

CUPS serveur d'impression

Ce tutoriel développe la mise en place d'un serveur d'impression CUPS.

Les clients Linux enverront directement leurs travaux d'impression à CUPS. Les clients Windows passeront par Samba qui transférera les travaux d'impression à CUPS. CUPS sera configuré en mode RAW (mode brut) c'est à dire qu'il n'utilisera aucun pilote pour formater les travaux d'impression avant de les envoyer aux imprimantes réseau.

Pourquoi procéder ainsi ?

Premièrement, il n'y a pas beaucoup de pilotes d'imprimantes récentes fournis dans CUPS. Deuxièmement, une imprimante de "bonne qualité" doit respecter les protocoles d'impression standards en acceptant les travaux d'impression bruts et en dialoguant correctement avec les services d'impression (informations transmises à CUPS dans notre cas). Certaines marques font cet effort, d'autres non ... partant du principe que 90% des acheteurs utilisent leurs pilotes Windows.

Installation des packages

Sur printer.alex.lan :

cupsys openssl libnss-ldap libpam-ldap nscd

Sur fs1.alex.lan et fs2.alex.lan :

cupsys-client

Configuration de CUPS

Modifiez le fichier /etc/resolv.conf :

```
search alex.lan srl.alex.lan alex.dmz
nameserver 172.17.0.1
nameserver 172.16.0.1
```

Modifiez le fichier /etc/network/interfaces :

```
# The loopback network interface
auto lo eth0
iface lo inet loopback

# The primary network interface
allow-hotplug eth0
iface eth0 inet static
address 172.17.0.5
netmask 255.255.0.0
gateway 172.17.0.254
up route add -net 172.18.0.0/16 gw 172.17.0.253
```

On peut gérer facilement CUPS depuis une interface web http. Par contre, pour les opérations d'administration (création, modification d'imprimantes, ...) il est conseillé de passer par une connexion https.

Nous allons donc générer une clef et un certificat SSL :

```
printer:~# openssl req -new -x509 -keyout /etc/cups/ssl/printer.key
-out /etc/cups/ssl/printer.crt -days 3650 -nodes

Generating a 1024 bit RSA private key
.....++++++
.....++++++
writing new private key to '/etc/cups/ssl/printer.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a
DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:FR
State or Province Name (full name) [Some-State]:Haute-Savoie
Locality Name (eg, city) []:Alex
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Alex
Organizational Unit Name (eg, section) []:
Common Name (eg, YOUR name) []:printer.alex.lan
Email Address []:root@alex.lan
printer:~#
```

Changez les droits sur la clef et le certificat :

```
printer:~# chmod 600 /etc/cups/ssl/printer.*
```

Modifiez le fichier /etc/cups/cupsd.conf :

```
# Sample configuration file for the Common UNIX Printing System (CUPS)
# scheduler. See "man cupsd.conf" for a complete description of this
# file.
#
# ServerName:
# ServerName indique le nom d'hôte qui doit être envoyé aux clients.
# Par défaut, le nom d'hôte FQDN dans le fichier /etc/hosts.
#
ServerName printer.alex.lan
#
```

```
# Port:
# Indique sur quel port CUPS sera en attente de connexion.
# Plusieurs lignes de Port peuvent être indiquées pour écouter sur
# plusieurs ports.
#
# Samba communique avec CUPS en mode non crypté.
# Il faut donc activer l'écoute IPP non crypté.
#
# Port 80
# Port 631
# Listen hostname
# Listen hostname:80
# Listen hostname:631
# Listen 1.2.3.4
# Listen 1.2.3.4:631
#
Port 631

#
# ServerCertificate:
# ServerCertificate définit l'emplacement du fichier de certificat SSL
# utilisé par le serveur lors de la négociation des connexions
# encryptées. Le certificat ne doit pas être encrypté (protégé par un mot
# de passe) car l'ordonnanceur fonctionne normalement en arrière-plan et
# et ne sera pas en mesure de demander un mot de passe.
#
ServerCertificate /etc/cups/ssl/printer.crt
#
# ServerKey:
# ServerKey indique l'emplacement du fichier de clef privée SSL utilisé
# par le serveur pour négocier les connexions encryptées.
#
ServerKey /etc/cups/ssl/printer.key

#
# SSLPort:
# SSLPort indique le port écouté pour les connexions sécurisées.
# Plusieurs lignes SSLPort peuvent être indiquées pour écouter les
# connexions sur plusieurs ports.
#
SSLPort 632

#
# Browsing:
# Browsing permet d'annoncer les imprimantes partagées sur le réseau.
#
Browsing Off

# Log general information in error_log - change "info" to "debug" for
# troubleshooting...
LogLevel warn
```

```
# Nom du groupe administrateur pour CUPS.
#SystemGroup lpadmin
SystemGroup 'Print Operators'

# Default authentication type, when authentication is required...
DefaultAuthType Basic

# Définition des accès aux ressources http.
#
# Accès à la page d'accueil de CUPS pour localhost, le réseau où se
# trouve le serveur et le réseau 172.18.0.0/16.
<Location />
Order Deny,Allow
Deny From All
Allow From 127.0.0.1
Allow From @LOCAL
Allow From 172.18.0.0/16
# Autorise l'adresse du proxy.
Allow From 172.16.0.4
</Location>

# Accès aux pages admin de CUPS.
# Demande une connexion cryptée et une authentification.
<Location /admin>
Encryption Required
AuthType Basic
Require user @SYSTEM
Order Deny,Allow
Deny From All
Allow From 127.0.0.1
Allow From @LOCAL
Allow From 172.18.0.0/16
# Autorise l'adresse du proxy.
Allow From 172.16.0.4
</Location>

# Accès aux pages de configuration de CUPS.
<Location /admin/conf>
AuthType Basic
Require user @SYSTEM
Order Deny,Allow
Deny From All
Allow From 127.0.0.1
Allow From @LOCAL
Allow From 172.18.0.0/16
# Autorise l'adresse du proxy.
Allow From 172.16.0.4
</Location>

# Définition des politiques de gestion des travaux d'impression.
<Policy default>
```

```
# Les opérations en rapport avec les travaux d'impression peuvent être
# faites par le propriétaire du travail envoyé, ou par les
administrateurs.
```

```
<Limit Send-Document Send-URI Hold-Job Release-Job Restart-Job Purge-
Jobs Set-Job-Attributes Create-Job-Subscription Renew-Subscription
Cancel-Subscription Get-Notifications Reprocess-Job Cancel-Current-Job
Suspend-Current-Job Resume-Job CUPS-Move-Job>
```

```
    Require user @OWNER @SYSTEM
    Order deny,allow
</Limit>
```

```
# Les opérations d'administration peuvent être faites uniquement par
# un membre du groupe administrateur.
```

```
<Limit Pause-Printer Resume-Printer Set-Printer-Attributes 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-Add-
Printer CUPS-Delete-Printer CUPS-Add-Class CUPS-Delete-Class CUPS-Accept-
Jobs CUPS-Reject-Jobs CUPS-Set-Default>
```

```
    AuthType Basic
    Require user @SYSTEM
    Order deny,allow
</Limit>
```

```
# Seulement le propriétaire du travail envoyé ou les administrateurs
# peuvent annuler un travail d'impression.
```

```
<Limit Cancel-Job CUPS-Authenticate-Job>
    Require user @OWNER @SYSTEM
    Order deny,allow
</Limit>
```

```
<Limit All>
    Order deny,allow
</Limit>
```

```
</Policy>
```

```
#
# Printcap: the name of the printcap file. Default is /etc/printcap.
# Leave blank to disable printcap file generation.
```

```
#
Printcap /var/run/cups/printcap
```

```
#
# PrintcapFormat: the format of the printcap file, currently either
# BSD or Solaris. The default is "BSD".
```

```
#
#PrintcapFormat BSD
#PrintcapFormat Solaris
```

```
#
# PrintcapGUI: the name of the GUI options panel program to associate
# with print queues under IRIX. The default is "/usr/bin/glpoptions"
# from ESP Print Pro.
#
# This option is only used under IRIX; the options panel program
# must accept the "-d printer" and "-o options" options and write
# the selected printer options back to stdout on completion.
#
#PrintcapGUI /usr/bin/glpoptions
```

Redémarrez le service CUPS :

```
printer:~# /etc/init.d/cupsys restart
Restarting Common Unix Printing System: cupsd.
printer:~#
```

Pour visualiser les ports écoutés par CUPS :

```
printer:~# netstat -paute | grep cups
tcp        0      0  *:ipp      *:*        LISTEN     root       7790       2334/cupsd
tcp        0      0  *:632      *:*        LISTEN     root       7792       2334/cupsd
tcp6       0      0  *:ipp      *:*        LISTEN     root       7789       2334/cupsd
tcp6       0      0  *:632      *:*        LISTEN     root       7791       2334/cupsd
printer:~#
```

Nous allons relier ce serveur aux annuaires OpenLDAP pour que CUPS puisse authentifier les membres du groupe administrateur et connaître les noms des utilisateurs qui lui envoient des travaux d'impression.

Copiez depuis le serveur pdc.alex.lan, le certificat des serveurs pdc et bdc, après avoir créé le répertoire /etc/ldap/tls :

```
printer:~# mkdir /etc/ldap/tls

printer:~# scp
root@172.17.0.3:/etc/ldap/tls/ldap_*dc_cert.pem /etc/ldap/tls/
```

Modifiez le fichier /etc/ldap/ldap.conf :

```
TLS_CACERTDIR /etc/ldap/tls
TLS_REQCERT allow

BASE dc=alex,dc=fr
URI ldaps://bdc.alex.lan ldaps://pdc.alex.lan
```

Modifiez le fichier /etc/libnss-ldap.conf :

```
base dc=alex,dc=fr

uri ldaps://bdc.alex.lan ldaps://pdc.alex.lan

ldap_version 3

scope one

timelimit 30

bind_timelimit 30

bind_policy soft

pam_filter objectclass=posixaccount

pam_login_attribute uid

nss_base_passwd      ou=Users,dc=alex,dc=fr?one
nss_base_shadow      ou=Users,dc=alex,dc=fr?one
nss_base_group       ou=Groups,dc=alex,dc=fr?one

# OpenLDAP SSL mechanism
# start_tls mechanism uses the normal LDAP port, LDAPS typically 636
#ssl start_tls
ssl on
```

Faites un lien symbolique de /etc/libnss-ldap.conf vers /etc/pam_ldap.conf :

```
printer:~# ln -sf /etc/libnss-ldap.conf /etc/pam_ldap.conf
```

Configuration de PAM avec LDAP

Modifiez le fichier /etc/pam.d/cupsys :

```
#@include common-auth
#@include common-account
#@include common-session
#@include common-password

auth required      pam_env.so
auth sufficient     pam_unix.so nullok_secure
auth sufficient     pam_ldap.so use_first_pass
auth required      pam_deny.so

account required    pam_unix.so
account sufficient  pam_ldap.so
```

```
session required      pam_limits.so
session required      pam_unix.so
session optional      pam_ldap.so
```

Modifiez le fichier `/etc/nsswitch.conf` :

```
passwd:      compat ldap
group:       compat ldap
shadow:      compat ldap

hosts:       files dns
networks:    files

protocols:   db files
services:    db files
ethers:      db files
rpc:         db files

netgroup:    nis
```

Modifiez le fichier `/etc/nscd.conf` :

```
#
# /etc/nscd.conf
#
# Currently supported cache names (services): passwd, group, hosts
#
# logfile                /var/log/nscd.log
# threads                6
# max-threads            128
server-user              nobody
# stat-user              somebody
debug-level              0
# reload-count           5
paranoia                 no
# restart-interval       3600

enable-cache             passwd             yes
positive-time-to-live    passwd             600
negative-time-to-live    passwd             20
suggested-size           passwd             400
check-files              passwd             yes
persistent               passwd             yes
shared                   passwd             yes

enable-cache             group              yes
positive-time-to-live    group              3600
negative-time-to-live    group              60
```


suggested-size	group	211
check-files	group	yes
persistent	group	yes
shared	group	yes
enable-cache	hosts	yes
positive-time-to-live	hosts	3600
negative-time-to-live	hosts	20
suggested-size	hosts	211
check-files	hosts	yes
persistent	hosts	yes
shared	hosts	yes

Redémarrez le service nscd :

```
printer:~# /etc/init.d/nscd restart
Restarting Name Service Cache Daemon: nscd.
```

Vous pouvez accéder à l'interface de gestion web de CUPS :
<http://printer.alex.lan:631>

Configuration des postes clients Linux

Créez le fichier /etc/cups/client.conf :

```
#
# ServerName:
# Le nom FQDN de votre serveur CUPS.
#
ServerName printer.alex.lan

#
# Encryption:
# Pour utiliser ou non encryption SSL, les valeurs possible :
#
# Always - Always use encryption (SSL)
# Never - Never use encryption
# Required - Use TLS encryption upgrade
# IfRequested - Use encryption if the server requests it
#
Encryption Always
```

Configuration des postes clients Windows

Depuis une session administrateur sur le poste Windows, tapez l'adresse \\fs dans l'explorateur de fichiers, authentifiez-vous avec n'importe quel compte du domaine.

Double cliquez sur l'icône de l'imprimante que vous souhaitez installer, un message apparait, validez par OK.

L'assistant d'ajout d'imprimante apparait, choisissez "Disque fourni...".

Insérez le CD du pilote pour l'imprimante concernée et indiquez le fichier .INF du pilote puis validez.

Choisissez le modèle d'imprimante, puis OK.

Une fenêtre apparait, allez dans le menu Imprimante > Propriétés > "Imprimer une page de test".

Source :

<http://www.cups.org/documentation.php/ref-cupsd-conf.html>

Document mis à jour : 09/01/08



Ce document est publié sous licence [Creative Commons Attribution, Partage à l'identique, Contexte non commercial 3.0](http://creativecommons.org/licenses/by-nc-sa/3.0/deed.fr) :
<http://creativecommons.org/licenses/by-nc-sa/3.0/deed.fr>