CRU

L'écho du CRU

Abonnement à l'écho du CRU :
http://listes.cru.fr/sympa/info/echo

Sommaire du n°6
Novembre 2005

- Mise en place d'une fédération d'identités Shibboleth sur REAUMUR
- GDS: Global Dialing System
- Autres informations

Mise en place d'une fédération d'identités Shibboleth sur REAUMUR

Dans le cadre du projet d'Université Numérique en Région « Aquitaine Campus Ouvert en Région » (UNR-ACOR), le service réseau inter-universitaire REAUMUR était chargé de la mise en place d'une infrastructure d'accès sans fil inter établissements avec authentification par « portail captif » dans des délais relativement courts.

Un des points les plus critiques de ce projet concernait l'authentification multi entités qui devait s'appuyer sur les différents annuaires des établissements partenaires tout en offrant le maximum de sécurité et de confort pour l'usager.

Plusieurs possibilités s'offraient à nous pour la réaliser : s'appuyer **directement** sur les services « classiques » d'authentification (serveurs RADIUS, proxy RADIUS, méta annuaire LDAP, proxy LDAP, serveurs CAS d'établissements) ou **indirectement**, et de façon potentiellement plus prometteuse, via un mécanisme d'authentification unique ou « Single Sign On » (SSO) et si possible, s'appuyant sur le mécanisme de SSO d'établissement CAS (SSO retenu dans l'UNR ACOR).

Compte tenu du fait que les établissements se trouvaient à divers stade dans la mise en production de leurs Environnement Numériques de Travail (ENT) et donc de leurs serveurs CAS, le mécanisme de SSO ne pouvait être une solution directement opérationnelle que s'il permettait d'exploiter simultanément les divers types d'authentification actuellement utilisés dans les établissements et pouvant être mis à notre disposition.

La solution la plus évoluée s'est avérée viable et s'est concrétisée par la mise en place d'une fédération d'identités Shibboleth (sans gestion d'attribut dans un premier temps) permettant aux usagers du service de portail captif, une fois authentifiés – via Shibboleth – sur leur serveurs CAS d'établissements, d'accéder sans ré authentification à leur ENT.

L'installation du produit Shibboleth ne présente pas de difficulté majeure en suivant le mode d'emploi rédigé par le CRU. En revanche, le déboggage initial permettant d'aboutir à une première configuration fonctionnelle s'avère quand même un peu délicat... Nous avons donc décidé de créer sur nos serveurs les fournisseurs d'identités nécessaires pour chaque établissement, afin de pouvoir garantir un démarrage sans retard du service. Pour les établissements qui n'auraient pas de serveur CAS en temps voulu, nous avons testé la possibilité d'exploiter un serveur RADIUS ou LDAP, ce qui se fait très simplement en utilisant les modules d'authentification d'Apache (mod_auth_radius, mod_ldap ou tout autre module définissant la variable REMOTE_USER) pour protéger l'accès à l'URL du fournisseur d'identités Shibboleth.

Le gain majeur sur le plan sécurité est que nous ne sommes, à aucun moment, amenés à manipuler (en clair ou en codé) les mots de passe des usagers au niveau de notre infrastructure, manipulations qui auraient été inévitables pour adapter une authentification par portail captif (HTTPS) à un protocole non HTTP (LDAP, RADIUS, ...)

Le dernier point à régler était de trouver un système de portail captif supportant Shibboleth. Comme nous n'en avons pas trouvé dans la nature, nous avons choisi d'adapter le système libre NoCatAuth, qui présente l'inconvénient majeur de ne plus être très activement développé, mais l'avantage d'être écrit en PERL pour la partie contrôle, et d'exploiter les mécanisme existants pour le reste (filtrage de paquets) : au final, une grande souplesse pour adapter rapidement le produit.

Au-delà de ce portail captif, disposer d'un mécanisme d'authentification répartie comme Shibboleth se présente comme un énorme bénéfice pour les structures inter-universitaires comme REAUMUR, car il permet d'offrir des services avec authentification pour l'ensemble de ses usagers, sans avoir à gérer localement des dizaines de milliers de comptes. Nous avons d'ailleurs commencé à migrer sous Shibboleth nos différentes applications web (tableau de bord réseau, gestion de services délégués...) et nos services inter-universitaires voisins sont également très intéressés. L'exemple le plus actuel étant celui du **Service Interétablissements de Coopération Documentaire des Universités de Bordeaux** (SICOD) pour la gestion des accès nomades aux ressources électroniques en ligne (revues électroniques).

Laurent Facq (REAUMUR)

GDS: Global Dialing System

GDS est un plan de numérotation pour la visioconférence IP similaire au plan de numérotation téléphonique de la norme E.164. Il permet aux terminaux H323 (visioconférence, téléphonie) d'établir des communications à travers l'Internet selon le schéma de numérotation:

<IAC><CC><OP><EN>
<IAC> International Access Code. Le code d'accès international est 00
<CC> Country Code. Le code pays est 33 pour le France
<OP> Organisational Prefix.
<EN> Endpoint Number.

Un plan de numérotation alphanumérique est prévu aussi dans GDS (par exemple nom.prenom@nom-de-domain.fr) mais il n'existe pas encore d'implémentation. Ce type de numérotation est disponible sur certains GK mais est spécifique.

GDS a été développé par ViDe (Video Development Initiative) dont le projet ViDeNet fourni un réseau virtuel IP pour la voix et la vidéo (http://www.vide.net/help/gdsintro.shtml). GDS permet de relier les zones H323 des grands réseaux académiques. Chaque zone dispose d'un Gatekeeper. Tous ces GK sont hiérarchisés au niveau international puis national.

Depuis mai-2005, Renater est relié à l'infrastructure de GK supportant GDS, le GK national est connecté par quatre liaisons internationales. Aujourd'hui, plus de trente sites de Renater peuvent communiquer avec GDS. Les sites concernés sont :

- Les universités de Bretagne sud, du Littoral Cote d'Opale, Monpellier3, Nice, Méditerranée, Paris11 Orsay, Valenciennes
- Les ENSAM de Paris, Aix, Lille, Bordeaux, Metz, Angers, Chalon, Cluny
- RAP, CRIHAN, CIRIL, Reaumur, CIREN Montpellier, IUFM Lille, École des Mines de Paris, ENST
- Institut National des Télécommunications, CIRAD, CEA Saclay, INSERM Île de France
- Villejuif, IRD Orléans et Bondy, CNRS Meudon et Pouchet
- Le GIP Renater

GDS permet aux terminaux H323 d'être joignables selon un plan d'adressage international. Ces terminaux doivent s'enregistrer sur des Gatekeeper qui résolvent aussi les problèmes liés à la sécurité et à l'adressage :

- Si le FireWall n'intègre pas le protocole H323, les ports TCP et UDP de chaque terminal H323 doivent être ouverts au delà de 1024. En effet, les adresses et les ports nécessaires aux communications vidéo et audio sont échangés dynamiquement dans des messages de signalisation.
- Les serveurs NAT traditionnels ne sont pas capables de gérer le protocole H323 car les adresses IP des terminaux sont échangés dans des messages de signalisation.

Les terminaux H323 (IP publique ou privée), sont sécurisés par le GK et communiquent sur Internet avec les autres terminaux qui ont adopté aussi la numérotation GDS.

Comment se raccorder à GDS

Un Gatekeeper doit être mis en service, il définit la zone de communication H323 de l'établissement. On recommande le logiciel GnuGK disponible sur http://www.gnugk.org. Il serait trop long de présenter dans sa totalité le fichier de configuration. Nous proposons au lecteur qui souhaiterait se faire aider et recevoir des exemples de configuration de consulter la page http://www.renater.fr/Services/H323/GKs.htm et d'utiliser la liste de diffusion http://listeuvhc.univ-valenciennes.fr/wws/info/visio. Nous ne présentons que quelques extraits du fichier :

```
[RoutedMode]
; la signalisation passe par le GK
GKRouted=1
SupportNATedEndpoints=1
; on limite la gamme de port à ouvrir
Q931PortRange=20000-20999
H245PortRange=30000-30999
[Proxy]
; on active le proxy, tous les appels passent par le GK
Enable=1
ProxyForNAT=1
[RasSrv::RewriteE164]
; définition du préfixe 032751 et du plan d'adressage local : <OP><EN>.
; Les <EN> commençant par 1 (ex. 1234) sont équivalent à <OP><EN>(ex.0327511234)
0327511=1
[RasSrv::Neighbors]
; la numérotation qui commence par 0 est envoyée vers le GK national.
GIPRenater=a.b.c.d;0 (adresse IP fournie par Renater)
```

L'établissement doit définir son préfixe <OP>. Pour l'instant, nous proposons d'utiliser le préfixe de la numérotation téléphonique E.164 du site. Ce préfixe doit être envoyé à prefixe-E164@renater.fr qui, après acceptation, établira le peering.

Pour valider une connexion GDS, le réseau académique du New-Jersey a mis à disposition des machines de test. http://www.njedge.net/techsection/
Un terminal H323 peut être appelé au 0019735965412. De ce site, on peut aussi appeler son propre terminal.

Attention, nous avons constaté que ce service très utile n'est plus opérationnel. Espérons qu'il le redevienne bientôt.

Guy Bisiaux (CRU)

Autres informations

- Publication de l'article lié au tutoriel JRES sur la fédération d'identités. Un article de fond sur le fonctionnement de Shibboleth, la fédération d'identités et les problématiques associées (PDF, 45 pages, 593 Ko) <http://federation.cru.fr/doc/shibboleth-jres2005-article.pdf>

- JRES, la grande réunion des informaticiens de la communauté aura lieu la semaine prochaine. De nombreuses personnes n'ont pu s'inscrire faute d'un nombre de place suffisant. Tous ceux qui ne peuvent être présents pourront cependant suivre en direct les conférences sur le réseau (voir les instructions sur http://www.jres.org/public/ViewObj.asp?id=56). Par la suite, vous retrouverez sur le site de la conférence une archive vidéo des différentes sessions.

- Le projet Sympa reste très actif. Il nous semble important de vous faire connaître les orientations de ce projet mais aussi de recueillir vos souhaits et vos réactions pour ce produit utilisé dans la plupart des établissements d'enseignement supérieur. A cet effet, un "wiki" a été ouvert pour vous présenter les grands chantiers et le petits aménagements déjà recensés.
  http://www.sympa.org/wiki/doku.php?id=project_direction