Authentification des utilisateurs - de LDAP à Kerberos

Pascal Aubry et François Dagorn (IFSIC / université de Rennes 1)

Introduction

Cet article explique comment il est possible de migrer l'authentification des utilisateurs de l'université de Rennes 1 depuis la solution actuelle basée sur l'annuaire LDAP vers une solution basée sur Kerberos, avec les objectifs suivants :

- Supprimer les failles de sécurité actuelles observées avec l'authentification LDAP.
- Proposer un mécanisme d'authentification autre que LDAP pour Windows 7.
- Disposer d'une authentification SSO depuis la session utilisateur sur les postes clients jusqu'aux applications web.

Nous commençons par décrire la situation actuelle, puis évoquons les solutions possibles. Après un très bref aperçu de Kerberos, nous montrons les tests qui ont été menés à bien puis proposons une stratégie de déploiement pour laquelle l'IFSIC serait pilote pour l'université.

1. La situation actuelle

1.1 Architecture

L'architecture informatique de l'université de Rennes 1 est aujourd'hui constituée de :

- **postes clients** (Windows XP, Linux et Mac OS X). A ces postes viendront s'ajouter à la rentrée 2010/2011 des postes Windows 7.
- **serveurs de fichiers**
  - Network Appliance (commun à toute l'Université) partagé en NFS pour les clients Unix et en CIFS pour les clients Windows
  - Serveurs de fichiers Unix partagés en NFS pour les clients Unix et/ou CIFS (Samba) pour les clients Windows
  - Serveurs de fichiers Windows partagés en CIFS pour les clients Windows
- **services applicatifs web**
- **serveurs d'impression** CUPS

1.2 Authentification

Le système d'authentification des usagers est architecturé autour de l'annuaire LDAP de l'établissement qui est dérivé journellement du système d'information. L'authentification LDAP est dans tous les cas réalisée par un *fast bind* sur l'annuaire du couple *uid*/*password* dont on veut valider l'authenticité, les mécanismes suivants sont mis en oeuvre :

- Les clients Unix se basent sur le module PAM pam_ldap.
- Les clients Windows XP utilisent le module PGina, qui stocke les informations de connexion des utilisateurs (*uid*/*password*) et les rejoue quand nécessaire auprès des serveurs pour effectuer les montages (*net use*).
- Les montages CIFS du Network Appliance transmettent les couples (*uid*/*password*) à l'annuaire LDAP pour validation.

- Les montages NFS (v3) sont effectués sans authentification, par confiance envers les clients autorisés.
- Les services applicatifs web sont CASifiés, l'authentification au niveau du serveur CAS est déléguée à l'annuaire LDAP.
- Les clients Windows impriment via des montages SMB sur les serveurs d'impression, l'authentification est faite par Samba via pam_ldap.
- Les clients Unix impriment en IPP, également via pam_ldap.

Notons qu'il s'agit d'un usage détourné de l'annuaire LDAP, conçu initialement comme un service de pages blanches pour la recherche d'informations (utilisateurs, machines) et est aujourd'hui principalement utilisé pour l'authentification. Cet usage est néanmoins très largement adopté dans nos universités et répond fonctionnellement bien au besoin car il permet de contrôler l'accès à tous les types de services nécessaires sur un réseau informatique (ouverture de sessions, impressions, partage de fichiers, ...). Il est de plus disponible dans tous les environnements utilisés (Linux, Windows, MacOS, Solaris, ...).

2. Pourquoi évoluer ?

L'utilisation de LDAP décrite plus haut est aujourd'hui relativement générale dans les universités, plusieurs problèmes liés à la sécurité des réseaux se posent pourtant.

2.1 Pour plus de sécurité

Les mots de passe des usagers doivent impérativement être acheminés en clair depuis les postes de travail qui hébergent des services jusqu'aux serveurs LDAP chargés des opérations de contrôles. L'utilisation du protocole sécurisé LDAPS (LDAP sur TLS) permet de contourner ce problème puisqu'il impose une session TLS avant tout dialogue LDAP. L'université de Rennes 1 n'utilise pas LDAPS et tous les postes de travail du réseau académique exposent les mots de passe des usagers aux yeux d'utilisateurs indélicats (l'empoisonnement ARP est facile à mettre en oeuvre). L'utilisation de services de fichiers mutualisés contrôlés par LDAP accentuent ce problème car les mots de passe doivent circuler en clair jusqu'aux services avant d'être acheminés ensuite (éventuellement en LDAPS) jusqu'aux serveurs LDAP. Dans ce cadre, les serveurs d'impressions (Samba, pam_ldap) ainsi que le serveur de fichiers communautaire de l'université de Rennes 1 sont aujourd'hui des maillons faibles de la sécurité du réseau de l'établissement.

2.2 A cause de l'apparition de Windows 7

En 2009, le nouveau système d'exploitaion Windows 7 est apparu, il ne s'intègre pas facilement dans un environnement contrôlé par LDAP.

Windows XP utilisait PGina pour intercepter le mot de passe de l'usager au moment de la phase de connexion, il le ressortait ensuite quand celà s'avérait nécessaire (utisation de partages, ...). Ce schéma ne peut plus fonctionner sous Windows 7, mais on ne peut toutefois pas renoncer à Windows 7 pour cette raison.

L'IFSIC a développé un outil similaire à PGina (Regina), il est en place et fonctionne. La méthode utilisée par Regina et PGina pour intercepter et utiliser le mot de passe en clair n'est néanmoins pas compatible avec les impératifs de sécurité d'un réseau informatique. Plus généralement, c'est l'utilisation de LDAP pour authentifier des usagers qui pose de gros problèmes de sécurité.

2.3 Pour un SSO de bout en bout

La généralisation des ENT a permis la mise en oeuvre de systèmes d'authentification unique pour les environnements web, mais on reste pour l'instant dans l'attente d'un système d'authentification allant de l'ouverture de session jusqu'aux applicatifs Web.

3. Les solutions

On distingue trois solutions possibles raisonnablement envisageables à la rentrée 2010/2011.

3.1 Ne rien faire

Bien que non sécurisé, le réseau est aujourd'hui fonctionnel, il peut rester en l'état.

Si cette solution est la plus envisageable en terme de coût, elle oblige néanmoins à utiliser une « verrue » supplémentaire pour Windows 7 (Regina).

3.2 Utiliser Active Directory quand c'est possible

Les deux failles principales sont le serveur de fichiers et les services d'impressions. S'il est relativement simple de contrôler les accès CIFS au serveur de fichier communautaire (par l'intermédiaire d'un serveur Active Directory utilisant une authentification NTLM nettement plus sûre que LDAP), cette solution ne règle pas complètement le problème car :

- les postes Linux utilisent actuellement des montages NFS dans lesquels le serveur de fichiers fait confiance au client (sécurité zéro). Quelle solution adopter alors ?
- les services d'impressions continuent à utiliser Samba + pam_ldap, faut-il les faire basculer aussi vers Active Directory ? Comment se passeraient alors les impressions depuis Linux ?

3.3 Changer de mécanisme d'authentification

Dans ce cadre, seule la solution Kerberos est envisageable.

Deux implémentations peuvent être envisagées :

1. La mise en place d'un « vrai » service Kerberos (MIT ou Heimal).
2. L'utilisation des fonctionnalités Kerberos de Active Directory.

La deuxième solution, décrite par Emmanuel Blindauer en 2005 (Kerberos : Linux, Windows et le SSO), est possible. Néanmoins,

- Elle oblige à s'appuyer sur une solution non libre pour l'authentification, coeur de la sécurité du système.
- Elle comporte certains problèmes décrits par le même auteur quatre ans plus tard (Référentiel d'authentification interopérable et ouvert: Kerberos) , dans lequel il confessait qu'il eut été plus judicieux de nommer l'article de 2005 « Active Directory = Windows + Linux + SSO + Problèmes ».

Notre choix se porte donc clairement sur la première solution.

4. Kerberos

Kerberos fonctionne en environnement hétérogène, assurant la sécurité des échanges sur un réseau non sûr et permettant la mise en place d'un véritable service d'authentification unique.

Kerberos utilise un système de chiffrement symétrique pour assurer un dialogue sécurisé entre deux protagonistes. Les dialogues s'opèrent en utilisant une clef secrète et partagée. Les algorithmes de chiffrement sont publics (AES, DES, 3DES, ...), toute la sécurité du système repose sur la confidentialité de la clef de chiffrement. Pour faciliter la gestion d'un tel système, Kerberos repose sur l'utilisation d'un tiers de confiance qui distribue les clefs aux utilisateurs et services abonnés (les *principals*). Un serveur Kerberos est appelé KDC (*Key Distribution Center*).

Kerberos est un service sûr qui assure la confidentialité, l'intégrité des données ainsi que la non-répudiation (les participants sont identifiés, y compris le serveur contrairement à NTLM). Le service d'authentification assure l'identification unique du client et lui procure un ticket de session qu'il pourra utiliser pour demander des tickets d'utilisation des services *kerbérisés*. Un ticket de session chiffré avec la clef d'un service *kerbérisé* constitue un ticket de service. On distingue deux fonctionnalités dans un service kerberos :

- le service d'authentification
- le service de délivrement de tickets de services.

Kerberos a été mis au point au MIT dans les années 1990, il est maintenant très largement déployé et est disponible dans tous les environnements aujourd'hui utilisés (Linux, Windows, MacOS, ...). Des universités françaises ont déjà migré leur systèmes d'authentification vers Kerberos, parmi celles-ci on peut citer les universités de Strasbourg et de Bordeaux 1.

5. Les tests effectués

Comme indiqué en 3.3, la possibilité d'utiliser le serveur Kerberos enlisé dans un service Active Directory de MicroSoft a été volontairement écartée et les tests ont été effectués avec un serveur Kerberos hébergé sur un serveur Linux.
Les éléments ci-dessous ont été validés.

5.1 Le service Kerberos

Un serveur kerberos (MIT 1.6.1) maître est fonctionnel sur **kerb1.univ-rennes1.fr**. Il est redondé par un second serveur esclave (**kerb2.univ-rennes1.fr**), dont la synchronisation avec le serveur maître est assurée par une *crontab* via le protocole *kprop*.

Une interface web (PHP, CASifiée) permet la gestion des principals clients (serveurs et stations de travail).

Voir : Installation des serveurs Kerberos

5.2 Le service CAS

Un serveur CAS (3.3.5) est fonctionnel sur **cas-kerb.univ-rennes1.fr**.

Ce serveur permet le SSO de bout en bout (depuis l'authentification sur les postes clients jusqu'à celle sur les applications web).

Il permet également l'alimentation du royaume Kerberos UNIV-RENNES1.FR par interception des authentifications LDAP.

Voir : Installation du serveur CAS

5.3 Les clients

L'authentification Kerberos s'intègre parfaitement (de manière native) dans les clients Linux, l'accès à tous les services a été validé : CAS, NFS v3 et v4 (sur serveurs linux et NetApp), Samba, CUPS.

L'authentification Kerberos seule est possible pour les clients Windows (XP et 7), mais l'accès au serveur NetApp nécessite l'intégration d'un sous-domaine Active Directory.

L'authentification des services Samba (sur serveur Unix), CUPS a été validée.

Voir :

- Intégration d'un client Linux
- Intégration d'un client Windows XP
- Configuration de Firefox pour le SSO
- Configuration de Internet Explorer pour le SSO

5.4 Les services de fichiers

Le montage des volumes NetApp a été validé à la fois en NFS depuis les clients Unix et en CIFS depuis les clients Windows, en s'appuyant sur un Active Directory pour lequel une relation d'approbation mutuelle avec le royaume Kerberos a été mis en place.

Les montages NFS v3 et v4 ainsi que Samba ont également été validés, ce qui permet aux entités l'utilisation de services de fichiers autonomes.

Voir :

- Mise en place d'un serveur Samba
- Mise en place d'un serveur NFS (v4-Kerberos)

5.5 Le service CUPS

Les clients Windows et Unix peuvent imprimer sur un serveur CUPS Kerbérisé de manière transparente.

Voir : Mise en place d'un serveur CUPS

5.6 Le service 802.1X

Un serveur FreeRadius a été configuré pour utiliser une base d'authentification Kerberos.
Le dispositif fonctionne mais ne peut pas être intégré dans le cadre de l'authentification unique.

Voir : 802-1x, Radius et Kerberos

6. Une stratégie de déploiement

Les tâches à réaliser pour mettre l'authentification Kerberos en production sont listées ci-dessous.

> **Passage à Kerberos de l'IFSIC d'abord, du reste de l'université ensuite**
>
> La seule condition pour que le passage de l'authentification Kerberos soit possible d'abord sur l'IFSIC avant de passer à toute l'université est que le NetApp puisse partager les mêmes volumes à la fois avec authentification Kerberos en NFS v4 (pour les clients Unix de l'IFSIC) et sans authentification en NFS v3 (pour les clients Unix du reste de l'université, qui pourraient ainsi migrer à Kerberos ultérieurement).
>
> Dans le cas où l'export mixte v4/Kerberos et v3/*Trusted* des mêmes volumes ne serait pas possible, il serait possible de rester en mode v3/*Trusted* en attendant que tous les clients NFS potentiels de l'université soient *Kerbérisés*. Les seuls prérequis pour le passage (dans une première étape) de l'IFSIC à Kerberos sont donc les tâches à réaliser au niveau du CRI et détaillées ci-dessous.
>
> Cette stratégie (conservation de NFS v3/*Trusted* tant que tous les clients NFS n'ont pas migré à Kerberos) semble la plus raisonnable.

Le passage de toute l'université à l'authentification Kerberos nécessiterait au niveau de chaque cellule les mêmes tâches que celles à effectuer à l'IFSIC.

6.1 Tâches au niveau du CRI

Serveurs Kerberos

Recréer une infrastructure de production pour les serveurs Kerberos kerb1.univ-rennes1.fr et kerb2.univ-rennnes1.fr.

Voir : Installation des serveurs Kerberos

Serveur CAS

Modifier le serveur CAS pour qu'il permette :

- l'authentification des tickets Kerberos des clients
- l'alimentation du royaume Kerberos avec les utilisateurs qui s'authentifient sur l'annuaire LDAP

Voir : Installation du serveur CAS

Application Sésame

Modifier l'application Sésame de l'université pour qu'elle permette :

- l'ajout des utilisateurs dans le royaume Kerberos lors de l'activation des comptes
- la modification du mot de passe des utilisateurs dans le royaume Kerberos (en plus de celle dans l'annuaire LDAP)
- la suppression des utilisateurs dans le royaume Kerberos lors de la suppression des comptes

Voir : Modification de l'application Sésame

NetApp

Ajouter les exports NFS v4 avec authentification Kerberos (et vérifier qu'ils sont compatibles avec les mêmes exports v3 sans authentification, sinon rester en v3/Trusted).

Ajouter l'authentification Kerberos aux exports CIFS en s'appuyant sur l'Active Directory.

Voir : Mise en place d'un serveur NFS (v4-Kerberos)

6.2 Tâches au niveau de l'IFSIC

Clients

Modifier tous les clients pour l'authentification Kerberos.

Voir :

- Intégration d'un client Linux
- Intégration d'un client Windows XP
- Configuration de Firefox pour le SSO
- Configuration de Internet Explorer pour le SSO

Serveur de fichiers

Modifier l'authentification des serveurs Samba et NFS (passage à Kerberos).

Voir :

- Mise en place d'un serveur Samba
- Mise en place d'un serveur NFS (v4-Kerberos)

Serveur d'impression

Remonter un serveur d'impression Kerberisé pour faciliter la transition.

Voir : Mise en place d'un serveur CUPS

7. Conclusion

Tout est techniquement prêt pour migrer d'une authentification basée sur LDAP à une authentification basée sur Kerberos.

Nous sommes prêts dès à présent à contribuer à cette migration en assistant les équipes du CRI pour la mise en production (Kerberos, CAS et Sésame).

Références

- ARCHANN, une architecture d'annuaire et d'authentification interopérable pour un SSO unifié en environnement hétérogène, Pascal Levy (Université de Paris 1), JRES 2009
- Kerberos et la sécurité, Emmanuel Brouillon (CEA), SSTIC 2004
- Kerberos : Linux, Windows et le SSO, Emmanuel Blindauer (IUT Robert Schuman Strasbourg), JRES 2005
- Configuring a Kerberos 5 Server, Redhat 9 manual
- Replacing NIS with Kerberos and LDAP HOWTO
- Kerberos/LDAP/NFSv4 HOWTO
- Authenticate Windows to Unix Kerberos
- Making WindowsXP authenticate login to a UNIX MIT KDC
- Single sign-on "How To" Guide
- Référentiel d'authentification interopérable et ouvert: Kerberos, Emmanuel Blindauer (IUT R.Schuman Université de Strasbourg), JRES 2009
- http://pig.made-it.com/kerberos.html
- http://nfsv4.bullopensource.org/doc/kerberosnfs/krbnfs_howto_v3.pdf