

CUSTOMIZE



YOUR



CAR



PROJET
EVOLUTION





<https://www.cyc.com>

Table des matières

H- ANNEXES	2
H.1 Lettre de mission	2
H.2 Planning de formation à l'environnement de travail GNU/Linux	3
H.3 Normes d'installation de salle réseau	4
H.4 Détail technique du matériel	6
H.5 Modèles OSI et TCP/IP	7
H.6 Protocole LACP	7
H.7 Installation et configuration de ProxMox	8
H.8 Installation et configuration de Ceph	12
H.9 Configuration du chiffrement ZFS	14
H.10 Protocole SNMP	15
H.11 Structure d'un nom de domaine	15
H.12 Configuration des serveurs DNS	16
H.13 Intégration Linux à Active Directory	19
H.14 Script de création des utilisateurs dans le domaine	22
H.15 Script de sauvegarde PowerShell	23
H.16 Procédure d'installation de Linux Mint	24



H- Annexes

H.1 Lettre de mission



Service informatique

Membres de la société Customize Your Car

Le 05 mars 2019

Société : Customize Your Car

Exercice clos le : 21 novembre 2019

[Direction générale de l'entreprise]

Dans le cadre de votre mission en tant que membre du service informatique de la société, nous vous confirmons ci-après les dispositions relatives à votre mission pour l'exercice du 21 novembre 2019.

Nature et étendue de la mission

Votre mission comprend :

- Déploiement d'un système d'information faisant cohabiter des serveurs DHCP et DNS sous Windows et GNU/Linux
- Le système d'information doit garantir que les serveurs puissent se relayer en cas de problème sur l'un d'entre eux
- Le personnel de la société doit bénéficier d'un accès à un espace de partage sécurisé ainsi qu'à un espace de stockage personnel de 20 Go
- Une solution d'impression par le réseau doit être établie pour tous les services
- L'intégrité des données de la société doit être assurée
- La supervision des solutions matérielles proposées doit être établie de manière simple et accessible.

Votre plan devra nous être communiqué pour le 4 novembre 2019 au format .pdf, dans une archive signée de votre [nom].[prénom] au format zip. Tout contenu annexe sera à nous transmettre dans un fichier séparé.

Après étude de votre plan d'action par nos soins, nous attendons de votre service une présentation accompagnée d'une démonstration sur matériel de ce dernier. La réunion sera tenue dans nos locaux en date du 21 novembre 2019.

Sous réserve de validation de notre part, les travaux seront alors conduits sous votre supervision.

H.2 Planning de formation à l'environnement de travail GNU/Linux

Population à former	87 IDE
Moyens à disposition	2 salles 10 ordinateurs portables des services Custom et Old 2 responsables informatiques 2 référents des services Custom et Old
Stratégie de formation	<i>Demi-journée en groupe : introduction à l'outil système par les référents</i> <i>Durée – 30 minutes</i> <i>Demi-journée en groupe : introduction aux raccourcis système</i> <i>Durée – 30 minutes</i> <i>Demi-journée en groupe : introduction à la suite bureautique</i> <i>Durée – 1 heure</i> <i>Demi-journée en groupe : initiation pratique à l'utilisation</i> <i>Durée – 2 heures</i> <i>Journée en groupe : Bilan d'utilisation (Mois+1)</i> <i>Durée – 7 heures</i>
Supports utilisés	Un manuel utilisateur (Linux Mint + Libre Office + Discord) Un support de formation à l'outil (Impress) Un support de formation pour référent (Impress + pdf) Référents expérimentés des services Custom et Old



H.3 Normes d'installation de salle réseau

Chaque salle réseau se déploie selon un nombre défini de normes en constante évolution. Afin de nous assurer que l'installation de la société dans les nouveaux locaux soit réalisée de manière règlementaire, nous avons observé les normes TIA/EIA qui ont défini les éléments suivants :

- Les dimensions des locaux techniques ;
- Le câblage horizontal ;
- Le backbone ;
- Le raccordement des postes de travail ;
- Les armoires de câblage ;
- Les salles de matériel et de terminaux ;
- Les installations d'entrée.
- En vertu de cette norme TIA/EIA-569, il est stipulé que pour toute structure à étages doit inclure un local technique par étage et qu'un local technique doit être installé tous les 1000m², lorsque la surface de l'étage desservi est supérieure à 1000m² ou que la distance du câblage horizontal est supérieure à 90 mètres.

De plus, pour une surface de 1000m², le local technique doit respecter une dimension de 3m par 3,4m au minimum, soit 10,2m² minimum.

En dehors des restrictions relatives aux surfaces, la pièce choisie pour l'installation d'un local technique doit être conforme aux règles applicables aux éléments qui suivent :

- Matériaux des murs, du sol et des plafonds ;
- Température et humidité ;
- Emplacement des appareils d'éclairage et leur type ;
- Prises de courant ;
- L'accès au local et à l'équipement ;
- L'accès aux câbles et leur support.

En premier lieu, le sol d'un local technique doit pouvoir supporter une charge de 4,8kPA. S'il s'agit d'un répartiteur intermédiaire, la charge minimale à supporter est réduite à 2,4kPA.

De plus, le local doit être doté d'un plancher technique qui servira à loger tous les câbles horizontaux provenant des zones de travail.

Dans le cas où cela ne serait pas possible, la pièce doit être carrelée et pourvue d'un bâti en échelle de 30,5 cm, installé de sorte à pouvoir supporter tous les équipements et câbles prévus dans l'installation du réseau. Ce dispositif permet de prévenir et contrôler la présence de poussière et de protéger les équipements contre l'électricité statique.

Par ailleurs, au moins deux des murs de la pièce doivent être habillés avec des panneaux de contreplaqué d'une épaisseur de 1,9 cm et d'une hauteur minimale de 2,4 m.

Concernant le répartiteur principal, ce dernier peut inclure le Point de Présence du site. Si tel est le cas, toutes les parois du local doivent être recouvertes de panneaux en contreplaqué de 1,9cm d'épaisseur avec un espace minimal de 4,6m d'espace au mur dédié aux terminaisons et équipements connexes.



Enfin, les matériaux employés doivent être conformes à toutes les réglementations applicables à la construction d'un local technique incluant le revêtement ignifuge du contreplaqué, les peintures ignifuges sur les parois externes, l'absence de faux plafond ou plafond suspendu pour éviter les accès non autorisés...

Le local technique doit maintenir une température ambiante de 21°C environ lorsque les équipements réseau sont en fonctionnement. Aucune canalisation d'eau ne doit passer au-dessus ou à l'intérieur du local, exception-faite de gicleurs dans des cas particuliers.

L'humidité du local doit être comprise entre 30% et 50%. Ainsi, les fils de cuivre des câbles à paires torsadées ne peuvent être détériorés par la corrosion au détriment de la qualité du réseau.

Pour un local technique, on doit respecter la présence d'au moins deux prises de courant alternatif duplex, non commutées et dédiées, raccordées sur des circuits séparés. Ces dernières doivent se situer à 1,8m l'une de l'autre, le long des murs du local et à une distance de 15cm au-dessus du sol.

De plus, un interrupteur gérant l'éclairage principal du local doit être fixé au mur à l'intérieur du local à proximité immédiate de la porte d'accès au local.

Ce même éclairage doit être installé à 2,6m minimum au-dessus du sol et être équivalent à 500lux minimum. Il est par ailleurs recommandé d'éviter les éclairages fluorescents à proximité des câbles car ils peuvent produire des interférences externes ; ils sont cependant tolérés s'ils ne portent pas atteinte à l'intégrité du réseau.

La porte du local technique doit faire au moins 90 cm de largeur et s'ouvrir vers l'extérieur du local afin de permettre aux personnes de sortir facilement de ce dernier. De plus, le verrou doit se situer sur l'extérieur de la porte et toute personne se situant à l'intérieur du local doit pouvoir en sortir à tout moment.

La norme TIA/EIA-569 prévoit aussi l'encadrement du câblage d'un local technique. Celle-ci stipule que tous les câbles partant du local vers les points intermédiaires doivent être protégés par un mandrin gainé ou un conduit de 10,2cm de diamètre. La longueur de ce conduit dépend alors du nombre de câbles du local technique.

Il est par ailleurs recommandé de prévoir des longueurs de conduit supplémentaires afin d'anticiper la croissance de l'installation en présence. Dans ce cadre, deux mandrins ou conduits supplémentaires doivent être réservés dans chaque local technique. Ces derniers doivent être placés à une distance de 15,2cm du mur.

Tous les câbles reliant les zones de travail au local technique doivent passer dans des mandrins de 10,2cm situés au-dessus de la porte du local lorsqu'il n'existe pas de plancher technique. Pour en garantir un support solide, les câbles doivent circuler du mandrin à un bâti en échelle de 30,5cm à l'intérieur du local, installé en fonction de la configuration et la disposition des équipements.

Enfin, toute ouverture dans les murs ou le plafond permettant au conduit ou au mandrin d'accéder au local doit être scellée avec un matériau ignifuge aux normes en vigueur.



H.4 Détail technique du matériel

Veuillez trouver les liens de la [documentation technique et utilisateur](#) des différents composants matériels de notre réseau :

Produit	Guides et manuels
Commutateur HPe ProCurve 3500yl PoE+	➤ Consulter
Commutateur HPe ProCurve 2530 PoE+	➤ Consulter
Routeur HPe FlexNetwork MSR958 PoE+	➤ Consulter
Point d'accès sans fil HPe Aruba AP-303H	➤ Consulter
Serveur HPe Proliant DL380 G7	➤ Consulter
Lecteur de bande HPe LTO-5 Ultrium 3000	➤ Consulter
Kit Console KVM LCD8500	➤ Consulter
Baies HPe 12-22U	➤ Consulter
iLo 3 Advanced	➤ Consulter

Certificate of Partnership FY19

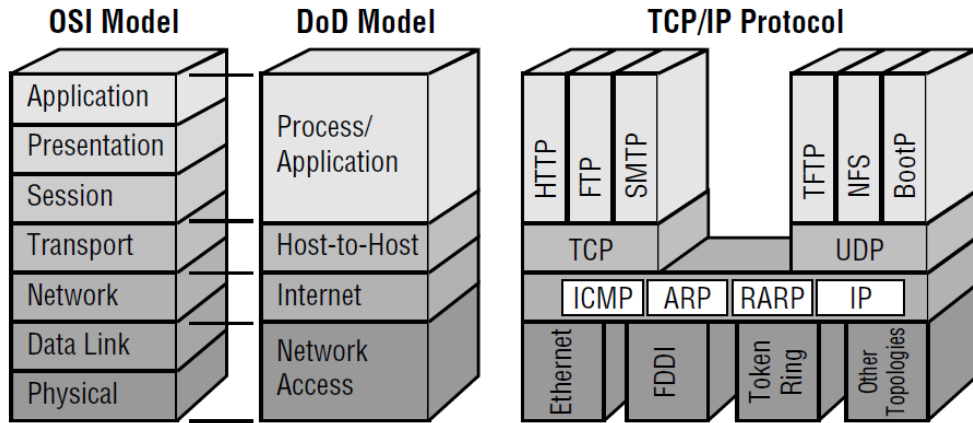


Nos tarifs d'acquisition ont été obtenus par le biais d'achats du matériel auprès des marchands spécialistes en matériel informatique professionnel reconditionné :

- Professionnels répertoriés sur [eBay](#)
- Professionnels répertoriés sur [LeBonCoin](#)
- Professionnels de [Bargain Hardware](#)
- Professionnels de [ServerParts4Less](#)
- Professionnels de [ServerMonkey](#)
- Professionnels de [DiscountElectronics](#)



H.5 Modèles OSI et TCP/IP



H.6 Protocole LACP

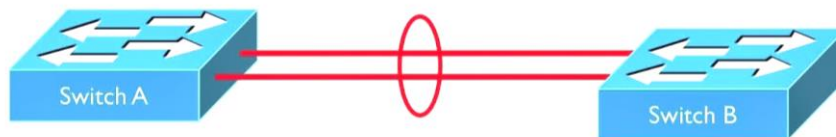
Le protocole d'agrégation de lien peut s'appliquer sur les couches 1 à 3 du modèle OSI.

Dans notre cas, nous intervenons au niveau 2 du modèle OSI en employant plusieurs raccords câblés sur des ports de mêmes commutateurs, routeurs et serveurs. A partir de ce point, nous créons depuis les ports physiques occupés, un seul et unique port virtuel sur les deux éléments du réseau concernés par l'application du protocole.

La mise en place de ce protocole n'est possible que si le même nombre de connexions sont établies d'un côté et de l'autre.

Un tel protocole ouvre alors la voie à un déploiement avancé d'un protocole intervenant en couche 4 du modèle OSI : le load-balancing.

LACP Port Negotiation



LACP Channel Mode	On	Passive	Active
On	✓	✗	✗
Passive	✗	✗	✓
Active	✗	✓	✓

H.7 Installation et configuration de Proxmox

ETAPE 1

Nous démarrons les hyperviseurs à partir d'une clé USB bootable contenant le système d'hypervision Proxmox.

Une fois l'initialisation serveur terminée, nous arrivons en présence de l'écran illustré à droite.

Choisir : Install Proxmox VE

Proxmox VE 5.4 (iso release 1) - <http://www.proxmox.com/>



Welcome to Proxmox Virtual Environment

Install Proxmox VE

Install Proxmox VE (Debug mode)

Rescue Boot

Test memory

ETAPE 2

Nous sommes invités à accepter les conditions générales d'utilisation de la solution d'hypervision.

Cliquer sur "I agree" pour accéder aux étapes suivantes de déploiement.



Proxmox VE Installer

END USER LICENSE AGREEMENT (EULA)

4. Intellectual Property Rights. The Programs and each components are owned by Proxmox and other licensors and are protected under copyright law and under other laws as applicable. The "Proxmox" trademark and the Proxmox company logo are registered trademarks of Proxmox in Austria and other countries. This EULA does not permit you to distribute the Programs or their components using Proxmox's trademarks, regardless of whether the copy has been modified. Title to the Programs and any component, or to any copy, modification, or merged portion shall remain with Proxmox and other licensors, subject to the applicable license.

5. Third Party Software. Proxmox may distribute third party software with the Programs. These third party programs are provided as a convenience to you, and are subject to their own license terms. If you do not agree to the applicable license terms for the third party software programs, then you may not install them.

6. Export Regulation. You warrant that you understand that the Programs and their components may be subject to export controls under the Austrian Export Administration Regulations.

7. Other terms. If any provision of this EULA is held to be unenforceable, the enforceability of the remaining provisions shall not be affected. Any claim, controversy or dispute arising under or relating to this EULA shall be governed by the laws of Austria (Europe), without regard to any conflict of laws provisions.

Copyright © 2013-2019 Proxmox Server Solutions GmbH. All rights reserved. "Proxmox" and the Proxmox logo are registered trademarks of Proxmox Server Solutions GmbH. "Linux" is a registered trademark of Linus Torvalds. All other trademarks are the property of their respective owners.

Abort

Previous

I agree

ETAPE 3

Nous accédons alors à l'interface de sélection du disque d'installation du système d'hypervision.

Nos disques SSD étant montés en lecteurs n°1 à 4 de la baie, sélectionner le lecteur disque : /dev/sda de 240 Go.

Target Harddisk: /dev/sda (120GB, VMware Virtual I)

Options

Previous

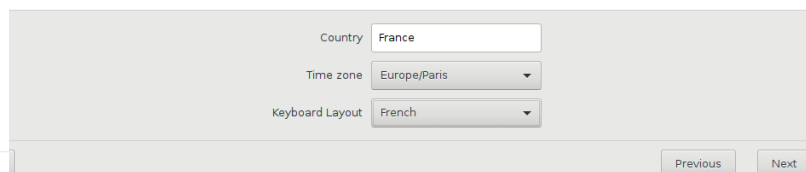
Next

ETAPE 4

Après confirmation, nous sommes invités à renseigner les informations relatives à l'implantation géographique de l'hyperviseur.

Dans notre cas, nous renseignons le pays France, la zone horaire Europe/Paris et l'interface clavier French.

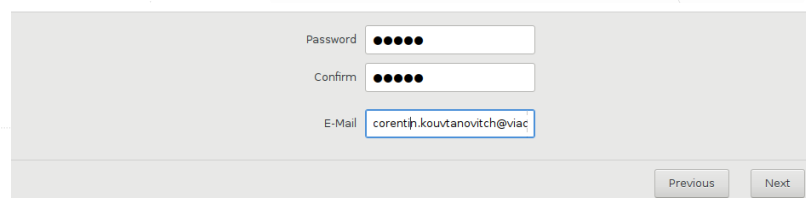
Pour éviter tout problème ultérieur, merci de bien vous assurer que l'interface native de votre clavier correspond à votre saisie.



ETAPE 5

Une fois les paramètres précédents confirmés, nous saisissons le mot de passe Administrateur du système d'hypervision (il peut être différent de celui de la machine d'hypervision).

De plus, une adresse mail doit être renseignée afin que l'administrateur système puisse bénéficier d'alertes directement sur sa boîte de messagerie.



ETAPE 6

Enfin, nous attribuons un FQDN à notre hyperviseur. Dans notre cas, nous renseignons SRVPM[1,2 ou 3].cyc.local

L'adresse IP associée au FQDN doit alors être renseignée : 172.16.0.249, 172.16.0.247 ou 172.16.0.245.

Le masque de sous-réseau est alors à saisir. Pour notre société, ce dernier est le suivant : 255.255.0.0

La passerelle à saisir va ici est l'adresse de notre routeur HSRP : 172.16.0.254.

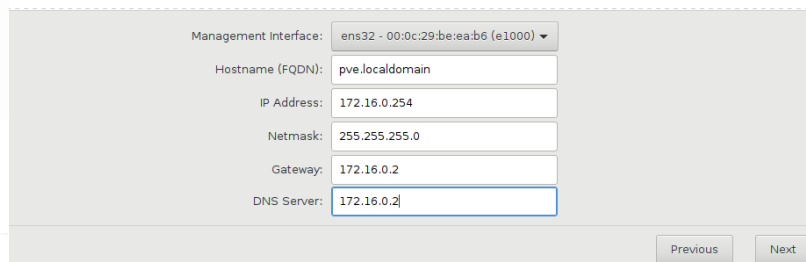
Afin de pouvoir procéder aux installations complémentaires et aux patches de mise à jour, nous renseignons temporairement la même adresse en guise de serveur DNS

Management Network Configuration

Please verify the displayed network configuration. You will need a valid network configuration to access the management interface after installation.

Afterwards press the Next button. You will be shown a list of the options that you chose during the previous steps.

- **IP address:** Set the IP address for your server.
- **Netmask:** Set the netmask of your network.
- **Gateway:** IP address of your gateway or firewall.
- **DNS Server:** IP address of your DNS server.



ETAPE 7

Un écran récapitulatif des paramètres renseignés nous est alors présenté avant de déployer le système d'hypervision sur les serveurs d'hypervision.

Merci de bien relire les informations saisies avant toute confirmation.

Passée cette étape, le processus d'installation devient irréversible.

Summary

Please verify the displayed informations. Afterwards press the **Install** button. The installer will begin to partition your drive and extract the required files.

Option	Value
Filesystem:	ext4
Disk(s):	/dev/sda
Country:	France
Timezone:	Europe/Paris
Keymap:	en-us
E-Mail:	corentin.kouvtanovitch@viacesi.fr
Management Interface:	ens32
Hostname:	pve
IP:	172.16.0.254
Netmask:	255.255.255.0
Gateway:	172.16.0.2
DNS:	172.16.0.2

Previous

Install

ETAPE 8

Une fois l'installation achevée, le serveur d'hypervision procède à un redémarrage.

Merci de bien veiller à retirer la clé USB bootable ayant servi au déploiement.

Une fois le reboot serveur achevé, une interface CLI (Command Line Interface) s'affiche à l'écran.

A ce stade, le serveur d'hypervision devient disponible en GUI par le biais d'un navigateur web d'un poste du réseau en saisissant son adresse en https dans la barre d'adresse, suivi du numéro de port d'accès.
(Exemple <https://172.16.0.249:8006>)

Type	Description	Utilisation ...	Uti
node	pve	5.1 %	20
storage	local (pve)	5.1 %	
storage	local-lvm (pve)	0.0 %	

Heure de début	Heure de fin	Nœud	Utilisateur	De...	Statut
Mai 15 11:21:55	Mai 15 11:21:55	pve	root@pam	Dé...	OK
Mai 15 09:38:58	Mai 15 09:38:58	pve	root@pam	Dé...	OK

ETAPE 9

Une fois nos 3 serveurs d'hypervision déployés (Ou plus à l'avenir), nous sommes amenés à les intégrer dans un cluster afin que ces derniers communiquent comme s'ils étaient un seul et même serveur d'hypervision sur notre site.

Pour cela, nous pouvons utiliser l'interface GUI à distance ou saisir les lignes de commande suivantes :

```
pvecm add 172.16.2.249
```

Une confirmation de la connexion au serveur portant cette adresse IP est demandée. Confirmer afin de joindre le serveur d'hypervision distant. Le cluster est créé.

```
root@srvpm2:~# pvecm add 172.16.0.254
Please enter superuser (root) password for '172.16.0.254':
Password for root@172.16.0.254: *****
Establishing API connection with host '172.16.0.254'
The authenticity of host '172.16.0.254' can't be established.
RSA256 key fingerprint is 42:38:E9:41:55:1B:1D:02:3F:a8:29:4A:53:E2:AC:92:25:CD:BC:04:87:4C:9B:12:29:BB:BC:5B:50:7A:1C.
Are you sure you want to continue connecting (yes/no)? yes
Login succeeded.
Request addition of this node
Join request OK, finishing setup locally
Stopping pve-cluster service
Backup old database to '/var/lib/pve-cluster/backup/config-1565788837.sql.gz'
Waiting for quorum...OK
(regenerate node files
Generate new node certificate
Merge authorized SSH keys and known hosts
Generated new node certificate, restart pveproxy and pvedemon services
Successfully added node 'srvpm2' to cluster.
root@srvpm2:~#
```

ETAPE 10

Afin de connaître le statut d'intégration des serveurs d'hypervision au cluster, la commande suivante peut être saisie dans l'interface CLI :

```
pvecm status
```

Le poids du nœud du cluster vous sera alors communiqué à l'écran ainsi que les références des autres nœuds du cluster, leur poids et leur adresse IP sur le réseau.

```
root@srvpm1:~# pvecm status
Quorum information
-----
Date:                Wed Aug 14 15:50:35 2019
Quorum provider:     corosync_votequorum
Nodes:               3
Node ID:              0x00000001
Ring ID:              1/28
Quorate:              Yes

Votequorum information
-----
Expected votes:       3
Highest expected:     3
Total votes:          3
Quorum:               2
Flags:                Quorate

Membership information
-----
Nodeid      Votes Name
0x00000001   1 172.16.0.254 (local)
0x00000002   1 172.16.0.253
0x00000003   1 172.16.0.252
root@srvpm1:~#
```

ETAPE 11

Saisir en CLI la commande pour ne plus être notifié de la souscription :

Echo "deb
<http://download.proxmox.com/debian/pve-stretch-pve-no-subscription>" > /etc/apt/sources.list

```
root@SRVPM3:~# echo "deb http://download.proxmox.com/debian/
pve stretch pve-no-subscription" > /etc/apt/sources.list
root@SRVPM3:~#
```

H.8 Installation et configuration de Ceph

ETAPE 1

Afin de déployer le service Ceph sur nos serveur d'hypervision, nous saisissons la commande suivante sous l'interface CLI :

```
apt install ceph-common
```

A partir de l'interface GUI, il est possible de procéder au déploiement du service Ceph sur la totalité des serveurs d'hypervision intégrés au cluster. Pour cela, il nous suffit de cliquer sur "Installer Ceph" dans l'onglet Ceph du menu de gestion du cluster.

```
root@shv:~# apt install ceph-common
Reading package lists... Done
Building dependency tree
Reading state information... Done
ceph-common is already the newest version (12.2.11+dfsg1-2.1).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@shv:~#
```

ETAPE 2

Après avoir procédé à l'installation des packages Ceph et leur mise à jour, nous créons alors les moniteurs et managers Ceph sur les hyperviseurs à l'aide des commandes suivantes :

```
pveceph createmon
```

```
pveceph createmgr
```

```
root@SRVPM2:~# pveceph createmon
Created symlink /etc/systemd/system/ceph-mon.target.wants/ceph-mon@SRVPM2.service -> /lib/systemd/system/ceph-mon@.service.
root@SRVPM2:~# pveceph createmgr
creating manager directory '/var/lib/ceph/mgr/ceph-SRVPM2'
creating keys for 'mgr.SRVPM2'
setting owner for directory
enabling service 'ceph-mgr@SRVPM2.service'
Created symlink /etc/systemd/system/ceph-mgr.target.wants/ceph-mgr@SRVPM2.service -> /lib/systemd/system/ceph-mgr@.service.
starting service 'ceph-mgr@SRVPM2.service'
root@SRVPM2:~#
```

ETAPE 3

Une fois les dispositifs de management et de supervision Ceph établis, nous nous assurons que tous les disques des hyperviseurs que nous voulons allouer à nos espaces de stockage soient au bon format.

Pour cela nous entrons dans la console la commande :

```
ceph-volume lvm zap /dev/sd[lettre du disque] -destroy
```

Cela efface tout contenu éventuel en présence sur le disque et le remet au bon format pour utilisation.

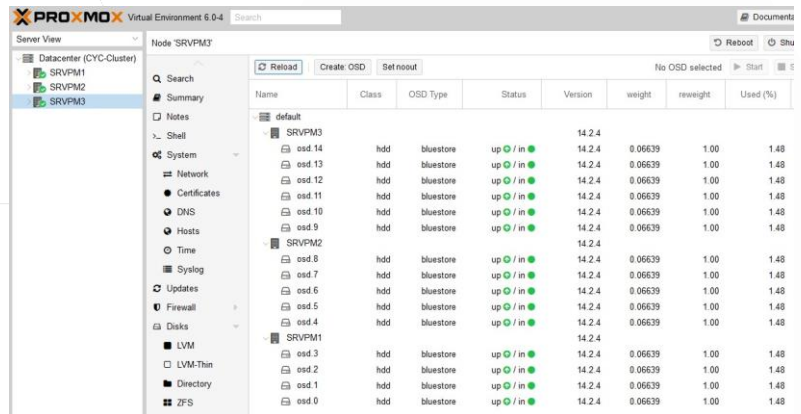
```
root@SRVPM1:~# ceph-volume lvm zap /dev/sdb --destroy
--> Zapping: /dev/sdb
Running command: /usr/sbin/wipefs --all /dev/sdb2
stdout: /dev/sdb2: 8 bytes were erased at offset 0x00000003 (ntfs): 4e 54 46 53 20 20 20 20
Running command: /bin/dd if=/dev/zero of=/dev/sdb2 bs=1M count=10
stderr: 10+0 records in
10+0 records out
10485760 bytes (10 MB, 10 MiB) copied, 0.00535657 s, 2.0 GB/s
--> Destroying partition since --destroy was used: /dev/sdb2
Running command: /usr/sbin/parted /dev/sdb --script -- rm 2
Running command: /usr/sbin/wipefs --all /dev/sdb1
stdout: /dev/sdb1: 8 bytes were erased at offset 0x00000003 (ntfs): 4e 54 46 53 20 20 20 20
stderr: 10+0 records in
10+0 records out
10485760 bytes (10 MB, 10 MiB) copied, 0.00568864 s, 1.8 GB/s
--> Destroying partition since --destroy was used: /dev/sdb1
Running command: /usr/sbin/parted /dev/sdb --script -- rm 1
Running command: /usr/sbin/wipefs --all /dev/sdb
stdout: /dev/sdb: 2 bytes were erased at offset 0x000001fe (dos): 55 aa
Running command: /bin/dd if=/dev/zero of=/dev/sdb bs=1M count=10
stderr: 10+0 records in
10+0 records out
10485760 bytes (10 MB, 10 MiB) copied, 0.00537982 s, 1.9 GB/s
--> Zapping successful for: <Raw Device: /dev/sdb>
```

ETAPE 4

Après avoir nettoyé nos disques, nous nous rendons dans l'espace OSD de Ceph (Menu latéral gauche) et cliquons sur "Create OSD" en haut de page.

Nous allouons alors un disque à chaque OSD du fait que nous ayons opté pour du matériel reconditionné. En cas de défaillance d'un disque, nous ne perdrons ainsi pas de groupement OSD. Le rétablissement des OSD en sera plus aisé.

Il est à noter que cette étape du déploiement est plus simple et rapide à effectuer depuis le GUI contrairement aux manipulations précédentes.

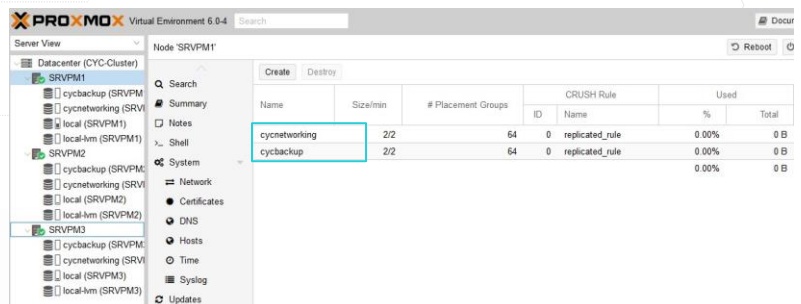


ETAPE 5

Enfin, nous créons nos deux pools de stockages, l'une destinée au stockage réseau de nos collaborateurs (cycnetworking) et l'autre à destination de nos sauvegardes en interne (cycbackup).

```
pveceph createpool [nom du pool]
```

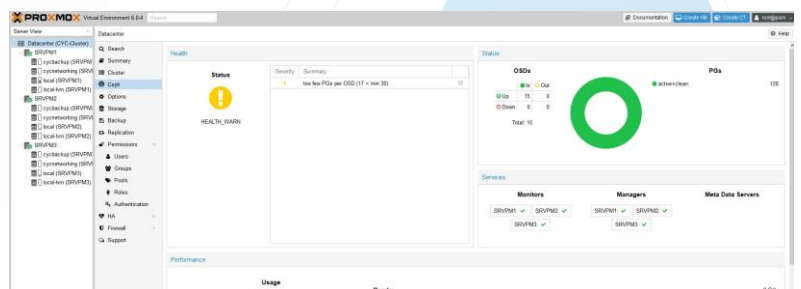
Nous allouons une taille de répartition de 3 (osd) pour un minimum de 2 en fonction. Cela garantit la continuité de nos données en cas de défaillance sur le réseau.



ETAPE 6

Nous pouvons alors vérifier l'état de nos pools depuis le cœur du cluster, en cliquant sur l'onglet Ceph.

Dans notre exemple à droite, la capacité des disques étant limitée, nous avons restreint le nombre de secteurs de vérification, ce qui nous renvoie une alerte de sécurité.

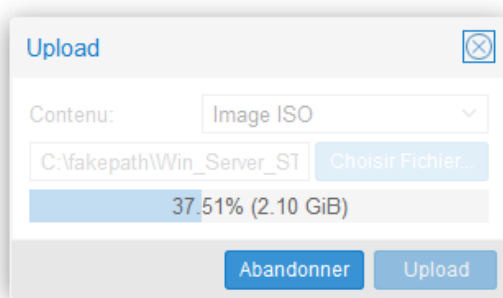


ETAPE 7

Une fois nos deux pools définies et déployées, nous initions le chargement des fichiers .iso d'installation des systèmes d'exploitation sur l'espace de stockage des serveurs d'hypervision.

Ces fichiers sont au nombre de trois :

- L'iso du système Windows Server 2019
- L'iso du système GNU/Linux PFSense
- L'iso du système GNU/Linux Linux Mint



H.9 Configuration du chiffrement ZFS

Le chiffrement ZFS est un système de chiffrement combinant un système de fichiers et un gestionnaire de volumes logiques. Grâce à ce dernier, il est possible d'augmenter le système de cache des disques SSD à faible coût de performance et d'y appliquer une gestion RAID.

Le nombre de disques présents dans notre maquette ne nous a pas permis de le mettre en place définitivement, mais les tests de faisabilité ont été effectués lors d'une installation précédente des hyperviseurs.

Ayant 4 disques SSD sur chacun de nos hyperviseurs, nous déployons le chiffrement ZFS sur ces derniers, en leur appliquant un niveau RAID10. La réplication liée à l'association de nos 3 hyperviseurs dans un cluster fait que nous bénéficierons alors de 3 volumes de 240 Go qui hébergeront notre système d'hypervision ainsi que nos serveurs virtuels (Windows serveur et PFSense).

Afin de paramétrer ce système de fichiers, la démarche est similaire à celle de pools sous Ceph. Tout d'abord, nous créons notre pool en y renseignant les quatre disques destinés à l'utilisation :

```
zpool create -f -o ashift=12 cycsystem mirror /dev/sda /dev/sdb mirror /dev/sdc /dev/sdb
```

Après cela, nous activons la compression au sein du pool créé :

```
zfs set compression=lz4 cycsystem
```

Enfin, nous déployons le daemon ZFS qui nous permet d'être averti par mail en cas d'évènement alarmant sur notre pool.

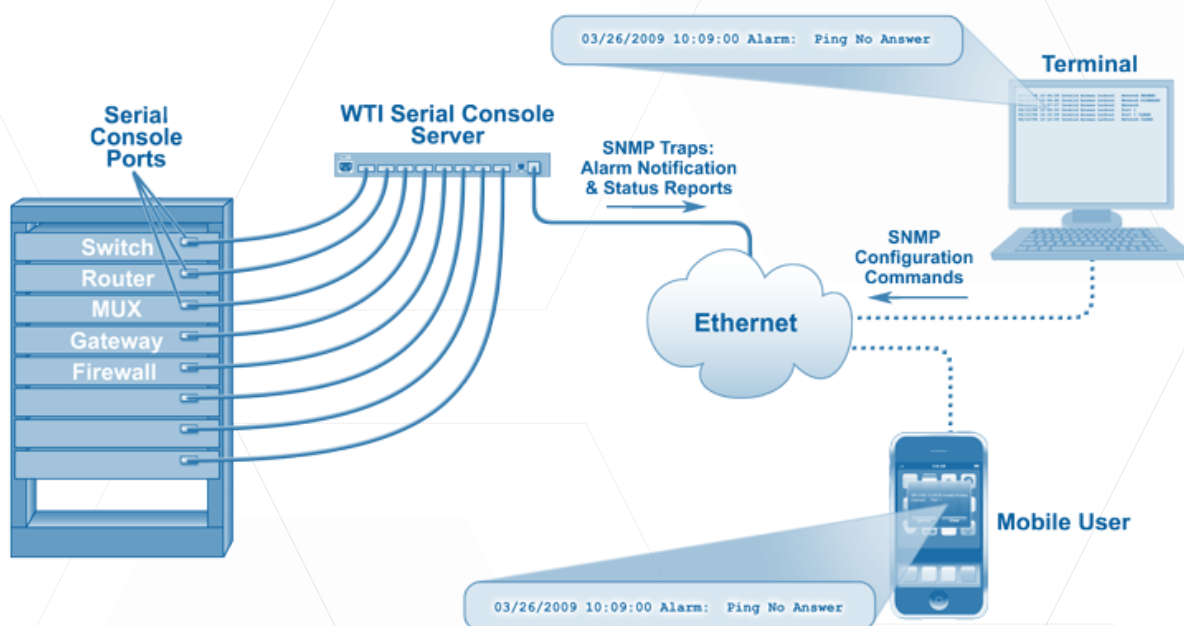
```
apt-get install zfs-zed
nano /etc//zfs/zed.d/zed.rc
ZED_MAIL_ADDR=''root''
```


H.10 Protocole SNMP

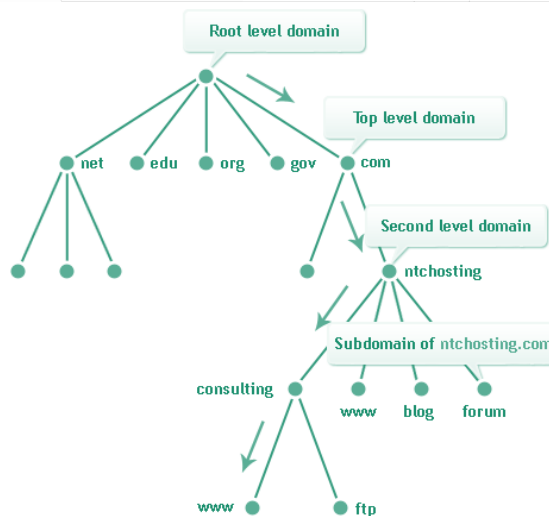
Le SNMP (Simple Network Management Protocol) consiste en un protocole de communication avec les équipements réseau ouvrant à la gestion des équipements de ce dernier et plus particulièrement, sa supervision (Veille et diagnostic ou prévention des problèmes réseaux et matériels à distance).

L'architecture de gestion offerte par SNMP se décompose en trois éléments :

- Equipements gérés du réseau (Commutateurs, routeurs, serveurs...)
- Agents que sont les applications de gestion de réseau internes au périphériques (Ces dernières transmettent alors les données locales au format SNMP)
- Système de gestion de réseau (NMS) que sont les consoles d'administration (KVM ou console distante).



H.11 Structure d'un nom de domaine



H.12 Configuration des serveurs DNS

```
<?xml version="1.0"?>
<pfsense>
  <version>19.1</version>
  <lastchange></lastchange>
  <system>
    <optimization>normal</optimization>
    <hostname>SRVPF</hostname>
    <domain>cyc.local</domain>
    <dnsserver></dnsserver>
    <dnsallowoverride></dnsallowoverride>
    <group>
      <name>all</name>
      <description><![CDATA[All Users]]></description>
      <scope>system</scope>
      <gid>1998</gid>
    </group>
    <group>
      <name>admins</name>
      <description><![CDATA[System Administrators]]></description>
      <scope>system</scope>
      <gid>1999</gid>
      <member>0</member>
      <priv>page-all</priv>
    </group>
  </system>
  <user>[Série de caractères masquée pour le rapport]</user>
  <nextuid>2000</nextuid>
  <nextgid>2000</nextgid>
  <timeservers>0.pfsense.pool.ntp.org</timeservers>
  <webgui>
    <protocol>http</protocol>
    <loginautocomplete></loginautocomplete>
    <ssl-certref>5db95964d29db</ssl-certref>
  </webgui>
  <disablenatreflection>yes</disablenatreflection>
  <disablesegmentationoffloading></disablesegmentationoffloading>
  <disablelargereceiveoffloading></disablelargereceiveoffloading>
  <ipv6allow></ipv6allow>
  <maximumtableentries>400000</maximumtableentries>
  <powerd_ac_mode>hadp</powerd_ac_mode>
  <powerd_battery_mode>hadp</powerd_battery_mode>
  <powerd_normal_mode>hadp</powerd_normal_mode>
  <bogons>
    <interval>monthly</interval>
  </bogons>
  <already_run_config_upgrade></already_run_config_upgrade>
</system>
<interfaces>
  <wan>
    <enable></enable>
    <if>em0</if>
    <mtu></mtu>
    <ipaddr>dhcp</ipaddr>
    <ipaddrv6></ipaddrv6>
    <subnet></subnet>
    <gateway></gateway>
    <blockpriv></blockpriv>
    <blockbogons></blockbogons>
    <dhcphostname></dhcphostname>
    <media></media>
    <mediaopt></mediaopt>
    <dhcp6-duid></dhcp6-duid>
    <dhcp6-ia-pd-len>0</dhcp6-ia-pd-len>
    <subnetv6></subnetv6>
    <gatewayv6></gatewayv6>
  </wan>
  <lan>
    <enable></enable>
    <if>em1</if>
    <ipaddr>172.16.0.100</ipaddr>
```

```

    <subnet>16</subnet>
    <ipaddrv6></ipaddrv6>
    <subnetv6></subnetv6>
    <media></media>
    <mediaopt></mediaopt>
    <track6-interface>wan</track6-interface>
    <track6-prefix-id>0</track6-prefix-id>
    <gateway></gateway>
    <gatewayv6></gatewayv6>
  </lan>
</interfaces>
<staticroutes></staticroutes>
<dhcpd>
  <lan>
    <enable></enable>
    <range>
      <from>172.16.1.10</from>
      <to>172.16.1.254</to>
    </range>
    <failover_peerip></failover_peerip>
    <dhcpleaseinlocaltime></dhcpleaseinlocaltime>
    <defaultleasetime></defaultleasetime>
    <maxleasetime></maxleasetime>
    <netmask></netmask>
    <gateway>172.16.0.100</gateway>
    <domain>cyc.local</domain>
    <domainsearchlist></domainsearchlist>
    <ddnsdomain></ddnsdomain>
    <ddnsdomainprimary></ddnsdomainprimary>
    <ddnsdomainkeyname></ddnsdomainkeyname>
    <ddnsdomainkeyalgorithm>hmac-md5</ddnsdomainkeyalgorithm>
    <ddnsdomainkey></ddnsdomainkey>
    <mac_allow></mac_allow>
    <mac_deny></mac_deny>
    <ddnsclientupdates>allow</ddnsclientupdates>
    <tftp></tftp>
    <ldap></ldap>
    <nextserver></nextserver>
    <filename></filename>
    <filename32></filename32>
    <filename64></filename64>
    <rootpath></rootpath>
    <numberoptions></numberoptions>
    <dnsserver>172.16.0.100</dnsserver>
    <dnsserver>172.16.0.102</dnsserver>
  </lan>
</dhcpd>

```

```

<dhcpdv6>[Série de caractères masquée pour le rapport]</dhcpdv6>
<srmpd>[Série de caractères masquée pour le rapport]</srmpd>
<diag>[Série de caractères masquée pour le rapport]</diag>
<syslog>[Série de caractères masquée pour le rapport]</syslog>
<nat>[Série de caractères masquée pour le rapport]</nat>
<filter>[Série de caractères masquée pour le rapport]</filter>

```

```

<shaper></shaper>
<ipsec></ipsec>
<aliases></aliases>
<proxyarp></proxyarp>
<cron>
  <item>
    <minute>1,31</minute>
    <hour>0-5</hour>
    <mday>*</mday>
    <month>*</month>
    <wday>*</wday>
    <who>root</who>
    <command>/usr/bin/nice -n20 adjkerntz -a</command>
  </item>
  <item>
    <minute>1</minute>
    <hour>3</hour>
    <mday>1</mday>
    <month>*</month>
    <wday>*</wday>
    <who>root</who>
    <command>/usr/bin/nice -n20 /etc/rc.update_bogons.sh</command>
  </item>
</cron>

```

```

</item>
  <item>
    <minute>1</minute>
    <hour>1</hour>
    <mday>*</mday>
    <month>*</month>
    <wday>*</wday>
    <who>root</who>
    <command>/usr/bin/nice -n20 /etc/rc.dyndns.update</command>
  </item>
  <item>
    <minute>*/60</minute>
    <hour>*</hour>
    <mday>*</mday>
    <month>*</month>
    <wday>*</wday>
    <who>root</who>
    <command>/usr/bin/nice -n20 /usr/local/sbin/expiretable -v -t 3600 virusprot</command>
  </item>
  <item>
    <minute>30</minute>
    <hour>12</hour>
    <mday>*</mday>
    <month>*</month>
    <wday>*</wday>
    <who>root</who>
    <command>/usr/bin/nice -n20 /etc/rc.update_urltables</command>
  </item>
  <item>
    <minute>1</minute>
    <hour>0</hour>
    <mday>*</mday>
    <month>*</month>
    <wday>*</wday>
    <who>root</who>
    <command>/usr/bin/nice -n20 /etc/rc.update pkg metadata</command>
  </item>
</cron>
<wol></wol>
<rrd>
  <enable></enable>
</rrd>

<load_balancer>[Série de caractères masquée pour le rapport]</load_balancer>
<widgets>[Série de caractères masquée pour le rapport]</widgets>

<openvpn></openvpn>
<dnshaper></dnshaper>

<unbound>[Série de caractères masquée pour le rapport]</unbound>
<revision>[Série de caractères masquée pour le rapport]</revision>

<cert>
  <refid>5db95964d29db</refid>
  <descr><![CDATA[webConfigurator default (5db95964d29db)]]></descr>
  <type>server</type>

  <crt>[Série de caractères masquée pour le rapport]</crt>
  <prv>[Série de caractères masquée pour le rapport]</prv>

</cert>
<gateways>
  <gateway_item>
    <interface>lan</interface>
    <gateway>172.16.0.254</gateway>
    <name>LAN</name>
    <weight>1</weight>
    <ipprotocol>inet</ipprotocol>
    <descr></descr>
  </gateway_item>
</gateways>
<dnsmasq>
  <custom_options></custom_options>
  <interface></interface>
</dnsmasq>
</pfsense>

```

H.13 Intégration Linux à Active Directory

En premier lieu, il faut procéder à l'intégration des machines Linux au domaine Active Directory via Samba4 en suivant les étapes et conseils de la documentation officielle [Samba](#) (Cette dernière se base sur une distribution Debian Jessie) :

En premier lieu, nous installons les packages nécessaires au couplage de nos services :

```
Export DEBIAN_FRONTEND=noninteractive
Apt-get install samba winbind krb5-user
Unset DEBIAN_FRONTEND
```

Une fois les packages installés, nous procédons alors à la modification du fichier `/etc/krb5.conf` afin de lui faire écouter notre domaine :

```
[libdefaults]
dns_lookup_realm = true
dns_lookup_kdc = true
default_realm = TRANQUILIT.LAN
```

La modification du fichier `krb5.conf` n'est cependant pas suffisante, il nous faut aussi faire correspondre les données incluses dans le fichier `/etc/samba/smb.conf` en changeant les lignes :

- realm
- password server
- workgroup
- idmap config
- wins server

La modification de ce fichier implique que l'on n'utilise pas les extensions unix RFC2307.

```
[global]
security = ads
realm = TRANQUILIT.LAN
password server = 192.168.87.11
workgroup = TRANQUILIT
winbind separator = +
idmap backend = tdb
idmap uid = 1000000-1999999
idmap gid = 1000000-1999999
idmap config TRANQUILIT: backend = rid
idmap config TRANQUILIT = range = 10000 - 49999
winbind enum users = yes
winbind enum groups = yes
template homedir = /home/%D/%U
template shell = /bin/bash
client use spnego = yes
client ntlmv2 auth = yes
encrypt passwords = yes
winbind use default domain = yes
restrict anonymous = 2
wins server = 192.168.87.11
printcap name = /dev/null
load printers = no
acl group control = yes
inherit acls = yes
map acl inherit = yes
ea support = yes
```

```
acl map full control = True
force unknown acl user = yes
inherit permissions = yes
nt acl support = yes
vfs objects = acl_xattr
[partages]
path = /home/partages
guest ok = no
write list = @ 'domain users'
writeable = yes
force create mode = 0770
force directory mode = 770
```

Maintenant que nous avons attribué les paramètres correspondants, nous relançons les services Samba :

```
/etc/init.d/samba restart
/etc/init.d/winbind restart
```

Une fois les services Samba relancés, nous modifions le fichier /etc/nsswitch.conf :

```
passwd:compat winbind
group: compat winbind
shadow: compat winbind
hosts: files dns
networks: files
protocols: db files
services: db files
ethers: db files
rpc: db files
netgroup: nis
```

Puis, nous mettons en place les DNS forward et reverse pour la machine concernée en rajoutant les outils Samba dans \$PATH :

```
echo 'export PATH=$PATH:/usr/local/samba/sbin:/usr/local/samba/win' >>
/root/.bashrc
source /root/.bashrc
```

Nous pouvons alors intégrer la machine au domaine :

```
/usr/local/samba/bin/net ads join -Uadministrateur
```

Pour nous assurer du bon paramétrage à ce stade, nous testons la configuration Kerberos en récupérant un ticket de ce service :

```
kinit administrateur
```

De nouveau, nous relançons les services :

```
/etc/init.d/samba restart
/etc/init.d/winbind restart
```

Suite au redémarrage des services, nous testons le winbind en appelant la liste des utilisateurs :

```
wbinfo -u
```

En cas d'échec, vérifier à nouveau les DNS et la configuration avec la commande suivante :

```
wbinfo -t
```

Afin d'intégrer alors les machines au domaine, il nous faut leur installer les paquets nécessaires :

```
apt-get install libpam-krb5
```

On réalise la même opération pour les fichiers serveur en y ajoutant la configuration PAM en plus à travers l'édition du fichier `/etc/pam.d/common-account` :

```
account [succes=2 new_authrok_redq=done default=ignore] pam_unix.so
account required pam_winbind.so
account requisite pam_deny.so
account required pam_permit.so
```

On procède ensuite à l'édition du fichier `/etc/pam.d/common-password` :

```
password [succes=2 default=ignore] pam_unix.so obscure sha512
password requisite pam_deny.so
password required pam_permit.so
```

Après avoir établi ces premiers paramètres, nous définissons ceux de session au travers du fichier `/etc/pam.d/common-session` :

```
session [default=1] pam_permit.so
session requisite pam_deny.so
session required pam_permit.so
session required pam_unix.so
session required pam_mkhomedir.so silent skel=/etc/skel.empty
session optional pam_windbind.so krb5_auth krb5_ccache type=FILE
```

Enfin, pour utiliser l'authentification kerberos avec le protocole ssh, nous nous assurons de la présence de la ligne qui suit dans le fichier `/etc/ssh/sshd_config` :

```
UsePAM yes
```

En ayant respecté ces différentes étapes, nos machines utilisateurs GNU/Linux sont désormais couplées à notre service serveur Active Directory.

H.14 Script de création des utilisateurs dans le domaine

```
try {
    Write-Warning "Création de l'utilisateur Active Directory"
    $cred = ConvertTo-SecureString -String "P@ssw0rd" -AsPlainText -Force
    $nom = Read-Host 'Nom ?'
    $prenom = Read-Host 'Prénom ?'
    New-ADUser -Name "$prenom $nom" -GivenName $prenom -Surname $nom -SamAccountName
"$prenom.$nom" -UserPrincipalName "$prenom.$nom" -AccountPassword $cred -Path
"OU=Utilisateurs,OU=ADCYC,DC=CYC,DC=local"-Verbose -ErrorAction Stop
    Enable-ADAccount "$prenom.$nom"
    $id = 0
    $Objects = foreach ($Machine in Get-ADGroup -filter * -SearchBase
"OU=Groupes,OU=ADCYC,DC=CYC,DC=local" -Verbose | Select-Object -Property Name ) {
        $ObjectProperties = @{
            ID = $id++
            Name = $Machine."Name"
        }
        New-Object psobject -Property $ObjectProperties -Verbose -ErrorAction Stop
    }
    Write-Warning "Ajout des groupes sur l'utilisateur Active Directory"
    Function othergroup(){
        clear
        $other = Read-Host 'Ajouter un autre groupe ? [Y/N]'
        switch ($other){
            'y' {
                MesGroupes
            }
            Default {
                clear
                sleep 1
                Write-Warning 'Utilisateur créé avec succès'
            }
        }
    }
    Function MesGroupes(){
        clear
        Write-Host ($Objects | Format-Table | Out-String)
        $group = Read-Host 'Index de Groupe ?'
        $group = $Objects | Where-Object -Property ID -eq $group | Select-Object -
Property Name
        if ($group -eq $null){
            Write-Warning 'Mauvais ID de groupe'
            MesGroupes
        }
        Add-ADGroupMember -Identity $group.Name -Members "$prenom.$nom"
        othergroup
    }
}
```



```
}
    MesGroupes
}
catch {
    Write-Error $_
    PAUSE
}
```

H.15 Script de sauvegarde PowerShell

```
#~ CONFIGURATION ~#
# Répertoire des fichiers à sauvegarder
$dossier="[répertoire de stockage : pool cycnetworking]"
# Répertoire de stockage des backups
$backup="[répertoire de backup : pool cycbackup]"
# Chemin du fichier de logs
$log=" [répertoire système]\deletelogs.txt"
# Nombre des derniers backup à conserver
$nb=21

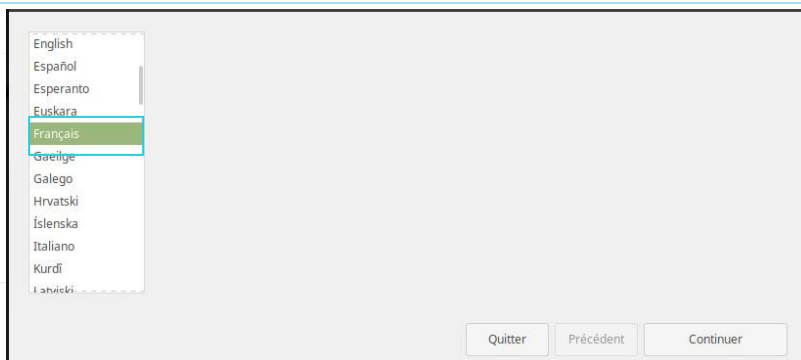
#~ NE PAS MODIFIER ~#
$now=get-date -UFormat %m_%d_%Y_%H%M%S
$sourceFolder = "$dossier"
$destinationZip = "$backup/backup_$now.zip"
[Reflection.Assembly]::LoadWithPartialName( "System.IO.Compression.FileSystem" )
[System.IO.Compression.ZipFile]::CreateFromDirectory($sourceFolder, $destinationZip)
if ( (Test-Path $log) -eq $True) {
    Remove-Item -Path $log
}
$FileNeedRemove = @(Get-ChildItem -path $backup -Recurse -File | Sort-Object -Property
CreationTimeUtc -Descending | Select-Object -Skip $nb)
if($FileNeedRemove.Count -gt 0) {
    if ( (Test-Path $log) -eq $False) {
        Tee-Object $log
    }
    $FileNeedRemove | Remove-Item
    echo "Deleted files List: `n" >> $log
    $FileNeedRemove | Select-Object -Property Name,Length |FT >> $log
} else {
write-host "Le nombre de fichiers est inférieur à $nb"
}
```

H.16 Procédure d'installation de Linux Mint

ETAPE 1

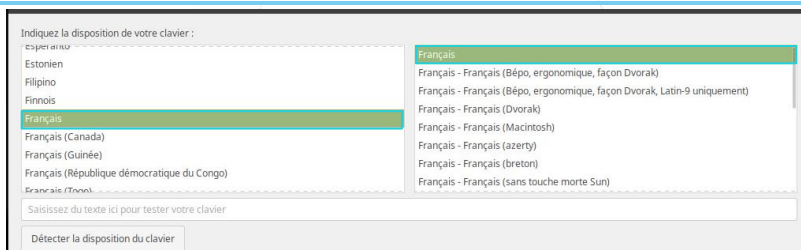
Le déploiement de Linux Mint peut être réalisé de deux manières différentes, en boot PxE depuis nos hyperviseurs ou par le biais d'une clé USB bootable.

Une fois le démarrage machine effectué, il nous est offert de choisir la langue du système : Français.



ETAPE 2

La langue système choisie, nous sommes invités à choisir la langue de disposition du clavier ainsi que le jeu de caractères de ce dernier.



ETAPE 3

Une fois les critères de langues validés, un écran nous proposant l'installation de logiciels tiers (drivers) nous est présenté.

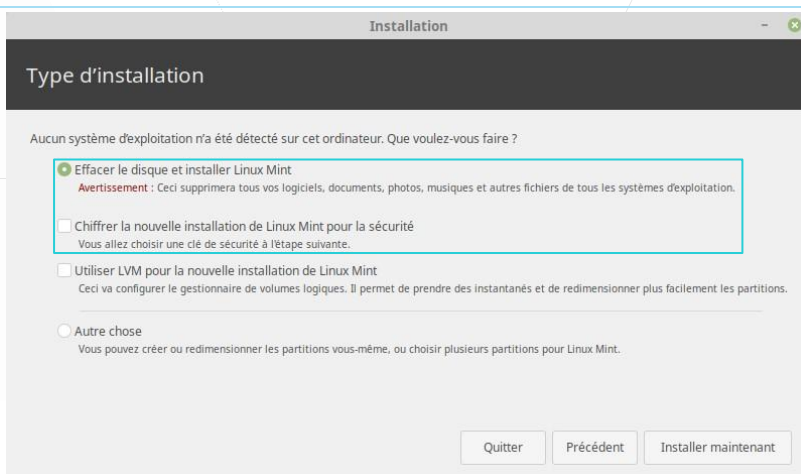
Cocher la case afin de ne pas à devoir rechercher les pilotes manuellement.



ETAPE 4

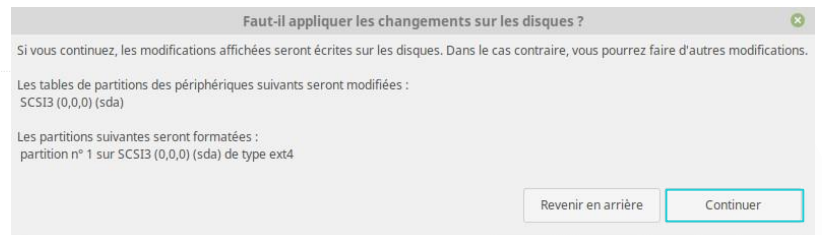
Nous sommes alors invités à choisir notre type d'installation. Remettant tous les postes de la société à niveau ; nous effaçons les disques des ordinateurs pour l'installation.

De plus, afin de renforcer la sécurité et limiter les risques de fuites/vol de données, nous cochons la case de chiffrement de l'installation (Chiffrement ZFS).



ETAPE 5

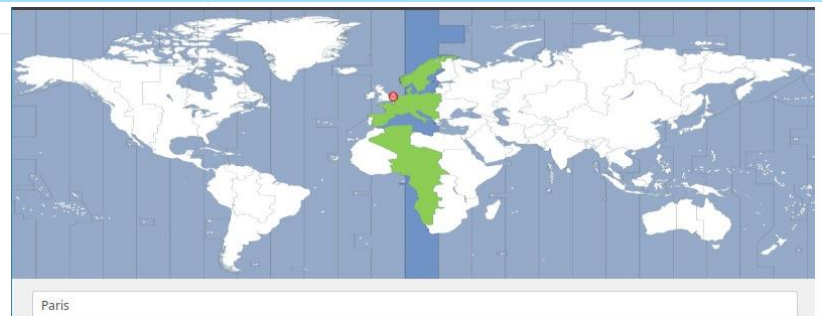
Après avoir choisi la clé de chiffrement de notre poste, nous sommes invités à valider l'installation. Cliquer sur continuer rend le processus d'installation irréversible.



ETAPE 6

Suite à la confirmation, nous devons choisir notre localisation.

Cette dernière est à valider en renseignant la capitale du pays d'implantation. Dans notre cas, il s'agit de Paris.



ETAPE 7

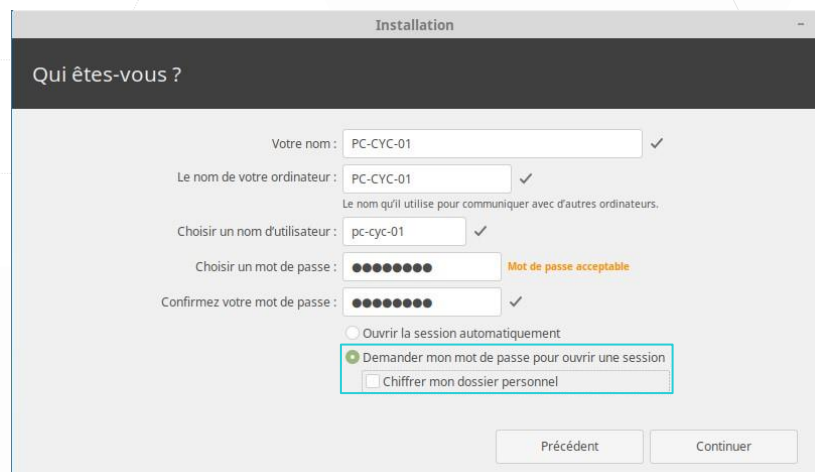
Vous voici alors face à de multiples champs à compléter. Pas de panique, remplissons-les dans l'ordre.

Tout d'abord, nous renseignons notre nom. Les postes appartenant à la société, nous renseignerons "Customize Your Car".

Ensuite, nous renseignons le nom du poste, respectant la nomenclature interne : PC-CYC-[3 premières lettres du service][numéro de poste]

Nous renseignons alors notre nom d'utilisateur et le mot de passe associé.

Pour plus de sécurité, nous exigeons que le mot de passe soit saisi pour l'ouverture de la session et que le dossier personnel soit chiffré.



ETAPE 8

Une fois l'étape précédente confirmée, l'installation se déclenche et une barre d'état nous en indique l'avancement.



ETAPE 9

Après validation de l'installation, une boîte de dialogue nous invite à redémarrer le poste. Cliquer sur "Restart Now". Après redémarrage, vous serez sur votre nouveau bureau. Félicitations !

