Retour d'expérience sur l'utilisation de Kerberos à l'INRIA

Guillaume Rousse

INRIA - DSI

Journées Réseau 2011

Plan

Plan

Intégration LDAP

Composants

- Heimdal
- OpenLDAP
- smbk5pwd

Gestion mot de passe

- synchronisation au changement de mot de passe
  opération spécifique nécessaire
- support ppolicy
- kpasswd désactivé

Intégration LDAP

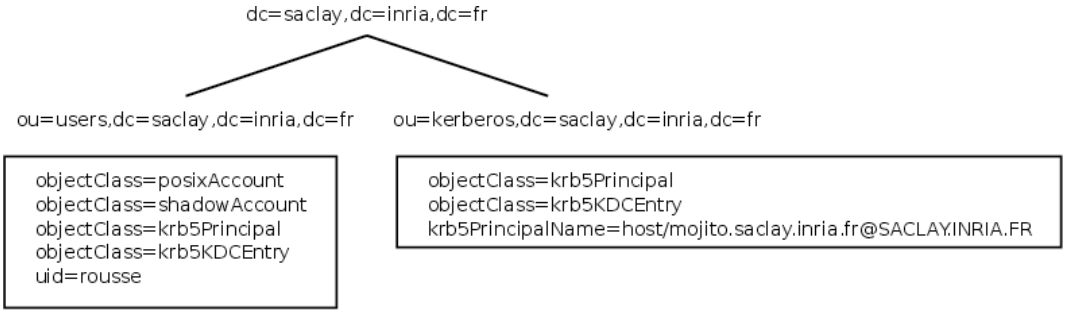
Composants

- Heimdal
- OpenLDAP
- smbk5pwd

Gestion mot de passe

- synchronisation au changement de mot de passe
  opération spécifique nécessaire
- support ppolicy
- kpasswd désactivé

Intégration LDAP

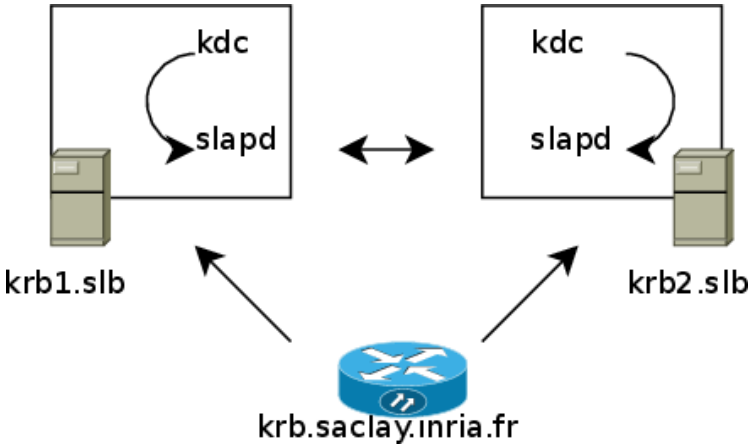


Architecture

Redondance

- configuration LDAP multi-maitres
- SLB assuré par équipement Cisco

Architecture



Configuration

Enregistrements DNS

```
; kdc
_kerberos._tcp          SRV     10 1 88 krb
_kerberos._udp          SRV     10 1 88 krb
; domaine par defaut pour la zone
_kerberos               TXT     "SACLAY.INRIA.FR"
```

Plan

Ticket vs mot de passe

Authentification par ticket

- utilisation d'un ticket
- support nécessaire au niveau du client et du protocole
- SSO et sécurité

Validation de mot de passe

- utilisation d'un mot de passe
- pas besoin de support spécifique
- ni SSO ni sécurité

Ticket vs mot de passe

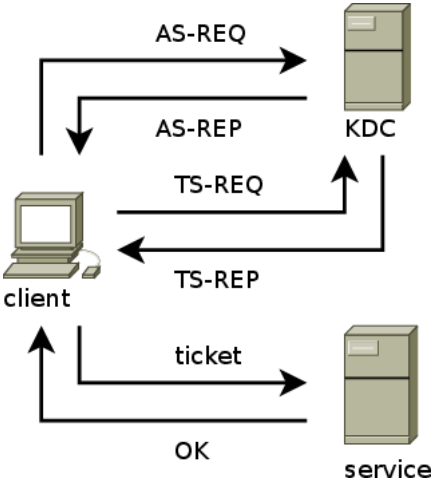
Authentification par ticket

- utilisation d'un ticket
- support nécessaire au niveau du client et du protocole
- SSO et sécurité

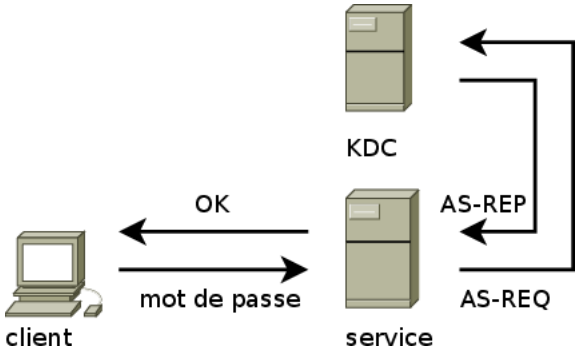
Validation de mot de passe

- utilisation d'un mot de passe
- pas besoin de support spécifique
- ni SSO ni sécurité

Authentification par ticket



Validation de mots de passe



Plan

Ouverture de session Unix

Détails technique

- ajout ou remplacement de la méthode d'authentification
- validation de mot de passe
- implementé par un module PAM (*pam-krb5* ou *pam_krb5*)

Intérêts

- intégration forte

Difficultés

- configuration nécessaire
- utilisation locale

Ouverture de session Unix

Détails technique

- ajout ou remplacement de la méthode d'authentification
- validation de mot de passe
- implementé par un module PAM (*pam-krb5* ou *pam_krb5*)

Intérêts

- intégration forte

Difficultés

- configuration nécessaire
- utilisation locale

Ouverture de session Unix

Détails technique

- ajout ou remplacement de la méthode d'authentification
- validation de mot de passe
- implementé par un module PAM (*pam-krb5* ou *pam_krb5*)

Intérêts

- intégration forte

Difficultés

- configuration nécessaire
- utilisation locale

SSH

Détails techniques

- ajout d'une méthode supplémentaire d'authentification
- authentification par ticket ou validation de mot de passe

Difficultés

- problème des répertoires personnels NFS kerberisés
- subtilités de configuration

`GSSAPIAuthentication`, `GSSAPIDelegateCredentials`, `KerberosAuthentication`

SSH

Détails techniques

- ajout d'une méthode supplémentaire d'authentification
- authentification par ticket ou validation de mot de passe

Difficultés

- problème des répertoires personnels NFS kerberisés
- subtilités de configuration

`GSSAPIAuthentication`, `GSSAPIDelegateCredentials`, `KerberosAuthentication`

LDAP

Détails techniques

- ajout d'une méthode supplémentaire d'authentification
- authentification par ticket
- implementé par SASL
- mapping identité SASL <=> identité LDAP

Intérêts

- accès en écriture facilité
- population concernée spécifique

LDAP

Détails techniques

- ajout d'une méthode supplémentaire d'authentification
- authentification par ticket
- implementé par SASL
- mapping identité SASL <=> identité LDAP

Intérêts

- accès en écriture facilité
- population concernée spécifique

Cups

Détails techniques

- remplacement de la méthode d'authentification unique
- activation distincte pour l'impression et l'interface Web

Problème

- pas de repli sur l'authentification Basic
  exclusion des clients web incapables de gérer Negotiate

Cups

Détails techniques

- remplacement de la méthode d'authentification unique
- activation distincte pour l'impression et l'interface Web

Problème

- pas de repli sur l'authentification Basic
  exclusion des clients web incapables de gérer Negotiate

Plan

Authentification HTTP

Détails techniques

- ajout d'une méthode supplémentaire d'authentification
- authentification par ticket ou validation de mot de passe
- implementé par un module apache (*mod_authkerb*)

Difficultés

- comportements variable des clients
- configuration nécessaire
- intérêt variable en fonction de l'application

Authentification HTTP

Détails techniques

- ajout d'une méthode supplémentaire d'authentification
- authentification par ticket ou validation de mot de passe
- implementé par un module apache (*mod_authkerb*)

Difficultés

- comportements variable des clients
- configuration nécessaire
- intérêt variable en fonction de l'application

Applications Web

Authentification

- aucune gestion (munin, nagios)
- gestion déléguable au serveur web (cacti)
- gestion interne modulaire
- gestion interne monolithique

Autorisation

- filtrage tout ou rien au niveau du serveur web
- gestion interne de profils d'utilisateur (nagios, cacti)

Applications Web

Authentification

- aucune gestion (munin, nagios)
- gestion déléguable au serveur web (cacti)
- gestion interne modulaire
- gestion interne monolithique

Autorisation

- filtrage tout ou rien au niveau du serveur web
- gestion interne de profils d'utilisateur (nagios, cacti)

Plan

NFS

Détails techniques

- support GSSAPI introduit dans NFSv4, rétroporté vers NFSv3
- authentification, chiffrement ou contrôle d'intégrité

Intérêts

- sécurisation des accès NFS basé sur l'utilisateur, plutôt que sur la machine

NFS

Détails techniques

- support GSSAPI introduit dans NFSv4, rétroporté vers NFSv3
- authentification, chiffrement ou contrôle d'intégrité

Intérêts

- sécurisation des accès NFS basé sur l'utilisateur, plutôt que sur la machine

NFS

Difficultés

- mauvais support NFSv4 sur filer NetApp
- interférence avec CIFS sur filer NetApp
- configuration complexe
- lourdeur du déploiement
  mise en place de fichiers keytab sur les clients

Ouverture de session Windows

Détails techniques

- relation de confiance
- configuration Kerberos sur la machine
- mapping compte utilisateurs

Intérêt

- plus de problème de synchronisation de mot de passe
  intégration complète
- exploit technique

Ouverture de session Windows

Détails techniques

- relation de confiance
- configuration Kerberos sur la machine
- mapping compte utilisateurs

Intérêt

- plus de problème de synchronisation de mot de passe
  intégration complète
- exploit technique

Ouverture de session Windows

Difficultés

- forte complexité technique
- lourdeur du déploiement
  modification de la base de registre nécessaire
- double identité utilisateur
  `utilisateur@DOMAINE.AD` **vs** `utilisateur@DOMAINE.KERBEROS`
- situations problématiques pénibles à investiguer
  Windows 7 double boot

Problème

- pas de repli sur l'authentification NTLM
  exclusion des machines hors du domaine AD

Ouverture de session Windows

Difficultés

- forte complexité technique
- lourdeur du déploiement
  modification de la base de registre nécessaire
- double identité utilisateur
  `utilisateur@DOMAINE.AD` **vs** `utilisateur@DOMAINE.KERBEROS`
- situations problématiques pénibles à investiguer
  Windows 7 double boot

Problème

- pas de repli sur l'authentification NTLM
  exclusion des machines hors du domaine AD

Plan

Différentes implémentations

MIT

- implémentation originale
- multi-plateforme

Heimdal

- conséquence des restrictions US à l'export
- base Kerberos pour Samba 4

Microsoft

- depuis windows 2000
- extension protocole : PAC

Différentes implémentations

MIT

- implémentation originale
- multi-plateforme

Heimdal

- conséquence des restrictions US à l'export
- base Kerberos pour Samba 4

Microsoft

- depuis windows 2000
- extension protocole : PAC

Différentes implémentations

MIT

- implémentation originale
- multi-plateforme

Heimdal

- conséquence des restrictions US à l'export
- base Kerberos pour Samba 4

Microsoft

- depuis windows 2000
- extension protocole : PAC

Différentes intégrations

Linux

- clients ligne de commande et graphiques disponibles
- intégration possible via PAM

MacOS

- implémentation MIT incluse
- support natif dans `keychain`

Windows

- intégration transparente au sein d'un domaine Active Directory
- quasiment inutilisable en dehors d'un domaine Active Directory

Différentes intégrations

Linux

- clients ligne de commande et graphiques disponibles
- intégration possible via PAM

MacOS

- implémentation MIT incluse
- support natif dans `keychain`

Windows

- intégration transparente au sein d'un domaine Active Directory
- quasiment inutilisable en dehors d'un domaine Active Directory

Différentes intégrations

Linux

- clients ligne de commande et graphiques disponibles
- intégration possible via PAM

MacOS

- implémentation MIT incluse
- support natif dans `keychain`

Windows

- intégration transparente au sein d'un domaine Active Directory
- quasiment inutilisable en dehors d'un domaine Active Directory

Différents comportements

Création du SPN

- utilisation du nom fourni
- utilisation du nom canonique

Solutions

- canonicalisation coté client
- canonicalisation coté serveur
- multiplication des principaux

Différents comportements

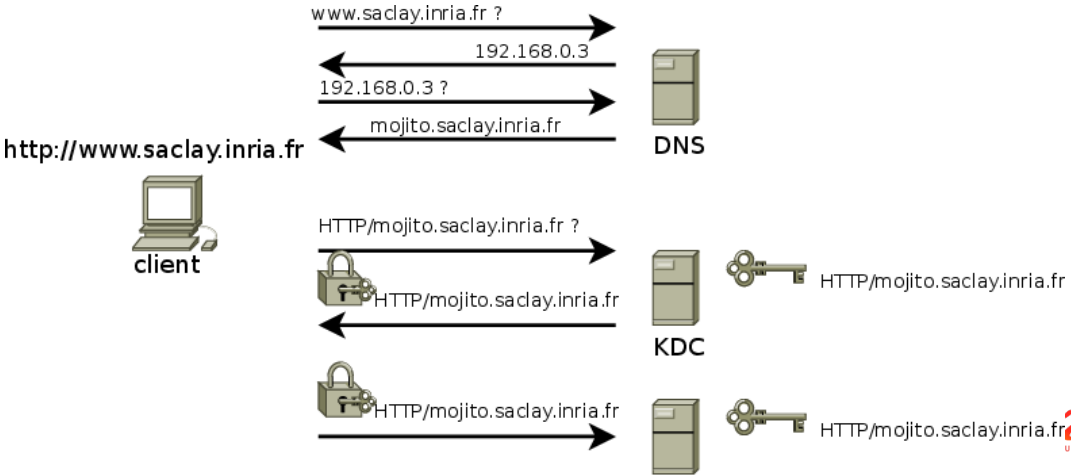
Création du SPN

- utilisation du nom fourni
- utilisation du nom canonique

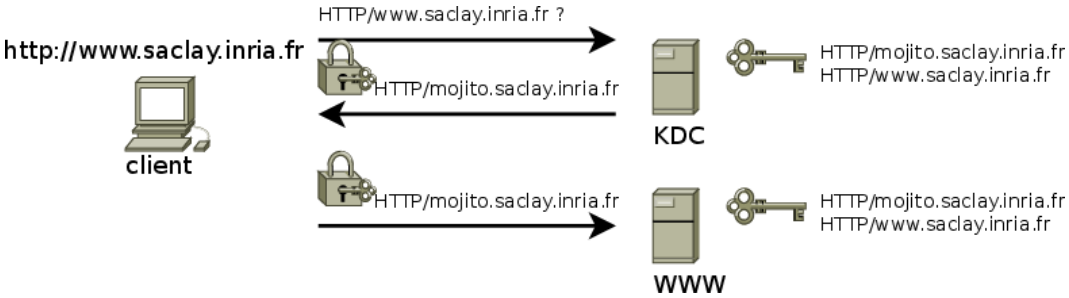
Solutions

- canonicalisation coté client
- canonicalisation coté serveur
- multiplication des principaux

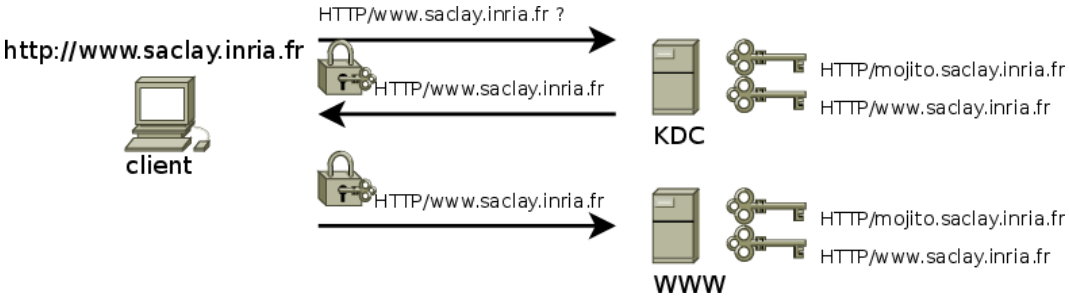
Canonicalisation coté client



Canonicalisation coté serveur



Multiplication des principaux



Plan

Évolutions

Kerberos

- Referals
- PKINIT

Intégration LDAP

- Schéma unique

  `http://tools.ietf.org/html/draft-chu-ldap-kdc-schema-00`

- Password Policy

  `http://tools.ietf.org/html/draft-behera-ldap-password-policy-10`

Évolutions

Kerberos

- Referals
- PKINIT

Intégration LDAP

- Schéma unique

  `http://tools.ietf.org/html/draft-chu-ldap-kdc-schema-00`

- Password Policy

  `http://tools.ietf.org/html/draft-behera-ldap-password-policy-10`

Conditions de succès

Deux critères

- audience cible
- conditions d'utilisation

Situations gagnantes

- public technique
- public quelconque
  - utilisation transparente
  - utilisation sans configuration
  - utilisation facultative

Conditions de succès

Deux critères

- audience cible
- conditions d'utilisation

Situations gagnantes

- public technique
- public quelconque
  - utilisation transparente
  - utilisation sans configuration
  - utilisation facultative