

Linux vsrver

-

Installation et utilisation

ATOL Conseils et Développements

3 bd Eiffel
21600 LONGVIC
contact@atolcd.com

 **atol** Conseils & Développements

www.atolcd.com

Tel : 03 80 68 81 68
Fax : 03 80 68 81 61

version 1.1

SOMMAIRE

Table des matières

Linux vserver.....	1
Installation et utilisation	1
SOMMAIRE.....	2
Présentation de vserver.....	3
Points forts.....	3
Installation (Debian).....	4
Packages nécessaires.....	4
Compilation du noyau.....	4
Configuration de l'hôte.....	5
Réseau.....	5
Fichiers de configuration de l'hôte.....	6
Gestion des vservers.....	7
Création.....	7
Dupliquer un vserver.....	7
Lancement / Arrêt.....	7
Visualiser le statut.....	8
Entrer dans l'environnement.....	8
Astuces.....	9
Outils adaptés.....	9
Partager un répertoire entre plusieurs vservers.....	9
Exécuter une tâche au démarrage d'un vserver.....	10
Renommer un vserver.....	10
Copier un vserver sur une autre machine.....	10
Erreur "can't set the new security context" à l'arrêt du vserver.....	11
Conflit IP entre vservers.....	11
Configurations spécifiques.....	12
X sous vserver.....	12
Mysql.....	12
vsFtpd.....	12
rsync.....	12
postgreSQL.....	12
Liens externes.....	13

Présentation de vserver

Vserver est un patch pour le noyau Linux et une série d'outils qui permettent de mettre en place facilement des environnements indépendants sur une même machine.

Par environnements différents on entend des environnements d'exécution qui permettent de lancer des processus dans des contextes séparés, en isolant les processus, les systèmes de fichiers, les ressources réseau, et tout ce qu'offre le noyau. C'est comme si (en simplifiant beaucoup) on lançait autant de fois le système Linux que voulu, sur une même machine, pour obtenir autant d'espaces de travail que voulu.

A un détail prêt, le noyau linux est partagé par tous les vservers.

- Sur les processus : Chaque numéro de processus est préfixé par un numéro de contexte
- Sur le système de fichier : Chaque environnement tourne sur un système qu'il peut seul utiliser.
- Sur le réseau : Chaque environnement ne peut utiliser que l'adresse réseau qui lui est attribuée.

Points forts

Chaque vserver est juste constitué d'une arborescence et d'un fichier de configuration. Cela veut dire que l'on peut librement déplacer un vserver simplement en recopiant ces fichiers !

Chaque environnement peut se voir associer des droits particuliers sur le système.

On peut limiter les ressources allouées à chaque vserver (processus, mémoire, quota disque, ..).

On peut relancer ou faire vivre un vserver sans toucher les autres.

Vserver ne consomme pas de ressources. Les seules ressources consommées le sont par les processus effectivement en cours d'exécution.

Installation (Debian)

Packages nécessaires

util-vserver	<i>Les outils pour manipuler les vservers et baculer d'un contexte à un autre</i>
vserver-debiantools	<i>Les outils pour gérer des vservers Debian</i>
kernel-patch-ctx	<i>Le patch vserver de sécurisation des contextes pour le noyau Linux</i>
kernel-source-2.4.27	<i>Les sources du noyau (le numéro de version peut changer)</i>
libncurses5-dev	<i>La librairie ncurses pour la configuration de noyau</i>
kernel-package	<i>Les outils de compilation de noyau</i>
fakeroot	<i>Pour compiler le noyau "à la sauce Debian"</i>

Compilation du noyau

Sinon pour les plus méticuleux :

- Décompresser les sources du noyau

```
# tar jxvf kernel-source-2.4.27.tar.bz2
# ln -s kernel-source-2.4.27 linux
```

- Patcher le noyau

```
# cd kernel-source-2.4.27
# ../kernel-patches/i386/apply/ctx
START applying ctx patch (Virtual private servers and security contexts)
Testing whether "Virtual private servers and security contexts" patch for
2.4.27 applies (dry run):
"Virtual private servers and security contexts" patch for 2.4.27 succeeded
Removing empty files:
Done.
END applying ctx patch
```

- Configurer le noyau

```
# make menuconfig
# make-kpkg clean
# make-kpkg --rootcmd fakeroot --revision=2.4.27 --append-to-version=-686-ctx
buildpackage
```

La configuration du noyau se fait selon les méthodes habituelles déjà largement documentées sur internet. (exemple pas au hasard : <http://people.via.ecp.fr/~alexis/formation-linux/config-noyau.html>)

L'option relative à vserver (et donc à ne pas oublier) est : *Block devices* ⇒ *Virtual root device support*

- Installer le noyau

```
# dpkg -i kernel-image-2.4.27-686-ctx_2.4.27_i386.deb
```

Configuration de l'hôte

Réseau

Voir http://lena.franken.de/linux/debian_and_vserver/vserver.html

- Configurer les démons pour une écoute sur l'hôte seulement
- Remplacer inetd par xinetd avec “apt-get install xinetd”
- Ajouter cette ligne à /etc/xinetd.conf (avec l'IP de votre serveur) :

```
defaults { bind = 10.95.81.15 }
```

- sshd: Dans /etc/ssh/sshd_config

```
ListenAddress 10.95.81.15
```

- Postfix : Dans /etc/postfix/main.cf

```
inet_interfaces = 10.95.81.15
```

- Vérifier /etc/resolv.conf pour le nom de serveur
- Y-a t'il d'autres ports utilisés sur le système hôte qui le sont aussi sur les systèmes fils ? Vérifier avec “netstat -l”

⇒ **Par tranquillité, tout service en écoute ne doit écouter que sur son interface externe. Ceci est valable aussi bien pour le “maitre” que pour les “esclaves”**

Fichiers de configuration de l'hôte

/etc/vservers.conf

```
# Configuration file for the vservers service
# BACKGROUND=yes
# start the vservers on tty9, in background so the rest of the
# boot process end early
BACKGROUND=no
VSERVERS_ROOT=/vservers
GENERATEMTAB=yes
```

/etc/vservers/util-vserver-vars

```
PKG_LIBDIR='/usr/lib/util-vserver'
SBINDIR='/usr/sbin'
VROOTDIR='/vservers'
```

/etc/vservers/test.conf

```
# Most easy thing is to have an own ip-address for each vserver
IPROOT=192.168.1.15
IPROOTMASK=255.255.255.0
# How shall the networkdevice be named from the view of the vserver
IPROOTDEV=eth0
# shown hostname
S_HOSTNAME=test
# lock = you are not allowed to create a new context in your context
# nproc = let ULIMIT-value be global for this context
S_FLAGS="lock nproc"
ULIMIT="-H -u 1000"
# What capabilities shall the server have? Look for explanation
S_CAPS="CAP_SYS_ADMIN"
# Start this server on booting? This will be checked in /etc/init.d/vservers
ONBOOT=yes
```

Gestion des vservers

Création

A partir du server racine

- Créer un fichier de configuration au nom du vserver, sur le modèle /etc/vservers/test.conf
- Initialiser le vserver (création de liens vers le serveur racine)

```
# vserver test build
```

(Cela va prendre plusieurs minutes la première fois)

A partir d'une image externe

- Créer un fichier de configuration au nom du vserver, sur le modèle /etc/vservers/test.conf
- Décompresser l'archive dans le dossier des vservers
- Initialiser le vserver

```
# vserver test build
```

A partir d'un miroir Debian

```
cd /vservers/  
debootstrap sarge nom_vserver http://miroir.debian/debian  
cp -r /etc/apt/* /vservers/nom_vserver/etc/apt/  
vserver nom_vserver start  
vserver nom_vserver enter  
apt-get update  
apt-get install locales  
base-config
```

A partir d'un miroir Debian (2)

```
newvserver --hostname nouveau_vserver --domain domain.tld --ip adresse_ip --  
mirror http://miroir.debian/debian
```

A partir d'un vserver existant (mon préféré, ne me demandez pas pourquoi)

```
vserver-copy vserver_source -d domain.tld -i adresse_ip vserver_destination
```

Dupliquer un vserver

```
dupvserver --vsroot /var/lib/vservers --from vserver1 --to vserver10 --ip  
192.168.0.10
```

⚠ Avant de lancer le vserver, vérifier ses fichiers /etc/hosts et /etc/resolv.conf

Lancement / Arrêt

```
# vserver test start
```

```
Starting the virtual server test1
Server test1 is not running
ipv4root is now 192.168.1.19
Host name is now test
New security context is 8
Starting PostgreSQL database server: postmaster autovacuum.
Starting Zope instance default...
  Waiting instances in late: default(0), done.
OpenPKG: start: openpkg, openldap, sasl, spamassassin, amavisd, apache
OpenPKG: start: clamav, dcron, imapd, postfix, proftpd, kolabd.
```

```
# vserver test1 stop
Stopping the virtual server test1
Server test1 is running
ipv4root is now 10.95.81.71
sleeping 5 seconds
```

Visualiser le statut

D'un serveur :

```
# vserver test status

Server test is running
232 processes running
Vserver uptime: 139 days 00:28
```

Globalement :

```
# vserver-stat

CTX   PROC   VSZ    RSS   userTIME   sysTIME   UPTIME  NAME      DESCRIPTION
0     43    92MB   5kB   3d06h07    11h10m06  139d12h22  root server
49154  24   109MB   6kB   1h17m27    38m46.24  139d12h21  testweb
49156  10    25MB   1kB   10m32.29   14m10.39  139d12h20  devoracle1
49158   9    22MB   1kB   10m29.95   14m04.63  139d12h20  devphp2
49159  22   228MB  12kB   27m24.38   27m45.74  139d12h20  devpostgis1
49160  10    25MB   1kB   22m47.15   25m24.00  139d12h19  devtomcat1
49161  13   455MB   2kB   3h05m51    1h14m43   139d12h19  postgresql1
49166  17   650MB  11kB   2h10m07    44m41.36  138d11h50  automatik1
49167  30   274MB  22kB   2h16m31    31m10.99  113d06h26  autobuild1
49172  72   799MB  923kB  23m43.59    7m19.36   69d06h35   devtomcat2
49176 135   742MB  532kB  42m51.18   22m32.53  57d11h44   masterdeb
49182  67    3GB   210kB   2h16m51    28m56.83  51d12h35   projet1
49183  50    1GB   121kB   29m20.57    5m48.79   7d04h22    devphp1
49186  14    51MB   4kB     3m31.82    2m23.59   5d09h06    nxserver
```

Entrer dans l'environnement

```
# vserver test enter
ipv4root is now 192.168.1.15
New security context is 5
```

Astuces

Outils adaptés

(Depuis le système hôte)

vtop	top global sur tous serveurs
vps	ps global sur tous serveurs
vpstree	pstree global sur tous serveurs
vdu	du qui ne se mélange pas avec les liens
vkill	kill global sur tous serveurs
vserver-copy	copie de vservers
vfiles	Extraire la liste des fichiers spécifiques (les liens durs) à un vserver (gain de place)
vunify	Inclure les fichiers manquants (liens symboliques) après un vfiles

Partager un répertoire entre plusieurs vservers

- Utiliser “mount –bind”

```
mount --bind /home /vservers/vserver1/home
mount --bind /home /vservers/vserver2/home
```

Exécuter une tâche au démarrage d'un vserver

- Créer un fichier “/etc/vservers/nom_vserver.sh”
- Ce fichier sera appelé avant le démarrage, après le démarrage, avant l’arrêt, et après l’arrêt d’un vserver, avec les arguments respectifs pre-start, post-start, pre-stop et post-stop.
- Le second argument sera le nom du vserver

ex :

```
#!/bin/sh
  case $1 in
    pre-start)
      mount --bind /home /vservers/$2/home
      ;;
    post-start)
      ;;
    pre-stop)
      ;;
    post-stop)
      umount /vservers/$2/home
      ;;
  esac
```

Renommer un vserver

- Stopper le vserver, puis taper

```
mv /vservers/anciennom /vservers/nouveaunom
mv /etc/vservers/anciennom.conf /etc/vservers/nouveaunom.conf
mv /etc/vservers/anciennom.sh /etc/vservers/nouveaunom.sh
```

Copier un vserver sur une autre machine

```
rsync -e ssh -avHl /vservers/XX nouveau-server:/vserver/XX
```

Erreur "can't set the new security context" à l'arrêt du vserver

```
# vserver test1 stop
Stopping the virtual server test1
Server test1 is running
ipv4root is now 10.95.81.71
Can't set the new security context
: Invalid argument
sleeping 5 seconds
```

- Trouver le numéro de contexte du vserver

```
# vserver test1 enter
ipv4root is now 10.95.81.71
Host name is now test1
New security context is 2
```

- Placer le numéro de contexte dans le fichier de conf du vserver

(*/etc/vservers/test1.conf*)

```
# Correction de l'erreur après "vserver test1 stop"
S_CONTEXT=2
```

Conflit IP entre vservers

Le nom d'une interface réseau est limité à **15 caractères**, y compris le "ethX:"

On peut donc avoir un nom d'interface avec 9 caractères significatifs jusqu'à 10 interfaces, et 8 caractères avec plus de 10 interfaces (à cause de "ethXX:").

Au delà, le nom de l'interface est **tronqué**, et le système considère les serveurs virtuels ayant la même racine commune comme étant une seule et même machine ⇒ Il y a conflit.

(et tant qu'on y est on ne peut pas avoir plus de 255 adresses par interfaces physique mais là 😊)

Configurations spécifiques

X sous vserver

X forwarding et ssh

Editer le fichier `/etc/ssh/sshd_conf`

```
X11Forwarding yes
X11UseLocalhost no
```

Ne pas oublier de renseigner l'ip de la machine dans `/etc/hosts` (sous la forme : "ip nom_d_hote").

Session X

Il faut ajouter au vserver la capacité `CAP_SYS_RAWIO` (dans la variable `S_CAPS` du fichier de configuration de vserver)

Sous debian, installer `x-window-system-core` et `xterm`

Mysql

Dans `/etc/mysql/my.cnf`

```
bind-address = 192.168.1.38
```

vsFtpd

Options à modifier dans `/etc/vsftpd.conf` :

```
listen_address=192.168.1.32
```

rsync

Options à modifier dans `/etc/default/rsync` :

```
--address=123.45.67.89
```

postgreSQL

Options à modifier dans `/etc/postgresql/postgresql.conf`

```
virtual_host = '192.168.1.32'
```

Liens externes

Excellente synthèse du “Debian Grimoire”	http://deb.riseup.net/vserver/
Présentation (fr)	http://mirabellug.org/wikini/wakka.php?wiki=VServers
Comment monter des vservers (fr)	http://linuxedouquebec.org/article.php3?id_article=69
Gerer des vservers (fr)	http://linuxedouquebec.org/article.php3?id_article=138
La page officielle	http://www.linux-vserver.org/
vserver sous Debian	http://lena.franken.de/linux/debian_and_vserver/
Les patches	http://www.13thfloor.at/vserver/project/
Images de systèmes Debian , Fedora et Redhat	http://www.lycos-vds.com/dists/
FAQ vserver	http://www.solucorp.qc.ca/howto.hc?projet=vserver
Le contenu de /etc/vservers	http://www-user.tu-chemnitz.de/~ensc/util-vserver/doc/conf/configuration.html
Les capabilities (droits des processus)	: http://www.lids.org/lids-howto/node34.html
Guide de l’administrateur vserver	http://www.linux-vserver.org/index.php?page=linux-vserver_administrators_guide