Oracle® HTTP Server

Release Notes

Release 2 (9.0.2) for Windows NT/2000

May 2002

A90331-01

This document summarizes the differences between Oracle HTTP Server and its documented functionality.

See Also: *Oracle9i Application Server Release Notes*

1 General Issues and Workarounds

This section describes general issues and their workarounds for Oracle HTTP Server.

1.1 Accessing mod_osso Protected Pages from Netscape 4.7 Requires Manual Configuration

You may not be able to access `mod_osso` protected pages from Netscape 4.7. If you want to access `mod_osso` protected pages from Netscape 4.7, then the partner application corresponding to `mod_osso` should be modified from the Single Sign-On server configuration console to point to Oracle9*i*AS Web Cache port number, which is usually 7777. For details on how to use the Single Sign-On console, refer to the appropriate Single Sign-On administration documentation on the documentation CD.

2 Configuration Issues and Workarounds

This section describes configuration issues and their workarounds for Oracle HTTP Server.

2.1 OPMN/Oracle HTTP Server Infrastructure Requires Special Setting for a Secure Web site

When using OPMN/Oracle HTTP Server infrastructure, you have to specify at least one `non_ssl` port. For a purely secure Web site, meaning it only accepts SSL connection, you have to provide an extra `non_ssl` port in `httpd.conf`. You can do so by adding the following to maintain a secure Web site:

```
Listen <port>

<VirtualHost _default_:port>
SSLEngine Off
<Location />
Order deny,allow
Deny from all
Allow from local host
Allow from <ip1 of a localhost>
Allow from <ip2 of a localhost>
Allow from <ip3 of a localhost>
</Location>
</VirtualHost>
```

This way security is maintained by restricting the non-ssl port to only accept traffic from local host.

2.2 *i*Planet Filter Intercepts All URLs Containing a Tilda.

When Windows NT *i*Planet is initially installed, it automatically sets up a filter which intercepts all URLs containing a tilda “~”. This filter is executed before the proxy and as a result causes the listener to attempt to handle all such URLs instead of the URLs being forwarded to the backend server by the proxy plugin module. The listener might not know how to serve the request and will return a “Not Found” error.

Example URL: `.../~David/hello.html`

As a workaround, under the `<Object name=”default”>` section of the listener’s `obj.conf` file, comment out the following line: `PathCheck fn=nt-uri-clean`. Once commented out, tilda-URLs will be forwarded on to the backend server by the proxy.

2.3 Single Sign-On Initially Gets 503 Errors When Attempting to Access Protected Page

When attempting to access a protected resource, you are redirected to the SSO Server. Here, you may receive 503 errors initially. To avoid this, disable the `KeepAlive` directive when you are using a server load balancer.

2.4 opmnctl stopproc Command Might Hang

If you issue the "`opmnctl stopproc`" command in a process seconds after the process was killed or abnormally terminated, the "`opmnctl stopproc`" command might hang. This might prevent you from issuing other process-related commands.

In this situation, issue the following commands:

```
opmnctl reload
opmnctl stopproc
```

If you are using `dcmctl`, then the "`dcmctl stop`" command will not hang, but fail. Issue the following commands to resolve the situation:

```
dcmctl updateconfig opmn
dcmctl stop
```

3 Administration Issues and Workarounds

This section contains known administration issues and their workarounds for Oracle HTTP Server.

3.1 Microsoft Internet Explorer Might Report Incorrect Host Header After a Redirect

If an infrastructure Single Sign-On Server install and a middle tier install are on the same machine (in different Oracle homes), Microsoft Internet Explorer reports an incorrect host header after a redirect. This incorrect host headed causes `mod_osso` to generate an error message when trying to access a protected resource after the user has been redirected from the Single Sign-On Server back to the original server. If you click on **Reload** in Internet Explorer, the session continues successfully. This issue will not occur if any of the following conditions are true:

- You do not use Microsoft Internet Explorer.
- Protected resource and the Single Sign-On Server are running behind Oracle HTTP Server instances with different server names or on different hosts. This is the most likely deployment.

- Single Sign-On Server and the protected resource are running behind a single Oracle HTTP Server port.

3.2 Microsoft Internet Explorer Might Report Errors When Two OSSO Protected Servers are on the Same Host

When you install an infrastructure instance of Oracle9*i*AS and a middle tier installation on the same machine, Microsoft Internet Explorer might report various errors where an incorrect host header is sometimes passed after redirection. Specifically, if you have already logged on via the Single Sign-On Server to the middle-tier instance and then click on a link that tries to redirect them to the infrastructure instance, you will receive an `OSSO` error page. Pressing the **Back** button allows you to continue to the page you originally wished to reach.

3.3 IASOBF and SSO Wallet Support is User-dependent

To run the Oracle HTTP Server with SSL server correctly after installation, you should create a wallet and have the certificates contained within it signed by the proper Certificate Authorities. Make sure that the `SSLWallet` directive in `httpd.conf` points to this new wallet rather than the default wallet provided by the installation. Oracle HTTP Server will not start if you fail to do one of the following:

- Obfuscate this new wallet's password by running:

  ```
  osslpassword -p password LocalSystem
  ```

  and place this obfuscated password in `httpd.conf` file using the Wallet Password directive (for example "`WalletPassword obfuscatedPassword`"). You can always choose to put the wallet password in `httpd.conf` in clear text but this is not recommended by Oracle.

- Make this new wallet an SSO wallet as the root user.

See Also: *Oracle9i Application Server Security Guide*

4 Documentation Errata

There are no known issues associated with Oracle HTTP Server documentation.