Infrastructure - Task #2852
Upgrade Gerrit to recent version
2019-04-01 23:45 - David Ostrovsky

**Status:** Closed  **Start date:**

**Priority:** Normal  **Due date:**

**Assignee:** Guilhem Moulin  **% Done:** 0%

**Category:** Gerrit  **Target version:** Q1/2020

**Tags:**  **URL:**

### Description

New Gerrit versions has fixed critical bugs added user friendly workflows and introduced many new features, like new backend NoteDb (replacement of ReviewDb), new Polymer based PolyGerrit UI (replacement of GWT UI) and new build tool: Bazel (replacement of Buck).

There was a discussion to discontinue community support for Java 7 and Gerrit releases <= 2.13.x: [1].

**Things to consider:**

- in 2.13 Java 7 is still supported.
- in 2.13 Buck build tool is used.

- in 2.14 Java 8 is mandatory.
- in 2.14 Bazel build tool is used.
- in 2.14 support for Soy templates was added. For backwards compatibility, support for Velocity templates (VTL) was kept.

- in 2.15 draft change workflow is removed and replaced with Work-In-Progress workflow and private changes.
- in 2.15 accounts table was moved to NoteDb (Git).
- in 2.15 new PolyGerrit UI is added as experimental UI.
- in 2.15 Soy template based EMail templates are supported.

- in 2.16 groups table was moved to NoteDb (Git).
- in 2.16 online migration from ReviewDb to NoteDb is supported for changes. Only one table is used after the migration, that is also removed in upcoming Gerrit 3.0 release (ETA: second quarter of 2019).
- in 2.16 GWT UI is deprecated.
- in 2.16 new core plugins are added: codemirror-editor, delete-project.
- in 2.16 support for Velocity templates (VTL) is completely removed. Site administrators must replace any Velocity templates (.vm files in $site/etc/mail/) with the equivalent Soy templates before upgrading to this version.

- in 3.0 GWT UI is removed.
- in 3.0 ReviewDb is removed and only offline migration is supported to NoteDb.
- in 3.0 new core plugins are added: gitiles.

[1] [https://groups.google.com/d/topic/repo-discuss/TP9ozTsazfU/discussion](https://groups.google.com/d/topic/repo-discuss/TP9ozTsazfU/discussion)

### History

#### #1 - 2019-04-02 00:11 - Guilhem Moulin

David Ostrovsky wrote:

> New Gerrit versions has fixed critical bugs […]

Critical bugs that haven't been backported to other supported branches?

#### #2 - 2019-04-02 07:41 - David Ostrovsky

Guilhem Moulin wrote:

> New Gerrit versions has fixed critical bugs […]

2022-03-20
Critical bugs that haven't been backported to other supported branches?

Let's call it just bugs. Only severe problems and major security vulnerabilities are backported to very old stable branches. Also Gerrit transitive dependencies: JGit, Apache SSHD, Eclipse Jetty and Apache Lucene only updated in recent versions and those updates are not back ported.

David Ostrovsky wrote:

 [...] and introduced many new features, like new backend NoteDb (replacement of ReviewDb), new Polymer based PolyGerrit UI (replacement of GWT UI) and new build tool: Bazel (replacement of Buck).

I would also add that PolyGerrit feature: "Diff on single page for all changed files" was always requested by so many users.

#3 - 2019-05-08 15:49 - Florian Effenberger

IIRC, there was an upgrade planned in the near future, also because of a required plugin

Guilhem, can you share the details on what's planned and when?

There's some urgent things in between, but sharing upfront here what's planned and when is a good idea, I think!

#4 - 2019-05-09 04:23 - Guilhem Moulin

Florian Effenberger wrote:

IIRC, there was an upgrade planned in the near future, also because of a required plugin

Guilhem, can you share the details on what's planned and when?

Would have been good (meaning saved a few mails) to have the request here rather than on hostmaster then :-)

Mike and Olivier would like a 2.16 test instance for the CodeMirror plugin. While I was able to build the plugin against 2.13, I was unable to make it work, I guess to changes in the JS API. I'll deploy a 2.16 test instance on vm178 along with our (2.13) stage instance. Upgrading the production instance to >2.13, given the sweat we have throw at upgrade paths, is unlikely to happen in 2019. (This was mentioned to Mike, in the infra call minutes, and on IRC several times already.) Unless an EOL is announced for 2.13, that is.

#5 - 2019-05-09 10:45 - Florian Effenberger

Mike and Olivier would like a 2.16 test instance for the CodeMirror plugin. While I was able to build the plugin against 2.13, I was unable to make it work, I guess to changes in the JS API. I'll deploy a 2.16 test instance on vm178 along with our (2.13) stage instance. Upgrading the production instance to >2.13, given the sweat we have throw at upgrade paths, is unlikely to happen in 2019. (This was mentioned to Mike, in the infra call minutes, and on IRC several times already.) Unless an EOL is announced for 2.13, that is.

Sorry for the confusion then, seems I got this one wrong. What we should discuss then however is when the CodeMirror plugin should go live, if that's bound to 2.16 - IMHO the plan was to have that in 2019 too, but let's talk this through in the next infra call or team meeting, before I do more wild guesses here that end up wrong ;-)
same problem: https://phabricator.wikimedia.org/T197192.

At this point I’d say that it makes sense to sync the upgrade path with the migration to TDF’s IdP for Single-Sign On authentication, and deprecate all other authentication methods to Gerrit’s web frontend. On our 2.16 stage I forked your OAuth2 plugin to make it work with our provider (LemonLDAP::NG — like for other IdP it’s only a matter of choosing the right paths to the various endpoints and then map the JSON object to an account).

#9 - 2019-09-06 09:09 - David Ostrovsky

At this point I’d say that it makes sense to sync the upgrade path with the migration to TDF’s IdP for Single-Sign On authentication, and deprecate all other authentication methods to Gerrit's web frontend.

I totally agree on this, and expected that gerrit is going to be moved to LDAP auth scheme, before upgrading to 2.15. I even had a discussion with migration steps with Norbert years ago, from OpenID/OAuth to LDAP.

On our 2.16 stage I forked your OAuth2 plugin to make it work with our provider (LemonLDAP::NG — like for other IdP it’s only a matter of choosing the right paths to the various endpoints and then map the JSON object to an account).

I would happily review your changes and would merge them upstream. Could you please upload your changes to oauth-plugin project in gerrit-review: [1]?

Another option would be to use: saml plugin, that I recently moved to gerrit-review and adapted to work against most recent gerrit versions: [2]. With saml plugin the real SSO should work out of the box and some enterprise customers already successful use this plugin in production.


#10 - 2019-09-06 11:35 - Guilhem Moulin

David Ostrovsky wrote:

At this point I’d say that it makes sense to sync the upgrade path with the migration to TDF’s IdP for Single-Sign On authentication, and deprecate all other authentication methods to Gerrit's web frontend.

I totally agree on this, and expected that gerrit is going to be moved to LDAP auth scheme, before upgrading to 2.15. I even had a discussion with migration steps with Norbert years ago, from OpenID/OAuth to LDAP.

Changing the authentication method to LDAP provides shared credentials not Single Sign-On. It also increases the attack surface as the service can access said shared credentials. Like for other services at TDF I have no plan to use LDAP authentication but instead use a proper WebSSO solution using for instance SAML 2.0 or Auth2 (we're using both).

On our 2.16 stage I forked your OAuth2 plugin to make it work with our provider (LemonLDAP::NG — like for other IdP it’s only a matter of choosing the right paths to the various endpoints and then map the JSON object to an account).

I would happily review your changes and would merge them upstream. Could you please upload your changes to oauth-plugin project in gerrit-review: [1]?

Another option would be to use: saml plugin, that I recently moved to gerrit-review and adapted to work against most recent gerrit versions: [2]. With saml plugin the real SSO should work out of the box and some enterprise customers already successful use this plugin in production.

Ah cool, I’ll test the SAML plugin also, LemonLDAP::NG has a SAML IdP and this shouldn't require fiddling around with the code.

#11 - 2019-12-26 18:42 - David Ostrovsky

This is done now and can be closed.

Also, adding the reference to the question about generic OAuth2 provider using gerrit-oauth plugin: [1]. And of course I am still interested to add support for the LemonLDAP::NG to the gerrit-oauth plugin. Is the source available in any publicly accessible repository? I could pick it up myself and upload to the canonical plugin repository: [2].


#12 - 2019-12-26 21:10 - Guilhem Moulin
Closing, and attaching patch against v2.16.1. The new LL::NG provider is trivially derived from your code for GitLab. I guess LEMONLDAP_PROVIDER_PREFIX should be changed to "llng-oauth:" though. Unfortunately, this means one can't use multiple LL::NG providers with the plugin — like for GitLab — but that's not something we care about anymore as we dropped support for third-party IdPs on Dec 25.

#13 - 2019-12-27 00:49 - David Ostrovsky

Closing, and attaching patch against v2.16.1.

Thanks! Unrelated to this issue, but could you also upload gitiles-plugin patch for marking diff chunks you applied to gitiles-plugin on gerrit.libreoffice.org site?

#14 - 2020-02-23 10:37 - David Ostrovsky

Closing, and attaching patch against v2.16.1. The new LL::NG provider is trivially derived from your code for GitLab.

I uploaded this CL for review: [1]. Note, that oauth plugin was bumped to the latest version of scribejava library to address this issue: [2].

I don't know whether or not LL::NG provider supports bearer token signature and basic authentication scheme, so that I commented out new auth and signature ways in the code. If you can figure out, whether or not new auth schemes are supported (or not), we can fix those comments: [3], [4].

I guess LEMONLDAP_PROVIDER_PREFIX should be changed to "llng-oauth:" though.

Right, I've changed the prefix as you have suggested to: "llng-oauth:".

Unrelated to this issue, but could you also upload gitiles-plugin patch for marking diff chunks you applied to gitiles-plugin on gerrit.libreoffice.org site?

Moreover, there was another request for highlighting of in line differences in Gitiles in this thread: [5] and I commented, that TDF infra team patched Gitiles and it would be great if this patch could be upstreamed. That's how truly open source driven projects work. So, please, consider to give your valuable contribution back to the Gerrit community. Thank you in advance.

[5] https://groups.google.com/d/msg/repo-discuss/TJmjeelXG1E/7f5ndn6HGAAJ

#15 - 2020-02-23 17:17 - Guilhem Moulin

- Target version changed from Qlater to Q1/2020

I don't know whether or not LL::NG provider supports bearer token signature and basic authentication scheme, so that I commented out new auth and signature ways in the code.

Dunno either. Will try to figure it out when we upgrade the service.

Moreover, there was another request for highlighting of in line differences in Gitiles in this thread: [5] and I commented, that TDF infra team patched Gitiles and it would be great if this patch could be upstreamed.

Ah right, there is too much sidetrack in that ticket... You're welcome to pick it up at https://git.libreoffice.org/gitiles/commit/e08d0507ae31c38db1d8302ab4d4d15141d909ef. I consider that to be a crude hack though, ideally JGit's
would extend its diff interface to offer something more fine-grained than line-based. IIRC what I do right now is to use JGit's EditList to build back hunks of RawTexts (in a non line-oriented fashion), then throw Neil Fraser's diff-match-patch at the substrings to get the fine-grained list of changes. Would make more sense to integrate that in JGit than in gitiles IMHO. (Also the submodule clutters the build system even more now that gitiles is a core plugin.)

Another patch you might be interested in: https://git.libreoffice.org/gitiles/commit/39626517c4671ee046f5a2b7fbb5243c622f176e. This is another ugly hack though, with some monkeypatching to access the raw content back. I'm not a Java programmer, so please bear with me :P

#16 - 2020-02-23 17:18 - Guilhem Moulin
(And if you wonder, yes I just created https://git.libreoffice.org/gitiles.)

#17 - 2020-02-23 21:36 - David Ostrovsky

You're welcome to pick it up at https://git.libreoffice.org/gitiles/commit/e08d0507ae31c38db1d8302ab4d4d15141d909ef.

Thanks. I conducted a custom release: [1] for the diff-match-patch library and adapted the patch to fetch it on the fly using Bazel's http_file() rule: [2]. It would be great, if you could create account on gerrit-review and sign the ACL, I would change the author in this CL: [2] to your name.

[1] https://github.com/davido/diff-match-patch/releases/tag/v1.0.0

#18 - 2020-02-23 22:37 - Guilhem Moulin

I conducted a custom release: [1] for the diff-match-patch library and adapted the patch to fetch it on the fly using Bazel's http_file() rule: [2].

Neat, thanks!

It would be great, if you could create account on gerrit-review and sign the ACL

I'm afraid I don't have a Google account :-P I suppose they don't offer non-Googley authentication methods?

#19 - 2020-07-04 21:31 - Guilhem Moulin

David Ostrovsky wrote:

I don't know whether or not LL::NG provider supports bearer token signature and basic authentication scheme, so that I commented out new auth and signature ways in the code. If you can figure out, whether or not new auth schemes are supported (or not), we can fix those comments: [3], [4].

I guess LEMONLDAP_PROVIDER_PREFIX should be changed to "llng-oauth:" though.

Right, I've changed the prefix as you have suggested to: "llng-oauth:".

Unrelated to this issue but I didn't forget to back after the LL::NG resp. gerrit upgrade :-)

The version we're running at the moment can be found at https://git.libreoffice.org/infra/gerrit-oauth/+log/refs/tags/v3.1.3+tdf. There are some minors modifications to your code:

57e5804 LemonLDAP::NG: Remove getBearerSignature() override
1367d2b LemonLDAP::NG: Fix default scope name
420273f LemonLDAP::NG: Set username claim name in accordance with specs

(420273f allows automatic username provisioning for SSH and HTTP.)

#20 - 2020-07-05 16:54 - David Ostrovsky

Guilhem Moulin wrote:

David Ostrovsky wrote:
I don't know whether or not LL::NG provider supports bearer token signature and basic authentication scheme, so that I commented out new auth and signature ways in the code. If you can figure out, whether or not new auth schemes are supported (or not), we can fix those comments: [3], [4].

I guess LEMONLDAP_PROVIDER_PREFIX should be changed to "llng-oauth:" though.

Right, I've changed the prefix as you have suggested to: "llng-oauth:".

Unrelated to this issue but I didn't forget to back after the LL::NG resp. gerrit upgrade ;-)  

The version we're running at the moment can be found at https://git.libreoffice.org/infra/gerrit-oauth/+log/refs/tags/v3.1.3+tdf. There are some minor modifications to your code:

57e5804 LemonLDAP::NG: Remove getBearerSignature() override  
1367d2b LemonLDAP::NG: Fix default scope name  
420273f LemonLDAP::NG: Set username claim name in accordance with specs

Cool, I have uploaded all your fixes:

https://gerrit-review.googlesource.com/c/plugins/oauth/+/274444 LemonLDAP::NG: Set username claim name in accordance with specs [NEW]  
https://gerrit-review.googlesource.com/c/plugins/oauth/+/274445 LemonLDAP::NG: Fix default scope  
https://gerrit-review.googlesource.com/c/plugins/oauth/+/274446 LemonLDAP::NG: Remove getBearerSignature() override [NEW]

Hopefully, you could switch to upstream once they are merged ;-)  

Also note, that you wouldn't have to build them yourself, but could download from the GerritForge CI: [1].


#21 - 2020-07-05 17:02 - Guilhem Moulin

David Ostrovsky wrote:

Cool, I have uploaded all your fixes:

Thanks!

Hopefully, you could switch to upstream once they are merged ;-)  

Also note, that you wouldn't have to build them yourself, but could download from the GerritForge CI: [1].

Yup that's what we did before the switch to our own IdP :-) Eliminating the delta between the upstream version and what we run would indeed be welcome.

#22 - 2020-07-05 17:26 - David Ostrovsky

Guilhem Moulin wrote:

David Ostrovsky wrote:

Cool, I have uploaded all your fixes:

Thanks!

Hopefully, you could switch to upstream once they are merged ;-)  

Also note, that you wouldn't have to build them yourself, but could download from the GerritForge CI: [1].

Yup that's what we did before the switch to our own IdP :-) Eliminating the delta between the upstream version and what we run would indeed be welcome.

All CLs are merged now, and CI build is green as well: [1].
<table>
<thead>
<tr>
<th>Files</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>tdf-oauth.patch</td>
<td>10.4 KB</td>
<td>2019-12-26</td>
<td>Guilhem Moulin</td>
</tr>
</tbody>
</table>