Red Hat JBoss Enterprise Application Platform 7.3

Patching and Upgrading Guide

Instructions for applying patches and implementing upgrades from one minor Red Hat JBoss Enterprise Application Platform release to the next.

Red Hat JBoss Enterprise Application Platform 7.3 Patching and Upgrading Guide

Instructions for applying patches and implementing upgrades from one minor Red Hat JBoss Enterprise Application Platform release to the next.

Legal Notice

Abstract

This book is a guide for patching or upgrading a Red Hat JBoss Enterprise Application Platform installation.

Table of Contents

CHAPTER 1. INTRODUCTION

1.1. ABOUT MIGRATIONS AND UPGRADES

Major Upgrades

A major upgrade or migration is required when an application is moved from one major release to another, for example, from JBoss EAP 6.4 to JBoss EAP 7.0. If an application follows the Java EE specifications, does not access deprecated APIs, and does not contain proprietary code, it might be possible to run the application in JBoss EAP 7 without any application code changes. However, the server configuration has changed in JBoss EAP 7 and requires migration. This type of migration is addressed in the JBoss EAP *Migration Guide*.

Minor Updates

JBoss EAP periodically provides point releases, which are minor updates that include bug fixes, security fixes, and new features. Information about the changes made in a point release are documented in the JBoss EAP *Migration Guide* and in the *7.3.0 Release Notes*.

You can use the JBoss Server Migration Tool to automatically upgrade from one point release to another, for example from JBoss EAP 7.0 to JBoss EAP 7.1. For information about how to configure and run the tool, see Using the JBoss Server Migration Tool.

If you prefer, you can perform a manual upgrade of the server configuration. Instructions on how to perform a manual upgrade are documented in this guide. For more information, see Upgrading JBoss EAP.

Cumulative Patches

JBoss EAP also periodically provides cumulative patches that contain bug and security fixes. Cumulative patches increment the release by the last digit, for example from 7.1.0 to 7.1.1. Patch installation is addressed in the Patching JBoss EAP chapter of this guide.

1.2. SUBSCRIBING TO SECURITY ANNOUNCEMENTS

Red Hat maintains a mailing list for security announcements. You can subscribe to this mailing list to be notified of security-related announcements that affect JBoss EAP.

CHAPTER 2. PATCHING JBOSS EAP

The method of applying a patch to JBoss EAP depends on your installation method. If you installed JBoss EAP using the ZIP or installer methods, you must use the ZIP-based patch management system . If you used RPMs to install JBoss EAP on Red Hat Enterprise Linux, you must use RPM patches.

> **IMPORTANT**
>
> Before applying or rolling back a patch, you should back up your JBoss EAP server, including all deployments and configuration files.

If you have a locally installed JBoss EAP Maven repository, you must also patch the Maven repository to the same cumulative patch version as your JBoss EAP server.

2.1. PATCHING A ZIP/INSTALLER INSTALLATION

Cumulative patches for a ZIP or Installer installation of JBoss EAP are available to download from the Red Hat Customer Portal .

For multiple JBoss EAP hosts in a managed domain environment, individual hosts can be patched from your JBoss EAP domain controller.

In addition to applying a patch, you can also roll back the application of a patch.

2.1.1. Important Notes on ZIP/Installer Installation Patching

- If you apply a patch that updates a module, the new patched JARs that are used at runtime are stored in *EAP_HOME*/**modules**/**system**/**layers**/**base**/**.overlays**/*PATCH_ID*/*MODULE*. The original unpatched files are left in *EAP_HOME*/**modules**/**system**/**layers**/**base**/*MODULE*, but these JARs are **not** used at runtime.

- In order to significantly decrease the size of cumulative patch releases for JBoss EAP 7, you now cannot perform a partial roll back of a cumulative patch. For a patch that has been applied, you will only be able to roll back the whole patch.
  For example, if you apply CP03 to JBoss EAP 7.0.0, you will not be able to roll back to CP01 or CP02. If you would like the ability to roll back to each cumulative patch release, each cumulative patch must be applied separately in the order they were released.

2.1.2. Applying a Patch

> **NOTE**
>
> JBoss EAP servers that have been installed using the RPM method cannot be updated using these instructions. See the RPM instructions for applying a patch instead.

You can apply downloaded patches to a JBoss EAP server using either the management CLI or the management console.

NOTE

You can manage the JBoss EAP XP patches only using the management CLI.

For information about JBoss EAP XP patch streams, see JBoss EAP XP manager for managing JBoss EAP XP patch streams in the *Using Eclipse MicroProfile in JBoss EAP* guide.

Applying a Patch to JBoss EAP Using the Management CLI

1. Log in to the Red Hat Customer Portal, and download the patch file from JBoss EAP Software Downloads.

2. From the management CLI, apply the patch using the following command, including the appropriate path to the patch file:

   ```
   patch apply /path/to/downloaded-patch.zip
   ```

   NOTE

   To patch another JBoss EAP host in a managed domain, you can specify the JBoss EAP host name using the **--host=** argument. For example:

   ```
   patch apply /path/to/downloaded-patch.zip --host=my-host
   ```

   The patch tool will warn if there are any conflicts in attempting to apply the patch. If there are conflicts, enter **patch --help** for the available arguments to re-run the command with an argument specifying how to resolve the conflicts.

3. Restart the JBoss EAP server for the patch to take effect:

   ```
   shutdown --restart=true
   ```

Applying a Patch to JBoss EAP Using the Management Console

1. Log in to the Red Hat Customer Portal, and download the patch file from JBoss EAP Software Downloads.

2. Open the management console and navigate to the **Patching** tab.

3. Add the patch using the **Add Patch** wizard.

   - For a standalone server:

     a. Click the Add (**+**) button.

     b. Click **Choose a file or drag it here**, select the downloaded patch to apply, and click **Next**.

     c. Configure any of the additional options and click **Finish**.

   - For a managed domain:

     a. Select the host to patch and click the Add (**+**) button.

b. Select whether to shut down the servers on the host, and click **Next**.

c. Click **Choose a file or drag it here**, select the downloaded patch to apply, and click **Next**.

d. Configure any of the additional options and click **Finish**.

4. Verify that the patch was applied successfully.

- If the patch was applied successfully, restart the server for the changes to take effect.

- If the patch application failed, review the error message. If there was a conflict, you can use the **Override All**, **Override Modules**, and **Override** fields in the **Add Patch** wizard to bypass content verification for items that the patch changes. Overriding conflicts will result in the content of the patch overriding any user modifications.

2.1.3. Rolling Back a Patch

You can roll back a previously applied JBoss EAP patch using either the management CLI or the management console.

> **IMPORTANT**
>
> Rolling back a patch using the patch management system is not intended as a general uninstall functionality. It is only intended to be used immediately after the application of a patch that had undesirable effects.

> **NOTE**
>
> You can manage the JBoss EAP XP patches only using the management CLI.
>
> For information about JBoss EAP XP patch streams, see JBoss EAP XP manager for managing JBoss EAP XP patch streams in the *Using Eclipse MicroProfile in JBoss EAP* guide.

Prerequisites

- A patch that was previously applied.

> **WARNING**
>
> When rolling back a patch, use caution when specifying the value of the **Reset Configuration** option:
>
> If set to **TRUE**, the patch rollback process will also roll back the JBoss EAP server configuration files to their pre-patch state. Any changes that were made to the JBoss EAP server configuration files after the patch was applied will be lost.
>
> If set to **FALSE**, the server configuration files will not be rolled back. In this situation, it is possible that the server will not start after the rollback, as the patch may have altered configurations, such as namespaces, which may no longer be valid and will have to be fixed manually.

Rolling Back a Patch Using the Management CLI

1. From the management CLI, use the **patch history** command to find the ID of the patch that you want to roll back.

   > **NOTE**
   >
   > If you are using a managed domain, you must add the **--host=*HOSTNAME*** argument to the commands in this procedure to specify the JBoss EAP host.

2. Roll back the patch with the appropriate patch ID from the previous step.

   ```
   patch rollback --patch-id=PATCH_ID --reset-configuration=TRUE
   ```

   The patch tool will warn if there are any conflicts in attempting to roll back the patch. If there are conflicts, enter **patch --help** for the available arguments to re-run the command with an argument specifying how to resolve the conflicts.

3. Restart the JBoss EAP server for the patch roll back to take effect:

   ```
   shutdown --restart=true
   ```

Rolling Back a Patch Using the Management Console

1. Open the management console and navigate to the **Patching** tab.

2. Roll back the patch using the **Rollback** wizard.

   - For a standalone server:

     a. Select the patch to roll back and click **Rollback**.

     b. Configure any of the additional options and click **Finish**.

   - For a managed domain:

     a. Select the host, select the patch to roll back, and click **Rollback**.

b. Select whether to shut down the servers on the host and click **Next**.

c. Configure any of the additional options and click **Finish**.

3. Verify that the rollback was successful.

- If the patch was rolled back successfully, restart the server for the changes to take effect.

- If the patch rollback failed, review the error message. If there was a conflict, you can use the **Override All**, **Override Modules**, and **Override** fields in the wizard to bypass content verification for items affected by the patch.

2.1.4. Clearing Patch History

When patches are applied to a JBoss EAP server, the content and history of the patches are preserved for use in rollback operations. If multiple cumulative patches are applied, the patch history may use a significant amount of disk space.

You can use the following management CLI command to remove all older patches that are not currently in use. When using this command, only the latest cumulative patch is preserved along with the GA release. This is only useful for freeing space if multiple cumulative patches have previously been applied.

```
/core-service=patching:ageout-history
```
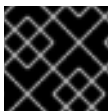
> **IMPORTANT**
>
> If you clear the patch history, you will not be able to roll back a previously applied patch.

2.2. PATCHING AN RPM INSTALLATION

Prerequisites

- Ensure that the base operating system is up to date, and is subscribed and enabled to get updates from the standard Red Hat Enterprise Linux repositories.

- Ensure that you are subscribed to the relevant JBoss EAP repository for the update.

> **WARNING**
>
> When updating an RPM installation, JBoss EAP is updated cumulatively with all RPM-released fixes for the subscribed repository.

- Back up all configuration files, deployments, and user data.
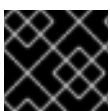
> **IMPORTANT**
>
> For a managed domain, the JBoss EAP domain controller should be updated first.

To install a JBoss EAP patch via RPM from your subscribed repository, update your Red Hat Enterprise Linux system using the following command:

```
# yum update
```

2.3. OPTIONAL: PATCH A LOCAL JBOSS EAP MAVEN REPOSITORY

If you have installed the JBoss EAP Maven repository, it may also need to be patched.

The JBoss EAP Maven repository is available online or as a downloaded ZIP file. If you use the publicly hosted online Maven repository, updates are automatically applied, and no action is required to update it. However, if you installed the Maven repository locally using the ZIP file , you are responsible for applying updates to the repository.

Whenever a cumulative patch is released for JBoss EAP, a corresponding patch is provided for the JBoss EAP Maven repository. This patch is available in the form of an incremental ZIP file that is unzipped into the existing local repository. It does not overwrite or remove any existing files, so there is no rollback requirement.

Use the following procedure to apply updates to your locally installed JBoss EAP Maven repository.

Prerequisites

- Valid access and subscription to the Red Hat Customer Portal.

- The JBoss EAP 7.3 Maven repository, previously downloaded and installed locally.

Update a Locally Installed JBoss EAP Maven Repository

1. Open a browser and log into the Red Hat Customer Portal .

2. Select **Downloads** from the menu at the top of the page.

3. Find **Red Hat JBoss Enterprise Application Platform** in the list and click on it.

4. Select the correct version of JBoss EAP from the **Version** drop-down menu, then click on **Patches** tab.

5. Find **Red Hat JBoss Enterprise Application Platform 7.3 Update *CP_NUMBER* Incremental Maven Repository** in the list, where *CP_NUMBER* is the cumulative patch number you want to update to, and then click **Download**.

6. Locate the path to your JBoss EAP Maven repository. This is referred to in the commands below as ***EAP_MAVEN_REPOSITORY_PATH***.

7. Unzip the downloaded Maven patch file directly into the directory of the JBoss EAP 7.3 Maven repository.

   a. For Red Hat Enterprise Linux, open a terminal and run the following command, replacing the values for the cumulative patch number and your Maven repository path.

   ```
   $ unzip -o jboss-eap-7.3.CP_NUMBER-incremental-maven-repository.zip -d
   EAP_MAVEN_REPOSITORY_PATH
   ```

b. For Microsoft Windows, use the Windows extraction utility to extract the ZIP file into the root of the *EAP_MAVEN_REPOSITORY_PATH* directory.

CHAPTER 3. UPGRADING JBOSS EAP

> **IMPORTANT**
>
> This chapter describes how to upgrade from one JBoss EAP 7 minor release to another. For example, upgrading from JBoss EAP 7.0 to JBoss EAP 7.1.
>
> If you are migrating from an earlier major release of JBoss EAP, for example from JBoss EAP 6 to JBoss EAP 7, see the *Migration Guide* instead.

3.1. PREPARING FOR THE UPGRADE

Before you upgrade JBoss EAP, you need to be aware of the following potential issues.

- If you back up and restore your configuration files when upgrading to newer point releases, you could overwrite new configurations that are in the new release and prevent new features from being enabled automatically. The recommended approach is to compare the old configuration to the new configuration, and only reapply specific configurations you need to keep. This can be done manually, or by creating a script that can apply the changes consistently to multiple server configuration files.

- If you back up and restore an existing configuration for the upgrade, when the server restarts and updates the configuration files the updated configuration may no longer be compatible with the previous version.

- The upgrade may remove temporary folders. Any deployments stored in the **data/content/** directory must be backed up prior to the upgrade, and restored after it completes. Otherwise, the server will fail to start due to the missing content.

- Prior to applying the upgrade, handle any open transactions and delete the **data/tx-object-store/** transaction directory.

- The persistent timer data in **data/timer-service-data** must be checked to determine whether it will still be applicable after the upgrade. Before the upgrade, review the **deployment-*** files in that directory to determine which timers are still in use.

3.2. UPGRADING A ZIP/INSTALLER INSTALLATION

Prerequisites

- Ensure that the base operating system is up to date.

- Back up all configuration files, deployments, and user data.

- Download the ZIP file of the JBoss EAP version you want to upgrade to.

> **IMPORTANT**
>
> For a managed domain, the JBoss EAP domain controller should be upgraded first.
>
> An upgraded JBoss EAP 7 domain controller can still manage other JBoss EAP 7 hosts in a managed domain, as long as the domain controller is running the same or more recent version than the rest of the domain.

1. Move the downloaded ZIP file to the desired location. It is recommended that this is a different location than the existing JBoss EAP installation.

> **NOTE**
>
> If you want to install the upgraded version of JBoss EAP to the same directory as the existing installation, you will need to move the existing installation to a different location before proceeding. This is to prevent modified configuration files, deployments, and upgrades from being lost.

2. Extract the ZIP archive. This installs a clean instance of the new JBoss EAP release.

3. Copy the *EAP_HOME*/**domain**/ and *EAP_HOME*/**standalone**/ directories from the previous installation over the new installation directories.

> **IMPORTANT**
>
> New features in the new release, such as new subsystems, may not be activated if the configuration files are copied from an older JBoss EAP installation. To use these new features, you must compare and update the old configuration files with the configuration files from the new version.

4. Review the changes made to the **bin** directory of the previous installation, and make the equivalent modifications to the new directory.

> **WARNING**
>
> Files in the **bin** directory should not be overwritten by the files from previous versions. Changes should be made manually.

5. Review the remaining modified files from the previous installation, and move these changes into the new installation. These files may include:

   - The **welcome-content** directory.

   - Custom modules in the **modules** directory.

6. **Optional:** If JBoss EAP was previously configured to run as a service, remove the existing service and configure a new service for the upgraded installation.

3.3. UPGRADING AN RPM INSTALLATION

Prerequisites

- Ensure that the base operating system is up to date, and is subscribed and enabled to get updates from the standard Red Hat Enterprise Linux repositories.

- Ensure that you are subscribed to the relevant JBoss EAP repository for the upgrade.

If you are subscribed to a previous minor JBoss EAP repository, you will need to change to the latest minor repository to get the upgrade.

For more information on JBoss EAP repositories, see the information on choosing a JBoss EAP repository and changing JBoss EAP repositories in the *Installation Guide*.

- Back up all configuration files, deployments, and user data.

> **IMPORTANT**
>
> For a managed domain, the JBoss EAP domain controller should be upgraded first.
>
> An upgraded JBoss EAP 7 domain controller can still manage other JBoss EAP 7 hosts in a managed domain, as long as the domain controller is running the same or more recent version than the rest of the domain.

1. After you have subscribed to the relevant JBoss EAP repository and the upgrade is available, run the following command to upgrade your JBoss EAP installation:

   ```
   # yum update
   ```

2. The RPM upgrade process will not replace any of your modified configuration files, and will instead create **.rpmnew** files for the default configuration of the new JBoss EAP version. To activate any new features in the new release, such as new subsystems, you must manually merge each **.rpmnew** file into your existing configuration files.

3.4. UPGRADING A CLUSTER

JBoss EAP does not support the creation of clusters where the nodes are made up of different versions of JBoss EAP servers. All nodes within a cluster must be the same JBoss EAP version.

The upgrade process for a cluster involves creating a new JBoss EAP cluster comprised of nodes running the newer JBoss EAP version, and then migrating all clustered traffic from the previous cluster to the new cluster. After this is completed, the previous JBoss EAP cluster can be shut down and removed.

See the chapter on configuring high availability in the *Configuration Guide* for creating a new cluster, and the section on migrating traffic between clusters to migrate traffic from the old cluster to the new one.

Revised on 2022-02-01 13:04:20 UTC