Oracle® Fusion Middleware

Release Notes for Oracle HTTP Server

11*g* Release 1 (11.1.1)

E55728-02

March 2017

This document describes all known issues for this release of Oracle HTTP Server.

ORACLE

Oracle Fusion Middleware Release Notes for Oracle HTTP Server, 11*g* Release 1 (11.1.1)

E55728-02

Primary Author: Trupthi NT

Contents

Preface

Oracle HTTP Server 11g (11.1.1) release notes summarizes release information related to issues fixed, general issues and their workarounds, deprecated and removed functionality, and more. This release of the product is in maintenance mode and will no longer have new features or content.

Audience

This document is intended for users of Oracle Fusion Middleware 11*g*.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Related Documents

For more information, see the following resources:

- Oracle HTTP Server 11*g* Documentation Library

  This contains all documentation for all Oracle HTTP Server 11*g* products.

- Oracle Technology Network

  This site contains additional documentation that is not included as part of the documentation libraries.

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

1

Introduction

This chapter introduces the Release Notes for Oracle HTTP Server. It includes the following sections:

Topics

1.1 Latest Release Information

This document is accurate at the time of publication. Oracle will update the release notes periodically after the software release. You can access the latest information and additions to these release notes on the Oracle Technology Network at: http://www.oracle.com/technetwork/indexes/documentation/index.html

1.2 Purpose of this Document

This document contains information related to the issues and release-specific user information associated with Oracle HTTP Server.

Oracle recommends you review its contents before installing, or working with the product.

1.3 System Requirements and Specifications

To install and configure Oracle HTTP Server successfully, see Reviewing System Requirements and Certification in *Oracle Fusion Middleware Installation Guide for Oracle Web Tier*.

1.4 Certification Information

To see versions of platforms and related software for which Oracle HTTP Server is certified and supported, go to http://www.oracle.com/technetwork/middleware/ias/downloads/fusion-certification-100350.html.

1.5 Licensing Information

Licensing information for Oracle HTTP Server is available at:

http://shop.oracle.com

1.6 Product Documentation

For complete documentation on Oracle HTTP Server go to http://docs.oracle.com/en/middleware/.

1.7 Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support at https://support.oracle.com

2

What's New in this Release

This chapter describes the features and improvements in Oracle HTTP Server. The following topics introduce the new and changed features of Oracle HTTP Server and other significant changes in the guides, and provides pointers to additional information.

Topics

2.1 New Features

This section describes the new features added to Oracle HTTP Server.

2.1.1 New Security Protocols and Ciphers for the Current Release

The current release of Oracle HTTP Server and Oracle Web Cache adds support for the TLSv1.1 and TSLv1.2 security protocols and the following ciphers. For the complete list of security protocols and ciphers supported by the current release of Oracle HTTP Server, see SSLProtocol and SSLCipherSuite in *Oracle Fusion Middleware Administrator's Guide for Oracle HTTP Server*.

- `TLS_RSA_WITH_AES_128_CBC_SHA256`
- `TLS_RSA_WITH_AES_256_CBC_SHA256`
- `TLS_RSA_WITH_AES_128_GCM_SHA256`
- `TLS_RSA_WITH_AES_256_GCM_SHA384`
- `TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA`
- `TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA`
- `TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256`
- `TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384`
- `TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256`
- `TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384`

2.1.2 Changes Related to Security Protocols

This section describes changes to ciphers and security protocols.

- Post-Patching/Post-Upgrade Instructions for SSLCipherSuite Directive
- Disable SSLv2 and SSLv3 Security Protocols
- Changes to SSL Configuration Screens in Fusion Middleware Control

2.1.2.1 Post-Patching/Post-Upgrade Instructions for SSLCipherSuite Directive

If you are upgrading from an Oracle HTTP Server 10*g* or 11.1.1.*x* release to 11.1.1.9, Oracle recommends that you review the ciphers used in your configuration. Oracle HTTP Server has removed support for certain weak ciphers in this release. If these weak ciphers are used in your SSL configuration, then the server might fail to start or the request from clients that use these ciphers will be denied. To correct this, update the SSLCipherSuite directive with the correct ciphers. For more information on the supported ciphers in 11.1.1.9 release, see SSLCipherSuite in *Administrator's Guide for Oracle HTTP Server*.

The following example illustrates a `SSLCipherSuite` configuration using all of the valid ciphers for the 11.1.1.9 release (Note that the ciphers should be entered as a comma-delimited list: no spaces between the comma and the cipher name and no line breaks. Line breaks have been added to the following example only for readability):

```
SSLCipherSuite
SSL_RSA_WITH_RC4_128_MD5,SSL_RSA_WITH_RC4_128_SHA,SSL_RSA_WITH_3DES_EDE_CBC_SHA,
SSL_RSA_WITH_AES_128_CBC_SHA,SSL_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SH
A256,
TLS_RSA_WITH_AES_256_CBC_SHA256,TLS_RSA_WITH_AES_128_GCM_SHA256,TLS_RSA_WITH_AES_256_
GCM_SHA384,
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_E
CDSA_WITH_AES_128_CBC_SHA256,
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
```

2.1.2.2 Disable SSLv2 and SSLv3 Security Protocols

Because of security concerns, the SSLv3 security protocol is disabled out-of-the-box in the Oracle HTTP Server 11.1.1.9 release.

If you are upgrading from an earlier release of Oracle HTTP Server, the SSLv3 and/or SSLv2 security protocol might be a part of your configuration. Oracle strongly recommends that you disable any SSLv3 or SSLv2 from Oracle HTTP Server. For more information, see Disable SSLv2 and SSLv3 Security Protocols in *Administrator's Guide for Oracle HTTP Server*.

2.1.2.3 Changes to SSL Configuration Screens in Fusion Middleware Control

- The SSLv3 security protocol is not supported by default. thus it does not appear in the SSL configuration screen in Fusion Middleware Control.
- Remove the cipher `SSL_RSA_WITH_DES_CBC_SHA` if it appears in your configuration. This cipher is not supported in the 11.1.1.9 release.

See also FMW Infrastructure Does Not Support Certain Protocols and Ciphers.

2.2 Deprecated Features

Oracle HTTP Server has deprecated the following features:

- mod_charset_lite Module has been Deprecated

2.2.1 mod_charset_lite Module has been Deprecated

The mod_charset_lite module has been deprecated in the current release. It will be removed from future releases.

3

Lifecycle Management Information

This chapter describes install and upgrade issues associated with Oracle HTTP Server.

Topics

3.1 Installing Oracle HTTP Server 11.1.1.*x* with Oracle WebLogic Server 12*c*

You can install Oracle HTTP Server 11.1.1.*x* with the Oracle WebLogic Server 12c JRF/ADF combination. For instructions, see *Oracle Fusion Middleware Certification/Compatibility Between 11g and 12c* (Doc ID 1576554.1) at My Oracle Support:

`https://support.oracle.com`

3.2 Warning Message When Installing on Linux X86v Platforms

During installation, you may notice the following warning message from the installers:

```
Java HotSpot(TM) Server VM warning: You have loaded
library /tmp/OraInstall2015-04-30_04-19-43AM/oui/lib/linux/
liboraInstaller.so which might have disabled stack guard. The VM
will try to fix the stack guard now. It's highly recommended
that you fix the library with 'execstack -c <libfile>', or link
it with '-z noexecstack'.
```

You can ignore this message, it is a known issue with Linux 32 and JDK7.

3.3 Oracle WebGate Support for Oracle HTTP Server

Oracle WebGate version 11.1.2.3 for Oracle HTTP Server supports only Oracle HTTP Server version 11.1.1.9 and not earlier versions. Earlier versions of WebGate for Oracle HTTP Server are supported against Oracle HTTP Server 11.1.1.9 as described in the certification matrix.

`http://www.oracle.com/technetwork/middleware/ias/downloads/fusion-certification-100350.html`

This is important for planning Oracle HTTP Server and WebGate updates if they will be performed separately. Specifically, the update to Oracle HTTP Server version

11.1.1.9 should be performed before an update to WebGate version 11.1.2.3 for Oracle HTTP Server.

4

Known Issues and Workaround

This chapter describes the issues associated with Oracle HTTP Server.

Topics

4.1 Notes on Using the Default Wallet

Issue

Impacted Platforms: Generic

The default wallet shipped with Oracle HTTP Server 11.1.1.9 is for demonstration purposes only and not for production use, so that users can access the site by using the HTTPS end point (default port 4443).

The default wallet uses MD5-based hashing which is no longer considered very secure. Users should create a new wallet with the `orapki` utility and use more secure hashing algorithms such as `SHA256`.

Workaround

The default wallet uses MD5-based hashing which is no longer considered very secure. Users should create a new wallet with the `orapki` utility and use more secure hashing algorithms such as `SHA256`.

For example, create a wallet with `auto_login_only` enabled:

```
orapki wallet create -wallet wallet_location -auto_login_only
```

Add a self-signed root certificate to the wallet. The `keysize` option specifies the requested certificate's key size and the `sign_alg` option specifies the hashing algorithm.

```
orapki wallet add -wallet wallet_location -dn certificate_dn -keysize 2048 -
sign_alg sha256 -self_signed -validity 365 -auto_login_only
```

For information on the `sign_alg` option of `orapki`, see Secure an API Gateway Domain in *Oracle Fusion Middleware Part 2. Manage an API Gateway Domain*. For information on creating a wallet and adding a user certificate, see orapki in *Administering Oracle Fusion Middleware*.

4.2 TLS v1.2 Fails with Internet Explorer When Using the Default Wallet

Issue

Impacted Platforms: Microsoft Windows

If you use this demonstration certificate with the TLS v1.2 protocol and attempt to access the Oracle HTTP Server HTTPS end point, then recent browsers such as Internet Explorer 11 will not be able to successfully connect with the end point. This is because the demonstration certificate is created using MD5-based hashing which is no longer considered very secure.

Workaround

However, if you want to test the TLS v1.2 protocol using the Internet Explorer browser, then create a new wallet and add a user certificate that uses one of the stronger hashing algorithms, such as `SHA256`. For an example of the `orapki` commands, see Notes on Using the Default Wallet.

Note:

Oracle HTTP Server 11.1.1.9 ships with a default self-signed certificate. This certificate is for demonstration purposes only and should not be used for development or production use cases.

4.3 Overriding the TLS Protocol with SSLv3 for IBM AIX Systems

Issue

Impacted Platforms: IBM AIX

If you are using Fusion Middleware Control or WLST commands to configure Oracle HTTP Server on IBM AIX, then the operations can fail. You will see SSL handshake errors in the Oracle HTTP Server log file when the JDK used by Oracle WebLogic Server is enabled only for the SSLv3 protocol. To avoid these errors, you must change the default value of the SSLProtocol directive in the `admin.conf` file (`$INSTANCE_HOME/config/OHS/<component_name>/admin.conf`).

Workaround

The default value for the SSLProtocol directive in the `admin.conf` file is `All`. This value includes the TLS protocols. To discard the TLS protocols from the configuration and enable the SSLv3 protocol, follow these steps:

1. Change the value of SSLProtocol directive in the `admin.conf` file to `SSLv3`.
2. Edit the `startWeblogic.sh` script to add the system property `ohsadmin.ssl.protocol`, as follows:

```
JAVA_OPTIONS="${JAVA_OPTIONS} -Dohsadmin.ssl.protocol=SSLv3"
```

4.4 FMW Infrastructure Does Not Support Certain Protocols and Ciphers

Issue

Impacted Platforms: Generic

If you are using Fusion Middleware Control or WLST commands to configure SSL for Oracle HTTP Server, you cannot configure the TLSv1.1 and TLSv1.2 protocols for the SSLProtocol directive or the following ciphers listed in the Workaround for the SSLCipherSuite directive.

Workaround

To enable or disable these protocols and ciphers, you must manually edit the `<file-location>/config/ssl.conf` file. For more information, see Configuring TLS v1.1 and TLS v1.2 Protocols and Ciphers in *Oracle Fusion Middleware Administrator's Guide for Oracle HTTP Server*.

Note:

The TLSv1.1 and TLSv1.2 protocols and the following ciphers are enabled by default.

- `SSL_RSA_WITH_AES_128_CBC_SHA`
- `SSL_RSA_WITH_AES_256_CBC_SHA`
- `TLS_RSA_WITH_AES_128_CBC_SHA256`
- `TLS_RSA_WITH_AES_256_CBC_SHA256`
- `TLS_RSA_WITH_AES_128_GCM_SHA256`
- `TLS_RSA_WITH_AES_256_GCM_SHA384`
- `TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA`
- `TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA`
- `TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256`
- `TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384`
- `TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256`
- `TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384`

If SSL is enabled for Oracle HTTP Server Virtual Hosts or the SSL configuration has been modified from the SSL Configuration page of Fusion Middleware Control configuration screen or WLST commands, the configuration of the above listed protocols and ciphers in `ssl.conf` file will be lost.To make any changes related to the SSL configuration for these protocols and ciphers, edit `ssl.conf` file directly by using the Advanced Configuration page in Fusion Middleware Control.

4.5 Certain Cipher Names are Invalid

Issue

Impacted Platforms: Generic

If you are using Fusion Middleware Control or WLST to configure SSL for Oracle HTTP Server, then choosing any one or both of these two ciphers: `TLS_RSA_WITH_AES_128_CBC_SHA` or `TLS_RSA_WITH_AES_256_CBC_SHA` will result in unexpected behavior from Oracle HTTP Server.

This is because Oracle HTTP Server fails to recognize these cipher names as valid. The valid cipher names are `SSL_RSA_WITH_AES_128_CBC_SHA` and `SSL_RSA_WITH_AES_256_CBC_SHA` respectively.

Workaround

To correct this problem, edit the `ssl.conf` file directly by using the Advanced Configuration page in Fusion Middleware Control and specify the correct cipher names.

4.6 After Patching Web Tier to 11.1.1.9 SSL Connection to WebLogic Server Fails

Issue

Impacted Platforms: All

A user patching from Web Tier/Oracle HTTP Server 11.1.1.x to 11.1.1.9 may run into a negotiation issue between mod_wl_ohs and WebLogic Server.

Workaround

1. Enable JSSE.
2. Force the plug-in to a supported protocol between Oracle HTTP Server and WebLogic Server (for example, TLSv1) using the `WebLogicSSLVersion` parameter. See Configuring SSL with WebLogic Proxy Plug-In and Oracle WebLogic Server and SSL Parameters for Web Server Plug-Ins in *Using Web Server Plug-Ins with Oracle WebLogic Server*.

5

Bugs Fixed in this Release

This chapter reviews issues known to exist in previous Oracle HTTP Server releases that have now been resolved.

Resolved issues are described in the following table:

Table 5-1 Resolved Issues for Release 11.1.1.9

Issue	Resolution
Security concerns about the SSLv3 protocol.	The SSLv3 security protocol has been disabled out-of-the-box for the 11.1.1.9 release. The TLS version 1.1 and 1.2 security protocols have been added to the 11.1.1.9 release.
An invalid_socket condition in Windows MPM is not handled properly.	Fixed an issue which caused an invalid_socket condition in windows MPM to be handled incorrectly.
A memory leak causes the TMP pool to be destroyed when a call to connect() fails.	Fixed a memory leak issue which destroyed the TMP pool when a call to connect() failed.
In the case of a bad configuration, the process was destroyed after the server was signaled.	Fixed the issue such that the destroy_and_exit_process() is called before signaling the server in the case of a bad configuration.
Insufficient information in error messages.	Filesystem paths have been added to some common error messages in OHS.
When setting the default location in mod_wl_ohs as a cluster, it overrides the values of other locations.	Fixed an issue where listeners (OHS, Apache, IIS, iPlanet) could not handle the numeric form of the WLS server IPv4 address if it was a negative number. This issue prevented requests from being proxied to the WLS server.
When setting default location in mod_wl_ohs as a cluster, it overrides others.	Fixed an issue where if WebLogicHost and WebLogicCluster were used for different Location/LocationMatch, the plug-in would route to an incorrect WLS server. Applicable for OHS and Apache plug-ins
The customer has SSL set-up between Apache (Plugin 11.1.1.7) and WLS. The requests work most of the time, but intermittently, after Apache restart, all the requests from Plugin to WLS fail.	Fixed an intermittent issue where SSL connections failed when the Apache server is restarted. The plugin was trying to send data over HTTP instead of HTTPS and hence WLS rejected the request.
OHS was consistently crashing when trying to connect over SSL.	Fixed an issue where the handshake was not being successfully completed between OHS and SSL.

Table 5-1 (Cont.) Resolved Issues for Release 11.1.1.9

Issue	Resolution
Although it is ignored by mod_ossl if present, the cipher SSL_RSA_WITH_DES_CBC_SHA is not supported and must be removed from the default ssl.conf file shipped with OHS.	The weak cipher SSL_RSA_WITH_DES_CBC_SHA has been removed from the SSL.CONF file.
In EM and OHS log files, the version for OHS is given as 11.1.1.6.	The OHS version has been updated to 11.1.1.9.0 so that the EM and OHS log file shows the correct version. Also the server signature in OHS log has been changed to replace "Oracel-Application-Server" with "Oracle-HTTP-Server".
Customers want to change the location of the DMS metrics file.	Fixed an issue where the DMS SHM file was hardcoded to be in the OHS log directory. The DMS SHM file can now be configured to be on NFS. Note that if the OHS log directory is located on an NFS mounted file system, then the shared memory map file OHS uses to maintain metrics can cause performance issues. This is not an issue on Windows.
An insufficient default memory size indicated in the OHS logs with the message beginning with: "dms_fail_shm_expansion: out of DMS shared memory in" may cause OHS to not start at all, or to start but stop supporting the metrics displayed by EM after logging the above message.	A new algorithm has been developed to calculate the amount of shared memory required for DMS.
Provisioning fails because file system is full. This was caused by too many core files created by httpd.worker.	This bug fixes intermittent crashes for certain HTTP requests. Applicable for OHS and Apache plug-in Can't access base bug. RN not needed.
iPlanet Webserver and other application servers can crash when configured with one-way SSL.	The issue that caused iPlanet Webserver and other application servers to crash with one-way SSL has been resolved.

6

Documentation Changes

This section describes the changes in Oracle HTTP Server documentation.

Topics

6.1 Information about third-party modules missing in Administrator's Guide for Oracle HTTP Server

The List of Included Modules section in *Administrator's Guide for Oracle HTTP Server* does not include information about the following third-party modules that are also bundled with Oracle HTTP Server by default.

- mod_cache.so (Windows only)
- mod_disk_cache.so (Windows only)