with `response`.

- Create a message security provider `msgsecurity-provider`:

  ```
  ../bin/wadm create-soap-auth-provider --port=8989 --user=admin
  --password-file=/tmp/admin.passwd --config=test
  --class=com.sun.xml.wss.provider.ServerSecurityAuthModule
  --request-policy-auth-source=content
  --request-policy-auth-recipient=before-content
  --request-policy-auth-recipient=before-content
  --request-policy-auth-recipient=before-content
  msgsecurity-provider
  ```
Add the required property server.config:
```
../bin/wadm set-soap-auth-provider-prop --port=8989 --user=admin
--password-file=/tmp/admin.passwd --config=test
--provider= msgsecurity-provider request-policy-auth-source=sender
```

List the provider properties:
```
../bin/wadm get-soap-auth-provider-prop --port=8989 --user=admin
--password-file=/tmp/admin.passwd --config=test
--provider= msgsecurity-provider
```

For more information about wadm commands and properties, see Sun Java System Web Server 7.0 Update 6 Administrator's Configuration File Reference.

### Enabling Providers for Message Security

You can enable the message security Web Services endpoints by specifying the default provider on the server side or by specifying in the message-binding element in sun-web.xml.

If you enable a default provider for message security, you also need an appropriate message security on the client side.

**Note** – You cannot specify a default provider using the Admin Console. You have to specify the default provider through the wadm command-line interface.

```
../bin/wadm set-config-prop --port=8989 --user=admin
--password-file=/tmp/admin.passwd --config=test
default-soap-auth-provider-name= msgsecurity-provider
```

### To Delete a Message Security Provider

1. Login to the Admin Console.
2. Select the configuration you want to modify and click Edit Configuration.
3. Click the Java tab.
4. Click the Authentication tab and scroll down to SOAP Authentication.
5. Click Delete.

#### Example 3–2

To Delete a Message Provider

To delete a message security provider through the command-line interface, type the following command:
wadm delete-soap-auth-provider --port=8989 --user=admin
--password-file=/tmp/admin.passwd --config=test msgsecurity-provider

Enabling Message Security Clients
Configure the message protection policies of client so that they are equivalent to the message protection policies of the server-side providers with which they interact. A typical stand-alone client is illustrated by the bundled sample from wsdl-soap12.

Deploying Web Services
You deploy a web service endpoint to the Web Server just as you would deploy any servlet or application. You can use the wadm deploy command to publish the web service. The Sun sun-web.xml deployment descriptor file provides optional web service enhancements using webservice-endpoint. For more information, see “Deploying the Server Configuration” in Sun Java System Web Server 7.0 Update 6 Administrator’s Guide and Java Web Services Developer Pack 2.0 (http://java.sun.com/webservices/docs/2.0/tutorial/doc/index.html).

Testing Web Services
To test Web Services you invoke a web service endpoint deployed on a web service client. A web service client is a Java program that makes a request to the service through a stub that acts as a proxy for the remote service. This stub is generated by the wsimport tool based on the WSDL file of the service.

▼ To Invoke a Web Service Client

1 WSDL of the deployed web service from URL http://host:port/context-root/endpoint?wsdl
2 Call wsimport to generate the client-side artifacts using the deployed Web Services's WSDL.
3 Implement the client to invoke the web service.

Clients can run a deployed web service by accessing its service-endpoint-address URL, which has the following format:

http://host:port/context-root/servlet-mapping-url-pattern

The context-root is defined in the web.xml file. The servlet-mapping-url-pattern is defined in the web.xml file.
In the following example, the context-root is my-ws and the servlet-mapping-url-pattern is /simple. You can view the WSDL file of the deployed service in a browser by adding ?WSDL to the end of the URL, for example,

http://localhost:8080/my-ws/simple?WSDL.

Web Services Samples

The fromwsdl-soap1 application features a simple web service that is implemented by a Java Servlet endpoint. The service endpoint interface defines a single operation, addNumbers, which takes two positive integers, and returns an integer that is the sum of the two input integers.

The fromwsdl-soap12 sample application demonstrates how to use the WS-Security functionality to secure an existing Web Services application. The instructions helps you to enable the WS-Security functionality of the Web Server so that it is used to secure the fromwsdl-soap12 application.

The fromwsdl-soap12 sample application is installed in the install_dir/samples/java/webapps/webservices/security/fromwsdl-soap12/ directory.
Developing Servlets

This chapter describes how to create servlets to control web application interactions running on a Web Server. In addition, this chapter describes the Web Server features used to augment the Java Servlet 2.5 standards.

This chapter has the following sections:

- “About Servlets” on page 45
- “Servlet Output” on page 46
- “Caching Servlet Results” on page 46
- “Maximizing Servlet Performance” on page 51
- “Servlet Internationalization Issues” on page 52
- “Migrating Legacy Servlets” on page 53

About Servlets

Servlets, like applets, are reusable Java applications. Servlets, however, run on a web server rather than in a web browser.

Servlets provide a component-based, platform-independent method for building web-based applications without the performance overheads, process limitations, and platform-specific liabilities of CGI programs.

Servlets supported by the Web Server are based on the Java Servlet 2.5 specification. Servlets are created compiled and packed into a Java web application archive WAR file and then deployed to the Web Server and managed at runtime by the servlet engine.

Basic characteristics of servlets include the following:

- Operate on input data that is encapsulated in a request object
- Respond to a query with data encapsulated in a response object
- Provide user session information persistence between interactions
Servlet Output

- Allow dynamic reloading while the server is running
- Can be addressed with URLs. For examples, buttons on an application's pages often point to servlets
- Can call other servlets and/or JSP pages

Servlet Output

By default, the System.out and System.err output of servlets is sent to the server log. During startup, server log messages are echoed to the System.err output. On Windows, no console is created for the System.err output.

You can change these defaults using the Admin Console. For more information, see “Setting Up Logging for Your Server” in Sun Java System Web Server 7.0 Update 6 Administrator's Guide.

Caching Servlet Results

Web Server can cache the results of invoking a servlet, a JSP page, or any URL pattern to make subsequent invocations of the same servlet, JSP page, or URL pattern faster. The Web Server caches the request results for a specific amount of time. In this way, if another data call occurs, the Web Server can return the cached data instead of performing the operation again. For example, if your servlet returns a stock quote that updates every 5 minutes, you set the cache to expire after 300 seconds.

If caching is enabled, Web Server can cache the results produced by the servlet javax.servlet.RequestDispatcher.include() or javax.servlet.RequestDispatcher.forward(). In Sun ONE releases, the result generated by a resource for which caching was enabled was never cached if that resource was the target of a javax.servlet.RequestDispatcher.include() or javax.servlet.RequestDispatcher.forward(). This result cached only if the resource was the target of the initial request.

```xml
<sun-web-app>
  <cache enable="true">
    <cache-mapping>
      <servlet-name>TestServlet</servlet-name>
      <dispatcher>REQUEST</dispatcher>
      <dispatcher>FORWARD</dispatcher>
    </cache-mapping>
  </cache>
</sun-web-app>
```

Whether to cache results and how to cache them depends on the data involved. For example, you do not need to cache the results of a quiz submission because the input to the servlet is
different each time. However, you could cache a high-level report showing demographic data taken from quiz results that is updated once an hour.

You can define how a Web Server web application handles response caching by editing specific fields in the sun-web.xml file. In this way, you can create programmatically standard servlets that still take advantage of this feature.

For more information about JSP caching, see “JSP Cache Tags” on page 61.

**Features of Caching**

Web Server has the following web application response caching capabilities:

- Caching is configurable based on the servlet name or the URI.
- When caching is based on the URI, the URI can include user-specified parameters in the query string. For example, a response from /garden/catalog?category=roses is different from a response from /garden/catalog?category=lilies. These responses are stored under different keys in the cache.
- Cache size, entry timeout, and other caching behaviors are configurable.
- Entry timeout is measured from the time an entry is created or refreshed. You can override this timeout for an individual cache mapping by specifying the cache-mapping element `timeout`.
- You can determine caching criteria programmatically by writing a cache helper class. For example, if a servlet only stores the time when a back-end data source was last modified, you can write a helper class to retrieve the last-modified timestamp from the data source and decide whether to cache the response based on that timestamp. See “CacheHelper Interface” on page 48.
- You can determine cache key generation programmatically by writing a cache key generator class. See “CacheKeyGenerator Interface” on page 50.
- All non-ASCII request parameter values specified in cache key elements must be URL encoded. The caching subsystem attempts to match the raw parameter values in the request query string.
- The newly updated classes affect data what gets cached. The web container clears the cache during dynamic deployment or reloading of classes.
- The following `HttpServletRequest` request attributes are:
  - `com.sun.appserv.web.cachedServletName`, the cached servlet target
  - `com.sun.appserv.web.cachedURLPattern`, the URL pattern being cached
Default Cache Configuration

If you enable caching but do not provide any special configuration for a servlet or JSP page, the default cache configuration is as follows:

- The default cache timeout is 30 seconds.
- Only the HTTP GET method is eligible for caching.
- HTTP requests with cookies or sessions automatically disable caching.
- No special consideration is given to Pragma:, Cache-control:, or Vary: headers.
- The default key consists of the servlet path minus pathInfo and the query string.
- A least-recently-used list is maintained to delete cache entries if the maximum cache size is exceeded.
- Key generation concatenates the servlet path with key field values, if any are specified.

CacheHelper Interface

The CacheHelper interface includes the following information:

```java
package com.sun.appserv.web.cache;
import java.util.Map
import javax.servlet.ServletContext;
import javax.servlet.http.HttpServletRequest;
/** CacheHelper interface is an user-extensible interface to customize:
 * a) the key generation b) whether to cache the response. */
public interface CacheHelper {
    // name of request attributes
    public static final String ATTR_CACHE_MAPPED_SERVLET_NAME =
            "com.sun.appserv.web.cachedServletName";
    public static final String ATTR_CACHE_MAPPED_URL_PATTERN =
            "com.sun.appserv.web.cachedURLPattern";
    public static final int TIMEOUT_VALUE_NOT_SET = -2;
    /** initialize the helper
     * @param context the web application context this helper belongs to
     * @exception Exception if a startup error occurs */
    public void init(ServletContext context, Map props) throws Exception;
    /** getCacheKey: generate the key to be used to cache this request
     * @param request incoming <code>HttpServletRequest</code> object
     * @returns the generated key for this requested cacheable resource. */
    public String getCacheKey(HttpServletRequest request);
    /** isCacheable: is the response to given request cacheable?
     * @param request incoming <code>HttpServletRequest</code> object
     * @returns true if the generated key is not null and it is not the default value */
    public boolean isCacheable(HttpServletRequest request);
}
```
Caching Example

The following example cache element in the sun-web.xml file:

```xml
<cache max-capacity="8192" timeout="60">
  <cache-helper name="myHelper" class-name="MyCacheHelper"/>
  <cache-mapping>
    <servlet-name>myservlet</servlet-name>
    <timeout name="timefield">120</timeout>
    <http-method>GET</http-method>
    <http-method>POST</http-method>
  </cache-mapping>
  <cache-mapping>
    <url-pattern> /catalog/* </url-pattern>
    <!-- cache the best selling category; cache the responses to
    -- this resource only when the given parameters exist. Cache
    -- only when the catalog parameter has lilies or roses
    -- but no other catalog varieties:
    -- /orchard/catalogbest&category=lilies
    -- /orchard/catalogbest&category=roses
    -- but not the result of
    -- /orchard/catalog?best&category=wild
  </cache-mapping>
</cache>
```

```java
public boolean isCacheable(HttpServletRequest request); /*
* @returns <code>true</code> if the response could be cached. or
* <code>false</code> if the results of this request must not be cached.
* /
public boolean isCacheable(HttpServletRequest request);
/** isRefreshNeeded: is the response to given request to be refreshed?
* @param request incoming <code>HttpServletRequest</code> object
* @returns <code>true</code> if the response needs to be refreshed.
* or return <code>false</code> if the results of this request
* dont need to be refreshed.
* /
public boolean isRefreshNeeded(HttpServletRequest request);
/** get timeout for the cached response.
* @param request incoming <code>HttpServletRequest</code> object
* @returns the timeout in seconds for the cached response; a return
* value of -1 means the response never expires and a value of -2 indicates
* helper cannot determine the timeout (container assigns default timeout)
* /
public int getTimeout(HttpServletRequest request);
/**
* Stop the helper from active use
* @exception Exception if an error occurs
* /
public void destroy() throws Exception;
}
```
CacheKeyGenerator Interface

The built-in default CacheHelper implementation enables web applications to customize the key generation. An application component in a servlet or JSP can set up a custom CacheKeyGenerator implementation as an attribute in the ServletContext.

The name of the context attribute is configurable as the value of the cacheKeyGeneratorAttrName property in the default-helper element of the sun-web.xml deployment descriptor. For more information, see “default-helper” on page 173.

The CacheKeyGenerator interface contains the following information:

```java
package com.sun.appserv.web.cache;
import javax.servlet.ServletContext;
import javax.servlet.http.HttpServletRequest;
/** CacheKeyGenerator: a helper interface to generate the key that
is used to cache this request.
* Name of the ServletContext attribute implementing the
* CacheKeyGenerator is configurable via a property of the
* default-helper in sun-web.xml:
*/
```
Maximizing Servlet Performance

Consider the following guidelines for improving servlet performance:

- Increase the Java heap size to help garbage collection. The Java heap size can be adjusted by adjusting the values specified to the -Xms and -Xmx jvm- options in server.xml. For example, <jvm-options>-Xms128m-Xmx256m</jvm-options> sets the minimum Java heap size to 128 MB and 256 MB. For more information, see Sun Java System Web Server 7.0 Update 6 Administrator's Guide.

  For information on tuning the Garbage Collector see, “Managing Memory and Garbage Collection” in Sun Java System Web Server 7.0 Update 6 Performance Tuning, Sizing, and Scaling Guide.

- Set the stack space if applications use deep recursion, or in any cases where very complex JSP pages are used.

  You can set the stack space using set-thread-pool-prop wadm command. For example, $wadm set-thread-pool-prop [other args] stack-size=544288. For more information, see Sun Java System Web Server 7.0 Update 6 NSAPI Developer’s Guide.

- Create servlet sessions only if required as the Session ID generator employs cryptographically unique random number generation algorithms. While sessions are being created, limit the size of sessions and configure them depending on whether the application uses short-lived or long-lived sessions. For more information on optimal session configuration, see “Configuring the Web Application’s Session Settings” in Sun Java System Web Server 7.0 Update 6 Performance Tuning, Sizing, and Scaling Guide.
Servlet Internationalization Issues

- Use servlet cache when possible. For more information, see "Caching Servlet Results" on page 46.
- Use precompiled JSPs if the JSPs do not change after deployment to the Web Server. The precompiled JSPs should include the reload-interval property setting in the jsp-config element in sun-web.xml. This eliminates time-consuming compilation and periodic checking by the Web Server.
- Reduce the number of directories in the classpath.
- Disable dynamic reloading.
- Disable the Java Security Manager.

For more information about maximizing servlet and JSP performance, see “Tuning Java Web Application Performance” in Sun Java System Web Server 7.0 Update 6 Performance Tuning, Sizing, and Scaling Guide.

For more information about container setting to maximize performance, see “Tuning Web Container Within Web Server 7.0” in Sun Java System Web Server 7.0 Update 6 Performance Tuning, Sizing, and Scaling Guide.

Servlet Internationalization Issues

This section describes how Web Server determines the character encoding for the servlet request and the servlet response. For information about encodings, see http://java.sun.com/j2se/1.5.0/docs/guide/intl/encoding.doc.html.

Servlet Request

When processing the servlet request, the server uses the following order of precedence, first to last, to determine the character encoding for the request parameters:

1. The ServletRequest.setCharacterEncoding() method.
2. A hidden field in the form, if specified using the form-hint-field attribute of the parameter-encoding element in the sun-web.xml file. For more information about this element, see "parameter-encoding Element" on page 183.
3. The character encoding specified in the default-charset attribute of the parameter-encoding element in the sun-web.xml file. For more information about this element, see "parameter-encoding Element" on page 183.

Servlet Response

When processing a servlet response, the server uses the following order of precedence, first to last, to determine the response character encoding:
1. The `ServletResponse.setContentType()` method or the `ServletResponse.setLocale()` method.
2. The default encoding, which is ISO-8859–1.

To specify the character encoding that should be set in the Content-type header of the response if the response locale is set using the `ServletResponse.setLocale` method, use the `locale=charset-map` under the `locale=charset-info` element in the `sun-web.xml` file. For more information about this element, see “`locale=charset-info` Element” on page 183.

---

Migrating Legacy Servlets

Netscape Enterprise Server/iPlanet Web Server versions 4.0 and 4.1 supported the Java Servlet 2.1 specification. This specification did not include web applications. A deployment scheme was developed to make servlet deployment simpler. With the advent of Java web applications (WAR files) and their deployment descriptors, maintaining a proprietary deployment system is no longer necessary.

iPlanet Web Server 6.0 supported both types of deployment schemes, but the 4.x implementation (referred to as legacy servlets) was marked as deprecated (See Chapter 8 Legacy Servlet and JSP Configuration of the iPlanet Web Server, Enterprise Edition Programmer’s Guide to Servlets).

Web Server versions 6.1 and 7.0 no longer support legacy servlets. The legacy properties files for the server you want to migrate (`servlet.properties`, `context.properties`, and `rules.properties`) are removed during migration.

Because no one-to-one mapping is possible for all of the features, legacy servlets cannot be migrated automatically. This section describes the main features involved in migrating legacy servlets to web applications.

This section includes the following topics:

- ”JSP file by Extension” on page 53
- ”Servlet by Extension of Servlet by Directory” on page 54
- ”Registering Servlets” on page 54

---

JSP file by Extension

In Web Server, JSP file by extension works as it did in previous releases. Any file name in the document tree with a suffix of `.jsp` is treated as a JSP environment as long as the Java is turned on for the virtual server.
Servlet by Extension of Servlet by Directory

Servlet extension is not supported in Web Server. You can deploy a web application to respond to a directory, but all of the servlets must be in the WEB-INF/classes directory of the web application. You can no longer copy a servlet in the .class file into the document tree and have it run as a servlet or have all of the contents of a directory run as a servlet. The web application treats only .class files as servlets.

Registering Servlets

The legacy servlet system used a two-step process of registering servlets (servlet.properties) and mapping them to a URL (rules.properties). In Web Server, the servlets must be moved into a web application. These settings will be maintained in the web.xml file of that web application.

A registered servlet has entries in both the servlet.properties and rules.properties files.

The following example uses a servlet file called BuyNow1A.class, which responds to /buynow. It is assumed that the web application is deployed at '/'

The servlet.properties file containing:

```
EXAMPLE 4–1  Registering Servlets Example

servlet.BuyNowServlet.classpath=D:/Netscape/server4/docs/
servlet/buy;D:/Netscape/server4/docs/myclasses
servlet.BuyNowServlet.code=BuyNow1A
servlet.BuyNowServlet.initArgs=arg1=45, arg2=online, arg3="quick shopping"
```

The rules.properties file has:

```
/buynow=BuyNowServlet
```

These settings must be translated to a web.xml setting. The servlet.properties setting translates into the servlet element.

The classpath is automated so no classpath setting is necessary. All classes to be used must be in the WEB-INF/classes directory or in a .jar file in the WEB-INF/lib directory of the web application.

The servlet-name element appears between the dots in the servlets.properties file. The code translates to the servlet-class. IntArgs translate to init-params. This entry will translate to the following entry:

```
<servlet>
  <servlet-name> BuyNowServlet </servlet-name>
  <servlet-class> BuyNow1A </servlet-class>
```
EXAMPLE 4–1  Registering Servlets Example  (Continued)

    <init-param>
      <param-name> arg1 </param-name>
      <param-value> 45 </param-value>
    </init-param>
    <init-param>
      <param-name> arg2 </param-name>
      <param-value> online </param-value>
    </init-param>
    <init-param>
      <param-name> arg3 </param-name>
      <param-value> 'quick shopping' </param-value>
    </init-param>
  </servlet>

The rules.properties entries translate to servlet-mapping elements. This entry translates to the following entry:

  <servlet-mapping>
    <servlet-name> BuyNowServlet </servlet-name>
    <url-pattern> /buynow </url-pattern>
  </servlet-mapping>

Some other entries in the servlet.properties file map to the web.xml file. This includes the following information:

- Servlets.startup: This servlet should contain the load-on-startup element.
- Servlets.config.reloadInterval: This setting translates to the dynamicreloadinterval attribute of the jvm element in servlet.xml. This instance-wide setting affects all virtual servers and all web applications.
- Servlet.sessionmgr: This element translates to the session-manager element in the sun-web.xml.
This chapter describes how to use JavaServer Pages (JSP™) page templates in a Web Server application.

This chapter has the following sections:

- "Introducing JSPs" on page 57
- “Compiling JSPs Using the Command-Line Compiler” on page 58
- “Debugging JSPs” on page 61
- "JSP Tag Libraries and Standard Portable Tags” on page 61
- "JSP Cache Tags” on page 61
- "JSP Search Tags” on page 65
- "JSP Internationalization Issues” on page 73

Introducing JSPs

JSPs are browser pages in HTML or XML. These pages contain Java code, which enables them to perform complex processing, conditionally output, and communicate with other application objects. JSPs in Web Server are based on the JSP 2.1 specification.

In a Web Server application, you can call a JSP from a servlet to handle the user interaction output. Because JSPs have the same application environment access as any other application component, you can use a JSP as an interaction destination.

JSPs are made up of JSP elements and template data. Template data is anything not in the JSP specification, including text and HTML tags. For example, minimal JSP file requires no processing by the JSP engine and is a static HTML page.

Web Server compiles JSPs into HTTP servlets the first time they are called or they can be precompiled for better performance. This processing makes them available to the application environment as standard objects and enables them to be called from a client using a URL.
JSPs run inside the Web Server JSP engine, which is responsible for interpreting tags that are specific to JSP and performing the actions they specify in order to generate dynamic content. This content, along with any template data surrounding it, is assembled into an output page and is returned to the caller.

Compiling JSPs Using the Command-Line Compiler

Web Server provides the following ways of compiling JSP 2.1-compliant source files into servlets:

- JSP are automatically compiled at runtime.
- The jspc command-line tool, described in this section, enables you to precompile JSPs at the command line.

You must disable dynamic reloading of JSP when deploying a web application archive that has precompiled JSP without the corresponding jsp source files. To do this, set the reload-interval property to -1 in the jsp-config element of the sun-web.xml file. For more information, see "JSP Element" on page 180.

The jspc command-line tool is located under install_dir/bin. The format of the jspc command is as follows:

```
jspc [options] file_specifier
```

The following table shows what file_specifier can contain in the jspc command.

<table>
<thead>
<tr>
<th>File Specifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>files</td>
<td>One or more JSP files to be compiled.</td>
</tr>
<tr>
<td>-webapp dir</td>
<td>A directory containing a web application. All JSPs in the directory and its subdirectories are compiled. You cannot specify a WAR, JAR, or ZIP file. You must first extract such files to an open directory structure.</td>
</tr>
</tbody>
</table>

The following table shows the basic options for the jspc command.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-help</td>
<td>Enables quiet mode (same as -v0). Only fatal error messages are displayed.</td>
</tr>
<tr>
<td>-v</td>
<td>Verbose mode.</td>
</tr>
</tbody>
</table>
### TABLE 5-2  Basic jspc Options  (Continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-d dir</td>
<td>Specifies the output directory for the compiled JSPs. Package directories are automatically generated based on the directories containing the uncompiled JSPs. The default top-level directory is the directory from which jspc is invoked.</td>
</tr>
<tr>
<td>-l</td>
<td>Specifies the name of the JSP on failure.</td>
</tr>
<tr>
<td>-s</td>
<td>Specifies the name of the JSP on success.</td>
</tr>
<tr>
<td>-p name</td>
<td>Specifies the name of the target package for all specified JSPs, overriding the default package generation performed by the -d option.</td>
</tr>
<tr>
<td>-c name</td>
<td>Specifies the target class name of the first JSP compiled. Subsequent JSPs are unaffected.</td>
</tr>
<tr>
<td>-mapped</td>
<td>Generates separate write() calls for each HTML line in the JSP.</td>
</tr>
<tr>
<td>die(#)</td>
<td>Generates an error return code (#) on fatal errors (default 1).</td>
</tr>
</tbody>
</table>
| -uribase dir | Specifies the URI directory to which compilations are relative. Applies only to explicitly declared JSP files. This path is the location of each JSP file relative to the uriroot. If this location cannot be determined, the default is /.
| -uriroot dir | A directory containing a web application. All JSPs in the directory and its subdirectories are compiled. You cannot specify a WAR, JAR, or ZIP file. You must first extract such files to an open directory structure. |
| -compile     | Compiles the generated servlets.                                               |
| -genclass    | Generates class files in addition to Java files.                               |
| -webinc file | Creates a partial servlet mappings in the file.                               |
| -web.xml file | Creates a complete web.xml structure in the file.                            |
| -ieplugin clsid | Java Plug-in classid for Internet Explorer.                            |
| classpath path | Overrides the java.class.path system property                        |
| xppoweredBy | Add the X-Powered-By response header.                                          |
| -trimSpaces | Trims spaces in text templates between actions and directives.               |
| -smap        | Generates SMAP info for JSR 45 debugging.                                      |
| -dumpmap     | Dumps SMAP info for JSR45 debugging into a file.                              |
| -compilerSourceVM release | Provides source compatibility with specified JDK™ release.       |
| -compilerTargetVM release | Generates class files for specified VM version.                              |
For example, this command compiles the hello JSP file and writes the compiled JSP under hellodir:

```shell
jspc -d hellodir -genclass hello.jsp
```

This command compiles all of the JSP files in the web application under webappdir into class files under jspclassdir:

```shell
jspc -d jspclassdir -genclass -webapp webappdir
```

To use either of these precompiled JSPs in a web application, put the classes under hellodir or jspclassdir into a JAR file, place the JAR file under WEB-INF/lib, and set the reload-interval property to -1 in the sun-web.xml file.

### Package Names Generated by the JSP Compiler

When a JSP is compiled, a package is created for it. The package name starts with jspc. For example, the generated package name for ~/SOURCE/JSP/myjsps/hello.jsp is precompiled as

```shell
jspc -webapp ~/SOURCE -d ~/test1/test2/test3
```

The generated servlet is located in

```shell
~/test1/test2/test3/org/apache/jsp/JSP/myjsps/hello_jsp.java
```

and defined in

```shell
org.apache.jsp.JSP.myjsps
```

The path for hello.jsp is derived from the directory in which the JSP is located.

In another example, the same hello.jsp is precompiled using the -p option, and is precompiled as

```shell
jspc -webapp ~/SOURCE -d ~/test1/test2/test3 -p app1.app2.app3
```

The generated servlet is located in

```shell
~/test1/test2/test3/app1/app2/app3/JSP/myjsps/hello_jsp.java
```

and defined inside package

```shell
app1.app2.app3.JSP.myjsps
```

Note that the package specified with the -p option (app1.app2.app3) overrides the standard org.apache.jsp but does not affect the package derived from the directory in which the JSP is located. Also, note that the -d option does not affect on the generated package name.

### Other JSP Configuration Parameters

For information about the various JSP configuration parameters you can use, see the section “jsp-config Element” on page 180. The JSP compiler uses the default values for parameters that are not included in the file.
Debugging JSPs

When you use Sun Java Studio Enterprise 8.1 to debug JSPs, you can set breakpoints in a JSP. For information about setting up debugging in Sun Java Studio Enterprise 8.1, see “Using Developer Tools for Debugging” on page 137.

JSP Tag Libraries and Standard Portable Tags

Web Server supports tag libraries and standard portable tags. For more information about tag libraries, see the JSP 2.1 specification at http://java.sun.com/products/jsp/download.html.

JSP Cache Tags

JSP cache tags enable you to cache JSP page fragments within the Java engine. Each fragment can be cached using different cache criteria. For example, suppose you have page fragments to view stock quotes and weather information. The stock quote fragment can be cached for 10 minutes, the weather report fragment for 30 minutes, and so on.

For more information about response caching as it pertains to servlets, see “Caching Servlet Results” on page 46.

JSP caching uses the custom tag library support provided by JSP 2.1. JSP caching is implemented by a tag library packaged into the install_dir/lib/.jar file, which is always on the server classpath. The sun-web-cache.tld tag description file is in the install_dir/lib/tlds directory and can be copied into the WEB-INF directory of your web application.

JSP caching is available in three different scopes: request, session, and application. The default is application.

To use a cache with the request scope, a web application must specify the com.sun.appserv.web.taglibs.cache.CacheRequestListener in its deployment descriptor, as follows:

```xml
<listener>
  <listener-class>
    com.sun.appserv.web.taglibs.cache.CacheRequestListener
  </listener-class>
</listener>
```

To use a cache in session scope, a web application must specify the com.sun.appserv.web.taglibs.cache.CacheSessionListener in its deployment descriptor, as follows:

```xml
<listener>
  <listener-class>
    com.sun.appserv.web.taglibs.cache.CacheSessionListener
  </listener-class>
</listener>
```
To use a cache with the application scope, a web application does not need to specify any listener. The com.sun.appserv.web.taglibs.cache.CacheContextListener is already specified in the sun-web-cache.tld file.

The JSP cache tags are as follows:
- “cache Tag” on page 62
- “flush Tag” on page 64

**cache Tag**

The cache tag enables you to cache fragments of your JSP pages. It caches the body between the beginning and ending tags according to the attributes specified. The first time the tag is encountered, the body content is executed and cached. Each subsequent time it is run, the cached content is checked to see whether it needs to be refreshed. If so, it is executed again, and the cached data is refreshed. Otherwise, the cached data is served.

**Attributes**

The following table describes attributes for the cache tag.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>key</td>
<td>servletPath_suffix</td>
<td>(Optional) The name used by the container to access the cached entry. The cache key is added to the servlet path to generate a key to access the cached entry. If no key is specified, a number is generated according to the position of the tag in the page.</td>
</tr>
<tr>
<td>timeout</td>
<td>60s</td>
<td>(Optional) The time in seconds after which the body of the tag is executed and the cache is refreshed. By default, this value is interpreted in seconds. To specify a different unit of time, add a suffix to the timeout value as follows: s for seconds, m for minutes, h for hours, and d for days. For example, 2h specifies two hours.</td>
</tr>
</tbody>
</table>
TABLE 5–3  cache Attributes  (Continued)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>nocache</td>
<td>false</td>
<td>(Optional) If set to true, the body content is executed and served as if no cache tag is active. This offers a way to programmatically decide whether the cached response should be sent or whether the body must be executed, even if the response is not cached.</td>
</tr>
<tr>
<td>refresh</td>
<td>false</td>
<td>(Optional) If set to true, the body content is executed and the response is cached again. This setting enables you to let you programmatically refresh the cache immediately, regardless of the timeout setting.</td>
</tr>
<tr>
<td>scope</td>
<td>application</td>
<td>Specifies the scope of the cache. Valid values are request, session, and application.</td>
</tr>
</tbody>
</table>

Example
The following example represents a cached JSP page.

```jsp
<%@ taglib prefix="mypfx" uri="/com/sun/web/taglibs/cache" %>
<%
    String cacheKey = null;
    if (session != null)
        cacheKey = (String)session.getAttribute("loginId");
    // check for nocache
    boolean noCache = false;
    String nc = request.getParameter("nocache");
    if (nc != null)
        noCache = "true";
    // force reload
    boolean reload=false;
    String refresh = request.getParameter("refresh");
    if (refresh != null)
        reload = true;
    %>
    <mypfx:cache key="<%= cacheKey %>/" nocache="<%= noCache %>/" refresh="<%= reload %>/" timeout="10m"/>
    <%
    String page = request.getParameter("page");
    if (page.equals("frontPage") {
        // get headlines from database
    } else {
        ...
    %>
    </mypfx:cache/>
    <mypfx:cache timeout="1h"/>
    <h2> Local News </h2>
    <%
// get the headline news and cache them
</mypfx:cache/>

flush Tag

This tag forces the cache to be flushed. If a key is specified, only the entry with that key is flushed. If no key is specified, the entire cache is flushed.

Attributes

The following table describes attributes for the flush tag. The left column lists the attribute name, the middle column indicates the default value, and the right column describes what the attribute does.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>key</td>
<td>servletPath_suffix</td>
<td>(Optional) The name used by the container to access the cached entry. The cache key is added to the servlet path to generate a key to access the cached entry. If no key is specified, a number is generated according to the position of the tag in the page.</td>
</tr>
<tr>
<td>scope</td>
<td>application</td>
<td>Specifies the scope of the cache. Valid values are request, session, and application.</td>
</tr>
</tbody>
</table>

Examples

To flush the entry with key="foobar":

<mypfx:flush key="foobar"/>

To flush the entire cache:

<% if (session != null && session.getAttribute("clearCache") != null) { %>
   <mypfx:flush />
<% } %/
JSP Search Tags

Web Server includes a set of JSP tags that can be used to customize the search query and search results pages in the search interface. This section describes the tags and how they are used.

The search tag library is packaged into the `install_dir/lib/webserv-rt.jar` file, which is always on the server classpath. The `sun-web-search.tld` tag description file can be found in the `install_dir/lib/tlds` directory, you can copy this file into the WEB-INF directory of your web application.

The search tags are as follows:

- "searchForm Tag" on page 65
- "CollElem Tag" on page 66
- "collection Tag" on page 67
- "colIItem Tag" on page 68
- "queryBox Tag" on page 68
- "submitButton Tag" on page 69
- "formAction Tag" on page 69
- "formSubmission Tag" on page 70
- "formActionMsg Tag" on page 70
- "search Tag" on page 71
- "resultIteration Tag" on page 71
- "Item Tag" on page 72
- "resultStat Tag" on page 72
- "resultNav Tag" on page 72

**Note** – The Web Server search feature is compliant for internalization, and supports multiple character encoding schemes in the same collection. Custom JSPs that expose search can be in any encoding.

**searchForm Tag**

This tag constructs an HTML form that contains default, hidden form elements such as the current search result index and number of records per page by default. The default names for the form, index, and number of records are `searchform`, `si`, and `ns`.

**Attributes**

The searchForm tag uses the following attributes:

- Name - Specifies the name of the form. The default is `searchform`. The name of a form is the identifier for all other tags.
- Action (Optional) - Specifies the form action.
- Method (Optional) - Specifies the method of submission, GET or POST. The default is GET.
- elemStart (Optional) - Specifies the name of the hidden Start element. If not specified, the
default si will be used.
- Start (Optional) - An integer indicating the starting index for displaying the search result.
The default is 1.
- elemNumShown (Optional) - The name of the nShown element. If not specified, the default
ns is used.
- numShown (Optional) - An integer indicating the number of results to be shown per page.
The value of the attribute will be retrieved by requesting parameter elemNumShown. The
default is 10.

Usage
<s1ws:form action="results.jsp" />
...
</s1ws:searchForm>

This example creates an HTML form tag <form action="results.jsp" method="GET">, along with two hidden input boxes:
- A hidden input box for starting the index named si with a value from the si parameter or
default 1
- A hidden input box for the number of records per page named ns with a value from the ns
parameter or default 20

CollElem Tag

This tag creates a hidden inputbox or select box, or multiple checkboxes, depending on the
attribute input. If only one collection exists, the tag will create a hidden inputbox by default.

Attributes

The CollElem tag uses the following attributes:
- Name- Specifies the name of the form element created. The default is c.
- Items (Optional) - A comma-delimited string representing search collections available. The
tag retrieves all collections available on the server if the attribute is empty.
- Type (Optional) - The type of form element used for displaying collections. Valid options
are hidden, select, and checkbox. The default value is hidden if one collection exists, and
checkbox if there are multiple collections.
- Rows (Optional) - Represents size if the type is select, or the number of rows. The default
behavior is to satisfy the Cols attribute first. That is, the collections will be listed in columns
as specified by the Cols attribute.
- **Cols** - Represents number of columns and is only required if type is checkbox. If Cols and Rows are not specified, the collections will be listed horizontally.
- **Defaults** - Specifies a comma-delimited string containing 1s or 0s indicating the selection status of the search collections. An item is selected if the setting is 1, and not selected if the setting is 0. If there is a form action exists, these values will be retrieved from the form elements.
- **cssClass (Optional)** - The class name used in every HTML tag created in this tag. This attribute is particularly useful when the type is checkbox, since an HTML table is used for the layout. See the sample code for details.

**Usage**
```
<s1ws:collElem type="checkbox" cols="2" values="1,0,1,0" cssClass="body"/>
```

This example creates checkboxes in 2 columns with a default name c with the first and third items selected. Fonts and any other HTML styles are defined in the css class body, which includes tr.body, td.body, and input.body.

**collection Tag**

This tag retrieves the name of the search collections on the server, iterates through them, and passes each of them to the collectionItem tag. Use this tag with collection item tags write your own HTML search collections.

**Attributes**

Optional - A comma-delimited string representing the search collections available. The tag retrieves all collections available on the server if the attribute is empty.

**Usage**
```
<table border=0>
  <s1ws:collection>
    <tr><td><input type=checkbox name="c" value="s1ws:collItem property="name" />
    <s1ws:collItem property="display name" />
    </td></tr>
  </s1ws:collection>
</table>
```

The above code will display all collections with checkboxes.
```
<select name=elementname>
  <s1ws:collection>
    <option value="s1ws:collItem property="name" />
  </s1ws:collection>
</select>
```
This function iterates through the available collections and passes each item to the collection item tag, which in turn displays the name and display name of the item.

**colItem Tag**

This tag displays the name and label of one collection item. This tag must be used inside the collection tag.

**Attributes**

Property - Specifies a keyword indicating which property the tag should output. Valid inputs include name, display name, and description. Default is name.

**Usage**

```xml
<select name=elementname>
    <slws:collection>
        <option value="<slws:colItem property="name" />"></slws:colItem>
        <option value="<slws:colItem property="display name" />"></slws:colItem>
    </slws:collection>
</select>
```

This function iterates through the available collections and passes each item to the collection item tag, which in turn displays the name and display name of the item.

**queryBox Tag**

This tag creates an input box.

**Attributes**

The `queryBox` tag uses the following attributes:

- name. (Optional) The name of the input box. The default is `qt`.
- default. (Optional) The default value for the query box. If the form is submitted, its value will be set using this setting.
- size. (Optional) The size of the input box. The default is 50.
- maxlength. (Optional) The `maxlength` of the input box. The default is 50.
- cssClass. (Optional) The CSS class.
Usage

<s1ws:queryBox size="30"/>

This example creates an input box with default name qt and size=30.

submitButton Tag

This tag creates a submit button.

Attributes

The submitButton tag uses the following attributes:

- name. (Optional) The name of the button. The default is sb.
- default. (Optional) The default value of the button, which will be searched.
- cssClass. (Optional) The CSS class name.
- style. The CSS style.
- image. The optional image for the button.

Usage

<s1ws:submitButton cssClass="navBar" style="padding: 0px; margin: 0px; width: 50px"> This example creates a submit button with default name sb.

formAction Tag

This tag performs the following sections:

- This tag handles form action.
- It retrieves all elements on the search form.
- Validates that there is at least one collection is selected and the query is not empty, and passes the values on to search and results tags as parents or through the page context.

Attributes

The formAction tag uses the following attributes:

- formId. Specifies the name of the form. If not specified, the default form searchForm will be used.
- ElemColl. (Optional) The name of the Collection element. The default name c is used.
- elemQuery. (Optional) The name of the Start element. The default name qt is used.
- elemStart. (Optional) The name of the Start element. The default name si is used.
- elemNumShown. (Optional) The name of the numShown element. The default name ns is used.

**Usage**

```html
<s1ws:formAction />
```

**formSubmission Tag**

This tag tests whether the form submission is successful.

**Attributes**

The formSubmission tag uses the following attributes:

- formId. Specifies the name of the form in question. This name must be the name assigned with `<formAction>`.
- success. Indicates if the form submission is successful. The values true or yes represents successful action. All other inputs are rendered as failure.

**Usage**

```html
<s1ws:formSubmission success="true">
    <s1ws:search>
        ...
    </s1ws:search>
</s1ws:formSubmission>
```

**formActionMsg Tag**

This tag prints out an error message from formAction, if any.

**Attributes**

The formActionMsg tag uses the following attributes:

- formId. (Optional) Specifies the name of the form in question. If not specified, the default ID is searchForm.
- elem. (optional) Specified the name of the element. Valid inputs are query and collection. When specified, the tag returns an error message, if any, regarding the element. Otherwise, all of the error messages generated are printed out.
Usage

<FormActionMsg elem="query">

This tag displays the message query text not specified if a query is not submitted.

The message is printed from the form action where the tag is placed.

search Tag

This tag executes a search query and returns search results. The search tag retrieves a query string and collections from either a form parent tag or the query and collection attributes. The search results are saved in the page context with a page or session scope.

Attributes

The search tag uses the following attributes:

- formId. Specifies the name of the form used for the search. The default form is used if the attribute is left empty. If this tag is used without a form, this attribute must be set to provide an identifier for the resultIterate tag.
- collection. (Optional) A comma-delimited string representing collections used for a search. If form action exists, this attribute is ignored and the values are retrieved by requesting the collection element.
- query. (Optional) Specifies the query text. If not provided, the text is retrieved from the query element.
- scope. Specifies an integer indicating the scope of the search results. The value 1, which is the default, indicates page scope. 2 indicates session scope.

Usage

<s1ws:search />

This search tag uses the default parameters and executes a search. The search results are saved in pageContext with a page scope.

<s1ws:search Collection="col1, col2" Query="Java Web Service" scope="2" /></s1ws:search>

This search tag executes a search in col1 and col2 using "Java Web Service" as the query string. The search results are saved in pageContext with a session scope.

resultIteration Tag

This tag retrieves the search results from either the parent search tag or the page context. The tag iterates through the results and passing the search items to the item tags.
Attributes
The resultIteration tag uses the following attributes:

- **formId**: Specifies the name of the form associated with the search results. The default form is used if the attribute is left empty. If this tag is used without a form, this attribute must be set as a reference to the search tag.
- **start**: Specifies an integer representing the starting position in the search results. The default is 0. The value is retrieved from the parent formAction tag or pageContext, or the parameter value.
- **numShown**: Specifies an integer indicating the number of results to be shown in one page. The default is 20. The value is retrieved from the parent formAction tag or pageContext.

Item Tag
This tag retrieves a search item from the Results parent tag and outputs its properties as specified by the property attribute.

Attributes
Property. Specifies a case-sensitive string representing field names in a search item, such as title, number, score, filename, URL, size, and date.

resultStat Tag
This tag returns numbers indicating number of records returned and the range currently displayed.

Attributes
The resultStat tag uses the following attributes:

- **formId**: Specifies the name of the form associated. The default form is used if the attribute is left empty. If this tag is used without a form, this attribute must be set as a reference to the search tag.
- **type**: Specifies the type of statistics data. Valid inputs are start, end, range (for example, 1-20), and total.

resultNav Tag
This tag creates a navigation bar.
Attributes

The `resultNav` tag uses the following attributes:

- **formId**: Specifies the name of the form associated with the navigation bar. The default form is used if the attribute is left empty. If this tag is used without a form, this attribute must be set as a reference to the search tag.

- **type**: Specifies the type of navigation bar. Valid values are full, previous, and next. A full navigation bar appears as follows: previous 1 2 3 4 5 6 7 8 9 10 next, where 5 is currently selected. The number of page number links is determined by the `offset` attribute and the number of pages available.

- **caption**: Only necessary if the type is previous or next and the default text is not needed. `caption` can be any HTML file.

- **offset**: Specifies the number of page links around the selected page. For example, if `offset=2`, the navigation bar would appear as follows: previous 3 4 5 6 7 next. Only required for type "full."

JSP Internationalization Issues

This section covers internationalization as it applies to the JSPs.

JSP Character Encoding

A JSP page uses a character encoding. For valid encodings to use, see [http://java.sun.com/j2se/1.5.0/docs/guide/intl/encoding.doc.html](http://java.sun.com/j2se/1.5.0/docs/guide/intl/encoding.doc.html).

The encoding can be described explicitly using the `pageEncoding` attribute of the `page` directive. The character encoding defaults to the encoding indicated in the `contentType` attribute of the `page` directive, if it is given.
Session objects maintain state and user identity across multiple page requests over the normally stateless HTTP protocol. A session persists for a specified period of time, across more than one connection or page request from the user. A session usually corresponds to one user, who might visit a site many times. The server can maintain a session either by using cookies or by rewriting URLs. Servlets can access the session objects to retrieve state information about the session.

This chapter describes sessions and session managers, and has the following sections:
- "Introducing Sessions" on page 75
- "Using Sessions" on page 77
- "Session Managers" on page 81

**Introducing Sessions**

The term *user session* refers to a series of user application interactions that are tracked by the server. Sessions are used for maintaining user specific state, including persistent objects such as handles to database result sets and authenticated user identities, among many interactions. For example, a session can be used to track a validated user login, followed by a series of directed activities for a particular user.

The session itself resides in the server. For each request, the client transmits the session ID in a cookie or, if the browser does not allow cookies, the server automatically writes the session ID into the URL.

The Web Server supports the servlet standard session interface, called *HttpSession*, for all session activities.

This section includes the following topics:
- “Sessions and Cookies” on page 76
- “Sessions and URL Rewriting” on page 76
- “Sessions and Security” on page 76
Note – As of Web Server, form-login sessions are no longer supported. You can use single sign-on sessions instead.

Sessions and Cookies

A cookie is a small collection of information that can be transmitted to a calling browser, which retrieves it on each subsequent call from the browser so that the server can recognize calls from the same client. A cookie is returned with each call to the site that created it, unless it expires.

Sessions are maintained automatically by a session cookie that is sent to the client when the session is first created. The session cookie contains the session ID, which identifies the client to the server on each successive interaction. If a client does not support or allow cookies, the server rewrites the URLs where the session ID appears in the URLs from that client.

You can configure whether and how sessions use cookies. For more information on related elements in the sun-web.xml file, see "session-properties Element" on page 160 and "cookie-properties Element" on page 161.

Sessions and URL Rewriting

You can also configure whether sessions use URL rewriting. For more information, see the sun-web.xml element "session-properties Element" on page 160.

Sessions and Security

The Web Server security model is based on an authenticated user session. Once a session has been created, the application user is authenticated if authentication is used and is logged into the session.

Additionally, you can specify that a session cookie is only passed on an HTTPS secured connection, so the session can only remain active on a secure channel.

For more information about security, see Chapter 8, “Securing Web Applications.”
Using Sessions

To use a session, first create a session using the HttpServletRequest method getSession(). Once the session is established, examine and set its properties using the provided methods. If desired, set the session to time out after being inactive for a defined time period, or invalidate it manually. You can also bind objects to the session, which store them for use by other components.

This section includes the following topics:
- “Creating or Accessing a Session” on page 77
- “Examining Session Properties” on page 78
- “Binding Data to a Session” on page 79
- “Invalidating a Session” on page 80

Creating or Accessing a Session

To create a new session or gain access to an existing session, use the HttpServletRequest method getSession(), as shown in the following example:

```java
HttpSession mySession = request.getSession();
```

getSession() returns the valid session object associated with the request, identified in the session cookie that is encapsulated in the request object. Calling the method with no arguments creates a session that is associated with the request if one does not already exist. Additionally, calling the method with a Boolean argument creates a session only if the argument is true.

The following example shows the doPost() method from a servlet that only performs the servlet’s main functions if the session is present. Note that the false parameter to getSession() prevents the servlet from creating a new session if one does not already exist.

```java
public void doPost (HttpServletRequest req, HttpServletResponse res) throws ServletException, IOException
{
    HttpSession session = req.getSession(false) ;
    if (session) {
        // session retrieved, continue with servlet operations
    }
    else{
        // no session, return an error page
    }
}
```
Note—The `getSession()` method should be called before anything is written to the response stream.

For more information about `getSession()`, see the Java Servlet 2.5 specification.

### Examining Session Properties

Once a session ID has been established, use the methods in the `HttpSession` interface to examine session properties. Use the methods in the `HttpServletRequest` interface to examine request properties that relate to the session.

The following table shows the methods used to examine session properties.

**TABLE 6-1  HttpSession Methods**

<table>
<thead>
<tr>
<th>HttpSession Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>getCreationTime()</code></td>
<td>Returns the session time in milliseconds since January 1, 1970, 00:00:00 GMT.</td>
</tr>
<tr>
<td><code>getId()</code></td>
<td>Returns the assigned session identifier. An HTTP session's identifier is a unique string that is created and maintained by the server.</td>
</tr>
<tr>
<td><code>getLastAccessedTime()</code></td>
<td>Returns the last time the client sent a request carrying the assigned session identifier (or -1 for a new session) in milliseconds since January 1, 1970, 00:00:00 GMT.</td>
</tr>
<tr>
<td><code>isNew()</code></td>
<td>Returns a Boolean value indicating that the session is new. A new session is one that the server has created and the client has not sent a request to it. This state means the client has not acknowledged or joined the session and may not return the correct session identification information when making its next request.</td>
</tr>
</tbody>
</table>

For example:

```java
String mySessionID = mySession.getId();
if (mySession.isNew()) {
    log.println(currentDate);
    log.println("client has not yet joined session " + mySessionID);
}
```

The following table shows the methods used to examine servlet request properties.
TABLE 6–2 HttpServletRequest Methods

<table>
<thead>
<tr>
<th>HttpServletRequest Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>getRequestedSessionId()</td>
<td>Returns the session ID specified with the request. This value might differ from the session ID in the current session if the session ID given by the client is invalid and a new session was created. Returns null if the request does not have a session associated with it.</td>
</tr>
<tr>
<td>isRequestedSessionIdValid()</td>
<td>Checks whether the request is associated with a currently valid session. If the session requested is not valid, it is not returned through the getSession() method.</td>
</tr>
<tr>
<td>isRequestedSessionIdFromCookie()</td>
<td>Returns true if the request’s session ID provided by the client is a cookie, or false otherwise.</td>
</tr>
<tr>
<td>isRequestedSessionIdFromURL()</td>
<td>Returns true if the request’s session ID provided by the client is a part of a URL, or false otherwise.</td>
</tr>
</tbody>
</table>

For example:

```java
if ( request.isRequestedSessionIdValid() ) {
    if ( request.isRequestedSessionIdFromCookie() ) {
        // this session is maintained in a session cookie
    }
    // any other tasks that require a valid session
} else {
    // log an application error
}
```

## Binding Data to a Session

You can bind objects to sessions to make them available across multiple user interactions.

The following table shows the HttpSession methods that provide support for binding objects to the session object.

TABLE 6–3 HttpSession Methods

<table>
<thead>
<tr>
<th>HttpSession Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>getAttribute()</td>
<td>Returns the object bound to a given name in the session, or null if there is no such binding.</td>
</tr>
<tr>
<td>getAttributeNames()</td>
<td>Returns an array of names of all attributes bound to the session.</td>
</tr>
</tbody>
</table>
TABLE 6–3 HttpSession Methods (Continued)

<table>
<thead>
<tr>
<th>HttpSession Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>setAttribute()</td>
<td>Binds the specified object into the session with the given name. Any existing binding with the same name is overwritten. For an object bound into the session to be distributed, it must implement the serializable interface.</td>
</tr>
<tr>
<td>removeAttribute()</td>
<td>Unbinds an object in the session with the given name. If there is no object bound to the given name, this method does nothing.</td>
</tr>
</tbody>
</table>

**Binding Notification with HttpSessionBindingListener**

Some objects require you to know when they are placed in or removed from a session. To obtain this information, implement the HttpSessionBindingListener interface in those objects. When your application stores or removes data with the session, the servlet engine checks whether the object being bound or unbound implements HttpSessionBindingListener. If it does, the Web Server notifies the object under consideration, through the HttpSessionBindingListener interface, that it is being bound into or unbound from the session.

**Invalidating a Session**

Direct the session to invalidate itself automatically after being inactive for a defined time period. Alternatively, invalidate the session manually with the HttpSession method invalidate().

**Invalidating a Session Manually**

To invalidate a session manually, call the following method:

```java
session.invalidate();
```

All objects bound to the session are removed.

**Setting a Session Timeout**

Session timeout is set using the session-timeout element in the web.xml deployment descriptor file. For more information, see the Java Servlet 2.5 specification.
Session Managers

Web Server provides the following session management options, which are described in this section:

- **memory**, the default session manager
- **file**, a provided manager that store sessions on the file system
- **IWS60**, a provided session manager that allows backward compatibility with any custom session managers you may have created using Web Server
- **MMAP** (UNIX Only), a provided persistent memory map (mmap) file-based session manager that works in both single-process and multi-process mode

### memory Option

The memory is the default memory based session manager.

#### Enabling memory

You can specify memory explicitly to change its default parameters. To do so, edit the `sun-web.xml` file for the web application as in the following example. Note that `persistence-type` must be set to `memory`.

```xml
<sun-web-app>
  ...
  <session-config>
    <session-manager persistence-type="memory">
      <manager-properties>
        <property name="reapIntervalSeconds" value="20" />
      </manager-properties>
    </session-manager>
  </session-config>
  ...
</sun-web-app>
```

For more information about the `sun-web.xml` file, see Chapter 9, "Deploying Web Applications."

#### Manager Properties for Memory

The following table describes `manager-properties` properties for the memory based session manager.
### TABLE 6-4 manager-properties for memory

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>reapIntervalSeconds</td>
<td>60</td>
<td>Specifies the number of seconds between checks for expired sessions. Setting this value lower than the frequency at which session data changes is recommended. For example, this value should be as low as possible (1 second) for a hit counter servlet on a frequently accessed web site, or you could lose the last few hits each time you restart the server.</td>
</tr>
<tr>
<td>maxSessions</td>
<td>-1</td>
<td>Specifies the maximum number of active sessions, or -1 (the default) for no limit.</td>
</tr>
<tr>
<td>sessionFilename</td>
<td>SESSIONS</td>
<td>Specifies the absolute or relative path name of the file in which the session state is preserved between application restarts, if preserving the state is possible. A relative path name is relative to the temporary directory for this web application.</td>
</tr>
</tbody>
</table>

#### file Session Manager

The file is another file-system-based session manager provided with Web Server. For session persistence, file can use a file to which each session is serialized. You can also create your own persistence mechanism.

#### Enabling the file Session Manager

You can specify file explicitly to change its default parameters. To do so, edit the sun-web.xml file for the web application as in the following example. Note that persistence-type must be set to file.

```xml
<sun-web-app>
  ...
  <session-config>
    <session-manager persistence-type="file">
      <manager-properties>
        <property name=reapIntervalSeconds value=20 />
      </manager-properties>
      <store-properties>
        <property name=directory value=sessions />
      </store-properties>
    </session-manager>
    ...
  </session-config>
</sun-web-app>
```
For more information about the sun-web.xml file, see Chapter 9, "Deploying Web Applications."

**Manager Properties for file**

The following table describes manager-properties properties for the file session manager.

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>reapIntervalSeconds</td>
<td>60</td>
<td>Specifies the number of seconds between checks for expired sessions. Setting this value lower than the frequency at which session data changes is recommended. For example, this value should be as low as possible (1 second) for a hit counter servlet on a frequently accessed web site, or you could lose the last few hits each time you restart the server.</td>
</tr>
<tr>
<td>maxSessions</td>
<td>-1</td>
<td>Specifies the maximum number of active sessions, or -1 (the default) for no limit.</td>
</tr>
</tbody>
</table>

**IWS60 Session Manager**

The IWS60 session manager ensures backward compatibility with any 6.0 session managers that you may have created.

IWS60 works in both single-process and multi-process mode. It can be used for sharing session information across multiple processes possibly running on different machines.

**Note** – The MaxProcs directive in the magnus.conf file determines whether the server is running in single-process or multi-process mode. If the value of MaxProcs is higher than 1 and no session manager is configured, then by default the session manager used is the IWS60 with file-based persistence. The MaxProcs is deprecated in Web Server 7.0.

For session persistence, IWS60 can use a database or a distributed file system (DFS) path that is accessible from all servers in a server farm. Each session is serialized to the database or distributed file system. You can also create your own persistence mechanism.

If Web Server is running in single-process mode, then by default, no session persistence mode is defined and therefore sessions are not persistent.
If Web Server is running in multi process mode, sessions are persistent by default. If a persistence mode is not defined, IWS60 uses a DFS.

Multi-process mode is supported only on UNIX platforms. All multi process mode features of IWS60 are ignored on Windows.

**Enabling IWS60**

You can enable IWS60 to change its default parameters. You can also enable IWS60 for a particular context if the server is running in single-process mode. To do so, edit the sun-web.xml file for the web application as in the following example. The `persistence-type` must be set to s1ws60.

```xml
<sun-web-app>
  ...
  <session-config>
    <session-manager persistence-type="s1ws60">
      <manager-properties>
        <property name="classname" value="com.iplanet.server.http.
session.IWSSessionManager"/>
        // other manager-related properties
      </manager-properties>
      <store-properties>
        <property name="classname" value="com.iplanet.server.http.
session.FileStore"/>
        <property name="directory" value="<directory name to store the
persistant_sessions>"/>
        // other store-related properties
      </store-properties>
    </session-manager>
  ...
  </session-config>
  ...
</sun-web-app>

In the case of persistent sessions:

```xml
<sun-web-app>
  ...
  <session-config/>
  <session-manager persistence-type="s1ws60">
    <manager-properties>
      <property name="classname" value="com.iplanet.server.http.
session.IWSSessionManager"/>
      // other manager-related properties
    </manager-properties>
    <store-properties>
      <property name="classname" value="com.iplanet.server.http.
session.FileStore"/>
      <property name="directory" value="<directory name to store the
persistant_sessions>"/>
      // other store-related properties
    </store-properties>
  </session-manager>
  ...
</sun-web-app>
```
For more information about the sun-web.xml file, see Chapter 9, “Deploying Web Applications.”

Manager Properties for IWS60

The following table describes manager-properties properties for the IWS60 session manager.

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>maxSessions</td>
<td>1000</td>
<td>The maximum number of sessions maintained by the session manager at any given time. The session manager refuses to create any more new sessions if maxSessions are already number of sessions present at that time.</td>
</tr>
<tr>
<td>timeOut</td>
<td>1800</td>
<td>The amount of time in seconds after a session is accessed by the client before the session manager destroys it. Those sessions that are not accessed for at least timeOut seconds are destroyed by the reaper method.</td>
</tr>
<tr>
<td>reapInterval</td>
<td>600</td>
<td>The amount of time in seconds that the SessionReaper thread sleeps before calling the reaper method again.</td>
</tr>
<tr>
<td>maxLocks</td>
<td>10</td>
<td>The number of cross-process locks to use for synchronizing access to individual sessions across processes. The default value is used if the value 0 is specified. This parameter is ignored in single-process mode.</td>
</tr>
<tr>
<td>Property Name</td>
<td>Default Value</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| session-data-store |                                                                              | The name of the class that determines the means of session persistence. The classes supplied with Web Server are: com.iplanet.server.http.session.JdbcStore  
|                  |                                                                              | ■ com.iplanet.server.http.session.FileStore  
|                  |                                                                              | If you do not specify the session-data-store parameter, sessions are not persistent in single-process mode, and FileStore is the default in multi-process mode.  
|                  |                                                                              | The JdbcStore and FileStore classes are subclasses of the session-data-store class. You can create your own class that implements session persistence by extending SessionDataStore. |
| session-failover-enabled |                                                                              | Specifies whether sessions are reloaded from the persistent store for every request, and always forced to true in multi-process mode.  
|                  |                                                                              | Applicable only if the session-data-store parameter is set to the JdbcStore or FileStore class.                                                                                                               |
| session-data-dir  | The following text is single path. server_root/server_id/SessionData  
|                  | virtual_server_id/web_app_URI                                                | The directory in which session data for all servers and web applications is kept.  
|                  |                                                                              | Applicable only if the session-data-store parameter is set to the FileStore class.                                                                                                                         |
| provider          | sun.jdbc.odbc.JdbcOdbcDriver                                                   | The JDBC driver. For more information about the JDBC API, see http://java.sun.com/products/jdbc/index.jsp  
|                  |                                                                              | Applicable only if the session-data-store parameter is set to the JdbcStore class.                                                                                                                         |
| url               | jdbc:odbc:LocalServer                                                         | Specifies the data source.  
|                  |                                                                              | Applicable only if the session-data-store parameter is set to the JdbcStore class.                                                                                                                         |
| table             | sessions                                                                     | Name of the SQL table that store sessions.  
<p>|                  |                                                                              | Applicable only if the session-data-store parameter is set to the JdbcStore class.                                                                                                                         |</p>
<table>
<thead>
<tr>
<th>Property Name</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>username</td>
<td>none</td>
<td>The login user name for the database. Applicable only if the <code>session-data-store</code> parameter is set to the <code>JdbcStore</code> class.</td>
</tr>
<tr>
<td>password</td>
<td>none</td>
<td>The login password for the database. Applicable only if the <code>session-data-store</code> parameter is set to the <code>JdbcStore</code> class.</td>
</tr>
<tr>
<td>reaperActive</td>
<td>true</td>
<td>When set to true, the session manager runs session reaper to remove expired sessions from the database. The default is true. Only one server in the cluster should run the reaper. Applicable only if the <code>session-data-store</code> parameter is set to the <code>JdbcStore</code> class.</td>
</tr>
<tr>
<td>accessTimeColumn</td>
<td>AccessTime</td>
<td>The name of the column that holds the last access time in minutes. The SQL type is <code>NUMERIC(9)</code>. Applicable only if the <code>session-data-store</code> parameter is set to the <code>JdbcStore</code> class.</td>
</tr>
<tr>
<td>timeOutColumn</td>
<td>TimeOut</td>
<td>The name of the column that holds the session timeout in minutes. The SQL type is <code>NUMERIC(9)</code>. Applicable only if the <code>session-data-store</code> parameter is set to the <code>JdbcStore</code> class.</td>
</tr>
<tr>
<td>sessionIdColumn</td>
<td>SessionID</td>
<td>The name of the column that holds the session ID. The SQL type is <code>VARCHAR(100)</code>. Applicable only if the <code>session-data-store</code> parameter is set to the <code>JdbcStore</code> class.</td>
</tr>
<tr>
<td>valueColumn</td>
<td>Value</td>
<td>The name of the column that holds the session object. The SQL type is <code>VARBINARY(4096)</code>. This column must be large enough to accommodate all of your session data. Applicable only if the <code>session-data-store</code> parameter is set to the <code>JdbcStore</code> class.</td>
</tr>
</tbody>
</table>
TABLE 6–6 manager-properties for IWS60 (Continued)

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>lookupPool</td>
<td>4</td>
<td>The number of dedicated connections that perform lookup operations on the database. For higher performance, use a precompiled SQL statement for each of these connections. Applicable only if the session-data-store parameter is set to the JdbcStore class.</td>
</tr>
<tr>
<td>insertPool</td>
<td>4</td>
<td>The number of dedicated connections that perform insert operations on the database. Each of these connections would have a precompiled SQL statement for higher performance. Applicable only if the session-data-store parameter is set to the JdbcStore class.</td>
</tr>
<tr>
<td>updatePool</td>
<td>4</td>
<td>The number of dedicated connections that perform update operations on the database. For higher performance, use a precompiled SQL statement for each of these connections. Applicable only if the session-data-store parameter is set to the JdbcStore class.</td>
</tr>
<tr>
<td>deletePool</td>
<td>2</td>
<td>The number of dedicated connections that perform delete operations on the database. For higher performance, use a precompiled SQL statement for each of these connections. Applicable only if the session-data-store parameter is set to the JdbcStore class.</td>
</tr>
</tbody>
</table>

**Note** – Prior to using JdbcStore, you must create the table in which the session information is stored. The name of the table is specified by the table parameter, and the table’s four columns are specified by the accessTimeColumn, timeOutColumn, sessionIdColumn, and valueColumn parameters.

**Note** – FileStore, JdbcStore, IWSSessionManager, IWSHttpSession, IWSHttpSessionManager, and SessionDataStore have been deprecated in Web Server.
Source Code for IWS60

The IWS60 session manager creates an IWSHttpSession object for each session. The source files for IWSSessionManager.java and IWSHttpSession.java are in the install_dir/lib directory. The source code files for IWSSessionManager.java and IWSHttpSession.java are provided, so you can use them as the starting point for defining your own session managers and session objects.

IWSSessionManager extends IWSHttpSessionManager. The class file for IWSHttpSessionManager is in the JAR file webser-rt.jar in the directory install_dir/lib. The IWS60 implements all of the methods in IWSHttpSessionManager that need to be implemented, so you can use IWSSessionManager as an example of how to extend IWSHttpSessionManager. When compiling your subclass of IWSSessionManager or IWSHttpSessionManager, be sure that the JAR file webser-rt.jar is in your compiler’s classpath.

The JdbcStore.java and FileStore.java source files and the source file for the parent class, SessionDataStore.java, are provided so you can modify the session persistence mechanism of IWS60. These files are also located in the install-dir/lib directory.

MMap Session Manager (UNIX Only)

MMap is a persistent memory map (mmap), file-based session manager that works in both single-process and multi-process mode.

Note – The MaxProcs directive in the magnus.conf file determines whether the server is running in single-process or multi-process mode. The Maxprocs is deprecated in Web Server 7.0.

Enabling MMap

You can enable MMap to change its default parameters. You can also enable MMap for a particular context if the server is running in single-process mode. To do so, edit the sun-web.xml file for the web application as in the following example. Note that persistence-type must be set to mmap.

```xml
<sun-web-app>
...
 <session-config>
   <session-manager persistence-type="mmap">
     ...
   </session-manager>
   ...
 </session-config>
...
</sun-web-app>
```
For more information about the sun-web.xml file, see Chapter 9, “Deploying Web Applications.”

**Manager Properties for MMap**

The following table describes manager-properties properties for the MMap session manager.

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>maxSessions</td>
<td>1000</td>
<td>The maximum number of sessions maintained by the session manager at any given time. The session manager refuses to create any more new sessions if maxSessions number of sessions are already present at that time.</td>
</tr>
<tr>
<td>maxValuesPerSession</td>
<td>10</td>
<td>The maximum number of values or objects a session can hold.</td>
</tr>
<tr>
<td>maxValueSize</td>
<td>4096</td>
<td>The maximum size of each value or object that can be stored in the session.</td>
</tr>
<tr>
<td>timeOut</td>
<td>1800</td>
<td>The amount of time in seconds after a session is last accessed by the client before the session manager destroys it. Those sessions that haven’t been accessed for at least timeOut seconds are destroyed by the reaper method.</td>
</tr>
<tr>
<td>reapInterval</td>
<td>600</td>
<td>The amount of time in seconds that the SessionReaper thread sleeps before calling the reaper method again.</td>
</tr>
<tr>
<td>maxLocks</td>
<td>1</td>
<td>The number of cross-process locks to use for synchronizing access to individual sessions across processes. The default value is used if the value 0 is specified. This parameter is ignored in single-process mode.</td>
</tr>
</tbody>
</table>

**Note** – MMap can only store objects that implement java.io.Serializable.
Developing Lifecycle Listeners

This chapter provides a basic overview, and a description of various features of lifecycle listeners in Web Server. It includes the following sections:

■ “Server Lifecycle Events” on page 91
■ “The LifecycleListener Interface” on page 92
■ “The LifecycleEvent Class” on page 92
■ “The Server Lifecycle Event Context” on page 92
■ “Deploying a Lifecycle Module” on page 93
■ “Considerations for Lifecycle Modules” on page 94
■ “Sample Lifecycle Configuration” on page 95

Server Lifecycle Events

Web Server goes through different events in its lifecycle:

■ init - This event includes reading configuration, initializing built-in subsystems, naming, security and logging services, and creating the web container.
■ startup - loading and initializing deployed applications.
■ service - The server is ready to service requests shut down: stopping and destroying loaded applications. The system is preparing to shut down.
■ terminating - The container is being closed, which terminates the built-in subsystems and server runtime environment.
■ reconfig - A transient server state in which a server thread is dynamically reconfiguring while the rest of the server in the service state. This state can occur several times during the life of the server.
The LifecycleListener Interface

Web Server enables you to write classes and customize various phases of the server lifecycle. For instance, you may have a startup code that ensures a remote data source is available for the applications. Such classes are notified by server lifecycle events. The Web Server defines a LifecycleListener interface that users can implement and register with the Server.

The syntax of this interface is as follows: public void handleEvent(LifecycleEvent event):

receives a lifecycle event.

In its event parameter, the programmatic interface for LifecycleListener provides the following features to the implementation classes:

- Access to initialization parameters
- A handler to the server run time environment for naming, logging and accessing resources
- Exception-handling mechanics

The LifecycleEvent Class

The LifecycleEvent class is an interface from the point of view to the developer, even if programmatically it is a class. This interface is the means by which these events are represented. This class informs you of the kind of event that happened through the getEventType() method and the data associated with the event (through the getData() method).

The Server Lifecycle Event Context

The LifecycleEventContext interface provides an access to the server runtime environment including the JNDI naming context and logging service. The following methods are defined in this interface:

- public String[] getCmdLineArgs() - Returns the server command line arguments.
- public javax.naming.Context getNamingContext() - Returns the naming context.
- public String getInstallRoot() - Returns the installation root.
- public String getInstanceName() - Returns the server instance name.
- public void log(java.util.logging.Level level, String message) - Logs the message to the server log, with verbosity level.
- public void log(java.util.logging.Level level, String message, Throwable throwable) - Logs the message and the stack trace for throwable, with verbosity level.

The following two methods are also used by this interface to keep backward compatibility with the 6.1 version of Web Server:
public void log(String message, Throwable throwable): Logs the message and the stack trace for throwable, with verbosity level.

public javax.naming.Context getInitialContext() - Similar to getNamingContext()

Deploying a Lifecycle Module

Server lifecycle listener classes are visible in the serve applications management area. You can add, delete, update, enable, and disable listener classes and set their parameters. Web Server will not support dynamic deployment of startup and shutdown classes. Any changes to these classes or their configuration requires server restart.

TABLE 7–1 Elements of the lifecycle

<table>
<thead>
<tr>
<th>Configurable element / attribute</th>
<th>Data type and Units</th>
<th>Range of values</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>lifecycle-module.name</td>
<td>String</td>
<td>Any non-null/non-empty unique string in lifecycle modules.</td>
<td>Must be specified while registering this lifecycle module.</td>
</tr>
<tr>
<td>lifecycle-module.class</td>
<td>String</td>
<td>Fully qualified Java class name.</td>
<td>Must implement the LifecycleListener interface.</td>
</tr>
<tr>
<td>lifecycle-module.enabled</td>
<td>Boolean</td>
<td>true or false.</td>
<td>Default is true.</td>
</tr>
<tr>
<td>lifecycle-module.load-order</td>
<td>Integer</td>
<td>0-100 Reserved. 100-MAXINT.</td>
<td>Order of loading the lifecycle event listeners in numerical order. Choose a load-order greater than or equal to 100 to avoid conflicts with internal lifecycle modules.</td>
</tr>
<tr>
<td>lifecycle-module.is-failure-fatal</td>
<td>Boolean</td>
<td>true or false</td>
<td>If you want the server to treat exceptions thrown from the listener classes as fatal and prevent continuation of normal startup, set this element to true.</td>
</tr>
</tbody>
</table>
### Considerations for Lifecycle Modules

When using keep the following points in mind of lifecycle module:

- The server lifecycle listener classes are called synchronously from the main server thread. Therefore, take extra precautions must be taken to ensure that the listener classes don’t block the server.
- The listener classes may create threads if appropriate. The threads must be stopped during the shutdown and termination phases.
- The resources allocated during initialization or startup events should be cleared.
- The listener classes are loaded in the context of server’s root class loader, which loads server-wide resources as well. Therefore, all the support classes needed by these server lifecycle event listener must be available at this class loader or its parent, the system class loader. As a consequence, you must ensure that the Java security manager policy files are appropriately set up, Otherwise, a lifecycle listener class trying to perform a `System.exec()` may get a security access violation.

### TABLE 7–1  Elements of the lifecycle (Continued)

<table>
<thead>
<tr>
<th>Configurable element / attribute</th>
<th>Data type and Units</th>
<th>Range of values</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>lifecycle-module.class-path</td>
<td>String</td>
<td>Optional</td>
<td>Points to the user-specified classpath for the listener class.</td>
</tr>
<tr>
<td>lifecycle-module.description</td>
<td>Element</td>
<td>Optional</td>
<td>Describes the lifecycle module.</td>
</tr>
<tr>
<td>property.name</td>
<td>String</td>
<td>Optional</td>
<td>User-specified parameter name. Part of the property element.</td>
</tr>
<tr>
<td>property.value</td>
<td>String</td>
<td>Optional</td>
<td>User-specified parameter value. Part of the property element.</td>
</tr>
<tr>
<td>property.description</td>
<td>String</td>
<td>Optional</td>
<td>User-specified description. Part of the property element.</td>
</tr>
</tbody>
</table>
Sample Lifecycle Configuration

The following example shows a portion of the server.xml that defines a lifecycle listener.

```xml
<lifecycle-module>
    <class-name>com.sun.ias.server.LifecycleListenerImpl</class-name>
    <is-failure-fatal>false</is-failure-fatal>
    <description>Sample lifecycle module</description>
    <property>
        <name>foo</name>
        <value>fooval</value>
    </property>
</lifecycle-module>
```

The following example shows a sample LifecycleListener implementation

```java
package com.sun.ias.server;
import java.util.Properties;
import java.util.logging.Level;
import com.sun.appserv.server.LifecycleEventContext;
import com.sun.appserv.server.ServerLifecycleException;
import com.sun.appserv.server.LifecycleEvent;
import com.sun.appserv.server.LifecycleListener;

public class LifecycleListenerImpl implements LifecycleListener {
    /** receive a server lifecycle event */
    @param event associated event
    @throws <code>ServerLifecycleException</code> for exception condition.
    */
    public void handleEvent(LifecycleEvent event) throws ServerLifecycleException {
        LifecycleEventContex ctx=event.getLifecycleEventContext();
        ctx.log(level.INFO, "got event" + event.getEventType() + "event data:" + event.getData());
        Properties props;
```
if (Lifecycle.event.INIT_EVENT == event.getEventType()) {
    System.out.println("LifecycleListener: INIT_EVENT");
    props = (Properties) event.getData();
    //handle INIT_EVENT
    return;
}

if (LifecycleEvent.STARTUP_EVENT == event.getEventType()) {
    System.out.println("LifecycleListener: START_EVENT");
    //handle STARTUP_EVENT
    return;
}

if (LifecycleEvent.READY_EVENT == event.getEventType()) {
    System.out.println("LifecycleListener: READY_EVENT");
    //handle READY_EVENT
    return;
}

if (LifecycleEvent.SHUTDOWN_EVENT == event.getEventType()) {
    System.out.println("LifecycleListener: SHUTDOWN_EVENT");
    //handle SHUTDOWN_EVENT
    return;
}

if (LifecycleEvent.TERMINATION_EVENT == event.getEventType()) {
    System.out.println("LifecycleListener: TERMINATION_EVENT");
    //handle TERMINATION_EVENT
    return;
}

}
This chapter describes the basic goals and features of Web Server security features related to the Java Servlet Container. It also describes how to write secure Java web applications containing components that perform user authentication and access authorization tasks.

This chapter has the following sections:

- “Supported Security Features” on page 97
- “Common Security Terminology” on page 98
- “Security Features Specific to the Web Server” on page 99
- “Container Security” on page 102
- “User Authentication by Servlets” on page 103
- “User Authentication for Single Sign-On” on page 104
- “User Authorization by Servlets” on page 105
- “Fetching the Client Certificate” on page 107
- “Using Web Services Message Security” on page 107
- “Programmatic Login” on page 116
- “Enabling the Java Security Manager” on page 117
- “The server.policy File” on page 118
- “Related Information” on page 120

**Supported Security Features**

Web Server provides highly secure, interoperable, and distributed component computing based on the Java EE security model. The security goals for Web Server include the following:

- Full compliance with the Java Servlet 2.5 security model, including role-based authorization. For more information, see the Security chapter in the Java Servlet 2.5 specification at http://java.sun.com/products/servlet/download.html.
- Support for single sign-on across all Web Server applications within a single security domain.
Common Security Terminology

- Support for several underlying authentication realms, such as simple file and LDAP. Certificate authentication is also supported for SSL client authentication. Solaris OS platform authentication is also supported.
- Support for declarative security through Web Server specific XML-based role mapping.
- Support for Java Security Manager enforcement.

For more information about Java EE security, see the Chapter 6, "Certificates and Keys," in *Sun Java System Web Server 7.0 Update 6 Administrator’s Guide*.

Common Security Terminology

This section provides an overview of the common security terminology.

The most common security processes are authentication, authorization, realm assignment, and role mapping.

- “Authentication” on page 98
- “Authorization” on page 98
- “Realms” on page 98
- “Java EE Application Role Mapping” on page 99

Authentication

Authentication verifies the user. For example, when the user provides a user name and password in a web browser, if those credentials match the permanent profile stored in the active realm, the user is authenticated. The user is associated with a security identity for the remainder of the session. For more information on authentication realms, see "Managing Authentication Realms" in *Sun Java System Web Server 7.0 Update 6 Administrator’s Guide*.

Authorization

Authorization permits a user to perform desired operations after being authenticated. For example, a human resources application might authorize managers to view personal employee information for all employees, but allow employees to view only their own personal information.

Realms

A realm, also called a security policy domain or a security domain in the Java EE specification, is a scope over which a common security policy is defined and enforced by the security administrator of the security service. Supported realms in Web Server are file, ldap, certificate, solaris, custom, and native.
Java EE Application Role Mapping

In the Java EE/Servlet security model, a client may be defined in terms of a security role. For example, a company might use its employee database to generate both a company-wide phone book application and payroll information obviously, While all employees might have access to phone numbers and email addresses, only some employees would have access to the salary information. Employees with the right to view or change salaries might be defined as having a special security role.

A role is different from a user group in that a role defines a function in an application, while a group is a set of users who are related in some way. For example, members of the groups astronauts, scientists, and pilots all fit into the role of SpaceShuttlePassenger.

In Web Server, roles correspond to users, groups or both used and groups configured in the active realm.

Security Features Specific to the Web Server

In addition to supporting the Java EE 1.4 security model, Web Server also supports the following features that are specific to the Web Server:

- Single sign-on across all Web Server applications within a single security domain
- Programmatic login
- The parallel Access Control List (ACL)-based security model, in addition to the Java EE/Servlet security model
- Support for secure ACL-based Java web applications, in addition to native content

This section discusses the following:

- “Web Server Security Model” on page 99
- “Web Application and URL Authorizations” on page 102

Web Server Security Model

Secure applications require a client to be authenticated as a valid application user and have authorization to access servlets and JSPs.

Applications with a secure web container may enforce the following security processes for clients:

- Authenticate the caller
- Authorize the caller for access to each servlet/JSP based on the applicable access control configuration
Authentication is the process of confirming an identity. Authorization means granting access to a restricted resource to an identity. Access control mechanisms enforce these restrictions. Authentication and authorization can be enforced by a number of security models and services.

Web Server provides authentication and authorization support through the following mechanisms, which are discussed in this section:

- ACL-based authentication and authorization
- Java EE/Servlet-based authentication and authorization

Whether performed by the ACL subsystem or the Java EE/Servlet authentication subsystem, authentication and authorization are still the two fundamental operations that define secure web content.

**ACL-Based Authentication and Authorization**

ACL-based access control is described at length in the "Configuring Access Control" in *Sun Java System Web Server 7.0 Update 6 Administrator's Guide*. This section provides a brief overview of the key concepts.

Web Server supports authentication and authorization through the use of locally stored ACLs, which describe what access rights a user has for a resource. For example, an entry in an ACL can grant a user named John read permission to a particular folder named misc:

```acl
"path=/export/user/990628.1/docs/misc/";

authenticate (user,group) {
    database = "default";
    method = "basic";
};

deny (all)
    (user = "John");
allow (read);
```

The core ACLs in Web Server support three types of authentication: basic, certificate, and digest.

- Basic authentication relies on lists of user names and passwords passed as cleartext.
- Certificates bind a name to a public key.
- Digest authentication uses encryption techniques to encrypt the user’s credentials.

The ACL-based access control model includes the following features:

- ACL-based authentication uses the following configuration files:
  - `install_dir/config/*.acl` files
install_dir/config/server.xml

Authentication is performed by auth-db modules that are configured in the server.xml file.

Authorization is performed by access control rules set in the install_dir/config/*.acl files, if ACLs are configured.

In addition, the Web Server SSL engine supports external crypto hardware to offload SSL processing and to provide optional tamper-resistant key storage.

For more information about ACL-based access control and the use of external crypto hardware, see the Web Server Administrator's Guide.

**Java EE/Servle- based Authentication and Authorization**

In addition to providing ACL-based authentication, Web Server also implements the security model defined in the Java EE 1.4 specification to provide several features that help you develop and deploy secure Java web applications.

A typical Java EE-based web application consists of the following parts, access to any or all of which can be restricted:

- Servlets
- JavaServer Pages (JSP) components
- HTML documents
- Miscellaneous resources, such as image files and compressed archives

The Java EE servlet-based access control infrastructure relies on the use of security realms. When a user tries to access the main page of an application through a web browser, the web container prompts for the user’s credential information. The container then passes the information for verification to the realm that is currently active in the security service.

A realm, represents a set of known users along with optional group membership information. The main implementation also encapsulates a mechanism for performing authentication against the data set.

The main features of the Java EE/Servlet-based access control model are described below:

- Java EE/Servlet-based authentication uses the following configuration files:
  - The web application deployment descriptor files web.xml and sun-web.xml
  - install_dir/config/server.xml

  Authentication is performed by Java security realms that are configured through <auth-realm> entries in the server.xml file.

- Authorization is performed by access control rules in the deployment descriptor file, web.xml, in case any such rules have been set.
Web Application and URL Authorizations

Secure web applications may have authentication and authorization properties. The web container supports three types of authentication: basic, certificate, and form-based. The core ACLs support basic, certificate, and digest. For more information about ACL configuration, see the Sun Java System Web Server 7.0 Update 6 Administrator’s Guide.

When a browser requests an application URL that requires authentication, the web container collects the user authentication information, for example, user name and password and passes it to the security service for authentication.

For Java EE web applications, Web Server checks the application’s web.xml file for information on which parts of the application are protected, and which roles are authorized to access. It also checks sun-web.xml to see whether the currently authenticated user belongs to one of the required roles, either directly through user mapping or indirectly through group mapping.

Container Security

The component containers are responsible for providing Java EE application security. Two security forms are provided by the container: programmatic security and declarative security.

Programmatic Security

In programmatic security, a servlet uses method calls to the security API, as specified by the Java EE security model, to make business logic decisions based on the caller or remote user’s security role. Programmatic security should only be used when declarative security alone is insufficient to meet the application’s security model.

The Java EE 1.4 specification defines programmatic security with respect to servlets as consisting of two methods of the servlet HttpServletRequest interface. Web Server supports these interfaces as defined in the specification.

In addition to the programmatic security defined in the Java EE specifications, Web Server also supports programmatic login. For more information, see “Programmatic Login” on page 116.

Declarative Security

Declarative security means that the security mechanism for an application is declared and handled externally to the application. Deployment descriptors describe the Java EE application’s security structure, including security roles, access control, and authentication requirements.
Web Server supports the DTDs specified by the Java EE 1.4 specification, and has additional security elements included in its own deployment descriptors. Declarative security is the application deployers responsibility.

**User Authentication by Servlets**

Web Server supports the web-based login mechanisms required by the Java EE 1.4 specification:

- “HTTP Basic Authentication” on page 103
- “SSL Mutual Authentication” on page 103
- “Form-Based Login” on page 104

The `login-config` element in the `web.xml` deployment descriptor file describes the authentication method used, the application’s realm name displayed by the HTTP basic authentication, and the form login mechanisms attributes.

The `login-config` element syntax is as follows:

```
<!ELEMENT login-config (auth-method?,realm-name?,form-login-config?)>
```

**Note** – The `auth-method` subelement of `login-config` is optional. However, but if it is not included, the server defaults to HTTP Basic Authentication, which is not very secure.

For more information about `web.xml` elements, see the Java Servlet 2.5 specification at [http://java.sun.com/products/servlet/download.html](http://java.sun.com/products/servlet/download.html)

For more information on `sun-web.xml` elements, see Chapter 9, “Deploying Web Applications.”

**HTTP Basic Authentication**

HTTP basic authentication (RFC 2617) is supported by Web Server. Because passwords are sent with base64 encoding, this authentication type is not very secure. Use SSL or another equivalent transport encryption to protect the password during transmission.

**SSL Mutual Authentication**

SSL 3.0 and the means to perform mutual client/server certificate-based authentication is a Java EE 1.4 specification requirement. This security mechanism provides user authentication using HTTPS (HTTP over SSL). For more information, see “Creating a Configuration” in *Sun Java System Web Server 7.0 Update 6 Administrator’s Guide*.
Form-Based Login

The login screen's look and feel cannot be controlled with the HTTP browsers built-in mechanisms. Java EE can to package a standard HTML or servlet JSP based form for logging in. The login form is associated with a web protection domain and is used to authenticate previously unauthenticated users.

Because passwords are sent unless protected by the underlying transport, this authentication type is not very secure. Use of SSL or another equivalent transport encryption to protect the password during transmission.

For the authentication to proceed appropriately, the login form action must always be j_security_check. For more information, see Chapter 4, “Developing Servlets.”

The following HTML sample shows how to program the form in an HTML page:

```html
<form method="POST" action="j_security_check">
    <input type="text" name="j_username" />
    <input type="password" name="j_password" />
</form>
```

You can specify the parameter encoding for the form. For details, see “parameter-encoding Element” on page 183.

User Authentication for Single Sign-On

Single sign-on across applications on the Web Server is supported by the Web Server servlets and JSPs. This feature allows multiple applications that require the same user sign-on information to share this information between them, rather than having the user sign on separately for each application. These applications are created to authenticate the user once. When needed, this authentication information is propagated to all other involved applications.

An example application using the single sign-on scenario could be a consolidated airline booking service that searches all airlines and provides links to different airline web sites. Once the user signs on to the consolidated booking service, the user information can be used by each individual airline site without requiring another sign-on.

Single sign-on operates according to the following rules:

- Single sign-on applies to web applications configured for the same realm and virtual server. The realm is defined by the realm-name element in the web.xml file. For information about virtual servers, see the Sun Java System Web Server 7.0 Update 6 Administrator's Guide.
- As long as users access only unprotected resources in any of the web applications on a virtual server, they are not challenged to authenticate themselves.
As soon users access a protected resource in any web application associated with a virtual server, they are challenged to authenticate using the login method defined for the web application currently being accessed.

Once authenticated, the roles associated with this user are used for access control decisions across all associated web applications, without challenging the user to authenticate to each application individually.

When the user logs out of one web application, for example, by invalidating or timing out the corresponding session if form-based login is used, the user’s sessions in all web applications are invalidated. Any subsequent attempt to access a protected resource in any application requires the users authorization.

The single sign-on feature uses HTTP cookies to transmit a token that associates each request with the saved user identity, so it can only be used in client environments that support cookies.

To configure single sign-on, set the following properties in the single-sign-on element of the server.xml file:

- **enabled**: If false, single sign-on is disabled for this virtual server, and users must authenticate separately to every application on the virtual server. The default is false.
- **idle-timeout**: Specifies the time after which a user’s single sign-on record becomes eligible for purging if no client activity is received. Because single sign-on applies across several applications on the same virtual server, access to any of the applications keeps the single sign-on record active. The default value is 5 minutes (300 seconds). Higher values provide longer single sign-on persistence for the users at the expense of more memory use on the server.

To configure single sign-on through CLI, see the enable-single-signon(1) and disable-single-signon(1) man pages.

The following example shows a configuration with all default values:

```xml
<single-sign-on>
  <enabled>1</enabled>
  <idle-timeout>300</idle-timeout>
</single-sign-on>
```

### User Authorization by Servlets

Servlets can be configured to permit access to users with the appropriate authorization level.

- “Defining Roles” on page 106
- “Defining Servlet Authorization Constraints” on page 106
Defining Roles

Security roles define an application function, made up of a number of users, groups, or both users and groups. The relationship between users and groups is determined by the specific realm implementation being used.

You can define roles in the Java EE deployment descriptor file, web.xml, and the corresponding role mappings in the Web Server deployment descriptor file, sun-web.xml. For more information about sun-web.xml, see Chapter 9, “Deploying Web Applications.”

Each security-role-mapping element in the sun-web.xml file maps a role name permitted by the web application to principals and groups. For example, a sun-web.xml file for a deployed web application might contain the following:

```xml
<sun-web-app>
  <security-role-mapping>
    <role-name>manager</role-name>
    <principal-name>jgarcia</principal-name>
    <principal-name>mwebster</principal-name>
    <group-name>team-leads</group-name>
  </security-role-mapping>
  <security-role-mapping>
    <role-name>administrator</role-name>
    <principal-name>dsmith</principal-name>
  </security-role-mapping>
</sun-web-app>
```

Note that the role-name in this example must match the role-name in the security-role element of the corresponding web.xml file.

For web applications, the roles are always specified in the sun-web.xml file. A role can be mapped to specific principals, to groups or both principals and groups. The principal or group names used must be valid principals or groups in the current realm.

Defining Servlet Authorization Constraints

At the servlet level, you can define access permissions using the auth-constraint element of the web.xml file.

The auth-constraint element on the resource collection must be used to indicate the user roles permitted to the resource collection. Refer to the Java Servlet specification for details on configuring servlet authorization constraints.
Fetching the Client Certificate

When you enable SSL and require client certificate authorization, your servlets have access to the client certificate as shown in the following example:

```java
if (request.isSecure()) {
    java.security.cert.X509Certificate[] certs;
    certs = request.getAttribute("javax.servlet.request.X509Certificate");
    if (certs != null) {
        clientCert = certs[0];
        if (clientCert != null) {
            // Get the Distinguished Name for the user.
            java.security.Principal userDN = clientCert.getSubjectDN();
            ...
        }
    }
}
```

The `userDN` is the fully qualified distinguished name for the user.

Using Web Services Message Security

In message security, security information is inserted into messages that travel through the networking layers and reaches the message destinations.

- Setting up `wadm`
- Configuring Message Security Provider
- Message Security Provider in Application

Configuring the Web Server for Message Security

This section describes the following topics:

- Actions of Request and Response Policy Configurations
- To configure other security facilities
- Security Enhancements to `server.xml`
- Security Enhancements to `sun-web.xml`

Actions of Request and Response Policy Configurations

The following table shows message protection policy configuration and the resulting message security operations performed by the WS-Security SOAP message security providers for that configuration.
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><code>auth-source= &quot;sender&quot;</code></td>
<td>The message contains the <code>wase:security</code> header that contains a <code>wsse:UsernameToken</code> with password.</td>
</tr>
<tr>
<td><code>auth-source= &quot;content&quot;</code></td>
<td>The content of the SOAP message body is signed. The message contains a <code>wsse:Security</code> header that contains the message body signature represented as a <code>ds:Signature</code>.</td>
</tr>
<tr>
<td><code>auth-source= &quot;sender&quot;</code>&lt;br&gt;<code>auth-recipient= &quot;before-content&quot;</code>&lt;br&gt;<code>OR</code>&lt;br&gt;<code>auth-recipient= &quot;after-content&quot;</code></td>
<td>The content of the SOAP message body is encrypted and replaced with the resulting <code>xenc:EncryptedData</code>. The message contains a <code>wsse:Security</code> header that contains a <code>wsse:UsernameToken</code> with password and an <code>xenc:EncryptedKey</code>. The <code>xenc:EncryptedKey</code> contains the key used to encrypt the SOAP message body. The key is encrypted in the public key of the recipient.</td>
</tr>
<tr>
<td><code>auth-source= &quot;content&quot;</code>&lt;br&gt;<code>auth-recipient= &quot;before-content&quot;</code></td>
<td>The content of the SOAP message body is encrypted and replaced with the resulting <code>xenc:EncryptedData</code>. The <code>xenc:EncryptedData</code> is signed. The message contains a <code>wsse:Security</code> header that contains an <code>xenc:EncryptedKey</code> and a <code>ds:Signature</code>. The <code>xenc:EncryptedKey</code> contains the key used to encrypt the SOAP message body. The key is encrypted in the public key of the recipient.</td>
</tr>
<tr>
<td><code>auth-source= &quot;content&quot;</code>&lt;br&gt;<code>auth-recipient= &quot;after-content&quot;</code></td>
<td>The content of the SOAP message body is signed, then encrypted, and then replaced with the resulting <code>xenc:EncryptedData</code>. The message contains a <code>wsse:Security</code> header that contains an <code>xenc:EncryptedKey</code> and a <code>ds:Signature</code>. The <code>xenc:EncryptedKey</code> contains the key used to encrypt the SOAP message body. The key is encrypted in the public key of the recipient.</td>
</tr>
<tr>
<td><code>auth-recipient= &quot;before-content&quot;</code>&lt;br&gt;<code>OR</code>&lt;br&gt;<code>auth-recipient= &quot;after-content&quot;</code></td>
<td>The content of the SOAP message body is encrypted and replaced with the resulting <code>xenc:EncryptedData</code>. The message contains a <code>wsse:Security</code> header that contains an <code>xenc:EncryptedKey</code>. The <code>xenc:EncryptedKey</code> contains the key used to encrypt the SOAP message body. The key is encrypted in the public key of the recipient.</td>
</tr>
<tr>
<td><code>No policy specified</code></td>
<td>No security operations are performed by the modules.</td>
</tr>
</tbody>
</table>
To Configure Other Security Facilities

The Web Server implements message security using message security providers integrated in its SOAP processing layer. The message security providers depend on other security facilities of Web Server.

1 If using a username token, configure a user database, if necessary.
When using a username and password token, an appropriate realm must be configured and an appropriate user database must be configured for the realm.

2 Manage certificates and private keys, if necessary.
After configuring the Web Server facilities for use by message security providers as described in "Managing Certificates" in *Sun Java System Web Server 7.0 Update 6 Administrator’s Guide*.

Security Enhancements to server.xml

The server element in server.xml contains one or more soap-auth-provider elements, each of which contains a list of configured soap message security providers. The server element also includes a default-soap-auth-provider-name for the default SOAP message-level authentication provider.


Administration Command-Line Interface (CLI) support is provided to add, remove, and list the soap-auth-provider element in server.xml. The CLI also supports adding a default-soap-auth-provider-name to server.xml.

Security Enhancements to sun-web.xml

Security-related additions to sun-web.xml are described in detail in the following sections.

Webservice-endpoint Element

The syntax for the webservice-endpoint element is as follows:

```xml
<!ELEMENT webservice-endpoint (port-component name, endpoint-address-uri?, (login-config<message-security-binding)?, transport-guarantee?, service-gname?, tie-class?, servlet-imp-class?)>
```

<table>
<thead>
<tr>
<th>Element Name</th>
<th>Occurrences</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>webservice-endpoint</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**TABLE 8–2 webservice-endpoint Element (Continued)**

<table>
<thead>
<tr>
<th>Element</th>
<th>1 or 0</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>port-component-name</td>
<td>1</td>
<td>Unique name of a Web Service within a module. This name should be the same as the endpoint: name in sun-jaxws.xml.</td>
<td>PCDATA</td>
</tr>
<tr>
<td>endpoint-address-uri</td>
<td>0 or 1</td>
<td>Unused for Web Server</td>
<td>PCDATA</td>
</tr>
<tr>
<td>login-config</td>
<td></td>
<td>Unused for Web Server</td>
<td></td>
</tr>
<tr>
<td>message-security-binding</td>
<td>0 or 1</td>
<td>Used to bind a Web Service endpoint or port to a specific security provider. This element can also be used to provide a definition of message security requirements to be enforced by the security provider.</td>
<td>See Table 8–3 message-security-binding</td>
</tr>
<tr>
<td>transport-guarantee</td>
<td>0 or 1</td>
<td>Unused for Web Server</td>
<td>PCDATA</td>
</tr>
<tr>
<td>service-qname</td>
<td>0 or 1</td>
<td>Unused for Web Server</td>
<td></td>
</tr>
<tr>
<td>tie-class</td>
<td>0 or 1</td>
<td>Unused for Web Server</td>
<td>PCDATA</td>
</tr>
<tr>
<td>servlet-impl-class</td>
<td>0 or 1</td>
<td>Unused for Web Server</td>
<td>Class name</td>
</tr>
</tbody>
</table>

**message-security-binding Element**

The **message-security-binding** element is used to bind a web service endpoint or port to a specific security provider.

The syntax for this element is as follows:
```xml
<!--ELEMENT message-security-binding (message-security*)-->
<!ATLIST message-security-binding
auth-layer %message-layer;#REQUIRED
provider-id CDATA #IMPLIED -->

**TABLE 8-3 message-security-binding Element**

<table>
<thead>
<tr>
<th>Element name</th>
<th>Occurrences</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>message-security</td>
<td>0 or more</td>
<td>Specifies the message security requirements of request and response for the endpoint or port</td>
<td>See Table 8-5</td>
</tr>
</tbody>
</table>

**TABLE 8-4 Attributes of the message-security-binding Element**

<table>
<thead>
<tr>
<th>Attribute name</th>
<th>Description</th>
<th>Type</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>auth-layer</td>
<td>Layer at which the security should be enforced</td>
<td>Entity</td>
<td>message-layer</td>
</tr>
<tr>
<td>provider-id</td>
<td>Identifies the provider-config that should be used</td>
<td>CDATA</td>
<td>If a value is not specified, then the default provider is used. If no default provider exists at the layer, the authentication requirements defined in the message-security-binding are not enforced.</td>
</tr>
</tbody>
</table>

**message-security Element**

The syntax for the message-security element is as follows:

```xml
<?ELEMENT message-security (message+, request-protection?, response-protection?)?>
```

**TABLE 8-5 message-security Element**

<table>
<thead>
<tr>
<th>Element name</th>
<th>Occurrences</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>message</td>
<td>1 or more</td>
<td>Describes the methods or operations to which the security requirements apply</td>
<td>Table 8-6</td>
</tr>
<tr>
<td>request-protection</td>
<td>0 or 1</td>
<td>Describes the authentication requirements applicable to a request</td>
<td>Table 8-7</td>
</tr>
</tbody>
</table>
```
**message Element**

The syntax for the message element is as follows: `<!ELEMENT (java-method?|operation-name?)>`. 

**Attributes of request-protection Element**

The syntax for the request-protection element is as follows.

```xml
<!ELEMENT request-protection EMPTY>
<!ATTLIST request-protection
auth-source (sender|content)#IMPLIED
auth-recipient (before-content |after-content)#IMPLIED
```

**TABLE 8–5 message-security Element (Continued)**

<table>
<thead>
<tr>
<th>Element name</th>
<th>occurrences</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>response-protection</td>
<td>0 or 1</td>
<td>Describes the authentication requirements applicable to a response</td>
<td>Table 8–8</td>
</tr>
</tbody>
</table>

**TABLE 8–6 message element**

<table>
<thead>
<tr>
<th>Element name</th>
<th>occurrences</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>java-method</td>
<td>0 or 1</td>
<td>Java methods on which the security should be enforced</td>
<td>Table 8–9</td>
</tr>
<tr>
<td>operation-name</td>
<td>0 or 1</td>
<td>WSDL name of an operation of the web service</td>
<td>PCDATA</td>
</tr>
</tbody>
</table>

**TABLE 8–7 request-protection Element**

<table>
<thead>
<tr>
<th>Attribute name</th>
<th>Description</th>
<th>Value</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>auth-source</td>
<td>Defines a requirement for message layer sender authentication for example, username and password or content authentication, for example, digital signature</td>
<td>sender or content</td>
<td>Implied</td>
</tr>
</tbody>
</table>
auth-recipient
Defines a requirement for message layer authentication of the receiver of a message to its sender for example, by XML encryption.
A before-content attribute value indicates that recipient authentication occurs before any content authentication.

before-content or after-content
Implied

response-protection Element

The syntax for the response-protection element is as follows:

```xml
<!ELEMENT response-protection EMPTY>
<!ATTLIST response-protection
auth-source (sender|content)#IMPLIED
auth-recipient (before-content |after-content)#IMPLIED
```

TABLE 8–8 Attributes of the response-protection Element

<table>
<thead>
<tr>
<th>Attribute name</th>
<th>Description</th>
<th>Value</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>auth-source</td>
<td>Defines a requirement for message layer sender authentication, for example, username and password or content authentication, for example, digital signature</td>
<td>sender or content</td>
<td>Implied</td>
</tr>
</tbody>
</table>
TABLE 8–8  Attributes of the response-protection Element (Continued)

<table>
<thead>
<tr>
<th>Element name</th>
<th>Occurrences</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>auth-recipient</td>
<td></td>
<td>Defines a requirement for message layer authentication of the receiver of a message to its sender, for example by XML encryption. The before-content attribute value indicates that recipient authentication occurs before any content authentication with respect to the target of the containing auth-policy.</td>
<td>before-content or after-content</td>
</tr>
</tbody>
</table>

java-method Element

The syntax for the java-method element is as follows:

```
<!ELEMENT java-method (method-name, method-params?)>
```

TABLE 8–9  java-method Element

<table>
<thead>
<tr>
<th>Element name</th>
<th>Occurrences</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>method-name</td>
<td>1</td>
<td>Name of the service method</td>
<td>PCDATA</td>
</tr>
<tr>
<td>method-params</td>
<td>0 or 1</td>
<td>List of the fully qualified Java type names of the method parameters.</td>
<td>Table 8–10</td>
</tr>
</tbody>
</table>

method-params Element

The syntax for method-params (method-param*) element is as follows:

TABLE 8–10  Attributes of the method-params Element

<table>
<thead>
<tr>
<th>Element name</th>
<th>Occurrences</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>method-params</td>
<td>0 or more</td>
<td>Fully qualified Java type name of a method parameter</td>
<td>PCDATA</td>
</tr>
</tbody>
</table>
**message-layer Entity**

The message-layer entity defines the value of the value of the auth-layer attribute.

The syntax for message-layer entity is:

```plaintext
<!Entity %message-layer "(SOAP)"
```

**Using Message Security Provider in an Application**

The following sub-web.xml example shows how to use the server.xml message security provider provider1 in a web application.

```xml
<?xml version="1.0" encoding="UTF-8"?>

<!--
    Copyright 2006-2007 Sun Microsystems, Inc. All rights reserved.
    Use is subject to license terms.
-->  
<!DOCTYPE sun-web-app PUBLIC "-//Sun Microsystems, Inc.//DTD Application Server 8.1 Servlet 2.5//EN" "http://www.sun.com/software/appserver/dtds/sun-web-app_2_4-1.dtd">

<sun-web-app>
    <context-root>/jaxws-fromwsdl-soap12</context-root>
    <servlet>
        <servlet-name>fromwsdl</servlet-name>
        <webservice-endpoint>
            <port-component-name>fromwsdl-soap12</port-component-name>
            <message-security-binding auth-layer="SOAP">
                <provider-id>provider1</provider-id>
            </message-security-binding>
        </webservice-endpoint>
    </servlet>
</sun-web-app>
```

**Note** – The `port-component-name` element should be the same as the name attribute in the `endpoint` element in `sun-jaxws.xml`. If the `provider-id` element is not specified in `sun-web.xml`, then the default `soap-auth-provider-name` configured in `server.xml` is be used as the provider.

Deploy the sample web application `fromwsdl-soap12.war` on to the Web Server.
Programmatic Login

Programmatic login enables a deployed Java EE application to invoke a login method. If the login is successful, a SecurityContext is established as if the client had authenticated using any of the conventional Java EE mechanisms.

Programmatic login is useful for applications with unique needs that cannot be accommodated by any of the Java EE standard authentication mechanisms.

This section discusses the following topics:

- “Precautions” on page 116
- “Granting Programmatic Login Permission” on page 116
- “ProgrammaticLogin Class” on page 117

Precautions

The Web Server is not involved in how the login information (username and password) is obtained by the deployed application. The application developer must ensure that the resulting system meets security requirements. If the application code reads the authentication information across the network, the application must determine whether to trust the user.

Programmatic login enables the application developer to bypass the Web Server-supported authentication mechanisms and feed authentication data directly to the security service. While flexible, this capability should not be used without some understanding of security issues.

Because this mechanism bypasses the container-managed authentication process and sequence, the application developer must be very careful in making sure that authentication is established before accessing any restricted resources or methods. The application developer must also verify the status of the login attempt and alter the behavior of the application accordingly.

The programmatic login state does not necessarily persist in sessions or participate in single sign-on.

Lazy authentication is not supported for programmatic login. If an access check is reached and the deployed application has not properly authenticated using the programmatic login method, access is denied immediately and the application might fail if not properly coded to account for this occurrence.

Granting Programmatic Login Permission

The ProgrammaticLoginPermission permission is required to invoke the programmatic login mechanism for an application. This permission is not granted by default to deployed applications because it is not a standard Java EE mechanism.
To grant the required permission to the application, add the following code to the
`instance_dir/config/server.policy` file:

```java
grant codeBase "file:jar_file_path" {
    permission com.sun.appserv.security.ProgrammaticLoginPermission
        "login";
};
```

The `jar_file_path` is the path to the application’s JAR file.

**Note** - If the Security Manager is disabled, it is not mandatory to grant permission.

For more information about the `server.policy` file, see “The `server.policy` File” on page 118.

**ProgrammaticLogin Class**

The `com.sun.appserv.security.ProgrammaticLogin` class enables a user to log in
programmatically.

The login method for servlets or JSPs has the following signature:

```java
public Boolean login(String user, String password,
        javax.servlet.http.HttpServletRequest request,
        javax.servlet.http.HttpServletResponse response)
```

This method performs the authentication. It returns true if the login succeeded, false if the login
failed.

**Enabling the Java Security Manager**

Web Server supports the Java Security Manager. The Java Security Manager is disabled by
default when you install the product, which can improve performance significantly for some
types of applications. Enabling the Java Security Manager might improve security by restricting
the rights granted to your Java EE web applications. To enable the Java Security Manager, add
the following JVM options to the `server.xml` file.

```xml
<jvm-options>-Djava.security.manager</jvm-options>
<jvm-options>-Djava.security.policy=instance_dir
/config/server.policy</jvm-options>
```

where `instance_dir` is the path to the installation directory of this server instance.
Whether you should run with the Security manager depends on your application and deployment needs.

Running with the Security Manager helps catch some specification issues with Java EE applications. All Java EE applications should be able to run with the Security Manager active and with only the default permissions. Therefore, the Security Manager should be turned on during development. Applications that can easily be deployed in environments where the Security Manager is always active, such as some versions of Sun Java System Application Server. Running with the Security Manager also helps isolate applications and may catch inappropriate operations.

The main drawback of running with the Security Manager is that it negatively affects performance. Depending on the application details and the deployment environment, this impact could be minor or quite significant.

The server.policy File

Each Web Server instance has its own standard Java Platform, Standard Edition (Java SE™ platform) policy file, located in the instance_dir/config directory. The file is named server.policy.

Web Server is a Java EE 1.4-compliant web server. As such, it follows the recommendations and requirements of the Java EE specification, including the optional presence of the Security Manager, which is the Java component that enforces the policy, and a limited permission set for Java EE application code.

This section includes the following topics:

- "Default Permissions" on page 118
- "Changing Permissions for an Application" on page 119

Default Permissions

Internal server code is granted all permissions by the AllPermission grant blocks to various parts of the server infrastructure code. Do not modify these entries.

Application permissions are granted in the default grant block. These permissions apply to all code not part of the internal server code listed previously.

A few permissions above the minimal set are also granted in the default server.policy file. These permissions are necessary due to various internal dependencies of the server implementation. Java EE application developers should not rely on these additional permissions.
Changing Permissions for an Application

The default policy for each instance limits the permissions of Java EE-deployed applications to the minimal set of permissions required for these applications to operate correctly. If you develop applications that require more than this default set of permissions, you can edit the server.policy file to add the custom permissions that your applications need.

You should add the extra permissions only to the applications that require them, not to all applications deployed to a server instance. Do not add extra permissions to the default set, which is the grant block with no codebase, which applies to all code. Instead, add a new grant block with a codebase specific to the application requiring the extra permissions, and only add the minimally necessary permissions in that block.

**Note** – Do not add java.security.AllPermission to the server.policy file for application code. Doing so completely defeats the purpose of the Security Manager, yet you still get the performance overhead associated with it.

As noted in the Java EE specification, an application should provide documentation of the additional permissions it needs. If an application requires extra permissions but does not document the set it needs, contact the application author for details.

As a last resort, you can iteratively determine the permission set an application needs by observing AccessControlException occurrences in the server log. If this information is not sufficient, you can add the -Djava.security.debug=all JVM option to the server instance. For details, see the Sun Java System Web Server 7.0 Update 6 Administrator’s Guide.

You can use the Java SE standard policy tool or any text editor to edit the server.policy file. For more information, see


For detailed information about the permissions you can set in the server.policy file, see:

http://java.sun.com/j2se/1.4.2/docs/guide/security/permissions.html.

For the Javadoc for the Permission class is see

http://java.sun.com/j2se/1.4.2/docs/api/java/security/Permission.html.
The following table describes where you can find more information about security and security configuration topics in the Web Server documentation:

<table>
<thead>
<tr>
<th>Subject</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring Java security and realm-based authentication</td>
<td>The chapter “Securing Your Web Server” in the Sun Java System Web Server 7.0 Update 6 Administrator’s Guide.</td>
</tr>
<tr>
<td>Certificates and public key cryptography</td>
<td>The chapter “Using Certificates and Keys” in the Sun Java System Web Server 7.0 Update 6 Administrator’s Guide.</td>
</tr>
<tr>
<td>ACL-based security</td>
<td>The chapter “Controlling Access to Your Server” in the Sun Java System Web Server 7.0 Update 6 Administrator’s Guide.</td>
</tr>
<tr>
<td>Configuring authentication services in the server.xml files</td>
<td>The chapter “Controlling Access to Your Server” in the Sun Java System Web Server 7.0 Update 6 Administrator’s Guide and Sun Java System Web Server 7.0 Update 6 Administrator’s Configuration File Reference.</td>
</tr>
</tbody>
</table>
Deploying Web Applications

This chapter describes how web applications are assembled and deployed in Web Server. The chapter has the following sections:

- “Web Application Structure” on page 121
- “Deployment Tools” on page 122
- “Creating Web Deployment Descriptors” on page 125
- “Deploying Web Applications” on page 125
- “Deploying Using JSR 88” on page 128
- “Managing Web Applications” on page 129
- “Enabling Web Applications” on page 130
- “Dynamic Reloading of Web Applications” on page 131
- “Classloaders” on page 132

Web Application Structure

Web applications have a directory structure, which is fully accessible from a mapping to the application’s document root (for example, /hello). The document root contains JSP files, HTML files, and static files such as image files.

A WAR file (web archive file) contains a complete web application in compressed form.

A special directory under the document root, WEB-INF, contains everything related to the application that is not in the public document tree of the application. No file contained in WEB-INF can be served directly to the client. The contents of WEB-INF include:

- /WEB-INF/classes/* - The directory for servlet and other classes.
- /WEB-INF/web.xml and /WEB-INF/sun-web.xml - XML-based deployment descriptors that specify the web application configuration, including mappings, initialization parameters, and security constraints.
The web application directory structure follows the structure outlined in the Java EE specification. The following example shows a sample directory structure of a simple web application.

```
+ hello/
   |--- index.jsp
   |--- META-INF/
   |     |--- MANIFEST.MF
   +--- WEB-INF/
       |--- web.xml
       |--- sun-web.xml
```

### Deployment Tools

#### Using Sun Java Studio Enterprise 8.1

Web Server supports Sun Java Studio Enterprise 8.1, Standard Edition. You can use Sun Java Studio to assemble and deploy web applications. Sun Java Studio Enterprise 8.1 is based on NetBeans™ software, and integrated with the Sun Java platform. Sun Java Studio Enterprise 8.1 also supports NetBeans 5.5.

Sun Java Studio support is available on all platforms supported by Sun Java Studio Enterprise 8.1. The plug-in for the Web Server is obtained in the following ways:

- From the Companion CD in the Sun Java Studio Enterprise 8.1 Media Kit
- By using the AutoUpdate feature of Sun Java Studio

**Note** – The Sun Java Studio Enterprise 8.1 for Web Server works only with a local Web Server (that is, with the IDE and the Web Server on the same machine).


The behavior of the Sun Java Studio Enterprise 8.1 plug-in for Web Server is the same as that for Sun Java System Application Server 8. If you’re using the Web Application Tutorial at the site listed above, for instance, you would set the Web Server instance as the default, and then take the same actions described in the tutorial.
For more information about Sun Java Studio Enterprise 8.1, visit http://www.sun.com/software/sundev/jde/

---

**Note** – For basic information about using Sun Java Studio Enterprise 8.1 to debug web applications, see “Using Developer Tools for Debugging” on page 137.

---

**Using NetBeans IDE 5.5**

NetBeans IDE 5.5 is an integrated development environment to create, deploy, and software Java EE web applications. This section describes how to use the NetBeans IDE 5.5 to create and deploy the web applications for Web Server.

▼ **To Install NetBeans IDE 5.5**

1. Download NetBeans IDE 5.5 from http://webserver.netbeans.org and install it.

2. After installation, launch the NetBeans IDE 5.5.

3. Download the latest plug-in.


5. Select Update Center of NetBeans, from the Tools menu.

6. Select Install Manually Downloaded Modules (.nbm Files) and click Next.

7. Add the downloaded .nbm files and click Next.

8. Select Web Server and click Next.

9. Select the Include option and click Yes to install the plug-in.

   The Web Server 7.0 plug-in is installed in the IDE.

▼ **To Register Web Server 7.0 in the NetBeans IDE 5.5**

1. Start the NetBeans.

2. Select Server node in the Runtime tab. Press mouse button and choose Add Server from the popup menu.

3. Select the Web Server to register the Web Server and click Next.
4 Provide the details of the Web Server installed on the local system or remote machine.

**Note** – The plug-in requires a local Web Server installation on the same machine, even if you are registering a remote Web server. The local installation is required for some of the Web Server jar files.

5 (Optional) If the Web Server contains multiple configuration, select the configuration.

- Select the Web Server node from the IDE drop-down list.
- Choose the configuration to use.

**Note** – The drop-down list contains configuration which have at least one virtual server and one instance.

6 Once the server is registered, it is listed in the Server node of the Runtime tab. Right click and choose Start.

7 You can expand the nodes and see all the web applications and resources.

▼ **Deploying Web Applications**

1 Start the NetBeans.

2 Select New Project from the File menu.

3 Select Web in the category list, and in the projects list, select web application. Then click Next.

4 From the Server drop-down list, select Web Server.

5 Click Next to complete the web project creation.

   Once the project is created, web project is displayed in the Projects tab. You can find all basic files created in the Web Server specific sun-web.xml deployment descriptor.

   The web application is now ready to compile, deploy.
Creating Web DeploymentDescriptors

Web Server web applications include two deployment descriptor files:


■ An optional Web Server - specific file (sun-web.xml) described later in this chapter.

The easiest way to create the web.xml and sun-web.xml files is to deploy a web application using Sun Java Studio Enterprise 8.1. For sample web.xml and sun-web.xml files, see “Sample Web Application XML Files” on page 189

Deploying Web Applications

You can deploy a web application using either the Admin console or the command-line interface.

▼ To Deploy Using Admin Console

Before You Begin
Select the virtual server, in which you need to deploy the web application.

1 Access the Admin Console.

2 Click the Add Web Application tab in the home page.
The Add Web Application screen appears.

3 Specify the location or package file path to upload to the Web Server.

4 Type the URI for your web application.
Specify the URI. This URI is the application’s context root and is relative to the server host.

5 Select JSP pre-compilation.

6 Click OK.
The Web Application page appears.

7 Click Save.

8 Click the Deployment Pending link in the top right of the screen.
The Configuration Deployment screen displays.
9 Click Deploy.
The web application is deployed.

For more information about using the Administration Console, see the Sun Java System Web Server 7.0 Update 6 Administrator's Guide

Deploying Using wadm

Note – Before you can manually deploy a web application, make sure that the server_root/bin directory is in your path.

You can use the wadm utility at the command line to deploy a WAR file into a virtual server web application environment as follows:

```
wadm [--user=admin-user] [--password-file=admin-pswd-file]
[--host=admin-host]
[--port=admin-port][--no-ssl]
[--rcfile=rcfile][--no-prompt][--commands-file=filename]
```

For more information about how to add, enable, and disable web applications, see the add-webapp(1).

The following table describes the command parameters. The left column lists the parameter, and the right column describes the parameter.

TABLE 9-1 Command Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--user</td>
<td>Specify the user name of the authorized Web Server administrator.</td>
</tr>
<tr>
<td>--password-file</td>
<td>Specify the password file. The password file contains the password to</td>
</tr>
<tr>
<td></td>
<td>authenticate administrators to the administration server. This file must</td>
</tr>
<tr>
<td></td>
<td>contain the line wadm_password=password. If you do not specify this option,</td>
</tr>
<tr>
<td></td>
<td>you will be prompted for a password while executing this command.</td>
</tr>
<tr>
<td>--host</td>
<td>Specify the name of the machine where the administration server is running.</td>
</tr>
<tr>
<td>--port</td>
<td>Specify the port number of the administration server. The default non-SSL</td>
</tr>
<tr>
<td></td>
<td>port is 8800 and the default SSL port is 8989.</td>
</tr>
<tr>
<td>--no-ssl</td>
<td>Specify this option to use a plain text connection to communicate with the</td>
</tr>
<tr>
<td></td>
<td>administration server. The default connection is SSL.</td>
</tr>
</tbody>
</table>
TABLE 9–1 Command Parameters (Continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--rcfile</td>
<td>Specify the name of the rcfile that has to be loaded while starting the wadm utility. rcfile can contain environment commands like set and unset, or a JACL script that needs to be run while starting wadm. The default file is ~/.wadmrc</td>
</tr>
<tr>
<td>--no-prompt</td>
<td>If you specify this option, wadm will prompt you for password while executing this command. Use this option if you have defined all passwords in a password file and specified the file using the --password-file option.</td>
</tr>
</tbody>
</table>

When you execute the wadm command, two things happen:

- A web application with the given uri_path and directory gets added to the server.xml file.
- The WAR file is extracted in the target directory.

The following shows a sample command.

```
wadm add-webapp --user=admin --password-file=admin.pwd --host=serverhost --port=8989 --config=config1 --vs=config1_vs_1 --uri=/testapp /abc/sample.war
```

After you have deployed an application, you can access it from a browser as follows:

```
http://vs_urlhost[:vs_port]/uri_path/[index_page]
```

The following table describes the parts of the URL.

TABLE 9–2 Parts of the URL

<table>
<thead>
<tr>
<th>Part</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vs_urlhost</td>
<td>One of the urlhosts values for the virtual server.</td>
</tr>
<tr>
<td>vs_port</td>
<td>(Optional) Only needed if the virtual server uses a non default port.</td>
</tr>
<tr>
<td>uri_path</td>
<td>The same path you used to deploy the application. This is also the context path.</td>
</tr>
<tr>
<td>index_page</td>
<td>(Optional) The page in the application that end users are meant to access first.</td>
</tr>
</tbody>
</table>

The following two examples show sample URLs:

```
http://sun.com:80/hello/index.jsp
```

```
http://sun.com/hello/
```
Deploying Using JSR 88

JSR 88 defines the contracts that enable the tool of multiple providers to configure and deploy applications on any platform product. The implementation requires both tools and Java EE platform products.

You can write your own JSR 88 client to deploy an application to the Web Server. For more information about JSR 88, see http://jcp.org/en/jsr/detail?id=88.

Auto-Deploying Web Applications

Using auto-deployment, you can quickly deploy one or more web applications just by copying them to a designated directory. The server auto-deploys web applications that are in the form of web archives (.war files) or in a directory in which a web archive has been exploded.

The following table illustrates the correlation between the name of the web archive or directory and the context path at which the application is automatically deployed.

<table>
<thead>
<tr>
<th>Web Application</th>
<th>Format</th>
<th>Context Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>instance_dir/auto-deploy/hello.war</td>
<td>Web Archive</td>
<td>/hello</td>
</tr>
<tr>
<td>instance_dir/auto-deploy/test</td>
<td>Directory</td>
<td>/test</td>
</tr>
<tr>
<td>instance_dir/auto-deploy/my_app.war</td>
<td>Web Archive</td>
<td>/my_app</td>
</tr>
</tbody>
</table>

Auto-deployment does not require the administration server to be up and running. Web applications that are auto-deployed are accessible on all the active virtual servers that have been configured in the server. Auto-deployment is intended for use in a development environment.

Note – During startup, the web applications for server.xml are deployed before any of the web applications in the auto-deploy directory.

Auto-Deploying a Web Application

1. Copy the web application (.war file or directory) to the following directory:
   instance_dir/auto-deploy
   where, instance_dir is the path to the installation directory of this server instance.

2. Start the instance. If the instance is already running, type the reconfig command:
   instance_dir/bin/reconfig
All web applications in the instance_dir/auto-deploy directory are automatically deployed to all the virtual servers in the instance.

**Removing an Auto-Deployed Web Application**

1. Delete the corresponding .war file or sub-directory in the directory:
   ```
   instance_dir/auto-deploy
   ```

2. Start the instance. If the instance is already running, type the `reconfig` command:
   ```
   instance_dir/bin/reconfig
   ```
   The deleted web applications are no longer accessible.

   You can also configure the server to periodically check the instance_dir/auto-deploy directory, for new or removed applications and automatically reflect these changes in the running instance. The `dynamic-reload-interval` attribute controls how often the server checks the auto-deploy directory for changes.

   For information on how to set the `dynamic-reload-interval` attribute through Admin console, see "Dynamic Reloading of Web Applications" on page 131. For information on how to set the `dynamic-reload-interval` attribute through CLI, see `set-servlet-container-prop(1)`.

---

### Managing Web Applications

Once deployed, the application or module exists in the central repository and can be referenced by a number of server instances. Initially, the server instances or clusters that you deployed as targets reference the application or module. To change the server instances and clusters that reference an application or module after it is deployed, change an application or modules targets using the Admin Console or change the application references using the `wadm`

Because the application is stored in the central repository, adding or deleting targets adds or deletes the same version of an application on different targets. However, an application deployed to more than one target can be enabled on one target and disabled on another target. Therefore, even if an application is referenced by a target, it is not available to you unless it is enabled on that target. In Web Server you can enable or disable a web application either using the Admin Console or command-line interface.
To Enable or Disable a Deployed Web Application

1. Access the Admin Console.
2. Select the server instance and click the edit Virtual Server tab.
3. Click the Web applications tab.
4. In the Web Applications table, select the web application.
   - To enable the application, click Enable.
   - To disable the application, click Disable.
5. Click Save.

Tip – Use the `enable-webapp` and `disable-webapp` commands to enable or disable the web application through the command-line interface. For more information, see the `enable-webapp(1)` and `disable-webapp(1)` man pages.

Enabling Web Applications

Web Server allows you to enable or disable a web application. You can do so in either of the following ways, as discussed in this section:

Enabling and Disabling Using the Admin Console

To enable or disable a deployed web application using the Admin Console, perform the following steps:

To Remove a Deployed Web Application

1. Access the Admin Console.
2. Select the server instance and click the edit Virtual Server tab.
3. Click the Web applications tab.
4. In the Web Applications table, select the web application or applications you want to remove and click Remove.
Tip – To remove a deployed web application through the command-line interface, use the remove-webapp command. For more information, see the remove-webapp(1) man page.

In the dialog box that appears, click OK.

Dynamic Reloading of Web Applications

To set dynamic reloading of web application, you must do the following:

▼ To Set Dynamic Reloading of Web Application

1. Access the Admin Console. Select the server instances and click the Edit Configuration tab.
2. Click the Java tab.
3. Click the Servlet Container tab.
4. In the Dynamic Reload Interval field, type an integer, that specifies the interval (in seconds) after which a deployed application will be checked for modifications and reloaded if necessary.
   - To enable dynamic reloading, you must specify a value greater than 0.
   - To disable dynamic reloading set the field to –1
5. Click Save.

Tip – To configure through the CLI, use the set-servlet-container-prop(1) command.

▼ To Load a New Servlet or Reload a Deployment Descriptor

1. Create an empty file named .reload at the root of the deployed module.
   For example:
   ```
   instance_dir/webapps/vs_id/uri/.reload
   ```
   where vs_id is the virtual server ID in which the web application is deployed, and uri is the value of the uri attribute of the webapp/ element.
2 Type touch .reload to explicitly update the .reload file's timestamp each time you make the above changes.

For JSPs, changes are reloaded automatically at a frequency set in the reload-interval property of the jsp-config element in the sun-web.xml file. To disable dynamic reloading of JSPs, set the reload-interval property to -1.

Classloaders

Web Server classloaders help you determine where and how you can position supporting JAR and resource files of your modules and applications.

In a Java Virtual Machine (JVM), the classloaders dynamically load a specific Java class file needed for resolving a dependency. For example, when an instance of java.util Enumeration needs to be created, one of the classloaders loads the relevant class into the environment.

Classloaders in the Web Server runtime follow the hierarchy shown in the following figure.
This hierarchy is a delegation hierarchy not a Java inheritance hierarchy. In the delegation design, a classloader delegates classloading to its parent before attempting to load a class itself. If the parent classloader cannot load a class, the findClass() method is called on the classloader subclass. In effect, a classloader is responsible for loading only the classes not available to the parent.

The exception is the web application classloader, which follows the delegation model in the Servlet specification. The web application Classloader looks in the local classloader before delegating to its parent. You can make the web application Classloader delegate to its parent.
first by setting delegate="true" in the class-loader element of the sun-web.xml file. For more information, see “ClassLoader Element” on page 179.

The following table describes Web Server classloaders.

<table>
<thead>
<tr>
<th>Classloader</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bootstrap</td>
<td>The Bootstrap Classloader loads the JDK classes. Only one instance of this classloader exists in the entire server.</td>
</tr>
</tbody>
</table>
| System              | The System Classloader loads the core Web Server classes. It is created based on the class-path-prefix, server-class-path, and class-path-suffix attributes of the <jvm/> element in the server.xml file.

The environment classpath is included if env-classpath-ignored="false" is set in the <jvm/> element. Only one instance of this classloader exists in the entire server.

If any changes are made to these attributes or classes, the server must be restarted for the changes to take effect.

For more information about the <jvm/> element in server.xml, see the Sun Java System Web Server 7.0 Update 6 Administrator’s Configuration File Reference. |
| Common              | The Common Classloader loads classes in the instance_dir/lib/classes directory, followed by JAR and ZIP files in the instance_dir/lib directory. The directories are optional. If they don’t exist, the Common Classloader is not created. If any changes are made to these classes, restart the server. |
| Web Application     | The Web Application Classloader loads the servlets and other classes in a specific web application from WEB-INF/lib and WEB-INF/classes and from any additional classpaths specified in the extra-class-path attribute of the class-loader element in sun-web.xml. For more information, see “ClassLoader Element” on page 179.

An instance of this classloader is created for each web application. If dynamic reloading has been enabled, any changes made to these attributes or classes are reloaded by the server without the need for a restart. For more information, see “Dynamic Reloading of Web Applications” on page 131. |
| JSP                 | The JSP Classloader loads the compiled JSP classes of JSPs. An instance of this classloader is created for each JSP file. Any changes made to a JSP are automatically detected and reloaded by the server unless dynamic reloading of JSPs has been disabled by setting the reload-interval property to -1 in the jsp-config element of the sun-web.xml file. For more information, see “jsp-config Element” on page 180. |
Debugging Web Applications

This chapter provides guidelines for debugging web applications in Web Server. The chapter includes the following sections:

- “Enabling Debugging” on page 135
- “JPDA Options” on page 136
- “Using Developer Tools for Debugging” on page 137
- “Debugging JSPs” on page 137
- “Generating a Stack Trace for Debugging” on page 137
- “Using Logging for Debugging” on page 138
- “Using Profiling for Debugging” on page 139

Debugging applications requires you to edit the server.xml file as described in this chapter. For more general information, see Sun Java System Web Server 7.0 Update 6 Administrator's Configuration File Reference.

**Enabling Debugging**

When you enable debugging, you enable both local and remote debugging. You can enable debugging through Admin Console or by editing server.xml.

Sun Java System Web Server debugging is based on the JPDA (Java™ Platform Debugger Architecture software). For more information, see “JPDA Options” on page 136

▼ To Enable Debugging Through Admin Console

1. Access the Admin Console.
2. Click the Edit Java Settings tab in the home page.
3. Click the JVM Settings tab.
4. Select the Enable Debug option to enable debugging. For more information about debug options, see "JPDA Options" on page 136.

5. Click Save.

▼ To Enable Debugging by Editing server.xml

- Set the following attributes of the jvm element in the server.xml file:
  - Set debug="true" to turn on debugging.
  - Add any desired JPDA debugging options in the debugoptions attribute. See "JPDA Options" on page 136.
  - To specify the port to use when attaching the JVM to a debugger. Specify address=port_number in the debugoptions attribute.

For details about the server.xml file, see the Sun Java System Web Server 7.0 Update 6 Administrator’s Configuration File Reference.

**JPDA Options**

The default JPDA options are as follows:

```
-Xdebug -Xrunjdwp:transport=dt_socket,server=y,suspend=n
```

If you change the value of suspend=y, the JVM starts in suspended mode and stays suspended until a debugger attaches to it. Use this option if you want to start debugging as soon as the JVM starts.

To specify the port to use when attaching the JVM to a debugger, specify address=port_number. You can also use the shared memory transport dt_shmem on the Win32 platform.

Using Developer Tools for Debugging

Sun Java Studio Enterprise 8.1 technology can be used for remote debugging if you want to manually attach the IDE to a remote Web Server started in debug mode.

▼ To Debug using NetBeans 5.5

Press mouse button the Web project name in the IDE. Choose Debug Project from the context menu.

Web Server will then start in debug mode and the IDE will pause executing the program at the breakpoint you have set in your application.

Debugging JSPs

When you use Sun Java Studio Enterprise 8.1 to debug JSPs, you can set breakpoints in either the JSP code or the generated servlet code. You can switch between them and see the same breakpoints in both the JSP code and the servlet code.

To set up debugging in Sun Java Studio Enterprise 8.1, see "Using Developer Tools for Debugging" on page 137.

Generating a Stack Trace for Debugging

For information about how to generate a Java stack trace for debugging, see

http://developer.java.sun.com/
developer/technicalArticles/Programming/Stacktrace/.

If the -Xrs flag is set for reduced signal usage in the server.xml file (under jvm), comment it out before generating the stack trace. If the -Xrs flag is used, the server might dump core and restart when you send the signal to generate the trace.

The stack trace goes to the system log file or to stderr based on the log attributes in server.xml.

For more information about the server.xml file, see the Sun Java System Web Server 7.0 Update 6 Administrator's Guide.

Displaying Stack Trace and Compiler Errors

Web Server supports, display-exception feature under server/servlet container which displays stack traces and compiler errors to the browser. This feature helps the user to view the log in the
browser and prevents them from looking into the server log file every time a compiler error occurs. You can enable or disable this feature by `set-servlet-container-prop` CLI or by selecting Display-Exception check box under set-servlet-container tab in Administration GUI.

**To Display Stack Trace and Compiler Error**

1. Create a JSP with syntax error.
2. Request for the log page through the browser.
   The browser displays the message Server Error.
3. Select Display-Exception check box under set-servlet-container tab in Administration GUI or enable the display-exception feature through set-servlet-container-prop CLI.
4. Request for the log page again through the browser.
   The browser displays the stack trace and compiler errors.

**Using Logging for Debugging**

You can use the Web Server log files to help debug your applications. For general information about logging, see the *Sun Java System Web Server 7.0 Update 6 Administrator's Guide*. For information about server.xml file, see the *Sun Java System Web Server 7.0 Update 6 Administrator’s Configuration File Reference*.

You can change logging settings in one of these ways:

**To Change the Log Settings**

1. Access the Admin Console.
2. Click the View Server Logs tab in the home page.
3. Set the log preferences.
4. Click Save to apply your changes.
Using Profiling for Debugging

You can use a profiler to perform remote profiling on the Web Server to discover choke point in server-side performance. This section describes how to configure these profilers for use with Web Server:

- “Using the HPROF Profiler” on page 139
- “Using the Optimizeit Profiler” on page 141

Using the HPROF Profiler

HPROF is a simple profiler agent shipped with the Java 2 SDK. It is a dynamically linked library that interacts with the Java™ Virtual Machine Profiler Interface (JVMPI) and writes out profiling information either to a file or to a socket in ASCII or binary format. This information can be further processed by a profiler front-end tool such as HAT.

HPROF can present CPU usage, heap allocation statistics, and monitor contention profiles. In addition, it can also report complete heap dumps and states of all of the monitors and threads in the Java virtual machine. For more details on the HPROF profiler, see the JDK documentation at:

http://java.sun.com/j2se/1.4.2/docs/guide/jvmpi/jvmpi.html

Once HPROF is installed, its libraries are loaded into the server process.

You can configure Web Server

▼ To Install the HPROF Profiler

1 Access the Admin Console.

2 Click the Edit Java Settings tab in the home page.
   The JVM General Settings screen appears.

3 Click Profilers.

4 Click New.
   The Create JVM Profiler popup appears.

5 Type the Name and select the JVM Profiler option to enable the profiler. Leave the Class Path and Native Library Path fields blank.

6 Click New to configure the JVM options.
Using Profiling for Debugging

7 **Click OK.**

   Edit the server.xml file as appropriate

   <!--hprof options-->
   <profiler name="hprof" enabled="true">
     <jvm-options>
       -Xrunhprof:file=log.txt,options
     </jvm-options>
   </profiler>

   **Note** – Do not use the -Xrs flag.

   Here is an example of options you can use:

   -Xrunhprof:file=log.txt,thread=y,depth=3

   The file option is important because it determines where the stack dump is written in step 6.

   The syntax of HPROF options is as follows:

   -Xrunhprof[:help]|[:option=value,option2=value2, ...]

   Using help lists options that can be passed to HPROF. The output is as follows:

   Hprof usage: -Xrunhprof[:help]|[:option=value,option2=value2,...]

   Option Name and Value Description Default
   heap=dump|sites|all heap profiling allcpu=samples|old CPU
   usage offformat=ab ascii or binary output
   afiler=<file> write data to file java.hprof(.txt for ascii)
   net=<host>:<port> send data over a socket write to file
   depth=<size> stack trace depth
   output cutoff point 0.0001lineno=y|n line number in traces?
   ythread=y|n thread in traces? ndoe=y|n dump on exit? y

8 **Change the PRODUCT_BIN assignment in the /install_dir/instance_dir/bin/startserv file from:**

   PRODUCT_BIN=webservd-wdog to PRODUCT_BIN=webservd

9 **Start the server by running the startserv script.**

   As the server runs in the foreground, the command prompt returns only after the server has been stopped.

10 **Find the process ID of the server process in another window or terminal.**

    % ps -ef | grep webservd

   This command lists two webservd processes. Look at the PPID (parent process ID) column and identify which of the two processes is the parent process and which is the child process. Note the PID (process ID) of the child process ID.
Send a SIGQUIT signal (signal 3) to the child process:
% kill -QUIT child_PID

Run the stopserv script from another window to stop the Web Server.
% ./stopserv

Stopping the server writes an HPROF stack dump to the file you specified using the file HPROF option. For general information about using a stack dump, see “Generating a Stack Trace for Debugging” on page 137.

Using the Optimizeit Profiler

Information about Optimizeit is available at:

http://www.borland.com/optimizetit/

Once Optimizeit is installed, its libraries are loaded into the server process.

To enable remote profiling with Optimizeit, do one of the following:

- Go to the Common Tasks page in the Admin Console, click the Edit Java Settings tab, click the Profiler link, and edit the following fields before selecting OK:
  - Profiler: Enable
  - Classpath: Optimizetit_dir/lib/optit.jar
  - Native Lib Path: Optimizetit_dir/lib
  - JVM Option: For each of these options, type the option in the JVM Option field, select Add, then check its box in the JVM Options list:
    - -DOPTITHOME=Optimizetit_dir
    - -Xrunoii
    - -Xbootclasspath/a:Optimizetit_dir/lib/oibcp.jar

  or

Enable remote profiling by editing server.xml file

<!-- Optimizeit options -->
<profiler classpath="Optimizetit_dir/lib/optit.jar"
nativelibrarypath="Optimizetit_dir/lib" enabled="true">
<jvm-options>
  -DOPTIT_HOME=Optimizetit_dir -Xboundthreads -Xrunoii
  -Xbootclasspath/a:Optimizetit_dir/lib/oibcp.jar
</jvm-options>
</profiler>

In addition, you might need to set the following in your server.policy file:
grant codeBase "file:Optimizeit_dir/lib/optit.jar" {
permission java.security.AllPermission;
};

For more information about the server.policy file, see "The server.policy File" on page 118.

When the server starts up with this configuration, you can attach the profiler.

**Note** – If any of the configuration options are missing or incorrect, the profiler might experience problems that affect the performance of the Web Server.
Deployment Descriptor Files

This chapter includes the following sections:

- “About Deployment Descriptor Files” on page 143
- “Migration Issues” on page 143
- “Extension to Standard Descriptors” on page 144
- “Sun Java System Web Server Descriptors” on page 144
- “The sun-web-app_2_5-0.dtd File” on page 144
- “Elements in the sun-web.xml File” on page 149
- “Sample Web Application XML Files” on page 189

About Deployment Descriptor Files

The deployment descriptor conveys the elements and configuration information of a web application between application developers, application assemblers, and deployers. For Java Servlets v.2.5, the deployment descriptor is defined in terms of an XML schema document.

Migration Issues

Migration creates a detailed log in the user-specified log file. For every instance, a log is created in the following syntax: MIGRATION_<server instance name>_MMM_DD/YYYY_HH.MM_AM/PM.log.

If no log directory exists, the log file is stored at install_dir/admin-server/logs.
Extension to Standard Descriptors

This section describes the supported extension to standard descriptors.

sun-web.xml

You define roles in the deployment descriptor file web.xml and the corresponding role mappings in the sun-web.xml deployment descriptor file for individually deployed web modules.

default-web.xml

default-web.xml is a global web deployment descriptor file that is shared by deployed web applications. It is used to configure the DefaultServlet and JspServlet servlets. In addition, it specifies: MIME mappings based on extensions Welcome files Global filters and security constraints Individual web applications inherit and might override the configuration settings inherited from default-web.xml with their own web.xml. The default-web.xml for each server instance is shared by all web applications deployed on the server instance. Depending on the configuration capabilities of the hosting application, a virtual server might replace the server-wide default-web.xml with its own. In that case, a virtual server's default-web.xml is shared by all web application deployed on the virtual server.

Sun Java System Web Server Descriptors

This section describes the Web Server descriptors.

The sun-web-app_2_5-0.dtd File

The sun-web-app_2_5-0.dtd file defines the structure of the sun-web.xml file, including the elements it can contain and the subelements and attributes these elements can have. The sun-web-app_2_5-0.dtd file is located in the install_dir/lib/dtds directory.

Note – Do not edit the sun-web-app_2_5-0.dtd file. Its contents change only with new versions of Web Server.

For general information about DTD files and XML, see the XML specification at http://www.w3.org/TR/2004/REC-xml-20040204.

Each element defined in a DTD file, which might be present in the corresponding XML file can contain subelements, and attributes described in the following sections.
Subelements

Elements can contain subelements. For example, the following file fragment defines the cache element:

```xml
<!ELEMENT cache (cache-helper*, default-helper?, property*, cache-mapping*)>
```

The `ELEMENT` tag specifies that a cache element can contain `cache-helper`, `default-helper`, `property`, and `cache-mapping` subelements.

The following table shows how optional suffix characters of subelements determine the requirement rules, or number of allowed occurrences, for the subelements.

<table>
<thead>
<tr>
<th>Subelement Suffix</th>
<th>Requirement Rule</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>element*</code></td>
<td>Can contain zero or more of this subelement.</td>
</tr>
<tr>
<td><code>element?</code></td>
<td>Can contain zero or one of this subelement.</td>
</tr>
<tr>
<td><code>element+</code></td>
<td>Must contain one or more of this subelement.</td>
</tr>
<tr>
<td><code>element</code> (no suffix)</td>
<td>Must contain only one of this subelement.</td>
</tr>
</tbody>
</table>

If an element cannot contain other elements, `EMPTY` or `(#PCDATA)` appears instead of a list of element names in parentheses.

Data

Some elements contain character data instead of subelements. These elements have definitions of the following format:

```xml
<!ELEMENT element-name (#PCDATA)>/
```

For example:

```xml
<!ELEMENT description (#PCDATA)>/
```

In the `sun-web.xml` file, white space is treated as part of the data in a data element. Therefore, no extra white space should appear before or after the data delimited by a data element. For example:
Attributes

Elements that have ATTLIST tags contain attributes (name-value pairs). For example:

```
<!ATTLIST cachemax-capacity CDATA  "4096"
timeout CDATA  "30"
enabled %boolean; "false">
```

A cache element can contain max-capacity, timeout, and enabled attributes.

The #REQUIRED label means that a value must be supplied. The #IMPLIED label means that the attribute is optional, and that Web Server generates a default value. Wherever possible, explicit defaults for optional attributes (such as "true") are listed.

Attribute declarations specify the type of the attribute. For example, CDATA means character data, and %boolean is a predefined enumeration.

Elements in the `default-web.xml` File

This section describes the XML elements in the `default-web.xml` file.

<table>
<thead>
<tr>
<th>Element</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>checkInterval</td>
<td>0</td>
<td>The checkInterval is the time in seconds between checks to see if a JSP file needs to be recompiled. If the development element is false and checkInterval is greater than zero it means the background compilations are enabled.</td>
</tr>
<tr>
<td>compiler</td>
<td>javac</td>
<td>Specifies the compiler Ant uses to compile JSP files. See the Ant documentation for more information: Compiles the JSP pages: <a href="http://antinstaller.sourceforge.net/manual/manual/">http://antinstaller.sourceforge.net/manual/manual/</a></td>
</tr>
<tr>
<td>compilerSourceVM</td>
<td></td>
<td>Allows source compatibility with the specified JDK release.</td>
</tr>
</tbody>
</table>
### TABLE A-2 default-web.xml Elements (Continued)

<table>
<thead>
<tr>
<th>Element</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>compilerTargetVM</td>
<td>true</td>
<td>Generates class files for the specified VM version</td>
</tr>
<tr>
<td>classdebuginfo</td>
<td>true</td>
<td>The JSP page gets compiled with debug information.</td>
</tr>
<tr>
<td>classpath</td>
<td>created dynamically based on the current web application</td>
<td>classpath is generated dynamically based on the current web application.</td>
</tr>
<tr>
<td>development</td>
<td>true</td>
<td>By default, JSP pages are recompiled since the request. The modifications are specified through the modificationTestInterval parameter. If false, checkInterval is enabled.</td>
</tr>
<tr>
<td>dumpSmap</td>
<td>false</td>
<td>If set to true, dumps SMAP information for JSR 45 debugging to a file. Set to false if suppressSmap is true.</td>
</tr>
<tr>
<td>enablePooling</td>
<td>true</td>
<td>Determines whether the tag handler pooling is enabled.</td>
</tr>
<tr>
<td>errorOnUserBeanInvalidClassAttribute</td>
<td>false</td>
<td>If set to true, issues an error when the value of the class attribute in a useBean action is not a valid bean class.</td>
</tr>
<tr>
<td>fork</td>
<td>true</td>
<td>fork compiles JSP pages with a separate JVM process.</td>
</tr>
<tr>
<td>genStrCharArray</td>
<td>false</td>
<td>If set to true, generates text strings as char arrays, which improves performance in some cases.</td>
</tr>
<tr>
<td>httpMethods</td>
<td>ALL METHODS</td>
<td>Comma separated list of HTTP methods are supported by JSP/Servlet. Wildcard (*) denotes all methods.</td>
</tr>
<tr>
<td>ieClassId</td>
<td>clsid:8AD9C840-044E-11D1-B3E9-00805F499093</td>
<td>Default value is sent to Internet Explorer when using the (<a href="">jsp:plugin</a> tags.</td>
</tr>
<tr>
<td>initialCapacity</td>
<td>32</td>
<td>Initial capacity of HashMap mapping JSPs to their corresponding servlets.</td>
</tr>
<tr>
<td>Element</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>initial-capacity</td>
<td></td>
<td>Same as initialCapacity. If both are specified, initialCapacity takes the precedence</td>
</tr>
<tr>
<td>javaEncoding</td>
<td>UTF-8</td>
<td>This element does the character encoding for Java™ files,</td>
</tr>
<tr>
<td>javaCompilerPlugin</td>
<td></td>
<td>The fully qualified class name of the JSP compiler plug-in.</td>
</tr>
<tr>
<td>keepgenerated</td>
<td>true</td>
<td>By default, the generated Java files are kept in the subdirectory after compilation.</td>
</tr>
<tr>
<td>modificationTestInterval</td>
<td>0</td>
<td>JSP files can only be modified during the specified time interval mentioned in seconds. By Default, value allows to modify JSP files in development mode without time constraint.</td>
</tr>
<tr>
<td>mappedfile</td>
<td>true</td>
<td>By default, the static content in a JSP page result in one print statement.</td>
</tr>
<tr>
<td>reload-interval</td>
<td>0</td>
<td>Specifies the frequency at which JSP files are checked for modifications. The frequency value is in seconds. If the value is 0 JSP pages are checked for modifications. –1 disables the checks for JSP page.</td>
</tr>
<tr>
<td>scratchdir</td>
<td></td>
<td>Work directory for the application The Java and class files are stored in this directory.</td>
</tr>
<tr>
<td>suppressSmap</td>
<td>false</td>
<td>If set to true, generation of SMAP information for JSR 45 debugging is suppressed.</td>
</tr>
<tr>
<td>trimSpaces</td>
<td>false</td>
<td>If set to true, trims white spaces in template text between actions or directives.</td>
</tr>
</tbody>
</table>
TABLE A-2  *default-web.xml Elements*  *(Continued)*

<table>
<thead>
<tr>
<th>Element</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>usePrecompiled</td>
<td>false</td>
<td>If true, JSP files are precompiled and their corresponding servlet classes have been bundled in the web application’s WEB-INF/lib or WEB-INF/classes. When JSP is accessed, it is not compiled and instead precompiled servlet class is used.</td>
</tr>
<tr>
<td>use-precompiled</td>
<td>false</td>
<td>Same as usePrecompiled. If both are specified, usePrecompiled takes the precedence.</td>
</tr>
<tr>
<td>minThreads</td>
<td>1</td>
<td>Minimum number of idle threads in the JSP compiler thread pool.</td>
</tr>
<tr>
<td>maxThreads</td>
<td>20</td>
<td>Maximum number of threads in the JSP compiler thread pool.</td>
</tr>
</tbody>
</table>

**Elements in the *sun-web.xml* File**

This section describes the XML elements in the *sun-web.xml* file. Elements are grouped as follows:

- “General Elements” on page 150
- “Security Elements” on page 154
- “Session Elements” on page 156
- “Reference Elements” on page 162
- “Caching Elements” on page 170
- “Classloader Element” on page 179
- “JSP Element” on page 180
- “Internationalization Elements” on page 183

This section also includes an alphabetical list of the elements for quick reference. See “Alphabetical List of *sun-web.xml* Elements” on page 187.

**Note** – Subelements must be defined in the order in which they are listed in each section, unless otherwise noted.

Each *sun-web.xml* file must begin with the following DOCTYPE header:

```
<!DOCTYPE sun-web-app PUBLIC "/Sun Microsystems, Inc./DTD Application Server 8.1 Servlet 2.5//EN"
http://www.sun.com/software/appserver/dtds/sun-web-app_2_4-1.dtd">
```
For an alphabetical list of elements in sun-web.xml, see “Alphabetical List of sun-web.xml Elements” on page 187

**General Elements**

General elements are as follows:

- “sun-web-app Element” on page 150
- “property Element” on page 153
- “description Element” on page 153

**sun-web-app Element**

This element Web Server-specific configuration for a web application. This element is the root element. The sun-web.xml file contain only one sun-web-app.

**Subelements**

The following table describes subelements for the sun-web-app element.

<table>
<thead>
<tr>
<th>Element</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;context-root Element&quot; on page 152</td>
<td>zero or more</td>
<td>Contains the web context roots for the web application</td>
</tr>
<tr>
<td>&quot;servlet Element&quot; on page 154</td>
<td>zero or more</td>
<td>Specifies a principal name for a servlet, which is used for the run-as role defined in web.xml</td>
</tr>
<tr>
<td>&quot;session-config Element&quot; on page 156</td>
<td>zero or one</td>
<td>Specifies the session manager, session cookie, and other session-related information</td>
</tr>
<tr>
<td>&quot;resource-env-ref Element&quot; on page 162</td>
<td>zero or more</td>
<td>Maps the absolute JNDI name to the resource-env-ref in the corresponding Java EE XML file</td>
</tr>
<tr>
<td>&quot;resource-ref Element&quot; on page 168</td>
<td>zero or more</td>
<td>Maps the absolute JNDI name to the resource-ref in the corresponding Java EE XML file</td>
</tr>
<tr>
<td>&quot;service-ref Element&quot; on page 163</td>
<td>zero or more</td>
<td>Specifies runtime settings for a web service reference</td>
</tr>
<tr>
<td>&quot;cache Element&quot; on page 170</td>
<td>zero or one</td>
<td>Configures caching for web application components</td>
</tr>
<tr>
<td>&quot;class-loader Element&quot; on page 179</td>
<td>zero or one</td>
<td>Specifies classloader configuration information</td>
</tr>
</tbody>
</table>
Elements in the sun-web.xml File

TABLE A-3  sun-web-app Subelements  (Continued)

<table>
<thead>
<tr>
<th>Element</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;jsp-config Element&quot; on page 180</td>
<td>zero or one</td>
<td>Specifies JSP configuration information</td>
</tr>
<tr>
<td>&quot;locale-charset-info Element&quot; on page 183</td>
<td>zero or one</td>
<td>Specifies internationalization settings</td>
</tr>
<tr>
<td>&quot;property Element&quot; on page 153</td>
<td>zero or more</td>
<td>Specifies a property, which has a name and a value</td>
</tr>
<tr>
<td>&quot;message-destination-name Element&quot; on page 185</td>
<td>zero or more</td>
<td>Specifies a logical message destination</td>
</tr>
<tr>
<td>&quot;webservice-description Element&quot; on page 186</td>
<td>zero or more</td>
<td>Specifies a web service description</td>
</tr>
</tbody>
</table>

Attributes

none

Properties

The following table describes the properties for the sun-web-app element.

TABLE A-4  sun-web-app Properties

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>crossContextAllowed</td>
<td>true</td>
<td>If true, allows this web application to access the contexts of other web applications using the ServletContext.getContext() method.</td>
</tr>
</tbody>
</table>
| encodeCookies         | true          | If true, Web Server URL encodes cookies before sending them to the client. If you don’t want cookies to be encoded, add the following setting to sun-web.xml directly under the <sun-web-app> tag:  
  <property name="encodeCookies" value="false"/>  
  Do not embed this setting in any other tag. |
### TABLE A-4 sun-web-app Properties (Continued)

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tempdir</td>
<td>instance_dir/generated/</td>
<td>Specifies a temporary directory for use by this web application. This value is used to construct the value of the javax.servlet.context.tempdir context attribute. Compiled JSPs are also placed in this directory.</td>
</tr>
<tr>
<td>singleThreadedServletPoolSize</td>
<td>5</td>
<td>Specifies the maximum number of servlet instances allocated for each SingleThreadModel servlet in the web application.</td>
</tr>
<tr>
<td>reuseSessionID</td>
<td>false</td>
<td>If true, this property causes the web application to reuse the JSESSIONID value (if present) in the request header as the session ID when creating sessions. The default behavior of web applications is not to reuse session IDs. Instead, applications generate cryptographically random session IDs for new sessions.</td>
</tr>
<tr>
<td>relativeRedirectAllowed</td>
<td>false</td>
<td>If true, allows the web application to send a relative URL to the client using the HttpServletResponse.sendRedirect() API (that is, it suppresses the container from translating a relative URL to a fully qualified URL).</td>
</tr>
</tbody>
</table>

**context-root Element**

This element contains the web context root of the application or web applications. This overrides the corresponding element in the web.xml file.

**Subelements**

none

**Attributes**

none
**property Element**

Specifies a property that has a name and a value. A property adds configuration information to its parent element that is:

- optional with respect to Web Server but Needed by a system or object that Web Server doesn’t have knowledge of, such as an LDAP server or a Java class

For example, a `manager-properties` element can include property subelements:

```xml
<manager-properties>
  <property name="reapIntervalSeconds" value="20"/>
</manager-properties>
```

The properties that `manager-properties` element uses depends on the value of the parent `session-manager` element `persistence-type` attribute. For details, see the description of the `session-manager` element.

**Subelement**

The following table describes subelement for the `property` element.

<table>
<thead>
<tr>
<th>Element</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;description Element&quot; on page 153</td>
<td>zero or one</td>
<td>Contains a text description of this element.</td>
</tr>
</tbody>
</table>

**Attributes**

The following table describes attributes for the `property` element.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>none</td>
<td>Specifies the name of the property or variable</td>
</tr>
<tr>
<td>value</td>
<td>none</td>
<td>Specifies the value of the property or variable</td>
</tr>
</tbody>
</table>

**description Element**

This element contains a text description of the parent element.

**Subelements**

none
Attributes
none

Security Elements
The security elements are as follows:

- "security-role-mapping Element" on page 154
- "servlet Element" on page 154
- "servlet-name Element" on page 155
- "role-name Element" on page 155
- "principal-name Element" on page 155
- "group-name Element" on page 156

security-role-mapping Element
This element maps roles to users or groups in the currently active realm.

Subelements
The following table describes subelements for the security-role-mapping element.

<table>
<thead>
<tr>
<th>Element</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;role-name Element&quot; on page 155</td>
<td>only one</td>
<td>Contains the role name</td>
</tr>
<tr>
<td>&quot;principal-name Element&quot; on page 155</td>
<td>requires at least one principal-name or group-name</td>
<td>Contains a principal (user) name in the current realm</td>
</tr>
<tr>
<td>&quot;group-name Element&quot; on page 156</td>
<td>requires at least one principal-name or group-name</td>
<td>Contains a group name in the current realm</td>
</tr>
</tbody>
</table>

Attributes
none

servlet Element
This element specifies a principal name for a servlet, which is used for the run-as role defined in web.xml.
Subelements

The following table describes subelements for the servlet element.

<table>
<thead>
<tr>
<th>Element</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;servlet-name Element&quot; on page 155</td>
<td>only one</td>
<td>Contains the name of a servlet, which is matched to a servlet-name in web.xml.</td>
</tr>
<tr>
<td>&quot;principal-name Element&quot; on page 155</td>
<td>only one</td>
<td>Contains a principal (user) name in the current realm.</td>
</tr>
</tbody>
</table>

Attributes

none

servlet-name Element

This element contains data that specifies the name of a servlet, which is matched to a servlet-name in web.xml. This name must be present in web.xml.

Subelements

none

Attributes

none

role-name Element

This element contains data that specifies the role-name in the security-role element of the web.xml file.

Subelements

none

Attributes

none

principal-name Element

This element contains data that specifies a principal (user) name in the current realm.
Elements in the sun-web.xml File

**Subelements**

none

**Attributes**

none

**group-name Element**

This element contains data that specifies a group name in the current realm.

**Subelements**

none

**Attributes**

none

### Session Elements

Session elements are as follows:

- "session-config Element" on page 156
- "session-manager Element" on page 157
- "manager-properties Element” on page 158
- "store-properties Element” on page 159
- "session-properties Element” on page 160
- “cookie-properties Element” on page 161

**Note** – The session manager interface is unstable. An unstable interface might be experimental or transitional. This interface therefore change change incompatibly, be removed, or be replaced by a more stable interface in the next release.

**session-config Element**

This element specifies session configuration information.

**Subelements**

The following table describes subelements for the session-config element.
### Elements

#### session-config Subelements

<table>
<thead>
<tr>
<th>Element</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;session-manager Element&quot; on page 157</td>
<td>zero or one</td>
<td>Specifies session manager configuration information</td>
</tr>
<tr>
<td>&quot;session-properties Element&quot; on page 160</td>
<td>zero or one</td>
<td>Specifies session properties</td>
</tr>
<tr>
<td>&quot;cookie-properties Element&quot; on page 161</td>
<td>zero or one</td>
<td>Specifies session cookie properties</td>
</tr>
</tbody>
</table>

### Attributes

none

**session-manager Element**

Specifications session manager information.

**Note** – As of Web Server, you cannot define a session manager either for a single sign-on session or for a virtual server. You must define session managers at the level of web applications.

### Subelements

The following table describes subelements for the session-manager element.

#### session-manager Subelements

<table>
<thead>
<tr>
<th>Element</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;manager-properties Element&quot; on page 158</td>
<td>zero or one</td>
<td>Specifies session manager properties.</td>
</tr>
<tr>
<td>&quot;store-properties Element&quot; on page 159</td>
<td>zero or one</td>
<td>Specifies session persistence (storage) properties.</td>
</tr>
</tbody>
</table>

### Attribute

The following table describes the persistence-type attribute for the session-manager element. The left column lists the attribute name, the middle column indicates the default value, and the right column describes what the attribute does.
Elements in the sun-web.xml File

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>persistence-type</td>
<td>memory</td>
<td>(Optional) Specifies the session persistence mechanism. Allowed values are memory, file, sIwS60, and mmap. Setting the value of persistence type to memory is equivalent to using Web Server's IwS60 without any store. Setting the value of persistence type to file is equivalent to using Web Server's IwS60 with FileStore.</td>
</tr>
</tbody>
</table>

**manager-properties Element**

This element specifies session manager properties.

**Subelement**

The following table describes the property subelement for the manager-properties element.

<table>
<thead>
<tr>
<th>Element</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;property Element&quot; on page 153</td>
<td>zero or more</td>
<td>Specifies a property, which has a name and a value.</td>
</tr>
</tbody>
</table>

**Attributes**

none

**Properties**

The following table describes properties for the manager-properties element.
TABLE A–13  manager-properties Properties

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>reapIntervalSeconds</td>
<td>60</td>
<td>Specifies the number of seconds between checks for expired sessions. Set this value lower than the frequency at which session data changes. For example, this value should be as low as possible 1 second for a hit counter servlet on a frequently accessed website or you could lose the last few hits each time you restart the server.</td>
</tr>
<tr>
<td>maxSessions</td>
<td>-1</td>
<td>Specifies the maximum number of active sessions, or -1 (the default) for no limit.</td>
</tr>
<tr>
<td>sessionFilename</td>
<td>none; state is not preserved across restarts</td>
<td>Specifies the absolute or relative path name of the file in which the session state is preserved between application restarts, if preserving the state is possible. A relative path name is relative to the temporary directory for this web application. Applicable only if the persistence-type attribute of the &quot;session-manager Element&quot; on page 157 element is memory.</td>
</tr>
</tbody>
</table>

store-properties Element

Specifies session persistence (storage) properties.

Subelement

The following table describes the property subelement for the store-properties element.

TABLE A–14  store-properties Subelement

<table>
<thead>
<tr>
<th>Element</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;property Element&quot; on page 153</td>
<td>zero or more</td>
<td>Specifies a property, which has a name and a value.</td>
</tr>
</tbody>
</table>

Attributes

none

Properties

The following table describes properties for the store-properties element.
TABLE A-15  store-properties Properties

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>reapIntervalSeconds</td>
<td>60</td>
<td>Specifies the number of seconds between checks for expired sessions for those sessions that are currently swapped out. Set this value lower than the frequency at which session data changes is recommended. For example, this value should be as low as possible 1 second for a hit counter servlet on a frequently accessed web site or you could lose the last few hits each time you restart the server.</td>
</tr>
<tr>
<td>directory</td>
<td>directory specified by javax.servlet.context .tempdir context attribute</td>
<td>Specifies the absolute or relative path name of the directory into which individual session files are written. A relative path is relative to the temporary work directory for this web application.</td>
</tr>
</tbody>
</table>

**session-properties Element**

This element specifies session properties.

**Subelements**

The following table describes the property subelement for the session-properties element.

TABLE A-16  session-properties Subelements

<table>
<thead>
<tr>
<th>Element</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;property Element&quot; on page 153</td>
<td>zero or more</td>
<td>Specifies a property, which has a name and a value.</td>
</tr>
</tbody>
</table>

**Attributes**

none

**Properties**

The following table describes properties for the session-properties element.
### Elements in the sun-web.xml File

**Table A-17**  
*session-properties Properties*

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>timeoutSeconds</td>
<td>600</td>
<td>Specifies the default maximum inactive interval (in seconds) for all sessions created in this web application. If set to 0, session expires immediately. If a session-timeout element is specified in the web.xml file, the session-timeout value overrides any timeoutSeconds value. If neither session-timeout nor timeoutSeconds is specified, the timeoutSeconds default is used. Note that the session-timeout element in web.xml is specified in minutes, not seconds.</td>
</tr>
</tbody>
</table>

| enableCookies    | true          | Uses cookies for session tracking if set to true. |
| enableURLRewriting| true          | Enables URL rewriting. This provides session tracking via URL rewriting when the browser does not accept cookies. You must also use an encodeURL or encodeRedirectURL call in the servlet or JSP. |

**cookie-properties Element**

This element specifies session cookie properties.

**Subelement**

The following table describes the property subelement for the cookie-properties element.

**Table A-18**  
*cookie-properties Subelement*

<table>
<thead>
<tr>
<th>Element</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>“property Element” on page 153</td>
<td>zero or more</td>
<td>Specifies a property, which has a name and a value</td>
</tr>
</tbody>
</table>

**Attributes**

none

**Properties**

The following table describes properties for the cookie-properties element.
Elements in the sun-web.xml File

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cookiePath</td>
<td>Context path at which the web application is installed.</td>
<td>Specifies the path name that is set when the session tracking cookie is created. The browser sends the cookie if the path name for the request contains this path name. If set to / (root), the browser sends cookies to all URLs served by the Web Server. You can set the path to a narrower mapping to limit the request URLs to which the browser sends cookies.</td>
</tr>
<tr>
<td>cookieMaxAgeSeconds</td>
<td>-1</td>
<td>Specifies the expiration time (in seconds) after which the browser expires the cookie. The default value of -1 indicates that the cookie never expires.</td>
</tr>
<tr>
<td>cookieDomain</td>
<td>unset</td>
<td>Specifies the domain for which the cookie is valid.</td>
</tr>
<tr>
<td>cookieComment</td>
<td>Sun Java System Web Server session tracking cookie</td>
<td>Specifies the comment that identifies the session tracking cookie in the cookie file. Applications can provide a more specific comment for the cookie.</td>
</tr>
</tbody>
</table>

Reference Elements
Reference elements are as follows:

- “resource-env-ref Element” on page 162
- “resource-env-ref-name Element” on page 163
- “resource-ref Element” on page 168
- “service-ref Element” on page 163
- “res-ref-name Element” on page 168
- “default-resource-principal Element” on page 169
- “name Element” on page 169
- “password Element” on page 169
- “jndi-name Element” on page 170

resource-env-ref Element
This element maps the “res-ref-name Element” on page 168 in the corresponding Java EE web.xml file resource-env-ref entry to the absolute jndi-name of a resource.

Subelements
The following table describes subelements for the resource-env-ref element.
Elements in the sun-web.xml File

TABLE A–20  resource-env-ref Subelements

<table>
<thead>
<tr>
<th>Element</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>“resource-env-ref-name Element” on page 163</td>
<td>only one</td>
<td>Specifies the res-ref-name in the corresponding Java EE web.xml file resource-env-ref entry.</td>
</tr>
<tr>
<td>“jndi-name Element” on page 170</td>
<td>only one</td>
<td>Specifies the absolute jndi-name of a resource.</td>
</tr>
</tbody>
</table>

Attributes

none

resource-env-ref-name Element

Contains data that specifies the “res-ref-name Element” on page 168 in the corresponding Java EE web.xml file resource-env-ref entry.

Subelements

none

Attributes

none

service-ref Element

This element specifies the runtime settings for a web service reference. Runtime information is only needed in the following cases:

- To define the port used to resolve a container-managed port
- To define the default Stub/Call property settings for Stub objects
- To define the URL of a final WSDL document to be used instead of the one associated with service-ref in the standard Java EE deployment descriptor

TABLE A–21  service-ref Subelements

<table>
<thead>
<tr>
<th>Element</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>“service-ref-name Element” on page 164</td>
<td>only one</td>
<td>Specifies the web service reference name relative to java:comp/env</td>
</tr>
<tr>
<td>“port-info Element” on page 164</td>
<td>zero or more</td>
<td>Specifies information for a port within a web service reference</td>
</tr>
</tbody>
</table>
Elements in the sun-web.xml File

<table>
<thead>
<tr>
<th>Element</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>service-ref</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td>&quot;call-property Element&quot; on page 166</td>
<td>zero or more</td>
<td>Specifies JAX-RPC property values that can be set on a javax.xml.rpc. Call object before it is returned to the web service client</td>
</tr>
<tr>
<td>&quot;service-impl-class Element&quot; on page 167</td>
<td>zero or more</td>
<td>Specifies the name of the generated service implementation class</td>
</tr>
<tr>
<td>&quot;service-qname Element&quot; on page 167</td>
<td>zero or one</td>
<td>Specifies the WSDL service element that is being referenced.</td>
</tr>
</tbody>
</table>

**service-ref-name Element**

This element specifies the web service reference name relative to java:comp/env.

**Subelements**

none

**Attributes**

none

**port-info Element**

Either a service-endpoint-interface or a wsdl-port or both ports must be specified. If both ports are specified, wsdl-port specifies the port that the container chooses for container-managed port selection. The same wsdl-port value must not appear in more than one port-info element within the same service-ref. If a service-endpoint-interface is using container-managed port selection, its value must not appear in more than one port-info element within the same service-ref.

**Subelements**

The following table describes subelements for the port-info element.

<table>
<thead>
<tr>
<th>Element</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;service-endpoint-interface Element&quot; on page 165</td>
<td>zero or one</td>
<td>Specifies the web service reference name relative to java:comp/env.</td>
</tr>
<tr>
<td>&quot;wsdl-port Element&quot; on page 165</td>
<td>zero or one</td>
<td>Specifies the WSDL port.</td>
</tr>
</tbody>
</table>


Elements in the *sun-web.xml* File

### TABLE A–22  port-info Subelements (Continued)

<table>
<thead>
<tr>
<th>Element</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;stub-property Element&quot; on page 166</td>
<td>zero or one</td>
<td>Specifies JAX-RPC property values that are set on the <code>javax.xml.rpc.Stub</code> object before it is returned to the web service client.</td>
</tr>
<tr>
<td>&quot;call-property Element&quot; on page 166</td>
<td>zero or one</td>
<td>Specifies JAX-RPC property values that are set on the <code>javax.xml.rpc.Stub</code> object before it is returned to the web service client.</td>
</tr>
<tr>
<td>&quot;message-security-binding Element&quot; on page 110</td>
<td>zero or one</td>
<td>Specifies a custom authentication provider binding.</td>
</tr>
</tbody>
</table>

**service-endpoint-interface Element**

This element specifies the web service reference name relative to `java:comp/env`.

**Subelements**

none

**Attributes**

none

**wsdl-port Element**

Specifies the WSDL port.

**Subelements**

The following table describes subelements for the `wsdl-port` element

<table>
<thead>
<tr>
<th>Element</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;namespaceURI Element&quot; on page 165</td>
<td>only one</td>
<td>Specifies the namespace URI.</td>
</tr>
<tr>
<td>&quot;localpart Element&quot; on page 166</td>
<td>only one</td>
<td>Specifies the local part of a QName.</td>
</tr>
</tbody>
</table>

**namespaceURI Element**

This element specifies the namespace URI.
Subelements

none

Attributes

none

localpart Element

Specifies the local part of a QName.

Subelements

none

Attributes

none

stub-property Element

This element specifies JAX-RPC property values that are set on a javax.xml.rpc.Stub object before it is returned to the web service client. The property names can be any properties supported by the JAX-RPC Stub implementation.

Subelements

The following table describes subelements for the stub-property element.

<table>
<thead>
<tr>
<th>Element</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;name Element&quot; on page 169</td>
<td>only one</td>
<td>Specifies the name of the entity.</td>
</tr>
<tr>
<td>&quot;value Element&quot; on page 179</td>
<td>only one</td>
<td>Specifies the value of the entity.</td>
</tr>
</tbody>
</table>

call-property Element

This element specifies JAX-RPC property values that can be set on a javax.xml.rpc.Call object before it is returned to the web service client. The property names can be any properties supported by the JAX-RPC Call implementation.
**Table A–25** call-property Subelements

<table>
<thead>
<tr>
<th>Element</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>“name Element” on page 169</td>
<td>only one</td>
<td>Specifies the name of the entity.</td>
</tr>
<tr>
<td>“value Element” on page 179</td>
<td>only one</td>
<td>Specifies the value of the entity.</td>
</tr>
</tbody>
</table>

**wsdl-override Element**

This element specifies a valid URL pointing to a final WSDL document. If not specified, the WSDL document associated with the `service-ref` in the standard J2EE deployment descriptor is used.

**Subelements**

none

**Attributes**

none

**service-impl-class Element**

Specifies the name of the generated service implementation class.

**Subelements**

none

**Attributes**

none

**service-qname Element**

This element specifies the WSDL service element that is being referred to.

**Subelements**

The following table describes subelements for the `service-qname` element.

**Table A–26** service-qname Subelements

<table>
<thead>
<tr>
<th>Element</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
</table>

Appendix A • Deployment Descriptor Files
Elements in the sun-web.xml File

Table A–26  service-qname Subelements (Continued)

<table>
<thead>
<tr>
<th>Element Type</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>namespaceURI Element</td>
<td>only one</td>
<td>Specifies the namespace URI.</td>
</tr>
<tr>
<td>localpart Element</td>
<td>only one</td>
<td>Specifies the local part of a QName.</td>
</tr>
</tbody>
</table>

resource-ref Element

This element maps the "res-ref-name Element" on page 168 in the corresponding Java EE web.xml file resource-ref entry to the absolute "jndi-name Element" on page 170 of a resource.

Subelements

The following table describes subelements for the resource-ref element. The left column lists the subelement name, the middle column indicates the requirement rule, and the right column describes what the element does.

Table A–27  resource-ref Subelements

<table>
<thead>
<tr>
<th>Element Type</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>res-ref-name Element</td>
<td>only one</td>
<td>Specifies the res-ref-name in the corresponding Java EE web.xml file resource-ref entry</td>
</tr>
<tr>
<td>jndi-name Element</td>
<td>only one</td>
<td>Specifies the absolute jndi-name of a resource</td>
</tr>
<tr>
<td>default-resource-principal Element</td>
<td>zero or one</td>
<td>Specifies the default principal (user) for the resource</td>
</tr>
</tbody>
</table>

Attributes

none

res-ref-name Element

This element contains data that specifies the res-ref-name in the corresponding Java EE web.xml file resource-ref entry.

Subelements

none

Attributes

none
**default-resource-principal** **Element**
This element specifies the default principal (user) for the resource.

If this element is used in conjunction with a JMS Connection Factory resource, the name and password subelements must be valid entries in Message Queue's broker user repository.

**Subelements**
The following table describes subelements for the **default-resource-principal** element.

<table>
<thead>
<tr>
<th>Element</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;name Element&quot; on page 169</td>
<td>only one</td>
<td>Contains the name of the principal</td>
</tr>
<tr>
<td>&quot;password Element&quot; on page 169</td>
<td>only one</td>
<td>Contains the password for the principal</td>
</tr>
</tbody>
</table>

**Attributes**
none

**name Element**
This element contains data that specifies the name of the principal.

**Subelements**
none

**Attributes**
none

**password Element**
This element contains data that specifies the password for the principal.

**Subelements**
none

**Attributes**
none
**jndi-name Element**

This element contains data that specifies the absolute `jndi-name` of a URL resource or a resource in the `server.xml` file.

**Note** – To avoid collisions with names of other enterprise resources in JNDI, and to avoid portability problems, all names in a Web Server application should begin with the string `java:comp/env`.

**Subelements**

none

**Attributes**

none

**Caching Elements**

For details about response caching as it pertains to servlets, see “Caching Servlet Results” on page 46 and “JSP Cache Tags” on page 61.

Caching elements are as follows:

- “cache Element” on page 170
- “cache-helper Element” on page 172
- “default-helper” on page 173
- “cache-mapping Element” on page 174
- “url-pattern Element” on page 175
- “cache-helper-ref Element” on page 175
- “timeout Element” on page 176
- “refresh-field Element” on page 176
- “http-method Element” on page 177
- “key-field Element” on page 177
- “constraint-field Element” on page 178
- “value Element” on page 179

**cache Element**

This element configures caching for web application components.

**Subelements**

The following table describes subelements for the cache element.
TABLE A–29  cache Subelements

<table>
<thead>
<tr>
<th>Element</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>“cache-helper Element” on page 172</td>
<td>zero or more</td>
<td>Specifies a custom class that implements the CacheHelper interface.</td>
</tr>
<tr>
<td>“default-helper” on page 173</td>
<td>zero or one</td>
<td>Allows you to change the properties of the default, built-in cache-helper class.</td>
</tr>
<tr>
<td>“property Element” on page 153</td>
<td>zero or more</td>
<td>Specifies a cache property, which has a name and a value.</td>
</tr>
<tr>
<td>“cache-mapping Element” on page 174</td>
<td>zero or more</td>
<td>Maps a URL pattern or a servlet name to its cacheability constraints.</td>
</tr>
</tbody>
</table>

Attributes

The following table describes attributes for the cache element.

TABLE A–30  cache Attributes

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>max-entries</td>
<td>4096</td>
<td>(Optional) Specifies the maximum number of entries the cache can contain. Must be a positive integer.</td>
</tr>
<tr>
<td>timeout-in-seconds</td>
<td>30</td>
<td>(Optional) Specifies the maximum amount of time in seconds that an entry can remain in the cache after it is created or refreshed. Can be overridden by a timeout element.</td>
</tr>
<tr>
<td>enabled</td>
<td>false</td>
<td>(Optional) Determines whether servlet and JSP caching is enabled. Legal values are on, off, yes, no, 1, 0, true, false.</td>
</tr>
</tbody>
</table>

Properties

The following table describes properties for the cache element.

TABLE A–31  cache Properties

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cacheClassName</td>
<td>com.sun.appserv.web.cache.LruCache</td>
<td>Specifies the fully qualified name of the class that implements the cache functionality. For a list of valid values, see “Cache Class Names” on page 172.</td>
</tr>
</tbody>
</table>
### TABLE A-31  cache Properties  

(Continued)

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MultiLRUSegmentSize</td>
<td>4096</td>
<td>Specifies the number of entries in a segment of the cache table that should have its own LRU (least recently used) list. Applicable only if cacheClassName is set to com.sun.appserv.web .cache.MultiLruCache.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MaxSize</td>
<td>unlimited; Long.MAX_VALUE</td>
<td>Specifies an upper bound on the cache memory size in bytes (KB or MB units). Example values are 32 KB or 2 MB. Applicable only if cacheClassName is set to com.sun.appserv.web .cache.BoundedMultiLruCache.</td>
</tr>
</tbody>
</table>

### Cache Class Names

The following table lists possible values of the cacheClassName property.

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>com.sun.appserv.web.cache.LruCache</td>
<td>A bounded cache with an LRU (least recently used) cache replacement policy.</td>
</tr>
<tr>
<td>com.sun.appserv.web.cache.BaseCache</td>
<td>An unbounded cache suitable if the maximum number of entries is known.</td>
</tr>
<tr>
<td>com.sun.appserv.web.cache.BoundedMultiLruCache</td>
<td>A cache suitable for limiting the cache size by memory rather than number of entries. Uses the MaxSize property.</td>
</tr>
</tbody>
</table>

### cache-helper Element

This element specifies a class that implements the CacheHelper interface. For details, see “CacheHelper Interface” on page 48.

### Subelement

The following table describes the property subelements for the cache-helper element.
TABLE A–33  cache-helper Subelement

<table>
<thead>
<tr>
<th>Element</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;property Element&quot; on page 153</td>
<td>zero or more</td>
<td>Specifies a property, which has a name and a value.</td>
</tr>
</tbody>
</table>

Attributes

The following table describes attributes for the cache-helper element.

TABLE A–34  cache-helper Attributes

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>default</td>
<td>Specifies a unique name for the helper class, which is referenced in the cache-mapping element.</td>
</tr>
<tr>
<td>class-name</td>
<td>none</td>
<td>Specifies the fully qualified class name of the cache helper, which must implement the com.sun.appserv.web.CacheHelper interface.</td>
</tr>
</tbody>
</table>

default-helper

This element allows you to change the properties of the built-in default cache-helper class.

Subelement

The following table describes the property subelements for the default-helper element.

TABLE A–35  default-helper Subelements

<table>
<thead>
<tr>
<th>Element</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;property Element&quot; on page 153</td>
<td>zero or more</td>
<td>Specifies a property, which has a name and a value.</td>
</tr>
</tbody>
</table>

Attributes

none

Property

The following table describes the cacheKeyGeneratorAttrName properties for the default-helper element.
Elements in the sun-web.xml File

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cacheKeyGeneratorAttrName</td>
<td>Uses the built-in default cache-helper key generation, which concatenates the servlet path with key-field values, if any</td>
<td>The caching engine looks in the ServletContext for an attribute with a name equal to the value specified for this property to determine whether a customized CacheKeyGenerator implementation is used. An application provide a customized key generator rather than using the default helper. See &quot;CacheKeyGenerator Interface&quot; on page 50.</td>
</tr>
</tbody>
</table>

**cache-mapping Element**

This element maps a URL pattern or a servlet name to its cacheability constraints.

**Subelements**

The following table describes subelements for the cache-mapping element.

<table>
<thead>
<tr>
<th>Element</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;servlet-name Element&quot; on page 155</td>
<td>requires one servlet-name or url-pattern</td>
<td>Contains the name of a servlet.</td>
</tr>
<tr>
<td>&quot;url-pattern Element&quot; on page 175</td>
<td>requires one servlet-name or url-pattern</td>
<td>Contains a servlet URL pattern for which caching is enabled.</td>
</tr>
<tr>
<td>&quot;cache-helper-ref Element&quot; on page 175</td>
<td>required if timeout, refresh-field, http-method, key-field, and constraint-field are not used</td>
<td>Contains the name of the cache-helper used by the parent cache-mapping element.</td>
</tr>
<tr>
<td>&quot;cache-mapping Element&quot; on page 174</td>
<td>zero or more</td>
<td>Specifies the RequestDispatcher methods for which caching is to be enabled on the target resource. Valid values are REQUEST, FORWARD, INCLUDE, and ERROR (default: REQUEST).</td>
</tr>
<tr>
<td>&quot;timeout Element&quot; on page 176</td>
<td>zero or one if cache-helper-ref is not used</td>
<td>Contains the cache-mapping specific maximum amount of time in seconds that an entry can remain in the cache after it is created or refreshed</td>
</tr>
</tbody>
</table>
### Attributes

none

#### `url-pattern` Element

This element contains data that specifies a servlet URL pattern for which caching is enabled. See the Java Servlet 2.5 specification.

#### Subelements

none

#### Attributes

none

#### `cache-helper-ref` Element

This element contains data that specifies the name of the cache-helper used by the parent cache-mapping element.

#### Subelements

none

#### Attributes

none
timeout **Element**

Contains data that specifies the cache-mapping specific maximum amount of time in seconds that an entry can remain in the cache after it is created or refreshed. If not specified, the default is the value of the `timeout` attribute of the cache element.

**Subelements**

none

**Attributes**

The following table describes attributes for the `timeout` element.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>none</td>
<td>Specifies the timeout input parameter, whose value is interpreted in seconds. The field's type must be <code>java.lang.Long</code> or <code>java.lang.Integer</code>.</td>
</tr>
<tr>
<td>scope</td>
<td>context.attribute</td>
<td>(Optional) Specifies the scope in which the input parameter can be present. Allowed values are <code>context.attribute</code>, <code>request.header</code>, <code>request.parameter</code>, <code>request.cookie</code>, <code>session.id</code>, and <code>session.attribute</code>.</td>
</tr>
</tbody>
</table>

refresh-field **Element**

This element specifies a field that gives the application component a programmatic way to refresh a cached entry.

**Subelements**

none

**Attributes**

The following table describes attributes for the `refresh-field` element.
## Attributes

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>none</td>
<td>Specifies the input parameter name. If the parameter is present in the specified scope and its value is true, the cache will be refreshed.</td>
</tr>
<tr>
<td>scope</td>
<td>request.parameter</td>
<td>(Optional) Specifies the scope in which the input parameter can be present. Allowed values are context.attribute, request.header, request.parameter, request.cookie, session.id, and session.attribute.</td>
</tr>
</tbody>
</table>

### http-method Element

This element contains data that specifies an HTTP method that is eligible for caching. The default is GET.

#### Subelements

- none

#### Attributes

- none

### key-field Element

Specifies a component of the key used to look up and extract cache entries. The web container looks for the named parameter, or field, in the specified scope.

If this element is not present, the web container uses the Servlet Path, the path section that corresponds to the servlet mapping that activated the current request. See the Servlet 2.5 specification, section SRV 4.4, for details on the Servlet Path.

#### Subelements

- none

#### Attributes

The following table describes attributes for the key-field element.
### TABLE A–40  Key-field Attributes

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>none</td>
<td>Specifies the input parameter name.</td>
</tr>
<tr>
<td>scope</td>
<td>request.parameter</td>
<td>(Optional) Specifies the scope in which the input parameter can be present. Allowed values are context.attribute, request.header, request.parameter, request.cookie, session.id, and session.attribute.</td>
</tr>
</tbody>
</table>

### constraint-field Element

Specifies a cache ability constraint for the given url-pattern or servlet-name.

All constraint-field constraints must pass for a response to be cached. If value constraints are listed, at least one of them must pass.

### Subelement

The following table describes the value subelements for the constraint-field element.

### TABLE A–41  constraint-field Subelements

<table>
<thead>
<tr>
<th>Element</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;value Element” on page 179</td>
<td>zero or more</td>
<td>Contains a value to be matched to the input parameter value</td>
</tr>
</tbody>
</table>

### Attributes

The following table describes attributes for the constraint-field element.

### TABLE A–42  constraint-field Attributes

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>none</td>
<td>Specifies the input parameter name.</td>
</tr>
<tr>
<td>scope</td>
<td>request.parameter</td>
<td>(Optional) Specifies the scope in which the input parameter can be present. Allowed values are context.attribute, request.header, request.parameter, request.cookie, session.id, and session.attribute.</td>
</tr>
<tr>
<td>cache-on-match</td>
<td>true</td>
<td>(Optional) If true, caches the response if matching succeeds. Overrides the same attribute in a value subelement.</td>
</tr>
</tbody>
</table>
value Element
This element specifies the value of the entity

Subelements
none

Attributes
none

Classloader Element
The Classloader element is named class-loader.

■ “class-loader Element” on page 179

class-loader Element
This element configures the classloader for the web application.

Subelements
none

Attributes
The following table describes attributes for the class-loader element.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>extra-class-path</td>
<td>null</td>
<td>(Optional) Specifies additional classpath settings for this web application. If this path is not an absolute path, it is treated as relative to &lt;web-app&gt; &lt;path&gt; value.</td>
</tr>
</tbody>
</table>
### JSP Element

The JSP elements is `jsp-config`.

- **“jsp-config Element” on page 180**

#### jsp-config Element

This element specifies JSP configuration information that enables web application to customize the compilation and execution of its JSP files.

#### Subelement

The following table describes the name subelement for the `jsp-config` element.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>delegate</td>
<td>false</td>
<td>(Optional) If true, the web application follows the standard classloader delegation model and delegates to its parent classloader first before looking in the local classloader. If false, the web application follows the delegation model specified in the Servlet specification and looks in its classloader before looking in the parent classloader. For a web component of a web service, you must set this value to true. Legal values are on, off, yes, no, 1, 0, true, false.</td>
</tr>
<tr>
<td>dynamic-reload-interval</td>
<td>value of the dynamicreloadinterval attribute of the <code>&lt;jvm&gt;</code> element in server.xml</td>
<td>(Optional) Enables an application to override the dynamicreloadinterval setting in server.xml. Specifies the frequency (in seconds) at which a web application is checked for modifications, and then reloaded if modifications have been made. Setting this value to less than or equal to 0 disables dynamic reloading of the application. If not specified, the value from server.xml is used. For more information about server.xml, see Sun Java System Web Server 7.0 Update 6 Administrator’s Configuration File Reference.</td>
</tr>
</tbody>
</table>
### TABLE A-44  **jsp-config Subelements**

<table>
<thead>
<tr>
<th>Element</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;name Element&quot; on page 169</td>
<td>zero or more</td>
<td>Specifies a property.</td>
</tr>
</tbody>
</table>

### Attributes

none

### Properties

The following table describes properties for the jsp-config element.

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ieClassId</td>
<td>clsid:8AD9C840-044E-11D1-B3E9-00805F499D93</td>
<td>The Java Plug-in COM class ID for Internet Explorer. Used by the (<a href="">jsp:plugin</a>) tags.</td>
</tr>
<tr>
<td>javaCompilerPlugin</td>
<td>internal JDK compiler (javac)</td>
<td>This property is deprecated in this release. By this, we mean this is supported in 7.0 but will NOT be supported in future release. If JSP Pages import classes from unnamed packages, the default-JDK compiler will throw a compile time error when JSP-generated servlets are compiled. To compile JSP-generated servlets, set the javaCompilerPlugin property to org.apache.jasper.compiler.SunJavaCompiler. Note: The jspc command-line compiler for JSPs no longer supports -javac option. Since this property is deprecated, you are strongly encouraged to modify JSPs so that the imported classes have a package name. See also the -deprecatedjavac switch of jspc, described in &quot;Compiling JSPs Using the Command-Line Compiler&quot; on page 58.</td>
</tr>
</tbody>
</table>

See also the `-deprecatedjavac` switch of jspc, described in "Compiling JSPs Using the Command-Line Compiler" on page 58.
<table>
<thead>
<tr>
<th>Property Name</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>javaEncoding</td>
<td>UTF8</td>
<td>Specifies the encoding for the generated Java servlet. This encoding is passed to the Java compiler used to compile the servlet as well. By default, the web container tries to use UTF8. If that fails, it tries to use the <code>javaEncoding</code> value. For encodings you can use, see: <a href="http://java.sun.com/j2se/1.5.0/docs/guide/intl/encoding.doc.html">http://java.sun.com/j2se/1.5.0/docs/guide/intl/encoding.doc.html</a></td>
</tr>
<tr>
<td>classdebuginfo</td>
<td>false</td>
<td>Specifies whether the generated Java servlets should be compiled with the debug option set (-g for javac).</td>
</tr>
<tr>
<td>keepgenerated</td>
<td>true</td>
<td>If set to true, keeps the generated Java files. If false, deletes the Java files.</td>
</tr>
<tr>
<td>mappedfile</td>
<td>false</td>
<td>If set to true, generates separate write calls for each HTML line and comments that describe the location of each line in the JSP file. By default, all adjacent write calls are combined and no location comments are generated.</td>
</tr>
<tr>
<td>scratchdir</td>
<td>Default work directory for the web application</td>
<td>The working directory created for storing all of the generated code.</td>
</tr>
<tr>
<td>reload-interval</td>
<td>0</td>
<td>Specifies the frequency (in seconds) at which JSP files are checked for modifications. Setting this value to 0 checks JSPs for modifications on every request. Setting this value to -1 disables checks for JSP modifications and JSP recompilation.</td>
</tr>
<tr>
<td>initial-capacity</td>
<td>32</td>
<td>Specifies the initial size of the hash table of compiled JSP classes (see the following example).</td>
</tr>
</tbody>
</table>

The following example illustrates the use of the `initial-capacity` property described in the table above. The example shows how you would configure a value of 1024:

```xml
<jsp-config> <property name="initial-capacity" value="1024" /></jsp-config>
```
Internationalization Elements

The internationalization elements are as follows:

- "parameter-encoding Element" on page 183
- "locale-charset-info Element" on page 183
- "locale-charset-map Element" on page 184

**parameter-encoding Element**

This element specifies a hidden field or default character set that determines the character encoding the web container uses to decode parameters for `request.getParameter` calls when the character set is not set in the request's `Content-Type`.

For encodings you can use, see

http://java.sun.com/j2se/1.4.2/docs/guide/intl/encoding.doc.html.

**Attributes**

The following table describes attributes for the `parameter-encoding` element.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>form-hint-field</td>
<td>none</td>
<td>The value of the hidden field in the form that specifies the parameter encoding.</td>
</tr>
<tr>
<td>default-charset</td>
<td>none</td>
<td>This value is used for parameter encoding if neither <code>request.setCharacterEncoding()</code> is called nor <code>form-hint-field</code> is found in the request.</td>
</tr>
</tbody>
</table>

**Subelements**

none

**Attributes**

none

**locale-charset-info Element**

Specifies the mapping between the locale and the character encoding that should be set in the `Content-type` header of the response if a servlet or JSP sets the response locale using the `ServletResponse.setLocale` method. This setting overrides the web container's default locale-to-charset mapping.
Subelements

The following table describes subelements for the `locale-charset-info` element.

<table>
<thead>
<tr>
<th>Element</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>locale-charset-map</code> Element</td>
<td>one or more</td>
<td>Maps a locale to a character set. Used only for request processing, and only if no <code>parameter-encoding</code> is defined.</td>
</tr>
<tr>
<td><code>parameter-encoding</code> Element</td>
<td>zero or one</td>
<td>Deprecated. Use the <code>parameter-encoding</code> element under <code>sun-web-app</code> instead. This setting is supported only for backward compatibility with applications developed under Web Server.</td>
</tr>
</tbody>
</table>

Attributes

The following table describes the `default-locale` attribute for the `locale-charset-info` element.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>DefaultValue</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default-locale</td>
<td>none</td>
<td>Although a value is required, the value is ignored. Use the <code>default-charset</code> attribute of the <code>parameter-encoding</code> element instead.</td>
</tr>
</tbody>
</table>

`locale-charset-map` Element

This element maps a locale to a specific character encoding.

For encodings you can use, see:

http://java.sun.com/j2se/1.4.2/docs/guide/intl/encoding.doc.html

Attributes

The following table describes attributes for the `locale-charset-map` element.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>DefaultValue</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>locale</td>
<td>none</td>
<td>Specifies the locale name.</td>
</tr>
</tbody>
</table>
The following table provides a `locale-charset-map` example, listing the locale and the corresponding charset:

**TABLE A–50 locale-charset-map Example**

<table>
<thead>
<tr>
<th>Locale</th>
<th>Charset</th>
</tr>
</thead>
<tbody>
<tr>
<td>ja</td>
<td>EUC-JP</td>
</tr>
<tr>
<td>zh</td>
<td>UTF-8</td>
</tr>
</tbody>
</table>

**message-destination Element**

This element specifies the name of a logical message-destination defined within an application. The `message-destination-name` matches the corresponding `message-destination-name` in the corresponding Java EE deployment descriptor file.

**Subelements**

The following table describes subelements for the `message-destination` element.

**TABLE A–51 message-destination Subelements**

<table>
<thead>
<tr>
<th>Elements</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;message-destination-name Element&quot; on page 185</td>
<td>only one</td>
<td>Specifies the name of a logical message destination defined within the corresponding Java EE deployment descriptor file</td>
</tr>
<tr>
<td>&quot;jndi-name Element&quot; on page 170</td>
<td>only one</td>
<td>Specifies the <code>jndi-name</code> of the associated entity</td>
</tr>
</tbody>
</table>

**message-destination-name Element**

This element specifies the name of a logical message destination defined within the corresponding Java EE deployment descriptor file.

**Subelements**

none
**webservice-description** Element

This element specifies a name and optional publish location for a web service.

**Subelements**

The following table describes subelements for the `webservice-description` element.

<table>
<thead>
<tr>
<th>Element</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;webservice-description-name Element&quot; on page 186</td>
<td>only one</td>
<td>Specifies a unique name for the web service within a web</td>
</tr>
<tr>
<td>&quot;wsdl-publish-location Element&quot; on page 186</td>
<td>zero or one</td>
<td>Specifies the URL of a directory to which the web services WSDL is published during deployment</td>
</tr>
</tbody>
</table>

**Attributes**

none

**webservice-description-name** Element

This element specifies a unique name for the web service within a web.

**Subelements**

none

**Attributes**

none

**wsdl-publish-location** Element

This element specifies the URL of a directory to which a web service's WSDL is published during deployment. Any required files are published to this directory, preserving their location relative to the module-specific WSDL directory (`META-INF/wsdl` or `WEB-INF/wsdl`).

**Subelements**

none

**Attributes**

none
Alphabetical List of sun-web.xml Elements

This section provides an alphabetical list for the easy lookup of sun-web.xml elements.

“cache Element” on page 170
“cache-helper Element” on page 172
“cache-helper-ref Element” on page 175
“cache-mapping Element” on page 174
“class-loader Element” on page 179
“constraint-field Element” on page 178
“context-root Element” on page 152
“cookie-properties Element” on page 161
“default-helper” on page 173
“default-resource-principal Element” on page 169
“description Element” on page 153
“group-name Element” on page 156
“http-method Element” on page 177
“jndi-name Element” on page 170
“jsp-config Element” on page 180
“key-field Element” on page 177
“locale-charset-info Element” on page 183
“locale-charset-map Element” on page 184
“manager-properties Element” on page 158
“message-destination Element” on page 185
“message-destination-name Element” on page 185
“message-security-binding Element” on page 110
“name Element” on page 169
“parameter-encoding Element” on page 183
Elements in the sun-web.xml File

"password Element" on page 169
"principal-name Element" on page 155
"property Element" on page 153
"refresh-field Element" on page 176
"res-ref-name Element" on page 168
"resource-env-ref Element" on page 162
"resource-env-ref-name Element" on page 163
"resource-ref Element" on page 168
"role-name Element" on page 155
"security-role-mapping Element" on page 154
"servlet Element" on page 154
"servlet-name Element" on page 155
"service-ref Element" on page 163
"session-config Element" on page 156
"session-manager Element" on page 157
"session-properties Element" on page 160
"store-properties Element" on page 159
"sun-web-app Element" on page 150
"timeout Element" on page 176
"url-pattern Element" on page 175
"value Element" on page 179
"webservice-description Element" on page 186
"webservice-description-name Element" on page 186
"webservice-endpoint Element" on page 109
Sample Web Application XML Files

This section includes sample web.xml and sun-web.xml files

- “Sample web.xml File” on page 189
- “Sample sun-web.xml File” on page 190

Sample web.xml File

The following is the sample web.xml file.

```xml
<web-app xmlns="http://java.sun.com/xml/ns/j2ee"
     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
     xsi:schemaLocation="http://java.sun.com/xml/ns/j2ee
http://java.sun.com/xml/ns/j2ee/web-app_2_4.xsd"
     version="2.5">
  <!--
  Copyright 2006 Sun Microsystems, Inc. All rights reserved.
  -->

  <servlet>
    <servlet-name>ServCache</servlet-name>
    <servlet-class>samples.webapps.caching.ServCache</servlet-class>
    <load-on-startup>0</load-on-startup>
  </servlet>

  <session-config>
    <session-timeout>30</session-timeout>
  </session-config>

  <taglib>
```

Note – For a list of sun-web.xml elements by category, see “Elements in the sun-web.xml File” on page 149.
Sample sun-web.xml File

The following example shows a sample sun-web.xml file.

```xml
<!DOCTYPE sun-web-app PUBLIC "-//Sun Microsystems, Inc.//DTD Application Server 8.1 Servlet 2.5//EN" "http://www.sun.com/software/appserver/dtdds/sun-web-app_2_4-1.dtd">

<!--
Copyright 2006 Sun Microsystems, Inc. All rights reserved.
-->

<sun-web-app>

    <session-config>
    <session-manager/>
    </session-config>

    <cache enabled="true" timeout-in-seconds="300">

        <cache-mapping>
        <servlet-name>ServCache</servlet-name>
        <key-field name="inputtext" scope="request.parameter"/>
        <constraint-field name="inputtext" scope="request.parameter">
        <value>one</value>
        <value>two</value>
        </constraint-field>
        </cache-mapping>
    </cache>

</sun-web-app>
```
Index

A
about
JSPs, 57-58
servlets, 45-46
sessions, 75-76
web applications, 25
accessing a session, 77-78
Admin Console, more information about, 12
Administration Console, using to, use Optimize it profiler, 141
Administration interface, using to, enable or disable web applications, 130
AllPermission, 118
application permissions, 118-119
default, 118
application role mapping, 99
ATTLIST tags, 146
auth-constraint, 106
authentication, 98, 100
authentication, 98, 100
ACL-based, 100-101
by servlets, 103-104
for single sign-on, 104-105
HTTP basic, 103
Java EE/Servlet-based, 101
secure web applications, 102
SSL mutual, 103
authorization, 98, 100
ACL-based, 100-101
by servlets, 105-106
client certificate, 107
certificates, 106
Java EE/Servlet-based, 101
authorization (Continued)
secure web applications, 102
B
binding objects to sessions, 79-80
Bootstrap Classloader, 134
C
cache class names, 172
cache element, 170-172
cache-helper, 172-173
cache-helper-ref, 175
cache-mapping, 174-175
cache tags, 61-64
cacheClassName property, 172
CacheHelper interface, 48-49
CacheKeyGenerator interface, 50-51
caching
default cache configuration, 48
example, 49-50
JSP, 61-64
servlet results, 46-51
Sun Java System Web Server features, 47
class-loader, 134, 179-180
classloaders, 132-134
Bootstrap, 134
Common, 134
JSP, 134
runtime hierarchy, 132
classloaders (Continued)
    System, 134
    Web Application, 133, 134
client
    certificates, 107
Common Classloader, 134
compiling JSPs, 58-60
configuring, 138
    servlet authorization constraints, 106
constraint-field, 178-179
cookie-properties, 161-162
cookies, 75, 76, 105, 161
cookies, encoding, 151
creating
    sessions, 77-78
    web deployment descriptors, 125
customizing search, 65-73

D
debugging
    enabling, 135-136
    generating stack trace for, 137-138
    JPDA options, 136
    JSPs, 137
    using log files, 138
    using NetBeans, 137
    using profilers, 139-142
    web applications, 135-142
default-helper, 173-174
default-resource-principal, 169
defining
    security roles, 106
    servlet authorization constraints, 106
deleting web applications, 126
deploying web applications, 121-134
deployment descriptor files
    sun-web.xml, 125
description element, 153-154
disabling web applications, 130
DTD files, 144
    attributes, 146
    data, 145-146
    subelements, 145

E
editing server.xml
    for debugging, 135
    to configure single sign-on, 105
elements in sun-web.xml, 149-189
    alphabetical list of, 187-189
    caching, 170-179
    classloader, 179-180
    general, 150-154
    internationalization, 183-186
    JSP, 180-182
    reference, 162-170
    security, 154-156
    session, 156-162
enabling
    debugging, 135-136
    IWS60, 84-85
    memory, 81
    the Java Security Manager, 117-118
    web applications, 130
encodeCookies, 151
examples
    caching, 49-50
    sun-web.xml file, 190
    web.xml file, 189-190

F
fetching client certificates, 107
file, manager properties, 83
FileStore.java, 89
form-based login, 104

DTD files (Continued)
    sun-web-app_2_4-1.dtd, 144-146
dynamic-reload-interval attribute, 180
dynamic reloading of web applications, 131-132
dynamicreloadinterval, 180

elements in sun-web.xml, 149-189
    alphabetical list of, 187-189
    caching, 170-179
    classloader, 179-180
    general, 150-154
    internationalization, 183-186
    JSP, 180-182
    reference, 162-170
    security, 154-156
    session, 156-162
enabling
    debugging, 135-136
    IWS60, 84-85
    memory, 81
    the Java Security Manager, 117-118
    web applications, 130
encodeCookies, 151
examples
    caching, 49-50
    sun-web.xml file, 190
    web.xml file, 189-190

F
fetching client certificates, 107
file, manager properties, 83
FileStore.java, 89
form-based login, 104
G

group-name, 156

H

HPROF profiler, 139-141
HTTP basic authentication, 103
http-method, 177
HTTPS authentication, 103

I

improving servlet performance, 51-52
internationalizing search, 65
invalidating a session, 80
IWS60, 83-89
  enabling, 84-85
  manager properties, 85-89
  source code, 89
IWSHttpSession, 89
IWSHttpSession.java, 89
IWSSessionManager.java, 89

J

Java class file, loading, 132-134
Java EE
  application role mapping, 99
  security model, 97-98
Java Security Manager, enabling, 117-118
Java Servlet 2.5 security model, 97
JDBC driver, for session management, 86
JdbcStore.java, 89
JDPA options, 136
jndi-name, 170
JSP
  about, 57-58
  caching, 61-64
  classloader, 134
  command-line compiler, 58-60
  debugging, 137
  package names, 60
  JSP (Continued)
    parameters, 60
    standard portable tags, 61
    tag libraries, 61
    using, 57-73
  jsp-config, 58, 180-182
  JSP tags, 61
    cache, 61-64
    library location, 61
    search, 65-73
  jspc command, 58
    basic options, 58
    example of, 60
    file specifiers, 58
    format of, 58
  jspc command-line tool, 58

K

key-field, 177

L

library location, JSP tags, 61
list of sun-web.xml elements, 187-189
locale-charset-info, 183-184
locale-charset-map, 184-185
logging, 138
login mechanisms
  form-based, 104
  HTTP basic authentication, 103
  SSL mutual authentication, 103

M

manager-properties, 158-159
memory, 81-82
  enabling, 81-82
  manager properties, 81-82
MMap, 89-90
MMapSessionManager, manager properties, 90
Index

N
name element, 169
NetBeans, using for debugging, 137

O
OptimizeIt profiler, 141-142

P
package names for JSPs, 60
parameter-encoding, 183
password element, 169
performance, improving for servlets, 51-52
permissions
  changing for an application, 119
default, 118
  setting in server.policy file, 119
persistent session manager, 89-90
portable tags, JSP, 61
principal-name, 155-156
profiling, 139-142
  HPROF profiler, 139-141
  OptimizeIt profiler, 141-142
programmatic login, 116-117
property element, 153

R
realms, 98
reaper method, 85, 90
refresh-field, 176-177
reloading web applications, 131-132
res-ref-name, 168
resource-env-ref, 162-163
resource-env-ref-name, 163
resource-ref, 168
role mappings, 106
role-name, 106, 155

S
search, internationalizing, 65
search tags, 65-73
  CollElem, 67-68
  CollItem, 68
  formAction, 69-70
  formActionMsg, 70-71
  formSubmission, 70
  Item, 72
  library location, 65
  queryBox, 68-69
  resultIteration, 71-72
  resultNav, 72-73
  resultStat, 72
  Search, 71
  searchForm, 65-66
  submitButton, 69
Secure Socket Layer (SSL), 103, 104, 107
security, 97-120
  and sessions, 76
  Java EE security model, 97-98
  terminology, 98-99
  web applications, 97-120
  Web Server features, 99-102
  Web Server goals, 97-98
  Web Server security model, 99-102
Security Manager, Java, 117-118
security-role-mapping, 106, 154
server.policy file, 118-119
server.xml, editing for debugging, 135
servlet element, 154-155
servlet-name, 155
servlets, 45-55
  about, 45-46
  authorization by, 105-106
  authorization constraints, 106
caching, 48, 49-50
caching results, 46-51
dexample of accessing, 127
improving performance, 51-52
output, 46
performance, 51-52
session managers, 75-90
sessions, 75
using, 45-55
session-config, 156-157
session-cookie, 76
session-manager, 157-158
session-managers, 75-90
IWS60, 83-89
memory, 81-82
MMap, 89-90
persistent, 89-90
session-properties, 160-161
session-properties, examining, 78-79
session-timeout, 80, 161
sessions
about, 75
and cookies, 76
and security, 76
and URL rewriting, 76
binding objects to, 79-80
creating or accessing, 77-78
examining session properties, 78-79
invalidating, 80
timeout, 80, 161
SHTML, using, 25
single sign-on, 99, 104-105
specifications
Java Servlet, 25
JSP, 25
SSL, 104, 107
SSL mutual authentication, 103
stackTrace, generating for debugging, 137-138
store-properties, 159-160
sun-web-app, 150
sun-web-app_2_4-1.dtd, 144-146
sun-web.xml elements, 149-189
alphabetical quick-reference list, 187-189
cache, 170-172
cache-helper, 172-173
cache-helper-ref, 175
cache-mapping, 174-175
class-loader, 179-180
constraint-field, 178-179
cookie-properties, 161-162
sun-web.xml elements (Continued)
default-helper, 173-174
default-resource-principal, 169
http-method, 177
jndi-name, 170
jsp-config, 180-182
key-field, 177
manager-properties, 158-159
name, 169
parameter-encoding, 183
password, 169
principal name, 155-156
refresh-field, 176-177
res-ref-name, 168
resource-env-ref, 162-163
resource-env-ref-name, 163
resource-ref, 168
role-name, 155
security-role, 106
security-role-mapping, 154
servlet, 154-155
servlet-name, 155
session-config, 156-157
session-manager, 157-158
session-properties, 160-161
store-properties, 159-160
sun-web-app, 150
timeout, 176
value, 179
sun-web.xml file
about, 106, 125
to, 127
creating, 125
defining roles, 106
elements in, 149-189
example, 190
structure of, 144-146
System Classloader, 134
T
tag libraries, JSP, 61
tags, JSP
cache, 61-64
tags, JSP (Continued)
search, 65-73
timeout element, 176

U
URL, parts of, 127
url-pattern, 175
URL rewriting and sessions, 76
using
JSPs, 57-73
NetBeans, 137
servlets, 45-55

V
value element, 179

W
wadm utility, 126
WAR files, 26, 121, 126
Web Application Classloader, 134
web applications, 25-32
about, 25
deployment, 121-134
directory structure of, 121-122
dynamic reloading of, 131-132
enabling and disabling, 130
Java Servlet and JSP specifications, 25
response caching, 47
securing, 97-120
web deployment descriptors, 125
WEB-INF directory, 121
web.xml elements
auth-constraint, 106
login-config, 103
more information about, 103
realm-name, 104
res-ref-name, 162
run-as role, 150
web.xml elements (Continued)
security-role, 155
servlet-name, 155
session-timeout, 161
web.xml file, 125
creating, 125
timeout, 176
example, 189-190
more information about, 103
webserv-rt.jar, 61, 65, 89