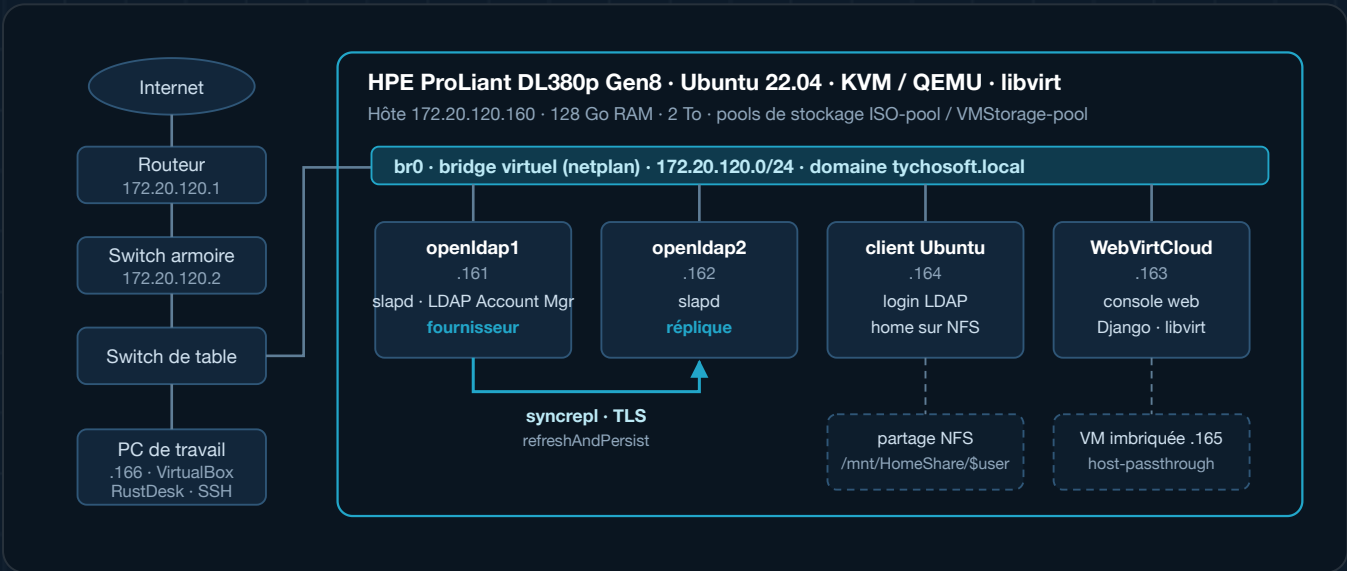


Infrastructure virtuelle Linux KVM

Alternative open source à VMware pour une PME fictive : hyperviseur KVM sur serveur physique, annuaire OpenLDAP redondant, comptes utilisateurs avec dossier personnel sur le réseau et administration web des machines virtuelles.

CADRE	PÉRIODE	CHARGE	NOTE OBTENUE
TPI · ETML Lausanne	2 mai – 5 juin 2024	88 heures, seul	5,3 / 6
Chef de projet : Nicolas Cuendet · Experts : Nemanja Pantic et Jean-Luc Roduit			



4 + 1

machines virtuelles, dont une imbriquée

2

serveurs d'annuaire répliqués en continu

7

objectifs évalués au cahier des charges

0

perte de données au basculement testé

KVM / QEMU

libvirt · virt-manager

netplan · bridge br0

OpenLDAP · syncrepl

TLS

PAM · NSS

NFS

WebVirtCloud

Virtualisation imbriquée

Ubuntu 22.04

01 Contexte et objectifs

L'entreprise fictive **TychoSoft** cherche une alternative moins coûteuse à VMware pour gérer son parc : postes, comptes utilisateurs et données. Le cahier des charges demande une infrastructure virtualisée sous Linux avec KVM, un annuaire centralisé à haute disponibilité et une administration des machines depuis un navigateur.

#	OBJECTIF ÉVALUÉ	BRIQUE TECHNIQUE
1	Installer et configurer l'hyperviseur KVM	QEMU/KVM, libvirt, virt-manager
2	Déployer une machine Linux servant de serveur de domaine principal	VM Ubuntu 22.04 openldap1
3	Configurer un annuaire utilisateurs	OpenLDAP (slapd), LDAP Account Manager
4	Comptes utilisateurs avec stockage personnel et authentification sur un client	PAM / NSS, home sur partage NFS
5	Interface d'administration web	WebVirtCloud (Django)
6	Client Linux déployé depuis l'interface web et intégré au domaine	VM imbriquée sous WebVirtCloud
7	Scénario de reprise de service en cas de panne du serveur principal	Réplication syncrepl + 2 ^e URI client

02 Méthode

Méthode en six étapes (s'informer, planifier, décider, réaliser, contrôler, évaluer), planification détaillée dans un diagramme de Gantt (ProjectLibre) et journal de travail comparant prévu et réel. Fil rouge en neuf jalons, de l'installation du serveur au scénario de reprise.



03 Plan d'adressage

MACHINE	RÔLE	ADRESSE
Hôte ProLiant	Hyperviseur KVM, bridge br0, partage NFS	172.20.120.160
openldap1 / openldap2	Annuaire principal / réplique	.161 / .162
WebVirtCloud	Console d'administration web	.163
Client Ubuntu / client imbriqué	Poste utilisateur du domaine	.164 / .165
PC de travail	Accès distant (VM VirtualBox, RustDesk, SSH)	.166

Plage réservée 172.20.120.160 – .169, masque /24, domaine tychosoft.local, réseau de laboratoire de l'école.

04 Choix techniques

Matériel

HPE ProLiant DL380p Gen8, 128 Go de RAM, 2 To de disques. Pools de stockage séparés pour les images ISO et les disques des VM.

Systèmes

Ubuntu 22.04 pour l'hôte et les VM (écosystème le plus standard, moins de soucis de compatibilité). Ubuntu 20.04 pour la VM d'accès sous VirtualBox.

Annuaire

Paquets OpenLDAP du dépôt Ubuntu (slapd, utilitaires LDAP) et LDAP Account Manager pour créer les comptes depuis le web.

Console web

WebVirtCloud, version communautaire la plus maintenue (dépôt retspen), retenue après des échecs d'installation de l'autre variante.

05 Réalisation : les points clés

Bridge réseau avec netplan

Beaucoup de tutoriels modifient encore `/etc/network/interfaces`, ignoré par Ubuntu récent. Le bridge est déclaré dans netplan pour que les VM obtiennent une adresse directement sur le réseau du laboratoire, comme des machines physiques.

```
network:
  version: 2
  bridges:
    br0:
      interfaces: [eno1]
      addresses: [172.20.120.160/24]
      routes: [{to: default, via: 172.20.120.1}]
      nameservers:
        addresses: [8.8.8.8, 1.1.1.1]
# sudo netplan generate && sudo netplan apply
```

Réplication de l'annuaire

openldap1 publie ses changements (overlay syncprov), openldap2 les reçoit en continu avec un compte dédié replicator aux droits limités. La réplication n'a fonctionné qu'une fois TLS configuré en premier.

```
# consommateur (openldap2)
olcSyncrepl: rid=001
provider=ldap://openldap1.tychosoft.local
binddn="cn=replicator,dc=tychosoft,dc=local"
searchbase="dc=tychosoft,dc=local"
type=refreshAndPersist retry="60 +"
starttls=critical
```

Authentification des postes

Le client résout les comptes via LDAP (NSS), s'authentifie via PAM et crée le dossier personnel à la première connexion. Les deux serveurs sont déclarés : si le premier ne répond plus, le client interroge le second.

```
# /etc/nsswitch.conf
passwd: files ldap
group: files ldap
shadow: files ldap
# /etc/pam.d/common-session
session optional pam_mkhomedir.so skel=/etc/skel
umask=0022
# /etc/ldap/ldap.conf
BASE dc=tychosoft,dc=local
URI ldap://openldap1.tychosoft.local
    ldap://openldap2.tychosoft.local
```

Dossier personnel sur le réseau

Les home des utilisateurs LDAP pointent vers `/mnt/HomeShare/$user`, un partage NFS hébergé sur l'hôte : les données ne dépendent pas des serveurs d'annuaire et survivent à leur panne.

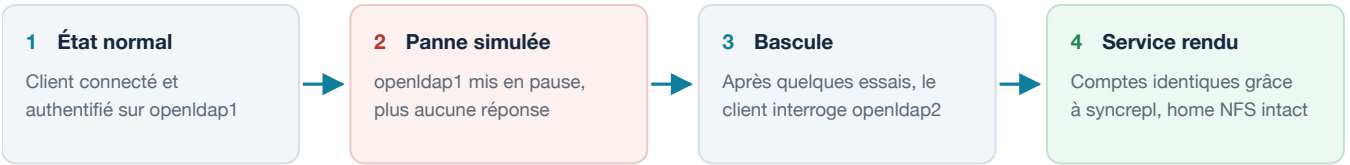
Virtualisation imbriquée

WebVirtCloud tourne dans une VM et lance lui-même une VM : il faut exposer les extensions CPU de l'hôte.

```
$ cat /sys/module/kvm_intel/parameters/nested
Y
<!-- XML de la VM dans virt-manager -->
<cpu mode="host-passthrough"/>
```

Extraits représentatifs des configurations décrites dans le rapport, mot de passe du compte de réplication omis.

06 Scénario de reprise de service



Tests documentés en plus : connectivité de l'hôte, services virt-manager et OpenLDAP actifs, réseau des VM, connexion aux deux annuaires, support de la virtualisation imbriquée, puis test global de bout en bout.

07 Bilan des objectifs

#	OBJECTIF	RÉSULTAT	REMARQUE
1	Hyperviseur KVM	Atteint	VM, pools de stockage et bridge conformes au schéma
2-3	Serveur de domaine et annuaire	Atteint	Branches People et Group, comptes utilisables sur les clients
4	Comptes et stockage personnel	Atteint	Session LDAP avec home sur le partage NFS
5	Console WebVirtCloud	Partiel	Gestion des VM par le web fonctionnelle ; connexion admin via LDAP en erreur 500/502
6	Client déployé via le web, dans le domaine	Partiel	VM imbriquée lente, mises à jour automatiques bloquant les paquets ; démontré sur un autre client
7	Reprise de service	Atteint	Bascule automatique sans perte de données

08 Ce que j'en retiens

- Sécuriser d'abord (TLS), répliquer ensuite : l'ordre évite des heures de débogage.
- Quand un point bloque, avancer sur le reste et y revenir : planning tenu à 1-2 jours près.
- Documenter chaque étape coûte du temps mais rend l'infrastructure transmissible.
- Sauvegardes : disques qcow2 compressés et définitions XML exportées avec virsh dumpxml.

09 Avec le recul, en 2026

- Ubuntu Server sans interface graphique, configuration en SSH et scripts.
- Installation des VM reproductible (cloud-init ou Ansible) plutôt que manuelle.
- LDAPS de bout en bout et étude préalable de django-auth-ldap pour la console.
- Désactiver les mises à jour automatiques le temps du déploiement d'une VM.