Red Hat JBoss Web Server 1.0

Release Notes 1.0.2

for use with Red Hat JBoss Web Server 1.0.2

Edition 1.0.2

Red Hat JBoss Web Server 1.0 Release Notes 1.0.2

for use with Red Hat JBoss Web Server 1.0.2
Edition 1.0.2

Rebecca Newton
rnewton@redhat.com

Legal Notice

Abstract

These release notes contain important information related to Red Hat JBoss Web Server 1.0.2. Read these Release Notes in their entirety before installing Red Hat JBoss Web Server 1.0.2.

Table of Contents

CHAPTER 1. INTRODUCTION

These release notes contain important information related to JBoss Enterprise Web Server 1.0.2. New features, known problems, resources, and other current issues are addressed here.

1.1. OVERVIEW

JBoss Enterprise Web Server is a fully-integrated and certified set of components for hosting Java web applications. It is comprised of the industry's leading web server (Apache HTTP Server), the popular Apache Tomcat Servlet container as well as load balancers (mod_jk and mod_cluster), the Tomcat Native library and others.

1.2. JBOSS COMPONENTS

This release of the JBoss Enterprise Web Server consists of the following components:

- **Apache Tomcat 5.5.33**: Apache Tomcat is an implementation of the Java Servlet and JavaServer Pages technologies. The Java Servlet and JavaServer Pages specifications are developed by Sun under the Java Community Process. Apache Tomcat version 5.5 implements the Servlet 2.4 and JavaServer Pages 2.0 specifications.

  > **NOTE**
  >
  > The default Red Hat Enterprise Linux 5 installation contains Apache Tomcat 5.5.23.
  >
  > The default Red Hat Enterprise Linux 6 installation contains Apache Tomcat 6-6.0.24.

- **Apache Tomcat 6.0.32**: Apache Tomcat is an implementation of the Java Servlet and JavaServer Pages technologies. The Java Servlet and JavaServer Pages specifications are developed by Sun under the Java Community Process. Apache Tomcat version 6.0 implements the Servlet 2.5 and JavaServer Pages 2.1 specifications.

- **Apache Tomcat Native 1.1.20**: Tomcat can use the Apache Portable Runtime to provide superior scalability, performance, and better integration with native server technologies. The Apache Portable Runtime is a highly portable library that is at the heart of Apache HTTP Server 2.x. APR has many uses, including access to advanced IO functionality (such as sendfile, epoll and OpenSSL), OS level functionality (random number generation, system status, etc), and native process handling (shared memory, NT pipes and Unix sockets). This package contains the Tomcat native library which provides support for using APR in Tomcat.

- **Apache Tomcat Connectors (mod_jk 1.2.31 and mod_cluster 1.0.10.GA_CP01)** : Apache Tomcat Connectors create bridges between Apache HTTP Server and Apache Tomcat using the binary AJP protocol. They also contains load balancers, which provide clustering and fault tolerance.

- **Apache HTTP Server 2.2.17**: The Apache HTTP Server Project is an effort to develop and maintain an open-source HTTP server for modern operating systems. The goal of this project is to provide a secure, efficient and extensible server that provides HTTP services in sync with the current HTTP standards.

NOTE

The default Red Hat Enterprise Linux 5 installation contains Apache HTTP Server 2.2.3-31.

The default Red Hat Enterprise Linux 6 installation contains Apache HTTP Server 2.2.15.

- **Hibernate 3.4.0.GA_CP04**: Hibernate contains Hibernate Core, Hibernate Annotations, and Hibernate EntityManager with JPA 1.0 APIs.

IMPORTANT

Red Hat products, including Red Hat Enterprise Linux, are signed with a Red Hat Key to indicate that these packages and JARs are shipped by Red Hat. With Red Hat Signed JARs you can be confident that your product distribution is exactly the distribution that was shipped by Red Hat.

1.3. SUPPORTED OPERATING SYSTEMS

This release of JBoss Enterprise Web Server is certified for the following operating systems:

- Red Hat Enterprise Linux 6, latest update (x86, x86_64)

- Red Hat Enterprise Linux 5, latest update (x86, x86_64)

- Red Hat Enterprise Linux 4, latest update (x86, x86_64)

- Solaris 10 (x86, x86_64, SPARC64)

- Solaris 9 (x86, SPARC32, SPARC64)

- Windows Server 2008 R2 (x86, x86_64)

- Windows Server 2003 SP2 (x86, x86_64)

CHAPTER 2. NEW WITH THIS RELEASE

The following are additions to Enterprise Web Server 1.0.2:

JBoss Hibernate

JBoss Hibernate is an implementation of the Java Persistence 1.0 identifier and is an Object/Relational Mapping solution for Java environments.

JBoss Enterprise Web Server consists of Hibernate Core 3.3.2.GA_CP04, Hibernate Annotations 3.4.0.GA_CP04, and Hibernate Entity Manager 3.4.0.GA_CP04.

mod_cluster

JBoss mod_cluster 1.0.10.GA_CP01 is an httpd-based load balancer. Like mod_jk, it uses a communication channel to forward requests from HTTPD to an application server node.

Red Hat Enterprise Linux 6

JBoss Enterprise Web Server 1.0.2 introduces support for Red Hat Enterprise Linux 6.

Support for Online Certificate Security Protocol

Apache httpd 2.2 contains support for Online Certificate Security Protocl (OCSP).

CHAPTER 3. EXCLUDED, DEPRECATED, AND REMOVED ITEMS

This section outlines the items which are excluded from this release, deprecated or removed. In order to maintain a high level of backwards compatibility and customer service, an item will usually be deprecated before it is removed from a release.

> **NOTE**
>
> The difference between an excluded item and a removed item is that an excluded item is one that is commonly a part of a component of the JBoss Enterprise Web Server but has never featured within a JBoss Enterprise Web Framework release. However, a removed item is one that has previously been in a release of the JBoss Enterprise Web Server and is no longer included.

3.1. EXCLUDED ITEMS

The following items have been excluded from this release of the JBoss Enterprise Web Server:

- `Tomcat Clustering` has been excluded from the `Apache Tomcat 6` component. Specifically the `catalina-tribes.jar` file has been removed. This has occurred to eliminate any possibility of session replication and because Red Hat does not believe this feature is suitable for medium or large scale production deployments.

3.2. DEPRECATED ITEMS

The following items have been deprecated for this release of the JBoss Enterprise Web Server:

- The `Tomcat Clustering` feature of `Apache Tomcat 5` is marked as deprecated for this release. Specifically the `catalina-cluster.jar` file has been deprecated.

3.3. REMOVED ITEMS

The following http modules have been removed from the Red Hat Enterprise Linux 6 distribution of this release of JBoss Enterprise Web Server:

- mod_file_cache

- mod_imagemap

- mod_mem_cache

These have been deemed obsolete. mod_disk_cache can be used instead of mod_file_cache and mod_mem_cache.

CHAPTER 4. INSTALLATION

Please see the *Installation Guide* for installation instructions.

CHAPTER 5. PRODUCT SUPPORT AND LICENSE WEBSITE LINKS

Product Page

http://www.jboss.com/products/platforms/webserver/

Support Processes

http://www.redhat.com/support/process/

Production Support Scope of Coverage

http://www.redhat.com/support/policy/soc/production

Production Support Service Level Agreement

http://www.redhat.com/support/policy/sla/production/

Developer Support Scope of Coverage

http://www.redhat.com/support/policy/soc/developer/

Developer Support Service Level Agreement

http://www.redhat.com/support/policy/sla/developer/

Product Update and Support Policy by Product

http://www.redhat.com/security/updates/jboss_notes/

JBoss End User License Agreement

http://www.redhat.com/licenses/jboss_eula.html

CHAPTER 6. DOCUMENTATION

The following issues are resolved with the introduction of the Enterprise Web Server Installation Guide available from docs.redhat.com

- JBPAPP-6062
- JBPAPP-5142
- JBPAPP-5141
- JBPAPP-4846
- JBPAPP-4823
- JBPAPP-4810
- JBPAPP-4777
- JBPAPP-4743
- JBPAPP-4742
- JBPAPP-4741
- JBPAPP-4737
- JBPAPP-4736
- JBPAPP-4735
- JBPAPP-3893
- JBPAPP-3816
- JBPAPP-3815
- JBPAPP-2251

CHAPTER 7. ISSUES FIXED IN THIS RELEASE

The following sections detail the issues fixed in this release of JBoss Enterprise Web Server.

General Fixed Issues

JBPAPP-4529

No request is forwarded to a worker node after it has failed, even though it is marked as available in the balance manager. This issue has been resolved with JBoss Enterprise Web Platform 1.0.2.

JBPAPP-4207

Running `service5.bat remove` on Windows disables the Tomcat service instead of removing it. This has been fixed JBoss Enterprise Web Server 1.0.2.

JBPAPP-3938

The manager application is unable to undeploy a .war application deployed on the Tomcat 5 server. Deploying an expanded .war throws a similar error but does undeploy the application. This issue is fixed with this release of JBoss Enterprise Web Server.

JBPAPP-3888

apachectl22 executes `/usr/sbin/httpd` instead of `/usr/sbin/httpd22`, which causes the wrong httpd version to run. This issue has been fixed and apachectl22 now runs `/usr/sbin/httpd22`.

JBPAPP-3789

Installing both Tomcat 5 and Tomcat 6 rpms causes Tomcat 5 to load the Tomcat 6 servlet JAR, `tomcat6-servlet-2.5-api.jar`, instead of `geronimo-j2ee-1.4-apis.jar`. Before Tomcat 6 is installed, Tomcat 5 uses:

```
/var/lib/tomcat5/common/lib/\[servlet\].jar ->
/usr/share/java/servlet.jar ->
/etc/alternatives/servlet -> /usr/share/java/geronimo-j2ee-1.4-apis.jar
```

After Tomcat 6 is installed, Tomcat 5 uses:

```
/var/lib/tomcat5/common/lib/\[servlet\].jar ->
/usr/share/java/servlet.jar ->
/etc/alternatives/servlet -> /usr/share/java/tomcat6-servlet-2.5-api.jar
```

This issue has been fixed by correcting the symlinks in tomcat5 so that it links to the servlet and jsp jars from the tomcat5 build instead of the alternatives one.

JBPAPP-3758

Configuration for the welcome page of Enterprise Web Server in httpd/conf.d/welcome redirects requests to /error/noindex.html file, but the noindex.html file in the httpd/www/error directory does not exist. Zips installed on Red Hat Enterprise Linux 5 do not work, as a result. This issue has been fixed with JBoss Enterprise Web Server 1.0.2.

JBPAPP-3753

Undeploying any web application in the **/manager** and **/admin** applications causes an infinite loop. We do not currently recommend using the **/manager** or **/admin** applications to undeploy applications from your server.

JBPAPP-3685

Attempting to edit server configuration details with the Tomcat 5 administration application results in some configuration information being lost from the configuration file (server.xml). This issue has been fixed with JBoss Enterprise Web Server 1.0.2.

JBPAPP-3658

Attempting to delete an existing host with the Tomcat 5 Administration Tool results in a **NullPointerException**. This has been fixed with JBoss Enterprise Web Server 1.0.2.

JBPAPP-3646

The Tomcat 6 test suite attempts to compile and execute **org.apache.catalina.tomcat.util.http.TestCookies** instead of **org.apache.tomcat.util.http.TestCookies**. This issue is fixed upstream and with this release of JBoss Enterprise Web Server.

JBPAPP-3644

Setting **SECURITY_MANAGER="true"** in **sysconfig/tomcat5** or **sysconfig/tomcat6** has no effect. This issue has been resolved by modifying catalina.sh to switch to -security mode if SECURITY_MANAGER=true is set.

mod_cluster Fixed Issues

JBPAPP-3349

Should you encounter an [emerg] create_mem_node <node file path> failed error, use the ipcrm -m command before restarting httpd.

Security Fixed Issues

CVE-2011-0419

It was found that the apr_fnmatch() function used an unconstrained recursion when processing patterns with the '*' wildcard. An attacker could use this flaw to cause an application using this function, which also accepted untrusted input as a pattern for matching (such as an httpd server using the mod_autoindex module), to exhaust all stack memory or use an excessive amount of CPU time when performing matching.

CVE-2011-0013

A cross-site scripting (XSS) flaw was found in the Manager application. A malicious web application could use this flaw to conduct an XSS attack, leading to arbitrary web script execution with the privileges of victims who are logged into and viewing Manager application web pages.

CVE-2010-4172

A cross-site scripting (XSS) flaw was found in the Manager application, used for managing web applications on Apache Tomcat. If a remote attacker could trick a user who is logged into the Manager application into visiting a specially-crafted URL, the attacker could perform Manager application tasks with the privileges of the logged in user.

CVE-2010-3718

It was found that web applications could modify the location of the Apache Tomcat host's work directory. As web applications deployed on Tomcat have read and write access to this directory, a malicious web application could use this flaw to trick Tomcat into giving it read and write access to an arbitrary directory on the file system.

CVE-2010-2068

A flaw was discovered in the way the mod_proxy_http module of the Apache HTTP Server handled the timeouts of requests forwarded by a reverse proxy to the back-end server. In some configurations, the proxy could return a response intended for another user under certain timeout conditions, possibly leading to information disclosure. Note: This issue only affected httpd running on the Windows operating system.

CVE-2010-1623

It was found that certain input could cause the apr-util library to allocate more memory than intended in the apr_brigade_split_line() function. An attacker able to provide input in small chunks to an application using the apr-util library (such as httpd) could possibly use this flaw to trigger high memory consumption.

CVE-2010-1452

A flaw was found in the way the mod_dav module of the Apache HTTP Server handled certain requests. If a remote attacker were to send a carefully crafted request to the server, it could cause the httpd child process to crash.

CVE-2010-1157

A possible minor information leak was found in the way Apache Tomcat generated HTTP BASIC and DIGEST authentication requests. For configurations where a realm name was not specified and Tomcat was accessed via a proxy, the default generated realm contained the hostname and port used by the proxy to send requests to the Tomcat server.

Windows and Solaris Security Issues

The following flaws were corrected in the packages for Solaris and Windows.

Multiple flaws in OpenSSL, which could possibly cause a crash, code execution, or a change of session parameters, have been corrected.

- CVE-2009-3245

- CVE-2010-4180

- CVE-2008-7270

Two denial of service flaws were corrected in Expat.

- CVE-2009-3720

- CVE-2009-3560

An X.509 certificate verification flaw was corrected in OpenLDAP.

- CVE-2009-3767

CHAPTER 8. KNOWN ISSUES WITH THIS RELEASE

Following is a list of known issues at the time of release.

General Known Issues

JBPAPP-6655

When Java is installed on Red Hat Enterprise Linux from RPM, the alternatives system determines which Java is used by default. A user will not normally have the JAVA_HOME environment variable set, and Java continues to work, but trying to use JSVC without JAVA_HOME set results in a Cannot Locate Java Home error. The workaround for this issue is to set JAVA_HOME manually, or use the -java-home option.

JBPAPP-6592

Deploying an application as a Tomcat 6 user with "tomcat, manager, admin" roles leads to a 403 error.

JBPAPP-6326

WAITFORREMOVE is not configurable, which means that there is a ten second delay when a node failsover to another node.

JBPAPP-6297

When using Tomcat 6, changing the default for loadMetricCapacity, loadHistory and loadDecayFactor throws a NullPointerException. To workaround this issue, use the default configuration for these classes.

JBPAPP-6197

Using the Tomcat shutdown procedure `/usr/sbin/tomcat6` or Red Hat Enterprise Linux 6 fails when JON is being used to manage a tomcat instance installed via RPMs.

JBPAPP-6133

Tomcat5 cannot start if the security manager is enabled.

JBPAPP-6128

JON does not discover Tomcat 5 and 6 on Windows so it cannot be used to monitor them.

JBPAPP-6096

The JON httpd plugin cannot discover httpd if `/etc/httpd` does not exist. This issue only occurs when Enterprise Web Server is installed via ZIP, and the workaround is to manually create `/etc/httpd` for Red Hat Enterprise Linux and Solaris, and `C:\apache` for Windows.

JBPAPP-4882

`manager.xml` cannot be installed when adding a virtual host through the host-manager on tomcat6.

JBPAPP-4873

Running tomcat 5 on Red Hat Enterprise Linux with security manager enabled fails to start with the default catalina.policy.

JBPAPP-4265

There is an issue with ldap:// with STARTTLS, which causes the server to respond with error code 500. The logs show that this is a user testuser authentication failed error.

JBPAPP-3900

The libraries provided by Tomcat 5 and 6 differ between the RPM and ZIP distributions. Refer to the JIRA for further details.

JBPAPP-3762

When JBoss Enterprise Web Server is run on the IBM Java Development Kit 1.6 using Java Security Manager, Tomcat 6 does not start.

JBPAPP-3734

Unless `<package>.noarch` is specified for Tomcat 5 packages, yum fetches all Tomcat 5 packages from the Red Hat Enterprise Linux 5 base channel instead of the JBoss Enterprise Web Server channel. The installation instructions have been modified to include a work-around for this issue.

JBPAPP-3628

When a virtual host is created using the `/host-manager/html` application, all actions work as expected, but the newly created host is not persistently added to the Tomcat configuration. Only the localhost is listed after server restart.

JBPAPP-3627

The *Host Manager Help* link in the `/host-manager` application leads to a HTTP 404 Error.

JBPAPP-3626

The links that Tomcat Web Application Manager displays for `/host-manager` and `/manager` result in a HTTP 404 Error. To work around this issue, add the following section to the `WEB-INF/web.xml` descriptor, immediately after the servlet-mapping section:

```
<welcome-file-list>
    <welcome-file>
    html/
    </welcome-file>
</welcome-file-list>
```

JBPAPP-3625

When Tomcat Native is used upon server shutdown, a "Server accept failed" error occurs because the AJP Connector continues to wait for a client connection during shutdown.

JBPAPP-3614

Due to a race condition caused by a bug in mod_proxy, a `503` error may be returned when a node is killed, instead of failing over to another node.

JBPAPP-2955

Tomcat error pages incorrectly identify the brew build.

JBPAPP-2655

`jaxp_parser_impl.jar` and `xml-commons-apis.jar` are not included in Tomcat 6. This can cause a `SAXParseException` when parsing XML with a specific encoding (for example, GBK). Tomcat 6 requires JDK5 or higher; these JARs are not included in Tomcat because the JAXP implementation (JAXP 1.3) is built into JDK5. If users require encoding that is not supported by JAXP 1.3, the user must provide an external implementation of that encoding. The workaround for the missing JARs is therefore to copy them from Tomcat 5 into Tomcat 6.

JBPAPP-2150

The presence of a `httpd-devel.i386` package in the Red Hat Enterprise Linux 5 base channel means that the `httpd-devel` may not be properly installed to the Red Hat Enterprise Linux x86_64 from the JBoss Enterprise Web Server channel. The correct way to install this package is to run the following command:

```
yum install httpd-devel.x86_64
```

JBPAPP-1966

Apache Tomcat handles SSL encryption and decryption such that browser-httpd communication takes place in HTTPS. However, communication between httpd and JBoss Enterprise Web Server takes place in plain HTTP. By default, redirects will also use HTTP. To use HTTPS redirects, define the following attributes on the JBoss HTTP Connector:

```
proxyName="www.somedomain.com" proxyPort="443" scheme="https"
```

If JBoss Enterprise Web Server handles redirect requests for both HTTP and HTTPS, you will need one HTTP connector per protocol.

Hibernate Known Issues

JBPAPP-5898

When scrolling a query that has a join fetch on a collection, only the first item in the collection is correctly loaded. The workaround for this issue is to remove the fetch join on the collection, but it does result in n+1 selects.

mod_cluster Known Issues

JBPAPP-6257

Sessions are sticky by default with Tomcat, so the Nodes do not failover. See *HTTP Load Balancing Connector Guide* for information on enabling failover.

APPENDIX A. REVISION HISTORY

Revision 1.0.2-51.1　　　　**Wed Feb 11 2015**　　　　**Lucas Costi**

Updated the Product Name to reflect the new name grouping for the product. No update was made to details in the guide.

Revision 1.0.2-51　　　　**Tue Jun 21 2011**　　　　**Rebecca Newton**

Final build for EWS 1.0.2.

INDEX