Présents : Frederick Bigrat, Jean-Marc Liger, Mikaël Ates, Pierre Cros, Dominique Launay, Mehdi Hached, Olivier Salaün

Le projet à été baptisé Univnautes et la liste univnautes@listes.entrouvert.com sera la liste de messagerie du projet.

Présentations

Entr'ouvert

Entr'ouvert a presenté l'équipe intervenant sur le projet :

- Pierre Cros : Gestion de projet relationnel
- Mikaël Ates : Gestion de projet technique
- Benjamin Dauvergne : En charge de la shibbolethisation de pfsense.
- Frédéric Péters : En charge de l'interface graphique
- Jérôme Schneider : Packaging, Maintien des plateformes de développement
  Entr'ouvert a par ailleurs évoqué l'arrivée sur le projet de Thomas Noël, Administrateur système et développeur, spécialiste du monde universitaire.

UNPIdF et partenaires

Frederick Bigrat a présenté l'UNPIdF et les partenaires impliqués dans le projet, en particulier les gens des projets Eduspot, Eduroam et le Siris. Chaque participants à la réunion a présenté son organisme/projet. Il y aura 6 ou 7 établissements partenaires supplémentaires dont le choix est en cours.
Olivier Salaün a présenté plus en détail le projet Eduspot, portail captif ayant pour SSID Eduspot et promouvant des règles communes pour tous ses membres en mettant l'accent sur la fédération d'identité.
Eduspot va suivre de très près le projet Univnautes : si celui-ci est jugé convaincant, la solution développée pourrait être retenue par Eduspot dans le cadre d'un déploiement universitaire large, voire au-delà. Olivier Salaün a d'ailleurs offert son aide sur les problématiques d'interopérabilité Lasso - Sibboleth.

Méthode de développement et de gestion de projet

Entr'ouvert utilise des méthodes de développement inspirés des méthodes agiles, itératives, qui valorisent les contacts fréquents et informels entre les différents partenaires.
Les réunions se tiendront à chaque fois qu'un des deux partenaires en exprimera le souhait et le compte-rendu des réunions se fera sur le wiki d'Entr'ouvert.

Présentation générale de la solution

Mikaël Ates a présenté la solution et ses 4 axes majeurs :

- Utilisation de pfSense, solution implémentant nativement l'ensemble des fonctionnalités nécessaires ;
- Assurer la compatibilité Shibboleth de pfSense grâce à la bibliothèque certifiée SAML 2.0 Lasso ;
- Remplacer l'interface de pfSense par une interface spécifique développée avec Django et modernisée ;
- Utiliser Nagios pour la supervision.

Points de vigilance

- Il a été rappelé que la solution ne devait pas être intrusive pour les fournisseurs d'identité (IdP), ne pas nécessiter de configuration complexe sur ces derniers. Entr'ouvert a confirmé que ses "bonnes pratiques" dans le cadre du déploiement de solutions samelisées interdisaient de déporter la complexité de la configuration au niveau de l'IdP.
- Entr'ouvert a rappelé que le projet ne portait pas sur le matériel. Pourtant, un certain de nombre de contrôleurs embarquent nativement un portail captif dont il faudra vérifier qu'il peut être désactivé.
- Concernant les logs, Entr'ouvert devra insister, lors de la présentation aux établissements partenaires, sur le fait que les logs des contrôleurs pourront être remontés vers le logiciel de supervision Nagios en utilisant le protocole SNMP. Il est important de montrer que le portail captif peu fonctionner en bonne intelligence avec le contrôleur.
- Dominique Launay a posé des questions concernant la sécurité et la possibilité en particulier d'une attaque de type "Man in the middle" ou ARP poisonning. Il a insisté sur la nécessité de mettre des listes ACL sur la borne et de ne pas permettre le dialogue direct entre machines. Mikaël Ates a indiqué qu'Entrouvert pouvait maintenir un document recensant quelques recommandations visant à assister les administrateurs dans la sécurisation de leur réseau.

Communication

Le projet est stratégique pour l'UNPIdF et sera accompagné d'une campagne de communication conséquente. Entr'ouvert accompagnera, à son niveau, cet effort de communication et profitera de ses nombreux contacts dans l'univers du logiciel libre pour contribuer à sa notoriété. Il y aura en particulier une journée d'étude consacrée à la gestion d'identité organisée par le Comité Réseau Université le 24 janvier. Même si celle-ci ne figure pas officiellement dans le planning, Entr'ouvert devra avoir avancé suffisamment en terme d'interface pour pouvoir offrir quelque chose qui puisse être présenté à cette occasion.
Mikaël Ates et Jean-Marc Liger ont aussi évoqué l'éventualité d'une communication commune aux JRES, c'est certainement une piste intéressante.

Divers

- Sur l'interface de connexion du SP se fait la sélection de l'IdP. Mikaël à évoqué comme piste pour éviter la liste déroulante un outil comme celui récemment présenté par Feide sur la liste du WG ULX de Kantara.
- Au moment de la connexion l'utilisateur doit être redirigé vers une page de l'UNIdF dans laquelle figurera l'éventuelle URL vers laquelle il souhaitait se diriger.
- Des développements supplémentaires pour permettre l'utilisation de la solution par des téléphones mobiles seront conduits dans un second projet.
- Entr'ouvert fournira une image iso pour les partenaires avec des instructions concernant l'installation.
- Toutes les options à l'exception de l'appliance ont été retenues
- L'intérêt de Supann a été évoqué. Comme les attributs ne sont pas remontés d'un IdP vers un SP, les attributs ne sont pas pris en compte.

Planning

Pour laisser un peu plus de temps pour les opérations de recettage début janvier, le planning a été revu comme suit :

- Première maquette après les fêtes : Première maquette le 4/01
- Recette première maquette le 28/01
- Version opérationnelle le 15/02
- Recette de la version opérationnelle le 15/03

À noter que la facturation ne peut être effectuée sur 2010. La première facture (accompte de 30%) sera donc envoyée à l'UNPIdF début janvier.

Prochaine réunion le mardi 7 décembre à 14H30 notamment avec les ingénieurs réseau des établissements partenaires où il sera question de l'intégration du portail captif dans des architectures où il y a déjà un contrôleur.