

KB - Cyber - OPNsense

- [KB-OPNSense - Réinitialiser l'accès à la webUI](#)
- [KB-OPNsense - Bind LDAP Active directory 2025](#)
- [KB - OPNSense - Interface web injoignable sur proxmox](#)

KB-OPNSense - Réinitialiser l'accès à la webUI

Applicable à : OPNsense > 9.*

Symptôme(s)

Suite à un changement dans le paramétrage de l'interface web d'administration (certificats, port, etc...).

Lors de la connexion à la webUI, impossible d'afficher la page.

Problème

Une erreur ou mauvaise application de la configuration empêche le service web de redémarrer correctement.

Solution

Prérequis : un accès au shell ou en SSH.

Se connecter au shell ou ssh.

Entrer la commande :

```
systemctl webui restart renew
```

Cela va forcer une réinitialisation du paramétrage de la webUI est remettre un certificat autosigné.

Sources

[WebGui access reset — OPNsense documentation](#)

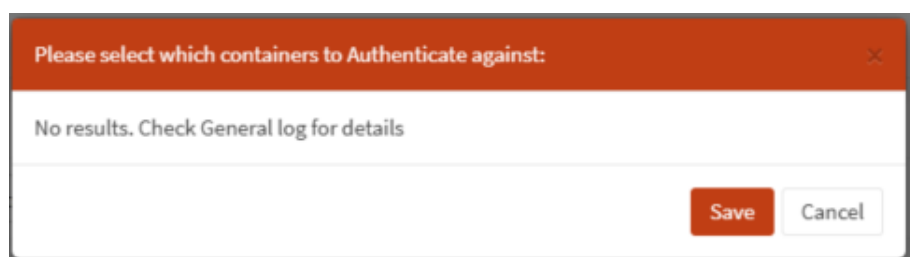
KB-OPNsense - Bind LDAP

Active directory 2025

Applicable à : OPNsense + Active directory (Windows Server 2025)

Symptôme(s)

Impossible d'établir une connexion LDAP ou LDAPS depuis l'OPNsense.



Date	Severity	Process	Line
2026-08-31T18:57:17	Error	opnsense	LDAP bind error [; Can't contact LDAP server]

Problème

Les nouvelles politiques de sécurités sur Windows Server 2025 sont trop restrictives et empêchent les clients linux / BSD de se connecter autrement qu'en LDAPS en ayant préalablement importé le certificat de la CA dans les trusts.

Solutions

1. Terminer la configuration LDAPS et importer le certificat de la CA dans '**trust --> certificates**'
2. Appliquer la solution de contournement ci-dessous :

Sur le serveur Active Directory, modifier la GPO '**Default Domain Policy**'.

```
=Computer Configuration
====Policies
=====Windows Settings
=====Security Settings
=====Local Policies
=====Security Options
=====Domain controller: LDAP server channel binding token
requirements: "When Supported"
=====Domain controller: LDAP server signing requirements: "None"
=====Domain controller: LDAP server Enforce signing requirements:
"Disabled"
=====Network security: LDAP client encryption requirements: "Negotiate
Sealing"
=====Network security: LDAP client signing requirements: "Negotiate
Signing"
```

Sources

[Unable to connect to LDAP \(Windows Server 2025\)](#)

KB - OPNSense - Interface web injoignable sur proxmox

Applicable à : OPNsense / PfSense toutes version

Symptôme(s)

Lors de l'utilisation du SDN sur proxmox (zones et vlan), Impossible d'accéder à l'interface web d'administration de l'OPNsense ou PfSense.

L'équipement réponds au Ping,

```
C:\Users\Administrator>ping 172.20.0.254

Pinging 172.20.0.254 with 32 bytes of data:
Reply from 172.20.0.254: bytes=32 time<1ms TTL=64
Reply from 172.20.0.254: bytes=32 time<1ms TTL=64
```

Le port réponds ouvert au test de connexion.

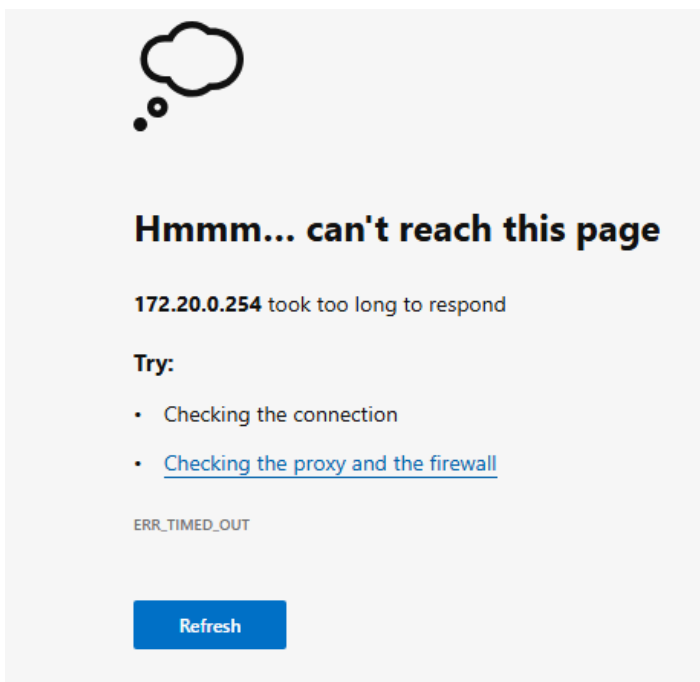
```
PS C:\Users\Administrator> Test-netconnection -ComputerName 172.20.0.254 -p 443

ComputerName      : 172.20.0.254
RemoteAddress     : 172.20.0.254
RemotePort        : 443
InterfaceAlias    : Ethernet
SourceAddress     : 172.20.0.1
TcpTestSucceeded  : True
```

Internet est accessible.

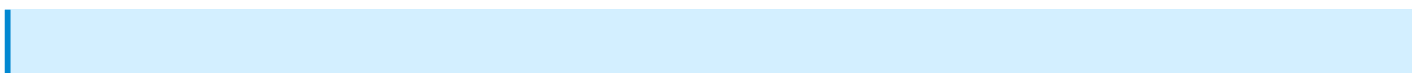


Mais la page d'administration est en timeout.



Problème

Le problème n'est pas entièrement compris à ce jour.



Information : Le problème se situe toutefois côté client et non côté OPNsense

L'hypothèse retenue est la suivante :

Afin de gérer la couche virtuelle de son réseau, le proxmox définit des plages d'adresses MAC pour ses bridges :

Exemples (vmbri0) :

virtio=BC:24:11:E3:A4:FB

virtio=BC:24:11:C8:C9:77

virtio=BC:24:11:81:AC:FD

Dans le cas de l'utilisation du SDN, Une réservation de plage est faite et attribuée au vswitch.

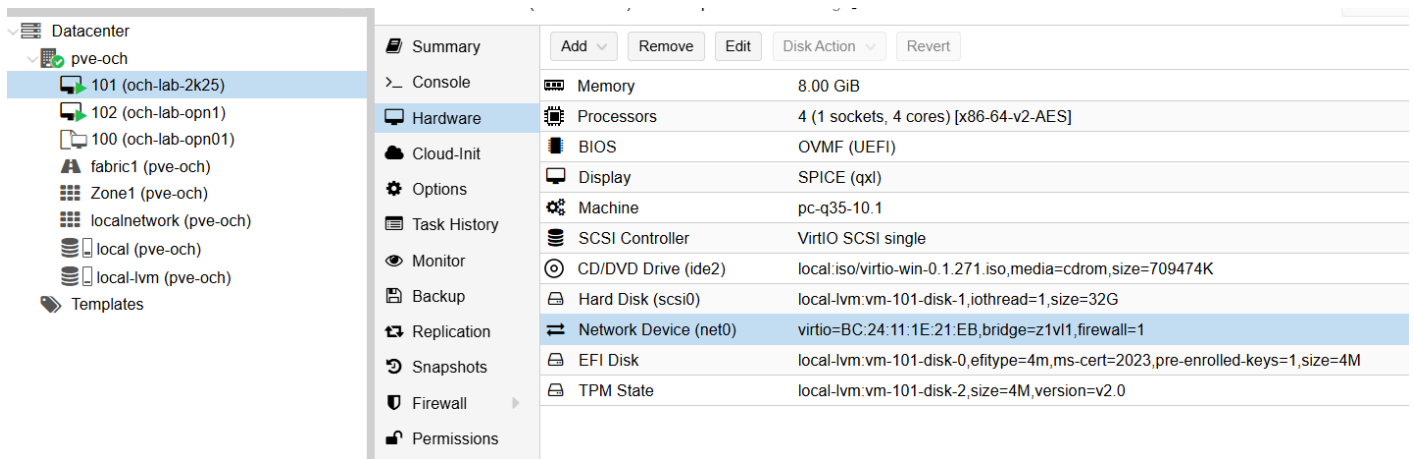
L'adresse MAC se trouve donc en dehors de la plage connue, ce qui doit créer un conflit sur l'OPNsense.

Si cela ne pose pas directement de problème sur le plan réseau (mise à jour des cache ARP), ce qui explique que le dysfonctionnement ne soit pas perceptible de la couche 1 à 3, il doit y avoir une vérification de sécurité sur l'interface web qui pose problème et détecte une incohérence au niveau de l'adresse MAC.

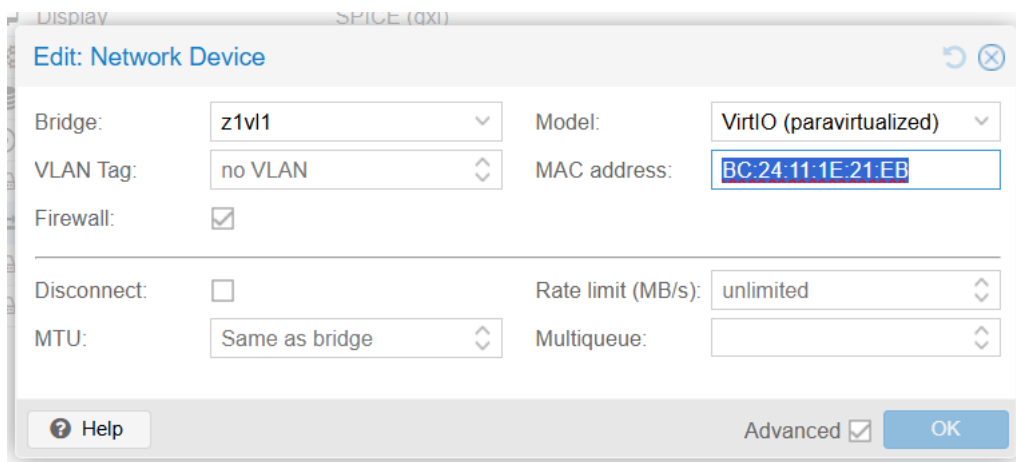
Solution

Prérequis : Accès à l'hyperviseur avec des droits suffisants sur le SDN.

Se connecter sur l'interface web du proxmox. Puis sur la page '**Hardware**' de la machine client concernée par le problème,



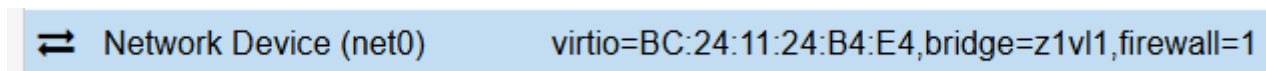
Editer les paramètres de la carte réseau, vérifier que la machine est bien sur le bon vlan :



Sélectionne et supprimer l'adresse MAC. Celle-ci repasse en '**Auto**'. Puis cliquer sur '**OK**'.

MAC address:

Cela va forcer l'interface à renouveler sa MAC address et ainsi lui en attribuer une présente dans la plage de réservation



Suite à ce changement, l'interface web est de nouveau accessible.



Username:

Password:

Login

OPNsense (c) 2014-2026 Deciso B.V.

Sources

Solution trouvée par **Ludwig.W - SIO2 (2026)** dans le cadre du programme BUG BOUNTY.