# VS-Tools, un outil destiné à enrichir et simplifier la mise en oeuvre des environnements Util-Vserver / Linux-Vserver

Laurent Spagnol

*CRI - Université de Reims*

UNIVERSITÉ
DE REIMS
CHAMPAGNE-ARDENNE

# Pourquoi Linux-Vserver ?

- Histoire d'un serveur Institutionnel:
  - Messagerie,  listes de diffusion, virtualhosts Apache, bases de données, réplica LDAP...
  - Machine hébergée à 200 Km de nos locaux !
- Des constats:
  - Nombreux services: mise en oeuvre complexe
  - Difficile (voire impossible) à optimiser
  - Des problèmes de performances

UNIVERSITÉ DE REIMS CHAMPAGNE-ARDENNE

# Pourquoi Linux-Vserver ?

- Et un jour, une attaque ...
  - Une faille PHP, escalade des privilèges, et un Rootkit installé
  - Trois jours d'interruption totale (le temps nécessaire pour réparer), et beaucoup d'incertitudes ...
  - Le pire a pourtant été évité: attaque «script-kiddie», firewall en amont, plantage pur et simple du serveur
- PLUS JAMAIS CA !
  - Compliquer la vie des pirates
  - Détecter les intrusions, réparer facilement et rapidement

# Pourquoi Linux-Vserver ?

- Une réponse: la virtualisation
- Mais des familles de solutions qui répondent à des besoins différents:
  - Noyau en espace utilisateur (UML, coLinux ...)
  - Machines virtuelles / émulateurs (QEMU, VMware Player, Bochs, VirtualPC, VirtualBox ...)
  - Hyperviseurs (Xen, VMware ESX ...)
  - Isolateurs (Linux-Vserver, Virtuozo / OpenVZ ...)

# Pourquoi Linux-Vserver ?

- Linux-Vserver
  - Est un «isolateur de contextes d'exécution»
    - Ils ne «voient» pas les autres processus
    - Ont des droits limités
  - Les machines virtuelles n'ont pas de noyau
    - Performances «natives»
    - Virtualisation relativement peu gourmande
  - Systèmes de fichiers «chrootés» sur l'hôte
    - Accès direct aux Vserveurs

# Pourquoi VS-Tools ?

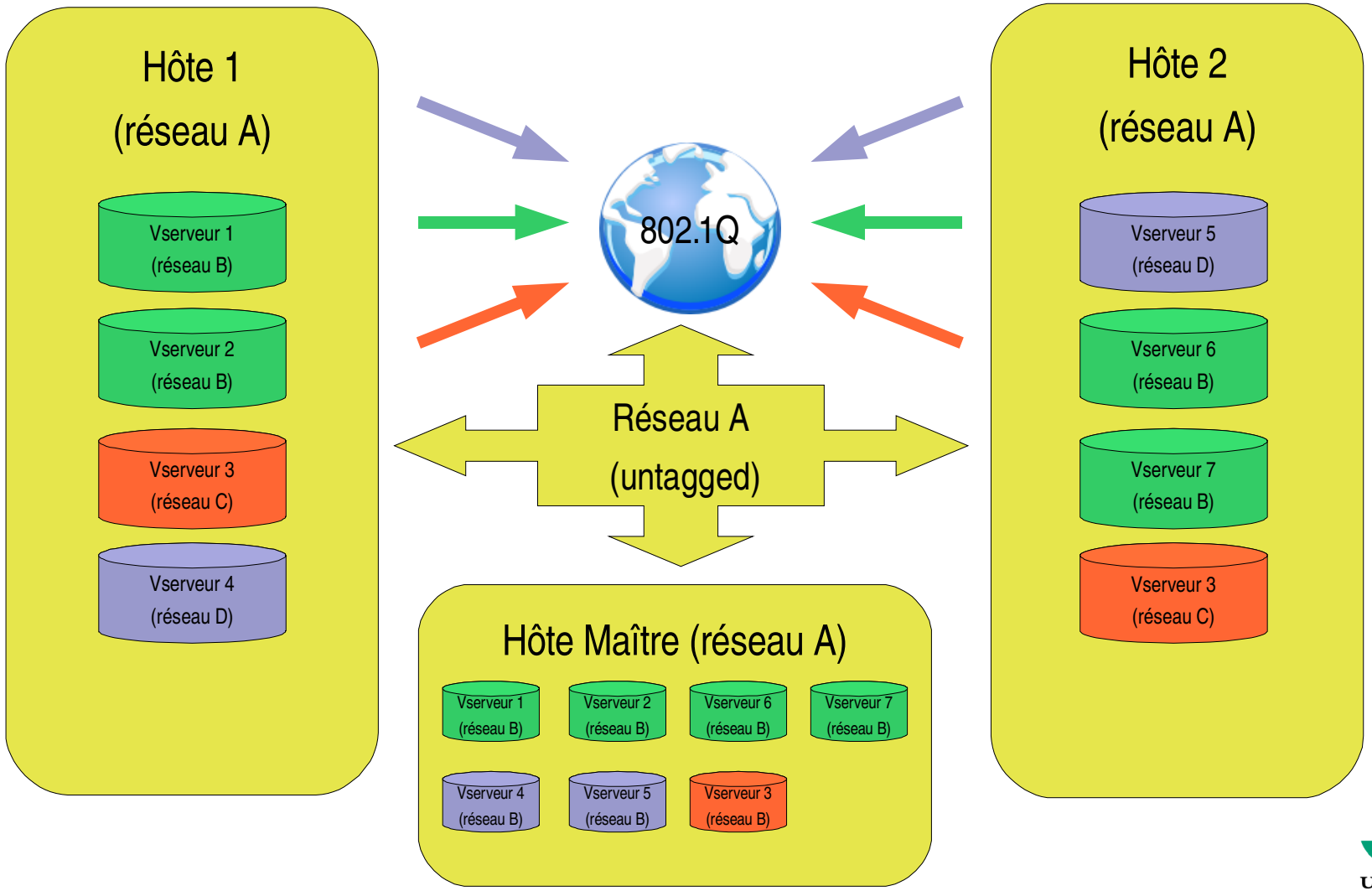
- Util-Vserver: «l'indispensable»
  - Est l'utilitaire officiel de Linux-Vserver
  - Fournit l'interface entre l'utilisateur, les machines virtuelles, et le noyau de l'hôte
  - Manque de fonctionnalités, mais sa conception permet d'en ajouter sans être modifié
- Vserver-Debiantools: «la touche Debian»
  - Intéressant, mais encore insuffisant

# Pourquoi VS-Tools ?

- VS-Tools: «le complément»
  - Création des Vserveurs simplifiée à l'extrême
    - ➔ arguments indispensables: un nom, et une adresse IPv4
  - Prise en charge automatique du routage et des VLANs
  - Gestion du firewall
  - Gestion (à chaud) des ressources
  - Surveillance et supervision (mail, Munin)
  - Déplacements et consolidation des Vserveurs

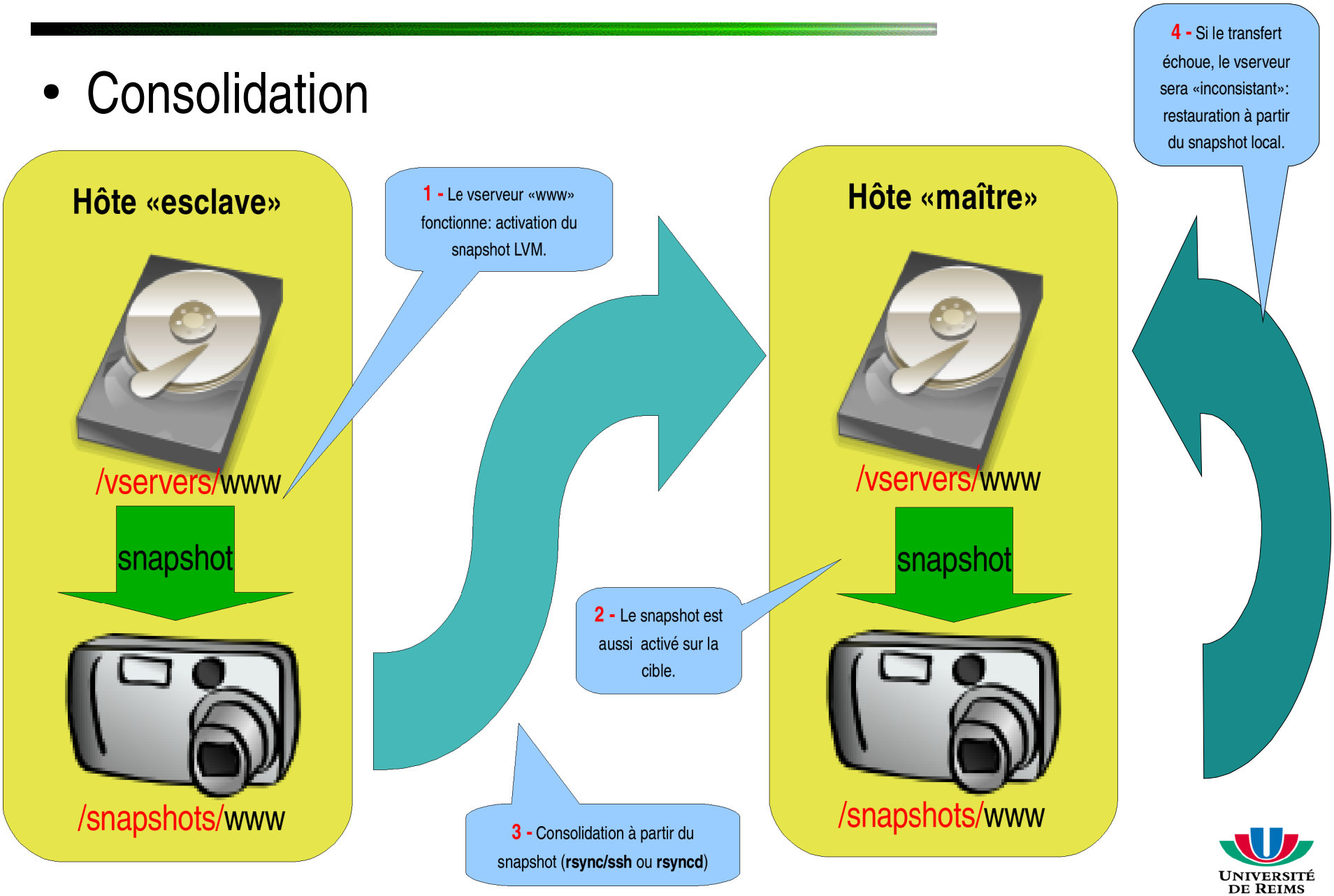
# Pourquoi VS-Tools ?

- Topologie



# Pourquoi VS-Tools ?

- Consolidation




UNIVERSITÉ DE REIMS CHAMPAGNE-ARDENNE

# Pourquoi VS-Tools ?

- Que des avantages (ou presque)
  - Une machine virtuelle par service
  - Configuration et optimisation simplifiées
  - Indépendance par rapport au matériel: les migrations sont une simple formalité !
  - Répartition des machines virtuelles en fonction de la charge
  - Plate-forme idéale pour le maquettage
- C'est intéressant même pour un seul Vserveur !

# Préparation d'un hôte Debian

- Généralités
  - L'hôte n'a pas vocation à faire fonctionner autre chose que les services de base (ssh, MTA, supervision) et les Vserveurs
    - ➔ Allouer un minimum d'espace disque
    - ➔ Installer uniquement le strict nécessaire
- Démarrage
  - Utiliser de préférence «image d'installation par le réseau»
    - ➔ http://cdimage.debian.org/debian-cd/4.0_r3/i386/iso-cd/debian-40r3-i386-netinst.iso

# Préparation d'un hôte Debian

- Réseau
  - Le système d'installation Debian ne supporte pas 802.1Q
    - ➔ Le réseau dédié aux hôtes doit être «untagged»
- Partitionnement
  - /dev/sda1 /boot ext3 100 Mo
  - /dev/sda5 swap 512 Mo
  - /dev/sda6 / ext3 1024 Mo
  - /dev/sda7 LVM Espace libre disponible

# Préparation d'un hôte Debian

- LVM
  - Ne pas utiliser plus de 90% du VG pour le LV (snapshots)
  - Monter le LV sur /var/lib/vservers
    - → Ext3: robuste
    - → XFS: «fsck» très rapide, extensible à chaud
- Installation du système de base
  - Utiliser un miroir réseau
  - «Système standard» uniquement

# Préparation d'un hôte Debian

- Le noyau

  *apt-get install linux-image-vserver-XXX*

  ➔ Attention: noyau compilé avec «CONFIG_HIGHMEM4G»

- Les utilitaires indispensables

  *apt-get install util-vserver ssh rsync lvm2 vlan mawk sed findutils mailx binutils bc lsof wget*

  – Installer et configurer un MTA (forcer le relayage des mails système).

  – Supprimer ou désactiver les services inutiles, et configurer le reste: rien ne doit écouter sur 0.0.0.0/0 !

# Préparation d'un hôte Debian

- Paramétrage du système
  - Modules noyau indispensables

    *echo "8021q">>/etc/modules ; echo "ip_tables">>/etc/modules*
  - Promotion automatique des adresses secondaires

    *echo "net.ipv4.conf.all.promote_secondaries=1">>/etc/sysctl.conf*
  - Ajoutez l'option «tagxid» au point de montage «/var/lib/vservers»
  - Fixer l'attribut «barrier»:

    *setattr --barrier /var/lib/vservers/*
  - Initialiser le compteur de contextes

    *echo 10000 > /etc/vservers/.defaults/context.next*

# Préparation d'un hôte Debian

- Installation de «vs-tools»
  - Il est préférable de commencer par l'hôte «maître»
    - Créer une paire de clés SSH
    - Télécharger et installer les scripts

      *wget https://listes.univ-reims.fr/sympa/d_read/vs-tools/Sources/Latest.tgz*

      *cd /usr/src ; tar -xzf Latest.tgz ; cd vs-tools ; sh install.sh*
  - Puis de configurer «vs-tools»
  - Et enfin de déployer l'ensemble sur tous les hôtes du pool

    *cd /usr/src/vs-tools ; sh update-hosts.sh*

# Configuration

- Généralités
  - Fichiers dans «/etc/vs-tools»
  - «networks.conf» prioritaire sur «create.conf»
  - «*.conf.sample»: écrasés lors des mises à jour
  - «firewall.conf», «monitor.conf»: modèles
  - «slaves.conf» et «backup.conf»: hôtes maîtres uniquement

# Configuration

- /etc/vs-tools/networks.conf
  - Définition des réseaux utilisables par les Vserveurs
  - Doit être identique sur tous les hôtes du pool
  - Une ligne par réseau:

```
# vlan_id,network_address/prefix,gateway[,domain[,nameserver nameserver ...]]

1,10.0.1.0/24,10.0.1.1,foo.bar,10.0.3.6
2,10.0.2.0/24,10.0.2.1
3,10.0.3.0/24,10.0.3.1,foo.bar,10.0.3.5 10.0.3.6
```

# Configuration

- /etc/vs-tools/create.conf
  - Définition des paramètres appliqués par défaut lors de la création des Vserveurs

```
DEFAULT_DEVICE=eth0
#MTU=1496

DEFAULT_DOMAIN=univ-reims.fr
DEFAULT_NAMESERVER="193.50.208.4"
#DEFAULT_PREFIX=24

DEFAULT_DISK_LIMIT=1024
DEFAULT_RSS_LIMIT=128
DEFAULT_TMPFS_LIMIT=16
DEFAULT_PROC_LIMIT=150
DEFAULT_CPU_LIMIT=9/10
```

```
FAKE_OS=2.6.8

CONTEXT_METHOD=cnt

DEFAULT_METHOD=template
DEFAULT_TEMPLATE=/vservers/TEMPLATES/etch1.tgz

DEFAULT_DISTRO=etch
MAIN_MIRROR=http://ftp.fr.debian.org/debian
UPDATE_MIRROR=http://security.debian.org
```

# Configuration

- /etc/vs-tools/monitor.conf ⇨ /etc/vservers/*/monitor.conf
  - Surveillance effectuée par l'hôte
  - Une instance par Vserveur
  - Remontées d'alertes par mail

```
MONITOR_MAILTO=root

MONITOR_POOLING=60

RSS_THRESHOLD=90
DISK_THRESHOLD=90
TMPFS_THRESHOLD=90
PROC_THRESHOLD=90
```

```
LOADAVG_15_THRESHOLD=2

MONITOR_RSS_HITS=yes
MONITOR_PROC_HITS=yes

MONITOR_SOCKETS=yes

#SOCKETS_FILTER="/apache2$| /var/run/apache2/cgisock\."
```

# Configuration

- /etc/vs-tools/firewall.conf ⇨ /etc/vservers/*/firewall.conf
  - Un jeu de règles par Vserveur
  - Contrôle par l'hôte uniquement
  - Les adresses des Vserveurs sont implicites
  - L'hôte est automatiquement isolé

```
enable
## Policy is ACCEPT (ESTABLISHED,RELATED is implicit)
allow to 10.9.53.27,10.7.21.12 to udp/53          # DNS
allow to 10.7.21.47 to tcp/25                     # Relayage mails systeme
allow from 10.8.3.5 to tcp/5666,tcp/4949          # Nagios, Munin
allow from 10.10.1.0/24,10.9.1.62 to tcp/22       # sshd
allow from 0/0 to tcp/80                          # httpd
## DENY is implicit
```

# Configuration

- /etc/vs-tools/slaves.conf
  - Hôte «maître» uniquement
  - Définition des hôtes «esclaves» du pool
  - rsyncd: voir «rsyncd.conf.sample»
  - Dans tous les cas, ne pas oublier la clé SSH !

```
vsh-00:noselect
vsh-01
vsh-02
#vsh-03
vsh-04:bwlimit=10m
vsh-05:compress,bwlimit=512k
vsh-06
vsh-07
```

# Configuration

- /etc/vs-tools/backup.conf
  - Hôte «maître» uniquement
  - Définition des Vserveurs à consolider
  - Sélection automatique de l'hôte

```
# Templates
etch1:cold
lamp:cold
# Supervision
nagios:hot
munin:hot
cri:hot
# Divers
jabber:hot
ldap:hot
```

# Exploitation

- Généralités
  - Toutes les commandes sont préfixées: «vs-»
  - Et documentées: «--help»
  - Certaines sont dédiées au «maître»
    - ➔ *vs-scan, vs-backup, vs-move, vs-get, vs-put, vs-remove*
  - L'activité de la librairie est consignée via Syslog
  - Elle peut être invoquée «manuellement»
    - ➔ vs-functions <nom fonction> <arguments>

# Exploitation

- Création des Vserveurs
  - Méthode «debootstrap»
    - Créer un Vserveur Debian «propre»
    - Surtout utile pour la création des «templates»

      *vs-create --name <vserveur> --interface <adresse IPv4> --debootstrap <distro>*
  - Méthode «template»
    - Créer un Vserveur à partir d'un «patron»
    - Très rapide ...

      *vs-create --name <vserveur> --interface <adresse IPv4> --template <fichier tgz>*
  - Il est préférable d'utiliser toujours le même hôte

# Exploitation

- Création des Vserveurs: les arguments
  - Seuls deux sont indispensables lorsque «create.conf» et «networks.conf» sont correctement configurés

    *vs-create --name <nom vserveur> --interface <adresse IPv4>*
  - Il est toujours possible de spécifier manuellement ceux qui seront prioritaires sur la configuration par défaut
    - Nom de domaine, serveur(s) DNS
    - Ressources systèmes

# Exploitation

- Statistiques et gestion des ressources
  - Afficher les statisques (de l'hôte ou d'un Vserveur)

    *vs-stats* ou *vs-stats --name <vserveur>*
  - Afficher les ressources

    *vs-limit --name <vserveur>*

    → *<host>:<vserver>:<rss>:<disk>:<tmpfs>:<proc>:<cpu>*
  - Modifier les ressources

    *vs-limit --name <vserveur> --rss <Mo> --disk <Mo> --tmpfs <Mo> --proc <nbr> --cpu <ratio>*
  - «--name» peut être remplacé par «--all»

# Exploitation

- Contrôle des Vserveurs
  - Il peuvent combiner plusieurs états
    - Démarrage (et arrêt) avec l'hôte
    - En fonctionnement ou arrêté
  - Afficher l'état

    *vs-control --name <vserveur>*

    → *<host>:<vserver>:<enabled/disabled>:<running/stopped>*
  - Changer l'état

    *vs-control --name <vserveur> --enable/--disable --start/--stop*
  - «--name» peut être remplacé par «--all»

# Exploitation

- Hébergement, consolidation
  - Seul l'hôte «maître» peut télécharger, consolider, ou supprimer les Vserveurs
  - Il doit disposer d'un espace de stockage suffisant
  - Il sélectionne automatiquement les hôtes en fonction des états des Vserveurs
  - L'utilisation des Snapshots LVM permet de sécuriser les téléchargements, et de réduire les durées d'interruption de services

# Exploitation

- Localiser les Vserveurs

  *vs-scan (facultatif: --name<vserveur> --host <hôte>)*

- Télécharger, déplacer, supprimer

  *vs-get --name <vserveur> (facultatif: --host <hôte>)*

  *vs-put --name <vserveur> --host <hôte>*

  *vs-move --name <vserveur> --dst_host <hôte> (facultatif: --src_host <hôte>)*

  *vs-remove --name <vserver> --host <hôte>*

- Consolidation

  *vs-backup (facultatif: --host <hôte>)*

# Exploitation

- Interfaces, VLANs, routage et Firewall
  - Activés et supprimés automatiquement lors des démarrage et arrêts des Vserveurs («start-stop-scripts»)
  - Afficher l'état

    *vs-net --name <vserver>*

    → *<host>:<vserver>:<ip>:<vlan>:<route>:<fw IN>:<fw OUT>*
  - Modifier l'état

    *vs-net --name <vserver> --route <up/down> --vlan <up/down> --fw <up/down>*
  - «--name» peut être remplacé par «--all»

# Exploitation

- Gestion des paquets
  - Les ACLs des Vserveurs doivent être très strictes
    - ➔ Interdire toute connexion non désirée, y compris pour les installations et mises à jour de paquets
  - La gestion des paquets est donc effectuée par les hôtes
    - ➔ Les Firewalls sont automatiquement désactivés et réactivés

    *vs-pkg --name <vserveur> --update_sources --list_upgrades --upgrade_all --install <paquet> ....*
  - Elle peut être indépendante des distributions ...

# Difficultés (pouvant être) rencontrées

- Caches ARP
- Routage & Firewall
- Ressources (tuning noyau)
- Accès aux périphériques
- Stockage, LVM (snapshots)
- «Prolifération» des hôtes et des Vserveurs

# Des questions ?

Une liste «Sympa» est à votre disposition

vs-tools@univ-reims.fr

Ainsi qu'un espace «documents»

`https://listes.univ-reims.fr/sympa/info/vs-tools`

UNIVERSITÉ
DE REIMS
CHAMPAGNE-ARDENNE