Redmine - Patch #38728

Correctly escape issue text in Gantt PNG export for ImageMagick convert

2023-06-15 17:30 - Holger Just

<table>
<thead>
<tr>
<th>Status:</th>
<th>New</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>Normal</td>
</tr>
<tr>
<td>Assignee:</td>
<td>Gantt</td>
</tr>
<tr>
<td>Category:</td>
<td>Gantt</td>
</tr>
<tr>
<td>Target version:</td>
<td>Candidate for next minor release</td>
</tr>
</tbody>
</table>

**Description**

According to [https://imagemagick.org/Usage/draw/#text](https://imagemagick.org/Usage/draw/#text), we need to quote the passed text and only escape the quote character and backslash with backslashes respectively. Redmine::Utils::Shell.shell_quote escapes the single quote for a wrong environment (namely a shell) which results in errors if an issue subject contains a single quote character.

The attached patch fixes this by using specific quoting/escaping for the ImageMagick convert command.

Note that the usual shell special characters (such as $, `, ...) do not need to be escaped here since the shellouts performed by MiniMagick are performed with Open3.popen3 which does not launch a shell but runs the command directly.

**History**

#1 - 2023-06-26 10:33 - Holger Just

To further explain this, when a ` character is included in an issue subject, right now, we would escape the generated command line argument to convert as follows (assuming the subject is foo `bar` baz)

```
text 2,16 'foo "bar" baz'
```

This is a single argument (including the spaces). As explained, there are no surrounding quotes around the command line argument as the command in not run through a shell by mini_magick but is directly passed to the command via Open3.popen3. Imagemagick performs some quote-parsing on its own to determine the single or double-quoted string as the last argument to a draw text rule.

However, due to the excessive escaping of the ` characters, imagemagick barfs as its parsing rules for the quoted string expects only a single quoted string (with internal quotes of the same type escaped by \\). This escaping rule as described in the above linked document is implemented by the patch. Thus, after the patch the same issue subject will result in the following command line argument:

```
text 2,16 'foo \'bar\' baz'
```

**Files**

0001-Correctly-escape-issue-text-in-Gantt-PNG-export-for-.patch 3.26 KB 2023-06-15 Holger Just