Mise en réseau Proxmox VE

WIZARDS & DICE

🖉 Créateur : Hugo CLAMOND – Responsable technique
📅 Date de Création : 06/02/2025

🖉 Dernier modificateur : Hugo CLAMOND – Responsable technique
📅 Date de modification : 06/02/2025
🔄 Version : 1.0

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

greta ARDÈCHE - DRÔME
FORMEZ-VOUS À DEMAIN

IUT A Valence
Université Grenoble Alpes

Table des matières

Table des figures

I. Les bridges

Ici sont détaillées les instructions pour configurer les bridges du PVE.
Il faut comprendre ici qu'un bridge est l'équivalent d'un commutateur virtuel sous Hyper-V, ou vSwitch sur Vmware.

A) Configuration

Dans certains cas, il est nécessaire de rattacher un bridge à une interface pour obtenir une connectivité au niveau physique. Par défaut, le bridge "vmbr0", créé directement suite à l'installation du serveur PVE, est rattaché à une interface physique. Cette dernière correspond à l'interface de sortie du PVE vers notre réseau physique.

Si vous souhaitez rattacher le bridge à une interface physique : avant d'entamer les manipulations, veuillez noter l'identifiant de l'interface que vous souhaitez rattacher au bridge. Dans cet exemple, nous prenons "enp3s0". Sinon, passez cette étape.

Cliquez sur le nœud sur lequel configurer le nouveau bridge. Aller dans le menu "Système" → "Réseau". Cliquez sur "Créer" → "Linux Bridge". Renseignez le nom choisi. Si vous souhaitez que le PVE soit accessible depuis une machine connectée au même bridge, vous devrez y renseigner une adresse IP. Si vous souhaitez, plus tard, créer des VLANs rattachés à ce bridge, cochez la case "Gère les VLAN".

Pour rattacher une interface Ethernet au bridge, vous devez y renseigner son identifiant dans le champ "Ports du pont (bridge)". Dans notre exemple, nous prenons alors "enp3s0". Si vous ne souhaitez pas rattacher d'interface au bridge, laissez le champ vide.

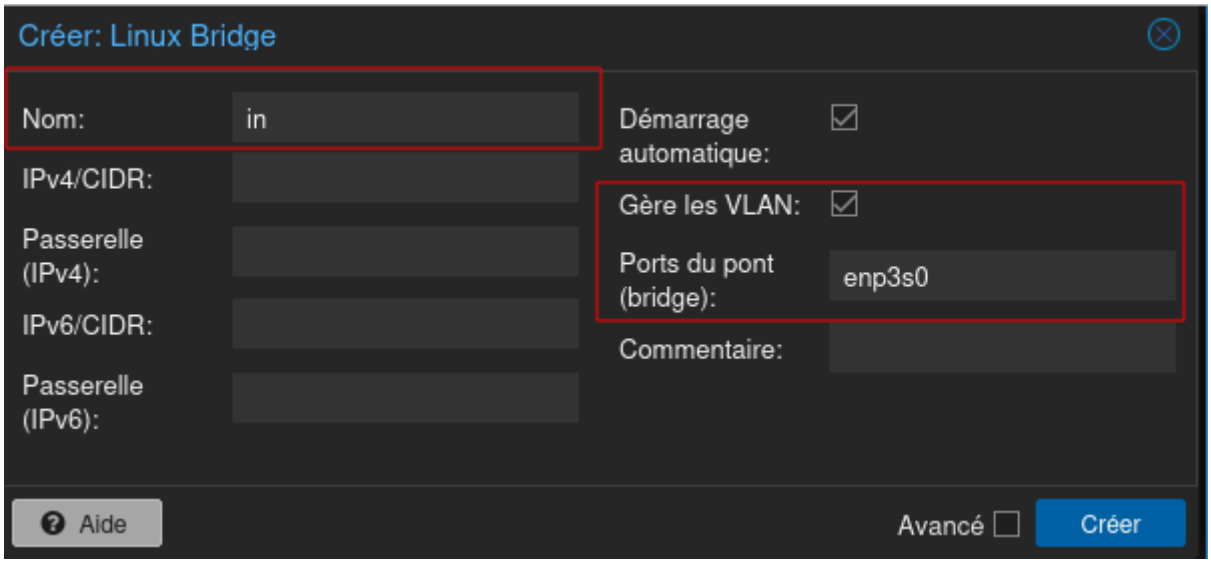

Figure 1: Création d'un bridge

B) Remarques importantes

La configuration des bridges comprend quelques limitations. La plus importante à retenir est qu'un seul bridge, dans tout le nœud, possède une passerelle. Dans notre cas, il s'agit de "vmbr0", notre bridge côté réseau physique. Peut-être n'ai-je pas été assez loin dans la configuration des bridges, mais attribuer une passerelle à un deuxième bridge fait sauter entièrement la connectivité à internet au mieux, la mise en réseau du PVE en elle-même au pire. Donc dans nos "best practices", nous préférerons attribuer la passerelle au bridge de sortie vers le réseau physique.

C) Adresses choisies

Les choix d'adresses IP "physiques" des PVE ont été totalement arbitraires et sont basés sur le déploiement initial effectué chez Hugo, sur son réseau physique 192.168.1.0/24. Ces adresses sont chacune affectées au bridge "vmbr0".

- SRV-PVE-AARD : 192.168.1.217 (chez Hugo)
- SRV-PVE-DRYN : 192.168.0.218 (chez Loïs)

Les PVE se suivaient dans l'adressage d'Hugo, aussi quand SRV-PVE-DRYN a été transféré chez Loïs pour la mise en place "définitive" pour le projet, seul le troisième digit a été changé pour coller au réseau de Loïs. (192.168.0.0/24)

II. Les VLANs

Ici sont détaillées les instructions pour configurer les VLANs d'un bridge.

Pour comparer, un Linux VLAN peut être le parallèle d'un groupe de ports d'un vSwitch sur un Vmware. En effet, le Linux VLAN est souvent rattaché à un bridge ou directement à une interface. Dans notre cas, nous associons uniquement les VLANs à des bridges.

L'intérêt de créer un Linux VLAN est, dans notre cas, de donner la possibilité au VLAN de se connecter au PVE. C'est pourquoi nous créons uniquement un VLAN pour le VLAN SERVERS, étant le seul VLAN à être autorisé à se connecter au PVE.

A) Configuration

Cliquez sur le nœud sur lequel configurer le nouveau bridge. Aller dans le menu "Système" → "Réseau". Cliquez sur "Créer" → "Linux VLAN".

Pour rattacher directement le VLAN à un bridge, il suffit d'entrer le nom du bridge – dans notre exemple, "in" – puis de le suivre par ".X", X correspondant à l'ID du VLAN. Renseignez l'adresse IP que doit prendre le VLAN et qui sera rattachée au PVE.

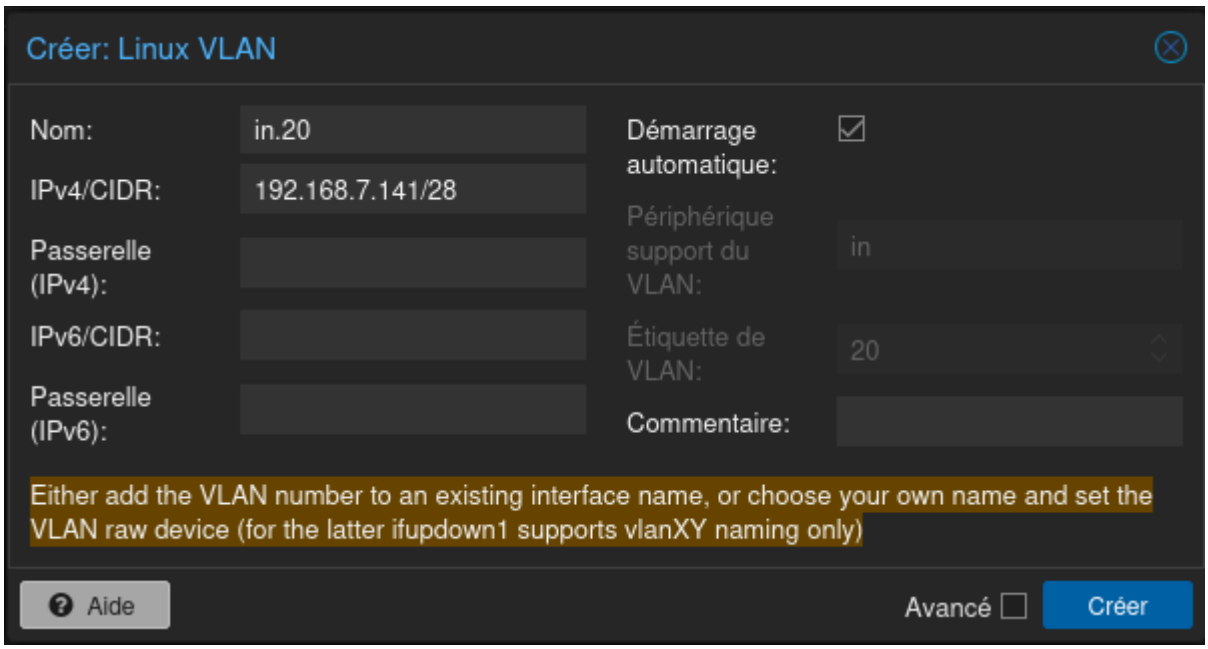

Figure 2: Création d'un Linux VLAN

B) Remarques importantes

Créer un Linux VLAN n'est pas la même chose que créer un bridge : il n'est pas possible de sélectionner le VLAN créé lors de la configuration d'une interface sur un hôte virtuel, lors de la création d'une VM par exemple.

C) Conclusion sur les bridges et VLANs

Nous obtenons donc la liste d'interfaces virtuelles suivante, donc des bridges et des VLANs.

Nom ↑	Type	Actif	Démarr…	Gère le…	Ports/escla…	Mode d'agr…	CIDR	Passerelle	Commentaire
dmz_priv	Linux Bridge	Oui	Oui	Non					
dmz_pub	Linux Bridge	Oui	Oui	Oui					
enp0s31f6	Carte réseau	Oui	Non	Non					
enp3s0	Carte réseau	Oui	Non	Non					
in	Linux Bridge	Oui	Oui	Oui	enp3s0				
in.20	Linux VLAN	Oui	Oui	Non			192.168.7.141/28		
vmbr0	Linux Bridge	Oui	Oui	Non	enp0s31f6		192.168.1.217/24	192.168.1.254	

Figure 3: Bridges et VLANs de SRV-PVE-AARD

III. Règles de pare-feu

Donner la possibilité au VLAN SERVERS d'accéder à l'interface web du PVE, c'est ouvrir une porte sur le réseau physique à l'aide du shell du PVE, et ce, sans que le trafic passe par le firewall ! C'est en effet une faille de sécurité majeure, et le pare-feu intégré au PVE est là pour y remédier.

Pour visualiser les règles de filtrage, cliquez sur le nœud visé → "Pare-feu". Pour ajouter une règle de pare-feu, cliquez simplement sur "Ajouter" sur l'interface. Pour vérifier que le service de pare-feu est bien actif, rendez-vous dans "Pare-feu" → "Options" et vérifiez que la ligne "Pare-feu" est sur "Oui". Si ce n'est pas le cas, cliquez sur la ligne puis sur "Éditer", ou double cliquez dessus, puis cochez l'unique option qui s'offre à vous.

Sur chaque nœud, nous trouverons l'ensemble de règles ci-dessous, règles qui ont pour fonction d'empêcher tout trafic de partir sur les réseau physiques en ping, ce qui empêche les scans d'IP. Les pings vers internet restent possibles et on autorise l'accès à l'interface web du PVE (TCP 8006) pour continuer à manager. La règle de block all à la fin permet le déboguer en cas de problème et rejette tout trafic n'ayant pas été explicitement autorisé ou bloqué par les règles d'au-dessus.

	Act	Type	Action	Macro	Interface	Protoc…	Source	Port s…	Destination	Port d…	Niveau de j…	Commentaire
0	☑	out	DROP		wg0	icmp			192.168.0.…		nolog	
1	☑	out	DROP		vmbr0	icmp			192.168.1.…		nolog	
2	☑	out	ACCEPT		in.20						nolog	
3	☑	out	ACCEPT		vmbr0	icmp					nolog	
4	☑	out	ACCEPT		vmbr0	udp				53	nolog	
5	☑	out	ACCEPT		vmbr0	tcp				443	nolog	
6	☑	out	ACCEPT		vmbr0	tcp				80	nolog	
7	☑	in	ACCEPT		in.20	icmp					nolog	
8	☑	in	ACCEPT		vmbr0	icmp					nolog	
9	☑	in	ACCEPT		in.20	tcp	192.168.7.…		192.168.7.…	8006	nolog	
10	☑	in	ACCEPT		vmbr0	tcp			192.168.1.…	8006	nolog	
11	☐	in	ACCEPT		vmbr0	tcp	192.168.27…		192.168.1.…	8006	nolog	
12	☑	in	ACCEPT		vmbr0	tcp	192.168.1.…		192.168.1.…	22	nolog	
13	☑	in	ACCEPT		vmbr0	tcp	192.168.27…		192.168.1.…	22	nolog	
14	☑	in	ACCEPT		in.20	tcp	192.168.7.…		192.168.7.…	22	nolog	
15	☑	out	REJECT								debug	

Figure 4: Règles de pare-feu de SRV-PVE-AARD