



Proxmox - environnement d'infrastructure virtualisée pour étudiants

26.11.2023

Leo Pellandini

Introduction

Un environnement d'infrastructure virtualisé pour étudiants. Chaque groupe d'étudiant (environ 10 personnes), doit pouvoir accéder à son infrastructure virtuelle, connectée à un réseau dédié, séparé des autres infrastructures, mais pouvant accéder à Internet par un uplink partagé. L'environnement est utilisé principalement pour faire de la bureautique ou des tâches calcul simples, et doit pouvoir accéder à Internet pour le partage de fichiers.

Pour mettre en œuvre cette stratégie, j'ai choisi de diviser l'environnement en trois pools, attribués à chaque professeur en fonction de l'année scolaire. Chaque professeur est entièrement responsable de son pool, avec la possibilité et la responsabilité de procéder à la maintenance des machines virtuelles à chaque année ou chaque semestre. Ils ont la faculté de créer des sauvegardes et des modèles spécifiques pour leurs élèves, ainsi qu'un accès à leur propre espace de stockage. Bien qu'ils n'aient pas de droits particuliers en matière de gestion des utilisateurs, ils conservent le contrôle sur la gestion de leur espace de stockage, de leur pool ainsi que de leurs VM.

Objectifs

1. Faciliter l'accès des élèves aux ressources requises en anticipant au mieux les variations de "comportement" liées à la création et à la gestion des machines virtuelles.
2. Permettre au professeur d'avoir leur espace par année scolaire ou ils ont presque tous les droits dessus afin qu'ils puissent donner leur cours de la manière la plus adaptée et simple.
Tout en leur fournissant des solutions diverses (comme des backups...) afin qu'ils aient des fonctionnalités adaptés à l'enseignement.

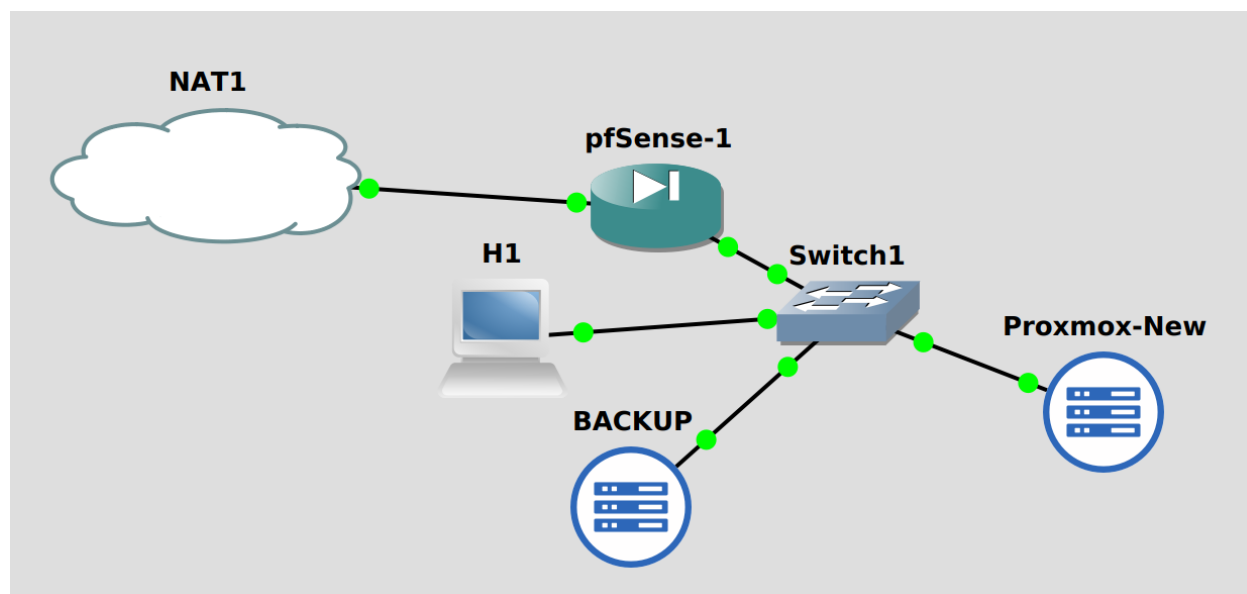
Git

Pour avoir accès au script voici le lien du git :

https://gitedu.hesge.ch/leo.pellandi/tp_proxmox

Topologie

La topologie "physique" est la suivante :



J'ai opté pour une infrastructure qui ressort sur internet via un pfSense afin de pouvoir instaurer des règles en fonction des besoins de l'école par exemple on peut bloquer l'accès à OpenIA (chatGPT) ainsi les étudiants n'auront pas accès à ce genre de site. On peut également mettre des règles pour interdire aux gens de ce réseau de sortir sur internet sur un port qui ne nous convient pas ...

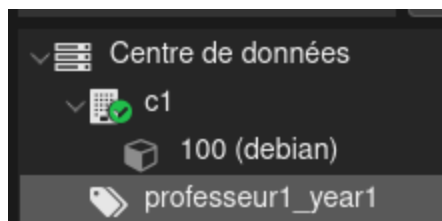
Au sein du LAN, j'ai implémenté un service DHCP avec le pfSense son pool est de 10.9.8.20 - 10.9.8.120 ainsi les machines Proxmox ont une ip statique. Ainsi les nouvelles machines comme H1 (que j'ai utilisé pour configurer le pfsense) se voient distribuées automatiquement d'adresse IP.

Utilisateurs et des groupes

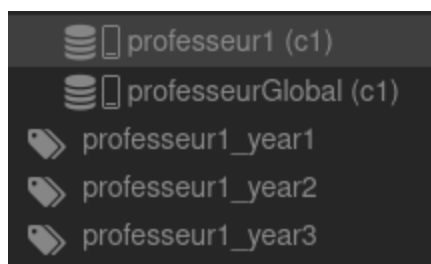
Etant donné qu'il y a "deux" rôles (profs et élèves), j'ai créé un groupe professeur pour les professeurs et un groupe par année (year1, year2, year3). Ainsi chaque prof à des pools annuels et les groupes correspondants eux possèdent les droits d'accès au pool de leur année respective.

year3	user3@pve
year2	user2@pve
year1	user1@pve
professeur	professeur1@pve

Les élèves ont eux accès au VM des pools auquel ils ont accès uniquement :



Quant aux professeurs ils ont accès à leurs pools et leur stockage privé ainsi que leur stockage public :



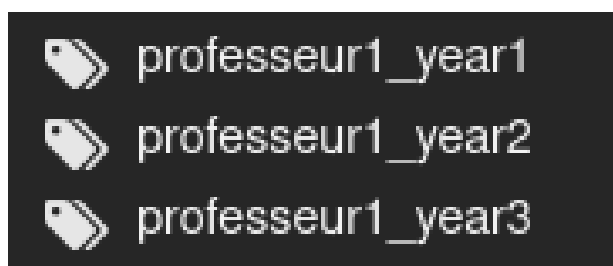
Les machines virtuelles sont créées uniquement par les professeurs, les étudiants peuvent uniquement les utiliser, les cloner et les snapshotés mais pas faire de rollback c'est un privilège attribué au professeur pour éviter les abus.

Pools

J'ai opté pour une gestion des pools assez simple. Etant donné que les professeurs changent moins souvent que les élèves, chaque professeur aurait accès à 3 pools (1 pour chaque année scolaire) et pourrait manager ces 3 pools à sa guise c'est-à-dire que à chaque fin d'année / semestre il serait responsable de supprimer les VM ...

Les professeurs gèrent leur pools par année et ont la responsabilité de gérer leur stockage et leur backup.

Les élèves eux sont attribués à un groupe qui est lui attribué au pool annuel de chaque professeur. Il ne peut qu'exécuter les machines virtuelles et faire des snapshots.



A chaque nouveau professeur il y a 3 nouveaux pools qui lui sont dédiés et réservés.

Permissions

L'outil proxmox permet une gestion des permissions très avancées il y a plusieurs permissions qui permettent de composer des rôles. Voici l'ensemble des privilèges que l'on peut attribuer et leur fonctionnalité.

Privilèges	Fonctionnalités
VM.Snapshot	Permet de créer des instantanés (snapshots) des machines virtuelles (VM) pour enregistrer leur état actuel.
VM.Clone	Autorise la duplication de machines virtuelles.
VM.Console	Accorde l'accès à la console des machines virtuelles, permettant une interaction directe.
Pool.Audit	Autorise l'audit des pools de ressources, offrant une visibilité sur l'utilisation des ressources.
VM.PowerMgmt	Permet la gestion de l'alimentation des machines virtuelles, y compris l'arrêt et le redémarrage.
VM.Audit	Donne la capacité d'auditer les actions effectuées sur les machines virtuelles. offrant une visibilité sur l'utilisation des VM.
Datastore.Allocate, Datastore.AllocateSpace, Datastore.AllocateTemplate, Datastore.Audit	Gère l'allocation d'espace sur les datastores et l'audit des actions liées aux datastores.
Group.Allocate	Autorise l'allocation de groupes.
Mapping.Audit, Mapping.Modify, Mapping.Use	Contrôle l'audit, la modification et l'utilisation des mappages. Permet de mapper le stockage ou les périphériques.
Permissions.Modify	Permet la modification des autorisations, y compris l'attribution et la révocation de droits.
Pool.Allocate	Autorise l'allocation de ressources au niveau du pool. C'est-à-dire la création de pool
Realm.Allocate, Realm.AllocateUser	Gère l'allocation de realms et d'utilisateurs dans les realms. Par exemple (AD-DS, LDAP...)

SDN.Allocate, SDN.Audit, SDN.Use	Gère l'allocation de ressources, l'audit et l'utilisation des Software-Defined Networks
Sys.Audit, Sys.Console, Sys.Incoming, Sys.Modify, Sys.PowerMgmt, Sys.Syslog	Gère divers aspects du système, y compris l'audit, la console, les événements entrants, la modification, la gestion de l'alimentation et le syslog.
User.Modify	Autorise la modification des paramètres des utilisateurs.
VM.Allocate	Permet l'allocation de ressources pour les machines virtuelles. (création)
VM.Backup	Autorise la sauvegarde des machines virtuelles.
VM.Config.CDROM, VM.Config.CPU, VM.Config.Cloudinit, VM.Config.Disk, VM.Config.HWType, VM.Config.Memory, VM.Config.Network, VM.Config.Options	Gère la configuration spécifique des machines virtuelles, y compris le CD-ROM, le CPU, Cloud-init, les disques, le type de matériel, la mémoire, le réseau et les options.
VM.Migrate	Autorise la migration des machines virtuelles entre les nœuds.
VM.Monitor	Permet la surveillance des performances des machines virtuelles.
VM.Snapshot.Rollback	Autorise le retour en arrière (rollback) des instantanés des machines virtuelles.

Voici donc un résumé de tous les privilèges disponibles sur Proxmox. Il faut ensuite créer des rôles et les attribuer au pool, stockage, réseau en les associant à des groupes ou des utilisateurs.

Réseau et permissions

Proxmox offre une administration et une gestion des réseaux assez complète. Pour donner un accès internet aux VMs il faut lier une interface bridée.

Les professeurs doivent avoir accès d'une manière ou d'une autre au réseau en l'occurrence uniquement en utilisation et non pas en création d'interface par exemple. Ainsi ils peuvent bridger leur VM afin qu'elles aient un accès internet.

Pour faire des ports bridgés afin d'avoir un accès internet sur nos VM, il faut faire comme ceci :

Il faut remplacer l'adresse 0.0.0.0 ...

Mais il faut aussi installer le service openvswitch :

```
root@c1:~# sudo systemctl status openvswitch-switch
● openvswitch-switch.service - Open vSwitch
   Loaded: loaded (/lib/systemd/system/openvswitch-switch.service; enabled; preset: enabled)
   Active: active (exited) since Mon 2023-11-06 11:59:47 UTC; 1min 1s ago
   Main PID: 3739 (code=exited, status=0/SUCCESS)
      CPU: 2ms

Nov 06 11:59:47 c1 systemd[1]: Starting openvswitch-switch.service - Open vSwitch...
Nov 06 11:59:47 c1 systemd[1]: Finished openvswitch-switch.service - Open vSwitch.
```

Voici comment faire en ligne de commande :

```
sudo apt update
sudo apt install openvswitch-switch
sudo systemctl start openvswitch-switch
sudo systemctl enable openvswitch-switch
systemctl restart pveproxy
systemctl restart pvedaemon
systemctl restart pvestatd
```

Les professeurs doivent avoir un accès au interface afin de créer leur VM et les bridger afin qu'elles aient un accès internet. Afin qu'ils puissent avoir accès au réseau (bridge...) il faut également qu'ils soient soumis au permission ci-dessous :

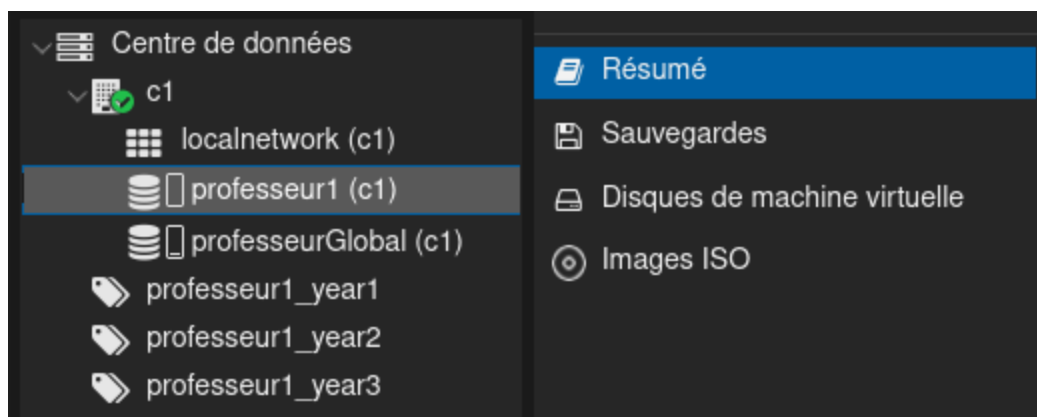
AccesProfNetwork SDN.Audit SDN.Use

AccessProfNetwork est attribué sur le groupe professeur concernant les permissions d'accès au network afin qu'ils puissent bénéficier de l'accès sur les interfaces créé par l'administrateur mais ils ne peuvent pas en créer. Ceci permet une gestion sécurisée du matériel réseau du système et une certaine autonomie de travail pour les professeurs.

Stockage

Chaque professeur à un stockage privé avec uniquement lui en temps que "chef". Les professeurs ont également accès à un stockage partagé entre professeurs où ils peuvent partager leurs modèles ou autres...

Ils ont le rôle PVDatastoreUser qui ne leur permet pas de manager le stockage mais de l'utiliser.



Les professeurs sont aussi PVDatastoreUser sur le stockage dédié au backup.

Permissions sur les pools

Pour gérer de manière optimale les rôles au sein de mes pools j'ai créé moi-même deux rôles. Un pour les élèves et un pour les professeurs :

Pour les élèves, j'ai remarqué que le privilège **VM.allocate** est un rôle qui permet à un utilisateur de créer de nouvelles machines virtuelles au sein de l'infrastructure de virtualisation. Voici ce que ce rôle permet de faire :

1. **Création de VM**
2. **Configuration des paramètres de la VM**
3. **Démarrage et arrêt des VM**
4. **Gestion de l'état de la VM**
5. **Exportation et importation de VM** : En général, ce rôle permet également d'exporter et d'importer des VM, ce qui peut être utile pour la sauvegarde, la migration ou le partage de VM.

Le soucis c'est que les élèves pourraient gérer leur stockage et les ressources comme ils le souhaitent ce qui n'est pas pensable on ne peut pas risquer qu'un élève booste toutes ses machines à fond...

J'ai donc opté pour :

AccesUserPool

Pool.Audit VM.Audit VM.Clone VM.Console VM.PowerMgmt VM.Snapshot

1. **VM.Audit permet de voir les VM d'un pool ou l'utilisateur à les accès**
2. **VM.Clone : Permet de cloner une VM.**
3. **VM.PowerMgmt : Gestion de l'allumage des VM.**
4. **VM.Snapshot : Gestion des snapshots pour les machines virtuelles et offre un niveau de contrôle sur la façon dont ces snapshots sont créés, gérés et utilisés pour la restauration des VM.**
5. **Pool.Audit : Permet aux élèves de voir les pools qui leur sont attribués**

Les snapshots ne risquent pas de générer des problèmes de stockage, c'est une fonctionnalité utile pour les élèves et sans trop de risque.

Pour les professeurs j'ai spécifié ces privilèges :

Il y a les mêmes privilèges que les élèves mais ils peuvent gérer la création, migration, backup des VM. Mais ils ne peuvent pas créer ou gérer les utilisateurs car ce n'est pas leur rôle et nous ne voudrions pas de gestion abusive des utilisateurs.

Les professeurs doivent avoir accès à des privilèges d'utilisateur du datastore sur leur zone de stockage afin de créer des VM.

Voici leur permission en entier.



AccesProfPool	Pool.Audit VM.Allocate VM.Audit VM.Backup VM.Clone VM.Config.CDROM VM.Config.CPU VM.Config.Cloudinit VM.Config.Disk VM.Config.HWType VM.Config.Memory VM.Config.Network VM.Config.Options VM.Console VM.Migrate VM.Monitor VM.PowerMgmt VM.Snapshot VM.Snapshot.Rollback
---------------	--

Ils ne peuvent donc pas créer de pool mais uniquement gérer ceux qui leur sont attribués. Ils ont également la possibilité d'effectuer des rollbacks sur les snapshots créés par les étudiants qui eux ne peuvent pas revenir en arrière car ils pourraient modifier la VM d'un autre camarade... Pour plus d'informations sur la nature de chaque privilège, référez vous au chapitre précédent (ils y sont tous documentés).

Backup server

Pour la gestion des backups j'ai créé un deuxième serveur proxmox où j'ai installé une machine virtuelle Proxmox Backup Server ainsi j'ai pu sur mon serveur proxmox principal lier cette machine de backup lorsqu'on crée un stockage de backup.

PBS est conçu pour s'intégrer parfaitement avec Proxmox Virtual Environment. Cela simplifie la gestion des sauvegardes pour les utilisateurs qui utilisent déjà PVE comme plateforme de virtualisation.

J'ai également appliqué le rôle de PVEdatastoreUser pour le groupe professeur sur ce stockage de Backup ainsi les professeurs peuvent backuper quand ils le souhaitent leur VM. C'est donc leur responsabilité de gérer le backup des VM cela permet une autonomie des professeurs et un coût plus bas pour les admins étant donné qu'ils ne doivent pas gérer cette partie de l'infrastructure.

C'est donc une zone partagée au sein des professeurs ils sont donc totalement responsable de sauver leurs données et de ne pas supprimer ceux des autres.

Sur le serveur de backup j'ai simplement ajouté un datastore nommé "backup" et configuré les adresses ip / gateway basique lors de la création de la machine virtuelle.

Etant donné que seulement les professeurs sont responsables de faire des backups, je n'ai pas instauré de job cron qui vont exécuter un script toutes les X heures afin de sauver l'entièreté du nœud ou autre. Ceci est une des limitations de mon système.

Avantages et limites de l'infrastructure

L'infrastructure est rigoureusement contrôlée, avec pour objectif principal la prévention des abus, tant de la part des élèves que des enseignants. Cette approche présente à la fois des avantages et des limites. D'un côté, la restriction de l'accès à certaines fonctionnalités offre une sécurité accrue et garantit la stabilité du système. De l'autre côté, cependant, elle peut entraver la créativité et l'autonomie de nos utilisateurs.

Dans le contexte éducatif, je considère que cette couche de protection est essentielle, compte tenu de la simplicité d'accès aux machines virtuelles (VM). Un contrôle strict est impératif pour éviter tout abus. Même du côté des enseignants, il est impératif de limiter leur gestion du système, afin d'éviter une multitude de possibilités qui pourraient surcharger l'infrastructure, la rendant dépourvue de structure et de règles claires.

Notons cependant que l'infrastructure présente des limitations en termes de haute disponibilité, en l'absence d'un cluster dédié. Cette décision résulte du domaine d'application spécifique aux écoles, où la mise en place et la maintenance d'une telle infrastructure s'avèreraient financièrement trop onéreuses. Bien que cette limitation soit compréhensible, elle impose des contraintes en matière de redondance et de disponibilité continue.

Un autre point de préoccupation réside dans l'accès généralisé des enseignants au stockage des sauvegardes, ce qui pourrait engendrer des problèmes potentiels. Par exemple, la suppression accidentelle d'une sauvegarde par un enseignant pourrait impacter les données d'un autre enseignant. Afin d'atténuer ce risque, des mesures supplémentaires de contrôle d'accès et de sauvegarde pourraient être envisagées pour garantir l'intégrité des données et prévenir toute perte accidentelle.

Un point de limite très important est au sein du réseau virtuel, je n'ai pas implémenté de pfSense ou de routeur virtuel ce qui implique que les VM doivent avoir des IP statiques et donc on est limité en nombre de VM due au subnet. Il faudrait impérativement implémenter un pfSense virtuel qui servirait de "NAT" pour sortir vers l'extérieur.

Potentiels problèmes de gestion futur / analyse de risque

L'infrastructure Proxmox de l'école peut potentiellement rencontrer plusieurs défis et problèmes à l'avenir, en fonction de l'évolution des besoins.

Voici quelques problèmes potentiels futurs :

Croissance de l'utilisation : Si le nombre d'utilisateurs, de machines virtuelles ou de charges de travail augmente, l'infrastructure pourrait devenir surchargée. Cela pourrait entraîner des problèmes de performances, de capacité de stockage insuffisante, et nécessiterait une mise à l'échelle de l'infrastructure.

Sécurité : Les menaces de sécurité évoluent constamment. Les mises à jour de sécurité régulières et la surveillance constante sont nécessaires pour protéger l'infrastructure contre les nouvelles vulnérabilités. Les accès non autorisés, les failles de sécurité, ou la négligence dans la gestion des autorisations pourraient entraîner des risques importants.

Gestion des sauvegardes : La gestion des sauvegardes doit être robuste pour éviter la perte de données. Des erreurs humaines, telles que la suppression accidentelle de sauvegardes critiques, peuvent poser des problèmes importants. Et également la surcharge du stockage dans le PBS peut poser des soucis.

Évolutivité : Si les besoins de l'école changent ou si de nouveaux services sont requis, l'infrastructure doit être en mesure de s'adapter rapidement. L'évolutivité peut devenir un problème car l'architecture choisie est très encadrée et si les objectifs futurs seraient de laisser plus de liberté au utilisateur cela peut poser problème.

Disponibilité et redondance : La limitation en haute disponibilité mentionnée précédemment peut devenir un problème si des périodes d'indisponibilité sont inacceptables.

Schéma d'amélioration virtuelle et physique

Voici l'infrastructure réseau que j'aimerais mettre en place.

