# JBoss EAP Management

# Goals

**After completing this section, a System Administrator should be able to do the following:**

**• Describe the management options available for JBoss EAP.**

# EAP 8 Administration Options

**EAP 8 is designed in a modular fashion, with multiple subsystems that can be customized to support Java EE application requirements, such as database connectivity, batch processing, and integration tools such as message queues. The subsystem configuration is maintained in the file standalone.xml (for standalone mode) and domain.xml (for a managed domain).**

**These configuration files can be customized using three different approaches:**

1. **Admin Console: This web application allows a web administrator to systems manage, through the use of a browser, most of the capabilities of their stand-alone or managed domain implementations.**
2. **Management CLI (Command Line Interface) - The CLI, through a terminal window, provides an administration template for viewing and modifying attributes, as well as performing operations, including batch operations, on a stand-alone server or managed domain. The CLI includes simple features such as contextual auto completion, built-in documentation of server configuration attributes, and command execution history.**

3. **Edit XML Configuration Files Manually – Settings for a stand-alone server or managed domain are persisted in XML configuration files that can be modified directly.**

## use

**No matter what technique is used to modify a configuration value, all changes are synchronized with the XML configuration files. If, for example, a value is changed through the management console, the underlying XML file is changed immediately, and the CLI will detect the change instantly. However, the management console may not get the latest updates made by the CLI due to web browser caching. The admin console displays data stored in the browser and may display outdated configuration data. A page refresh is needed to resolve the issue.**

**Warning**

**Do not edit the XML configuration files manually if EAP is running. Changes made to the XML file will most likely be lost. First, stop any EAP controllers or servers, or use the management console or CLI.**

**To access the EAP 8 management console, launch your web browser and navigate to http:// localhost:9990**

**By default, the EAP 8 administration console is secured, and you must provide the username and password you entered during the installation process (jbossadm/JBoss@RedHat123).**

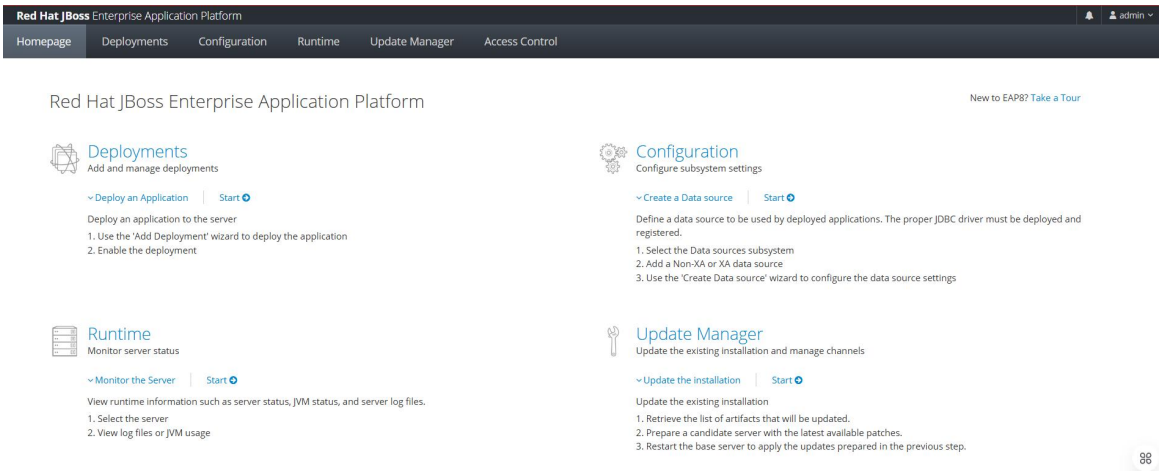


***Figure 1.19:***
***EAP 8 Management Console***

**To access the JBoss EAP CLI, start a terminal, navigate to the JBOSS_HOME/bin folder, and run the jboss-cli.sh script. For example:**

```
$ ./jboss-cli.sh --connect
[standalone@localhost:9990 /] :product-info {

    "outcome" =>
    "success", "result" =>
    [{"summary" => {
        "host-name" => "workstation.lab.example.com", "instance-
        identifier" => "6b407cda-46ea-44e9-b9d5-23236000f2a8", "product-
        name" => "JBoss EAP", "product-version" => "8.0.0.GA",
        "product-community-identifier" => "Product",
        "product-home" => "/opt/jboss-eap-8.0",
        "standalone-or- domain-identifier" =>
        "STANDALONE_SERVER",
        "host-operating-system" => "Red Hat Enterprise Linux Server 7.2 (Maipo)",

        ...
    }}]
    }
```

**Enter 'quit' or 'q' to exit the CLI.**

**If you invoke the CLI without any arguments, it will run in 'disconnected' mode. To connect to the server, use the --connect command option.**

**Another option to connect to the EAP 8 standalone server instance, or to a domain controller, is to use the connect <IPAddress> CLI command.**

**For an EAP instance running locally, the JBoss CLI tool will not prompt for credentials, by default, but for EAP instances running on a different host, the admin user credentials will be prompted during startup. Login. It is also possible to disable automatic authentication for local access, for security reasons. This topic will be discussed later.**

**Finally, the XML configuration file can be edited with a text editor. For the standalone server, the file is available at JBOSS_HOME/standalone/ configuration/standalone.xml.**

```
<server xmlns="urn:jboss:domain:4.1">
    <extensions>
        <extension module="org.jboss.as.clustering.infinispan"/>
        ...
    </extensions>
    <management>
        ...
    </management>
    <profile>
        <subsystem xmlns="urn:jboss:domain:logging:3.0">
     ...
```

**The file is made up of multiple extension tags that represent all the modules needed by EAP to start a subsystem. Also, multiple subsystem tags are declared and grouped together in the profile tag, which represents each customization that a subsystem needs.**

**Similarly, the managed domain also has the same set of configurations defined in JBOSS_HOME/domain/configuration/domain.xml. The structure and differences will be discussed later in this course.**

# Creation of administrative users

**The EAP installer creates an administrative user during the installation process.**

**If additional administrative users are required, or if the installation was NOT performed using the EAP installer, new users can be created using the add user.sh script present in the JBOSS_HOME/bin folder.**

**The script can also be used to manage accounts for testing applications, using the security features of Jakarta EE (Java Authentication and Authorization System, JAAS), if the applications have not been configured to use external identity stores, such as a database. data or an LDAP server.**

**There are two different types of users that can be added:**

- **The Administration user type is responsible for accessing the tools administrative from EAP. The credentials will be stored in the JBOSS_HOME/standalone/ configuration/mgmt-users.properties file, with an encrypted password.**
- **Java EE applications will use the Application user type via JAAS, and similar to the admin user option, the content will be stored in JBOSS_HOME/standalone/configuration/app- users.properties.**

**There is no need to restart an EAP server instance (or managed domain) when changing user files. EAP will automatically detect changes to these files.**

**They are simple text files, and the passwords stored in them are encrypted (technically, the correct term is *hashed).* Lines beginning with hash (#) are comments.**

**Later in this book, it will also be shown that host controllers in a managed domain may require special users to connect to the domain controller. These users can also be created using the add-user.sh script.**

## use

**By default, all management operations are available to all administration users, but EAP also supports the concept of Role-Based Authentication Control (RBAC) which requires customization to activate. RBAC allows you to configure users who are not granted full administrative privileges, but only a subset of them, and**
**only for a subset of server instances in a managed domain.**