Les clients Scribe

EOLE 2.5

création : Mai 2015 Version : révision : Avril 2018

EOLE 2.5

Version : révision : Avril 2018

Date : création : Mai 2015

Editeur : Pôle national de compétences Logiciels Libres

Auteur(s) : Équipe EOLE

Pour toute information concernant ce projet vous pouvez nous joindre :

- Par courrier électronique : eole@ac-dijon.fr
- Par FAX : 03-80-44-88-10
- Par courrier : EOLE-DSI - 2G, rue du Général Delaborde - 21000 DIJON
- Le site du Pôle national de compétences Logiciels Libres : http://eole.orion.education.fr

Table des matières

Chapitre 1

Les clients GNU/Linux

1. Principe du client GNU / Linux

L'objectif est d'obtenir des postes de travail sous GNU / Linux dont l'authentification et le montage des répertoires de travail se fait sur les modules Scribe ou Horus.

Authentification PAM / LDAP

Un système GNU / Linux peut aller chercher dans différents endroits pour authentifier des utilisateurs. Par défaut il utilise le fichier `/etc/passwd`.

Cependant on peut lui ajouter d'autres sources de données.

Le module PAM[p.142] va permettre de vérifier, à la demande d'un service, la validité d'une authentification à un service d'authentification tel que LDAP[p.142] ou Kerberos[p.141].

Aussi, il ne suffit pas de modifier la configuration de PAM pour que cela fonctionne. En général, il faut également installer un service qui va pouvoir activer ce pont entre PAM et le service d'authentification :

- `libpam-ldap` permet à PAM d'utiliser LDAP pour l'authentification
- `libpam-krb5` permet de faire le pont entre PAM et Kerberos pour l'authentification

L'authentification sur les postes clients GNU / Linux va principalement se baser sur 2 services :

- NSS (Name Service Switch, NS Switch) est une bibliothèque générique de résolution de nom.

  Elle permet :
  - d'authentifier les utilisateurs via le LDAP ;
  - d'obtenir les informations des utilisateurs à travers le LDAP.
- nslcd est utilisé pour lier l'authentification LDAP et de récupérer ses informations

  nslcd est un démon qui va faire des requêtes LDAP pour les processus locaux qui veulent faire utilisateur, groupe et autres recherches de nommage (NSS) ou de faire l'authentification des utilisateurs, d'autorisation ou de modification de mot de passe (PAM)
- nscd qui fera un cache et vous évitera des problèmes liés à la performance et au coupure du réseau.

NSS

Les informations telles que les noms d'utilisateurs, groupes et autres, stockées dans des fichiers situés dans `/etc/`, vont être fournies grâce à NSS (Name Service Switch) à l'aide du serveur LDAP du module Scribe.

Un serveur LDAP peut gérer les bases de données suivantes :

- aliases (alias de messagerie, ignoré par la plupart des démons de courrier) ;

- ethers (adresses Ethernet) ;
- group (groupes d'utilisateurs) ;
- hosts (noms et adresses d'hôte) ;
- netgroup (groupes d'hôtes et d'utilisateurs pour le contrôle d'accès) ;
- networks (informations concernant le réseau) ;
- passwd (comptes des utilisateurs) ;
- protocols (protocoles réseau) ;
- rpc (base de données des numéros de programmes rpc) ;
- services (liste des services réseau Internet) ;
- shadow (informations sécurisées sur les comptes utilisateurs).

Les données gérer dans l'annuaire LDAP du module Scribe sont :

- passwd (comptes des utilisateurs) ;
- group (groupes d'utilisateurs) ;
- shadow (informations sécurisées sur les comptes utilisateurs).

#fixme : à compléter

Il existe actuellement deux paquets disponibles pour configurer les requêtes NSS via LDAP :

- `libnss-ldap`
  plus mature mais plus complexe, `libnss-ldap` a quelques problèmes connus au démarrage
- `libnss-ldapd`
  plus simple, amélioré, mais moins mature

Le choix entre les deux dépend des besoins, ici `libnss-ldapd` a été retenu.

nslcd

nslcd (local LDAP name service daemon) est un démon qui va faire des requêtes LDAP pour les processus locaux basés sur un fichier de configuration simple.

nslcd utilise nscd pour mettre en cache les informations et permet de limiter les requêtes au serveur LDAP.

Le durée du cache peut être réglé en modifiant les valeurs `xxx-time-to-live` dans le fichier `/etc/nscd.conf`, les valeurs par défaut suffise dans la plupart des cas.

Montage des répertoires partagés

Il existe actuellement 2 méthodes pour mettre en place des montages distants depuis le client GNU/Linux ver le module Scribe :

- méthode basée sur NFS ;
- méthode basée sur les montages Samba.

Méthode basée sur NFS

La méthode basée sur le partage de fichiers NFS[p.142] est valable aussi bien pour des clients GNU/Linux existants que pour la mise en œuvre des clients légers Eclair (serveur de clients légers).

Pour fonctionner, le client GNU/Linux a besoin que le service NFS soit installé et activé sur le module Scribe.

Le logiciel Gaspacho permet d'appliquer des configurations sur les postes clients.

Tous les comptes locaux ont un accès au module Scribe.

#fixme

Méthode basée sur Samba

Cette solution basée sur SMB[p.143] est valable pour des clients GNU/Linux.

Un fichier de configuration doit être ajouté sur le module Scribe pour la prise en charge des partages.

Pour fonctionner, le client GNU/Linux doit pouvoir monter des partitions distante par SMB avec l'utilitaire `cifs-utils.`

Le logiciel Gaspacho permet d'appliquer des configurations sur les postes clients.

Cette méthode crée autant de comptes sur l'ordinateur client qu'il y a de comptes dans l'annuaire du module Scribe.

#fixme

Intégration dans l'environnement graphique

Un certains nombres de modification permette une intégration plus forte dans l'environnement graphique.

Appliquer des règles

Gaspacho est une application qui permet de configurer automatiquement le poste de travail de l'utilisateur selon son profil.

2. Configuration des comptes utilisateurs sur le serveur

Configuration des comptes utilisateurs

Les utilisateurs du module Scribe doivent avoir l'interpréteur de commande activé.

Cette manipulation se fait au moment de l'importation des utilisateurs sur le module Scribe.

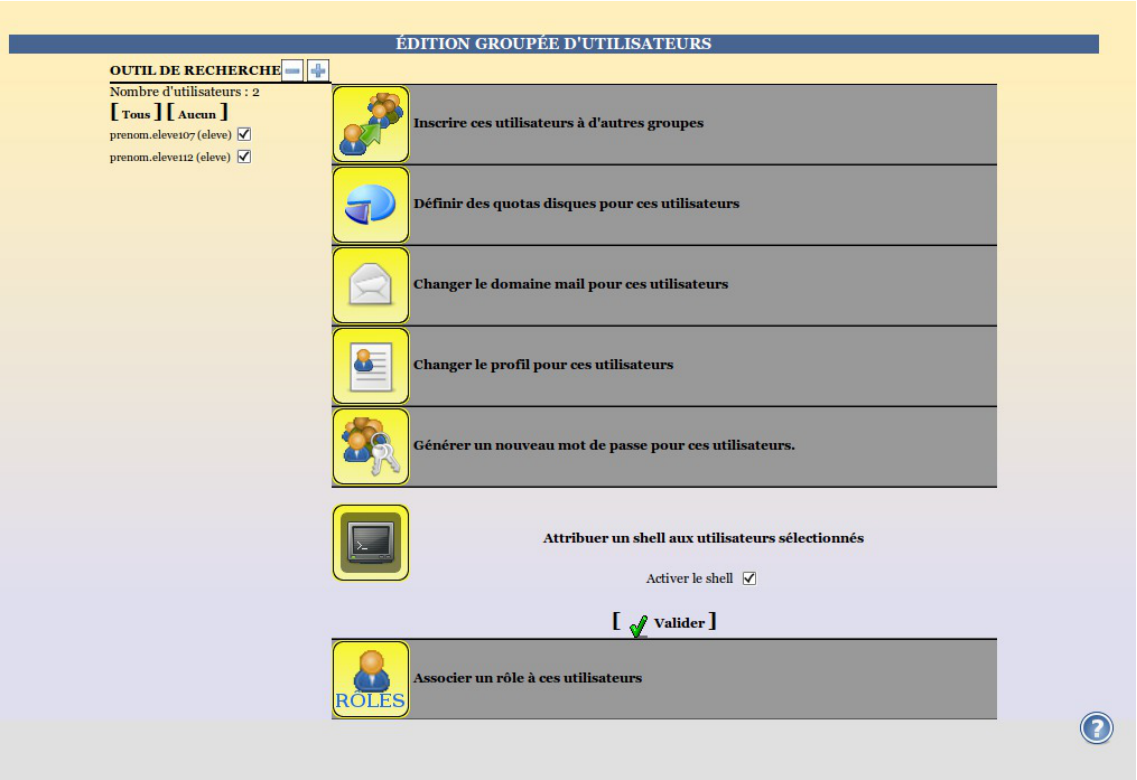
Si l'importation a été faite, il est possible de faire une édition groupée des utilisateurs devant avoir un

interpréteur de commande activé.

Dans l'EAD → Gestion → Édition groupée.

Sélectionner les critères de recherche et cliquer sur le bouton Lister.

Décocher les utilisateurs en trop si besoin et cliquer sur Modifier le shell associé à ces utilisateurs.



L'option ☑ Activer le shell est cochée, cliquer alors sur le bouton Valider.

Une fenêtre affiche `Le shell des utilisateurs sélectionnés a bien été modifié`.

Activation massive du shell en ligne de commande

La commande suivante permet d'activer le shell de tous les utilisateurs en une seule fois :

```
# ldapsearch -x cn=DomainUsers|grep memberUid:|awk '{print $2}' | while read i
> do
```

```
> echo "mise en place du shell pour $i"
> smbldap-usermod -s /bin/bash $i
> done
```

Commande en une seule ligne :

```
# ldapsearch -x cn=DomainUsers|grep memberUid:|awk '{print $2}' | while read i ; do echo "mise en place du shell pour $i"; smbldap-usermod -s /bin/bash $i; done
```

Ne pas forcer le changement de mot de passe

Dans le cas d'une création de nouveaux comptes utilisateurs, il ne faut pas utiliser la fonctionnalité `forcer le changement de mot de passe à la première connexion` se trouvant dans les outils d'importation des comptes et de l'édition groupée de l'EAD. La connexion du client serait impossible car il ne gère pas le changement de mot de passe.

#fixme
Si vous utilisez l'authentification par proxy dans votre établissement il faut obligatoirement spécifier l'utilisateur/mot de passe sous GNU/Linux (L'authentification transparente du proxy utilise un mécanisme interne de Microsoft).

3. Authentification LDAP depuis le client GNU / Linux

La procédure suivante propose l'intégration d'un client Ubuntu 15.04 vivid à jour :

```
root@pclinux:/home/eole# apt-get update && apt-get upgrade
```

L'adresse du poste client est obtenu par DHCP et le nom de machine du module Scribe est résolue.

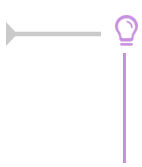
Configuration de l'authentification LDAP
http://wiki.debian.org/fr/LDAP/NSS

Installation de libnss-ldapd

L'installation de libnss-ldapd se fait à l'aide de la commande apt-get install :

```
root@pclinux:/home/eole# apt-get install libnss-ldapd
```

Des paquets supplémentaires seront installés : `ldap-utils` `libpam-ldapd` `nscd` `nslcd` `nslcd-utils`



La configuration de `libnss-ldapd` et `nslcd` est interactive en fin d'installation.

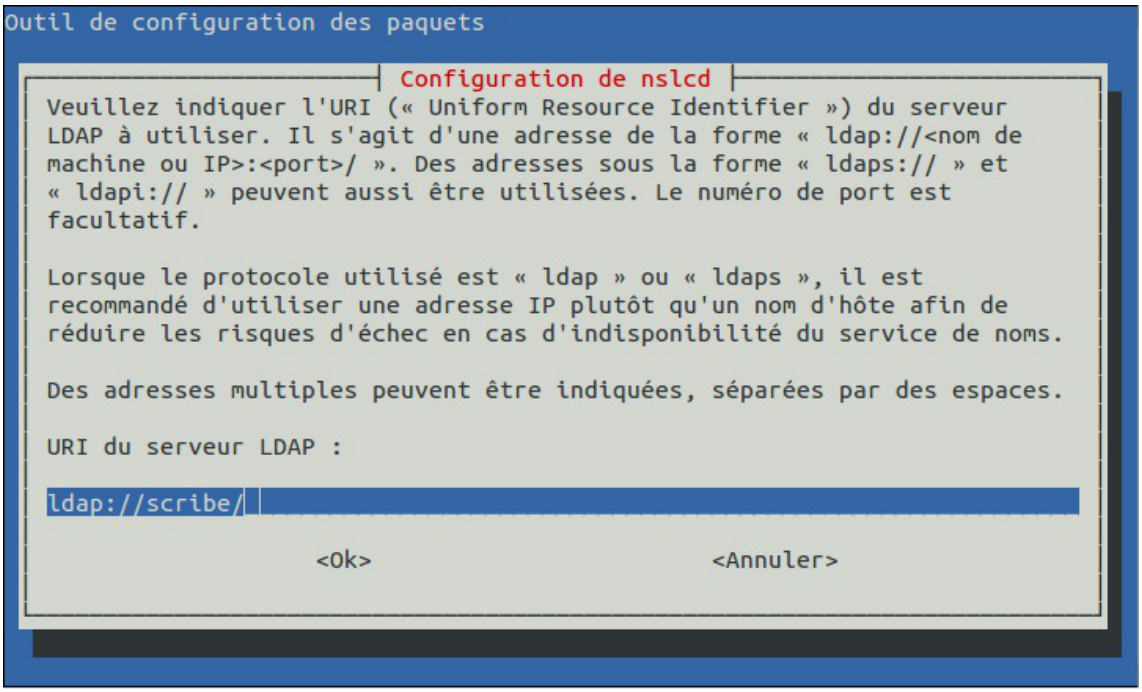
Pour une configuration manuelle avec édition des fichiers de configuration il faut ajouter

> l'option -y à la commande `apt-get install` :
> `root@pclinux:/home/eole# apt-get -y install libnss-ldapd`

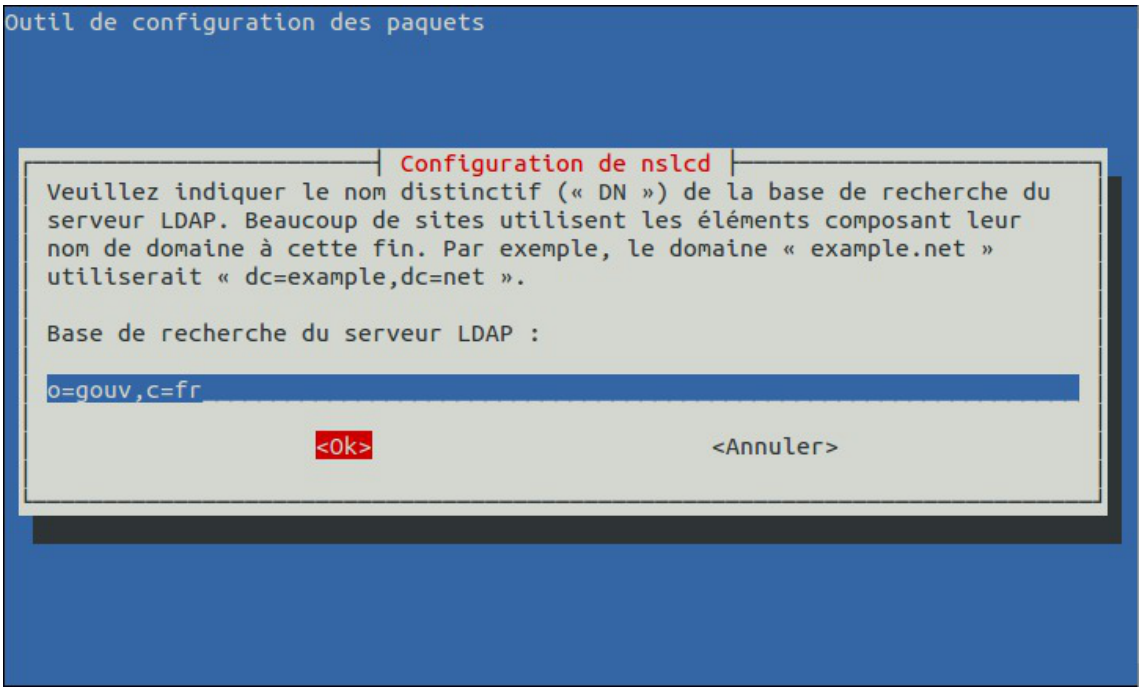
Configuration interactive

Si l'installation 0 question n'a pas été adoptée 3 écrans permettent, à la fin de l'installation , de configurer le service :

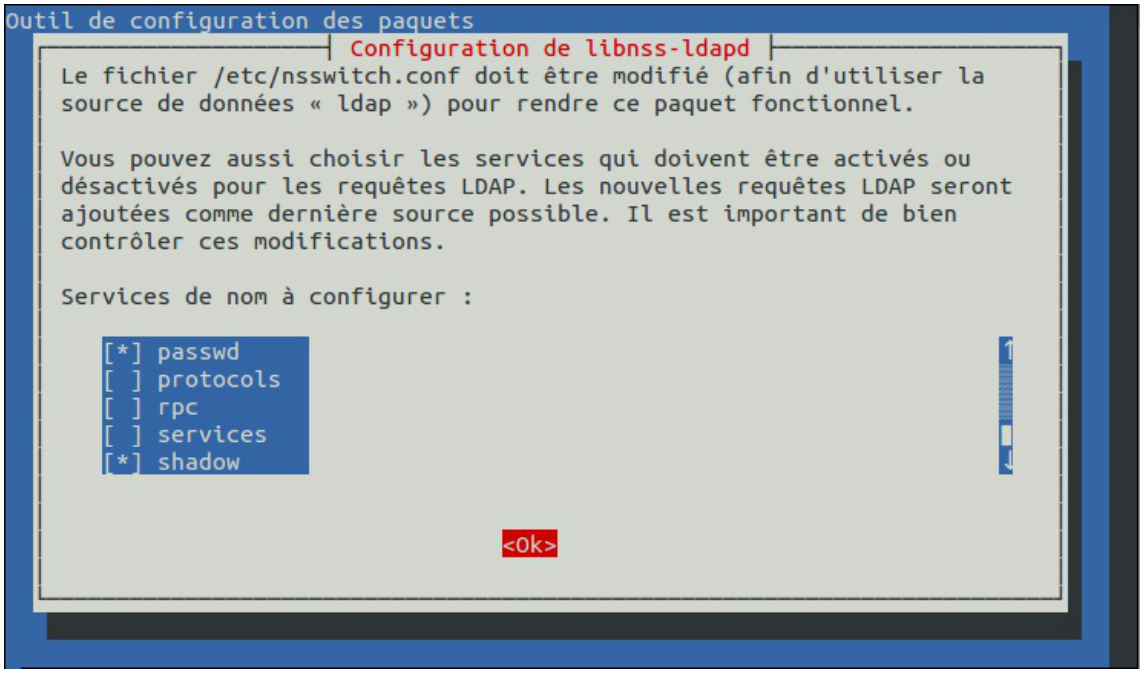
- configuration de `nslcd` : saisir l'adresse ou le nom de machine du module Scribe, il ne faut pas omettre le / à la fin, le port peut être spécifié ;



- configuration de `nslcd` : saisir le nom distinctif de la base de recherche, saisir `o=gouv, c=fr` ;



- configuration `nsswitch` des ressources à chercher dans l'annuaire LDAP : cocher `passwd`, `group` et `shadow` ;



Configuration manuelle

La configuration peut-être réalisée ou adaptée en éditant les fichiers suivants :

- /etc/nslcd.conf

```
# The location at which the LDAP server(s) should be reachable.
uri ldap://scribe/
# The search base that will be used for all queries.
base o=gouv,c=fr
```

- /etc/nsswitch.conf

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

Le mode compat est destiné à travailler avec NIS[p.142].

Test de liaison avec l'annuaire LDAP :

root@pclinux:/home/eole# ldapsearch -h scribe:389 -b o=gouv,c=fr -x uid=utilisateurScribe

```
root@pclinux:/home/eole# ldapsearch -h scribe:389 -b o=gouv,c=fr
-x uid=test.prof
uid: test.prof
uidNumber: 10034
gidNumber: 10001
homeDirectory: /home/t/test.prof
```

```
sambaLogonTime: 0
sambaLogoffTime: 2147483647
sambaKickoffTime: 2147483647
sambaPwdCanChange: 0
sambaSID: S-1-5-21-1756604377-3768680913-3336469871-21068
sambaPrimaryGroupSID:
S-1-5-21-1756604377-3768680913-3336469871-21003
sambaProfilePath: \\scribe\netlogon\profil
sambaHomePath: \\scribe\test.prof\perso
sambaHomeDrive: U:
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: posixAccount
objectClass: shadowAccount
objectClass: inetOrgPerson
objectClass: sambaSamAccount
objectClass: administrateur
objectClass: ENTPerson
objectClass: ENTAuxEnseignant
objectClass: radiusprofile
cn: test prof
sn: prof
givenName: test
displayName: test prof
gecos: test prof
LastUpdate: 20151107
ENTPersonLogin: test.prof
ENTPersonJointure: ENT
ENTPersonProfils: enseignant
ENTPersonNomPatro: prof
codecivilite: 1
ENTPersonSexe: M
personalTitle: M.
intid: 12
radiusTunnelType: VLAN
radiusFilterId: Enterasys:version=1:policy=Enterprise User
radiusTunnelMediumType: IEEE-802
mail: test.prof@etb1.ac-test.fr
mailHost: localhost
```

```
mailDir: /home/mail/test.prof/
typeadmin: 0
loginShell: /bin/bash
sambaAcctFlags: [U]
sambaPwdLastSet: 1447316673
sambaPwdMustChange: 1447316673
shadowLastChange: 16751
# search result
search: 2
result: 0 Success
# numResponses: 2
# numEntries: 1
```

```
root@pclinux:/home/eole# getent passwd utilisateurScribe
utilisateurScribe:x:10034:10001:test prof:/home/u/utilisateurScribe:/bin/bash
root@pclinux:/home/eole#
```

```
root@pclinux:/home/eole# getent passwd test.prof
test.prof:x:10034:10001:test prof:/home/t/test.prof:/bin/bash
root@pclinux:/home/eole#
```

Tester la prise en compte des utilisateurs

ssh test.prof@10.1.2.52

test.prof@10.1.2.52's password:

Welcome to Ubuntu 15.04 (GNU/Linux 3.19.0-15-generic x86_64)

4. Problèmes d'authentification rencontrés et solutions

Pendant le débogage nscd peut masquer les problèmes en fournissant des entrées de son cache, il est donc préférable de stopper nscd (démon de Name Service Caching) avec la commande suivante :

```
# service nscd stop
```

Reconfigurer libnss-ldapd et nslcd

Si la configuration post installation ne convient pas il est possible de relancer la configuration de `libnss-ldapd` et de `nslcd` avec la commande dpkg-reconfigure.

```
# dpkg-reconfigure libnss-ldapd
```

```
# dpkg-reconfigure nslcd
```

Utilisation de la commande `dpkg-reconfigure` :

```
# dpkg-reconfigure libnss-ldapd
```

et

```
# dpkg-reconfigure nslcd
```

Problème de cache

Un ou plusieurs mots de passe de compte utilisateurs ont été changé sur le module Scribe. Il faut rafraîchir le cache de `nscd`.

Nettoyer le cache

Nettoyer le cache avec la commande `nscd` :

```
# nscd -i passwd
# nscd -i group
# nscd -i shadow
```

Relancer le service permet également de vider le cache :

```
# service nscd restart
```

Utiliser l'outil nss-updatedb

Le paquet `nss-updatedb` fourni la commande `nss_updatedb` qui permet de créer des bases de données de type Berkeley DB stockant les données équivalentes aux `passwd` et `group` du NSS. Il faut l'invoquer régulièrement afin de maintenir à jour ces bases de données.

Cela permet à un utilisateur du domaine de se reconnecter à sa session lorsqu'il est hors ligne.

Installer l'outil `nss-updatedb` :

```
root@pclinux:/etc# apt-get install nss-updatedb
Lecture des listes de paquets... Fait
```

Utiliser manuellement l'outil `nss-updatedb` :

```
root@pclinux:/etc# nss_updatedb ldap
passwd... done.
group... done.
```

Il faut informer le système qu'il peut utiliser ces bases de données comme source pour `passwd`, `group` et `shadow` en ajoutant `db` aux entrées respectives du fichier `/etc/nsswitch.conf` :

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

Désactiver le cache de nscd

Il est possible de désactiver le cache dans le fichier de configuration /etc/nscd.conf en ajoutant les options désirées :

```
enable-cache passwd no
enable-cache group no
enable-cache shadow no
```

Pour en savoir plus, consulter le manuel à l'aide de la commande man :

```
# man nscd.conf
```

Perte de l'authentification

Il n'est plus possible de se connecter depuis le poste client ni avec le gestionnaire de connexion (display manager) ni en ligne de commande dans un tty.

Il faut s'assurer du bon fonctionnement du module Scribe avec la commande diagnose.

Il faut ensuite tester si le service LDAP distant répond :

```
root@pclinux:/home/eole# ldapsearch -h scribe:389 -b o=gouv,c=fr -x uid=utilisateurScribe
```

la commande getent :

```
# getent passwd test.prof
```

Si elle ne renvoie plus rien il faut relancer le service nscd avec la commande suivante :

```
# service nscd restart
```

Activer et consulter les logs de nscd

L'activation des logs pour nscd se fait dans le fichier /etc/nscd.conf.

Il faut dé-commenter la ligne `logfile /var/log/nscd.log` et passer la variable `debug-level` à `1` ou plus de verbosité.

Pour plus d'information il faut consulter la page de manuel :

```
# man nscd.conf
```

Pour rendre effectif le changement il faut relancer le service :

```
root@pclinux:/home/eole# service nscd restart
```

La consultation des journaux se fait à l'aide de la commande tail :

```
root@pclinux:/home/eole# tail -f /var/log/nscd.log
```

Pour lancer le service libnss-ldapd en mode débogage

Arrêter `nscd`

```
# service nscd stop
```

Arrêter le démon de `libnss-ldapd`

```
# service nslcd stop
```

Lancer le démon de `libnss-ldapd` en mode débogage

```
# nslcd -d
```

5. Partages avec NFS

La méthode basée sur le partage de fichiers NFS[p.142] est valable aussi bien pour des clients GNU/Linux existants que pour la mise en œuvre des clients légers Eclair (serveur de clients légers).

Pour fonctionner, le client GNU/Linux a besoin que le service NFS soit installé et activé sur le module Scribe.

Le logiciel Gaspacho permet d'appliquer des configurations sur les postes clients.

Configuration du partage de fichiers sur le module Scribe

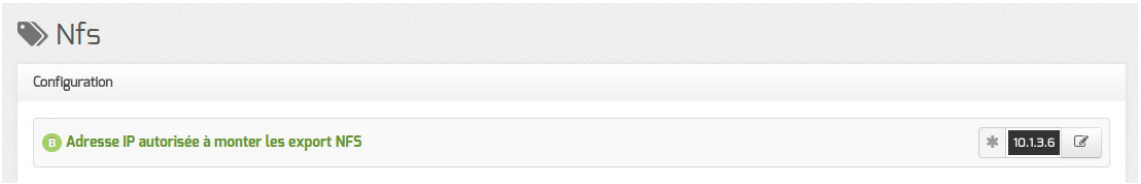
Sur le module Scribe il faut installer le paquet `eole-nfs` :

```
# apt-eole install eole-nfs
```

L'installation du paquet ajoute :

- un nouveau service dans l'onglet `Services` de l'interface de configuration du module `Activer le serveur NFS` est par défaut à `oui`
- et un nouvel onglet nommé `Nfs` est disponible

Il faut ensuite autoriser le module Eclair ou les clients Linux à monter les export NFS du module Scribe. Pour cela, se rendre dans l'interface de configuration du module Scribe, dans l'onglet `Nfs` et saisir l'adresse IP (Interface-0) du module Eclair ou les adresses des clients GNU/Linux dans le champ `Adresse IP autorisée à monter les exports NFS`.



Il faut ensuite procéder à la reconfiguration du module Scribe avec la commande `reconfigure`.

Test manuel de montage

Pour le support du système de fichiers NFS sur le client il faut installer le paquet `nfs-common` :

```
# apt-get install nfs-common
```

Pour tester la prise en charge il est possible de procéder à un montage manuelle d'une partition distante :

```
# mdkir /mnt/montage
# mount -t nfs -o auto,nouser,rsize=8192,wsize=8192,timeo=14,intr,acl,nolock,async scribe:/home/ /mnt/montage
```

Pour démonter la partition :

```
# umount /mnt/montage
```

Si le test de montage renvoie la ligne suivante c'est qu'il faut autoriser l'adresse IP du client dans l'onglet Nfs du module Scribe :

```
mount.nfs: access denied by server while mounting scribe:/home/
```

Configuration pour le montage à la connexion

Pour permettre à PAM de monter des volumes pour une session utilisateur il faut installer la bibliothèque libpam-mount :

```
root@pclinux:/home/eole# apt-get install libpam-mount
```

#fixme

Voir aussi...

eole-nfs

6. Partages avec Samba

Cette solution basée sur SMB[p.143] est valable pour des clients GNU/Linux.

Un fichier de configuration doit être ajouté sur le module Scribe pour la prise en charge des partages.

Pour fonctionner, le client GNU/Linux doit pouvoir monter des partitions distante par SMB avec l'utilitaire `cifs-utils.`

Le logiciel Gaspacho permet d'appliquer des configurations sur les postes clients.

Paramétrer le module Scribe

Pour que les partages fonctionnent sur un module Scribe 2.4 il faut ajouter le fichier de configuration `/etc/samba/conf.d/partages-linux.conf` avec le contenu suivant :

```
[eclairng]
path = %H/.ftp
comment = montage linux
read only = no
browseable = no
invalid users = nobody guest
inherit permissions = yes
inherit acls = yes
create mask = 0664
directory mask = 0775
valid users = %U
write list = %U
```

```
guest ok = no
hide files = /config_eole/
```

Ce fichier permet de partager le répertoire `.ftp` de l'utilisateur qui lui contient les liens symboliques vers les répertoires de l'utilisateur.

Pour que le changement soit pris en compte sur le module il faut reconfigurer le serveur à l'aide de la commande `reconfigure` :

```
# reconfigure
```

Test manuel de montage

Le protocole SMB/CIFS permet un partage de fichiers multiplate-forme avec des systèmes Linux.

Le paquet `cifs-utils` fournit des utilitaires pour gérer les montages des systèmes de fichiers en réseaux CIFS.

```
# apt-get install cifs-utils
```

Pour tester la prise en charge il est possible de procéder à un montage manuelle d'une partition distante :

```
# mdkir /mnt/montage
```

Récupérer l'UID de l'utilisateur

```
root@pclinuxlxde:/home/eole# getent passwd test.prof
test.prof:x:10034:10001:test prof:/home/t/test.prof:/bin/bash
root@pclinuxlxde:/home/eole#
```

Montage manuel

```
root@pclinux:/home/eole# mount -t cifs //scribe/perso /mnt/montage -o noexec,nosetuids,mapchars,cifsacl,serverino,nobrl,iocharset=utf8,user=test.p
Password for test.prof@//scribe/perso: ******
root@pclinux:/home/eole#
```

Pour démonter la partition :

```
# umount /mnt/montage
```

Si le test de montage renvoie la ligne suivante c'est qu'il faut autoriser l'adresse IP du client dans l'onglet Nfs du module Scribe :

```
mount.nfs: access denied by server while mounting scribe:/home/
```

Configuration pour le montage à la connexion

Pour permettre à PAM de monter des volumes pour une session utilisateur il faut installer la bibliothèque `libpam-mount` :

```
root@pclinux:/home/eole# apt-get install libpam-mount
```

Il faut ensuite éditer le fichier de configuration /etc/security/pam_mount.conf.xml et ajouter les volumes à monter dans la rubrique `<!-- Volume definitions -->` du fichier.

Les points de montage sont créés automatiquement.

```
<volume user="*" fstype="cifs" server="scribe" path="professeurs" mountpoint="/media/professeurs" />
<volume user="*" fstype="cifs" server="scribe" path="perso" mountpoint="~/Documents" />
<volume user="*" fstype="cifs" server="arg1" path="eclairng" mountpoint="/media/serveur-scribe" />
```

```
<volume user="*" fstype="cifs" server="scribe" path="commun" mountpoint="/media/commun" />
<volume user="*" fstype="cifs" server="scribe" path="groupes" mountpoint="/media/groupes" />
```

Il faut également ajouter les paramètres des volumes à monter dans la rubrique `<!-- pam_mount parameters: Volume-related -->` du fichier.

```
<cifsmount>mount -t cifs //%(SERVER)/%(VOLUME) %(MNTPT) -o "noexec,nosetuids,mapchars,cifsacl,serverino,nobrl,iocharset=utf8,us
OPTIONS)"</cifsmount>
```

#fixme

Empêcher ou personnaliser la création des dossiers Musique, Vidéo, Téléchargement,...

`xdg-user-dirs` est un outil de gestion qui définit un lot de répertoires standards prêts à l'emploi (Documents, Images, Musique, Téléchargements, Vidéos notamment) dans le répertoire /home de l'utilisateur.

Il est possible d'empêcher la création par le système des répertoires par défaut de l'utilisateur (Musique, Vidéo, Téléchargement,...).
Pour cela il faut éditer le fichier /etc/xdg/user-dirs.conf et de passer `enabled=True` à `False`.

Il est possible de personnaliser les répertoires par défaut de l'utilisateur (Musique, Vidéo, Téléchargement,...).
Pour cela il faut éditer le fichier /etc/xdg/user-dirs.defaults et commenter les répertoires non souhaités

et inversement.

Voir aussi...

eole-fichier-primaire

7. Intégration dans un environnement graphique

Le gestionnaire de connexion, DM pour display manager en anglais, peut-être différent d'une distribution GNU / Linux à une autre :

- LightDM pour Unity, qui se lit light display manager ;
- GDM pour GNOME, qui se lit gnome display manager ;
- KDM pour KDE qui se lit KDE display manager ;
- XDM pour X Window qui se lit X display manager ;
- Entrance pour Enlightenment ;
- LDM, gestionnaire d'affichage spécialement écrit pour LTSP.

LightDM

Si plusieurs gestionnaire de connexion sont installés il est possible de choisir lightdm comme celui par défaut avec la commande `dpkg-reconfigure` :

```
# dpkg-reconfigure lightdm
```

Selon la version de la distribution le fichier de configuration qui permet de personnaliser le comportement de LightDM peut être différent :

- `/etc/lightdm/lightdm.conf` sur Ubuntu inférieure à 14.04 ;
- `/usr/share/lightdm/lightdm.conf.d/50-xubuntu.conf` sur Ubuntu supérieure égal 14.04 ;
- `/usr/share/lightdm/lightdm.conf.d/60-xubuntu.conf` sur Ubuntu supérieure à 14.04.

La modification du fichier de configuration nécessite le redémarrage du service :

```
# service lightdm restart
```

Activer la touche NumLock (VerrNum)

Un paquet supplémentaire peut être installé pour gérer la touche NumLock (VerrNum) :

```
# apt-get install numlockx
```

Pour sa prise en charge dans LightDM ajouter la ligne suivante dans la rubrique `[SeatDefaults]` :

```
greeter-setup-script=/usr/bin/numlockx on
```

Exécution d'un script à la déconnexion

Créer un script `/etc/lightdm/logoffscript.sh` avec les actions à réaliser à la déconnexion de l'utilisateur.

Pour sa prise en charge dans LightDM ajouter la ligne suivante dans la rubrique `[SeatDefaults]` :

```
session-cleanup-script=/etc/lightdm/logoffscript.sh
```

démontage et suppression du répertoire personnel

```
umount -f $HOME
# suppression du répertoire personnel local à chaque déconnexion,
# sauf pour le compte administrateur local
# if [ $USER != adminprof ]&&[ $USER != adminskel ]; then
# if [ $USER != adminprof ]&&[ $USER != adminskel ]&&[ $USER != prof ]&&[ $USER != invite ]; then
if [ $USER != adminprof ]; then
# on vérifie qu'il n'y a plus de répertoire monté dans /home/$USER/ mount | grep "/home/"| grep $USER ; if [ $? = 0 ]; then exit 1,; fi
rm -r $HOME
fi
exit 0
```

Autres possibilités

Il est également possible de :

- masquer tous les utilisateurs
  `greeter-hide-users=true`
- permettre la saisie manuelle
  `greeter-show-manual-login=true`

Documentation LightDM

- http://wiki.ubuntu.com/LightDM
- http://doc.ubuntu-fr.org/lightdm

KDM

Si plusieurs gestionnaire de connexion sont installés il est possible de choisir KDM comme celui par défaut avec la commande `dpkg-reconfigure` :

```
# dpkg-reconfigure kdm
```

GDM

Si plusieurs gestionnaire de connexion sont installés il est possible de choisir GDM comme celui par défaut avec la commande `dpkg-reconfigure` :

```
# dpkg-reconfigure gdm
```

8. Installation de Gaspacho

Gaspacho est une application qui permet de configurer automatiquement le poste de travail de l'utilisateur selon son profil.

Installation

Pour installer le service Gaspacho sur le module Scribe il faut installer le paquet `eole-gaspacho` :

```
# apt-eole install eole-gaspacho
```

L'installation du paquet ajoute un nouveau service dans l'onglet `Services` de l'interface de configuration du module. `Activer Gaspacho` est par défaut à `oui` et un nouvel onglet nommé `Gaspacho` est disponible en mode expert.

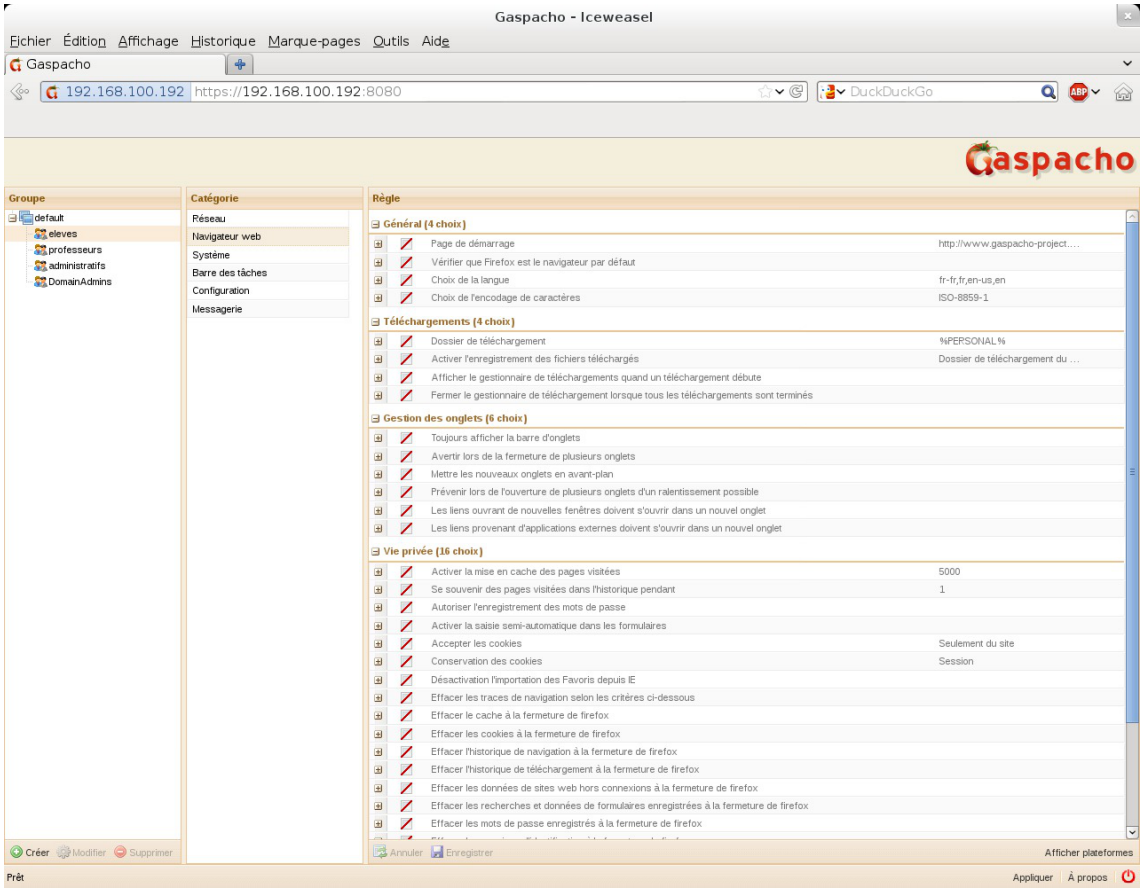
Celui-ci vous permet de choisir qui détermine les entrées DNS via la variable `Utiliser des entrées DNS des clients plutôt que le nom fourni par l'agent` qui par défaut est à `non`. Par défaut, les entrées DNS sont donc imposées par l'agent Gaspacho.

Les changement des paramètres de configuration nécessite la reconfiguration du module à l'aide de la commande `reconfigure`.

Accès à l'application

Gaspacho est accessible sur le module à l'adresse `https://<adresse serveur>:8080`.

Le compte à utiliser est le compte `admin` du module Scribe.



Vue d'ensemble de l'application Gaspacho

Plus d'informations sur Gaspacho sont disponibles dans la documentation dédiée et sur le site du projet : http://www.gaspacho-project.net/.

Gaspacho côté client

#fixme

9. Scripts d'intégration pour GNU / Linux

Des scripts utilisant Samba permettent d'intégrer des clients GNU/Linux au domaine Scribe, ils sont à installer sur chacun des clients.

Une adaptation sur le module Scribe en version supérieure ou égale à 2.4 est nécessaire pour le bon fonctionnement des partages.

Le logiciel Gaspacho permet d'appliquer des configurations sur les postes clients.

Les scripts d'intégration

Les scripts et leurs adaptations sont le résultat du travail de plusieurs personnes :

- Christophe Dezé (Rectorat de Nantes)
- Cédric Frayssinet (Mission Tice Académie de Lyon)
- Xavier Garel (Mission Tice Académie Lyon)

- Simon Bernard (Dane Reseau Lyon)
- Kalai Mehdi (Académie de Poitiers)

Deux méthodes sont possibles pour récupérer les scripts :

- scripts versionnés ;
- archive par version de GNU/Linux.

Dans les deux cas les scripts seront à personnaliser et à modifier en fonction du contexte et de la version GNU/Linux des clients.

Scripts versionnés avec Git

Les scripts versionnés sont mis à disposition par la Délégation Académique au Numérique Éducatif de Lyon à l'adresse suivante :

https://github.com/dane-lyon/clients-linux-scribe

Ces scripts permettent d'intégrer des clients Gnu/Linux dans un environnement EOLE Scribe.

Les clients supportés sont les suivants :

- Ubuntu (Environnement Unity) 12.04 et 14.04
- Xubuntu (Environnement XFCE) 14.04
- Lubuntu (Environnement LXDE) 14.04
- Linux (Environnement Mate ou Cinammon) Mint 17 ou 17.1 ou 17.2

Pour récupérer l'ensemble du projet versionnés, il faut avoir Git d'installer sur son poste :

```
$ git clone https://github.com/dane-lyon/clients-linux-scribe.git
$ cd clients-linux-scribe/
```

La procédure d'utilisation est disponible dans le fichier `README.md` du projet ou à l'adresse suivante :

https://github.com/dane-lyon/clients-linux-scribe

Scripts archivés

Les différentes archives de scripts d'intégration proposées par les contributeurs concernent des versions de GNU/Linux et des environnements de bureau différents.

Ils sont mis à disposition à l'adresse suivante : http://eole.ac-dijon.fr/pub/Contribs/Clients_Linux/

Exemple d'intégration avec les scripts archivés

La procédure d'écrite ci-dessous a été testée avec un poste client Xubuntu

Elle utilise l'archive qui concerne l'intégration d'une station Debian 8 proposée par par notre collègue Jean-François Mai, du collège République de Cholet et basé sur le travail de :

- Christophe Dezé (Rectorat de Nantes)
- Cédric Frayssinet (Mission Tice Académie de Lyon)

- Xavier Garel (Mission Tice Académie Lyon)
- Simon Bernard (Dane Reseau Lyon)
- Kalai Mehdi (Académie de Poitiers)

La procédure pour Debian 8 est entièrement décrite et mise à disposition :
http://eole.ac-dijon.fr/pub/Contribs/Clients_Linux/debian_debian_scribe-1.pdf

Installer les scripts sur le poste GNU/Linux

#fixme

Paramétrer le module Scribe

Pour que les partages fonctionnent sur un module Scribe 2.4 il faut ajouter le fichier de configuration `/etc/samba/conf.d/partages-linux.conf` avec le contenu suivant :

```
[eclairng]
path = %H/.ftp
comment = montage linux
read only = no
browseable = no
invalid users = nobody guest
inherit permissions = yes
inherit acls = yes
create mask = 0664
directory mask = 0775
valid users = %U
write list = %U
guest ok = no
hide files = /config eole/
```


Ce fichier permet de partager le répertoire `.ftp` de l'utilisateur qui lui contient les liens symboliques vers les répertoires de l'utilisateur.

Pour que le changement soit pris en compte sur le module il faut reconfigurer le serveur à l'aide de la commande `reconfigure` :

```
# reconfigure
```

Résolution de problème

La commande `getent passwd` permet de savoir si les utilisateurs LDAP ont été ajouté aux utilisateurs

locaux :

```
root@ejabber:~# getent passwd prenom.prof26
prenom.prof26:x:10437:10000:Prenom PROF26:/home/p/prenom.prof26:/bin/false
root@ejabber:~#
```

9.1. Paramétrage des clients GNU/Linux

9.1.1. Clients Debian

Client Jessie (Debian 8)

Pour l'intégration d'une station Debian 8 à un serveur Scribe, vous pouvez vous reporter à la procédure décrite par notre collègue Jean-François Mai, du collège République de Cholet et basé sur le travail de :

- Christophe Dezé (Rectorat de Nantes)
- Cédric Frayssinet (Mission Tice Académie de Lyon)
- Xavier Garel (Mission Tice Académie Lyon)
- Simon Bernard (Dane Reseau Lyon)
- Kalai Mehdi (Académie de Poitiers)

http://eole.ac-dijon.fr/pub/Contribs/Clients_Linux/debian_debian_scribe-1.pdf

Scripts d'intégration

Des scripts d'intégration sont mis à disposition à l'adresse suivante par Jean-François Mai, du collège République de Cholet : http://eole.ac-dijon.fr/pub/Contribs/Clients_Linux/

Le script suivant s'occupe uniquement de l'intégration : http://eole.ac-dijon.fr/pub/Contribs/Clients_Linux/debian_gnu_linux_jessie_in_scribe2.4-v1.0c.tar.gz

Le script suivant installe un système avec un environnement minimal MATE et enfin s'occupe de l'intégration : http://eole.ac-dijon.fr/pub/Contribs/Clients_Linux/debian_gnu_linux_jessie_in_scribe2.4-mate-core-v1.0b.

Pour utiliser un des scripts proposés en téléchargement, vous devez le rendre exécutable.

Si vous n'êtes pas à l'aise avec la ligne de commande clic droit → Propriétés → permettre l'exécution du programme.

Sinon lancez un terminal et tapez la commande suivante :

```
$ chmod +x nom du script.sh
```

Beaucoup d'informations sont présentes dans le fichier `readme.txt` de l'archive.

Problème des partages sur un serveur EOLE Scribe 2.4

Pour avoir les partages avec un client GNU/Linux et un serveur Scribe 2.4, il suffit d'ajouter le fichier

`partages-linux.conf` de configuration dans `/etc/samba/conf.d/`.

Le fichier doit contenir :

```
[eclairng]
path = %H/.ftp
comment = disque personnel pour 98 et 95
read only = no
browseable = no
invalid users = nobody guest
inherit permissions = yes
inherit acls = yes
create mask = 0664
directory mask = 0775
valid users = %U
write list = %U
guest ok = no
hide files = /config eole/
```

Pour rendre le changement opérant il faut procéder à la reconfiguration du module :

```
# reconfigure
```

Client Wheezy (Debian 7)

Pour l'intégration d'une station Debian 7 à un serveur Scribe, vous pouvez vous reporter à la procédure décrite par notre collègue Jean-François Mai, du collège République de Cholet et basé sur le travail de :

- Christophe Dezé (Rectorat de Nantes)
- Cédric Frayssinet (Mission Tice Académie de Lyon)
- Xavier Garel (Mission Tice Académie Lyon)
- Simon Bernard (Dane Reseau Lyon)
- Kalai Mehdi (Académie de Poitiers)

http://eole.ac-dijon.fr/pub/Contribs/Clients_Linux/debian_gnu_linux_wheezy_in_EOLE_scribe-v1.0.pdf (37Mo)

Scripts d'intégration

Des scripts d'intégration sont mis à disposition à l'adresse suivante par Jean-François Mai, du collège République de Cholet : http://eole.ac-dijon.fr/pub/Contribs/Clients_Linux/

Le script suivant installe un système avec un environnement minimal MATE et enfin s'occupe de l'intégration :

http://eole.ac-dijon.fr/pub/Contribs/Clients_Linux/debian_gnu_linux_wheezy_in_scribe-v1.0h.tar.gz [http://eole.ac-dijon.fr/pub/Contribs/Clients_Linux/debian_gnu_linux_jessie_in_scribe2.4-mate-core-v1.0b.tar.gz]

Pour utiliser un des scripts proposés en téléchargement, vous devez le rendre exécutable.

Si vous n'êtes pas à l'aise avec la ligne de commande clic droit → Propriétés → permettre l'exécution du

programme.

Sinon lancez un terminal et tapez la commande suivante :

```
$ chmod +x nom du script.sh
```

Beaucoup d'informations sont présentes dans le fichier `readme.txt` de l'archive.

Problème des partages sur un serveur EOLE Scribe 2.4

Pour avoir les partages avec un client GNU/Linux et un serveur Scribe 2.4, il suffit d'ajouter le fichier `partages-linux.conf` de configuration dans `/etc/samba/conf.d/`.

Le fichier doit contenir :

```
[eclairng]
path = %H/.ftp
comment = disque personnel pour 98 et 95
read only = no
browseable = no
invalid users = nobody guest
inherit permissions = yes
inherit acls = yes
create mask = 0664
directory mask = 0775
valid users = %U
write list = %U
guest ok = no
hide files = /config eole/
```

Pour rendre le changement opérant il faut procéder à la reconfiguration du module :

```
# reconfigure
```

9.1.2. Clients Ubuntu

Client Hardy Heron (8.10)

Pour l'intégration d'une station Ubuntu 8.10 à un serveur Scribe, vous pouvez vous reporter à la procédure décrite par notre collègue Mehdi Kalai, de l'académie de Poitiers :

http://www.m-k.cc/spip.php?article1

Scripts d'intégration

Des scripts d'intégration ont été développés par Christophe Dezé de l'académie de Nantes.

Ils sont mis à disposition à l'adresse suivante : http://eole.ac-dijon.fr/pub/Contribs/Clients_Linux/

Ces scripts sont disponibles pour plusieurs versions de GNU/Linux Ubuntu :

- Ubuntu 8.04 **LTS** (Hardy Heron)

- Ubuntu 8.10 (Intrepid Ibex)
- Ubuntu 9.04 (Jaunty Jackalope)
- Ubuntu 9.10 (Karmic Koala)
- Ubuntu 10.04 **LTS** (Lucid Lynx)
- Ubuntu 10.10 (Maverick Meerkat)
- Ubuntu 11.04 (Natty Narwhal)
- Ubuntu 12.04 (The Precise Pangolin)

Pour utiliser un des scripts proposés en téléchargement, vous devez le rendre exécutable.

Si vous n'êtes pas à l'aise avec la ligne de commande clic droit → Propriétés → permettre l'exécution du programme.

Sinon lancez un terminal et tapez la commande suivante :

```
$ chmod +x nom_du_script.sh
```

9.1.3. Clients Mandriva

Client Mandriva 2010

Pour l'intégration d'une station Mandriva 2010 à un serveur Scribe, vous pouvez vous reporter à la procédure décrite par notre collègue Mehdi Kalaï, de l'académie de Poitiers :

http://www.m-k.cc/spip.php?article2

9.1.4. Clients Mageia

Scripts d'intégration

Un script d'intégration a été développés par Mehdi Kalaï de l'académie de Poitiers.

Il est mis à disposition dans : http://eole.ac-dijon.fr/pub/Contribs/Clients_Linux/

Ce script n'est disponible que pour la version 2 de Mageia.

Pour utiliser un des scripts proposés en téléchargement, vous devez le rendre exécutable.

Si vous n'êtes pas à l'aise avec la ligne de commande clic droit → Propriétés → permettre l'exécution du programme.

Sinon lancez un terminal et tapez la commande suivante :

```
$ chmod +x nom_du_script.sh
```

10. Liens vers des contributions externes

Installation de postes clients GNU/Linux Ubuntu par Cédric Frayssinet.

L'objectif de ce guide est d'obtenir des postes de travail prêts à l'utilisation et qui peuvent être restaurés dans leur état initial en quelques minutes par une personne sans compétence informatique particulière à

partir d'une image OSCAR.

OSCAR permettra également de déployer rapidement un ensemble de postes identiques à partir d'un poste modèle.

Ce guide fait parti des ressources technico-pédagogiques accessibles publiquement sur le site de la Délégation Académique au Numérique Éducatif et du CRDP de l'académie de LYON.

http://nefertiti.crdp.ac-lyon.fr/wk/cdch/postes_clients_ubuntu_32_64_bits

http://www2.ac-lyon.fr/wiki-dane/mardi/integration_poste_x_ubuntu_sur_scribe

Scripts d'intégration des clients Gnu/Linux dans un environnement EOLE Scribe

Les scripts versionnés sont mis à disposition par la Délégation Académique au Numérique Éducatif de Lyon à l'adresse suivante :

https://github.com/dane-lyon/clients-linux-scribe

Archives de scripts d'intégration

Les différentes archives de scripts d'intégration proposées par les contributeurs concernent des versions de GNU/Linux et des environnements de bureau différents.

Ils sont mis à disposition à l'adresse suivante : http://eole.ac-dijon.fr/pub/Contribs/Clients_Linux/

Chapitre 2

Les clients Windows

1. Installation et configuration des clients Windows

1.1. Principe

Scribe agissant comme un contrôleur de domaine, les stations Windows doivent dans un premier temps être intégrées dans le domaine.

Afin d'interagir davantage avec Scribe, un programme client a été développé pour les stations Windows.

Il doit être installé sur chaque station intégrée au domaine.

Mises à jour et sécurité

Les mises à jour n'apportent pas seulement de nouvelles fonctionnalités, elles corrigent aussi des failles de sécurité.

Il est donc important que **les clients soient aussi à jour**.

Cela concerne aussi bien le **système d'exploitation** (Windows Update) que **les programmes installés** (Firefox, Java, QuickTime, etc .).

Des vulnérabilités peuvent, en effet, toucher n'importe quel programme.

Ne pas appliquer les mises à jour rendrait votre système vulnérable aux attaques.

Rappelons à ce sujet que, statistiquement, la majorité des attaques proviennent de l'intérieur et non de l'extérieur.

1.2. Configuration réseau

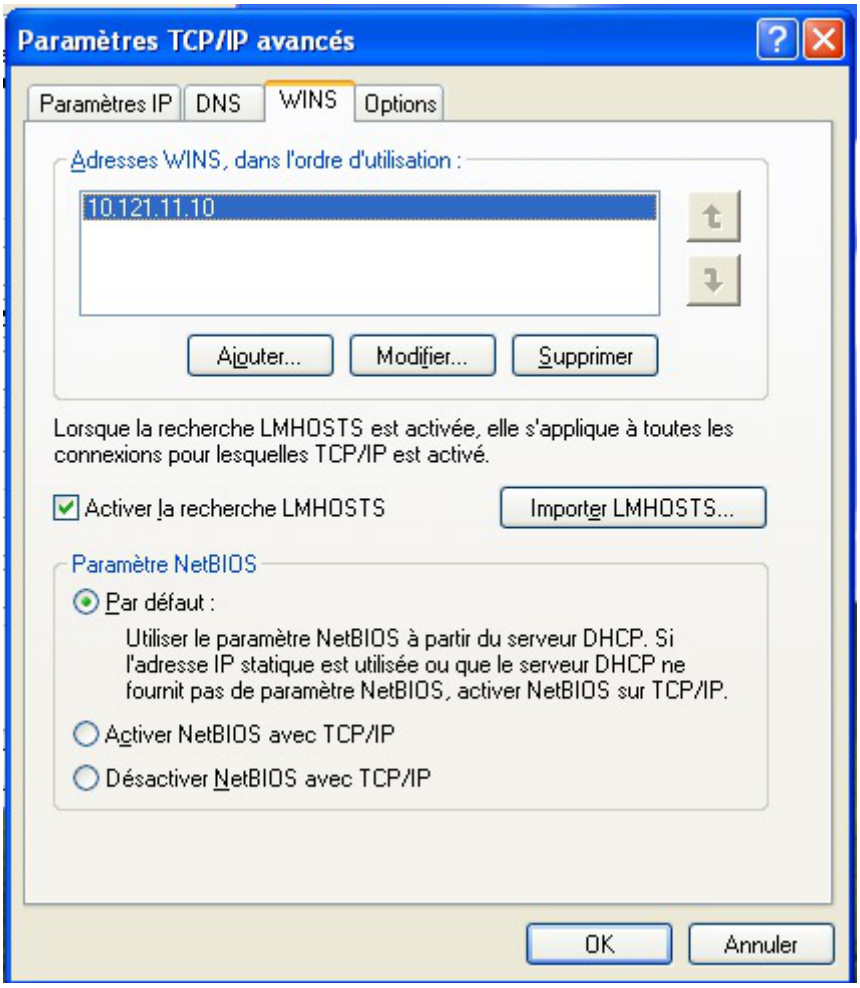
Avant l'intégration au domaine, il est indispensable de s'assurer que les paramètres réseau de la station soient corrects (adresse IP, passerelle, DNS, WINS).

Plusieurs cas sont possibles :

- la station obtient son adresse IP du serveur DHCP du serveur EOLE, dans ce cas il n'y a rien à faire ;
- la station obtient son adresse IP d'un serveur DHCP autre que le serveur EOLE, il faudra veiller à paramétrer l'adresse du serveur WINS[p.143] ;
- la station est adressée manuellement, il faudra veiller à paramétrer l'adresse du serveur WINS.

Configuration du serveur WINS sous Windows XP

Pour accéder à la configuration du serveur WINS il faut aller dans `Panneau de configuration`, `Connexions réseau`, faire un clic droit sur l'icône `réseau local` et sélectionner `propriétés`, puis double-cliquer sur `☑ Protocole Internet (TCP/IP)`, cliquer sur `Avancé...` et enfin sélectionner l'onglet `WINS`.



Configuration du serveur WINS dans Windows XP

1.3. Intégration et installation du client Scribe automatique

PrepaWin et IntegrDom sont à utiliser sur un module Scribe 2.5.1.

À partir de la version 2.5.2 du module il faut utiliser JoinEOLE.

1.3.1. JoinEOLE pour 2.5.2

Préparation de Windows 10

Depuis la version 1709 de Windows 10, l'intégration au domaine d'une station nécessite au préalable d'activer le support de partage de fichiers SMB 1.0/CIFS sur les postes clients.

Depuis la version 1903 de Windows 10, le fonctionnement des profils obligatoires n'est plus garanti.

Accéder au répertoire personnel de l'administrateur du domaine

Depuis la version 1709 de Windows 10, il est impossible d'accéder au lecteur réseau en mode invité.
Pour accéder au répertoire de l'administrateur avant la jonction au domaine il faut :

- soit appliquer une clé de registre pour supprimer cette interdiction ;
- soit monter un lecteur réseau en spécifiant les identifiants de connexion.

https://support.microsoft.com/de-ch/help/4046019/guest-access-smb2-disabled-by-default-in-windows-1(

Réactiver l'accès aux partages guest via une clé de registre

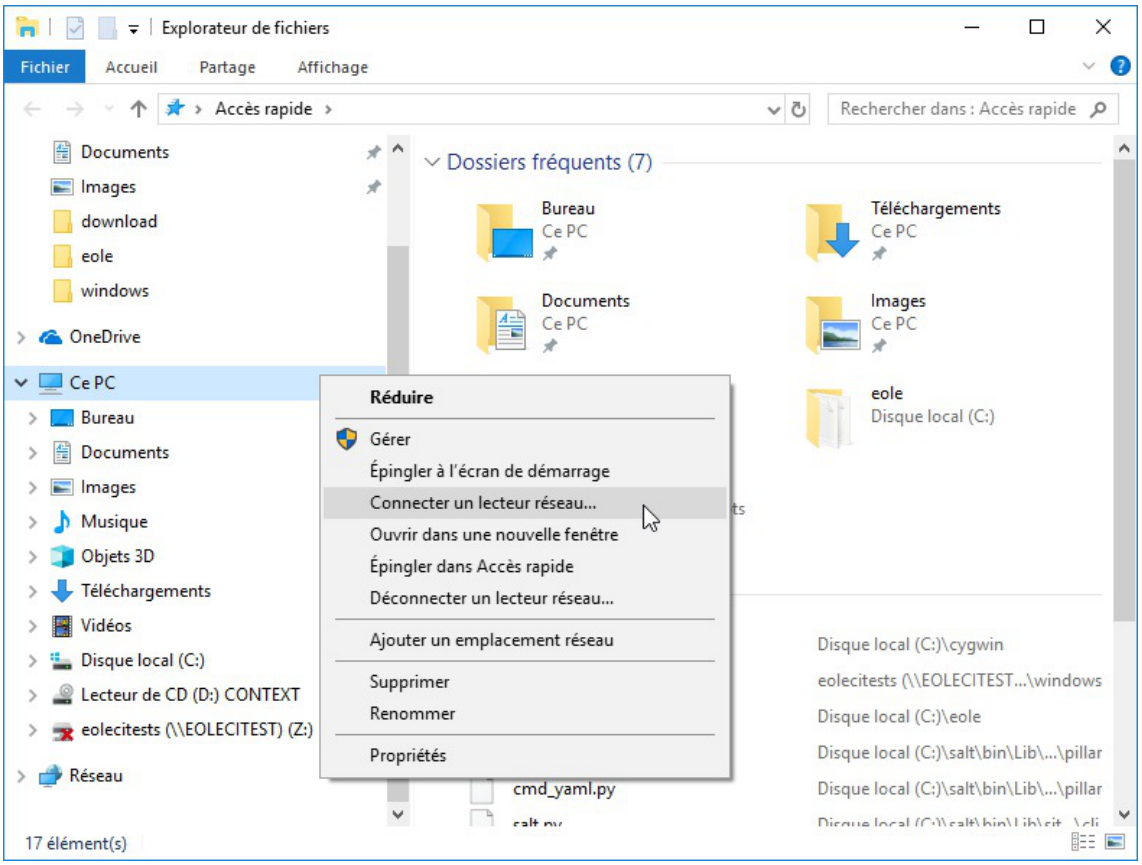
La clé de registre suivante permet de réactiver la possibilité de se connecter à un partage non sécurisé.

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters]
"AllowInsecureGuestAuth"=dword:00000001
```

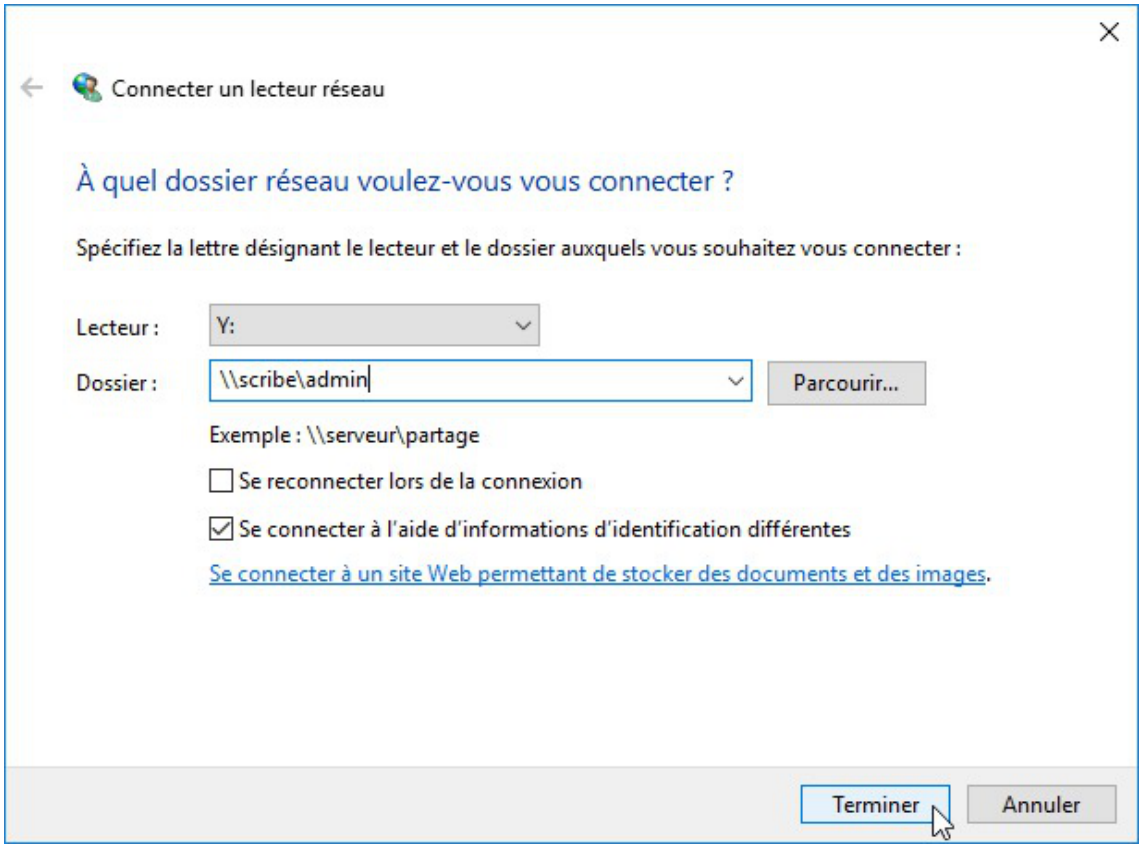
Monter un répertoire en spécifiant les identifiants de connexion

Pour accéder au répertoire personnel de l'administrateur :

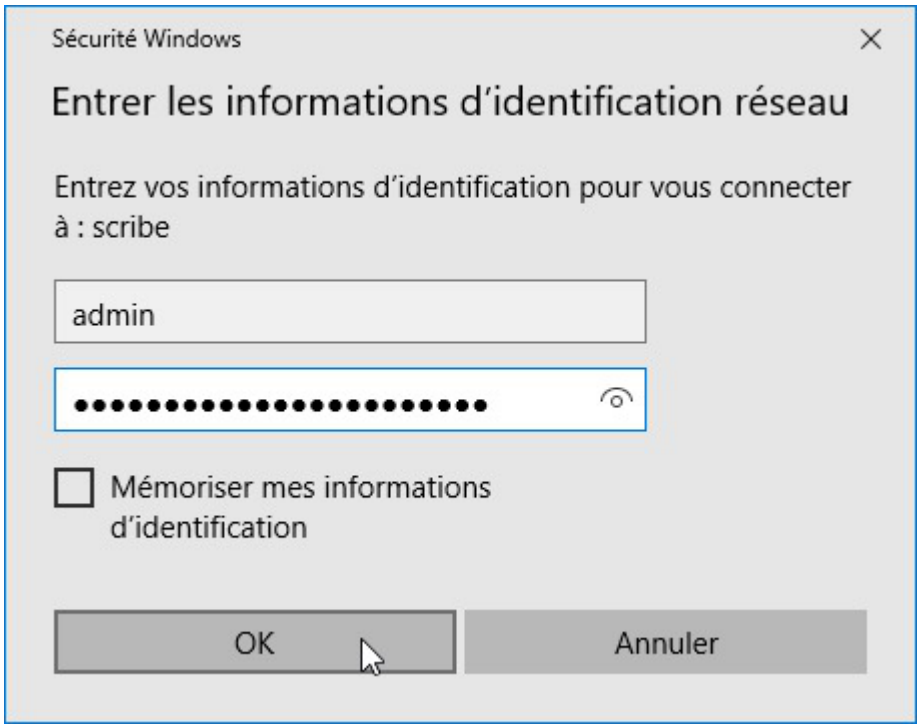
- Se connecter sur le poste en tant qu'administrateur ;
- Se rendre dans l'explorateur de fichier ;



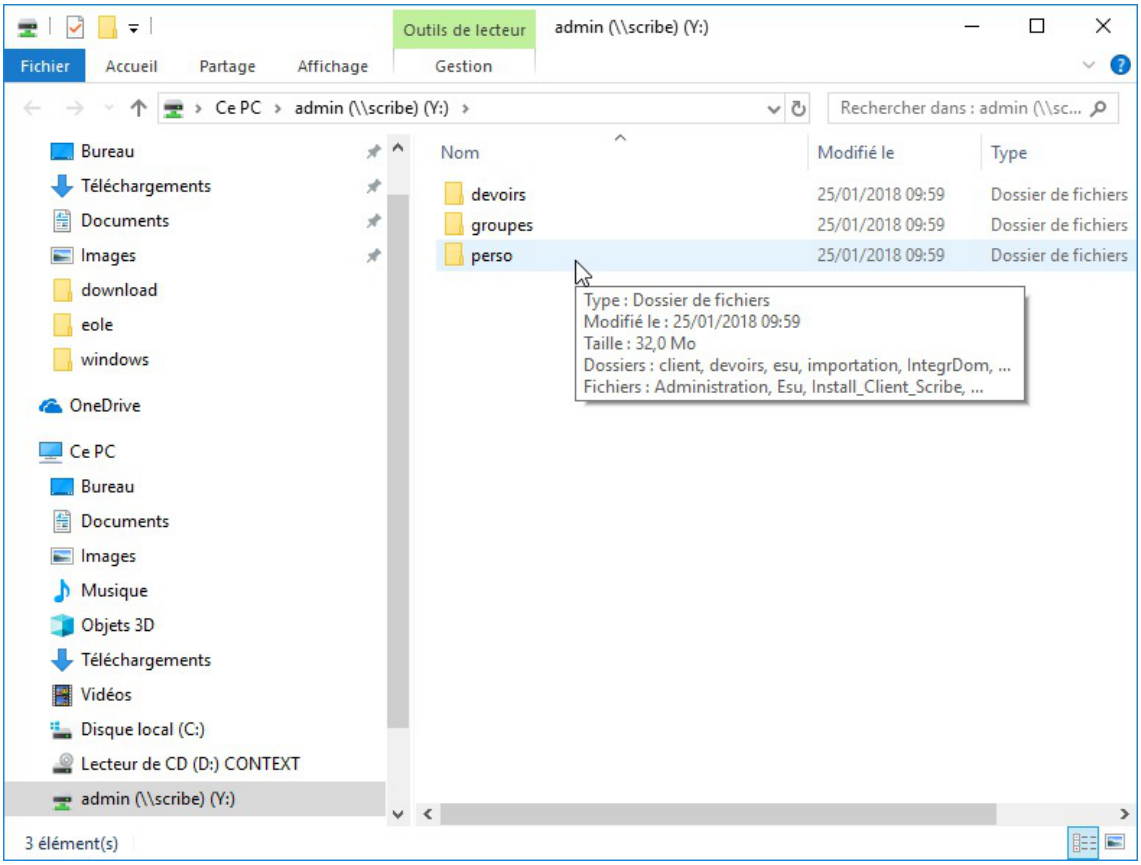
- Faire un clique droit sur `Ce PC` ;



- Saisir \\scribe\admin dans le champ `Dossier`, décocher ☑ Se reconnecter lors de la connexion, cocher ☑ Se connecter à l'aide d'informations d'identification différentes et cliquer sur le bouton Terminer ;



- Saisir le compte `admin` et la clé secrète associée ("mot de passe") et cliquer sur le bouton OK ;

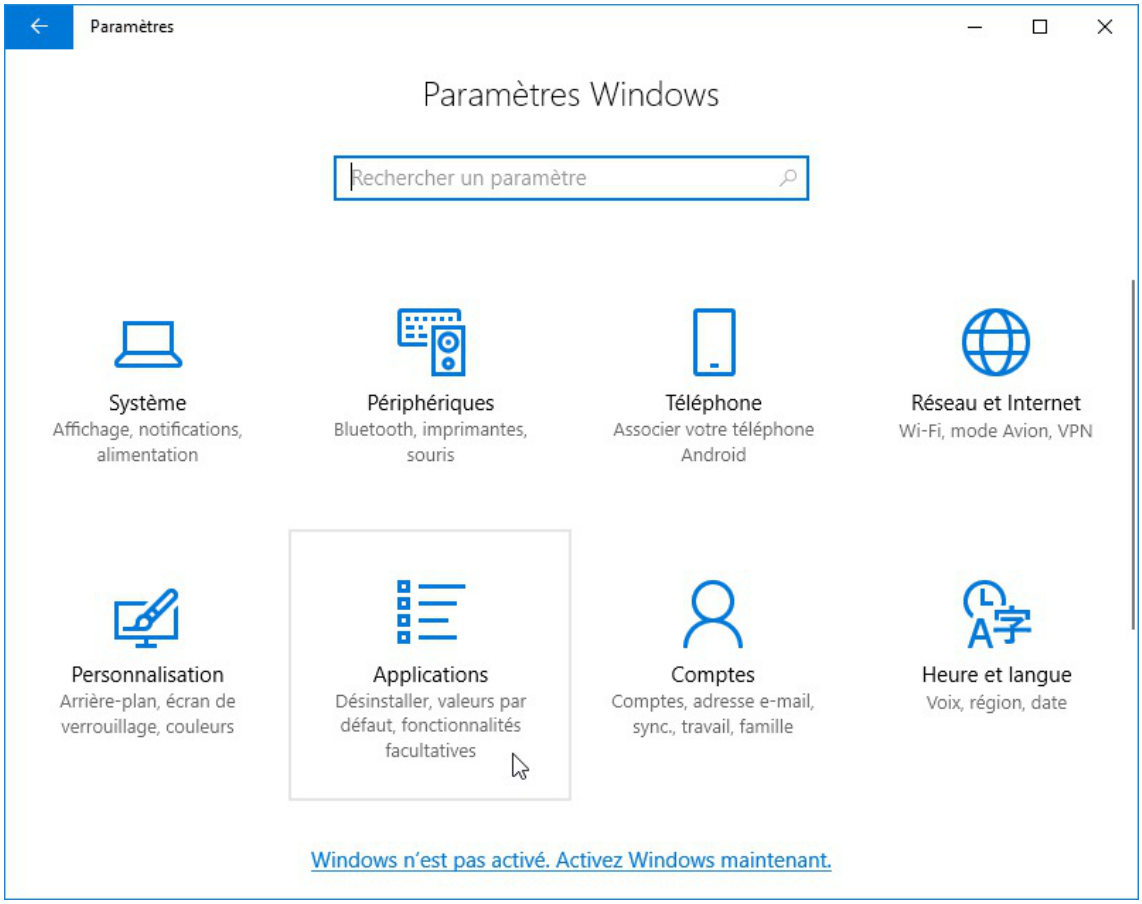


Activer le support de partage de fichiers SMB 1.0/CIFS

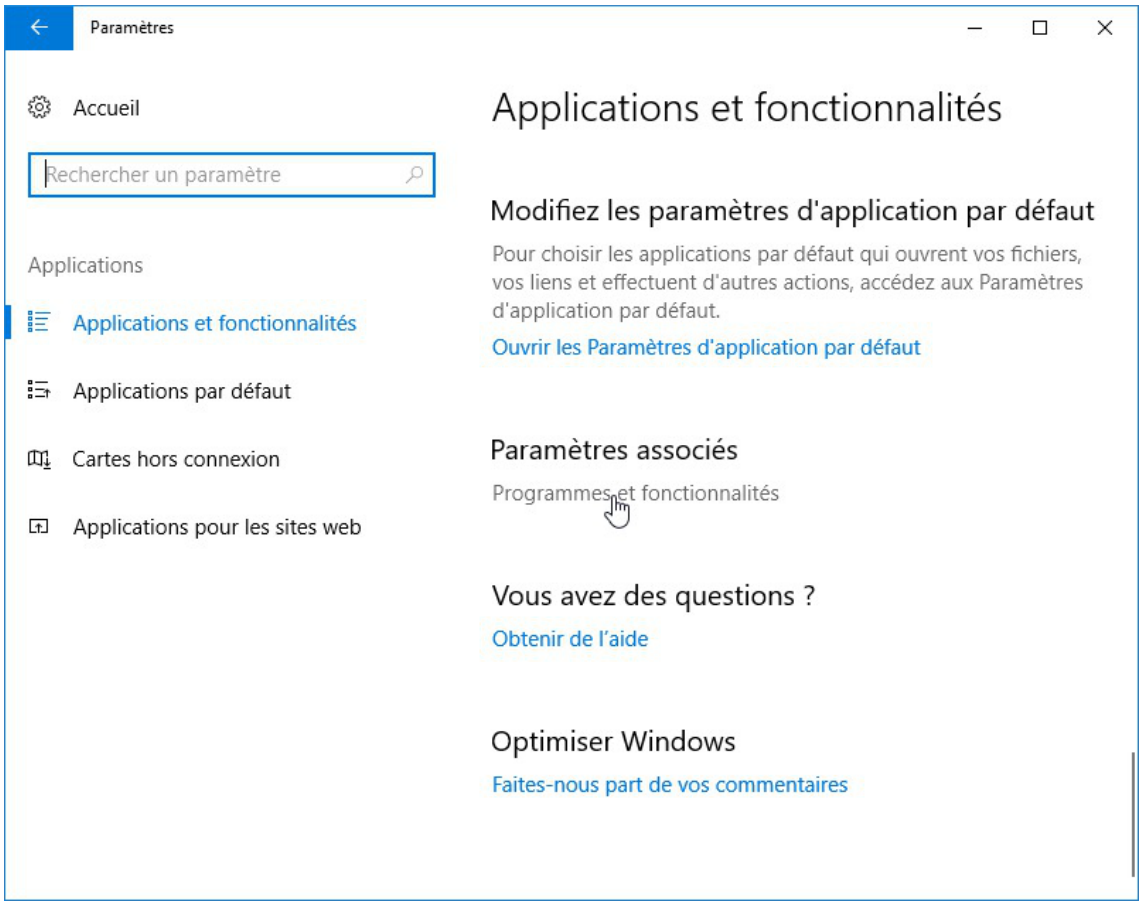
Sur un module EOLE à jour, l'activation du `support de partage de fichiers SMB 1.0/CIFS` est réalisée automatiquement par JoinEOLE et sa commande d'activation a été ajoutée au script `Win10.bat`.

Paramétrer Windows de la façon suivante :

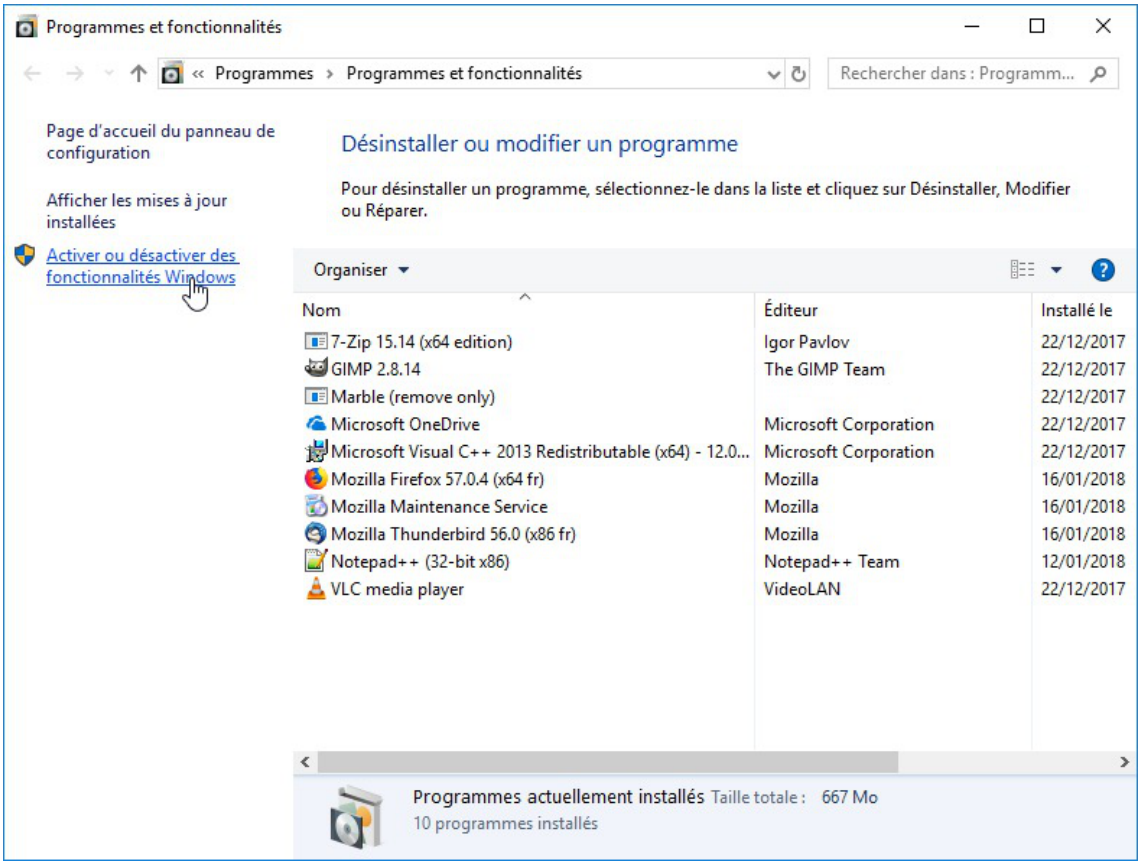
- Menu `Windows` et sélectionner `Paramètres` ;



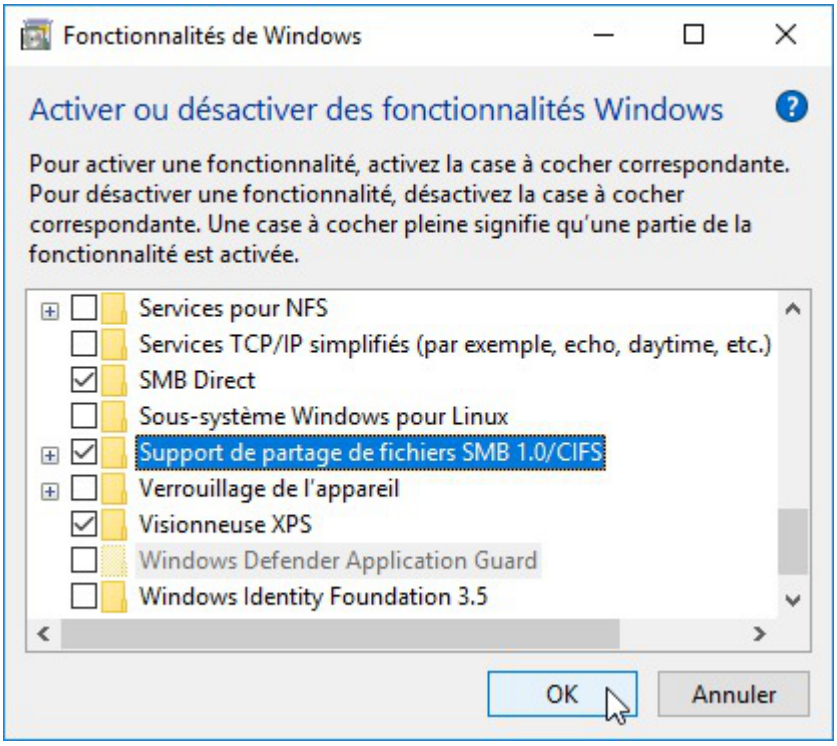
- Cliquer sur `Applications` ;



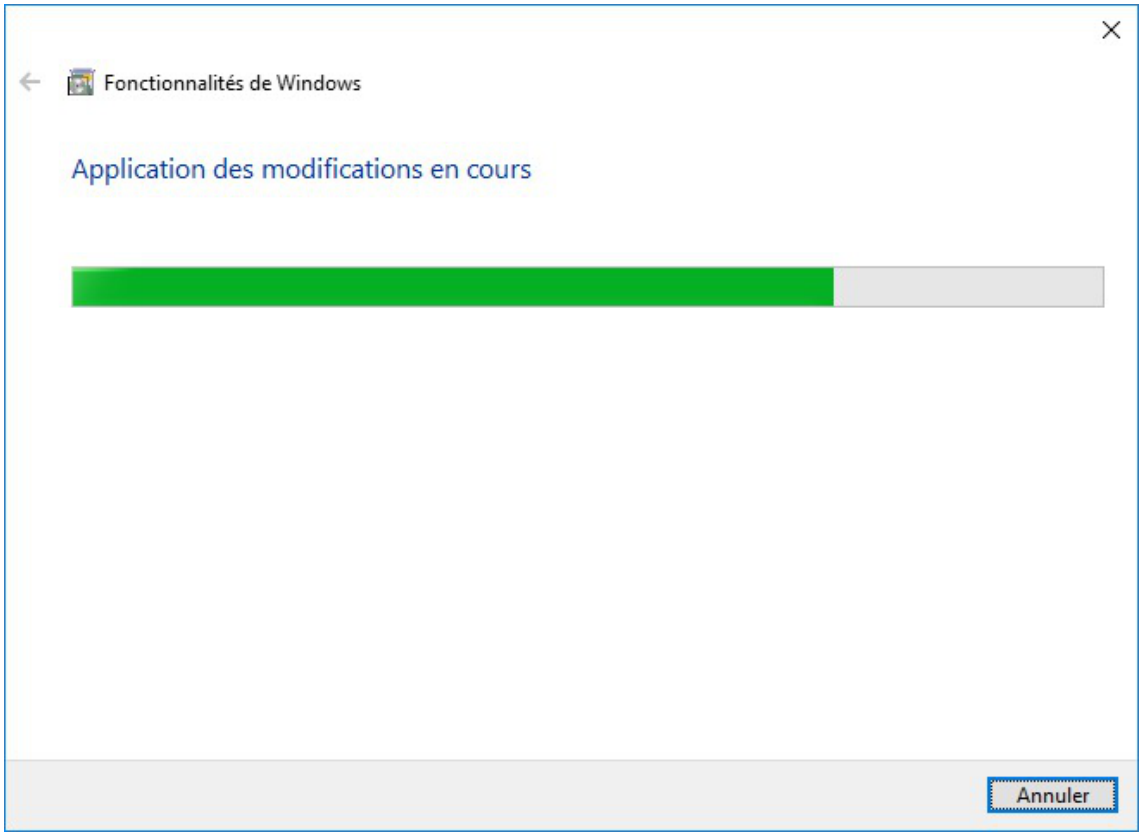
- Descendre et cliquer sur `Programmes et fonctionnalités` ;



- Cliquer sur `Activer ou désactiver des fonctionnalités Windows` ;



- Descendre dans la liste et cocher ☑ Support de partage de fichiers SMB 1.0/CIFS , cliquer sur `OK`, les modifications s'appliquent ;



Préparation de Windows 7

Les stations Windows 7 ne nécessitent aucune action préalable à l'utilisation de JoinEOLE.

Utilisation de JoinEOLE

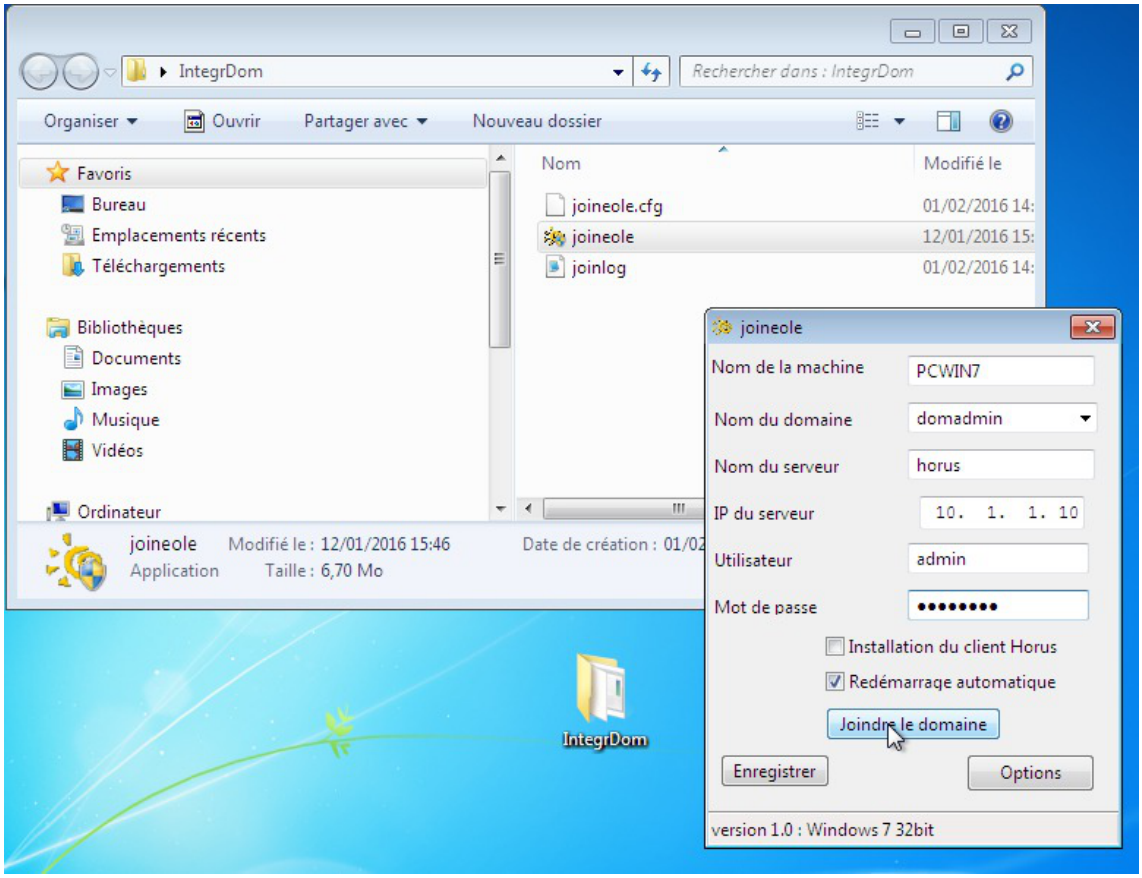
À partir de la version 2.5.2 du module, PrepaWin et IntegrDom ont été supprimés au profit du script JoinEOLE qui est disponible dans le dossier `IntegrDom` situé dans le répertoire perso de l'`admin`.

L'outil JoinEOLE prépare la station, la joint au domaine et installe de façon optionnelle le client pour Scribe ou Horus. De ce fait, il peut également être utilisé pour joindre les postes à un domaine Horus sur lequel le logiciel ESU n'est pas activé.

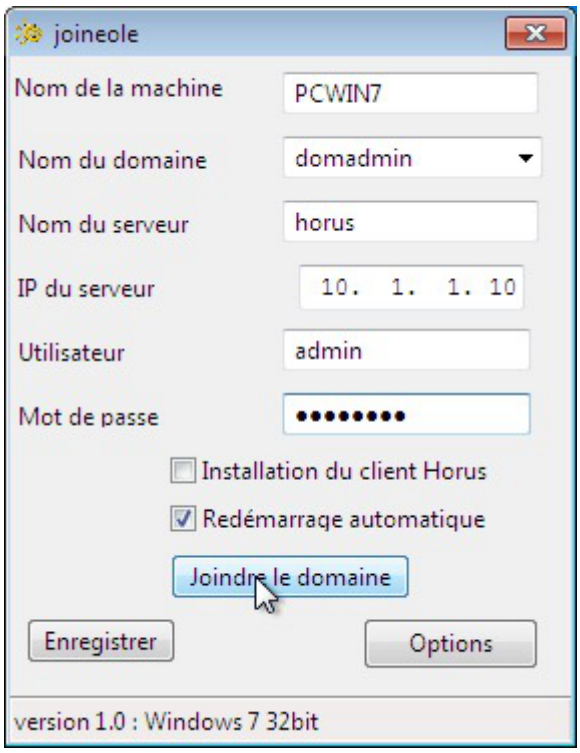
Le logiciel JoinEOLE est une contribution de Christophe Dezé de l'académie de Nantes.

Il n'est pas possible de lancer l'exécution de JoinEOLE directement depuis le lecteur réseau car l'utilitaire ne gère par les chemins UNC[p.143].

Il faut donc copier l'utilitaire en copiant le répertoire `IntegrDom` sur la machine cliente et lancer son exécution.



Il faut préciser le nom de la machine à intégrer, le nom du domaine auquel la machine doit être raccrochée, le nom netbios du serveur ainsi que l'adresse IP du serveur Scribe ou Horus.



L'utilitaire permet l'intégration au domaine et installe directement le client si ☑ Installation du client est cochée.

La case Redémarrer automatiquement est précochée.

Une fois les paramètres renseignés il faut cliquer sur Joindre le domaine et cliquer sur Enregistrer. La machine affiche un message indiquant qu'elle va redémarrer.

1.3.2. PrepaWin pour 2.5.1

PrepaWin et IntegrDom sont à utiliser sur un module Scribe 2.5.1.

À partir de la version 2.5.2 du module il faut utiliser JoinEOLE.

Le logiciel `PrepaWin` permet de préparer et d'intégrer une station Windows XP ou Seven Professionnel 32 ou 64 bits sur un domaine Scribe.

Pour plus d'informations, vous pouvez consulter le document suivant :

http://eole.ac-dijon.fr/pub/Documentations/divers/IntegrDom_PrepaWin_Scribe.pdf [http://eole.ac-dijon.fr/pub/Documentations/divers/IntegrDom_PrepaWin_Scribe.pdf]

Le logiciel `PrepaWin` est une contribution de Jérôme Labriet de l'académie de Besançon.

1.3.3. IntegrDom pour 2.5.1

PrepaWin et IntegrDom sont à utiliser sur un module Scribe 2.5.1.

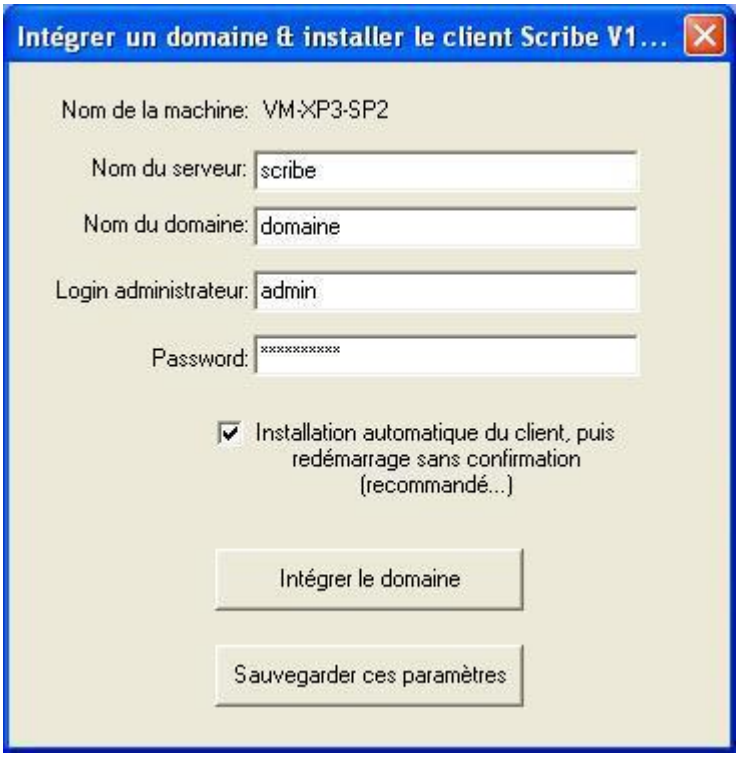
À partir de la version 2.5.2 du module il faut utiliser JoinEOLE.

Le logiciel `IntegrDom` est fourni dans le répertoire personnel de l'utilisateur `admin`.

Cet outil permet de joindre une station XP au domaine et d'y installer le client Scribe en une seule fois.

Il est possible de pré-paramétrer le logiciel. Pour cela :

- se connecter en admin sur une station déjà intégrer au domaine ;
- lancer le programme `U:\IntegrDom\IntegrDom.exe` ;
- remplir les paramètres de configuration ;
- cliquer sur *Sauvegardez les paramètres* ;
- copier le contenu du répertoire `U:\IntegrDom\` sur une clé USB.



Intégration au domaine et installation automatique du client Scribe

Pour joindre une nouvelle station au domaine, il faut :

- connecter la clé USB sur la station ;
- lancer `IntegrDom.exe` depuis la clé USB ;
- cliquer sur *Intégrer le domaine*.

Les erreurs éventuellement retournées par IntegrDom sont celles retournées par l'utilisation de la fonction NetJoinDomain : http://msdn.microsoft.com/en-us/library/aa370433(v=vs.85).aspx.

Le logiciel `IntegrDom` est une contribution de Daniel Piquée de l'académie de la Réunion.

1.3.4. Joinscribe

`joinscribe` est un outil d'intégration au domaine et d'installation du client Scribe qui s'exécute depuis le serveur.

L'outil joinscribe n'est pas pré-installé sur le serveur Scribe.

Il s'installe manuellement, saisir les commandes suivantes :

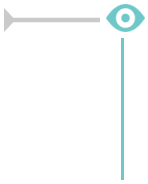
```
# Query-Auto
# apt-eole install joinscribe
```

Avant d'exécuter joinscribe, il faut préparer le poste client de la manière suivante :

- dans les "options des dossiers", onglet `Affichage`, décocher l'option `☑ Utiliser le partage de fichiers simple` ;

- mettre un mot de passe à l'utilisateur administrateur ;
- désactiver le pare-feu de Windows.

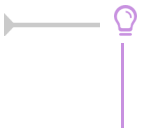
Une fois les postes clients préparés, lancer `joinscribe` depuis la console du serveur Scribe.



Exemple d'utilisation de joinscribe :

`joinscribe -d 192.168.1.1 -f 192.168.1.254`

`joinscribe -d 192.168.1.25`



En cas de problème, consulter sur le serveur Scribe les fichiers /var/log/joinscribe/ et sur le poste client c:\windows\eole\tmp\ParamIntegr.log.

Le logiciel `joinscribe` est une contribution de Christophe Dezé de l'académie de Nantes.

1.4. Intégration et installation du client Scribe manuelle

Intégration au domaine avec Windows 10

Préparation de Windows 10

L'intégration au domaine d'une station Windows 10 nécessite l'application préalable des clés de registre suivantes :

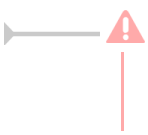
```
[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManWorkstation\Parameters]
"DNSNameResolutionRequired"=dword:00000000
"DomainCompatibilityMode"=dword:00000001


[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\NetworkProvider\HardenedPaths]
"\\\\*\\netlogon"="RequireMutualAuthentication=0,RequireIntegrity=0,RequirePrivacy=
0"
```

Le fichier Win_Samba3DomainMember.reg mis à disposition dans /home/esu/Console/ et accessible dans le dossier personnel de l'utilisateur `admin` contient ces clés de registre.

L'intégration au domaine d'une station Windows 10 nécessite également l'exécution en tant qu'Administrateur des commandes suivantes

```
sc.exe config lanmanworkstation depend= bowser/mrxsmb10/nsi
sc.exe config mrxsmb20 start= disabled
powershell.exe -Command "Enable-WindowsOptionalFeature -Online -FeatureName
SMB1Protocol -NoRestart"
```

Le script Win10.bat mis à disposition dans /home/esu/Console/ et accessible dans le dossier personnel de l'utilisateur `admin` contient ces commandes.



Depuis la version 1709 de Windows 10, l'intégration au domaine d'une station nécessite au

préalable d'activer le support de partage de fichiers SMB 1.0/CIFS sur les postes clients.

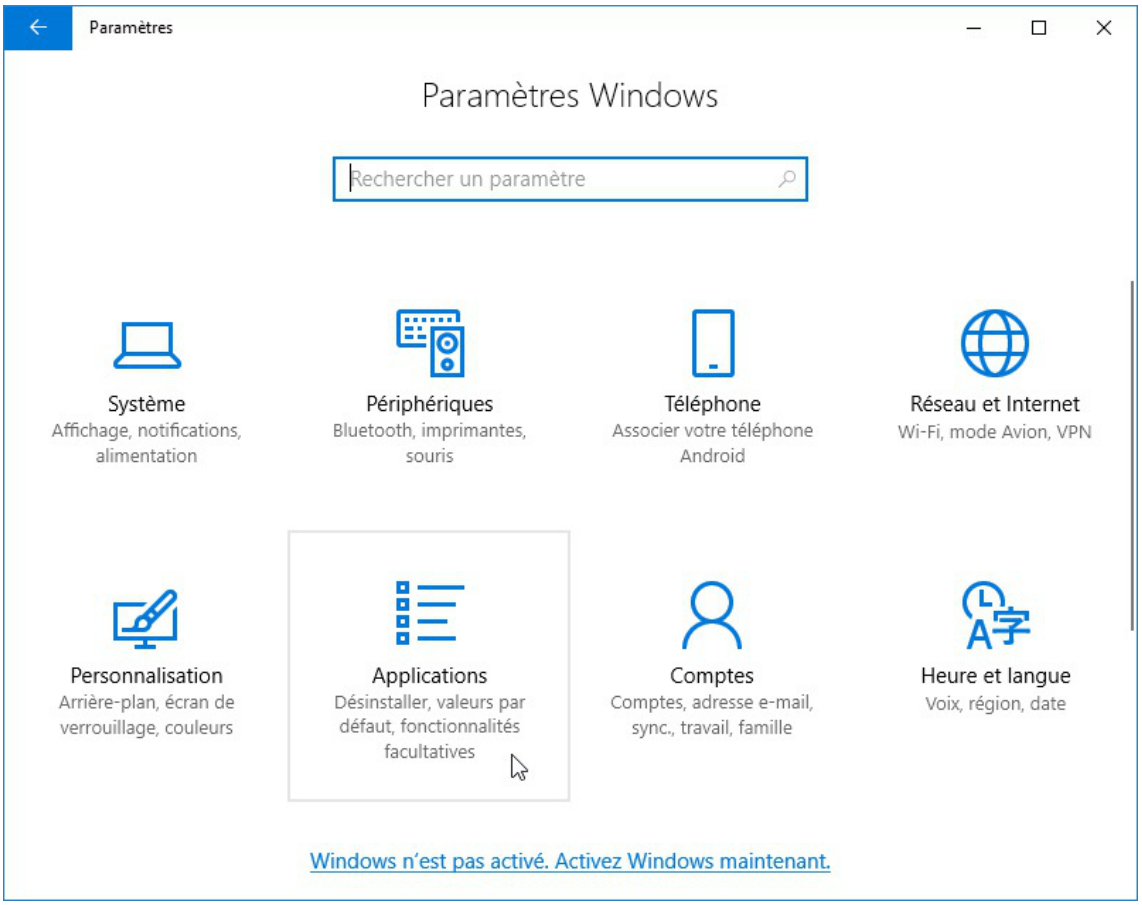
Depuis la version 1903 de Windows 10, le fonctionnement des profils obligatoires n'est plus garanti.

Activer manuellement le support de partage de fichiers SMB 1.0/CIFS

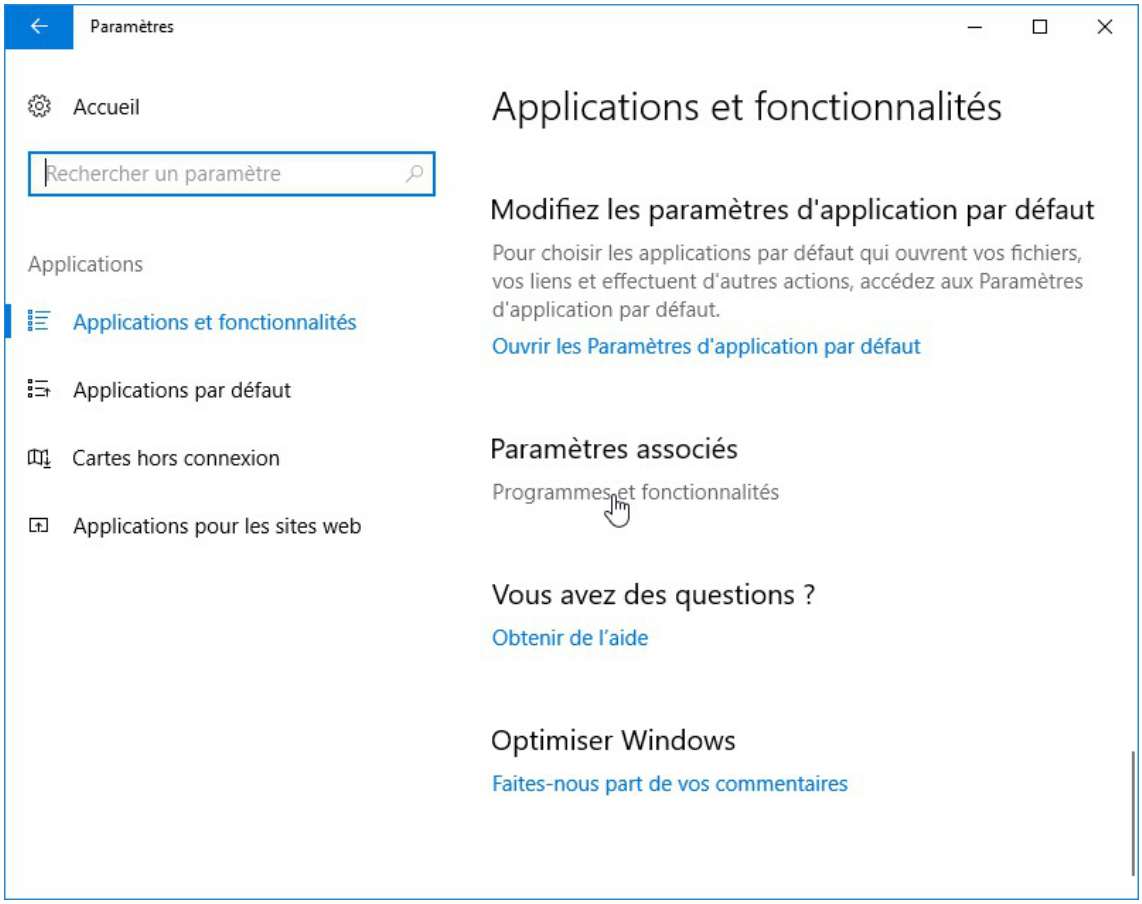
Sur un module EOLE à jour, l'activation du `support de partage de fichiers SMB 1.0/CIFS` est réalisée automatiquement par JoinEOLE et sa commande d'activation a été ajoutée au script `Win10.bat`.

Paramétrer Windows de la façon suivante :

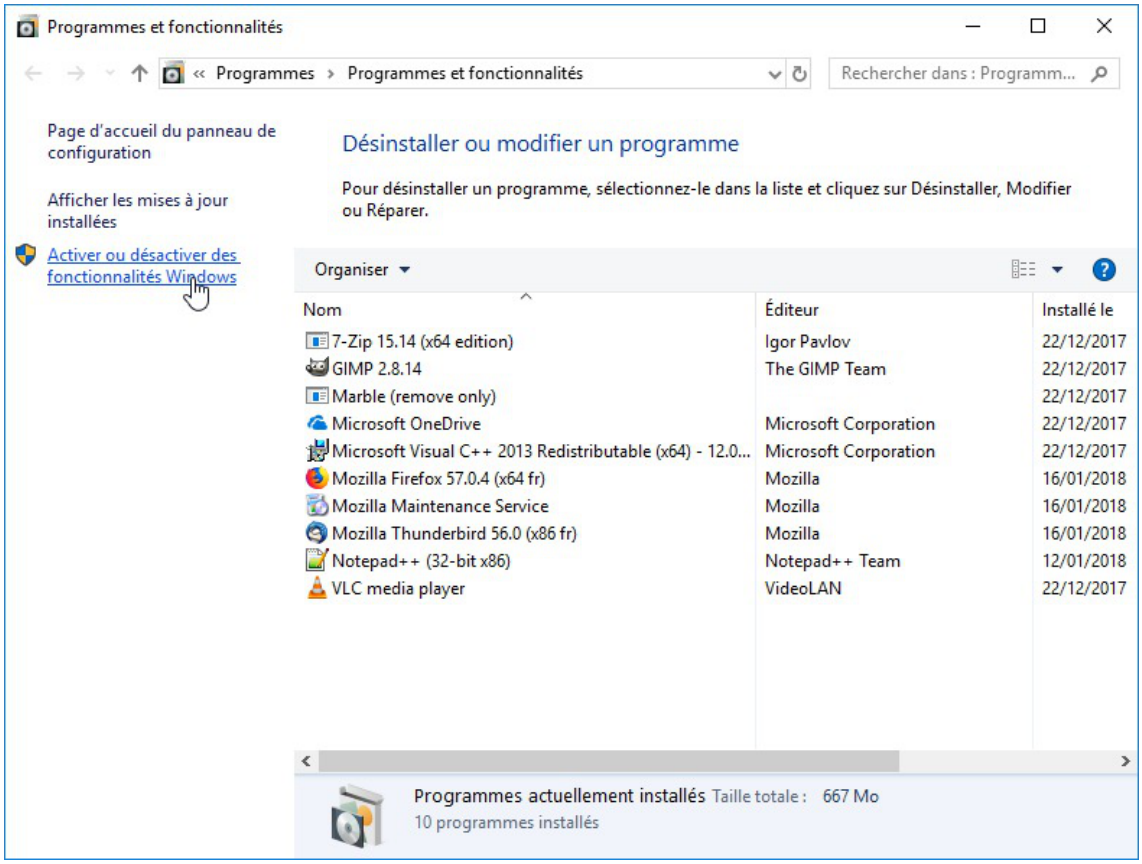
- Menu `Windows` et sélectionner `Paramètres` ;



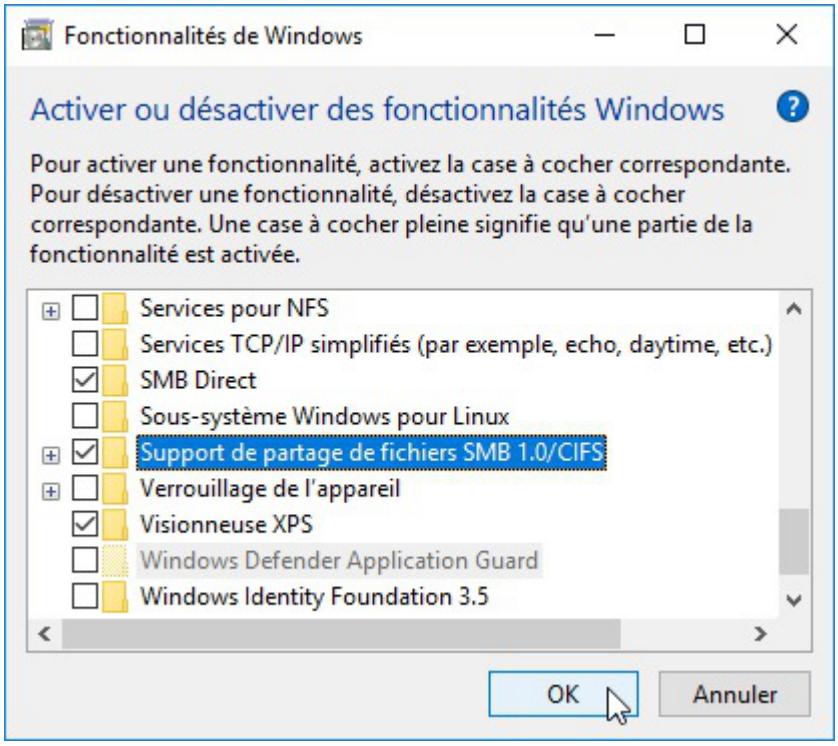
- Cliquer sur `Applications` ;



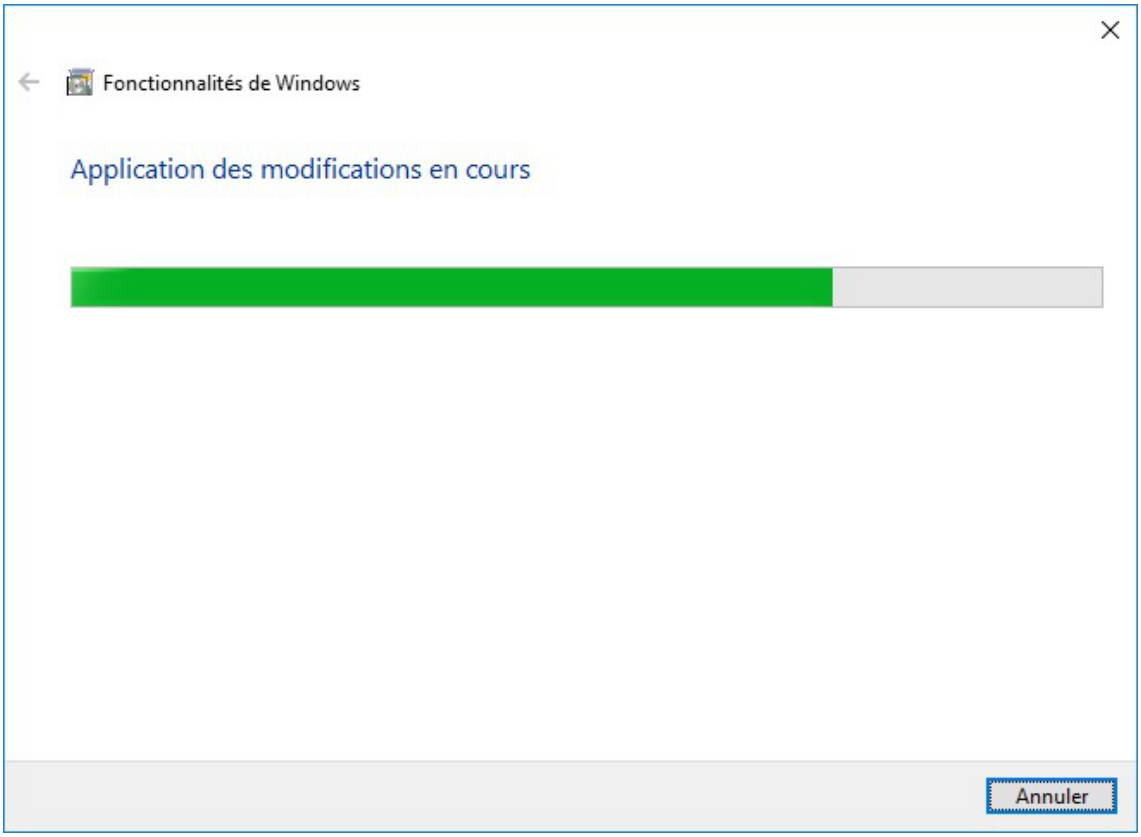
- Descendre et cliquer sur `Programmes et fonctionnalités` ;



- Cliquer sur `Activer ou désactiver des fonctionnalités Windows` ;



- Descendre dans la liste et cocher ☑ Support de partage de fichiers SMB 1.0/CIFS , cliquer sur OK, les modifications s'appliquent ;



Accéder au répertoire personnel de l'administrateur du domaine

Depuis la version 1709 de Windows 10, il est impossible d'accéder au lecteur réseau en mode invité.

Pour accéder au répertoire de l'administrateur avant la jonction au domaine il faut :

- soit appliquer une clé de registre pour supprimer cette interdiction ;

- soit monter un lecteur réseau en spécifiant les identifiants de connexion.

https://support.microsoft.com/de-ch/help/4046019/guest-access-smb2-disabled-by-default-in-windows-1(

Réactiver l'accès aux partages guest via une clé de registre

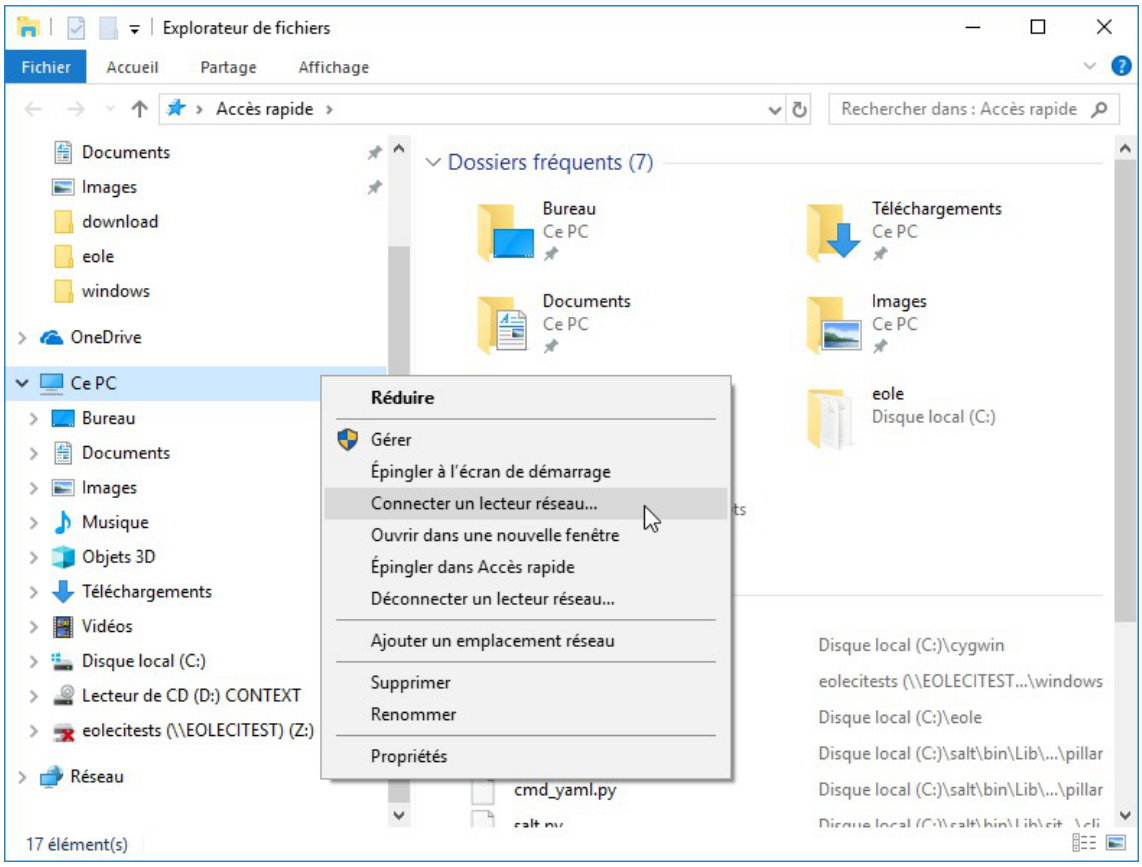
La clé de registre suivante permet de réactiver la possibilité de se connecter à un partage non sécurisé.

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters]
"AllowInsecureGuestAuth"=dword:00000001
```

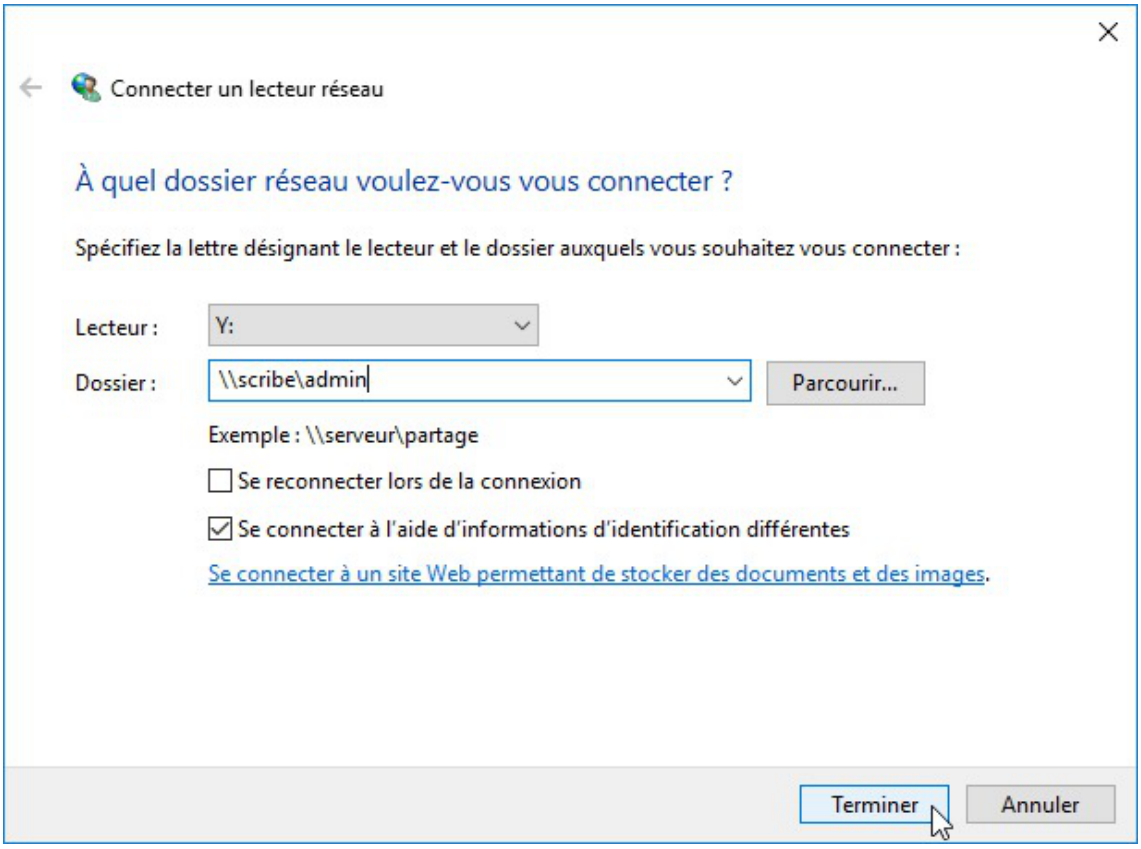
Monter un répertoire en spécifiant les identifiants de connexion

Pour accéder au répertoire personnel de l'administrateur :

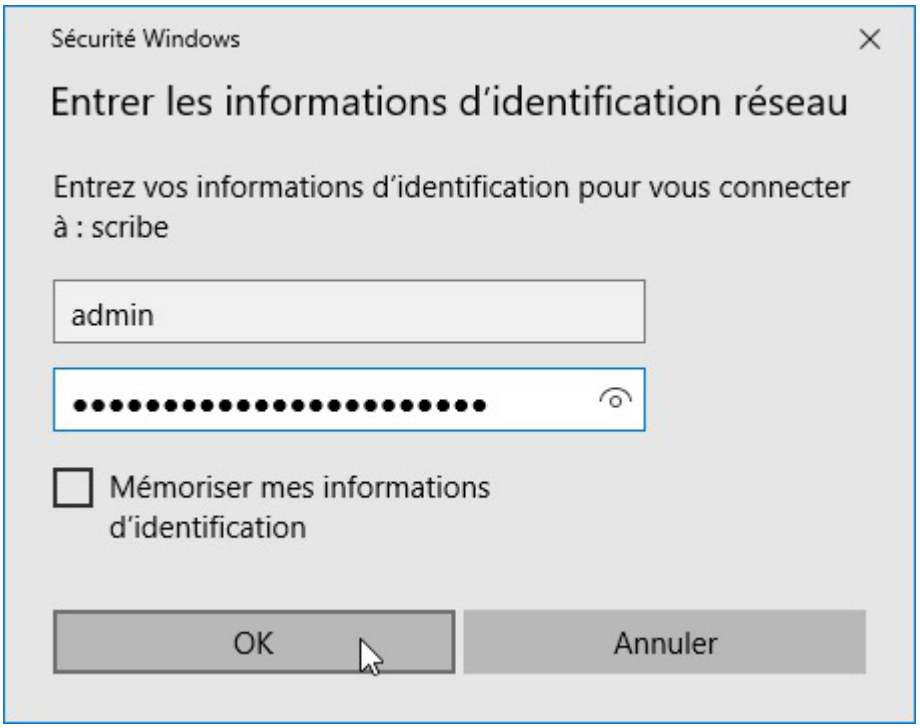
- Se connecter sur le poste en tant qu'administrateur ;
- Se rendre dans l'explorateur de fichier ;



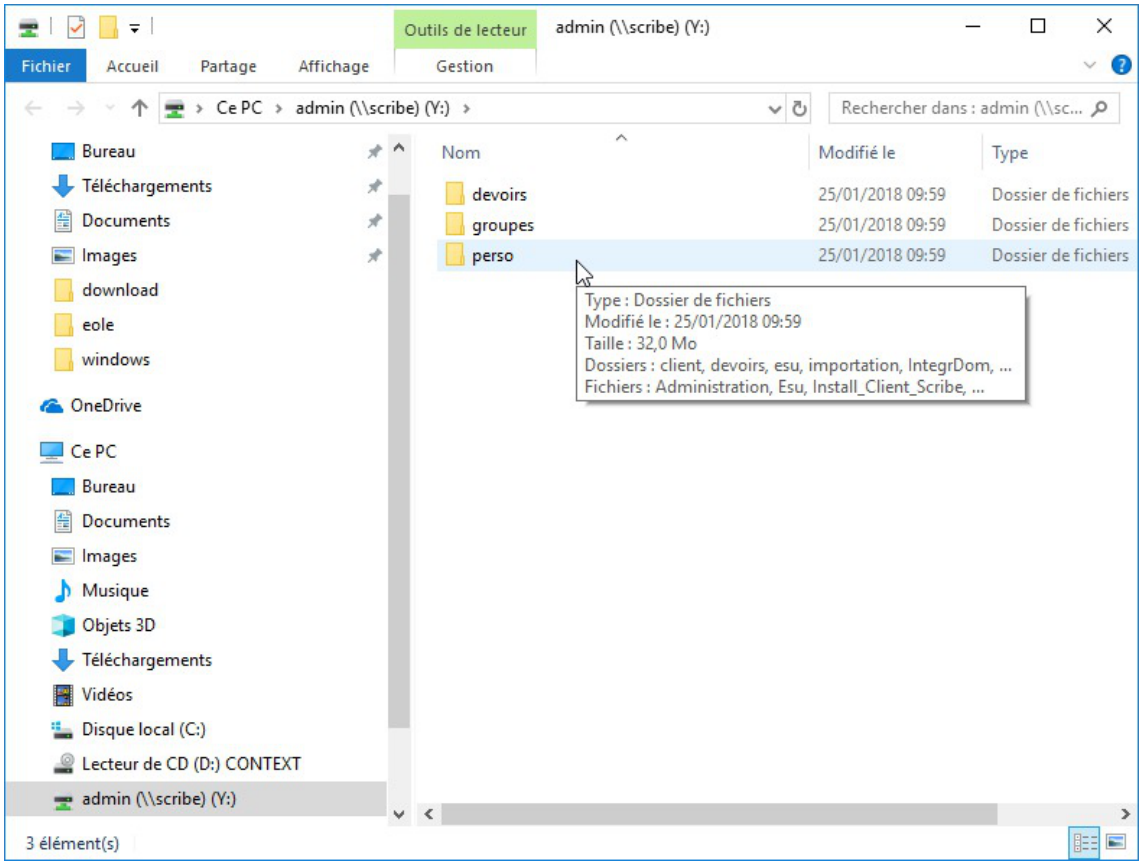
- Faire un clique droit sur `Ce PC` ;



- Saisir `\\scribe\admin` dans le champ `Dossier`, décocher ☑ Se reconnecter lors de la connexion, cocher ☑ Se connecter à l'aide d'informations d'identification différentes et cliquer sur le bouton `Terminer` ;



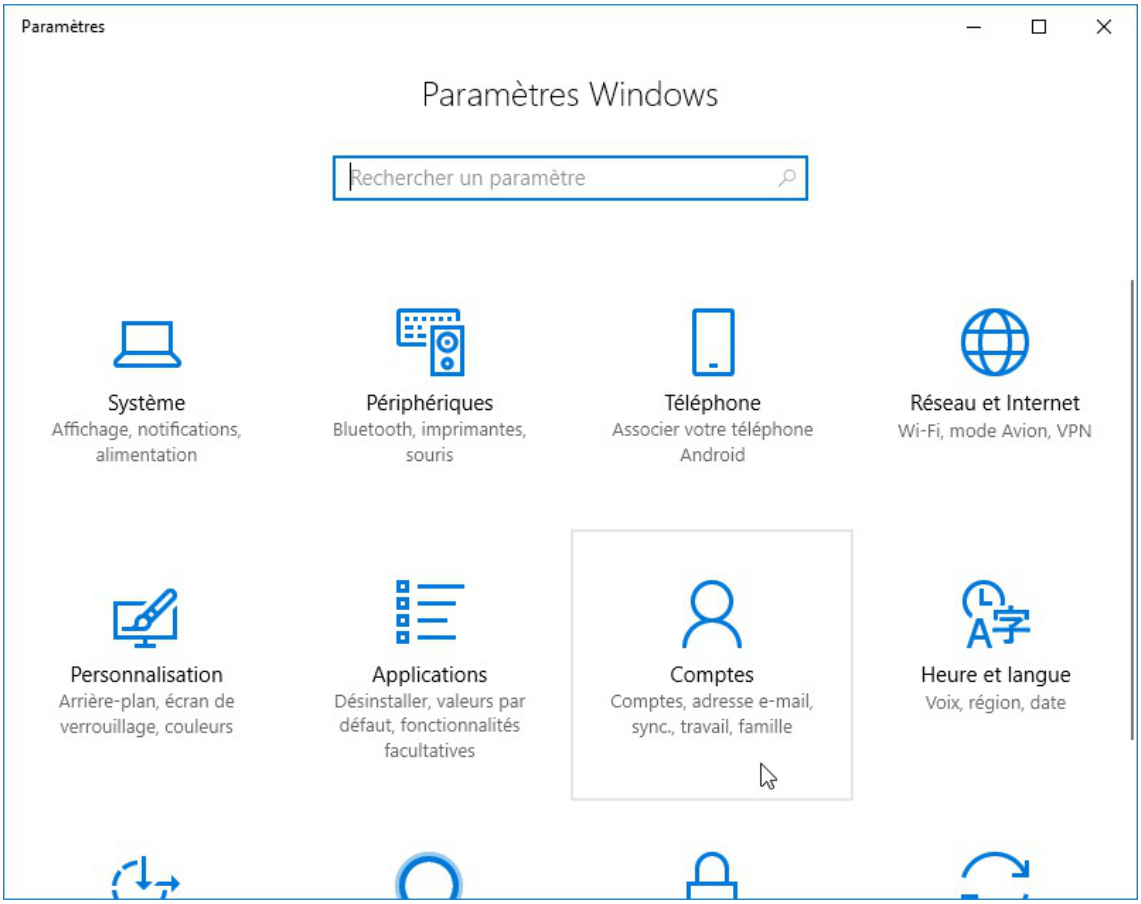
- Saisir le compte `admin` et la clé secrète associée ("mot de passe") et cliquer sur le bouton `OK` ;



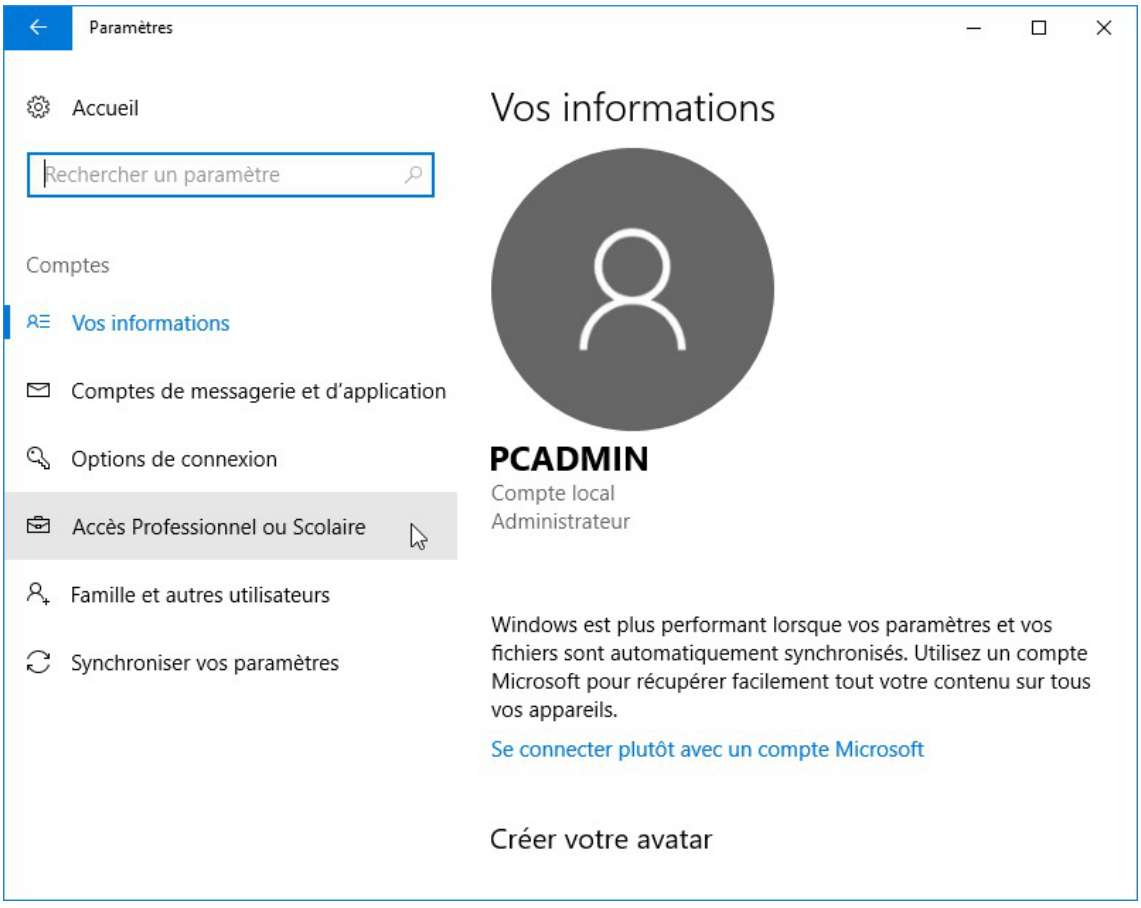
Jonction au domaine

Ajouter la station au domaine de la façon suivante :

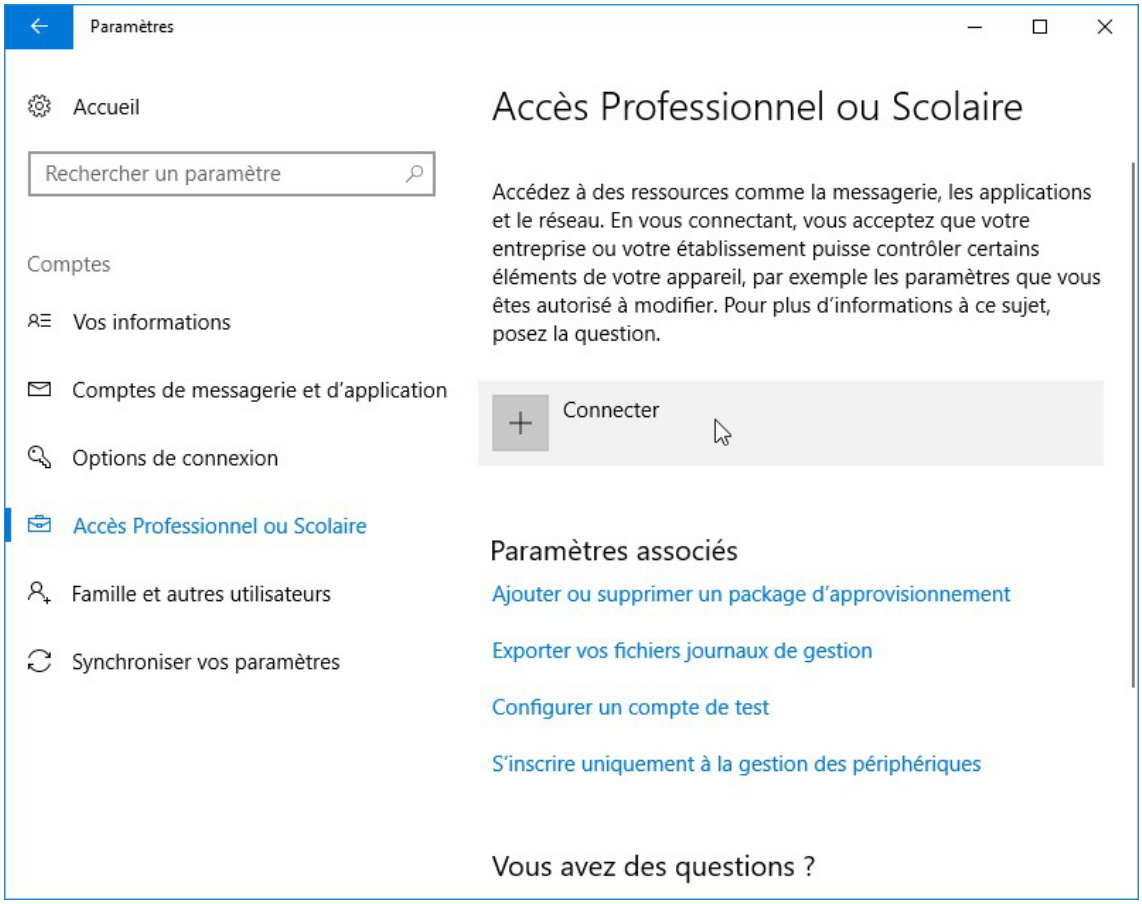
- Menu `Windows` et sélectionner `Paramètres` ;



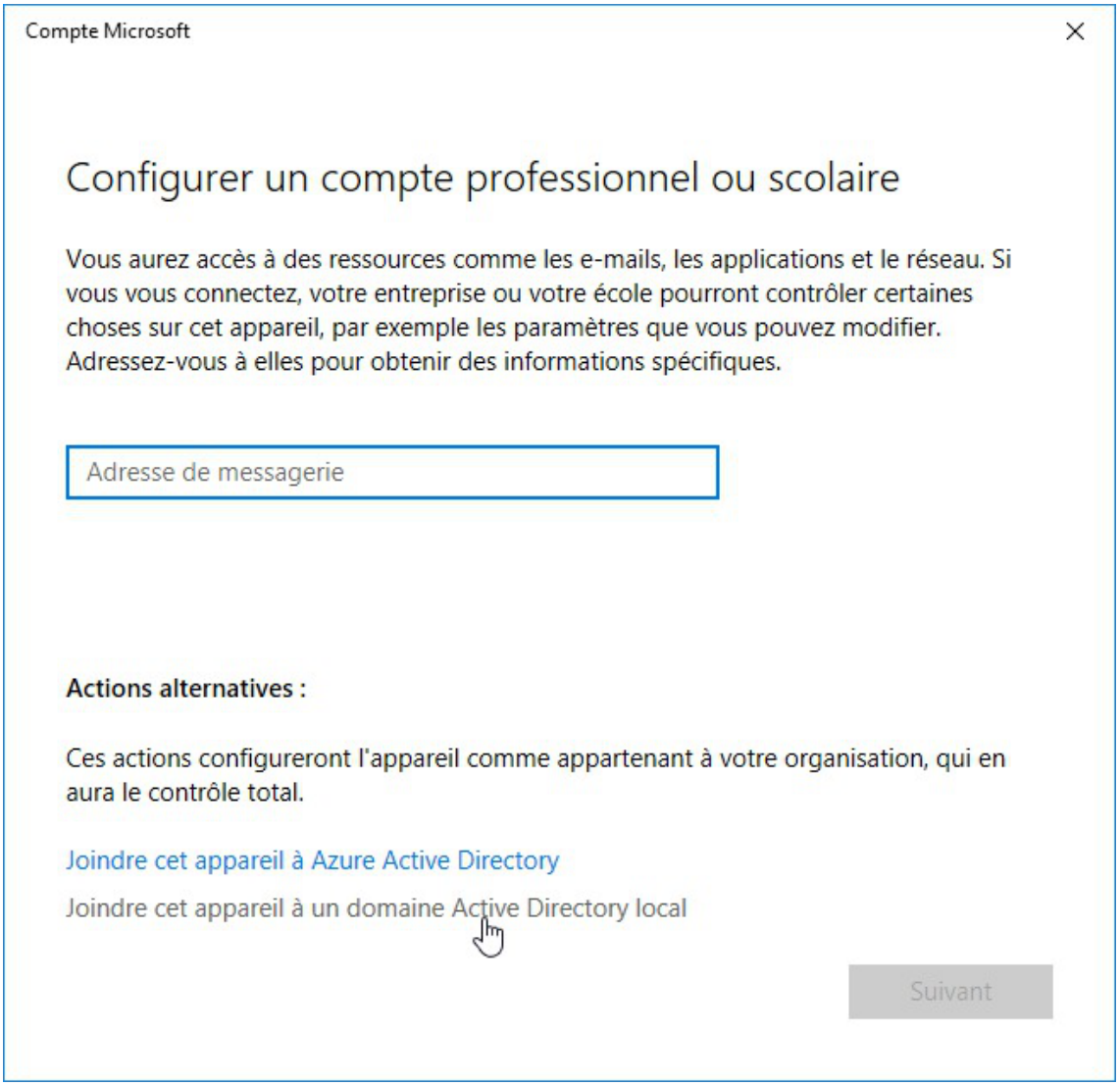
- Cliquer sur Comptes ;



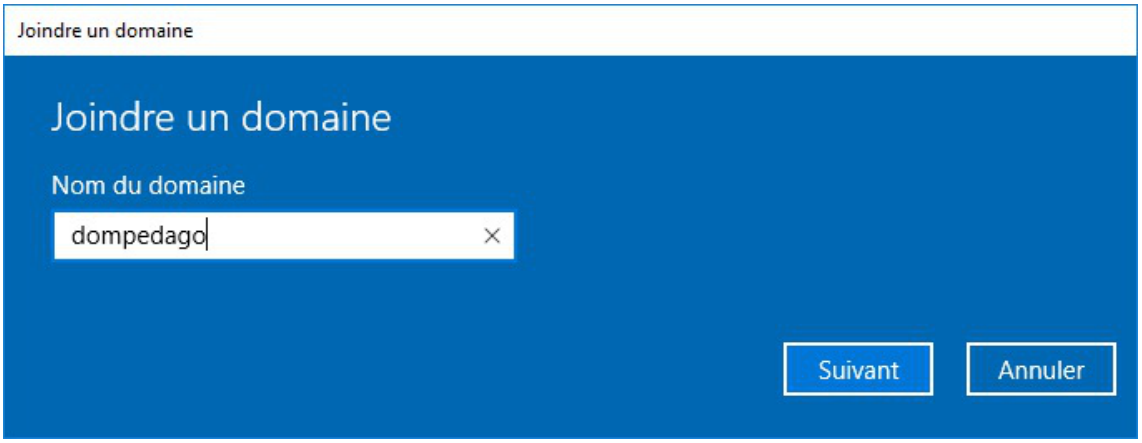
- Cliquer sur Accès Professionnel ou Scolaire dans le menu de gauche ;



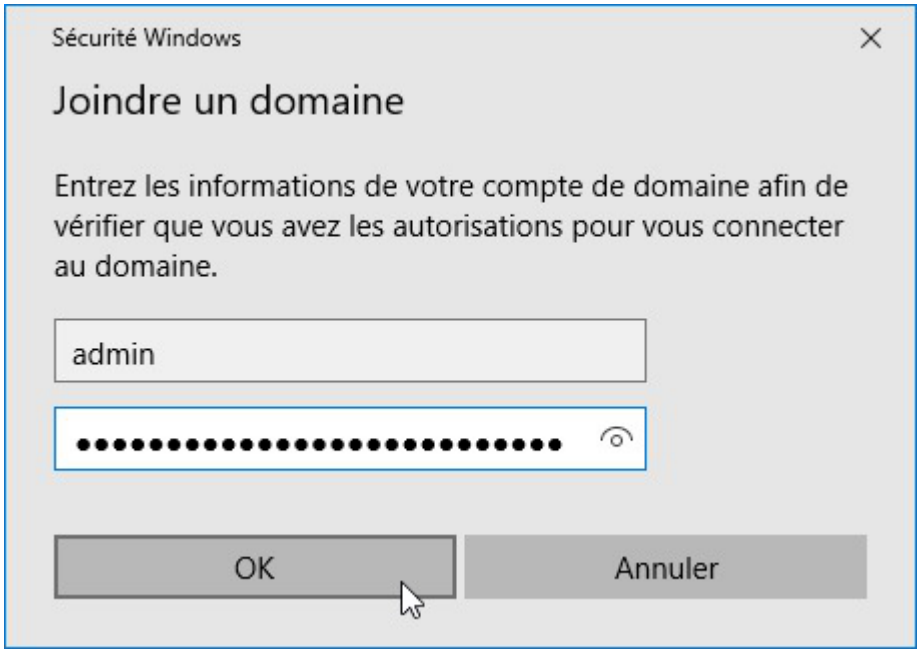
- Cliquer sur `Connecter` ;



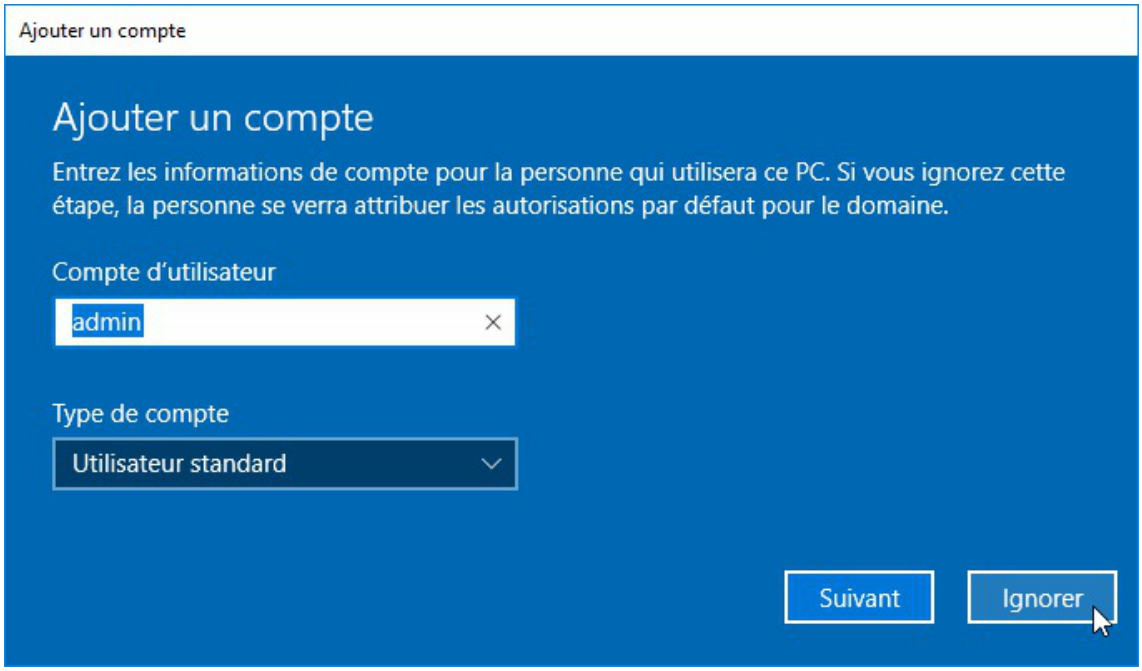
- Cliquer sur `Joindre cet appareil à un domaine Active Directory local` ;



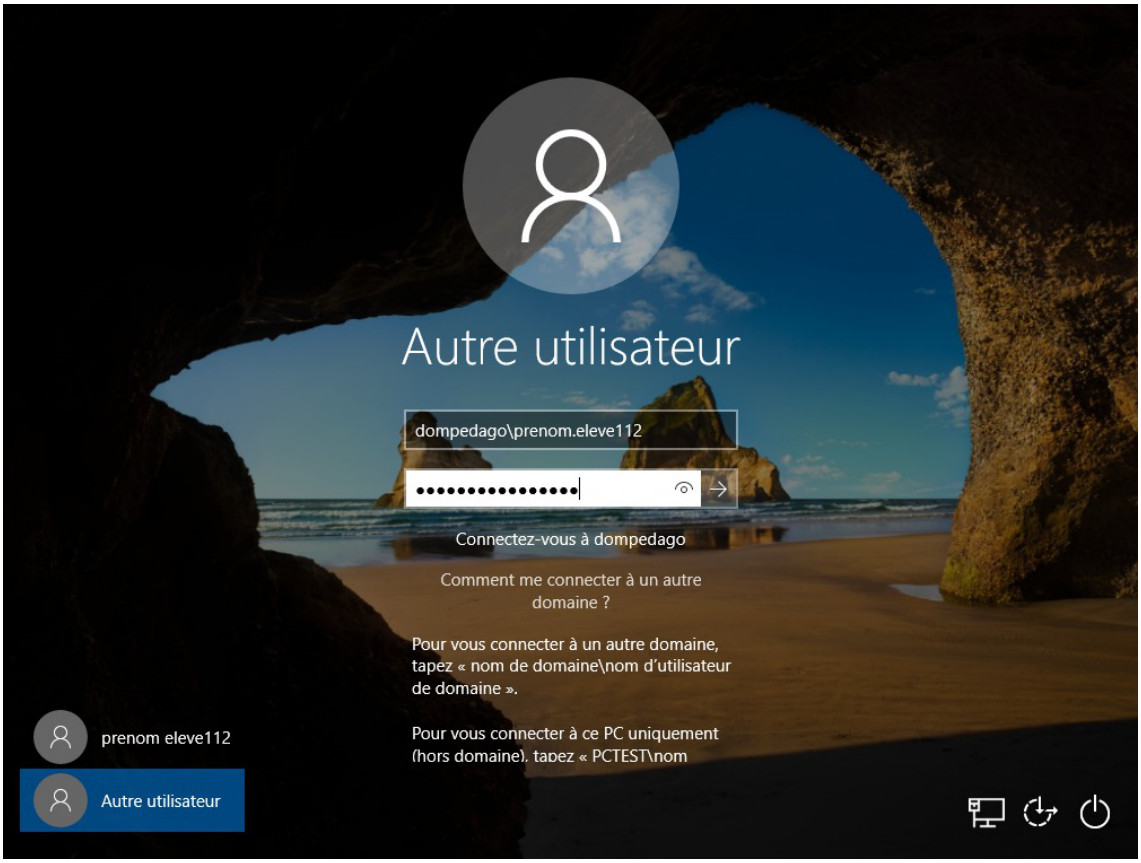
- Saisir le nom du domaine et cliquer sur `Suivant` ;



- Saisir le nom du compte administrateur du domaine ainsi que la clé secrète ("mot de passe") associée au compte et cliquer sur le bouton `OK` ;



- Il ne faut pas tenir compte de la proposition d'ajout de compte, cliquer sur le bouton `Ignorer` et accepter de redémarrer ;



- Cliquer sur `Autre utilisateur` et saisir le nomDuDomaine\pnom ainsi que la clé secrète ("mot de passe") pour démarrer la session.

Intégration au domaine avec Windows 7

Préparation de Windows 7

L'intégration au domaine d'une station Windows 7 nécessite l'application préalable des clés de registre suivantes :

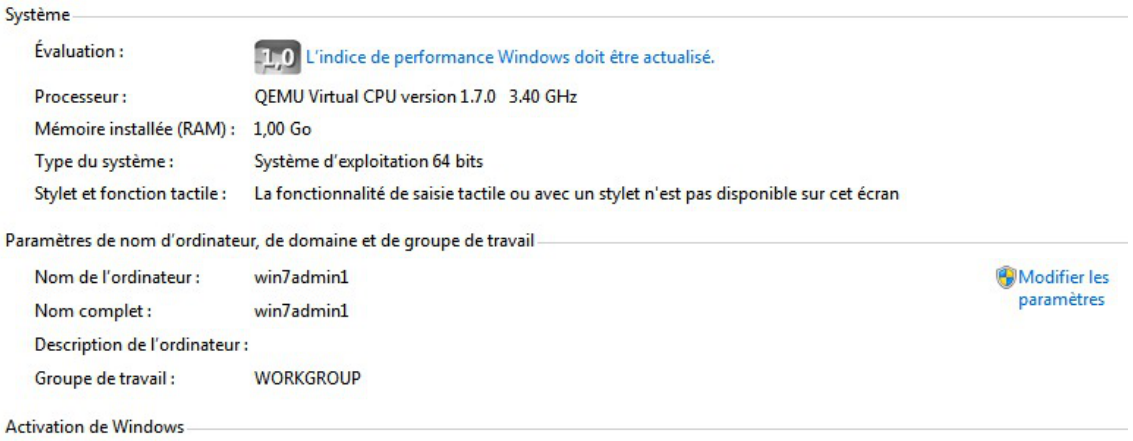
```
[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManWorkstation\Parameters]
"DNSNameResolutionRequired"=dword:00000000
"DomainCompatibilityMode"=dword:00000001


[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\NetworkProvider\HardenedPaths]
"\\\\*\\netlogon"="RequireMutualAuthentication=0,RequireIntegrity=0,RequirePrivacy=0"
```

Un fichier `Win7_Samba3DomainMember.reg` est mis à disposition pour modifier la base de registre dans `/home/esu/Console/`.

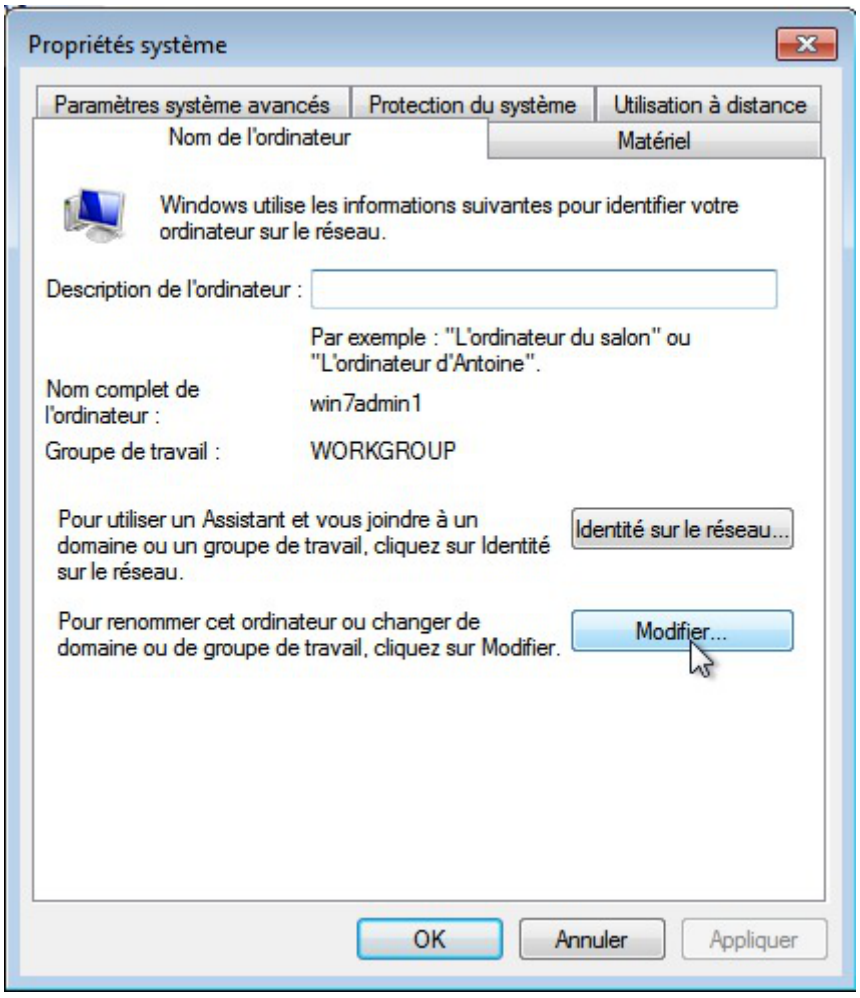
Jonction au domaine

Ajoutez la station au domaine de la façon suivante :

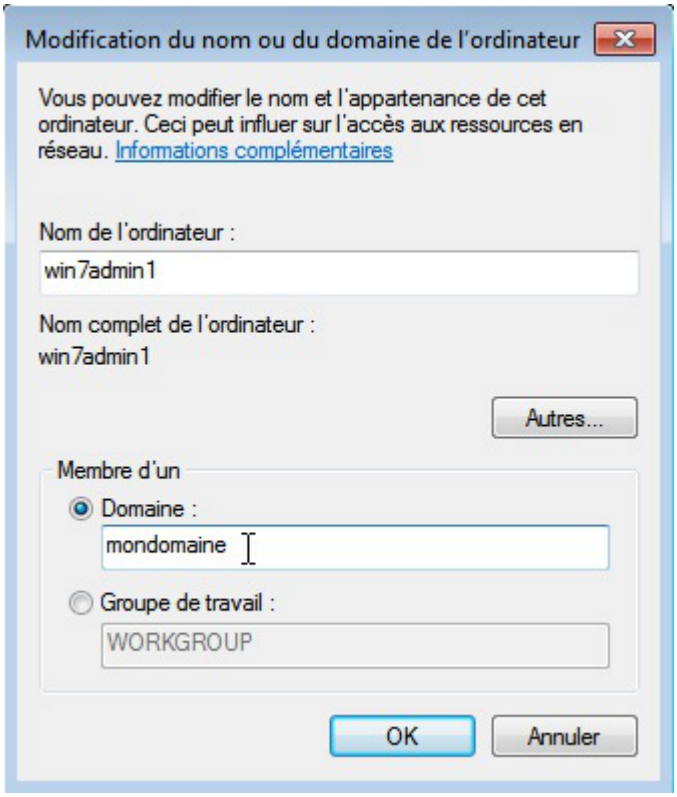
- Aller dans le menu `Démarrer` ;
- Clic droit sur `Ordinateur` et sélectionner `Propriétés` ;



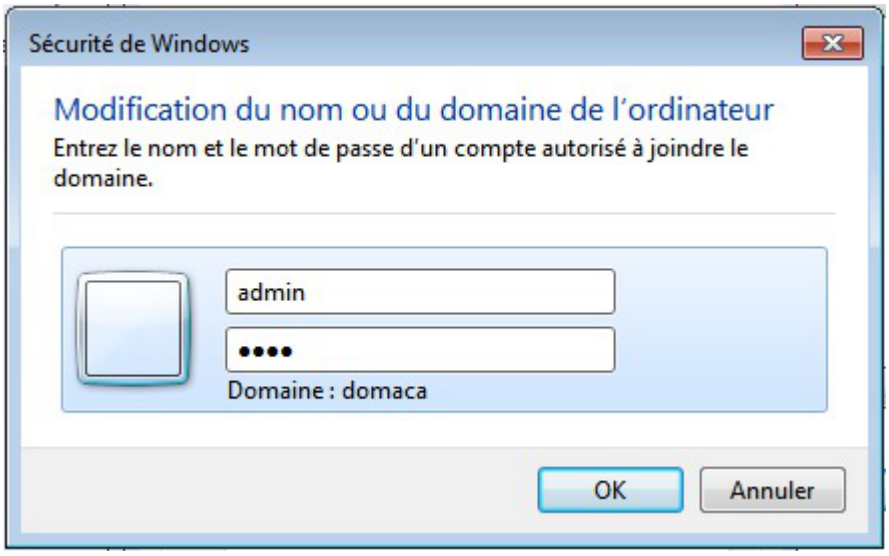
- Cliquer sur Modifier les paramètres ;



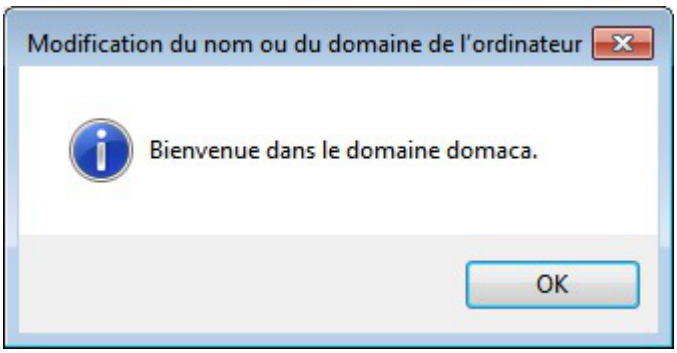
- Cliquer sur le bouton Modifier... ;



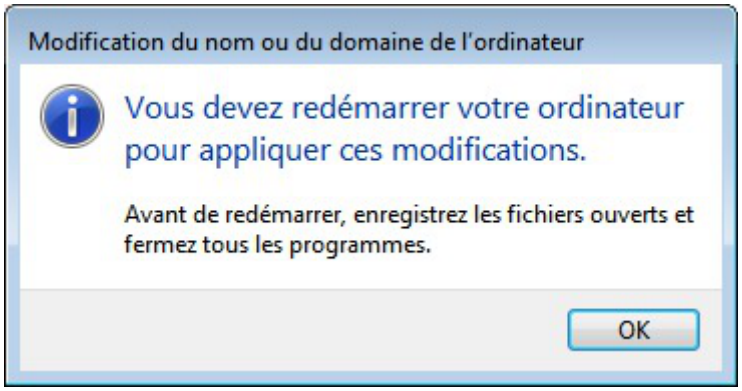
- Renseigner le nom de domaine Samba et cliquer sur `OK` ;



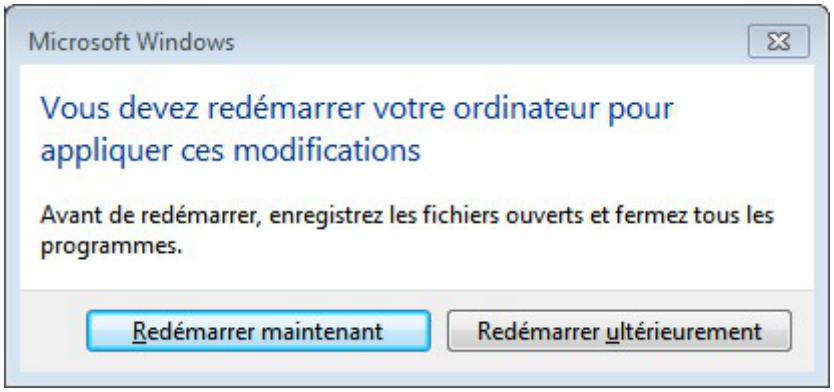
- Utiliser le compte `admin` ou un compte ayant les droits suffisants pour finaliser l'intégration ;



- Confirmer le message de bienvenue ;



- Confirmer le message d'avertissement ;

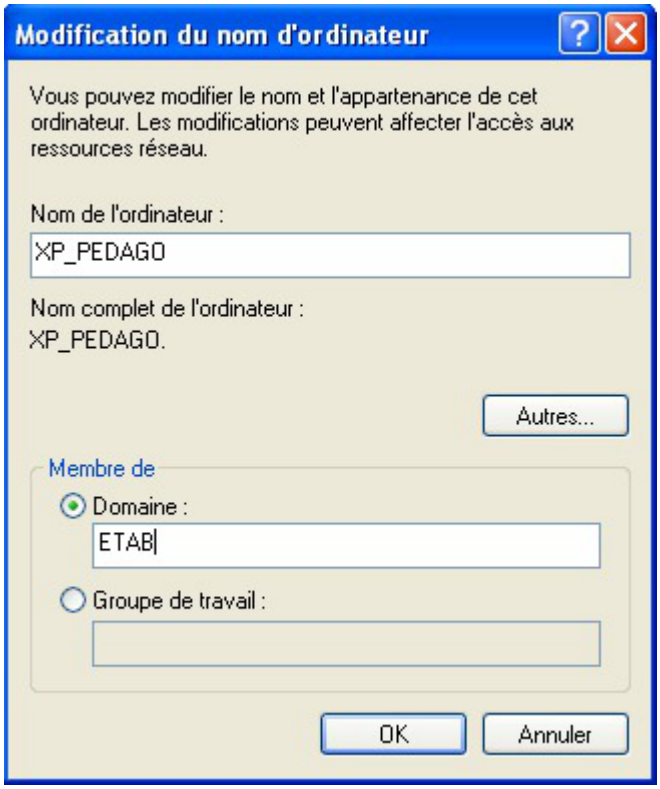


- Redémarrer maintenant.

Intégration au domaine pour Windows XP

Ajoutez la station au domaine de la façon suivante :

- clic droit sur le `Poste de travail` ;
- `Propriétés` ;
- onglet `Nom de l'ordinateur` ;
- cliquer sur `Modier...` ;
- sélectionner `◉ Domaine` :
- dans `Membre de` renseigner le nom du `◉ Domaine` ;
- valider : utiliser *admin* ou un compte ayant les droits suffisants pour finaliser l'intégration ;
- redémarrer.



Intégration manuelle au domaine

Installation du client Scribe

Pré-requis à l'installation du client Scribe

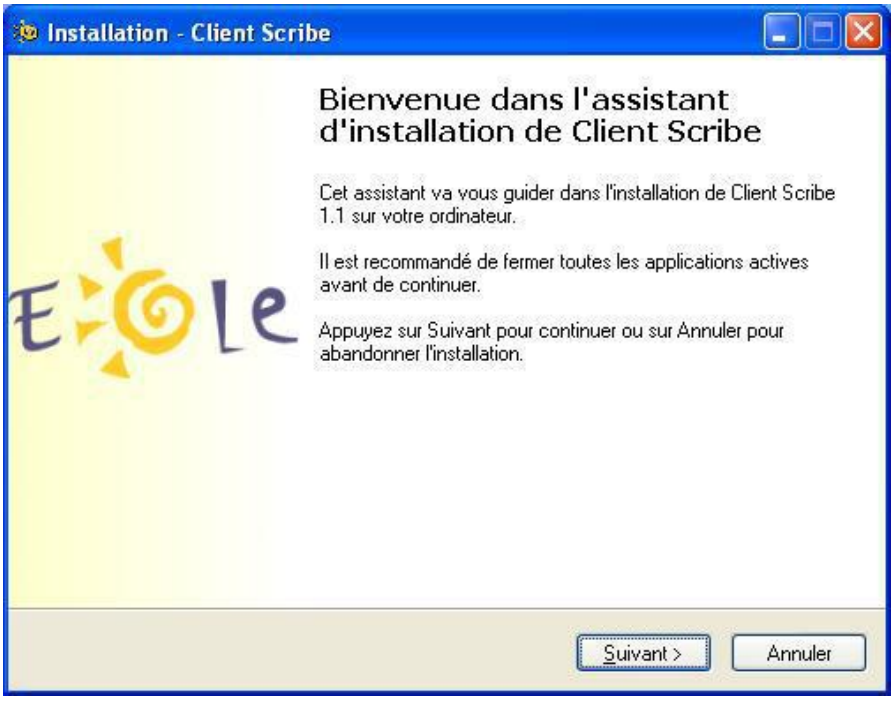
Le service pack 3 pour Windows XP est recommandé pour un fonctionnement correct du client Scribe.

Windows Vista est compatible avec l'ensemble des applications.

Il est indispensable que la station soit mise à l'heure avant son intégration au domaine, pour cela exécutez la commande `net time /SET /YES \\<adresse ip scribe>`.

Installation manuelle du client

L'installeur du client possède un raccourci accessible avec l'utilisateur **admin** dans `U:\Install_Client_Scribe`.



Installation du client Scribe

Une fois installé, le programme d'installation demande un redémarrage.

Après cela, l'ouverture de session suivante devrait ressembler à cela :

Bureau par défaut de l'utilisateur "admin"

Versions 64 bits

Pour les versions 64 bits de Windows 7, une version spécifique du client Scribe avait été diffusée.

Depuis, les deux installeurs ont été fusionnés et l'exécutable `cliscribe-setup.exe` détecte

automatiquement l'architecture du système.

Windows 2000

L'installeur du client Scribe utilise le programme `sc.exe`. Les utilisateurs de windows 2000 trouveront cet exécutable dans le windows 2000 resource kit [http://support.microsoft.com/kb/927229] .
`sc.exe` peut aussi être copié depuis windows XP dans `%WINDIR%\System32`.

Installation et redémarrage automatique

Il est possible d'installer le client en mode automatique à l'aide d'un fichier .bat contenant ceci :

echo off
rem il faut empecher le redemarrage par le premier installeur
echo Installation du service de mise a jour
U:\client\cliscribe-updater-setup.exe /VERYSILENT /NORESTART
echo Installation du client
U:\client\cliscribe-setup.exe /VERYSILENT
echo redemarrage...
echo on

En fin d'installation le système redémarrera sans poser de question.

1.5. Mise à jour du client Scribe

Le client Scribe installé sur les stations Windows est automatiquement mis à jour si une nouvelle version est disponible sur le serveur. L'installeur du client Scribe présent sur le serveur est fourni par le paquet *controle-vnc-client*. Autrement-dit, si le paquet *controle-vnc-client* est mis à jour sur le serveur, les clients Windows se mettront automatiquement à jour au prochain redémarrage.

Principe de la mise à jour du client :

- lors de l'installation du client Scribe, le fichier `%WINDIR%\Eole\install.ini` est créé. Ce fichier contient la version du client installé ;
- à chaque démarrage de la station le service de mise à jour du client vérifie sur le serveur si une nouvelle version est disponible en téléchargeant le fichier `http://<adresse_module>:8790/install.ini` ;
- si une nouvelle version est disponible, le service désinstalle l'ancienne version, redémarre, installe la nouvelle version et redémarre à nouveau.

Le fichier de référence du serveur est `/home/client_scribe/install.ini`. (lié pour "*admin*" dans `U:\client\install.ini`).

Les opérations effectuées par le service de mise à jour du client Scribe sont journalisées dans `%WINDIR%\cliscribe_updater.log`.

Le service de mise à jour du client Scribe est accompagné d'une fenêtre d'indication de l'avancement qui s'affiche lorsqu'un utilisateur ouvre une session pendant la mise à jour du client Scribe.

Fenêtre d'avancement de la mise à jour

Si pour une raison précise la mise à jour des clients doit être **ponctuellement** désactivée, il est possible de le faire :

- par station, en renseignant "VERSION = 0" dans le fichier `%WINDIR%\Eole\install.ini` ;
- pour toutes les stations, en renseignant "VERSION = 0" dans le fichier `/home/client_scribe/install.ini`.

Il est fortement déconseillé de désactiver la mise à jour du client parce que :

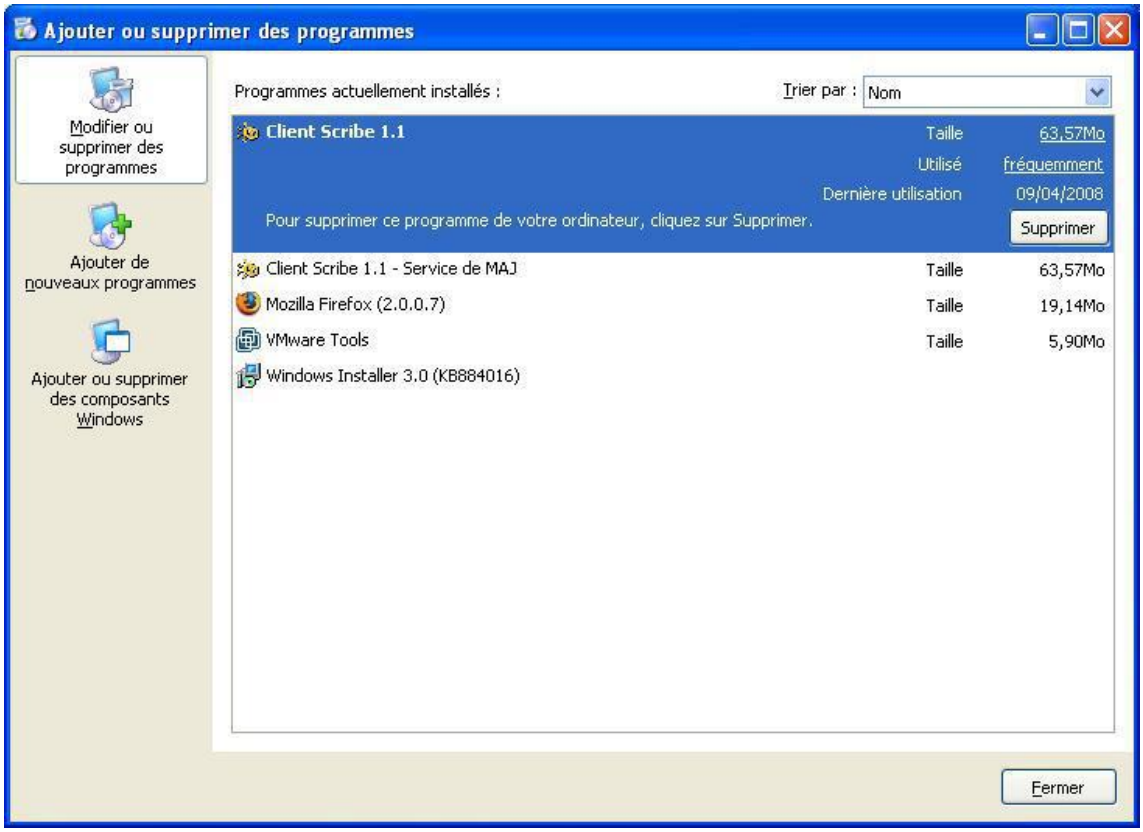
- le serveur sera à jour et pas le client, certaines actions risquent de ne plus fonctionner ;
- les nouvelles fonctionnalités ne seront pas disponibles ;
- les mises à jour peuvent contenir des corrections de sécurité.

Aucune aide ne pourra être apportée si le client n'est pas à jour.

1.6. Désinstallation du client Scribe

La désinstallation du client Scribe s'effectue dans :

- `Panneau de configuration`
- `Ajout/Suppression de programmes`



Désinstallation du client Scribe

Le client Scribe est composé de deux parties :

- le client ;
- le service de mise à jour du client.

Elles sont installées simultanément mais demandent une désinstallation séparée.

Le service de mise à jour du client doit être désinstallé avant le client car, au démarrage de la machine, si le client n'est pas trouvé, le service de mise à jour le réinstallera automatiquement.

2. Administration des clients Windows

Afin de faciliter l'administration des clients, divers outils ont été développés et installés sur le module Scribe :

- **ESU**, configuration du poste client et de l'environnement de l'utilisateur, composé d'une console et d'un client ;
- **Gestion-postes**, action sur les élèves par les professeurs (observation/diffusion de poste, blocage temporaire, ...) ;
- l'**EAD**, action sur les postes et les utilisateurs.

Fonctionnement général sous Windows

Sur un module Scribe installé de façon standard (pas d'adaptations locales), de l'installation du poste client à sa mise en production, on peut décrire les étapes comme ceci :

- installation du poste client ;
- intégration au domaine Scribe ;
- installation du client Scribe ;
- utilisation.

À cet instant les utilisateurs peuvent utiliser le poste client. Le module Scribe est livré avec une configuration ESU par défaut sous la forme d'un groupe de machine "**grp_eole**" comportant trois groupes d'utilisateurs : **DomainAdmins**, **professeurs** et **eleves**.

Ensuite, via la **console ESU**, l'administrateur ("**admin**" par défaut) peut personnaliser la configuration, ajouter des groupes de machines, des groupes d'utilisateurs, modifier les règles, etc.

Fichiers invisibles sur les partages

Tous les noms de fichiers commençant par un point sont invisibles dans les partages Windows.

Dans la configuration de Samba, plusieurs types de fichiers ont été ajoutés pour les rendre invisibles des utilisateurs :

- desktop.ini : les fichiers `desktop.ini` générés par le fonctionnement de Windows sont cachés à l'utilisateur (`hide files = /desktop.ini/` dans le fichier `smb.conf`). En mode expert, la liste des fichiers cachés peut être personnalisée grâce à la variable `Fichiers à masquer dans le partage` ;
- $recycle.bin : les fichiers `$recycle.bin` générés par le fonctionnement de Windows sont cachés et inaccessibles par l'utilisateur (`veto files = /$RECYCLE.BIN/` dans le fichier `smb.conf`) ;
- .scanned:* : si l'anti-virus temps réel est activé, les fichier `.scanned:*` générés par Scannedonly[p.142] sont cachés et inaccessibles par l'utilisateur (`veto files = /.scanned:*/`).

2.1. L'ouverture de session

Le client Scribe/ESU fonctionne sous forme de service. Ce service est accompagné de deux applications s'exécutant dans l'environnement de l'utilisateur à l'ouverture de session.

En plus d'appliquer la configuration ESU, le client Scribe gère l'observation et la diffusion de l'écran du poste, le blocage Internet et le "mode devoir", l'arrêt, le redémarrage et la fermeture forcée de session depuis l'EAD.

Lorsqu'un utilisateur du domaine Scribe ouvre une session sur un poste Windows, un ensemble d'actions sont effectuées. Certaines sont des mécanismes internes à Windows, d'autres sont spécifiques à Scribe.

Après qu'un utilisateur du domaine ait validé son mot de passe la session s'ouvre :

- le profil de l'utilisateur est installé ;
- exécution de `%WINDIR%\Eole\cliscribe\logon.exe`.

Le programme `logon.exe` effectue les actions suivantes :

- lecture du fichier `\\<scribe>\netlogon\<login>\WinXP.txt` et exécution des instructions ;
- requête sur le serveur pour :
  - l'application des règles ESU ;
  - l'application du blocage ;

- l'application du mode d'observation (vnc_viewonly).

Simulation d'ouverture de session

Lors de la mise en place de la configuration d'ESU, il est souvent nécessaire de ré-ouvrir une session pour tester les nouveaux paramétrages.

La ré-application des règles sans avoir à ré-ouvrir une session peut se faire avec :

`Démarrer => Exécuter => "%WINDIR%\Eole\cliscribe\logon.exe"`

Généralités sur les scripts personnalisés

Il est possible d'ajouter des commandes à exécuter à l'ouverture de session.

Ces commandes doivent être renseignées dans un fichier `.txt` se trouvant dans un des sous-répertoire de `\\<scribe>\netlogon\scripts`.

Ces scripts peuvent être ajoutés pour :

- un utilisateur → `/home/netlogon/scripts/users/admin.txt` ;
- un groupe → `/home/netlogon/scripts/groups/eleves.txt` ;
- une machine → `/home/netlogon/scripts/machines/poste01.txt` ;
- un OS (Win95, Win2K, WinXP, Samba, Vista) → `/home/netlogon/scripts/os/WinXP.txt` ;

Windows 7 et Windows 10 sont traités de la même manière que Windows Vista *(OS=Vista)*.

Les noms de machines doivent être écrits en minuscules.

- un OS et un utilisateur → `/home/netlogon/scripts/os/Win2K/admin.profil.txt` ;
- un OS et un groupe → `/home/netlogon/scripts/os/WinXP/professeurs.txt`.

Les scripts personnalisés sont concaténés dans le script principal, par défaut au début de celui-ci. Si des instructions doivent être effectuée après (nécessité d'avoir accès au lecteur `commun` par exemple), placez la balise **%%NetUse%%** et ajoutez les instructions ensuite.

L'éditeur Bloc-note de Windows (`notepad.exe`) ne gère pas correctement les sauts de ligne.

Les fichiers personnalisés édités avec ce logiciel peuvent donc être invalides.

Pour éditer les fichiers personnalisés sous Windows, il est recommandé d'utiliser `Notepad++` à la place.

Lors de la personnalisation d'un script d'ouverture de session il peut être tentant d'utiliser un système d'élévation de pouvoir afin d'installer et paramétrer des applications. Le problème de cette élévation de pouvoir est qu'elle utilise un compte Windows local. En cas d'accès à un partage du serveur Scribe, la connexion se fait avec le compte de la machine (`sevenk64-1$`) et non avec le compte de l'élève (`eleve.test`) ou de l'enseignant (`enseignant.test`) qui se connecte.

Scripts personnalisés pour exécuter des commandes

Pour exécuter des commandes il faut utiliser l'instruction `cmd`.

Par défaut le programme d'ouverture de session affiche le programme et attend la fin de son exécution pour continuer. Un programme qui ne se ferme pas (ex. notepad.exe) provoquera des ouvertures de session très longue et incomplètes.

- l'option NOWAIT permet de ne pas attendre la fin de l'exécution du programme ;
- l'option HIDDEN permet de masquer la fenêtre.

Le format est :

cmd,commande,[options]

Exécuter *notepad.exe* pour l'utilisateur *user.assr* lorsqu'il ouvre une session sur un poste Windows XP :

Fichier *<scribe>**netlogon**scripts**os**WinXP**user.assr.txt* :

```
cmd,%WINDIR%\notepad.exe,NOWAIT
```

Scripts personnalisés pour monter des lecteurs

Pour monter des lecteurs il faut utiliser l'instruction `lecteur`.

Si la lettre spécifiée est déjà utilisée par une ressource réseau, celle-ci est déconnectée avant ré-utilisation de la lettre pour la nouvelle ressource. Dans le cas contraire (lecteur local, clé USB, CD-Rom, lecteur carte, etc.), la première lettre disponible est utilisée.

Le format est :

lecteur,lettre:,partage

Monter le partage *monserveur**partage* sur la lettre *V:* pour tous les utilisateurs du domaine :

Fichier *<scribe>**netlogon**scripts**groups**DomainUsers.txt* :

```
lecteur,V:,\\monserveur\partage
```

2.2. Les profils utilisateurs

Les profils utilisateurs représentent l'environnement par défaut des utilisateurs.

Il existe trois types de profils qui sont gérés par les modules EOLE :

- le **profil local** :

  il est stocké sur la station Windows, l'environnement est donc différent lorsque l'utilisateur change de poste.

- le **profil itinérant** :

  il est stocké dans le répertoire personnel de l'utilisateur, l'environnement suit l'utilisateur.

- le **profil obligatoire** :

  il est stocké dans un répertoire commun, l'environnement est le même pour tous **mais** il faut générer

les profils avant de pouvoir l'utiliser.

Il n'y a rien de particulier à faire pour les profils locaux ou itinérants par contre les profils obligatoires doivent être créés.

Pour plus d'informations concernant les profils d'utilisateurs, veuillez consulter la documentation officielle de Microsoft :

http://technet.microsoft.com/fr-fr/library/cc738303%28v=WS.10%29.aspx

Profils utilisateurs vs ESU

Il est important de distinguer les profils utilisateurs (notion interne à Windows) et ESU.

En effet les profils utilisateurs sont appliqués en premier et définissent un environnement de départ. La configuration ESU est appliquée après et modifie, ajoute ou supprime des paramètres de cet environnement.

Par exemple, le menu démarrer est contenu dans le profil de l'utilisateur mais si un chemin alternatif est défini dans ESU (Console ESU : `Windows => Dossiers`) alors, le menu démarrer utilisé sera celui défini dans ESU, et non celui du profil.

2.2.1. Création de profil obligatoire sous Windows XP

Introduction

Le profil obligatoire permet de stocker les paramètres utilisateur et les logiciels installés sur les postes clients. Il est téléchargé depuis le serveur à chaque ouverture de session et supprimé de la station à la fermeture de la session. Les utilisateurs repartent d'un environnement standard à chaque session.

Ces préconisations peuvent être adaptée suivant votre expérience et vos besoins.

Ajout d'un utilisateur spécifique

Il est conseillé d'utiliser un utilisateur fictif pour créer le profil obligatoire.

Cet utilisateur doit être configuré avec un **profil local** et être membre du groupe **DomainAdmins**.

C'est l'utilisateur spécifique **admin.profil** qui sera utilisé pour la suite.

Préparation de la station

Nettoyage de la station

Si des profils autre que locaux (exceptés les profils admin et admin.profil) sont déjà présents sur la machine, il est préférable de les supprimer.

Afin d'éviter des effets de bords, n'installer que les logiciels nécessaires à la génération du profil.

Il arrive que certains logiciels mal programmés paramètrent des valeurs qui provoquent une erreur lorsque le profil est appliqué sur une station où le logiciel n'est pas installé.

Installation des programmes à pré-paramétrer dans le profil obligatoire

Toutes les applications n'ont pas forcément besoin d'être paramétrées dans le profil obligatoire. Il peut arriver que certaines applications n'apprécient pas ce mode de fonctionnement. Il est nécessaire de faire des tests pour en déterminer la liste.

L'utilisation d'un logiciel de virtualisation (proposant l'enregistrement de l'état à un instant t) permet d'installer une version propre de Windows et de repartir du profil utilisé lors de la dernière copie.

Génération du profil

Pour générer un profil prêt à être copié il faut pré-paramétrer les applications, l'explorateur et le bureau :

- ouvrir une session avec l'utilisateur "*admin.profil*" sur un client XP ;
- utiliser les logiciels installés (LibreOffice, Firefox, Encyclopédies, etc.) ;
- supprimer le fond d'écran pour éviter sa diffusion sur les autres profils (paramètres Windows ou clic droit sur le bureau) ;
- fermer la session.

Le profil est prêt à être copié.

Les préférences de vue des fichiers

- ouvrir le poste de travail ;
- dans le menu `Affichage` ;
- sélectionnez `Détails` ;
- fermer la fenêtre

Lorsque les utilisateurs ouvriront le Poste de travail, les informations sur les fichiers seront affichées en "Détails".

La validation d'une licence

Par exemple le logiciel privateur Acrobat Reader demande, lors de son premier lancement, de valider sa licence.

Cette question est posée une fois par session à un utilisateur "profil obligatoire", la validation n'étant pas retenue lors de la fermeture de session.

Pour résoudre ce problème il faut valider la licence lors de la génération du profil avec *admin.profil.*

Ce type de comportement (validation, paramètres non retenus d'une session à l'autre) est généralement lié au profil obligatoire. Les informations sont enregistrées dans une partie du profil fourni par le profil obligatoire.

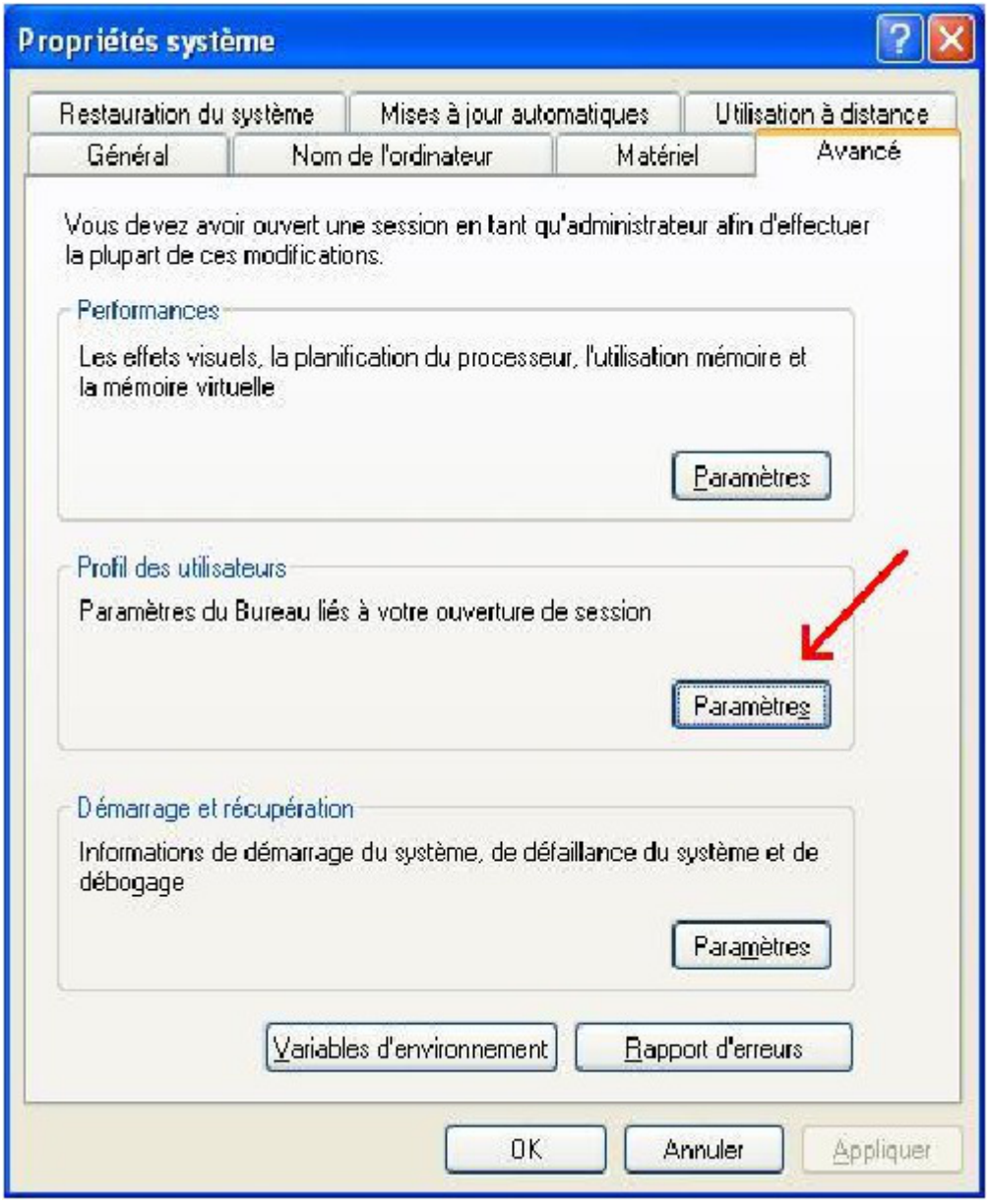
Ceci est à opposer aux informations stockées dans le répertoire `Applications Data` redirigé par défaut par ESU dans le répertoire `U:\.Config\Applications Data`.

Ces dernières informations sont donc retrouvées lors de la prochaine ouverture de session.

> Par exemple, LibreOffice enregistre la validation de sa licence une fois pour toutes.
>
> Le fond d'écran bénéficie d'une gestion particulière dans ESU :
>
> - la spécification d'un fichier image à afficher
> - l'ajout d'informations textuelles en haut à droite.
>
> Les deux étant incompatibles, il vaut mieux le désactiver pour éviter tout effet de bord. Pour se faire sélectionner `Aucun` dans `Propriétés de l'affichage/Bureau/Arrière-plan`.

Copie du profil

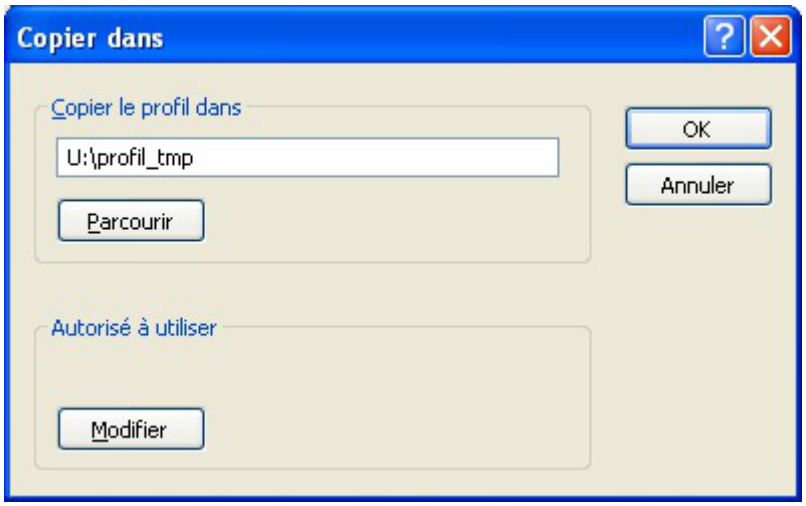
Ouvrir une session avec l'utilisateur `admin`. Aller dans le `Panneau de configuration` → `Système` → `Propriétés` → `Avancé`. Dans le cadre `Profil des utilisateurs` cliquer sur `Paramètres`.
Dans la nouvelle fenêtre, sélectionner le profil correspondant à l'utilisateur `admin.profil`.



Dans la partie `Autorisé à utiliser` cliquer sur `Modifier`. Entrer `tout le monde` puis cliquer sur `Vérifier les noms`.

Et cliquer sur `OK`.

Dans le champ `Copier le profil dans` indiquer un répertoire temporaire non existant ou vide (un sous répertoire du répertoire personnel de l'utilisateur `admin` par exemple) et cliquer sur `OK`.



Une fois le profil copié la dernière fenêtre se ferme automatiquement.

Copier ensuite le contenu du dossier dans : `\\<adresse_serveur>\netlogon\profil`

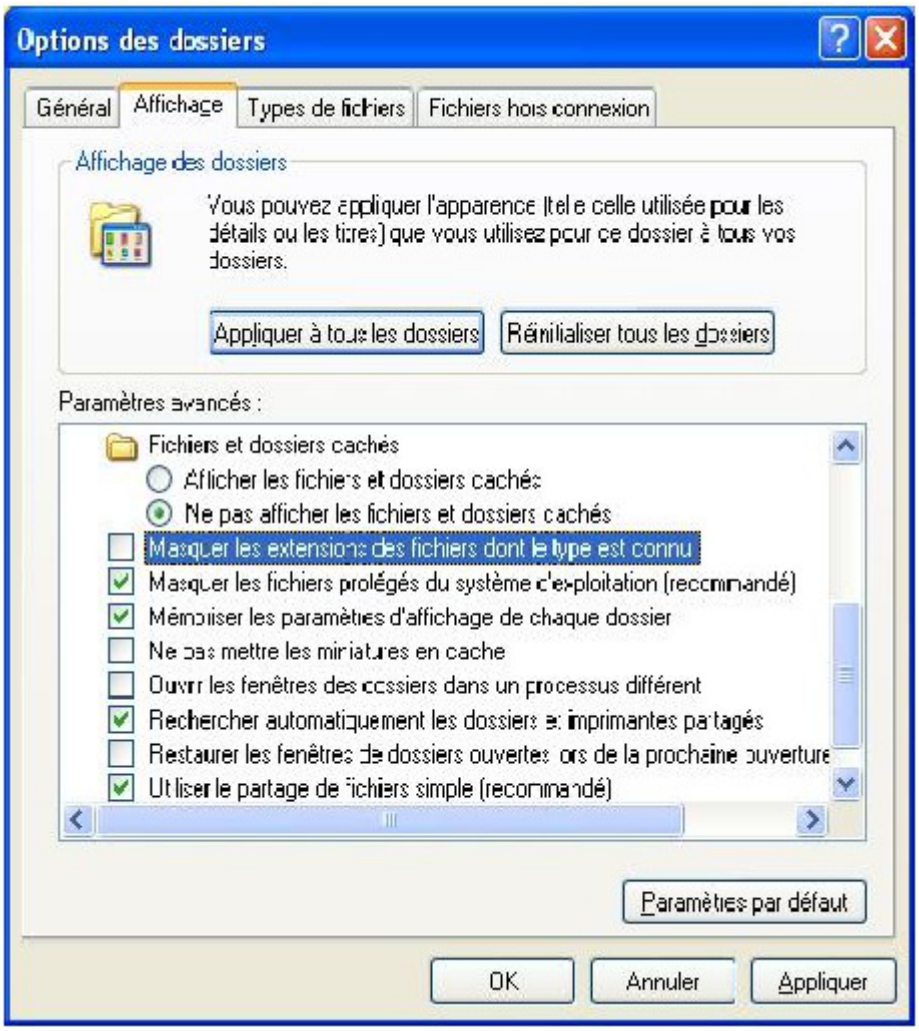
Sur le module Scribe, il est également possible d'utiliser le dossier `\\<adresse_serveur>\netlogon\profil2`

Ceci permet de spécifier un profil différent pour certains utilisateurs (ex. : profil pour les professeurs et profil2 pour les élèves).

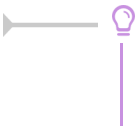
> Lorsque le profil est copié directement sur le serveur dans le répertoire `\\<adresse_serveur>\netlogon\profil\` , Windows applique automatiquement les droits d'écriture à tout le monde sur le dossier profil.
>
> Le passage par un répertoire temporaire évite d'avoir à manipuler les droits et diminue le risque d'erreur.

Dans le dossier `\\<adresse_serveur>\netlogon\profil\` renommer le fichier `ntuser.dat` en `ntuser.man` (ne pas confondre avec un éventuel fichier `ntuser.dat.txt`).

Pour y parvenir il faut d'abord afficher les extensions des fichiers connus (dans l'explorateur, "`Outils/Options des dossiers.../Affichage`", décocher "`☑ Masquer les extensions des fichiers dont le type est connu`").



Le profil obligatoire est désormais fonctionnel.



Si des difficultés sont rencontrées lors de la copie du profil sur le serveur, une solution consiste à renommer le dossier et à en créer un nouveau.

2.2.2. Création de profil obligatoire sous Windows 7

Pour générer un profil obligatoire sous Windows 7, la marche à suivre est à peu près la même que pour Windows XP :

1. créer un utilisateur `admin.profil` possédant un profil local ;
2. ouvrir une session avec `admin.profil` ;
3. paramétrer le profil et fermer la session ;
4. ouvrir une session avec `admin` pour copier le profil.

La subtilité se trouve ici, sous Windows 7 le bouton `Copier vers` est grisé pour les utilisateurs du domaine.

Une des solutions permettant de contourner le problème est d'utiliser un utilitaire nommé `Windows Enabler`.

- http://www.yamprod.net/index.php?tag/Windows%207%20Seven%20profil%20copy%20copie%20prc
- http://www.angelfire.com/falcon/speedload/Enabler.htm

Sous Windows 7 SP1, pour que `Windows Enabler` fonctionne, il faut impérativement désactiver l'UAC[p.143] et redémarrer la machine.

Comme pour Windows XP, il ne faut pas copier le profil directement vers `\\scribe\netlogon\profil.V2` mais plutôt passer par un dossier temporaire (exemple `U:\profil_seven`). Sans ça Windows va automatiquement placer des ACLs trop permissives sur le dossier `profil.V2` ce qui risque d'entraîner des dysfonctionnements.

Pour Windows Vista et Windows 7, le suffixe `.V2` est ajouté à la fin du chemin du profil.

A part ajouter cette extension au dossier dans lequel le profil est copié, il n'y a rien à paramétrer.

2.2.3. Les sessions locales

Si des chemins ont étés modifiés par ESU (`Groupe de machine` → `Windows` → `Dossiers`), à l'ouverture d'une session locale le programme `logon.exe` redéfinit les chemins d'accès aux icônes du *Menu démarrer* et du *Bureau* avec leurs valeurs par défaut.

En effet, les lecteurs réseaux peuvent être indisponibles lors de l'ouverture d'une session locale.

Sous Windows Vista et Windows 7 ce processus nécessite une élévation de droits au niveau de l'U[p.143]AC[p.143].

Le programme `logon.exe` affiche alors la question : `Ré-initialiser le Menu démarrer et le Bureau` ? suivit par celle de l'UAC[p.143] (si il est activé) pour la validation de l'action.

L'UAC[p.143] est un mécanisme censé protéger le système d'actions malencontreuses ou frauduleuses.

Lorsqu'un utilisateur, même *Administrateur*, effectue une action requérant des privilèges d'administrateur (lancement de `regedit.exe`, configuration du réseau, installation de nouveaux programmes, etc.), l'UAC bloque l'action et affiche une demande de confirmation pour l'exécution de l'action.

L'UAC n'est pas indispensable, il peut donc être désactivé.

2.3. Gestion des configurations clientes avec ESU

2.3.1. Introduction

Présentation

ESU[p.141] pour Environnement Sécurisé des Utilisateurs est une application de gestion avancée des postes clients.

Il permet de configurer le poste de travail à l'ouverture de session en fonction du nom de l'utilisateur ou des groupes dont il est membre et du nom de la machine cliente.

Les fonctionnalités principales d'ESU sont :

- paramétrage des restrictions sur le poste (par exemple : désactivation de la modification de l'heure, masquer des lecteurs dans le poste de travail, etc.) ;
- affichage d'un fond d'écran avec possibilité d'y inscrire des informations complémentaires ;
- installation d'imprimantes réseau (possibilité de coupler avec l'auto-installation des pilotes) ;
- paramétrage d'applications (par exemple : page de démarrage Firefox) ;
- redirection de dossiers vers un lecteur réseau (Ex. : Mes Documents, Bureau, Menu Démarrer) ;
- interdiction d'accès à un groupe de machines à certains utilisateurs.

Ces fonctionnalités sont représentées sous forme de règles dans le fichier de référence `\\<adresse_serveur>\esu\Console\ListeRegles.xml`

ESU est pleinement compatible Windows 98/Me/2k/2k3/XP/Vista.

Structure générale de l'outil

ESU se compose de deux parties :

- la console, qui sert à paramétrer l'ensemble des règles ;
- le client, qui applique les règles sur le poste.

Le dossier `\\<adresse_serveur>\esu\Console` contient la console, des modèles de groupes de machines et d'utilisateurs et l'éditeur de la liste de règles.

Le dossier `\\<adresse_serveur>\esu\Base` contient les paramètres définis dans la console ESU.

2.3.2. La console ESU

2.3.2.a. Présentation

La console ESU sert à paramétrer les règles qui seront appliquées sur les machines clientes lors de l'ouverture de session. La liste des règles disponibles est définie dans le fichier `\\<adresse_serveur>\esu\Console\ListeRegles.xml`. Elles sont réparties en deux groupes :

- les règles "machines" définissant le comportement global des machines, elles sont appliquées quelque soit l'utilisateur qui se connecte ;

- les règles "utilisateurs" définissant l'environnement de l'utilisateur comme les restrictions, le paramétrage de l'explorateur et du fond d'écran, etc.

Par défaut, seul l'utilisateur **admin** a accès à la console. Pour faciliter l'accès un raccourci est créé dans son répertoire personnel (U:).

La console est organisée en trois parties :

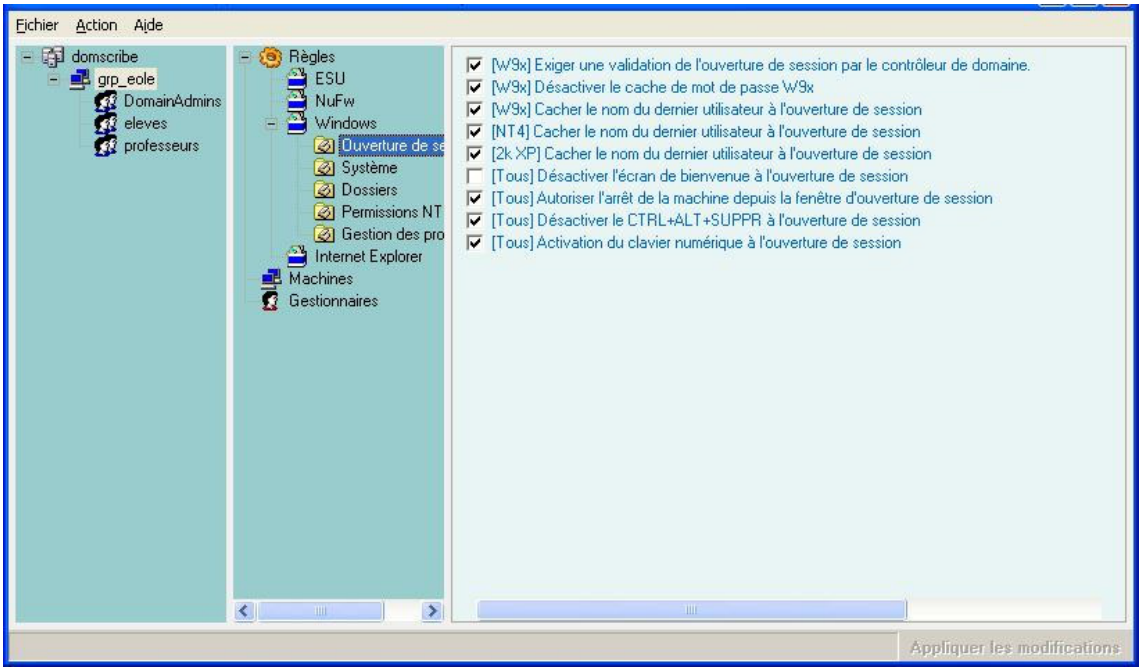
- la première liste les groupes de machines du domaine, et les utilisateurs/groupes gérés dans ce groupe de machines ;
- la seconde contient les différentes catégories de règles. Ces catégories peuvent comporter des sections ;
- la troisième partie affiche les règles et leur paramétrage.

La première colonne montre l'organisation générale d'ESU. La première ligne indique le nom du domaine.

Celui-ci contient un ensemble de groupes de machines définis en fonction du nom des machines. Chaque groupe de machine contient des utilisateurs ou des groupes d'utilisateurs.

Lors de l'ouverture de session, ESU va chercher à quel groupe de machines appartient la machine sur laquelle l'utilisateur se connecte. Si un groupe de machine est trouvé, ESU va chercher s'il contient l'utilisateur ou un des groupes auxquels l'utilisateur appartient.

La liste des groupes de machines et des utilisateurs est parcourue du haut vers le bas. Si une machine appartient à plusieurs groupes, le premier sera utilisé, les autres ignorés. Il en va de même pour les utilisateurs/groupes d'utilisateurs.



Fenêtre principale d'ESU

2.3.2.b. Les groupes de machines

Création d'un nouveau groupe de machines

Les groupes de machines servent à regrouper les machines dans une même configuration en fonction de leur nom.

A l'installation du module, ESU est pré-configuré avec un groupe de machines *grp_eole* paramétré afin de prendre en compte toutes les machines du domaine (Simplement le caractère "*").

Ce groupe de machines a été pré-créé afin de servir d'exemple et pour que l'installation du client Scribe soit suffisante pour obtenir une station pleinement fonctionnelle dès la première ouverture de session.

Pour créer votre propre groupe, faites un clic droit sur le *domaine* et sélectionnez "**Nouveau groupe de machines**" ou sélectionnez le domaine et utilisez le raccourci clavier `Ctrl+N`.

Renseignez le nom du groupe de machine (ici *technologie*) et paramétrez les noms des machines à ajouter au groupe.

Ajout des noms de machines appartenant au groupe

Par défaut les nouveaux groupes de machines sont créés en utilisant le modèle ESU `U:\esu\Console\Modeles\GM\GroupeMachine_[Scribe].xml`.

Ce modèle ajoute automatiquement les groupes *DomainAdmins*, *eleves* et *professeurs* avec un ensemble de règles pré-configurées (dossier redirigés, restrictions, etc.).

Il est possible de prendre en compte plusieurs machines en une fois en utilisant le caractère étoile, exemple : "techno*".

Utilisation du jocker (*) pour paramétrer les noms de machines prises en compte par le groupe

Une fois le groupe de machines créé, il faut établir sa priorité par rapport au groupe de machine *grp_eole* (si il n'a pas été supprimé) : clic droit sur le groupe de machine et choisir "**Augmenter la priorité**".

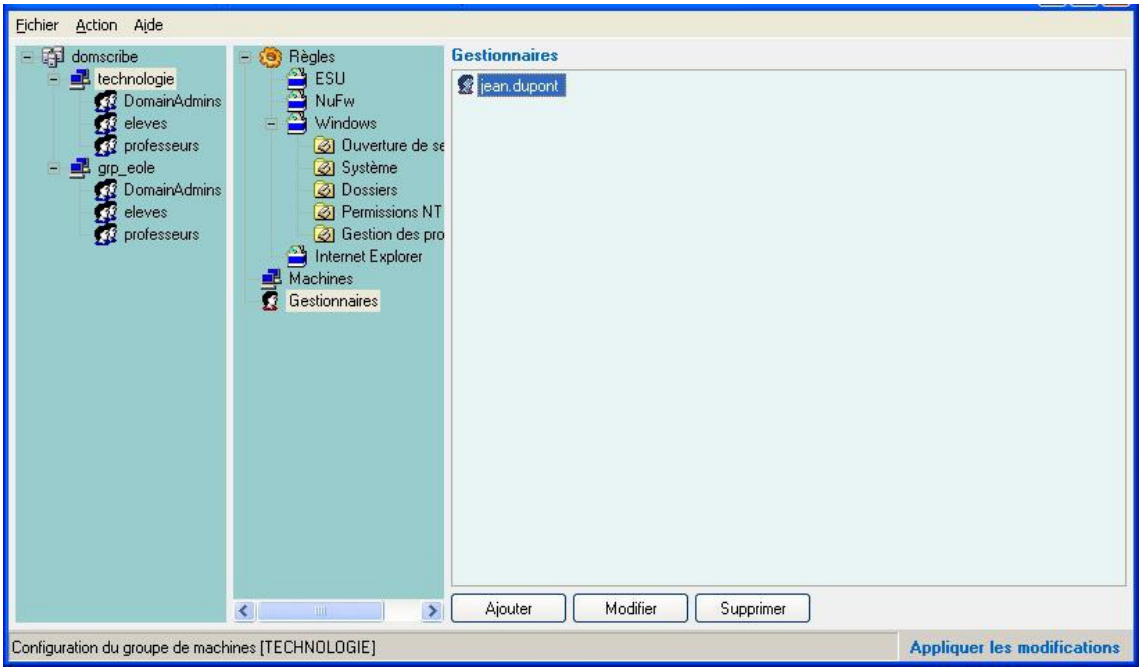
Augmenter la priorité d'un utilisateur

Les Gestionnaires

L'item "**Gestionnaires**" permet de déléguer l'administration d'un ou plusieurs groupes de machines à un autre utilisateur ou à un autre groupe. Lorsqu'un utilisateur lance la console, il n'a accès qu'aux groupes

de machines pour lesquels il est défini comme gestionnaire.

Le gestionnaire peut modifier la configuration ESU de son groupe de machines et a aussi accès en écriture au répertoire contenant les icônes (`I:\<nom_du_groupe_de_machines>\`).



Ajout de gestionnaires dans un groupe de machines

Il est également possible d'ajouter un gestionnaire au niveau du domaine. Il aura le droit d'administrer l'ensemble des groupes de machines définis dans ESU et d'en ajouter

Lorsqu'un utilisateur est gestionnaire ESU il est automatiquement inscrit au groupe `Administrateurs` de la ou des machines Windows concernées.

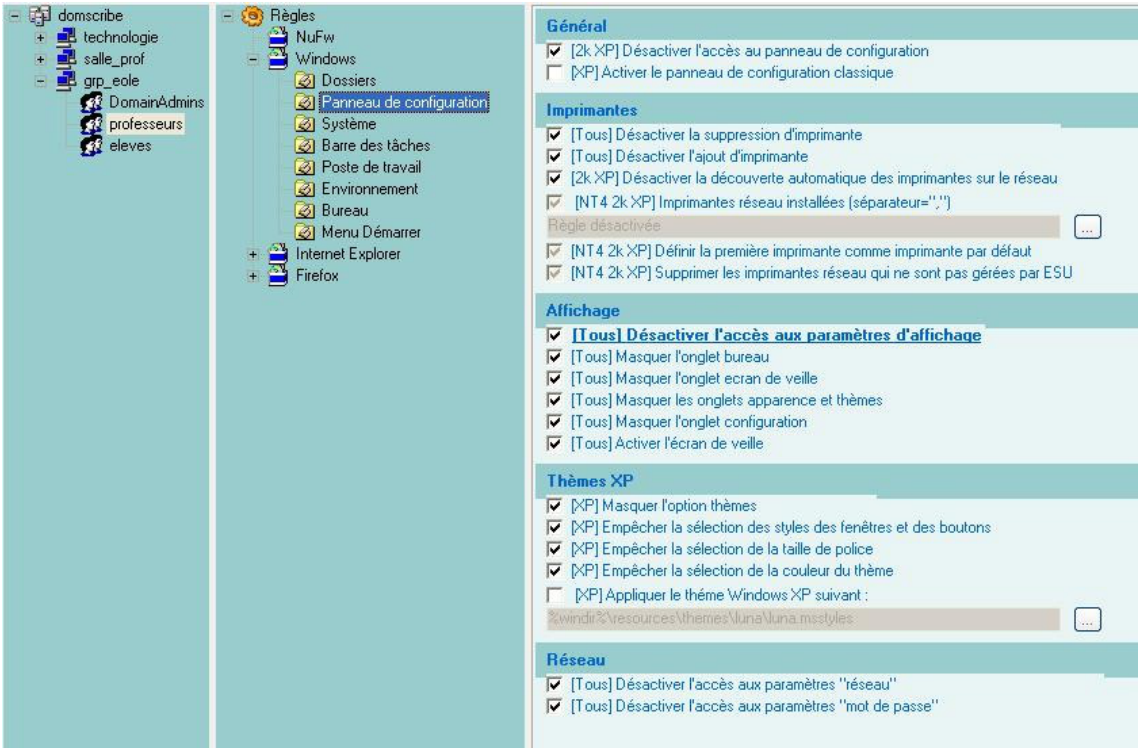
Le groupe DomainAdmins

Les membres du groupes DomainAdmins ont un accès complet à la console Esu sans qu'il ne soit nécessaire de les ajouter comme gestionnaires.

D'une manière générale, les membres du groupe DomainAdmins ont les droits d'écriture (donc de suppression) sur l'ensemble des partages du serveur (partages groupe, dossiers personnels, Esu, etc.).

2.3.2.c. Les utilisateurs et groupes d'utilisateurs

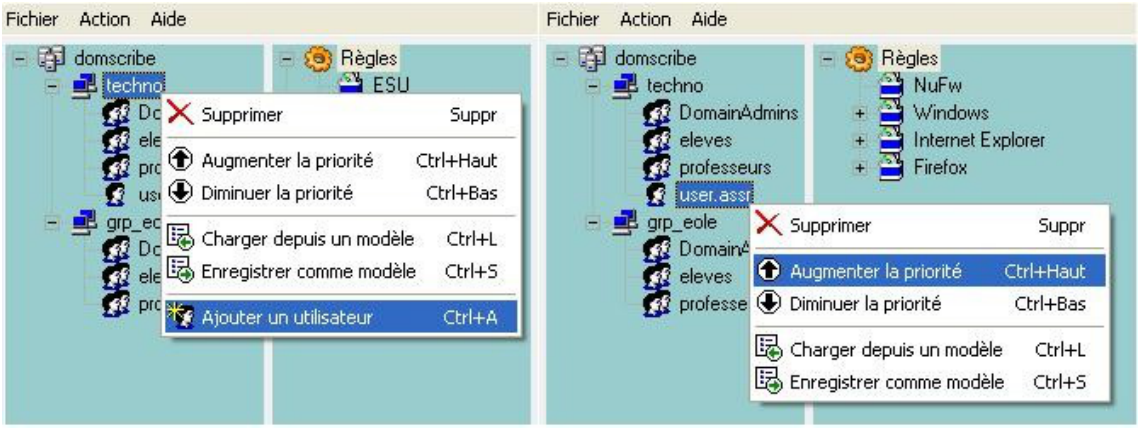
Un environnement différent peut être appliqué en fonction du nom de l'utilisateur ou des groupes auxquels il appartient.



Exemple de paramétrage de règles pour un utilisateur ou un groupe d'utilisateurs

Création d'un nouveau groupe d'utilisateurs dans un groupe de machines.

Un clic droit sur le nom du groupe de machine permet d'ajouter un utilisateur ou un groupe. Un clic droit sur l'utilisateur ou le groupe permet de le supprimer ou de régler sa priorité.



Ajouter un utilisateur ou un groupe d'utilisateurs

Comme pour les groupes de machines, les utilisateurs et groupes sont parcourus de haut en bas. ESU s'arrête à la première correspondance.

Ici, l'utilisateur *user.assr* fait partie du groupe *eleves*. Pour lui appliquer une configuration spécifique, il faut lui affecter une priorité supérieure à celle du groupe *eleves*.

Augmenter la priorité d'un utilisateur

2.3.2.d. Les imprimantes

Ceci ne concerne pas les postes Windows Me et inférieur et nécessite l'utilisation de ESU.

Dans la partie règle utilisateurs, que l'on obtient en cliquant sur un groupe d'utilisateurs dans la colonne de gauche, sélectionner "*Panneau de Configuration*" section "*Imprimantes*".

A cet endroit vous pouvez spécifier le chemin UNC (\\<scribe>\<imprimante>) d'accès aux imprimantes disponibles pour ce groupe de machine et ce groupe d'utilisateur.

Ainsi élèves et professeurs peuvent avoir des imprimantes différentes sur un même poste et un utilisateur peut avoir des imprimantes différentes en fonction du poste et du groupe de machines auquel il appartient.

2.3.2.e. Le proxy

Depuis la version EOLE 2.3, la configuration du proxy ESU s'effectue dans l'interface de configuration du module.

Voir aussi...

Onglet Esu : Configuration du proxy ESU

2.3.2.f. Trucs et astuces

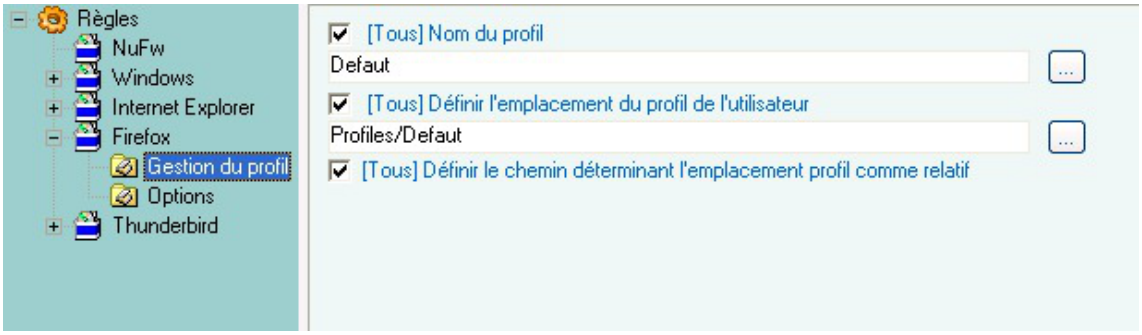
Les dossiers d'icônes

- les icônes placées dans `R:\grp_eole\_Machine\Bureau` seront visibles par tous les utilisateurs ;
- les icônes placées dans `R:\grp_eole\professeurs\Bureau` ne seront visibles que par les professeurs.

Attention, l'utilisateur *admin* fait partie du groupe *professeurs* mais, il est également membre du groupe *DomainAdmins*. Au vu des priorités, c'est le dossier défini d'icônes du groupe *DomainAdmins* (`R:\grp_eole\professeurs\Bureau`) qui lui sera proposé.

Firefox

Afin de paramétrer correctement la *Gestion du profil* Firefox avec ESU, il faut sélectionner au moins une *Option*, la page de démarrage par exemple.



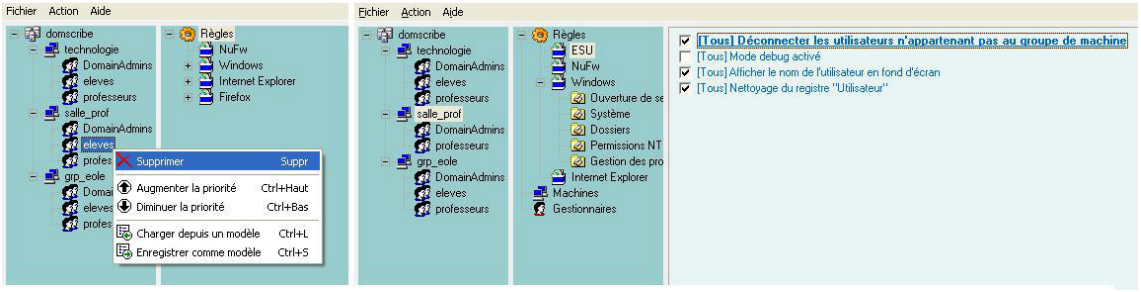
Configuration ESU du profil Firefox

Configuration ESU des options Firefox

Accès limité à un poste en fonction de l'utilisateur

Pour limiter l'accès à un poste, il suffit de ne configurer que les groupes d'utilisateurs autorisés et de cocher *Déconnecter les utilisateurs n'appartenant pas au groupe de machines*.

Ici les utilisateurs ne faisant pas partie des groupes *DomainAdmins* ou *professeurs* (par exemple les élèves) seront déconnectés automatiquement.



Limiter l'accès à un poste

Modèles de restrictions

Des modèles pré-configurés sont livrés avec ESU :

Pour les groupes de machines

- `U:\esu\Console\Modeles\GM\GroupeMachine_[Scribe].xml`

Ce modèle est utilisé par défaut lors de la création d'un groupe de machines.

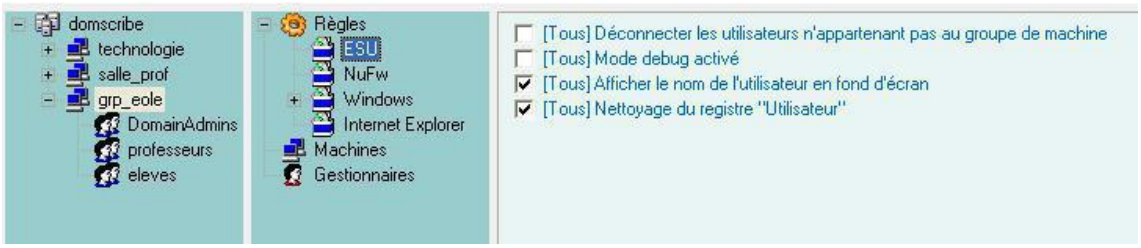
Pour les groupes d'utilisateurs

- `U:\esu\Console\Modeles\GU\GroupeUtilisateur_DomainAdmins[Scribe].xml`
- `U:\esu\Console\Modeles\GU\GroupeUtilisateur_eleves[Scribe].xml`
- `U:\esu\Console\Modeles\GU\GroupeUtilisateur_professeurs[Scribe].xml`

Ces modèles peuvent être utilisés lors de l'ajout d'un utilisateur ou d'un groupe dans un groupe de machines (ex. *user.assr*).

2.3.3. Personnalisation du fond d'écran

Il est possible de modifier le contenu du texte à afficher sur le fond d'écran lorsque l'option *Afficher le nom de l'utilisateur en fond d'écran* est cochée dans la Console ESU.



La personnalisation se fait par utilisateur/groupe d'utilisateurs à l'aide d'un fichier texte ayant l'extension **.bgd**. Ce fichier doit se trouver dans *U:\esu\Base***<groupe_de_machine>******<utilisateur_ou_groupe>** *.bgd*.

Pour modifier le texte du fond d'écran pour les membres du groupe *DomainAdmins* dans le groupe de machine *grp_eole*, créez le fichier **U:\esu\Base\grp_eole\DomainAdmins.bgd**.

Ce fichier peut contenir des variables suivantes :

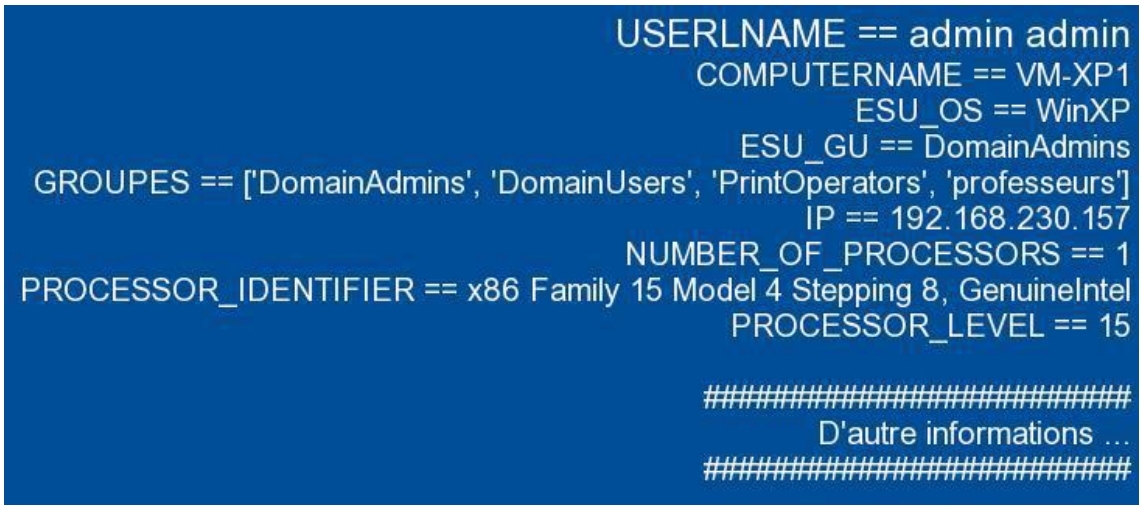
- Toutes les variables d'environnement Windows (%WINDIR%, %PATH%, ...)
- %ESU_PROXY_HOST%
- %ESU_PROXY_PORT%
- %ESU_PROXY_BYPASS%
- %ESU_PDC%
- %ESU_DOMAINE%
- %ESU_OS%
- %ESU_PARTAGE_ICONES%
- %ESU_LECTEUR_ICONES%
- %ESU_GU%#%ESU_GM%
- %USERNAME%
- %USERLNAME%
- %GROUPES%
- %SID%
- %IP%

Exemple de configuration personnalisée du texte en fond d'écran

Contenu du fichier :

USERLNAME == %USERLNAME%
COMPUTERNAME == %COMPUTERNAME%
ESU_OS == %ESU_OS%
ESU_GU == %ESU_GU%
GROUPES == %GROUPES%
IP == %IP%
NUMBER_OF_PROCESSORS == %NUMBER_OF_PROCESSORS%
PROCESSOR_IDENTIFIER == %PROCESSOR_IDENTIFIER%
PROCESSOR_LEVEL == %PROCESSOR_LEVEL%
##########################

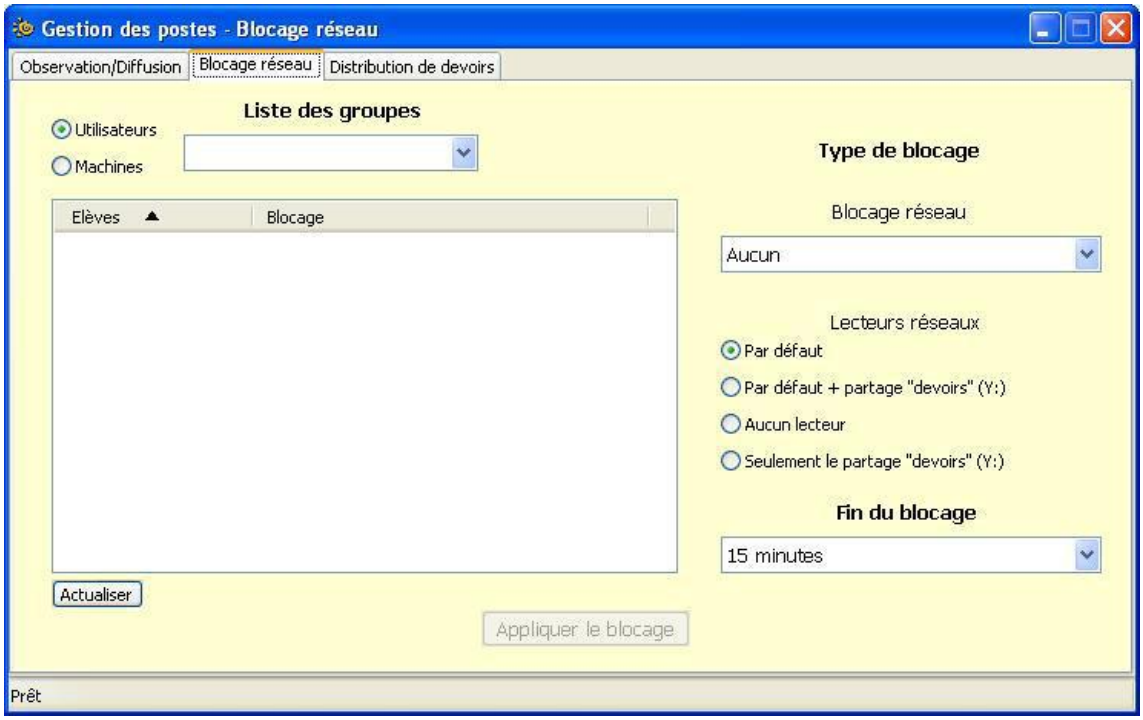
D'autre informations ...
##########################
Résultat :



Si l'utilisateur possède un profil local et que l'option ESU `GroupeMachine > GroupeUsers > Windows > Bureau > Papier peint > Chemin vers l'image appliquée en fond d'écran` est grisée, le texte par défaut et le texte personnalisé se superposent.

2.4. L'application Gestion-postes

Gestion-postes est une application pour le système d'exploitation Microsoft Windows, accessible uniquement par les enseignants (`P:\Gestion-postes`) qui permet diverses opérations sur une sélection de postes ou d'utilisateurs.



L'application propose trois outils accessibles via trois onglets :

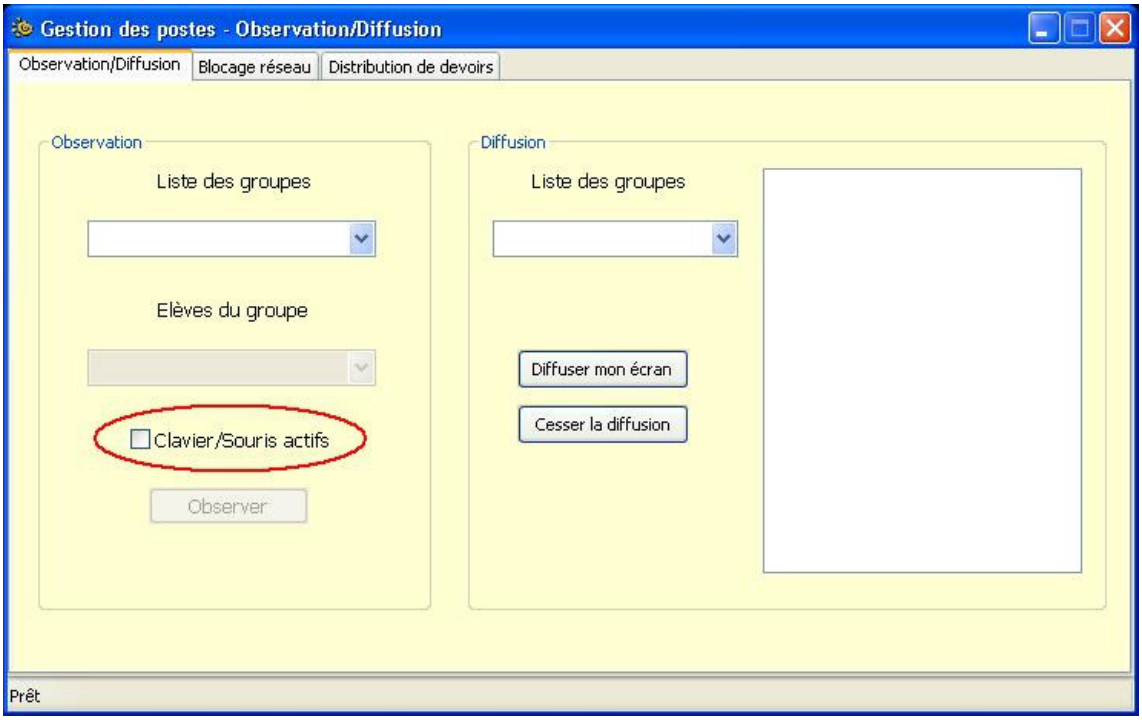
- le premier onglet sert à l'observation et la diffusion d'un poste. Il n'est possible d'observer que des élèves, en revanche un professeur peut diffuser son poste sur celui d'un autre professeur. Il est bien entendu indispensable que l'observateur et l'observé soient tous les deux connectés ;
- le second onglet contient le "*mode devoir*" : blocage de l'accès aux partages et/ou à Internet pour des élèves. Il **n**'est **pas** indispensable que les élèves à bloquer soient connectés. Le blocage s'appliquera dès leur ouverture de session ;
- le troisième onglet permet de distribuer des documents. Ces documents peuvent être distribués à tous les groupes (niveau, classe, équipe pédagogique, matière, groupe...) et peuvent être accompagnés de données en lecture seule qui ont l'avantage de ne pas être dupliquées sur le serveur.

Il n'existe pas d'équivalent pour des clients GNU Linux. Par contre, l'application EOP est accessible au travers d'un navigateur web.

2.4.1. Observation / Diffusion du poste

Observation

L'observation consiste à afficher le poste d'un élève dans une fenêtre sur le poste du professeur. La sélection d'un élève à observer se fait par classe ou par groupe, seuls les élèves connectés sont listés.



Observation, activation de la prise en main du poste (clavier et souris de l'observateur actifs)

La liste des élèves connectés affiche l'identifiant de l'élève et le nom de la machine sur laquelle il est connecté.

Une fois l'élève sélectionné, cliquer sur Observer. La requête est transmise au serveur et à la station de l'élève ce qui peut prendre quelques instants.

L'application permet d'observer plusieurs élèves en même temps, cependant le nombre dépend de la qualité et de la vitesse du réseau.

Le niveau d'observation VNC[p.143] est paramétrable dans l'EAD : Outil / VNC.

Trois niveaux d'observation :

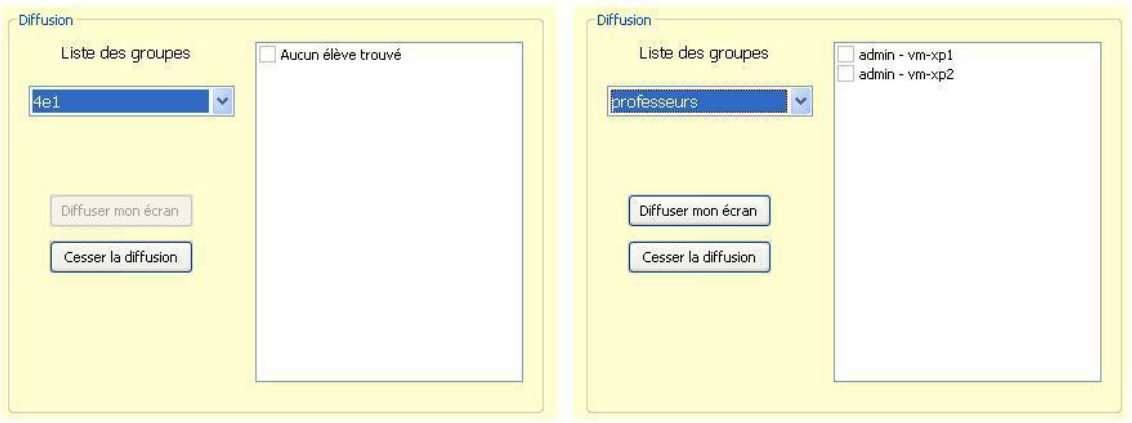
- Désactivé ;
- Visualisation simple ;
- Visualisation et contrôle.

En mode *Visualisation et contrôle*, l'utilisateur pourra choisir via la coche *Clavier/Souris actifs* s'il veut pouvoir prendre la main sur la station élève.

Une ré-ouverture de session sur le poste client est nécessaire afin de prendre le changement du mode de contrôle de VNC en compte.

Diffusion

La diffusion est l'affichage du poste du professeur sur un ou plusieurs postes élève et/ou professeur. La sélection se fait par classe, par groupe ou par membre du groupe *professeurs*. Comme pour l'observation, seuls les utilisateurs connectés sont listés.



Le bouton Cesser la diffusion arrête la diffusion immédiatement sur tous les postes.

Toute nouvelle diffusion (nouveau clic sur le bouton Diffuser mon écran) **interrompra** la diffusion précédente.

La qualité du réseau influe directement sur le nombre maximum de diffusions simultanées possibles.

2.4.2. Bloquer Internet / Masquer les partages (Mode devoir)

Les professeurs peuvent restreindre l'accès à Internet et/ou aux partages ainsi que monter le partage *devoir* pendant une période donnée.

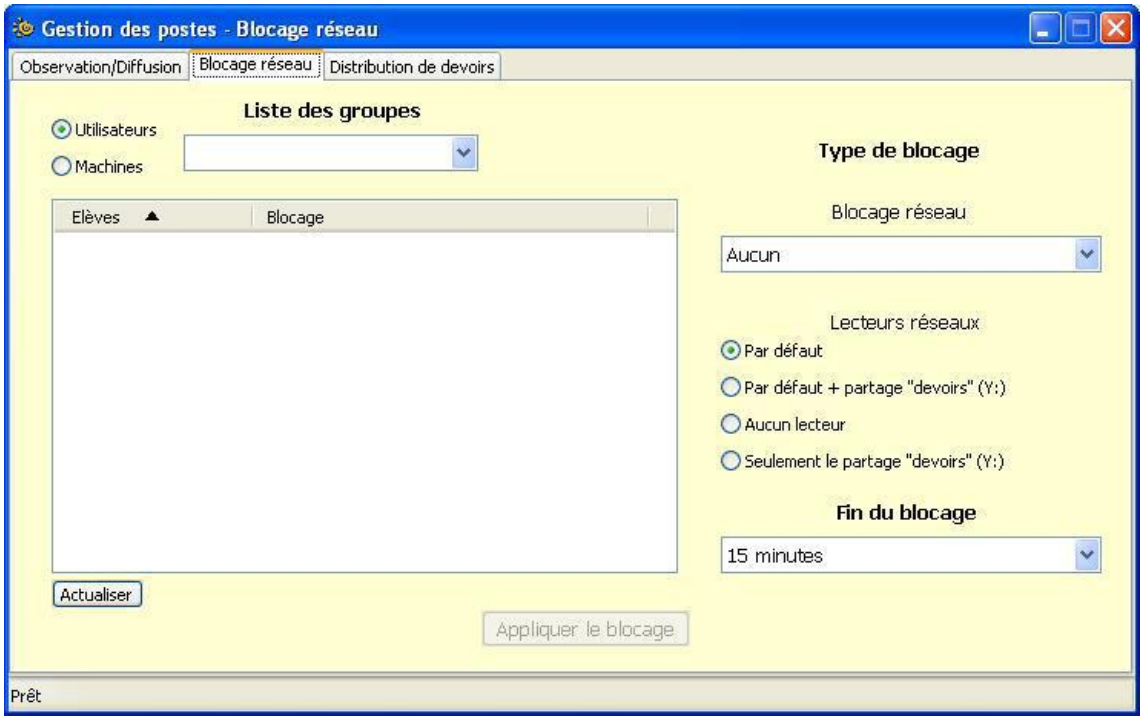
Ces restrictions sont appliquées immédiatement si l'élève est connecté, sinon elles sont appliquées à l'ouverture de session.

Lorsque la période d'interdiction est écoulée l'environnement de l'élève est automatiquement remis en mode normal s'il est encore connecté.

Blocage Internet

La sélection du blocage Internet se fait via la liste déroulante `Type de blocage`.

Le blocage Internet interdit tous les accès réseau en dehors des services DNS, VNC et du service Samba (ports 137-139 et 445) à destination du module Scribe. Cela afin de permettre l'ouverture d'une session sur le domaine et d'accéder aux partages. Aucun accès à internet, direct ou par proxy, n'est possible.



Le blocage réseau peut s'appliquer à un utilisateur ou à une machine.

Il est possible de sélectionner plusieurs utilisateurs en même temps en gardant la touche Maj ou Ctrl enfoncée.

Masquer les lecteurs réseaux

En plus du blocage de l'accès à Internet, l'application permet de masquer les lecteurs réseau spécifiques au module Scribe pour une durée donnée afin que l'élève n'ait plus accès à son dossier personnel ni aux dossiers groupes et dossiers communs (choix `Aucun lecteur réseau`).

Les documents sont distribués dans le dossier "devoirs" situé sur le serveur. Il est accessible en chemin UNC [p.143] par \\<adresse_du_serveur>\<login_utilisateur>\devoirs

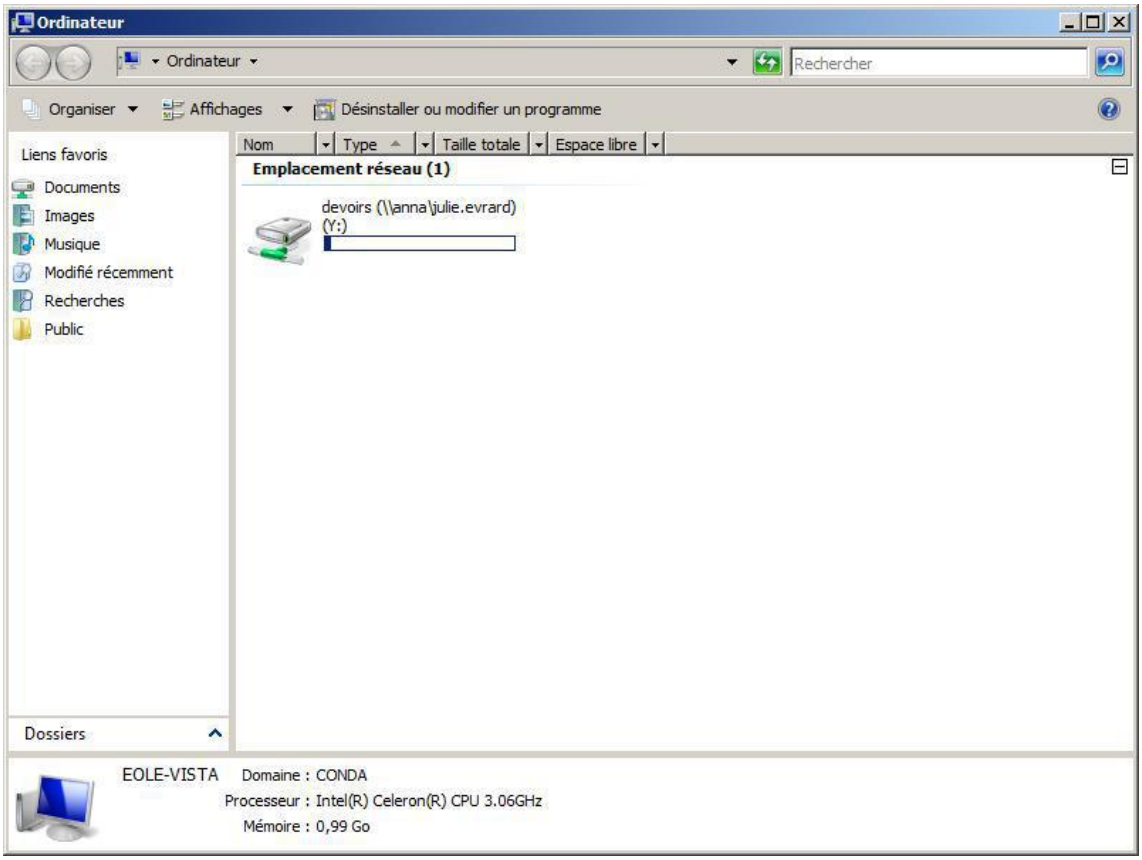
L'application propose de monter ce dossier comme nouveau lecteur nommé `Y:`

Sélectionner le bouton radio `Seulement le partage "devoirs"` masquera tous les lecteurs puis connectera le dossier "devoirs" de l'utilisateur au lecteur Y: dans le poste de travail.

Associé au blocage réseau, ce choix permet d'isoler l'utilisateur et l'empêche de diffuser ou de récupérer le ou les documents. Aucun utilisateur ne peut donc prendre connaissance des documents à l'avance.

Pour masquer tous les lecteurs et connecter le dossier "devoirs" de l'utilisateur au lecteur Y: il faut sélectionner le bouton radio `Seulement le partage "devoirs"`.

Associé au blocage réseau, ce choix permet d'isoler l'utilisateur. Cela l'empêchera de récupérer et de diffuser le devoir vers d'autres utilisateurs.



Comme pour le blocage de l'accès Internet, le masquage des partages a une durée limitée. À la fin de cette période, si l'élève est encore connecté sur un client, il retrouvera son environnement initial automatiquement.

Gestion-postes offre la possibilité de spécifier une liste de lecteurs à afficher même si l'un des choix `Aucun lecteur` ou `Seulement le partage "devoirs"` a été fait. Pour ce faire il faut placer un fichier nommé `lecteurs.txt` dans `P:\gestion-postes\`

Le fichier doit contenir une liste de lettres de lecteur à afficher sans les deux points ":" et séparées par des virgules ",".

Exemple de contenu du fichier `lecteurs.txt` :

```
c,d,s
```

2.4.3. Distribution de devoirs

La distribution peut être composée de deux éléments :

- le ou les documents sous forme d'un ou plusieurs fichiers. Ils seront copiés dans chacun des dossiers personnels `devoirs`/ `nom_de_l'enseignant` / `<nom_du_devoir>` des utilisateurs du groupe sélectionné. Les utilisateurs auront un accès en lecture et en écriture à ces fichiers (modification/suppression) ;
- les données jointes au(x) document(s) qui sont des fichiers supplémentaires dont la modification est impossible. Ils sont copiés une seule fois à un endroit spécifique du serveur. Des liens symbolique vers ces fichiers sont créés dans le sous-répertoire `donnees` du répertoire `devoirs`/ `nom_de_l'enseignant` / `nom_devoir` de chacun des utilisateurs.

Si la distribution de document est un travail éducatif, la distribution s'effectue en suivant les 4 étapes suivantes :

- distribuer ;
- ramasser ;
- rendre : distribution des devoirs corrigés ;
- supprimer : effacement des fichiers du devoir.

Distribuer

La distribution de document commence par la sélection d'un ou plusieurs fichiers dans `Devoir à distribuer`. L'ajout de fichiers dans `Donnée` est facultatif, ces fichiers supplémentaires accompagneront le devoir mais leur modification sera impossible.

Il faut nommer le devoir dans le champ `Nom du devoir` , c'est sous ce nom qu'il apparaîtra pour l'utilisateur et pour le gérer (ramassage).

Ensuite il faut sélectionner le groupe auquel le devoir doit être distribué. Tous les groupes sont présents dans la liste, y compris les groupes incluant des utilisateurs *professeurs*.

La case `Uniquement aux élèves du groupe` est cochée par défaut. Décochée, elle permet d'envoyer les documents aux autres membres du groupe, comme par exemple aux enseignants.

Par défaut, l'option `Dans le dossier 'perso\devoirs'` étant sélectionnée, les documents seront distribués dans le répertoire personnel des utilisateurs.

L'option `Dans le partage 'devoirs' (non accessible par défaut)` permet de préparer la distribution différée de documents. Ce travail de préparation peut donc se faire aussi bien à l'extérieur qu'à l'intérieur de l'établissement. La distribution ne sera effective qu'au travers du logiciel `Gestion-postes`.

Cliquer sur `Distribuer`, une boite de dialogue affiche le nombre de devoirs prêts à être distribués et demande confirmation.

Lorsque la distribution est terminée, un message affiche le nombre de documents effectivement distribués et le nom du répertoire de stockage. Ce nom est automatiquement associé au devoir, il correspond à <identifiant_du_distributeur>-<numéro_devoir>. Ce sous-dossier est présent dans le répertoire "devoirs" de l'utilisateur. Il contient l'ensemble des documents et des liens vers les données.

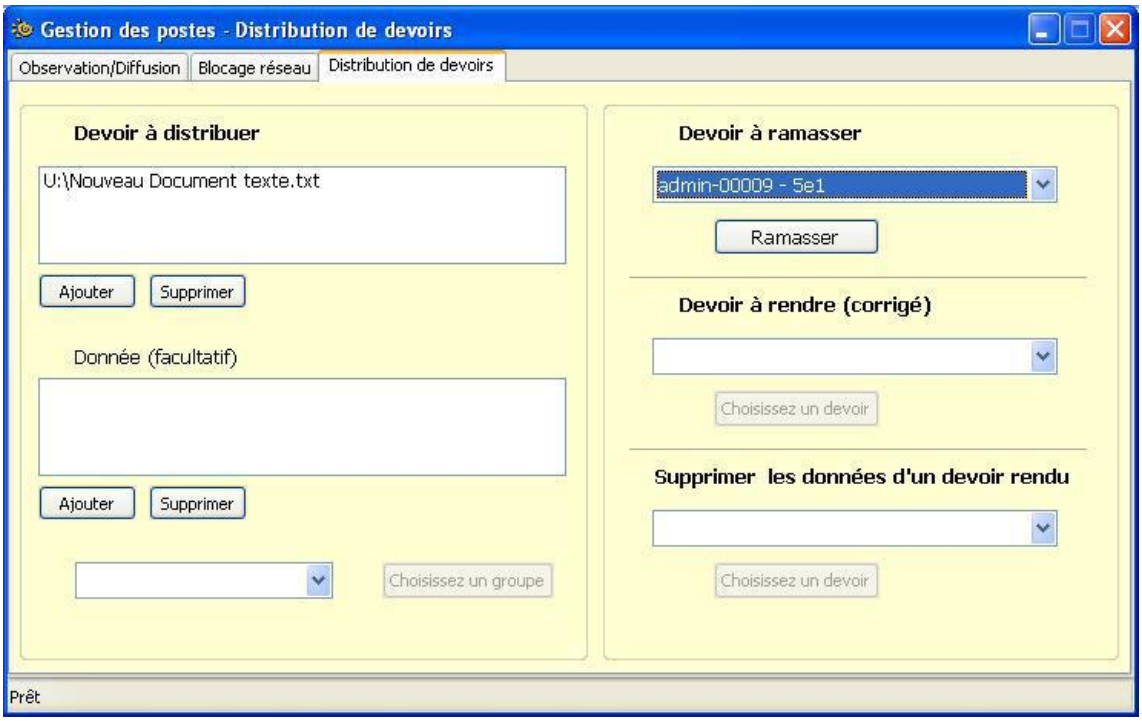
L'opération peut prendre du temps dans le cas de fichiers volumineux et de nombreux membres dans le groupe cible.

Veillez à ne pas fermer l'application pendant la distribution.

N'étant copiées qu'une fois puis liées dans les dossiers "devoirs", les données ont l'avantage d'économiser de l'espace disque sur le serveur.

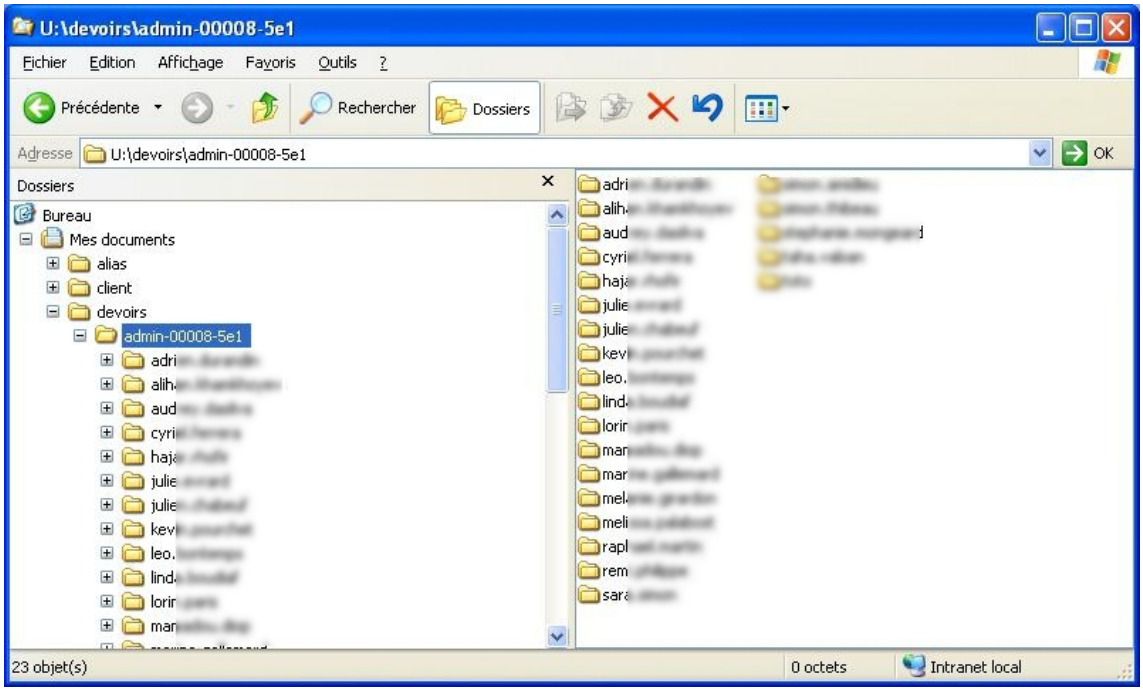
Ramasser

Sélectionner le devoir à ramasser. Dans la liste déroulante, le nom du groupe auquel a été distribué le devoir est affiché à côté du nom du devoir.



À la fin du ramassage, un message rend compte de l'opération. Si un élève a supprimé le dossier du devoir, celui-ci ne pourra pas être ramassé, un répertoire du nom de l'élève sera quand même créé mais sera vide.

L'action ramassage des devoirs effectue une copie des fichiers du devoir (sans les données) dans le répertoire "devoirs" du dossier personnel de celui qui exécute le ramassage et prend la forme `U:\devoirs\<nom_devoir>-<groupe_cible>\<identifiant_de_l'élève>\`



Lors du ramassage d'un devoir, tous les fichiers et dossiers contenus dans `U:\devoirs\<nom_devoir>\` (sauf le répertoire `donnees`) sont recopiés. Il est donc possible de donner comme devoir la création d'un nouveau fichier.

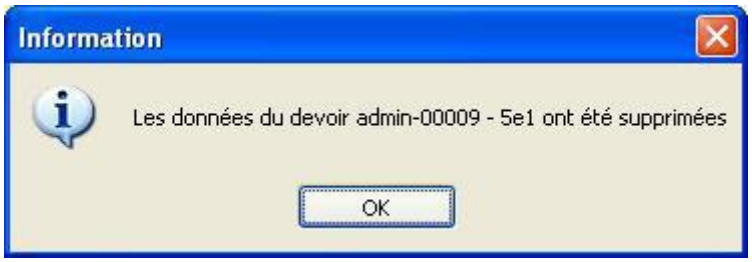
Rendre les copies corrigées

Tout comme sur une version papier, la correction peut s'effectuer sur la copie en éditant directement le fichier mais elle peut aussi bien se faire sous forme d'ajout de fichier. En effet, c'est tout le dossier qui sera copié dans le répertoire personnel de l'élève lors de la restitution de la correction. La restitution se fait dans le répertoire personnel des utilisateurs à savoir `U:\devoirs\<nom_devoir>\correction\`

Une boîte de dialogue informe du résultat de l'opération.

Suppression des données

Lorsqu'un enseignant distribue des données en plus des documents, elles sont copiées dans `U:\devoirs\.distribues` et des liens vers ces fichiers sont ensuite créés dans le répertoire `nom_du_devoir` \ `donnes` de chacun des destinataires.
Il est possible de supprimer ces fichiers lorsqu'ils sont devenus inutiles.



- La suppression des données entraînera également la suppression du dossier `<nom_du_devoir>` \ `donnees` dans le dossier des destinataires.
- Cette fonctionnalité permet de supprimer les données liées à une distribution de document qui ne seraient plus utiles par la suite. Elle permet donc d'économiser de la place sur le serveur de stockage.

2.5. Administration avancée des clients Scribe

2.5.1. Contrôle à distance d'un poste

Exécution de commandes à distance sur le poste

Il est possible de dialoguer avec le service Scribe installé sur les postes clients avec l'utilitaire `cliscribe.py` :
La syntaxe de la commande est :

```
# /usr/share/eole/controlevnc/cliscribe.py <IP_POSTE_CLIENT> <OPTION> <ARGUMENTS>
```

L'option `-h` permet d'avoir de l'aide sur la commande :

```
# /usr/share/eole/controlevnc/cliscribe.py -h
```

La liste des options est :

- -k ou --killproc <NOM_DU_PROGRAMME>
  termine un programme en cours d'exécution, "explorer.exe" par exemple
- -s ou --shutdown <NIVEAU>
  permet d'éteindre le poste : 0 = éteindre (défaut), 1 = reboot, 2 = fermeture de session
- -e ou --execute <NOM_DU_PROGRAMME>

exécute un programme dans l'environnement du service (BUILTIN\SYSTEM)

- -eu ou --executeuser <NOM_DU_PROGRAMME>

  exécute un programme dans l'environnement de l'utilisateur connecté s'il y en a un, sinon renvoie une erreur

  (un utilisateur doit avoir une session ouverte)

- -vc ou --vncconnect <IP_VIEWER_LISTEN>

  exécute la commande `winvnc -connect <IP_VIEWER_LISTEN>` (vncviewer doit être en mode "listen" sur le poste <IP_VIEWER_LISTEN>)

- -va <ÉTAT> ou --vncactive <ÉTAT>

  permet de démarrer ou d'arrêter winvnc sur le client :

  0 = arrête winvnc sur IP_CLIENT, 1 = démarre winvnc sur IP_CLIENT

- -vi <ÉTAT> ou --vncinputs <ÉTAT>

  permet d'activer, désactiver le clavier et la souris pour winvnc sur le client :

  0 = désactive le clavier/souris pour winvnc, 1 = active le clavier/souris pour winvnc

- -f <FW_ACTION> ou --firewall <FW_ACTION>

  permet de gérer le pare-feu sur le client : activation, désactivation, initialisation, ajout de règles, suppression de règles, modification de la politique par défaut

  <FW_ACTION> doit ressembler à `INIT|ADD::rule|DEL::Nom|SETMODE::<in>;;<out>|ACTIVATE::True|False` :

  - INIT initialise les règles de bases (fait une simple initialisation, ne lit pas le fichier `liste_fwregles.eol`)
  - ADD::rule

    Exemple : ADD::'Nom;; ip_src=XX;;ip_dst=XX;;action=XX;;proto=XX;;port_dst=XX;;program=XX'

    - ip_src/dst = me|any|<ip>
    - action=allow|block
    - proto=tcp|udp|icmp|any
  - DEL::Nom
  - SETMODE::<in>;;<out>
  - ACTIVATE::True|False

Terminer un programme en cours d'exécution

```
# /usr/share/eole/controlevnc/cliscribe.py 172.16.0.45 --killproc firefox.exe
```

Exécuter un programme dans l'environnement du service

```
# /usr/share/eole/controlevnc/cliscribe.py 172.16.0.45 --execute '\\scribe\wpkg\wpkg_client_install.bat'
```

(noter les simple quotes ou apostrophes autour de la commande à exécuter)

Initialiser les règles de bases du pare-feu

```
# /usr/share/eole/controlevnc/cliscribe.py 172.16.0.45 --firewall
```

```
INIT
```

Bloquer l'accès au port TCP 123 par la machine 1.2.3.4 vers la machine 172.16.0.45

```
# /usr/share/eole/controlevnc/cliscribe.py 172.16.0.45 --firewall
'ADD::maregle;;ip_src=1.2.3.4;;ip_dst=me;;action=block;;proto=tcp;;p
```

Bloquer l'accès au réseau/à Internet pour firefox.exe

```
# /usr/share/eole/controlevnc/cliscribe.py 172.16.0.45 --firewall
'ADD::maregle;;ip_src=me;;ip_dst=any;;action=block;;proto=any;;progr
Files\Mozilla Firefox\firefox.exe"'
```

Ne fonctionne que sur Vista et supérieur.

Supprimer toutes les règles de pare-feu nommées maregle

```
# /usr/share/eole/controlevnc/cliscribe.py 172.16.0.45 --firewall
'DELL::maregle'
```

Affichage à distance d'un poste client

Il existe 2 méthodes pour prendre la main sur un poste :

- VNC ;
- Le *Bureau à distance Windows*.

VNC

Après s'être connecté en SSH (ssh -X ou putty+Xming) les commandes suivantes permettent l'affichage du poste :

Installer xtightvncviewer

```
# apt-get install xtightvncviewer
```

```
# nohup vncviewer -listen 0 &
```

```
# /usr/share/eole/controlevnc/cliscribe.py 172.16.0.45 --vncinputs
<IP_SCRIBE>
```

Cette méthode ne fonctionne que si un utilisateur est connecté sur le poste.

Bureau à distance

Après s'être connecté en SSH (ssh -X ou putty+Xming) :

Installer rdesktop

```
# apt-eole install rdesktop
```

Activer le bureau à distance

```
# /usr/share/eole/controlevnc/cliscribe.py 172.16.0.45 --execute 'REG ADD
```

```
"HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server" /v
fDenyTSConnections /t REG_DWORD /d 0 /f'
```

Redémarrer la machine pour prendre en compte l'activation du bureau à distance

```
# /usr/share/eole/controlevnc/cliscribe.py 172.16.0.45 --shutdown 1 #
```

Attendre que la machine redémarre et exécuter rdesktop

```
# rdesktop 172.16.0.45
```

On peut spécifier une résolution

```
# rdesktop 172.16.0.45 -g 1400x900
```

Cette méthode ferme la session distante s'il y en a une d'ouverte.

2.5.2. Le Pare-feu du poste client

Paramétrage du pare-feu sur les postes clients

Il est nécessaire d'avoir un accès "root".

Le fichier `/home/client_scribe/liste_fwregles.eol` contient les règles de pare-feu appliquées à chaque démarrage du poste (à chaque démarrage du service Scribe sur le poste pour être précis).

Ajout d'une règle

Une règle possède la structure suivante :

```
OS : :"NOM_REGLE" ; ;proto="PROTOCOLE" ; ;program="PROGRAMME"
; ;ip_src=IP_SOURCE ; ;ip_dst=IP_DISTANTE ; ;port_dst=PORT_DISTANT ; ;action
```

- OS : WinXP, Vista (séparer par "|" pour plusieurs OS)
- NOM_REGLE : seulement des caractères alphanumériques, sans accents et sans espaces
- PROTOCOLE : any, tcp, udp, icmp
- PROGRAMME : chemin local ou réseau d'un programme
- IP_SOURCE : adresse IP source
- IP_DISTANTE : adresse IP distante
- PORT_DISTANT : port distant
- ACTION : allow, block

Par exemple :

On a un serveur AutoCad avec l'IP 172.16.0.21, on veut y autoriser l'accès en cas de blocage réseau par `Gestion-postes` :

```
WinXP|Vista:: "AcadServeur" ;; proto = "any" ;; ip_src = "any" ;; ip_dst =
172.16.0.21 ;; action = "allow"
```

Il est indispensable de générer une nouvelle *somme md5* à chaque modification de `/home/client_scribe/liste_fwregles.eol` pour que le service Scribe puisse en valider l'intégrité lors de son téléchargement.

```
md5sum /home/client_scribe/liste_fwregles.eol > /home/client_scribe/liste_fwregles.eol.MD5SUM
```

`/home/client_scribe/liste_fwregles.eol` est un template Creole, cela signifie qu'il est écrasé à chaque reconfigure/mise à jour.

Pour pérenniser les modifications réalisées dans `/home/client_scribe/liste_fwregles.eol` :

```
cp /home/client_scribe/liste_fwregles.eol /usr/share/eole/creole/modif
gen_patch
reconfigure
```

2.5.3. Wake on Lan

Le standard Wake on Lan[p.143] permet le réveil d'une machine à distance et présente des intérêts variés.

Par exemple, on peut vouloir démarrer les stations la nuit pour exécuter WPKG[p.143] et ainsi appliquer les installations et mises à jour sans perturber les utilisateurs.

La nouvelle version du logiciel ecoStations intègre la fonctionnalité Wake on Lan pour les postes clients gérés par le serveur Scribe.

Installation du paquet wakeonlan

Le paquet `wakeonlan` fournit l'application permettant de réveiller les stations à distance.

Pour l'installer :

```
# apt-eole install wakeonlan
```

Récupération des adresses MAC

Il est nécessaire de disposer des adresses MAC[p.141] des stations à réveiller.

Les adresses MAC des stations sur lesquelles le client Scribe est installé sont disponibles peuvent être listées en utilisant le script `manage_stations.py` :

```
# /usr/share/eole/controlevnc/manage_stations.py --list-all
seven64-1;192.168.230.131;08:00:27:85:0C:95;pcwin7,10.1.2.51,02:00:0A:01:02
```

Le caractère `;` délimite les stations et le caractère `,` permet de séparer les informations associées à chacune des stations.

Paramétrage des stations

Il est nécessaire de paramétrer le Wake on Lan dans le BIOS[p.141] des stations à réveiller.

Cela se fait en général dans le menu du BIOS : `Alimentation/Power, Wake On Lan/Remote Wake Up=> Enabled`.

Démarrage d'une station à distance

Une fois le BIOS paramétré et la station éteinte, exécutez la commande suivante sur le serveur :

```
# wakeonlan 08:00:27:85:0C:95
```

Démarrage de toutes les stations à distance

Pour demander le démarrage de toutes les stations, il faut exécuter la commande wakeonlan pour chacune des adresses MAC des stations listées :

```
/usr/share/eole/controlevnc/manage_stations.py --list-all | sed 's/;/\n/g' |  while read i;
do
    mac=$(echo $i|cut -d ',' -f 3);
    wakeonlan $mac;
done
```

Voir aussi...

> ecoStations : gérer l'extinction et l'allumage des postes à des horaires donnés [p.98]

2.5.4. Gestion des ACLs

Cette partie décrit le fonctionnement entre les ACLs Linux/Samba et les droits sous Windows.

Préambule

Par défaut Linux/Unix connaît trois type de permissions :

- R : Lire (Read)
- W : Écrire (Write)
- X : Exécuter (eXecute)

Le droit d'exécution pour un dossier permet de rentrer dedans.

Le droit de lecture pour un dossier permet de lister son contenu.

Par défaut Linux/Unix considère trois type d'utilisateurs :

- U : utilisateur (user)
- G : groupe (group)
- O : propriétaire (owner)

Les ACLs permettent de compléter ces permissions et de paramétrer des droits particulier pour un utilisateur ou un groupe.

Sur un module EOLE, les ACLs ne sont supportées que sur la partition `/home`.

Attention sur un dossier qui possède des ACLs, les droits Unix sont mal affichés par la commandes `ls -l` ou par l'alias `ll`, il faut utiliser la commande `getfacl` pour les afficher correctement et `setfacl` pour les modifier.

Seules les ACLs par défaut sont hérités, les droits Unix positionnés à `777` sur un dossier n'est pas hérité par les fichiers et dossiers qui seront créés dedans.

Exemple d'un mauvais affichage des droits Unix

```
root@scribe:~# ls -ld /home/workgroups/commun/
```

> `drwxr-x---+ 5 root root 4096 févr. 12 11:35 /home/workgroups/commun/`
>
> D'après cette commande, les droit Unix sont `750`, le signe `+` indique qu'il y a des ACLs.

Affichage des droits avec la commande getfacl

La commande `getfacl` liste les droits Unix, les ACLs et les ACLs par défaut :

`root@scribe:~# getfacl /home/workgroups/commun/`

`getfacl : suppression du premier / des noms de chemins absolus`

`# file: home/workgroups/commun/`

`# owner: root`

`# group: root`

`user::rwx` ← droit Unix 7

`group::---` ← droit Unix 0 (juste avant la commande `ls -ld` affichait un `5` pour le groupe)

`group:administratifs:r-x` ← ACL

`group:professeurs:r-x` ← ACL

`group:eleves:r-x` ← ACL

`mask::r-x`

`other::---` ← droit Unix 0

`default:user::rwx`

`default:group::---`

`default:group:administratifs:r-x` ← ACL par défaut

`default:group:professeurs:r-x` ← ACL par défaut

`default:group:eleves:r-x` ← ACL par défaut

`default:mask::r-x`

`default:other::---`

On voit que pour le groupe la commande `ls -ld` n'affiche pas les bons droits : `5` au lieu de `0`.

Modifier des droits

Si on veut modifier des droits :

`root@scribe:~# mkdir /home/workgroups/commun/toto`

`root@scribe:~# setfacl -Rm g:eleves:rwx /home/workgroups/commun/toto`

Option de la commande setfacl :

- `-R` pour être récursif
- `-m` pour modifier
- `g:` : indique qu'il s'agit d'un groupe, suivi du nom du groupe ou rien pour le groupe propriétaire
- `:rwx` : lui donne les droits Read Write eXecute

`root@scribe:~# getfacl /home/workgroups/commun/toto/|grep eleves`

`group:eleves:rwx`

`default:group:eleves:r-x`

La même commande mais pour les ACLs par défaut (celles qui seront héritées par le contenu) :

```
root@scribe:~# setfacl -Rdm g:eleves:rwx /home/workgroups/commun/toto
```

- `-d` pour indiquer que l'on modifie les ACLs par défaut

```
root@scribe:~# getfacl /home/workgroups/commun/toto/|grep eleves
group:eleves:rwx
default:group:eleves:rwx
```

Seuls les dossiers possèdent des ACLs par défaut, pour l'héritage. Les fichiers n'en ont donc pas.

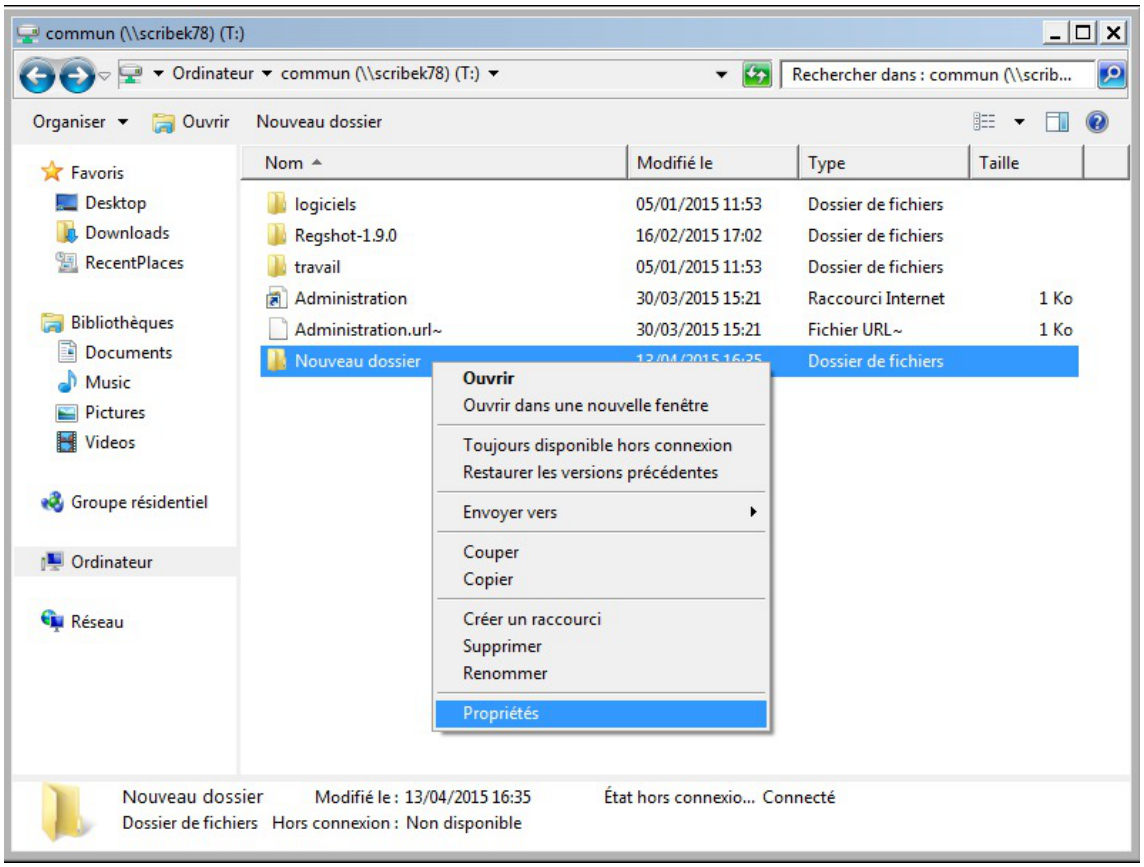
Pour plus d'information il faut se reporter à la page de manuel de la commande :

```
# man getfacl
```

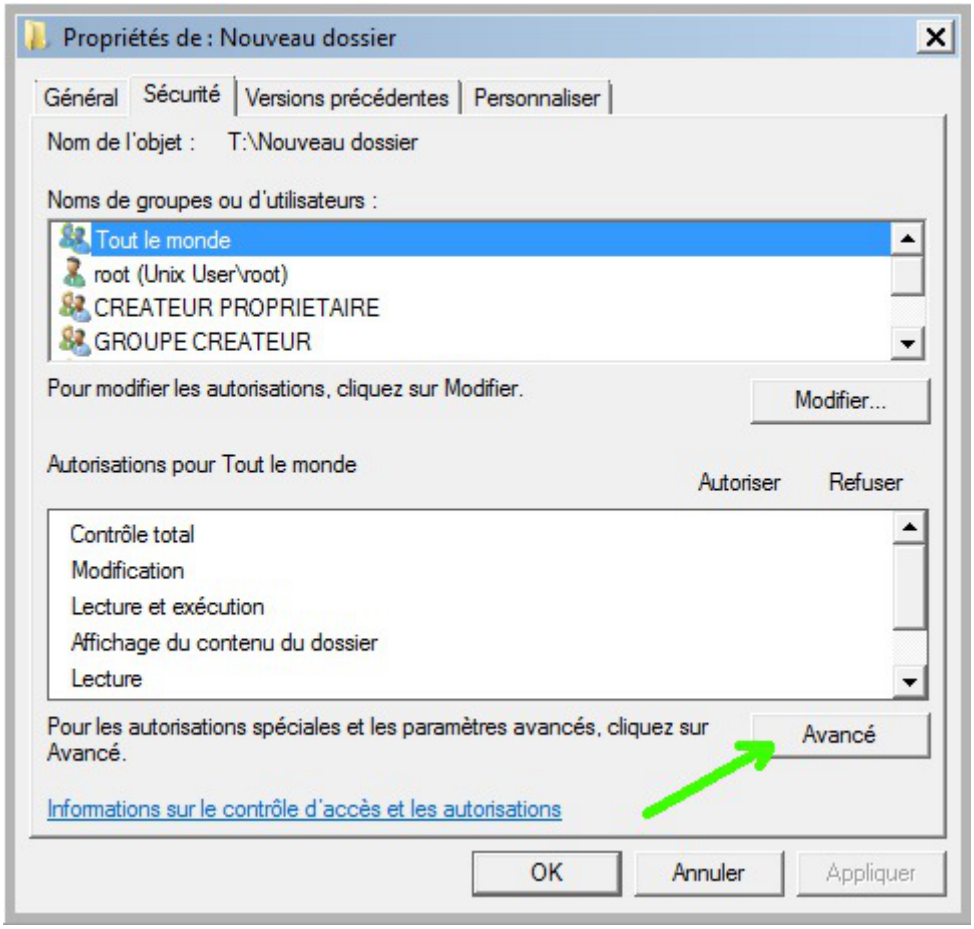
ou

```
# man setfacl
```

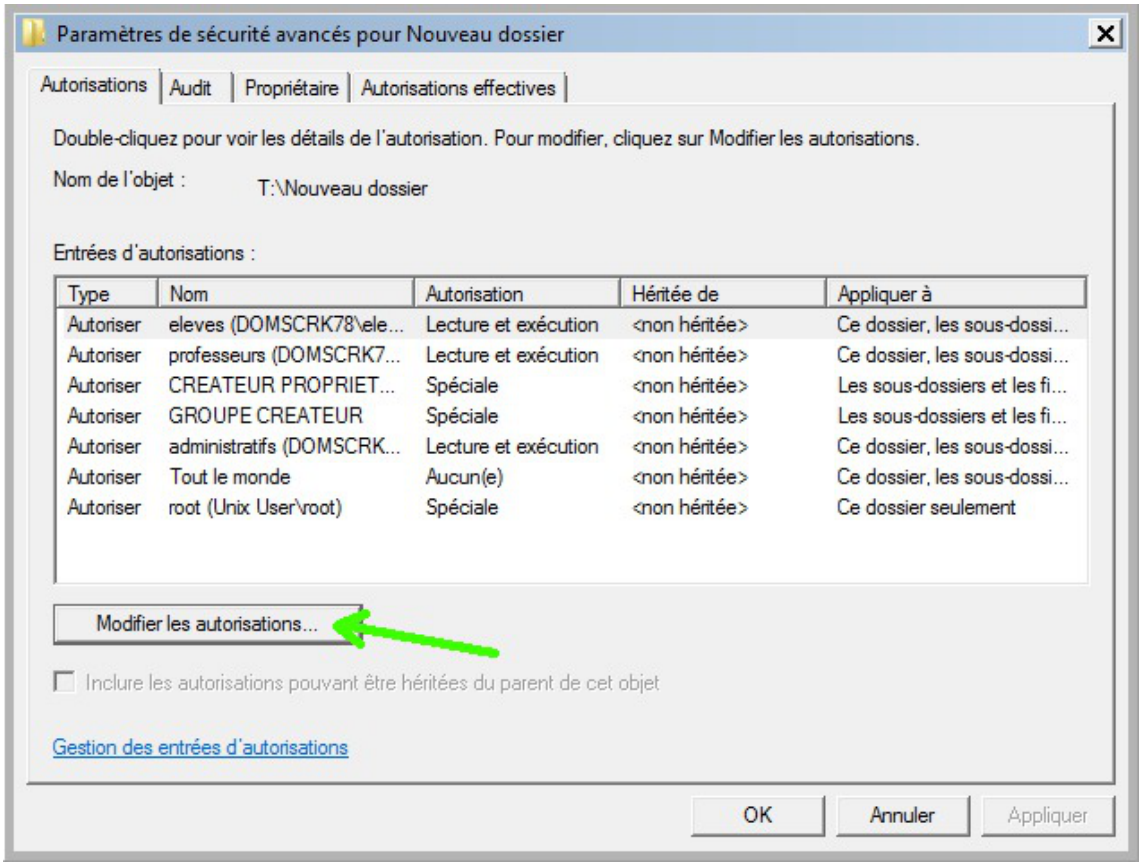
Le plus simple est de gérer les ACLs depuis Windows, pour cela faire un clic droit sur un fichier ou sur un dossier et cliquer sur l'action `Propriétés`.



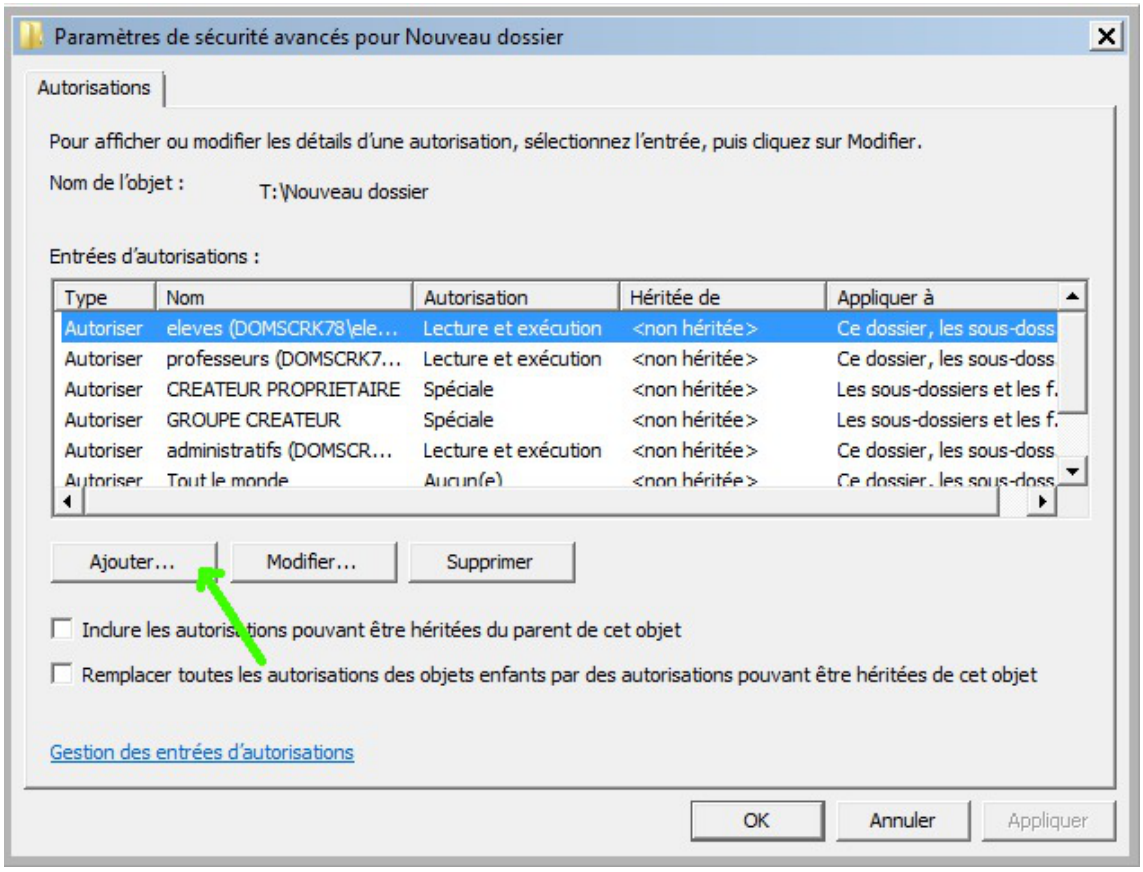
On obtient la fenêtre de propriétés du fichier ou du dossier sélectionné, pour modifier les autorisations il faut se rendre dans l'onglet `Sécurité`, choisir le nom de groupes ou d'utilisateurs, puis cliquer sur le bouton `Avancé`.



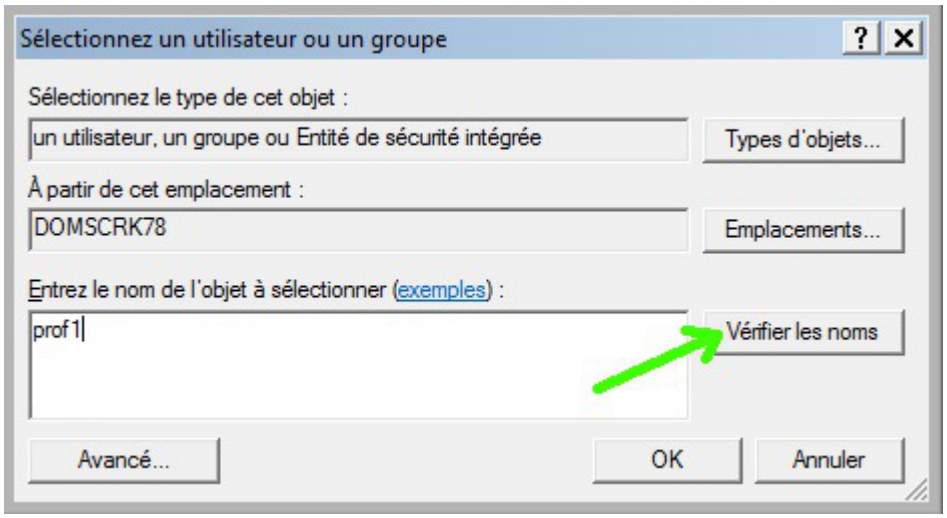
Dans l'onglet Autorisations, cliquer sur l'entrée désirée puis cliquer sur le bouton Modifier les autorisations… .



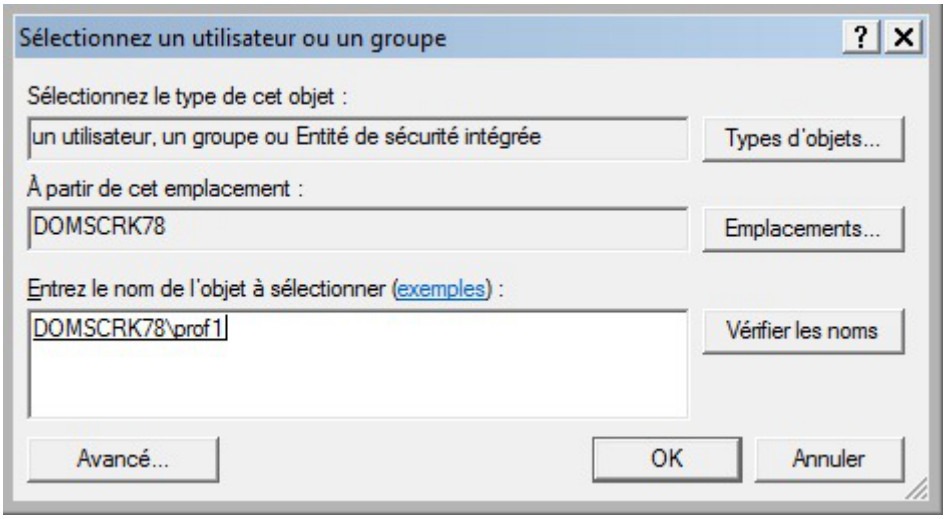
Parmi les modifications des autorisations il est possible d'ajouter, de modifier ou de supprimer. Cliquer sur le bouton Ajouter….



Entrer un nom d'utilisateur ou le nom d'un groupe et cliquer sur le bouton Vérifier les noms.



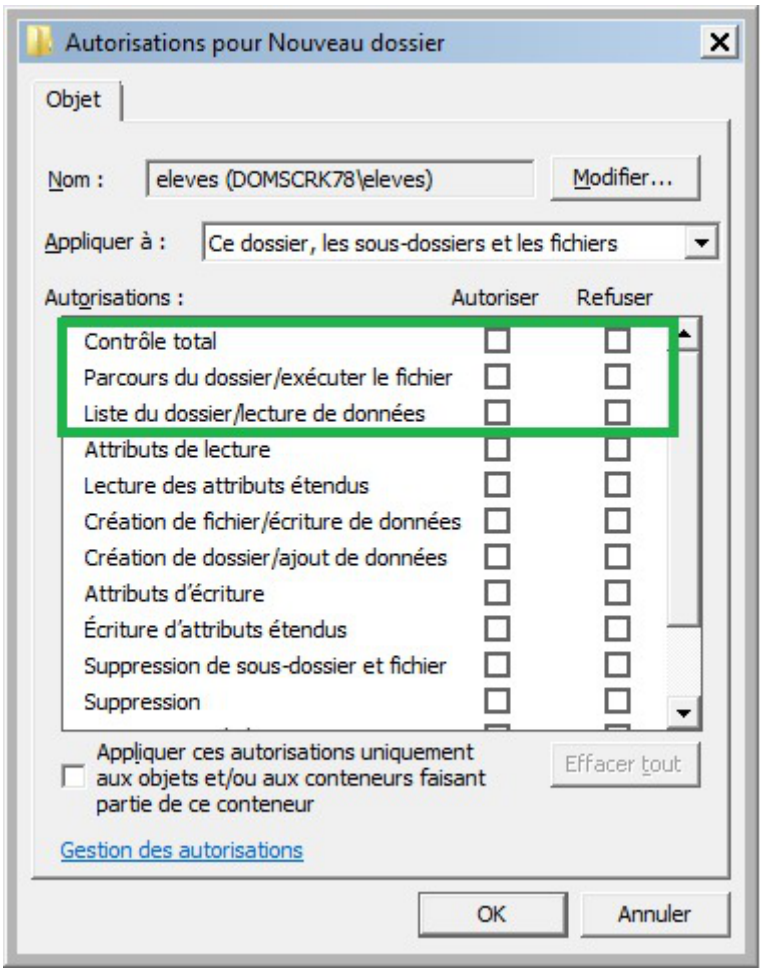
Valider avec le bouton OK.



Cocher les autorisations désirées et valider avec le bouton OK.

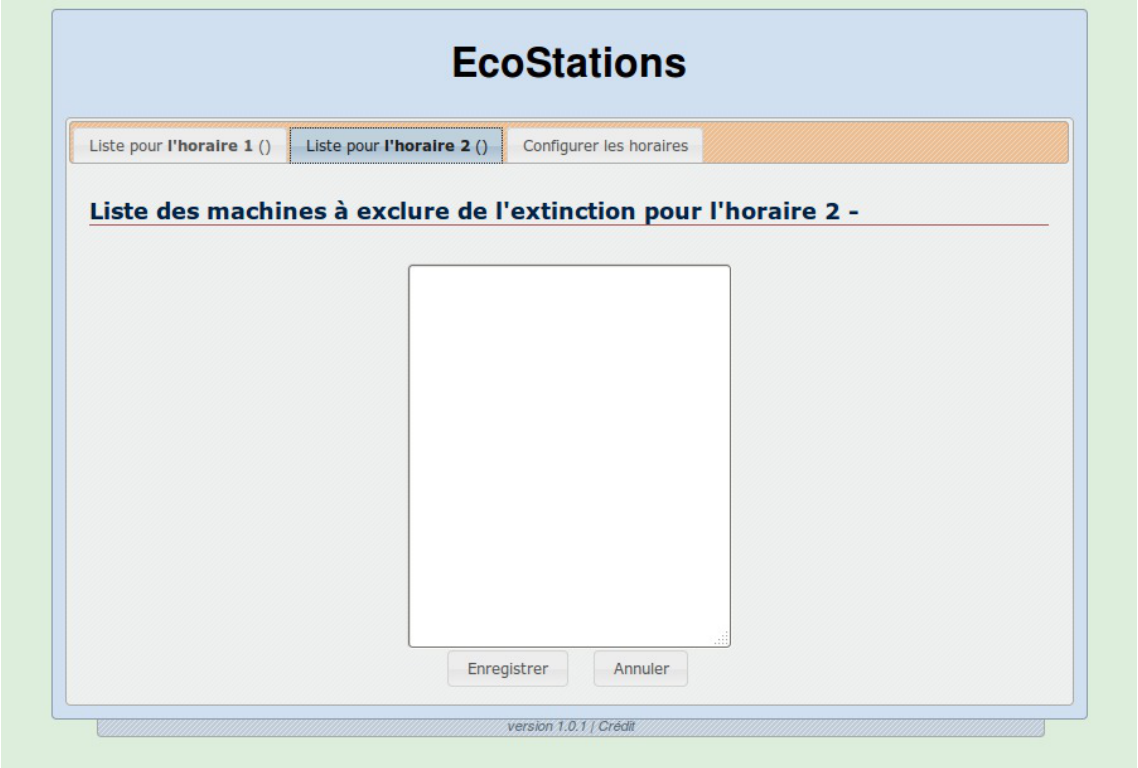
Il faut par contre garder à l'esprit que côté serveur on n'a que 3 droits : **R**ead **W**rite et e**X**ecute.

Seules les 3 premières cases à cocher proposées avec cette méthode sont supportées par le serveur Scribe. Les autres ne fonctionnent pas. Les droits sur les autres lignes vont se placer automatiquement.



2.6. ecoStations : gérer l'extinction et l'allumage des postes à des horaires donnés

Présentation



ecoStations est un outil qui permet d'éteindre le parc informatique d'un établissement suivant une procédure assez souple pour permettre d'intégrer la notion d'internat par exemple ou de station à laisser allumée constamment.

Il faut renseigner via une interface web, deux listes de stations du parc L1 et L2 ainsi que deux horaires distincts H1 et H2.

À l'heure H1, toutes les stations de l'établissement seront éteintes exceptées les stations listées dans L1 ; puis à l'heure H2, toutes les stations de l'établissement seront éteintes exceptées les stations listées dans L2.

Ainsi, les stations listées dans L1 et L2 ne seront pas éteintes.

ecoStations a été développé en étroite collaboration entre Olivier Hacquard, Pascal Ratte, Laurent Etignard, Frédéric Lamy, Valéry Georges et Jérôme Labriet.

La documentation d'utilisation (disponible dans l'espace contribution) a été rédigée par Pierre Mariot.

http://dev-eole.ac-dijon.fr/projects/ecostations/

Montée de version de l'application ecoStations

L'application ecoStations qui permet de gérer l'extinction et l'allumage des postes à des horaires donnés passe en version 2.4.8.

L'ajout d'un script permet notamment d'annuler le re-démarrage d'une station.

Installation d'ecoStations

ecoStations s'installe manuellement, saisir les commandes suivantes dans un terminal :

```
# Query-Auto
```

```
# apt-eole install eole-ecostations
```

L'application n'est pas disponible immédiatement après l'installation.
L'opération nécessite une reconfiguration du serveur avec la commande `reconfigure`.

L'application fonctionne uniquement sur le module Scribe.

Pour désactiver rapidement et temporairement (jusqu'au prochain reconfigure) l'application web il est possible d'utiliser la commande suivante :

```
# a2dissite nom de l'application
```

Le nom de l'application à mettre dans la commande est celui que l'on trouve dans le répertoire `/etc/apache2/sites-available/`

Pour activer cette nouvelle configuration il faut recharger la configuration d'Apache avec la commande :

```
# service apache2 reload
```

Pour réactiver l'application avec cette méthode il faut utiliser les commandes suivantes :

```
# a2ensite nom de l'application
```

```
# service apache2 reload
```

Accès à l'application web

Pour accéder à l'application se rendre à l'adresse : `http://<adresse serveur>/ecostations`
L'authentification se fait **obligatoirement** par le biais du serveur SSO, ce service doit donc être actif.

Rôles des utilisateurs

Seul l'utilisateur `admin` est autorisé à se connecter à l'application.

Utilisation

Les postes clients doivent avoir été pré-configurés avec `power_config.cmd` afin de supprimer la mise en veille automatique qui bloque l'ordre d'extinction.

Une documentation d'utilisation est disponible dans l'espace de contributions EOLE à l'adresse suivante :
http://eoleng.ac-dijon.fr/documentations/2.4/contributions/

2.7. Gestion des quotas disque

Il est possible, pour chaque utilisateur, de limiter la quantité de données qu'il peut stocker sur le serveur en lui imposant un quota disque maximum.
Les quotas sont composés d'une limite douce (soft) et d'une limite dure (hard).

2.7.1. Visualisation des quotas disque dans l'EAD

Désynchronisation des quotas disque

Il peut arriver qu'il y ait une désynchronisation entre l'utilisation réelle du disque et le système de vérification des quotas.

Cela se traduit généralement par le fait que des utilisateurs sont considérés à tort comme dépassant leur quota disque.

La commande `quotacheck` permet de corriger le problème. Son utilisation demande quelques précautions.

Exemple d'utilisation de quotacheck sur le module Scribe où `/home` est la partition utilisée pour les données et les quotas utilisateurs.

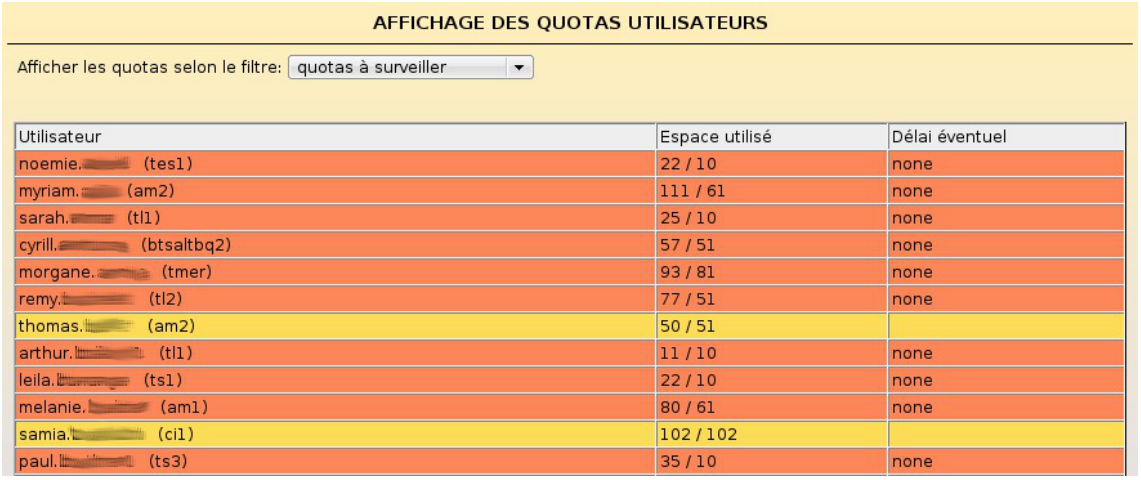
1. arrêter les différents services susceptibles d'écrire sur la partition (samba, proftpd, exim4, ...) ;
2. démonter les éventuels montages liés à cette partition (images ISO, ...) ;
3. désactiver les quotas sur la partition : `quotaoff /home` ;
4. lancer la vérification des quotas : `quotacheck -vug /home` ;
5. réactiver les quotas sur la partition : `quotaon /home` ;
6. remonter les partitions : `mount -a` ;
7. démarrer les services précédemment arrêtés.

Cette procédure est également à appliquer dans le cas où la commande `repquota -a` ne rend plus la main.

Les quotas sur le module Scribe

Pour consulter les quotas, le menu `Outils/Quotas disque` de l'EAD permet d'afficher les quotas utilisateurs selon 3 filtres :

- Quotas dépassés
- Quotas à surveiller (quotas presque atteint)
- Tous les quotas



AFFICHAGE DES QUOTAS UTILISATEURS

Afficher les quotas selon le filtre: quotas à surveiller

Utilisateur	Espace utilisé	Délai éventuel
noemie. (tes1)	22 / 10	none
myriam. (am2)	111 / 61	none
sarah. (tl1)	25 / 10	none
cyrill. (btsaltbq2)	57 / 51	none
morgane. (tmer)	93 / 81	none
remy. (tl2)	77 / 51	none
thomas. (am2)	50 / 51	
arthur. (tl1)	11 / 10	none
leila. (ts1)	22 / 10	none
melanie. (am1)	80 / 61	none
samia. (ci1)	102 / 102	
paul. (ts3)	35 / 10	none

Affichage des quotas utilisateur dans l'EAD

Les quotas sont appliqués sur la partition `/home`. Les quotas concernent, ainsi, l'ensemble des fichiers créés par l'utilisateur sur le serveur (dossiers personnels, partages équipe pédagogique, classe, groupes, etc.).

Fonctionnement des quotas disque

Il est possible, pour chaque utilisateur, de limiter la quantité de données qu'il peut stocker sur le serveur en lui imposant un quota disque maximum.

Les quotas sont composés d'une limite douce (soft) et d'une limite dure (hard).

Les règles suivantes s'appliquent à l'utilisateur :

- il ne peut pas dépasser la limite dure ;
- il peut dépasser la limite douce pendant 7 jours ;
- passé ce délai, seule la limite douce est prise en compte et il est obligé de supprimer des données afin de repasser en dessous de celle-ci ;
- à partir de là, le processus de la limite douce/dure reprend et l'utilisateur peut à nouveau dépasser la limite douce pour une durée maximale de 7 jours.

Dans l'EAD, c'est la limite douce qui est indiquée.

Sur les modules Scribe et Horus, la limite dure vaut le double de la limite douce.

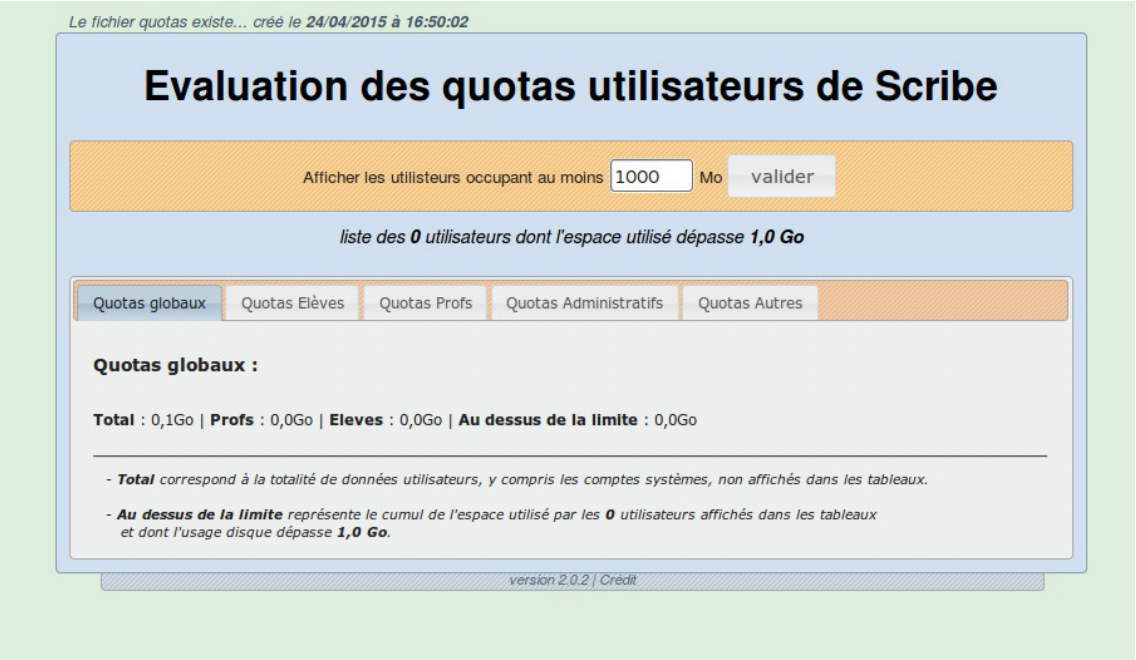
2.7.2. Infosquota : gestion des quotas utilisateurs

Présentation

Infosquota est un outil qui permet de mettre en place les quotas de manière très souple et très pédagogique. Chaque utilisateur apprend à gérer son quota en suivant une information claire sur son évolution.

Grâce à son outil de visualisation, Infosquota permet de retrouver les fichiers que les utilisateurs ont ventilé hors de leur lecteur partagé personnel. En effet les fichiers dispersés dans d'autres volumes sont

comptabilisés dans le quota de l'utilisateur.



Infosquota a été développé par Olivier Hacquard et Jérôme Labriet (Académie de Besançon) en étroite collaboration avec Bruno Debeve (Académie de Bordeaux), Frédéric Poyet (Académie de Dijon) et Pierre Mariot (Académie de Besançon) dans le cadre du projet EOLE.

http://dev-eole.ac-dijon.fr/projects/infquot

Les derniers développements mis à disposition par Bruno Debeve ont également été intégrés.

http://www.debeve.net/infosquota_dev/

Installation d'Infosquota

Infosquota s'installe manuellement, saisir les commandes suivantes dans un terminal :

```
# Query-Auto
# apt-eole install eole-infosquota
```

L'application n'est pas disponible immédiatement après l'installation.

L'opération nécessite une reconfiguration du serveur avec la commande `reconfigure`.

L'application fonctionne uniquement sur le module Scribe.

Pour désactiver rapidement et temporairement (jusqu'au prochain reconfigure) l'application web il est possible d'utiliser la commande suivante :

```
# a2dissite nom_de_l'application
```

Le nom de l'application à mettre dans la commande est celui que l'on trouve dans le répertoire `/etc/apache2/sites-available/`

> Pour activer cette nouvelle configuration il faut recharger la configuration d'Apache avec la commande :
>
> `# service apache2 reload`
>
> Pour réactiver l'application avec cette méthode il faut utiliser les commandes suivantes :
>
> `# a2ensite nom_de_l'application`
>
> `# service apache2 reload`

L'initialisation de l'application (recherche des fichiers) s'effectue lors de l'instance ou du reconfigure suivant l'installation du paquet.

La mise à jour des fichiers s'effectue de façon hebdomadaire.

Accès à l'application web

Pour accéder à l'application se rendre à l'adresse : `http://<adresse serveur>/quotas/`

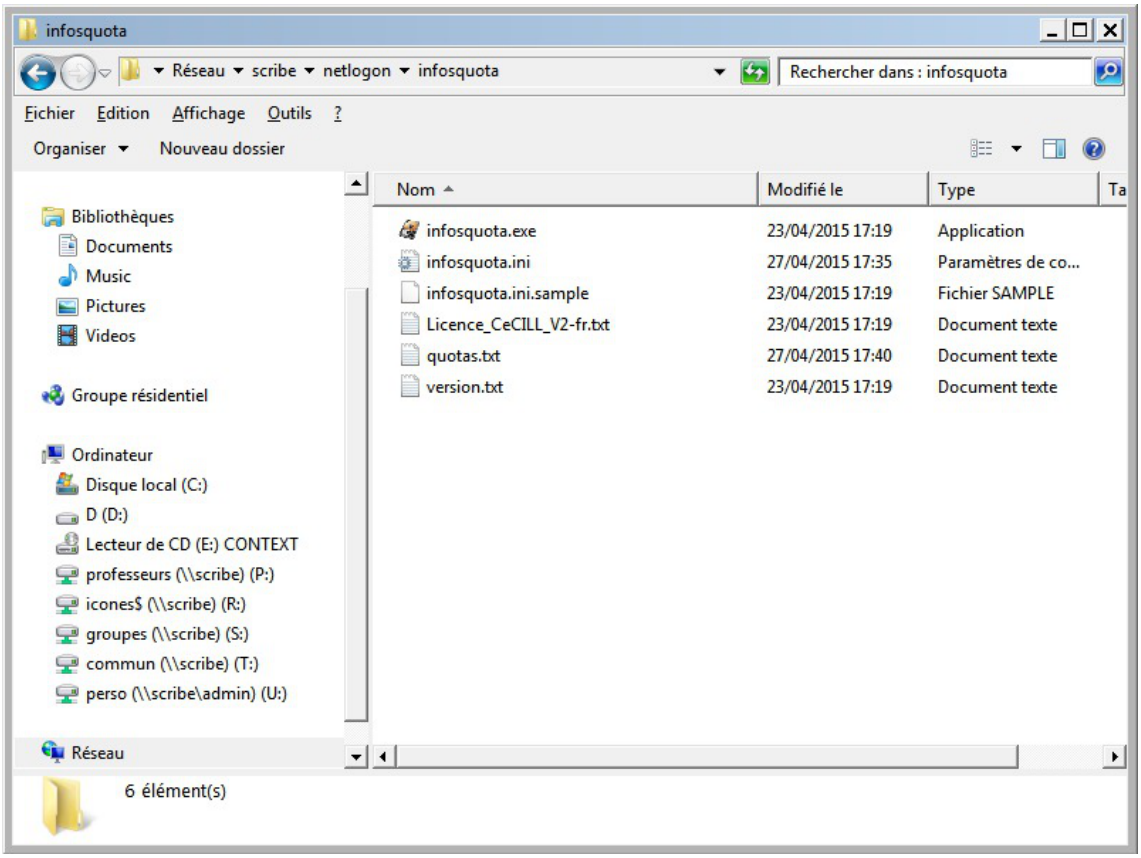
L'authentification se fait **obligatoirement** par le biais du serveur SSO, ce service doit donc être actif.

Rôles des utilisateurs

Seul l'utilisateur `admin` est autorisé à se connecter à l'application.

Utilisation

L'exécutable `infosquotas.exe` est lancé au démarrage de la session et affiche les messages qui conviennent selon la configuration des quotas établie dans l'EAD et celle des alertes saisies dans le fichier `\\scribe\netlogon\infosquota.ini`.



Une documentation d'utilisation est disponible dans l'espace de contributions EOLE à l'adresse suivante :
http://eoleng.ac-dijon.fr/documentations/2.4/contributions/

Remarques

L'utilisation du disque par utilisateur est enregistrée dans le fichier : `/home/netlogon/infosquota/quotas.txt`.

Le journal généré par le script de recherche des fichiers est disponible dans : `/var/log/infosquota/recherche-fich-users.log`.

La liste des fichiers ventilés d'un utilisateur est stockées dans le fichier : `/var/www/html/outils/quotas/log/<login>.log`.

2.7.3. Envoi de courrier électronique en cas de dépassement des quotas

Dans l'onglet `Samba` de l'interface de configuration du module en mode expert, il est possible d'activer l'envoi d'un courrier électronique à un utilisateur dans le cas où celui-ci dépasse le quota disque.

Il faut bien sûr que l'utilisateur ait une adresse de courrier électronique valide définie dans l'annuaire.

> Les fichiers déplacés dans la corbeille sont inclus dans le calcul de l'espace disque occupé par l'utilisateur. Pour limiter les dépassements de quota disque, il est conseillé de paramétrer une durée de conservation assez courte.

Voir aussi...

> Onglet Samba : Configuration du contrôleur de domaine

3. Résolution des problèmes du client

3.1. Problèmes à l'inscription au domaine

Lorsqu'un problème survient pendant l'inscription au domaine ou à l'ouverture de session, plusieurs pistes sont à explorer.

Sur le serveur

Vérifier l'état du serveur avec la commande `diagnose`.

Vérifier la communication avec le client à l'aide de la commande `tcpcheck` :

```
# tcpcheck 2 <IP station>:139
```

> Sur le serveur les commandes doivent être exécutées avec l'utilisateur `root`, soit sur la console soit en SSH.

Sur un client Windows

Vérifier la configuration réseau de la station avec la commande `ipconfig /all`

Vérifier la communication du client avec le serveur avec les commandes :

```
ping <adresse module>
```

```
nbtstat -A <adresse module>
```

3.2. Problèmes avec le Client Scribe

Le client Scribe enregistre ses actions dans les fichiers :

- %WINDIR%\cliscribe.log
- %WINDIR%\cliscribe_logon.log
- %WINDIR%\cliscribe_updater.log
- %TMP%\cliscribe_utilisateur-<login>.log

Ces fichiers peuvent être utilisés pour vérifier l'exécution du client Scribe et détecter d'éventuelles erreurs. Le niveau de verbosité est renseigné dans la base de registre sous : `HKEY_LOCAL_MACHINE\Software\Eole\Scribe` : "log_level".

Le niveau de verbosité peut être paramétré dans la console ESU `Domaine => Groupe de machine => "Client Scribe" => "Activer le mode debug du client"`.

Ce sont les valeurs du module *logging* de *Python* qui sont utilisées :

- CRITICAL

- ERROR
- WARNING
- INFO
- DEBUG

Lorsque le niveau de journalisation (`HKEY_LOCAL_MACHINE\Software\Eole\Scribe` : "`log_level`") est placé sur "**debug**" la fenêtre de mise à jour reste ouverte 40 secondes en cas d'avertissement ("warning") ou d'erreur ("error").

Les "traceback"

Le client Scribe ainsi que l'application *Gestion-postes* peuvent générer des erreurs en cas de problème.

Ces erreurs peuvent contenir le mot "**traceback**". Il s'agit de la pile d'appel (dernières instructions du programme) ayant conduit à cette erreur. Cela permet de retrouver plus rapidement la cause du problème.

Si vous rencontrez une telle erreur et que vous ne savez pas l'interpréter, pensez à joindre le contenu du traceback à votre demande (copie d'écran d'un popup ou fichier de log).

Le fichier de logon

Lors de l'ouverture de session, le client Scribe lit le fichier de logon de l'utilisateur.

Ce fichier se trouve sur le serveur dans le partage `\\scribe\netlogon`.

Le nom du fichier se compose du login et du système d'exploitation avec lequel l'utilisateur se connecte, par exemple : `adminWinXP.txt`.

En cas de problème de génération du fichier de logon il peut être utile de tester sa création manuellement, pour ce faire il faut exécuter la commande suivante :

```
/usr/share/eole/fichier/dyn-logon.py -u <login> -o <type_os> -m <nom_machine_win> -i <ip_machine_win>
```

où :

- <login> est login dont le fichier logon pose problème
- <type_os> : Win2K, WinXP, Vista, Win2K3
- <nom_machine_win> : le nom de la machine Windows
- <ip_machine_win> : l'IP de la machine Windows

Les erreurs sur le client

Lorsque le client affiche une erreur elle ne s'est pas forcément produite sur le client.

En effet, lorsque le client se connecte au serveur, le résultat de l'ensemble des actions exécutées sur le serveur est renvoyé au client, y compris les erreurs.

Un "traceback" peut donc contenir une pile d'appel d'un programme se trouvant sur le serveur.

Les fichiers de journalisation (log) du serveur contiendront alors une copie de l'erreur.

Pour tester la communication du serveur avec le client, faire sur le serveur :

```
tcpcheck 2 <ip station>:8788
```

3.3. Problèmes Controle-vnc

C'est le service sur le serveur Scribe qui communique avec le *service client Scribe* installé sur les clients Windows. Il applique la configuration ESU et gère entre autre le blocage et la distribution de devoirs.

Son fichier de journalisation (log) est `/var/log/controle-vnc/main.log`. Pensez à l'examiner lorsque vous rencontrez des problèmes sur le client (traceback par exemple).

3.4. Problèmes de droits sur les répertoires partagés

Si des dysfonctionnements persistent et qu'ils semblent causés par des répertoires manquants dans les partages ou des problèmes de droits d'accès, il est possible de réinitialiser les droits à l'aide des utilitaires `droits_user.py` et `droits_partage.sh`.

droits_user.py

La commande `/usr/share/eole/backend/droits_user.py` vérifie la présence des répertoires personnels des utilisateurs (y compris le sous-dossier `prive` des élèves) et leur ré-applique les droits par défaut.

Dans sa dernière version (Scribe>=2.5.1), il est possible d'exécuter ce script pour un utilisateur donné en précisant son login en tant que paramètre du script : `/usr/share/eole/backend/droits_user.py toto`

droits_partage.sh

La commande `/usr/share/eole/backend/droits_partage.sh` vérifie la présence des répertoires partagés (y compris les sous-dossiers `donnees` et `travail` pour les classes et les groupes) et leur ré-applique les droits par défaut.

Dans sa dernière version (Scribe>=2.5.1), il est possible d'exécuter ce script pour un groupe donné en précisant son nom en tant que paramètre du script : `/usr/share/eole/backend/droits_user.py 3eme1`

4. Déploiement d'applications pour Windows avec WPKG

WPKG est une application de déploiement d'applications pour Windows.

Elle permet l'installation, la mise à jour et la dés-installation automatique de logiciels.

http://wpkg.org/

L'application WPKG est composée d'un exécutable (`wpkg.js`) et de fichiers de configuration XML copiés dans un dossier partagé sur le serveur de fichier.

Les fichiers XML sont séparés en 3 parties :

- **packages**, les applications installables ;
- **hosts**, les postes ou groupes de postes ;
- **profiles**, la liste de packages à installer pour un host.

Le fichier `wpkg.js` doit être exécuté sur les postes Windows. Il lit les fichiers XML (`config/host/profiles/packages`) et installe en conséquence les applications sur les postes.
Afin d'exécuter `wpkg.js` automatiquement il faut utiliser un lanceur, au choix :

- WPKG Client ;
- Wpkg-GP ;
- une tâche planifiée Windows ;
- n'importe quel autre programme capable d'exécuter wpkg.js.

Dans le cas de l'utilisation de WPKG Client et de Wpkg-GP, ils s'installent sous forme de service Windows et s'exécute au démarrage de la machine.

WPKG Client peut également s'exécuter à l'arrêt du poste.

Les fichiers de configuration sont les suivants :

- wpkg.js (ou moteur WPKG) : `config.xml` ;
- WPKG Client : `settings.xml` ;
- Wpkg-GP : `wpkg-gp.ini`.

4.1. Installation et configuration

Installation et utilisation de WPKG sur un serveur EOLE

WPKG peut être utilisé sur un serveur Scribe ou Horus si le paquet `eole-wpkg` est installé.
Le paquet s'installe avec la commande :

```
# apt-eole install eole-wpkg
```

L'application WPKG est alors est stockée dans le répertoire partagé `\\<SERVEUR>\wpkg`
Elle est paramétré en accès anonyme et en lecture seule (lecture/écriture pour DomainAdmins).

L'accès au répertoire partagé wpkg n'étant pas très pratique, on peut ajouter un lien symbolique dans le dossier personnel (U:) de l'utilisateur admin (comme c'est déjà le cas pour le partage esu) :

```
# ln -s /home/wpkg/ /home/a/admin/perso/wpkg
```

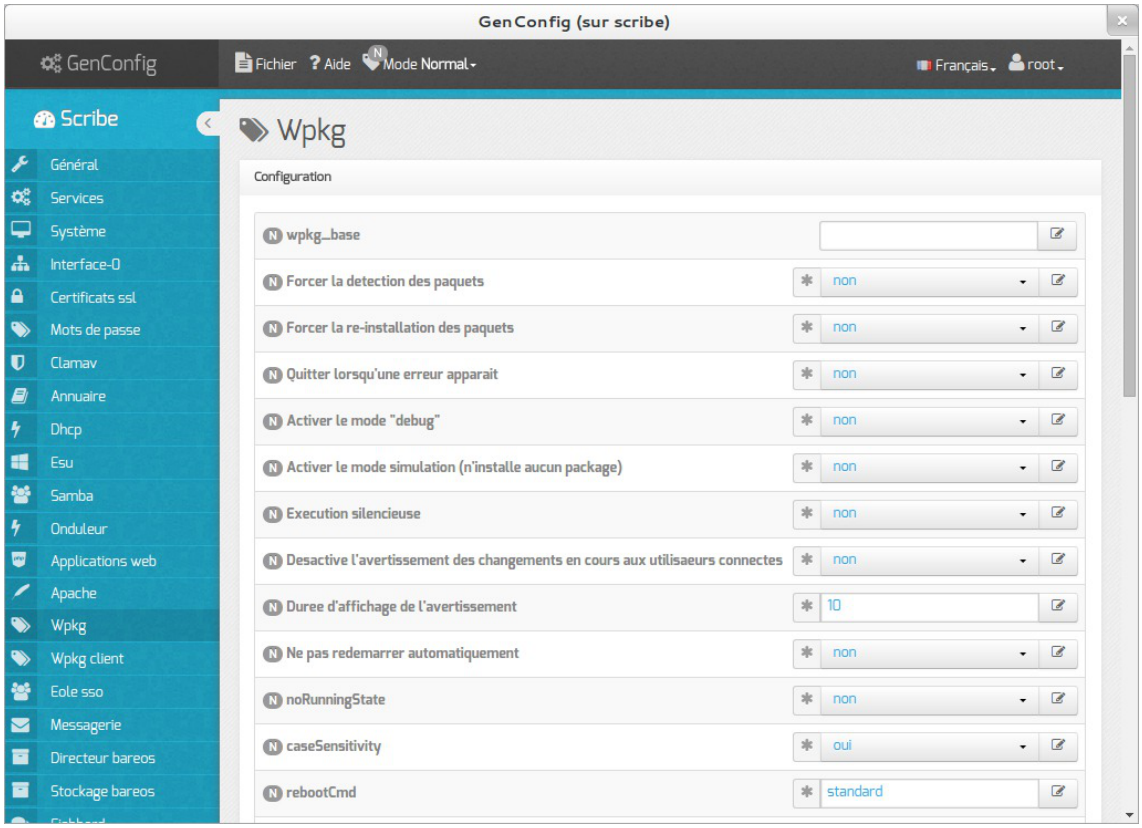
Le paquet `eole-wpkg` fournit les dictionnaires et templates permettant de gérer la configuration de WPKG depuis le serveur Zéphir.

Configuration

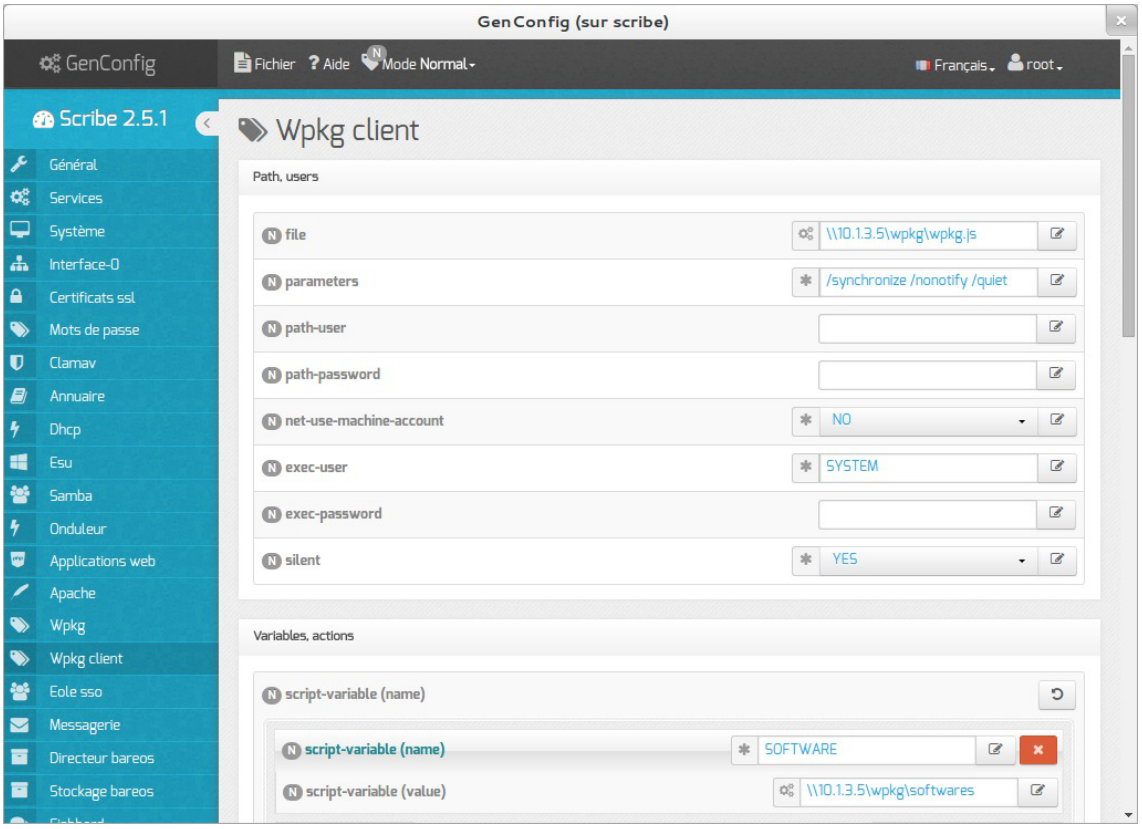
L'outil de gestion de la configuration est l'interface de configuration du module.

Dans l'interface de configuration du module, dans l'onglet `Services`, le service `Gérer la configuration WPKG` est à `oui` par défaut et 2 onglets concernant WPKG sont visibles :

- Wpkg : les options paramétrables du fichier `config.xml` (options de wpkg.js)



- Wpkg client : les options paramétrables des fichiers `settings.xml` (WPKG Client) et `wpkg-gp.ini` (Wpkg-GP)



#fixme compléter l'essentiel de la configuration

Il faut ensuite reconfigurer le serveur à l'aide de la commande `reconfigure` :

```
# reconfigure
```

Installation du client WPKG

Il existe plusieurs façons d'exécuter le moteur `wpkg.js` sur un poste Windows. Il est recommandé d'utiliser les applications suivantes :

- WPKG Client pour Windows XP : http://wpkg.org/files/client/stable/
- Wpkg-GP pour Windows Vista et supérieurs : https://drive.google.com/folderview?id=0B9Eadi-crzpOVEtTM01aYm5YNm8&usp=drive_web

> Il ne faut installer que l'un des deux, installer WPKG Client et Wpkg-GP sur la même machine provoque des comportements inattendus.

Des scripts `.bat` permettent une installation des clients sans question. Pour que ces scripts fonctionnent il faut télécharger les clients en prenant soin de les placer au bon endroit et de bien les nommer.

Après avoir téléchargé les clients (Wpkg-GP et WPKG Client), pour que les scripts fonctionnent il faut les renommer en :

- `WPKG_Client32.msi`
- `WPKG_Client64.msi`

- `Wpkg-GP_x86.exe`
- `Wpkg-GP_x64.exe`

Depuis un poste Windows, télécharger les 4 installeurs (2 en 32bits et 2 en 64bits) et les copier de manière à obtenir :

- `\\<SERVEUR>\wpkg\WPKG_Client32.msi`
- `\\<SERVEUR>\wpkg\WPKG_Client64.msi`
- `\\<SERVEUR>\wpkg\Wpkg-GP_x86.exe`
- `\\<SERVEUR>\wpkg\Wpkg-GP_x64.exe`

Configuration du contenu de WPKG avec l'application Wpkg-Manage

Un fois WPKG installé, il faut configurer les applications et leurs dépendances ainsi que les machines sur lesquelles elles seront installées.

Wpkg-Manage est une application écrite par Christophe Dezé de l'académie de Nantes permettant de gérer la configuration utilisateur de WPKG.

La configuration consiste à définir :

- des hosts, liste de machines associés à un profile ;
- des profiles, liste de paquets à installer ou à mettre à jour ;
- des packages, descriptions des applications à installer (commandes, tests, etc.).

http://eole.ac-dijon.fr/pub/Outils/Wpkg-manage/

Wpkg-Manage permet de gérer le contenu de WPKG, ses fonctionnalités principales sont :

- import des groupes de machines ESU dans WPKG ;
- association des groupes de machines avec les paquets ;
- possibilité de génération de nouveau paquets ;
- téléchargement semi-automatique des installeurs (`.exe`, `.msi`) ;
- fichiers exemples de paquets.

L'installation de l'application Wpkg-Manage doit se faire manuellement depuis le serveur :

```
# wget http://eoleng.ac-dijon.fr/pub/Outils/Wpkg-manage/wpkg-manage.zip
# unzip wpkg-manage.zip
# mv wpkg-manage /home/wpkg/
```

WPKG utilise les notions suivantes :

- hosts (nom de la machine, possibilité d'expression régulière. Ex.: "cdi.*")
  http://wpkg.org/Hosts.xml:fr
- packages (description d'une application, version, chemin vers .exe, etc.)
  http://wpkg.org/Packages.xml:French
- profiles (association entre les "hosts" et les "packages" à y installer)

> http://wpkg.org/Profiles.xml:French

Tests et exécutions manuelles

Il est parfois nécessaire d'exécuter WPKG manuellement sur un poste client pour faire des vérifications.

Il est possible d'exécuter directement le moteur WPKG sans utiliser le client à condition de renseigner les variables WPKG :

```
set ip-scribe=<ADRESSE_IP_SCRIBE>
set SOFTWARE=\\%ip-scribe%\wpkg\softwares
cscript \\%ip-scribe%\wpkg\wpkg.js /synchronize /nonotify /quiet
```

WPKG Client

Si le client est paramétré pour s'exécuter à l'arrêt de la station, il suffit d'arrêter le service WPKG :

```
net stop wpkgservice
```

Si le client s'exécute au démarrage de la station, il suffit de redémarrer le service :

```
taskkill /F /IM WPKGSrv.exe
net start wpkgservice
```

Wpkg-GP

Pour exécuter Wpkg-GP :

```
C:\Program Files\Wpkg-GP\Wpkg-GP-Test.exe
```

4.2. Les packages WPKG

Présentation

Les packages WPKG sont les fichiers décrivant l'installation et la désinstallation des applications Windows. Ils sont contenus dans le répertoire `wpkg/packages/`.

Les packages contiennent, entre autres, la version du logiciel et le chemin vers le programme d'installation.

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- OpenSource -->
<packages>
<package id="7zip"
name="7-Zip"
revision="%version%"
reboot="false"
priority="0">
<variable name="version" value="922" />
<variable name="longversion" value="9.22" />
```

```
<variable architecture="x86" name="platf" value="" />
<variable architecture="x64" name="platf" value="-x64" />
<check type="logical" condition="or">
<check type="file" condition="versionequalto" path="%PROGRAMFILES%\7-Zip\7zFM.exe" value="%longversion%.0.0" />
<check type="file" condition="versionequalto" path="%PROGRAMFILES(x86)%\7-Zip\7zFM.exe" value="%longversion%.0.0" />
</check>
<download dl="http://sourceforge.net/projects/sevenzip/files/7-Zip/%longversio destname="7zip/7z%version%.msi" />
<download dl="http://sourceforge.net/projects/sevenzip/files/7-Zip/%longversio destname="7zip/7z%version%-x64.msi" />
<install cmd='msiexec /qn /norestart /i "%SOFTWARE%\7zip\7z%version%%platf%.msi"' />
<upgrade cmd='msiexec /qn /norestart /i "%SOFTWARE%\7zip\7z%version%%platf%.msi"' />
<remove cmd='msiexec /qn /x "%SOFTWARE%\7zip\7z%version%%platf%.msi"' />
</package>
</packages>
```

Explication sur les balises :

- id : identifiant WPKG de l'application ;
- name : nom de l'application à afficher ;
- revision : nombre entier définissant la version de l'application, il doit être incrémenté pour que WPKG mette l'application à jour ("upgrade") ;
- check : test(s) pour vérifier la présence d'une application (si elle est déjà installée) ;
- install : commande(s) à exécuter pour installer l'application ;
- upgrade/downgrade : commandes pour mettre à jour / rétrograder une application ;
- remove : commande pour désinstaller une application.

Davantage d'explications sur le site officiel de WPKG : http://wpkg.org/Packages.xml:French

Le projet EOLE wpkg-package propose des packages adaptés à l'environnement EOLE :

http://dev-eole.ac-dijon.fr/projects/wpkg-package/

Il contient des fichiers `<package>.xml` directement fonctionnels dans un environnement Horus/Scribe, à quelques (exceptions) près, ainsi que des icônes, des scripts et des outils (dans le dossier `softwares`).

http://dev-eole.ac-dijon.fr/projects/wpkg-package/repository/

Liste des applications supportées :

http://dev-eole.ac-dijon.fr/projects/wpkg-package/repository/revisions/master/show/packages

Téléchargement du projet wpkg-packages

Sous Windows

Le logiciel TortoiseGit permet de récupérer les `.xml` sur nos dépôts : http://tortoisegit.org/

Une fois installé, récupérer le projet `wpkg-packages` à l'adresse http://dev-eole.ac-dijon.fr/git/wpkg-package.git

Sous GNU / Linux

La manipulation peut se faire depuis le serveur Scribe/Horus.

Il est nécessaire d'installer Git :

```
# apt-eole install git-core curl
```

Pour télécharger l'ensemble des fichiers `<packages>.xml` du dépôt il faut le cloner :

```
# cd /root
# git clone https://dev-eole.ac-dijon.fr/git/wpkg-package
```

Lorsque que le dépôt est déjà cloné il faut le mettre à jour :

```
# cd /root/wpkg-package
# git pull
```

Les fichiers `<packages>.xml` sont à copier dans le dossier d'installation de WPKG, la commande rsync permet de ne copier que les nouveaux paquets :

```
# cd /root/wpkg-package
# rsync -Cav . /home/wpkg
```

Certains fichiers `<packages>.xml` contiennent une balise `<eoledl>`. Cette balise indique l'URL où télécharger le ou les installeurs de l'application.

Pour télécharger l'ensemble des installeurs :

```
# cd /home/wpkg/packages/
# ./download installers.py
```

Certains installeurs nécessitent un traitement particulier avant de pouvoir être exécutés automatiquement par WPKG, c'est le cas par exemple du logiciel Java.

Icônes

Le projet wpkg-package contient un dossier nommé `icones` avec les icônes du Bureau et du Menu démarrer correspondantes aux packages.

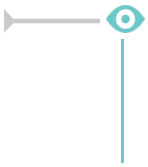
Ce dossier contient les icônes pour Windows 32-bits et 64-bits dans des sous-dossiers séparés, les chemins de ces icônes pouvant être différents.

Softwares

Le projet `wpkg-package` contient un dossier nommé `Softwares` nécessaire à l'exécution de certains packages. Il faut en copier le contenu dans le dossier `wpkg\softwares\` (dossier correspondant à la variable `%SOFTWARE%`). Ce dossier contient notamment un sous-dossier nommé `tools` qui rassemble divers outils comme par exemple nircmd, setacl, wget...

Fonctionnement du téléchargements des installeurs

Le fichier `.xml` contient une ou plusieurs balises `<eoledl>`.



```
<eoledl dl="http://launchpad.net/ocsinventory-windows-agent/2.0/2.0.3/+download/OCS-NG-Windows-Agent-Setup.exe" destname="ocsinventory\" unzip='1' />
```


- dl : lien vers le fichier à télécharger ;
- destname : nom d'un dossier ou d'un fichier ;

  Dans le cas d'un dossier aucun changement de nom est effectué, le fichier est seulement placé dans le dossier. Dans le cas d'un nom de fichier, le fichier téléchargé est renommé.

  Dans tous les cas, si le dossier n'existe pas il est créé. Pour qu'un nom soit considéré comme un dossier il doit se finir par le caractère `/` ou `\`.
- unzip : indique s'il faut désarchiver le fichier téléchargé.

Contributions

Il est possible de contribuer à la maintenance de ces fichiers et à l'ajout de nouveaux packages. Il faut demander l'ouverture d'un accès sur la forge ou communiquer sur les listes de discussion.

Pour la création d'un nouveau paquet, voici quelques recommandations.

Convention de nommage

Certaines règles sont à respecter lors de la création d'un nouveau package afin de garder un système unifié et pérenne.

Un package est identifiable par les deux balises suivantes :

- id : identifiant unique de l'application dans WPKG (sensible à la casse) ;
- name : nom de l'application.

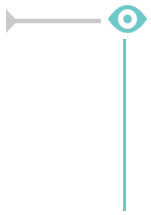
Le champ id est le plus important, il doit respecter les conventions suivantes :

- sans espace ;
- tout en minuscules ;
- sans numéro de version (`firefox` et non `firefox15`).

Tests des packages : check

La plupart des installeurs ajoute une entrée `Uninstall` pour apparaître dans la section `Ajout/Suppression de programmes` de Windows.

On peut utiliser cette clé pour tester la présence d'une application. Mais une clé de registre ne prouve pas qu'une application est réellement présente. Il faut aussi tester l'existence des fichiers de l'application.



```
<check type="uninstall" condition="exists" path="QT Lite %version%" />
<check type="file" condition="exists" path="%progfiles%\QT Lite\QuickTimePlayer.exe" />
```

Validation de la syntaxe XML

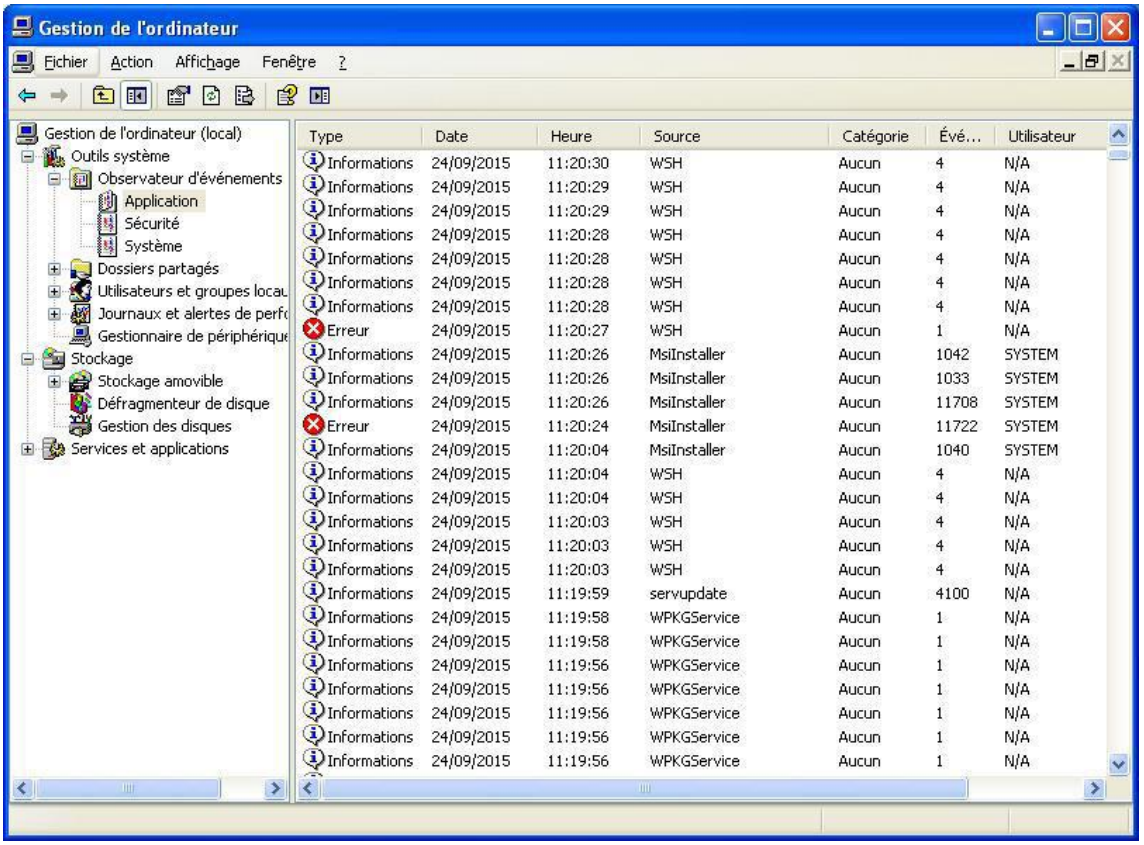
Il est toujours possible de faire une faute de frappe dans un fichier XML, un validateur XML en ligne permet de vérifier la syntaxe XML du fichier : http://xmlvalidation.com/.

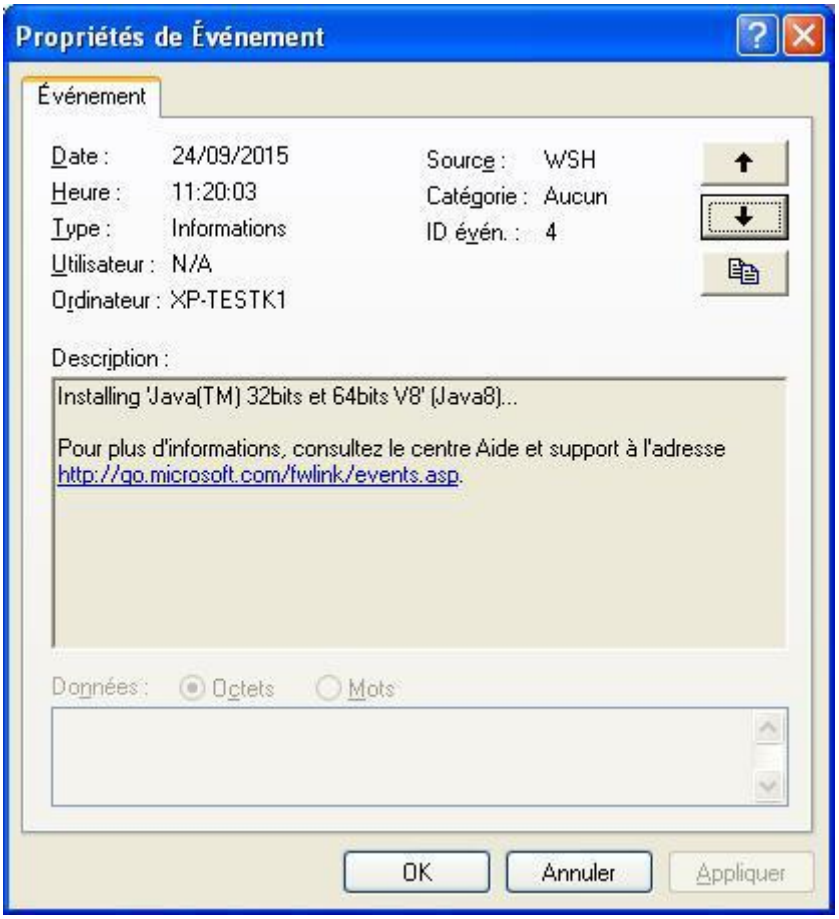
Voir aussi...

WPKG logiciels avec traitement particulier [p.124]

4.3. Journalisation des actions WPKG

Par défaut WPKG journalise ses actions dans l'observateur d'événements Windows, accessible dans la console de gestion de l'ordinateur (Microsoft Management Console) qui s'obtient avec un clic droit sur le `Poste de travail` puis `Gérer` dans le menu contextuel.





Il est possible d'activer le mode debug pour avoir plus d'informations dans la console de gestion de l'ordinateur. Pour se faire il faut passer la variable `Activer le mod`e

> `"debug"` à `oui` dans l'onglet `Wpkg` de l'interface de configuration du module.

Pour corriger les erreurs et les dysfonctionnement d'une application ou simplement pour connaître le détail de ce qu'effectue WPKG, on peut activer la création d'un fichier de journalisation. La quantité d'informations journalisées est paramétrable.

Pour une station particulière

Lors de sa prochaine exécution, WPKG va créer un fichier de log : `C:\wpkg-[HOSTNAME].log`

WPKG Client

- Ouvrir `%PROGRAMFILES%\wpkg\wpkginst.exe` ;
- Dans WPKG parameters renseigner :
  `/synchronize /nonotify /quiet /log_file_path:c: /logLevel:31`
- Sauver à l'aide de l'action `Save` et fermer `wpkginst.exe`.

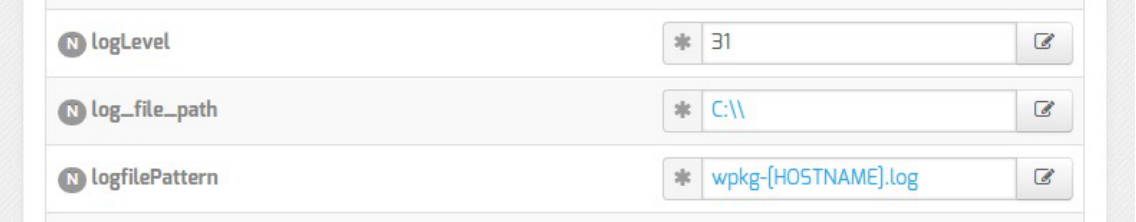
Wpkg-GP

- Ouvrir `%PROGRAMFILES%\wpkg-gp\Wpkg-gp.ini` ;
- À la fin de la ligne commençant par "WpkgCommand =" ajouter :
  `/log_file_path:c: /logLevel:31`
- Sauver et fermer le fichier.

Pour toutes les stations

Sur le serveur il faut utiliser l'interface de configuration du module en mode normal et se rendre dans l'onglet `Wpkg`.

Il faut placer la variable `logLevel` à la valeur 31 et remplir si besoin les variables `log file path` et `logfilePattern`.



Enregistrer et quitter l'interface de configuration du module.

Pour appliquer la configuration il faut reconfigurer le module à l'aide de la commande reconfigure :

```
# reconfigure
```

Par défaut les journaux se trouveront dans `C:\wpkg-<nom-poste>.log`

Granularité des logs

La variable `logLevel` permet d'indiquer le niveau de détails de la journalisation souhaité sous forme d'un nombre.

Ce nombre est le résultat d'une opération de masquage, il faut additionner les valeurs suivantes pour choisir le niveau de journalisation souhaité :

- 0 désactive la journalisation ;
- 1 erreurs ;
- 2 avertissements ;
- 4 informations ;
- 8 audit success ;
- 16 audit failure.

- variable `logLevel` à 31 (1 + 2 + 4 + 8 + 16) → journalise tout
- variable `logLevel` à 3 (1 + 2) → journalise seulement les erreurs et les avertissements

4.4. WPKG scripts de pre et post installation

L'utilisation de dossiers dans un lecteur réseau pour les icônes du Menu Démarrer et du Bureau pose problème avec WPKG.

Une erreur se produit lorsque WPKG installe une application dont l'installeur crée des icônes dans le Menu démarrer et sur le Bureau et qu'une session sur le domaine Scribe est ouverte avant ou pendant l'installation.

Problématique

Voici l'exemple de l'erreur rencontrée à l'installation d'OpenOffice avec WPKG.

```
Type de l'événement : Erreur
Source de l'événement : MsiInstaller
Catégorie de l'événement : Aucun
ID de l'événement : 11327
Date : 08/02/2011
Heure : 11:52:19
Utilisateur : AUTORITE NT\SYSTEM
Ordinateur : POSTE-ADMIN1
Description :
Produit : OpenOffice.org 3.3 -- Erreur 1327.Lecteur R:\ non valide
```

Lors de l'ouverture de session, ESU ré-écrit les chemins d'accès aux dossiers contenant les icônes du "Bureau" et du "Menu Démarrer" en les faisant pointer sur le lecteur `R:`.

Sous Windows il existe 2 type de chemins :

- utilisateur, ces chemins peuvent varier d'un utilisateur à l'autre, on y place les icônes qu'on ne veut rendre visible que pour un groupe donné ("gestion-postes" pour les professeurs par exemple) ;
- machine, ces chemins sont les mêmes pour tous les utilisateurs.

Les chemins utilisateur sont dans HKEY_CURRENT_USER et les chemins machine dans HKEY_LOCAL_MACHINE.

WPKG est exécuté dans le contexte de l'utilisateur BUILTIN\SYSTEM.

Sous Windows (de 2000 et supérieurs) existe la notion d'environnement utilisateur.

Les lecteurs réseaux, par exemple, ne sont disponibles que pour l'utilisateur qui les a connectés.

Ici, le lecteur `R:` n'est accessible que pour l'utilisateur qui a ouvert la session et n'est pas disponible pour l'utilisateur BUILTIN\SYSTEM.

On peut constater le phénomène de visu :

- activer le Bureau à distance sur un poste ;
- ouvrir, sur ce même poste, une session sur le domaine ;
- aller sur un autre poste et ouvrir une session **administrateur local** via une connexion Bureau à distance.

Dans le poste de travail de la session du domaine on voit le lecteur `R:`, il est absent dans la session **administrateur local**.

L'installeur OpenOffice, par défaut, lorsqu'il est exécuté en mode silencieux (comme avec WPKG), veut créer des icônes dans le Menu démarrer.

> Il regarde dans HKEY_LOCAL_MACHINE et trouve `R:\%ESU_GM%\Menu Démarrer`.
>
> S'exécutant dans l'environnement BUILTIN\SYSTEM l'installeur ne trouve donc pas le lecteur `R:` et annule sa procédure d'installation. On peut observer le dossier `%PROGRAMFILES%\OpenOffice\` qui grossi à l'installation et qui disparaît ensuite avec l'annulation de l'installation.

Solutions

Le principe est d'éviter qu'un utilisateur n'ouvre une session pendant l'installation d'un programme et permette à l'installeur de créer des icônes dans HKEY_LOCAL_MACHINE avec des chemins qui pointent vers le lecteur `C:`.

Augmenter le temps de blocage pendant lequel WPKG accède au poste de travail

Il est possible d'allonger le temps maximal pendant lequel WPKG bloque l'accès au poste de travail pendant son exécution, ceci se paramètre dans l'interface de configuration du module, dans l'onglet `Wpkg client` avec la variable `logon-delay`.

Il faut ensuite appliquer la nouvelle configuration sur les clients, voir la section Application de la nouvelle configuration WPKG sur les clients.

#fixme

Le blocage du poste fait apparaître une boîte de dialogue qui affiche "WPKG installe les applications et applique les paramètres..."/"Veuillez patienter et ne pas redémarrer votre ordinateur...".

Scripts de pre et de post-installation

Une deuxième solution consiste à restaurer les chemins par défaut des icônes du Bureau et du Menu démarrer avant l'installation du logiciel et exécuter WPKG à l'arrêt du poste plutôt qu'au démarrage.

Deux scripts permettent de sauvegarder et de restaurer les chemins :

- script de pré-installation va sauvegarder les chemins pour les dossiers d'icônes du Bureau et du Menu Démarrer et placer les chemins par défaut ;
- script de post-installation va restaurer les chemins sauvegardés en pré-installation (facultatif si on exécute WPKG à l'arrêt de la station).

Malgré l'utilisation de ces scripts, il est quand même possible de faire planter l'installation. Il suffit qu'un utilisateur ouvre une session pendant l'installation, juste après le script de pré-installation. À ce moment le chemin pointe quand même vers le lecteur `R:` et l'installation échouera.

Exécuter WPKG lors de l'arrêt de la machine permet d'éviter ce dernier cas de figure. Cela permet aussi d'accéder directement à l'ordinateur plutôt que de devoir attendre l'installation des logiciels.

On peut alors expliquer aux utilisateurs qu'ils peuvent :

- accéder immédiatement au poste avec des logiciels par forcément à jour ;
- redémarrer la machine pour avoir des logiciels à jour si besoin.

Préparation des scripts

Il faut placer les 3 fichiers suivants à la racine du partage `\\scribe\wpkg` :

- `preinstall.bat`
- `postinstall.bat`
- `bureau-menu_demarrer.reg`

Remplacer dans l'exemple suivant ADRESSE_IP_SCRIBE par la valeur correspondante à votre serveur et enregistrer le résultat dans un fichier nommé `preinstall.bat`

```
rem remet les chemins par defaut avant l'installation
regedit /E %WINDIR%\sauv_menu-dem.reg "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explor
Shell Folders"
regedit /S "\\ADRESSE_IP_SCRIBE\wpkg\bureau-menu_demarrer.reg"
```

Copier l'exemple suivant et enregistrer le résultat dans un fichier nommé `postinstall.bat`

```
rem remet les chemins comme ils etaient avant l'installation
regedit /S %WINDIR%\sauv_menu-dem.reg
del /F %WINDIR%\sauv_menu-dem.reg
```

Le fichier `bureau-menu_demarrer.reg` est téléchargeable à l'adresse :
http://dev-eole.ac-dijon.fr/attachments/download/116/bureau-menu_demarrer.reg

Utilisation des scripts `preinstall.bat` et `postinstall.bat`

Deux méthodes sont possibles pour utiliser ces scripts :

- appeler `preinstall.bat` et `postinstall.bat` depuis `<nom_du_package>.xml` dans les balises `<install>` et `<update>`

  Cette méthode présente l'avantage de ne pas avoir à modifier la configuration des clients WPKG mais présente l'inconvénient de devoir les appeler pour chaque application dont l'installeur crée des icônes sur le Bureau et/ou dans le Menu démarrer.

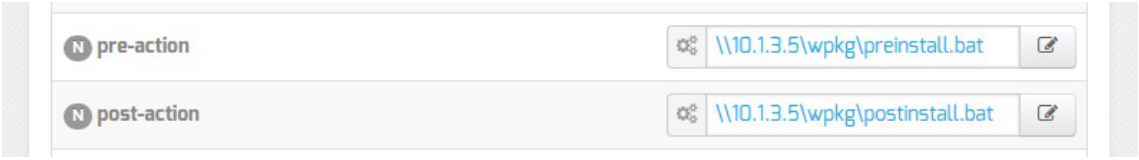
- utiliser les actions `pre-action` et `post-action` de WPKG

  Cette méthode a l'avantage d'être faite une bonne fois pour toute mais demande à mettre la configuration WPKG à jour sur chaque poste.

Configuration des clients WPKG

Il faut modifier la configuration des clients WPKG pour qu'ils exécutent les 2 scripts en pre et post installation, pour cela il faut utiliser l'interface de configuration du module et vérifier dans l'onglet `wpkg`

`client` les chemins des variables `pre-action` et `post-action`.



Il faut également passe la variable `run-on-shutdown` à `YES`.

Ne pas hésiter à augmenter la valeur de la variable `shutdown-delay`.

Principe de fonctionnement des délais dans WPKG :

- s'il n'y a aucune installation ou mise à jour à faire alors l'arrêt est immédiat ;
- s'il y a une installation ou une mise à jour est à faire WPKG exécute les installeurs et attend qu'ils se terminent le temps défini dans la variable `shutdown-delay`. Si le temps est dépassé WPKG force l'arrêt de la station même si l'installation du logiciel n'est pas terminée. Si il reste du temps et que l'installation des logiciels est terminée la station s'éteindra.

Le principe est le même pour `logon-delay` qui est utilisé si WPKG s'exécute au démarrage de la station (`run-on-shutdown` à `NO`).

Application de la nouvelle configuration WPKG sur les clients

Il faut appliquer la nouvelle configuration en exécutant `wpkg_client_update_conf.bat` sur chacun des clients WPKG.

La mise à jour des clients un par un peut paraître fastidieuse, il existe des outils pour faciliter cela :

- Winexe ;
- cliscribe.py.

4.5. WPKG logiciels avec traitement particulier

Java

Sur Windows Vista/Seven il faut décompacter l'installeur Java pour récupérer le `.msi` et les fichiers qui l'accompagnent. Cette manipulation doit être effectuée sur un poste Vista ou supérieur.

Lancer manuellement l'installeur `jre-7uX-windows-XXX.exe` (en double-cliquant dessus).

Une fois que la fenêtre de l'installeur s'affiche, ne cliquer sur aucun bouton. Il faut se rendre dans le menu

`Démarrer` puis `Exécuter` : `%USERPROFILE%\AppData\LocalLow\Oracle\Java\`
Déplacer le dossier `jre1.7.0_XX` qui s'y trouve dans `\\<SERVEUR>\wpkg\softwares\java\`

Si vous avez une version 64bits de Windows, il faut effectuer deux fois cette manipulation. Une fois pour la version i586 et une fois pour la version x64.

4.6. Quelques références

Documentation écrite par la DANE de l'académie de Lyon

WPKG sur un environnement Scribe

http://www2.ac-lyon.fr/serv_ress/mission_tice/wiki/doku.php?id=scribe:wpkg

Documentation écrite par l'académie de la Réunion

WPKG - Généralités

http://tice974.ac-reunion.fr/wiki-administrateurs/doku.php?id=scribe:wpkg:1.principe&ticket=

WPKG - Installation sur un serveur Scribe

http://tice974.ac-reunion.fr/wiki-administrateurs/doku.php?id=scribe:wpkg:2.installation_sur_scribe&ticke

Wpkg-Manage : interface de gestion des packages à installer

http://tice974.ac-reunion.fr/wiki-administrateurs/doku.php?id=scribe:wpkg:3.wpkg_manage

WPKG - Mise à jour des XML et installeurs

http://tice974.ac-reunion.fr/wiki-administrateurs/doku.php?id=scribe:wpkg:4.maj

WPKG - Tests

http://tice974.ac-reunion.fr/wiki-administrateurs/doku.php?id=scribe:wpkg:5.tests

Mise à jour des clients Wpkg-GP (Seven et Windows 8) en version 0.17

http://tice974.ac-reunion.fr/wiki-administrateurs/doku.php?id=scribe:wpkg:6.maj_wpkg_gp

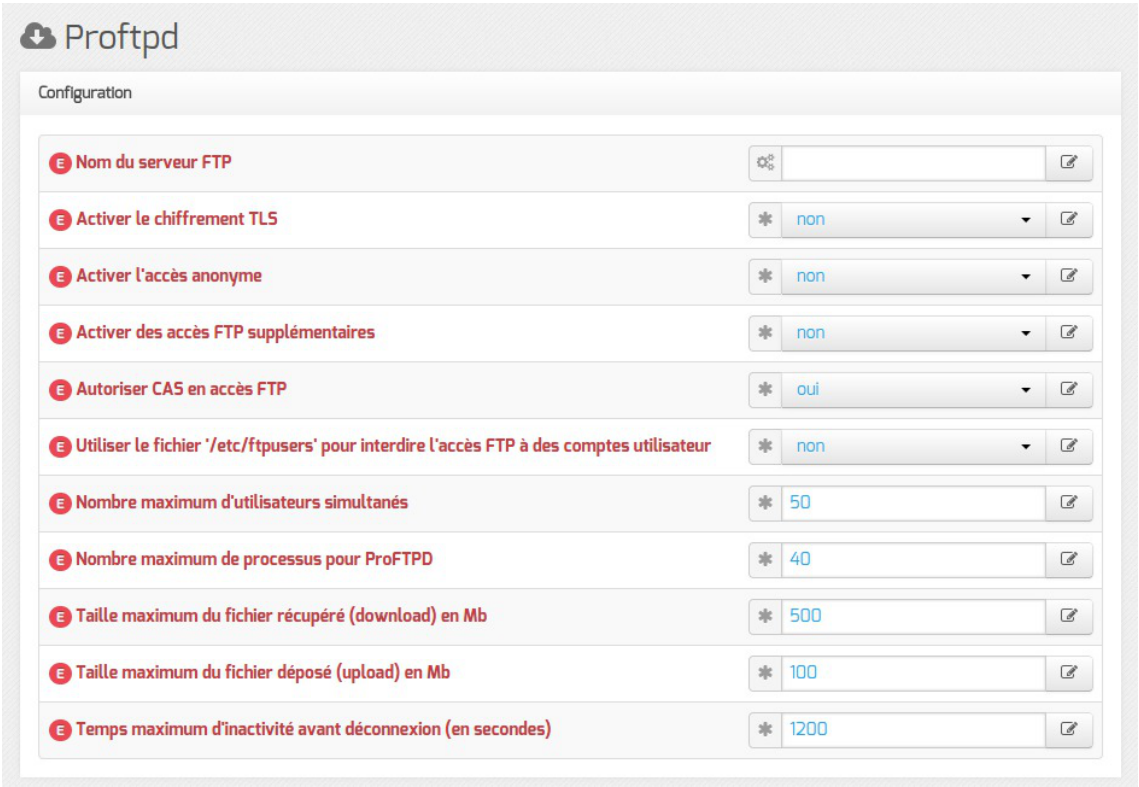
Chapitre 3

Les clients FTP

Les utilisateurs peuvent accéder à leurs données par l'intermédiaire d'un client FTP (gFTP, Filezilla, ...).

Le serveur FTP est activable/désactivable dans l'onglet Services par l'intermédiaire de l'option `Activer l'accès FTP`. Le serveur FTP est basé sur le logiciel libre ProFTPD.
http://www.proftpd.org/

L'onglet Proftpd n'apparaît en mode expert que si le service est activé.



Vue de l'onglet Ftp de l'interface de configuration du module

Paramétrage du serveur ProFTPD

Nom du serveur FTP

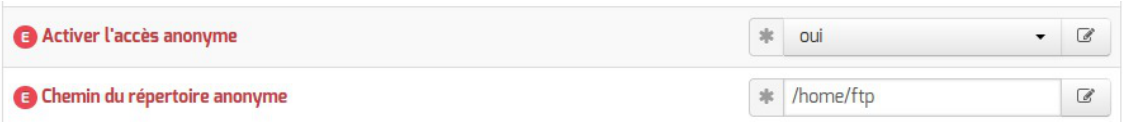
Ce paramètre permet de personnaliser le nom du serveur FTP. Ce nom apparaît lorsqu'on se connecte en FTP sur le serveur avec un client ou en ligne de commande.

Activer le chiffrement TLS

Passer cette option à `oui` permet d'activer le chiffrement TLS mais son utilisation est déconseillée car les échanges réalisés avec du FTP sécurisé ne passent pas ou passent difficilement les pare-feux.

Activer l'accès anonyme

L'accès anonyme permet d'ouvrir l'accès en anonyme sur le répertoire de votre choix.



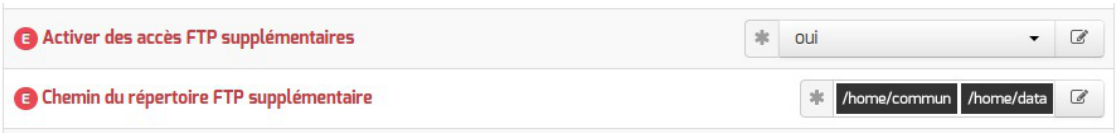
Si la variable est passée à `oui` une nouvelle variable `Chemin du répertoire anonyme` s'affiche, sa valeur est un chemin absolu. Ce répertoire doit être créé manuellement s'il n'existe pas. L'utilisateur `anonymous` peut télécharger depuis le répertoire spécifié, il n'a pas par défaut les droits d'écriture.

Le fichier de configuration contient la directive `<Limit WRITE>` :

```
<Limit WRITE>
DenyAll
</Limit>
```

Activer des accès FTP supplémentaires

L'accès FTP supplémentaire permet d'ouvrir l'accès à des comptes existants sur le répertoire de votre choix.



Si la variable est passée à `oui` une nouvelle variable `Chemin du répertoire FTP supplémentaire` s'affiche, sa valeur est un chemin absolu. Ce répertoire doit être créé manuellement s'il n'existe pas et les droits doivent être ajustés. Les utilisateurs du module peuvent lire et écrire dans le répertoire spécifié.

Autoriser CAS en accès FTP

Cette option doit être activée pour l'utilisation de l'application Pydio sur le serveur.

Utiliser le fichier /etc/ftpusers pour interdire l'accès FTP à des comptes utilisateur

Cette option ajoute la directive `file=/etc/ftpusers` au fichier de configuration `/etc/pam.d/proftpd`.

Le fichier `/etc/ftpusers` contient une liste des utilisateurs qui ne doivent pas se connecter via service FTP. Ce fichier est utilisé non seulement pour l'administration système mais également pour augmenter la sécurité du réseau. Il contient typiquement la liste des utilisateurs qui soit n'ont rien à faire avec le transfert FTP, soit ont trop de privilèges pour être autorisés à se connecter à ce serveur. De tels utilisateurs sont en général `root`, `daemon`, `bin`, `uucp` et `news`.

La liste du fichier `/etc/ftpusers` peut être complétée avec des utilisateurs systèmes ou LDAP dont il faut désactiver l'accès au service FTP.

Attention dans les accès FTP le mot de passe transite en clair sur le réseau.

Nombre maximum d'utilisateurs simultanés

Par défaut à `50` cette variable permet d'ajuster le nombre d'utilisateurs simultanés autorisés à se connecter en FTP.

Nombre maximum de processus pour ProFTPD

Par défaut à `40` cette variable permet d'ajuster le nombre maximum de processus simultanés du logiciel

ProFTPD.

Taille maximum du fichier récupéré (download) en Mb

Par défaut à `500` cette variable permet d'ajuster la taille maximum des fichiers pouvant être téléchargés.

Taille maximum du fichier déposé (upload) en Mb

Par défaut à `100` cette variable permet d'ajuster la taille maximum des fichiers pouvant être déposés.

Temps maximum d'inactivité avant déconnexion (en secondes)

Par défaut à `1200` secondes (20 minutes) cette variable permet d'ajuster le temps d'inactivité avant déconnexion.

Accès FTP

Une fois l'accès FTP activé, il est possible d'accéder au service avec un client FTP (Filezilla, gFTP), par un navigateur web ou avec une application web FTP (Pydio, anciennement Ajaxplorer, sur le module Scribe).

Accès par un navigateur web

Pour accéder aux documents avec un navigateur web il faut préciser le protocole dans l'URL :

`ftp://user@<adresse_serveur>/`

ou

`ftp://<adresse_serveur>/`

Accès par une application web

Pour accéder aux fichiers par l'application web Pydio, il faut l'activer dans l'onglet `Applications web`. Pydio (anciennement Ajaxplorer) n'est pas pré-installé sur le module Horus (il s'installe avec la commande `apt-eole`, voir la documentation sur les applications web). Suite à une reconfiguration du serveur, l'application sera accessible à l'adresse `http://<adresse_serveur>/pydio/` moyennant l'authentification (mire EoleSSO).

Avec un client FTP (en mode passif par défaut) le mode actif doit impérativement être configuré. Dans ce mode c'est le client FTP qui détermine le port de connexion à utiliser.

Anti-virus ClamAV

Si l'anti-virus ClamAV est activé, la recherche de virus en temps réel sur le FTP est activé par défaut. Il est possible de désactiver cette option dans l'onglet `Clamav` en passant `Activer l'anti-virus temps réel sur FTP` à `non`.

Accès au dossier personnel des élèves par FTP

Sur les modules Scribe et AmonEcole, les professeurs n'ont, par défaut, pas accès au dossier personnel de leurs élèves par l'intermédiaire du protocole FTP.

Cette restriction peut être levée en répondant `oui` à la question `Activer l'accès aux dossiers personnels des élèves pour les professeurs` . Cette option diminue légèrement la sécurité du serveur.

Chapitre 4

Les clients Jabber

Jabber, également connu sous le nom de XMPP, est un ensemble de protocoles standards ouverts de l'IETF de messagerie instantanée et de présence, et plus généralement une architecture décentralisée d'échange de données.

Jabber est également un système de collaboration en quasi-temps-réel et d'échange multimédia via Jingle, dont la VoIP (téléphonie sur Internet), la visioconférence et l'échange de fichiers sont des exemples d'applications.

1. Mise en place du serveur jabber

Le service jabber (ejabberd) n'est pas pré-installé sur le module Scribe mais il est pré-packagé en tant que paquet additionnel.

Il faut donc installer le paquet manuellement avec la commande :

```
# apt-eole install eole-ejabberd
```

La configuration du serveur ejabberd peut être personnalisée dans l'onglet Ejabberd de l'interface de configuration du module.

- `Nom de domaine de la messagerie instantanée de l'établissement (ex : monetab.ac-aca.fr)` permet de personnaliser le nom de domaine des adresses de contact XMPP ;
- `Message de bienvenue` permet de personnaliser le message affiché lors de la connexion d'un utilisateur ;
- `Voir les autres utilisateurs sans autorisation préalable` active le module `shared roster ldap` qui permet de mettre en contact des utilisateurs sans entente préalable.

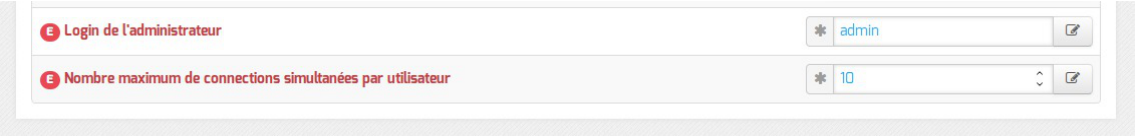
Le service n'est pas disponible immédiatement après l'installation.

L'opération nécessite une reconfiguration du serveur avec la commande reconfigure.

Le service est activé par défaut, il peut être désactivé en répondant `non` à la question `Activer le serveur de messagerie instantanée ejabberd` dans l'onglet Services de l'interface de

configuration du module.

La configuration du serveur ejabberd peut être affinée dans l'onglet `Ejabberd` de l'interface de configuration du module en mode expert.



- `Login de l'administrateur` permet de définir l'utilisateur qui sera administrateur du serveur ejabberd ;
- `Nombre maximum de connections simultanées par utilisateur` permet de limiter le nombre de connexions simultanées par utilisateur.

Vous pouvez vérifier que vous êtes effectivement connecté en lançant la commande suivante sur le serveur :

```
# ejabberdctl connected-users
```

D'autres commandes `ejabberdctl` sont disponibles et documentées avec l'option `help` :

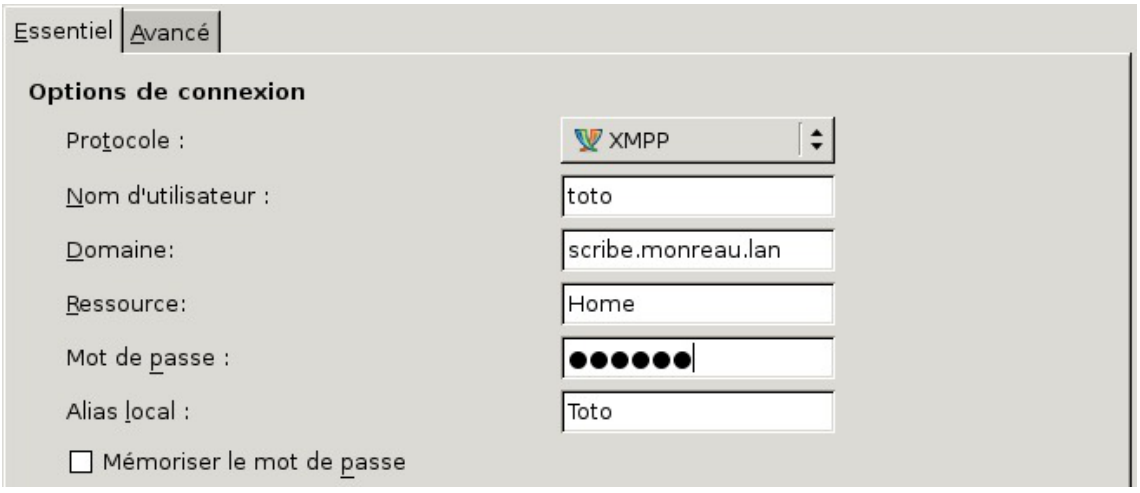
```
root@ejabber:~# ejabberdctl help
```

2. Configuration d'un client

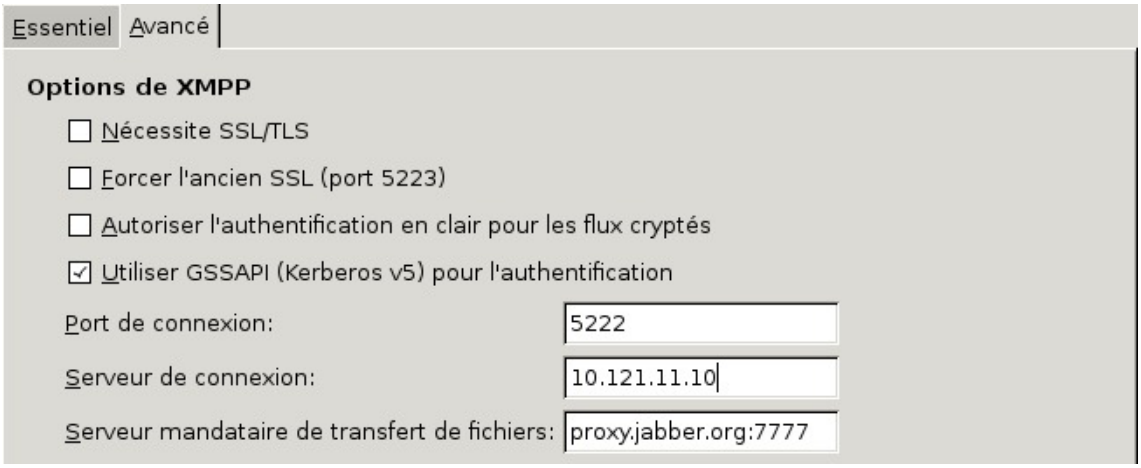
Une fois le service mis en place, il est possible de s'y connecter en utilisant un compte présent dans l'annuaire.

De nombreux logiciels sont compatibles jabberd, les plus connus sont : Pidgin, Gajim, Coccinella et Kopete.

Configuration de Pidgin



Configuration de Pidgin : onglet Essentiel

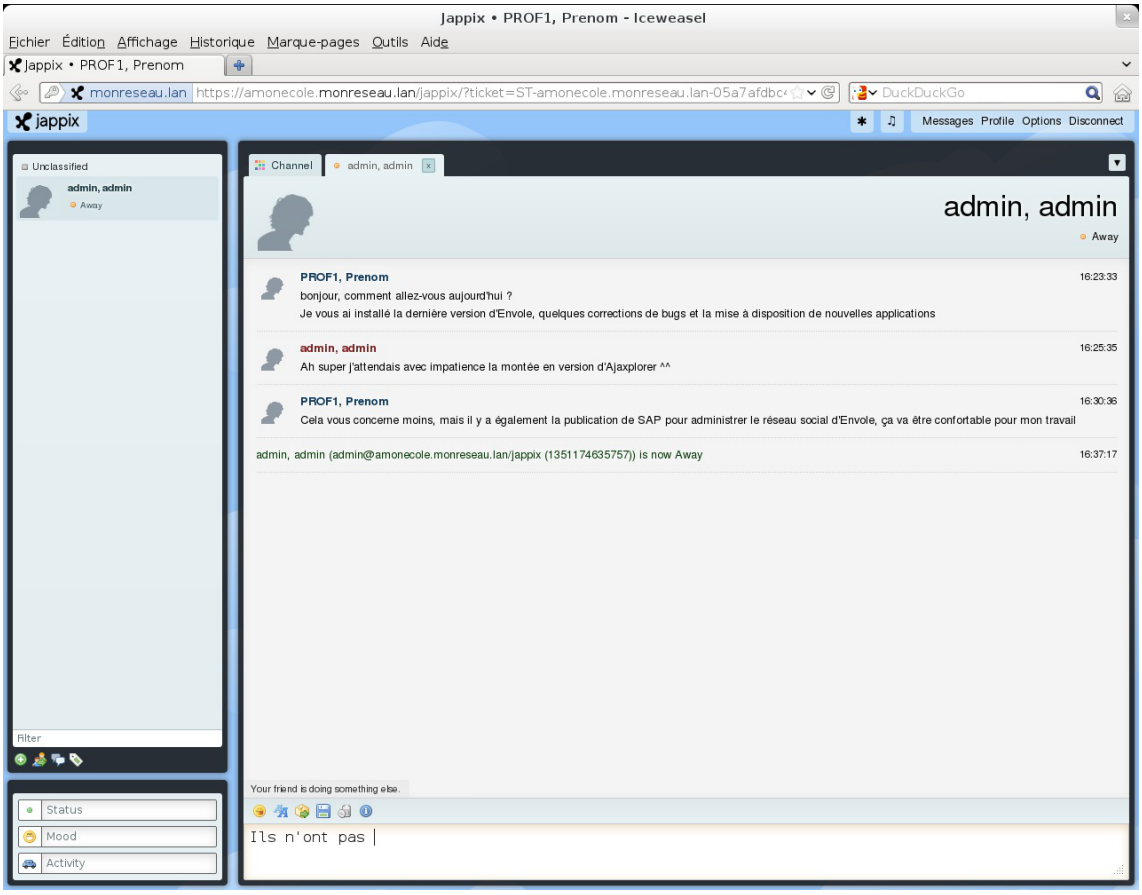


Configuration de Pidgin : onglet Avancé

Il est également possible d'utiliser le client web Jappix sur les modules Scribe et AmonEcole.

3. Jappix : client web Jabber

Présentation



Fenêtre de discussion de Jappix

Jappix est un client web de communication instantanée. Il est libre et basé sur le protocole XMPP[p.144].
Il permet une communication en temps réel entre les personnes possédant un compte XMPP.

Cette communication se fait simplement en utilisant un navigateur web moderne.

Un canal est à disposition pour laisser des messages de statut.

http://jappix.com

Installation

Jappix s'installe manuellement, saisir les commandes suivantes :

```
# Query-Auto
```

```
# apt-eole install eole-jappix
```

L'application n'est pas disponible immédiatement après l'installation.

L'opération nécessite une reconfiguration du serveur avec la commande `reconfigure`.

Si le serveur Jabber n'est pas installé un conteneur supplémentaire doit être créé, il faut donc exécuter la commande `gen_conteneurs` comme le propose la commande reconfigure.

Cette commande doit être suivie de la ré-instanciation du module avec la commande instance :

```
# instance /etc/eole/config.eol
```

L'application nécessite que le service `ejabberd` soit activé.

Dans l'interface de configuration du module, onglet `Services`, mettre `Activer le serveur de messagerie instantanée ejabberd` à `oui`.

L'application est très sensible à la configuration réseau mise en œuvre et son fonctionnement requiert notamment des noms DNS.

La configuration recommandée est donc la suivante :

domain_jabber_etab = eolesso_adresse = web_url = ssl_subjectaltname_ns = "nom_de_domaine"

Si cette configuration n'est pas respectée, l'erreur suivante s'affichera :

```
Erreur » Service indisponible
```

Attention la modification de certains de ces paramètres nécessite de régénérer les certificats.

Pour désactiver rapidement et temporairement (jusqu'au prochain reconfigure) l'application web il est possible d'utiliser la commande suivante :

```
# a2dissite nom de l'application
```

Le nom de l'application à mettre dans la commande est celui que l'on trouve dans le répertoire `/etc/apache2/sites-available/`

Pour activer cette nouvelle configuration il faut recharger la configuration d'Apache avec la commande :

```
# service apache2 reload
```

Pour réactiver l'application avec cette méthode il faut utiliser les commandes suivantes :

```
# a2ensite nom de l'application
```

```
# service apache2 reload
```

Pour désactiver l'application pour une période plus longue voir définitivement, il faut

> désactiver l'application depuis l'interface de configuration du module, dans l'onglet `Applications web`.
> L'opération nécessite une reconfiguration du module avec la commande `reconfigure`.

Accéder à l'application

Pour accéder à l'application se rendre à l'adresse : `http://<adresse serveur>/jappix/`

Rôles des utilisateurs

Tous les utilisateurs présents dans l'annuaire ont un accès à l'application.

Remarques

Par défaut il n'est pas possible de téléverser des fichiers dans le canal car il n'y a pas de gestion des quotas et la partition du conteneur pourrait se remplir très vite :

En attendant, il est tout de même possible d'activer cette fonctionnalité en créant un répertoire accessible en écriture à Apache :

`# ssh reseau`

`# mkdir /usr/share/jappix/store/share`

`# chown www-data:root /usr/share/jappix/store/share`

`ctrl + d` pour sortir de la connexion SSH.

Chapitre 5

Résolution des problèmes du client

1. Problèmes à l'inscription au domaine

Lorsqu'un problème survient pendant l'inscription au domaine ou à l'ouverture de session, plusieurs pistes sont à explorer.

Sur le serveur

Vérifier l'état du serveur avec la commande `diagnose`.

Vérifier la communication avec le client à l'aide de la commande `tcpcheck` :

```
# tcpcheck 2 <IP_station>:139
```


Sur le serveur les commandes doivent être exécutées avec l'utilisateur `root`, soit sur la console soit en SSH.

Sur un client Windows

Vérifier la configuration réseau de la station avec la commande `ipconfig /all`

Vérifier la communication du client avec le serveur avec les commandes :

```
ping <adresse_module>
nbtstat -A <adresse_module>
```

2. Problèmes avec le Client Scribe

Le client Scribe enregistre ses actions dans les fichiers :

- %WINDIR%\cliscribe.log
- %WINDIR%\cliscribe_logon.log
- %WINDIR%\cliscribe_updater.log
- %TMP%\cliscribe_utilisateur-<login>.log

Ces fichiers peuvent être utilisés pour vérifier l'exécution du client Scribe et détecter d'éventuelles erreurs. Le niveau de verbosité est renseigné dans la base de registre sous : `HKEY_LOCAL_MACHINE\Software\Eole\Scribe` : "log_level".

Le niveau de verbosité peut être paramétré dans la console ESU `Domaine => Groupe de machine => "Client Scribe" => "Activer le mode debug du client"`.

Ce sont les valeurs du module *logging* de *Python* qui sont utilisées :

- CRITICAL

- ERROR
- WARNING
- INFO
- DEBUG

Lorsque le niveau de journalisation (`HKEY_LOCAL_MACHINE\Software\Eole\Scribe` : " `log_level` ") est placé sur "**debug**" la fenêtre de mise à jour reste ouverte 40 secondes en cas d'avertissement ("warning") ou d'erreur ("error").

Les "traceback"

Le client Scribe ainsi que l'application *Gestion-postes* peuvent générer des erreurs en cas de problème.

Ces erreurs peuvent contenir le mot "**traceback**". Il s'agit de la pile d'appel (dernières instructions du programme) ayant conduit à cette erreur. Cela permet de retrouver plus rapidement la cause du problème.

Si vous rencontrez une telle erreur et que vous ne savez pas l'interpréter, pensez à joindre le contenu du traceback à votre demande (copie d'écran d'un popup ou fichier de log).

Le fichier de logon

Lors de l'ouverture de session, le client Scribe lit le fichier de logon de l'utilisateur.

Ce fichier se trouve sur le serveur dans le partage `\\scribe\netlogon`.

Le nom du fichier se compose du login et du système d'exploitation avec lequel l'utilisateur se connecte, par exemple : `adminWinXP.txt`.

En cas de problème de génération du fichier de logon il peut être utile de tester sa création manuellement, pour ce faire il faut exécuter la commande suivante :

```
/usr/share/eole/fichier/dyn-logon.py -u <login> -o <type_os> -m <nom machine win> -i <ip machine win>
```

où :

- <login> est login dont le fichier logon pose problème
- <type_os> : Win2K, WinXP, Vista, Win2K3
- <nom_machine_win> : le nom de la machine Windows
- <ip_machine_win> : l'IP de la machine Windows

Les erreurs sur le client

Lorsque le client affiche une erreur elle ne s'est pas forcément produite sur le client.

En effet, lorsque le client se connecte au serveur, le résultat de l'ensemble des actions exécutées sur le serveur est renvoyé au client, y compris les erreurs.

Un "traceback" peut donc contenir une pile d'appel d'un programme se trouvant sur le serveur.

Les fichiers de journalisation (log) du serveur contiendront alors une copie de l'erreur.

Pour tester la communication du serveur avec le client, faire sur le serveur :

```
tcpcheck 2 <ip station>:8788
```

3. Problèmes Controle-vnc

C'est le service sur le serveur Scribe qui communique avec le *service client Scribe* installé sur les clients Windows. Il applique la configuration ESU et gère entre autre le blocage et la distribution de devoirs.

Son fichier de journalisation (log) est `/var/log/controle-vnc/main.log`. Pensez à l'examiner lorsque vous rencontrez des problèmes sur le client (traceback par exemple).

4. Problèmes de droits sur les répertoires partagés

Si des dysfonctionnements persistent et qu'ils semblent causés par des répertoires manquants dans les partages ou des problèmes de droits d'accès, il est possible de réinitialiser les droits à l'aide des utilitaires `droits_user.py` et `droits_partage.sh`.

droits_user.py

La commande `/usr/share/eole/backend/droits_user.py` vérifie la présence des répertoires personnels des utilisateurs (y compris le sous-dossier `prive` des élèves) et leur ré-applique les droits par défaut.

Dans sa dernière version (Scribe>=2.5.1), il est possible d'exécuter ce script pour un utilisateur donné en précisant son login en tant que paramètre du script : `/usr/share/eole/backend/droits_user.py toto`

droits_partage.sh

La commande `/usr/share/eole/backend/droits_partage.sh` vérifie la présence des répertoires partagés (y compris les sous-dossiers `donnees` et `travail` pour les classes et les groupes) et leur ré-applique les droits par défaut.

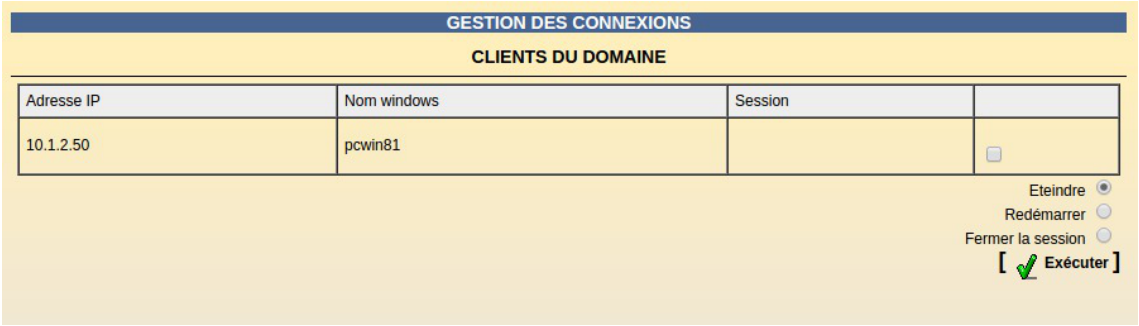
Dans sa dernière version (Scribe>=2.5.1), il est possible d'exécuter ce script pour un groupe donné en précisant son nom en tant que paramètre du script : `/usr/share/eole/backend/droits_user.py 3eme1`

Chapitre 6

Gestion des machines

Gestion des clients du domaine

Le menu `Outils/Stations/Machines` permet d'obtenir la liste des machines démarrées ayant un client Scribe Windows installé et d'agir sur celles-ci.



Les postes de la liste peuvent être éteints ou redémarrés.

Il est également possible de forcer la fermeture de la session de l'utilisateur connecté sur ces postes.

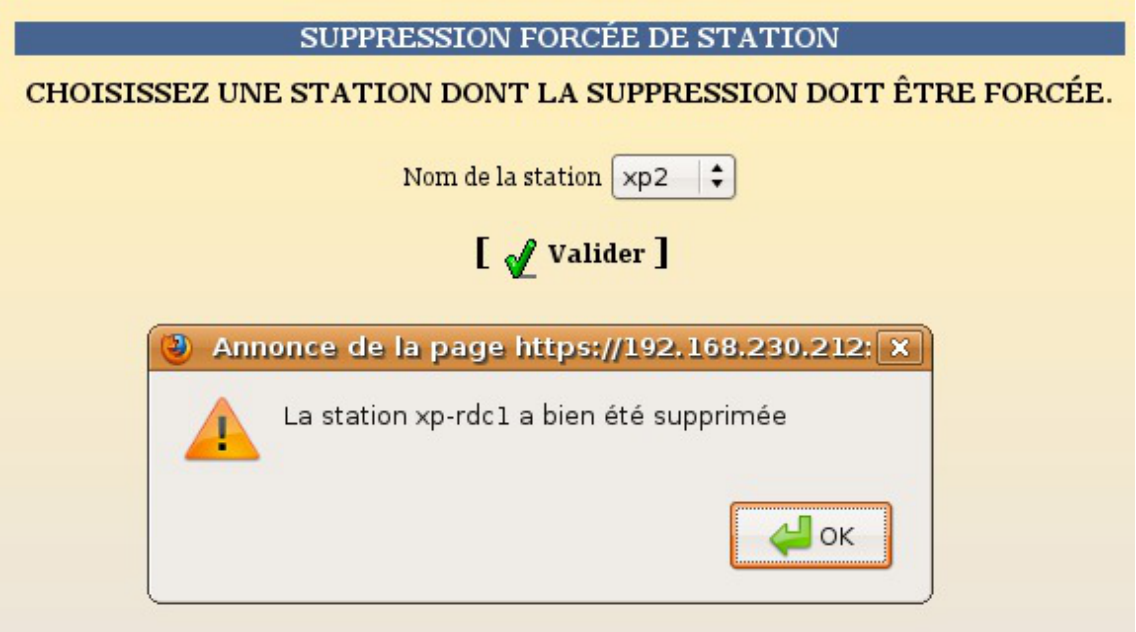
Ces actions sont forcées, si une session est ouverte, le travail de l'utilisateur **NE sera PAS sauvegardé** et la **fermeture des applications forcée**.

D'autres options d'affichage étaient proposées avant l'arrêt du support de Windows XP. Elles sont incompatibles avec les dernières version de Windows et ont été supprimées à partir de la version 2.5.2 d'EOLE :

- "Maîtres explorateurs" : liste des maîtres explorateurs appartenant à un groupe de travail spécifique ;
- "Contrôleur de domaine" : liste des contrôleurs du domaine avec le nom du domaine qu'il contrôle ;
- "Toutes les stations" : liste toutes les machines présentes dans les propositions précédentes.

Suppression d'une machine

Le menu `Outils/Stations/suppression de la station` permet de consulter la liste des stations Windows enregistrées dans l'annuaire et, si nécessaire, de supprimer l'un de ces comptes de machine.



Suppression d'une machine dans l'EAD Scribe

La ré-inscription d'une station dans le domaine (formatage et réinstallation d'une machine avec un nom identique) peut parfois renvoyer une erreur.

La suppression du compte de la station peut aider à résoudre le problème.

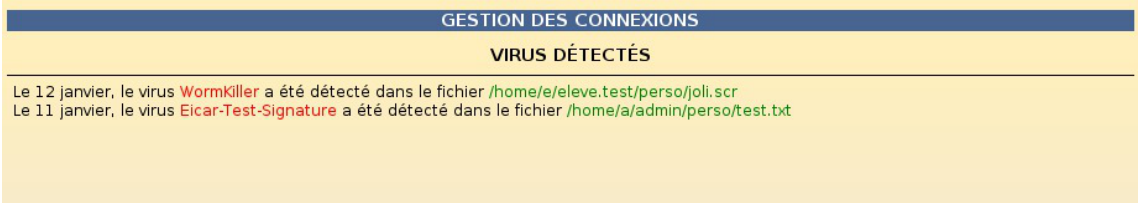
Chapitre 7

Observation des virus

Le menu `Outils/Détection de virus` de l'EAD permet de consulter les fichiers infectés détectés et mis en quarantaine par le serveur.

Il s'agit uniquement de fichiers qui ont été copiés dans l'un des répertoires partagés du serveur.

Chaque ligne indique la date, le nom du virus et le chemin du fichier infecté.



Affichage des virus détectés dans l'EAD

Lorsqu'un virus est détecté, il est renommé avec le préfixe `.virus:` et devient masqué pour l'utilisateur.

L'antivirus protège aussi le serveur de messagerie. Il ne protège par contre pas les stations.

Il est plus prudent, voire indispensable, suivant le système d'exploitation d'installer un anti-virus sur les stations clientes.

La détection des virus n'a lieu que si le module es configuré de la façon suivante :

- onglet `Services` : `Activer l'anti-virus ClamAV` à `oui`
- onglet `Clamav` : `Activer l'anti-virus temps réel sur SMB` à `oui`

Glossaire

adresse MAC *= Media Access Control*	Une adresse MAC, parfois nommée adresse physique, est un identifiant physique stocké dans une carte réseau ou une interface réseau similaire. À moins qu'elle n'ait été modifiée par l'utilisateur, elle est unique au monde. Toutes les cartes réseau ont une adresse MAC, même celles contenues dans les PC et autres appareils connectés (tablette tactile, smartphone,consoles de jeux). Une adresse MAC est généralement représentée sous la forme hexadécimale en séparant les octets par un double point. Par exemple 5E:FF:56:A2:AF:15. Source Wikipédia : http://fr.wikipedia.org/wiki/Adresse MAC
BIOS *= Basic Input Output System*	Le BIOS est un ensemble de fonctions contenu dans une mémoire morte (ROM) de la carte mère d'un ordinateur. Cette mémoire permet à l'ordinateur d'effectuer des opérations élémentaires lors de sa mise sous tension. Le BIOS comprend entre autres : • un logiciel nécessaire à l'amorçage de l'ordinateur ; • le prise en charge bas niveau des communications avec les périphériques ; • des outils de diagnostic.
ESU *= Environnements Sécurisés des Utilisateurs*	Environnement Sécurisé des Utilisateurs (ESU) est un projet initialement développé par Olivier Adams du CRDP de Bretagne qui est maintenant publié par EOLE et distribué sous licence CeCILL. Cet outil permet aux administrateurs de réseaux en établissement scolaire de définir (très simplement) les fonctions laissées disponibles aux utilisateurs des postes informatiques. ESU propose de nombreuses fonctions : • limitation des accès aux paramètres de Windows (panneau de configuration...) ; • définition par salle ou par poste des lecteurs réseaux, icônes du bureau, menu démarrer et limitation des fonctions ; • configuration des imprimantes partagées sur les postes ; • configuration des navigateurs (Internet Explorer et Mozilla Firefox) ; • éditeur de règles permettant de rajouter autant de règles que vous le souhaitez.

Kerberos	Kerberos est un protocole d'authentification réseau qui repose sur un mécanisme de clés secrètes (chiffrement symétrique) et l'utilisation de tickets, et non de mots de passe en clair, évitant ainsi le risque d'interception frauduleuse des mots de passe des utilisateurs. Source Wikipédia : http://fr.wikipedia.org/wiki/Kerberos_(protocole)
LDAP *= Lightweight Directory Access Protocol*	À l'origine un protocole permettant l'interrogation et la modification des services d'annuaire, LDAP a évolué pour représenter une norme pour les systèmes d'annuaires.
NFS *= Network File System*	NFS est est un protocole développé par Sun Microsystems qui permet à un ordinateur d'accéder à des fichiers via un réseau. Ce système de fichiers en réseau permet de partager des données principalement entre systèmes UNIX. Des implémentations existent pour Macintosh et Microsoft Windows. NFS est compatible avec IPv6 sur la plupart des systèmes.
NIS *= Network Information Service*	Network Information Service nommé aussi Yellow Pages est un protocole client serveur développé par Sun permettant la centralisation d'informations sur un réseau UNIX. Son but est de distribuer sur un réseau les informations contenues dans des fichiers de configuration contenant par exemple les noms d'hôte (/etc/hosts), les comptes utilisateurs (/etc/passwd), etc. Un serveur NIS stocke et distribue donc les informations administratives du réseau, qui se comporte ainsi comme un ensemble cohérent de comptes utilisateurs, groupes, machines, etc. Source Wikipédia : http://fr.wikipedia.org/wiki/Network_Information_Service
PAM *= Pluggable Authentication Modules*	PAM est un mécanisme permettant d'intégrer différents schémas d'authentification de bas niveau dans une API de haut niveau, permettant de ce fait de rendre indépendants du schéma les logiciels réclamant une authentification. PAM est une création de Sun Microsystems et est supporté en 2006 sur les architectures Solaris, Linux, FreeBSD, NetBSD, AIX et HP-UX. L'administrateur système peut alors définir une stratégie d'authentification sans devoir recompiler des programmes d'authentification. PAM permet de contrôler la manière dont les modules sont enfichés dans les programmes en modifiant un fichier de configuration. Les programmes qui donnent aux utilisateurs un accès à des privilèges doivent être capables de les authentifier. Lorsque vous vous connectez sur le système, vous indiquez votre nom et votre mot de passe. Le processus de connexion vérifie que vous êtes bien la personne que vous prétendez être. Il existe d'autres formes d'authentification que l'utilisation des mots de passe, qui peuvent d'ailleurs êtres stockés sous différentes formes.

Scannedonly	Scannedonly est composé d'un module VFS (Virtual File System) Samba et d'un service d'exploration qui garantissent que seuls les fichiers qui ont été scannés pour les virus sont visibles et accessibles à l'utilisateur final. http://olivier.sessink.nl/scannedonly/
SMB	Le protocole SMB permet le partage de ressources (fichiers et imprimantes) sur des réseaux locaux avec des PC équipés d'un système d'exploitation Windows.
UAC *= User Account Control*	UAC, contrôle du compte de l'utilisateur en français est un mécanisme de protection des données introduit dans les systèmes d'exploitations Windows Vista et 7. UAC est aussi connu sous ses dénominations précédentes durant le développement de Windows Vista, à savoir UAP (User Account Protection) et LUP (Least User Privilege). Ce mécanisme permet d'exécuter par défaut les programmes avec des droits restreints, évitant ainsi que des applications puissent tourner avec des droits administratifs, qui permettraient de modifier la sécurité du système d'exploitation.
UNC *= Universal Naming Convention ou Uniform Naming Convention*	UNC est une convention sur une manière de définir l'adresse d'une ressource sur un réseau. Plutôt que de spécifier une lettre de lecteur et un chemin d'accès (par exemple, `D:\lecteur`), on utilise la syntaxe suivante `\\serveur\partage\répertoire\nomFichier`
VNC *= Virtual Network Computing*	VNC est un système de visualisation et de contrôle de l'environnement de bureau d'un ordinateur distant. Il permet au logiciel client VNC de transmettre les information de saisie du clavier et de la souris à l'ordinateur distant, possédant un logiciel serveur VNC à travers un réseau informatique. Il utilise le protocole RFB pour les communications.
Wake on Lan *= WoL*	Wake on Lan est un standard des réseaux Ethernet qui permet à un ordinateur éteint d'être démarré à distance. Source Wikipédia : http://fr.wikipedia.org/wiki/Wake-on-LAN
WINS *= Windows Internet Name Service*	WINS est un serveur de noms et services pour les ordinateurs utilisant NetBIOS.

WPKG	WPKG est un logiciel de déploiement, de mise à jour et de suppression automatisés des paquetages pour Windows. Il peut être utilisé pour pousser/tirer des paquetages logiciels tels que des Services Packs, des hotfix, ou des programmes d'installation depuis un serveur central (par exemple Samba ou Active Directory). Il peut être lancé en tant que service, afin d'installer des logiciels en tâche de fond, sans interaction avec l'utilisateur. Configuré comme tel, il peut fonctionner même si l'utilisateur qui ouvre la session ne bénéficie pas de privilèges administrateur. WPKG peut installer des paquetages MSI, Installshield, Packagesfortheweb, Inno Setup, Nullsoft, ainsi que tous les autres installateurs de programme et aussi des scripts. Source Wikipédia : http://fr.wikipedia.org/wiki/Wpkg
XMPP *= Extensible Messaging and Presence Protocol*	XMPP peut être traduit par « Protocole extensible de présence et de messagerie »), et est un ensemble de protocoles standards ouverts de l'Internet Engineering Task Force (IETF) pour la messagerie instantanée, et plus généralement une architecture décentralisée d'échange de données. XMPP est également un système de collaboration en quasi-temps-réel et d'échange multimédia via le protocole Jingle, dont la Voix sur réseau IP (téléphonie sur Internet), la visioconférence et l'échange de fichiers sont des exemples d'applications. XMPP est constitué d'un protocole TCP/IP basé sur une architecture client-serveur permettant les échanges décentralisés de messages instantanés ou non, entre clients, au format Extensible Markup Language (XML). XMPP est en développement constant et ouvert au sein de l'IETF.