A dark blue vertical bar on the left side of the page. A blue arrow points to the right from the bar, containing the date.

11/11/2017

# Documentation Création d'un Template Debian 9.2 et Windows

Version 1.0 : Version Initiale

Several thin, curved lines in dark blue and light grey that sweep upwards from the bottom left corner of the page.

Fabien MAUHOURLAT  
[NOM DE LA SOCIETE]

# Création d'un Template Debian 9.2 et Windows

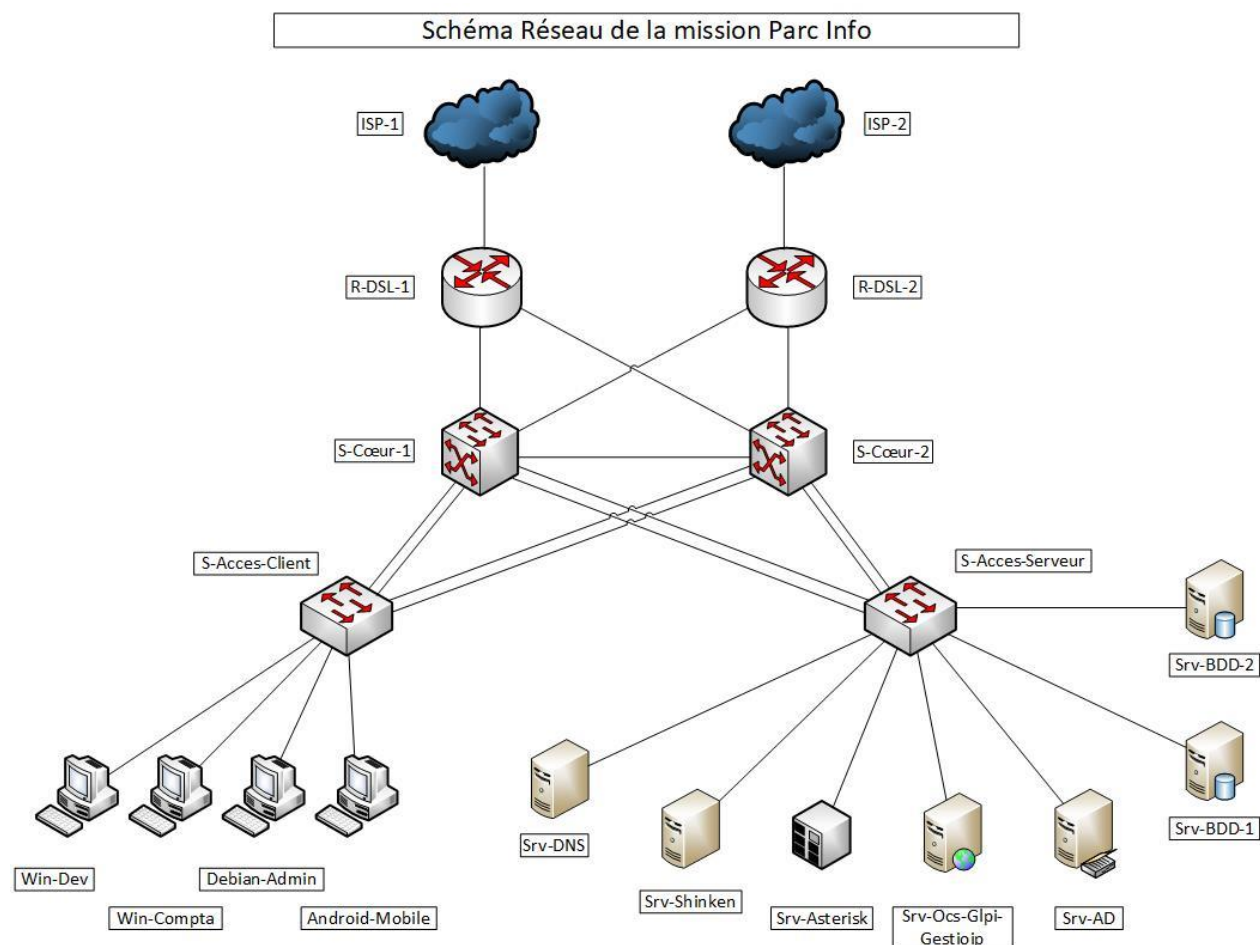
## Contexte :

Pour permettre un déploiement rapide de l'infrastructure il est nécessaire de réaliser des template ou des images qui vont servir de master pour tous les serveur et clients.

Sous linux après avoir configuré le template et cloner la machine il suffit juste de changer l'adresse ip puis de renouveler les clés hôtes du service critique SSH pour réaliser un déploiement en un minimum de temps.

Ainsi la solution sysprep sous windows permet de reinitialiser l'identifiant de sécurité ce qui permet de cloner la machine sans risque de conflit lors de l'intégration de la nouvelle machine dans l'Active Directory.

## Voici l'architecture mise en place :



# Sommaire

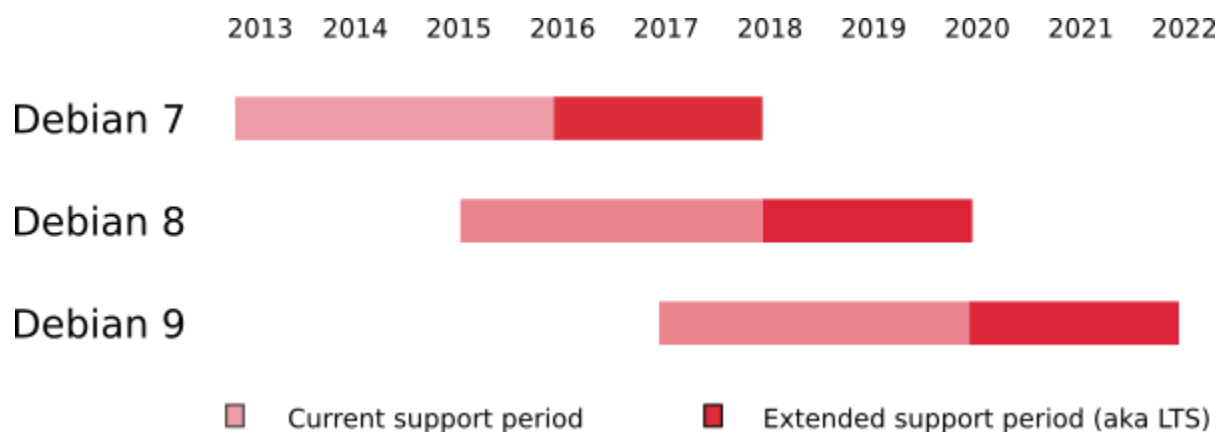
- I. Présentation et choix des solutions
- II. Configuration du template Linux
- III. Configuration du template Windows
- IV. Déploiement du template Linux
- V. Déploiement du template Windows
- VI. Annexes

## I. Présentation et choix des solutions

### Choix de la solution Debian 9 :

Après 26 mois de développement, le projet Debian est fier d'annoncer sa nouvelle version stable n° 9 (nom de code Stretch), qui sera gérée pendant les cinq prochaines années grâce à l'effort combiné de l'équipe de sécurité de Debian ainsi qu'à celui de l'équipe de gestion à long terme de Debian.

Dans Stretch, la variante par défaut de MySQL est maintenant MariaDB. Le remplacement des paquets de MySQL 5.5 ou 5.6 par la variante MariaDB 10.1 se produira automatiquement lors de la mise à niveau.



### Choix des solution Windows :

Présentation du fonctionnement les différentes branches de Windows 10 :

Avec l'arrivée de Windows 10 Microsoft utilise comme modèle le service.

Microsoft va améliorer les fonctionnalités du système avec des mises à jour de fonctionnalité 2 à 3 fois par an plutôt que de proposer un nouveau système d'exploitation tous les trois ans.

#### **CB : Current Branch ou phase pilote**

Current Branch est la branche recevant la nouvelle build en premier. Elle aura été en amont validée par les betas testeurs grâce au programme « Windows Insider ».

#### **CBB : Current Branch for Business ou phase production**

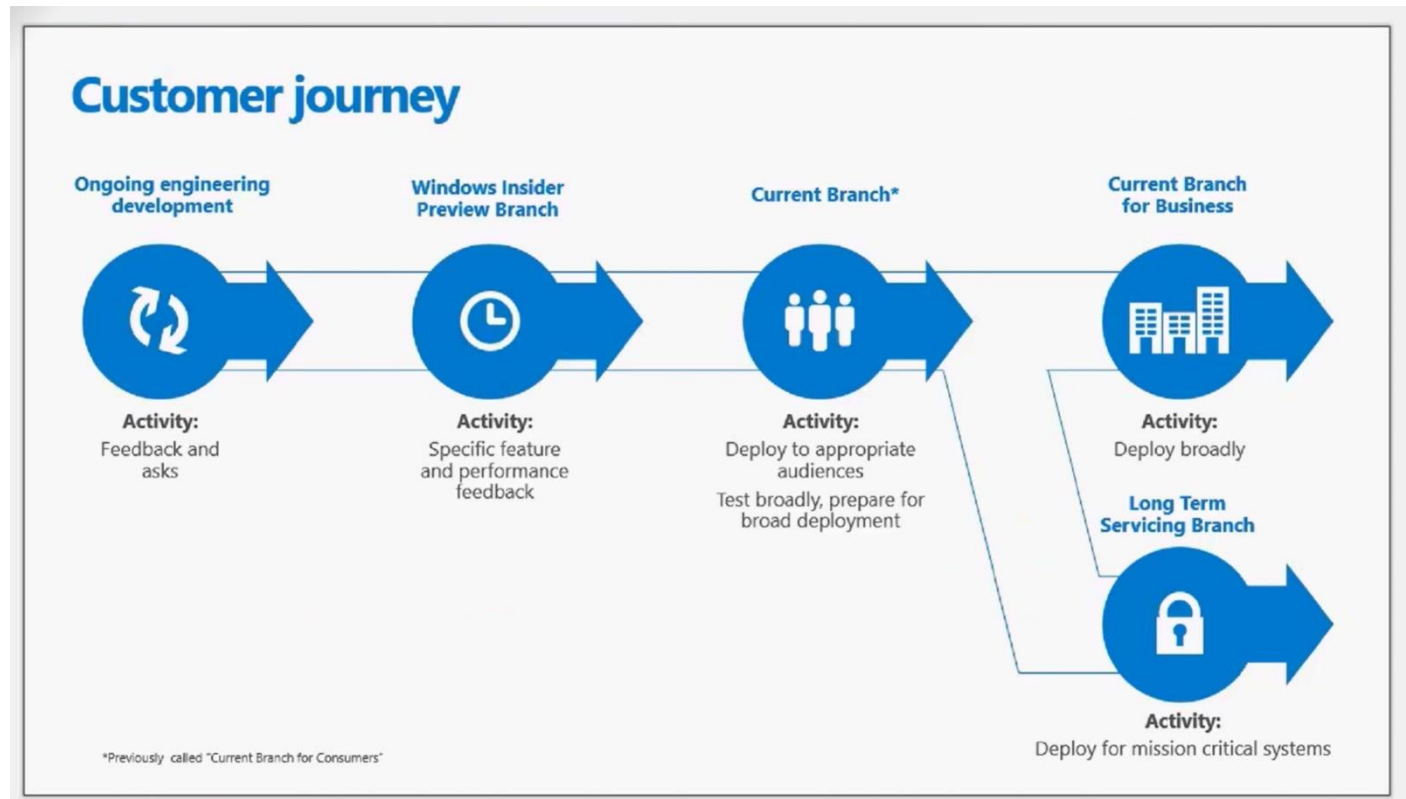
Après environ 4 mois, Microsoft annonce que la build a atteint la maturité attendue pour être déployer en entreprise. Nous recommandons nos clients d'effectuer les tests avec leurs environnements avant tout déploiement.

### LTSB : Long Term Service Branch

Enfin pour les postes critiques, la branche « Long Term service Branch » aura quant à elle un support de 10 ans. (5 ans en support standard et 5 en support étendu).

Cette version n'inclut pas le Windows Store, les Windows Universal Apps installés par défaut ainsi que Microsoft Edge.

C'est cette version qui a été choisie pour l'infrastructure grâce notamment à une meilleure stabilité du système.



Du coté des serveurs la version standard de 2012 r2 a été choisi dans la configuration de l'infrastructure du fait principalement qu'elle dispose de toutes les fonctionnalités de Windows server. La version Datacenter permet de faire de la virtualisation plus avancée mais pas nécessaire ici.



### Choix de la solution VMware workstation :

**VMware Workstation** est un outil de virtualisation de poste de travail créé par la société VMware, il peut être utilisé pour mettre en place un environnement de test pour développer de nouveaux logiciels, ou pour tester l'architecture complexe d'un système d'exploitation avant de l'installer réellement sur une machine physique.

### **Systèmes d'exploitation invités supportés**

Un système d'exploitation invité peut être Windows, Linux, et d'autres systèmes d'exploitation couramment utilisés.

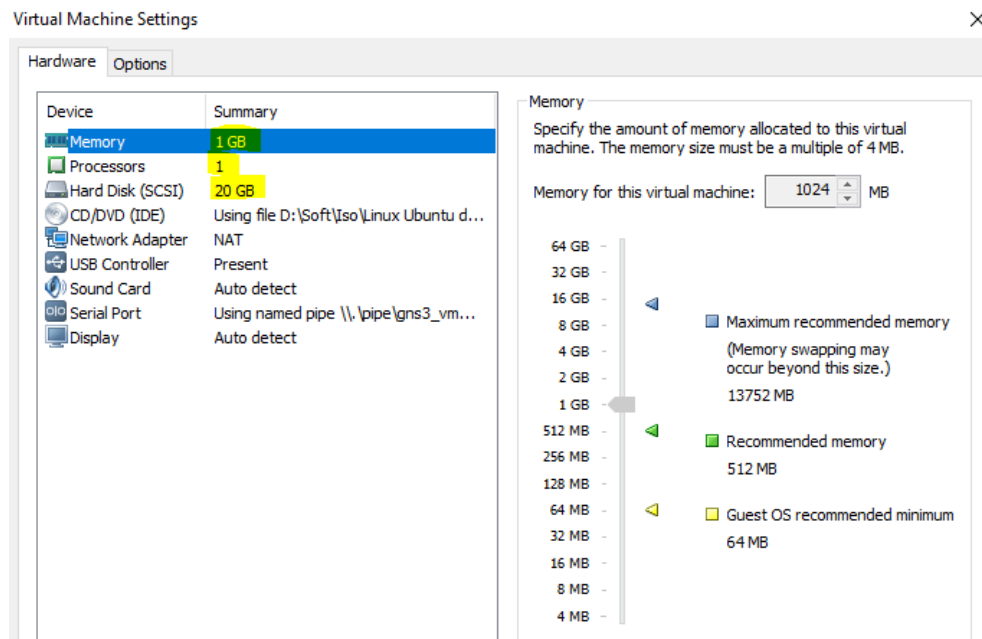
VMware workstation a été utilisé dans cette note technique en version 12.5.7.

## II. Configuration du template Linux

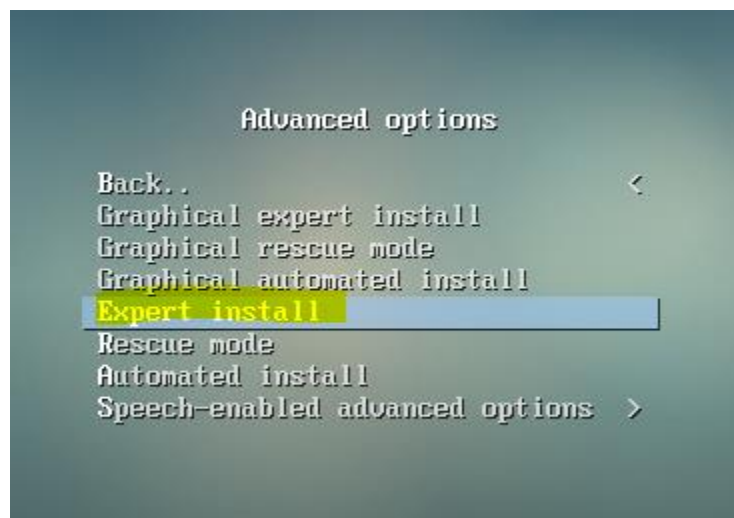
### 1. Installation de la machine virtuelle sous debian 9.2 :

Créer la machine virtuelle avec les spécification suivantes :

- 1gb de RAM
- 1 processeur
- Et 20GB de disque dur virtuel



Démarrer l'installation de la VM en mode expert :



**Schéma du partitionnement des disques grâce au LVM :**

Répertoire	Taille GB	Systèmes de fichier
Swap	1 GB	Linux Swap
/boot	250 MB	Ext3
/	3.7 GB	LVM Ext4
/usr	6 GB	LVM Ext4
/var	5 GB	LVM Ext4
/tmp	2.5 GB	LVM Ext4
/home	3 GB	LVM Ext4

**Lors du choix de partitionnement des disques créer trois partitions :**

- Une partition swap de 1GB
- Une partition de BOOT de 250MB
- Et une partition en LVM qui va nous servir a créé les autres partitions du système :

```

[!!] Partitionner les disques

Voici la table des partitions et les points de montage actuellement configurés. Vous
pouvez choisir une partition et modifier ses caractéristiques (système de fichiers, point
de montage, etc.), un espace libre pour créer une nouvelle partition ou un périphérique
pour créer sa table des partitions.

Partitionnement assisté
Configurer le RAID avec gestion logicielle
Configurer le gestionnaire de volumes logiques (LVM)
Configurer les volumes chiffrés
Configurer les volumes iSCSI

SCSI1 (0,0,0) (sda) - 21.5 GB VMware, VMware Virtual S
n° 1 primaire 248.5 MB f ext3 /boot
n° 2 primaire 1.0 GB f swap swap
n° 3 primaire 20.2 GB K lvm

Annuler les modifications des partitions
Terminer le partitionnement et appliquer les changements

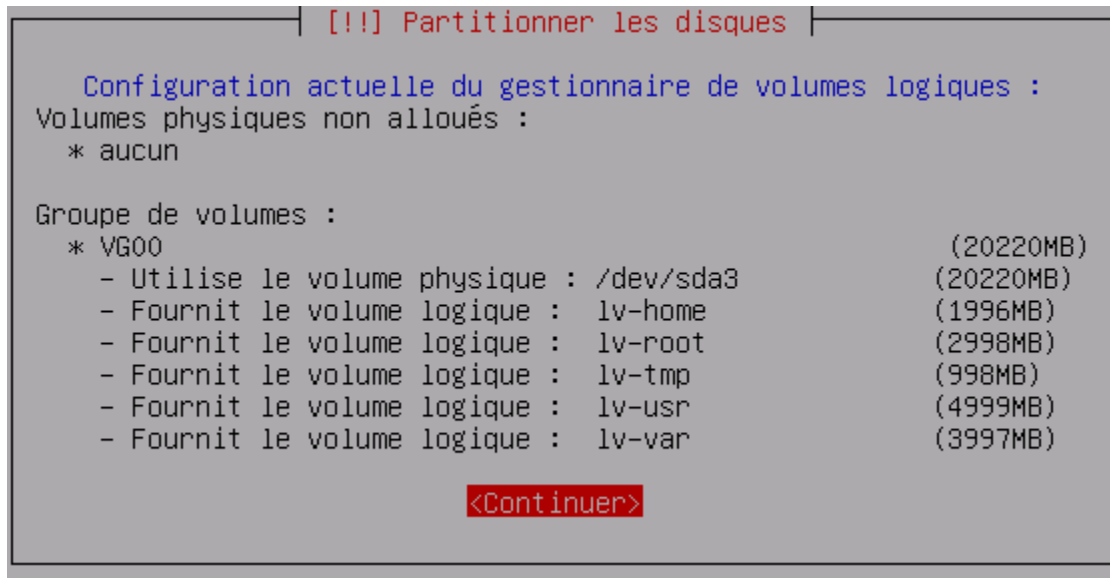
<Revenir en arrière>

```

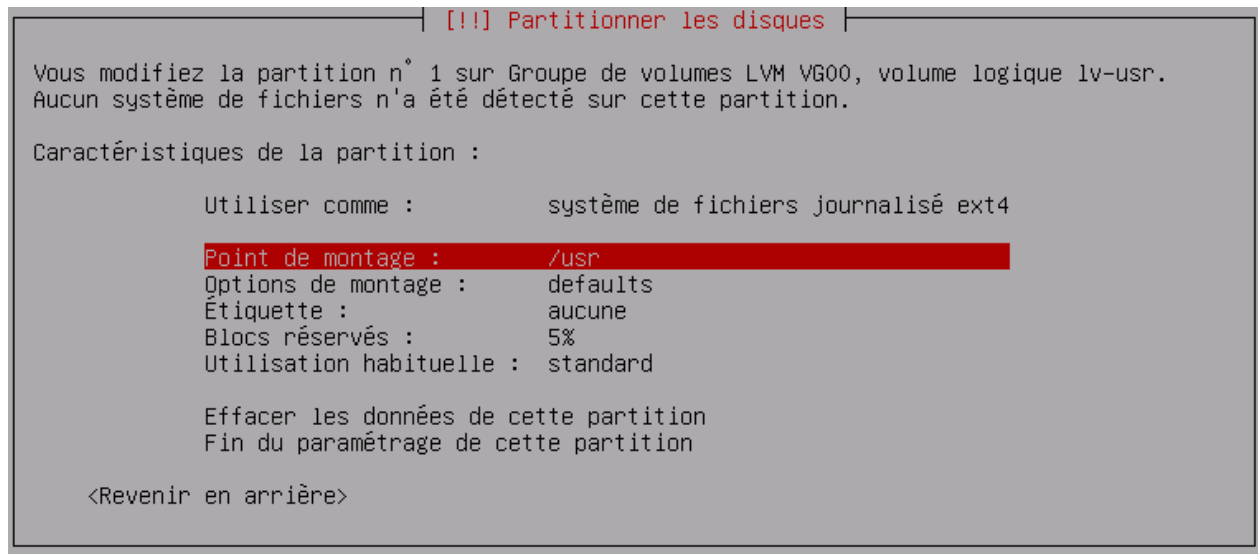


Après avoir terminée les changements sur le disque il faut configurer les LVM en suivant le schéma ci-dessus :

- Crée chaque partition à partir du volume groupe VG00



Formater ensuite chaque partition en EXT4 puis appliquer le point de montage :



Récapitulatif des partitions au format LVM et de leur point de montage associés :

```

[!!] Partitionner les disques

Voici la table des partitions et les points de montage actuellement configurés. Vous
pouvez choisir une partition et modifier ses caractéristiques (système de fichiers, point
de montage, etc.), un espace libre pour créer une nouvelle partition ou un périphérique
pour créer sa table des partitions.

Partitionnement assisté
Configurer le RAID avec gestion logicielle
Configurer le gestionnaire de volumes logiques (LVM)
Configurer les volumes chiffrés
Configurer les volumes iSCSI

Groupe de volumes LVM VG00, volume logique lv-home - 2.0 GB Linux device-mapper (line
n° 1 2.0 GB f ext4 /home
Groupe de volumes LVM VG00, volume logique lv-root - 3.0 GB Linux device-mapper (line
n° 1 3.0 GB f ext4 /
Groupe de volumes LVM VG00, volume logique lv-tmp - 998.2 MB Linux device-mapper (lin
n° 1 998.2 MB f ext4 /tmp
Groupe de volumes LVM VG00, volume logique lv-usr - 5.0 GB Linux device-mapper (linea
n° 1 5.0 GB f ext4 /usr
Groupe de volumes LVM VG00, volume logique lv-var - 4.0 GB Linux device-mapper (linea
n° 1 4.0 GB f ext4 /var
SCSI1 (0,0,0) (sda) - 21.5 GB VMware, VMware Virtual S
n° 1 primaire 248.5 MB F ext3 /boot
n° 2 primaire 1.0 GB F swap swap
n° 3 primaire 20.2 GB K lvm

Annuler les modifications des partitions
Terminer le partitionnement et appliquer les changements

<Revenir en arrière>

```

Appliqué les changements sur le disque :

```

[!!] Partitionner les disques

Si vous continuez, les modifications affichées seront écrites sur les disques. Dans le
cas contraire, vous pourrez faire d'autres modifications.

Les tables de partitions des périphériques suivants seront modifiées :
Groupe de volumes LVM VG00, volume logique lv-home
Groupe de volumes LVM VG00, volume logique lv-root
Groupe de volumes LVM VG00, volume logique lv-tmp
Groupe de volumes LVM VG00, volume logique lv-usr
Groupe de volumes LVM VG00, volume logique lv-var

Les partitions suivantes seront formatées :
Groupe de volumes LVM VG00, volume logique lv-home de type ext4
Groupe de volumes LVM VG00, volume logique lv-root de type ext4
Groupe de volumes LVM VG00, volume logique lv-tmp de type ext4
Groupe de volumes LVM VG00, volume logique lv-usr de type ext4
Groupe de volumes LVM VG00, volume logique lv-var de type ext4

Faut-il appliquer les changements sur les disques ?

<Oui> <Non>

```

Lors de la sélection des paquets à installer désélectionner tous sauf utilitaires usuels du système



Une fois l'installation finit on peut afficher les LVM et leur espace utilisé avec la commande `df -h` :

```
root@debian-temp:~# df -h
Sys. de fichiers      Taille Utilisé Dispo Uti% Monté sur
udev                  494M      0  494M   0% /dev
tmpfs                  100M    3,3M   97M   4% /run
/dev/mapper/VG00-lv--root 2,7G    254M  2,3G  10% /
/dev/mapper/VG00-lv--usr  4,6G    230M  4,1G   6% /usr
tmpfs                  499M      0  499M   0% /dev/shm
tmpfs                  5,0M      0   5,0M   0% /run/lock
tmpfs                  499M      0  499M   0% /sys/fs/cgroup
/dev/mapper/VG00-lv--home 1,8G     5,6M  1,7G   1% /home
/dev/mapper/VG00-lv--tmp  922M     2,4M  856M   1% /tmp
/dev/mapper/VG00-lv--var  3,7G    173M  3,3G   5% /var
/dev/sda1              226M     24M  191M  11% /boot
root@debian-temp:~#
```

Le système d'exploitation utilisé dans cette note technique est la version 9.2 de Debian (Stretch) et la version du noyau utilisé est le 4.9.0.

```
fabien@debian-template:/etc/shinken/brokers$ lsb_release -a
No LSB modules are available.
Distributor ID: Debian
Description:    Debian GNU/Linux 9.2 (stretch)
Release:        9.2
Codename:       stretch
fabien@debian-template:/etc/shinken/brokers$ uname -a
Linux debian-template 4.9.0-3-amd64 #1 SMP Debian 4.9.30-2+deb9u5 (2017-09-19) x86_64 GNU/Linux
fabien@debian-template:/etc/shinken/brokers$
```

## 2. Configuration et durcissement de la VM linux :

### Installation des paquets pour la compilation et autres :

- Paquet compilation : headers linux, build-essential (contient make)
- Paquets réseau : wget, curl, git, net-tool snmpd, dnsutils
- Paquets autres : vmware tools et vim

apt install sudo wget curl openssh-server openssh-client dnsutils snmpd git open-vm-tools net-tool vim  
build-essential linux-headers(uname -r)

```
fabien@debian-temp:~$ cat /etc/group | grep sudo
sudo:x:27:prof,fabien
fabien@debian-temp:~$
```

```
# User privilege specification
root    ALL=(ALL:ALL) ALL
fabien  ALL=(ALL:ALL) ALL
prof    ALL=(ALL:ALL) ALL
```

### Installation et configuration du protocole SSH :

Sudo apt install openssh-server openssh-client

sudo systemctl start sshd

sudo systemctl enable sshd

sudo vim /etc/ssh/sshd\_config

```
Protocol 2
Port 47000
ListenAddress 192.168.1.5
AllowUsers fabien prof
ClientAliveInterval 300
ClientAliveCountMax 0
IgnoreRhosts yes # Disable RSH
PermitRootLogin no
PermitEmptyPasswords no
Allowtcpforwarding no
X11Forwarding no
PasswordAuthentication no
SyslogFacility AUTH
LogLevel INFO
StrictModes yes
MaxAuthTries 3
MaxSessions 3
```

PubkeyAuthentication yes  
 HostbasedAuthentication no  
 IgnoreUserKnownHosts no

```
fabien@Srv-Ocs-Glpi-Gestioip:/$ sudo netstat -ntpl
[sudo] Mot de passe de fabien :
Connexions Internet actives (seulement serveurs)
Proto Recv-Q Send-Q Adresse locale      Adresse distante     Etat      PID/Program name
tcp        0      0 127.0.0.1:3306       0.0.0.0:*             LISTEN    4212/mysqld
tcp        0      0 0.0.0.0:80           0.0.0.0:*             LISTEN    4402/apache2
tcp        0      0 0.0.0.0:47000        0.0.0.0:*             LISTEN    633/sshd
tcp        0      0 0.0.0.0:443          0.0.0.0:*             LISTEN    4402/apache2
fabien@Srv-Ocs-Glpi-Gestioip:/$
```

### De façon optionnel on peut attribuer un mot de passe au bootloader Grub :

```
sudo grub-mkpasswd-pbkdf2

sudo vim /etc/grub.d/40_custom

set superusers="root"

password_pbkdf2 root
grub.pbkdf2.sha512.10000.D3C1674D850A57811A32846C9243831D84DF7413C6053AEA879367B23D88
DD778DFF478A58DF50CFD6ACA07FA26DB5CF2CFA015D40E8569EFA30665389D91AEF.ECB8BF8BB202B
F348B0ED1B8714AC6$

sudo update-grub
```

### Durcissement du noyau Linux :

#### Désactivation de l'IPv6 :

```
fabien@Srv-Ocs-Glpi-Gestioip:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:9e:73:3e brd ff:ff:ff:ff:ff:ff
    inet 192.168.75.80/24 brd 192.168.75.255 scope global ens33
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe9e:733e/64 scope link
        valid_lft forever preferred_lft forever
fabien@Srv-Ocs-Glpi-Gestioip:~$
```

```
fabien@Srv-Ocs-Glpi-Gestioip:~$ sudo netstat -ntpl
[sudo] Mot de passe de fabien :
Connexions Internet actives (seulement serveurs)

```

Proto	Recv-Q	Send-Q	Adresse locale	Adresse distante	Etat	PID/Program name
tcp	0	0	127.0.0.1:3306	0.0.0.0:*	LISTEN	774/mysqld
tcp	0	0	0.0.0.0:47000	0.0.0.0:*	LISTEN	647/sshd
tcp	0	0	127.0.0.1:25	0.0.0.0:*	LISTEN	1088/exim4
tcp6	0	0	:::80	:::*	LISTEN	804/apache2
tcp6	0	0	:::1:25	:::*	LISTEN	1088/exim4
tcp6	0	0	:::443	:::*	LISTEN	804/apache2

```
fabien@Srv-Ocs-Glpi-Gestioip:~$
```

### sudo vim /etc/sysctl.conf

net.ipv6.conf.all.disable\_ipv6 = 1

net.ipv6.conf.default.disable\_ipv6 = 1

net.ipv6.conf.lo.disable\_ipv6 = 1

net.ipv6.conf.eth0.disable\_ipv6 = 1

```
fabien@Srv-Ocs-Glpi-Gestioip:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast
    link/ether 00:0c:29:9e:73:3e brd ff:ff:ff:ff:ff:ff
    inet 192.168.75.80/24 brd 192.168.75.255 scope global ens33
        valid_lft forever preferred_lft forever
fabien@Srv-Ocs-Glpi-Gestioip:~$
```

```
fabien@Srv-Ocs-Glpi-Gestioip:~$ sudo netstat -ntpl
[sudo] Mot de passe de fabien :
Connexions Internet actives (seulement serveurs)

```

Proto	Recv-Q	Send-Q	Adresse locale	Adresse distante	Etat	PID/Program name
tcp	0	0	127.0.0.1:3306	0.0.0.0:*	LISTEN	750/mysqld
tcp	0	0	0.0.0.0:80	0.0.0.0:*	LISTEN	752/apache2
tcp	0	0	0.0.0.0:47000	0.0.0.0:*	LISTEN	636/sshd
tcp	0	0	127.0.0.1:25	0.0.0.0:*	LISTEN	1037/exim4
tcp	0	0	0.0.0.0:443	0.0.0.0:*	LISTEN	752/apache2

```
fabien@Srv-Ocs-Glpi-Gestioip:~$
```

# IP Spoofing protection

net.ipv4.conf.all.rp\_filter = 1

net.ipv4.conf.default.rp\_filter = 1

# Ignore ICMP broadcast requests

net.ipv4.icmp\_echo\_ignore\_broadcasts = 1

# Ignore Directed pings

net.ipv4.icmp\_echo\_ignore\_all = 0

```
# Disable source packet routing (tracert etc)
net.ipv4.conf.all.accept_source_route = 0
net.ipv4.conf.default.accept_source_route = 0

# Ignore send redirects
# Ne pas envoyer de redirections ICMP
net.ipv4.conf.all.send_redirects = 0
net.ipv4.conf.default.send_redirects = 0

# Block SYN attacks
net.ipv4.tcp_syncookies = 1
net.ipv4.tcp_max_syn_backlog = 2048
net.ipv4.tcp_synack_retries = 2
net.ipv4.tcp_syn_retries = 5

# Loguer les paquets ayant des IPs anormales
# (adresse source falsifiée ou non routable)
net.ipv4.conf.all.log_martians = 1
net.ipv4.icmp_ignore_bogus_error_responses = 1

# Ignore ICMP redirects
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.all.secure_redirects = 0
net.ipv4.conf.default.accept_redirects = 0
net.ipv4.conf.default.secure_redirects = 0
```

### **Configuration d'IP tables sur le serveur :**

## On supprime les règles iptables.

```
iptables -F
iptables -X
```

## On drop tout le trafic entrant.

```
iptables -P INPUT DROP
iptables -P OUTPUT ACCEPT
iptables -P FORWARD ACCEPT
```

```
# Autorise le loopback (127.0.0.1)
iptables -A INPUT -i lo -j ACCEPT
```

```
# ICMP (le ping)
iptables -A INPUT -p icmp -j ACCEPT
```

```
iptables -A INPUT -p tcp -i ens33 --dport 47000 -j ACCEPT
iptables -A INPUT -p udp -i ens33 --dport 161 -j ACCEPT
iptables -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
```

```
fabien@Srv-Ocs-Glpi-Gestioip:~$ sudo iptables -L
Chain INPUT (policy DROP)
target    prot opt source                destination
ACCEPT    all  --  anywhere              anywhere
ACCEPT    icmp --  anywhere              anywhere
ACCEPT    tcp  --  anywhere              anywhere    tcp dpt:47000
ACCEPT    tcp  --  anywhere              anywhere    tcp dpt:http
ACCEPT    tcp  --  anywhere              anywhere    tcp dpt:https
ACCEPT    udp  --  anywhere              anywhere    udp dpt:snmp
ACCEPT    all  --  anywhere              anywhere    state RELATED,ESTABLISHED

Chain FORWARD (policy ACCEPT)
target    prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target    prot opt source                destination
fabien@Srv-Ocs-Glpi-Gestioip:~$
```

iptables-save > /etc/iptables\_rules\_v4

```
# Generated by iptables-save v1.6.0 on Mon Nov  6 06:30:54 2017
*filter
:INPUT DROP [13:4399]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [4:452]
-A INPUT -i lo -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i ens33 -p tcp -m tcp --dport 47000 -j ACCEPT
-A INPUT -i ens33 -p udp -m udp --dport 161 -j ACCEPT
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
COMMIT
# Completed on Mon Nov  6 06:30:54 2017
```

/etc/network/interfaces

post-up iptables-restore < /etc/iptables\_rules\_v4

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug ens33
iface ens33 inet static
    address 192.168.10.1/24
    gateway 192.168.10.250
    dns-nameservers 192.168.10.230
    dns-search bora-bora.nc
    post-up iptables-restore < /etc/iptables-rules
```



## I. Installation de l'agent OCS

### **Installation des paquets pour la compilation et autres :**

#### **Installation des dépendance de Perl :**

- apt-get -y install -y dmidecode libxml-simple-perl libio-compress-perl libnet-ip-perl libwww-perl libdigest-md5-perl libnet-ssleay-perl
- libcrypt-ssleay-perl (pour utiliser SSL)
- libnet-snmp-perl (pour utiliser la fonctionnalité de scans SNMP)
- apt-get -y install libcrypt-ssleay-perl libnet-snmp-perl libproc-pid-file-perl libproc-daemon-perl net-tools libsys-syslog-perl pciutils smartmontools read-edid nmap
- sudo cpan -i Module::Install

#### **Téléchargement de la tarball OCS Server :**

- git clone <https://github.com/OCSInventory-NG/UnixAgent.git>

#### **Décompression de la tarball dans ./ :**

- tar -xzf Ocsinventory-Unix-Agent-2.3.tar.gz
- cd Ocsinventory-Unix-Agent-2.3
- perl Makefile.PL
- make
- make install

#### **L'installation est détaillée à l'étape d'après :**

- Répertoire d'installation :
  - /etc/ocsinventory-agent
- Répertoire des logs :
  - /var/lib/ocsinventory-agent

```

fabien@debian-template:~/UnixAgent$ sudo make install
Manifesting 1 pod document
Manifesting 4 pod documents
Appending installation info to /usr/local/lib/x86_64-linux-gnu/perl/5.24.1/perllocal.pod
[ ! -f run-postinst ] || /usr/bin/perl postinst.pl
Do you want to configure the agent
Please enter 'y' or 'n'?> [y]
Where do you want to write the configuration file?
 0 -> /etc/ocsinventory
 1 -> /usr/local/etc/ocsinventory
 2 -> /etc/ocsinventory-agent
?> 2
Do you want to create the directory /etc/ocsinventory-agent?
Please enter 'y' or 'n'?> [y]
Should the old unix_agent settings be imported ?
Please enter 'y' or 'n'?> [y] n
[info] The config file will be written in /etc/ocsinventory-agent/ocsinventory-agent.cfg,
What is the address of your ocs server?> 192.168.10.1
Do you need credential for the server? (You probably don't)
Please enter 'y' or 'n'?> [n]
Do you want to apply an administrative tag on this machine
Please enter 'y' or 'n'?> [y]
tag?> linux-server
Do you want to install the cron task in /etc/cron.d
Please enter 'y' or 'n'?> [y]
Where do you want the agent to store its files? (You probably don't need to change it)?> [/var/lib/ocsinventory-agent]
Do you want to create the /var/lib/ocsinventory-agent directory?

Please enter 'y' or 'n'?> [y]
Should I remove the old unix_agent
Please enter 'y' or 'n'?> [n]
Do you want to activate debug configuration option ?
Please enter 'y' or 'n'?> [y]
Do you want to use OCS Inventory NG Unix Unified agent log file ?
Please enter 'y' or 'n'?> [y]
Specify log file path you want to use?> /var/log/ocsinventory-agent
Do you want disable SSL CA verification configuration option (not recommended) ?
Please enter 'y' or 'n'?> [n] y
Do you want to set CA certificate chain file path ?
Please enter 'y' or 'n'?> [y] n
Do you want to use OCS-Inventory software deployment feature?
Please enter 'y' or 'n'?> [y]
Do you want to use OCS-Inventory SNMP scans feature?
Please enter 'y' or 'n'?> [y]
Do you want to send an inventory of this machine?
Please enter 'y' or 'n'?> [y] n
Setting OCS Inventory NG server address...
Looking for OCS Inventory NG Unix Unified agent installation...
ocsinventory agent presents: /usr/local/bin/ocsinventory-agent
Setting crontab...
Creating /var/lib/ocsinventory-agent directory...
Creating /etc/ocsinventory-agent directory...
Writing OCS Inventory NG Unix Unified agent configuration
Creating /var/lib/ocsinventory-agent/http:192.168.10.1_ocsinventory directory...
Creating /var/lib/ocsinventory-agent/http:192.168.10.1_ocsinventory/snmp directory...
Copying SNMP MIBs XML files...
Activating modules if needed...
New settings written! Thank you for using OCS Inventory
fabien@debian-template:~/UnixAgent$ █

```

**Configuration de l'agent dans le fichier (dépend du répertoire d'installation) :**

- `sudo vim /etc/ocsinventory-agent/ocsinventory-agent.cfg`

```
tag=linux-server
server=http://192.168.75.80/ocsinventory
basevardir=/var/lib/ocsinventory-agent
logfile=/var/log/ocsinventory-agent
ssl=0
debug=1
```

### III. Déploiement du template

#### I. Configuration du fichier interface :

sudo vim /etc/network/interfaces

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug ens33
iface ens33 inet static
    address 192.168.10.1/24
    gateway 192.168.10.250
    dns-nameservers 192.168.10.230
    dns-search bora-bora.nc
```

Vérifier que l'adresse ip a bien été attribué apres le redemarrage avec :

➤ ip address show ou ifconfig

```
fabien@Srv-Ocs-Glpi-Gestioip:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:9e:73:3e brd ff:ff:ff:ff:ff:ff
    inet 192.168.75.80/24 brd 192.168.75.255 scope global ens33
        valid_lft forever preferred_lft forever
fabien@Srv-Ocs-Glpi-Gestioip:~$ _
```

#### II. Pour changer le nom de la machine :

sudo hostnamectl set-hostname Srv-Ocs-Glpi-Gestioip

sudo vim /etc/hosts

```
127.0.0.1    localhost
192.168.75.80 Srv-Ocs-Glpi-Gestioip

# The following lines are desirable for IPv6 capable hosts
::1        localhost ip6-localhost ip6-loopback
ff02::1    ip6-allnodes
ff02::2    ip6-allrouters
```

```
sudo apt install resolvconf
```

```
sudo vim /etc/resolv.conf
```

```
# Dynamic resolv.conf(5) file for glibc resolver(3) generated by resolvconf(8)
#     DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
nameserver 192.168.10.230
search bora-bora.nc
~
```

### III. Generer les clé ssh de l'hote :

```
rm /etc/ssh/ssh_host_*
```

```
ssh-keygen -A
```

```
fabien@cluster_parch_info_OGG_1:~$ sudo hostname
cluster_parch_info_OGG_1
fabien@cluster_parch_info_OGG_1:~$ sudo ssh-keygen -A
ssh-keygen: generating new host keys: RSA DSA ECDSA ED25519
fabien@cluster_parch_info_OGG_1:~$ ls /etc/ssh/
moduli      sshd_config.back      ssh_host_ecdsa_key      ssh_host_ed25519_key.pub
ssh_config  ssh_host_dsa_key      ssh_host_ecdsa_key.pub  ssh_host_rsa_key
sshd_config ssh_host_dsa_key.pub  ssh_host_ed25519_key    ssh_host_rsa_key.pub
fabien@cluster_parch_info_OGG_1:~$ _
```

### IV. Modifier les règles IP tables :

Règles IP table du serveur web ocs et glpi :

- iptables-save > /etc/iptables\_rules\_v4

```
# Generated by iptables-save v1.6.0 on Mon Nov 6 06:30:54 2017
*filter
:INPUT DROP [13:4399]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [4:452]
-A INPUT -i lo -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i ens33 -p tcp -m tcp --dport 47000 -j ACCEPT
-A INPUT -i ens33 -p tcp -m tcp --dport 80 -j ACCEPT
-A INPUT -i ens33 -p tcp -m tcp --dport 443 -j ACCEPT
-A INPUT -i ens33 -p udp -m udp --dport 161 -j ACCEPT
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
COMMIT
# Completed on Mon Nov 6 06:30:54 2017
~
```

```
fabien@Srv-Ocs-Glpi-Gestioip:~$ sudo iptables -L
Chain INPUT (policy DROP)
target    prot opt source                destination
ACCEPT    all  --  anywhere               anywhere
ACCEPT    icmp --  anywhere               anywhere
ACCEPT    tcp  --  anywhere               anywhere            tcp dpt:47000
ACCEPT    tcp  --  anywhere               anywhere            tcp dpt:http
ACCEPT    tcp  --  anywhere               anywhere            tcp dpt:https
ACCEPT    udp  --  anywhere               anywhere            udp dpt:snmp
ACCEPT    all  --  anywhere               anywhere            state RELATED,ESTABLISHED

Chain FORWARD (policy ACCEPT)
target    prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target    prot opt source                destination
fabien@Srv-Ocs-Glpi-Gestioip:~$
```

## IV. Annexes