Question en attente

Est-ce qu'on garde le SSID eduspot ou est-ce qu'on le fait évoluer vers eduspot-nom-de-l-univ ? La question doit être posée à Renater. On peut garder eduspot et avoir à côté un SSID nom-de-l-univ qui renvoie vers la même solution. Mais pour les établissements mitoyens ça ne permet pas de faire la différence.

Problèmes rapportés à traiter

- Dans l'annuaire Paris 3 y a les entrées des anciens étudiants pour lesquels on ne souhaite pas donner un accès Eduspot. Il faudrait pouvoir filtrer en fonction d'un attribut.
- Fuite mémoire à Paris I. Problème de perf globale sur leur wifi. Demande s'il ya d'autres limites que le nombre de lease pour Eduspot et il n'y en a. Il faut jouer sur la plage DHCP et sur les délais (DHCP et session du portail captif). Thomas indique qu'il va faire un bilan des bonnes valeurs qui ont
  été déterminées sur les sites en production, et mettre la documentation d'Univnautes à jour sur ce sujet.
- Lille : augmentation de la plage DHCP parce qu'ils montent vite en nombre de lease, ils sont passés sur un /22. Voir le nombre de lease, le total en entête (permet d'augmenter le plage DHCP si on est en limite, y a une accroche dhcp par les smartphone même quandil n'y pas de connexion). Et mettre une alerte par mail aux admins quand on atteint un certain seuil de lease. Lease time est asses elevé par défaut, il faut peut-être le baisser à 1h (juste au-dessus de la durée d'expiration de la session).
- Inalco : Ça bloque quand on active pas le NAT. Volonté de connecter à 2 serveurs syslog en même temps (EDIT : c'est possible jusqu'à 3).
- Siris : fichier de lock qui n'est pas supprimé dans le répertoire /tmp à corriger. Bug qui nécessite de redémarrer le portail captif après téléchargement de la liste des IdP. Mais ça n'arrive pas à chaque fois (peut-être uniquement quand la liste a changé ?). Ça n'existe que depuis la mise à jour de juillet sans doute. Thomas va relire le script de téléchargement et chercher un éventuel problème. Échanges à prévoir pour préciser les choses.
- Schéma de connexion manquant à mettre dans la documentation
- Sabin : sous FX la page d'accueil après authent met une minute à se charger ? Benoit a vraisemblablement expliqué la cause : cela se produit lorsque FX essaye de contacter les serveurs de révocation OCSP.
- Problème de déconnexion : pas de fin de session (mais la durée paramétrable) et pas de logout (problème de Shibboleth). Le problème est connu et fait partie des problématiques portail captif. Aucune solution définitive n'existe.

Carte de France

Entr'ouvert a présenté le nouvel écran de connexion d'univnautes (à partir de la prochaine version disponible deuxième quinzaine de janvier). Il se base sur une carte de France des IdP de la fédération Renater et permet de multiplier les modes d'accès (voix, clic sur la carte ou dans la liste, recherche textuelle) à l'IdP de son université d'orignie. L'interface est pensée pour fonctionner avec les appareils mobiles. Thomas va envoyer l'URL de la maquette sur la liste afin d'avoir des premiers retours/remarques/critiques.

Fonctionnalités à développer en 2013

Entr'ouvert fait un certain nombre de propositions suite aux besoin exprimés par les différents universités utilisatrices.

IdP local

Il faudrait augmenter les capacité de l'IdP local pour lui permettre de :

- créer des comptes en masse
- créer des comptes provisoires et permettre d'avoir une date d'activation du compte en plus de la date de fin de validité
- Gérer les attributs pour permettre le contrôle d'accès

Plutôt que de continuer à développer cet IdP local un peu restrictif pour lequel les besoins vont croissant, Entr'ouvert recommande l'installation d'un véritable IdP intégré à la solution et qui servira de base pour le POC (Proof of concept) IdP Cloud.

POC IdP Cloud

Entr'ouvert propose, sous forme de démonstrateur, la mise à disposition d'un fournisseur d'identité multi-protocole (SAML,OpenId, Google, Facebook...) dans le Cloud ou hébergé par les universités qui le souhaitent. Ça se décompose comme suit :

- Déploiements d'hôtes IdP à la volée :
  - génération de fichiers d'hôtes virtuels apache2 ;
  - génération de settings django ;

    - outils systèmes de lancement des hôtes ;
    - intégration d'une css pour les pages utilisateurs (couleur des titres, paragraphes, liens, etc.) et d'une image de l'université (pour la bannière)
    - Déport de la page de Login sur le cloud ;
    - Tests de charge et premières optimisations.

- Interface minimale de souscription permettant entre autres paramètres de souscription de recueillir le nom de domaine, un certificat, un css et une image.

- Interface minimale d'administration et de supervision des hôtes.

POC système de contrôle d'accès

Entr'ouvert propose, sous forme de démonstrateur, la mise à disposition d'un environnement de fédération d'identité, qui facilite le travail des administrateurs, sécurise l'accès aux applications et permet une granularité très fine. Il se décomposerait comme suit :

- Couplage IdP et Reverse-Proxy pour le support multi-protocolaires ;
- Intégration au Reverse-Proxy d'un module de contrôle d'accès gérant les attributs d'identités et les rôles ;
- Interface d'administration pour définir une politique de contrôle d'accès en fonction des utilisateurs, de leurs attributs, de leurs rôles et du service ou des URLs demandés ;
- Support du protocole de délégation d'autorisation XACML ;
- Démonstration avec une application typique des universités à définir.

Divers

- Le contrôle sur les attributs peut être un frein au développement d'Eduspot. Si on exige des attributs 50% des IdP Shibboleth ne fonctionnent plus. Il faut prendre cette dimension en compte.

- Journée nationale sur la fédération d'identité en avril/mai sur Paris et dans deux ans la même journée mais en province. Entr'ouvert doit participer.