Be Seeing You
stef[@|.]genesix.org

serveur Debian 8 - Genesix v2 - Installation

Tux the Penguin by Carlos Pardo

J'utilise Linux non par satisfaction philosophique, mais pour trois raisons :

ça marche, ça marche à chaque fois, et ça marche à chaque fois de la même manière.

Kha.

Debian v8 - Serveur GENESIX v2 (Xen 4.4) - Installation

Indice	Validation	Objet	Réd.
1	25/11/16	Édition initiale	sr
12	02/01/17	Installation initiale : raid, lvm et xen	sr
17	01/04/17	Reprise de l'installation : réseau, domu	sr
40	12/05/17	Refonte de la documentation, ajout réseau, sécurité et performances	sr
49	23/05/17	Éclatement en deux documents : installation et exploitation	sr
52	25/05/17	Schéma architecture, suppression chapitre monitoring et anonymisation du document	sr
56	26/05/17	Exploitation restante en annexe, ajout navigation, corrections diverses	sr
57	28/05/17	Déport des tests réseau dans un document dédié aux tests	sr
64	20/06/17	Ajout sysctl.conf commun dom0 et domUs, corrections de typos	sr
66	03/07/17	Déport de la création d'un groupe de Fiffie-Hellman fort dans ce document	sr
74	30/07/17	Corrections de typos sur les hosts, mise à jour des connexions SSH par clés	sr
89	07/11/17	Mise à jour de la création d'un groupe de Diffie-Hellman fort	sr
96	22/12/17	Synchro horloge RTC et système périodique & ajustement de la dérive RTC (dom0 & domU)	sr
99	03/02/18	Ajouts Meltdown/Spectre, options de noyau au boot, normalisation nommage des dom	sr
100	19/02/18	Mise à jour de la section décrivant les bridges, corrections de typos	sr
102			

- Positionner le curseur sur l'avant dernière ligne du tableau (celle au dessus de « Édition courante ») ;
- Créer une nouvelle ligne dans le tableau ;
- Sélectionner et copier la dernière ligne, de « Validation » à « Rédacteur » (tout sauf la première colonne) ;
- Positionner le curseur sur l'avant dernière ligne, dans la colonne « Validation » ;
- Coller ;
  Reporter l'indice de la dernière ligne dans la nouvelle ligne.

Impression	25/05/17 - 14:03
Édition	SR - 807:40:21

« Be seeing you » Number six, The prisoner - « I have been studying how I may compare this prison where I live unto the world » - Richard II, Act V

Table des matières

stef[@|.]genesix.org

Généralités

1 Introduction

Ce document est dédié à la communauté OVH, aux corps OVH et aux piliers et pilières du bar@ovh. Mention spéciale à Octave en particulier et à la famille Klaba en général qui, gardant leur intégrité depuis le début de l'aventure, ont transmuté OVH en multinationale.

Longue vie et Prospérité. © Spock.

1.1 Présentation

Ce document décrit l'installation d'un serveur dédié chez OVH, sous Debian 8 Jessie stable et la version Xen 4.4 associée, et ne comprenant que des machines virtuelles para-virtualisées sous Debian 8 Jessie stable, stockées dans des volumes LVM, l'ensemble (boot, hyperviseur, swap et LVM) étant sous RAID 1 logiciel.

Debian 8 Jessie est maintenue jusqu'en mai 2018 et, en mode LTS, jusqu'en mai 2020.

Les références à l'hébergeur sont spécifiques à OVH mais peuvent être extrapolées.

Toute la configuration présentée a été réellement implémentée dans un serveur de production. Cette configuration est fonctionnelle et un soin particulier a été apporté à sa confection.

L'auteur encourage toute remarque constructive ou destructive (!) sur les choix présentés.

Par manque de temps, il n'y a pas de traduction en anglais (ou toute autre langue), mais une traduction (dans n'importe quelle langue) est vivement encouragée.

La mise à jour de ce document est permanente. De plus, il y aura une version Debian 9 Stretch et Xen 4.8. Les sections manquantes ou à développer sont signalées par le tag <<<TODO>>>.

1.2 Navigation

- Créer l'hyperviseur dom0

dom0 hyperviseur
dom initial
dom commun
dom0 réseau
dom0 sécurité

- Créer le domU modèle

domU modèle
domU réseau
domU sécurité

dom initial
dom commun

❑ Dupliquer le domU modèle dans un nouveau domU

domU duplication

1.3 Conventions

❑ Rédaction

<<<TODO>>>	Section du document à développer ou non encore rédigé

❑ Codification

Hyperviseur	dom0
VM	domuNNN (NNN=3 chiffres)
Serveur	rs11 : r = réseau,informatique, téléphonie + s = serveur + 11= n° d'ordre du serveur
Domaine	domaine.tld
Préfixe port SSH	pp

❑ IPs & ports SSH

IP serveur	i.j.k.l
Port SSH	pp63 : avec l=63
Bloc 16 IP FO	x.y.z.160/28 : IP de x.y.z.160 à x.y.z.175
Ports SSH	pp160 à pp175
Préfixe port SSH	pp

❑ IP et MAC des domUs

Réseaux intranets	n°1 : 192.168.**1**.x, n°2 : 192.168.**2**.x, etc.
Préfixe MAC Xen normalisé	00:16:3E

Pour le domu**210** (IP FO x.y.z.**164**) :

Interface	*Pont ou intranet*	*IP*	*MAC configurée*
eth**0**	br**210**	x.y.z.**164**	00:16:3E:0**0**:0**1**:**64**
eth**1**	veth**1**	192.168.**1**.**210**	00:16:3E:0**1**:0**2**:**10**
eth**2**	veth**2**	192.168.**2**.**210**	00:16:3E:0**2**:0**2**:**10**

❑ Noms

Host dom0	Host domu911
Host domu911	domu911.rs11
Domaine du dom0	dom0.rs11.domaine.tld

Host dom0	Host domu911
Domaine du domu911	domu911.rs11.domaine.tld

2 Serveur

Les caractéristiques complètes sont décrites dans : Debian v8 - Serveur GENESIX v2 (Xen 4.4) - Exploitation.

Caractéristiques utiles du serveur, dans le cadre de ce document :

Gamme	OVH
Type	Enterprise - SP-64-S (legacy)
Matériel	Supermicro, carte mère : X9SR

http://www.supermicro.com.tw/products/motherboard/Xeon/C600/X9SRE.cfm

Processeur

Processeur	Intel Xeon E5 1620v2
Cœurs / Threads	4 cores / 8 threads
Fréquence	3.7 GHz / 3,9 GHz
Cache	10 Mo
Préfixe port SSH	pp

http://ark.intel.com/fr/products/75779/Intel-Xeon-Processor-E5-1620-v2-10M-Cache-3_70-GHz

Équipement

RAM	64Go DDR3 ECC 1600 MHz
Disques	2x 2To
RAID	Soft
Carte réseau	1 GBps
Bande passante	500Mbps avec burst à 1 GHz
Trafic	Illimité
IPv4	1
IPv6	/64
IP failover	256 incluses
Anti-DDoS	Inclus
Espace de backup	500 G

3 Architecture

3.1 Généralités

L'architecture est fondée sur Xen et Debian :
- Xen : https://wiki.xenproject.org/wiki/Xen_Project_Software_Overview ;

- Debian : https://www.debian.org.

Genesix assure les services Web d'une startup, d'un part coté clients (sites Web, etc...) et d'autre part coté entreprise (infrastructure, cloud drive, sites Web, gestion commerciale, etc...), le tout ségrégué dans différents dom (VM en typologie Xen). En fonction du développement de l'activité, les domUs (VMs) seront déportés et/ou dupliqués dans d'autres serveurs.

3.2 Conception

La ligne directrice est le concept KISS (Keep It Simple Stupid).

Simple ne veux pas dire simpliste.

Les objectifs suivants ont été retenus :
- Simplicité ;
- Performance ;
- Souplesse ;
- Fiabilité ;
- Sécurité

Les objectifs se traduisent par l'architecture suivante :

	Simplicité	*Performance*	*Souplesse*	*Fiabilité*	*Sécurité*
Banalisation de l'OS sur tous les dom	X		X		
OS GNU/Linux Debian Jessie stable 8.6, kernel 3.16 ou 4.9 backporté suivant nécessité	X	X	X	X	X
Xen 4.4, l'hyperviseur libre plus polyvalent que KVM, avec des performances similaires à KVM		X	X	X	
Para Virtualisation (PV) uniquement, support des domUs sur LVM, lui-même sur RAID		X	X	X	
Aucune interface graphique de configuration. Cette dernière s'effectue en console via le manuel du serveur	X	X	X	X	X
Pas de routeur séparé en domU.	X	X	X	X	X
Le serveur accepte soit des groupes de domUs sur une seule IP, soit des domUs unitaires routées avec IP			X		
Outils de sécurité standard (rootkit, fail2ban)	X	X	X	X	X
Utilisation native des fonctionnalités réseau du noyau (interfaces, bridges, routages, pare-feu)	X	X	X	X	X

On obtient ainsi un serveur KISS, performant et très souple (en particulier concernant le mix des groupes de domUs nattées sur une seule IP et des VM unitaires routées avec IP spécifique).

Les domUs routées avec leur propres IP sont essentielles pour la réalisation de certains services, comme la VOIP. En effet, cette dernière est impossible à natter convenablement dans ce type de configuration et la solution classique est alors d'utiliser un VPN. Mais ce dernier peut avoir un impact fortement négatif sur la qualité de la communication. D'où l'importance d'avoir des domUs disposant de leurs propres IP.

3.3 Partitionnement

Le partitionnement est réduit à sa plus simple expression. Le manager d'OVH ne permet pas de partitionnements évolués, qui ne sont envisageables qu'avec debootstrap en rescue. Il n'est donc pas possible de cumuler simplement dès l'installation initiale les avantages du RAID1 (fiabilité) et de LVM (performances des domUs de Xen)

La partition de l'hyperviseur peut être extrêmement réduite. Un hyperviseur Xen en service depuis 5 ans, sur une Debian Etch, prend 1,5 Go.

```
Sys. de fichiers    Taille  Uti. Disp. Uti% Monté sur
/dev/md0              461M   93M  345M  22% /boot
/dev/md1              7,4G  1,5G  5,5G  21% /

576M    /usr
540M    /var
377M    /var/log
208M    /lib
83M     /boot
5,8M    /bin
5,8M    /etc
4,7M    /sbin
200K    /dev
16K     /tmp
```

L'hyperviseur sera sur une partition de 5,5 Go, le swap (obligatoire dans l'installation OVH) sera de 512 Mo et l'espace restant sera dédié aux VM, via LVM :

Partitions	*dom*	*Format*	*Affectation*	*Disque (Go)*
raid1 n°1	dom0	ext4fs	hyperviseur	5,5
raid1 n°2	domUx	ext4fs	espace VM	reste, via LVM
raid1 n°3		swap	hyperviseur	0,5

4 Sécurité

4.1 Généralités

❑ dom0

L'ouverture du dom0 est minimale. Seul un port SSH, non standard, est accessible à partir d'internet. Pendant le développement, l'accès est possible à partir d'un couple user/mot de passe (fort). Au passage à l'exploitation, l'accès est réduit à une clé SSH, disponible coté client sur un support sécurité (carte ou clé usb openpgp).

A partir du dom0, il est possible de se connecter aux domU. L'inverse n'est pas possible.

❑ domUs

L'ouverture des domUs est minimale. Seul un port SSH, non standard, est accessible à partir d'internet. Pendant le développement, l'accès est possible à partir d'un couple user/mot de passe (fort).

Au passage à l'exploitation, l'accès est réduit à une clé SSH, disponible coté client sur un support sécurité (carte ou clé usb openpgp).

Les domU liés par un intranet qui leur est propre (veth1, veth2, etc...) peuvent se connecter entre eux, dans la limite des ports ouverts spécifiquement (le défaut est une fermeture totale).

4.2 domU de supervision

Le domu50 est réservé à la supervision.

L'ouverture de ce domU est minimale. Seul un port SSH, non standard, est accessible à partir d'internet. Pendant le développement, l'accès est possible à partir d'un couple user/mot de passe (fort). Au passage à l'exploitation, l'accès est réduit à une clé SSH, disponible coté client sur un support sécurité (carte ou clé usb openpgp).

❑ CDES

Le domU de supervision contient le CDES : Centre de Délivrance des Éléments de Sécurité.

Le CDES gère :
- Le serveur de mot de passe, fondé sur Clipperz ;
- Les clés SSH de tous les domU ;
- Les certificats Let's Encrypt et leur diffusion vers les domU utilisateurs.

Ce CDES n'est pour l'instant qu'un jeu de scripts géré en entrée par des cron et des dates de certificats et produisant en sortie des certificats à jour, gérant leur distribution, avec envoi d'email d'informations. A terme, il sera implémenté sous la forme d'une véritable application Web sécurisée.

❑ Supervision

Le domU de supervision comprend les outils d'exploitation suivants :

<<< TODO>>>

4.3 Meltdown/Spectre

➪ Consultez : référence sysAdmin/Système - Debian/Noyau/Meltdown/Spectre.

Référence Xen : https://wiki.xenproject.org/wiki/Respond_to_Meltdown_and_Spectre

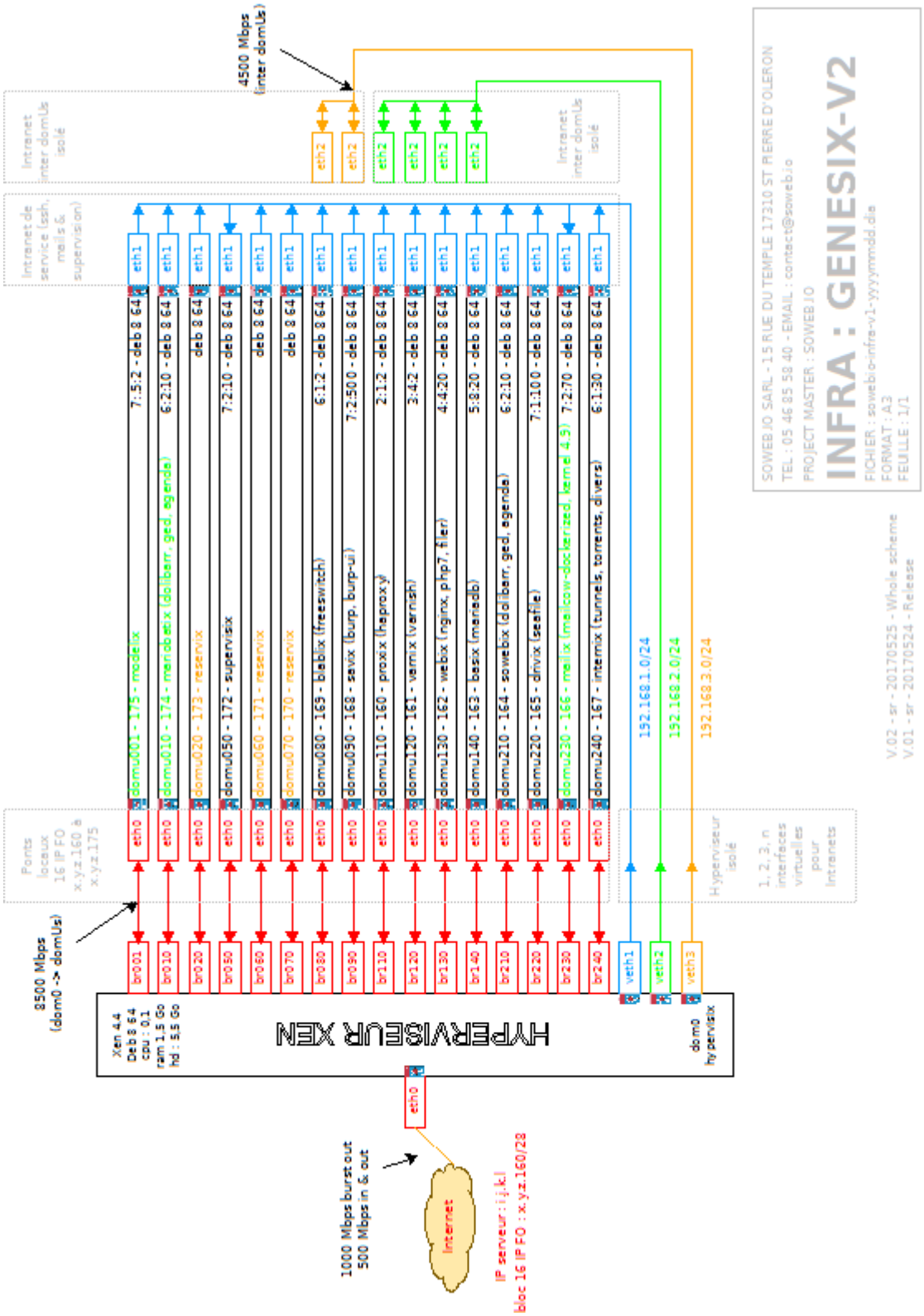

Illustration 1 : Genesix v2 - Architecture réseau

stef[@|.]genesix.org

dom0 hyperviseur

1 OVH

1.1 Distribution

Debian 8.4 stable 64 bits (c'est une 8.6 qui sera installée initialement)

Français
[x] Installation personnalisée

1.2 Partitionnement

Le manager OVH est très limité et impose une swap. On ne dit rien et on agira ensuite.

```
1  primary  ext4 /    raid1 5488 Mo
2  primary  ext4 /srv raid1 espace restant
3  primary  swap swp  raid1 512 Mo
```

La partition de l'hyperviseur (n°1) est fixée à environ 5,5 Go pour permettre les duplications de domu, qui requièrent 2 Go. Un hyperviseur consommant environ 1,5 Go, on gardera environ 2 Go d'espace disque de marge.

1.3 Configuration système

Hostname personnalisé : dom0.rs11.domaine.tld
[x] Utiliser le noyau de la distribution **<- Utiliser le noyau d'origine et non pas le spécifique OVH**

2 OVHcheries

Ce jeu de mot est amical car j'apprécie énormément OVH et son esprit, mais il décrit bien l'étendue des adaptations à réaliser, entre le noyau à changer, la swap à mettre en RAID 1 et la règle syslog-ng pour RTM : *il y a quand même un peu de temps à passer.*

2.1 Partitionnement

Le partitionnement effectué par le script OVH réserve une première partition pour le « boot BIOS[1] ». Pas le temps d'en chercher la raison. De ce fait, la numérotation des volumes RAID « md » s'en trouve décalée.

	RAID1	*dom*	*Format*	*Affectation*	*Disque (Go)*
/dev/sdx1					
/dev/sdx2	/dev/md2	dom0	ext4fs	hyperviseur dom0	5,5
/dev/sdx3	/dev/md3	domUs	lvm	espace domUs	reste

[1] Parlant de BIOS d'ailleurs, j'aurais bien aimé avoir accès au BIOS pour booster un peu le CPU. Je devine que l'option « power management » est forcé à « maximum performance » mais, paradoxalement, il faut choisir une autre option pour pouvoir activer le pilote Linux ad-hoc et contrôler manuellement la fréquence des coeurs (et ainsi pouvoir friser les 4 GHz par coeur).

	RAID 1	dom	For-mat	Affectation	Disque (Go)
/dev/sdx4	/dev/md4		swap	hyperviseur dom0	0,5

2.2 Mise à jour des sources et des paquets

Appliquer :

➪ dom initial

2.3 Remettre le noyau d'origine Debian

J'étais pourtant sûr d'avoir « [x] Utiliser le noyau de la distribution » mais je devais être en mode « poisson rouge ».

```
root@system: uname -r
3.14.32-xxxx-grs-ipv6-64
```

Ça, c'est du noyau OVH, avec GRSecurity, et à coup sûr sans le support Xen. Une vérification plus tard, via ftp://ftp.ovh.net/made-in-ovh/bzImage/latest-production confirme cette crainte.

Un petit tour sur packages.debian.org nous informe que le dernier noyau stable pour jessie est : linux-image-3.16.0-4-amd64. Par ailleurs, la page précise : « This kernel also runs on a Xen hypervisor. It supports both privileged (dom0) and unprivileged (domU) operation. »

```
root@system: aptitude install linux-image-3.16.0-4-amd64

    firmware-linux-free{a}  initramfs-tools{a}  klibc-utils{a}  libklibc{a}  libuuid-perl{a}  linux-base{a}
  linux-image-3.16.0-4-amd64
0 paquets mis à jour, 7 nouvellement installés, 0 à enlever et 0 non mis à jour.
```

Il faut ensuite déterminer quel noyau GRUB doit lancer (en partant de 0 pour la première entrée du menu, donc dans notre cas, c'est la seconde entrée, donc 1) :

```
root@system: grep menuentry /boot/grub/grub.cfg

menuentry "GNU/Linux with OVH Kernel, OVH kernel 3.14.32-xxxx-grs-ipv6-64"
menuentry 'Debian GNU/Linux, avec hyperviseur Xen'
menuentry 'Debian GNU/Linux'
```

Et renseigner /etc/default/grub :

```
/etc/default/grub
…
GRUB_DEFAULT = 1
…
```

Mettre à jour GRUB et rebooter.

```
root@system: update-grub

Création du fichier de configuration GRUB…
Found linux image: /boot/bzImage-3.14.32-xxxx-grs-ipv6-64
Image Linux trouvée : /boot/vmlinuz-3.16.0-4-amd64
Image mémoire initiale trouvée : /boot/initrd.img-3.16.0-4-amd64
Image Linux trouvée : /boot/vmlinuz-3.16.0-4-amd64
Image mémoire initiale trouvée : /boot/initrd.img-3.16.0-4-amd64
Image Linux trouvée : /boot/vmlinuz-3.16.0-4-amd64
Image mémoire initiale trouvée : /boot/initrd.img-3.16.0-4-amd64
fait


root@system: reboot
```

Vérification :

```
root@system: uname -r

3.16.0-4-amd64
```

Là, tout de suite, on se sent mieux.

Mais pourquoi Xen n'est-il pas intégré par défaut dans un noyau de *serveur* OVH ? La réponse est peut-être dans l'usage de GRSecurity, désormais abandonné depuis peu par OVH, puisque le développement libre a cessé[2]. La question d'un noyau spécifique mériterait d'être mieux expliquée. *Il y a certainement d'excellentes raisons à ça, mais faudrait-il encore les connaître*.

2.4 Swap en RAID1

La swap n'est pas en RAID1 par défaut, ce qui me semble une erreur de fiabilité majeure. *Je serais intéressé d'avoir un avis éclairé sur la question*.

En cas de panne d'un des disques, la swap sera corrompue et l'hyperviseur plantera immanquablement. Ce n'est certes pas ce que l'on souhaite, d'autant plus que les besoins en RAM de ce dernier sont faibles et très bien maîtrisés.

On pourrait la supprimer totalement et la reverser à la partition précédente /dev/md2 qui accueillera le LVM, mais il a été choisi de la reverser à la RAM, sous forme d'une swap de 512 Mo, afin de pouvoir, éventuellement, tester l'abaissement de la RAM physique allouée à l'hyperviseur.

Par défaut, une valeur très conservative de 1,5[3] Go de RAM physique a été affectée à l'hyperviseur.

Cette valeur est déjà très conséquente pour un gros serveur virtualisé (tant que l'on n'utilise pas des systèmes de stockage particuliers tels ZFS, ce qui n'est pas notre cas). On étudiera plus dans quelques pages le calcul de la mémoire nécessaire.

[2] https://grsecurity.net/passing_the_baton.php

[3] Voir chapitre 4.2 Paramétrage de Xen paramétrage du dom0

```
root@system: free -htl
             total       used       free     shared    buffers     cached
Mem:           31G       740M        30G        48M       116M       465M
Low:           31G       740M        30G
High:           0B         0B         0B
-/+ buffers/cache:       157M        31G
Swap:         1,0G         0B       1,0G
Total:         32G       740M        31G

-- Couper la swap

root@system: swapoff -a

root@system: free -htl
             total       used       free     shared    buffers     cached
Mem:           31G       740M        30G        48M       116M       465M
Low:           31G       740M        30G
High:           0B         0B         0B
-/+ buffers/cache:       157M        31G
Swap:           0B         0B         0B
Total:         31G       740M        30G
```

Commenter /dev/sda4 et /dev/sdb4 dans /etc/fstab, en profiter pour commenter également définitivement /dev/md3, puisqu'il va servir de volume RAID1 pour LVM :

/etc/fstab

```
# <file system> <mount point>   <type>  <options>       <dump>  <pass>

/dev/md2        /       ext4    errors=remount-ro,relatime      0       1
#/dev/md3        /srv    ext4    defaults,relatime       1       2
#/dev/sda4       swap    swap    defaults        0       0
#/dev/sdb4       swap    swap    defaults        0       0
proc            /proc   proc    defaults                0       0
sysfs           /sys    sysfs   defaults                0       0
tmpfs           /dev/shm        tmpfs   defaults        0       0
devpts          /dev/pts        devpts  defaults        0       0
```

Redémarrer :

```
root@system: reboot
```

Vérifier numéro de la partition de swap :

```
root@system: fdisk -l /dev/sda

Disque /dev/sda : 223,6 GiB, 240057409536 octets, 468862128 secteurs
Unités : secteur de 1 × 512 = 512 octets
Taille de secteur (logique / physique) : 512 octets / 4096 octets
taille d'E/S (minimale / optimale) : 4096 octets / 4096 octets
Type d'étiquette de disque : dos
Identifiant de disque : 0xa21fbdec

Device     Boot     Start       End   Sectors   Size Id Type

/dev/sda1          40       2048       2009 1004,5K BIOS boot
/dev/sda2        4096   11241471   11237376    5,4G Linux RAID
/dev/sda3    11241472 3905974271 3894732800    1,8T Linux RAID
/dev/sda4  3905974272 3907020799    1046528    511M Linux swap
```

Changer le type de partition :

stef[@|.]genesix.org

```
root@system: fdisk /dev/sda

Bienvenue dans fdisk (util-linux 2.25.2).
Les modifications resteront en mémoire jusqu'à écriture.
Soyez prudent avant d'utiliser la commande d'écriture.

Commande (m pour l'aide) : t
Numéro de partition (1-3, 3 par défaut) : 3
Code Hexa (taper L pour afficher tous les codes) :L

...
 21 Linux RAID                     A19D880F-05FC-4D3B-A006-743F0F84911E
...

Code Hexa (taper L pour afficher tous les codes) :21

Type de partition « Linux swap » modifié en « Linux RAID ».

Commande (m pour l'aide) : w
La table de partitions a été altérée.
Appel d'ioctl() pour relire la table de partitions.
Échec de relecture de la table de partitions.: Périphérique ou ressource occupé

Le noyau continue à utiliser l'ancienne table. La nouvelle sera utilisée lors du prochain démarrage
ou après avoir exécuté partprobe(8) ou kpartx(8).
```

Procéder à l'identique pour /dev/sdb et redémarrer :

```
root@system: reboot
```

Création du RAID1 pour la swap :

```
-- uniquement en cas de fail après une première passe
root@system: mdadm --zero-superblock /dev/sda4
root@system: mdadm --zero-superblock /dev/sdb4

-- Sinon passer directement à cette étape
root@system: mdadm --create /dev/md4 --level=1 --raid-disks=2 /dev/sda4 /dev/sdb4

-- Créer le point de montage du RAID1 et créer la swap
root@system: touch /dev/md/4
root@system: mkswap /dev/md4

-- Sauvegarder et recréer la conf
root@system: mv /etc/mdadm/mdadm.conf /etc/mdadm/mdadm.conf.bak
root@system: /usr/share/mdadm/mkconf > /etc/mdadm/mdadm.conf
```

Mettre à jour /etc/fstab :

/etc/fstab

```
# <file system> <mount point>   <type>  <options>       <dump>  <pass>

/dev/md2        /       ext4    errors=remount-ro,relatime      0       1
/dev/md4        swap    swap    defaults        0       0
#/dev/md3        /srv    ext4    defaults,relatime       1       2
#/dev/sda4       swap    swap    defaults        0       0
#/dev/sdb4       swap    swap    defaults        0       0
proc            /proc   proc    defaults                0       0
sysfs           /sys    sysfs   defaults                0       0
tmpfs           /dev/shm        tmpfs   defaults        0       0
devpts          /dev/pts        devpts  defaults        0       0
```


stef[@|.]genesix.org

Redémarrer :

```
root@system: reboot
```

On retrouve une swap active, cette fois en RAID1 :

```
root@system: free -htl
             total       used       free     shared    buffers     cached
Mem:           31G       169M        31G       8,8M       7,6M        46M
Low:           31G       169M        31G
High:           0B         0B         0B
-/+ buffers/cache:       115M        31G
Swap:         510M         0B       510M
Total:         31G       169M        31G
```

Noter que la taille de la swap est désormais divisée par deux. Les deux partitions originelles de 512 Mo ne s'additionnent plus.

2.5 Monitoring RAID

Dans /etc/mdadm/mdadm.conf, vérifier :

/etc/mdadm/mdadm.conf

```
…
MAILADDRE root
…
```

Modifier /etc/rc.local :

/etc/rc.local

```
#!/bin/sh -e
#
# rc.local
#
# This script is executed at the end of each multiuser runlevel.
# Make sure that the script will "exit 0" on success or any other
# value on error.
#
# In order to enable or disable this script just change the execution
# bits.
#
# By default this script does nothing.

#true > /etc/motd
#if [ -e /etc/lsb-release ]
#then
#       . /etc/lsb-release
#       [ -n "${DISTRIB_DESCRIPTION}" ] && echo "${DISTRIB_DESCRIPTION}" > /etc/motd
#fi
#uname -a >> /etc/motd
#echo >> /etc/motd
#echo "server    : `cat /root/.mdg 2>/dev/null`" >> /etc/motd
#echo "ip         : `cat /etc/network/interfaces | grep "address" | head -n 1 | cut -f 2 -d " "`"
>> /etc/motd
#echo "hostname  : `hostname`" >> /etc/motd
#echo >> /etc/motd
#/bin/cp /etc/motd /etc/issue

…
/sbin/mdadm --monitor --scan --daemonize
```

```
…

exit 0
```

Test email :

```
root@system: mdadm --monitor --test --oneshot /dev/md2
```

Spécifier un seul réseau raid est suffisant pour obtenir les informations sur tous les réseaux.

```
from    : mdadm monitoring <dom0.rs11@domaine.tld>
subject : TestMessage event on /dev/md2:dom0.rs11
to      : postmaster@domaine.tld

---

This is an automatically generated mail message from mdadm
running on dom0.rs11

A TestMessage event had been detected on md device /dev/md4.

Faithfully yours, etc.

P.S. The /proc/mdstat file currently contains the following:

Personalities : [raid1]
md4 : active (auto-read-only) raid1 sda4[0] sdb4[1]
      522944 blocks super 1.2 [2/2] [UU]

md3 : active raid1 sda3[0] sdb3[1]
      1947366336 blocks [2/2] [UU]
      bitmap: 0/15 pages [0KB], 65536KB chunk

md2 : active raid1 sda2[0] sdb2[1]
      5618624 blocks [2/2] [UU]

unused devices: <none>
```

2.6 RTM

RTM est une tache de supervision mise en place par OVH pour contrôler le serveur. Les résultats sont, entre autres, disponibles dans le panel d'administration d'OVH.
RTM est fort utile et doit être conservé, mais se signale dans /var/log/auth.log, au rythme de son lancement par *cron*, *toutes les minutes* (voir /etc/crontab), avec ce genre de log :

```
Apr  9 06:20:01 hypervisix CRON[22592]: pam_unix(cron:session): session opened for user root by (uid=0)
Apr  9 06:20:01 hypervisix CRON[22592]: pam_unix(cron:session): session closed for user root
Apr  9 06:21:01 hypervisix CRON[22634]: pam_unix(cron:session): session opened for user root by (uid=0)
Apr  9 06:21:01 hypervisix CRON[22634]: pam_unix(cron:session): session closed for user root
```

Ce qui rend auth.log illisible sur l'information pertinente, à savoir les véritables connexions, ou tentatives de connexions.

Ce problème, dont RTM n'est pas responsable, est réglé dans le chapitre dom Commun.

❑ Références

http://guide.ovh.com/RealTimeMonitoring
https://docs.ovh.com/pages/releaseview.action?pageId=9928706 (IP du monitoring OVH)
ftp://ftp.ovh.net/made-in-ovh/rtm

RTM est installé dans /usr/local/rtm.

3 LVM

3.1 Préalables

LVM, c'est beau, mais utilisé sans précautions, ça plantera forcément un jour et l'enfer tu connaîtras. Utiliser LVM sans un bon RAID est aussi subtil que de piloter un tracto-pelle en état d'ivresse ou de plonger dans une piscine vide : ça va *forcément* mal finir.

LVM est très intéressant pour un serveur avec des VM. Les performances sont bien meilleures[4] qu'avec des VM en fichiers, on a plus de souplesse également en redimensionnement, les snapshots et les backups sont facilités.

3.2 Installation

Le paquet lvm2 est déjà installé par défaut

Affecter à LVM le volume RAID1 /dev/md2 :

```
root@system: pvcreate /dev/md3
  Physical volume "/dev/md3" successfully created

root@system: vgcreate vg0 /dev/md3
  Volume group "vg0" successfully created

root@system: vgdisplay vg0
  --- Volume group ---

  --- Volume group ---
  VG Name               vg0
  System ID
  Format                lvm2
  Metadata Areas        1
  Metadata Sequence No  1
  VG Access             read/write
  VG Status             resizable
  MAX LV                0
  Cur LV                0
  Open LV               0
  Max PV                0
  Cur PV                1
  Act PV                1
  VG Size               1,81 TiB
  PE Size               4,00 MiB
  Total PE              475430
  Alloc PE / Size       0 / 0
  Free  PE / Size       475430 / 1,81 TiB
  VG UUID               fCMe1V-alUL-pYMJ-F2fn-OdwJ-eTys-O43p9A
```

[4] http://www.systutorials.com/2260/xen-domus-io-performance-of-lvm-and-loopback-backed-vbds

3.3 Contrôles

Test du LVM :

```
root@system: lvcreate -nvoltest -L2G vg0
  Logical volume "voltest" created

-- Infos sur les volumes physiques
root@system: pvs
  PV         VG   Fmt  Attr PSize PFree
  /dev/md3   vg0  lvm2 a--  1,81t 1,81t

-- Infos sur les « volumes groups »
root@system: vgs
  VG   #PV #LV #SN Attr   VSize VFree
  vg0    1   1   0 wz--n- 1,81t 1,81t

-- Infos sur les « logical volumes »
root@system: lvs
  LV      VG   Attr       LSize Pool Origin Data%  Meta%  Move Log Cpy%Sync Convert
  voltest vg0  -wi-a----- 2,00g

root@system: lvremove /dev/vg0/voltest
Do you really want to remove active logical volume voltest? [y/n]: y
  Logical volume "voltest" successfully removed
```

4 Xen

4.1 Installation

```
root@system: aptitude install xen-hypervisor-4.4-amd64

Les NOUVEAUX paquets suivants vont être installés :

   bridge-utils{a} ca-certificates{a} dbus{a} grub-xen-bin{a} grub-xen-host{a} ipxe-qemu{a} liba-
sound2{a} libasound2-data{a}    libasyncns0{a} libbluetooth3{a} libboost-system1.55.0{a} libboost-
thread1.55.0{a} libbrlapi0.6{a} libcaca0{a}    libcurl3-gnutls{a} libdbus-1-3{a} libdirectfb-1.2-
9{a}  libfdt1{a}  libflac8{a}  libice6{a}  libiscsi2{a}  libjpeg62-turbo{a}       libldap-2.4-2{a}
libnspr4{a} libnss3{a} libogg0{a} libopus0{a} libpixman-1-0{a} libpulse0{a} librados2{a} librbd1{a}
   librtmp1{a} libsasl2-2{a} libsasl2-modules{a} libsasl2-modules-db{a} libsdl1.2debian{a} libsec-
comp2{a} libsm6{a}    libsndfile1{a} libspice-server1{a} libusbredirparser1{a} libvdeplug2{a} lib-
vorbis0a{a} libvorbisenc2{a} libx11-6{a}     libx11-data{a} libx11-xcb1{a} libxau6{a} libxcb1{a}
libxdmcp6{a} libxen-4.4{a} libxenstore3.0{a} libxext6{a} libxi6{a}    libxtst6{a} libyajl2{a} qemu-
system-common{a} qemu-system-x86{a} qemu-utils{a} seabios{a} sharutils{a} x11-common{a}    xen-hy-
pervisor-4.4-amd64 xen-utils-4.4{a} xen-utils-common{a} xenstore-utils{a}

0 paquets mis à jour, 66 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de télécharger 19,3 Mo d'archives. Après dépaquetage, 66,2 Mo seront utilisés.
Voulez-vous continuer ? [Y/n/?]

.../...
```

4.2 Configuration

❑ Xen par défaut au démarrage

```
root@system: dpkg-divert --divert /etc/grub.d/08_linux_xen --rename /etc/grub.d/20_linux_xen
Ajout de « détournement local de /etc/grub.d/20_linux_xen en /etc/grub.d/08_linux_xen »
```

❑ Paramétrage de Xen

Utiliser la nouvelle toolstack « xl » (https://wiki.xen.org/wiki/Choice_of_Toolstacks)

Editer /etc/default/xen :

/etc/default/xen

```
#-------------------------------------------------------------------------------
# Default Xen configuration file
#-------------------------------------------------------------------------------

# Toolstack sélectionnée (redémarrer pour la prise en compte)

TOOLSTACK=xl

#-------------------------------------------------------------------------------
# EOF
#-------------------------------------------------------------------------------
```

Editer /etc/default/xendomains :

/etc/default/xendomains

```
#-------------------------------------------------------------------------------
# Default domU configuration file
#-------------------------------------------------------------------------------

# Pas de sauvegarde/restauration des domaines à l'arrêt/restauration

XENDOMAINS_SAVE=""
XENDOMAINS_RESTORE=false

# Répertoire des domU à lancer au démarrage du dom0

XENDOMAINS_AUTO=/etc/xen/auto

# Watchdog à l'arrêt des dom0 sur arrêt du dom0

XENDOMAINS_STOP_MAXWAIT=300

#-------------------------------------------------------------------------------
# EOF
#-------------------------------------------------------------------------------
```

Editer /etc/xen/xl.conf :

/etc/xen/xl.conf

```
#-------------------------------------------------------------------------------
# Global XL configuration file
#-------------------------------------------------------------------------------

# Mémoire dom0 fixe (un domU ne peut pas récupérer de la mémoire du dom0)

autoballoon=0

#-------------------------------------------------------------------------------
# EOF
#-------------------------------------------------------------------------------
```

❑ Paramétrage du dom0

- Références

https://wiki.xen.org/wiki/Tuning_Xen_for_Performance
https://wiki.xenproject.org/wiki/Xen_Project_Best_Practices
https://wiki.xen.org/wiki/Credit_Scheduler

- Ajustement de la mémoire

Appliquer cette formule, très conservatrice, valable tant que l'on n'utilise pas des systèmes de stockage particuliers tels ZFS : dom0_mem = 502 + int(physical_mem * 0.0205) . Il est possible de réduire le résultat au multiple de 256 arrondi par défaut (i.e. 1173 Mo arrondis à 1024 Mo pour 32 Go de ram et 1536 Mo pour 64 Go de ram).

Mémoire physique (Go)	*Mémoire dom0 (Mo)*
2	543
4	585
8	669
16	837
32	1173
64	1845

- Fixation des CPU alloués au dom0

Il est bénéfique de fixer la ou les CPU utilisés pour le dom0. Ce serveur est équipé d'un processeur 4 cœurs hyperthreadés, soient 8 vcpu. Cela signifie qu'un coeur va pouvoir exécuter deux threads (processus) à la fois.

Pour le dom0, il est souhaitable d'allouer un cœur entier, soit 2 vcpu via dom0_max_vcpus=2 puis de fixer ces vcpu (thread) à leur cpu (coeur physique) respectif par dom0_vcpus_pin. L'effet de ce paramétrage peut être constaté par :

```
root@system: xl vcpu-list

Name                                ID  VCPU   CPU State   Time(s) CPU Affinity
Domain-0                             0     0    0   r--    2001.4  0
Domain-0                             0     1    1   -b-    2544.7  1
domu001                              3     0    7   -b-       1.2  7
```

Le dom0 a bien 2 vcpus affectées, avec une affinité sur les cpu 0-1, donc le même cœur physique.

Pour ce serveur, il reste 3 cpu 2-3, 4-5 et 6-7, donc 6 vcpu numérotées 2,3,4,5,6,7.

- Ajustement du « schedule rate » et du « timeslice credit »

sched_ratelimit_us est déjà par défaut à 1000us et n'est repris en paramètre que pour référence.

sched_credit_tslice_ms est à 30 ms par défaut, ce qui est une valeur élevée, plutôt adaptée à du calcul intensif. Il est préférable de descendre à 10ms ou 5 ms.

- Augmentation du nombre de périphériques « loop »

Par défaut le pilote de périphérique « loop » n'autorise que 8 périphériques « loop ». Les domUs en mode bloc (quoique déconseillées pour des raisons de performance) utilisant deux périphériques « loop » par domU, il peut être prudent d'augmenter le nombre de périphériques « loop », même s'il n'est pas prévu d'utiliser de tels domUs :

Éditer /etc/default/grub :

```
/etc/default/grub

…
GRUB_CMDLINE_LINUX_DEFAULT="max_loop=64"
…
GRUB_TIMOUT = 0
…
GRUB_DISABLE_RECOVERY="true"
…
GRUB_CMDLINE_XEN="dom0_mem=1536M,max:1536M dom0_max_vcpus=2 dom0_vcpus_pin sched_ratelimit_us=1000
sched_credit_tslice_ms=10"
```

Mettre à jour GRUB :

```
root@system: update-grub

Création du fichier de configuration GRUB…
Found linux image: /boot/bzImage-3.14.32-xxxx-grs-ipv6-64

fait
```

Redémarrer :

```
root@system: reboot
```

4.3 Finalisations

❑ Répertoire de lancement automatique

Créer le répertoire pour le lancement automatique des domUs au démarrage :

```
root@system: mkdir /etc/xen/auto
```

❑ Amélioration de la commande xl

Pour éviter d'avoir à spécifier le chemin /etc/xen à chaque fois que l'on souhaite lancer un domU, modifier le lien symbolique du script /usr/sbin/@xl :

```
/usr/sbin/@xl

#!/bin/sh -e

curr_dir=`pwd` # Sauvegarde du chemin courant
cd /etc/xen    # Passage dans le répertoire des comUxxx.cfg

COMMAND="$(basename $0)"
TOOLSTACK=$(. /usr/lib/xen-common/bin/xen-toolstack); RET=$?; [ $RET -eq 0 ] || exit $RET

if [ "$(basename "$TOOLSTACK")" != "$COMMAND" ]; then
    echo "ERROR:  A different toolstack ($(basename "$TOOLSTACK")) have been selected!" >&2
    exit 1
fi

exec "$TOOLSTACK" "$@"

cd $curr_dir  # Retour au répertoire courant
```

Cette modification peut être écrasée à l'occasion d'une mise à jour de Xen.

Xen-Tools

Installer le paquet d'assistance à la création des domU :

```
root@system: aptitude install xen-tools

root@hyper:~# aptitude install xen-tools
Les NOUVEAUX paquets suivants vont être installés :

   debootstrap{a} debugedit{a} libauthen-sasl-perl{a} libconfig-inifiles-perl{a} libdata-validate-
domain-perl{a}    libdata-validate-ip-perl{a} libdata-validate-uri-perl{a} libelf1{a} libencode-lo-
cale-perl{a}  libexpect-perl{a}      libfile-listing-perl{a}  libfile-slurp-perl{a}  libfile-which-
perl{a} libfont-afm-perl{a} libhtml-form-perl{a}     libhtml-format-perl{a} libhtml-parser-perl{a}
libhtml-tagset-perl{a}  libhtml-tree-perl{a}  libhttp-cookies-perl{a}       libhttp-daemon-perl{a}
libhttp-date-perl{a} libhttp-message-perl{a} libhttp-negotiate-perl{a} libio-html-perl{a}
   libio-pty-perl{a} libio-socket-ssl-perl{a} libio-stty-perl{a} liblist-moreutils-perl{a} liblog-
message-perl{a}     liblog-message-simple-perl{a} liblua5.2-0{a} liblwp-mediatypes-perl{a} liblwp-
protocol-https-perl{a} libmagic1{a}    libmailtools-perl{a} libnet-domain-tld-perl{a} libnet-http-
perl{a} libnet-ipv6addr-perl{a} libnet-netmask-perl{a}     libnet-smtp-ssl-perl{a} libnet-ssleay-
perl{a} libnetaddr-ip-perl{a} libnetwork-ipv4addr-perl{a} librpm3{a} librpmbuild3{a}
   librpmio3{a} librpmsign1{a} libsocket6-perl{a} libterm-size-perl{a} libterm-ui-perl{a} libtext-
template-perl{a}   liburi-perl{a} libwww-perl{a} libwww-robotrules-perl{a} rinse{a} rpm{a} rpm-com-
mon{a} rpm2cpio{a} xen-tools

0 paquets mis à jour, 60 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de télécharger 11,7 Mo d'archives. Après dépaquetage, 22,8 Mo seront utilisés.
Voulez-vous continuer ? [Y/n/?]

.../...
```

4.4 Contrôles

Contrôle de l'installation de Xen :

```
root@system: xl info

host                   : hypersix
release                : 3.16.0-4-amd64
version                : #1 SMP Debian 3.16.36-1+deb8u2 (2016-10-19)
machine                : x86_64
nr_cpus                : 8
max_cpu_id             : 7
nr_nodes               : 1
cores_per_socket       : 4
threads_per_core       : 2
cpu_mhz                : 3700
```

```
hw_caps                : bfebfbff:2c100800:00000000:00007f00:77bee3ff:00000000:00000001:00000281
virt_caps              : hvm hvm_directio
total_memory           : 65501
free_memory            : 63124
sharing_freed_memory   : 0
sharing_used_memory    : 0
outstanding_claims     : 0
free_cpus              : 0
xen_major              : 4
xen_minor              : 4
xen_extra              : .1
xen_version            : 4.4.1
xen_caps                  : xen-3.0-x86_64 xen-3.0-x86_32p hvm-3.0-x86_32 hvm-3.0-x86_32p hvm-3.0-
x86_64
xen_scheduler          : credit
xen_pagesize           : 4096
platform_params        : virt_start=0xffff800000000000
xen_changeset          :
xen_commandline           : placeholder dom0_mem=1536M,max:1536M dom0_max_vcpus=2 dom0_vcpus_pin
sched_ratelimit_us=1000 sched_credit_tslice_ms=10
cc_compiler            : gcc (Debian 4.9.2-10) 4.9.2
cc_compile_by          : carnil
cc_compile_domain      : debian.org
cc_compile_date        : Thu Sep  8 18:27:06 UTC 2016
xend_config_format     : 4
```

Contrôle de la prise en compte des paramètres au boot :

```
root@system: xl sched-credit
Cpupool Pool-0: tslice=10ms ratelimit=1000us
Name                                ID Weight  Cap
Domain-0                             0    256    0


root@system: free -htl

             total       used       free     shared    buffers     cached
Mem:          1,4G       214M       1,2G       4,7M       9,9M        73M
Low:          1,4G       214M       1,2G
High:           0B         0B         0B
-/+ buffers/cache:       131M       1,3G
Swap:         510M         0B       510M
Total:        1,9G       214M       1,7G

root@system: xl vcpu-list
Name                                ID  VCPU   CPU State   Time(s) CPU Affinity
Domain-0                             0     0    0   -b-      40.5  0
Domain-0                             0     1    1   r--      36.3  1
```

Mémoire dom0 limitée à 1 Go, Schedule Rate et Timeslice mis à jour, dom0 limité à un coeur (2 cpu avec l'hyperthreading)

5 Hardware

➪ lspci, lsusb, smartmontools sont déjà disponibles.

5.1 Horloges RTC & système

```
root@system : aptitude install ntpdate
```

Créer /etc/cron.weekly/synctime :

```
/etc/cron.weekly/synctime

ntpdate pool.ntp.org || ( hwclock --adjust; hwclock --hctosys )
```

Appliquer les droits :

```
root@system : chmod +x /etc/cron.weekly/synctime
```

Note du man de hwclock : « It is good to do a *hwclock* --adjust just before the *hwclock* --hctosys at system startup time, and maybe periodically while the system is running via cron. »

5.2 SmartmonTools

Appliquer le chapitre « Smartmontools » de « serveur Debian 8 - APPLICATIONS »

5.3 Lm-sensors

Installer :

```
root@system: aptitude install lm-sensors
```

Après installation mais avant le redémarrage, tester par la séquence :

```
root@system: sensors-detect (confirmer le lancement au démarrage de coretemp)

sensors-detect
# sensors-detect revision 6209 (2014-01-14 22:51:58 +0100)
# System: Supermicro X9SRE/X9SRE-3F/X9SRi/X9SRi-3F [0123456789]

.../...
Intel digital thermal sensor...                             Success!
    (driver `coretemp')
.../...
Trying family `VIA/Winbond/Nuvoton/Fintek'...               Yes
Found `Nuvoton NCT5577D/NCT6776F Super IO Sensors'          Success!
    (address 0xa30, driver `nct6775')
.../...
Found `IPMI BMC KCS' at 0xca2...                            Success!
    (confidence 8, driver `to-be-written')
.../...
Probing for `Winbond W83627DHG/W83667HG/W83677HG'...        Success!
    (confidence 8, driver `use-isa-instead')
.../...
Probing for `Winbond W83791SD'...                           No
Client found at address 0x48

Now follows a summary of the probes I have just done.
Just press ENTER to continue:

Driver `coretemp':
  * Chip `Intel digital thermal sensor' (confidence: 9)

Driver `to-be-written':
  * ISA bus, address 0xca2
    Chip `IPMI BMC KCS' (confidence: 8)

Driver `nct6775':
  * ISA bus, address 0xa30
```

```
    Chip `Nuvoton NCT5577D/NCT6776F Super IO Sensors' (confidence: 9)

Note: there is no driver for IPMI BMC KCS yet.
Check http://www.lm-sensors.org/wiki/Devices for updates.

To load everything that is needed, add this to /etc/modules:
#----cut here----
# Chip drivers
coretemp
nct6775
#----cut here----
If you have some drivers built into your kernel, the list above will
contain too many modules. Skip the appropriate ones!

Do you want to add these lines automatically to /etc/modules? (yes/NO)yes
Successful!

Monitoring programs won't work until the needed modules are
loaded. You may want to run '/etc/init.d/kmod start'
to load them.

Unloading i2c-dev... OK
Unloading cpuid... OK

root@hypersix:/etc/default# /etc/init.d/kmod start
[ ok ] Starting kmod (via systemctl): kmod.service.


root@system: sensors (pour afficher les informations d'environnement)

i350bb-pci-0300
Adapter: PCI adapter
loc1:         +48.0°C  (high = +120.0°C, crit = +110.0°C)

coretemp-isa-0000
Adapter: ISA adapter
Physical id 0:  +32.0°C  (high = +86.0°C, crit = +100.0°C)
Core 0:         +29.0°C  (high = +86.0°C, crit = +100.0°C)
```

6 Finalisations

Appliquer :

- dom commun
- dom0 réseau
- dom0 sécurité

stef[@|.]genesix.org

dom0 réseau

1 Introduction

1.1 Présentation

Sur internet, en avril 2017, et à notre connaissance, aucune documentation ne décrit une implémentation fonctionnelle Debian 8.x / Xen 4.4+, utilisant la nouvelle toolstack par défaut XL, compatible OVH (et autres hébergeurs de serveurs dédiés physiques) permettant de :
- Ne perdre aucune IP dans un bloc d'IP FO ;
- Bridger une IP sur une VM sans bridger l'interface physique ;
- Autoriser le mix de VM nattées avec IP alias et de VM bridgées
- Autoriser des sous réseaux de VM séparés (intranets isolés les uns des autres).

Ce chapitre présente décrit une architecture non conventionnelle, compatible avec l'infrastructure des hébergeurs de serveurs et une implémentation fonctionnelle autorisant la connexion d'une IP publique sur une VM Xen via une route et un pont virtuel.

1.2 Problèmes documentaires

Depuis la version 4.5, la toolstack XM n'est plus intégrée et est totalement remplacée par la toolstack XL. Par un choix de conception (tout à fait compréhensible), la toolstack XL délègue à la distribution Linux, via l'administrateur, toute la partie réseau. Les automatismes de XM, qui créaient à la volée (plus ou moins bien) le réseau approprié (et rendait donc Xen plug'n play), ont donc disparus.

Aujourd'hui, la plupart des informations disponibles sur internet concernent :
- XenServer, qui est une émanation différente de Xen et utilisant la toolstack XE ;
- Xen jusqu'à la version 4.0, qui utilise exclusivement la toolstack XM ;
- Xen 4.1...4.4, qui autorise les toolstacks XM et XL mais avec des exemples n'utilisant que XM.

Sur internet, en avril 2017, hormis des centaines d'articles obsolètes, des forums pleins de questions d'administrateurs plantés ou des solutions inapplicables qui bridgent avec l'interface physique, *on ne trouve quasiment rien*.

1.3 Problèmes techniques

La plupart des hébergeurs de serveurs imposent une règle stricte : ne jamais configurer son interface physique comme un bridge, afin de ne pas diffuser une adresse MAC virtuelle sur le réseau de l'hébergeur.

Ne pas s'y conformer déclenche une fermeture immédiate du port réseau du serveur.

2 Solutions

2.1 Solutions non retenues

❑ Par bridge sur l'interface physique

Comme évoqué au paragraphe précédent, seuls les mode nat et route sont exploitables.

❑ par IP alias

Afin d'illustrer cette solution, j'ai déterré une thread, agrémentée du « point de vue du chef », avec comme proposition de solution l'ip aliasing, avec du Port-Forward pour les flux entrants et du SNAT pour les flux sortants.

---

https://forum.ovh.com/showthread.php/18800

```
oles@ovh.net
27/07/2007, 00h10
vous devez activer dans le kernel l'option hidden d'arp.
il ne faut pas que le kernel du serveur de base envoit
plus d'1 mac au switch. si c'est le cas, le switch coupe
votre port, car c'est un type d'attaque connu.

oles@ovh.net
27/07/2007, 01h45
non c'est pas ce que je dis.

dans kernel, si tu as eth0 et eth1, par défaut linux balance le mac
de eth1 sur eth1 et eth0 et l'inverse. c'est, soit disant, pour
augmenter les chances que ça marche. il faut desactiver l'option
dans /proc tout simplement. ainsi les interfaces virtuels que tu vas
créer ne vont pas balancer les mac sur eth0.

echo 1 > /proc/sys/net/ipv4/conf/all/arp_filter
et ça devrait ne plus poser de problemes.

artiflo
31/08/2007, 10h19

Merci, c'est malheureusement pareil. Le switch shutdown le port.

fulup
31/08/2007, 15h50

Pour faire suite à quelques mail que j'ai eu suite a ce thread voici quelques complement d'info. La
config par default de XEN en mode Bridge ne conviend pas a un hebergement multualisé qu'il soit
OVH, Dedibox ou autre. En effet par default le mode bridge de XEN genere des adresses MAC privées
pour les interfaces virtuelles des domU et lance des requettes DHCP pour obtenir une IP. Si l'on
reprend la meme config en remplacant les requettes DHCP par une IP fix en dur au niveau des domU,
il n'en reste pas moins que meme si l'adresse IP est bonne l'adresse MAC sera fausse, et que le
switch va bloquer tout votre traffic, ce qui est plus que normal.

Pour resoudre le probleme, plutot que je jouer a changer la logique des tables ARP du kernel, la
bonne solution consiste a donner toutes les adresses Failover comme alias de domO (ifconfig eth0:1
IP-failover-1, ...) et a mettre en place un sous reseau d'adresses privées pour les domU, ceci afin
de ne pas touchez pas la logique OVH et garder toutes vos bedouilles domU invisibles de l'infra-
structure OVH.

Pour ce faire, une fois toutes vos adresses failover misent en alias sur votre interface Ethernet
officielle dans domU, vous utiliser le Port-Forward pour rediriger les flux entrant (web,
mail, ...) vers le domU choisi et le SNAT pour les flux sortant (supervision, backup, ...). Il est
donc parfaitement inutile de changer les parametres de config de votre kernel !!!

Vous pouvez generez vos regles IPTABLE a la main, ou utiliser un script from le mien qui faira le
travail pour vous si vous accepter d'avoir une machine virtuelle par adresse IP http://www.fri-
du.org/download/sample...en-Scripts.tgz

- remplacer le Xen network script par network/Fridu-network.script. Le script XEN ne conviend pas
car bridge les domU avec l'interface ethernet ce qui dans notre cas n'est pas une bonne solution.
```

```
Donner une adresse privée à votre bridge dans /etc/xen/xend-config.sxp, ex: (network-script 'Fridu-
aXen-network.script brname=br0 braddr=10.10.1.1 brmask=255.255.255.0')
- donner a vos domU des adresses IP dans le range de votre bridge ex: domU-A=10.10.1.2, domU-
B=10.10.1.3,...
- editer le regle de votre firewall /etc/sysconfig/Fridu-firewall.config pour autorisé SSH a ce
connecter sur domU et faire le redirecte de vos port vers la bonne machine (voir example dans Fri-
du-firewall-Basic.config, plus Guru pour le mode Multi-IP)
- Verifier sur tout semble OK "Fridu-firewall.script start dummy=1 dump=/dev/tty"
- Valide votre firewall Fridu-firewall.script start
```

Comme déjà évoqué maintes fois, cette solution, pour autant qu'elle soit parfaitement valable, comporte quelques inconvénients, en imposant :
- Un script iptables dom0 volumineux si le serveur comporte beaucoup de domU ;
- De multiples scripts liés à Xen, ce qui n'est plus dans l'esprit de la toolstack XL ;
- De grandes difficultés à mettre en place un PABX dans une VM (je suis preneur de tout script iptables réellement fonctionnel pour gérer, en toute sécurité, les flux de multiples communications VOIP (incluant chacune une connexion SIP et deux connexions RDP aux ports variables).

2.2 Solution retenue

L'inspiration a été trouvée sur une page du site de l'hébergeur Hetzner[5], avec l'implémentation d'une solution pour Debian Lenny et hyperviseur KVM.

Cette solution a été adaptée à Debian 8 Jessie et Xen 4.4. Le dom0 route, sans natting FORWARD/SNAT ni ARP proxying, ce qui implique :
- Que les règles générales d'iptables du dom0 ne sont pas appliquées aux domUs ;
- Qu'on protégera chaque domU par ses règles spécifiques ;
- Que des règles particulières peuvent être appliquées au trafic entre domUs.
- Que des règles particulières peuvent être appliquées au trafic entre le dom0 et les domUs.

Avec cette solution :

- L'absence de natting FORWARD/SNAT favorise les services le traversant mal, tel la VOIP ;
- L'absence d'ARP proxying favorise la sécurité ;
- Libvirt gère seulement les domUs, pas le réseau.

Concrètement, cette solution permet, pour un bloc d'IP :

- D'exploiter toutes les IP du bloc *sans devoir en perdre trois* (IP de réseau, de passerelle et de broadcast) selon les préconisations d'OVH et des autres hébergeurs ;
- De contourner l'impossibilité de bridger l'interface physique, sous peine d'être immédiatement déconnecté pour diffusion de MAC locales en provenances des domUs de Xen ;
- D'avoir des intranets étanches entre différents groupes de domUs ;
- De ne pas grever les performances avec seulement trois règles iptables pour un bloc d'IP.

[5] https://wiki.hetzner.de/index.php/KVM_mit_Nutzung_aller_IPs_aus_Subnetz/en

❑ Architecture

Un environnement virtualisé sous Xen est composé de l'hyperviseur, le dom0 et de VMs, les domUs.

Si cet ensemble n'était pas virtualisé, le dom0 et les domUs seraient des ordinateurs reliés à switch, et ce switch serait relié à un routeur protégeant cet intranet du monde extérieur.

Si l'on prend toutes ces boites physiques pour les virtualiser dans une GNU/Linux Debian Xen, les dom0 et domUs reprennent leur place dans le serveur hébergé, le switch devient un bridge et le routeur devient netfilter (netfilter comprend les sous-systèmes iptables, conntrack et nat) :

- Le domU est connecté à un switch virtuel appelé bridge ;
- Le bridge est un switch avec deux ordinateurs connectés ;
- Le dom0 reçoit le flux du bridge et le route via netfilter.

❑ Notes

Hors mode bridge, donc en route ou natting, dans le panel d'OVH, il ne faut pas qu'une MAC virtuelle soit définie pour l'IP, sinon cette dernière n'est pas fonctionnelle.

L'implémentation nécessite :
- Des IP publiques, de préférences des IP FO (Fail Over) ;
- Les paquets Debian iptables et bridge-utils.

3 Implémentation

3.1 Reverse DNS

Le reverse DNS doit correspondre au nom de host.

❑ Créer l'entrée du reverse DNS

A partir du panel d'OVH, créer une entrée A dans la zone DNS domaine.tld :

```
dom0.rs11.domaine.tld. IN A i.j.k.l
```

Vérification (compter jusqu'à quelques heures pour la propagation) :

```
root@system: dig dom0.rs11.domaine.tld +short
i.j.k.l
```

❑ Reverse du serveur

A droite de [ns123456.ip-i-j-k.eu], cliquer sur le crayon [/].

Remplacer « ns123456.ip-i-j-k.eu » par « dom0.rs11.domaine.tld »

Vérification (compter jusqu'à quelques heures pour la propagation) :

```
root@system: >dig -x i.j.k.l +short

dom0.rs11.domaine.tld.
```

3.2 Interfaces

Mettre à jour /etc/modules afin de créer (une ou plusieurs) interface(s) virtuelle(s) :

```
…
# Interfaces virtuelles (2)
dummy numdummmies=2
…
```

Mettre à jour /etc/network/interfaces :

/etc/network/interfaces

```
#-------------------------------------------------------------------------------
# Interfaces - Configuration réseau pour GENESIX v2
#-------------------------------------------------------------------------------

#-------------------------------------------------------------------------------
# Interface locale
#-------------------------------------------------------------------------------

auto lo
iface lo inet loopback

#-------------------------------------------------------------------------------

auto eth0
iface eth0 inet static
        address         i.j.k.l
        netmask         255.255.255.0
        network         i.j.k.0
        broadcast       i.j.k.255
        gateway         i.j.k.254
        pointopoint     i.j.k.254


#-------------------------------------------------------------------------------
# Interfaces ponts pour les eth0 des domUs - bloc(s) d'IP(s) publiques(s)
#-------------------------------------------------------------------------------

auto  br001
iface br001 inet static
        address 192.168.175.1
        netmask 255.255.255.0
        pre-up brctl addbr $IFACE
        post-up route add -host x.y.z.175 $IFACE
        post-down brctl delbr $IFACE

auto  br010
iface br010 inet static
        address 172.30.174.1
        netmask 255.255.255.0
        pre-up brctl addbr $IFACE
        post-up route add -host x.y.z.174 $IFACE
        post-down brctl delbr $IFACE

auto  br020
iface br020 inet static
        address 192.168.173.1
```

```
        netmask 255.255.255.0
        pre-up brctl addbr $IFACE
        post-up route add -host x.y.z.173 $IFACE
        post-down brctl delbr $IFACE

auto  br050
iface br050 inet static
        address 192.168.172.1
        netmask 255.255.255.0
        pre-up brctl addbr $IFACE
        post-up route add -host x.y.z.172 $IFACE
        post-down brctl delbr $IFACE

auto  br060
iface br060 inet static
        address 192.168.171.1
        netmask 255.255.255.0
        pre-up brctl addbr $IFACE
        post-up route add -host x.y.z.171 $IFACE
        post-down brctl delbr $IFACE

auto  br070
iface br070 inet static
        address 192.168.170.1
        netmask 255.255.255.0
        pre-up brctl addbr $IFACE
        post-up route add -host x.y.z.170 $IFACE
        post-down brctl delbr $IFACE

auto  br080
iface br080 inet static
        address 192.168.169.1
        netmask 255.255.255.0
        pre-up brctl addbr $IFACE
        post-up route add -host x.y.z.169 $IFACE
        post-down brctl delbr $IFACE

auto  br090
iface br090 inet static
        address 192.168.168.1
        netmask 255.255.255.0
        pre-up brctl addbr $IFACE
        post-up route add -host x.y.z.168 $IFACE
        post-down brctl delbr $IFACE

auto  br110
iface br110 inet static
        address 192.168.160.1
        netmask 255.255.255.0
        pre-up brctl addbr $IFACE
        post-up route add -host x.y.z.160 $IFACE
        post-down brctl delbr $IFACE

auto  br120
iface br120 inet static
        address 192.168.161.1
        netmask 255.255.255.0
        pre-up brctl addbr $IFACE
        post-up route add -host x.y.z.161 $IFACE
        post-down brctl delbr $IFACE

auto  br130
iface br130 inet static
        address 192.168.162.1
        netmask 255.255.255.0
        pre-up brctl addbr $IFACE
        post-up route add -host x.y.z.162 $IFACE
        post-down brctl delbr $IFACE

auto  br140
iface br140 inet static
        address 192.168.163.1
        netmask 255.255.255.0
        pre-up brctl addbr $IFACE
        post-up route add -host x.y.z.163 $IFACE
        post-down brctl delbr $IFACE

auto  br210
iface br210 inet static
```


stef[@|.]genesix.org

```
        address 192.168.164.1
        netmask 255.255.255.0
        pre-up brctl addbr $IFACE
        post-up route add -host x.y.z.164 $IFACE
        post-down brctl delbr $IFACE

auto  br220
iface br220 inet static
        address 192.168.165.1
        netmask 255.255.255.0
        pre-up brctl addbr $IFACE
        post-up route add -host x.y.z.165 $IFACE
        post-down brctl delbr $IFACE

auto  br230
iface br230 inet static
        address 192.168.166.1
        netmask 255.255.255.0
        pre-up brctl addbr $IFACE
        post-up route add -host x.y.z.166 $IFACE
        post-down brctl delbr $IFACE

auto  br240
iface br240 inet static
        address 192.168.167.1
        netmask 255.255.255.0
        pre-up brctl addbr $IFACE
        post-up route add -host x.y.z.167 $IFACE
        post-down brctl delbr $IFACE

#--------------------------------------------------------------------------
# Interfaces virtuelles pour les eth1, eth2, ethX des domUs
#--------------------------------------------------------------------------

auto  dummy0
iface dummy0 inet manual

auto  veth1
iface veth1 inet static
        address   192.168.1.254
        netmask   255.255.255.0
        network   192.168.1.0
        broadcast 192.168.1.255
        bridge_ports dummy0
        bridge_stp off
        bridge_fd 0
        bridge_maxwait 0
        post-up ifconfig veth1 hw ether 00:16:3E:01:02:54

auto  dummy1
iface dummy1 inet manual

auto  veth2
iface veth2 inet static
        address   192.168.2.254
        netmask   255.255.255.0
        network   192.168.2.0
        broadcast 192.168.2.255
        bridge_ports dummy1
        bridge_stp off
        bridge_fd 0
        bridge_maxwait 0
        post-up ifconfig veth2 hw ether 00:16:3E:02:02:54

auto  dummy2
iface dummy2 inet manual

auto  veth3
iface veth3 inet static
        address   192.168.3.254
        netmask   255.255.255.0
        network   192.168.3.0
        broadcast 192.168.3.255
        bridge_ports dummy2
        bridge_stp off
        bridge_fd 0
        bridge_maxwait 0
        post-up ifconfig veth3 hw ether 00:16:3E:03:02:54
```

```
#-------------------------------------------------------------------------
# EOF
#-------------------------------------------------------------------------
```

Le paramètre *pointopoint* autorise un lien direct entre l'interface eth0 et son vis-à-vis, qui est nécessaire en regard du netmask restrictif, afin que les IP publiques des domUs puissent dans tous les cas atteindre l'eth0 du serveur.

Nous souhaitons pouvoir router entre les domUs, afin de contrôler les interactions entre eux, ce qui implique d'avoir un bridge par domU, avec une entrée dans la table de routage, le tout identifié par une IP de classe privée autonome (unique et ne faisant pas partie d'un réseau).

Ces opérations sont réalisées pour chaque bridge « br+[6] », dans l'exemple ci-dessous, provenant du script iptables décrit à la section suivante :

```
$IPTABLES -A FORWARD -i $EXTIF -o br+    -d x.y.z.160/28 -j ACCEPT # Internet > VM
$IPTABLES -A FORWARD -i br+    -o $EXTIF -s x.y.z.160/28 -j ACCEPT # domUs > Internet
```

Une fois en place, avec la plupart des domU lançés (sauf cinq, identifiables à leur bridge id à 0 et l'absence d'interface vif) et bridgés sur le bloc d'IP externes, et trois réseaux intranets (dont un inutilisé), on devrait obtenir ce genre de réponse :

```
root@system: brctl show

bridge name     bridge id               STP enabled     interfaces

br001           8000.000000000000       no
br010           8000.feffffffffff       no              vif26.0
br020           8000.000000000000       no
br050           8000.feffffffffff       no              vif27.0
br060           8000.000000000000       no
br070           8000.000000000000       no
br080           8000.feffffffffff       no              vif28.0
br090           8000.feffffffffff       no              vif29.0
br110           8000.feffffffffff       no              vif36.0
br120           8000.feffffffffff       no              vif35.0
br130           8000.000000000000       no
br140           8000.feffffffffff       no              vif34.0
br210           8000.feffffffffff       no              vif30.0
br220           8000.feffffffffff       no              vif31.0
br230           8000.feffffffffff       no              vif32.0
br240           8000.feffffffffff       no              vif33.0

veth1           8000.00163e010254       no              vif26.1 br010
                                                        vif27.1 br050
                                                        vif28.1 br080
                                                        vif29.1 br090
                                                        vif30.1 br210
                                                        vif31.1 br220
                                                        vif32.1 br230
                                                        vif33.1 br240
                                                        vif34.1 br110
                                                        vif35.1 br120
                                                        vif36.1 br140

veth2           8000.00163e020254       no              vif34.2 br110
                                                        vif35.2 br120
```

[6]Le « + » en syntaxe iptables est similaire à « * » en système de fichiers. Exemple avec « br+ » : toute interface commençant par « br » sera prise en compte.

```
                                                        vif36.2 br140

veth3           8000.00163e030254       no
```

3.3 Firewall/Routeur

❑ Conception

Le Firewall/Routeur du dom0 est inclus dans le dom0 lui-même et n'est pas déporté dans un domU. Il est fermé par défaut, et n'autorise que le strict nécessaire.

Il est totalement contenu dans un shell script, segmenté en deux grandes parties : la configuration du réseau et la configuration des règles.

Le nombre de ports ouvert est limité au strict nécessaire, et sur des ports non standards. Certains ports, comme les ports DNS ou HTTP, sont standard et ne peuvent répondre à cette exigence.

La sécurité locale est déléguée aux domUs.

❑ Script Iptables

Usage :

```
Genesix   (R) Firewall pour domUs Xen 4.4. Version 20170510.
Copyright (C) Stephane Riviere 2007-2017, tous droits libres.

Usage: /etc/firewall/firewall {start|stop|reload/restart|status}
```

Script :

```
#! /bin/sh
#------------------------------------------------------------------------------
#--- Firewall pour GENESIX v2 (dom0 Xen - HYPERVISEUR)
#------------------------------------------------------------------------------
#
# 20160125 : Initial release
# 20170413 : Genesix v2 update
# 20170510 : Genesix v2 full caps
# 20170515 : Genesix v2 add dropped packets debugging, symbols renaming
# 20170620 : Genesix v2 move all network parameters to /etc/sysctl.conf

VER=20170620

#------------------------------------------------------------------------------
### BEGIN INIT INFO
# Provides:          firewall
# Required-Start:    $remote_fs $syslog
# Required-Stop:     $remote_fs $syslog
# Default-Start:     2 3 4 5
# Default-Stop:      0 1 6
# Short-Description: Démarre les règles iptables
# Description:       Charge la configuration du pare-feu iptables
### END INIT INFO
#------------------------------------------------------------------------------

#--- Definitions

IPTABLES="/sbin/iptables"
DESC=Firewall

EXTIF=eth0

VIRTIF1=veth1
```

```
VIRTIF2=veth2
VIRTIF3=veth3

#--- Script

d_start() {


#=============================================================================
#=== FIREWALL INIT
#=============================================================================

        #--- Suppression de toutes les regles

        echo "$DESC : IPTABLES : Suppression de toutes les regles."

        $IPTABLES -F
        $IPTABLES -X
        $IPTABLES -t nat -F

        echo "$DESC : IPTABLES : Nouvelles chaines log."

# Debug
#       $IPTABLES -N LOG_DROP
#       $IPTABLES -A LOG_DROP -m limit --limit 1/s -j LOG --log-prefix '[Firewall DROP] '
#       $IPTABLES -A LOG_DROP -j DROP

# Not used
#       $IPTABLES -N LOG_ACCEPT
#       $IPTABLES -A LOG_ACCEPT -j LOG --log-prefix '[Firewall ACCEPT] '
#       $IPTABLES -A LOG_ACCEPT -j ACCEPT

        $IPTABLES -N LOG1_DROP
        $IPTABLES -A LOG1_DROP -j LOG --log-prefix '[Firewall TCP STATE] '
        $IPTABLES -A LOG1_DROP -j DROP

        $IPTABLES -N LOG2_DROP
        $IPTABLES -A LOG2_DROP -j LOG --log-prefix '[Firewall INVALID SOURCE] '
        $IPTABLES -A LOG2_DROP -j DROP

# Not used
#       $IPTABLES -N LOG3_DROP
#       $IPTABLES -A LOG3_DROP -m limit --limit 1/s -j LOG --log-prefix '[Firewall NEW TCP NOT SYN] '
#       $IPTABLES -A LOG3_DROP -j DROP

# Not used
#       $IPTABLES -N LOG4_DROP
#       $IPTABLES -A LOG4_DROP -m limit --limit 1/s -j LOG --log-prefix '[Firewall LIMITING INCOMING] '
#       $IPTABLES -A LOG4_DROP -j DROP

        $IPTABLES -N LOG5_DROP
        $IPTABLES -A LOG5_DROP -j LOG --log-prefix '[Firewall INVALID PACKET] '
        $IPTABLES -A LOG5_DROP -j DROP

        $IPTABLES -N LOG6_DROP
        $IPTABLES -A LOG6_DROP -j LOG --log-prefix '[Firewall BANNED COUNTRY] '
        $IPTABLES -A LOG6_DROP -j DROP

        echo "$DESC : IPTABLES : Drop par defaut."

        $IPTABLES -P INPUT   DROP
        $IPTABLES -P OUTPUT  DROP
        $IPTABLES -P FORWARD DROP

        echo "$DESC : IPTABLES : Interface locale OK."

        $IPTABLES -A INPUT  -i lo -j ACCEPT
        $IPTABLES -A OUTPUT -o lo -j ACCEPT

        echo "$DESC : IPTABLES : Autorisation PING."

        $IPTABLES -A INPUT  -p icmp -j ACCEPT
        $IPTABLES -A OUTPUT -p icmp -j ACCEPT
        $IPTABLES -A INPUT  -p igmp -j ACCEPT
        $IPTABLES -A OUTPUT -p igmp -j ACCEPT

#=============================================================================
#=== FIREWALLL PROTECTION
#=============================================================================

        #-----------------------------------------------------------------
        #--- Protection de base
        #-----------------------------------------------------------------

        echo "$DESC : IPTABLES : Limitations PING (ping of the death)."

        # Limitations Ping
        $IPTABLES -A INPUT   -p icmp --icmp-type echo-request -m limit --limit 10/s -j ACCEPT

        # SYN flooding protection
```

```
        $IPTABLES -N syn-flood
        $IPTABLES -A INPUT -i $EXTIF -p tcp --syn -j syn-flood
        $IPTABLES -A syn-flood -m limit --limit 10/s --limit-burst 15 -j RETURN
        $IPTABLES -A syn-flood -m limit --limit 1/s -j LOG --log-prefix '[Firewall SYN FLOOD MAXRATE] '
        $IPTABLES -A syn-flood -j DROP

        # Fragments
        $IPTABLES -A INPUT -i $EXTIF -f -j LOG --log-prefix "[Firewall FRAGMENTS] : "
        $IPTABLES -A INPUT -i $EXTIF -f -j DROP

        # All of the bits are cleared
        $IPTABLES -A INPUT -p tcp --tcp-flags ALL NONE -j LOG1_DROP

        # SYN and FIN are both set
        $IPTABLES -A INPUT -p tcp --tcp-flags SYN,FIN SYN,FIN -j LOG1_DROP

        # SYN and RST are both set
        $IPTABLES -A INPUT -p tcp --tcp-flags SYN,RST SYN,RST -j LOG1_DROP

        # FIN and RST are both set
        $IPTABLES -A INPUT -p tcp --tcp-flags FIN,RST FIN,RST -j LOG1_DROP

        # FIN is set without the expected accompanying ACK
        $IPTABLES -A INPUT -p tcp --tcp-flags ACK,FIN FIN -j LOG1_DROP

        # PSH is set without the expected accompanying ACK
        $IPTABLES -A INPUT -p tcp --tcp-flags ACK,PSH PSH -j LOG1_DROP

        # URG is set without the expected accompanying ACK
        $IPTABLES -A INPUT -p tcp --tcp-flags ACK,URG URG -j LOG1_DROP

        #----------------------------------------------------------------------
        #--- Protection localisee
        #----------------------------------------------------------------------

        echo "$DESC : IPTABLES : Adresses IP invalides."

        # Adresses IP invalides
        #IPTABLES -A INPUT -i $EXTIF -s 192.168.0.0/16 -j LOG2_DROP
        $IPTABLES -A INPUT -d 127.0.0.0/8 -j LOG2_DROP

        # Adresses IP bannies par pays
        $IPTABLES -A INPUT -m geoip --src-cc CN -j LOG6_DROP #DROP
        $IPTABLES -A INPUT -m geoip --src-cc HK -j LOG6_DROP #DROP
        $IPTABLES -A INPUT -m geoip --src-cc KR -j LOG6_DROP #DROP
        $IPTABLES -A INPUT -m geoip --src-cc RU -j LOG6_DROP #DROP

        # Paquets invalides
        $IPTABLES -A INPUT -p tcp -m state --state INVALID -j DROP

#=============================================================================
#=== FIREWALL EXTIF
#=============================================================================

        echo "$DESC : IPTABLES : Autorisation des connexions sur $EXTIF."

        # Autorisation des connexions sortantes sur EXTIF
        $IPTABLES -A OUTPUT -o $EXTIF -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT

        # Autorisation des connexions entrantes existantes sur EXTIF
        $IPTABLES -A INPUT  -i $EXTIF -m state --state ESTABLISHED,RELATED -j ACCEPT

        echo "$DESC : IPTABLES : Règles $EXTIF de routage."

        #--- Redirection du bloc d'IP : x.y.z.160/28 ------------------

        echo "$DESC : IPTABLES : Redirection de bloc IP vers les domU."

        $IPTABLES -A FORWARD -i $EXTIF -o br+     -d x.y.z.160/28 -j ACCEPT # Internet > VM
        $IPTABLES -A FORWARD -i br+    -o $EXTIF -s x.y.z.160/28 -j ACCEPT # domUs > Internet
#       $IPTABLES -t nat -A POSTROUTING -o eth0 -s 192.168.1.0/24 -j SNAT --to-source i.j.k.l

        echo "$DESC : IPTABLES : Regles NET de routage vers le dom0."

        #--- SSH -------------------------------------------------------------

        $IPTABLES -A INPUT  -i $EXTIF -m state --state NEW,ESTABLISHED -p tcp --dport 60063 -j ACCEPT
        $IPTABLES -A OUTPUT -o $EXTIF -m state --state ESTABLISHED -p tcp --sport 60063 -j ACCEPT

        #--- IPERF -----------------------------------------------------------

        #$IPTABLES -A INPUT  -i $EXTIF -m state --state NEW,ESTABLISHED -p tcp --dport 65001 -j ACCEPT
        #$IPTABLES -A OUTPUT -o $EXTIF -m state --state ESTABLISHED -p tcp --sport 65001 -j ACCEPT


#=============================================================================
#=== FIREWALL VIRTF1 (pour supervision & messages de service)
#=============================================================================

        echo "$DESC : IPTABLES : Autorisation des connexions sur $VIRTIF1."
```


```
        # Autorisation des connexions sortantes sur VIRTIF1
        $IPTABLES -A OUTPUT -o $VIRTIF1 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT

        # Autorisation des connexions entrantes existantes sur VIRT0
        $IPTABLES -A INPUT  -i $VIRTIF1 -m state --state ESTABLISHED,RELATED -j ACCEPT

        echo "$DESC : IPTABLES : Règles $VIRTIF1 de routage."

        #--- SSH ------------------------------------------------------------

        #Hyperviseur isolé des domUs
        #$IPTABLES -A INPUT  -i $VIRTIF1 -m state --state NEW,ESTABLISHED -p tcp --dport 60063 -j ACCEPT
        #$IPTABLES -A OUTPUT -o $VIRTIF1 -m state --state ESTABLISHED -p tcp --sport 60063 -j ACCEPT


#=============================================================================
#=== FIREWALL VIRTIF2 (intranet pour groupes de domUs)
#=============================================================================

        echo "$DESC : IPTABLES : Autorisation des connexions sur $VIRTIF2."

        # Autorisation des connexions sortantes sur VIRTIF2
        $IPTABLES -A OUTPUT -o $VIRTIF2 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT

        # Autorisation des connexions entrantes existantes sur VIRTIF2
        $IPTABLES -A INPUT  -i $VIRTIF2 -m state --state ESTABLISHED,RELATED -j ACCEPT

        echo "$DESC : IPTABLES : Règles $VIRTIF2 de routage."

        #--- XXX ------------------------------------------------------------

        # Sans


#=============================================================================
#=== FIREWALL VIRTIF3 (intranet pour groupes de domUs)
#=============================================================================

        echo "$DESC : IPTABLES : Autorisation des connexions sur $VIRTIF3."

        # Autorisation des connexions sortantes sur VIRTIF3
        $IPTABLES -A OUTPUT -o $VIRTIF3 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT

        # Autorisation des connexions entrantes existantes sur VIRTIF3
        $IPTABLES -A INPUT  -i $VIRTIF3 -m state --state ESTABLISHED,RELATED -j ACCEPT

        echo "$DESC : IPTABLES : Règles $VIRTIF3 de routage."

        #--- XXX ------------------------------------------------------------

        # Sans

#=============================================================================
#=== FIREWALL LIMITATION DE DEBIT
#=============================================================================

#       # Limit incoming connection 30/secondes pour le port80
#       $IPTABLES -I INPUT -p tcp --dport 80 -i $EXTIF -m state --state NEW -m recent --set
#       $IPTABLES -I INPUT -p tcp --dport 80 -i $EXTIF -m state --state NEW -m recent --update --seconds 60 --hit-
count 30 -j LOG4_DROP

#       # UDP flood
#       $IPTABLES -N udp-flood
#       $IPTABLES -A INPUT -p udp -j udp-flood
#       $IPTABLES -A udp-flood -m limit --limit 1/s --limit-burst 2 -j RETURN
#       $IPTABLES -A udp-flood -m limit --limit 1/s -j LOG --log-prefix '[Firewall UDP FLOOD MAXRATE] '
#       $IPTABLES -A udp-flood -j DROP

        # Suppression des requêtes BPC/DHCP OVH (dom0)
        $IPTABLES -A INPUT -s 5.135.140.252 -j DROP
        $IPTABLES -A INPUT -s 5.135.140.253 -j DROP

        # Block and log udp
         $IPTABLES -A INPUT -p udp -m limit --limit 3/m --limit-burst 5 -j LOG --log-prefix '[Firewall DENIED UDP
PORT] '
        $IPTABLES -A INPUT -p udp -j DROP

        # Block and log tcp
         $IPTABLES -A INPUT -p tcp -m limit --limit 3/m --limit-burst 5 -j LOG --log-prefix '[Firewall DENIED TCP
PORT] '
        $IPTABLES -A INPUT -p tcp -j DROP


#=============================================================================
#=== FIREWALL INTERDICTION DU RELIQUAT
#=============================================================================

        echo "$DESC : IPTABLES : Regles finales : interdiction generale du reliquat."
```


stef[@|.]genesix.org

```
        # Debug reliquat (ne pas oublier de décommenter la règle dans FIREWALL INIT)
        #$IPTABLES -A INPUT   -j LOG_DROP
        #$IPTABLES -A OUTPUT  -j LOG_DROP
        #$IPTABLES -A FORWARD -j LOG_DROP

        # Normal
        $IPTABLES -A INPUT   -j DROP
        $IPTABLES -A OUTPUT  -j DROP
        $IPTABLES -A FORWARD -j DROP

        echo "$DESC : SCRIPT : Firewall demarre et operationnel."

}

d_stop() {

        echo "$DESC : SCRIPT : Suppression des regles."

        echo -n "$DESC : IPTABLES : Purge de la table des filtres : "
        $IPTABLES -t filter -F
        $IPTABLES -t filter -X
        echo "fait."

        echo -n "$DESC : IPTABLES : Purge la table NAT : "
        $IPTABLES -t nat -F
        $IPTABLES -t nat -X
        echo "fait."

        echo -n "$DESC : IPTABLES : Purge la table MANGLE : "
        $IPTABLES -t mangle -F
        $IPTABLES -t mangle -X
        echo "fait."

        echo -n "$DESC : IPTABLES : Accepter tout trafic : "
        $IPTABLES -P INPUT   ACCEPT
        $IPTABLES -P OUTPUT  ACCEPT
        $IPTABLES -P FORWARD ACCEPT
        echo "fait."

        echo "$DESC : SCRIPT : Firewall arrete"

}

d_status() {

        $IPTABLES -L

}

# Gestion des instructions du service

echo ""
echo "Genesix   (R) Firewall pour dom0 Xen 4.4. Version $VER."
echo "Copyright (C) Stephane Riviere 2007-2017, tous droits libres."
echo ""

case "$1" in
    start)
        d_start
        ;;
    stop)
        d_stop
        ;;
    reload)
        d_stop
        sleep 1
        d_start
        ;;
    restart)
        d_stop
        sleep 1
        d_start
        ;;
    status)
        d_status
        ;;
    *)
    echo "Usage: $0 {start|stop|reload/restart|status}"
    echo ""
    exit 1
    ;;
esac

exit 0
#------------------------------------------------------------------------------
#--- EOF
#------------------------------------------------------------------------------
```


stef[@|.]genesix.org

3.4 Configuration Systemd

❑ Droits d'exécution du script Iptables

```
root@system: chmod 755 /etc/firewall/firewall
```

❑ Configuration Systemd

Installer le fichier de configuration dans /etc/systemd/system :

/etc/systemd/system/firewall.service

```
[Unit]
Description=firewall

[Service]
Type=oneshot
ExecStart=/etc/firewall/firewall start
ExecStop=/etc/irewall/firewall stop
RemainAfterExit=yes

[Install]
WantedBy=multi-user.target
```

❑ Démarrage, contrôle et arrêt manuels :

```
root@system: iptables -L

root@system: systemctl start firewall
root@system: iptables -L

root@system: systemctl status firewall

root@system: systemctl stop firewall
root@system: iptables -L
```

❑ Création du démarrage automatique

```
root@system: systemctl enable firewall
```

Redémarrer pour tester le lancement automatique.

dom0 sécurité

1 Clés SSH

Créer le répertoire pour les clés SSH /root/.ssh et générer les clés :

```
root@system: mkdir /root/.ssh
root@system: ssh-keygen -t rsa -b 4096

Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
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:
e0:f7:73:a8:95:97:ec:a1:a4:60:75:ba:a2:94:32:8f root@dom0.rs11
The key's randomart image is:
+---[RSA 4096]----+
|                 |
|                 |
|      .          |
|     . .         |
|      . S .      |
|     . o + + .   |
|  o o o . B *    |
|   * ... * * .   |
|  E o. .+ . .    |
+-----------------+
```

2 Fail2ban

Sécurisation des accès.

➪ Appliquer le chapitre « Fail2Ban » de « serveur Debian 8 - APPLICATIONS »

Ce chapitre comprend le rejet des IP par pays via le firewall et la mise à jour régulière des IP.

domU modèle

1 domu001 modèle debian 8 64

Modèle pour la création de tous les autres dom Debian 8 64 bits.

1.1 Génération

Créer le fichier de configuration /etc/xen-tools/domu001.gen :

/etc/xen-tools/domu001.gen

```
#-------------------------------------------------------------------------------
# Fichier de création pour domU001 - Modèle Debian 8 64 via xen-create-image
#
# Utiliser les multiples d'unités G, M, k si nécessaire
#-------------------------------------------------------------------------------

# Main setup values

hostname = domu001

size     = 5G        # Volume domU
memory   = 512M      # Memory at boot
maxmem   = 512M      # Memory at max

# Networking setup values

ip         = 192.168.1.1
netmask    = 255.255.255.0
gateway    = 192.168.1.254
broadcast  = 192.168.1.255

# Architecture

kernel = /boot/vmlinuz-`uname -r`             # Default kernel is determined by dom0
initrd = /boot/initrd.img-`uname -r`          # Default ramdisk is determined by dom0
mirror = `xt-guess-suite-and-mirror --mirror` # Default mirror for debootstrap
dist   = `xt-guess-suite-and-mirror --suite`  # Default distribution is determined by dom0

arch   = amd64      # amd64 | i386
pygrub = 1          # Use pygrub at boot - recommended : https://wiki.xen.org/wiki/PyGrub

lvm          = vg0  # LVM volume group
fs           = ext4 # Filesystem
ext4_options = noatime,nodiratime,errors=remount-ro
noswap       = 1    # No swap

# Installation

install-method = debootstrap
genpass        = 0  # No password generation
passwd         = 1  # Ask for new root password
extension      =    # No extension for generated file

#-------------------------------------------------------------------------------
# EOF
#-------------------------------------------------------------------------------
```

Lancer la génération :

```
root@system: cp /etc/xen-tools/domu001.gen /etc/xen-tools/xen-tools.conf

root@system: xen-create-image


General Information
--------------------
Hostname       :  domu001
```

```
Distribution    :  jessie
Mirror          :  http://http.debian.net/debian/
Partitions      :  /               5G    (ext4)
Image type      :  full
Memory size     :  512M
Max mem size    :  512M
Bootloader      :  pygrub

Networking Information
----------------------
IP Address 1    : 192.168.1.1 [MAC: 00:16:3E:2C:4F:AF]
Netmask         : 255.255.255.0
Broadcast       : 192.168.1.255
Gateway         : 192.168.1.254


Creating ext4 filesystem on /dev/vg0/domu001-disk
Done
Installation method: debootstrap
Done

Running hooks
Done

No role scripts were specified.  Skipping

Creating Xen configuration file
Done

No role scripts were specified.  Skipping
Setting up root password
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
All done


Logfile produced at:
         /var/log/xen-tools/domu001.log

Installation Summary
--------------------
Hostname        :  domu001
Distribution    :  jessie
MAC Address     :  00:16:3E:2C:4F:AF
IP Address(es)  :  192.168.1.1
RSA Fingerprint :  2e:46:2c:c1:19:a6:7b:af:72:be:ef:85:34:12:d1:b1
Root Password   :  N/A
```

Le processus prend plusieurs minutes

Mettre en forme le fichier de configuration généré (les paramètres ajoutés sont commentés) :

/etc/xen/domu001.cfg

```
#-----------------------------------------------------------------------------
# domU001 - Modèle Debian 8 64 via xen-create-image
#
# Configuration file for the Xen instance domu1, created
# by xen-tools 4.5 on Mon Dec 12 16:45:30 2016.
#-----------------------------------------------------------------------------

name        = 'domu001'

vcpus       = '1'     # Number of vcpu allowed
cpus        = '7'     # Physical cpu affinity
memory      = '512'
maxmem      = '512'

bootloader  = '/usr/lib/xen-4.4/bin/pygrub'
root        = '/dev/xvda1 ro'
extra       = 'nokaiser nopti'  # Additional kernel boot options (related to meltdown/spectre)
```


stef[@|.]genesix.org

```
disk        = [ 'phy:/dev/vg0/domu001-disk,xvda1,w', ]

# domU avec communication inter domU
vif = [ 'ip=x.y.z.175,mac=00:16:3E:00:00:01,bridge=br001',        # IP publique
        'ip=192.168.1.1,   mac=00:16:3E:01:00:01,bridge=veth1' ]  # IP locale

#  Comportement

on_poweroff = 'destroy'
on_reboot   = 'restart'
on_crash    = 'restart'

#----------------------------------------------------------------------------
# EOF
#----------------------------------------------------------------------------
```

⇨ Tous les paramètres sont décrits dans le man suivant :

```
root@system: man xl.cfg
```

Lancer le domU001 :

```
root@system: xl create domu001

root@system: xl console domu001 (sortie par Ctrl + 5) <-cinq
```

1.2 Réseau

Appliquer :

⇨ domU réseau
⇨ domU sécurité

1.3 Paramétrage

Une fois l'accès au réseau établi, appliquer :

⇨ dom initial
⇨ dom commun

domU duplication

1 Création du domu010 à partir du modèle domu001

Caractéristiques du domu010 :
- Nom : domu010
- Host : domu010.rs11
- Hostname : domu010.rs11.domaine.tld
- eth0 sur IP FO x.y.z.174 (via pont br010)
- eth1 sur IP 192.168.1.10 (via intranet veth1)

1.1 dom0 - Duplication LVM

⇨ Arrêter, si ce n'était pas le cas, le modèle domu001 :

```
root@system: xl shutdown domu001
```

Suivre les instructions ci-dessous :

```
root@system: lvs

  LV           VG   Attr       LSize Pool Origin Data%  Meta%  Move Log Cpy%Sync Convert
  domu001-disk vg0  -wi-a----- 1,95g

# Créer un snapshot du domU (immédiat)

root@system: lvcreate --size 2G --snapshot --name domutmp-disk /dev/vg0/domu001-disk

  Reducing COW size 2,00 GiB down to maximum usable size 1,96 GiB.
  Logical volume "domuNNN-disk" created

root@system: lvs

  LV           VG   Attr       LSize Pool Origin       Data%  Meta%  Move Log Cpy%Sync Convert
  domu001-disk vg0  owi-a-s--- 1,95g
  domutmp-disk vg0  swi-a-s--- 1,96g      domu001-disk 0,00

# Copier le snapshot dans un fichier

root@system: dd if=/dev/vg0/domutmp-disk of=/root/domutmp.img bs=1k

2048000+0 enregistrements lus
2048000+0 enregistrements écrits
2097152000 octets (2,1 GB) copiés, 28,4737 s, 73,7 MB/s

#----------
# Si duplication vers système distant, du système distant :
root@system: root@system:> scp -c arcfour root@system-origin:/root/domutmp.img /root
#----------

# Création du volume d'accueil

root@system: lvcreate --size 2G --name domu010-disk vg0

  Logical volume "domu010-disk" created

# Copier le fichier dans le volume d'accueil

root@system: dd if=/root/domutmp.img of=/dev/vg0/domu010-disk bs=1k

2048000+0 enregistrements lus
2048000+0 enregistrements écrits
2097152000 octets (2,1 GB) copiés, 56,9182 s, 36,8 MB/s

root@system: lvs
```


stef[@].]genesix.org

```
  LV           VG   Attr       LSize Pool Origin Data%  Meta%  Move Log Cpy%Sync Convert
  domu001-disk vg0  owi-a-s--- 1,95g
  domu010-disk vg0  -wi-ao---- 2,00g
  domutmp-disk vg0  swi-a-s--- 1,96g      domu001-disk 0,00
```

Ajuster la taille du volume, si nécessaire :

```
root@system: lvs

  LV           VG   Attr       LSize  Pool Origin       Data%  Meta%  Move Log Cpy%Sync Convert
  domu001-disk vg0  owi-a-s---  2,00g
  domu010-disk vg0  -wi-a-----  2,95g

root@system: lvextend -L +2G /dev/vg0/domu010-disk

root@system: e2fsck -f /dev/vg0/domu010-disk

root@system: resize2fs /dev/vg0/domu010-disk

root@system: lvs

  LV           VG   Attr       LSize  Pool Origin       Data%  Meta%  Move Log Cpy%Sync Convert
  domu001-disk vg0  owi-a-s---  2,00g
  domu010-disk vg0  -wi-a-----  9,95g
```

Supprimer, si nécessaire, le volume temporaire :

```
root@system: lvremove /dev/vg0/domutmp-disk
root@system: rm /root/domutmp.img
```

Relancer, si nécessaire, le modèle domu001 :

```
root@system: xl create domu001
```

Notes

La conversion de snapshot en volume linéaire, plus efficace sur une même machine que l'emploi de « dd », ne semble pas fonctionner (boot et mount impossible). Cette procédure *inopérante* est indiquée ici en attendant la résolution du problème :

```
root@system: lvs

  LV           VG   Attr       LSize Pool Origin Data%  Meta%  Move Log Cpy%Sync Convert
  domu001-disk vg0  -wi-a----- 1,95g

# Créer un snapshot du domU (immédiat)

root@system: lvcreate --size 2G --snapshot --name domu010-disk /dev/vg0/domu001-disk

  Reducing COW size 2,00 GiB down to maximum usable size 1,96 GiB.
  Logical volume "domuNNN-disk" created

root@system: lvs

  LV           VG   Attr       LSize Pool Origin       Data%  Meta%  Move Log Cpy%Sync Convert
  domu010-disk vg0  owi-a-s--- 1,95g      domu001-disk 0,00
```


stef[@|.]genesix.org

```
  domu001-disk vg0  swi-a-s--- 1,96g

# Convertir le snapshot en volume autonome (non immédiat en fonction du volume)

root@system: lvconvert --splitsnapshot /dev/vg0/domu010-disk

Do you really want to split off active logical volume domuNNN-disk? [y/n]: y

  Logical Volume vg0/domu010-disk split from its origin.

# Affichage progression

root@system: dmsetup status

vg0-domu010--disk: 0 9216000 raid raid1 2 AA 1812384/4112384 idle 0

# Conversion terminée

root@system: dmsetup status

vg0-domu010--disk: 0 4096000 linear
vg0-domu001--disk: 0 4112384 linear

root@system: lvs

  LV           VG   Attr       LSize Pool Origin Data%  Meta%  Move Log Cpy%Sync Convert
  domu010-disk vg0  -wi-a----- 1,95g
  domu001-disk vg0  -wi-a----- 1,96g
```

1.2 dom0 - Paramétrage du domu010

❑ Configuration

Créer le fichier de configuration approprié :

/etc/xen/domu010.cfg

```
#-------------------------------------------------------------------------------
# domu010 - Modèle Debian 8 64 via xen-create-image
#-------------------------------------------------------------------------------

name        = 'domu010'

vcpus       = '1'     # Number of vcpu allowed
cpus        = '7'     # Physical cpu affinity
memory      = '512'
maxmem      = '512'

bootloader  =   '/usr/lib/xen-4.4/bin/pygrub'
root        =   '/dev/xvda1 ro'
disk        = [ 'phy:/dev/vg0/domu010-disk,xvda1,w', ]

# domU avec communication inter domU

vif = [ 'ip=x.y.z.pp174,               mac=00:16:3E:00:00:10,bridge=br010',   # IP publique
        'ip=192.168.1.10,       mac=00:16:3E:01:00:10,bridge=veth1' ]  # IP locale

#  Comportement

on_poweroff = 'destroy'
on_reboot   = 'restart'
on_crash    = 'restart'

#-------------------------------------------------------------------------------
# EOF
#-------------------------------------------------------------------------------
```

En particulier, ajuster :

```
name        = 'domu010'

vcpus       = '1'     # Number of vcpu allowed
cpus        = '7'     # Physical cpu affinity
memory      = '512'
maxmem      = '512'

disk        = [ 'phy:/dev/vg0/domu010-disk,xvda1,w', ]

# domU avec communication inter domU

vif = [ 'ip=x.y.z.pp174,               mac=00:16:3E:00:00:10,bridge=br010',    # IP publique
        'ip=192.168.1.10,       mac=00:16:3E:01:00:10,bridge=veth1' ]  # IP locale
```

❑ Lancement automatique du domu010 au démarrage du dom0

Créer le lien symbolique :

```
root@system: ln -s /etc/xen/domu010 /etc/xen/auto/domu010
```

❑ Lancement du domu010 :

```
root@system: xl create domu010

root@system: xl console domu010 (sortie par Ctrl + 5) <-cinq
```

1.3 domu010 - Paramétrage

⇨ Pour ce paramétrage via « xl console », utiliser « nano ».

❑ Réseau

Mettre à jour l'adresse de l'IP failover publique :

/etc/network/interfaces (domu010)

```
#-------------------------------------------------------------------------------
# Interfaces - Configuration réseau
#-------------------------------------------------------------------------------

#-------------------------------------------------------------------------------

auto lo
iface lo inet loopback

#-------------------------------------------------------------------------------

auto eth0
iface eth0 inet static
 address x.y.z.174
 gateway i.j.k.l
 netmask 255.255.255.255
 pointopoint i.j.k.l

#-------------------------------------------------------------------------------

# domU avec communication inter-domUs
auto eth1
iface eth1 inet static
 address 192.168.1.10
```

```
 netmask 255.255.255.0

#------------------------------------------------------------------------------
# EOF
#------------------------------------------------------------------------------
```

❑ SSH

Mettre à jour le port SSH :

/etc/ssh/sshd_config (domu010)

```
…
Port pp174
…
```

❑ Firewall

Mettre à jour le port SSH :

/etc/firewall/firewall (domu010)

```
…

SSHPORT=pp174

…
```

Redémarrer :

```
root@system: Ctrl + 5
root@system: xl shutdown domuNNN
root@system: xl create domuNNN
```

Se connecter par SSH et poursuivre le paramétrage :

```
root@system: aptitude update
root@system: aptitude upgrade
```

❑ Hosts

Pour ce paramétrage via SSH, reprendre l'utilisation de « mc ».

/etc/hostname

```
domu010.rs11
```

/etc/hosts

```
#------------------------------------------------------------------------------
#--- Hosts
#------------------------------------------------------------------------------

127.0.0.1       localhost.localdomain           localhost
```

```
# A paramétrer en fonction du dom

127.0.0.1       domu010.rs11.genesix.org        domu010
149.202.150.174 domu010.rs11.genesix.org        domu010

# veth1 : Intranet de supervision

192.168.1.1     domu001.veth1.local             domu001v1
192.168.1.10    domu010.veth1.local             domu010v1
192.168.1.20    domu020.veth1.local             domu020v1

192.168.1.50    domu050.veth1.local             domu050v1
192.168.1.60    domu060.veth1.local             domu060v1
192.168.1.70    domu070.veth1.local             domu070v1
192.168.1.80    domu080.veth1.local             domu080v1
192.168.1.90    domu090.veth1.local             domu090v1

192.168.1.110   domu110.veth1.local             domu110v1
192.168.1.120   domu120.veth1.local             domu120v1
192.168.1.130   domu130.veth1.local             domu130v1
192.168.1.140   domu140.veth1.local             domu140v1

192.168.1.210   domu210.veth1.local             domu210v1
192.168.1.220   domu220.veth1.local             domu220v1
192.168.1.230   domu230.veth1.local             domu230v1
192.168.1.240   domu240.veth1.local             domu240v1

192.168.1.254   dom0.veth1.local                dom0v1

# veth2 : Intranet Web

192.168.2.110   domu110.veth2.local             domu110v2
192.168.2.120   domu120.veth2.local             domu120v2
192.168.2.130   domu130.veth2.local             domu130v2
192.168.2.140   domu140.veth2.local             domu140v2

192.168.2.254   dom0.veth2.local                dom0v2

# veth3 : Intranet de réserve

# ...

192.168.3.254   dom0.veth3.local                dom0v3

#------------------------------------------------------------------------------
#--- EOF
#------------------------------------------------------------------------------
```

❑ Bannière domu010

/etc/banner

```
<newline>

##########################################################

 #####  ####### #     # #######  #####    ###   #     #
#     # #       ##    # #       #     #    #     #   #
#       #       # #   # #       #          #      # #
#  #### #####   #  #  # #####    #####     #       #
#     # #       #   # # #             #    #      # #
#     # #       #    ## #       #     #    #     #   #
 #####  ####### #     # #######  #####    ###   #     #

  SP-64-S Xeon E5 1620v2 4c/8t 3.9GHz 64Go ECC 2x2To

            OVH RBX5 Genesix (v2) domu010 <---------- mettre à jour n° de domu : 010

##########################################################
<newline>
<newline>
```

❑ Postfix

/etc/postfix/translate_from

```
root@localhost                domu010.rs11@domaine.tld
root@domu010.rs11             domu010.rs11@domaine.tld
root@domu010.rs11.domaine.tld domu010.rs11@domaine.tld
```

/etc/postfix/translate_to

```
root@domu010.rs11                    postmaster@domaine.tld
root@domu010.rs11.domaine.tld        postmaster@domaine.tld
postmaster@domu010.rs11.domaine.tld postmaster@domaine.tld
www-data@domu010.rs11.domaine.tld    postmaster@domaine.tld
```

Créer les .db :

```
root@system:    postmap /etc/postfix/translate_from
root@system:    postmap /etc/postfix/translate_to
```

❑ Reverse DNS

Le reverse DNS doit correspondre au nom de host.

❑ Créer l'entrée du reverse DNS

A partir du panel d'OVH, créer une entrée A dans la zone DNS domaine.tld :

```
domu010.rs11.domaine.tld. IN A x.y.z.174
```

Vérification (compter jusqu'à quelques heures pour la propagation) :

```
root@system: dig domu010.rs11.domaine.tld +short

x.y.z.174
```

❑ Reverse du serveur

A droite de [x.y.z.174], cliquer sur l'engrenage [O] > Modifier le reverse.

Remplacer « ip174.ip-x-y-z.eu. » par « domu010.rs11.domaine.tld. »

Vérification (compter jusqu'à quelques heures pour la propagation) :

```
root@system: dig -x x.y.z.174 +short

domu010.rs11.domaine.tld.
```

2 domu010 - Sécurité

2.1 Clés SSH publiques et privées

Créer le répertoire pour les clés SSH /root/.ssh et générer les clés :

```
root@system: mkdir /root/.ssh
root@system: ssh-keygen -t rsa -b 4096

Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
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:
e0:f7:73:a8:95:97:ec:a1:a4:60:75:ba:a2:94:32:8f root@dom0.rs11
The key's randomart image is:
+---[RSA 4096]----+
|                 |
|                 |
|      .          |
|     . .         |
|      . S .      |
|     . o + + .   |
|  o o o . B *    |
|   * ... * * .   |
|  E o. .+ . .    |
+-----------------+
```

3 Accès au domu010 par clé SSH

3.1 Accès par dom0 (hyperviseur)

Les clés privées id_rsa et publiques id_rsa.pub ont été crées dans /root/.ssh lors de l'installation du dom0. Le répertoire ./ssh et le fichier authorized_keys sont des noms imposés.

❑ Copie de la clé

A partir du dom0, copier la clé publique du dom0 vers le domu010, en passant par l'intranet de supervision veth1, en utilisant l'alias domu010v1 :

```
root@system: ssh-copy-id -p pp174 <user-root>@domu010v1


The authenticity of host '[domu010v1]:pp174 ([192.168.1.10]:pp174)' can't be established.
ECDSA key fingerprint is 24:.../...:50.
Are you sure you want to continue connecting (yes/no)? yes
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are
already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to
install the new keys

########################################################

 #####  ####### #     # #######  #####    ###   #     #
#     # #       ##    # #       #     #    #    #   #
#       #       # #   # #       #          #     # #
#  #### #####   #  #  # #####    #####     #      #
#     # #       #   # # #             #    #     # #
#     # #       #    ## #       #     #    #    #   #
```

```
 #####  ####### #     # #######  #####    ###   #     #

  SP-64-S Xeon E5 1620v2 4c/8t 3.9GHz 64Go ECC 2x2To

             OVH RBX5 Genesix (v2) domu010

######################################################

<user-root>@domu010v1's password: **********************

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh -p pp174 'sr@domu010v1'"
and check to make sure that only the key(s) you wanted were added.
```

❑ Contrôle

A partir du dom0, vérifier la connexion par clé :

```
root@system: ssh -p pp174 <user-root>@domu010v1

######################################################

 #####  ####### #     # #######  #####    ###   #     #
#     # #       ##    # #       #     #    #     #   #
#       #       # #   # #       #          #      # #
#  #### #####   #  #  # #####    #####     #       #
#     # #       #   # # #             #    #      # #
#     # #       #    ## #       #     #    #     #   #
 #####  ####### #     # #######  #####    ###   #     #

  SP-64-S Xeon E5 1620v2 4c/8t 3.9GHz 64Go ECC 2x2To

             OVH RBX5 Genesix (v2) domu010

######################################################

Last login: Thu Jun 22 12:16:03 2017 from ****.fbx.proxad.net

14:33-root@domu010:~>
```

❑ Script d'accès

Créer le script et lui donner les droits d'exécution :

```
root@system: touch /usr/local/bin/domu010
root@system: chmod 755 /usr/local/bin/domu010
```

Editer le scripts d'accès à domu010 :

```
/usr/local/bin/domu010

#!/bin/sh

ssh -p pp174 <user-root>@domu010v1
```

3.2 Accès par dom50 (superviseur)

Les clés privées id_rsa et publiques id_rsa.pub ont été crées dans /root/.ssh lors de l'installation du domu50.

❑ Copie de la clé

A partir du domu50, copier la clé publique du domu50 vers le domu010, en passant par l'intranet de supervision veth1, en utilisant l'alias domu010v1 :

```
root@system: ssh-copy-id -p pp174 <user-root>@domu010v1
```

❑ Contrôle

A partir du domu50, vérifier la connexion par clé :

```
root@system: ssh -p pp174 <user-root>@domu010v1
```


stef[@|.]genesix.org

domU réseau

1 Introduction

Caractéristiques du domU modèle domu001 :
- Nom : domu001
- Host : domu001.rs11
- Hostname : domu001.rs11.domaine.tld
- eth0 sur IP FO x.y.z.175 (via pont br001)
- eth1 sur IP 192.168.1.1 (via intranet veth1)

1.1 Présentation

⇨ Se reporter au chapitre : dom0 réseau

2 Implémentation

2.1 Reverse DNS

Le reverse DNS doit correspondre au nom de host.

❑ Créer l'entrée du reverse DNS

A partir du panel d'OVH, créer une entrée A dans la zone DNS domaine.tld :

```
domu001.rs11.domaine.tld. IN A x.y.z.175
```

Vérification (compter jusqu'à quelques heures pour la propagation) :

```
root@system: dig domu175.rs11.domaine.tld +short
x.y.z.175
```

❑ Reverse du serveur

A droite de [x.y.z.175], cliquer sur l'engrenage [O] > Modifier le reverse.

Remplacer « ip175.ip-x-y-z.eu. » par « domu001.rs11.domaine.tld. »

Vérification (compter jusqu'à quelques heures pour la propagation) :

```
root@system: dig -x x.y.z.175 +short
domu001.rs11.domaine.tld.
```

2.2 Interfaces

Mettre à jour :

/etc/network/interfaces (domu001)

```
#-------------------------------------------------------------------------------
# Interfaces - Configuration réseau
#-------------------------------------------------------------------------------

#-------------------------------------------------------------------------------

auto lo
iface lo inet loopback

#-------------------------------------------------------------------------------

auto eth0
iface eth0 inet static
 address x.y.z.175
 gateway i.j.k.l
 netmask 255.255.255.255
 pointopoint i.j.k.l

#-------------------------------------------------------------------------------

# domU avec communication inter-domUs
auto eth1
iface eth1 inet static
 address 192.168.1.1
 netmask 255.255.255.0

#-------------------------------------------------------------------------------
# EOF
#-------------------------------------------------------------------------------
```

Notez les adressages non conventionnels des paramètres *gateway* et *pointopoint* de l'eth0, soit l'IP du dom0.

2.3 Firewall/Routeur

❑ Conception

Le Firewall/Routeur du domU est fermé par défaut, et n'autorise que le strict nécessaire.

Il est totalement contenu dans un shell script, segmenté en deux grandes parties : la configuration du réseau et la configuration des règles.

Le nombre de ports ouvert est limité au strict nécessaire, et sur des ports non standards. Certains ports, comme les ports DNS ou HTTP, sont standard et ne peuvent répondre à cette exigence.

❑ Script Iptables

Usage :

```
Genesix   (R) Firewall pour domUs Xen 4.4. Version 20170510.
Copyright (C) Stephane Riviere 2007-2017, tous droits libres.

Usage: /etc/firewall/firewall {start|stop|reload/restart|status}
```

Script :

```
#! /bin/sh
#------------------------------------------------------------------------------
#--- Firewall pour GENESIX v2 (domUs Xen - MACHINES VIRTUELLES)
#------------------------------------------------------------------------------
#
# 20091031 : ks25865
# 20160125 : Initial release
# 20170413 : Genesix v2 update
# 20170510 : Genesix v2 full caps
# 20170515 : Genesix v2 add dropped packets debugging, symbols renaming
# 20170620 : Genesix v2 move all network parameters to /etc/sysctl.conf

VER=20170620

#------------------------------------------------------------------------------
### BEGIN INIT INFO
# Provides:          firewall
# Required-Start:    $remote_fs $syslog
# Required-Stop:     $remote_fs $syslog
# Default-Start:     2 3 4 5
# Default-Stop:      0 1 6
# Short-Description: Démarre les règles iptables
# Description:       Charge la configuration du pare-feu iptables
### END INIT INFO
#------------------------------------------------------------------------------

#--- Definitions

IPTABLES="/sbin/iptables"
DESC=Firewall

EXTIF=eth0

VIRTIF1=eth1
VIRTIF2=eth2

SSHPORT=pp175

#--- Script

d_start() {

#==============================================================================
#=== FIREWALL INIT
#==============================================================================

        #--- Suppression de toutes les regles

        echo "$DESC : IPTABLES : Suppression de toutes les regles."

        $IPTABLES -F
        $IPTABLES -X
        $IPTABLES -t nat -F

        echo "$DESC : IPTABLES : Nouvelles chaines log."

# Debug
#        $IPTABLES -N LOG_DROP
#        $IPTABLES -A LOG_DROP -m limit --limit 1/s -j LOG --log-prefix '[Firewall DROP] '
#        $IPTABLES -A LOG_DROP -j DROP

# Not used
#        $IPTABLES -N LOG_ACCEPT
#        $IPTABLES -A LOG_ACCEPT -j LOG --log-prefix '[Firewall ACCEPT] '
#        $IPTABLES -A LOG_ACCEPT -j ACCEPT

        $IPTABLES -N LOG1_DROP
        $IPTABLES -A LOG1_DROP -j LOG --log-prefix '[Firewall TCP STATE] '
        $IPTABLES -A LOG1_DROP -j DROP

        $IPTABLES -N LOG2_DROP
        $IPTABLES -A LOG2_DROP -j LOG --log-prefix '[Firewall INVALID SOURCE] '
        $IPTABLES -A LOG2_DROP -j DROP

# Not used
#       $IPTABLES -N LOG3_DROP
#       $IPTABLES -A LOG3_DROP -m limit --limit 1/s -j LOG --log-prefix '[Firewall NEW TCP NOT SYN] '
#       $IPTABLES -A LOG3_DROP -j DROP

# Not used
#       $IPTABLES -N LOG4_DROP
#       $IPTABLES -A LOG4_DROP -m limit --limit 1/s -j LOG --log-prefix '[Firewall LIMITING INCOMING] '
#       $IPTABLES -A LOG4_DROP -j DROP

        $IPTABLES -N LOG5_DROP
        $IPTABLES -A LOG5_DROP -j LOG --log-prefix '[Firewall INVALID PACKET] '
        $IPTABLES -A LOG5_DROP -j DROP

        $IPTABLES -N LOG6_DROP
```

```
        $IPTABLES -A LOG6_DROP -j LOG --log-prefix '[Firewall BANNED COUNTRY] '
        $IPTABLES -A LOG6_DROP -j DROP

        echo "$DESC : IPTABLES : Drop par defaut."

        $IPTABLES -P INPUT   DROP
        $IPTABLES -P OUTPUT  DROP
        $IPTABLES -P FORWARD DROP

        echo "$DESC : IPTABLES : Interface locale OK."

        $IPTABLES -A INPUT  -i lo -j ACCEPT
        $IPTABLES -A OUTPUT -o lo -j ACCEPT

        echo "$DESC : IPTABLES : Autorisation PING."

        $IPTABLES -A INPUT  -p icmp -j ACCEPT
        $IPTABLES -A OUTPUT -p icmp -j ACCEPT
        $IPTABLES -A INPUT  -p igmp -j ACCEPT
        $IPTABLES -A OUTPUT -p igmp -j ACCEPT


#================================================================================
#=== FIREWALL PROTECTION
#================================================================================

        #-------------------------------------------------------------------
        #--- Protection de base
        #-------------------------------------------------------------------

        echo "$DESC : IPTABLES : Limitations PING (ping of the death)."

        # Limitations Ping
        $IPTABLES -A INPUT   -p icmp --icmp-type echo-request -m limit --limit 10/s -j ACCEPT

        # SYN flooding protection
        $IPTABLES -N syn-flood
        $IPTABLES -A INPUT -i $EXTIF -p tcp --syn -j syn-flood
        $IPTABLES -A syn-flood -m limit --limit 10/s --limit-burst 15 -j RETURN
        $IPTABLES -A syn-flood -m limit --limit 1/s -j LOG --log-prefix '[Firewall SYN FLOOD MAXRATE] '
        $IPTABLES -A syn-flood -j DROP

        # Fragments
        $IPTABLES -A INPUT -i $EXTIF -f -j LOG --log-prefix '[Firewall FRAGMENTS] '
        $IPTABLES -A INPUT -i $EXTIF -f -j DROP

        # All of the bits are cleared
        $IPTABLES -A INPUT -p tcp --tcp-flags ALL NONE -j LOG1_DROP

        # SYN and FIN are both set
        $IPTABLES -A INPUT -p tcp --tcp-flags SYN,FIN SYN,FIN -j LOG1_DROP

        # SYN and RST are both set
        $IPTABLES -A INPUT -p tcp --tcp-flags SYN,RST SYN,RST -j LOG1_DROP

        # FIN and RST are both set
        $IPTABLES -A INPUT -p tcp --tcp-flags FIN,RST FIN,RST -j LOG1_DROP

        # FIN is set without the expected accompanying ACK
        $IPTABLES -A INPUT -p tcp --tcp-flags ACK,FIN FIN -j LOG1_DROP

        # PSH is set without the expected accompanying ACK
        $IPTABLES -A INPUT -p tcp --tcp-flags ACK,PSH PSH -j LOG1_DROP

        # URG is set without the expected accompanying ACK
        $IPTABLES -A INPUT -p tcp --tcp-flags ACK,URG URG -j LOG1_DROP

        #-------------------------------------------------------------------
        #--- Protection localisee
        #-------------------------------------------------------------------

        echo "$DESC : IPTABLES : Adresses IP invalides."

        # Adresses IP invalides
        #IPTABLES -A INPUT -i $EXTIF -s 192.168.0.0/16 -j LOG2_DROP
        $IPTABLES -A INPUT -d 127.0.0.0/8 -j LOG2_DROP

        # Adresses IP bannies par pays
        iptables -A INPUT -m geoip --src-cc CN -j LOG6_DROP #DROP
        iptables -A INPUT -m geoip --src-cc HK -j LOG6_DROP #DROP
        iptables -A INPUT -m geoip --src-cc KR -j LOG6_DROP #DROP
        iptables -A INPUT -m geoip --src-cc RU -j LOG6_DROP #DROP

        # Paquets invalides
        $IPTABLES -A INPUT -p tcp -m state --state INVALID -j DROP


#================================================================================
#=== FIREWALL EXTIF
#================================================================================
```

```
        echo "$DESC : IPTABLES : Autorisation des connexions sur $EXTIF."

        # Autorisation des connexions sortantes sur EXTIF
        $IPTABLES -A OUTPUT -o $EXTIF -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT

        # Autorisation des connexions entrantes existantes sur EXTIF
        $IPTABLES -A INPUT  -i $EXTIF -m state --state ESTABLISHED,RELATED -j ACCEPT

        echo "$DESC : IPTABLES : Regles $EXTIF de routage."

        #--- SSH ------------------------------------------------------------

        $IPTABLES -A INPUT  -i $EXTIF -m state --state NEW,ESTABLISHED -p tcp --dport $SSHPORT -j ACCEPT
        $IPTABLES -A OUTPUT -o $EXTIF -m state --state ESTABLISHED     -p tcp --sport $SSHPORT -j ACCEPT

        #--- DNS ------------------------------------------------------------

#       $IPTABLES -A INPUT  -i $EXTIF -m state --state NEW,ESTABLISHED -p tcp --dport 53 -j ACCEPT
#       $IPTABLES -A OUTPUT -o $EXTIF -m state --state ESTABLISHED     -p tcp --sport 53 -j ACCEPT
#       $IPTABLES -A INPUT  -i $EXTIF -m state --state NEW,ESTABLISHED -p udp --dport 53 -j ACCEPT
#       $IPTABLES -A OUTPUT -o $EXTIF -m state --state ESTABLISHED     -p udp --sport 53 -j ACCEPT

        #--- WEB ------------------------------------------------------------

#       $IPTABLES -A INPUT  -i $EXTIF -m state --state NEW,ESTABLISHED -p tcp --dport 80  -j ACCEPT
#       $IPTABLES -A OUTPUT -o $EXTIF -m state --state ESTABLISHED     -p tcp --sport 80  -j ACCEPT
#       $IPTABLES -A INPUT  -i $EXTIF -m state --state NEW,ESTABLISHED -p tcp --dport 443 -j ACCEPT
#       $IPTABLES -A OUTPUT -o $EXTIF -m state --state ESTABLISHED     -p tcp --sport 443 -j ACCEPT

        #--- EMAIL ----------------------------------------------------------

        # SMTPS tcp
#       $IPTABLES -A INPUT  -i $EXTIF -m state --state NEW,ESTABLISHED -p tcp --dport 465 -j ACCEPT
#       $IPTABLES -A OUTPUT -o $EXTIF -m state --state ESTABLISHED     -p tcp --sport 465 -j ACCEPT

        # SASL tcp
#       $IPTABLES -A INPUT  -i $EXTIF -m state --state NEW,ESTABLISHED -p tcp --dport 587 -j ACCEPT
#       $IPTABLES -A OUTPUT -o $EXTIF -m state --state ESTABLISHED     -p tcp --sport 587 -j ACCEPT

        # IMAPS tcp
#       $IPTABLES -A INPUT  -i $EXTIF -m state --state NEW,ESTABLISHED -p tcp --dport 993 -j ACCEPT
#       $IPTABLES -A OUTPUT -o $EXTIF -m state --state ESTABLISHED     -p tcp --sport 993 -j ACCEPT

        # POP3S tcp
#       $IPTABLES -A INPUT  -i $EXTIF -m state --state NEW,ESTABLISHED -p tcp --dport 995 -j ACCEPT
#       $IPTABLES -A OUTPUT -o $EXTIF -m state --state ESTABLISHED     -p tcp --sport 995 -j ACCEPT

        #--- APRS -----------------------------------------------------------

        # APRSC T2FRANCE IGATE tcp udp
#       $EXTIF -m state --state NEW,ESTABLISHED -p tcp --dport 14580 -j ACCEPT
#       $IPTABLES -A OUTPUT -o $EXTIF -m state --state ESTABLISHED     -p tcp --sport 14580 -j ACCEPT
#       $IPTABLES -A INPUT  -i $EXTIF -m state --state NEW,ESTABLISHED -p udp --dport 14580 -j ACCEPT
#       $IPTABLES -A OUTPUT -o $EXTIF -m state --state ESTABLISHED     -p udp --sport 14580 -j ACCEPT

        # APRSC T2FRANCE HTTP-Upload tcp udp
#       $IPTABLES -A INPUT  -i $EXTIF -m state --state NEW,ESTABLISHED -p tcp --dport 8080 -j ACCEPT
#       $IPTABLES -A OUTPUT -o $EXTIF -m state --state ESTABLISHED     -p tcp --sport 8080 -j ACCEPT
#       $IPTABLES -A INPUT  -i $EXTIF -m state --state NEW,ESTABLISHED -p udp --dport 8080 -j ACCEPT
#       $IPTABLES -A OUTPUT -o $EXTIF -m state --state ESTABLISHED     -p udp --sport 8080 -j ACCEPT

        # APRSC T2FRANCE HTTP-Status tcp
#       $IPTABLES -A INPUT  -i $EXTIF -m state --state NEW,ESTABLISHED -p tcp --dport 14501 -j ACCEPT
#       $IPTABLES -A OUTPUT -o $EXTIF -m state --state ESTABLISHED     -p tcp --sport 14501 -j ACCEPT


#=============================================================================
#=== FIREWALL VIRTIF1
#=============================================================================

        echo "$DESC : IPTABLES : Autorisation des connexions sur $VIRTIF1."

        # Autorisation des connexions sortantes sur VIRTIF1
        $IPTABLES -A OUTPUT -o $VIRTIF1 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT

        # Autorisation des connexions entrantes existantes sur INTIF
        $IPTABLES -A INPUT  -i $VIRTIF1 -m state --state ESTABLISHED,RELATED -j ACCEPT

        echo "$DESC : IPTABLES : Regles $VIRTIF1 de routage."

        #--- SSH ------------------------------------------------------------

        $IPTABLES -A INPUT  -i $VIRTIF1 -m state --state NEW,ESTABLISHED -p tcp --dport $SSHPORT -j ACCEPT
        $IPTABLES -A OUTPUT -o $VIRTIF1 -m state --state ESTABLISHED     -p tcp --sport $SSHPORT -j ACCEPT

        #--- IPERF ----------------------------------------------------------

        #$IPTABLES -A INPUT  -i $VIRTIF1 -m state --state NEW,ESTABLISHED -p tcp --dport 65001 -j ACCEPT
        #$IPTABLES -A OUTPUT -o $VIRTIF1 -m state --state ESTABLISHED     -p tcp --sport 65001 -j ACCEPT
```

```
#=============================================================================
#=== FIREWALL VIRTIF2
#=============================================================================

        echo "$DESC : IPTABLES : Autorisation des connexions sur $VIRTIF2."

        # Autorisation des connexions sortantes sur VIRTIF2
        $IPTABLES -A OUTPUT -o $VIRTIF2 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT

        # Autorisation des connexions entrantes existantes sur INTIF
        $IPTABLES -A INPUT  -i $VIRTIF2 -m state --state ESTABLISHED,RELATED -j ACCEPT

        echo "$DESC : IPTABLES : Regles $VIRTIF2 de routage."

        #--- XXX ----------------------------------------------------------------

        #$IPTABLES -A INPUT  -i $VIRTIF2 -m state --state NEW,ESTABLISHED -p tcp --dport $SSHPORT -j ACCEPT
        #$IPTABLES -A OUTPUT -o $VIRTIF2 -m state --state ESTABLISHED     -p tcp --sport $SSHPORT -j ACCEPT


#=============================================================================
#=== FIREWALL LIMITATIONS DE DEBIT
#=============================================================================

#       # Limit incoming connection 30/secondes pour le port80
#       $IPTABLES -I INPUT -p tcp --dport 80 -i $EXTIF -m state --state NEW -m recent --set
#       $IPTABLES -I INPUT -p tcp --dport 80 -i $EXTIF -m state --state NEW -m recent --update --seconds 60 --hit-
count 30 -j LOG4_DROP

#       # UDP flood
#       $IPTABLES -N udp-flood
#       $IPTABLES -A INPUT -p udp -j udp-flood
#       $IPTABLES -A udp-flood -m limit --limit 1/s --limit-burst 2 -j RETURN
#       $IPTABLES -A udp-flood -m limit --limit 1/s -j LOG --log-prefix '[Firewall UDP FLOOD MAXRATE] '
#       $IPTABLES -A udp-flood -j DROP

        # Block and log udp
         $IPTABLES -A INPUT -p udp -m limit --limit 3/m --limit-burst 5 -j LOG --log-prefix '[Firewall DENIED UDP
PORT] '
        $IPTABLES -A INPUT -p udp -j DROP

        # Block and log tcp
         $IPTABLES -A INPUT -p tcp -m limit --limit 3/m --limit-burst 5 -j LOG --log-prefix '[Firewall DENIED TCP
PORT] '
        $IPTABLES -A INPUT -p tcp -j DROP


#=============================================================================
#=== FIREWALL INTERDICTION DU RELIQUAT
#=============================================================================

        echo "$DESC : IPTABLES : Regles finales : interdiction generale du reliquat."

        # Debug reliquat (ne pas oublier de commenter la règle dans FIREWALL INIT)
        #$IPTABLES -A INPUT   -j LOG_DROP
        #$IPTABLES -A OUTPUT  -j LOG_DROP
        #$IPTABLES -A FORWARD -j LOG_DROP

        # Normal
        $IPTABLES -A INPUT   -j DROP
        $IPTABLES -A OUTPUT  -j DROP
        $IPTABLES -A FORWARD -j DROP

        echo "$DESC : SCRIPT : Firewall demarre et operationnel."

}

d_stop() {

        echo "$DESC : SCRIPT : Suppression des regles."

        echo -n "$DESC : IPTABLES : Purge de la table des filtres : "
        $IPTABLES -t filter -F
        $IPTABLES -t filter -X
        echo "fait."

        echo -n "$DESC : IPTABLES : Purge la table NAT : "
        $IPTABLES -t nat -F
        $IPTABLES -t nat -X
        echo "fait."

        echo -n "$DESC : IPTABLES : Purge la table MANGLE : "
        $IPTABLES -t mangle -F
        $IPTABLES -t mangle -X
        echo "fait."

        echo -n "$DESC : IPTABLES : Accepter tout trafic : "
        $IPTABLES -P INPUT   ACCEPT
```

```
        $IPTABLES -P OUTPUT  ACCEPT
        $IPTABLES -P FORWARD ACCEPT
        echo "fait."

        echo "$DESC : SCRIPT : Firewall arrete"

}

d_status() {

        $IPTABLES -L

}

# Gestion des instructions du service

echo ""
echo "Genesix   (R) Firewall pour domUs Xen 4.4. Version $VER."
echo "Copyright (C) Stephane Riviere 2007-2017, tous droits libres."
echo ""

case "$1" in
    start)
        d_start
        ;;
    stop)
        d_stop
        ;;
    reload)
        d_stop
        sleep 1
        d_start
        ;;
    restart)
        d_stop
        sleep 1
        d_start
        ;;
    status)
        d_status
        ;;
    *)
    echo "Usage: $0 {start|stop|reload/restart|status}"
    echo ""
    exit 1
    ;;
esac

exit 0

#------------------------------------------------------------------------------
#--- EOF
#------------------------------------------------------------------------------
```

2.4 Configuration Systemd

❑ Droits d'exécution du script Iptables

```
root@system: chmod 755 /etc/firewall/firewall
```

❑ Configuration Systemd

Installer le fichier de configuration dans /etc/systemd/system :

/etc/systemd/system/firewall.service

```
[Unit]
Description=firewall

[Service]
Type=oneshot
ExecStart=/etc/firewall/firewall start
ExecStop=/etc/irewall/firewall stop
RemainAfterExit=yes

[Install]
```


stef[@|.]genesix.org

```
WantedBy=multi-user.target
```

❑ Démarrage, contrôle et arrêt manuels :

```
root@system: iptables -L

root@system: systemctl start firewall
root@system: iptables -L

root@system: systemctl status firewall

root@system: systemctl stop firewall
root@system: iptables -L
```

❑ Création du démarrage automatique

```
root@system: systemctl enable firewall
```

Redémarrer pour tester le lancement automatique.

stef[@|.]genesix.org

1 Groupe de Diffie-Hellman fort

https://fr.wikipedia.org/wiki/%C3%89change_de_cl%C3%A9s_Diffie-Hellman

❑ Groupe de 2048 bits vs 4096 bits

Un groupe de 2048 bits est suffisant en 2017. Il nécessite une à deux minutes pour être créé.

Un groupe de 4096 bits est un luxe réservé à des applications critiques. La création d'un groupe de 4096 bits va prendre a minima 5 à 20 minutes , 12 minutes sur une thread d'un core @ 3,7 GHz, voire bien plus sur une VM partageant un coeur parmi plusieurs autres VM.

```
root@system: nice -n 19 openssl dhparam -out /etc/ssl/certs/dhparam.pem 4096

.....+.....................+.................
+.....................................................................................
…/…
+.....................................................................................
.............+..............................+.....................++*++*
```

❑ Renouvellement du groupe

Le groupe doit être régulièrement renouvellé, par un process en tâche de fond à une priorité minimale (via nice), toutes les nuits pour une application critique et toutes les semaines ou tous les mois pour les autres :

/etc/cron.[daily|weekly]/diffie-hellman

```
#!/bin/bash

nice -n 19 openssl dhparam -out /etc/ssl/certs/dhparam.pem 2048
echo -e "Le groupe de Diffie-Hellman EST renouvele. \n" | mail -s "[Diffie-Hellman] cron " postmaster@genesix.org
```

```
root@system: chmod 755 /etc/cron.[daily|weekly]/diffie-hellman
```

2 Fail2ban

Sécurisation des accès.

➪ Appliquer le chapitre « Fail2Ban » de « serveur Debian 8 - APPLICATIONS »

Ce chapitre comprend le rejet des IP par pays via le firewall et la mise à jour régulière des IP.

stef[@|.]genesix.org

1 Mise à jour des sources

A faire dès la première connexion.

Remplacement des sources OVH par les sources Debian :

/etc/apt/sources.list

```
deb http://http.debian.net/debian/ jessie main contrib non-free
deb-src http://http.debian.net/debian/ jessie main contrib non-free

deb http://security.debian.org/ jessie/updates main contrib non-free
deb-src http://security.debian.org/ jessie/updates main contrib non-free

# jessie-updates, previously known as 'volatile'
deb http://ftp.fr.debian.org/debian/ jessie-updates main contrib non-free
deb-src http://ftp.fr.debian.org/debian/ jessie-updates main contrib non-free

# jessie-backports, previously on backports.debian.org
deb http://http.debian.net/debian/ jessie-backports main
deb-src http://http.debian.net/debian/ jessie-backports main
```

2 Mise à jour des paquets

```
root@system: apt-get update
root@system: apt-get upgrade

root@system: dpkg -l
```

Passage au XXI^{ème} siècle : nettoyage des vimeries[7] paléolithiques et installation d'aptitude :

```
root@system: apt-get purge vim vim-*

root@system: dpkg -l

root@system: apt-get install aptitude
root@system: aptitude keep-all
```

Et maintenant, on n'utilise plus que aptitude

3 Résolutions DNS

Pour dom0

Configuration comme un domU, dans l'attente d'un serveur DNS local, installé plus avant dans la configuration.

[7] Vi procure certainement l'expérience utilisateur la plus proche de l'éditeur IBM XEDIT sur console IBM 3270, connectée à un main-frame IBM 3090 des années 1980. La seule différence est que vi ne nécessite pas, pour son utilisation, plusieurs tonnes de matériels, logés dans une salle climatisée, et consommant autant d'énergie qu'un TGV. C'est évidemment un énorme plus.

❑ Pour domU

/etc/resolv.conf

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

Recharger le réseau puis tester le réseau et la résolution DNS par :

```
root@system: systemctl restart networking
root@system: ping 8.8.8.8
root@system: ping www.google.fr
```

4 Nom de host

❑ Pour le dom0

domaine racine du serveur : domaine.tld
Nom du serveur : rs11
Nom du dom0 : dom0

/etc/hostname

```
dom0.rs11
```

/etc/hosts

```
#------------------------------------------------------------------------------
#--- Hosts
#------------------------------------------------------------------------------

127.0.0.1       localhost.localdomain           localhost

# A paramétrer en fonction du dom

127.0.0.1       dom0.rs11.domaine.tld           dom0
i.j.k.l         dom0.rs11.domaine.tld           dom0

# veth1 : Intranet de supervision

192.168.1.1     domu001.veth1.local             domu001v1
192.168.1.10    domu010.veth1.local             domu010v1
192.168.1.20    domu020.veth1.local             domu020v1

192.168.1.50    domu050.veth1.local             domu050v1
192.168.1.60    domu060.veth1.local             domu060v1
192.168.1.70    domu070.veth1.local             domu070v1
192.168.1.80    domu080.veth1.local             domu080v1
192.168.1.90    domu090.veth1.local             domu090v1

192.168.1.110   domu110.veth1.local             domu110v1
192.168.1.120   domu120.veth1.local             domu120v1
192.168.1.130   domu130.veth1.local             domu130v1
192.168.1.140   domu140.veth1.local             domu140v1

192.168.1.210   domu210.veth1.local             domu210v1
192.168.1.220   domu220.veth1.local             domu220v1
192.168.1.230   domu230.veth1.local             domu230v1
192.168.1.240   domu240.veth1.local             domu240v1

192.168.1.254   dom0.veth1.local                dom0v1
```

```
# veth2 : Intranet Web

192.168.2.110   domu110.veth2.local             domu110v2
192.168.2.120   domu120.veth2.local             domu120v2
192.168.2.130   domu130.veth2.local             domu130v2
192.168.2.140   domu140.veth2.local             domu140v2

192.168.2.254   dom0.veth2.local                dom0v2

# veth3 : Intranet de réserve

# ...

192.168.3.254   dom0.veth3.local                dom0v3

#------------------------------------------------------------------------------
#--- EOF
#------------------------------------------------------------------------------
```

❑ Pour le domU modèle

Caractéristiques du domU modèle domu001 :
- Nom : domu001
- Host : domu001.rs11
- Hostname : domu001.rs11.domaine.tld
- eth0 sur IP FO x.y.z.175 (via pont br001)
- eth1 sur IP 192.168.1.1 (via intranet veth1)

Adapter cette configuration en fonction de la codification des domUs :

/etc/hostname

```
domu001.rs11
```

/etc/hosts

```
#------------------------------------------------------------------------------
#--- Hosts
#------------------------------------------------------------------------------

127.0.0.1       localhost.localdomain           localhost

# A paramétrer en fonction du domU

127.0.0.1       domu001.rs11.domaine.tld        domu110
x.y.z.175       domu001.rs11.domaine.tld        domu110

# veth1 : Intranet de supervision

192.168.1.1     domu001.veth1.local             domu001v1
192.168.1.10    domu010.veth1.local             domu010v1
192.168.1.20    domu020.veth1.local             domu020v1

192.168.1.50    domu050.veth1.local             domu050v1
192.168.1.60    domu060.veth1.local             domu060v1
192.168.1.70    domu070.veth1.local             domu070v1
192.168.1.80    domu080.veth1.local             domu080v1
192.168.1.90    domu090.veth1.local             domu090v1

192.168.1.110   domu110.veth1.local             domu110v1
192.168.1.120   domu120.veth1.local             domu120v1
192.168.1.130   domu130.veth1.local             domu130v1
192.168.1.140   domu140.veth1.local             domu140v1

192.168.1.210   domu210.veth1.local             domu210v1
192.168.1.220   domu220.veth1.local             domu220v1
192.168.1.230   domu230.veth1.local             domu230v1
192.168.1.240   domu240.veth1.local             domu240v1
```

```
192.168.1.254   dom0.veth1.local                dom0v1

# veth2 : Intranet Web

192.168.2.110   domu110.veth2.local             domu110v2
192.168.2.120   domu120.veth2.local             domu120v2
192.168.2.130   domu130.veth2.local             domu130v2
192.168.2.140   domu140.veth2.local             domu140v2

192.168.2.254   dom0.veth2.local                dom0v2

# veth3 : Intranet de réserve

# ...

192.168.3.254   dom0.veth3.local                dom0v3

#-------------------------------------------------------------------------------
#--- EOF
#-------------------------------------------------------------------------------
```

➪ La codification des domUs est détaillée dans serveur Debian 8 - genesix v2 (Xen 4.4).ods

❑ Contrôle

Vérifier la suppression complète de l'ancien nom :

```
root@system: cd /etc
root@system: grep -rin <ancien nom>

...

# remplacer toutes les occurrences de <ancien nom> par <nouveau nom>
```

5 Configuration système

Remplacer /etc/sysctl.conf par :

```
#-------------------------------------------------------------------------------
#--- sysctl.conf pour GENESIX v2 (dom0 & domUs Xen)
#-------------------------------------------------------------------------------
#
# 20170620 : Initial release
# 20170620 : Syntax errors cleaning
# 20170801 : More syntax errors corrected
#
#-------------------------------------------------------------------------------


#--- Files

# System number of file handles
fs.file-max=4000000

# Process number of file handles (Default : 1048576 - 1024x1024)
fs.nr_open=4000000


#--- Memory

# VM Special - 0 instructs the kernel not to initiate swap until the amount of free
# and file-backed pages is less than the high water mark in a zone (Default : 60)
vm.swappiness=0
```


stef[@|.]genesix.org

```
# VM Special - (Default : 40%)
vm.dirty_ratio=100

# VM Special - (Default : 10%)
vm.dirty_background_ratio=1

# Maximum number of memory map areas a process may have (Default : 65536)
vm.max_map_count=262144


#--- Kernel

# Increase message queue (Default : 16384)
kernel.msgmnb=65536
kernel.msgmax=65536

# Make the addresses of mmap base, stack and VDSO page randomized
kernel.randomize_va_space=1

# Increase pid range (Default : 32768)
kernel.pid_max=65536


#--- Network : settings

# Router mode (ie more than one interface)
net.ipv4.ip_forward=1

# Mandatory with high connection rates
net.ipv4.ip_local_port_range=1024 65535

# Protect against the common 'SYN flood attack'.
net.ipv4.tcp_syncookies=1

# Protect Against TCP Time-Wait
net.ipv4.tcp_rfc1337=1

# Increase the tcp-time-wait buckets pool size to prevent simple DOS attacks
net.ipv4.tcp_max_tw_buckets=1440000

# Enables fast recycling of TIME_WAIT sockets.
net.ipv4.tcp_tw_recycle=1

# Allow reuse of sockets in TIME_WAIT state for new connections
# only when it is safe from the network stack's perspective.
net.ipv4.tcp_tw_reuse=1

# Maximal number of timewait sockets (Default : 16384)
net.ipv4.tcp_max_tw_buckets=5880000

# Maximal number of remembered connection requests (Default : 128)
net.ipv4.tcp_max_syn_backlog=3240000

# Maximal number of TCP sockets not attached to any user file handle  (Default : 16384)
net.ipv4.tcp_max_orphans=262144

# Decrease number of times SYNs for an TCP connection attempt will be retransmitted (Default : 6)
net.ipv4.tcp_syn_retries=3

# Decrease the time default value for connections to keep alive
net.ipv4.tcp_keepalive_time=300
net.ipv4.tcp_keepalive_probes=5
net.ipv4.tcp_keepalive_intvl=15

# Decrease the time default value for tcp_fin_timeout connection (Default : 60)
net.ipv4.tcp_fin_timeout=15

# Decrease number of times SYNACKs for passive TCP connection. (Default : 5)
net.ipv4.tcp_synack_retries=3

# The congestion window will not be timed out after an idle period
net.ipv4.tcp_slow_start_after_idle=0

# Congestion control choices available to non-privileged processes
net.ipv4.tcp_congestion_control=cubic

# Increase maximum number of neighbor entries allowed (Default : 1024)
net.ipv4.neigh.default.gc_thresh3=450560
```


stef[@|.]genesix.org

```
# Increase maximum number of entries to keep in the ARP cache (Default : 512).
net.ipv4.neigh.default.gc_thresh2=450560

# Increase minimum number of entries to keep in the ARP cache (Default : 512)
net.ipv4.neigh.default.gc_thresh1=225280

# Increase the ARP stale time (Default : 60)
net.ipv4.neigh.default.gc_stale_time=7200

# Disallow redirects
net.ipv4.conf.default.send_redirects=0

# Disallow packets with SRR option (Default : 1)
net.ipv4.conf.default.secure_redirects=0

# Disallow source routing
net.ipv4.conf.default.accept_source_route=0

# Disallow redirects (prevent MITM attacks)
net.ipv4.conf.default.accept_redirects=0

# Disallow redirects (prevent MITM attacks)
net.ipv4.conf.all.send_redirects=0

# Disallow redirects (prevent MITM attacks)
net.ipv4.conf.all.secure_redirects=0

# Strict mode as defined in RFC3704 Strict Reverse Path
net.ipv4.conf.all.rp_filter=1

# Don't log packets with impossible addresses to kernel log
net.ipv4.conf.all.log_martians=0

# Disallow packets with SRR option (Default : 1)
net.ipv4.conf.all.accept_source_route=0

# Disallow redirects
net.ipv4.conf.all.accept_redirects=0

# Disable select acknowledgments (SACKS) (Default : 0)
net.ipv4.tcp_sack=0

# Disallow TCP to send "duplicate" SACK (Default : 0)
net.ipv4.tcp_dsack=0

# Disable FACK congestion avoidance and fast retransmission (Default : 1)
net.ipv4.tcp_fack=0


#--- Network : icmp

# Allow ping
net.ipv4.icmp_echo_ignore_all=0

# Ignore all ICMP ECHO and TIMESTAMP sent via broadcast/multicast
net.ipv4.icmp_echo_ignore_broadcasts=1


#--- Network core : queue

# Network device queuing discipline for very high traffic
net.core.default_qdisc=fq

# Max input packets queued, when receives packets faster than kernel can process them. (Default :
1000)
net.core.netdev_max_backlog=64000


#--- Network core : socket buffer

# Max send socket buffer size in bytes (Default : 212992, Max : 67108864)
net.core.wmem_max=12582912

# Default send socket buffer size in bytes (Default : 212992, Max : 67108864)
net.core.wmem_default=31457280

# Max receive socket buffer size in bytes (Default : 212992, Max : 67108864)
net.core.rmem_max=12582912
```


stef[@|.]genesix.org

```
# Default receive socket buffer size in bytes (Default : 212992, Max : 67108864)
net.core.rmem_default=31457280

# Increase number of incoming connections (Default : 128)
net.core.somaxconn=4096

# Increase number of incoming connections backlog (Default : 1000)
net.core.netdev_max_backlog=65536

# Increase the maximum amount of option memory buffers (Default : 20480)
net.core.optmem_max=25165824


#--- Network ipv4 : increase buffer-space

# (Default : 4096 87380 6291456, Max : 4096 87380 33554432)
net.ipv4.tcp_rmem=8192 87380 16777216

# (Default : 4096 16384 4194304, Max : 4096 65536 33554432)
net.ipv4.tcp_wmem=8192 65536 16777216

# (Default : 4096)
net.ipv4.udp_rmem_min=16384

# (Default : 4096)
net.ipv4.udp_wmem_min=16384

# buffer-space allocatable in units 4096 bytes (Default : 95226 126969 190452, computed at boot)
net.ipv4.tcp_mem=65536 131072 262144

# buffer-space allocatable in units 4096 bytes (Default : 95226 126969 190452, computed at boot)
net.ipv4.udp_mem=65536 131072 262144


#------------------------------------------------------------------------------
#--- EOF
#------------------------------------------------------------------------------
```


stef[@|.]genesix.org

dom commun

1 Étendue de l'installation

Cette procédure commune concerne aussi bien le dom0 que les domUs.

⇨ Il faut être connecté en root avant de poursuivre.

2 Environnement utilisateur

2.1 Locales

Cocher : fr_FR.UTF-8* sur le premier écran et sélectionner fr_FR.UTF-8 sur le second :

```
root@system: dpkg-reconfigure locales
```

2.2 Midnight Commander

Installer le paquet :

```
root@system: aptitude install mc
root@system: mc
```

```
  Left     File     Command     Options     Right
┌<- ~ ──────────────────────────────────────.[^]>┐┌<- ~ ──────────────────────────────────────.[^]>┐
│.n          Name             │  Size   │Modify time ││.n          Name             │  Size   │Modify time │
│/..                          │UP--DIR  │Nov  4 23:24 ││/..                          │UP--DIR  │Nov  4 23:24 │
│/.cache                      │   4096  │Nov  5 09:54 ││/.cache                      │   4096  │Nov  5 09:54 │
│/.config                     │   4096  │Nov  5 09:54 ││/.config                     │   4096  │Nov  5 09:54 │
│/.local                      │   4096  │Nov  5 09:54 ││/.local                      │   4096  │Nov  5 09:54 │
│/.pki                        │   4096  │Nov  4 23:26 ││/.pki                        │   4096  │Nov  4 23:26 │
│/.ssh                        │   4096  │Nov  4 23:50 ││/.ssh                        │   4096  │Nov  4 23:50 │
│ .bash_logout                │     18  │Dec 29  2013 ││ .bash_logout                │     18  │Dec 29  2013 │
│ .bash_profile               │    176  │Dec 29  2013 ││ .bash_profile               │    176  │Dec 29  2013 │
│ .bashrc                     │    176  │Dec 29  2013 ││ .bashrc                     │    176  │Dec 29  2013 │
│ .cshrc                      │    100  │Dec 29  2013 ││ .cshrc                      │    100  │Dec 29  2013 │
│ .mdg                        │      7  │Nov  4 23:26 ││ .mdg                        │      7  │Nov  4 23:26 │
│ .rnd                        │   1024  │Nov  4 23:26 ││ .rnd                        │   1024  │Nov  4 23:26 │
│ .tcshrc                     │    129  │Dec 29  2013 ││ .tcshrc                     │    129  │Dec 29  2013 │
│ gpm-libs-1.2~7.x86_64.rpm   │  33048  │Nov  5 10:05 ││ gpm-libs-1.2~7.x86_64.rpm   │  33048  │Nov  5 10:05 │
│ mc-4.8.18-1.1.x86_64.rpm    │1993892  │Oct  2 21:33 ││ mc-4.8.18-1.1.x86_64.rpm    │1993892  │Oct  2 21:33 │
│ slang-2.2.4-~7.x86_64.rpm   │ 524056  │Nov  5 09:53 ││ slang-2.2.4-~7.x86_64.rpm   │ 524056  │Nov  5 09:53 │
│                             │         │             ││                             │         │             │
└─────────────────────────────┴─────────┴─────────────┘└─────────────────────────────┴─────────┴─────────────┘
 gpm-libs-1.20.7-5.el7.x86_64.rpm                      UP--DIR
└──────────────────────────── 16G/18G (89%) ─┘└──────────────────────────── 16G/18G (89%) ─┘
Hint: Want your plain shell? Press C-o, and get back to MC with C-o again.
#                                                                              [^]
 1Help    2Menu     3View     4Edit     5Copy     6RenMov  7Mkdir    8Delete   9PullDn  10Quit
```

Puis, dans MC :

```
F9 > Gauche & Droite > Mode de listage :
        Liste brève des fichiers ;
        [x] : mini afficheur ;
        half type name | mtime | size | owner | group | mode:8 | perm:11

F9 > Options > Bits d'affichage
        Entrée / affichage d'encodage : UTF-8
```

```
        [x] Entrée 8 bits

F9 > Options > Enregistrer la configuration.
```

F9 > Options > Enregistrer la configuration.

Pour rétablir l'éditeur de MC, si un autre éditeur (par exemple nano) est également installé :

```
root@system: select-editor
```

Lancer une nouvelle console pour la prise en compte de l'encodage UTF-8.

2.3 Console

Prompt

Modifier /etc/bash.bashrc :

- PS1 ;
- Dé-commenter la personnalisation du titre de la fenêtre du terminal ;
- Dé-commenter la complétion des commandes.

/etc/bash.bashrc

```
…

PS1="\e[0;31m${debian_chroot:+($debian_chroot)}$(date +%H:%M)-\u@\h:\w>\e[0m"

PS1="${debian_chroot:+($debian_chroot)}$(date +%H:%M)-\u@\h:\w>"

# Commented out, don't overwrite xterm -T "title" -n "icontitle" by default.
#If this is an xterm set the title to user@host:dir

case "$TERM" in
xterm*|rxvt*)
    PROMPT_COMMAND='echo -ne "\033]0;${USER}@${HOSTNAME}: ${PWD}\007"'
    ;;
*)
    ;;
esac

# enable bash completion in interactive shells
if ! shopt -oq posix; then
  if [ -f /usr/share/bash-completion/bash_completion ]; then
    . /usr/share/bash-completion/bash_completion
  elif [ -f /etc/bash_completion ]; then
    . /etc/bash_completion
  fi
fi

…
```

2.4 Historique

Améliorer la configuration de l'historique :

/root/.bashrc

stef[@|.]genesix.org

```
...
# export PS1=...
...

# Ignorer les commandes consécutives
export HISTCONTROL=ignoreboth

# Nb de cmds mises en historique au chargement du shell
export HISTSIZE=1000

# Nb de cmds enregistrées dans ./bash_history
export HISTFILESIZE=50000

# Format de l'horodatage
export HISTTIMEFORMAT="%d/%m/%Y %H:%M:%S "
```

Consultation de l'historique horodatée :

```
root@system:  history | tail -n 5

  300  17/10/2009 14:40:09 ls
  301  17/10/2009 14:40:15 mc
  302  17/10/2009 14:40:28 logout
  303  17/10/2009 14:41:49 mc
  304  17/10/2009 14:43:23 history | tail -n 5
```

2.5 Bannière du système

❑ Messages inutiles au login

Vider les fichiers ci-dessous pour supprimer les messages inutiles au login :

```
# Le vidage des trois fichiers est nécessaire sinon, il y a réapparition au démarrage suivant.

root@system: echo > /etc/motd
root@system: echo > /etc/issue
root@system: echo > /usr/share/base-files/motd
```

⇨ Pour le dom0, commenter le code dans /etc/rc.local, à l'exception de « exit 0 ».

❑ Bannière

Afin de simplifier le setup, toutes les bannières sont identiques, au numéro de dom près.

Installer le paquet sysvbanner et générer la bannière, en fonction du tableau ci-dessus :

```
root@system:  aptitude install sysvbanner
root@system:  banner GENESIX > /etc/banner
```

Puis, pour les bannières suivantes, recopier la bannière en changeant seulement le dom.

⇨ Un nom de bannière de plus de 15 caractères est ignoré.

Il est intéressant que tous les fichiers de bannière commencent par « banner », afin de pouvoir les retrouver facilement dans le répertoire /etc.

Etoffer /etc/banner et insérer une ligne au dessus et deux lignes en dessous :

❑ Bannière dom0/Uxxx

/etc/banner

```
<newline>

#######################################################

 #####  ####### #     # #######  #####    ###   #     #
#     # #       ##    # #       #     #    #     #   #
#       #       # #   # #       #          #      # #
#  #### #####   #  #  # #####    #####     #       #
#     # #       #   # # #             #    #      # #
#     # #       #    ## #       #     #    #     #   #
 #####  ####### #     # #######  #####    ###   #     #

  SP-64-S Xeon E5 1620v2 4c/8t 3.9GHz 64Go ECC 2x2To

             OVH RBX5 Genesix (v2) dom0/Uxxx

#######################################################
<newline>
<newline>
```

2.6 Création de l'utilisateur {AD}

Ajouter l'utilisateur :

```
root@system: adduser --no-create-home {AD}
root@system: passwd {AD} (même mot de passe que root)
```

Editer /etc/passwd et mettre à jour :

/etc/passwd

```
…
{AD}:x:0:0:,,,:/root:/bin/bash
…
```

Editer /etc/group et mettre à jour :

/etc/group

```
…
{AD}:x:0
…
```

3 Système

3.1 Horloge système

```
root@system : aptitude install ntpdate
```

Créer /etc/cron.weekly/synctime :

```
/etc/cron.weekly/synctime

ntpdate pool.ntp.org
```

Appliquer les droits :

```
root@system : chmod +x /etc/cron.weekly/synctime
```

Un domU n'a pas d'horloge RTC, elle n'a pas besoin d're ajustée.

3.2 Logs

Les logs peuvent être améliorés, par exemple, le fichier de log /var/log/auth.log est pollué par les crons avec ce genre de log :

```
Apr  9 06:20:01 hypervisix CRON[22592]: pam_unix(cron:session): session opened for user root by (uid=0)
Apr  9 06:20:01 hypervisix CRON[22592]: pam_unix(cron:session): session closed for user root
Apr  9 06:21:01 hypervisix CRON[22634]: pam_unix(cron:session): session opened for user root by (uid=0)
Apr  9 06:21:01 hypervisix CRON[22634]: pam_unix(cron:session): session closed for user root
```

Ce qui rend auth.log illisible sur l'information pertinente, à savoir les véritables connexions, ou tentatives de connexions.

Par ailleurs, les logs iptables sont répartis sur différents logs standards, qui noient également l'information.

Enfin, il peut être intéressant d'opter pour le remplacement de rsyslog par syslog-ng.

❑ Syslog-ng

Passage au XXI^{ème} siècle : nettoyage des (r)syslogueries paléolithiques et installation de syslog-ng :

<Nom paquets>	*Commentaires*	*Commentaires étendus*
syslog-ng	log	

```
root@system: aptitude install syslog-ng
```

Mofifier /etc/syslog-ng/syslog-ng.conf :

```
#------------------------------------------------------------------------
# syslog-ng.conf
```

```
#------------------------------------------------------------------------

@version: 3.5
@include "scl.conf"
@include "`scl-root`/system/tty10.conf"

#   Syslog-ng   configuration   file,   compatible   with   default   Debian   syslogd   installat
ion.

#--- Global options.

# custom settings tuned to max-connections
#flush_lines(100);
#log_fetch_limit(100);
#log_iw_size(100);
#log_fifo_size(1000);

options {
 flush_lines(100);
 log_fifo_size(1000);
 chain_hostnames(off);
 flush_lines(0);
 use_dns(no);
 use_fqdn(no);
 owner("root");
 group("adm");
 perm(0640);
 stats_freq(0);
 bad_hostname("^gconfd$");
};

#---
#--- Sources
#---

source s_src { system(); internal(); };

# Pour mailcow-dockerized (domu230)
#source    s_mailcow    {    tcp(    log_fetch_limit(100)    log_iw_size(100)    ip(0.0.0.0)    port(5
24) max-connections(50)); };

#---
#--- Destinations
#---

destination d_auth   { file("/var/log/auth.log"); };
destination d_cron   { file("/var/log/cron.log"); };
destination d_daemon { file("/var/log/daemon.log"); };

destination d_firewall { file("/var/log/firewall.log"); };

# Pour mailcow-dockerized (domu230)
#destination d_mailcow         { file("/var/log/mailcow.log"); };
#destination d_mailcow-postfix { file("/var/log/mailcow-postfix.log"); };
#destination d_mailcow-phpfpm  { file("/var/log/mailcow-phpfpm.log"); };
#destination d_mailcow-sogo    { file("/var/log/mailcow-sogo.log"); };
#destination d_mailcow-dovecot { file("/var/log/mailcow-dovecot.log"); };

destination d_kern   { file("/var/log/kern.log"); };
destination d_syslog { file("/var/log/syslog"); };
destination d_user   { file("/var/log/user.log"); };

destination d_mail     { file("/var/log/mail.log"); };
destination d_mailinfo { file("/var/log/mail.info"); };
destination d_mailwarn { file("/var/log/mail.warn"); };
destination d_mailerr  { file("/var/log/mail.err"); };

destination d_debug    { file("/var/log/debug"); };
destination d_error    { file("/var/log/error"); };
destination d_messages { file("/var/log/messages"); };

destination d_console     { usertty("root"); };
destination d_console_all { file(`tty10`); };
destination d_xconsole    { pipe("/dev/xconsole"); };

#destination d_ppp { file("/var/log/ppp.log"); };
#destination d_uucp   { file("/var/log/uucp.log"); };
#destination d_lpr    { file("/var/log/lpr.log"); };
```


stef[@|.]genesix.org

```
#---
#--- Filters
#---

filter f_dbg    { level(debug); };
filter f_info   { level(info); };
filter f_notice { level(notice); };
filter f_warn   { level(warn); };
filter f_err    { level(err); };
filter f_crit   { level(crit .. emerg); };
filter   f_debug      {   level(debug)   and   not   facility(auth,   authpriv,   news,   mail)   and
not filter(f_firewall); };
filter f_error  { level(err .. emerg) ; };
filter    f_messages    {    level(info,notice,warn)    and       not    facility(auth,authpriv,cron
,daemon,mail,news) and not filter(f_firewall); };

filter f_auth { facility(auth, authpriv) and not message("cron:session"); };
filter f_cron { facility(cron) and not message("/usr/local/rtm/bin/rtm"); };
filter f_daemon { facility(daemon) and not filter(f_debug); };

filter f_firewall { message("\\[Firewall"); };

# Pour mailcow-dockerized (domu230)
#filter     f_mailcow-postfix     {     message("whitelist_forwardinghosts")     or     message("post
#fix"); };
#filter f_mailcow-phpfpm  { message(".php"); };
#filter f_mailcow-sogo    { message("sogo"); };
#filter f_mailcow-dovecot { message("imap"); };

filter f_kern { facility(kern) and not filter(f_firewall); };

filter   f_local   {   facility(local0,   local1,   local3,   local4,   local5,   local6,   local7
) and not filter(f_debug); };
filter f_mail { facility(mail) and not filter(f_debug); };
filter   f_syslog3   {   not   facility(auth,   authpriv,   mail)   and   not   filter(f_firewall)
and not message("/usr/local/rtm/bin/rtm"); };
filter f_user { facility(user) and not filter(f_debug); };
filter f_cother { level(debug, info, notice, warn) or facility(daemon, mail); };

filter f_console { level(warn .. emerg); };

#filter f_uucp { facility(uucp) and not filter(f_debug); };
#filter f_cnews { level(notice, err, crit) and facility(news); };
#filter f_news { facility(news) and not filter(f_debug); };
#filter f_lpr { facility(lpr) and not filter(f_debug); };
#filter f_ppp { facility(local2) and not filter(f_debug); };

#--- Log paths

log { source(s_src); filter(f_auth); destination(d_auth); };
log { source(s_src); filter(f_cron); destination(d_cron); };
log { source(s_src); filter(f_daemon); destination(d_daemon); };

log { source(s_src); filter(f_firewall); destination(d_firewall); };

# Pour mailcow-dockerized (domu230)
#log {source(s_mailcow); filter(f_mailcow-postfix); destination(d_mailcow-postfix); };
#log {source(s_mailcow);filter(f_mailcow-phpfpm);destination(d_mailcow-phpfpm); };
#log {source(s_mailcow);filter(f_mailcow-sogo);destination(d_mailcow-sogo); };
#log {source(s_mailcow);filter(f_mailcow-dovecot);destination(d_mailcow-dovecot); };
#log { source(s_mailcow); destination(d_mailcow); };

log { source(s_src); filter(f_kern); destination(d_kern); };
log { source(s_src); filter(f_syslog3); destination(d_syslog); };
log { source(s_src); filter(f_user); destination(d_user); };

log { source(s_src); filter(f_mail); destination(d_mail); };
log { source(s_src); filter(f_mail); filter(f_info); destination(d_mailinfo); };
log { source(s_src); filter(f_mail); filter(f_warn); destination(d_mailwarn); };
log { source(s_src); filter(f_mail); filter(f_err); destination(d_mailerr); };

log { source(s_src); filter(f_debug); destination(d_debug); };
log { source(s_src); filter(f_error); destination(d_error); };
log { source(s_src); filter(f_messages); destination(d_messages); };

log {source(s_src);filter(f_console);destination(d_console_all);destination(d_xconsole); };
log { source(s_src); filter(f_crit); destination(d_console); };
```


stef[@|.]genesix.org

```
# Include all config files in /etc/syslog-ng/conf.d/

@include "/etc/syslog-ng/conf.d/*.conf"

#----------------------------------------------------------------------------
# EOF
#----------------------------------------------------------------------------
```

Ajouter la rotation du log iptables.log dans /etc/logrotate.d/rsyslog :

```
/etc/logrotate.d/rsyslog

…

/var/log/cron.log
/var/log/firewall.log
/var/log/debug
…
```

Créer les fichiers de log et recharger les services :

```
root@system: touch /var/log/cron.log
root@system: chown root:adm /var/log/cron.log

root@system: touch /var/log/iptables.log
root@system: chown root:adm /var/log/firewall.log

root@system: systemctl restart syslog-ng
root@system: systemctl restart cron
```

Il est possible de débugguer avec la commande :

```
root@system: /usr/sbin/syslog-ng -F
```

Les erreurs de configuration dans /etc/syslog-ng/syslog-ng.conf seront alors listées.

- Notes

La fonction message() accepte les expression régulières. Dans ce cas utiliser des guillemets simples, afin que les caractères spéciaux ()[].*?+ ^$|\ soient directement interprétés. Dans les autres cas, utiliser des guillemets doubles et si la chaîne contient les caractères spéciaux ()[].*?+ ^$|\ utiliser le caractère d'échappement \ (la simplicité est le mal).

https://www.balabit.com/documents/syslog-ng-ose-latest-guides/en/syslog-ng-ose-guide-admin/html/regular-expressions.html

❑ Rsyslog

Ce paragraphe s'adresse à ceux qui ne souhaiteraient pas passer à syslog-ng.

Pour régler les problèmes évoqués, modifier /etc/rsyslog.conf :

/etc/rsyslog.conf

```
…

###############
#### RULES ####
###############

## Lignes originales
#
#auth,authpriv.*                 /var/log/auth.log
#*.*;auth,authpriv.none         -/var/log/syslog
##cron.*                         /var/log/cron.log

:msg, contains, "[Firewall"     -/var/log/iptables.log
& ~

:msg, contains, "pam_unix(cron:session)"  ~
auth,authpriv.*                 /var/log/auth.log

*.*;cron,auth,authpriv.none,cron.none    -/var/log/syslog
cron.*                          /var/log/cron.log

…
```

Ajouter la rotation du log iptables.log dans /etc/logrotate.d/rsyslog :

/etc/logrotate.d/rsyslog

```
…

/var/log/cron.log
/var/log/firewall.log
/var/log/debug
…
```

Créer les fichiers de log et recharger les services :

```
root@system: touch /var/log/cron.log
root@system: chown root:adm /var/log/cron.log

root@system: touch /var/log/iptables.log
root@system: chown root:adm /var/log/firewall.log

root@system: systemctl restart rsyslog
root@system: systemctl restart cron
```

3.3 Postfix, hostname & hosts

➪ Appliquer le chapitre « Postfix » de « serveur Debian 8 - APPLICATIONS »

4 Finalisations

4.1 Autres paquets

<Nom paquets>	*Commentaires*	*Commentaires étendus*
sshfs	télémaintenance ssh	

Installer les paquets de la liste ci-dessus par la commande :

```
root@system: aptitude install sshfs
```

❑ Connectivité pendant la mise au point

Il faut assurer la « connectivité » pendant la phase de mise au point. Le dom doit toujours être accessible ! En cas d'erreur dans le firewall du dom, on aura ainsi une « seconde chance ».

⇨ A la fin de la mise au point, supprimer le port 22.

Editer /etc/ssh/sshd_config :

/etc/ssh/sshd_config

```
…
port ppNNN
port 22
…
PermitRootLogin yes
…
Banner /etc/banner
…
AllowUsers {AD}
…
```

Recharger le fichier de configuration :

```
root@system: service ssh reload
```

⇨ Sans se déconnecter de l'accès en cours, tester la nouvelle configuration SSH

```
root@system: ssh -p {Px:port} {AD}@{Px:ip}
```

Après avoir appliqué tout le chapitre, redémarrer :

```
root@system: reboot
```

Se re-connecter avec l'utilisateur {AD} :

```
root@system: ssh -p {Px:port} {AD}@{Px:ip}
```

⇨ Retourner maintenant au chapitre d'origine

Annexes

1 Exploitation

➪ Les informations d'exploitation sont décrites dans : serveur debian v8 - Genesix v2 - Exploitation.odt

2 Paquets d'origine à l'installation

Installation Debian 8.6, avec noyau d'origine, après suppression des paquets vim :

```
root@system: dpkg -l

Souhait=inconnU/Installé/suppRimé/Purgé/H=à garder
| État=Non/Installé/fichier-Config/dépaqUeté/échec-conFig/H=semi-installé/W=attend-traitement-déclenchements
|/ Err?=(aucune)/besoin Réinstallation (État,Err: majuscule=mauvais)
||/ Nom                          Version           Architecture      Description
+++-============================-=================-=================-=======================================================
ii  acl                          2.2.52-2          amd64             Access control list utilities
ii  acpi                         1.7-1             amd64             displays information on ACPI devices
ii  acpi-support-base            0.142-6           all               scripts for handling base ACPI events such as the pow
ii  acpid                        1:2.0.23-2        amd64             Advanced Configuration and Power Interface event daem
ii  adduser                      3.113+nmu3        all               add and remove users and groups
ii  apt                          1.0.9.8.3         amd64             commandline package manager
ii  apt-utils                    1.0.9.8.3         amd64             package management related utility programs
ii  base-files                   8+deb8u6          amd64             Debian base system miscellaneous files
ii  base-passwd                  3.5.37            amd64             Debian base system master password and group files
ii  bash                         4.3-11+b1         amd64             GNU Bourne Again SHell
ii  bc                           1.06.95-9         amd64             GNU bc arbitrary precision calculator language
ii  bind9                        1:9.9.5.dfsg-9+de amd64             Internet domain Name Server
ii  bind9-host                   1:9.9.5.dfsg-9+de amd64             Version of 'host' bundled with BIND 9.X
ii  bind9utils                   1:9.9.5.dfsg-9+de amd64             Utilities for BIND
ii  bsdmainutils                 9.0.6             amd64             collection of more utilities from FreeBSD
ii  bsdutils                     1:2.25.2-6        amd64             basic utilities from 4.4BSD-Lite
ii  btrfs-tools                  3.17-1.1          amd64             Checksumming Copy on Write Filesystem utilities
ii  busybox                      1:1.22.0-9+deb8u1 amd64             Tiny utilities for small and embedded systems
ii  bzip2                        1.0.6-7+b3        amd64             high-quality block-sorting file compressor - utilitie
ii  console-setup                1.123             all               console font and keymap setup program
ii  console-setup-linux          1.123             all               Linux specific part of console-setup
ii  coreutils                    8.23-4            amd64             GNU core utilities
ii  cpio                         2.11+dfsg-4.1+deb amd64             GNU cpio -- a program to manage archives of files
ii  cron                         3.0pl1-127+deb8u1 amd64             process scheduling daemon
ii  dash                         0.5.7-4+b1        amd64             POSIX-compliant shell
ii  debconf                      1.5.56            all               Debian configuration management system
ii  debconf-i18n                 1.5.56            all               full internationalization support for debconf
ii  debian-archive-keyring       2014.3            all               GnuPG archive keys of the Debian archive
ii  debianutils                  4.4+b1            amd64             Miscellaneous utilities specific to Debian
ii  diffutils                    1:3.3-1+b1        amd64             File comparison utilities
ii  dmeventd                     2:1.02.90-2.2+deb amd64             Linux Kernel Device Mapper event daemon
ii  dmidecode                    2.12-3            amd64             SMBIOS/DMI table decoder
ii  dmsetup                      2:1.02.90-2.2+deb amd64             Linux Kernel Device Mapper userspace library
ii  dnsutils                     1:9.9.5.dfsg-9+de amd64             Clients provided with BIND
ii  dpkg                         1.17.27           amd64             Debian package management system
ii  e2fslibs:amd64               1.42.12-2         amd64             ext2/ext3/ext4 file system libraries
ii  e2fsprogs                    1.42.12-2         amd64             ext2/ext3/ext4 file system utilities
ii  efibootmgr                   0.11.0-3          amd64             Interact with the EFI Boot Manager
ii  ethtool                      1:3.16-1          amd64             display or change Ethernet device settings
ii  findutils                    4.4.2-9+b1        amd64             utilities for finding files--find, xargs
ii  gcc-4.9-base:amd64           4.9.2-10          amd64             GCC, the GNU Compiler Collection (base package)
ii  gettext-base                 0.19.3-2          amd64             GNU Internationalization utilities for the base syste
ii  gnupg                        1.4.18-7+deb8u3   amd64             GNU privacy guard - a free PGP replacement
ii  gpgv                         1.4.18-7+deb8u3   amd64             GNU privacy guard - signature verification tool
ii  grep                         2.20-4.1          amd64             GNU grep, egrep and fgrep
ii  groff-base                   1.22.2-8          amd64             GNU troff text-formatting system (base system compone
ii  grub-common                  2.02~beta2-22+deb amd64             GRand Unified Bootloader (common files)
ii  grub-efi-amd64-bin           2.02~beta2-22+deb amd64             GRand Unified Bootloader, version 2 (EFI-AMD64 binari
ii  grub-pc                      2.02~beta2-22+deb amd64             GRand Unified Bootloader, version 2 (PC/BIOS version)
ii  grub-pc-bin                  2.02~beta2-22+deb amd64             GRand Unified Bootloader, version 2 (PC/BIOS binaries
ii  grub2-common                 2.02~beta2-22+deb amd64             GRand Unified Bootloader (common files for version 2)
ii  gzip                         1.6-4             amd64             GNU compression utilities
ii  hddtemp                      0.3-beta15-52     amd64             hard drive temperature monitoring utility
ii  hostname                     3.15              amd64             utility to set/show the host name or domain name
ii  ifupdown                     0.7.53.1          amd64             high level tools to configure network interfaces
ii  init                         1.22              amd64             System-V-like init utilities - metapackage
ii  init-system-helpers          1.22              all               helper tools for all init systems
ii  initscripts                  2.88dsf-59        amd64             scripts for initializing and shutting down the system
ii  insserv                      1.14.0-5          amd64             boot sequence organizer using LSB init.d script depen
ii  installation-report          2.58              all               system installation report
ii  iproute2                     3.16.0-2          amd64             networking and traffic control tools
ii  iptables                     1.4.21-2+b1       amd64             administration tools for packet filtering and NAT
ii  iputils-ping                 3:20121221-5+b2   amd64             Tools to test the reachability of network hosts
ii  irqbalance                   1.0.6-3           amd64             Daemon to balance interrupts for SMP systems
ii  isc-dhcp-client              4.3.1-6+deb8u2    amd64             DHCP client for automatically obtaining an IP address
ii  isc-dhcp-common              4.3.1-6+deb8u2    amd64             common files used by all of the isc-dhcp packages
ii  kbd                          1.15.5-2          amd64             Linux console font and keytable utilities
ii  keyboard-configuration       1.123             all               system-wide keyboard preferences
```

```
ii  kmod                          18-3              amd64        tools for managing Linux kernel modules
ii  krb5-locales                  1.12.1+dfsg-19+de all          Internationalization support for MIT Kerberos
ii  less                          458-3             amd64        pager program similar to more
ii  libacl1:amd64                 2.2.52-2          amd64        Access control list shared library
ii  libapt-inst1.5:amd64          1.0.9.8.3         amd64        deb package format runtime library
ii  libapt-pkg4.12:amd64          1.0.9.8.3         amd64        package management runtime library
ii  libasprintf0c2:amd64          0.19.3-2          amd64        GNU library to use fprintf and friends in C++
ii  libattr1:amd64                1:2.4.47-2        amd64        Extended attribute shared library
ii  libaudit-common               1:2.4-1           all          Dynamic library for security auditing - common files
ii  libaudit1:amd64               1:2.4-1+b1        amd64        Dynamic library for security auditing
ii  libbind9-90                   1:9.9.5.dfsg-9+de amd64        BIND9 Shared Library used by BIND
ii  libblkid1:amd64               2.25.2-6          amd64        block device id library
ii  libboost-iostreams1.55.0      1.55.0+dfsg-3     amd64        Boost.Iostreams Library
ii  libbsd0:amd64                 0.7.0-2           amd64        utility functions from BSD systems - shared library
ii  libbz2-1.0:amd64              1.0.6-7+b3        amd64        high-quality block-sorting file compressor library -
ii  libc-bin                      2.19-18+deb8u6    amd64        GNU C Library: Binaries
ii  libc6:amd64                   2.19-18+deb8u6    amd64        GNU C Library: Shared libraries
ii  libcap-ng0:amd64              0.7.4-2           amd64        An alternate POSIX capabilities library
ii  libcap2:amd64                 1:2.24-8          amd64        POSIX 1003.1e capabilities (library)
ii  libcap2-bin                   1:2.24-8          amd64        POSIX 1003.1e capabilities (utilities)
ii  libcomerr2:amd64              1.42.12-2         amd64        common error description library
ii  libcryptsetup4:amd64          2:1.6.6-5         amd64        disk encryption support - shared library
ii  libdb5.3:amd64                5.3.28-9          amd64        Berkeley v5.3 Database Libraries [runtime]
ii  libdebconfclient0:amd64       0.192             amd64        Debian Configuration Management System (C-implementat
ii  libdevmapper-event1.02.1      2:1.02.90-2.2+deb amd64        Linux Kernel Device Mapper event support library
ii  libdevmapper1.02.1:amd64      2:1.02.90-2.2+deb amd64        Linux Kernel Device Mapper userspace library
ii  libdns-export100              1:9.9.5.dfsg-9+de amd64        Exported DNS Shared Library
ii  libdns100                     1:9.9.5.dfsg-9+de amd64        DNS Shared Library used by BIND
ii  libedit2:amd64                3.1-20140620-2    amd64        BSD editline and history libraries
ii  libefivar0:amd64              0.15-3            amd64        Library to manage UEFI variables
ii  libestr0                      0.1.9-1.1         amd64        Helper functions for handling strings (lib)
ii  libexpat1:amd64               2.1.0-6+deb8u3    amd64        XML parsing C library - runtime library
ii  libffi6:amd64                 3.1-2+b2          amd64        Foreign Function Interface library runtime
ii  libfreetype6:amd64            2.5.2-3+deb8u1    amd64        FreeType 2 font engine, shared library files
ii  libfuse2:amd64                2.9.3-15+deb8u2   amd64        Filesystem in Userspace (library)
ii  libgcc1:amd64                 1:4.9.2-10        amd64        GCC support library
ii  libgcrypt20:amd64             1.6.3-2+deb8u2    amd64        LGPL Crypto library - runtime library
ii  libgdbm3:amd64                1.8.3-13.1        amd64        GNU dbm database routines (runtime version)
ii  libgeoip1:amd64               1.6.2-4           amd64        non-DNS IP-to-country resolver library
ii  libglib2.0-0:amd64            2.42.1-1+b1       amd64        GLib library of C routines
ii  libgmp10:amd64                2:6.0.0+dfsg-6    amd64        Multiprecision arithmetic library
ii  libgnutls-deb0-28:amd64       3.3.8-6+deb8u3    amd64        GNU TLS library - main runtime library
ii  libgnutls-openssl27:amd6      3.3.8-6+deb8u3    amd64        GNU TLS library - OpenSSL wrapper
ii  libgpg-error0:amd64           1.17-3            amd64        library for common error values and messages in GnuPG
ii  libgpm2:amd64                 1.20.4-6.1+b2     amd64        General Purpose Mouse - shared library
ii  libgssapi-krb5-2:amd64        1.12.1+dfsg-19+de amd64        MIT Kerberos runtime libraries - krb5 GSS-API Mechani
ii  libhogweed2:amd64             2.7.1-5+deb8u1    amd64        low level cryptographic library (public-key cryptos)
ii  libicu52:amd64                52.1-8+deb8u3     amd64        International Components for Unicode
ii  libidn11:amd64                1.29-1+deb8u2     amd64        GNU Libidn library, implementation of IETF IDN specif
ii  libirs-export91               1:9.9.5.dfsg-9+de amd64        Exported IRS Shared Library
ii  libisc-export95               1:9.9.5.dfsg-9+de amd64        Exported ISC Shared Library
ii  libisc95                      1:9.9.5.dfsg-9+de amd64        ISC Shared Library used by BIND
ii  libisccc90                    1:9.9.5.dfsg-9+de amd64        Command Channel Library used by BIND
ii  libisccfg-export90            1:9.9.5.dfsg-9+de amd64        Exported ISC CFG Shared Library
ii  libisccfg90                   1:9.9.5.dfsg-9+de amd64        Config File Handling Library used by BIND
ii  libjson-c2:amd64              0.11-4            amd64        JSON manipulation library - shared library
ii  libk5crypto3:amd64            1.12.1+dfsg-19+de amd64        MIT Kerberos runtime libraries - Crypto Library
ii  libkeyutils1:amd64            1.5.9-5+b1        amd64        Linux Key Management Utilities (library)
ii  libkmod2:amd64                18-3              amd64        libkmod shared library
ii  libkrb5-3:amd64               1.12.1+dfsg-19+de amd64        MIT Kerberos runtime libraries
ii  libkrb5support0:amd64         1.12.1+dfsg-19+de amd64        MIT Kerberos runtime libraries - Support library
ii  liblocale-gettext-perl        1.05-8+b1         amd64        module using libc functions for internationalization
ii  liblogging-stdlog0:amd64      1.0.4-1           amd64        easy to use and lightweight logging library
ii  liblognorm1:amd64             1.0.1-3           amd64        Log normalizing library
ii  liblvm2cmd2.02:amd64          2.02.111-2.2+deb8 amd64        LVM2 command library
ii  liblwres90                    1:9.9.5.dfsg-9+de amd64        Lightweight Resolver Library used by BIND
ii  liblzma5:amd64                5.1.1alpha+201206 amd64        XZ-format compression library
ii  liblzo2-2:amd64               2.08-1.2          amd64        data compression library
ii  libmnl0:amd64                 1.0.3-5           amd64        minimalistic Netlink communication library
ii  libmount1:amd64               2.25.2-6          amd64        device mounting library
ii  libncurses5:amd64             5.9+20140913-1+b1 amd64        shared libraries for terminal handling
ii  libncursesw5:amd64            5.9+20140913-1+b1 amd64        shared libraries for terminal handling (wide characte
ii  libnetfilter-acct1:amd64      1.0.2-1.1         amd64        Netfilter acct library
ii  libnettle4:amd64              2.7.1-5+deb8u1    amd64        low level cryptographic library (symmetric and one-wa
ii  libnewt0.52:amd64             0.52.17-1+b1      amd64        Not Erik's Windowing Toolkit - text mode windowing wi
ii  libnfnetlink0:amd64           1.0.1-3           amd64        Netfilter netlink library
ii  libnuma1:amd64                2.0.10-1          amd64        Libraries for controlling NUMA policy
ii  libp11-kit0:amd64             0.20.7-1          amd64        Library for loading and coordinating access to PKCS#1
ii  libpam-modules:amd64          1.1.8-3.1+deb8u1+ amd64        Pluggable Authentication Modules for PAM
ii  libpam-modules-bin            1.1.8-3.1+deb8u1+ amd64        Pluggable Authentication Modules for PAM - helper bin
ii  libpam-runtime                1.1.8-3.1+deb8u1  all          Runtime support for the PAM library
ii  libpam0g:amd64                1.1.8-3.1+deb8u1+ amd64        Pluggable Authentication Modules library
ii  libparted2:amd64              3.2-7             amd64        disk partition manipulator - shared library
ii  libpcap0.8:amd64              1.6.2-2           amd64        system interface for user-level packet capture
ii  libpci3:amd64                 1:3.2.1-3         amd64        Linux PCI Utilities (shared library)
ii  libpcre3:amd64                2:8.35-3.3+deb8u4 amd64        Perl 5 Compatible Regular Expression Library - runtim
ii  libpipeline1:amd64            1.4.0-1           amd64        pipeline manipulation library
ii  libpng12-0:amd64              1.2.50-2+deb8u2   amd64        PNG library - runtime
ii  libpopt0:amd64                1.16-10           amd64        lib for parsing cmdline parameters
ii  libprocps3:amd64              2:3.3.9-9         amd64        library for accessing process information from /proc
ii  libpsl0:amd64                 0.5.1-1           amd64        Library for Public Suffix List (shared libraries)
ii  libpython-stdlib:amd64        2.7.9-1           amd64        interactive high-level object-oriented language (defa
ii  libpython2.7-minimal:amd      2.7.9-2+deb8u1    amd64        Minimal subset of the Python language (version 2.7)
ii  libpython2.7-stdlib:amd6      2.7.9-2+deb8u1    amd64        Interactive high-level object-oriented language (stan
ii  libreadline5:amd64            5.2+dfsg-2        amd64        GNU readline and history libraries, run-time librarie
ii  libreadline6:amd64            6.3-8+b3          amd64        GNU readline and history libraries, run-time librarie
ii  libselinux1:amd64             2.3-2             amd64        SELinux runtime shared libraries
ii  libsemanage-common            2.3-1             all          Common files for SELinux policy management libraries
ii  libsemanage1:amd64            2.3-1+b1          amd64        SELinux policy management library
```


stef[@|.]genesix.org

```
ii  libsepol1:amd64           2.3-2              amd64        SELinux library for manipulating binary security poli
ii  libsigc++-2.0-0c2a:amd64 2.4.0-1            amd64        type-safe Signal Framework for C++ - runtime
ii  libslang2:amd64           2.3.0-2            amd64        S-Lang programming library - runtime version
ii  libsmartcols1:amd64       2.25.2-6           amd64        smart column output alignment library
ii  libsqlite3-0:amd64        3.8.7.1-1+deb8u2   amd64        SQLite 3 shared library
ii  libss2:amd64              1.42.12-2          amd64        command-line interface parsing library
ii  libssl1.0.0:amd64         1.0.1t-1+deb8u5    amd64        Secure Sockets Layer toolkit - shared libraries
ii  libstdc++6:amd64          4.9.2-10           amd64        GNU Standard C++ Library v3
ii  libsystemd0:amd64         215-17+deb8u5      amd64        systemd utility library
ii  libtasn1-6:amd64          4.2-3+deb8u2       amd64        Manage ASN.1 structures (runtime)
ii  libtext-charwidth-perl    0.04-7+b3          amd64        get display widths of characters on the terminal
ii  libtext-iconv-perl        1.7-5+b2           amd64        converts between character sets in Perl
ii  libtext-wrapi18n-perl     0.06-7             all          internationalized substitute of Text::Wrap
ii  libtinfo5:amd64           5.9+20140913-1+b1  amd64        shared low-level terminfo library for terminal handli
ii  libudev1:amd64            215-17+deb8u5      amd64        libudev shared library
ii  libusb-0.1-4:amd64        2:0.1.12-25        amd64        userspace USB programming library
ii  libusb-1.0-0:amd64        2:1.0.19-1         amd64        userspace USB programming library
ii  libustr-1.0-1:amd64       1.0.4-3+b2         amd64        Micro string library: shared library
ii  libuuid1:amd64            2.25.2-6           amd64        Universally Unique ID library
ii  libwrap0:amd64            7.6.q-25           amd64        Wietse Venema's TCP wrappers library
ii  libxml2:amd64             2.9.1+dfsg1-5+deb  amd64        GNOME XML library
ii  libxtables10              1.4.21-2+b1        amd64        netfilter xtables library
ii  locales                   2.19-18+deb8u6     all          GNU C Library: National Language (locale) data [suppo
ii  login                     1:4.2-3+deb8u1     amd64        system login tools
ii  logrotate                 3.8.7-1+b1         amd64        Log rotation utility
ii  lsb-base                  4.1+Debian13+nmu1  all          Linux Standard Base 4.1 init script functionality
ii  lvm2                      2.02.111-2.2+deb8  amd64        Linux Logical Volume Manager
ii  man-db                    2.7.0.2-5          amd64        on-line manual pager
ii  manpages                  3.74-1             all          Manual pages about using a GNU/Linux system
ii  manpages-de               1.8-1              all          German manpages
ii  manpages-es               1.55-10            all          Spanish man pages
ii  manpages-fr               3.65d1p1-1         all          French version of the manual pages about using GNU/Li
ii  manpages-it               2.80-5             all          Italian version of the manual pages
ii  manpages-pl               1:0.6-2            all          Polish man pages
ii  manpages-pt               20040726-4         all          Portuguese Versions of the Manual Pages
ii  mawk                      1.3.3-17           amd64        a pattern scanning and text processing language
ii  mdadm                     3.3.2-5+deb8u1     amd64        tool to administer Linux MD arrays (software RAID)
ii  mime-support              3.58               all          MIME files 'mime.types' & 'mailcap', and support prog
ii  mount                     2.25.2-6           amd64        Tools for mounting and manipulating filesystems
ii  mtr-tiny                  0.85-3             amd64        Full screen ncurses traceroute tool
ii  multiarch-support         2.19-18+deb8u6     amd64        Transitional package to ensure multiarch compatibilit
ii  nano                      2.2.6-3            amd64        small, friendly text editor inspired by Pico
ii  ncurses-base              5.9+20140913-1     all          basic terminal type definitions
ii  ncurses-bin               5.9+20140913-1+b1  amd64        terminal-related programs and man pages
ii  ncurses-term              5.9+20140913-1     all          additional terminal type definitions
ii  net-tools                 1.60-26+b1         amd64        NET-3 networking toolkit
ii  netbase                   5.3                all          Basic TCP/IP networking system
ii  netcat-traditional        1.10-41            amd64        TCP/IP swiss army knife
ii  nfacct                    1.0.1-1.1          amd64        netfilter accounting object tool
ii  ntpdate                   1:4.2.6.p5+dfsg-7  amd64        client for setting system time from NTP servers
ii  openssh-client            1:6.7p1-5+deb8u3   amd64        secure shell (SSH) client, for secure access to remot
ii  openssh-server            1:6.7p1-5+deb8u3   amd64        secure shell (SSH) server, for secure access from rem
ii  openssh-sftp-server       1:6.7p1-5+deb8u3   amd64        secure shell (SSH) sftp server module, for SFTP acces
ii  openssl                   1.0.1t-1+deb8u5    amd64        Secure Sockets Layer toolkit - cryptographic utility
ii  os-prober                 1.65               amd64        utility to detect other OSes on a set of drives
ii  parted                    3.2-7              amd64        disk partition manipulator
ii  passwd                    1:4.2-3+deb8u1     amd64        change and administer password and group data
ii  pciutils                  1:3.2.1-3          amd64        Linux PCI Utilities
ii  perl                      5.20.2-3+deb8u6    amd64        Larry Wall's Practical Extraction and Report Language
ii  perl-base                 5.20.2-3+deb8u6    amd64        minimal Perl system
ii  perl-modules              5.20.2-3+deb8u6    all          Core Perl modules
ii  procps                    2:3.3.9-9          amd64        /proc file system utilities
ii  psmisc                    22.21-2            amd64        utilities that use the proc file system
ii  python                    2.7.9-1            amd64        interactive high-level object-oriented language (defa
ii  python-minimal            2.7.9-1            amd64        minimal subset of the Python language (default versio
ii  python2.7                 2.7.9-2+deb8u1     amd64        Interactive high-level object-oriented language (vers
ii  python2.7-minimal         2.7.9-2+deb8u1     amd64        Minimal subset of the Python language (version 2.7)
ii  readline-common           6.3-8              all          GNU readline and history libraries, common files
ii  reiserfsprogs             1:3.6.24-1         amd64        User-level tools for ReiserFS filesystems
ii  rsync                     3.1.1-3            amd64        fast, versatile, remote (and local) file-copying tool
ii  rsyslog                   8.4.2-1+deb8u2     amd64        reliable system and kernel logging daemon
ii  screen                    4.2.1-3+deb8u1     amd64        terminal multiplexer with VT100/ANSI terminal emulati
ii  sed                       4.2.2-4+b1         amd64        The GNU sed stream editor
ii  sensible-utils            0.0.9              all          Utilities for sensible alternative selection
ii  smartmontools             6.3+svn4002-2+b2   amd64        control and monitor storage systems using S.M.A.R.T.
ii  startpar                  0.59-3             amd64        run processes in parallel and multiplex their output
ii  systemd                   215-17+deb8u5      amd64        system and service manager
ii  systemd-sysv              215-17+deb8u5      amd64        system and service manager - SysV links
ii  sysv-rc                   2.88dsf-59         all          System-V-like runlevel change mechanism
ii  sysvinit-utils            2.88dsf-59         amd64        System-V-like utilities
ii  tar                       1.27.1-2+deb8u1    amd64        GNU version of the tar archiving utility
ii  task-english              3.31+deb8u1        all          General English environment
ii  task-ssh-server           3.31+deb8u1        all          SSH server
ii  tasksel                   3.31+deb8u1        all          tool for selecting tasks for installation on Debian s
ii  tasksel-data              3.31+deb8u1        all          official tasks used for installation of Debian system
ii  tcpdump                   4.6.2-5+deb8u1     amd64        command-line network traffic analyzer
ii  traceroute                1:2.0.20-2+b1      amd64        Traces the route taken by packets over an IPv4/IPv6 n
ii  tzdata                    2016i-0+deb8u1     all          time zone and daylight-saving time data
ii  ucf                       3.0030             all          Update Configuration File(s): preserve user changes t
ii  udev                      215-17+deb8u5      amd64        /dev/ and hotplug management daemon
ii  usbutils                  1:007-2            amd64        Linux USB utilities
ii  util-linux                2.25.2-6           amd64        Miscellaneous system utilities
ii  util-linux-locales        2.25.2-6           all          Locales files for util-linux
ii  vlan                      1.9-3.2            amd64        user mode programs to enable VLANs on your ethernet d
ii  wget                      1.16-1+deb8u1      amd64        retrieves files from the web
ii  whiptail                  0.52.17-1+b1       amd64        Displays user-friendly dialog boxes from shell script
ii  xfsprogs                  3.2.1              amd64        Utilities for managing the XFS filesystem
ii  xkb-data                  2.12-1             all          X Keyboard Extension (XKB) configuration data
```

```
ii  zlib1g:amd64             1:1.2.8.dfsg-2+b1 amd64             compression library - runtime
```


stef[@|.]genesix.org