



JBoss Enterprise Application Platform 6

Release Notes

New Features, Known Issues, and Support Information for JBoss Enterprise
Application Platform 6.0.0

Edition 2

JBoss Enterprise Application Platform 6 Release Notes

New Features, Known Issues, and Support Information for JBoss Enterprise Application Platform
6.0.0
Edition 2

Tom Wells
Red Hat Engineering Content Services
twells@redhat.com

Misty Stanley-Jones
Red Hat Engineering Content Services
misty@redhat.com

Legal Notice

Copyright © 2012 Red Hat, Inc..

This document is licensed by Red Hat under the [Creative Commons Attribution-ShareAlike 3.0 Unported License](#). If you distribute this document, or a modified version of it, you must provide attribution to Red Hat, Inc. and provide a link to the original. If the document is modified, all Red Hat trademarks must be removed.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, JBoss, OpenShift, Fedora, the Infinity logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux ® is the registered trademark of Linus Torvalds in the United States and other countries.

Java ® is a registered trademark of Oracle and/or its affiliates.

XFS ® is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL ® is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js ® is an official trademark of Joyent. Red Hat Software Collections is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack ® Word Mark and OpenStack logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

Abstract

Release notes for the JBoss Enterprise Application Platform 6.0.0 General Availability release, including new features, resolved issues, supported and unsupported configurations, and known issues.

Table of Contents

1. INTRODUCTION	2
1.1. Providing Feedback	2
1.2. Overview	2
2. NEW FEATURES	2
2.1. Specific New Features	3
3. UNSUPPORTED FEATURES	4
4. FEATURES PROVIDED AS TECH PREVIEW ONLY	5
5. COMPONENTS	5
6. RESOLVED ISSUES	5
7. KNOWN ISSUES	9
A. REVISION HISTORY	17

1. INTRODUCTION

Welcome to JBoss Enterprise Application Platform 6. As you become familiar with the newest version of JBoss Enterprise Application Platform, these Release Notes provide you with information about new features, newly-resolved issues, and known issues. Use this document in conjunction with the entire JBoss Enterprise Application Platform 6 suite of documentation, available at <http://docs.redhat.com/>.

1.1. Providing Feedback

To provide feedback on this document, file a bug at <https://bugzilla.redhat.com>, using product **JBoss Enterprise Application Platform**, version **6.0**, and component **documentation-Release_Notes**. For your convenience, you can use the following URL, which fills in the product, version, and component automatically: https://bugzilla.redhat.com/enter_bug.cgi?component=documentation%20-%20release%20notes&product=JBoss%20Enterprise%20Application%20Platform%206&version=6.0

1.2. Overview

JBoss Enterprise Application Platform 6 is Red Hat's response to significant changes in the way organizations develop and deploy enterprise applications. As organizations seek to lower operational costs and reduce time to market for new applications, JBoss Enterprise Application Platform 6 has been rebuilt for a vision of the future, boasting an innovative modular, cloudy-ready architecture, powerful management and automation, and world class developer productivity.

JBoss Enterprise Application Platform 6 is Java EE 6 certified and features powerful yet flexible management, improved performance and scalability, and many new features to improve developer productivity. All with Red Hat's market-leading reputation for certification and support, ensuring your administration and development needs continue to drive forward into the future and beyond.

2. NEW FEATURES

JBoss Enterprise Application Platform 6 is based upon JBoss Application Server 7.1.2. It supports the Java Enterprise Edition 6 specification (including the new Web Profile). Some of the key features of JBoss Enterprise Application Platform 6 include:

- Fully-modular classloading system - Classes are loaded and unloaded as needed, for a small footprint and efficient use of system resources. This makes the container slim by default, and increases security by only exposing APIs you actually use.
- Flexible management - You can manage the Enterprise Application Platform using the web-based Management Console, console-based Management CLI, or the Management API, which uses a REST-like interface and JSON output. You can use batch scripts or custom applications, to ease administration.
- Managed domains - Managed domains combine virtual servers on physical hosts into server groups, which share configuration and deployments which propagate automatically. All configuration is performed centrally, from the domain controller. You can also run multiple instances on the same physical host easily, due to the socket binding groups and automatic port offsets.

- Fast server starts and restarts - Developers will appreciate how quickly JBoss Enterprise Application Platform starts and restarts. This has benefits in production environments, but is indispensable in development environments where frequent restarts are necessary. Less time spent waiting means more time spent developing.
- Infinispan can be used as the cache provider for the HornetQ second-level cache and the HTTP session cache.
- JBoss Enterprise Application Platform 6 is compliant with Section 508 of the *Americans With Disabilities Act*, for ease of use for users of assistive technologies.
- JBoss Enterprise Application Platform 6's web-based Management Interface and log messages are internationalized and localized into Japanese, Simplified Chinese, French, German, Portuguese, and Spanish.

2.1. Specific New Features

The following new features are a small representation of overall improvements of JBoss Enterprise Application Platform 6. Refer to the individual URLs of the bugs for more details.

Clustering

JBPAPP-8574 - An external mechanism for determining the master status of a SingletonService is now exposed.

JBoss Enterprise Application Platform 5 provides an API to determine if a singleton service is active on a given cluster node. JBoss Enterprise Application Platform 6 includes a similar feature via the `org.jboss.as.clustering.singleton.Singleton.isMaster` method.

Hibernate / JPA

Obtain an Entity By A Natural Identifier

In the past, you have been able to obtain an entity by an identifier. One of the new features of Hibernate 4.x, which is included as a component of JBoss Enterprise Application Platform 6, is the ability for an application to obtain an entity by using a natural identifier. This feature is provided via the `session.byId()` and `session.bySimpleNaturalId(AAA.class).load` methods of the `Resource` class. The following is a simple example of this feature.

```
import java.lang.String;

@Entity
public class User {
    @Id
    @GeneratedValue
    Long id;

    @NaturalId
    String system;

    @NaturalId
    String userName;

    ...
}
```

```
// use getReference() to create associations...
Resource aResource = (Resource) session.byId( Resource.class
).getReference( 123 );
User aUser = (User) session.byNaturalId( User.class )
    .using( "system", "prod" )
    .using( "userName", "steve" )
    .getReference();
aResource.assignTo( user );

// use load() to pull initialized data
return session.byNaturalId( User.class )
    .using( "system", "prod" )
    .using( "userName", "steve" )
    .load();
```

3. UNSUPPORTED FEATURES

Some configurations that worked for JBoss Enterprise Application Platform 5 are no longer supported. Please review them.

Infinispan API

The direct use of the Infinispan API is not supported in JBoss Enterprise Application Platform 6. Infinispan is used as an implementation detail for various clustering technologies internal to JBoss Enterprise Application Platform. The API's module.xml incorrectly indicates that direct use is possible, even though this is not the case. This will be fixed in a future release. Direct use of the Infinispan API requires a subscription to JBoss Data Grid.

IPv6 Limitations of JDK 6

The following IPv6 limitations are caused by JDK 6, and are not defects in JBoss Enterprise Application Platform 6.

IPv6 on Microsoft Windows Server

JDK 6 on Microsoft Windows Server has only a partial IPv6 implementation, which is not sufficient to run EAP6. Full IPv6 support on Microsoft Windows Server requires JDK 7.

IPv6 on Red Hat Enterprise Linux

Due to a JDK 6 bug in Oracle JDK 6 on Red Hat Enterprise Linux, any address specified on a client (the network point establishing the connection) which contains a **zone-id** will fail. To use a **zone-id**, either upgrade to JDK 7, or use IcedTea/OpenJDK 6, which is available for Red Hat Enterprise Linux, and does not exhibit this bug. For more information about the bug, refer to http://bugs.sun.com/bugdatabase/view_bug.do?bug_id=6800096. More information about this limitation is available in this document, at [JBPAPP-8833 - EJB client does not work with zone-id of link-local IPv6 addresses](#).

JPA 2.0 Context Propagation Outside of a JTA Transaction

Hibernate's JPA implementation did not adhere to JPA 2.0 standards in that previously, an extended persistence context could be propagated outside a JTA transaction. This has been fixed, and Hibernate now complies with the specification. If your application uses an extended persistence context (XPC) to

allow queuing or batching of data modifications, you may need to make changes to your application. Refer to the JBoss Enterprise Application Platform 6 Migration Guide for instructions on updating your application. For more information about this decision, refer to <https://issues.jboss.org/browse/AS7-1663> .

Tanuki Service Wrapper

The Tanuki Service Wrapper is not supported with JBoss Enterprise Application Platform 6. More information can be found at <https://issues.jboss.org/browse/JBPAPP-8651> .

XA Recovery on Microsoft SQL Server 2008 with version 3.x JDBC driver

XA recovery does not work with Microsoft SQL Server 2008 using version 3.x JDBC drivers. This is due to a bug in the JDBC drivers, which has been addressed in version 4.x of the JDBC drivers. Refer to <https://issues.jboss.org/browse/JBPAPP-8983> and <https://community.jboss.org/thread/145358?start=0&tstart=0> for more information.

4. FEATURES PROVIDED AS TECH PREVIEW ONLY

The following configurations and features are known to have issues and are provided as tech previews only. They are not supported in a production environment.

Clustered Remote EJB Invocations with DIST SYNC Cache

Clustered remote EJB invocations fail if a server shuts down and you use the DIST SYNC cache. This issue is under investigation and clustered remote EJB invocations with the DIST SYNC cache are not supported in a production environment. This functionality is provided as a Tech Preview only.

JBoss OSGi

JBoss OSGi, an implementation of the OSGi specification, is provided as a technology preview only.

WS-AT/XA Bridge

The WS-AT/XA transaction bridge functionality is provided as a technology preview only, and is not supported in a production environment.

5. COMPONENTS

The JBoss Enterprise Application Platform 6 component matrix is available at the following location: <https://access.redhat.com/knowledge/articles/112673> .

6. RESOLVED ISSUES

Security

CVE-2012-2148 - Property replacement in any descriptor ignores java security policies

Due to descriptor replacement code executing from within the AS7 module context, java security policies may be bypassed during property replacement. New configuration flags have been added to enable/disable property replacement as required. Property replacement in jboss-descriptors are enabled by default as exploiting this flaw can be done only under very rare use cases of the server. Malicious applications can no longer exploit this flaw when property replacement is disabled.

CVE-2012-2312 - When reusing threads from a thread pool, the security context also gets reused.

Due to an incorrect implementation of security context propagation, the old security context of reused threads was retained, instead of being purged. A local attacker could use this flaw to escalate privileges in a malicious application deployed to JBoss Enterprise Application Platform. The security

subsystem now uses the `ThreadLocal` option by default. Security contexts no longer leak into the thread pool, and this flaw cannot be exploited in the default configuration.

CVE-2012-2377 - JGroups diagnostics service enabled by default with no authentication when a JGroups channel is started

When a JGroups channel was started, the JGroups diagnostics service was enabled by default with no authentication. This service was exposed via IP multicast. An attacker on an adjacent network could then exploit this flaw to read diagnostics information and invoke JMX operations on the server (limited remote code execution). To fix this issue, the `jgroups-diagnostics` socket binding has been removed. The JGroups diagnostics service is no longer exposed, unless explicitly enabled.

Clustering

JBPAPP-8925 - Failure in clustered SSO failover

If a server participating in clustered SSO was shut down normally, the undeployment on that server triggered a removal of the associated elements from the SSO cache on the second node. This problem did not occur if the server was shut down abnormally. This was due to an error in the `DistributableSessionManager.stop()` method. This error has been corrected, and the problem no longer occurs.

JBPAPP-9090 - Poor handling of network failures between the master Host Controller and slave servers

Bugs were reported regarding network disruption detection. If a node was disrupted, the master would continue to send messages to the slave, and the slave would not be able to rejoin the cluster when it returned to the network, because the master still saw it as registered.

These issues have been resolved by updating the Remoting subsystem to better detect network disruptions and unregister slave servers which have become unavailable.

JBPAPP-8835 - Clustered SSO failure.

There was an issue where SSO credentials were correctly replicated and stored in `SSOClusterManager.cache`, but the lookup method failed to retrieve it, returning a `null` value. This issue has been fixed.

JBPAPP-8466 - The `mod_cluster` service was running for a short time after its connector was shutdown

During server shutdown, the connector used for `mod_cluster` communication was shutdown before the `mod_cluster` service was stopped. This resulted in many failed `mod_cluster` requests in the intervening time period. A service dependency has now been added on the web connector service and the `mod_cluster` subsystem must now declare which connector it is using. This means that the `mod_cluster` service will be automatically be stopped when the connector is shutdown.

Consoles

JBPAPP-8911 - Requirement of the `wsdl-host` attribute of the Webservice provider was not enforced

While the presence of the `wsdl-host` attribute in the Webservice provider configuration was previously not required, even though if it is not present, JBoss Enterprise Application Platform will not start. The Management API now checks for and enforces the requirement for this attribute to be set.

EJB

JBPAPP-8921 - NullPointerException in method `SessionContext.wasCancelCalled` if the call is not asynchronous or remote

`NullPointerException` was thrown instead of `IllegalStateException`, if the `wasCancelCalled` is not invoked from within an asynchronous business method invocation with return type `Future<V>`. In addition, if the method as called on a method which was defined as synchronous, and called remotely, an exception was returned instead of a boolean value. This bug has been fixed, and the exception no longer occurs.

JBPAPP-8573 - EJB components do not have dependencies on the `ModuleDeployment` service.

Due to the lack of a service dependency on the `ModuleDeployment` service, remote invocations were rendered unavailable before the EJB shut down. This issue has been fixed.

JBPAPP-8138 - `isDone()` method doesn't return true after `cancel()` call on EJB asynchronous method.

Method `isDone()` was not returning `true` after `cancel()` call on Future object bound to call of EJB asynchronous method. This issue has been fixed.

JBPAPP-8920 - Server side implementation of the Future instance returned for an asynchronous EJB method invocation had a flaw in the `isDone()` method.

The server side implementation of the Future instance returned for an asynchronous EJB method invocation had a flaw in the `isDone()` method. As a result, the `isDone()` method on an EJB was not always returning true when the `cancel()` method was called asynchronously. The `isDone()` method now properly registers an asynchronous call to `cancel()`, and always returns true after `cancel()` has been called.

Hibernate / JPA

JBPAPP-8031 - NullPointerException occurs in `CacheAdapterImpl` when evicting the entity cache.

A `NullPointerException` occurred when evicting the entity cache using method `emf.getCache().evictAll();`. This occurred because `CacheAdapterImpl` did not check for a `null` value returned from the `cache.getRpcManager()` method. This has been resolved by adding a check for a `null` value.

JBPAPP-8398 - Spurious `ERROR` message logged when deploying JPA 1.0 applications

When deploying a JPA 1.0 application with an `orm.xml` file, the following message was logged in the console:

```
00:25:55,990 ERROR [org.hibernate.internal.util.xml.ErrorLogger] (MSC
service thread 1-3) HHH000196: Error parsing XML (5) : cvc-complex-
type.3.1: Value '1.0' of attribute 'version' of element 'entity-
mappings' is not valid with respect to the corresponding attribute use.
Attribute 'version' has a fixed value of '2.0'
{code}
```

This `ERROR` message confusing because the application deployed correctly, despite the message. This has been resolved by not logging an error message as long as the `orm.xml` is valid, whether the application uses JPA 1.0 or 2.0.

JBPAPP-8842 - NullPointerException in the PreCollectionRemove listener

If collection removal actions were added by the `DefaultAutoFlushEventListener.onAutoFlush()` method, they need to be removed if the flush is not actually needed, because no updates involve the specified query spaces. A fix to the bug **HHH-6862** introduced a situation where these collection removal actions were no longer removed in this situation. As a result, when the session was flushed, duplicate collection actions were added to the action queue. The first of these actions executed properly, but set the value of `CollectionEntry.loadedPersister` to `null`. If Hibernate Envers was used, the second removal action involving the same collection would fail with a `NullPointerException` when `EnversPreCollectionRemoveEventListenerImpl.onPreRemoveCollection()` called `collectionEntry.getLoadedPersister().isInverse()`. This problem has been fixed, and the duplication and exception no longer occur.

JBPAPP-9142 - Infinispan 2LC did not allow entities to be deleted

When deleting a Readonly or Immutable Entity from the 2LC, the Readonly cache strategy was used, and an `UnsupportedOperationException` exception was thrown.

This was resolved by using a read/write cache strategy, and the entities can now be removed from the 2LC.

HornetQ / JMS**JBPAPP-8935 - JMS clients cannot authenticate to the messaging subsystem**

JMS clients could not authenticate to the messaging subsystem. A `JMSSecurityException` was thrown if the `ApplicationRealm` security realm was removed from the remoting subsystem. This was due to a race condition in the security realm mechanism, and the issue has been resolved by fixing that race condition.

HTTP Connectors**JBPAPP-8919 - Apache JK status manager issues**

Apache `mod_jk` includes a status manager API. When operations were run with it, the changes were not applied. This occurred via the API and the JK Status Manager web interface. This was due to an error with shared memory synchronization. This error has been corrected, and the JK Manager works as expected.

PicketLink**JBPAPP-8462 - Issue where JBossPDP was not able to read policies from the deployed archive.**

Previously there was an issue where JBossPDP could not be instantiated as it was not able to read required archived policies that it was deployed with. A fix has been implemented to allow file URIs to be correctly handled by JBossPDP `isDirectory()`.

Scripts and Utilities**JBPAPP-8844 - An exception was thrown when running the `jdr.sh` utility**

An `NullPointerException` was thrown when attempting to execute the `jdr.sh` utility. This occurred because the utility had a bug which prevented it from working with unsigned JARs. This problem has been fixed, and the utility now works as expected.

7. KNOWN ISSUES

Security

CVE-2012-2672 - Mojarra: deployed web applications can read FacesContext from other applications under certain conditions

The FacesContext instance that is made available during application startup is held in a ThreadLocal. The reference is not properly cleaned up in all cases. As a result, if a JSF WAR calls `FacesContext.getCurrentInstance()` during application startup, another WAR can get access to the leftover context and thus get access to the other WAR's resources. The cause of this issue is still under investigation.

CVE-2012-2379 - Apache CXF does not verify that elements were signed / encrypted by a particular Supporting Token

A flaw was found in the way Apache CXF verifies that XML elements were signed or encrypted by a particular Supporting Token. CXF checks to ensure these elements are signed or encrypted by a Supporting Token, but not whether the correct token is used. A remote attacker could use this flaw to transmit confidential information without the appropriate security, and potentially to circumvent access controls on web services exposed via CXF. This issue will be fixed in a future release of JBoss Enterprise Application Platform 6.

CVE-2012-2378 - Child policies of WS-SecurityPolicy 1.1 not applied on the client side

Apache CXF does not properly enforce some child policies of WS-SecurityPolicy 1.1 on the client side. In certain circumstances, this could lead to a client failing to sign or encrypt certain elements as directed by the security policy. As a result, there could be insecure transmissions of information (information disclosure). This issue will be fixed in a future release of JBoss Enterprise Application Platform 6.

CVE-2012-2333 - openssl: record length handling integer underflow

It was discovered that OpenSSL did not properly handle TLS record length values from the received TLS packets. After subtracting the number of padding bytes from the record length value, it did not check the resulting record length before subtracting the size of explicit IV (initialization vector for CBC encryption modes). This could result in an integer underflow of the record length value, leading to a buffer over-read and out-of-bounds access. A remote TLS peer could use this to crash an application using OpenSSL (usually a TLS or DTLS server) by sending a specially TLS packet. This issue will be fixed in a future release of JBoss Enterprise Application Platform 6.

RPMs

JBPAPP-9043 - RPM distribution contains unsupported signed jars

The signed jars present in the RPM distribution for Red Hat Enterprise Linux 6 are unsupported. These jars will be removed in a later release of JBoss Enterprise Application Platform 6.

Clustering

JBPAPP-8423 - Failover during state transfer sometimes fail with exception StateTransferInProgressException.

Failovers during state transfer sometimes fail with the above exception, due to problems with the Infinispan cache. This can cause the entire cluster to become unresponsive.

JBPAPP-8426 - Clean shutdown of a cluster results in an error message.

If you shut down your cluster cleanly, you may still receive error messages such as **Problems unmarshalling remote command from byte buffer**. This will be fixed with an update to the Infinispan component.

JBPAPP-8428 - A JGroups error can occur because of a crashed cluster.

You may see messages such as **failed sending diag rsp to /10.16.88.172:47231: java.io.IOException: Message too long** if a cluster node crashes. This message has to do with parsing debugging information, not with a problem in the runtime itself. The logging error will be fixed by an update to the JGroups component.

JBPAPP-8696 - NotSerializableException can occur when undeploying a clustered application

Undeploying an application from one node in a cluster can result in **NotSerializableException** exceptions. This is due to a race condition between the shutdown of the web deployment (including the session manager) and the stopping of the dependent **DistributedCacheManagerFactory**, which depends on the cache container. The cache container stops while the web session cache is in the process of stopping and the externalizer on which it depends suddenly becomes null, causing the **NotSerializableException**. The fix for this issue is still under investigation.

JBPAPP-8703 - An exception occurs during a node shutdown when using DIST SYNC cache mode, and during a server crash using REPL SYNC cache mode

An exception sometimes occurs during shutdown of a cluster node when using DIST SYNC cache mode, or during a node crash when using REPL SYNC cache mode. The exception appears in the logs as follows:

```
"Exception acquiring ownership of HASH (via SharedLocalYieldingClusterLockManager)"
```

The root cause of this exception is unknown, and this issue is under investigation.

JBPAPP-8937 - Sessions lost when a node crashes using DIST SYNC cache mode

In some instances, when a node crashed, its session was not found in cache and a new session was created. This only occurs when a server is killed, not during a graceful shutdown. The root cause and solution are under investigation.

JBPAPP-8940 - Sessions sometimes fail to passivate with a timeout message indicating that 0 milliseconds have passed

Sessions sometimes fail to passivate with the following log message:

```
Execution error: org.infinispan.util.concurrent.TimeoutException: Unable to acquire lock after [0 milliseconds] on key [ULsh1+wHh0iUAR33vnqM2H8E] for requestor [Thread[ContainerBackgroundProcessor[StandardEngine[jboss.web]],5,main]]!
```

This is a cache eviction, and should result in **ERROR** messages. The logic of the **RetryCacheInvoker** class needs to be modified to log at the appropriate severity level.

JBPAPP-8941 - CDI beans with SET replication trigger are not replicated

Due to a bug in the Weld component, the **setAttribute** method is not called correctly. This causes CDI beans with the **SET** replication trigger to fail to be replicated. The workaround is to use the **SET_AND_NON_PRIMITIVE_GET** trigger for these beans. This will be fixed in a future release.

JBPAPP-8960 - Singleton Service fails on Microsoft Windows Server with an IllegalStateException

An error like the following can be seen on Microsoft Windows:

```
IllegalStateException: JBAS010350: Expected result from singleton provider only, but instead received 0 results
```

This issue is under investigation and seems to be due to timing. The fix will be to make the **getValueRef** method retry if the new master has not yet been notified. Until this fix is in place, the workaround is to add a **Thread.sleep()** call to your code to delay the **getValueRef()** call.

JBPAPP-9083 - Slow response time in Remote EJB invocation on cluster membership change

On server shutdown or crash, membership changes can take up to one minute to complete. This issue is currently under investigation.

JBPAPP-9084 - TimeoutException during shutdown in REPL SYNC cache mode

A **TimeoutException** can occur during node shutdown when using REPL SYNC cache mode. The root cause of this issue is still under investigation.

JBPAPP-9086 - Stale session data received during node shutdown when using DIST SYNC cache mode

During testing, a few cases showed that stale session data was received when a node shut down and DIST SYNC cache mode was used. This issue is still under investigation.

JBPAPP-9088 - Clustered sessions are lost on server shutdown when using DIST ASYNC cache mode

In some situations, clustered sessions are lost when a server shuts down when using DIST ASYNC cache mode. The cause of this issue is still under investigation.

JBPAPP-9092 - Failures on clustered remote EJB invocations in event of server shutting down using DIST SYNC cache

Clustered remote EJB invocations fail if a server shuts down and you use the DIST SYNC cache. This issue is under investigation and clustered remote EJB invocations with the DIST SYNC cache are not supported in a production environment. This functionality is provided as a Tech Preview only.

JBPAPP-9136 - NoSuchEJBException when using sync replication with remote EJBs

A **NoSuchEJBException** can occur when using clustered remote EJBs with sync replication. The stateful session bean cache is lost and the client does not receive a valid reply. The cause of this issue is under investigation.

JBPAPP-9183 - WeldListener: java.lang.NullPointerException when using session passivation

A **WeldListener: java.lang.NullPointerException** is thrown occasionally when using session passivation. The client receives a HTTP response **503**, along with the exception text. The cause of this bug is under investigation.

JBPAPP-9254 - 500 status codes returned to the HTTP client upon server shut-down

500 status codes are sometimes returned to the HTTP client upon server shut-down. This issue is currently under investigation.

Consoles**JBPAPP-8959 - mod_cluster SSL configuration fails to save**

There are problems with saving the **mod_cluster** SSL configuration in both the web-based management console and the console-based management CLI. The values appear to be saved but they are not written to the configuration file correctly. The work-around is to edit the **domain.xml** or **standalone.xml** file directly to edit these values.

EJB**JBPAPP-8833 - EJB client does not work with zone-id of link-local IPv6 addresses**

IPv6 addresses include an optional **zoneid** parameter for use with link-local addresses, to differentiate between multiple local interfaces. If you attempt to start JBoss Enterprise Application Platform with an interface binding which contains a **zoneid**, a **java.lang.RuntimeException: Operation failed with status WAITING** exception occurs. This cannot be fixed due to limitations in Oracle JDK 6 and JDK 6 provided by other vendors, which prevent any fix from reliably working on all Linux distributions. This problem does not occur with JDK 7, or OpenJDK 6.

JBPAPP-8987 - Cannot deploy EJBs if the Remoting subsystem is not installed

You cannot deploy EJBs if the Remoting subsystem is deployed. This is because of a bug which introduced hard dependencies between the two subsystems. To work around this issue, make sure that the Remoting subsystem is enabled.

JBPAPP-9140 - Remote EJB clients hang after calling method `EJBClient.createSession` when using DIST mode

Remote EJB clients sometimes hang after calling method **EJBClient.createSession** when using DIST mode. The cause of this bug is still under investigation.

HTTP Connectors**JBPAPP-9226 - Unresolvable APR Symlinks on Red Hat Enterprise Linux**

Apache portable runtime (APR) binaries are not natively packaged as part of JBoss Enterprise Application Platform, or JBoss Enterprise Web Server, for Red Hat Enterprise Linux. Symlinks are used to reference the base Red Hat Enterprise Linux libraries. This can result in an issue with unresolvable symlinks when trying to use APR binaries if the following packages are not installed: **apr**, **apr-util**, **apr-devel**, **apr-util-devel**.

The fix for this issue will be shipped via a Red Hat Enterprise Linux APR update against the bugzilla referenced in the JIRA.

JBPAPP-9308 - Strict conditions on starting Apache with `mod_cluster` on Windows servers

On Windows servers, Apache with `mod_cluster` in JBoss Enterprise Application Platform 6 can only be started if the following conditions are met:

1. The user must have administration rights.
2. User Account Control (UAC) must be disabled.

JBPAPP-9310 - Apache portable runtime (APR) libraries fail to load on Windows servers

On Windows servers, Apache portable runtime (APR) libraries will fail to load unless a user with administration rights is being used with User Account Control (UAC) disabled.

HornetQ / JMS

JBPAPP-8336 - HornetQ servers cannot create clusters when they are bound to IPv6 link-local addresses

Due to a JDK bug, if you use link local addresses, zone-ids are used to distinguish which interface is chosen. This problem does not affect global addresses. A workaround will be included in a future version of the Netty component.

JBPAPP-8501 - Class `RemoteConnectionFactory` not found

When looking up a `RemoteConnectionFactory` from a remote client, the class is not found and a `NamingException` occurs. This is because many fields are not serializable, and will be fixed in a future release of the HornetQ component. The workaround is to use local lookups.

JBPAPP-9005 - Memory leaks when deploying message-driven beans

Memory leaks have occurred during testing of message-driven beans (MDBs). After 1000 deployments of a quickstart application, the memory footprint of the application server was increased by 100 or more megabytes. The performance differed depending on which JVM was used. The highest memory footprint was seen with the 64-bit Oracle JVM. The leakage occurs in the client session factories created by the HornetQ resource adapter during MDB deployment, but not cleaned up properly during undeployment.

This memory leak will be fixed by a future upgrade to the HornetQ component. However, the testing scenario is not considered a risk for a production environment.

JBPAPP-9178 - Segmentation fault with the HornetQ object store on Red Hat Enterprise Linux 6 with AIO and IBM JDK

JBoss Enterprise Application Platform 6 fails to start due to a segmentation error if the HornetQ object store is enabled and the server is running on Red Hat Enterprise Linux 6 using AIO natives and IBM JDK. This is caused by limitations with IBM JDK and Native Buffers. The workaround to this issue is to use NIO instead of AIO for storage, when using IBM JDK.

JBPAPP-8910 - No pre-defined way to deploy a JMS bridge.

There is currently no pre-defined way to deploy a JMS bridge (i.e. `org.hornetq.jms.bridge.impl.JMSBridgeImpl`). In JBoss AS 6 and earlier the bridge could be deployed as an MBean or JBoss MC bean, but the current configuration schema doesn't support it.

Hibernate

JBPAPP-8864 - Problem in caching proper natural-id-values when obtaining result by naturalIdQuery using NaturalIdLoadAccess

`NaturalIdLoadAccess` behaves inconsistently when trying to load entities from 2Lcache after an update of their natural-id values from a non-transactional scenario. Hibernate does not currently support proper 2L caching of entities with natural ids in scenarios where there is a mix of transactional and non-transactional access to the database.

IPv6

JBPAPP-8778 - Unable to bind management interface to IPv6 in Domain Mode, if passed at the command line

In a managed domain, turning off the default preference for using an IPv4 network stack by passing `-Djava.net.preferIPv4Stack=false` as an argument to `domain.sh` or `domain.bat` does not work. Without turning off this preference, IPv6 addresses cannot be used for the sockets opened by EAP processes. For example, this will not work:

```
bin/domain.sh -Djava.net.preferIPv4Stack=false -bmanagement=:::1
```

The workaround for this issue is to edit the `bin/domain.conf` or `bin\domain.conf.bat` scripts, and set `-Djava.net.preferIPv4Stack=false`.

JBPAPP-9202 - Wrong format of IPv6 addresses in log entries

IPv6 addresses should be formatted with square brackets ([and]) around them, such as in `http://[2620:52:0:105f::ffff:2]:9990`. The brackets are missing in the log files for JBoss Enterprise Application Platform 6. This issue is scheduled to be fixed in a future release.

JBPAPP-8286 - IPv4 sockets are opened when the server uses IPv6 in a Microsoft Windows environment

If JBoss Enterprise Application Platform 6 is started in Microsoft Windows server with the IPv4 stack disabled and the IPv6 stack enabled, IPv4 sockets are still opened. This issue is still under investigation.

AS7-3834 - Socket bind for JIoEndpoint fails on shutdown when using link-local IPv6 address

If you start JBoss Enterprise Application Platform 6 with a link local IPv6 address, specifying the numeric zone-id, the server starts correctly but hangs or takes several minutes, when shutting down. This problem only occurs on JDK6. The workaround if you need this behavior is to use JDK7. A possible fix is under investigation. This issue also relates to [AS7-3752](#).

IPv6 Testing Limitations

IPv6 support is untested on the Solaris platform. In addition, a connection from JBoss Enterprise Application Platform 6 to a database server which uses an IPv6 address is untested.

IPv4 and IPv6 Interoperability

Not all combinations of IPv4 and IPv6 client/server compatibility have been tested on all supported operating systems.

JAX-WS

Artifacts modified from AS7 version

Some JAX-WS artifacts have been modified from the AS7 version to fix issues with JBossWS JAXB. This can cause incompatibilities with applications developed against AS7 and deployed in JBoss Enterprise Application Platform 6. Refer to [JBPAPP-8023](#) and [JBPAPP-7781](#) for details.

The following list shows the replacements and changes to the artifacts.

POM

- `javax.xml.bind:jaxb-api:2.2.3` was replaced by `org.jboss.spec.javax.xml.bind:jboss-jaxb-api_2.2_spec`
- `org.jvnet.wagon-svn:wagon-svn:1.8 extension` was removed
- `com.sun.istack:istack-commons-runtime:2.5-redhat-1` and `com.sun.xml.txw2:txw2:201103-redhat-1` were added
- The following artifacts were also added.

```
com.sun.codemodel:codemodel:2.5-redhat1,
com.sun.xml.dtd-parser:dtd-parser:1.2-redhat-1,
com.sun.istack:istack-commons-tools:2.5-redhat-1,
com.github.relaxng:relaxngDatatype:2011.1-redhat-1,
org.kohsuke.rngom:rngom:201103-redhat-1,
com.sun.xml.xsom:xsom:20110101-redhat-1,
xml-resolver:xml-resolver:1.2-redhat-1
remove: org.jvnet.wagon-svn:wagon-svn:1.8 extension
```

JAR

- `com/sun/xml/txw2/*`, `com/sun/istack/*` were removed.
- The following files were also removed:

```
1.0/*
com/sun/codemodel/*
com/sun/istack/tools/*
org/apache/xml/internal/resolver/*
com/sun/xml/dtdparser/*
com/sun/xml/xsom/*
org/relaxng/datatype/*
org/kohsuke/rngom/*
*.rng
```

Logging

[JBPAPP-9159](#) - Re-creating a logging handler fails with message **JBAS014749: Operation handler failed**

If you create a logging handler from the Management CLI using the `:add` operation, remove it using the `:remove` operation, and then add it again using the `:add` operation, the second addition fails with the message **JBAS014749: Operation handler failed: null**. The workaround is to remove the service from the subsystem, and add it back again. This issue is still under investigation.

Picketlink

JBPAPP-8311 - Vault error "Exception encountered:PB00019: Processing Failed:Unable to get Keystore:"

There is a regression in JBoss Vault where the following exception occurs: **Exception encountered:PB00019: Processing Failed:Unable to get Keystore:.** The cause of this regression is currently under investigation.

Scripts and Utilities

JBPAPP-8984 - The -server parameter is not added for the process controller or host controller when using IBM JDK

When using the IBM JDK version 6 or 7, the **-server** parameter is not added to the process controller or host controller commands, when using a managed domain. The error is found in the **domain.sh** script, starting at line 76. The workaround is to edit the **domain.sh** script to add the **-server** parameter. This will be fixed in a future release.

JBPAPP-9133 - JDR script utility is unable to connect to the localhost

The JDR utility (**EAP_HOME/bin/jdr.sh** or **jdr.bat**) fails to connect to the localhost, with the message **JBOSS API call failed, falling back to HTTP: Controller Client is not available.** The cause of this error is still under investigation.

JBPAPP-9249 - Some script utilities do not work correctly on Microsoft Windows Server if the variables \$JBOSS_HOME or \$JAVA_HOME contain space symbols.

The utilities **vault.bat** and **jconsole.bat** will not work correctly if the path to **\$JAVA_HOME** or **\$JBOSS_HOME** contains a space symbol.

The workaround is to install JBoss Enterprise Application Platform to a location that does not have spaces in the directory path.

A. REVISION HISTORY

Revision 0.0-7.400 Rebuild with publican 4.0.0	2013-10-31	Rüdiger Landmann
Revision 0.0-7 BZ#896430 - updated components URL	Tue Feb 26 2013	Darrin Mison
Revision 0.0-6 Added OSGi entry to the Technical Preview section of the release notes.	Fri Sept 21 2012	Tom Wells
Revision 0.0-5 Updated documentation for JBoss Enterprise Application Platform 6.	Fri Sept 21 2012	Tom Wells
Revision 0.0-4 Fixed Bugzilla issues related to unsupported features.	Fri Sept 21 2012	Tom Wells
Revision 0.0-3 Updated edition of the JBoss Enterprise Application Platform 6.0.0 Release Notes.	Thu Aug 30 2012	Tom Wells
Revision 0.0-2 Updated edition of the JBoss Enterprise Application Platform 6.0.0 Release Notes.	Thu Aug 30 2012	Tom Wells
Revision 0.0-1 First edition of the JBoss Enterprise Application Platform 6 Release Notes.	Wed Jun 20 2012	Tom Wells