Kerberos

Nicolas Grenèche

Centre de Ressources Informatique (CRI) - Université d'Orléans
Projet SDS - LIFO et ENSI de Bourges
nicolas.greneche@univ-orleans.fr

11/07/2011

Sommaire

UNIVERSITÉ D'ORLÉANS

Plan

UNIVERSITE D'ORLEANS

Pourquoi Kerberos ?

- SSO système ;
- Environnement hétérogène ;
- Tolérance aux pannes ;
- Supporté par beaucoup d'applications.

UNIVERSITE D'ORLEANS

Plan

UNIVERSITE D'ORLEANS

Les acteurs

- KDC (Key Distribution Center) : AS (Authentication Server) et TGS (Ticket Granting Server) ;
- Principals (Utilisateurs, machines et services) : nom associé à un jeu de clés (la même passphrase dérivée selon plusieurs algorithmes ou enctypes) ;
- Realm.

UNIVERSITE D'ORLEANS

Plan

UNIVERSITE D'ORLEANS

Le protocole : AS

Cette phase associée à l'authentification de l'utilisateur lui permet de récupérer son TGT (Ticket Granting Ticket).

- Le client envoi une requête AS-REQ comprenant :
  - Nom de son principal (CPN Client Principal Name) ;
  - Timestamp (chiffré avec sa clé privée si pré-authentification).
- Le serveur envoi une réponse AS-REP comprenant :
  - Une partie chiffrée avec la clé de l'utilisateur comprenant une clé de session avec le KDC S ;
  - Une partie chiffrée avec la clé secrète du serveur de ticket comportant notamment S, un timstamp et l'adresse IP de l'utilisateur (optionnel). C'est le TGT (Ticket Granting Ticket).

Le protocole : TGS (1/2)

Cette phase est associée à l'accès à un service kerberisé par l'utilisateur. L'utilisateur possède un TGT valide et une clé de session S lui permettant de chiffrer ses échanges avec le KDC.

- Le client envoi une requête TGS-REQ comprenant :
  - Le SPN (Service Principal Name) : le nom du principal de l'application. Le plus souvent de la forme SERVICE/fqdn@REALM (par exemple IMAP/mailer.exemple.fr@EXEMPLE.FR pour un serveur de courrier IMAP) ;
  - Un authentificateur qui contient le nom du principal de l'utilisateur et un timestamp le tout chiffré avec la clé de session S ;
  - le TGT de l'utilisateur.

Le protocole : TGS (2/2)

- Le serveur envoi une réponse TGS-REP comprenant :
  - Une partie chiffrée avec la clé de session S comportant une clé de session de service s. Cette clé s va se partager entre le client et le service kerberizé visé ;
  - Une partie chiffrée avec la clé du service (c'est à dire les clés attachées au principal SERVICE/fqdn@REALM représentant l'application) comportant également la clé de session de service s, un timestamp et l'IP du client ayant demandé un accès au service (attention aux mécanismes de translation d'adresses). Cette partie constitue le ticket de service.

Enfin, le client présente à l'application le ticket de service obtenu. Cette partie n'est pas normalisée. La clé du principal attaché à l'application est stockée dans un fichier appelé keytab.

UNIVERSITÉ D'ORLÉANS

Sécurité :

- Service KDC ;
- Pré-authentification pour le dialogue avec l'AS (timestamp dans l'AS-REQ chiffré avec la clé de l'utilisateur) ;
- KDC Spoofing : requête vers le KDC-TGS pour le principal host/fqdn@REALM pour finaliser l'ouverture de session (obligatoire dans sssd et optionnel pour pam_kerberos).

Plan

UNIVERSITE D'ORLEANS

Kerberization d'une application

Lorsque l'on cherche à activer le support de Kerberos dans une application, cela se résume à trois actions :

- Créer un principal pour l'application ;
- Activer le support de Kerberos dans l'application ;
- Installer un keytab sur le serveur hébergeant l'application (attention aux permissions et au chroot).

UNIVERSITE D'ORLEANS

Activation du support de Kerberos

Pour une application donnée, le support de Kerberos peut se faire de trois manières :

- L'application intègre le code pour gérer Kerberos dans ces sources via les librairies MIT / Heimdal ;
- L'application supporte la configuration de l'authentification via les PAM (Pluggable Authentication Module) ;
- L'application supporte la SASL (Simple Authentication and Security Layer).

UNIVERSITE D'ORLEANS

Keytab

Fichier contenant les clés du principal associé à l'application.

- Exporté depuis le KDC, attention à la distribution (SCP) ;
- Permissions ;
- Standard : /etc/krb5.keytab, sinon définition dans l'application ou via KRB5_KTNAME.

UNIVERSITE D'ORLEANS

Plan

UNIVERSITÉ D'ORLÉANS

Tolérance aux pannes

- Définition de plusieurs KDC sur les clients ;
- Mécanismes de réplication :
  - iprop (incrémental / synchrone) ;
  - hprop / kprop (complète / asynchrone).

UNIVERSITE D'ORLEANS

Plan

UNIVERSITE D'ORLEANS

Problématique

- OpenLDAP pour les utilisateurs ;
  - Schémas UNRC et Supann ;
  - Utilisateurs déversés depuis un base de donnée Oracle Harpège / Apogée dans un Slapd maitre ;
  - Réplicas accessibles par les applications nécessitants un backend LDAP.
- Changement de mot de passe se fait sur les bases Oracle, ensuite c'est déversé dans LDAP.

UNIVERSITE D'ORLEANS

Architecture et composants utilisés

- Utilisation du schéma hdb et de l'overlay smbk5pwd sur le OpenLDAP maitre :
  - Schéma hdb compatible avec nos schémas ;
  - Overlay smbk5pwd intercepte l'opération étendue (exop) de changement de mot de passe LDAP pour générer les clés associé au principal.
- Réplication du KDC maitre vers des esclaves SANS serveur Slapd associé :
  - L'exposition réseau des KDC esclaves diffère de celles des réplicas LDAP ;
  - Le KDC reste minimal ;
  - Synchronisation complète hprop dans un cron. L'incrémental ne fonctionne pas pour nous.

UNIVERSITÉ D'ORLÉANS

Windows

- Approbation entre les AD des composantes et le KDC du CRI ;
- Mappage des comptes Windows ;
- Connexion au poste de travail avec son uid LDAP (numéro Harpège / Apogée).

UNIVERSITE D'ORLEANS

Problèmes

- Rattachement des postes itinérants (liés à aucun domaine) ;
  - Création d'un realm dédié pour eux ;
  - Approbation entre ce realm et celui du CRI ;
  - Interface web sur ce realm dédié pour que les correspondants puissent y créer les principals associés à leurs machines itinérantes.
- Communication (Kerberos fait peur).

UNIVERSITE D'ORLEANS