Architecture

U-Auth est une application web, fournisseur de service de la fédération Renater. U-Auth affiche les IdP de la fédération et propose à l'utilisateur de lancer le SSO sur l'IdP de son choix.

U-Auth pilote un serveur LDAP. Un compte aléatoire est créé pour chaque utilisateur dès qu'il réussi son authentification via un IdP de la fédération.

Un serveur Radius est configuré pour diffuser les identités du serveur LDAP.

Le portail captif qui désire utiliser U-Auth est configuré pour :

- afficher la page de connexion de U-Auth à la place de la sienne (redirection HTTP, ou sinon dans le HTML)
- utiliser le serveur radius.

Une fois la connexion réussie et le compte LDAP crée, U-Auth envoie les données de connexion au portail captif (par un POST via le client wifi).

Le portail captif interroge alors le radius avec les données du compte. Radius vérifie l'information sur le LDAP et confirme l'accès au portail captif.

Pré-requis sur le portail captif (intégré ou non au contrôleur)

Cette architecture implique que le portail captif de départ sache faire de l'UAM (https://en.wikipedia.org/wiki/Universal_access_method) :

- rediriger sa page d'accueil de login vers une URL externe (redirect HTTP, sinon redirection dans le HTML (meta http-equiv="Refresh") voire javascript)
- accepter un POST login + mot de passe

Exemples de portails captifs UAM : PacketFence, Cisco Meraki, pfSense, … Si vous avec un portail captif et que vous désirez savoir s'il est compatible U-Auth (UAM), contactez Entr'ouvert.

Cinématique

Error executing the **plantuml** macro (Missing partial wiki_external_filter/_macro_image with {:locale=>[:en], :formats=>[:pdf], :variants=>[], :handlers=>[:raw, :erb, :html, :builder, :ruby, :rsb]}. Searched in: * "/usr/share/redmine/plugins/wiki_external_filter/app/views" * "/usr/share/redmine/plugins/wiki_external_filter/app/views" * "/usr/share/redmine/plugins/redmine_entrouvert/app/views" * "/usr/share/redmine/plugins/plantuml/app/views" * "/usr/share/redmine/plugins/localizable/app/views" * "/usr/share/redmine/app/views")

Notes

- L'utilisation d'un LDAP permet d'utiliser un portail captif utilisant des comptes LDAP au lieu de radius.
- Les comptes invités sont des comptes directement gérés dans U-Auth.

Backoffice pour un site (un établissement)

Un site (typiquement, un établissement) qui utilise U-Auth, dispose d'un accès à un backoffice dédié pour :

- indiquer les IdP qu'il veut utiliser parmi ceux de la fédération (accès "administrateur du site")
- gérer des comptes invités (accès "gestionnaire d'invités")
- modifier des éléments de présentation de la page d'accueil (logotypes, textes, css, ...)

Système d'administration

Le "super administration" d'U-Auth crée les site et les comptes backoffice correspondants.