Install BackupPC

BackupPC is a very powerful backup system run on the server machine. You find all the necessary documentation on http://backuppc.sourceforge.net, including configuration instructions.

Installation

```
apt-get install backuppc
```

Take a note of the pre-assigned password <pwd> during the run of the installation script

Changing Password

Creating or initializing the password file:

```
htpasswd -c /etc/backuppc/htpasswd backuppc
```

Adding users to backuppc to access the CGI interface:

```
htpasswd /etc/backuppc/htpasswd <user>
```

To disable authentication, comment the auth instructions in /etc/backuppc/apache.conf and restart backuppc and apache.

Main Configuration

If you do not install BackupPC on a machine which's sole purpose is to backup data, you should move the target data space to a separate mount point or even a separate harddisk.

```
cd /var/lib
mv backuppc /backup  # move the content as set up by the installer to a
separate mount point, e.g. /backup
ln -s /backup/backuppc backuppc  # create a symlink so all the default paths
are maintained
```

 *If you install and run BackupPC on a machine with Gnome desktop running, you need to exclude ~/.gvfs from the backup path to avoid the task aborting when trying to access the path (see config file below)* 

Details how to setup clients for backup are found in the documentation. Following are example config files and some hints for different types of clients.

Find important global settings which differ from the default below.

Global config: config.pl

```
# Global config
# run nightly cleanup at 3am, run backups between 4am and 4pm and at 9pm
$Conf{WakeupSchedule} = [3..16, 21];

# Smbclient share user name.  This is passed to smbclient's -U argument.
$Conf{SmbShareUserName} = '<smb_user>';
$Conf{SmbSharePasswd} = '<pwd>';

# Minimum period of 7 days between full and incremental backups
$Conf{FullPeriod} = 6.97;
$Conf{IncrPeriod} = 0.97;

# Remove full backups after <FullAgeMax> days but keep at least
<FullKeepCntMin>
$Conf{FullKeepCntMin} = 1;
$Conf{FullAgeMax}     = 90;

# Keep <IncrKeepCnt> incremental backups
$Conf{IncrKeepCnt} = 30;

# Remove full backups after <IncrAgeMax> days but keep at least
<IncrKeepCntMin>
$Conf{IncrKeepCntMin} = 3;
$Conf{IncrAgeMax}     = 30;

# For clients which are regularly online specify blackout periods
# when no backups will be started
$Conf{BlackoutPeriods} = [
    { # weekdays
      hourBegin =>  9.0,
      hourEnd   => 23.0,
      weekDays  => [1, 2, 3, 4, 5],
    },
    { # weekend
      hourBegin => 12.0,
      hourEnd   => 23.0,
      weekDays  => [0, 6],
    },
];

# Only increase the ping time if you need to access a client outside your
LAN
$Conf{PingMaxMsec} = 20;
```

Configuration for Windows clients

all Windows

- If the client is member of a different domain or workgroup than the BackupPC server, you need to indicate the machine's name together with the user name for the Samba client to work. Set the user name in the client config to <machine_name>/<smb_user>, ex: machine_name=VENUS, smb_user=panther

```
$Conf{SmbShareUserName} = 'VENUS/panther';
```

- Check with the following command from the server wether your Samba Client access works:

```
smbclient '//clientname/C$' -U username
```

Windows XP

- Disable “simple file sharing” in Folder Options... / View.
- Windows XP Professional establishes invisible default shares (“C$”, “D$”, etc.) for administration, which BackupPC can use to access the machine. Windows XP Home Edition does not establish admin shares, therefore we need to explicitely share the drives for BackupPC to access the machine. I chose the share names according to the drive labels, e.g. “System” and “Data” in below's example config file.
- Check 'Start/Settings/Control Panel/Administrative Tools/Local Security Policy' and then 'Security Settings/Local Policies/Security Options/' entry 'Network access: Sharing and Security model for local accounts' from 'Guest only - local users authenticate as Guest' to 'Classic - local users authenticate as themselves'.
- Enable File and Printer Sharing in Windows Firewall. Edit exceptions.../Change scope to your local server address (e.g. 192.168.1.11/255.255.255.0) Related error message: *NT_STATUS_ACCESS_DENIED*.
- Check wether IRPStackSize exists in HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters. If it does not, create it. Start with an initial value of Decimal 21, increase by 3 until the conntection works. Related error message: *NT_STATUS_INSUFF_SERVER_RESOURCES*.

Windows 7

- Go to Control Panel>Network and Internet>Network and Sharing Center>Advanced sharing settings and:

```
Turn on network discovery
Turn on file and print sharing
```

Other settings can be left at their default.

- Windows 7 and Vista do not enable the C$ shares by default. Run Regedit and modify the following key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
DWORD LocalAccountTokenFilterPolicy=1
```

Configuration scripts

gemini (localhost) - Ubuntu BackupPC server

Config: localhost.pl

```
# Gemini - BackupPC settings
#
$Conf{XferMethod} = 'tar';

$Conf{TarShareName} =  ['/etc', '/root', '/home', '/usr/local', '/var/www/',
'/srv/share'];

$Conf{TarClientCmd} = '/usr/bin/env LC_ALL=C $tarPath -c -v -f - -C
$shareName'
                    . ' --totals';

# remove extra shell escapes ($fileList+ etc.) that are
# needed for remote backups but may break local ones
$Conf{TarFullArgs} = '$fileList';
$Conf{TarIncrArgs} = '--newer=$incrDate $fileList';

# Files to exclude from backup
$Conf{BackupFilesExclude} = ['/tmp', '/temp', '/proc', '/mnt', '/dev',
'/sys',
                             '/srv/media', '/srv/webcam', '/srv/share/_*',
'/backup', '/var/vm',
                             '/home/<admin user>/.gvfs'];
```

To allow backuppc to backup all files on localhost, you need to either access the tar command through ssh, or use sudo:

```
$Conf{TarClientCmd} = '/usr/bin/sudo $tarPath -c -v -f - -C $shareName'
                        .' --totals';
```

visudo:

```
backuppc ALL = NOPASSWD: /bin/tar
```

titan - Windows XP Professional client

Config: titan.pl

```
# Titan - BackupPC settings
#
$Conf{XferMethod} = 'smb';

$Conf{SmbShareName} = ['C$', 'D$'];

$Conf{SmbShareUserName} = <XP_admin_user>;
$Conf{SmbSharePasswd} = <XP_admin_user's password>;

# Files to exclude from backup
$Conf{BackupFilesExclude} = {
      'C$' => ['/WINDOWS/temp', '/temp'],
      'D$' => ['/Capture', '/_*'],
      };
```

pluto - Windows XP Home Edition client

Config: pluto.pl

```
# Pluto - BackupPC settings
#
$Conf{XferMethod} = 'smb';

$Conf{SmbShareName} = ['System', 'Data'];

$Conf{SmbShareUserName} = <XP_admin_user>;
$Conf{SmbSharePasswd} = <XP_admin_user's password>;

# Files to exclude from backup
$Conf{BackupFilesExclude} = {
      'System' => ['/WINDOWS/temp', '/temp'],
      'Data' => ['/_*', '/iTunes', '/Download', '/TrueImage'],
      };
```

venus - Linux Ubuntu client

Other than for the local host (e.g. the server machine), rsync is much more efficient than tar to backup remote files. rsync communicates through an ssh connection with the client, which we first need to set up. Besides the instructions which you will find in the BackupPC documentation, the following needs to be considered:

- make sure ssh and rsync are installed on the server and the clients

```
apt-get install ssh rsync
```

- use ssh-keygen to generate rsa2 keypairs for users “root” and “backuppc”. To test the ssh connection, it is also helpful to generate a keypair for your admin login “admin”. The keys need to be generated as the respective user, so you would enter:

```
sudo -u backuppc -s
ssh-keygen
```

- in Feisty, the newly generated public keys are found in the following locations:

```
admin   : /home/admin/.ssh
root    : /root/.ssh
backuppc: /var/lib/backuppc/.ssh  #which is /backup/backuppc/.ssh if you
followed the guide above
```

- add the public keys to the authorized_keys files of the client, on the server you enter (using a usb stick mounted at /media/usb):

```
root@gemini:~# cp ~/.ssh/id_rsa.pub /media/usb/admin.pub
root@gemini:~# cp /root/.ssh/id_rsa.pub /media/usb/root.pub
root@gemini:~# cp /var/lib/backuppc/.ssh /media/usb/backuppc.pub
```

- on the client you enter:

```
root@venus:~# cat /media/usb/admin.pub >> ~/.ssh/authorized_keys
root@venus:~# cat /media/usb/root.pub >> /root/.ssh/authorized_keys
root@venus:~# cat /media/usb/backuppc.pub >> /root/.ssh/authorized_keys
# the last line is necessary to allow user "backuppc" to connect to the
client as "root"
```

- the following lines in the file /etc/ssh/sshd_config on the client need to be modified as follows:

```
AllowUsers admin root
PermitRootLogin yes
```

- for security reasons, add the following before the public keys in file /root/.ssh/authorized_keys on the client, which will limit root access on the client to the BackupPC server machine:

```
from="gemini.condrau.com" ssh-rsa AAA...  # or
from="192.168.1.100" ssh-rsa AAA
```

- enter the port number for the ssh connection in BackupPC's config file, if you do not use default port 22 (which is advisable)
- test the ssh connection as admin user from the server:

```
ssh -p <portnum> venus
```

- test the ssh connection as root from the server:

```
sudo -s
ssh -p <portnum> venus
```

- test the ssh connection as backuppc user who logs in as root from the server (which is what the backuppc task will do):

```
sudo -u backuppc -s
ssh -p <portnum> -l root venus
```

- if anything goes wrong, enter above commands with the “-v” option to get additional info: “ssh -v -p <portnum> ...”

Config: venus.pl

```
# Venus - BackupPC settings
#
$Conf{XferMethod} = 'rsync';

$Conf{RsyncClientCmd} = '$sshPath -p 50221 -q -x -l root $host $rsyncPath
$argList';
$Conf{RsyncClientRestoreCmd} = '$sshPath -p 50221 -q -x -l root $host
$rsyncPath $argList';

# Files to exclude from backup
$Conf{BackupFilesExclude} = ['/tmp', '/temp', '/proc', '/mnt', '/dev',
'/sys', '/srv'];
```

Copy content of entire partition

```
rsync -avH /backup /mnt/new_backup/
```