

Délégation et gestion des droits dans Proxmox VE



Trois questions fondamentales

- Où ?
- Quoi ?
- Qui ?

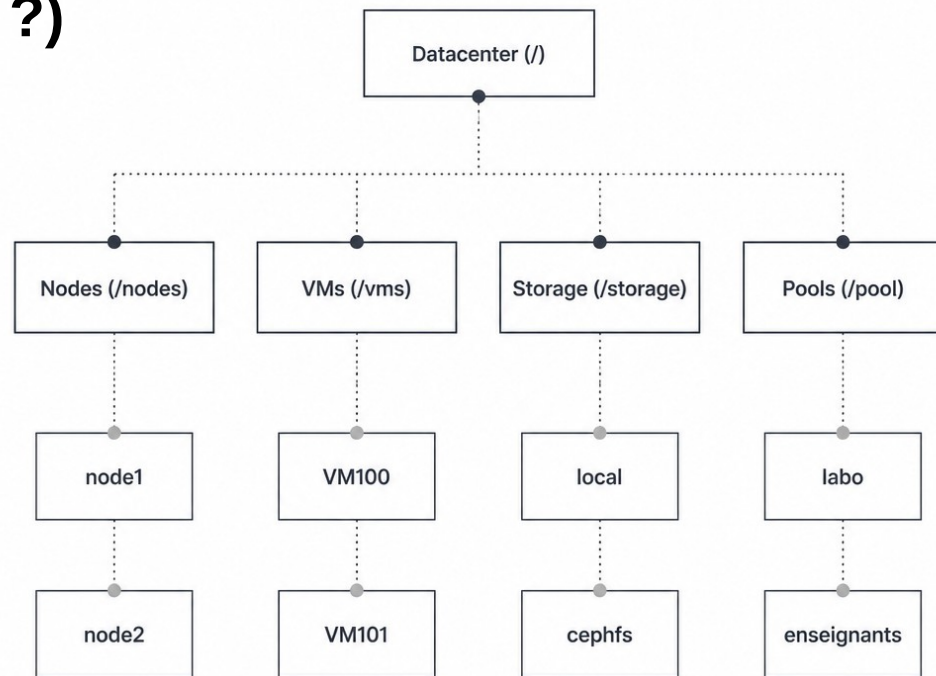
Note : Les permissions sont héritées.

	Add	Remove	
Search	Path ↑	User/Group/API Token	Role
Summary	/	ernest@pam	Administrator
Notes	/	root@pamlevZ2lpM1D7F6K0zc78Ae	Administrator
Cluster	/	zabbix@pve	Administrator
Ceph	/	@chronos	NoAccess
Options	/	ansible_user@pve	PVEAdmin
Storage	/	api_user@pve	PVEAuditor
Backup	/	api_user@pvelapi_user_token	PVEAuditor
Replication	/	@chronos	auditeur
Permissions	/nodes	@chronos	NoAccess
Users	/nodes/pve5380	@chronos	PVEAdmin
API Tokens	/nodes/pve5380	@chronos	PVETemplateUser
Two Factor	/nodes/pve5380	@chronos	PVEAdmin
Groups	/pool	@chronos	PVEDatastoreUser
Pools	/pool/chronos	@chronos	PVEAdmin
Roles	/sdn	@chronos	PVESDNUser
Realms	/storage/PBS14200	@chronos	PVEDatastoreUser
HA	/storage/chronos	@chronos	PVEDatastoreAdmin
SDN	/vms	@chronos	NoAccess
Zones	/vms	@chronos	PVEVMAAdmin
VNets	/vms/184	@chronos	PVEAdmin
	/vms/206	@chronos	PVETemplateUser
	/vms/250	@chronos	PVEAdmin

Les périmètres d'application (Où ?)

Exemples :

- / — Tout le cluster
- /nodes — Tous les nœuds
- /nodes/node1 — Un nœud
- /vms — Toutes les VM
- /vms/100 — Une VM précise
- /storage/local — Un stockage
- /pool/labo — Un groupe de ressources



Rôle et privilèges (Quoi ?)

Datacenter

</

Mode CLI : `pveum role list`

Les utilisateurs (Qui ?) 1/5

Exemple n°1

Administrateur complet : `root@pam`

Périmètre

/ — Datacenter entier

Utilisateur

`root@pam`

Rôle

Administrator

Les utilisateurs (Qui ?) 2/5

Exemple n°2

Utilisateur autonome sur sa VM

Solution 1 — Rôle standard

Attribuer **PVEVMUser** sur /vms/100

- ✓ Console, démarrage/arrêt
- ✓ Backups de la VM (doit avoir accès à un storage)
- ✗ Pas de snapshots
- ✗ Pas de restauration
- ✗ Pas de modification matérielle

Rôle attribué : PVEVMUser

- **VM.Audit** : Visualiser les VM et leurs configurations.
- **VM.Backup** : Sauvegarder et restaurer une VM.
- **VM.Config.CDROM** : Gérer les lecteurs CD/DVD virtuels.
- **VM.Config.Cloudinit** : Modifier la configuration cloud-init.
- **VM.Console** : Accéder à la console VNC/SPICE.
- **VM.GuestAgent.Audit** : Interroger l'état du QEMU Guest Agent.
- **VM.GuestAgent.FileRead** : Lire des fichiers depuis l'invité via le Guest Agent.
- **VM.GuestAgent.FileSystemMgmt** : Gérer le système de fichiers (ex: exécuter fstrim).
- **VM.GuestAgent.FileWrite** : Écrire des fichiers sur l'invité via le Guest Agent.
- **VM.PowerMgmt** : Démarrer, arrêter, suspendre et redémarrer la VM.

Les utilisateurs (Qui ?) 3/5

Exemple n°2

Utilisateur autonome sur sa VM

Solution 2 — Rôle personnalisé

Attribuer **VMUserAutonome** sur `/vms/100`

- ✓ Console, démarrage/arrêt
- ✗ Backups de la VM
- ✓ Snapshots et Rollbacks autorisés
- ✗ Pas de restauration
- ✗ Pas de modification matérielle

Rôle créé : **VMUserAutonome** (privilèges minimaux nécessaires)

- **VM.Audit** : Visualiser les VM et leurs configurations.
- **VM.Config.Options** : Modifier (notamment) les informations du cadre « Notes ».
- **VM.Console** : Accéder à la console VNC/SPICE.
- **VM.PowerMgmt** : Démarrer, arrêter, suspendre et redémarrer la VM.
- **VM.Snapshot** : Prendre un snapshot
- **VM.Snapshot.Rollback** : Revenir à l'état précédent d'un snapshot

Les utilisateurs (Qui ?) 4/5

Exemple n°3

Utilisateur pouvant sauvegarder et restaurer

Solution 3 — Rôle personnalisé

Attribuer **VM_User_Save_rest** sur /vms/100

- ✗ Console, démarrage/arrêt
- ✓ Backups de la VM
- ✗ Pas de Snapshots ni Rollbacks
- ✓ Restauration autorisée
- ✗ Pas de modification matérielle

Rôle créé : **VM_User_Save_rest** (privilèges minimaux nécessaires)

- **Datastore.Allocate** : Créer et enregistrer des objets sur un stockage.
- **Datastore.AllocateSpace** : Allouer de l'espace sur un stockage.
- **Datastore.Audit** : Visualiser les stockages et leur contenu.
- **SDN.Use** : Utiliser un réseau SDN pour une VM.
- **VM.Allocate** : Créer une nouvelle VM.
- **VM.Audit** : Visualiser les VM et leurs configurations.
- **VM.Backup** : Sauvegarder et restaurer une VM.
- **VM.Clone** : Cloner ou restaurer une VM à partir d'une image.
- **VM.Config.CDRom** : Gérer les lecteurs CD/DVD virtuels.
- **VM.Config.CPU** : Modifier la configuration du processeur.
- **VM.Config.Cloudinit** : Modifier la configuration cloud-init.
- **VM.Config.Disk** : Gérer les disques virtuels.
- **VM.Config.HWType** : Modifier les paramètres matériels de la VM.
- **VM.Config.Memory** : Modifier la mémoire de la VM.
- **VM.Config.Network** : Gérer les interfaces réseau.
- **VM.Config.Options** : Modifier (notamment) les informations du cadre « Notes ».

Les utilisateurs (Qui ?) 5/5

Exemple n°3

Utilisateur pouvant sauvegarder et restaurer (part.2)

Datacenter

Search

Summary

Notes

Cluster

Ceph

Options

Storage

Backup

Replication

Permissions

Users

Add Remove

Path ↑	User/Group/API Token	Role	Propagate
/	ernest@pam	Administrator	true
/	zabbix@pve	Administrator	true
/	ansible_user@pve	PVEAdmin	true
/	api_user@pve	PVEAuditor	true
/	root@pam!evZ2lpM1D7F6K0zc78Ae	Administrator	true
/	api_user@pve!api_user_token	PVEAuditor	true
/sun/zones/localnetwork/vmbr0	chrono_user@pve	VM_User_Save_rest	true
/storage/PBS14200	chrono_user@pve	VM_User_Save_rest	true
/storage/pool0	chrono_user@pve	VM_User_Save_rest	true
/vms/184	chrono_user@pve	VM_User_Save_rest	true

Délégation par pools

Objectif : Appliquer les permissions sur un ensemble de ressources plutôt qu'individuellement.

Resource Pool: chrono			
Summary	Add Remove		
Members	Type ↑	Description	Disk usage...
Permissions	qemu	184 (vmchrono2)	
	qemu	225 (vmchronopool)	
	storage	stor_chrono (pve1380)	19.1 %

Pool : chrono

Des VMs : VM184 · VM225

Un storage : stor_chrono

Permissions : /pool/ chrono

Attribution d'un ou plusieurs

Rôles → utilisateur ou groupe

Backup	/pool/chrono	chrono_user@pve	VM_User_Save_rest
Replication	/storage/PBS14200	chrono_user@pve	VM_User_Save_rest
Permissions			

Quotas : limites natives de Proxmox VE

Proxmox VE **ne propose pas de quota utilisateur global** natif. On ne peut pas limiter un utilisateur à « 500 Go et 8 VM » directement.

Approches de contournement :

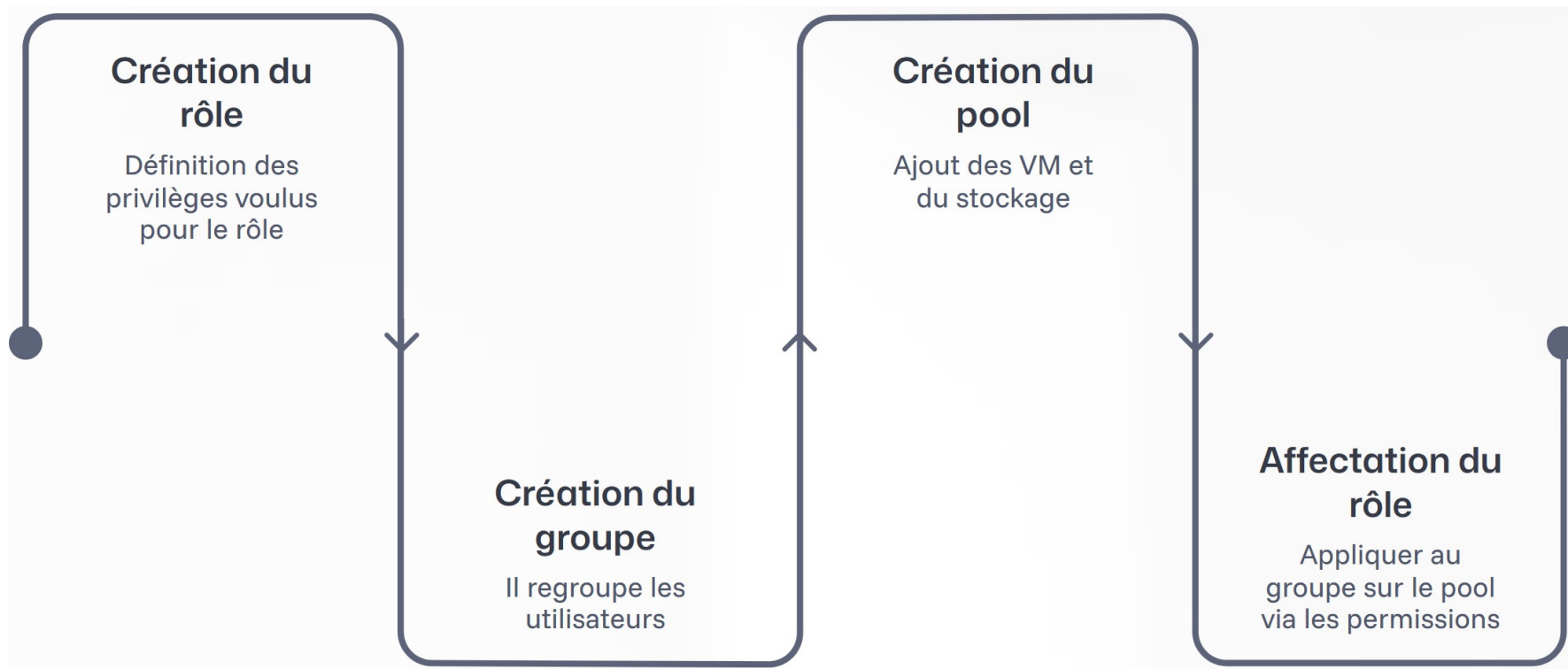
Quotas de stockage

ZFS datasets, CephFS, NFS ou Proxmox Backup Server

Permissions restrictives

Interdire `VM.Allocate` et `Datastore.AllocateSpace`

Résumé : la chaîne de configuration (1/2)



Résumé : la chaîne de configuration (2/2)

Via l'interface (GUI)

Datacenter → Permissions

- Roles → Create
- Groups → Add
- Pools → Add
- Ajouter les permissions sur le pool

Via la CLI

```
pveum role add <nom du rôle> --privs \  
"VM.Audit,VM.Console,VM.PowerMgmt,VM.Snapshot,VM.Backup,VM.Clone,VM.Allocate,VM  
.Config.Options"
```

```
pveum group add <nom du groupe>  
pveum user groupadd user@pve <nom du groupe>
```

```
pveum pool add <nom du pool>  
pvesh set /pools/chrono --vms \ <VMID1>,<VMID2>,<VMID3>  
pvesh set /pools/chrono --storage <nom storage 1>,<nom storage 2>
```

```
pveum acl modify /pool/<nom du pool> -group <nom du groupe> -role <nom du rôle>
```