Le projet Univnautes : implémentation d'un portail captif Eduspot au sein de l'Université Numérique Paris Ile-de-France

Frédérick Bigrat
Université Numérique Paris Ile-de-France (UNPIdF)
Centre Tolbiac, 90 rue de Tolbiac, 75013 Paris

Jean-Marc Liger
Service Interuniversitaire du Réseau Informatique de la Sorbonne (SIRIS)
Chancellerie des Universités de Paris, 46 rue Saint-Jacques, 75230 Paris Cedex 5

Pierre Cros, Thomas Noël, Mikaël Ates
Société Entr'ouvert
19 rue du Château, 75014 Paris

Résumé

Univnautes est une implémentation d'un portail captif Eduspot actuellement en production au sein de l'université Numérique Paris Ile-de-France (UNPIdF). Ce projet associe 23 établissements d'Île-de-France dont 17 universités (450 000 étudiants et personnels), ainsi que plusieurs acteurs nationaux ou régionaux.

Univnautes s'appuie sur les recommandations du groupe support Eduspot visant à simplifier, au niveau national, l'accès au réseau sans-fil des utilisateurs. Le portail captif Eduspot repose sur un ensemble de pratiques communes de RENATER, dont la Fédération Education-Recherche comme infrastructure d'authentification.

Univnautes est une solution technique entièrement open source, développée par la société Entr'ouvert à partir du pare-feu pfSense 2.0 (BSD)[1], de la librairie Lasso[2] (GNU GPLv2) et du portail Authentic 2[3] (GNU AGPv3).

L'installation s'effectue à partir d'une image ISO sur une machine disposant de deux interfaces, WAN avec un accès à Internet (DNS, HTTP et HTTPS au moins) et LAN connecté au réseau Ethernet client sur lequel sont connectés les points d'accès diffusant le SSID eduspot.

Une fois la solution configurée, les mises à jour d'Univnautes se font en quelques minutes et quelques clics via la page d'accueil ou via le menu «System/Firmware/Auto update». L'ensemble de la configuration peut-être sauvegardé dans un simple fichier XML.

Depuis la version 20110724, Univnautes sait détecter les clients de type mobiles (smartphone), à savoir les navigateurs des plateformes Android, iPhone, iPad, BlackBerry, etc. Si un tel navigateur est détecté, une interface spécifique est affichée, principalement des «gros boutons» faciles à gérer par écran tactile.

Enfin la version 20110915 intègre un fournisseur d'identités (IdP) qui permet d'autoriser des utilisateurs locaux (les «comptes invités») créés sur le système pfSense.

Mots clefs

Portail captif, Eduspot, Univnautes, pfSence, Open Source, UNPIdF

---

[1] http://www.pfsense.org

[2] http://lasso.entrouvert.org

[3] http://dev.entrouvert.org/projects/authentic

1 Introduction

Le projet Univnautes est une implémentation d'un portail captif Eduspot développé au sein de l'université Numérique Paris Ile-de-France (UNPIdF). Il s'appuie sur les recommandations du groupe support Eduspot visant à simplifier, au niveau national, l'accès au réseau sans-fil des utilisateurs. Il repose sur un ensemble de pratiques communes de RENATER, dont la Fédération Education-Recherche comme infrastructure d'authentification. Il est développé par la société éditrice de logiciels libres Entr'ouvert, spécialisée en « Identité Numérique ».

2 Présentation générale de la conduite du projet UnivNautes

2.1 L'UNR Paris Ile de France

L'Université Numérique Paris Île-de-France (UNPIdF) est un projet soutenu par le Ministère de l'enseignement supérieur et de la recherche et porté par l'université Paris 1 Panthéon – Sorbonne. Ce projet associe 23 établissements d'Île-de-France dont 17 universités (450 000 étudiants et personnels), ainsi que plusieurs acteurs nationaux ou régionaux.

L'UNPIdF a pour objectif général d'être une structure d'appui au développement des usages du numérique particulièrement dans les domaines de l'administration, de la gestion, de l'enseignement, de la formation et de la culture. Pour atteindre cet objectif, les établissements membres de l'Université Numérique Paris Île-de-France mutualisent ressources et compétences pour développer ou renforcer les infrastructures et services numériques utiles à leurs communautés. Le résultat attendu de cette évolution vers le numérique est une nouvelle qualité de la vie universitaire et de la vie étudiante qui devrait se traduire notamment par une meilleure réussite des étudiants.

Pour ce faire, l'UNPIdF fédère de nombreux projets et chantiers ayant une composante fonctionnelle et/ou technique (développement logiciel, mise en place d'architectures techniques, innovation technologique, …) mais aussi des impacts sur les procédures et les organisations (accompagnement des usagers, mise en place de nouvelles procédures, évolutions des métiers, …).

Ainsi l'ensemble des services administratifs et techniques et les composantes d'un établissement sont concernés par de nouveaux services dans le domaine de la scolarité (e-administration), de la pédagogie (cours en lignes, plateformes pédagogiques, …), de la documentation (bibliothèques électroniques) et de la vie étudiante (services numériques divers).

Enfin tous ces services doivent pouvoir être accessibles en ligne pour les étudiants ou le personnel des universités, et quel que soit l'établissement où l'utilisateur se trouve.

2.2 Un projet de Portail Captif basé sur la Fédération d'Identité du CRU

Afin d'offrir à l'ensemble de ses utilisateurs et visiteurs les avantages de la mobilité, l'UNPIdF a souhaité mettre en place au sein de ses établissements partenaires un portail captif commun permettant un accès au réseau sans fil WiFi, via une authentification s'appuyant sur la Fédération d'Identité du CRU déjà en place (Shibboleth 2.0 uniquement).

Le concept du portail captif peut-être assimilé à une solution d'authentification qui comporte un certain nombre de modules ou fonctionnalités. Parmi eux, une page web accessible en HTTP et HTTPS permettant soit le choix de l'organisme auprès duquel l'on souhaite s'authentifier (liste déroulante), mécanisme s'appuyant sur la Fédération d'identité Shibboleth, soit la possibilité de s'authentifier par l'intermédiaire d'une base d'authentification locale (LDAP, AD, Radius). La solution retenue présente avantage d'être multi-constructeur et multiplateforme puisque n'importe quel périphérique équipé d'un navigateur dialoguant en HTTP et HTTPS permet de s'authentifier.

Le projet de déploiement d'un portail captif mutualisé est resté au stade de l'étude en 2009. L'opération a été prise en charge en 2010 par le groupe de travail mobilité et réseaux (G5) en coordination avec le groupe référentiels et SI (G2) avant de devenir Groupe projet « UnivNautes » après proposition au Comité Opérationnel de l'UNPIdF en novembre 2010.

2.3 La problématique du site Sorbonne au cœur du projet UnivNautes

Le Service Interuniversitaire du Réseau Informatique de la Sorbonne (SIRIS) administre les équipements du réseau informatique de la Sorbonne communs à la Chancellerie des universités de Paris, aux universités Paris Panthéon-Sorbonne (Paris 1), Sorbonne Nouvelle (Paris 3), Paris-Sorbonne (Paris 4) et Paris Descartes (Paris 5), à l'École pratique des Hautes Études, à l'École nationale des Chartes et à la bibliothèque inter-universitaire de la Sorbonne, et leur connexion à l'Internet via le réseau académique parisien (RAP) et RENATER.

Confronté depuis sa création à la problématique multi-établissements du réseau fédérateur du site Sorbonne, le SIRIS a contribué significativement au projet UnivNautes en réaffirmant la nécessité d'un SSID unique et commun et en soulignant l'apport décisif d'une authentification basée sur la Fédération d'Identité du CRU qui deviendra ensuite la Fédération RENATER.

2.4 Le projet UnivNautes base de travail du projet national Eduspot

Cette nouvelle impulsion pour le projet de portail captif dont la réalisation était longtemps restée en souffrance, la volonté d'un SSID commun, et enfin les questions posées en marge d'une formation Shibboleth à Olivier Salaün et Medhi Hached - afin de déterminer si le CRU pouvait fournir et maintenir une liste de Fournisseurs d'Identité qui supporteraient le projet - sont en partie à l'origine de ce qui allait devenir ultérieurement le projet national de mobilité Eduspot.

3 Une solution technique basée sur le pare-feu pfSense 2.0, la librairie la librairie Lasso et le portail Authentic 2

3.1 Présentation de la solution technique

La société Entr'ouvert a remporté l'appel d'offre lancé en novembre 2011 en proposant d'implémenter une solution technique basée sur les technologies Open Source suivantes :

- le portail captif pfSense dans sa version 2.0Beta basé sur le noyau FreeBSD 8.0 ;
- son offre de librairie Lasso implémentation conforme aux spécifications SAML2 (certifiée conforme par Liberty Alliance, maintenant Kantara Initiative), donc interopérable avec l'implémentation Shibboleth 2.0 ;
- son offre de portail d'authentification Authentic 2 reposant sur la librairie Lasso et le Framework Python Django.

3.2 Installation du produit UnivNautes

Une machine avec deux interfaces est requise :

- une interface *WAN* avec un accès à Internet (DNS, HTTP et HTTPS au moins). Pour simplifier les tests, une interface connectée à un réseau adressé par DHCP est idéal ;
- une interface *LAN* connectée à un réseau Ethernet client. Si on veut tester avec des clients wifi, on peut installer sur ce réseau un (ou plusieurs) point d'accès diffusant le SSID *eduspot.*

Attention : sur l'interface LAN, un serveur DHCP sera activé par le portail captif Univnautes. Il vaut donc mieux tester sur un réseau indépendant et non utilisé.

Le téléchargement de l'image la plus récente se fait depuis http://isos.univnautes.entrouvert.com/ :

- Les fichiers .iso sont destinés à être gravés sur cédérom, ou utilisés en tant que cédérom par le démarreur de KVM, VirtualBOX, VMWare, etc... ;
- Les fichiers .img sont des images pour clé USB, agréable pour une installation sur machine physique.

Depuis le cédérom (notamment lors d'une installation sur machine virtuelle), il suffit de taper [Enter]. En revanche depuis une clé USB, il faut prendre le choix numéro 3 (Boot pfSense using USB device).

Le noyau FreeBSD est alors lancé. Au bout de quelques secondes arrivent les messages des scripts de démarrage liés à pfSense et Univnautes et enfin on arrive au choix qui propose de lancer l'installation du système.

L'installation se déroule en quelques étapes. Puisque tout le système est pré-configuré, il est possible d'accepter directement les choix par défaut pour réaliser une installation rapide. Une partition BSD va occuper tout le disque dur de la machine et le système va y être copié intégralement. L'installation va prendre quelques secondes sur une machine rapide (quelques minutes sur une machine virtuelle KVM).

3.3 Configuration du produit UnivNautes

Par défaut, le portail est livré avec des paramètres de tests. Son nom est *univnautes.entrouvert.lan*, le serveur HTTPS associé possède un certificat auto-signé (donc invalide par défaut pour les navigateurs), le certificat pour la fédération est un certificat associé au nom *univnautes.entrouvert.lan* dans la fédération de test de RENATER.

En production, il faut donc modifier tout cela, idéalement dans cet ordre :

1. donner un nom dans le domaine DNS de l'établissement (par exemple *eduspot.univ-paris42.fr*) ;
2. placer un certificat valide sur le serveur HTTPS correspondant, obtenu auprès du CRU/RENATERr via le RSSI, valide pour le nom choisi précédemment ;
3. créer un nouveau certificat pour la fédération ;
4. déclarer les métadonnées SAML finale (associant le nom choisi et le certificat pour la fédération) auprès de la fédération RENATER.

Vous trouverez ci-dessous les détails pour chaque étape.

3.4 Choix du nom du portail (DNS forwarder)

Par défaut, le portail s'appelle *univnautes.entrouvert.lan*, il est associé à l'adresse IP 10.42.0.1 par le forwarder DNS local (10.42.0.1 étant l'adresse IP de l'interface LAN). En production, il faut changer ce nom dans le DNS.

Pour cela, se rendre dans *Services/DNS Forwarder* et ajouter le nom dans les *overrides*, en lui associant l'IP 10.42.0.1 (ou l'IP de l'interface LAN, si vous l'avez changée).

3.5 Certificat et clé HTTPS

Par défaut, le portail est accessible en HTTPS et utilise un certificat et une clé de test. Cela donne des messages d'alerte voire d'erreur sur les navigateurs.

Pour modifier le certificat HTTPS du portail, il faut se rendre sur la page *Services/Captive Portal* et y indiquer :

- *HTTPS server name* : le nom du serveur (celui qui est déclaré dans le certificat) ;
- *HTTPS certificate* : le certificat au format PEM ;
- *HTTPS private key* : la clé privée associée, au format PEM ;
- *HTTPS intermediate certificate* : le certificat de l'AC émettrice (en cas de certificat auto-signé de test, recopier le certificat), au format PEM.

Lorsque ces paramètres sont modifiés, le service *cp_univnautes* est automatiquement relancé pour prendre en compte les modifications.

3.6 Certificat et clé pour la fédération

Sur l'onglet *Univnautes* dans la page *Services/Captive portal*, on indique :

- *SAML Private Key* : clé privée ;
- *SAML Signing Key (Certificate)* : certificat (clé publique).

L'outil *System/Cert Manager* peut être utilisé pour générer la clé et le certificat SAML. Ils n'ont pas besoin d'être signés par une autorité reconnue.

Lorsque ces paramètres sont modifiés, le service *cp_univnautes* est automatiquement relancé pour prendre en compte les modifications.

3.7 Déclaration des métadonnées dans la fédération RENATER

Une fois le service relancé avec les nouvelles données SAML, les métadonnées XML du portail sont accessibles sur la page https://nom_du_portail/authsaml2/metadata (attention: *nom_du_portail* doit être le nom choisi pour le serveur HTTPS). Il s'agit d'un fichier XML, qui peut être téléchargé et lu avec un éditeur de texte.

Ces données du service doivent être enregistrées dans la fédération.

Pour les tests, chacun peut utiliser la fédération de test https://federation.renater.fr/test/enregistrement. Sur l'interface d'enregistrement d'un fournisseur de service (SP), il faut entrer les données une à une :

- Intitulé du service : *Portail Captif Univnautes - Université xyz ;*
- URL du service : https://nom_du_portail ;
- URL de vos méta données : **n'indiquez rien ici !** En effet l'URL du portail n'est pas joignable sur Internet ; il faut donc renseigner les paramètres ci-dessous un par un ;
- entityID : https://nom_du_portail/authsaml2/metadata ;
- URL du service AssertionConsumerService SAML 1.0 : vide (notre fournisseur ne travaille qu'en SAML 2.0) ;
- URL du service AssertionConsumerService SAML 2.0 : https://nom_du_portail/authsaml2/singleSignOnPost ;
- Certificat X.509 : copier-coller du champ *SAML Signing Key (Certificate)* de la page *Services/Captive Portal/Univnautes*, en **retirant les première et dernière lignes** contenant les -----BEGIN CERTIFICATE----- et -----END CERTIFICATE-----

3.8 Forcer le rechargement des metadonnées et whitelist

Les métadonnées et la whitelist sont téléchargées chaque heure. Cependant, il peut être utile d'actualiser immédiatement ces données. Pour cela, deux techniques :

- soit depuis la console (en direct ou en *ssh*), taper : # univnautes-update-metadata.sh ;
- soit depuis l'interface web d'administration, se rendre sur la page *Services / Captive portal*, sur l'onglet *Univnautes* et cliquer sur le bouton [Save] en bas de page, sans modifier de paramètre. Cela recharge whitelist IP et metadonnées.

Dans les deux cas, pour vérifier, se rendre dans *Status / System Logs* sur l'onglet *Portal Auth* : vous devez voir une ligne disant à peu près ceci update-metadata: Loaded 117 providers.

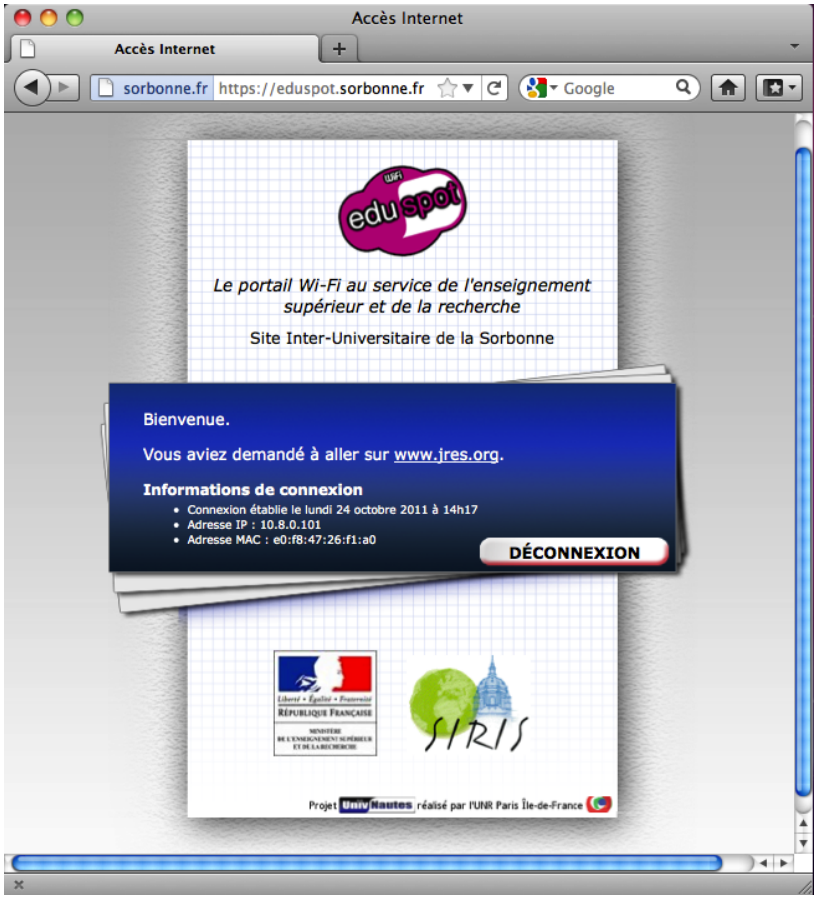
4 Conclusion

Univnautes est une implémentation totalement intégrée du projet Eduspot très facile à déployer et à maintenir. Une fois la solution configurée, les mises à jour d'Univnautes se font en quelques minutes et quelques clics via la page d'accueil ou via le menu «System/Firmware/Auto update». L'ensemble de la configuration peut-être sauvegardé dans un simple fichier XML.

Depuis la version 20110724, Univnautes sait détecter les clients de type mobiles (smartphone), à savoir les navigateurs des plateformes Android, iPhone, iPad, BlackBerry, etc. Si un tel navigateur est détecté, une interface spécifique est affichée, principalement des «gros boutons» faciles à gérer par écran tactile.

Enfin la version 20110915 intègre un fournisseur d'identités (IdP) qui permet d'autoriser des utilisateurs locaux (les «comptes invités») créés sur le système pfSense.

UnivNautes ne dispose pas encore de support IPv6 mais des développements sont prévus en ce sens.



5 Bibliographie

[1] Jean-Marc Liger, Théodore, Aslamatzidis ,Multimédia et Didactique, Internet au service d'une activité émergente : le Sambo. Dans Actes du *congrès JORRESCAM 2000*, 119, Amiens Avril 2000.

[2] Mikaël Ates, Christophe Gravier, Jeremy Lardon, Jacques Fayolle, et Bruno Sauviac, Architectures de fédération d'identités et interopérabilité. Dans *Actes du congrès JRES2007*, http://2007.jres.org/articles/79.pdf

[3] Frédérick Bigrat, Pierre Cros et Thomas Noël, Le projet Univnautes : une solution Open source de portail captif mutualisé et orienté Fédération Recherche. Dans *Journée Fédération 2011,* Paris 24 Janvier 2011.