COMPTE RENDU TECHNIQUE - AP 16

Techniciens : Killian Goncalves & Cristopher Boni Fuentes Groupe : 8 Date : Février 2026

Mission 0 : Prérequis et contraintes

- **Répartition des tâches :** Utilisation d'un diagramme de Gantt(lien Gantt) pour planifier les durées et la répartition entre les membres de l'équipe (Killian et Cristopher).

- **Mise à jour du schéma réseau :** Intégration des nouvelles machines virtuelles (Grafana, Prometheus, WebDAV) dans la topologie existante(lien shema).

la, configuration srv samba avec le nom changé et une ip fixe

```
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
sio@Srvsamba:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
    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: ens18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gro
    link/ether bc:24:11:bc:af:5b brd ff:ff:ff:ff:ff:ff
    altname enp0s18
    altname enxbc2411bcaf5b
    inet 192.168.11.121/24 brd 192.168.11.255 scope global ens18
       valid_lft forever preferred_lft forever
    inet6 fe80::be24:11ff:febc:af5b/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
sio@Srvsamba:~$ _
```

```
  GNU nano 8.4
127.0.0.1       localhost
192.168.11.121  Srvsamba

# The following lines are des
::1     localhost ip6-localho
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

```
  GNU nano 8.4
Srvsamba
```

referencement glpi -agent des serveurs
un wget pour installer le paquet

```
root@Srvsamba:/tmp# wget https://github.com/glpi-project/glpi-ag
ent/releases/download/1.15/glpi-agent-1.15-linux-installer.pl
--2026-03-17 16:04:30--  https://github.com/glpi-project/glpi-ag
ent/releases/download/1.15/glpi-agent-1.15-linux-installer.pl
Connexion à 172.16.0.51:8080… connecté.
requête Proxy transmise, en attente de la réponse… 302 Found
Emplacement : https://release-assets.githubusercontent.com/githu
b-production-release-asset/228588138/142ae593-88c1-40c5-b393-cb0
```

avecc chmod on lui donne des droit

```
root@Srvsamba:/tmp# chmod +x glpi-agent-1.15-linux-installer.pl
```

on lance le glpi-agent et on lui donne l'adresse du serveur

```
er.pl
root@Srvsamba:/tmp# ./glpi-agent-1.15-linux-installer.pl
Installing glpi-agent v1.15...
glpi-agent is about to be installed as service

Provide an url to configure GLPI server:
> 192.168.13.19
```

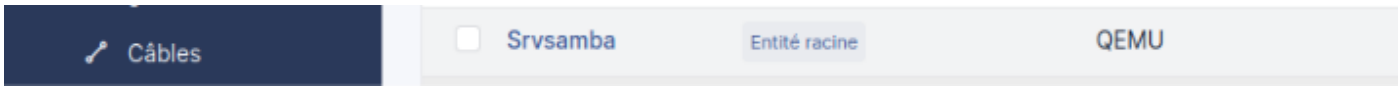
on redemarre et on active le glpi agent

```
root@cliSamba:/tmp# systemctl restart glpi-agent
root@cliSamba:/tmp#  systemctl enable glpi-agent
```

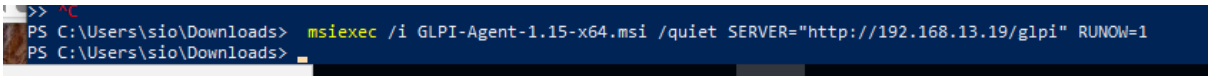
puis on force l'installation

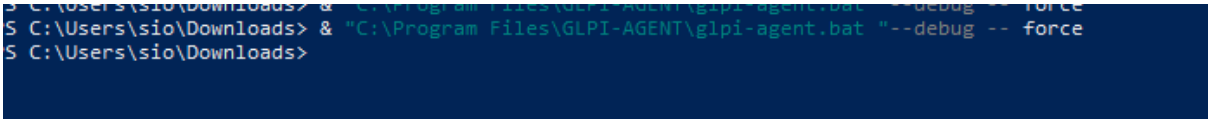
```
root@cliSamba:/tmp#  glpi-agent --debug --force
[debug] Logger backend Stderr initialized
[debug] GLPI Agent (1.15-1)
```

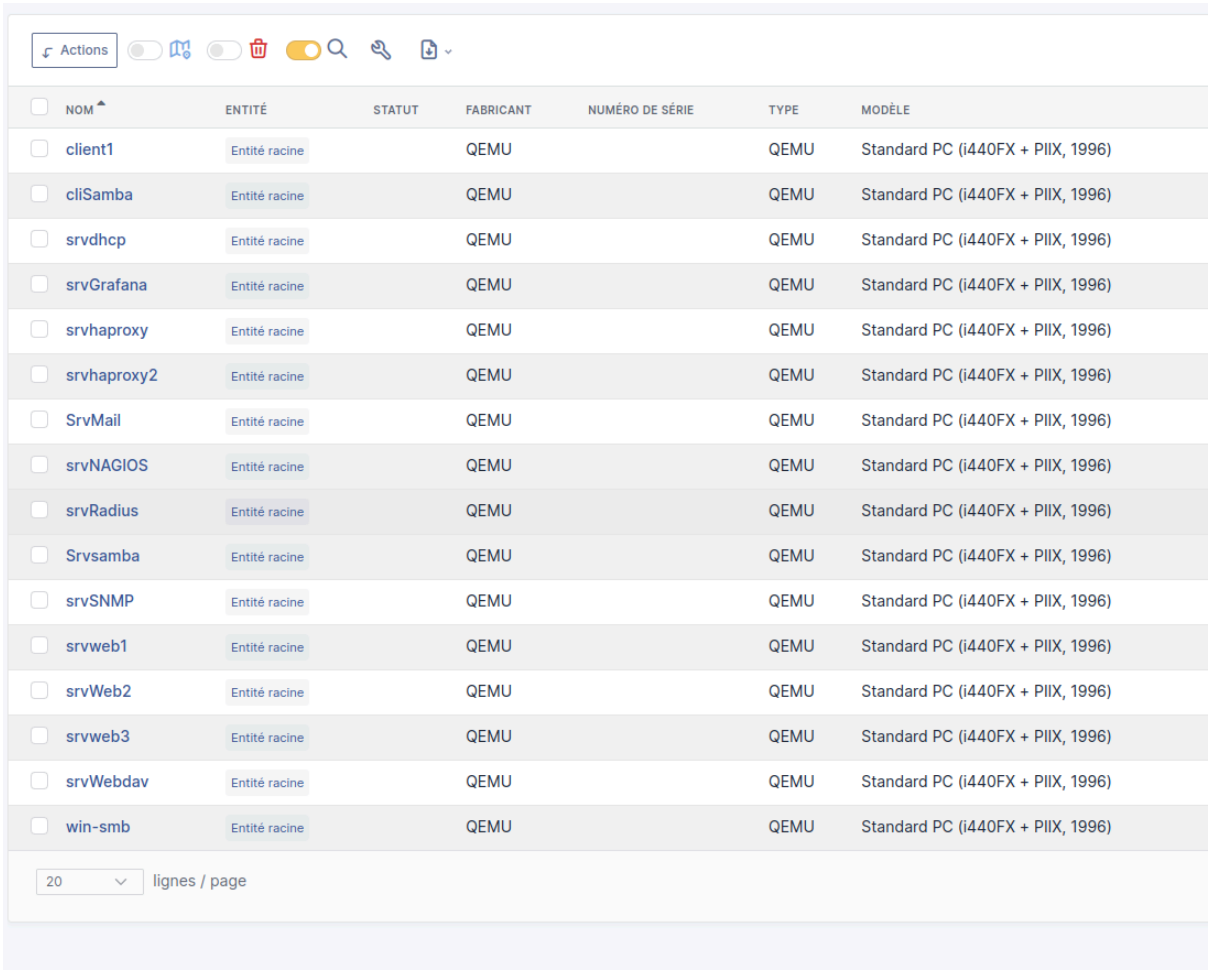
voici le résultat des serveurs et clients



INSTALLATION GLPI-AGENT SUR WINDOWS







Mission 1 : SAMBA

1. Fonctionnement et avantages de Samba

Samba permet à Linux de partager des fichiers et des imprimantes avec Windows. Son avantage est de rendre les deux systèmes totalement compatibles sur le même réseau.

2. Rôle d’un contrôleur de domaine (DC)

Réponse : C'est le serveur "chef" qui centralise tous les comptes utilisateurs et vérifie les mots de passe lors de chaque connexion au réseau.

3. Importance du DNS et du temps

Code : `ntpstat` (temps) et `dig @localhost google.com` (DNS)

Le DNS sert à trouver les serveurs par leur nom. Le temps est crucial : un décalage de plus de 5 minutes bloque la connexion pour sécurité.

4. Rôle des tickets Kerberos

Code : `klist` (pour voir ses tickets)

C'est un "pass" numérique. Une fois connecté, le ticket prouve votre identité aux autres services sans avoir à retaper votre mot de passe.

5. Rôle du fichier /etc/samba/smb.conf

Code : `nano /etc/samba/smb.conf`

C'est le fichier de réglages principal. Il sert à nommer le serveur et à lister tous les dossiers que l'on souhaite partager.

🔧 Phase Pratique :

6. Mise en place de SAMBA en tant que serveur de fichiers

(mdp final : Sio2026!)

Installation des paquets Samba sur le serveur Debian pour activer les services de partage.

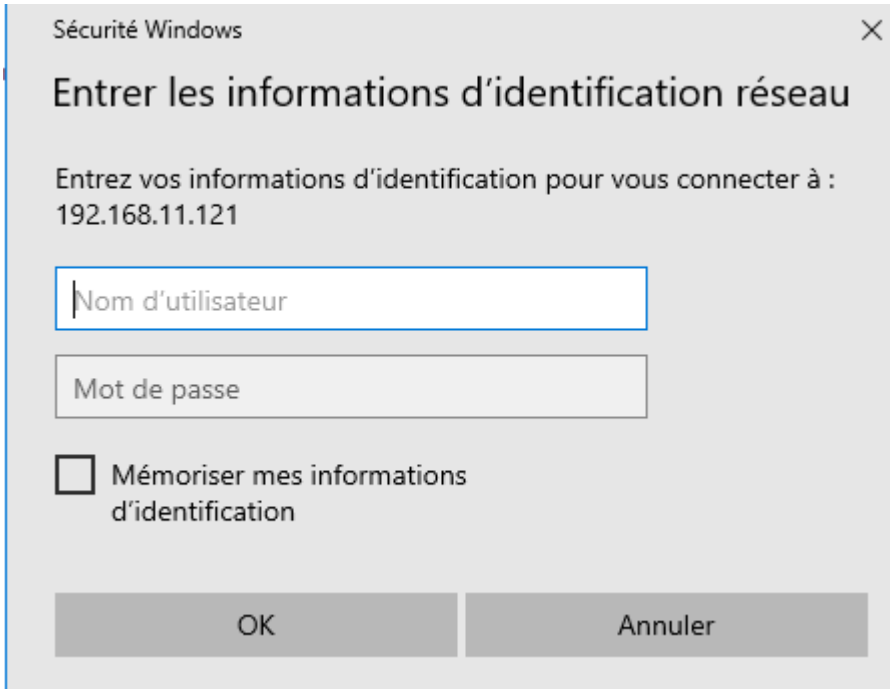
Création du répertoire physique `/sambashare` sur le disque du serveur.

Paramétrage du partage dans le fichier de configuration (chemin, droits d'écriture et visibilité)

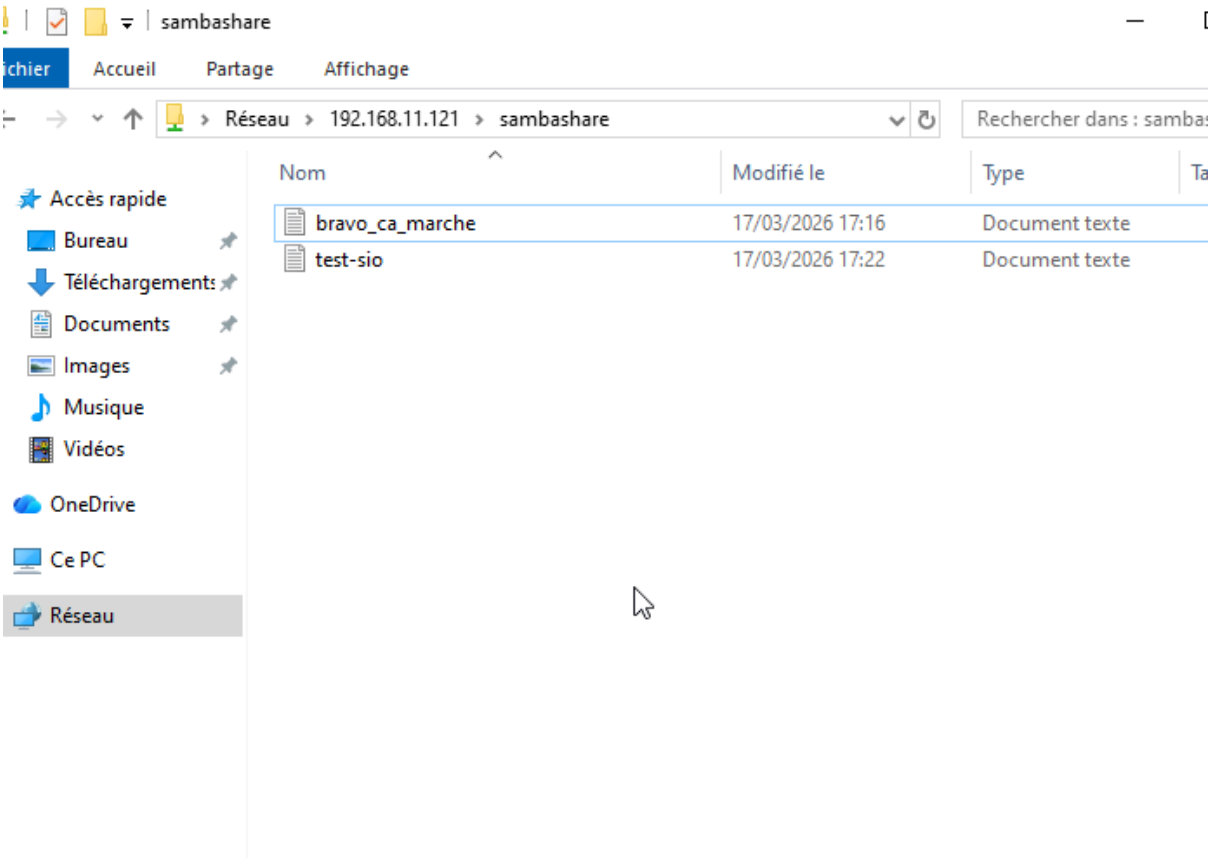
Création de l'utilisateur "sio" dans la base de données Samba avec la commande `smbpasswd`

```
root@Srvsamba:~# smbpasswd -a sio
New SMB password:
Retype new SMB password:
Added user sio.
```

Fenêtre d'authentification sur le client Windows pour accéder au partage



Affichage des fichiers de test (`bravo_ca_marche.txt`) dans l'explorateur Windows



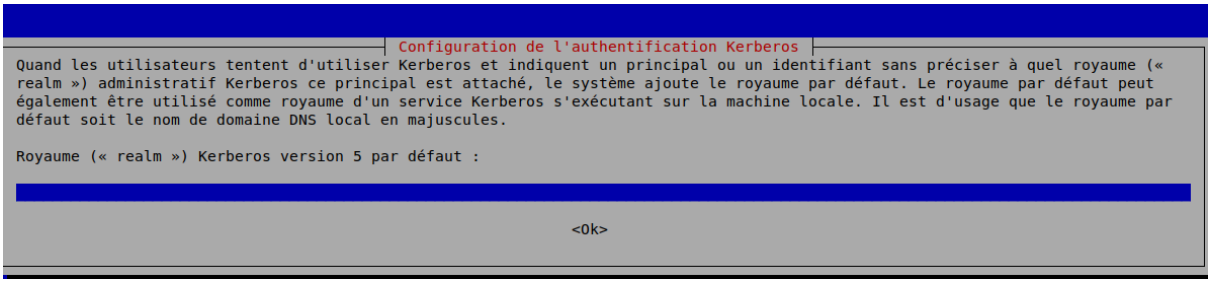
Utilisation de la commande `smbstatus` pour confirmer la connexion active du client sur le serveur

```
root@Srvsamba:~# touch /home/sio/sambashare/bravo_ca_marche.txt
root@Srvsamba:~# touch /home/sio/sambashare/test-sio.txt
root@Srvsamba:~# smbstatus

Samba version 4.22.8-Debian-4.22.8+dfsg-0+deb13u1
PID     Username     Group        Machine                                   Protocol Version  Encryption           Signing
----------------------------------------------------------------------------------------------------------------------------------------
4123    sio          sio          192.168.14.130 (ipv4:192.168.14.130:59053) SMB3_11           -                    partial(AES-128-CMAC
)

Service      pid     Machine       Connected at                     Encryption   Signing
---------------------------------------------------------------------------------------------
sambashare   4123    192.168.14.130 mar. mars 17 16:51:17 2026 CET   -            -


Locked files:
Pid          User(ID)   DenyMode   Access      R/W        Oplock           SharePath   Name   Time
---------------------------------------------------------------------------------------------------
4123         1000       DENY_NONE  0x100081    RDONLY     LEASE(RH)        /home/sio/sambashare   .   Tue Mar 17 17:22:11 2026
4123         1000       DENY_NONE  0x100081    RDONLY     NONE             /home/sio/sambashare   .   Tue Mar 17 16:51:18 2026
4123         1000       DENY_NONE  0x100081    RDONLY     NONE             /home/sio/sambashare   .   Tue Mar 17 16:51:18 2026

root@Srvsamba:~# ls -l /home/sio/sambashare
total 0
-rw-rw-r-- 1 root root 0 17 mars  17:16 bravo_ca_marche.txt
-rw-rw-r-- 1 root root 0 17 mars  17:22 test-sio.txt
root@Srvsamba:~#
```

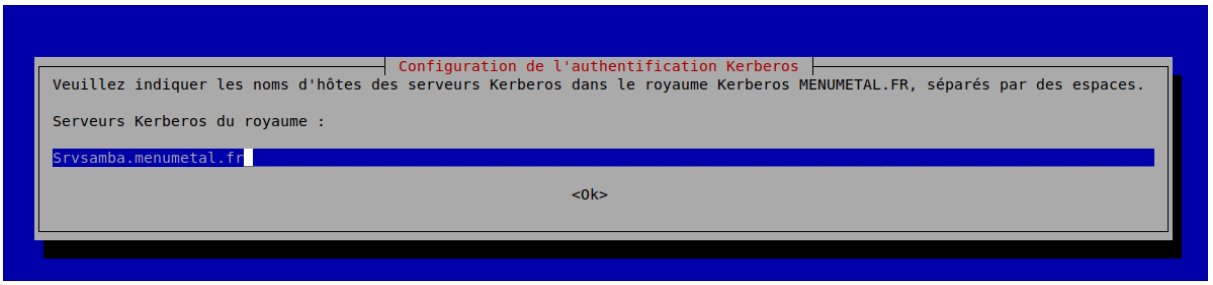
Installation du rôle de contrôleur de domaine et des outils Kerberos.

```
apt install samba-ad-dc krb5-user bind9-dnsutils
```

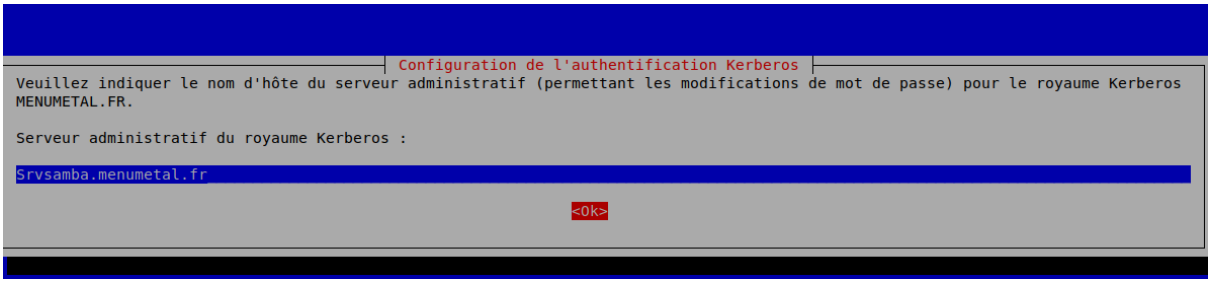
Paramétrage du royaume (Realm) `MENUMETAL.FR` pour la gestion des tickets d'authentification.



Saisie du nom d'hôte du serveur (`Srvsamba.menumetal.fr`) pour identifier les serveurs Kerberos du royaume.



Saisie du nom royaume Kerberos



Désactivation et masquage (`mask`) des anciens services Samba (`smbd`, `nmbd`, `winbind`) pour éviter tout conflit avec le futur rôle de contrôleur de domaine AD DC.

```
root@Srvsamba:~# systemctl disable --now smbd nmbd winbind
Synchronizing state of smbd.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install disable smbd
Synchronizing state of nmbd.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install disable nmbd
Synchronizing state of winbind.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install disable winbind
Removed '/etc/systemd/system/multi-user.target.wants/smbd.service'.
Removed '/etc/systemd/system/multi-user.target.wants/winbind.service'.
Removed '/etc/systemd/system/multi-user.target.wants/nmbd.service'.
Removed '/etc/systemd/system/smb.service'.
Removed '/etc/systemd/system/nmb.service'.
root@Srvsamba:~#  systemctl mask smbd nmbd winbind
Created symlink '/etc/systemd/system/smbd.service' → '/dev/null'.
Created symlink '/etc/systemd/system/nmbd.service' → '/dev/null'.
Created symlink '/etc/systemd/system/winbind.service' → '/dev/null'.
root@Srvsamba:~#
```

Réactivation (`unmask`) et démarrage automatique du service `samba-ad-dc`

```
root@Srvsamba:~# systemctl unmask samba-ad-dc
root@Srvsamba:~# systemctl enable samba-ad-dc
Synchronizing state of samba-ad-dc.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable samba-ad-dc
root@Srvsamba:~#
```

Déplacement du fichier de configuration Samba d'origine vers un fichier `.orig`

```
root@Srvsamba:~# mv /etc/samba/smb.conf /etc/samba/smb.conf.orig
root@Srvsamba:~#
```

Attribution d’un mdp sur Admin

```
Administrator password:
```

: Aperçu du nouveau fichier `smb.conf` généré, incluant le nom du domaine (`MENUMETAL.FR`), le rôle de contrôleur de domaine et les partages réseaux obligatoires `sysvol` et `netlogon`

```
# Global parameters
[global]
        dns forwarder = 127.0.0.53
        netbios name = SRVSAMBA
        realm = MENUMETAL.FR
        server role = active directory domain controller
        workgroup = MENUMETAL

[sysvol]
        path = /var/lib/samba/sysvol
        read only = No

[netlogon]
        path = /var/lib/samba/sysvol/menumetal.fr/scripts
        read only = No
```

Suppression du lien vers le fichier de configuration DNS actuel (`unlink`) pour pouvoir configurer manuellement le serveur DNS interne de Samba

```
root@Srvsamba:~# unlink /etc/resolv.conf
```

Édition du fichier `/etc/resolv.conf` pour pointer vers l'adresse locale (`127.0.0.1`) et définir le domaine de recherche `menumetal.fr` afin que le serveur utilise son propre service DNS

```
 GNU nano 8.4                                  /etc/resolv.conf *
nameserver 127.0.0.1
search menumetal.fr
```

vérification du statut du service `samba-ad-dc` qui apparaît bien comme **"active (running)"**

```
root@Srvsamba:~# cp -f /var/lib/samba/private/krb5.conf /etc/krb5.conf
root@Srvsamba:~# systemctl start samba-ad-dc
root@Srvsamba:~# systemctl status samba-ad-dc
● samba-ad-dc.service - Samba AD Daemon
     Loaded: loaded (/usr/lib/systemd/system/samba-ad-dc.service; enabled; preset: enabled)
     Active: active (running) since Tue 2026-03-17 17:55:31 CET; 11s ago
 Invocation: 50c9d401e82b407485757a6cc91e729a
       Docs: man:samba(8)
```

Utilisation de la commande `klist` pour vérifier la validité du ticket d'authentification de l'administrateur, suivie d'un test de résolution DNS confirmant que le nom du serveur est bien lié à son adresse IP.

```
Password for Administrator@MENUMETAL.FR:
Warning: Your password will expire in 41 days on mar. 28 avril 2026 18:44:55
root@Srvsamba:~# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: Administrator@MENUMETAL.FR

Valid starting       Expires              Service principal
17/03/2026 17:56:39  18/03/2026 03:56:39  krbtgt/MENUMETAL.FR@MENUMETAL.FR
        renew until 18/03/2026 17:56:25
root@Srvsamba:~# host -t A srvsamba.menumetal.fr
srvsamba.menumetal.fr has address 192.168.11.121
```

Utilisation de `samba-tool` pour afficher les informations détaillées du serveur DNS intégré, confirmant que le service est opérationnel sur l'adresse `192.168.11.121`

```
Srvsamba
root@Srvsamba:~# samba-tool dns serverinfo $(hostname -f)
Password for [Administrator@MENUMETAL.FR]:
  dwVersion                  : 0xece0205
  fBootMethod                : DNS_BOOT_METHOD_DIRECTORY
  fAdminConfigured           : FALSE
  fAllowUpdate               : TRUE
  fDsAvailable               : TRUE
  pszServerName              : srvsamba.menumetal.fr
  pszDsContainer             : CN=MicrosoftDNS,DC=DomainDnsZones,DC=menumetal,DC=fr
  aipServerAddrs             : ['192.168.11.121']
  aipListenAddrs             : ['192.168.11.121']
  aipForwarders              : []
  dwLogLevel                 : 0
  dwDebugLevel               : 0
  dwForwardTimeout           : 3
  dwRpcPrototol              : 0x5
  dwNameCheckFlag            : DNS_ALLOW_MULTIBYTE_NAMES
  cAddressAnswerLimit        : 0
  dwRecursionRetry           : 3
  dwRecursionTimeout         : 8
  dwMaxCacheTtl              : 86400
  dwDsPollingInterval        : 180
  dwScavengingInterval       : 168
  dwDefaultRefreshInterval   : 72
  dwDefaultNoRefreshInterval : 72
  fAutoReverseZones          : FALSE
  fAutoCacheUpdate           : FALSE
  fRecurseAfterForwarding    : FALSE
  fForwardDelegations        : TRUE
  fNoRecursion               : FALSE
  fSecureResponses           : FALSE
  fRoundRobin                : TRUE
  fLocalNetPriority          : FALSE
  fBindSecondaries           : FALSE
  fWriteAuthorityNs          : FALSE
  fStrictFileParsing         : FALSE
  fLooseWildcarding          : FALSE
  fDefaultAgingState         : FALSE
  dwRpcStructureVersion      : 0x2
  aipLogFilter               : []
  pwszLogFilePath            : None
  pszDomainName              : menumetal.fr
  pszForestName              : menumetal.fr
  pszDomainDirectoryPartition : DC=DomainDnsZones,DC=menumetal,DC=fr
  pszForestDirectoryPartition : DC=ForestDnsZones,DC=menumetal,DC=fr
  dwLocalNetPriorityNetMask  : 0xff
  dwLastScavengeTime         : 0
  dwEventLogLevel            : 4
  dwLogFileMaxSize           : 0
  dwDsForestVersion          : 4
  dwDsDomainVersion          : 4
  dwDsDsaVersion             : 4
  fReadOnlyDC                : FALSE
```

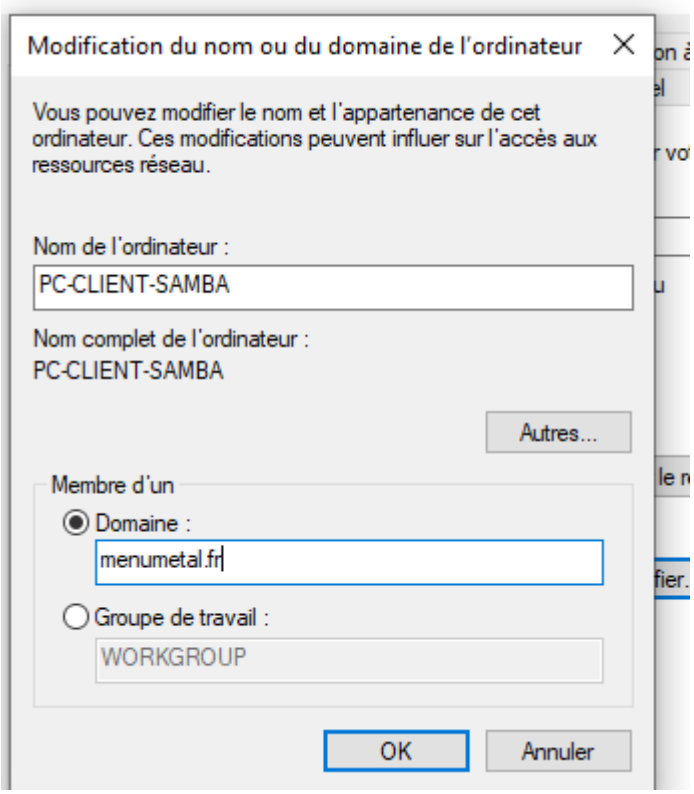
Utilisation de `samba-tool` pour créer l'Unité d'Organisation (OU) "People" et y ajouter les groupes "IT" et "Commercial" afin de structurer l'annuaire Active Directory

```
root@Srvsamba:~# samba-tool ou create "OU=People,DC=menumetal,DC=fr"
Added ou "OU=People,DC=menumetal,DC=fr"
root@Srvsamba:~# samba-tool group add IT --groupou=OU=People
Added group IT
root@Srvsamba:~# samba-tool group add Commercial --groupou=OU=People
Added group Commercial
root@Srvsamba:~#
```

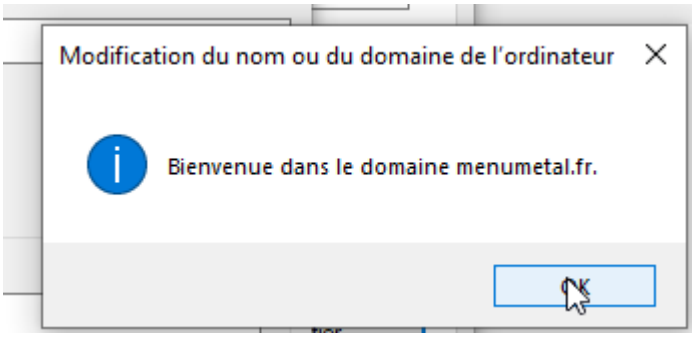
Création des comptes utilisateurs (`user-it1`, `user-it2`, etc.) dans l'OU "People" avec leurs mots de passe, suivie de l'ajout des membres dans leurs groupes respectifs

```
root@Srvsamba:~# samba-tool user create user-it1 Sio2026! --userou=OU=People
User 'user-it1' added successfully
root@Srvsamba:~# samba-tool user create user-it2 Sio2026! --userou=OU=People
User 'user-it2' added successfully
root@Srvsamba:~# samba-tool user create user-com1 Sio2026! --userou=OU=People
User 'user-com1' added successfully
root@Srvsamba:~# samba-tool user create user-com2 Sio2026! --userou=OU=People
User 'user-com2' added successfully
root@Srvsamba:~# samba-tool group addmembers IT user-it1,user-it2
Added members to group IT
root@Srvsamba:~# samba-tool group addmembers Commercial user-com1,user-com2
Added members to group Commercial
```

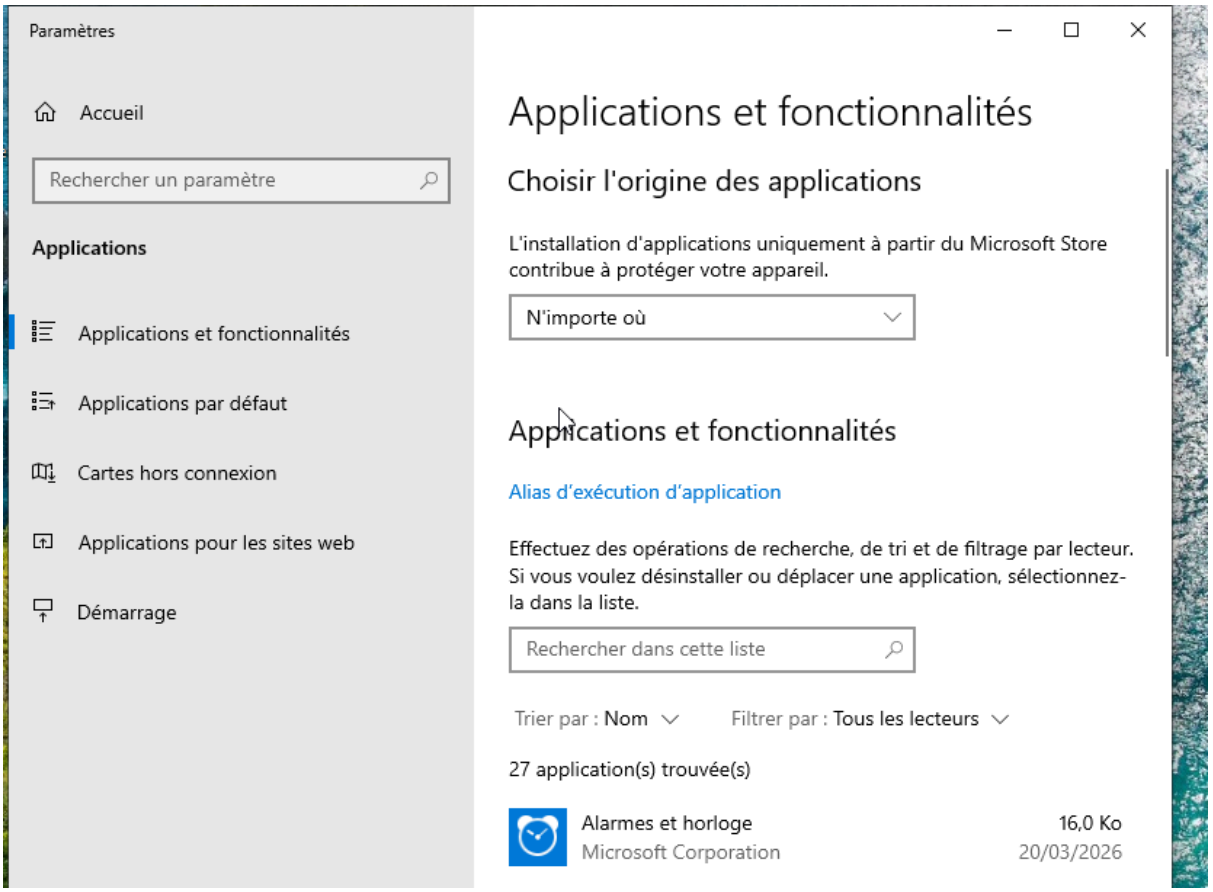
Après avoir changé le nom du PC, je l'ai rajouté au domaine menumetal.fr



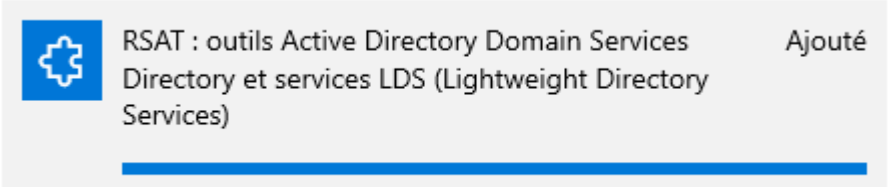
Confirmation de l'entrée sur le domaine



Accès aux paramètres de Windows pour ajouter des fonctionnalités facultatives au système



installation de rsat



Mission 2 – Sécurisation d’un switch

1. Préconisations de l’ANSSI

a. Les VLANs

Les **VLAN (Virtual LAN)** permettent de segmenter le réseau pour améliorer la sécurité et limiter la propagation d’attaques.

Bonnes pratiques :

- Séparer les types de trafic (LAN, DMZ, administration, invités).
- Ne pas utiliser le VLAN par défaut pour les machines.
- Restreindre les VLAN autorisés sur les trunks.
- Mettre les ports inutilisés dans un VLAN isolé et les désactiver.

Objectif : **réduire les risques d’attaques latérales dans le réseau** 🔐

---

b. Différence VLAN par défaut / VLAN natif (Cisco)

VLAN par défaut (VLAN 1)

- VLAN créé automatiquement sur les switches Cisco.
- Tous les ports y sont initialement associés.
- Utilisé par plusieurs protocoles (CDP, VTP…).
- Recommandation : **ne pas l’utiliser pour les machines**.

VLAN natif

- VLAN utilisé sur les **liens trunk** pour les trames **non taguées**.
- Par défaut il est souvent **VLAN 1**.
- Bonne pratique : **changer le VLAN natif pour éviter les attaques VLAN hopping**.

---

c. Accès distant aux switches

Deux méthodes :

Comptes locaux

- Créés directement sur le switch
- Utilisés si le serveur d'authentification est indisponible.

Comptes centralisés

- Via serveur **RADIUS ou TACACS+**
- Permet une gestion centralisée des utilisateurs.

Bonnes pratiques :

- Désactiver **Telnet**
- Utiliser **SSH**
- Mettre des mots de passe forts
- Limiter les IP autorisées à se connecter

🔐 Objectif : sécuriser l'administration réseau.

---

d. Sécurité des ports (Port Security)

La **port security** limite les équipements autorisés sur un port.

Fonctionnalités :

- Limiter le nombre d'adresses MAC
- Associer une MAC spécifique à un port
- Bloquer un port en cas d'intrusion

Modes possibles :

- **Protect** → ignore les nouvelles MAC
- **Restrict** → bloque + enregistre un log
- **Shutdown** → désactive le port

But : empêcher un utilisateur de brancher un équipement non autorisé.

---

e. Intérêt de la journalisation

La **journalisation (logs)** permet de :

- détecter les incidents
- analyser les attaques
- tracer les actions administrateur
- surveiller le réseau

Les logs sont souvent envoyés vers un **serveur Syslog centralisé**.

📊 Exemple d'événements :

- connexion admin
- violation port security
- DHCP
- changement de configuration

---

f. DHCP Snooping

Le **DHCP snooping** protège contre les **faux serveurs DHCP**.

Fonctionnement :

- Le switch distingue les ports **trusted** (serveur DHCP) et **untrusted** (clients).
- Il bloque les réponses DHCP provenant de ports non autorisés.

Protection contre :

- DHCP rogue
- attaques **Man in the Middle**

---

g. SNMPv2c : GET vs TRAP

SNMP sert à superviser les équipements réseau.

GET

- requête envoyée par le serveur de supervision
- permet de **lire des informations** sur l'équipement

Exemples :

- utilisation CPU
- état des interfaces
- trafic réseau

TRAP

- message **envoyé automatiquement par l'équipement**
- signale un événement
-

Exemples :

- port down
- panne

- alerte sécurité

📡 Différence principale :
GET = interrogation
TRAP = notification automatique

Question 2 : Vérification des accès distants (Telnet et SSH)

1. Objectif

L'objectif est de vérifier si les services d'administration à distance sont opérationnels sur les commutateurs Cisco et HP, tout en évaluant la conformité avec les recommandations de sécurité (utilisation de SSH au lieu de Telnet).

---

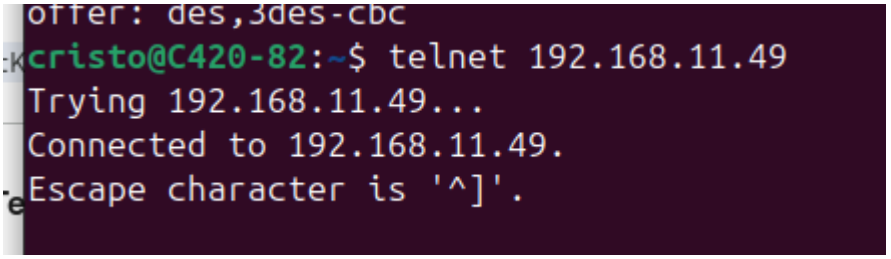
2. Tests sur le commutateur HP (192.168.11.49)

A. Accès via Telnet

Nous avons testé la connexion Telnet depuis le terminal de la VM Linux. Le service répond correctement et demande l'authentification.

- **Résultat :** Fonctionnel.
- **Observation :** Bien que fonctionnel, ce protocole n'est pas sécurisé car les identifiants circulent en clair sur le réseau.

-

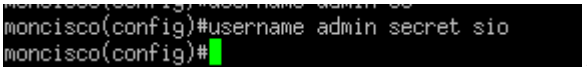


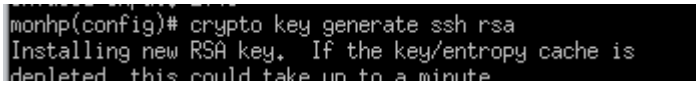
-

B. Accès via SSH

Nous avons tenté une connexion SSH. La commande a retourné une erreur de négociation de sécurité.

- **Résultat :** Échec de connexion.
- **Analyse de l'erreur :** Le switch HP utilise des algorithmes de chiffrement obsolètes (`diffie-hellman-group1-sha1`) et une longueur de clé RSA trop faible (512 bits) pour les clients SSH modernes.





---

3. Tests sur le commutateur Cisco (192.168.11.42)

A. Accès via Telnet

Le test de connexion Telnet vers l'IP de management du Cisco a été effectué.

- **Résultat :** Fonctionnel (Accès via le mot de passe VTY).

B. Accès via SSH

Contrairement au switch HP, le switch Cisco supporte des versions plus récentes du protocole SSH (v2) avec des clés de 1024 bits minimum.

```
^C
cristo@C420-82:~$ ssh -o KexAlgorithms=+diffie-hellman-group1-sha1 -o HostKeyAlg
orithms=+ssh-rsa -o Ciphers=+aes128-cbc admin@192.168.11.42
admin@192.168.11.42's password:
Permission denied, please try again.
admin@192.168.11.42's password:
 Interdit au public
moncisco>
```

- **Résultat :** Fonctionnel.

---

4. Synthèse des résultats

Équipement	Accès Telnet	Accès SSH	État de conformité
Switch HP	✅ Succès	❌ Échec	**Non conforme** (Sécurité obsolète)
Switch Cisco	✅ Succès	✅ Succès	**Conforme**

Ajouter un PC portable dans le vlan LAN, il obtiendra un IP dynamique via votre serveur DHCP sous Linux

ON utilise un dhcp windows server

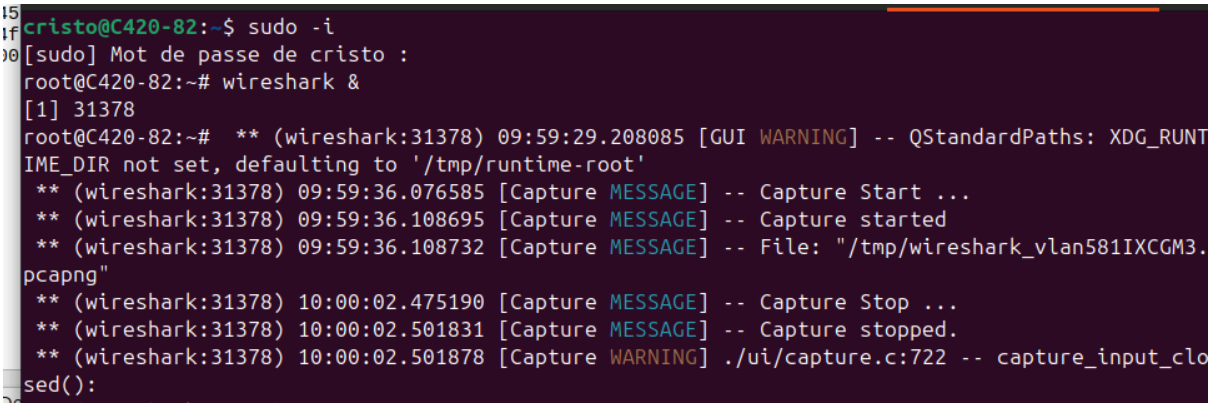
```
root@srvdhcp:~# systemctl status isc-dhcp-server.service
● isc-dhcp-server.service - LSB: DHCP server
     Loaded: loaded (/etc/init.d/isc-dhcp-server; generated)
     Active: active (running) since Tue 2025-11-18 17:51:52 CET; 4min 40s ago
 Invocation: 1b7001dfb76b40a2bc70699ad41f2981
       Docs: man:systemd-sysv-generator(8)
    Process: 4270 ExecStart=/etc/init.d/isc-dhcp-server start (code=exited, status=0/SUCCESS)
      Tasks: 1 (limit: 2303)
     Memory: 3.9M (peak: 5.9M)
        CPU: 76ms
     CGroup: /system.slice/isc-dhcp-server.service
             └─4282 /usr/sbin/dhcpd -4 -q -cf /etc/dhcp/dhcpd.conf ens18

nov. 18 17:51:50 srvdhcp dhcpd[4282]: Internet Systems Consortium DHCP Server 4.4.3-P1
nov. 18 17:51:50 srvdhcp systemd[1]: isc-dhcp-server.service: This usually indicates unclean termination of a previous run, or ser
nov. 18 17:51:50 srvdhcp dhcpd[4282]: Copyright 2004-2022 Internet Systems Consortium.
nov. 18 17:51:50 srvdhcp systemd[1]: Starting isc-dhcp-server.service - LSB: DHCP server...
nov. 18 17:51:50 srvdhcp dhcpd[4282]: All rights reserved.
nov. 18 17:51:50 srvdhcp dhcpd[4282]: For info, please visit https://www.isc.org/software/dhcp/
nov. 18 17:51:50 srvdhcp dhcpd[4282]: Wrote 0 leases to leases file.
nov. 18 17:51:50 srvdhcp dhcpd[4282]: Server starting service.
nov. 18 17:51:52 srvdhcp isc-dhcp-server[4270]: Starting ISC DHCPv4 server: dhcpd.
nov. 18 17:51:52 srvdhcp systemd[1]: Started isc-dhcp-server.service - LSB: DHCP server.
lines 1-22/22 (END)
```

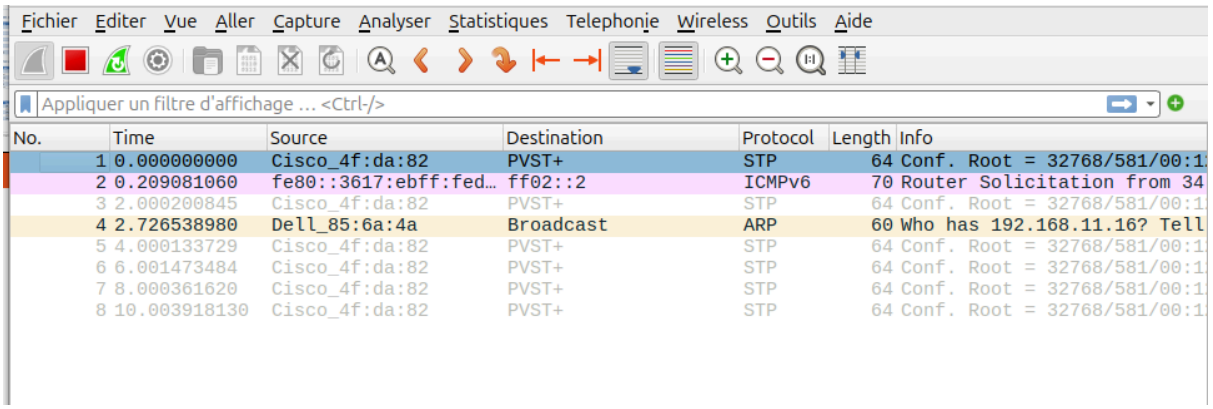
voici les résultat sur un pc client portable

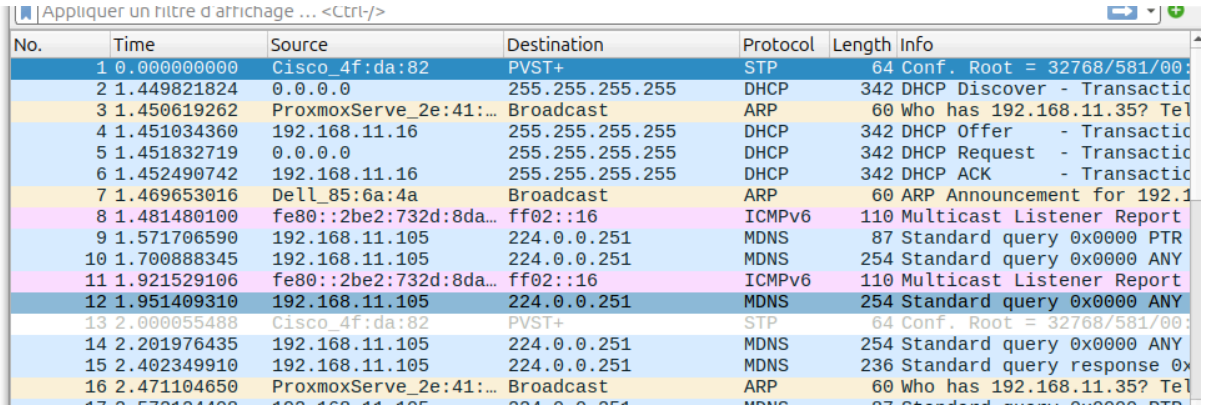
```
root@sio-proto:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default ql
en 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp9s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group
default qlen 1000
    link/ether e0:db:55:85:6a:4a brd ff:ff:ff:ff:ff:ff
    inet 192.168.11.105/24 brd 192.168.11.255 scope global dynamic enp9s0
       valid_lft 691140sec preferred_lft 691140sec
    inet6 fe80::577:5c70:7609:2cb7/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
root@sio-proto:~#
```

wireshark cisco:
avec la commande dhclient -v en envoie des traces et wireshark scanne les traces

```
root@sio-proto:~# dhclient -v
Internet Systems Consortium DHCP Client 4.4.1
Copyright 2004-2018 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/enp9s0/e0:db:55:85:6a:4a
Sending on   LPF/enp9s0/e0:db:55:85:6a:4a
Sending on   Socket/fallback
DHCPDISCOVER on enp9s0 to 255.255.255.255 port 67 interval 3 (xid=0x156aa648)
DHCPOFFER of 192.168.11.105 from 192.168.11.16
DHCPREQUEST for 192.168.11.105 on enp9s0 to 255.255.255.255 port 67 (xid=0x48a66a15)
DHCPACK of 192.168.11.105 from 192.168.11.16 (xid=0x156aa648)
bound to 192.168.11.105 -- renewal in 268238 seconds.
root@sio-proto:~#
```







Quelle est la commande à utiliser qui permet d'obtenir les adresses MAC acquises par les commutateurs ? Récupérer les adresses MAC acquises par vos switches

Port	**Adresse MAC (Format HP)**	**Hôte / Équipement associé**
1	f8b156-aa12ce	**Switch Cisco** (Lien d'interconnexion / Trunk)
1	001b0d-4fda85	Autre équipement du réseau (via Uplink)

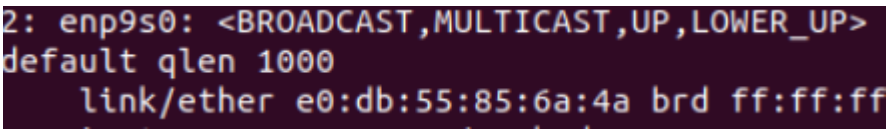
1	bc2411-a172dd	Serveur / VM (via réseau Proxmox/Uplink)
1	bc2411-c6c483	Serveur / VM (via réseau Proxmox/Uplink)
2	e0db55-8a6cb1	**PC Portable de test** (VLAN 581)
7	e0db55-856a4a	**PC autorisé** (Configuré dans la sécurité de port)

```
moncisco#show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 All    0012.d909.2980    STATIC      CPU
 All    0012.d909.2981    STATIC      CPU
 All    0012.d909.2982    STATIC      CPU
 All    0012.d909.2983    STATIC      CPU
 All    0012.d909.2984    STATIC      CPU
 All    0012.d909.2985    STATIC      CPU
 All    0012.d909.2986    STATIC      CPU
 All    0012.d909.2987    STATIC      CPU
 All    0012.d909.2988    STATIC      CPU
 All    0012.d909.2989    STATIC      CPU
 All    0012.d909.298a    STATIC      CPU
 All    0012.d909.298b    STATIC      CPU
 All    0012.d909.298c    STATIC      CPU
 All    0012.d909.298d    STATIC      CPU
 All    0012.d909.298e    STATIC      CPU
 All    0012.d909.298f    STATIC      CPU
 All    0012.d909.2990    STATIC      CPU
```

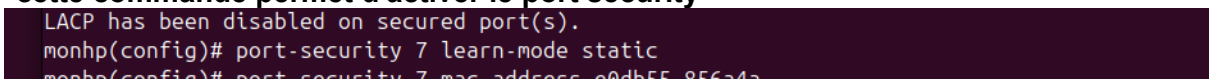
Question 7 : Mise en place de la sécurité par port (Port Security)

a. Sécuriser manuellement (Statique)

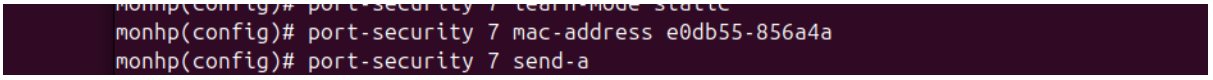
On associe une adresse MAC précise à un port. Si une autre machine se branche, le port se bloque.

- **l'ip mac hp**
- 

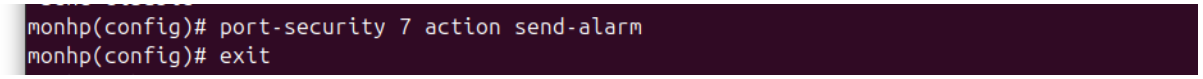
cette commande permet d'activer le port security



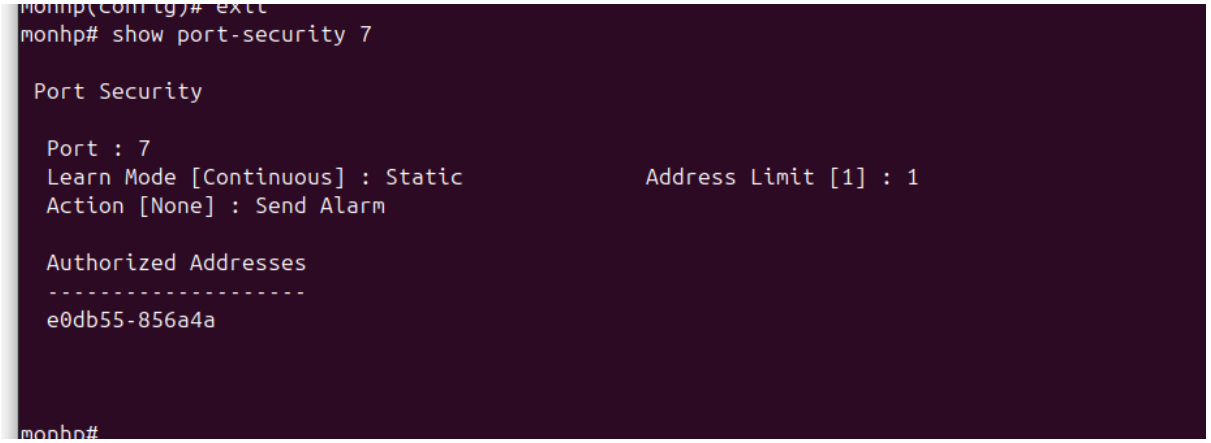
cette commande permet d'enregistrer



envoie une alarme



avec la commande show port-security on peut regarder les mac autorisé



cette commande permet regarder les intrusion.log

```
monhp# show port-security intrusion-log

 Status and Counters - Intrusion Log

  Port MAC Address   Date / Time
  ---- ------------- --------------------------
  2    bc2411-1edb61 01/01/90 18:37:25


monhp# show port-security intrusion-log
```

cette commande desactive le port si l’adresse mac est pas la bonne

```
monhp# configure
monhp(config)# port-security 2 action send-disable
monhp(config)#
```

voici un test

```
W 01/01/90 18:37:25 FFI: port 2 - Security Violation
I 01/01/90 18:37:25 ports: port 2 is now off-line
```

8. Sauvegarder les nouvelles configurations sur le serveur TFTP

HP TFTP: avec cette commande on envoie une config du switch

```
monhp# copy running-config tftp 192.168.13.6 config_hp_securise.cfg
```

dans le serveur tftp on fait un ls -lh /srv/tftp/config_hp_securise.cfg

```
root@srvTFTP:~# ls -lh /srv/tftp/config_hp_securise.cfg
-rw-rw-rw- 1 nobody nogroup 805 20 mars  13:46 /srv/tftp/config_hp_securise.cfg
```

avec la commande cat on voit tout les configuration du switch hp

```
root@srvTFTP:~# cat /srv/tftp/config_hp_securise.cfg
; J4900B Configuration Editor; Created on release #H.08.83

hostname "monhp"
interface 1
   no lacp
exit
interface 2
   disable
   no lacp
exit
interface 7
   no lacp
  it
  default-gateway 192.168.13.254
  mp-server community "public" Unrestricted
vlan 1
   name "DEFAULT_VLAN"
   untagged 3-26
   no ip address
   no untagged 1-2
   exit
vlan 581
   name "LAN"
   untagged 2
   ip address 192.168.11.49 255.255.255.0
   tagged 1
   exit
vlan 580
   name "GESTION"
   untagged 1
   ip address 192.168.13.101 255.255.255.0
   exit
vlan 582
   name "DMZ"
   exit
port-security 2 learn-mode static action send-disable mac-address e0db55
port-security 7 learn-mode static action send-alarm mac-address e0db5585
```

TFTP CISCO:

avec le copy running-config startup config on lance une copie

```
moncisco#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

et avec copy running-config tftp on envoie la copie au serveur tftp

```
moncisco#copy running-config tftp
Address or name of remote host []? 192.168.13.6
Destination filename [moncisco-confg]?
.!!
4553 bytes copied in 7.160 secs (636 bytes/sec)
moncisco#
```

AVEC UN CAT sur le srvTFTP on constate les configuration cisco

```
interface FastEthernet0/48
 switchport mode dynamic desirable
!
interface GigabitEthernet0/1
 switchport mode dynamic desirable
!
interface GigabitEthernet0/2
 switchport mode dynamic desirable
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan581
 ip address 192.168.11.42 255.255.255.0
!
ip default-gateway 192.168.11.254
ip classless
ip http server
ip http secure-server
!
!
control-plane
!
banner motd  Interdit au public
!
line con 0
 password 7 045802150C2E
 login
line vty 0 4
 login local
 transport input ssh
line vty 5 15
 login
!
end
root@srvTFTP:~#
```

dans ce fichier dhcpd.conf on ajoute cet ligne

dans le fichier rsyslog.conf on ajoute cet ligne pour envoyer les logs