

## Table des matières

Configurations de base.....	2
Accès aux paramètres réseau.....	2
Nommer la machine .....	4
Set date & timezone .....	4
Enabling Remote Desktop (RDP) On the Core Server .....	5
Adding a local administrator account backdoor .....	6
Restart and update the server.....	7
Checking Settings and configuration after rebooting.....	8
Launching PowerShell on the CORE Server .....	10
Enabling PowerShell Remoting .....	10
Enabling ICMP "Ping" .....	10
Disable WinProxy Settings (If Necessary) .....	10
Set CORE Server for PowerShell Remote Management Rights .....	11
Optional Firewall Settings You Might Choose:.....	11
Enable Remote Management in Current Firewall Profile Settings .....	11
Disabling the Firewall Entirely During the Setup Process (Optional).....	11
Updating CORE Server Using "sconfig".....	12
Attention.....	12
Tester si une règle de pare-feu bloque DNS.....	14

# Configurer Windows Server CORE

(pour aller plus loin & pour aller encore plus loin)

## Configurations de base

<https://www.youtube.com/watch?v=HfF9VdwavyQ&list=PLZcHRARJMstVNn8Q2wMwu7loNLBgg8UsB>

Menu

```
ca: SConfig: Windows Server 2025 Standard Evaluation, WIN-8H5AGCJQD68
=====
Bienvenue dans Windows Server 2025 Standard Evaluation
=====

1) Domaine ou groupe de travail :      Groupe de travail : WORKGROUP
2) Nom de l'ordinateur :              WIN-8H5AGCJQD68
3) Ajouter l'administrateur local
4) Gestion à distance :             Activé
5) Paramètre de mise à jour :        Téléchargez uniquement
6) Installer les mises à jour
7) Bureau à distance :              Désactivé
8) Paramètres réseau
9) Date et heure
10) Paramètre des données de diagnostic : Nécessaire
11) Activation de Windows
12) Fermer la session utilisateur
13) Redémarrer le serveur
14) Arrêter le serveur
15) Quitter vers la ligne de commande (PowerShell)

Entrez un nombre pour sélectionner une option: 8.
```

## Accès aux paramètres réseau

```
=====
Paramètres réseau
=====

Cartes réseau disponibles :
# | Adresse IP      | Nom          | Description
5 | 169.254.193.54 | Ethernet0   | Intel(R) 82574L Gigabit Network Connecti...
Sélectionnez le numéro d'index de la carte réseau (Vide = annuler): 5.
```

On veut définir l'adresse de la carte réseau (Network adapter Address)

SConfig: Windows Server 2025 Standard Evaluation, WIN-8H5AGCJQD68

```
=====
Paramètres de carte réseau
=====

Index NIC :      5
Nom :          Ethernet0
Description :   Intel(R) 82574L Gigabit Network Connection
Adresse IP :   169.254.193.54,
                fe80::5872:4cd5:fcd8:6ca3
Masque de sous-réseau : 255.255.0.0
DHCP activé :   True

Passerelle par défaut : 192.168.1.1
1er serveur DNS :     9.9.9.9
2e serveur DNS :     1.1.1.1
3e serveur DNS :

1) Définir l'adresse de la carte réseau
2) Définir les serveurs DNS
3) Effacer les paramètres du serveur DNS
4) Renommer la carte réseau

Entrez la sélection (Vide = annuler): 1
Sélectionnez le protocole (D)HCP ou l'adresse IP (S)tatique (Vide = annuler): S
Entrer une adresse IP statique : (Vide = annuler): 192.168.1.31
Entrer un masque de sous-réseau (Vide=255.255.255.0):
Entrez la passerelle par défaut (Vide = annuler): 192.168.1.1
```

L'adressage statique a été correctement activé. DHCP n'est pas activé pour cette carte réseau.  
La passerelle a été correctement définie.  
Définition de l'adresse de la carte réseau effectuée avec succès.  
(Appuyez sur ENTRÉE pour continuer): ■

TADAM !

SConfig: Windows Server 2025 Standard Evaluation, WIN-8H5AGCJQD68

```
=====
Paramètres de carte réseau
=====

Index NIC :      5
Nom :          Ethernet0
Description :   Intel(R) 82574L Gigabit Network Connection
Adresse IP :   192.168.1.31,
                fe80::5872:4cd5:fcd8:6ca3
Masque de sous-réseau : 255.255.255.0
DHCP activé :   False

Passerelle par défaut : 192.168.1.1
1er serveur DNS :     9.9.9.9
2e serveur DNS :     1.1.1.1
3e serveur DNS :

1) Définir l'adresse de la carte réseau
2) Définir les serveurs DNS
3) Effacer les paramètres du serveur DNS
4) Renommer la carte réseau

Entrez la sélection (Vide = annuler):
```

## Nommer la machine

```
SCConfig: Windows Server 2025 Standard Evaluation, WIN-8H5AGCJQD68

=====
 Bienvenue dans Windows Server 2025 Standard Evaluation
=====

1) Domaine ou groupe de travail :      Groupe de travail : WORKGROUP
2) Nom de l'ordinateur :             WIN-8H5AGCJQD68
3) Ajouter l'administrateur local
4) Gestion à distance :            Activé

5) Paramètre de mise à jour :       Téléchargez uniquement
6) Installer les mises à jour
7) Bureau à distance :            Désactivé

8) Paramètres réseau
9) Date et heure
10) Paramètre des données de diagnostic : Nécessaire
11) Activation de Windows

12) Fermer la session utilisateur
13) Redémarrer le serveur
14) Arrêter le serveur
15) Quitter vers la ligne de commande (PowerShell)

Entrez un nombre pour sélectionner une option: 2
```

```
SCConfig: Windows Server 2025 Standard Evaluation, WIN-8H5AGCJQD68

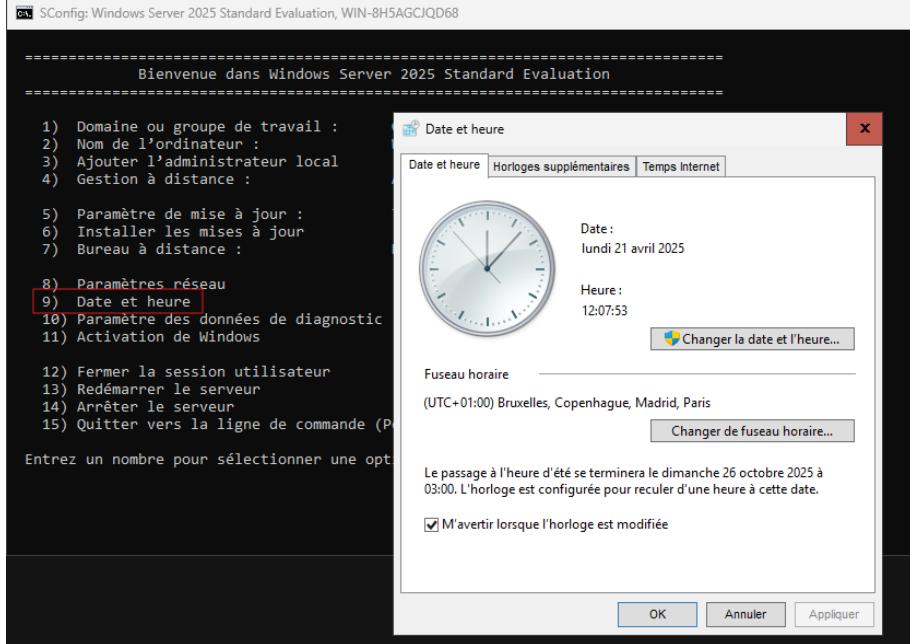
=====
 Nom de l'ordinateur
=====

Nom de l'ordinateur actuel : WIN-8H5AGCJQD68

Entrer un nouveau nom d'ordinateur (Vide = annuler): SRV-DC-01
Modification en cours du nom d'ordinateur... Merci de patienter.
AVERTISSEMENT : Les modifications seront prises en compte après le redémarrage de l'ordinateur WIN-8H5AGCJQD68.
Redémarrer maintenant ? (O)ui ou (N)on:
```

## Set date & timezone

= paramètre necessary for replication



## Enabling Remote Desktop (RDP) On the Core Server

Just to make things easier to set up we're gonna choose the option the less secure (but they will be expelled then from our configuration settings)

```
■ SConfig: Windows Server 2025 Standard Evaluation, WIN-8H5AGCJQD68
=====
Bienvenue dans Windows Server 2025 Standard Evaluation
=====

1) Domaine ou groupe de travail :      Groupe de travail : WORKGROUP
2) Nom de l'ordinateur :             WIN-8H5AGCJQD68
3) Ajouter l'administrateur local
4) Gestion à distance :             Activé
5) Paramètre de mise à jour :        Téléchargez uniquement
6) Installer les mises à jour
7) Bureau à distance :              Activé (tous les clients)

8) Paramètres réseau
9) Date et heure
10) Paramètre des données de diagnostic : Nécessaire
11) Activation de Windows

12) Fermer la session utilisateur
13) Redémarrer le serveur
14) Arrêter le serveur
15) Quitter vers la ligne de commande (PowerShell)

Entrez un nombre pour sélectionner une option: 7
```

```
■ SConfig: Windows Server 2025 Standard Evaluation, WIN-8H5AGCJQD68
=====
Bureau à distance
=====

Statut du bureau à distance : Désactivé

Souhaitez-vous (A)ctiver ou (D)ésactiver le Bureau à distance? (Vide = annuler): A

 1) Autoriser uniquement les clients exécutant le Bureau à distance l'authentification au niveau du réseau (NLA) qui
est plus sécurisée
 2) Autoriser les clients exécutant n'importe quelle version du Bureau à distance (moins sécurisé)

Entrez la sélection (Vide = annuler): 2
Activation du Bureau à distance...
La configuration du Bureau à distance a correctement réussi.
(Appuyez sur ENTRÉE pour continuer):
```

## Adding a local administrator account backdoor

Voir raison de cette config dans Deepseek prompt sur les bonnes pratiques de nomination des machines AD.

```
cl SConfig: Windows Server 2025 Standard Evaluation, WIN-8H5AGCJQD68
```

```
=====
 Bienvenue dans Windows Server 2025 Standard Evaluation
=====

 1) Domaine ou groupe de travail : Groupe de travail : WORKGROUP
 2) Nom de l'ordinateur : WIN-8H5AGCJQD68
 3) Ajouter l'administrateur local
 4) Gestion à distance : Activé

 5) Paramètre de mise à jour : Téléchargez uniquement
 6) Installer les mises à jour
 7) Bureau à distance : Activé (tous les clients)

 8) Paramètres réseau
 9) Date et heure
 10) Paramètre des données de diagnostic : Nécessaire
 11) Activation de Windows

 12) Fermer la session utilisateur
 13) Redémarrer le serveur
 14) Arrêter le serveur
 15) Quitter vers la ligne de commande (PowerShell)
```

```
Entrez un nombre pour sélectionner une option: 3
```

```
cl SConfig: Windows Server 2025 Standard Evaluation, WIN-8H5AGCJQD68
```

```
=====
 Ajouter l'administrateur local
=====

Si l'utilisateur spécifié n'existe pas, il sera créé.
Spécifier l'utilisateur à ajouter au groupe d'administrateurs local (Vide = annuler): BackDoor
Mot de passe de BackDoor: *****
Un utilisateur a été créé.
Ajout en cours de BackDoor au groupe d'administrateurs local... Merci de patienter.
BackDoor est correctement ajouté au groupe d'administrateurs local.
(Appuyez sur ENTRÉE pour continuer):
```

MDP = Orangina.98

## Restart and update the server

On restart le système :

```
SConfig: Windows Server 2025 Standard Evaluation, WIN-8H5AGCJQD68
```

```
=====
 Bienvenue dans Windows Server 2025 Standard Evaluation
=====

 1) Domaine ou groupe de travail : Groupe de travail : WORKGROUP
 2) Nom de l'ordinateur : WIN-8H5AGCJQD68
 3) Ajouter l'administrateur local
 4) Gestion à distance : Activé

 5) Paramètre de mise à jour : Téléchargez uniquement
 6) Installer les mises à jour
 7) Bureau à distance : Activé (tous les clients)

 8) Paramètres réseau
 9) Date et heure
 10) Paramètre des données de diagnostic : Nécessaire
 11) Activation de Windows

 12) Fermer la session utilisateur
 13) Redémarrer le serveur
 14) Arrêter le serveur
 15) Quitter vers la ligne de commande (PowerShell)
```

```
Entrez un nombre pour sélectionner une option: 13
Voulez-vous vraiment redémarrer ? (O)ui ou (N)on: -
```

## Checking Settings and configuration after rebooting

Vérifier l'adresse IP :

```
SConfig: Windows Server 2025 Standard Evaluation, SRV-DC-01
```

```
AVERTISSEMENT : Pour empêcher le lancement de SConfig lors de la connexion, tapez
=====
 Bienvenue dans Windows Server 2025 Standard Evaluation
=====

 1) Domaine ou groupe de travail : Groupe de travail : WORKGROUP
 2) Nom de l'ordinateur : SRV-DC-01
 3) Ajouter l'administrateur local
 4) Gestion à distance : Activé

 5) Paramètre de mise à jour : Téléchargez uniquement
 6) Installer les mises à jour
 7) Bureau à distance : Activé (tous les clients)

 8) Paramètres réseau
 9) Date et heure
 10) Paramètre des données de diagnostic : Nécessaire
 11) Activation de Windows

 12) Fermer la session utilisateur
 13) Redémarrer le serveur
 14) Arrêter le serveur
 15) Quitter vers la ligne de commande (PowerShell)

Entrez un nombre pour sélectionner une option: 15-
```

Également nous pourrions tester une connexion SSH pour être sûre :7

```
Administrator : C:\WINDOWS\system32\cmd.exe
AVERTISSEMENT : Pour lancer de nouveau l'outil de configuration du serveur, exéutez « SConfig »
PS C:\Users\Administrateur> ipconfig

Configuration IP de Windows

Carte Ethernet Ethernet0 :

    Suffixe DNS propre à la connexion... :
        Adresse IPv6 de liaison locale... : fe80::5872:4cd5:fcd8:6ca3%5
        Adresse IPv4... : 192.168.1.31
        Masque de sous-réseau... : 255.255.255.0
        Passerelle par défaut... : 192.168.1.1
PS C:\Users\Administrateur> Start-Service sshd
PS C:\Users\Administrateur>
```

Youpi ça marche !

## Launching PowerShell on the CORE Server

```
administrateur@SRV-DC-01 C:\Users\Administrateur>powershell  
Windows PowerShell  
Copyright (C) Microsoft Corporation. Tous droits réservés.  
Installez la dernière version de PowerShell pour de nouvelles fonctionnalités et améliorations ! https://aka.ms/PSWindow  
s  
PS C:\Users\Administrateur> |
```

## Enabling PowerShell Remoting

```
Enable-PSRemoting -SkipNetworkProfileCheck -Force :
```

Commenté [RK1]: A faire plus tard

## Enabling ICMP "Ping"

```
netsh advfirewall firewall add rule name = "ICMP Allow incoming V4 echo request"  
protocol=icmpv4:8,any dir=in action=allow
```

Commenté [RK2]: Usage de cette commande

```
PS C:\Users\Administrateur> netsh advfirewall firewall add rule name="Autorise les pings ICMP & Echo Reply v4" protocol=icmpv4:8,any dir=in action=allow  
OK.  
PS C:\Users\Administrateur>
```

## Pourquoi réaliser un test ICMP (Ping) ?

Le **Ping** (basé sur le protocole **ICMP - Internet Control Message Protocol**) est un outil de diagnostic réseau essentiel. Voici ses principales utilisations :

### 1. Vérifier la connectivité de base

- Tester si une machine est joignable (en ligne ou hors ligne).
- Vérifier qu'un hôte répond sur le réseau (local ou distant).
- Déetecter les problèmes de configuration IP (ex : mauvaise adresse, sous-réseau incorrect).

Exemple :

## Disable WinProxy Settings (If Necessary)

```
command: netsh winhttp show proxy command: netsh winhttp reset proxy |
```

Commenté [RK3]: A faire peut-être plus tard

```

PS C:\Users\Administrateur> netsh winhttp show proxy
Paramètres de proxy WinHTTP actuels :
    Accès direct (sans serveur proxy).

PS C:\Users\Administrateur> netsh winhttp reset proxy
Paramètres de proxy WinHTTP actuels :
    Accès direct (sans serveur proxy).

PS C:\Users\Administrateur>

```

## Set CORE Server for PowerShell Remote Management Rights

WinRM quickconfig

```

PS C:\Users\Administrateur> WinRM quickconfig
Le service WinRM est déjà en cours d'exécution sur cet ordinateur.
WinRM n'est pas configuré pour la gestion à distance de cet ordinateur.
Les modifications suivantes doivent être effectuées :

Configurez LocalAccountTokenFilterPolicy pour attribuer des droits d'administration à distance à des utilisateurs locaux.

Effectuer ces modifications [y/n] ? y
WinRM a été mis à jour pour la gestion à distance.

LocalAccountTokenFilterPolicy configuré pour attribuer des droits d'administration à distance à des utilisateurs locaux.

PS C:\Users\Administrateur>

```

## Optional Firewall Settings You Might Choose:

Enable-NetFirewallRule -DisplayGroup "File and Printer Sharing"

```
PS C:\Users\Administrateur> Enable-NetFirewallRule -DisplayGroup "Partage de fichiers et d'imprimantes"
```

command: Enable-NetFirewallRule -DisplayGroup "Remote Event Log Management"

command: Enable-NetFirewallRule -DisplayGroup "Remote Desktop"

```
PS C:\Users\Administrateur> Enable-NetFirewallRule -DisplayGroup "Partage de fichiers et d'imprimantes"
```

```
PS C:\Users\Administrateur> Enable-NetFirewallRule -DisplayGroup "Gestion à distance des journaux des événements"
PS C:\Users\Administrateur> Enable-NetFirewallRule -DisplayGroup "Bureau à distance (WebSocket)"
PS C:\Users\Administrateur>
```

## Enable Remote Management in Current Firewall Profile Settings

command: netsh advfirewall set currentprofile settings remotemanagement enable

```
PS C:\Users\Administrateur> netsh advfirewall set currentprofile settings remotemanagement enable
```

```
Ok.
```

```
PS C:\Users\Administrateur>
```

## Disabling the Firewall Entirely During the Setup Process (Optional)

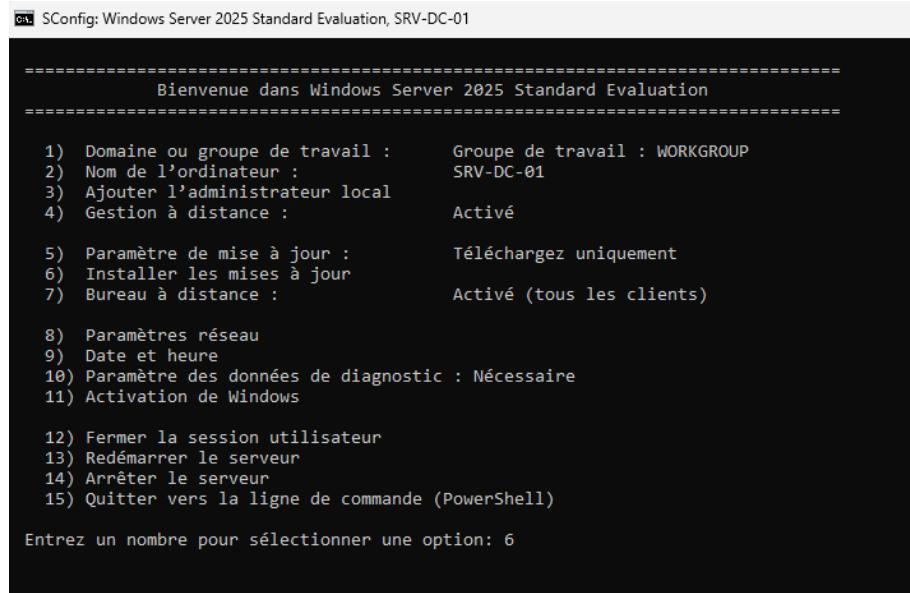
command: Set-NetFirewallProfile -Profile Domain,Public,Private -Enabled False

```
PS C:\Users\Administrateur> Set-NetFirewallProfile -Profile Domain,Public,Private -Enabled False
PS C:\Users\Administrateur> Set-NetFirewallProfile -Profile Domain,Public,Private -Enabled False
PS C:\Users\Administrateur>
```

**Commenté [RK4]:** On le fait pour faciliter le process sinon il faudrait ensuite revenir pour remettre comme il fallait.

Changing Passwords from the Command Console on a CORE Server command: net user administrator P@ssw0rd 19

## Updating CORE Server Using "sconfig"



```
SConfig: Windows Server 2025 Standard Evaluation, SRV-DC-01

=====
 Bienvenue dans Windows Server 2025 Standard Evaluation
=====

1) Domaine ou groupe de travail : Groupe de travail : WORKGROUP
2) Nom de l'ordinateur : SRV-DC-01
3) Ajouter l'administrateur local
4) Gestion à distance : Activé
5) Paramètre de mise à jour : Téléchargez uniquement
6) Installer les mises à jour
7) Bureau à distance : Activé (tous les clients)

8) Paramètres réseau
9) Date et heure
10) Paramètre des données de diagnostic : Nécessaire
11) Activation de Windows

12) Fermer la session utilisateur
13) Redémarrer le serveur
14) Arrêter le serveur
15) Quitter vers la ligne de commande (PowerShell)

Entrez un nombre pour sélectionner une option: 6
```

Recherche de toutes les mises à jour :

**Attention** ! Pour la recherche de mises à jour, cas particulier pour le serveur DNS 9.9.9.9  
(en fait pas spécialement du serveur 999, serait, plus à qqhc qui bloque les requêtes DNS :

**Commenté [RK5]:** A mettre dans le readME

```
PS C:\Users\Administrateur> nslookup www.microsoft.com
DNS request timed out.
    timeout was 2 seconds.
Serveur :   UnKnown
Address:  9.9.9.9

DNS request timed out.
    timeout was 2 seconds.
*** Le délai de la requête sur UnKnown est dépassé.
PS C:\Users\Administrateur> Get-NetIPConfiguration

InterfaceAlias      : Ethernet0
InterfaceIndex      : 5
InterfaceDescription: Intel(R) 82574L Gigabit Network Connection
NetProfile.Name     : Réseau
IPv4Address         : 192.168.1.31
IPv6DefaultGateway  :
IPv4DefaultGateway  : 192.168.1.1
DNSServer           : 9.9.9.9
                           1.1.1.1
```

```
PS C:\Users\Administrateur> ping 9.9.9.9

Envoi d'une requête 'Ping' 9.9.9.9 avec 32 octets de données :
Délai d'attente de la demande dépassé.
```

```
PS C:\Users\Administrateur> ping 192.168.1.1

Envoi d'une requête 'Ping' 192.168.1.1 avec 32 octets de données :
Réponse de 192.168.1.1 : octets=32 temps=5 ms TTL=128
Réponse de 192.168.1.1 : octets=32 temps=1 ms TTL=128
Réponse de 192.168.1.1 : octets=32 temps<1ms TTL=128
Réponse de 192.168.1.1 : octets=32 temps=1 ms TTL=128

Statistiques Ping pour 192.168.1.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 5ms, Moyenne = 1ms
PS C:\Users\Administrateur>
```

## Tester si une règle de pare-feu bloque DNS

```
PS C:\Users\Administrateur> Get-NetFirewallRule -DisplayName "*DNS*"

Name          : MDNS-Out-UDP-Domain-Active
DisplayName   : mDNS (UDP-Sortie)
Description   : Règle de trafic sortant pour le trafic mDNS
                [UDP]
DisplayGroup : mDNS
Group         : @%SystemRoot%\system32\firewallapi.dll,-37302
Enabled       : True
Profile       : Domain
Platform      : {}
Direction    : Outbound
Action        : Allow
EdgeTraversalPolicy : Block
LooseSourceMapping : False
LocalOnlyMapping : False
Owner         :
PrimaryStatus :
Status        : La règle a été analysée à partir de la banque.
                (65536)
EnforcementStatus : NotApplicable
PolicyStoreSource : PersistentStore
PolicyStoreSourceType : Local
RemoteDynamicKeywordAddresses : {}
PolicyAppId    :
PackageName    :

Name          : MDNS-Out-UDP-Public-Active
DisplayName   : mDNS (UDP-Sortie)
Description   : Règle de trafic sortant pour le trafic mDNS
                [UDP]
DisplayGroup : mDNS
Group         : @%SystemRoot%\system32\firewallapi.dll,-37302
Enabled       : True
Profile       : Public
```

La règle pare-feu CoreNet-DNS-Out-UDP est bien **activée** → donc **ce n'est probablement pas le pare-feu Windows local** qui bloque.

## 1. Vérifie depuis une autre machine (par exemple un PC sur le même réseau) :

Sur un PC branché au même switch/routeur :

- Ouvre un terminal et tape :

```
bash
```

 Copy  Edit

```
ping 8.8.8.8
```

ou

```
bash
```

 Copy  Edit

```
nslookup www.microsoft.com
```

 Si ça marche depuis le PC mais pas depuis le serveur → alors une règle (pare-feu ou NAT) spécifique empêche le serveur de sortir.

 Si ça ne marche pas non plus depuis le PC → c'est le routeur ou box Internet qui bloque les connexions sortantes.

- Conclusion : Le blocage est au niveau de la passerelle (192.168.1.1) ou de l'infrastructure réseau (box, routeur, firewall matériel, VLAN, etc.)

### Étapes que je te recommande maintenant

#### 1. Tester depuis un autre poste sur le même réseau (ex : un PC Windows)

```
cmd
ping 8.8.8.8
nslookup www.microsoft.com
```

- Si ça fonctionne sur le PC mais pas sur le serveur :  
→ C'est une restriction spécifique sur le serveur (routage/NAT filtré, firewall amont, VLAN isolé...).
- Si ça ne fonctionne pas non plus sur le PC :  
→ C'est le routeur ou box Internet (ou une politique réseau) qui empêche les machines internes de sortir.

```
PS C:\Users\Rachel> ping 8.8.8.8

Envoi d'une requête 'Ping' 8.8.8.8 avec 32 octets de données :
Réponse de 8.8.8.8 : octets=32 temps=8 ms TTL=117
Réponse de 8.8.8.8 : octets=32 temps=7 ms TTL=117
Réponse de 8.8.8.8 : octets=32 temps=9 ms TTL=117
Réponse de 8.8.8.8 : octets=32 temps=7 ms TTL=117

Statistiques Ping pour 8.8.8.8:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 7ms, Maximum = 9ms, Moyenne = 7ms
PS C:\Users\Rachel> nslookup www.microsoft.com
Serveur :   livebox.home
Address: 2a01:cb1c:12d7:6b00:3ab5:c9ff:fe35:7c70

Réponse ne faisant pas autorité :
Nom : e13678.dscb.akamaiedge.net
Addresses: 2a02:26f0:df:3b3::356e
           2a02:26f0:df:399::356e
           2a02:26f0:df:39b::356e
           2a02:26f0:df:395::356e
           2a02:26f0:df:383::356e
           2.20.41.218
Aliases: www.microsoft.com
          www.microsoft.com-c-3.edgekey.net
          www.microsoft.com-c-3.edgekey.net.globalredir.akadns.net
```