

Guide de l'administrateur

Généralités

Larpe est un reverse proxy (mandataire inverse) Liberty Alliance. Il permet à n'importe quel fournisseur de services d'utiliser les fonctionnalités Liberty Alliance (fédération d'identité, Single Sign-On et Single Logout) sans avoir à modifier le code du fournisseur de service lui-même. Il repose sur la bibliothèque Lasso, certifiée par le consortium Liberty Alliance.

Licences

Lasso et Larpe sont publiés selon les termes de la [licence GNU GPL](#).

Sites testés avec Larpe

Les moteurs de sites suivants ont été testés et fonctionnent parfaitement avec Larpe (liste non exhaustive) :

- Mediawiki (ex: <http://fr.wikipedia.org/wiki/Accueil>) ;
- Sympa (ex : <http://demo.sympa.org/sympa>) ;
- Egroupware (ex: http://www.stylite.de/egroupware_demo) ;
- Docuwiki (ex: <http://www.dokuwiki.org/dokuwiki>) ;
- GForge (ex: <http://gforge.org/gf/project/test/>) ;
- Dacode (ex: <http://linuxfr.org/pub/>) ;
- Iconito (ex: <http://demo.iconito.fr/index.php?module=kernel>) ;
- Espace-famille Concerto (ex: <http://demonstration.espace-famille.net/demo/index.do>) ;
- Agirhe (ex: <http://www.agirhe-cdg.fr/accueil.aspx>) ;
- Ciril net RH ;
- Integra RH (Pré-remplissage de formulaires) ;

ainsi que d'autres sites spécifiques et non publics.

Installation

Logiciels requis

Larpe a besoin des logiciels suivants :

- Lasso (0.6.3 ou ultérieur) avec ses bindings Python ;
- Python (2.3 ou ultérieur) ;
- Python CGI ;
- Quixote (2.0 ou ultérieur) ;
- Apache (2.0 ou ultérieur) et les modules suivants : * Proxy ; * Proxy HTML ; * Proxy HTTP (pour Apache 2.2 uniquement) ; * CGI ; * Python ; * Rewrite ; * Headers ;
- libxml2.

Vous avez également besoin d'un fournisseur d'identité Liberty Alliance, installé sur le même serveur ou non. Nous recommandons [Authentic](#) pour cet usage.

Installation sur Debian GNU/Linux Sarge

Ajoutez la ligne suivante dans le fichier

```
/etc/apt/sources.list
```

, cela vous donnera l'accès au dépôt où le paquet Larpe se trouve :

```
deb http://deb.entrouvert.org/ sarge main
```

En tant que root tapez :

```
# apt-get update
# apt-get install larpe
```

Installation sur une autre distribution GNU/Linux

Commencez par installer ces logiciels :

- Python (2.3 ou ultérieur) ;
- Python SCGI ;
- Apache (2.0 ou ultérieur) et les modules suivants : * Proxy HTML ; * SCGI ; * Python ;
- libxml2.

Téléchargez et installez ensuite ces logiciels supplémentaires :

- [Lasso](#) ;
- [Quixote](#) ;
- [Larpe](#).

Décompressez les sources que vous avez téléchargées :

```
$ tar xzf larpe*.tar.gz
$ cd larpe*
```

Contrôlez les quelques variables au début du Makefile et modifiez les si nécessaire. Puis pour installez Larpe, en tant que root :

```
# make install
```

Larpe est alors installé mais pas encore configuré. Vous pouvez le lancer avec :

```
# su www-data
$ /usr/sbin/larpectl.py start
```

Vous pouvez créer un script init.d pour le lancer au démarrage.

Pour désinstaller Larpe, tapez en tant que root :

```
# make uninstall
```

Configuration d'Apache 2

Préambule pour les distributions autres que Debian

Chargez les modules Apache 2 suivants, avec les outils propres à votre distribution :

- proxy ;
- proxy_html ;
- proxy_http (Apache 2.2 uniquement) ;
- scgi ;
- mod_python ;
- rewrite ;
- headers.

Si c'est votre première installation de Larpe, le fichier /etc/apache2/sites-available/apache2-vhost-larpe n'existe pas. Copiez le depuis les sources de Larpe en tant que root :

```
# cp apache2-vhost-larpe /etc/apache2/sites-available/apache2-vhost-larpe
```

Pour toute les distributions

Éditez le fichier /etc/apache2/sites-available/apache2-vhost-larpe pour configurer Apache 2 pour Larpe. Vous verrez ces lignes :

```
ServerName localhost
ServerAdmin root@localhost
```

Remplacez ces valeurs par votre nom de domaine pour Larpe et votre adresse email. Il se peut que vous deviez changer également cette ligne en fonction de votre configuration Apache2 :

```
<VirtualHost *:80>
```

Si le nom d'hôte que vous avez choisi n'est pas dans votre DNS, n'oubliez pas d'ajouter une entrée dans votre fichier `/etc/hosts`. Si vous souhaitez utiliser SSL (https) pour Larpe ou pour n'importe quel site configuré dans Larpe, il vous faudra configurer le support SSL dans votre serveur Apache2 en premier lieu. Activez cet hôte virtuel en tant que root :

```
# a2ensite apache2-vhost-larpe
```

Vous pouvez recharger apache (toujours en tant que root). Avec la plupart des distributions, c'est :

```
# /etc/init.d/apache2 reload
```

Dans Fedora :

```
# /etc/init.d/httpd reload
```

Larpe fonctionne, l'interface d'administration est accessible <http://votre-nom-de-domaine/admin/>.

Larpe

- Hôtes
- Utilisateurs
- Paramètres
- Journaux

Administration

Relais inverse Liberty Alliance

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 59 Temple Place - Suite 330, Boston, MA 02111-1307, USA.

Configuration de Larpe

Configuration du fournisseur d'identité

Si vous ne disposez pas encore d'un fournisseur d'identité, vous pouvez installer [Authentic](#).

Vous trouverez des informations sur la façon d'installer et de configurer Authentic dans le [Guide de l'administrateur Authentic](#). Dans l'interface d'administration de Larpe, cliquez sur "Paramètres", puis sur "Fournisseur d'identité".

Larpe

- Hôtes
- Utilisateurs
- Paramètres
- Journaux

Administration > Paramètres

Paramètres

Nouveau fournisseur d'identité

Méta-données ■

Parcourir...

Clé publique

Parcourir...

Chaîne de certification

Parcourir...

Valider

Indiquez l'endroit où se trouve le fichier de metadata de votre fournisseur d'identité puis cliquez sur Valider. Votre fournisseur d'identité est maintenant configuré dans Larpe, vous pouvez configurer autant de fournisseurs de service que vous le souhaitez.

Configuration d'un fournisseur de service

Afin de restreindre l'accès à l'interface d'administration de Larpe, vous devez configurer Larpe en tant que fournisseur de service. Cliquez sur "Paramètres", puis sur "Fournisseur de service".

Larpe

[Administration](#) > [Paramètres](#)

Paramètres

Configuration du fournisseur d'identité

Nom de l'organisation ■

[Valider](#) [Annuler](#)

[Hôtes](#)
[Utilisateurs](#)
[Paramètres](#)
[Journaux](#)

Saisissez un "Nom d'organisation" puis cliquez sur Valider. Sauvegardez les metadata du fournisseur de service en faisant un clic droit puis "enregistrer sous" (elle concerne ID-FF 1.2). Configurez ce fournisseur de service sur votre fournisseur d'identité à l'aide du fichier de metadata.

Création d'un compte utilisateur

Maintenant, vous pouvez créer un utilisateur qui aura les droits d'accès à l'interface d'administration. Dans l'interface d'administration de Larpe, cliquez sur "Utilisateurs", puis "Nouvel utilisateur".

Larpe

[Administration](#) > [Utilisateurs](#) > [Nouveau](#)

Utilisateurs

Nouvel utilisateur

Nom de l'utilisateur ■

Courriel

[Valider](#) [Annuler](#)

[Hôtes](#)
[Utilisateurs](#)
[Paramètres](#)
[Journaux](#)

Saisissez un nom et éventuellement un courriel. Cliquez sur le bouton "jeton" (l'engrenage), sur le bouton "générer", puis sur le bouton "envoyer par courriel". Ensuite, lisez le mail reçu et cliquez sur le lien qu'il contient. Un single Sign-On sera initié avec le fournisseur d'identité. Si vous n'étiez pas encore authentifié, votre mot de passe vous est demandé. Votre compte est alors fédéré et l'accès à l'interface d'administration est restreint.

Configuration de l'hôte

Cette section détaille comment configurer un nouveau fournisseur de services (aussi appelé hôte) en utilisant Larpe.

Paramètres de l'hôte

Cliquez sur "Hôte" puis sur "Nouvel Hôte".

Hôtes

Nouvel hôte

Nom du site ■

Adresse racine du site d'origine ■

Page d'authentification

S'il y a une page d'authentification séparée

Page du formulaire d'authentification

Si le formulaire d'authentification n'est pas dans une page séparée et pas non plus dans la page d'adresse de déconnexion

Adresse de déconnexion

Nom d'hôte inversé (sur le relais inverse) ■

Répertoire inversé (sur le relais inverse)

Utiliser SSL

☐

Cela concerne uniquement la connexion entre le navigateur et Larpe

Valider

Annuler

Saisissez les paramètres suivants :

- Nom du site : Le nom que vous voulez donner au fournisseur de service ;
- Adresse racine du site original : l'URL racine de votre fournisseur de service. Si l'URL est du genre <http://sp.example.com/index.html>, saisissez simplement <http://sp.example.com/> ;
- Page d'authentification : si la page qui contient le formulaire d'authentification est sur une page séparée, saisissez son adresse ici ;
- Page contenant le formulaire d'authentification : si vous n'avez pas rempli le champ précédent et que le formulaire d'authentification ne se trouve pas sur la page racine, saisissez l'URL de la page contenant le formulaire d'authentification ici ;
- Adresse de Logout : adresse de Logout du site original qui permettra de bénéficier du Single Logout ;
- Nom d'hôte inversé : le nom de domaine que vous voulez utiliser pour accéder à votre fournisseur de service à travers le reverse proxy. Si vous utilisez le nom de domaine de Larpe ici, vous devez choisir également un répertoire inverse ;
- Répertoire inverse : un sous-répertoire où vous voulez pouvoir accéder à votre fournisseur de service à travers le reverse proxy. Si vous mettez en place ce répertoire, votre fournisseur de service sera accessible à http://reversed_host_name/reversed_directory/. Si vous ne le faites pas, il sera accessible à http://reversed_host_name/. Cliquez sur Valider. Vous verrez tous les paramètres courants concernant cette hôte. Votre nouvel hôte n'est probablement pas configuré complètement pour le SSO mais vous devriez d'ores et déjà pouvoir accéder à sa page d'accueil. Si vous avez un message d'avertissement stipulant qu'il n'est pas encore totalement configuré, ignorez le provisoirement pour vérifier que le site est accessible. Ajoutez ce nouveau nom d'hôte à votre DNS (ou localement à /etc/hosts). Cliquez ensuite sur "Nouvelle URL pour cet hôte" pour vérifier que vous pouvez y accéder.

Exemple d'hôte : Linuxfr

Pour vous aider à configurer votre propre fournisseur de service, nous fournissons un exemple d'un service fonctionnel. Pour paramétrer Linuxfr, saisissez les éléments suivants :

- Nom du site : Linuxfr ;
- Adresse racine du site original : <http://linuxfr.org/> ;
- Page d'authentification : rien ici ;

- Page contenant le formulaire d'authentification : <http://linuxfr.org/pub/> ;
- Adresse de Logout : http://linuxfr.org/close_session.html ;
- Nom d'hôte inversé : linuxfr.reverse-proxy.example.com ;
- Répertoire inverse : rien ici.

Avec "reverse-proxy.example.com" comme nom d'hôte paramétré préalablement pour votre reverse proxy. N'oubliez pas d'ajouter ce nouvel hostname à votre DNS (ou localement à votre fichier /etc/hosts). Vous pouvez alors aller sur Linuxfr <http://linuxfr.reverse-proxy.example.com/>

Paramétrage final de l'hôte

Vous pouvez maintenant accéder à votre fournisseur de service, il reste une dernière étape pour utiliser les fonctionnalités Liberty Alliance. Cliquez sur "Hôtes", puis sur l'icône d'édition du fournisseur de service concerné. Sauvegardez les metadata du fournisseur de service en faisant un clic droit puis "enregistrer sous" (elle concerne ID-FF 1.2). Configurez ce fournisseur de service sur votre fournisseur d'identité avec ce fichier de metadata.

Fichiers

larpe-admin.png	44,6 ko	22 avril 2011	Jérôme Schneider
larpe-host-new.png	38,2 ko	22 avril 2011	Jérôme Schneider
larpe-idp.png	20,9 ko	22 avril 2011	Jérôme Schneider
larpe-sp-new.png	16,6 ko	22 avril 2011	Jérôme Schneider
larpe-user-new.png	17 ko	22 avril 2011	Jérôme Schneider

Larpe2

- Réécrire complète
- Utilisation de Django
- Utilisation d'apache ????
- Organisation d'un EO camp pour lancer le mouvement ?

Larpe Administrator Guide

Overview

Larpe is a Liberty Alliance Reverse Proxy. It allows any service provider (that is a website) to use Liberty Alliance features (Identity federation, Single Sign On and Single Logout) without changing the code of the service provider itself. It uses the Lasso library which is certified by the Liberty Alliance consortium.

Licenses

Lasso and Larpe are released under the terms of the [GNU GPL license](#).

Sites tested with Larpe

The following site engines have been tested and fully work with Larpe (non-exhaustive) :

- Mediawiki (ex: <http://fr.wikipedia.org/wiki/Accueil>) ;
- Sympa (ex : <http://demo.sympa.org/sympa>) ;
- Egroupware (ex: http://www.stylite.de/egroupware_demo) ;
- Docuwiki (ex: <http://www.dokuwiki.org/dokuwiki>);
- GForge (ex: <http://gforge.org/gf/project/test/>) ;
- Dacode (ex: <http://linuxfr.org/pub/>) ;
- Iconito (ex: <http://demo.iconito.fr/index.php?module=kernel>) ;
- Espace-famille Concerto (ex: <http://demonstration.espace-famille.net/demo/index.do>) ;
- Agirhe (ex: <http://www.agirhe-cdg.fr/accueil.aspx>) ;
- Ciril net RH ;
- Integra RH (Pré-remplissage de formulaires) ;

as well as other specific and not public sites.

Installation

Required softwares

Larpe needs the following softwares:

- Lasso (0.6.3 or later) with its Python binding;
 - Python (2.3 or later);
 - Python CGI;
 - Quixote (2.0 or later);
 - Apache (2.0 or later) and the following modules: * Proxy; * Proxy HTML; * Proxy HTTP (for Apache 2.2 only); * CGI; * Python; * Rewrite; * Headers;
 - libxml2.
- You will also need a Liberty Alliance Identity Provider, be it on the same server or not. We recommend [[<http://authentic.labs.libre-entreprise.org/Authentic>]] for that need.

Installation on Debian GNU/Linux Sarge

Add the following line in the file /etc/apt/sources.list, this will give you access to the repository where Larpe is stored:

```
deb http://deb.entrouvert.org/ sarge main
```

As root type:

```
# apt-get update
# apt-get install larpe
```

Installation on another GNU/Linux distribution

First install these softwares:

- Python (2.4 or later);
- Python CGI;
- Apache (2.0 or later) and the following modules: * Proxy HTML; * CGI; * Python;
- libxml2.

Then download and install these additional softwares:

- [Lasso](#)
- [Quixote](#)
- [Larpe](#)

Uncompress the sources you have downloaded

```
$ tar xzf larpe*.tar.gz
$ cd larpe*
```

Check the few variables at the beginning of the Makefile and change them if needed.

Then install Larpe, as root:

```
# make install
```

Larpe is installed (but not configured yet), you can run it with:

```
# su www-data
$ /usr/sbin/larpectl.py start
```

You may want to create an init.d script to start it at boot time later.

When you want to uninstall Larpe, just type, as root:

```
# make uninstall
```

Apache 2 configuration

Preamble for other distributions than Debian

Load the following Apache 2 modules, using your distribution specific tools :

- proxy;
- proxy_html;
- proxy_http (for Apache 2.2 only);
- scgi;
- mod_python;
- rewrite;
- headers.

If it is your first installation of Larpe, the file `/etc/apache2/sites-available/apache2-vhost-larpe` will not exist. Copy it from Larpe sources, as root:

```
# cp apache2-vhost-larpe /etc/apache2/sites-available/apache2-vhost-larpe
```

For all distributions

Edit the file `/etc/apache2/sites-available/apache2-vhost-larpe` to configure Apache 2 for Larpe. You will see these lines:

```
ServerName localhost
ServerAdmin root@localhost
```

Replace these values with your domain name for Larpe and your email address.

You may also need to change this line, depending on your general Apache 2 configuration:

```
<VirtualHost*:80>
```

If the hostname you chose is not served by your DNS, don't forget to add an entry to your `/etc/hosts` file.

If you intend to use SSL (https) for Larpe or for any site you will configure in Larpe, you will have to configure SSL support on your Apache 2 server first.

Activate this virtual host, as root:

```
# a2ensite apache2-vhost-larpe
```

You can then reload Apache (still as root). In most distributions, it is:

```
# /etc/init.d/apache2 reload
```

In Fedora:

```
# /etc/init.d/httpd reload
```

Larpe now works, the administration interface is reachable at http://your_domain_name/admin/.

[Hosts](#)[Users](#)[Settings](#)[Logs](#)[Administration](#)

Liberty Alliance Reverse Proxy

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 59 Temple Place - Suite 330, Boston, MA 02111-1307, USA.

Larpe configuration

Identity Provider configuration

If you don't have an Identity Provider yet, you can install [Authentic](#). You can find information to install and configure it on [Authentic manual](#).

In Larpe administration interface, click on "Settings", then "Identity Provider".

[Hosts](#)[Users](#)[Settings](#)[Logs](#)[Administration](#) > [Settings](#)

Settings

New Identity Provider

Metadata ■

 [Parcourir...](#)

Public Key

 [Parcourir...](#)

CA Certificate Chain

 [Parcourir...](#)

Fill in the metadata file that you've got from your Identity Provider then click Submit. Your Identity Provider is now configured in Larpe, you can then configure as many Service Providers as you want.

Service Provider configuration

In order to restrict access to Larpe administration, you must configure Larpe as a Service Provider.

Click on "Settings", then "Service Provider".

Larpe

[Administration](#) > [Settings](#)

Settings

Service Provider Configuration

Organisation Name ■

Fill an "Organisation Name" then click "Submit".

Save the Service Provider Metadata (for ID-FF 1.2) (right click then "Save as"). Configure this Service Provider on your Identity Provider with this metadata file.

Creation of a user account

Now, you must create a user account, who will be given access rights on the administration interface.

In Larpe administration interface, click on "Users", then "New User".

Larpe

[Administration](#) > [Users](#) > [New](#)

Users

New User

User Name ■

Email

Give it a name and optionnaly his email address.

Then click on the "token" button (with gear icon), then "generate" button, then "send by email" button.

After that, get your email on the address you just gave, and click on the link in this email.

A Single Sign On will be initiated to the Identity Provider. If you, or the user you created the account for, were not authenticated yet, it will ask for your password. After that, your account is federated, and the administration interface will be restricted.

Next time you go unauthenticated on the administration interface, it will initiate an SSO to the identity provider as well.

Host configuration

This section explains how to configure new Service Providers (also named "Hosts") with Larpe.

Host settings

Click on "Hosts" then "New Host".

Hosts

New Host

Site name ■

Original site root address ■

Authentication page

If there is a separate authentication page

Authentication form page

If the authentication form is not in a separate page and not in the index page either

Logout address

Reversed host name ■

Reversed directory

Use SSL

☐

This only affects the connection between the browser and Larpe

Fill in the following parameters:

- Site name : the name you want to give to your Service Provider;
 - Original site root address : the root url of your Service Provider. If the url of your main page is something like <http://sp.example.com/index.html>, just put <http://sp.example.com/>;
 - Authentication page: if the page which contains the authentication form for your Service Provider is on a separate page, fill the url of this page here;
 - Authentication form page: if you didn't fill the previous field and if the authentication form is not on the first page of your Service Provider either, fill the url of the page which contains the authentication form here;
 - Logout address : when you want Single Sign On and Identity Federation, you probably want Single Logout too. If so, fill the logout url of your original site here;
 - Reversed host name : the domain name where you want to access your Service Provider through the reverse proxy. If you use Larpe's domain name here, you must set a reversed directory;
 - Reversed directory : a subdirectory where you want to access your Service Provider through the reverse proxy. If you set a reversed directory, your service provider will be accessible at http://reversed_host_name/reversed_directory/. If you don't set one, it will be accessible at http://reversed_host_name/.
- Then click "Submit".

You will see all the current parameters for this host. Your new host is probably not fully configured for SSO but you should already be able to access its home page. If you have a warning message telling it's not fully configured, just ignore it for the moment and check if this host is accessible already:

Add this new hostname to your DNS (or locally in /etc/hosts).

Then click on the "New url for this host" field on the current page to check you can access this new host.

Host example : Linuxfr

To help you setup your own Service Provider, we provide an example of a working Service Provider to guide you.

To setup Linuxfr, fill in the following parameters:

- Site name: Linuxfr;

- Original site address : <http://linuxfr.org/>;
 - Authentication page: Nothing here;
 - Authentication form page: <http://linuxfr.org/pub/>;
 - Logout address: http://linuxfr.org/close_session.html;
 - Reversed host name: linuxfr.reverse-proxy.example.com;
 - Reversed directory: Nothing here.
- With "reverse-proxy.example.com" being the hostname you've set up before for your reverse-proxy.

Don't forget to add this new hostname to your DNS (or locally in /etc/hosts) as well.

You can then go to the reversed Linuxfr at <http://linuxfr.reverse-proxy.example.com/>.

Host final setup

Now that you can access your Service Provider, you need a final step to use Liberty Alliance features. Click on "Hosts", then click on the "Edit" icon of the Service Provider you've just configured. Save the Service Provider Metadata (for ID-FF 1.2) (right click then "Save as"). Configure this Service Provider on your Identity Provider with this metadata file.

Fichiers

larpe-admin.png	44,6 ko	21 avril 2011	Jérôme Schneider
larpe-host-new.png	34,3 ko	21 avril 2011	Jérôme Schneider
larpe-idp-new.png	19,7 ko	21 avril 2011	Jérôme Schneider
larpe-sp-new.png	16,9 ko	21 avril 2011	Jérôme Schneider
larpe-user-new.png	14,5 ko	21 avril 2011	Jérôme Schneider

Larpe

What is Larpe?

Larpe is a Liberty Alliance Reverse Proxy. It allows any service provider (that is a website) to use Liberty Alliance features (Identity federation, Single Sign On and Single Logout) without changing the code of the service provider itself. Its Liberty Alliance compliance relies on Lasso, a free (GNU GPL) implementation of the Liberty Alliance specifications.

It is a Quixote application and is commonly run inside Apache web server.

Features

- Neat and simple administration interface;
- SAML 2.0 support;
- Liberty Alliance ID-FF 1.2 support;
- Allows the integration of a service within a circle of trust in some hours;
- Entirely graphical configuration of the service provider without fiddling with its code;
- Automatically generated metadatas;
- Logs and Audit : Logs are displayed within the administration interface. They deliver informations about different types of events.

Documentation

- [Larpe Administrator Guide](#) (English)
- [Guide de l'administrateur](#)

Download

The most recent version of Larpe is 1.1.1 and was released on July 20th 2010.

Source

- Latest stable version: [larpe-1.1.1.tar.gz](#)
- Development version (git read only repository)

```
git clone http://repos.entrouvert.org/larpe.git
```

Contact

You can contact us on [Larpe mailing list](#)

Future

- [Larpe2](#) Description of the future Larpe based on Django