

How to Proxmox 2.1 avec multicast et cluster

Configuration server proxmox 2.1

Pour les serveurs secondaires suivre l'étape 1 jusqu'à la fin puis passer directement à l'étape 4

Tout d'abord vérifier le fichier `/etc/apt/sources.list` :

```
deb http://ftp.fr.debian.org/debian/ squeeze main contrib
# PVE packages provided by proxmox.com
deb http://download.proxmox.com/debian squeeze pve
# security updates
deb http://security.debian.org/ squeeze/updates main contrib
```

Normalement il n'y a rien à changer mais certains hébergeurs modifient ce fichier pour y mettre leurs serveurs caches, à vous de voir si vous voulez les utiliser ou jouer la sécurité en interrogeant directement les serveurs debian de proxmox.

Ensuite lancer un update:

```
#apt-get update
```

Puis un upgrade:

```
#apt-get upgrade
```

Le système est maintenant à jour.

1. Configuration de l'interface réseau virtuelle

Pour cela on utilise le module dummy.

Ensuite tapez la ligne suivante:

```
#echo "options dummy numdummies=2" > /etc/modprobe.d/dummy.conf
```

L'interface dummy0 est parfois déjà utilisée d'où la nécessité d'en créer deux.

Ensuite on charge le module:

```
#modprobe dummy
```

On reboot.

Puis on affiche les interfaces réseau avec:

```
#ifconfig -a | grep Link | grep -v inet6
```

Vérifier que les interfaces dummy0 et dummy1 apparaissent.

Editez ensuite le fichier `/etc/network/interfaces`

On crée une nouvelle interface virtuelle openvpnbr0:

```
auto openvpnbr0
iface openvpnbr0 inet static
address 172.16.0.1
netmask 255.240.0.0
network 172.16.0.0
broadcast 172.16.0.255
bridge_ports dummy1
bridge_stp off
bridge_fd 0
post-up route add -net 224.0.0.0 netmask 240.0.0.0 dev openvpnbr0
```

Pour l' IP vous êtes libres quant à son choix mais il est important de choisir un réseau non routable.
L'adresse IP virtuelle de ce premier server est donc 172.16.0.1 et repose sur un réseau privé de classe C (/24), pour l'installation d'un second server l'IP sera 172.16.0.2 puis pour un troisième 172.16.0.3 etc...

On redémarre les interfaces:

```
#/etc/init.d/networking restart
```

Si tout s'est bien passé vous devriez voir apparaître votre nouvelle interface virtuelle avec un :

```
#ifconfig openvpnbr0
```

```
openvpnbr0 Link encap:Ethernet HWaddr 32:6b:fa:62:e1:b0
inet adr:172.16.0.2 Bcast:172.16.0.255 Masque:255.240.0.0
adr inet6: fe80::f8a3:21ff:fe9d:efea/64 Scope:Lien
UP BROADCAST RUNNING PROMISC MULTICAST MTU:1500 Metric:1
RX packets:894309 errors:0 dropped:0 overruns:0 frame:0
TX packets:854860 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 lg file transmission:0
RX bytes:177615983 (169.3 MiB) TX bytes:188724615 (179.9 MiB)
```

Vérifiez que l'interface pingue correctement:

```
#ping 172.16.0.1
```

Si l'interface ne pingue pas, il faut vérifier les différents paramètres. Et si les paramètres sont bons rebootez...

Apache:

Editez le fichier /etc/apache2/apache2.conf puis commentez la ligne « Include ports.conf »

Redémarrez apache:

```
#/etc/init.d/apache2 restart
```

Editez le fichier /etc/hosts:

```
127.0.0.1 localhost.localdomain localhost
172.16.0.1 nsxxxxxx.ovh.net nsxxxxxx pvelocalhost ---> mettre votre IP privée à la place de l'IP publique
```

Il doit ressembler à ça, si ce n'est pas le cas, y apporter les modifications nécessaires.

Puis editez le fichier /etc/resolv.conf qui doit ressembler à ça:

```
nameserver 127.0.0.1
nameserver 213.186.33.99
search ovh.net
search ovh.net
```

Puis on edite le fichier /etc/default/bootlogd et on modifie:

```
BOOTLOGD_ENABLE=Yes
```

On reboot:

```
#shutdown -r now
```

2. Installation d'openvpn (server primaire) pour les servers secondaires passez directement à l'étape 4

```
#apt-get install openvpn
```

Puis on prépare les certificats:

```
#cp -av /usr/share/doc/openvpn/examples/easy-rsa/2.0 /etc/openvpn/easy-rsa
```

```
#cd /etc/openvpn/easy-rsa
```

```
#tail -n 8 vars
```

Editez la fin du fichier à votre convenance, une fois que c'est fait, on peut passer à la préparation des certificats.

```
#source ./vars
```

NOTE: If you run ./clean-all, I will be doing a rm -rf on /etc/openvpn/easy-rsa/keys

```
#!/clean-all
```

```
#!/build-dh
```

```
1 Generating DH parameters, 1024 bit long safe prime, generator 2
2 This is going to take a long time
3 .....+.....
4 ..+.....+.....
5 .....
6 ...+.....++*++*++*
```

```
#!/pkitool --initca
```

```
1 Using CA Common Name: Mon organisation CA
2 Generating a 1024 bit RSA private key
3 ...++++++
4 .....++++++
5 writing new private key to 'ca.key'
6 -----
```

Génération de la clé serveur:

```
#!/pkitool --server proxmox-server-1
```

```
1 Generating a 1024 bit RSA private key
2 .....++++++
3 .....++++++
4 writing new private key to 'proxmox-server-1.key'
5 -----
6 Using configuration from /etc/openvpn/easy-rsa/openssl.cnf
7 Check that the request matches the signature
8 signature OK
9 The subject's Distinguished Name is as follows
10 countryName      PRINTABLE: 'FR'
11 localityName     PRINTABLE: 'Ma ville'
12 organizationName PRINTABLE: 'Mon organisation'
13 commonName       PRINTABLE: 'proxmox-server-1'
14 emailAdress      IA5STRING: 'mon-email@domain.ff'
15 Certificate is to be certified until Mar 13 14:33:45 2012 GMT (3650 days)
16
17 Write out database with 1 new entries
18 data base updated
```

Puis:

```
#openvpn --genkey --secret ./keys/ta.key
```

Génération de la clé cliente (pour les autres servers):

```
#!/pkitool proxmox-client-1
```

```
1 Generating a 1024 bit RSA private key
2 .....++++++
3 .....++++++
4 writing new private key to 'proxmox-client-1.key'
5 -----
6 Using configuration from /etc/openvpn/easy-rsa/openssl.cnf
7 Check that the request matches the signature
8 signature OK
9 The subject's Distinguished Name is as follows
10 countryName          PRINTABLE: 'FR'
11 localityName         PRINTABLE: 'Ma ville'
12 organizationName     PRINTABLE: 'Mon organisation'
13 commonName           PRINTABLE: 'proxmox-client-1'
14 emailAdress          IA5STRING: 'mon-email@domain.ff'
15 Certificate is to be certified until Mar 13 14:33:45 2012 GMT (3650 days)
16
17 Write out database with 1 new entries
18 data base updated
```

On sauvegarde les clés:

```
#cd /etc/openvpn/easy-rsa/keys
#tar cvzf /root/proxmox-server-1-keys.tar.gz proxmox-server-1.crt proxmox-server-1.key ca.crt dh1024.pem
ta.key
#tar cvzf /root/proxmox-client-1-keys.tar.gz proxmox-client-1.crt proxmox-client-1.key ca.crt ta.key
```

Gardez les précieusement car sans elles vous ne pourrez rien faire!

3. configuration du server primaire openvpn

```
#cd /etc/openvpn
#zcat /usr/share/doc/openvpn/examples/sample-config-files/server.conf.gz > server.conf
```

Affichez le fichier server.conf

```
#cat server.conf | grep -v -e '^;' | grep -v -e '^#' | grep -v -e '^$'
```

Il doit ressembler à ça, si ce n'est pas le cas, éditez le et modifiez le en fonction.

```
Local ***.***.***.*** ----> adresse IP publique
port 1194 ----> Par défaut openvpn écoute sur le port 1194 mais vous pouvez le changer
proto udp
dev tap0
ca ca.crt
cert proxmox-server-1.crt ----> précisez le nom des fichiers qui correspondent
key proxmox-server-1.key # This file should be kept secret ----> précisez le nom des fichiers qui correspondent
dh dh1024.pem
server-bridge 172.16.0.1 255.240.0.0 172.16.0.0 172.16.0.12 ----> le premier paramètre est l' IP de l'interface virtuelle, ensuite le masque,
client-to-client puis la plage d'adresses IP qui sera attribuée aux clients qui se
duplicate-cn connecteront sur le server.
keepalive 10 120
tls-auth ta.key 0 # This file is secret
comp-lzo
max-clients 10
```

```
user nobody
group nogroup
persist-key
persist-tun
status openvpn-status.log
log-append openvpn.log
verb 3
```

```
mode server
tls-server
script-security 2
up "/etc/openvpn/up.sh"
down "/etc/openvpn/down.sh"
mssfix 1300
fragment 1300
```

Scripts up.sh et down.sh

```
#vi /etc/openvpn/up.sh
```

```
#!/bin/bash
/sbin/ifconfig openvpnbr0 promisc
/sbin/ifconfig tap0 up promisc
/usr/sbin/brctl addif openvpnbr0 tap0
```

```
#vi /etc/openvpn/down.sh
```

```
#!/bin/bash
/usr/sbin/brctl delif openvpnbr0 tap0
/sbin/ifconfig tap0 down -promisc
/sbin/ifconfig openvpnbr0 -promisc
```

Ne pas oublier de rendre ces scripts exécutable

```
#chmod 0755 up.sh down.sh
```

Ajout des clés:

```
#tar xvzf /root/proxmox-server-1-keys.tar.gz
```

Lancement du serveur openvpn:

```
#!/etc/init.d/openvpn restart
```

Si tout s'est bien passé vous devez voir ceci dans le fichier de log /etc/openvpn/openvpn.log :

```
Fri Jun 22 10:49:24 2012 OpenVPN 2.1.3 x86_64-pc-linux-gnu [SSL] [LZO2] [EPOLL] [PKCS11] [MH] [PF_INET6] [eurephia]
built on Feb 21 2012
Fri Jun 22 10:49:24 2012 NOTE: when bridging your LAN adapter with the TAP adapter, note that the new bridge adapter will often take on its
own IP address that is different from what the LAN adapter was previously set to
Fri Jun 22 10:49:24 2012 NOTE: the current --script-security setting may allow this configuration to call user-defined scripts
Fri Jun 22 10:49:24 2012 Diffie-Hellman initialized with 1024 bit key
Fri Jun 22 10:49:24 2012 /usr/bin/openssl-vulnkey -q -b 1024 -m <modulus omitted>
Fri Jun 22 10:49:24 2012 Control Channel Authentication: using 'ta.key' as a OpenVPN static key file
Fri Jun 22 10:49:24 2012 Outgoing Control Channel Authentication: Using 160 bit message hash 'SHA1' for HMAC authentication
Fri Jun 22 10:49:24 2012 Incoming Control Channel Authentication: Using 160 bit message hash 'SHA1' for HMAC authentication
Fri Jun 22 10:49:24 2012 TLS-Auth MTU parms [ L:1574 D:166 EF:66 EB:0 ET:0 EL:0 ]
Fri Jun 22 10:49:24 2012 Socket Buffers: R=[133120->131072] S=[133120->131072]
Fri Jun 22 10:49:24 2012 TUN/TAP device tap0 opened
Fri Jun 22 10:49:24 2012 TUN/TAP TX queue length set to 100
Fri Jun 22 10:49:24 2012 /etc/openvpn/up.sh tap0 1500 1574 init
Fri Jun 22 10:49:24 2012 Data Channel MTU parms [ L:1574 D:1300 EF:42 EB:135 ET:32 EL:0 AF:3/1 ]
Fri Jun 22 10:49:24 2012 GID set to nogroup
Fri Jun 22 10:49:24 2012 UID set to nobody
Fri Jun 22 10:49:24 2012 UDPv4 link local (bound): [AF_INET]***.***.***.**:1194
Fri Jun 22 10:49:24 2012 UDPv4 link remote: [undef]
Fri Jun 22 10:49:24 2012 MULTI: multi_init called, r=256 v=256
Fri Jun 22 10:49:24 2012 IFCONFIG POOL: base=172.16.0.0 size=13
Fri Jun 22 10:49:24 2012 Initialization Sequence Completed
```

4. configuration openvpn (servers secondaires)

```
#apt-get install openvpn
```

Puis on se rend dans le répertoire d'openvpn et on récupère la config client par défaut:

```
#cd /etc/openvpn
```

```
#cp -av /usr/share/doc/openvpn/examples/sample-config-files/client.conf .
```

Puis on affiche le fichier de configuration `cat client.conf | grep -v -e '^;' | grep -v -e '^#' | grep -v -e '^$'`

Il doit ressembler à ça, si ce n'est pas le cas, y apporter les modifications nécessaires:

```
client
dev tap0
proto udp
remote ***.***.***.*** 1194 -----> précisez l'adresse IP publique du server primaire
resolv-retry infinite
nobind
user nobody
group nogroup
persist-key
persist-tun
ca ca.crt
cert nsxxxxxx.crt
key nsxxxxxx.key
ns-cert-type server
tls-auth ta.key 1
comp-lzo
verb 3
log-append openvpn.log
script-security 2
up "/etc/openvpn/up.sh"
down "/etc/openvpn/down.sh"
mssfix 1300
fragment 1300
```

certificats et scripts:

Retournez sur le server primaire afin de copier les clés:

```
#scp /root/proxmox-client-1-keys.tar.gz ***.***.***.***:/root/ -----> IP publique server secondaire
```

```
#scp /etc/openvpn/up.sh /etc/openvpn/down.sh ***.***.***.***:/etc/openvpn-----> IP publique server secondaire
```

On retourne sur le server secondaire et on décompresse les clés:

```
#tar xvzf /root/proxmox-client-1-keys.tar.gz
```

Et on lance le client openvpn:

```
#!/etc/init.d/openvpn restart
```

Si tout s'est bien passé vous devriez voir ceci dans le fichier de log `/etc/openvpn/openvpn.log`:

```

Fri Jun 22 10:49:48 2012 OpenVPN 2.1.3 x86_64-pc-linux-gnu [SSL] [LZO2] [EPOLL] [PKCS11] [MH] [PF_INET6] [eurephia] built on Feb 21 2012
Fri Jun 22 10:49:48 2012 NOTE: the current --script-security setting may allow this configuration to call user-defined scripts
Fri Jun 22 10:49:48 2012 /usr/bin/openssl-vulnkey -q -b 1024 -m <modulus omitted>
Fri Jun 22 10:49:48 2012 Control Channel Authentication: using 'ta.key' as a OpenVPN static key file
Fri Jun 22 10:49:48 2012 Outgoing Control Channel Authentication: Using 160 bit message hash 'SHA1' for HMAC authentication
Fri Jun 22 10:49:48 2012 Incoming Control Channel Authentication: Using 160 bit message hash 'SHA1' for HMAC authentication
Fri Jun 22 10:49:48 2012 LZO compression initialized
Fri Jun 22 10:49:48 2012 Control Channel MTU parms [ L:1578 D:166 EF:66 EB:0 ET:0 EL:0 ]
Fri Jun 22 10:49:48 2012 Socket Buffers: R=[133120->131072] S=[133120->131072]
Fri Jun 22 10:49:48 2012 Data Channel MTU parms [ L:1578 D:1300 EF:46 EB:135 ET:32 EL:0 AF:3/1 ]
Fri Jun 22 10:49:48 2012 Fragmentation MTU parms [ L:1578 D:1300 EF:45 EB:135 ET:33 EL:0 AF:3/1 ]
Fri Jun 22 10:49:48 2012 Local Options hash (VER=V4): 'a257ef04'
Fri Jun 22 10:49:48 2012 Expected Remote Options hash (VER=V4): '8f3da10b'
Fri Jun 22 10:49:48 2012 NOTE: UID/GID downgrade will be delayed because of --client, --pull, or --up-delay
Fri Jun 22 10:49:48 2012 UDPv4 link local: [undef]
Fri Jun 22 10:49:48 2012 UDPv4 link remote: [AF_INET]***.***.***.**:1194
Fri Jun 22 10:49:48 2012 TLS: Initial packet from [AF_INET]***.***.***.**:1194, sid=49a4f4e3 7b301afb
Funston_CA/emailAddress=me@myhost.mydomain
Fri Jun 22 10:49:48 2012 VERIFY OK: nsCertType=SERVER
Fri Jun 22 10:49:48 2012 VERIFY OK: depth=0, /C=US/ST=CA/L=SanFrancisco/O=Fort-Funston/CN=nsxxxxxx/emailAddress=me@myhost.mydomain
Fri Jun 22 10:49:48 2012 Data Channel Encrypt: Cipher 'BF-CBC' initialized with 128 bit key
Fri Jun 22 10:49:48 2012 Data Channel Encrypt: Using 160 bit message hash 'SHA1' for HMAC authentication
Fri Jun 22 10:49:48 2012 Data Channel Decrypt: Cipher 'BF-CBC' initialized with 128 bit key
Fri Jun 22 10:49:48 2012 Data Channel Decrypt: Using 160 bit message hash 'SHA1' for HMAC authentication
Fri Jun 22 10:49:48 2012 Control Channel: TLSv1, cipher TLSv1/SSLv3 DHE-RSA-AES256-SHA, 1024 bit RSA
Fri Jun 22 10:49:48 2012 [nsxxxxxx] Peer Connection Initiated with [AF_INET]***.***.***.**:1194
Fri Jun 22 10:49:50 2012 SENT CONTROL [nsxxxxxx]: 'PUSH_REQUEST' (status=1)
Fri Jun 22 10:49:50 2012 PUSH: Received control message: 'PUSH_REPLY,route-gateway 172.16.0.1,ping 10,ping-restart 120,ifconfig 172.16.0.0
255.240.0.0'
Fri Jun 22 10:49:50 2012 OPTIONS IMPORT: timers and/or timeouts modified
Fri Jun 22 10:49:50 2012 OPTIONS IMPORT: --ifconfig/up options modified
Fri Jun 22 10:49:50 2012 OPTIONS IMPORT: route-related options modified
Fri Jun 22 10:49:50 2012 TUN/TAP device tap0 opened
Fri Jun 22 10:49:50 2012 TUN/TAP TX queue length set to 100
Fri Jun 22 10:49:50 2012 /sbin/ifconfig tap0 172.16.0.0 netmask 255.240.0.0 mtu 1500 broadcast 172.31.255.255
Fri Jun 22 10:49:50 2012 /etc/openvpn/up.sh tap0 1500 1578 172.16.0.0 255.240.0.0 init
Fri Jun 22 10:49:51 2012 GID set to nogroup
Fri Jun 22 10:49:51 2012 UID set to nobody
Fri Jun 22 10:49:51 2012 Initialization Sequence Completed

```

Cette étape est importante:

Testons le multicast ---> ATTENTION il est important de réussir le multicast sinon ça ne marchera pas.

Installer le paquet ssm ping sur tous les servers:

```
#apt-get install ssm ping
```

Puis sur le server primaire mettez vous en écoute:

```
#ssm pingd
```

et lancer la diffusion depuis le server secondaire:

```
#asmping 224.0.2.1 172.16.0.1
```

Si tout va bien vous devriez voir ceci:

```

asmping joined (S,G) = (*,224.0.2.234)
pinging 172.16.0.1 from 172.16.0.2
unicast from 172.16.0.1, seq=1 dist=0 time=38.699 ms
multicast from 172.16.0.1, seq=1 dist=0 time=76.405 ms
unicast from 172.16.0.1, seq=2 dist=0 time=38.802 ms
multicast from 172.16.0.1, seq=2 dist=0 time=76.238 ms
unicast from 172.16.0.1, seq=3 dist=0 time=38.859 ms
multicast from 172.16.0.1, seq=3 dist=0 time=76.621 ms

unicast from 172.16.0.1, seq=4 dist=0 time=38.670 ms
multicast from 172.16.0.1, seq=4 dist=0 time=77.186 ms

```

5. Créer un cluster (si vous voulez juste rajouter un noeud sur un cluster existant passez directement au paragraphe suivant)

Sur le server primaire:

```
#pvecm create nom-du-cluster
```

Generating public/private rsa key pair.

Your identification has been saved in /root/.ssh/id_rsa.

Your public key has been saved in /root/.ssh/id_rsa.pub:

The key fingerprint is:

xx:xx [root@proxmox-server-1](#)

The key's randomart image is:

```
+--[ RSA 2048 ]-----+
|
|          . So o
|         . ...O o
|        ... o* =
|       +oo . = .
|      . +E*oo.
|
+-----+
```

Restarting pve cluster filesystem: pve-cluster[dcdb] crit: unable to read cluster config file

'/etc/cluster/cluster.conf' - Failed to open file '/etc/cluster/cluster.conf': No such file or directory

[dcdb] notice: wrote new cluster config '/etc/cluster/cluster.conf'

[dcdb] crit: cman_tool version failed with exit code 1#010

Starting cluster:

Checking if cluster has been disabled at boot... [OK]

Checking Network Manager... [OK]

Global setup... [OK]

Loading kernel modules... [OK]

Mounting configs... [OK]

Starting cman... [OK]

Waiting for Quorum... [OK]

Starting fenced... [OK]

Starting dlm control... [OK]

Unfencing self... [OK]

Sur les servers secondaires:

```
#pvecm add 172.16.0.1
```

Generating public/private rsa key pair.

Your identification has been saved in /root/.ssh/id_rsa.

Your public key has been saved in /root/.ssh/id_rsa.pub:

The key fingerprint is:

xx:xx [root@proxmox-server-2](#)

The key's randomart image is:

```
+--[ RSA 2048 ]-----+
|.o.o
|.o+= E
|.oo.*
| .. * o
| = o + S
| * o +
| .
| .
+-----+
```

The authenticity of host '172.16.0.1 (172.16.0.1)' can't be established.

RSA key fingerprint is xx:xx.

Are you sure you want to continue connecting (yes/no)? **Yes**

[root@172.16.0.1](#)'s password:
copy corosync auth key

```
stopping pve-cluster service
stopping pve cluster filesystem: pve-cluster
backup old database
starting pve cluster filesystem: pve-cluster
Starting cluster:
  Checking if cluster has been disabled at boot... [ OK ]
  Checking Network Manager... [ OK ]
  Global setup... [ OK ]
  Loading kernel modules... [ OK ]
  Mounting configfs... [ OK ]
  Starting cman.... [ OK ]
  Waiting for Quorum... [ OK ]
  Starting fenced... [ OK ]
  Starting dlm controld... [ OK ]
  Unfencing self... [ OK ]
generating node certificates
unable to create directory '/etc/pve/priv' - File exists
```

Pour voir l'état du cluster:

```
#pvecm status
```

Redimensionner la partition racine:

```
#vgdisplay pve
```

```
--- Volume group ---
VG Name          pve
System ID
Format           lvm2
Metadata Areas   1
Metadata Sequence No 2
VG Access        read/write
VG Status        resizable
MAX LV           0
Cur LV          1
Open LV          1
Max PV           0
Cur PV          1
Act PV           1
VG Size          257,93 GiB
PE Size          4,00 MiB
Total PE         66029
Alloc PE / Size  66029 / 257,93 GiB
Free PE / Size   0 / 0
VG UUID          Qt2Su4-OD3t-zXeu-BkNu-gzid-732A-t7rjgK
```

```
#lvdisplay pve
```

```
--- Logical volume ---
LV Path          /dev/pve/data
LV Name          data
VG Name          pve
LV UUID          K1327L-Rq70-aRVj-zn4L-OJVP-Rr6S-kbXZSv
LV Write Access  read/write
LV Creation host, time ,
LV Status        available
# open           1
LV Size          257,93 GiB
Current LE       66029

Segments         1
Allocation       inherit
```

Read ahead sectors auto
- currently set to 256
Block device 253:0

```
#umount /dev/mapper/pve-data
```

```
#e2fsck -f /dev/pve/data
```

```
e2fsck 1.41.12 (17-May-2010)
Passe 1 : vérification des i-noeuds, des blocs et des tailles
Passe 2 : vérification de la structure des répertoires
Passe 3 : vérification de la connectivité des répertoires
Passe 4 : vérification des compteurs de référence
Passe 5 : vérification de l'information du sommaire de groupe
/dev/pve/data : 20/16908288 fichiers (0.0% non contigus), 580670/67613696 blocs
```

```
# resize2fs -p /dev/pve/data 150G
```

```
resize2fs 1.41.12 (17-May-2010)
En train de retailler le système de fichiers sur /dev/pve/data à 39321600 (4k) blocs.
Début de la passe 2 (max = 6)
Relocalisation de blocs XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
Début de la passe 3 (max = 2064)
Examen de la table d'i-noeuds XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
Début de la passe 4 (max = 14)
Mise à jour des références d'i-noeudsXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
Le système de fichiers /dev/pve/data a maintenant une taille de 39321600 blocs.
```

```
#lvresize -L 150G /dev/pve/data
```

```
WARNING: Reducing active logical volume to 150,00 GiB
THIS MAY DESTROY YOUR DATA (filesystem etc.)
Do you really want to reduce data? [y/n]: y
Reducing logical volume data to 150,00 GiB
Logical volume data successfully resized
```

```
# mount /dev/mapper/pve-data
```

```
# vgdisplay
```

```
--- Volume group ---
VG Name          pve
System ID
Format           lvm2
Metadata Areas   1
Metadata Sequence No 3
VG Access        read/write
VG Status        resizable
MAX LV           0
Cur LV          1
Open LV          1
Max PV           0
Cur PV          1
Act PV           1
VG Size          257,93 GiB
PE Size          4,00 MiB
Total PE         66029
Alloc PE / Size  38400 / 150,00 GiB
Free PE / Size   27629 / 107,93 GiB
VG UUID          Qt2Su4-OD3t-zXeu-BkNu-gzid-732A-t7rjgK
```