

UTILISER LXC SUR PROXMOX



LXC, ou Linux Containers, est une **technologie de virtualisation légère** qui permet d'exécuter plusieurs environnements d'exploitation Linux isolés (conteneurs) sur un serveur Proxmox hôte (ou une machine Debian hôte). Contrairement aux machines virtuelles traditionnelles, les conteneurs LXC partagent le même noyau du système d'exploitation de l'hôte, ce qui les rend plus efficaces en termes de ressources et plus rapides à démarrer.

Les avantages des conteneurs LXC :

1. **Efficacité des ressources** : En partageant le noyau de l'hôte, les conteneurs LXC utilisent moins de ressources matérielles par rapport aux machines virtuelles, ce qui permet de maximiser l'utilisation du matériel.
2. **Démarrage rapide** : Les conteneurs LXC se lancent en quelques secondes, ce qui les rend idéaux pour le déploiement rapide d'applications.
3. **Isolation légère** : Bien que les conteneurs partagent le noyau, ils restent isolés les uns des autres, garantissant une sécurité et une stabilité adéquates.

1 – AJOUT D'UN MODELE LXC SUR PROXMOX VE

Afin d'utiliser les conteneurs LXC sur Proxmox VE, il est nécessaire de disposer de « **modèles** ». Pour cela, suivez les indications ci-dessous :

- Connectez-vous à l'interface de gestion de votre serveur Proxmox
- Dans le volet de gauche, cliquez sur « **Local** » et, dans le volet de droite, sur « **Modèles de conteneurs** »
- Cliquez le bouton « **Modèles** » ; une fenêtre affiche de nombreux modèles disponibles :

Type	Paquet	Version	Description
Section: mail (2 items)			
lxc	proxmox-mailgateway-7.3-standard	7.3-1	Proxmox Mailgateway 7.3
lxc	proxmox-mail-gateway-8.2-standard	8.2-1	Proxmox Mail Gateway 8.2
Section: system (19 items)			
lxc	rockylinux-9-default	20240912	LXC default image for rockylinux-9
lxc	debian-11-standard	11.7-1	Debian 11 Bullseye (standard)
lxc	opensuse-15.6-default	20240910	LXC default image for opensuse-15.6
lxc	ubuntu-22.04-standard	22.04-1	Ubuntu 22.04 Jammy (standard)
lxc	alpine-3.19-default	20240207	LXC default image for alpine-3.19 (20240207)
lxc	fedora-41-default	20241118	LXC default image for fedora-41 (20241118)
lxc	devuan-5.0-standard	5.0	Devuan 5 (standard)
lxc	ubuntu-24.04-standard	24.04-2	Ubuntu 24.04 Noble (standard)
lxc	fedora-40-default	20240909	LXC default image for fedora-40 (20240909)

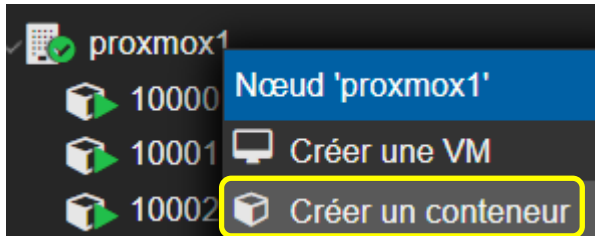
De nombreux modèles sont disponibles et regroupés dans des catégories dont « **System** » et « **TurnKey** ».

- Dans la section « **System** », cliquez le modèle « **debian-12-standard** »
- Cliquez le bouton bleu « **Télécharger** » et patientez pendant le téléchargement du modèle

2 – CREATION D'UN CONTENEUR LXC SUR PROXMOX

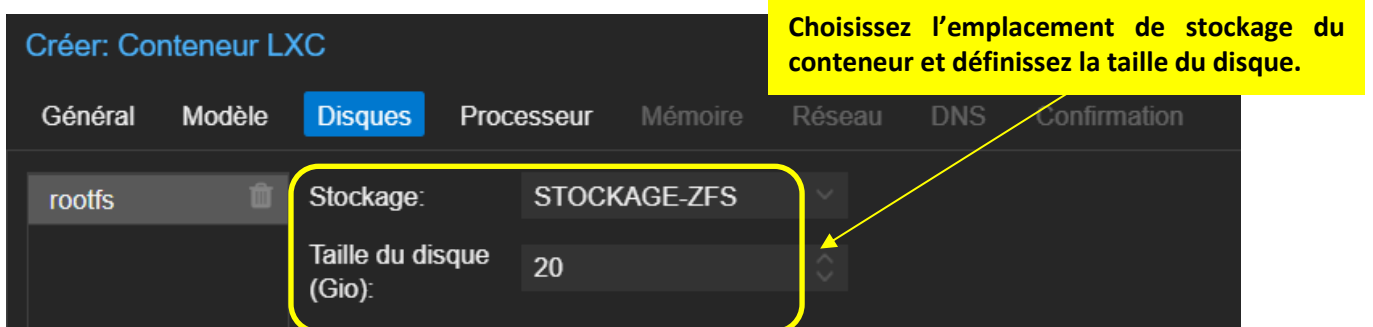
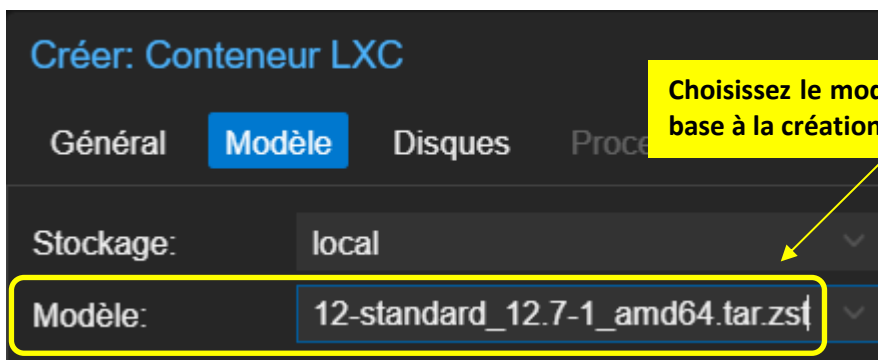
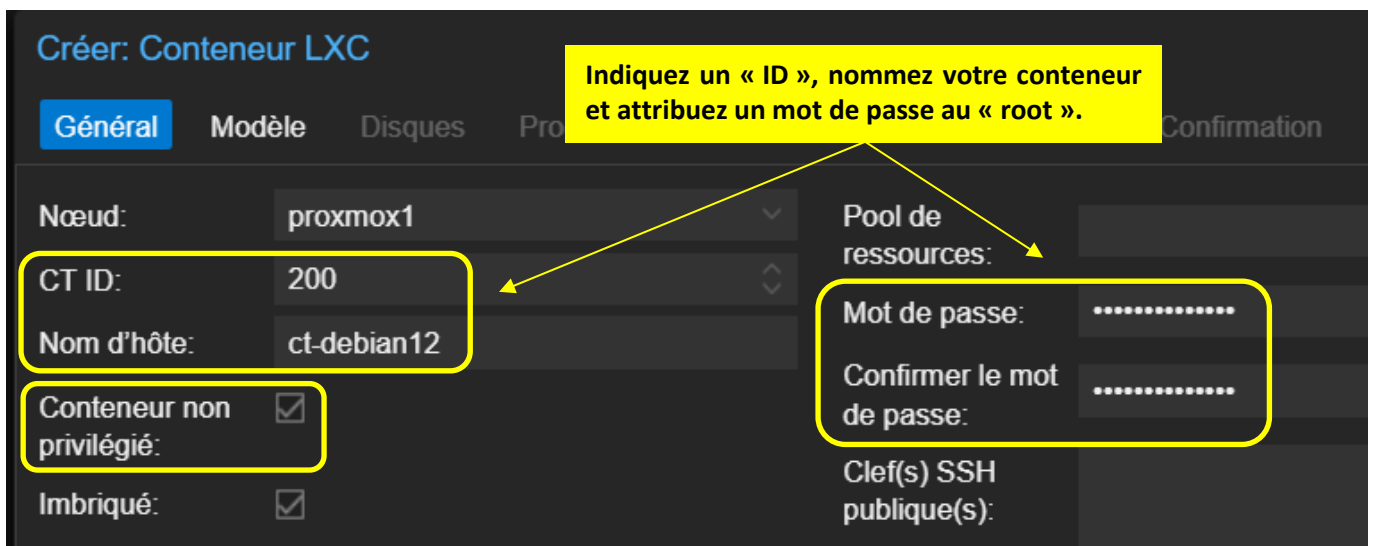
Une fois le modèle « debian-12-standard » téléchargé, nous devons créer le conteneur LXC correspondant sur l'hôte Proxmox de la manière suivante :

- Depuis l'interface de gestion de votre serveur Proxmox, cliquez, en haut à droite, le bouton « **Créer un conteneur** » ; il est possible, également, de faire un clic droit sur le nom du nœud Proxmox et de cliquer « **Créer un Conteneur** » :



Faites un clic droit sur le nom du nœud Proxmox afin de créer un nouveau conteneur.

Un assistant s'affiche ; complétez les fenêtres des différentes étapes (en cliquant « **Suivant** » à chaque fois) :



Créer: Conteneur LXC

Général Modèle Disques **Processeur** Mémoire Réseau DNS Confirmation

Cœurs: 1

Attribuez le nombre de cœurs souhaités (en fonction du modèle installé).

Créer: Conteneur LXC

Général Modèle Disques Processeur **Mémoire** Réseau DNS Confirmation

Mémoire (MiB): 1024

Spécifiez la taille de la mémoire vive que vous souhaitez allouer au conteneur.

Espace d'échange (swap) (MiB): 512

Créer: Conteneur LXC

Général Modèle Disques Processeur Mémoire **Réseau** DNS Confirmation

Vous pouvez spécifier, ici, une adresse statique ou dynamique selon votre architecture réseau.

Nom: eth0

Adresse MAC: auto

Pont (bridge): vmbr1

Étiquette de VLAN: aucun VLAN

Pare-feu:

Donnez un nom à votre interface réseau (eth0 par défaut) et sélectionnez le vmbr adéquat.

IPv4: Statique DHCP

IPv4/CIDR:

Passerelle (IPv4):

IPv6: Statique DHCP SLAAC

Créer: Conteneur LXC

Général Modèle Disques Processeur Mémoire Réseau **DNS** Confirmation

Domaine DNS: utiliser les valeurs de l'hôte

Serveurs DNS: utiliser les valeurs de l'hôte

Nous avons laissé, ici, les valeurs de l'hôte (mais vous pouvez les modifier si nécessaire).

Créer: Conteneur LXC

Général Modèle Disques Processeur Mémoire Réseau DNS **Confirmation**

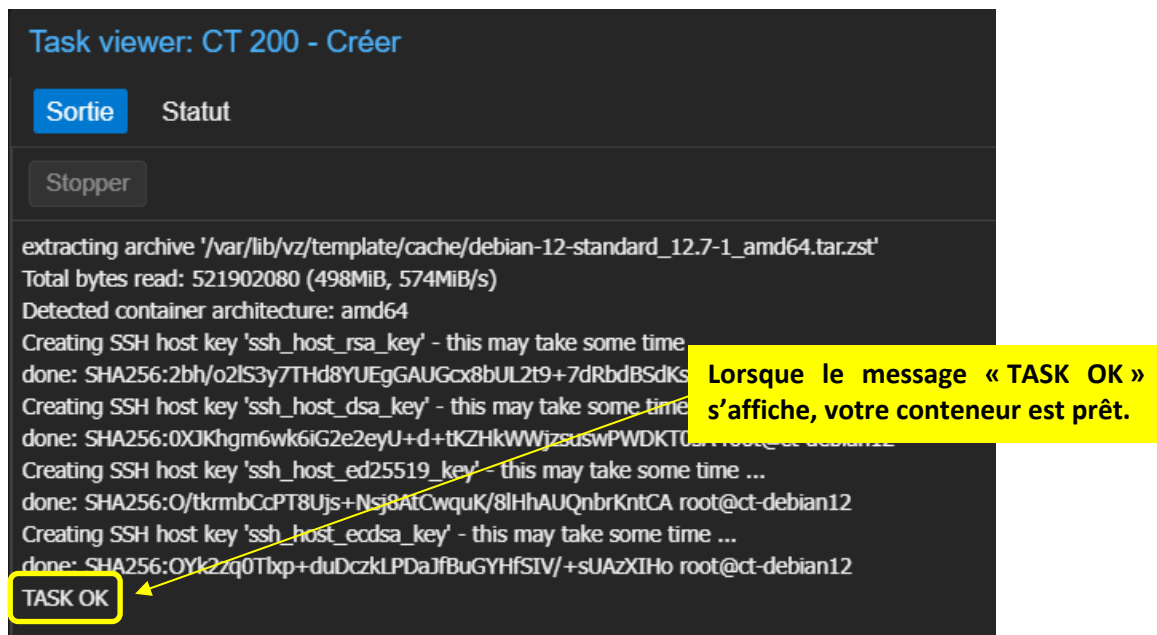
Key	Value
cores	1
features	nesting=1
hostname	debian.12
memory	1024
net0	name=eth0,bridge=vmbr1,ip=dhcp
nodename	proxmox1
ostemplate	local:virt/Debian-12-standard_12.7.1_arm64.tar.xz
passwd	
rootfs	STORAGE:253-20
sub-public-keys	
swap	512
unprivileged	1
vmid	200

Démarrer après création

Avancé Retour

Vérifiez votre configuration et, si tout est correct, cliquez le bouton « Terminer » pour lancer la création du conteneur sur votre serveur Proxmox.

Patientez pendant la création du conteneur jusqu'à l'obtention du message « **Task OK** » :

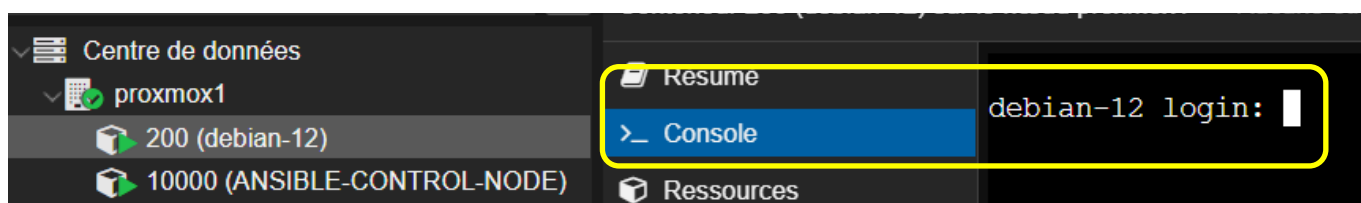


Une fois le conteneur créé dans l'interface de gestion de Proxmox, faites-le démarrer. Pour cela, vous pouvez procéder ainsi :

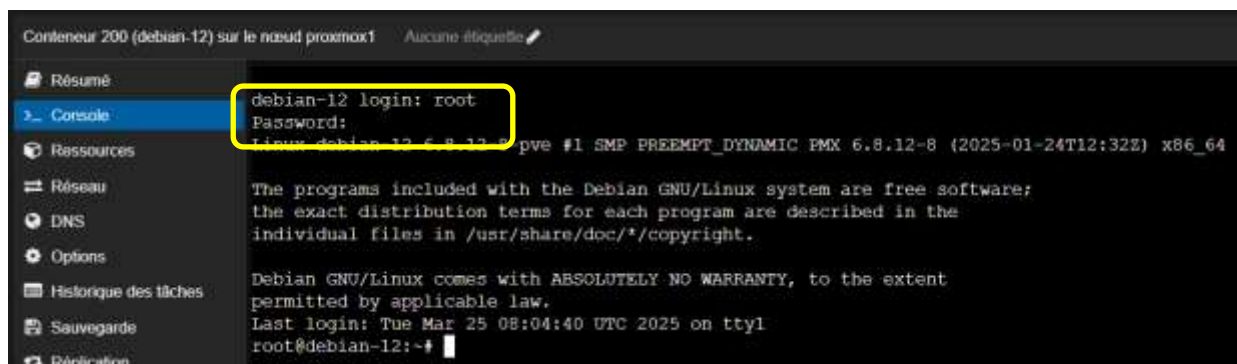
- Faites un clic droit sur le conteneur et cliquez « Démarrer » :



- Si vous cliquez sur « **Console** » dans le volet de droite, vous verrez l'affichage du login de votre machine Debian (si vous ne voyez pas le login, pressez la touche « Entrée » une fois) :



- Saisissez vos identifiants de connexion « **root** » ; vous êtes logué à votre conteneur :



- Saisissez la commande « **ip a** » afin de vérifier que votre conteneur a bien reçu une adresse dynamique de votre routeur IPFire (réseau LAN 192.168.10.xxx) :

```

root@debian-12:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
   inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
   inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0@if25: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
   link/ether bc:24:11:07:9a:55 brd ff:ff:ff:ff:ff:ff
   inet 192.168.10.5/24 brd 192.168.10.255 scope global dynamic eth0
       valid_lft 3383sec preferred_lft 3383sec
   inet6 fe80::be24:11ff:fe07:9a55/64 scope link
       valid_lft forever preferred_lft forever

```

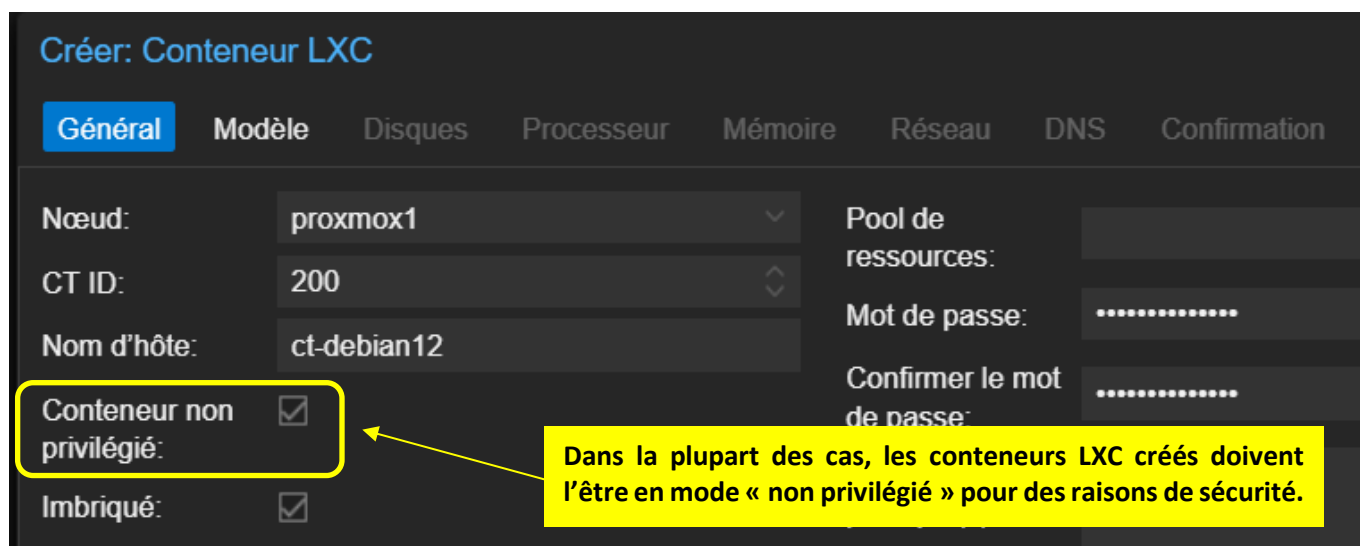
Notre conteneur a bien reçu une adresse IP dynamique de notre routeur IPFire.

On constate, dans la capture ci-dessus, qu’une carte réseau virtuelle nommée « **eth0** » a bien été ajoutée et que l’adresse IP dynamique affectée correspond bien à l’étendue DHCP de notre réseau local.

Le conteneur est donc bien dans notre réseau local (derrière notre IPFire) et non dans un réseau bridgé comme Docker (adresse de type 172.17.0.xxx). A partir de cet instant, vous disposez d’une machine Debian fonctionnelle.

3 – CONTENEUR NON PRIVILEGIE ET PRIVILEGIE : QUELLE DIFFERENCE

Lors de la création du conteneur, l’option « **Conteneur non privilégié** » était cochée par défaut :



Les conteneurs LXC (Linux Containers) sur Proxmox peuvent être configurés en mode privilégié ou non privilégié. Voici les principales différences entre les deux modes :

Conteneur Privilégié

- **Accès Complet aux Ressources** : Un conteneur privilégié a accès à toutes les fonctionnalités du noyau Linux et peut exécuter des opérations qui nécessitent des privilèges élevés.
- **Sécurité** : Moins sécurisé car il peut potentiellement affecter l'hôte et d'autres conteneurs.
- **Utilisation** : Idéal pour des applications qui nécessitent un accès direct au matériel ou des fonctionnalités spécifiques du noyau.

Exemples d'utilisation du mode privilégié :

1. **Applications nécessitant un accès direct au matériel** : Par exemple, des applications de virtualisation imbriquée ou des outils de diagnostic matériel.
2. **Applications nécessitant des fonctionnalités spécifiques du noyau** : Par exemple, des modules noyau spécifiques ou des configurations réseau avancées.

Conteneur Non Privilégié (option par défaut à choisir dans la plupart des cas)

- **Accès Restreint** : Un conteneur non privilégié a des restrictions sur les opérations qu'il peut effectuer, ce qui limite les risques de sécurité.
- **Sécurité** : Plus sécurisé car il isole mieux le conteneur de l'hôte et des autres conteneurs.
- **Utilisation** : Adapté pour la plupart des applications standard qui n'ont pas besoin d'accès direct au matériel ou de fonctionnalités spécifiques du noyau.

Exemples d'utilisation du mode non privilégié :

1. **Serveurs Web** : Hébergement de sites web ou d'applications web.
2. **Bases de Données** : Exécution de bases de données comme MySQL.
3. **Applications de Développement** : Environnements de développement et de test pour des applications logicielles.

Le choix entre un conteneur privilégié et non privilégié dépend des besoins spécifiques de l'application que vous souhaitez exécuter. **Pour des raisons de sécurité, il est généralement recommandé d'utiliser des conteneurs non privilégiés.**

4 – A PROPOS DE L'OPTION CONTENEUR IMBRIQUE

L'option "conteneur imbriqué" (ou "nested container") lors de la création d'un conteneur LXC sur Proxmox **permet d'exécuter des conteneurs ou des machines virtuelles à l'intérieur d'un conteneur existant.**

Un conteneur imbriqué permet :

- **De faire fonctionner la « virtualisation Imbriquée »** : cela permet d'exécuter des hyperviseurs ou des conteneurs à l'intérieur d'un conteneur LXC. Cela signifie que vous pouvez avoir une machine virtuelle ou un autre conteneur fonctionnant à l'intérieur de votre conteneur LXC principal.
- **De faire de l'isolation** : l'isolation offre une couche supplémentaire qui peut être utile pour des environnements de test ou de développement.

Exemples d'utilisation du mode conteneur imbriqué :

1. **Environnements de Développement** : Permet aux développeurs de tester des configurations complexes sans affecter l'hôte principal. Par exemple, tester des applications qui nécessitent leur propre environnement de conteneurisation.
2. **Formation et Éducation** : Utilisé pour des laboratoires de formation où les étudiants peuvent expérimenter avec des conteneurs ou des machines virtuelles sans risquer de perturber l'infrastructure principale.
3. **Tests de Sécurité** : Permet de créer des environnements isolés pour tester des configurations de sécurité ou des scénarios d'attaque sans compromettre l'hôte principal.