

Tomcat Private Instances

Overview

Private instances

Configuration

Default configuration

Configure applications

Configure SSL

Test your configuration

Proxies

Manage services as a user

Tomcat security

Additional documentation

Overview

Notes:

- Apache Tomcat® requires cPanel & WHM version 76 or higher.
- We **strongly** recommend that only experienced Tomcat administrators use Tomcat.

Tomcat runs as a per-user private instance. This allows each cPanel account user to manage their own Tomcat services and configuration.

Private instances

Each user's instance of Tomcat runs its applications as the user. The user can stop and start services, and manage their Tomcat configuration to suit their needs. This differs from the EasyApache 3 implementation, where users shared the Tomcat implementation.

The private instance approach increases the security of your system and operates on the user's designated ports.

Configuration

Note:

A cPanel user **must** possess shell access to perform these actions.

When you enable Tomcat for a user account, the system sets up a blank environment for the user. The system creates the environment in the following location, where `user` represents the user's username:

```
/home/user/ea-tomcat85/conf
```

Default configuration

EasyApache 4 makes the following configuration changes from the default Tomcat 8.5 behavior to the `~/ea-tomcat85/conf/server.xml` file:

- Disables the shutdown port by default.
- Sets the `xpoweredBy` attribute of all Connectors to a `false` value.
- Remove the `redirectPort` attribute.
- Adds the `ErrorReportValue` class to all hosts with the `showServerInfo` value set to a `false` value.
- Sets the following host attributes to a `false` value:
 - `autoDeploy`
 - `deployOnStartup`
 - `deployXML`

Configure applications

To use the Tomcat instance, configure the desired applications in the `/home/user/ea-tomcat85/webapps` directory. You can also set up a proxy to point to the app's location. For more information about proxies, read our [Tomcat Proxies](#) documentation.

Note:

If you migrated from EasyApache 3 to EasyApache 4, the system configured each Tomcat user's domains in the user's `~/ea-tomcat85/conf/server.xml` file. It also set up include files with a proxy to duplicate the EasyApache 3 proxy behavior.

To deploy a Tomcat application, edit the `Context` element in the `Host` section of your `~/ea-tomcat85/conf/server.xml` file. Your entry might resemble the following example, where `user` represents the user's username:

```
<Context path="/" docBase="/home/user/ea-tomcat85/webapps/ROOT/">
</Context>
```

Configure SSL

If you want to use SSL in Tomcat, you **must** configure it manually.

To configure SSL, perform the following steps:

1. Request a port for SSL from the system administrator. The system administrator can assign these ports with the `cpuser_port_authority` script.
2. Configure the port to use SSL in the `~/ea-tomcat85/conf/server.xml` file.
 - a. Add the `redirectPort` attribute.
 - b. Add the appropriate SSL connector.

For example, you wanted to configure SSL with HTTP, your entry might resemble the following example, where `10000` represents your assigned HTTP port, and `10003` represents the SSL port:

```
<Connector port="10000" protocol="HTTP/1.1"
connectionTimeout="20000" redirectPort="10003" />
<Connector port="10003"
protocol="org.apache.coyote.http11.Http11Protocol"
SSLEnabled="true" scheme="https" secure="true" sslProtocol="TLS"
keystoreFile="/path/to/keystorefile"
keystorePass="my_keystore_password"/>
```

Note:

We **strongly** recommend that you do **not** store plain text passwords in files. However, if you do, you **must not** loosen the `.conf` file permissions.

For more information, read Tomcat's [SSL/TLS Configuration](#) documentation.

Test your configuration

We provide the `/opt/cpanel/ea-tomcat85/test.jsp` test script so that you can make sure that your Tomcat configuration works.

Warning:

We recommend that you only use this script to test your server's functionality. Setting your applications to deploy on startup is a security risk.

To test your configuration, perform the following steps:

1. Run the following commands, where `user` represents the username:

```
su - user
echo "export PATH=$(dirname $(readlink
/usr/local/cpanel/3rdparty/bin/perl)): $PATH" >> /home/cpuser/.bashrc
source ~/.bashrc
```

2. Edit the `~/ea-tomcat85/conf/server.xml` file and change the following value:

```
deployOnStartup="true"
```

3. Copy the test script:

```
cp /opt/cpanel/ea-tomcat85/test.jsp
/home/cpuser/ea-tomcat85/webapps/ROOT/
```

4. Restart Tomcat:

```
ubic restart ea-tomcat85
```

5. Check your HTTP connector's port:

```
egrep 'Connector port.*HTTP' ~/ea-tomcat85/conf/server.xml
```

6. Load the test script:

Note:

In this example, 10010 represents the port number returned in step 5 and `user.domain` represents the domain name:

```
curl http://user.domain:10010/test.jsp
```

Proxies

You **must** set up Apache proxies manually. You can also configure Tomcat to mimic the EasyApache 3 proxy behavior in a personal instance. For more information, read our [Tomcat Proxies](#) documentation.

Manage services as a user

To manage services in Tomcat, users can use the `cpuser_service` manager and Ubic subsystem. This script adds services and allows users to easily stop and restart their services.

For example, run the following command on the command line to restart your Tomcat service:

```
ubic restart ea-tomcat85
```

Note:

If Uvic does **not** exist in your PATH, you **must** add it to your configuration. For example, you might add the following line to your `.bashrc` file:

```
export PATH=$(dirname $(readlink
/usr/local/cpanel/3rdparty/bin/perl)): $PATH
```

Important:

Jailshell users **cannot** see the status of their previously started Tomcat service. The default jailshell permissions **only** allow users to view their current session's processes. If they attempt to restart an already active service with Uvic, the system will launch a duplicate process.

Tomcat security

If your desired Tomcat applications support it, we **strongly** recommend that you enable Tomcat's [Security Manager](#). This adds extra security, but may break some applications. For more information, read Tomcat's [Security Manager How To](#) documentation.

Additional documentation

Suggested documentation For cPanel users For WHM users For developers

- [Tomcat](#)
- [The cpuser_service_manager script and the Uvic subsystem](#)

Content by label

There is no content with the specified labels



- [Tomcat Private Instances](#)
- [Tomcat](#)
- [Tomcat Proxies](#)
- [EasyApache 4 Release Notes](#)
- [EasyApache 4 Recommendations](#)

- [WHM API 1 Functions - ea4_tomcat85_rem](#)
- [WHM API 1 Functions - ea4_tomcat85_list](#)
- [WHM API 1 Functions - ea4_tomcat85_add](#)
- [WHM API 1 Functions - php_set_vhost_versions](#)
- [WHM API 1 Functions - ea4_metainfo](#)