Tiki Suite LDAP

LDAP's role is central in ClearOS & Tiki Suite. So here is a page to centralize all documentation & issues. Everything related to LDAP and any component of Tiki Suite (Tiki, Openfire Meetings, Thunderbird, etc.) should be here or a link to it..

Configuring Tiki to work with ClearOS's LDAP

If Tiki is installed on the ClearOS which has OpenLDAP

Works with 12.2: A user enters his own username/password (which are managed in ClearOS), and the user is logged in to Tiki.

- tiki-admin.php: make sure you are not just using basic prefs, but also advanced and even experimental
- tiki-admin.php?page=login -> General preferences -> Authentication Method: Tiki and LDAP
- tiki-admin.php?page=login -> LDAP ->check "Create user if not in Tiki"

For the other settings, no need to change when the Tiki is installed on the same machine as ClearOS

unconfirmed bug with 12.0 and 12.1: http://dev.tiki.org/item4816

2014-07-30: old test server with latest 12.x and clearos-updates-testing (thus latest code of ClearOS 6.6) -> Activating "Use SSL (ldaps)" (auth_ldap_ssl) breaks the authentication for users.

Latest 12.x from 2014-08-15: This config works for authentication, and the sync of Real name, country and email, but not groups

If Tiki and ClearOS-LDAP are on different servers

tips from Peter 2014-02-25

> For security reasons, anonymous binds are only allowed from localhost. To allow anonymous binds from remote connections, change the last configuration block in /etc/openldap/slapd.conf from: access to * by self write by peername.ip=127.0.0.1 read by * none stop To: access to * by self write by * read by * none stop And restart LDAP: service slapd restart The Tiki configuration is almost the same as the attached screenshot. Changes: - Hostname - Port (636) - Use SSL (enabled) - Base DN (whatever it is on the remote LDAP server)

No such attachment on this page

Old info (still valid?) "If the site is accessible via LDAPS, you need to use the port 636, otherwise the port 389. In this situation you can still access from the same server ldaps via 389 "Publish Policy" to "Local Network". This will set LDAP to listen for incoming requests on your LAN interface. See also: http://doc.tiki.org/LDAP+authentication#Certificate_Problems"

Peter Baldwin (2014-03-04) wrote:

> *TLS on http://demo.tiki.org*
>
> *For some reason, I am unable to enable SSL support in the Tiki LDAP settings. I see a TLS error in the old test server LDAP logs, but I have no idea what's going on the client side. Any clues to what is happening on the client side? It has something to do with the client-side SSL/TLS settings (Ubuntu?). I can't duplicate this issue in my development environment (a ClearOS client).*

Todos

Solve binding

Advice from Peter (ClearOS) wrote:

> *It does not look like the LDAP connector in Tiki Wiki includes native support for the "LDAP Bind Type". It uses the following format for authenticating users:*
>
> ***uid=test**,ou=Users,ou=Accounts,dc=clear6,dc=lan*
>
> *But ClearOS uses:*
>
> ***cn=test guy3**,ou=Users,ou=Accounts,dc=clear6,dc=lan*
>
> *Why does ClearOS use a full name instead of a username? The gory technical details are explained by David in this bug report:*
>
> *http://tracker.clearfoundation.com/view.php?id=129*
>
> *I can probably hack the code to add a new "LDAP Bind Type". I'll give it a try.*

So it looks like we need a new ClearOS "bind_type" in lib/auth/ldap.php

Here are some tests as per the script at: http://doc.tiki.org/LDAP+authentication#Debugging
old test server/connect_as_manager.php
old test server/connect_as_tesla.php

Sync user data from ClearOS-LDAP to Tiki upon login

According to http://doc.tiki.org/LDAP+authentication#How_it_works, all this should work if properly configured. Perhaps by solving the binding above, it will all work? 😀

- Users full name
- Users email address
- Users country information
- Users group membership
- Group name and description

Should there be a "create group if it doesn't exist" option? So Tiki wouldn't be polluted by unused groups from LDAP.

Sync OpenLDAP & Tracker data

- It's all documented here: LDAP Tracker Field
  - But binding doesn't seem to work: old test server/tiki-admin_dsn.php

Solve TLS issue

- There is a fix which breaks things for others (ask Marc for details)

Forgot my password

- Tiki has such a feature: tiki-remind_password.php
- How can this work if password is not managed in Tiki, but in ClearOS-LDAP? (You can just turn off this feature in Tiki, but the admin panel should give you a warning)
  - To make things more tricky, it's actually possible that some users are managed in Tiki, and the rest in ClearOS-LDAP

Prevent naming conflicts

In terms of sync of users/groups between ClearOS & Tiki, analyze & document any limitation to avoid future issues

- See ClearOS conventions for usernames & passwords
- In Tiki, groups can have the same name as a user, but not in ClearOS
- In TIki, restrictions on usernames are configurable. See tiki-admin.php?page=login -> General preferences -> Username
  - Use email as username
  - Minimum & Maximum length
  - Force lowercase
  - Username pattern

Self-registration via Tiki

A note from Peter (ClearOS)

> What happens with LDAP if it's a Tiki-powered site that users self-register? One option: hook into the ClearOS API. A code example looks something like: $user = User_Factory::create('test_user'); $user_info['core']['first_name'] = 'Test'; $user_info['core']['last_name'] = 'User'; $user->add($user_info, 'password'); You can add e-mail addresses, and whatever other data you see in the web-based interface. The API is agnostic to the accounts engine (notably, OpenLDAP and Samba 4 Directory).

Make a Tiki Suite profile

With all the optional configuration at tiki-admin.php?page=login (LDAP tab), improve Tiki Suite profile.

FreeSWITCH

This is for later. Here are some notes

- Small proof of concept for FreeSWITCH
- Blue.box feature request
- FusionPBX feature request
- https://wiki.freeswitch.org/wiki/Mod_ldap

SabreDAV

SabreDAV could be interesting for ClearOS and Tiki (already in Kolab)

- http://tracker.clearfoundation.com/view.php?id=1260
- LDAP backend for contacts with SabreDAV (which could be included in Tiki)

Documentation

- LDAP authentication
- LDAP Tracker Field How to sync data from OpenLDAP to Tiki Trackers (Tiki's database & form generator)
- A nice guide: http://wiki.gentoo.org/wiki/Centralized_authentication_using_OpenLDAP
- Tiki LDAP FAQ
- http://www.clearcenter.com/support/documentation/user_guide/directory_server
- http://www.clearcenter.com/support/documentation/clearos_guides/accessing_ldap_data
- http://www.clearfoundation.com/docs/howtos/connect_jitsi_to_clearos_directory
- http://www.clearfoundation.com/docs/howtos/connect_thunderbird_to_clearos_directory
- http://www.clearfoundation.com/docs/howtos/phpldapadmin
- http://plugins.piwik.org/LoginLdap

Forums

- ClearOS LDAP forum

- Tiki LDAP forum

Feature requests & bug reports

- LDAP Sync Not working Correctly **Important to check this one**
- LDAP External Groups Being Flagged as Internal
- Add Global Address Book app
- Review state of /etc/openldap/ldap.conf
- Investigate the addition of a Single Sign On (SSO) solution
- Templatable default e-mail address
- phpLDAPadmin reports: "Automatically removed attribute or objectClass from template"
- https://dev.tiki.org/External+Authentication

Developer info

Any development should be done in trunk, and backported to 12.x LTS and/or 13.x if relevant. See Where to commit

- http://sourceforge.net/p/tikiwiki/code/HEAD/tree/branches/12.x/doc/devtools/tiki-sync_ldap.php
  - Should this be on a cron job?
- http://sourceforge.net/p/tikiwiki/code/HEAD/tree/branches/12.x/lib/auth/ldap.php
- http://sourceforge.net/p/tikiwiki/code/HEAD/tree/branches/12.x/lib/userslib.php
- http://sourceforge.net/p/tikiwiki/code/HEAD/tree/branches/12.x/lib/core/Tracker/Field/Ldap.php
- tiki-syslog.php entries can give very useful info when moused over
  - tiki-admin.php?page=login -> LDAP -> Write LDAP debug Information in Tiki Logs Reset to default
- As of Tiki12, vendor_extra/pear/Net/LDAP2.php is used.
  - "This package is not maintained"
  - Zend\Ldap is an alternative
  - Tiki 12.x has version 2.0.9 (2010-02-16), and there are several newer versions available
    - https://packagist.org/packages/zendframework/zend-ldap

Related tools

https://www.fusiondirectory.org/
https://www.openhub.net/p/compare?project_0=phpLDAPadmin&project_1=LDAP+Account+Manager&project_2=LdapSaisie