

DOCUMENTATION PROJET ALLSAFE

Par Alexandre GUITRE-MEYER , Franck HINTERREITE R, Erik MARKOSYAN et Curtis AMOAKON.

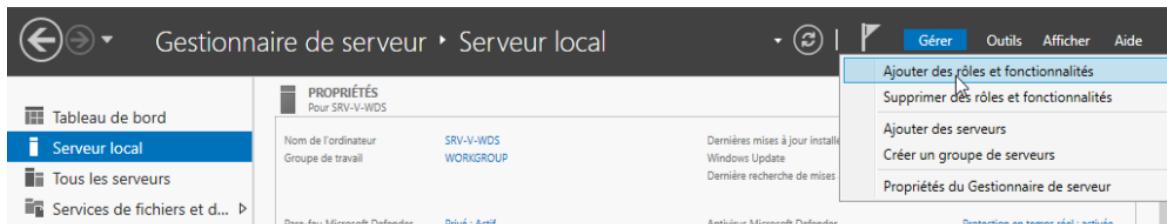
SECURISATION WINDOWS

I. Installation et configurer le serv_ice AD CS

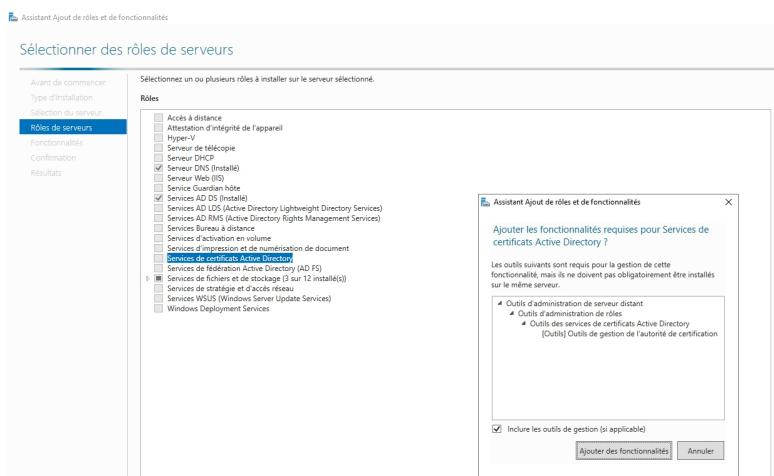
Service de certificats Active Directory (AD CS) est un service qui permet aux administrateurs réseau de créer et gérer des certificats d'infrastructure à clé publique (PKI) utilisés dans les protocoles de communication et d'authentification sécurisés.

A. Installation serv ice AD CS

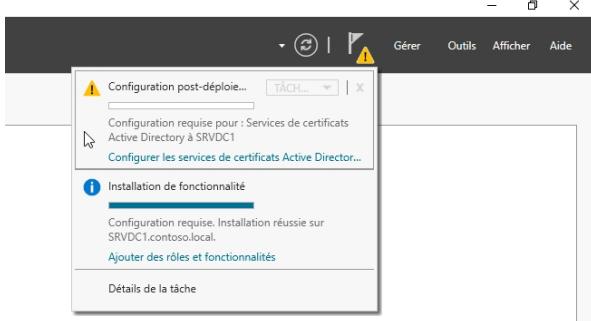
- Pour installer le rôle AD CS, cliquez-en haut à droit sur « Gérer » puis « ajoutez des rôles et fonctionnalités »



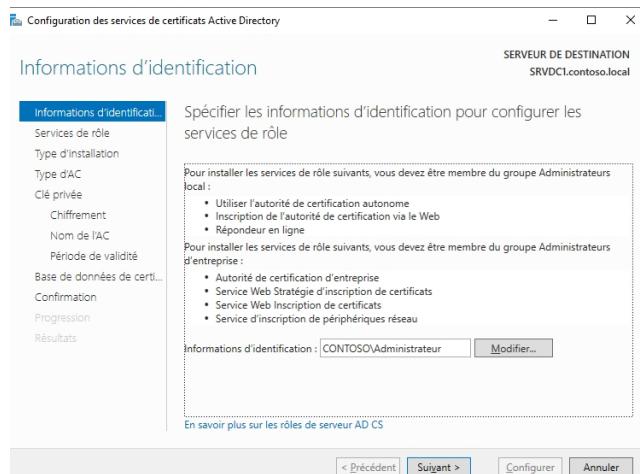
- Cliquez sur « Suivant » jusqu'à arriver sur la page « sélection des rôles de serveurs », Sélectionnez « Services de certificats Active Directory » puis cliquez sur « Suivant ». Cliquez sur « Ajouter des fonctionnalités » puis sur « Installer » :



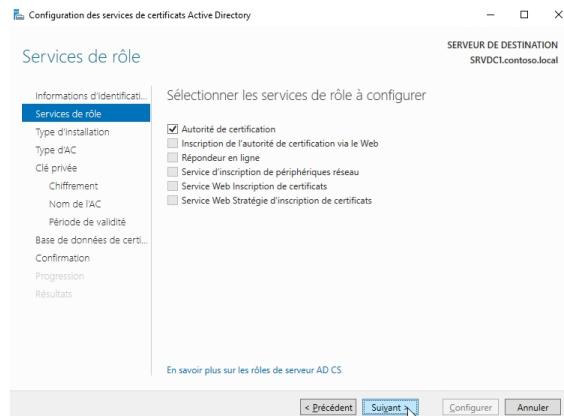
- Fermez la page après l'installation et cliquez-en haut à gauche sur le drapeau pour configurer le service AD CS :



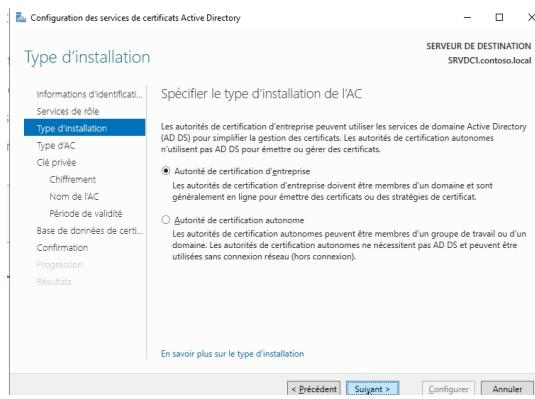
- Gardez l'information d'identification de l'administrateur et cliquez sur « Suivant » :



- Cochez « Autorité de certification » puis cliquez sur « Suivant » :



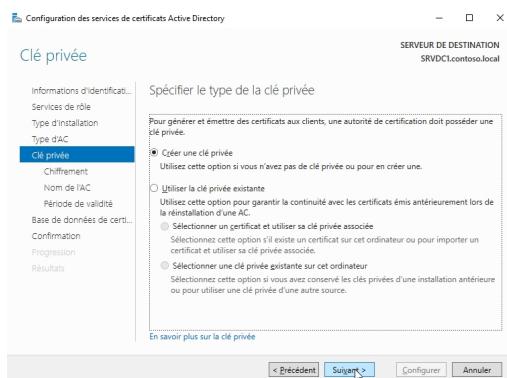
- Laissez « Autorité de certification d'entreprise » puis cliquez sur « Suivant » :



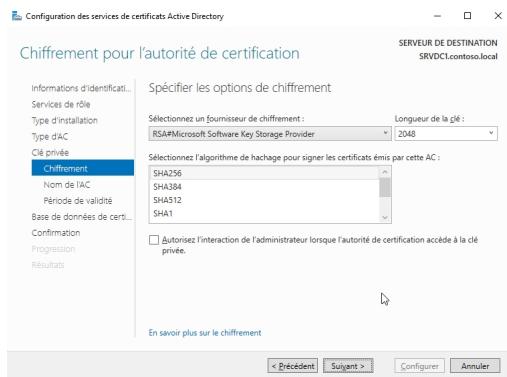
- Laissez « Autorité de certification racine » puis cliquez sur « Suivant » :



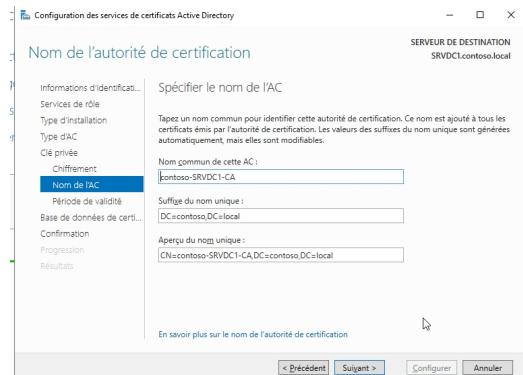
- Laissez « Créez un clé privée » puis cliquez sur « Suivant » :



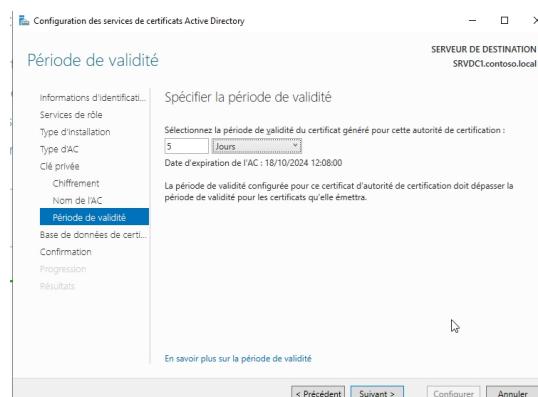
- Laissez tous les paramètres par défaut puis cliquez sur « Suivant » :



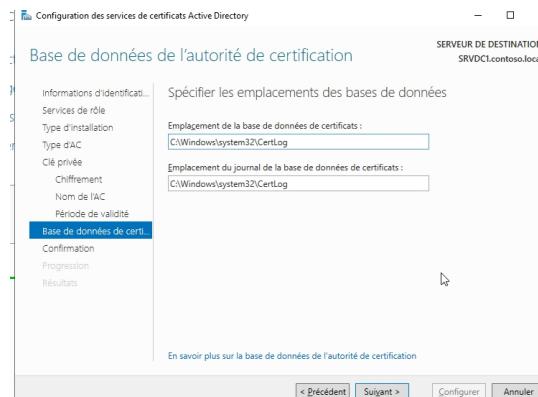
- Laissez tous les paramètres par défaut puis cliquez sur « Suivant » :



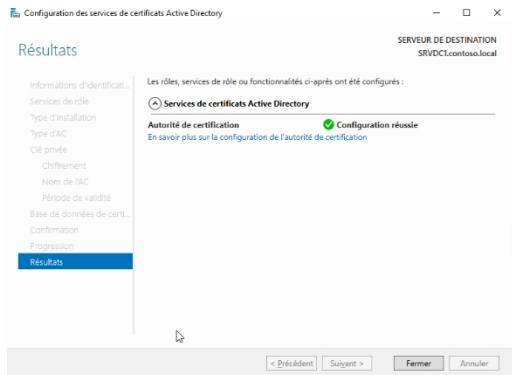
- Modifier la période de validité en jours puis cliquez sur « Suivant » :



- Laissez tous les paramètres par défaut puis cliquez sur « Suivant » :



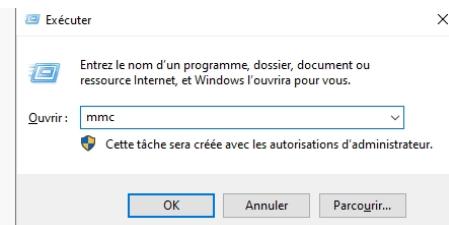
- Une fenêtre affichera un récapitulatif des paramètres fait, cliquez sur « Configurer » puis cliquez sur « Fermer » :



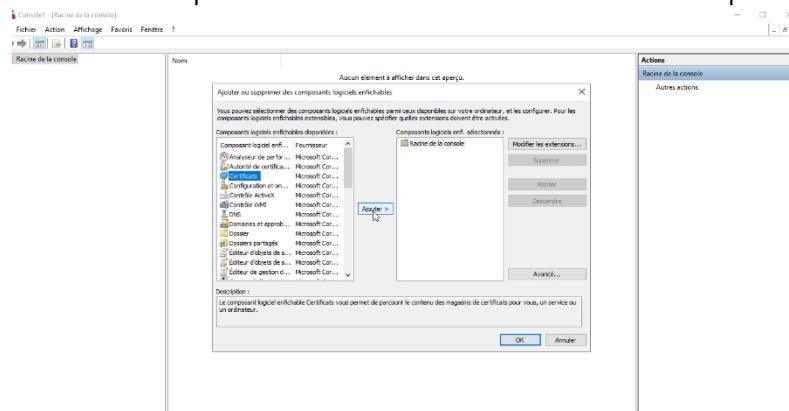
B. Création d'un certificat pour le serveur Windows et demande de certificat sur le post Windows

a. **Création du certificat sous Windows Server 2022**

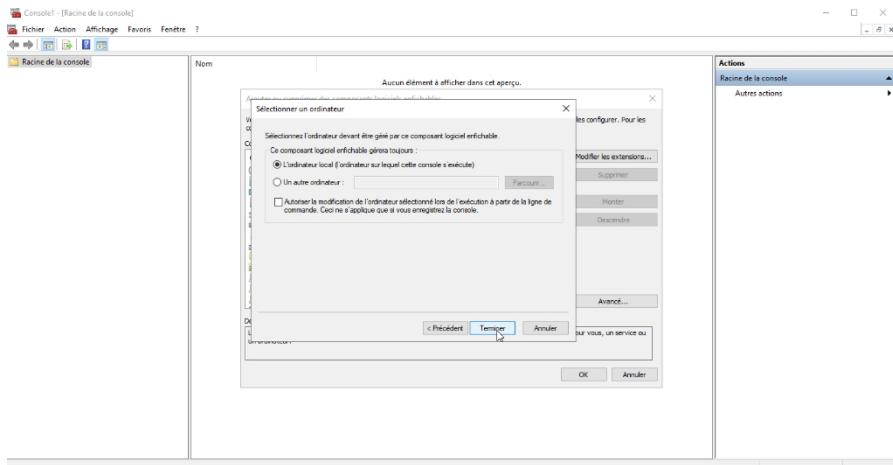
- Appuyez sur la touche Windows + R et tapez « mmc » pour accéder à Microsoft Management Console qui est la console de gestion des outils d'administration :



- Cliquez sur l'onglet « Fichier », sélectionnez « Ajoutez/Supprimer un logiciel enfichable » puis sélectionnez « Certificats » et cliquez sur « Ajouter » :

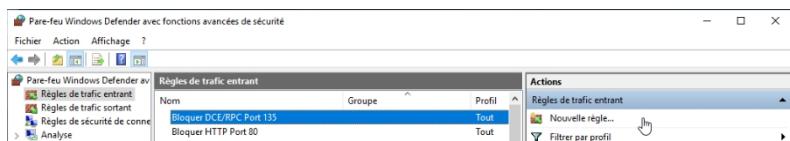


- Une fenêtre va vous demander de choisir un compte, sélectionnez « Un compte d'ordinateur » puis sélectionnez « L'ordinateur local » et cliquez sur « Terminer » :

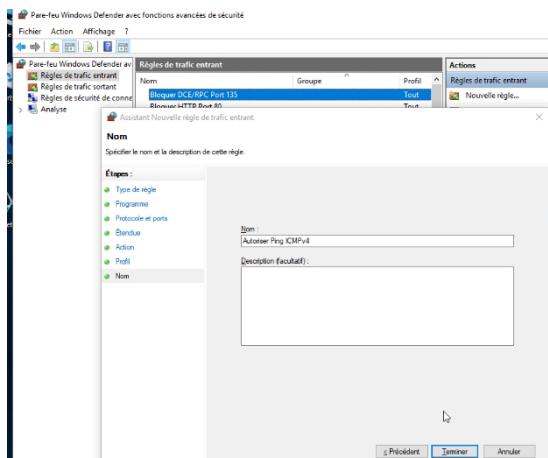


b. Pré configuration du post Windows

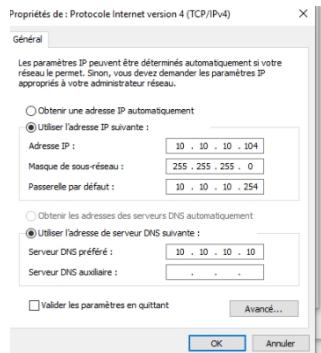
- Pour le post Windows, il faut le joindre au domaine AD du serveur Windows. Paramétrer une règle de pare-feu pour que le serveur ping le post Windows, tapez dans la barre de démarrage « Pare-feu », cliquer sur « Paramètre avancé », puis sur « Règle de trafic entrant » et « Nouvelle règle » :



- Cliquer sur « Personnalisées », puis « Tous les programmes », sélectionner « ICMPv4 », « Suivant », « Autoriser la connexion » puis « Suivant », nommer la règle en « Autoriser Ping ICMPv4 » et cliquer sur « Terminer » :



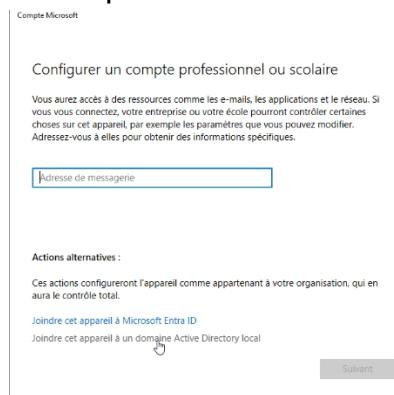
- Configurer la carte réseau du post Windows en lui mettant une IP fixe, masque de sous réseau, Passerelle par défaut et de l'adresse du serveur DNS. Appuyer sur la touche Windows + X, cliquer sur « Connexions réseau », puis sur « Propriété » puis sur « IPv4 » et remplir information comme ci-dessous :



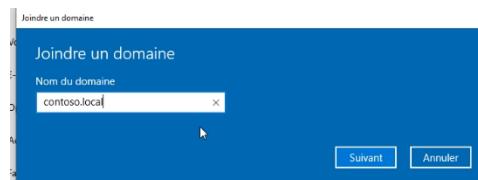
- Taper dans la barre de Démarrage « Compte » puis cliquer sur « Accès Professionnel ou Scolaire » et sur « Se connecter » :



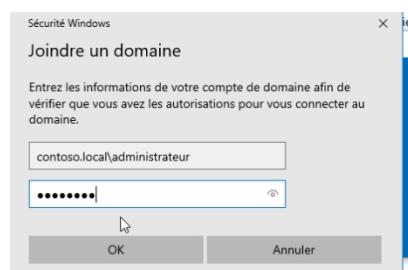
- Cliquer sur « Joindre cet appareil à un domaine Active Directory local » :



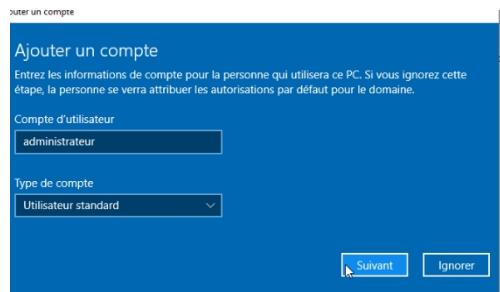
- Taper le nom de domaine :



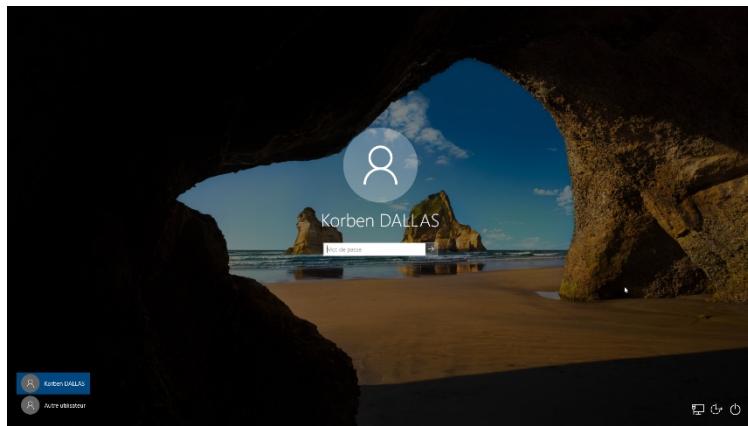
- Taper l'identifiant de l'administrateur et son mot de passe :



- Cliquer sur « Suivant » puis « redémarrer maintenant » :

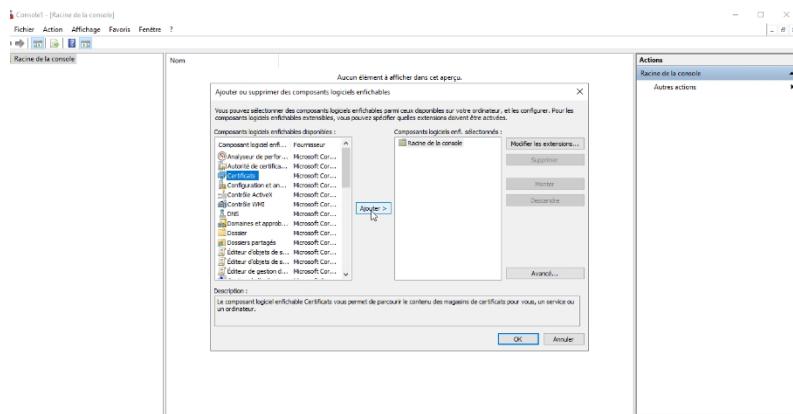


- Vous pouvez vous connecter autant qu'administrateur ou utilisateur :

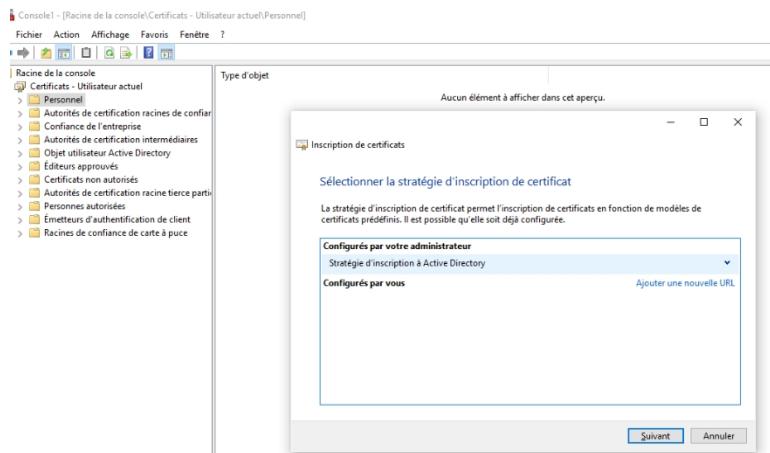


c. Demande de certifications avec le post Windows

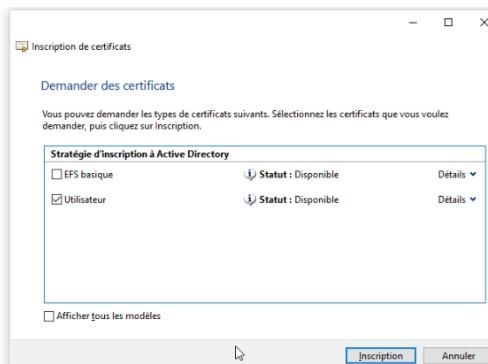
- Appuyer sur la touche Windows + R, trapper « mmc.msc », Cliquez sur l'onglet « Fichier », sélectionnez « Ajoutez/Supprimer un logiciel enfichable » puis sélectionnez « Certificats » et cliquez sur « Ajouter » :



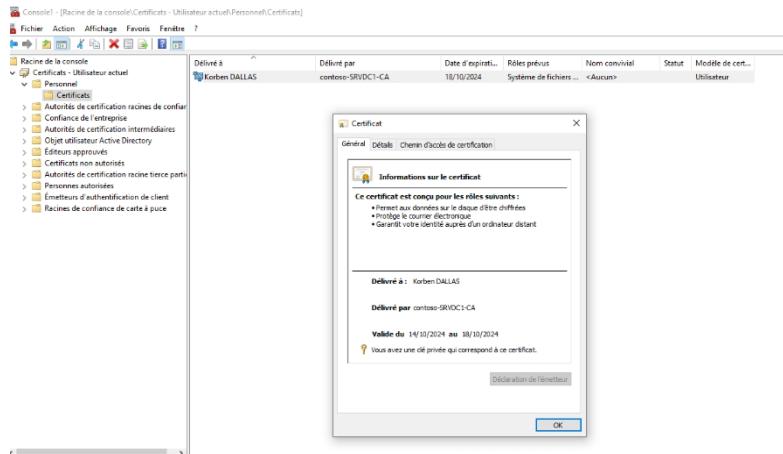
- Dans le « Certificats - Utilisateur actuel », clic droit sur dossier « Personnel » sélectionner « Toutes les tâches » puis cliquer sur « Demander nouveau certificat ». Cliquer sur « Suivant » et sélectionner « Stratégie d'inscription à Active Directory » :



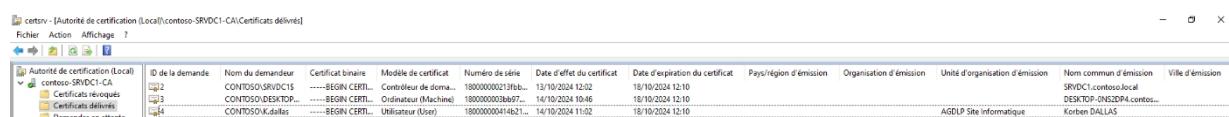
- Sélectionner « Utilisateur », puis cliquer sur « Inscription » et « Terminer » :



- Double cliquer sur le certificat délivré pour voir si le rôle sélectionné sur le serveur est bien le bon :



- Côté serveur on peut voir les certificats délivrés avec l'outil « Autorité de certification », cet outil permet de contrôler les demandes, les modifier ou les révoquer :



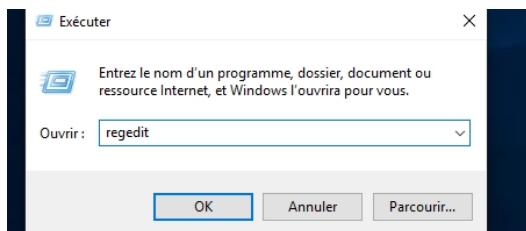
I- Désactivation des protocoles LLMNR et NetBIOS

Désactivation LLMNR et NetBIOS sur les post Windows qui sont des protocoles obsolètes souvent exploiter dans des attaques MITM pour obtenir des informations d'identification via des attaques de type NTLM Relay.

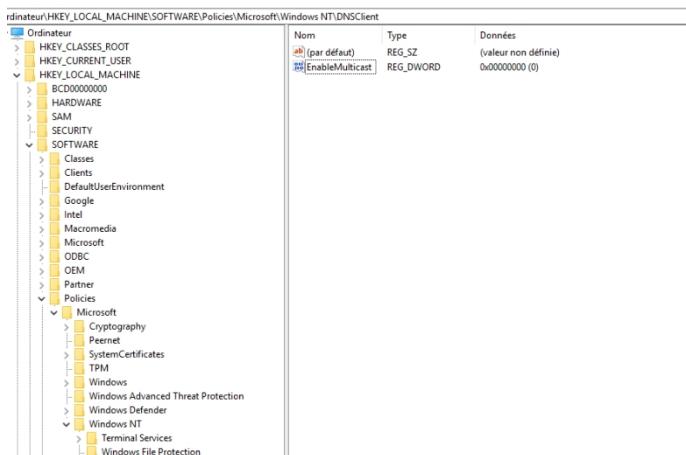
a. Désactivation LLMNR avec éditeur de registre

LLMNR est un protocole utilisé pour la résolution de noms dans les réseaux locaux quand un serveur DNS n'est pas disponible. Cependant, il peut être utilisé par des attaquants pour intercepter ou rediriger le trafic réseau.

- Pour accéder à l'éditeur de registre appuyez sur les touches Windows + R, puis tapez « regedit » :



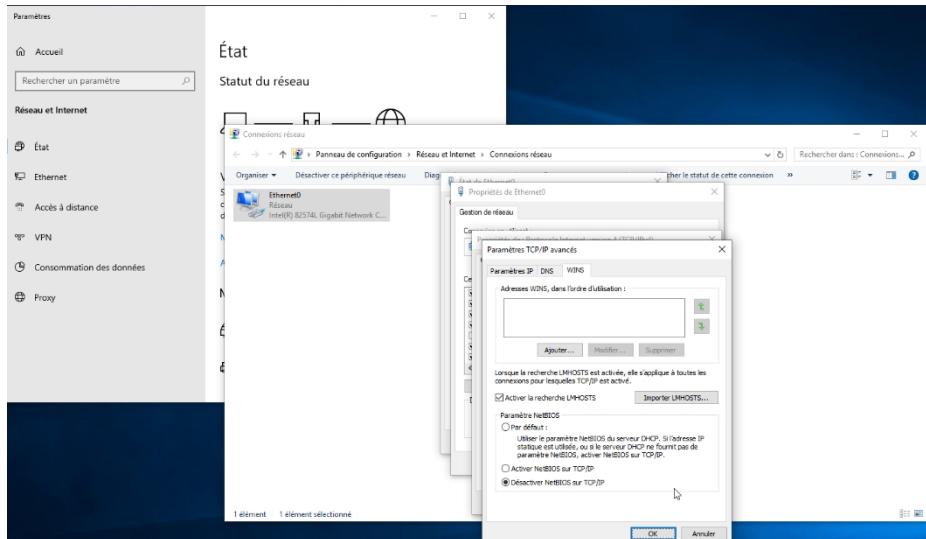
- Accédez à la clé « HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\DNSClient » puis créez une nouvelle valeur DWORD (32-bit) nommé « EnableMulticast » et mettre sa valeur à 0 pour désactiver LLMR :



b. Désactivation NetBIOS

NetBIOS est un ancien protocole de résolution de noms qui fonctionne sur TCP/IP. Il est souvent utilisé dans les réseaux locaux mais peut être une cible pour des attaques d'empoisonnement et de déni de service.

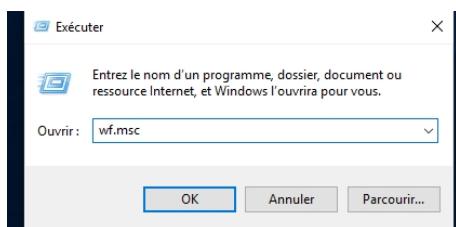
- Appuyez sur les touches Windows + X, sélectionnez « Connexions au réseau », puis sur « Modifier les options d'adaptation ». Cliquez sur la carte réseau à paramétrier, puis sur « Propriétés », puis double cliquez sur « Protocole Internet version 4 (TCP/IP4) » et sur « Avancé » ;
- Allez dans l'onglet « WINS », puis sélectionnez « Désactivez NetBIOS sur TCP/IP » et cliquez sur « OK » :



II- Configuration du Pare-feu

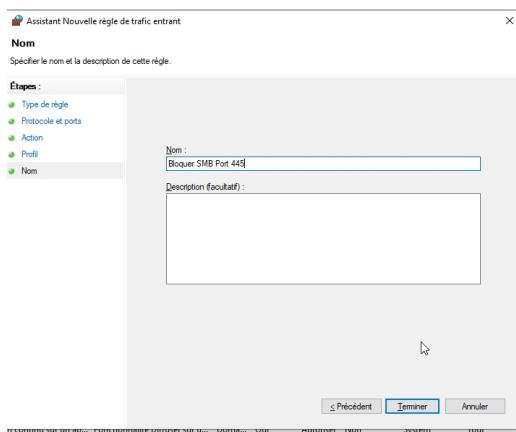
Configurer un pare-feu avec des **règles restrictives** pour limiter les connexions non autorisées à des ports spécifiques et filtrer les paquets ARP non sollicités est essentiel pour améliorer la sécurité de votre réseau. Voici les étapes pour atteindre ces objectifs sous Windows (avec **Windows Defender Firewall**).

- Appuyez sur les touches Windows + R et tapez « wf.msc » :



- Pour créer une règle entrante pour bloquer les connexions non autorisées, cliquez sur « Règles de trafic entrant » au niveau du panneau de gauche. Sélectionnez « Port » puis cochez « TCP » puis tapez le port local spécifique à bloquer ou restreindre comme le port 445 pour SMB :

- Sélectionnez « Bloquer la connexion », gardez cochez tous les types de connexions puis nommer la règle en « Bloquer SMB Port 445 » et cliquez sur « Terminer » :



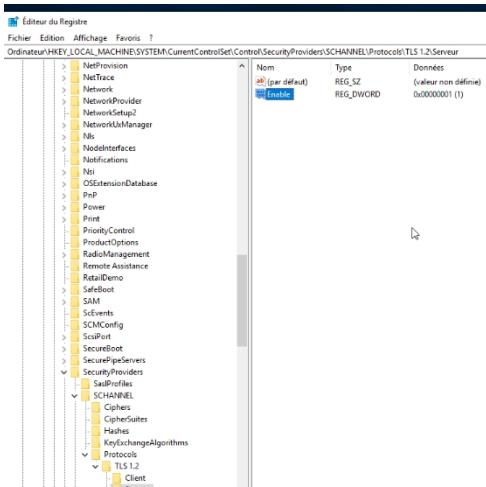
- L'image ci-dessous montre une autre règle à mettre en place pour bloquer des ports sensibles :

Règles de trafic entrant									
Nom	Groupe	Profil	Activée	Action	Remplacer	Programme	Adresse locale	Adresse distante	Protocole
Bloquer DCE/RPC Port 135		Tout	Oui	Bloquer	Non	Tout	Tout	Tout	TCP
Bloquer NetBIOS Port 137		Tout	Oui	Bloquer	Non	Tout	Tout	Tout	TCP
Bloquer HTTP Port 80		Tout	Oui	Bloquer	Non	Tout	Tout	Tout	TCP
Bloquer SMB Port 445		Tout	Oui	Bloquer	Non	Tout	Tout	Tout	TCP

III- Activer le chiffrements TLS

Activer des protocoles de chiffrement forts tels que TLS 1.2 ou TLS 1.3 est une mesure de sécurité importante pour protéger les communications sur Internet.

- Accéder à l'éditeur de registre puis accéder à la clé « HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols ». Si la clé « TLS 1.2 » n'existe pas cliquer gauche sur « Protocols » puis créer la clé avec dedans la clé « Client » et « Serveur ». Pour chaque clé créer une nouvelle valeur DWORD (32-bit) nommée « Enable » et mettre sa valeur à 1 pour activer TLS 1.2 :



IV- Configurer entrées ARP statiques

Pour sécuriser un réseau contre les attaques d'empoisonnement ARP (ARP spoofing), il est utile de configurer des entrées ARP statiques. Cela permet de fixer les adresses MAC associées aux adresses IP des appareils critiques, empêchant ainsi un attaquant de falsifier ces adresses par le biais de requêtes ARP.

- Tapez la commande « arp -s » dans le terminal de commande « cmd » exécuter en tant qu'administrateur en mettant l'IP et l'adresse MAC du client ou du serveur ou d'un routeur pour fixer l'IP et l'adresse MAC de l'appareil :

```
Administrator : Invite de commandes
Microsoft Windows [version 10.0.17763.437]
(c) 2018 Microsoft Corporation. Tous droits réservés.

C:\Windows\system32>arp -s 10.10.10.10 00-0C-29-78-85-3B
```

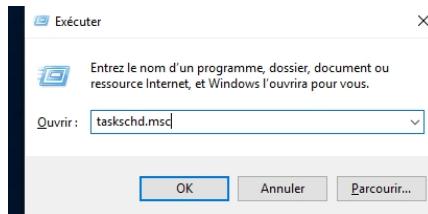
- Pour savoir si elle a été bien prise en compte tapez « arp -a » :

```
C:\Windows\system32>arp -a
Interface : 10.10.10.104 --- 0x6
Adresse Internet    Adresse physique      Type
10.10.10.10          00-0c-29-78-85-3b  statique
10.10.10.150         00-50-56-f7-93-2b  dynamique
10.10.10.254         00-50-56-eb-2f-8d  dynamique
10.10.10.255         ff-ff-ff-ff-ff-ff  statique
224.0.0.22            01-00-5e-00-00-16  statique
224.0.0.251           01-00-5e-00-00-fb  statique
224.0.0.252           01-00-5e-00-00-fc  statique
239.255.255.250      01-00-5e-7f-ff-fa  statique
255.255.255.255      ff-ff-ff-ff-ff-ff  statique
```

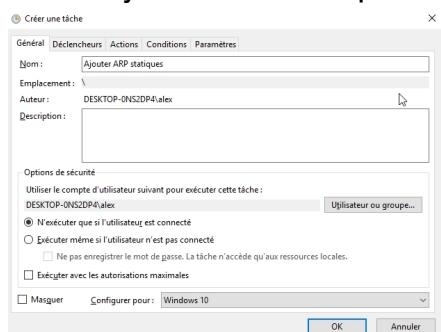
- Automatisation avec script pour remettre ces entrées fixes après chaque démarrage, ouvrir un Bloc-notes et créer un fichier batch nommer « `set_static_arp.bat` » :

 set_static_arp - Bloc-notes
Fichier Edition Format Affichage Aide
@echo off
arp -s 10.10.10.10 00-0c-29-78-85-3b

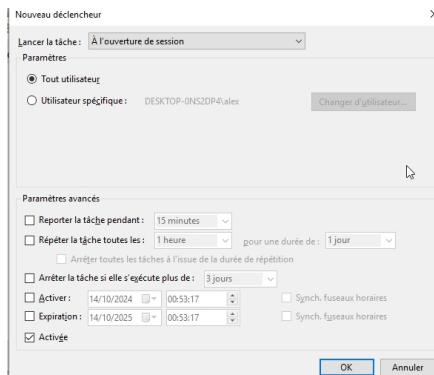
- Enregistrer le sous C:\Script\set_static_arp.bat puis appuyer sur les touches Windows + R et tapez « `taskschd.msc` » :



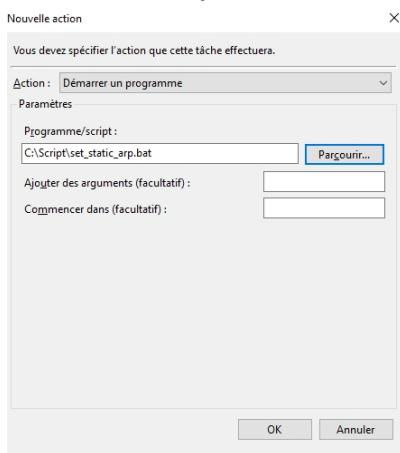
- Cliquez sur Crée une tâche dans le volet droit, donner un nom à la tâche « Ajouter ARP statiques » :



- Dans l'onglet « Déclencheurs », cliquez sur « Nouveau », et sélectionnez « À l'ouverture de session » et sélectionnez pour « Tout utilisateur » puis cliquer sur « Ok » :



- Dans l'onglet « Actions », cliquez sur « Nouveau », puis choisissez « Démarrer un programme » et entrez le chemin vers votre script batch « C:\Script\set_static_arp.bat » et cliquez sur « Ok » pour enregistrer la tâche :



V- Logiciel XArp

XArp est un outil puissant pour la gestion et la surveillance du protocole ARP dans un réseau. En permettant la détection des anomalies et la manipulation des requêtes ARP, il joue un rôle essentiel dans la sécurité réseau et l'analyse des performances. Si vous envisagez d'utiliser ArpX, assurez-vous de comprendre ses fonctionnalités et de l'utiliser de manière éthique et conforme aux politiques de votre organisation.

- Télécharger le via internet, après installation ouvrir le, vous pouvez modifier le niveau de sécurité avec la flèche en haut à droite :

Xarp - unregistered version
[Buy Xarp Professional](#) | [Help](#)

Status: ARP attacks detected!

- [View detected attacks](#)
- [Read the 'Handling ARP attacks' help](#)
- [View Xarp info](#)

Get Xarp Professional now!
[Register Xarp Professional](#)

Security level set to: basic

The basic security level operates a selective detection algorithm that can detect all intended effects. This is the suggested level for default environments.

aggressive
high
basic
minimal

IP	MAC	Host	Vendor	Interface	Online	Cache	First seen	Last seen	How often seen
10.10.10.10	00:0c:29:78:45:2a	10.10.10.10	Vmware, Inc.	Etc - Intel(R) S...	unknown...	yes	14/10/2024 11:42:18	14/10/2024 11:42:24	6
10.10.10.104	00:0c:29:a1-ef-2a	10.10.10.104	Vmware, Inc.	Etc - Intel(R) S...	unknown...	no	14/10/2024 11:42:18	14/10/2024 11:42:24	283
10.10.10.190	00:50:56:a7-4f-40	10.10.10.190	Vmware, Inc.	Etc - Intel(R) S...	unknown...	no	14/10/2024 11:42:22	14/10/2024 11:42:22	1
10.10.10.254	00:50:56:2f-8d	10.10.10.254	Vmware, Inc.	Etc - Intel(R) S...	unknown...	yes	14/10/2024 11:42:24	14/10/2024 11:42:24	3

Xarp - -->

OK

< Alert 4 of 7 >

14/10/2024 11:31:58

DirectARPRequestFilter: targeted request.
destination mac of arp request not set to broadcast/invalid address

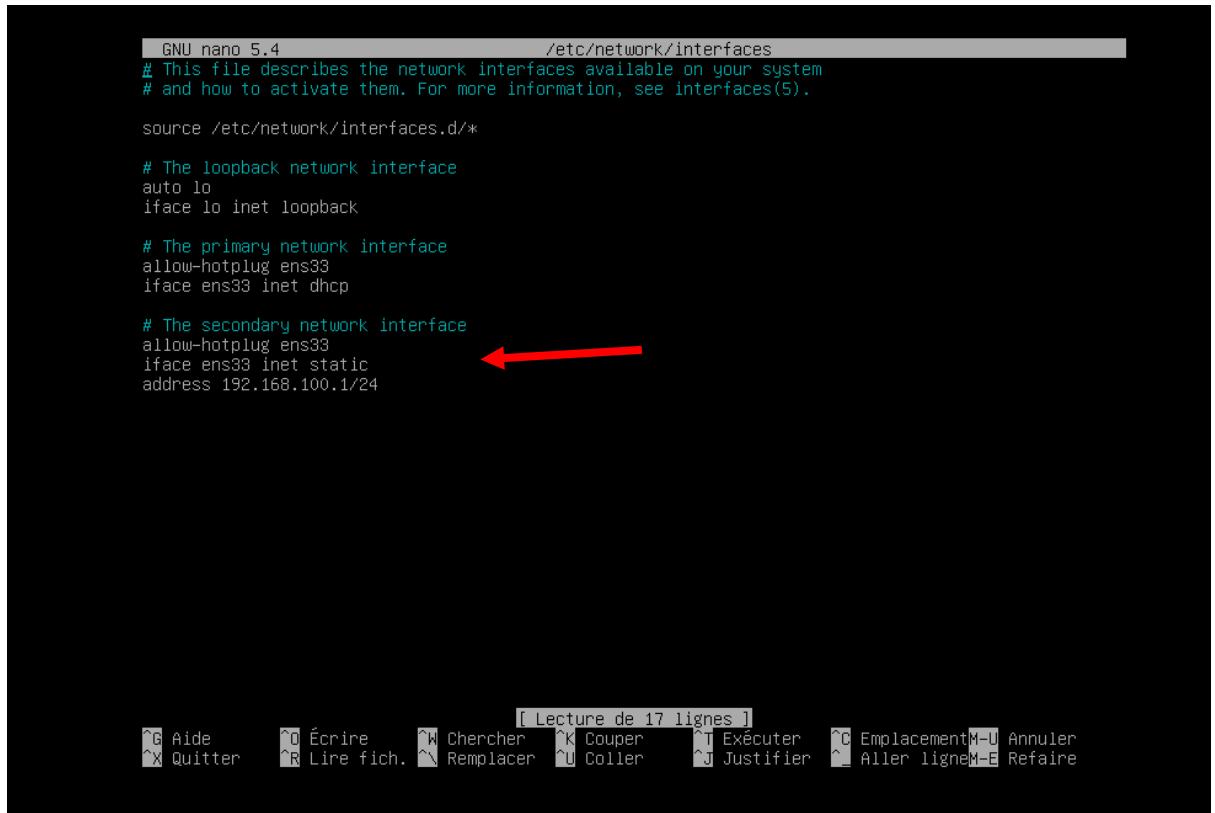
```
Interface : 0mc
[...]
source mac: 00:0c:29:78:45:2a
dest mac : 00:50:56:a7-4f-8d
: b8:b7:6
[arp]
direction : out
type : request
source ip : 10.10.10.104
dest ip : 10.10.10.104
source mac: 00:0c:29:a1-ef-2a
dest mac : 00:50:56:a7-4f-40
```

Xarp 2.2.2 • 4 mappings • 1 interface • 3 alerts

SECURISATION LINUX

I- Configuration du serveur DHCP sous Debian 11

- On met une IP Static à la machine virtuelle en la renseignant dans le fichier de configuration : nano /etc/network/interfaces



```
GNU nano 5.4          /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug ens33
iface ens33 inet dhcp

# The secondary network interface
allow-hotplug ens33
iface ens33 inet static
    address 192.168.100.1/24

[ Lecture de 17 lignes ]
^G Aide      ^O Écrire      ^W Chercher      ^K Couper      ^T Exécuter      ^C Emplacement^M-U Annuler
^X Quitter   ^R Lire fich.  ^V Remplacer   ^U Coller       ^J Justifier   ^L Aller ligne^M-E Refaire
```

- On vérifie que l'IP s'est bien mise.

```
Debian GNU/Linux 11 debian11-CORE tty1

debian11-CORE login: root
Password:
Linux debian11-CORE 5.10.0-18-amd64 #1 SMP Debian 5.10.140-1 (2022-09-02) x86_64

The programs included with the Debian GNU/Linux system are free software;
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.
Last login: Tue Oct 15 09:20:14 CEST 2024 on tty1
root@debian11-CORE:~# 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
            valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:3f:b4:19 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
        inet 192.168.100.1/24 brd 192.168.100.255 scope global ens33
            valid_lft forever preferred_lft forever
        inet6 fe80::20c:29ff:fe3f:b419/64 scope link
            valid_lft forever preferred_lft forever
root@debian11-CORE:~#
```

- On installe les paquets DHCP

```
root@debian11-CORE:~# apt install isc-dhcp-server
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
isc-dhcp-server est déjà la version la plus récente (4.4.1-2.3+deb11u1).
Les paquets suivants ont été installés automatiquement et ne sont plus nécessaires :
  apache2-bin apache2-data apache2-utils libapr1 libaprutil1 libaprutil1-db-sqlite3
  libaprutil1-ldap libcurl4 liblua5.3-0 libwrap0 openssh-sftp-server runit-helper ssl-cert
Veuillez utiliser « apt autoremove » pour les supprimer.
0 mis à jour, 0 nouvellement installés, 0 à enlever et 0 non mis à jour.
root@debian11-CORE:~# _
```

- On renseigne dans le fichier `/etc/default/isc-dhcp-server` l'interface sur laquelle va écouter le service DHCP. Dans notre cas c'est « `ens33` ».

```
GNU nano 5.4                               /etc/default/isc-dhcp-server
# Defaults for isc-dhcp-server (sourced by /etc/init.d/isc-dhcp-server)

# Path to dhcpcd's config file (default: /etc/dhcp/dhcpcd.conf).
DHCPDV4_CONF=/etc/dhcp/dhcpcd.conf
#DHCPDV6_CONF=/etc/dhcp/dhcpcd6.conf

# Path to dhcpcd's PID file (default: /var/run/dhcpcd.pid).
#DHCPDV4_PID=/var/run/dhcpcd.pid
#DHCPDV6_PID=/var/run/dhcpcd6.pid

# Additional options to start dhcpcd with.
#       Don't use options -cf or -pf here; use DHCPD_CONF/ DHCPD_PID instead
#OPTIONS=""

# On what interfaces should the DHCP server (dhcpcd) serve DHCP requests?
#       Separate multiple interfaces with spaces, e.g. "eth0 eth1".
INTERFACESv4="ens33"                         ←
INTERFACESv6=""
```

[Lecture de 18 lignes]

^G Aide **^O Écrire** **^W Chercher** **^K Couper** **^T Exécuter** **^C Emplacement****M-U Annuler**
^X Quitter **^R Lire fich.** **^Y Remplacer** **^U Coller** **^J Justifier** **^L Aller ligne****M-E Refaire**

- On configure les options du serveur DHCP dans le fichier `/etc/dhcp/dhcpd.conf`

On a renseigné la durée de bail sur 24 heures ainsi que la durée maximale sur 48 heures.

```
GNU nano 5.4                               /etc/dhcp/dhcpd.conf

# dhcpd.conf
#
# Sample configuration file for ISC dhcpcd

#
# option definitions common to all supported networks...
option domain-name "example.org";
option domain-name-servers ns1.example.org, ns2.example.org;

# Bail de 24H
default-lease-time 86400;                  ←
# Bail maxi de 48H
max-lease-time 172800;

# The ddns-updates-style parameter controls whether or not the server will
# attempt to do a DNS update when a lease is confirmed. We default to the
# behavior of the version 2 packages ('none', since DHCP v2 didn't
# have support for DDNS.)
ddns-update-style none;

# If this DHCP server is the official DHCP server for the local
# network, the authoritative directive should be uncommented.
#authoritative;

# Use this to send dhcp log messages to a different log file (you also
# have to hack syslog.conf to complete the redirection).
#log-facility local7;

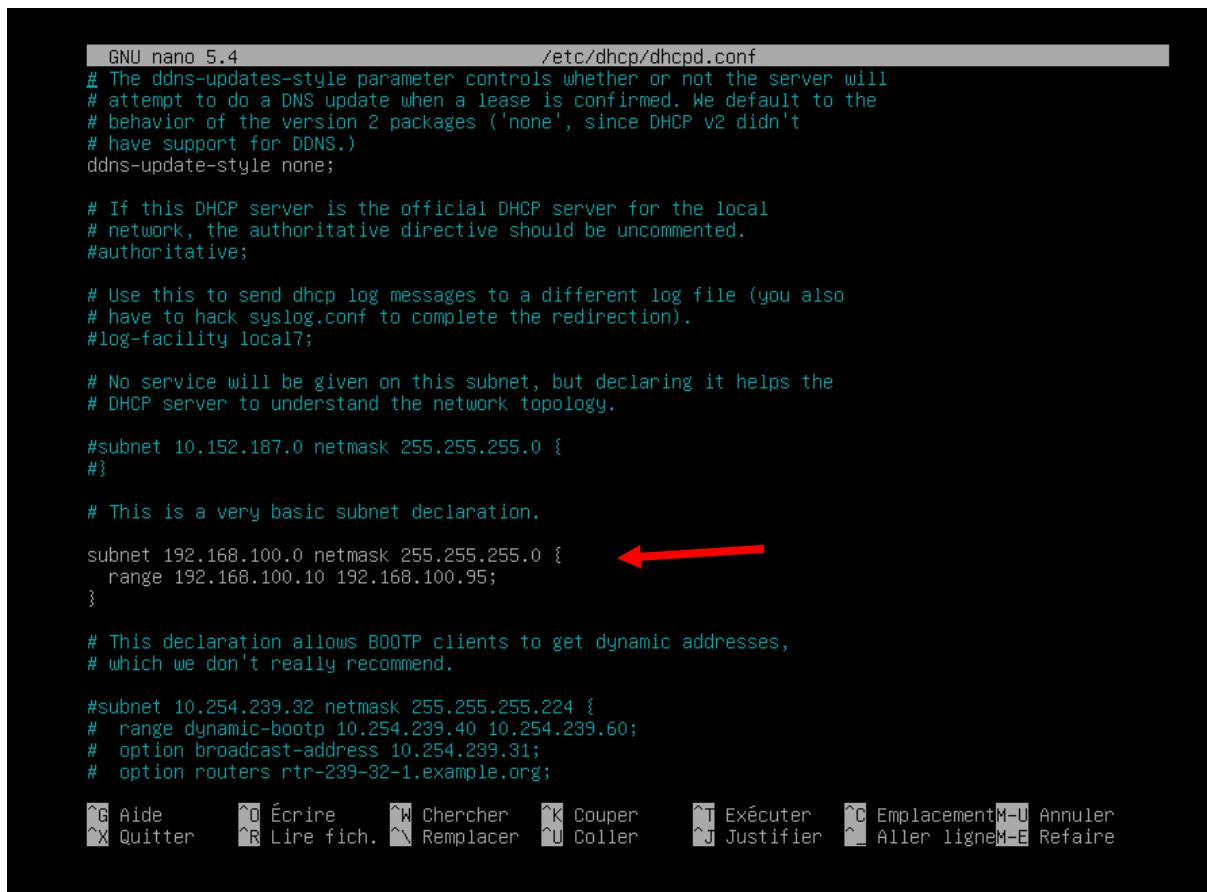
# No service will be given on this subnet, but declaring it helps the
# DHCP server to understand the network topology.

#subnet 10.152.187.0 netmask 255.255.255.0 {
#}

[ Lecture de 108 lignes ]

^G Aide      ^O Écrire      ^K Chercher      ^C Couper      ^T Exécuter      ^C Emplacement M-U Annuler
^X Quitter   ^R Lire fich.  ^V Remplacer   ^U Coller       ^J Justifier   ^L Aller ligne M-E Refaire
```

- On renseigne également l'adresse du réseau, le masque de sous-réseau ainsi que la plage d'adresse.



```

GNU nano 5.4                               /etc/dhcp/dhcpd.conf
# The ddns-updates-style parameter controls whether or not the server will
# attempt to do a DNS update when a lease is confirmed. We default to the
# behavior of the version 2 packages ('none', since DHCP v2 didn't
# have support for DDNS.)
ddns-update-style none;

# If this DHCP server is the official DHCP server for the local
# network, the authoritative directive should be uncommented.
#authoritative;

# Use this to send dhcp log messages to a different log file (you also
# have to hack syslog.conf to complete the redirection).
#log-facility local7;

# No service will be given on this subnet, but declaring it helps the
# DHCP server to understand the network topology.

#subnet 10.152.187.0 netmask 255.255.255.0 {
#}

# This is a very basic subnet declaration.

subnet 192.168.100.0 netmask 255.255.255.0 {           ←
    range 192.168.100.10 192.168.100.95;
}

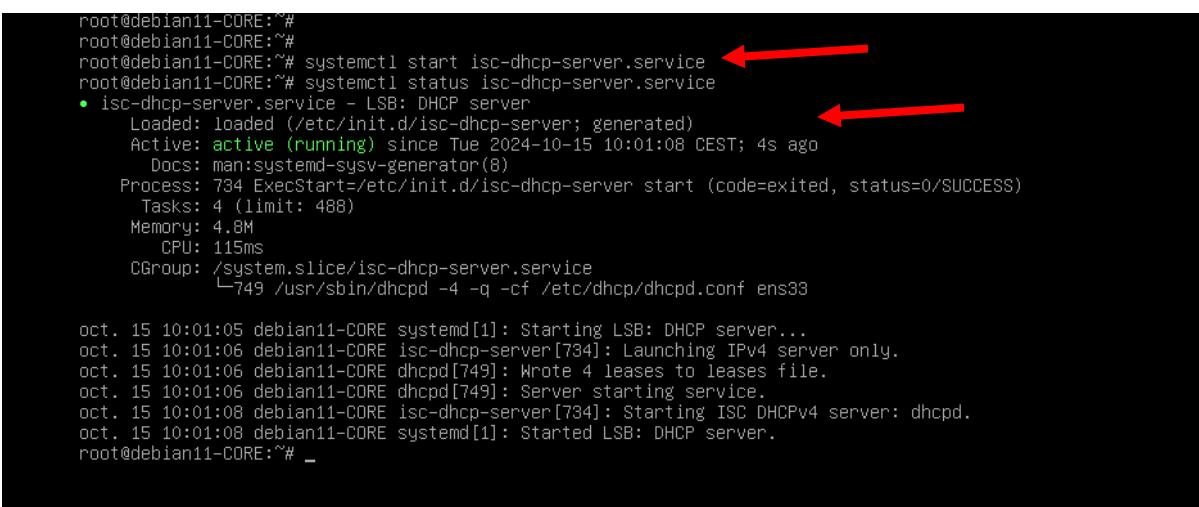
# This declaration allows BOOTP clients to get dynamic addresses,
# which we don't really recommend.

#subnet 10.254.239.32 netmask 255.255.255.224 {
#    range dynamic-bootp 10.254.239.40 10.254.239.60;
#    option broadcast-address 10.254.239.31;
#    option routers rtr-239-32-1.example.org;

```

^A Aide ^O Écrire ^W Chercher ^K Couper ^T Exécuter ^C Emplacement M-U Annuler
 ^X Quitter ^R Lire fich. ^U Remplacer ^J Justifier ^L Aller ligne M-E Refaire

- On n'oublie pas de démarrer le service DHCP avec la commande : `systemctl start isc-dhcp-server`
 Et de vérifier que le service est bien actif avec la commande : `systemctl status isc-dhcp-server`



```

root@debian11-CORE:~#
root@debian11-CORE:~#
root@debian11-CORE:~# systemctl start isc-dhcp-server.service           ←
root@debian11-CORE:~# 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 2024-10-15 10:01:08 CEST; 4s ago
     Docs: man:systemd-sysv-generator(8)
   Process: 734 ExecStart=/etc/init.d/isc-dhcp-server start (code=exited, status=0/SUCCESS)
   Tasks: 4 (limit: 488)
   Memory: 4.8M
      CPU: 115ms
   CGroup: /system.slice/isc-dhcp-server.service
           └─749 /usr/sbin/dhcpd -4 -q -cf /etc/dhcp/dhcpd.conf ens33

oct. 15 10:01:05 debian11-CORE systemd[1]: Starting LSB: DHCP server...
oct. 15 10:01:06 debian11-CORE isc-dhcp-server[734]: Launching IPv4 server only.
oct. 15 10:01:06 debian11-CORE dhcpcd[749]: Wrote 4 leases to leases file.
oct. 15 10:01:06 debian11-CORE dhcpcd[749]: Server starting service.
oct. 15 10:01:08 debian11-CORE isc-dhcp-server[734]: Starting ISC DHCPv4 server: dhcpd.
oct. 15 10:01:08 debian11-CORE systemd[1]: Started LSB: DHCP server.
root@debian11-CORE:~# 

```

- Une fois le service lancé, on accède au client Linux Mint et on s'assure qu'il obtient bien une adresse IP correspondant à la plage d'adresse renseigné dans le service DHCP.

```

linuxmint@linuxmint-virtual-machine:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    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: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default
    link/ether 00:0c:29:9a:42:9e brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.100.10/24 brd 192.168.100.255 scope global dynamic noprefixroute
        valid_lft 85169sec preferred_lft 85169sec
        inet6 fe80::23f3:dbd1:cf1e:5b74/64 scope link noprefixroute
            valid_lft forever preferred_lft forever
linuxmint@linuxmint-virtual-machine:~$ █

```

II- Sécurisation du client Linux Mint

- On commence par sécuriser contre les attaques DHCP après avoir obtenu une IP du DHCP

Pour ce faire, on utilise `iptables` pour bloquer les paquets DHCP non légitimes sur les ports 67 et 68 qui correspondent aux ports serveurs et clients pour envoyer des réponses et des requêtes DHCP.

```

linuxmint@linuxmint-virtual-machine:~$ sudo iptables -A INPUT -p udp --sport 67:68 --dport 67:68 -j DROP
linuxmint@linuxmint-virtual-machine:~$ █

```

- Enfin on sécurise contre les attaques ARP Poisoning.

On ajoute une entrée ARP Statique qui correspond dans notre cas à l'adresse IP et l'adresse MAC du routeur. Ainsi on s'assure de la correspondance adresse IP/MAC et qui ne peut pas être altérer par des attaquants.

```
linuxmint@linuxmint-virtual-machine:~$ sudo arp -s 192.168.100.2 00:0c:29:87:a7:13
[sudo] Mot de passe de linuxmint :
linuxmint@linuxmint-virtual-machine:~$
```

SECURISATION COMMUTATEURS CISCO

1. Protection des ports (Port Security)

Le **Port Security** sur un switch Cisco permet de contrôler et limiter le nombre de périphériques autorisés à se connecter à un port physique. Cela protège contre les accès non autorisés et les attaques comme l'usurpation d'adresses MAC.

Objectif principal du port security :

- Empêcher l'accès au réseau à des périphériques non autorisés en limitant le nombre d'adresses MAC que chaque port peut apprendre et accepter.

Avantages du port security :

- **Sécurité accrue** : Réduit les risques d'accès non autorisés.
- **Prévention des usurpations d'adresses MAC**.
- **Contrôle strict des périphériques** autorisés sur le réseau.

Fonctionnalités clés du port security :

- Limitation du nombre de périphériques connectés par port.
- **Apprentissage des adresses MAC** :
 - **Statique** : Adresses configurées manuellement.
 - **Dynamique** : Adresses apprises temporairement.
 - **Sticky** : Adresses apprises de façon persistante après redémarrage.

Actions en cas de violation :

- **Protect** : Bloque les paquets non autorisés tout en maintenant le port actif.
- **Restrict** : Bloque les paquets et génère des alertes.
- **Shutdown** : Désactive le port en cas de violation.

Exemple de configuration :

```
Switch(config)# interface fastEthernet 0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 2
Switch(config-if)# switchport port-security violation shutdown
Switch(config-if)# switchport port-security mac-address sticky
```

2. Mise en place du DHCP Snooping

Le **DHCP Snooping** surveille et filtre les messages DHCP pour prévenir des attaques comme le DHCP spoofing ou starvation.

Fonctionnement :

- **Ports de confiance (trusted)** : Autorise tous les messages DHCP.
- **Ports non fiables (untrusted)** : Bloque les réponses DHCP non autorisées.

Protection contre les attaques DHCP :

- **DHCP Spoofing** : Bloque les serveurs DHCP non autorisés.

- **DHCP Starvation** : Limite le nombre de requêtes DHCP par port.

Exemple de configuration :

```
Switch(config)# ip dhcp snooping
Switch(config)# ip dhcp snooping vlan 10
Switch(config)# interface fastEthernet 0/1
Switch(config-if)# ip dhcp snooping trust
Switch(config)# interface range fastEthernet 0/2 - 24
Switch(config-if-range)# ip dhcp snooping limit rate 10
```

3. Activation du Dynamic ARP Inspection (DAI)

Le **Dynamic ARP Inspection (DAI)** protège contre les attaques **ARP Spoofing** en vérifiant l'authenticité des requêtes ARP.

Objectif principal :

- Empêcher l'usurpation d'adresses ARP en validant les correspondances entre adresses IP et MAC.

Fonctionnalités clés du DAI :

- Vérification des paquets ARP avec la table DHCP snooping.
- **Ports de confiance (trusted)** : Non soumis à l'inspection ARP.
- **Ports non fiables (untrusted)** : Inspection stricte des paquets ARP.

Exemple de configuration :

```
Switch(config)# ip arp inspection vlan 10
Switch(config)# interface fastEthernet 0/1
Switch(config-if)# ip arp inspection trust
Switch(config)# interface range fastEthernet 0/2 - 24
Switch(config-if-range)# ip arp inspection limit rate 15
```

4. Activation du Storm Control

Le **Storm Control** limite le trafic réseau indésirable généré par des tempêtes de broadcast, multicast ou unicast inconnu.

Objectif principal :

- Empêcher les tempêtes de trafic qui peuvent submerger le réseau.

Fonctionnalités clés du Storm Control :

- **Limitation du trafic par type** : Broadcast, Multicast, ou Unicast inconnu.
- **Seuil de déclenchement** : Pourcentage de la bande passante pour chaque type de trafic.

Exemple de configuration :

```
Switch(config)# interface fastEthernet 0/1
Switch(config-if)# storm-control broadcast level 10.00
Switch(config-if)# storm-control multicast level 5.00
Switch(config-if)# storm-control unicast level 5.00
```

```
Switch(config-if)# storm-control action shutdown
```