Configuring Business Central settings and properties
Abstract

This document describes how to customize and manage the various features of Business Central in Red Hat Process Automation Manager 7.2.
# Table of Contents

PREFACE ....................................................................................................................... 4

CHAPTER 1. USER AND GROUP MANAGEMENT ................................................................. 5
  1.1. CREATING USERS .................................................................................................. 5
  1.2. EDITING USERS ..................................................................................................... 5
  1.3. CREATING GROUPS ............................................................................................... 6
  1.4. EDITING GROUPS .................................................................................................. 7

CHAPTER 2. SECURITY MANAGEMENT ........................................................................... 8
  2.1. SECURITY MANAGEMENT PROVIDERS .................................................................. 8
    2.1.1. Configuring the Red Hat JBoss EAP security management provider based on property files 8
    2.1.2. Configuring the Red Hat JBoss EAP security management provider based on property files and CLI mode 9
  2.2. PERMISSIONS AND SETTINGS ............................................................................... 10
    2.2.1. Changing permissions for groups and roles in Business Central ......................... 11
    2.2.2. Changing the Business Central home page ......................................................... 12
    2.2.3. Setting priorities ............................................................................................. 12

CHAPTER 3. MANAGING ARTIFACTS .............................................................................. 13
  3.1. VIEWING AN ARTIFACT ......................................................................................... 13
  3.2. DOWNLOADING AN ARTIFACT .............................................................................. 13
  3.3. UPLOADING AN ARTIFACT ................................................................................... 13

CHAPTER 4. MANAGING DATA SOURCES ..................................................................... 15
  4.1. ADDING A DATABASE DRIVER .............................................................................. 15
  4.2. DELETING A DATABASE DRIVER ......................................................................... 15
  4.3. ADDING A DATA SOURCE ..................................................................................... 15
  4.4. EDITING A DATA SOURCE .................................................................................... 16
  4.5. DELETING A DATA SOURCE .................................................................................. 16

CHAPTER 5. DATA SETS AUTHORING .......................................................................... 17
  5.1. ADDING DATA SETS .............................................................................................. 17
  5.2. EDITING DATA SETS ............................................................................................ 18
  5.3. DATA REFRESH ..................................................................................................... 18
  5.4. CACHING ............................................................................................................... 18
    Client cache ............................................................................................................. 19
    Back end cache ....................................................................................................... 19

CHAPTER 6. CUSTOMIZING PROJECT PREFERENCES ...................................................... 20

CHAPTER 7. CUSTOMIZING ARTIFACT REPOSITORY PROPERTIES .............................. 22

CHAPTER 8. CUSTOMIZING LANGUAGE SETTINGS ....................................................... 23

CHAPTER 9. CUSTOMIZING PROCESS ADMINISTRATION .............................................. 24

CHAPTER 10. CUSTOMIZING THE PROCESS DESIGNER ................................................ 25

CHAPTER 11. SSH KEYS ................................................................................................. 26
  11.1. DEFAULT SSH KEYSTORE .................................................................................. 26
  11.2. CUSTOM SSH KEYSTORE .................................................................................. 26
  11.3. CREATING AN SSH KEY .................................................................................... 27
  11.4. REGISTERING YOUR SSH PUBLIC KEY WITH THE SSH KEYSTORE .................. 27
  11.5. DELETING AN SSH KEY ..................................................................................... 28
As an administrator, you can customize Business Central using the **Admin Settings**. You can use the **Admin Settings** to customize the following items:

- **Roles**: Set the home page, priority, and permissions of a role.
- **Groups**: Set the home page, priority, and permissions of a group as well as create and delete groups.
- **Users**: Create and delete users as well as add a group or role to a user and view its permissions.
- **Artifacts**: View M2 repository artifacts, upload artifacts, view, and download JAR files.
- **Data Source**: Add, update, or delete data sources and database drivers.
- **Data Sets**: Create, modify, or delete data sets.
- **Projects**: View and edit project preferences such as file export properties, space properties, default values, and advanced GAV properties.
- **Artifact Repository**: Manage artifact repository properties.
- **Languages**: Set the Business Central language.
- **Process Designer**: Set diagram editor properties.

**Prerequisites**

- Installed Red Hat JBoss Enterprise Application Platform 7.1.0. For more information, see [Red Hat JBoss EAP 7.1.0 Installation Guide](#).
- Installed Red Hat Process Automation Manager. For more information, see [Installing and configuring Red Hat Process Automation Manager on Red Hat JBoss EAP](#).
- Red Hat Process Automation Manager is running and you can log in to Business Central with the **admin** role.
CHAPTER 1. USER AND GROUP MANAGEMENT

Business Central defines three types of entities for security management – users, groups, and roles. Permissions can be assigned to both roles and groups. Business Central provides the following roles:

- process-admin
- manager
- admin
- analyst
- developer
- user

**NOTE**
If a role’s identifier is present in the application’s Role Registry only then it is considered a role otherwise it’s a group.

You can use Business Central to create and manage as many users and groups as you require. A user must be assigned at least one user-specific role to login to Business Central. User privileges depends on permissions from the groups and roles the user is a member of. Note that role or group priority is taken into account in case a user has several roles or groups assigned to it.

1.1. CREATING USERS

You can create as many Business Central users as you require. User privileges and settings are controlled by the roles assigned to a user and the groups that a user belongs to.

**Procedure**
1. Log in to Business Central and click **Admin → Users**.
2. Click **New user**, enter a user name, and then click **Next**.
3. If desired, click the **Groups** tab, click **Add to groups**, and then select the groups that you want this user to belong to. Then click **Add to selected groups**.
4. Click the **Roles** tab, click **Add roles**, and then select the roles that you want to give this user. Then click **Add to selected roles**.
5. Click **Create**.
6. Click **Yes** to set a password for the user and click **Change**.

**NOTE**
The user must have at least one role to access Business Central.

1.2. EDITING USERS
You can edit the users of Business Central according to your needs. From the Users option in Settings, you can change the group and role of a user. All user permissions are based on the group and role permissions of the user. You can view the user permissions from the Permissions tab.

Procedure

1. Log in to Business Central.
2. Select Admin → Users.
3. From All users, click the user you want to edit. All user details are displayed in the right pane.
4. Click Edit.
   - Complete the following steps to add groups to users:
     a. From Groups, click Add to groups. The Group selection for user window opens.
     b. Select or deselect the groups you want the user to be a part of.
     c. Click Add to selected groups.
   - Complete the following steps to add roles to users:
     a. From Roles tab, click Add roles. The Role selection for user window opens.
     b. Select or deselect the roles you want to assign to the user.
     c. Click Add to selected roles.
   - Complete the following step to view user permissions:
     a. Click the Permissions tab and expand the attributes to view user permissions.
   - Complete the following steps to change the user’s password,
     a. Click Change Password. The Change password for user window opens.
     b. Enter and confirm the new password and click Change.
   - Complete the following steps to delete the user,
     a. Click Delete and then click Yes to remove the user.
5. Click Save to apply the changes.

1.3. CREATING GROUPS

In Business Central, groups allow you to control permissions for a collection of users. You can create as many groups as you want but a group must have at least one user.

Procedure

1. Log in to Business Central.
2. Select Admin → Groups.
3. Click **New group**, enter a group name, and then click **Next**.

4. Select the users that you want to belong to this group, and then click **Add selected users**. The newly created group is listed under **All groups**.

### 1.4. EDITING GROUPS

You can edit a group’s attributes such as home page, priority, and permissions according to your requirements. From the **Groups** option in **Settings**, you can modify or delete a group.

**Procedure**

1. Log in to Business Central.

2. Select **Admin → Groups**.

3. From **All groups**, click the group you want to edit. All user details are displayed in the right pane.

4. Select the home page from the **Home Page** list.

5. Select the priority from the **Priority** list.

6. In the **Permissions** section, expand the resource attribute and change its permission.

   **NOTE**

   You can add exceptions to **Pages**, **Editor**, **Spaces**, and **Projects** permissions.

7. Click **Save** to apply the changes.

   **NOTE**

   Use **Delete** to remove a group from Business Central.
CHAPTER 2. SECURITY MANAGEMENT

Security management is the process of managing users, groups, and permissions. You can control access to Business Central resources and features from the Business Central Security management page.

Business Central defines three types of entities for security management: users, groups, and roles. You can assign permissions to both roles and groups. A user inherits permissions from the groups and roles that the user is a member of.

2.1. SECURITY MANAGEMENT PROVIDERS

In the context of security management, a realm restricts access to different application resources. Realms contain information about users, groups, roles, and permissions. A concrete user and group management service implementation for a specific realm is called a security management provider.

If the built-in security management providers do not meet the requirements of your application security realm, then you can build and register your own security management provider.

NOTE

If the security management provider is not installed, the user interface for managing the security realm is not available. After you install and configure a security management provider, the user and group management features are automatically enabled in the security management user interface.

Business Central includes the Red Hat JBoss EAP security management provider which supports realm types based on the contents of the application-users.properties or application-roles.properties property file.

2.1.1. Configuring the Red Hat JBoss EAP security management provider based on property files

You can build and register your own Red Hat JBoss EAP security management provider. To use the Red Hat JBoss EAP security management provider based on property files, complete the steps in this procedure.

Prerequisites

- Red Hat JBoss EAP is installed.

Procedure

1. To use an existing users or roles property file from the Red Hat JBoss EAP instance, include the following system properties in the EAP_HOME/standalone/configuration/application-users.properties and EAP_HOME/standalone/configuration/application-roles.properties files, as shown in the following example:

   `<property name="org.uberfire.ext.security.management.wildfly.properties.realm" value="ApplicationRealm"/>
   <property name="org.uberfire.ext.security.management.wildfly.properties.users-file-path"`
The following table provides a description and default value for these properties:

### Table 2.1. Red Hat JBoss EAP security management provider based on property files

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>org.uberfire.ext.security.management.wildfly.properties.realm</td>
<td>The name of the realm. This property is not mandatory.</td>
<td>ApplicationRealm</td>
</tr>
<tr>
<td>org.uberfire.ext.security.management.wildfly.properties.users-file-path</td>
<td>The absolute file path for the users property file. This property is mandatory.</td>
<td>/standalone/configuration/application-users.properties</td>
</tr>
<tr>
<td>org.uberfire.ext.security.management.wildfly.properties.groups-file-path</td>
<td>The absolute file path for the groups property file. This property is mandatory.</td>
<td>/standalone/configuration/application-roles.properties</td>
</tr>
</tbody>
</table>

2. Create the `security-management.properties` file in the root directory of your application. For example, create the following file:

```
src/main/resources/security-management.properties
```

3. Enter the following system property and security provider name as a value in the `security-management.properties` file:

```
<property name="org.uberfire.ext.security.management.api.userManagementServices" value="WildflyUserManagementService"/>
```

### 2.1.2. Configuring the Red Hat JBoss EAP security management provider based on property files and CLI mode

To use the Red Hat JBoss EAP security management provider based on property files and CLI mode, complete the steps in this procedure.

**Prerequisites**

- Red Hat JBoss EAP is installed.

**Procedure**

1. To use an existing users or roles property file from the Red Hat JBoss EAP instance, include the following system properties in the `EAP_HOME/standalone/configuration/application-users.properties` and `EAP_HOME/standalone/configuration/application-roles.properties` files, as shown in the following example:

```
<property name="org.uberfire.ext.security.management.wildfly.cli.host" value="localhost"/>
<property name="org.uberfire.ext.security.management.wildfly.cli.port" value="9990"/>
```
The following table provides a description and default value for these properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>org.uberfire.ext.security.management.wildfly.cli.host</code></td>
<td>The native administration interface host.</td>
<td>localhost</td>
</tr>
<tr>
<td><code>org.uberfire.ext.security.management.wildfly.cli.port</code></td>
<td>The native administration interface port.</td>
<td>9990</td>
</tr>
<tr>
<td><code>org.uberfire.ext.security.management.wildfly.cli.user</code></td>
<td>The native administration interface username.</td>
<td>NA</td>
</tr>
<tr>
<td><code>org.uberfire.ext.security.management.wildfly.cli.password</code></td>
<td>The native administration interface user’s password.</td>
<td>NA</td>
</tr>
<tr>
<td><code>org.uberfire.ext.security.management.wildfly.cli.realm</code></td>
<td>The realm used by the application’s security context.</td>
<td>ApplicationRealm</td>
</tr>
</tbody>
</table>

2. Create the `security-management.properties` file in the root directory of your application. For example, create the following file:

```xml
<property name="org.uberfire.ext.security.management.wildfly.cli.user" value="<USERNAME>"/
<property name="org.uberfire.ext.security.management.wildfly.cli.password" value="<USER_PWD>"/>
<property name="org.uberfire.ext.security.management.wildfly.cli.realm" value="ApplicationRealm"/>
```

3. Enter the following system property and security provider name as a value in the `security-management.properties` file:

```xml
<property name="org.uberfire.ext.security.management.api.userManagementServices" value="WildflyCLIUserManagementService"/>
```

## 2.2. PERMISSIONS AND SETTINGS

A permission is an authorization granted to a user to perform actions related to a specific resource within the application. For example, a user can have following permissions:

- View a page.
- Save the project.
- View a repository.
Delete a dashboard.

You can grant or deny a permission and a permission can be global or resource specific. You can use permissions to protect access to resources and customize features within the application.

2.2.1. Changing permissions for groups and roles in Business Central

In Business Central, you cannot change permissions for an individual user. However, you can change permissions for groups and roles. The changed permissions apply to users with the role or that belong to a group that you changed.

**NOTE**

Any changes that you make to roles or groups affect all of the users associated with that role or group.

**Prerequisites**

- You are logged in to Business Central with the **admin** user role.

**Procedure**

1. To access the **Security management** page in Business Central, select the **Admin** icon in the top-right corner of the screen.

2. Click **Roles**, **Groups**, or **Users** on the Business Central **Settings** page. The **Security management** page opens on the tab for the icon that you clicked.

3. From the list, click the role or group you want to edit. All details are displayed in the right panel.

4. Set the **Home Page** or **Priority** under the **Settings** section.

5. Set the Business Central, page, editor, space, and project permissions under the **Permissions** section.

6. Click the arrow next to a resource type to expand the resource type whose permissions you want to change.
7. Optional: To add an exception for a resource type, click Add Exception and then set the permissions as required.

**NOTE**
You cannot add an exception to the Business Central resource type.

8. Click Save.

### 2.2.2. Changing the Business Central home page

The home page is the page that appears after you log in to Business Central. By default, the home page is set to Home. You can specify a different home page for each role and group.

**Procedure**

1. In Business Central, select the Admin icon in the top-right corner of the screen and select Roles or Groups.
2. Select a role or group.
3. Select a page from the Home Page list.
4. Click Save.

**NOTE**
The role or group must have read access to a page before you can make it the home page.

### 2.2.3. Setting priorities

A user can have multiple roles and belong to multiple groups. The Priority setting determines the order of precedence of a role or group.

**Prerequisites**

- You are logged in to Business Central with the admin user role.

**Procedure**

1. In Business Central, select the Admin icon in the top-right corner of the screen and select Roles or Groups.
2. Select a role or group.
3. Select a priority from the Priority menu, and then click Save.

**NOTE**
If a user has a role or belongs to a group that has conflicting settings, the settings of the role or group with the highest priority applies.
CHAPTER 3. MANAGING ARTIFACTS

You can manage artifacts from the Artifacts page in Business Central. The artifact repository is a local Maven repository and there is only one Maven repository for each installation. Business Central recommends using Maven repository solutions like Sonatype Nexus™, Apache Archiva™, or JFrog Artifactory™.

The Artifacts page lists all the artifacts in the Maven repository. You can also upload a new artifact to the Maven repository using the Upload button.

NOTE

Only *.jar, *.kjar, or pom.xml files can be uploaded to the Artifacts repository.

3.1. VIEWING AN ARTIFACT

You can view all the content of the local maven repository from the Artifacts page.

Procedure

1. Log in to Business Central.
2. Select Admin → Artifacts.
3. Click Open to view the artifact details.
4. Click Ok to go back to the Artifacts page.

3.2. DOWNLOADING AN ARTIFACT

You can download and save an artifact from Business Central’s repository to a project’s local storage.

Procedure

1. Log in to Business Central.
2. Select Admin → Artifacts.
3. Click Download.
4. Browse to the directory where you want to save the artifact and click Save.

3.3. UPLOADING AN ARTIFACT

You can upload an artifact from the local storage to a project in Business Central.

Procedure

1. Log in to Business Central.
2. Select Admin → Artifacts.
3. Click Upload.
4. Click Choose File and browse to the directory from where you want to upload the artifact.

5. Click Upload.

NOTE

In case you are using a non-maven artifact, first deploy the artifact to the maven repository using mvn deploy command and then refresh the artifact list in Business Central.
CHAPTER 4. MANAGING DATA SOURCES

Business Central provides data source management which gives you the ability of defining data sources for accessing a database. These data sources are then used by other Business Central components such as the data sets. A database driver, on the other hand, is used for enabling communication between a data source and the targeted database.

From the Data Source Authoring page you can add data sources and database drivers to Business Central.

NOTE

Business Central provides a default data source that can be used but can neither be edited nor deleted.

4.1. ADDING A DATABASE DRIVER

You can add a new database driver to Business Central according to your requirements.

Procedure

1. Log in to Business Central.
2. Select Admin → Data Sources. The Data Sources Authoring page opens.
3. In the DataSource Explorer pane, click Add Driver. The New driver window opens.
4. In the New driver window, enter the Name, Driver Class Name, Group Id, Artifact Id, and the Version of the database driver.
5. Click Finish to add the driver to Business Central.

4.2. DELETING A DATABASE DRIVER

You can remove database drivers from the Data Source Definition pane of Business Central.

Procedure

1. Log in to Business Central.
2. Select Admin → Data Sources. The Data Sources Authoring page opens.
3. In the DataSource Explorer pane, select the driver you want to delete. The Data Source Definition pane lists the driver details.
4. Click Remove.
5. Click Delete to delete the driver.

4.3. ADDING A DATA SOURCE

You can add a new data source to Business Central from the Data Sources Authoring page.
Procedure

1. Log in to Business Central.

2. Select Admin → Data Sources. The Data Sources Authoring page opens.

3. In the DataSource Explorer pane, click Add DataSource. The New data source window opens.

4. In the New data source window, enter the data source Name, database Connection URL, User and Password, and Driver.

5. Click Test Connection to verify the connection to the database.

6. Click Finish to add the data source to Business Central.

4.4. EDITING A DATA SOURCE

You can edit the properties of a data source and also test its connection to the database in Business Central.

Procedure

1. Log in to Business Central.

2. Select Admin → Data Sources. The Data Sources Authoring page opens.

3. In the DataSource Explorer pane, click the data source you want to edit. The Data Source Definition pane lists the data source details.

4. In the Data Source Definition pane, make the necessary changes to the Name, Connection URL, User, Password, and the Driver fields.

5. Click Test Connection to verify the connection to the database.

6. Click Update.

7. Click Save to confirm the changes to the data source.

4.5. DELETING A DATA SOURCE

You can delete an existing data source from the DataSource Explorer pane in Business Central.

Procedure

1. Log in to Business Central.

2. Select Admin → Data Sources. The Data Sources Authoring page opens.

3. In the DataSource Explorer pane, click the data source you want to delete. The Data Source Definition pane lists the data source details.

4. Click Remove.

5. Click Delete to confirm the deletion of the data source.
CHAPTER 5. DATA SETS AUTHORING

A data set is a collection of related sets of information. It can be stored in many ways, such as in a database, in a Microsoft Excel file, in memory, and so on. A data set definition instructs Business Central how to access, read, and parse a data set. Business Central does not store data. It enables you to define access to a data set regardless of where the data is stored.

For example, if data is stored in a database, a valid data set could contain the entire database or a subset of the database as a result of an SQL query. In both cases, the data is used as input for the reporting components of Business Central which then displays the information.

To access a data set, you must create and register a data set definition, which will define where the data set is stored, how it can be accessed, read, and parsed, and what columns it contains.

NOTE
The Data Sets page is visible only to users with admin role.

5.1. ADDING DATA SETS

You can create a new data set to fetch data from an external data source and use that data for the reporting components.

Procedure

1. Log in to Business Central and click the gear icon.
2. Click Data Sets → Data Set Explorer → New Data Set.
3. Select one of the following the provider types:
   - **Bean**: Use to generate a data set from a Java class
   - **CSV**: Use to generate a data set from a remote or local CSV file
   - **SQL**: Use to generate a data set from an ANSI-SQL compliant database
   - **Elastic Search**: Use to generate a data set from Elastic Search nodes
   - **Execution Server**: Use to generate a data set using the custom query feature of an Execution Server

   NOTE
   KIE Server must be configured with this option.

4. Complete the Data Set Creation Wizard and click **Test**.

   NOTE
   Depending on the provider you chose, the configuration steps will differ.

5. Click Save.
5.2. EDITING DATA SETS

You can edit existing data sets to ensure that the data fetched to the reporting components is up-to-date.

Procedure

1. Log in to Business Central, click the gear icon, and then click **Data Sets**.

2. In the **Data Set Explorer** pane, search for the data set you want to edit and click **Edit**.

3. In the **Data Set Editor** pane, use the appropriate tab to edit the data as required. The tabs will differ based on the data set provider type you chose.
   For example, the following changes are applicable for editing a **CSV** data provider.
   - **CSV Configuration**: Enables you to change the name of the data set definition, the source file, the separator, and other properties.
   - **Preview**: Enables you to preview the data. After you click **Test** in the **CSV Configuration** tab, the system executes the data set lookup call and if the data is available, a preview appears. Note that the **Preview** tab has two sub-tabs:
     - **Data columns**: Enables you to specify what columns are part of your data set definition.
     - **Filter**: Enables you to add a new filter.
   - **Advanced**: Enables you to manage:
     - **Caching**: See Section 5.4, “Caching” for more information.
     - **Cache life-cycle**: See Section 5.3, “Data refresh” for more information.

4. After making the required changes, click **Validate**.

5. Click **Save**.

5.3. DATA REFRESH

The data refresh feature enables you to specify an interval of time after which a data set (or data) is refreshed. The **Refresh on stale data** feature refreshes the cached data when the back-end data changes.

5.4. CACHING

Business Central provides caching mechanisms for storing data sets and performing data operations using in-memory data. Caching data reduces network traffic, remote system payload, and processing time. To avoid performance issues, configure the cache settings in Business Central.

For any data lookup call that result in a data set, the caching technique will determine where the data lookup call is executed and where the resulting data set is stored. An example of a data lookup call would be all the mortgage applications whose locale parameter is set as "Urban".

Business Central data set functionality provides two cache levels:

- **Client level**
Client cache
When the cache is turned on, the data set is cached in a web browser during the lookup operation and further lookup operations do not perform requests to the back end. Data set operations like grouping, aggregations, filtering, and sorting are processed in the web browser. Enable client caching only if the data set size is small, for example, for data sets with less than 10 mb size. For large data sets, browser issues such as slow performance or intermittent freezing can occur. Client caching reduces the number of back end requests including requests to the storage system.

Back end cache
When the cache is enabled, the process engine caches the data set. This reduces the number of requests to the remote storage system. All data set operations are performed in the process engine using in-memory data. Enable back-end caching only if the data set size is not updated frequently and it can be stored and processed in memory. Using back-end caching is also useful in cases with low latency connectivity issues with the remote storage.

NOTE
Back end cache settings are not always visible in the Advanced tab of the Data Set Editor because Java and CSV data providers rely on back end caching (data set must be in the memory) in order to resolve any data lookup operation using the in-memory process engine.
CHAPTER 6. CUSTOMIZING PROJECT PREFERENCES

A project stores assets and is part of a space. A space can hold multiple projects.

For example, an organization has many departments, such as HR, Payroll, Engineering, R&D, and so on. Each department maps to a space. And every department can have their own projects.

You can create a new Project from scratch or clone projects from an existing Git repository.

Procedure

1. Log in to Business Central.

2. Select Admin → Projects. The Projects page opens.

3. Project Preferences has the following four options,

   - **File exporting** option. It has the following properties,

     Table 6.1. File exporting properties

     | Field             | Description                                                                 |
     |-------------------|-----------------------------------------------------------------------------|
     | PDF orientation   | Determines whether the PDF orientation is portrait or landscape.            |
     | PDF units         | Determines whether the PDF unit is PT, MM, CN or IN.                        |
     | PDF page format   | Determines whether the PDF page format is A[0–10], B[0–10], or C[0–10].    |

   - **Spaces** option. It has the following properties,

     Table 6.2. Spaces properties

     | Field               | Description                                                                 |
     |---------------------|-----------------------------------------------------------------------------|
     | Name                | The default name of the space that is created automatically if none exists. |
     | Owner               | The default owner of the space that is created automatically if none exists.|
     | Group ID            | The default group id of the space that is created automatically if none exists.|
     | Alias (in singular) | Determines the customized alias (singular) of the space.                     |
     | Alias (in plural)   | Determines the customized alias (plural) of the space.                       |
- **Default values** option. It has following properties,

Table 6.3. Default values properties

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>The default version number of a project when creating projects using the Quick setup option.</td>
</tr>
<tr>
<td>Description</td>
<td>The default description of a project when creating projects using the Quick setup option.</td>
</tr>
<tr>
<td>Branch</td>
<td>The default branch to be used when using a Git repository.</td>
</tr>
</tbody>
</table>

- **Default values** option. It has following properties,

Table 6.4. Advanced GAV preference properties

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable GAV conflict check?</td>
<td>Determines whether to enable or disable the GAV conflict check. Disabling this feature will allow projects to have the same GAV(Group ID, Artifact, Version).</td>
</tr>
<tr>
<td>Allow child GAV edition?</td>
<td>Determines whether to allow child/sub-projects to have GAV edition.</td>
</tr>
</tbody>
</table>

4. Click **Save**.
CHAPTER 7. CUSTOMIZING ARTIFACT REPOSITORY PROPERTIES

In some cases, projects need to resolve external dependencies to build domain model Jars. A repository contains the needed artifacts which has the following features:

- It’s a Maven repository.
- All snapshots are time stamped.
- Mostly stored in the local hard drive

By default, the artifact repository is in $WORKING_DIRECTORY/repositories/kie.

Procedure

1. Log in to Business Central.
3. Make selections and enter information in the Properties section.
4. Click Save.
CHAPTER 8. CUSTOMIZING LANGUAGE SETTINGS

You can change the language settings of Business Central from the Settings page. Business Central supports seven languages - English, German, Spanish, French, Japanese, Portuguese, and Chinese(Simplified). The default language is English.

Procedure

1. Log in to Business Central.

2. Select Admin → Languages. The Language Selector window opens.

3. Select the desired language from the Language list.

4. Click Ok.
CHAPTER 9. CUSTOMIZING PROCESS ADMINISTRATION

You can customize the default pagination option in Business Central by editing the Default items per page property on the Process Administration page.

Procedure

1. Log in to Business Central.

2. Select Admin → Process Administration.

3. From the Properties section, update the Default items per page property and click Save.

NOTE

You can specify 10, 20, 50 or 100 items to display on each page.
CHAPTER 10. CUSTOMIZING THE PROCESS DESIGNER

You can customize the process designer in Business Central by editing the properties of the diagram editor from the Settings page.

Procedure

1. Log in to Business Central.

2. Go to Admin → Process Designer.

3. In the Properties section, update any of the following properties and click Save:

   - Select the Auto hide category panel check box to automatically hide a category toolbar panel.

   - In the Drawing area width field, enter an integer value between 2800 and 5600 to set the width of the drawing area.

   - In the Drawing area height field, enter an integer value between 1400 and 2800 to set the height of the drawing area.

   - Select the Enable HiDPI check box if you are using a high resolution display and are seeing blurry text and objects. This option is disabled by default.
CHAPTER 11. SSH KEYS

Business Central provides an SSH keystore service to enable user SSH authentication. It provides a configurable default SSH keystore, extensible APIs (for custom implementations), and support for multiple SSH public keys formats.

You can access the SSH Keys option from the Admin page to register your SSH public keys.

11.1. DEFAULT SSH KEYSTORE

The default SSH keystore included with Business Central provides a file-based storage mechanism to store a user’s public keys. By default, Business Central uses the *.security folder as the root directory. However, it is possible to use a custom storage path by setting the value of the appformer.ssh.keys.storage.folder system property point to a different folder.

The SSH public keys are stored in the {securityFolderPath}/pkeys/{userName} folder structure.

Each SSH public key consists of the following files, located in the storage folder:

- `{keyId}.pub`: This file contains the SSH public key content. As the file name determines the logic key ID on the system, ensure that the file name is not modified during runtime. For example:

  ssh-rsa
  AAAAB3NzaC1yc2EAAAADAQABAAABAADmak4Wu23RZ6XmN94bOsqecZxuTa4RRhhQmHmTZjMB7HM5/90u/B/gb/GhsPEu1nAXL0nP56tT/MPQ8vRm2C2W9A7CzN5+z5yyL3W01YZy3kzslk77CjULjhrfcQSL3b2sPG5jv5E5/nyC/swSytcwT/PE7aXTS9H6cHKUdYPzl94SHoBxWRIk7Pi9d+eLB+hmdzvbVa1ezuSa8yu2kh6Nxe0i5iRj2rscetDtpOimC1jMoC6ZDrBvZSxL9F6fTmwfDnmmTiJveBtv9nAbnAvlWliS0VOkdx1s3GxXeZYAcKbcsK9sJzusptk5dxGsG2Z8vlnaqiN60aOQ7b7tcumcZYYwU0G9gRX8sGsVrw39gsDIGYP2A4bRr7ecHnlNg1b0HCchA5+QCDk4Hzb1UmHmPA26g9c3Wgm2qedvQdVJxu3mlwYoqL40aXPs6980PvFJUjpiVSznF50dpNwsmzJZeF1HdTXTgZD1Nh54ogZf7czyUNFlNkE69yJDbTHjpQd0cKUQnu9tVxmlBzhX3iyF4VcsMeADcf28wlA3n4LZnC/GwonYlq5+G93zjF0kPlhme8c2XuPuCX795isxyJ8SB/AlwPJAheTm0y0s0I1l4eWqxsDxkBQgN+tvU0czrVMssHJEJb4o0FL7IHHOW56/nMd9w== userName

- `{keyId}.pub.meta`: This file contains the key metadata in JSON format. A new metadata file is dynamically generated if a key has no metadata. For example:

  ```json
  {
  "name":"Key",
  "creationDate":"Oct 10, 2018 10:10:50 PM",
  "lastTimeUsed":"Oct 11, 2018 12:11:23 PM"
  }
  ```

11.2. CUSTOM SSH KEYSTORE

You can extend and customize the default SSH keystore according to your requirements. Use the appformer.ssh.keystore system property to specify the Java class name of the SSH service to use. If this property is not defined or it contains an incorrect value then the default SSH keystore is loaded.
NOTE
To create a custom implementation of the SSH keystore, your java class must implement the org.uberfire.ssh.service.backend.keystore.SSHKeyStore class defined in the uberfire-ssh-api module.

11.3. CREATING AN SSH KEY

Before you can add or register SSH keys to Business Central, you must generate an SSH key on your system.

Procedure

1. Open a terminal on your system.
2. Run the ssh-keygen command to create the SSH key as shown in the following example, where <user_login> is your user name.

   ssh-keygen -t rsa -b 4096 -C "<user_login>"

   NOTE
   The SSH key formats supported by Business Central keystore are ssh-rsa, ssh-dss, ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, and ecdsa-sha2-nistp521.

3. When prompted, press the Enter key and accept the default key file location as shown in the following example, where <user_login> is your user name.

   Enter a file in which to save the key (/home/<user_login>/.ssh/id_rsa): [Press enter]

4. At the command prompt, enter and confirm the passphrase.

   Enter passphrase (empty for no passphrase): [Type a passphrase]
   Enter same passphrase again: [Type passphrase again]

5. Start the ssh-agent.

   eval "$(ssh-agent -s)"
   Agent pid <any-number-here>

6. Add the new SSH private key to the ssh-agent. If you have used a different key name, replace id_rsa in code.

   ssh-add ~/.ssh/id_rsa

11.4. REGISTERING YOUR SSH PUBLIC KEY WITH THE SSH KEYSTORE

You must register your newly created SSH public key with the Business Central keystore.

Procedure

1. Open a terminal on your system.
2. Run the `cat` command as shown in the following example, where `id_rsa` is your key name.

```
cat ~/.ssh/id_rsa.pub
```

3. Copy the contents of your SSH public key.

4. Log in to Business Central.

5. Select **Admin → SSH Keys**.

6. From the **SSH Keys** page, click **Add SSH Keys**.

7. In the **Add SSH Key** window, enter a name in the **Name** field and copy the contents of the SSH public key to the **Keys** field.

   **NOTE**

   The **Name** and the **Key** fields are mandatory.

8. Click **Add SSH Key** to register the key.

### 11.5. DELETING AN SSH KEY

You can delete an SSH key from Business Central by from the **SSH Keys** page.

**Procedure**

1. Log in to Business Central.

2. Select **Admin → SSH Keys**.

3. All of the SSH keys are listed on the **SSH Keys** page.

4. To delete an SSH key, click the delete icon (trash can).

5. Click the **Delete SSH Key** to confirm the deletion.
CHAPTER 12. LDAP CONNECTION

Business Central provides a dedicated **UserGroupCallback** implementation for LDAP servers with Red Hat Process Automation Manager to enable the user task service to retrieve information on users, groups, and roles directly from an LDAP service.

You can configure the following LDAP **UserGroupCallback** implementation properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ldap.bind.user</td>
<td>User name for connecting to the LDAP server <em>(optional if the LDAP server accepts anonymous access).</em></td>
</tr>
<tr>
<td>ldap.bind.pwd</td>
<td>Password for connecting to the LDAP server <em>(optional if the LDAP server accepts anonymous access).</em></td>
</tr>
<tr>
<td>ldap.user.ctx</td>
<td>Context in LDAP with user information <em>(mandatory)</em></td>
</tr>
<tr>
<td>ldap.role.ctx</td>
<td>Context in LDAP with group and role information <em>(mandatory)</em></td>
</tr>
<tr>
<td>ldap.user.roles.ctx</td>
<td>Context in LDAP with user group and role membership information <em>(optional if not specified and ldap.role.ctx property is used instead).</em></td>
</tr>
<tr>
<td>ldap.user.filter</td>
<td>Filter for searching user information; usually contains substitution keys {0}, which are replaced with parameters <em>(mandatory)</em></td>
</tr>
<tr>
<td>ldap.role.filter</td>
<td>Filter for searching group and role information, usually contains substitution keys {0}, which are replaced with parameters <em>(mandatory)</em></td>
</tr>
<tr>
<td>ldap.user.roles.filter</td>
<td>Filter for searching user group and role membership information, usually contains substitution keys {0}, which are replaced with parameters <em>(mandatory)</em></td>
</tr>
<tr>
<td>ldap.user.attr.id</td>
<td>Attribute name of the user ID in LDAP <em>(optional; if not specified, uid property is used instead).</em></td>
</tr>
<tr>
<td>ldap.roles.attr.id</td>
<td>Attribute name of the group and role ID in LDAP <em>(optional; if not specified, cn property is used instead).</em></td>
</tr>
<tr>
<td>ldap.user.id.dn</td>
<td>User ID in a DN, instructs the callback to query for user DN before searching for roles <em>(optional; is false by default).</em></td>
</tr>
</tbody>
</table>
12.1. LDAP USERGROUPCALLBACK IMPLEMENTATION

You can use the LDAP UserGroupCallback implementation by configuring the respective LDAP properties in one of the following ways:

- **Programmatically**: Build a properties object with the respective LDAPUserGroupCallbackImpl properties and create LDAPUserGroupCallbackImpl with the properties object as its parameter.

  ```java
  import org.kie.api.PropertiesConfiguration;
  import org.kie.api.task.UserGroupCallback;
  ...
  Properties properties = new Properties();
  properties.setProperty(LDAPUserGroupCallbackImpl.USER_CTX, "ou=People,dc=my-domain,dc=com");
  properties.setProperty(LDAPUserGroupCallbackImpl.ROLE_CTX, "ou=Roles,dc=my-domain,dc=com");
  properties.setProperty(LDAPUserGroupCallbackImpl.USER_ROLES_CTX, "ou=Roles,dc=my-domain,dc=com");
  properties.setProperty(LDAPUserGroupCallbackImpl.USER_FILTER, "(uid={0})");
  properties.setProperty(LDAPUserGroupCallbackImpl.ROLE_FILTER, "(cn={0})");
  properties.setProperty(LDAPUserGroupCallbackImpl.USER_ROLES_FILTER, "(member={0})");
  UserGroupCallback ldapUserGroupCallback = new LDAPUserGroupCallbackImpl(properties);
  UserGroupCallbackManager.getInstance().setCallback(ldapUserGroupCallback);
  ```

- **Declaratively**: Create the `jbpm.usergroup.callback.properties` file in the root of your application or specify the file location as a system property: `-Djbpm.usergroup.callback.properties=FILE_LOCATION_ON_CLASSPATH`
  Ensure that you register the LDAP callback when starting the user task server.

  ```bash
  #ldap.bind.user=
  #ldap.bind.pwd=
  ldap.user.ctx=ou=People,dc=my-domain,dc=com
  ldap.role.ctx=ou=Roles,dc=my-domain,dc=com
  ldap.user.roles.ctx=ou=Roles,dc=my-domain,dc=com
  ```

**Property** | **Description**
--- | ---
`java.naming.factory.initial` | Initial context factory class name; is `com.sun.jndi.ldap.LdapCtxFactory` by default.
`java.naming.security.authentication` | Authentication type (possible values are none, simple, and strong; is simple by default).
`java.naming.security.protocol` | Security protocol to be used, for example, ssl.
`java.naming.provider.url` | LDAP url (by default `ldap://localhost:389`; if the protocol is set to ssl then `ldap://localhost:636`)
```
ldap.user.filter=(uid={0})
ldap.role.filter=(cn={0})
ldap.user.roles.filter=(member={0})
#ldap.user.attr.id=
#ldap.roles.attr.id=
```

Additional resources

- Roles and users
- *Red Hat Single Sign-On Server Administration Guide*
- Defining LDAP login domain
- LDAP login module
- LDAPExtended login module
- AdvancedLDAP login module
- AdvancedAdLDAP login module
- LDAP connectivity options
- LDAPUsers login module
CHAPTER 13. DATABASE CONNECTION

Business Central provides a dedicated UserGroupCallback implementation for database server with Red Hat Process Automation Manager to enable the user task service. The user task service helps in retrieving information on users and groups (roles) directly from databases.

You can configure the following database UserGroupCallback implementation properties:

Table 13.1. Database UserGroupCallback properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>db.ds.jndi.name</td>
<td>JNDI name of the data source used for connections</td>
</tr>
<tr>
<td>db.user.query</td>
<td>Verifies the user existence</td>
</tr>
<tr>
<td>db.user.roles.query</td>
<td>Collects the groups for a given user</td>
</tr>
<tr>
<td>db.roles.query</td>
<td>Verifies the group existence</td>
</tr>
</tbody>
</table>

13.1. DATABASE USERGROUPCALLBACK IMPLEMENTATION

In database UserGroupCallback implementation, you must create the required database. You can use this implementation by configuring the respective database properties in one of the following ways:

- Programmatically: Build a properties object with the respective DBUserGroupCallbackImpl properties and create DBUserGroupCallbackImpl using the same properties object as its parameter.
  For example:

  ```java
  import static org.jbpm.services.task.identity.DBUserGroupCallbackImpl.DS_JNDI_NAME;
  import static org.jbpm.services.task.identity.DBUserGroupCallbackImpl.PRINCIPAL_QUERY;
  import static org.jbpm.services.task.identity.DBUserGroupCallbackImpl.ROLES_QUERY;
  import static org.jbpm.services.task.identity.DBUserGroupCallbackImpl.USER_ROLES_QUERY;
  ...
  props = new Properties();
  props.setProperty(DS_JNDI_NAME, "jdbc/jbpm-ds");
  props.setProperty(PRINCIPAL_QUERY, "select userId from Users where userId = ?");
  props.setProperty(ROLES_QUERY, "select groupId from UserGroups where groupId = ?");
  props.setProperty(USER_ROLES_QUERY, "select groupId from UserGroups where userId = ?");
  
  callback = new DBUserGroupCallbackImpl(props);
  ```

- Declaratively: Create the jbpm.usergroup.callback.properties file in the root of your application or specify the file location as a system property.
  For example:

  ```bash
  -Djbpm.usergroup.callback.properties=FILE_LOCATION_ON_CLASSPATH
  ```
Ensure that you register the database callback when starting the user task server.

For example:

```java
System.setProperty("jbpm.usergroup.callback.properties", 
"/jbpm.usergroup.callback.db.properties");
callback = new DBUserGroupCallbackImpl(true);
...
db.ds.jndi.name = jdbc/jbpm-ds
db.user.query = select userId from Users where userId = ?
db.roles.query = select groupId from UserGroups where groupld = ?
db.user.roles.query = select groupld from UserGroups where userld = ?
```

Additional resources

- Roles and users
CHAPTER 14. CONFIGURING MAVEN USING SETTINGS.XML FILE

Java application development uses the Apache Maven build automation tool to build and manage software projects. Maven uses Project Object Model (POM) configuration XML files to define both, the project properties and the build process.

Maven uses repositories to store Java libraries, plug-ins, and other build artifacts. Repositories can be either local or remote. A local repository is a download of artifacts from a remote repository cached on a local machine. A remote repository is any other repository accessed using common protocols, such as http:// when located on an HTTP server, or file:// when located on a file server. The default repository is the public remote Maven 2 Central Repository. Configuration of Maven is performed by modifying the settings.xml file. You can either configure global Maven settings in the M2_HOME/conf/settings.xml file, or user-level settings in the USER_HOME/.m2/settings.xml file.

Additional resources

- Configuring an external Maven repository for Business Central
- Packaging and deploying a project in Maven
- Maven settings and repositories for Red Hat Process Automation Manager
- System integration with Maven
- Welcome to Apache Maven
- Apache Maven Project - Introduction to Repositories
- Apache Maven Parent POMs Reference.
CHAPTER 15. MANAGING GAV CHECKS

In Business Central, projects are identified using Maven naming convention or GAV (group Id, artifact, and version) data. GAV values differentiate projects and project versions as well as identify dependencies with particular projects.

By default, Business Central detects duplicate GAVs. This feature can be disabled by users with the admin role.

Enabling GAV checks and child GAV edition

Procedure

1. Log in to Business Central.
2. Select Menu → Design → Projects.
3. Double-click the project to open it.
4. In the Project Editor window, click the Settings tab.
5. Make the following selections from the General Settings tab.
   a. Select Disable GAV conflict check to enable other projects to have the same GAV.
   b. Select Allow child GAV edition to enable child projects to have GAV edition.
6. Click Save.

   NOTE

   Click Reset to undo all changes.

7. Click Save again to confirm the changes.

NOTE

You can disable the duplicate GAV detection feature by setting the org.guvnor.project.gav.check.disabled system property to true when you start Business Central.

$ ~/<EAP_HOME>/bin/standalone.sh -c standalone-full.xml -Dorg.guvnor.project.gav.check.disabled=true
CHAPTER 16. REPOSITORY HOOKS

In Business Central, you can use scripts, known as hooks, to configure the repository to trigger a specified action every time a particular event happens.

16.1. CONFIGURING GIT HOOKS

Business Central can automatically push changes to a remote repository using Git hooks. After you configure the post-commit hook, Business Central automatically pushes your changes to the remote repository.

NOTE
Currently only post-commit hooks are supported. Post-commit hooks are triggered after the commit process finishes.

Prerequisites

- Red Hat Process Automation Manager projects exist in an external Git repository.
- Credentials required for read access to that external Git repository are available.

Procedure

1. Log in to Business Central.

2. Select Menu → Projects.

3. Select or create the space into which you want to import the projects.

4. Click on the right side of the screen and select Import Project.

5. In the Import Project window, enter the URL (for example, https://github.com/USERNAME/REPOSITORY_NAME.git) and credentials for the Git repository that contains the project that you want to import and click Import. The project is added to the Business Central Git repository and is available in the created or default space.

IMPORTANT
Use the HTTPS or Git protocol instead of a SCP-style SSH URL. Business Central does not support the basic SSH URL and an error appears if you use this URL.

6. In a terminal window, change to the created repository.

   ```
   cd JBOSS_HOME/bin/.niogit/REPOSITORY_NAME.git
   ```

7. Create the post-commit file in the JBOSS_HOME/bin/.niogit/REPOSITORY_NAME.git/hooks directory, set the permissions to rwxr--r-- and add the following content:
8. Make sure that the configuration was successful by creating a new guided rule in Business Central:
   a. Select **Menu → Projects → Add Asset → Guided Rule**.
   b. Fill in the required information in the displayed **Create new Guided Rule** window.
   c. Click **Ok**. Business Central automatically pushes all changes to the remote repository.

You can also specify the `org.uberfire.nio.git.hooks` system property. Specify a directory with default hook files as the value for this property. This directory will be copied to the newly created Git repositories. See the following example of a `standalone.xml` file with this setting below:

```xml
<system-properties>
  <property name="org.uberfire.nio.git.hooks" value="/opt/jboss-as/git-hooks"/>
  ...
</system-properties>
```

### Additional resources

- [Customizing Git Hooks](#)

## 16.2. GIT HOOK EXIT CODES

When a git hook exits an integer value is returned which determines the status of the git hook execution. This integer value is known as a git hook exit code. The execution status can be a success, warning or failure.

### 16.2.1. Types of exit codes

Business Central has the following three types of exit codes:

**Successful notification**

0: Success. A git hook that exits with code 0 displays a success notification in the user interface.

**Warning notification**

1..30: Warning. A git hook that exits with a code between 1 and 30 (inclusive) will display a warning notification in user interface.

**Error notification**

Anything else: Error. Any other code number will be displayed as an error notification.

### IMPORTANT

UNIX systems only support error codes between 0 (success) and 255 (error). Any exit code outside of this range is converted to a different code which might result in displaying a wrong notification message. Windows systems don’t have this limitation and can support a wide range of exit codes.
16.3. CUSTOMIZING GIT HOOK NOTIFICATIONS

Business Central provides a mechanism that enables users to receive feedback about git hook executions using customized messages based on a hook’s exit code.

Procedure

1. To enable notifications, in the standalone.xml file set the appformer.git.hooks.bundle system property to point to a *.properties file containing the custom messages for each exit code. For example:

   `<system-properties>
   <property name="appformer.git.hooks.bundle" value="/opt/jboss-as/git-hooks-messages/Messages.properties">
   </property>
   ...
   </system-properties>`

2. To display the messages, each line of the *.properties must have the following format:

   `<exit_code>=<display_message>

   where, `<exit_code>` is the git hook exit code and `<display_message>` is the custom message that is displayed to a user.

   Exit code messages with this format appear similar to the following example:

   0=Success
   1=Display Message 1
   .
   .
   31=Display Message 31

**NOTE**

It’s not necessary to define all the possible exit codes in the *.properties file. Notifications appear only for the exit codes defined in the *.properties file.

16.3.1. Internationalize git hook notifications

You can internationalize the notification messages by placing different *.properties files in the directory specified for the appformer.git.hooks.bundle system property. The names of the localized files have the format `<filename>_<lang>.properties`. These files must contain the same entries as in the original file.

For example, you have specified the system property to point to Messages.properties. Now you can create localized message properties files like Messages_en.properties for English, Messages_fr.properties for French, Messages_it.properties for Italian, and so on. The notification service will choose the one based on the user language and if there are no available translations for a language then it will use the default ones specified in the Messages.properties file.
IMPORTANT

The notification service only supports the ISO 8859-1 (Latin 1) character set in the *.properties file. If you want to use extended characters, please escape them using their Unicode code.
CHAPTER 17. VIEWING PROCESS INSTANCE LOGS

You can view all the process events of an instance from its Logs tab. The instance logs list all the current and previous process states. Business Central has two types of logs for process instances, Business and Technical logs.

Procedure

1. Log in to Business Central.
2. Select Menu → Manage → Process Instances.
3. On the Manage Process Instances page, click the process instance whose log you want to view.
4. Select the Logs tab:
   - Click Business to view the business events log.
   - Click Technical to view the technical events log.
   - Click Asc or Desc to change the order of the log files.
APPENDIX A. VERSIONING INFORMATION

Documentation last updated on Wednesday, April 28, 2021.