Infrastructure - Task #1585

single sign-on (SSO)

2015-11-06 11:38 - Michael Meeks

Status: In Progress
Priority: Normal
Assignee: Guilhem Moulin
Category:
Target version: Q4/2020
Tags:

Start date:
Due date:
% Done: 0%

URL:

Description

Having to remember, and manage a slew of different credentials for different pieces of infrastructure: from bugzilla, to redmine, to SilverStrip etc. is a royal pain.

Surely we can use a consistent credential store for all of these.

Related issues:
Related to Infrastructure - Task #989: Setup public LDAP server for SSO
Closed

History

#1 - 2015-11-06 13:09 - Bjoern Michaelsen

So to revamp the discussion on this one: The key questions was if we should use OpenID or a TDF-wide LDAP.

- For OpenID the concern is if all services support it:
  - all supporting it, would probably just need some config tweaks
  - Bugzilla proved problematic in the past (at least at freedesktop it wasn’t easily implemented)
  - askbot and gerrit: we are already using OpenID
  - other services: (do we miss any here?)

Norbert suggested setting up our own LDAP instead. Questions/Comments on that from my side:

- do all services support LDAP? Redmine, Silverstripe, mediawiki, Bugzilla, askbot, gerrit, (missing services)?
- how do we bootstrap new accounts? impact on onramping? (e.g. to get a freedesktop account, you needed to file a bug on bugzilla, for which you needed yet another account)
- LDAP would be a new SPOF for ~all infra. It would require us to provide LDAP as a HA service, make sure that routing between LDAP and all other services are HA too (e.g. ability to push patches would be depending on three SPOFs: gerrit itself, connection between gerrit and LDAP, LDAP itself)

#2 - 2015-11-06 14:05 - Bjoern Michaelsen

Found: [https://wiki.documentfoundation.org/Infra/Services](https://wiki.documentfoundation.org/Infra/Services)

services missing from above:

- Plone (extensions, templates, conference website) [https://pypi.python.org/pypi/plone.openid](https://pypi.python.org/pypi/plone.openid)
- ownCloud (according to [https://en.wikipedia.org/wiki/OwnCloud](https://en.wikipedia.org/wiki/OwnCloud) native open-id support)
- moztrap (done as per [https://bugs.documentfoundation.org/show_bug.cgi?id=47658](https://bugs.documentfoundation.org/show_bug.cgi?id=47658))

---

#3 - 2015-11-09 10:05 - Florian Effenberger

- Project changed from Foundation to Infrastructure
- Assignee set to Alexander Werner
- Target version set to Q1/2016

SSO was a topic during the last in-person admin meeting, adding this to Alex’ pile to watch out for progress

The current plan - Alex, correct my if I’m wrong - is that Robert and AlexV will evaluate Samba for LDAP directory services

Alex, can you get some status update and see where we are, and if LDAP based on Samba is a likely scenario?

Based on that, current (and realistic future) services need to be evaluated whether LDAP works with them, and/or if an OpenID gateway exists (if such thing exists at all)

---

#4 - 2015-11-10 15:52 - Dennis Roczek
Florian Effenberger wrote:

SSO was a topic during the last in-person admin meeting, adding this to Alex’ pile to watch out for progress.
The current plan - Alex, correct my if I’m wrong - is that Robert and AlexV will evaluate Samba for LDAP directory services.
Alex, can you get some status update and see where we are, and if LDAP based on Samba is a likely scenario?
Based on that, current (and realistic future) services need to be evaluated whether LDAP works with them, and/or if a OpenID gateway exists (if such thing exists at all)

Just to write it down:
HELPWIKI and OwnCloud should be test services to see how proper the Samba service is working. HELPWIKI and TDFWIKI then would be my part.
;

(@björn: you missed all three services :-D )

#5 - 2016-01-13 15:45 - Alexander Werner
- Subject changed from Single Sign On to Creating a Proof of Concept for SSO

#6 - 2016-03-04 14:09 - Florian Effenberger
- Status changed from New to In Progress

#8 - 2016-03-04 15:16 - Norbert Thiebaud

no, no, no, no, no...
We have to stop this ‘I like to have ponny but no-one care to do it so let’s buy it’ trend.

For infra we have some people on payroll, and we have volunteers... we have to make do with that.
If SSO is not making progress then so be it.. either people can live without it, or they can step in and help make it happen.

#9 - 2016-03-07 10:47 - Florian Effenberger

  no, no, no, no, no,...
  We have to stop this ‘I like to have ponny but no-one care to do it so let's buy it’ trend.

  For infra we have some people on payroll, and we have volunteers... we have to make do with that.
  If SSO is not making progress then so be it.. either people can live without it, or they can step in and help make it happen.

Fine for me, of course, but my remembering is that there are a few board members who would like to have this, which is why I turned into a budget item that the board then can vote on.

What would be your proposal then how to handle the request?

#10 - 2016-03-07 11:57 - Michael Meeks

It seems to me entirely appropriate to have the board make the budget prioritization decision on this one in the normal budgeting sheet.

But of course, Norbert has a great point wrt. existing staff time and trying to use this to build community input into sysadmin.

#11 - 2016-04-05 11:53 - Florian Effenberger
- Target version changed from Q1/2016 to Q2/2016

Some good news on that
During CeBIT, the idea has grown that we could have a look at UCS (Univention Corporate Server) which nowadays is completely free of charge, and could provide a nice LDAP solution out of the box.
Plan IIRC is to set that up in a VM and give it a try - if that works, the LDAP mystery would have been solved in parts.
Let's see how this turns out, but it sounds quite promising to me.
In parallel, Alex is in contact with a local FLOSS supporting company who might help us out as well with getting knowledge and up to speed

Also talked to Norbert that investing into getting the knowledge if need be (rather than investing into services and creating bus external factors) sounds sensible

All in all, finally some progress :-)

2021-02-25
Shifting to later due to the infra changes

Re-assigning to Guilhem, who is working on this now

Feel free to update as you see fit and check with Norbert, with whom you've been talking about that item in some detail I guess

Where do we stand wrt. this ticket?

From the top of my head, the system is running, with a small user portal to create accounts, change and recover passwords, and is used in production by a LibO Online instance.

Next step is to give it a test drive with more of our production systems. IIRC Norbert volunteered to try it out with Gerrit.

The wiki might also be a nice testbed.

Now that we moved most services to more modern software, LDAP integration should be easier to handle than before.

Can you give a quick status update, so we can outline the next steps?

Yeah; unfortunately the migrations took most of my time and I had very little time to work on that the last 2-3 months :-/ I hope it'll be a little bit smoother now

TestLink also supports it: https://github.com/TestLinkOpenSourceTRMS/testlink-code/search?utf8=%E2%9C%93&q=ldap

Some status update:

- LDAP self-signup service in place
- LibreOffice online instance connected to it
- TestLink connected to it as well
- gathering further experience and then rolling out to further services like wiki others
• **Getting testers is crucial!** In the past, people were reluctant to migrate their accounts over, and to get some real-life data, we need a critical mass to actually use it

#### #23 - 2017-07-27 16:26 - Jean Spiteri

What is needed to be tested? Can there be any further explanation on how someone can help here?

#### #24 - 2017-07-28 08:51 - Florian Effenberger

What is needed to be tested? Can there be any further explanation on how someone can help here?

So far it's rolled out for TestLink and a LibreOffice online instance. For testing, it'd be great if you could create yourself an account at [https://user.documentfoundation.org](https://user.documentfoundation.org) and see how TestLink works with that, as this is the recent service we've added to SSO.

Thanks a lot!

#### #25 - 2017-11-06 11:04 - Florian Effenberger

- Target version changed from Q3/2017 to Q4/2017

#### #26 - 2017-11-11 02:44 - Thorsten Behrens

Just added some more email addresses, wondering where we are with this? Which services are supposed to work?

#### #27 - 2017-11-11 03:13 - Thorsten Behrens

Oh, and something else - having 2FA available at least if we enable this for gerrit would be good.

- [https://github.com/privacyidea/privacyidea](https://github.com/privacyidea/privacyidea)

#### #28 - 2017-11-13 00:51 - Guilhem Moulin

Thorsten Behrens wrote:

> Just added some more email addresses, wondering where we are with this? Which services are supposed to work?

Tried to give a comprehensive update during my LibCon17 talk (and also to the reports to BoD). In a nutshell, the “Linked Account” section of the frontend is purely informational, it’s there for users to help us with account merging by adding the list addresses they use on all TDF services (the address is verified by the service and also by the SSO frontend so we can tie the profile to the SSO account). We use it to measure adoption among active contributors.

Few services have been entirely migrated to a “real” WebSSO yet (where unauthenticated users are redirected to a central authentication portal, then back to the service after successful authentication). Only LimeSurvey (SAML 2.0), YOURLS, and Etherpad (sub-HTTP requests).

Some services (TDF & Collabora NextCloud, Silverstripe, TestLink) support dual auth method (LDAP binding + internal database) and I’m manually changing changing auth method to LDAP for accounts the email address of which I can find in the LDAP DIT. Not a real SSO solution since users need to authenticate to each service individually (with the same set of credentials from LDAP), and the attack surface is not ideal since a compromise of any service can lead to compromise of SSO credentials. But all accounts need to migrated before we can implement a proper solution using SAML or similar.

Unfortunately we’re still in the poking phase (and finding the thin line between gentle reminders and harassment). The DIT is slowly populating but for instance we still have ⅓ of addresses subscribed to the tdf-members list which are not in LDAP (either as primary or secondary address). I’d like to work on the wiki next; I deployed SAML 2.0 to the testwiki and demo-ed it during my LibOCon17 talk, but last time I checked, of the 400-ish contributors of the past 90 days only 50 or so have a **verified** address in LDAP. So the critical point at which we can lock out users is not quite reached yet.

#### #29 - 2017-11-26 17:43 - Guilhem Moulin

Guilhem Moulin wrote:

> last time I checked, of the 400-ish contributors of the past 90 days only 50 or so have a **verified** address in LDAP. So the critical point at which we can lock out users is not quite reached yet.

After the last infra call Dennis pointed out that we should only count contributors which also made edits (that weren’t deleted afterwards), otherwise end up counting spammers. I count 138 unique such contributors in the last 90 days:
SELECT DISTINCT user_email
FROM user JOIN recentchanges ON user_id = rc_user
WHERE rc_source = "mw.edit"
AND rc_bot = 0
AND rc_deleted = 0
AND user_email_authenticated IS NOT NULL;

of which 60% (83) are not known to LDAP yet. We'll add a banner to the login page before poking users individually.

#30 - 2018-05-09 12:09 - Florian Effenberger
- Target version changed from Q4/2017 to Q2/2018

Users are slow with getting their accounts created
Next set of services we can deploy are Wiki, Silverstripe and Redmine
The plan is to enforce SSO with some heads-up time
In theory, we can disable again if we miss a critical mass, but unless there's really an urgency, this sounds like the way to go to get users migrated to this so they have a need to create their LDAP account

Plan is around early June for the next services to be deployed with SSO

#31 - 2019-07-25 14:35 - Florian Effenberger
- Priority changed from High to Normal
- Target version changed from Q2/2018 to Q3/2019

Wiki, Silverstripe and Redmine are connected in the meantime
Connected is also LimeSurvey, Nextcloud
Pending are WordPress, Jitsi (no auth at all for the moment), Piwik, Bugzilla, AskBot
Weblate will have SSO enabled from the beginning, so will the TSP

#32 - 2020-01-15 12:03 - Florian Effenberger
- Target version changed from Q3/2019 to Q1/2020

Gerrit done as well

#33 - 2020-08-04 17:32 - Florian Effenberger
- Target version changed from Q1/2020 to Q4/2020

- next smaller services, one by one, starting in Q4: Jitsi, maybe Riot, TSP
- next big service: Bugzilla - needs transition period
- not a priority right now, need to plan this in
- Bugzilla 6.0 might provide SSO out of the box, but this has no ETA