Mise en place d'un serveur CUPS

Installation du serveur CUPS

Configuration Système

Ajouter dans le fichier **/etc/group** un groupe pour les administrateurs du serveur CUPS :

```
admin:x:19999:ayello,dagorn,diascorn,frlemass,paubry
```

Ces utilisateurs seront autorisés pour certaines opérations spéciales (par exemple l'ajout d'imprimantes, la destruction de jobs ne leur appartenant pas, ...).

Configuration de Kerberos

Deux *principals* sont nécessaires :

- **ipp/server.ifsic.univ-rennes1.fr** pour les impressions
- **HTTP/server.ifsic.univ-rennes1.fr** pour l'accès à l'interface web de CUPS

```
[root@server ~]# kadmin
Authenticating as principal root/admin@UNIV-RENNES1.FR with password.
Password for root/admin@UNIV-RENNES1.FR:
kadmin:  addprinc -randkey ipp/server.ifsic.univ-rennes1.fr
WARNING: no policy specified for ipp/server.ifsic.univ-rennes1.fr@UNIV-RENNES1.FR; defaulting to no policy
Principal "ipp/server.ifsic.univ-rennes1.fr@UNIV-RENNES1.FR" created.
kadmin:  ktadd ipp/server.ifsic.univ-rennes1.fr
Entry for principal ipp/server.ifsic.univ-rennes1.fr with kvno 3, encryption type Triple DES cbc mode with HMAC
/sha1 added to keytab WRFILE:/etc/krb5.keytab.
Entry for principal ipp/server.ifsic.univ-rennes1.fr with kvno 3, encryption type ArcFour with HMAC/md5 added
to keytab WRFILE:/etc/krb5.keytab.
Entry for principal ipp/server.ifsic.univ-rennes1.fr with kvno 3, encryption type DES with HMAC/sha1 added to
keytab WRFILE:/etc/krb5.keytab.
Entry for principal ipp/server.ifsic.univ-rennes1.fr with kvno 3, encryption type DES cbc mode with RSA-MD5
added to keytab WRFILE:/etc/krb5.keytab.
kadmin:  addprinc -randkey HTTP/server.ifsic.univ-rennes1.fr
WARNING: no policy specified for HTTP/server.ifsic.univ-rennes1.fr@UNIV-RENNES1.FR; defaulting to no policy
Principal "HTTP/server.ifsic.univ-rennes1.fr@UNIV-RENNES1.FR" created.
kadmin:  ktadd HTTP/server.ifsic.univ-rennes1.fr
Entry for principal HTTP/server.ifsic.univ-rennes1.fr with kvno 3, encryption type Triple DES cbc mode with HMAC
/sha1 added to keytab WRFILE:/etc/krb5.keytab.
Entry for principal HTTP/server.ifsic.univ-rennes1.fr with kvno 3, encryption type ArcFour with HMAC/md5 added
to keytab WRFILE:/etc/krb5.keytab.
Entry for principal HTTP/server.ifsic.univ-rennes1.fr with kvno 3, encryption type DES with HMAC/sha1 added to
keytab WRFILE:/etc/krb5.keytab.
Entry for principal HTTP/server.ifsic.univ-rennes1.fr with kvno 3, encryption type DES cbc mode with RSA-MD5
added to keytab WRFILE:/etc/krb5.keytab.
kadmin:  exit
[root@server ~]#
```

Configuration de CUPS

La configuration de CUPS se fait dans le fichier **/etc/cups/cupds.conf** :

On précise le groupe des administrateurs du serveur :

```
#SystemGroup sys root
SystemGroup admin
```

On autorise l'administration distante :

```
#Listen localhost:631
Port 631
Listen /var/run/cups/cups.sock
```

On indique que l'authentification par défaut sera Kerberos :

```
DefaultAuthType Negotiate
```

On indique que la politique par défaut des imprimantes sera kerberos (cf plus bas) :

```
DefaultPolicy kerberos
```

On écrit enfin la politique kerberos en adaptant légèrement la politique prédéfinie authenticated :

```
<Policy kerberos>
  <Limit Create-Job Print-Job Print-URI>
    AuthType Default
    Require valid-user
    Order deny,allow
  </Limit>
  <Limit Send-Document Send-URI Hold-Job Release-Job Restart-Job Purge-Jobs Set-Job-Attributes Create-Job-
Subscription Renew-Subscription Cancel-Subscriptio\
n Get-Notifications Reprocess-Job Cancel-Current-Job Suspend-Current-Job Resume-Job CUPS-Move-Job CUPS-Get-
Document>
    AuthType Default
    Require user @OWNER @SYSTEM
    Order deny,allow
  </Limit>
  <Limit CUPS-Add-Modify-Printer CUPS-Delete-Printer CUPS-Add-Modify-Class CUPS-Delete-Class CUPS-Set-Default>
    AuthType Default
    Require user @SYSTEM
    Order deny,allow
  </Limit>
  <Limit Pause-Printer Resume-Printer Enable-Printer Disable-Printer Pause-Printer-After-Current-Job Hold-New-
Jobs Release-Held-New-Jobs Deactivate-Printer \
Activate-Printer Restart-Printer Shutdown-Printer Startup-Printer Promote-Job Schedule-Job-After CUPS-Accept-
Jobs CUPS-Reject-Jobs>
    AuthType Default
    Require user @SYSTEM
    Order deny,allow
  </Limit>
  <Limit Cancel-Job CUPS-Authenticate-Job>
    AuthType Default
    Require user @OWNER @SYSTEM
    Order deny,allow
  </Limit>
  <Limit All>
    Order deny,allow
  </Limit>
</Policy>
```

NB : par rapport à la politique **authenticated**, on rajoute simplement la directive **Require valid-user** pour les opérations *Create-Job*, *Print-Job* et *Print-URI*, qui limitera l'impression aux utilisateurs authentifiés.

Debug

Pour obtenir plus d'informations, positionner la directive **LogLevel** à **debug** dans **/etc/cups/cupds.conf** :

```
LogLevel debug
```

Les logs se trouvent dans **/var/log/cups/error_log**.

Intégration des clients

Linux

Chaque client Linux a son propre serveur CUPS, qui ne fait que rediriger vers le serveur principal.

Pour cela, on indique simplement dans le fichier **/etc/cups/client.conf** vers quel serveur rediriger toutes les requêtes :

```
ServerName server.ifsic.univ-rennes1.fr
```

Windows