

Projet BackupPC

pingouin lol Lien pour [syntaxe DokuWiki](#)

Installation et configuration de BackupPC :

Installation

BackupPC

Après avoir installé Ubuntu, il faut rafraîchir la liste des paquets disponibles puis installer BackupPC et toutes ses dépendances. Il faut répondre non quand l'installateur nous demande d'installer un serveur mail. Il est inutile de noter le mot de passe généré pour l'utilisateur « backuppc » car il sera changé après.

Pour changer ce mot de passe, exécutez

```
# htpasswd /etc/backuppc/htpasswd backuppc
```

Choisissez votre mot de passe et confirmez-le.

Désormais l'interface de configuration de backuppc est accessible avec l'identifiant « backuppc » et le mot de passe défini précédemment, à l'adresse « http://ip_serveur/backuppc ».

On pourra passer l'interface en Français dans le menu « Edit Config → CGI ».

Un disque différent de celui hébergeant le système sera utilisé pour stocker les données. Il faut monter ce disque sous « /backuppc ». Par défaut, BackupPC stocke les données sous « /var/lib/backuppc ». Pour des raisons de sécurité (si la configuration de BackupPC est écrasée), nous allons laisser ce répertoire de sauvegarde dans cette configuration mais déporter le stockage des données au moyen d'un lien symbolique

```
# sudo rsync -va /var/lib/backuppc /backuppc/
```

Ici, on copie les données de BackupPC dans le nouveau dossier de stockage, en conservant les droits sur les fichiers et les dossiers

On supprime « /var/lib/backuppc » : `# rm -rf /var/lib/backuppc/`

On crée le lien symbolique permettant de ne pas changer la configuration de BackupPC :

```
# ln -s /backuppc /var/lib/backuppc/
```

Enfin, on déclare backuppc comme utilisateur et groupe propriétaire de ce lien :

```
# chown -Rh backuppc:backuppc /var/lib/backuppc/
```

SSH

Génération de clefs SSH (RSA)

Il faut générer une paire de clefs pour pouvoir sauvegarder les stations. On se connecte en tant que backuppc :

```
# sudo -i -u backuppc
```

Puis on génère une paire de clefs RSA de longueur 4096 bits :

```
$ ssh-keygen -t rsa -b 4096
```

Ces clefs seront stockées dans “ /backuppc/.ssh/ ”.

Configuration

Coté serveur

Différentes méthodes seront présentées, selon le système à sauvegarder (UNIX libre, Windows ou OSX).

Il faut modifier la configuration de BackupPC via l'interface Web afin d'ajouter notre client à la liste des stations à sauvegarder et définir les commandes de sauvegarde :

Serveur → Modifier les machines → Machines : ajouter @IP_Client. Le champ “ utilisateurs ” indique le nom d'utilisateur qui aura accès à l'interface Web. Il faudra affecter un mot de passe à l'utilisateur avec la commande :

```
# htpasswd /etc/backuppc/htpasswd utilisateur
```



Hôtes

Choisissez un hôte... ▾

Chercher

Serveur

État

- [Bilan des machines](#)
- [Modifier la configuration](#)
- [Modifier les machines](#)
- [Options d'administration](#)
- [Fichier journal](#)
- [Vieux journaux](#)
- [Résumé des courriels](#)
- [Files actuelles](#)
- [Documentation](#)
- [Wiki](#)
- [SourceForge](#)

Éditeur de configuration

Sauvegarder

[Horaire](#) [Xfer](#) [Courriel](#) [Serveur](#) [Paramètres de sauvegarde](#) [Machines](#) [CGI](#)

Machines

	host	dhcp user	moreUsers
Détruire	148.60.210.222	<input type="checkbox"/> flavien	
Détruire	148.60.210.69	<input type="checkbox"/> windows	
Ajouter			

Hosts

Hosts

host
 148.60.210.222 | | flavien | || Détruire | 148.60.210.69 | | windows | |
| Ajouter | | | | |

Hosts

Pour ajouter une machine, choisissez Ajouter et entrez ensuite le nom. Pour faire une copie de la configuration d'une autre machine, entrez le nom de la machine comme NOUVEAU=ACOPIER. Cela va écraser toute configuration par défaut pour cette machine. Vous pouvez aussi faire cela pour une machine existante. Pour détruire une machine cliquer sur le bouton Détruire. Les ajouts, destructions et modifications ne prennent effet que lorsque que vous cliquez sur le bouton Sauvegarder. Aucune des sauvegardes des machines ne sera détruite, donc si vous effacez une machine par erreur, créez-la à nouveau. Pour détruire les sauvegardes d'une machine, vous devez effacer les fichiers manuellement dans /var/lib/backuppc/pc/HOST

UNIX libre

Dans le menu " Hôtes " en haut à gauche : choisir @IP_Client dans la liste. Modifier la configuration → xfer → XferMethod : choisir " rsync ". Sauvegarder. Il faut renseigner le dossier racine à sauvegarder. L'utilisateur " backup " doit avoir un accès en lecture à ce dossier et à son contenu.

[Xfer](#) [Horaire](#) [Courriel](#) [Paramètres de sauvegarde](#)

Paramètres des transferts

[XferMethod](#)
 Écraser rsync ▾

[XferLogLevel](#)
 Écraser 1

[ClientCharset](#)
 Écraser

[ClientCharsetLegacy](#)
 Écraser iso-8859-1

[RsyncShareName](#)
 Écraser Insérer /var/backups/test-backup
Ajouter

[RsyncCsumCacheVerifyProb](#)
 Écraser 0.01

Inclure/Exclure

[BackupFilesOnly](#)
 Écraser Nouvelle clé: Ajouter

[BackupFilesExclude](#)
 Écraser Nouvelle clé: Ajouter

[RsyncClientPath](#)
 Écraser /usr/bin/rsync

[RsyncClientCmd](#)
 Écraser \$sshPath -q -x -l backup 148.60.210.222 /usr/bin/s

[RsyncClientRestoreCmd](#)
 Écraser \$sshPath -q -x -l backup 148.60.210.222 /usr/bin/s

Onglet Xfert → pour rsync → chapitre Chemins/Commandes/Args Rsync indiquer pour " RsyncClientCmd " : " \$sshPath -q -x -l backup @IP_Client /usr/bin/sudo \$rsyncPath \$argList+ ". pour " RsyncClientRestoreCmd " : " \$sshPath -q -x -l backup @IP_Client /usr/bin/sudo \$rsyncPath \$argList+ ".

Enfin il faut copier la clef publique (id_rsa.pub) précédemment générée dans " ~/.ssh/authorized_keys ". Si tout a bien été configuré, on peut se connecter en SSH au client depuis le serveur

ssh backup@IP_Client

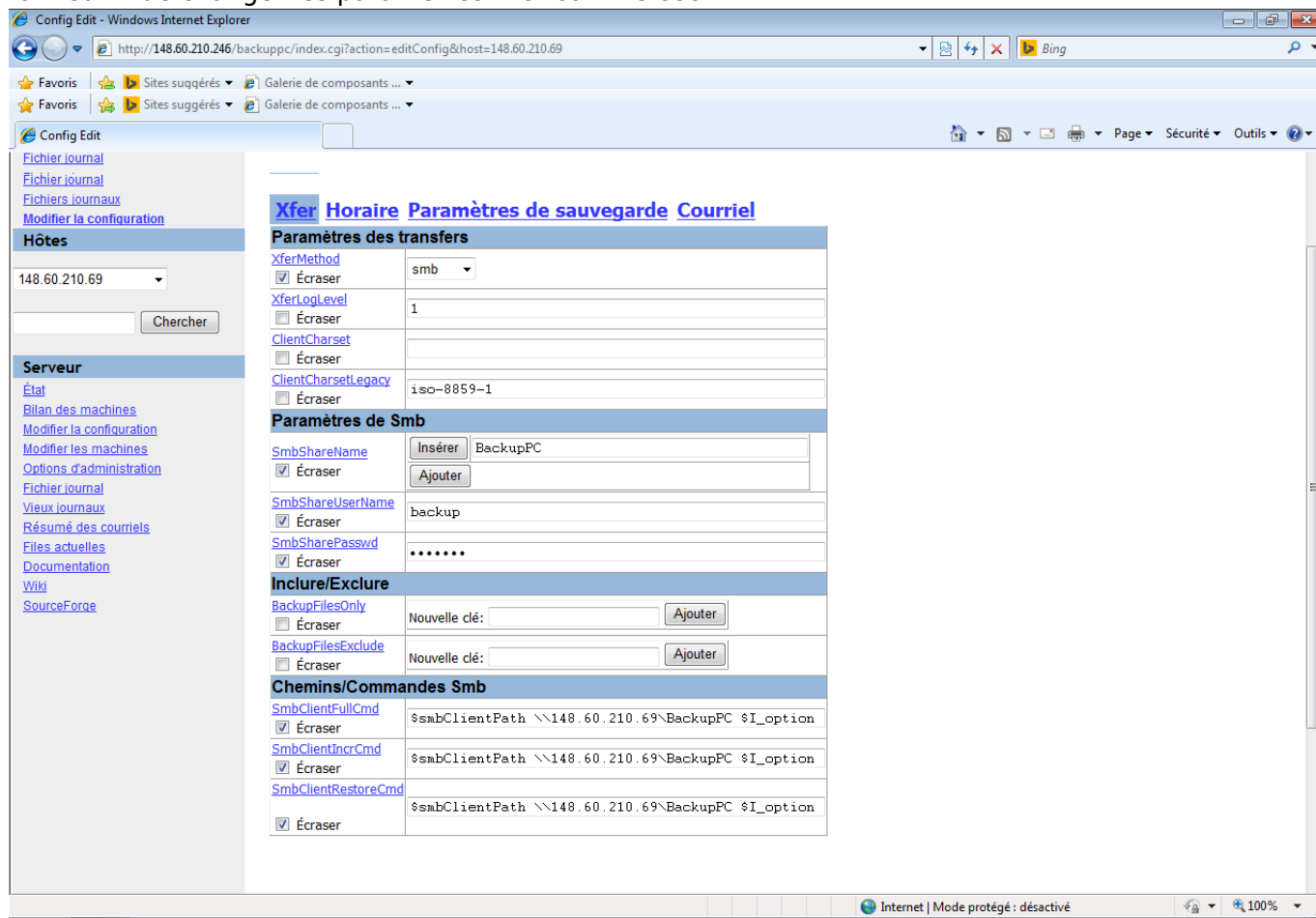
Cette commande doit être lancée en tant que " backuppc " .

Windows

Ici il est possible d'utiliser deux méthodes. Soit on utilise le système classique de partage de fichiers Windows mais les échanges ne seront pas chiffrés, soit on utilise Cygwin pour avoir un environnement UNIX permettant l'utilisation de SSH et donc de chiffrer les échanges.

SMB

Ici il suffit de changer les paramètres Xfer comme ceci :



où le mot de passe smb est le mot de passe défini à la création de l'utilisateur backup.

Cygwin

La configuration du serveur est identique à celle pour les postes UNIX libres. Il faut simplement rajouter ".exe" au nom de la commande rsync et supprimer "/usr/bin/sudo" dans les commandes.

OSX

Coté client

De même la configuration dépend du système.

UNIX libre

Le compte utilisé sur les machines UNIX clientes sera le compte " backup ", présent par défaut sous Ubuntu. Il faudra le créer s'il n'existe pas. On crée le dossier ".ssh" dans le dossier personnel de " backup " sur le client. Enfin, il faut définir " backup " comme utilisateur et groupe propriétaire du dossier ".ssh". Il faut maintenant modifier la configuration du serveur SSH (/etc/ssh/sshd_config) côté client (à installer s'il n'est pas présent). Passer la directive " PermitRootLogin " à no ; Desactive le login root par ssh "PasswordAuthentication no " Desactive l'authentification par mot de passe : seule l'authentification par clefs sera autorisée. Il ne reste plus qu'à modifier la configuration de sudo afin de restreindre son usage à la commande rsync pour l'utilisateur " backup " :

```
#visudo /etc/sudoers
```

Ajouter la ligne : " backup ALL=NOPASSWD: /usr/bin/rsync ".

Windows

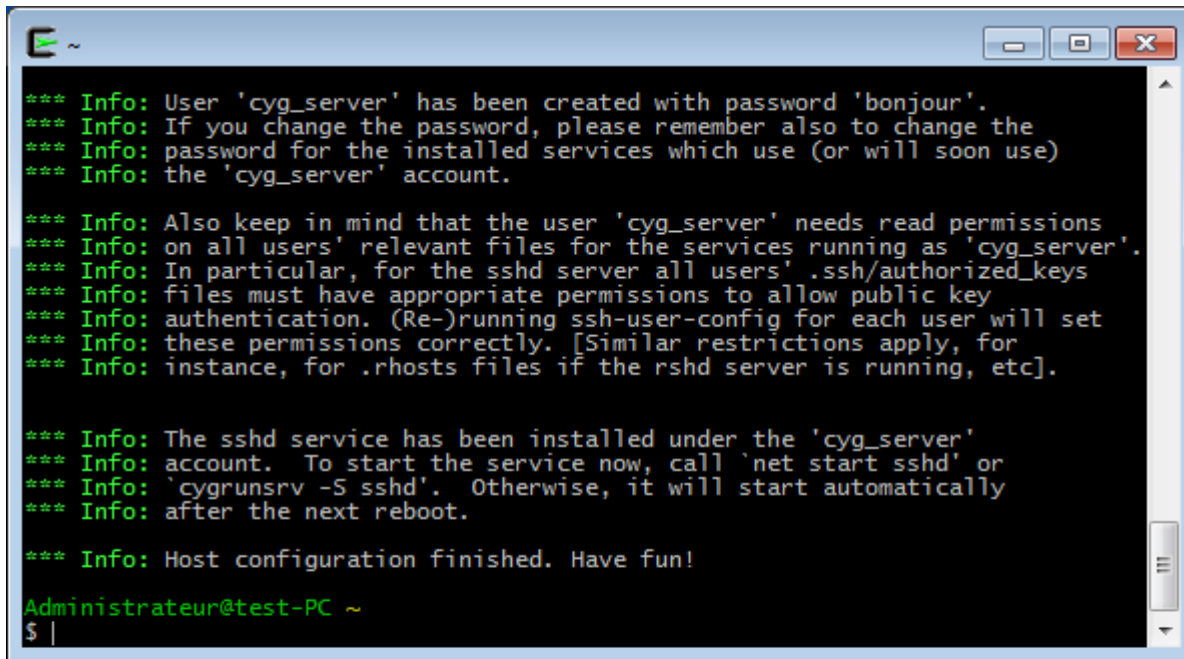
Cygwin

Il faut télécharger l'installateur de Cygwin sur le site officiel. Ensuite il faut le lancer puis laisser tous les paramètres par défaut (on choisira un dépôt dans la liste). Il faut choisir les paquets OpenSSH et rsync dans la liste des logiciels à installer

puis terminer l'installation. On clique sur l'icône Cygwin présente sur le bureau afin de configurer la station pour la sauvegarde. Rentrer la commande :

```
#ssh-host-config
```

Répondre " yes " aux quatre premières questions, faire entrée pour la valeur de Cygwin ; répondre no puis yes. Choisir un mot de passe pour l'utilisateur.

A screenshot of a Cygwin terminal window. The window title is "Cygwin" and it has standard Windows window controls (minimize, maximize, close). The terminal output shows several informational messages: 1. "User 'cyg_server' has been created with password 'bonjour'." 2. "If you change the password, please remember also to change the password for the installed services which use (or will soon use) the 'cyg_server' account." 3. "Also keep in mind that the user 'cyg_server' needs read permissions on all users' relevant files for the services running as 'cyg_server'." 4. "In particular, for the sshd server all users' .ssh/authorized_keys files must have appropriate permissions to allow public key authentication. (Re-)running ssh-user-config for each user will set these permissions correctly. [Similar restrictions apply, for instance, for .rhosts files if the rshd server is running, etc]." 5. "The sshd service has been installed under the 'cyg_server' account. To start the service now, call 'net start sshd' or 'cygrunsrv -S sshd'. Otherwise, it will start automatically after the next reboot." 6. "Host configuration finished. Have fun!" The prompt is "Administrateur@test-PC ~" and the cursor is on a new line with a "\$" character.

```
*** Info: User 'cyg_server' has been created with password 'bonjour'.  
*** Info: If you change the password, please remember also to change the  
*** Info: password for the installed services which use (or will soon use)  
*** Info: the 'cyg_server' account.  
  
*** Info: Also keep in mind that the user 'cyg_server' needs read permissions  
*** Info: on all users' relevant files for the services running as 'cyg_server'.  
*** Info: In particular, for the sshd server all users' .ssh/authorized_keys  
*** Info: files must have appropriate permissions to allow public key  
*** Info: authentication. (Re-)running ssh-user-config for each user will set  
*** Info: these permissions correctly. [Similar restrictions apply, for  
*** Info: instance, for .rhosts files if the rshd server is running, etc].  
  
*** Info: The sshd service has been installed under the 'cyg_server'  
*** Info: account. To start the service now, call 'net start sshd' or  
*** Info: 'cygrunsrv -S sshd'. Otherwise, it will start automatically  
*** Info: after the next reboot.  
  
*** Info: Host configuration finished. Have fun!  
  
Administrateur@test-PC ~  
$ |
```

Il faut à présent démarrer le serveur SSH. Pour cela, ouvrir une console classique (cmd.exe) et entrer :

```
# net start sshd
```



```
Administrateur : C:\Windows\system32\cmd.exe
C:\Users\Administrateur>net start ssh
Le nom de service n'est pas valide.
Vous obtiendrez une aide supplémentaire en entrant NET HELPMSG 2185.
C:\Users\Administrateur>net start sshd
Le service CYGWIN sshd démarre.
Le service CYGWIN sshd a démarré.
C:\Users\Administrateur>
```

Il faut désormais créer l'utilisateur backup sous Cygwin et sous Windows.
Pour Cygwin :

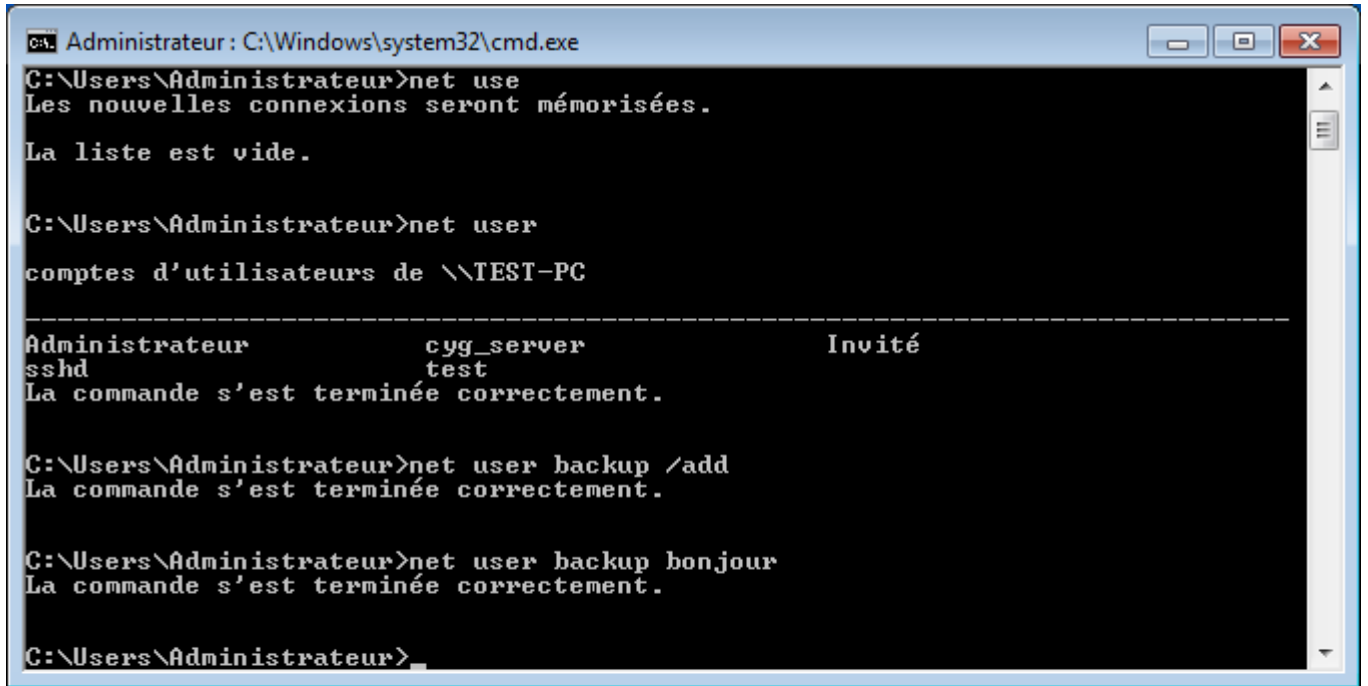
```
# mkpasswd.exe -u backup -l >> /etc/passwd
```

puis :

```
# passwd backup
```

\\pour affecter un mot de passe à backup Pour Windows :

```
# net user backup /add puis :
# net user backup *
```

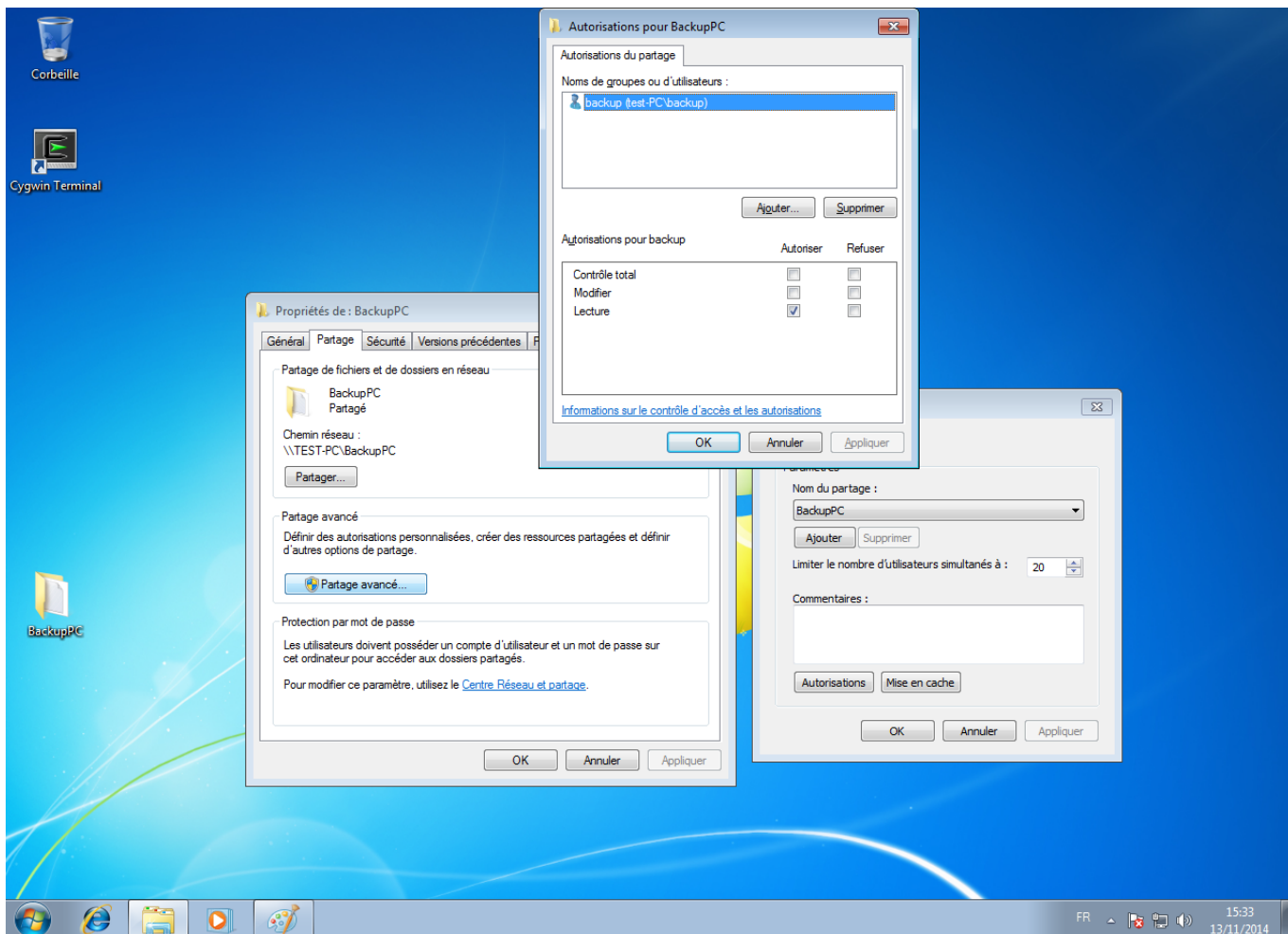


Enfin il faut affecter les droits de lecture à backup sur le dossier à sauvegarder : clic-droit sur le dossier → sécurité → ajouter → renseigner backup comme utilisateur et affecter les droits.



SMB

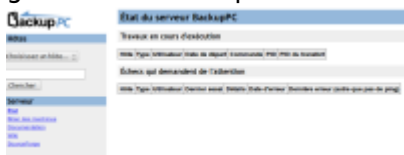
Côté client, il faut créer le partage sur le dossier à sauvegarder



OSX

Utilisation

Cette partie est indépendante du système sauvegardé. Vous pouvez accéder à l'interface web de gestion de BackupPC : [External Link](#) avec les identifiants donnés par votre administrateur.

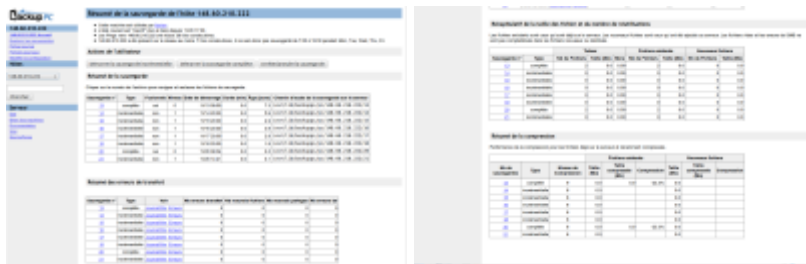


En cliquant sur " Bilan des machines " dans le menu de gauche, vous

accédez au bilan des sauvegardes de votre station.



En cliquant sur l'adresse IP qui correspond à votre identifiant sur le serveur, vous accédez aux détails des



sauvegardes (réussite, échec...). Dans cette interface, vous pouvez lancer ou annuler des sauvegardes totales (il faut en faire une à la première connexion) et des sauvegardes incrémentales (seul le contenu qui a changé depuis la dernière sauvegarde est sauvegarder). BackupPC a une routine qui lance des sauvegardes à intervalles réguliers. En cliquant sur " Explorer les sauvegardes " à gauche, il est possible de lister les



dossiers et les fichiers de chaque sauvegarde. En sélectionnant une sauvegarde puis des fichiers et dossiers, il est possible de restaurer ces fichiers et ces dossiers en cliquant sur " Restaurer les fichiers sélectionnés ". Vous arrivez ensuite sur une page vous proposant



trois méthodes de restauration. La première utilise une restauration directe : les fichiers et les dossiers seront copiés à leur place originelle sur le client. Cette méthode n'est pas utilisée dans la maquette car elle suppose que le serveur ait un accès en écriture aux dossiers du client, ce qui n'est pas envisageable. Les deux autres méthodes créent une archive que vous pouvez télécharger. Ce sera ensuite à vous de restaurer les fichiers et les dossiers manuellement. Les archives zip seront principalement utilisées pour les postes Windows. Les archives tar seront plutôt pour les postes UNIX (libres et OSX).

From: <http://wiki.lahoud.fr/> - wikiroute

Permanent link: <http://wiki.lahoud.fr/doku.php?id=backuppc&rev=1416501336>

Last update: 2014/11/20 17:35

