PROCÉDURE TECHNIQUE · BTS SIO SISR

Cloisonnement des permissions utilisateurs sous Proxmox VE

Isoler chaque groupe d'étudiants dans son pool, avec uniquement le stockage et les ponts réseau dont il a besoin, sans exposer le nœud physique.

Auteur	Plot 1
Contexte	TP réalisé en équipe — Plot 1, domaine ngrange.local
Version	2.0 — novembre 2026
Environnement	Proxmox VE (interface web et outil `pveum`), authentification « Proxmox VE authentication server »
Durée estimée	30 min

Identifiants d'accès — Plot 1

Machine / service	Adresse	Identifiant	Mot de passe
Proxmox VE	https://100.101.0.13:8006	`root@pam`	`non fourni`
Comptes SIO créés	realm @pve	`SIO1@pve, SIO2@pve`	`à définir`

Sommaire

1. Objectif
2. Architecture et prérequis
3. Principe : le modèle de permissions
4. Préparer groupes, utilisateurs et pools
5. Droits du groupe SIO1
6. Droits du groupe SIO2
7. Activer la vue Pool côté utilisateur
8. Vérification
9. Dépannage
10. Sécurité et bonnes pratiques
11. Aide-mémoire : Proxmox VE au quotidien

1. Objectif

Un seul hyperviseur Proxmox VE sert plusieurs groupes d'étudiants. Chaque groupe doit pouvoir créer et administrer **ses** machines virtuelles, monter les ISO mises à disposition et brancher ses cartes réseau virtuelles, mais ne doit **ni voir ni modifier** les ressources des autres groupes, ni toucher à la configuration du serveur physique.

Le cloisonnement repose sur trois éléments : un **pool** par groupe (périmètre des VM), des **droits sur le stockage** (ISO et disques) et des **droits SDN** par pont réseau (`vmbr0`, `vmbr1`, `vmbr2`). Tous les droits sont attribués à un **groupe**, jamais à un utilisateur isolé.

2. Architecture et prérequis

Élément	Groupe SIO1	Groupe SIO2
Groupe Proxmox	`SIO1`	`SIO2`
Compte utilisateur (exemple de l'original)	`SIO1@pve`	compte du même type, ex. `SIO2@pve` *(exemple)*
Pool de ressources	`Pool-SIO1`	`Pool-SIO2`
Nœud physique	`<NOEUD>` *(nom du nœud non fourni : à relever sous Datacenter)*	
Stockages partagés	`local` (ISO déposées par root) · `local-lvm` (disques des VM)	
Ponts réseau autorisés	`vmbr0` uniquement	`vmbr1` et `vmbr2`

Prérequis :

- Accès au compte `root@pam` (interface web `https://100.101.0.13:8006` ou shell du nœud).
- Les ponts `vmbr0`, `vmbr1`, `vmbr2` existent sur le nœud et sont visibles sous *Datacenter* > *SDN* (zone `localnetwork`).
- Les images ISO ont été téléversées par root dans le stockage `local` (*ISO Images* > *Upload*).

> **À savoir**
> Les identifiants de l'interface (`SIO1@pve` , `Pool-SIO1` …) sont ceux du TP. Les noms du groupe SIO2 et la création des comptes sont donnés à titre d'exemple pour rendre la procédure rejouable.

3. Principe : le modèle de permissions

Une permission Proxmox associe trois informations : un **chemin** (objet protégé), un **sujet** (utilisateur ou groupe) et un **rôle** (ensemble de privilèges). Par défaut, un droit posé sur un chemin est hérité par les objets enfants (option *Propagate* cochée) : un droit sur `/pool/Pool-SIO1` couvre donc toutes les VM du pool.

Rôle	Ce qu'il autorise	Utilisé sur
`PVEVMAdmin`	Administration complète des VM (création, démarrage, console, snapshots, suppression)	le pool
`PVEDatastoreUser`	Voir un stockage et y allouer de l'espace ; suffit pour monter une ISO	`local`
`PVEDatastoreAdmin`	Idem, plus la gestion du stockage et de ses volumes	`local-lvm`
`PVEAuditor`	Lecture seule (aucune modification)	le nœud
`PVESDNUser`	Droit d'utiliser un pont/réseau virtuel pour y connecter une carte réseau de VM	chaque pont autorisé

4. Préparer groupes, utilisateurs et pools

1 Créer les groupes, les pools et rattacher les VM

Les droits ne s'appliquent qu'à des objets existants : on crée d'abord les groupes et les pools. Interface : *Datacenter* > *Permissions* > *Groups* / *Pools*. Équivalent en ligne de commande, depuis le shell du nœud :

```
# Groupes
pveum group add SIO1 --comment "Étudiants SIO1"
pveum group add SIO2 --comment "Étudiants SIO2"

# Pools (un par groupe)
pvesh create /pools --poolid Pool-SIO1
pvesh create /pools --poolid Pool-SIO2

# Rattacher les stockages visibles dans la vue Pool
pvesh set /pools/Pool-SIO1 --storage local,local-lvm
pvesh set /pools/Pool-SIO2 --storage local,local-lvm
```

2 Créer les comptes et les placer dans leur groupe

Un compte sans groupe n'hérite d'aucun droit : l'appartenance au groupe est ce qui active la matrice de la section suivante. Interface : *Datacenter* > *Permissions* > *Users* > *Add* (realm *Proxmox VE authentication server*).

```
pveum user add SIO1@pve --groups SIO1 --comment "Compte étudiant SIO1"
pveum passwd SIO1@pve        # saisie interactive du mot de passe
pveum user add SIO2@pve --groups SIO2 --comment "Compte étudiant SIO2"
pveum passwd SIO2@pve
```

5. Droits du groupe SIO1

3 Appliquer la matrice de droits SIO1

Connecté en `root@pam`, ouvrir *Datacenter* > *Permissions* > *Add* > *Group Permission* et créer les cinq entrées ci-dessous (une par ligne, cocher *Propagate*). Chaque ligne répond à un besoin précis de l'assistant de création de VM.

Chemin (Path)	Rôle	Pourquoi
`/pool/Pool-SIO1`	PVEVMAdmin	Administrer toutes les VM du pool, et uniquement celles-ci
`/storage/local`	PVEDatastoreUser	Lister et monter les ISO déposées par root
`/storage/local-lvm`	PVEDatastoreAdmin	Allouer l'espace des disques virtuels
`/nodes/<NOEUD>`	PVEAuditor	Voir le nœud (l'assistant de création de VM l'exige), sans pouvoir le modifier
`/sdn/zones/localnetwork/vmbr0`	PVESDNUser	Brancher les cartes réseau sur `vmbr0` exclusivement

Commandes équivalentes :

```
pveum acl modify /pool/Pool-SIO1                    --groups SIO1 --roles PVEVMAdmin
pveum acl modify /storage/local                     --groups SIO1 --roles
PVEDatastoreUser
pveum acl modify /storage/local-lvm                 --groups SIO1 --roles
PVEDatastoreAdmin
pveum acl modify /nodes/<NOEUD>               --groups SIO1 --roles PVEAuditor
pveum acl modify /sdn/zones/localnetwork/vmbr0      --groups SIO1 --roles PVESDNUser
```

> **Point de vigilance**
> Le rôle `PVEDatastoreAdmin` sur `local-lvm` (valeur du TP d'origine) donne plus que nécessaire : il permet aussi de supprimer des volumes et de gérer le stockage. Pour créer des disques, `PVEDatastoreUser` (qui contient le privilège d'allocation d'espace) suffit. Le privilège minimal est recommandé si les étudiants n'ont pas à administrer le stockage ; à valider par un test de création de VM.

6. Droits du groupe SIO2

4 Appliquer la matrice de droits SIO2

Même démarche pour le second environnement. La différence porte sur le pool et sur les **deux** ponts autorisés : SIO2 n'a aucun droit sur `vmbr0`.

Chemin (Path)	Rôle	Pourquoi
`/pool/Pool-SIO2`	PVEVMAdmin	Administrer les VM du pool SIO2
`/storage/local`	PVEDatastoreUser	Lire les ISO
`/storage/local-lvm`	PVEDatastoreAdmin	Allouer les disques virtuels
`/nodes/<NOEUD>`	PVEAuditor	Visibilité du nœud pour l'assistant
`/sdn/zones/localnetwork/vmbr1`	PVESDNUser	Premier pont réseau autorisé
`/sdn/zones/localnetwork/vmbr2`	PVESDNUser	Second pont réseau autorisé

```
pveum acl modify /pool/Pool-SIO2                    --groups SIO2 --roles PVEVMAdmin
pveum acl modify /storage/local                     --groups SIO2 --roles
PVEDatastoreUser
pveum acl modify /storage/local-lvm                 --groups SIO2 --roles
PVEDatastoreAdmin
pveum acl modify /nodes/<NOEUD>               --groups SIO2 --roles PVEAuditor
pveum acl modify /sdn/zones/localnetwork/vmbr1      --groups SIO2 --roles PVESDNUser
pveum acl modify /sdn/zones/localnetwork/vmbr2      --groups SIO2 --roles PVESDNUser
```

Matrice de synthèse

Ressource	SIO1	SIO2
Pool-SIO1	PVEVMAdmin	aucun accès
Pool-SIO2	aucun accès	PVEVMAdmin
Stockage `local` (ISO)	PVEDatastoreUser	PVEDatastoreUser
Stockage `local-lvm` (disques)	PVEDatastoreAdmin	PVEDatastoreAdmin
Nœud <NOEUD>	PVEAuditor	PVEAuditor
`vmbr0`	PVESDNUser	aucun accès
`vmbr1`	aucun accès	PVESDNUser
`vmbr2`	aucun accès	PVESDNUser

7. Activer la vue Pool côté utilisateur

5 **Passer l'interface en « Pool View »**

La vue par défaut (*Server View*) est organisée autour du nœud : un utilisateur restreint n'y retrouve pas ses ressources et pense à tort que ses droits sont absents. Se connecter avec le compte étudiant (ex. `SIO1@pve`, realm *Proxmox VE authentication server*), puis, dans la liste déroulante située au-dessus de *Datacenter*, remplacer *Server View* par *Pool View*.

L'arborescence n'affiche alors que le pool autorisé et les stockages rattachés ; le nœud physique est masqué. Ce choix est mémorisé par le navigateur : il est à refaire sur un nouveau poste.

8. Vérification

Côté administrateur (shell du nœud) :

```
pveum acl list | grep -E "SIO1|SIO2"
pveum user permissions SIO1@pve --path /sdn/zones/localnetwork/vmbr0
pveum user permissions SIO1@pve --path /sdn/zones/localnetwork/vmbr1
pveum user permissions SIO2@pve --path /pool/Pool-SIO1
```

Côté étudiant (compte `SIO1@pve`, Pool View) :

Test	Résultat attendu
Arborescence	Seuls `Pool-SIO1` et les stockages sont visibles ; pas de `Pool-SIO2`
Création d'une VM (*Create VM*), onglet OS	Les ISO du stockage `local` sont listées
Onglet Disks	`local-lvm` est proposé ; la création aboutit
Onglet Network, champ Bridge	Seul `vmbr0` est proposé (`vmbr1` et `vmbr2` absents ou refusés)
VM créée dans `Pool-SIO1`	Démarrage et console fonctionnent
Accès au nœud (*Shell*, *Network*, *Updates*)	Refusé (*Permission check failed*)

Résultat attendu

Le compte SIO1 crée et pilote ses VM sur `vmbr0` uniquement ; le compte SIO2 en fait autant sur `vmbr1` et `vmbr2` ; aucun des deux ne voit les ressources de l'autre ni n'administre le nœud. `pveum user permissions` ne liste aucun privilège pour SIO2 sur `/pool/Pool-SIO1`.

9. Dépannage

Symptôme	Cause probable	Solution
L'étudiant ne voit aucune VM ni aucun pool	Vue *Server View* active, ou compte non membre du groupe	Passer en *Pool View* ; vérifier `pveum user list` (colonne groupes)
Aucune ISO proposée à la création de la VM	Droit manquant sur `/storage/local`, ou ISO absente	Ajouter `PVEDatastoreUser` ; téléverser l'ISO en root
« Permission check failed (/storage/local-lvm, Datastore.AllocateSpace) »	Droit absent sur `local-lvm`	Ajouter le rôle sur `/storage/local-lvm`
Le champ Bridge est vide ou refusé	Droit SDN absent sur le pont, ou chemin mal saisi	Vérifier le chemin exact `/sdn/zones/localnetwork/vmbrX` ; `pveum acl list`
Erreur à la création : chemin `/nodes/…` ou `/vms/…` refusé	Rôle d'audit absent sur le nœud, ou VM créée hors du pool	Ajouter `PVEAuditor` sur le nœud ; choisir le pool dans l'assistant (onglet General)
Droits non appliqués après modification	Session web ouverte avec les anciens droits	Se déconnecter puis se reconnecter

10. Sécurité et bonnes pratiques

- Attribuer les droits à des **groupes** : l'arrivée ou le départ d'un étudiant se gère par l'appartenance au groupe, sans retoucher les ACL.
- Appliquer le **moindre privilège** : pas de rôle `Administrator` aux étudiants ; préférer `PVEDatastoreUser` à `PVEDatastoreAdmin` lorsque c'est suffisant.
- Ne jamais utiliser `root@pam` pour le travail quotidien ; activer l'authentification à deux facteurs sur les comptes à privilèges (*Datacenter* > *Permissions* > *Two Factor*).
- Auditer régulièrement : `pveum acl list` doit correspondre à la matrice documentée ; supprimer les droits d'un groupe avec `pveum acl delete <chemin> --groups <groupe> --roles <rôle>`.
- Ne pas rattacher le même pont à deux groupes sans raison : le pont reste le vrai cloisonnement réseau entre environnements.
- Documenter chaque ajout de pool ou de pont dans la matrice de synthèse pour garder la cohérence.

11. Aide-mémoire : utiliser Proxmox VE au quotidien

Référence rapide pour ne plus chercher les gestes courants. Les chemins sont donnés pour l'interface web (port 8006) ; chaque tâche a son équivalent en ligne de commande depuis le shell du nœud (*Node* > *Shell*

ou SSH). Les identifiants (`205` = SRV-ARTICA, `230` = exemple, `pve2`, `eno2`, noms de fichiers) sont des **exemples** à adapter.

Créer une VM

Bouton **Create VM** (en haut à droite). Onglets de l'assistant :

Onglet	Champs importants
General	Node, VM ID, Name, *Resource Pool* (pour que le groupe voie la VM)
OS	Storage `local` > ISO image ; Type et version du système invité
System	Machine `q35`, BIOS (OVMF pour l'UEFI), SCSI Controller *VirtIO SCSI single*, case *Qemu Agent*
Disks	Bus *SCSI*, Storage (`local-lvm`), Disk size, option *Discard* sur stockage fin
CPU / Memory	Cores, Type (`host` pour les performances ; `x86-64-v2-AES` si migration entre hôtes différents), Memory en Mio
Network	Bridge (`vmbr0` …), VLAN Tag, Model *VirtIO*

```
qm create 205 --name SRV-ARTICA --memory 2048 --cores 2 --cpu host --ostype l26 --agent
1 \
  --scsihw virtio-scsi-single --scsi0 local-lvm:32 \
  --net0 virtio,bridge=vmbr0 --ide2 local:iso/debian.iso,media=cdrom --boot
order='scsi0;ide2'
qm start 205
```

Après installation : installer `qemu-guest-agent` dans l'invité, puis éjecter l'ISO (*Hardware* > *CD/DVD Drive* > *Do not use any media*).

Créer un conteneur LXC

Prérequis : un modèle dans *local* > *CT Templates* > *Templates* (choisir, *Download*). Puis **Create CT** : General (Hostname, Password ou clé SSH, *Unprivileged container* coché), Template, Disks, CPU, Memory, Network (IPv4 statique ou DHCP), DNS.

```
pveam update
pveam available --section system
pveam download local debian-12-standard_12.7-1_amd64.tar.zst     # nom = exemple
pct create 200 local:vztmpl/debian-12-standard_12.7-1_amd64.tar.zst --hostname ct1 \
  --memory 512 --rootfs local-lvm:8 --unprivileged 1 \
  --net0 name=eth0,bridge=vmbr0,ip=dhcp --password
pct start 200
```

Téléverser une ISO

Datacenter > *nœud* > `local` *(stockage)* > *ISO Images* : **Upload** (fichier local) ou **Download from URL** (téléchargement direct par le serveur, avec contrôle de somme possible). Le stockage doit avoir le contenu « ISO image » activé (*Datacenter* > *Storage* > *Edit* > *Content*).

```
cd /var/lib/vz/template/iso && wget https://exemple.org/image.iso
pvesm list local --content iso
```

Templates et clones

- **Convertir en modèle** : clic droit sur la VM arrêtée > *Convert to template* (irréversible ; la VM ne démarre plus).
- **Cloner** : clic droit > *Clone*. *Full Clone* : copie indépendante. *Linked Clone* : rapide et économe, mais dépend du modèle et du type de stockage.

```
qm template 205
qm clone 205 230 --name SRV-TEST --full 1 --target pve1
pct template 200 && pct clone 200 201 --hostname ct2
```

> **À savoir**
> Après clonage, changer le nom d'hôte, l'IP et l'identifiant machine de l'invité (`/etc/machine-id` sous Linux, sysprep sous Windows).

Snapshots

VM > *Snapshots* > *Take Snapshot* (Name, Description, *Include RAM* pour restaurer en état de marche) ; **Rollback** restaure, **Remove** supprime. Un snapshot n'est **pas** une sauvegarde : il reste sur le même stockage.

```
qm snapshot 205 avantmaj --description "avant mise à jour"
qm listsnapshot 205
qm rollback 205 avantmaj
qm delsnapshot 205 avantmaj
pct snapshot 200 avantmaj
```

Sauvegardes vzdump et restauration

Action	Chemin d'interface	Champs importants
Sauvegarde immédiate	*VM* > *Backup* > *Backup now*	Storage cible, Mode (*Snapshot* sans arrêt, *Suspend*, *Stop*), Compression `ZSTD`
Sauvegarde planifiée	*Datacenter* > *Backup* > *Add*	Sélection (VM, pool), Schedule, Retention (ou *Prune* du stockage)
Restauration	*Stockage* > *Backups* > *fichier* > *Restore*	Storage cible, VM ID (vide = identifiant d'origine, attention à l'écrasement), *Start after restore*

```
vzdump 205 --storage local --mode snapshot --compress zstd
qmrestore /var/lib/vz/dump/vzdump-qemu-205-AAAA_MM_JJ-HH_MM_SS.vma.zst 230 --storage
local-lvm
pct restore 201 /var/lib/vz/dump/vzdump-lxc-200-AAAA_MM_JJ-HH_MM_SS.tar.zst --storage
local-lvm
```

> **Attention**
> Stocker aussi les sauvegardes hors de l'hyperviseur (NFS, SMB ou Proxmox Backup Server) : un disque défaillant emporterait VM et sauvegardes. Tester une restauration de temps en temps.

Créer un bridge (vmbr) et un bridge compatible VLAN

Nœud > *System* > *Network* > *Create* > *Linux Bridge*. Champs : **Name** (`vmbr1`), **IPv4/CIDR** et **Gateway** (vides si l'hôte n'a pas besoin d'IP sur ce pont), **Bridge ports** (carte physique, ex. `eno2`, vide pour un réseau purement interne), case **VLAN aware**. Cliquer sur **Apply Configuration** : la modification ne s'applique qu'à ce moment. Sur la carte réseau d'une VM, le champ *VLAN Tag* sélectionne ensuite le VLAN.

```
# /etc/network/interfaces (extrait, noms = exemples)
auto vmbr1
iface vmbr1 inet manual
        bridge-ports eno2
        bridge-stp off
        bridge-fd 0
        bridge-vlan-aware yes
        bridge-vids 2-4094

ifreload -a        # appliquer sans redémarrer
bridge vlan show   # contrôler les VLAN
```

Un nouveau pont doit ensuite recevoir ses droits SDN (`PVESDNUser`, voir section 5) pour être utilisable par un groupe.

Utilisateurs, groupes, pools et rôles personnalisés

Datacenter > *Permissions* : sous-menus *Users*, *Groups*, *Pools* (création des pools sous *Datacenter* > *Pools*), *Roles* (rôle personnalisé : *Create* + liste de privilèges) et *Permissions* > *Add* pour lier chemin, sujet et rôle. Procédure complète : sections 4 à 6.

```
pveum role add Operateur --privs "VM.Audit VM.Console VM.PowerMgmt"
pveum acl modify /pool/Pool-SIO1 --groups SIO1 --roles Operateur
pveum role list ; pveum acl list ; pveum user permissions SIO1@pve
```

Réaliser une migration

Nécessite un **cluster** (*Datacenter* > *Cluster* > *Create Cluster* / *Join*) : sur un nœud unique, la migration n'existe pas. Clic droit sur la VM > **Migrate** : choisir *Target node* et le mode (*Online* à chaud si le stockage

est partagé ou avec `--with-local-disks` ; sinon arrêter la VM). Vérifier que le pont et les stockages existent sur la cible.

```
qm migrate 205 pve2 --online                      # stockage partagé
qm migrate 205 pve2 --online --with-local-disks   # disques locaux
pct migrate 200 pve2 --restart                    # conteneur LXC (redémarrage)
```

Console noVNC et accès distant

VM > *Console* ouvre noVNC dans le navigateur (menu *Console* : Ctrl+Alt+Suppr, SPICE, xterm.js). Pour un conteneur, *CT* > *Console* ; le shell du nœud est sous *Node* > *Shell*. Si la console est noire : vérifier que la VM est démarrée, le type d'affichage (*Hardware* > *Display*) et l'accès au port 8006.

```
qm terminal 205       # console série (nécessite un port série dans la VM)
pct enter 200         # shell dans le conteneur depuis l'hôte
```

Commandes qm, pct et pvesm utiles

Commande	Rôle
`qm list` · `pct list`	Lister VM / conteneurs
`qm status 205` · `qm config 205`	État et configuration
`qm start|shutdown|stop|reset 205`	Démarrer, arrêt propre, arrêt forcé, redémarrage brutal
`qm set 205 --memory 4096 --cores 4`	Modifier la configuration
`qm resize 205 scsi0 +10G`	Agrandir un disque (puis étendre dans l'invité)
`qm unlock 205`	Lever un verrou après tâche interrompue
`pct exec 200 -- ip a` · `pct push` / `pull`	Exécuter une commande, copier un fichier
`pvesm status`	État et espace libre des stockages
`pvesm list local-lvm`	Contenu d'un stockage
`pvesh get /cluster/resources`	Vue d'ensemble de l'API (VM, stockages, nœuds)

Quotas et limites de ressources

Proxmox limite les ressources **par VM ou conteneur**, pas par pool ou utilisateur ; pour plafonner un groupe, encadrer ce que chaque VM peut consommer et le nombre de VM créées.

Ressource	Emplacement (*VM* > *Hardware*)	Équivalent CLI
CPU : cœurs, plafond de temps CPU	Processors : Cores, *CPU limit*	`qm set 205 --cores 2 --cpulimit 1`
Mémoire, ballooning	Memory : Memory, Minimum memory	`qm set 205 --memory 4096 --balloon 1024`
Débit disque	Hard Disk > Edit > *Advanced* : limites en Mo/s et IOPS	`qm set 205 --scsi0 local-lvm:vm-205-disk-0,mbps_rd=50,mbps_wr=50`
Débit réseau	Network Device : *Rate limit (MB/s)*	`qm set 205 --net0 virtio,bridge=vmbr0,rate=10`
Conteneur LXC	*CT* > *Resources*	`pct set 200 --memory 1024 --cores 1 --cpulimit 1`

Raccourcis et emplacements utiles

Élément	Emplacement
Interface web	`https://100.101.0.13:8006`
Configuration d'une VM / d'un CT	`/etc/pve/qemu-server/<id>.conf` · `/etc/pve/lxc/<id>.conf`
Stockages, utilisateurs et droits	`/etc/pve/storage.cfg` · `/etc/pve/user.cfg`
Réseau de l'hôte	`/etc/network/interfaces`
ISO, modèles de CT, sauvegardes (stockage `local`)	`/var/lib/vz/template/iso` · `/var/lib/vz/template/cache` · `/var/lib/vz/dump`
Journal des tâches	Panneau *Tasks* en bas de l'interface ; `journalctl -u pveproxy`, `journalctl -u pvedaemon`
Documentation locale	`https://100.101.0.13:8006/pve-docs/` et `man qm`, `man pveum`

Sources : documentation officielle Proxmox VE — chapitre « User Management » (permissions, rôles, pools) et manuel de `pveum` (pve.proxmox.com/pve-docs) · Procédure rédigée à partir d'un TP réalisé en équipe.