

# Tutoriel complet : Active Directory, DNS, DHCP et Accès à distance (SSH/RDP)

---

## 1. Contexte réseau et objectifs

Ce tutoriel couvre l'installation et la configuration d'un serveur Windows Server 2025 dans un environnement pédagogique. Le serveur est contrôleur de domaine Active Directory (sisr.local), DNS, et DHCP. Deux réseaux sont gérés : 192.168.0.0/24 et 192.168.1.0/24. Un routeur VyOS assure le relais DHCP entre les deux réseaux.

Objectifs :

- Installer et configurer Active Directory et DNS (sisr.local)
- Configurer le redirecteur DNS vers 10.63.101.1
- Installer et autoriser le rôle DHCP
- Créer et tester des étendues DHCP pour les deux réseaux
- Mettre en place des accès sécurisés SSH et RDP

## 2. Pré-requis et configuration IP fixe

Serveur Windows 2025 :

- Nom : srv.sisr.local
- IP fixe : 192.168.0.1/24
- Passerelle : 192.168.0.254
- DNS préféré : 192.168.0.1

Configuration via PowerShell :

```
New-NetIPAddress -InterfaceAlias "Ethernet0" -IPAddress 192.168.0.1 -  
PrefixLength 24 -DefaultGateway 192.168.0.254  
Set-DnsClientServerAddress -InterfaceAlias "Ethernet0" -ServerAddresses  
192.168.0.1
```

Ajout des fonctionnalités à la demande (possibilité d'obtenir des interfaces graphiques de gestion à la demande). Effectuez un snapshot avant d'exécuter l'installation

```
dism /online /Add-Capability /capabilityname:"ServerCore.AppCompatibility~~~~~0.0.1.0"
```

Tester

```
PS C:\Users\Administrateur> explorer (afficher l'explorateur de fichiers)  
PS C:\Users\Administrateur> ise (affiche l'éditeur de script)
```

## 3. Installation d'Active Directory (sisr.local)

Désactiver l'expiration du mot de passe de l'administrateur local (Vous pouvez l'activer par la suite)

Effectuez un snapshot avant d'exécuter l'installation. Installation et promotion du serveur en contrôleur de domaine. Le serveur redémarre automatiquement après la promotion.

## 4. Configuration du DNS (redirecteur)

Ajout du redirecteur DNS vers le serveur DNS du réseau SIO du lycée 10.63.101.1. Utiliser plutôt l'adresse de la passerelle du NAT du commutateur VMNet8 de l'hyperviseur VMWare Workstation. On trouve cette adresse dans le fichier de configuration /etc/resolv.conf du résolveur du routeur vyos .  
Tester avec : *Get-DnsServerForwarder*

## 5. Installation et autorisation du rôle DHCP

Installation du rôle DHCP et autorisation du serveur dans Active Directory :

## 6. Création des étendues DHCP

### Étendue LAN1 (192.168.0.0/24)

```
Add-DhcpServerv4Scope -Name "LAN1" -StartRange 192.168.0.100 -EndRange  
192.168.0.200 -SubnetMask 255.255.255.0 -State Active  
Set-DhcpServerv4OptionValue -Scopeld 192.168.0.0 -Router 192.168.0.254 -  
DnsServer 192.168.0.1 -DnsDomain "sisr.local"
```

### Étendue LAN2 (192.168.1.0/24)

```
Add-DhcpServerv4Scope -Name "LAN2" -StartRange 192.168.1.100 -EndRange  
192.168.1.200 -SubnetMask 255.255.255.0 -State Active  
Set-DhcpServerv4OptionValue -Scopeld 192.168.1.0 -Router 192.168.1.254 -  
DnsServer 192.168.0.1 -DnsDomain "sisr.local"
```

## 7. Vérifications

*Côté serveur :*

```
Get-DhcpServerv4Scope  
Get-DhcpServerv4OptionValue -Scopeld 192.168.0.0  
Get-DhcpServerv4OptionValue -Scopeld 192.168.1.0
```

*Côté clients Windows :*

```
ipconfig /release  
ipconfig /renew  
ipconfig /all
```

*Côté clients Linux :*

```
dhclient -v  
ip a
```

## 8. A retenir

- Un serveur DHCP dans un domaine doit être autorisé dans Active Directory
- Chaque réseau doit avoir sa propre étendue
- Le routeur joue le rôle de relais DHCP pour le réseau secondaire
- L'intégration DNS permet la résolution de noms et l'enregistrement dynamique

## 9. Mise en place d'un accès SSH sécurisé

Installation du service OpenSSH et configuration de base

Sécurisation :

- Utiliser un groupe AD (ex: SISR-Admins)
- Activer PubkeyAuthentication, désactiver PasswordAuthentication
- Placer les clés publiques dans C:\ProgramData\ssh\administratorsAuthorized\_keys

## 10. Mise en place d'un accès RDP sécurisé

Activation de RDP avec NLA\* et restriction firewall :

*Ajouter un groupe AD aux utilisateurs autorisés pour sécuriser :*

*Add-LocalGroupMember -Group "Remote Desktop Users" -Member "SISR\SISR-Admins"*

## 11. Script récapitulatif complet

Un script PowerShell complet regroupant toutes les étapes (AD, DNS, DHCP, SSH, RDP) peut être fourni pour automatiser la configuration.

Ce script doit être exécuté en tant qu'administrateur du domaine. <# -- Désactiver l'expiration du mot de passe Administrateur local ---#>

```
Set-LocalUser -Name "Administrateur" -PasswordNeverExpires $true  
<# ----- Installation de l'Active Directory (DNS inclus) et la forêt sisr.local -----#>  
Install-WindowsFeature -Name AD-Domain-Services -IncludeManagementTools
```

```
$DelegationDNS = $false  
$CheminBDD = "C:\Windows\NTDS"  
$NiveauDomaine = "Win2025"  
$NomDeDomaine = "sisr.local"  
$NomNetBios = "SISR"  
$NiveauForet = "Win2025"  
$InstallationDNS = $true  
$CheminLOG = "C:\Windows\NTDS"  
$NePasRebooter = $false  
$CheminSYSVOL = "C:\Windows\SYSVOL"  
$MotDePasseRestauration = ConvertTo-SecureString "Bts2526P@$$word59" -Force  
  
Install-ADDSForest -CreateDnsDelegation:$DelegationDNS `  
    -DatabasePath $CheminBDD `  
    -DomainMode $NiveauDomaine `  
    -DomainName $NomDeDomaine `  
    -DomainNetbiosName $NomNetBios `  
    -ForestMode $NiveauForet `  
    -InstallDns:$InstallationDNS `  
    -LogPath $CheminLOG `  
    -NoRebootOnCompletion:$NePasRebooter `  
    -SysvolPath $CheminSYSVOL `  
    -SafeModeAdministratorPassword $MotDePasseRestauration `  
    -Force:$true `  
    -Confirm:$false
```

```

<#--- Installation et configuration des étendues du serveur DHCP avec autorisation #>
Install-WindowsFeature -Name DHCP -IncludeManagementTools
Add-DhcpServerInDC -DnsName "srv.sisr.local" -IpAddress 192.168.0.1
Get-DhcpServerInDC

Add-DhcpServerv4Scope -Name "LAN1" -StartRange 192.168.0.100 -EndRange 192.168.0.200 -
SubnetMask 255.255.255.0 -State Active
Set-DhcpServerv4OptionValue -Scopeld "192.168.0.0" -Router 192.168.0.254 -DnsServer
192.168.0.1 -DnsDomain "sisr.local"

Add-DhcpServerv4Scope -Name "LAN2" -StartRange 192.168.1.100 -EndRange 192.168.1.200 -
SubnetMask 255.255.255.0 -State Active
Set-DhcpServerv4OptionValue -Scopeld "192.168.1.0" -Router 192.168.1.254 -DnsServer
192.168.0.1 -DnsDomain "sisr.local"

<# ---- Script Installation de l'accès à distance SSH -----#>
Add-WindowsCapability -Online -Name OpenSSH.Server~~~~~0.0.1.0
Start-Service sshd
Set-Service sshd -StartupType Automatic
New-NetFirewallRule -Name "OpenSSH-Server-In" -DisplayName «SSH» -Direction Inbound -
Protocol TCP -LocalPort 22 -Action Allow -RemoteAddress
192.168.0.0/24,192.168.1.0/24,10.63.0.0/16

<# ----Script : Enable-RDP-Secure-Fixed.ps1 ---- Objet :
    - Activer RDP + NLA et restreindre le pare-feu aux sous-réseaux autorisés
    - Utilise un TABLEAU pour -RemoteAddress
    - Si la restriction échoue sur les règles intégrées, crée des règles dédiées et désactive les
intégrées
#>

# === Paramètres à adapter ===
$AllowedSubnets = @('192.168.0.0/16','10.63.0.0/16') # ! Tableau, pas une chaîne

Write-Host "==> Activation de RDP et NLA..." -ForegroundColor Cyan

# 1) Activer RDP + NLA
Set-ItemProperty -Path 'HKLM:\System\CurrentControlSet\Control\Terminal Server' -Name
fDenyTSConnections -Value 0
Set-ItemProperty -Path 'HKLM:\System\CurrentControlSet\Control\Terminal
Server\WinStations\RDP-Tcp' -Name UserAuthentication -Value 1

# 2) Règles intégrées (noms internes, indépendants de la langue)
$tcpRuleName = 'RemoteDesktop-UserMode-In-TCP'
$udpRuleName = 'RemoteDesktop-UserMode-In-UDP'

$tcpRule = Get-NetFirewallRule -Name $tcpRuleName -ErrorAction SilentlyContinue
$udpRule = Get-NetFirewallRule -Name $udpRuleName -ErrorAction SilentlyContinue

$tcpRestricted = $false

```

```

$udpRestricted = $false

if ($tcpRule) {
    Write-Host "==> Activation de la règle intégrée: $tcpRuleName" -ForegroundColor Green
    Enable-NetFirewallRule -Name $tcpRuleName
    try {
        # Essai 1 : restriction via Set-NetFirewallRule (tableau)
        Set-NetFirewallRule -Name $tcpRuleName -RemoteAddress $AllowedSubnets -Profile Any -ErrorAction Stop
        $tcpRestricted = $true
    } catch {
        Write-Warning "Restriction directe sur $tcpRuleName impossible. Tentative via Set-NetFirewallAddressFilter..."
        try {
            # Essai 2 : via le filtre d'adresse associé
            $ruleObj = Get-NetFirewallRule -Name $tcpRuleName
            Set-NetFirewallAddressFilter -AssociatedNetFirewallRule $ruleObj -RemoteAddress $AllowedSubnets -ErrorAction Stop
            $tcpRestricted = $true
        } catch {
            Write-Warning "Échec de la restriction sur la règle intégrée TCP."
        }
    }
} else {
    Write-Host "==> Règle intégrée $tcpRuleName introuvable." -ForegroundColor Yellow
}

if ($udpRule) {
    Write-Host "==> Activation de la règle intégrée: $udpRuleName" -ForegroundColor Green
    Enable-NetFirewallRule -Name $udpRuleName
    try {
        Set-NetFirewallRule -Name $udpRuleName -RemoteAddress $AllowedSubnets -Profile Any -ErrorAction Stop
        $udpRestricted = $true
    } catch {
        Write-Warning "Restriction directe sur $udpRuleName impossible. Tentative via Set-NetFirewallAddressFilter..."
        try {
            $ruleObj = Get-NetFirewallRule -Name $udpRuleName
            Set-NetFirewallAddressFilter -AssociatedNetFirewallRule $ruleObj -RemoteAddress $AllowedSubnets -ErrorAction Stop
            $udpRestricted = $true
        } catch {
            Write-Warning "Échec de la restriction sur la règle intégrée UDP."
        }
    }
} else {
    Write-Host "==> Règle intégrée $udpRuleName introuvable." -ForegroundColor Yellow
}

```

```

# 3) Si on n'a pas réussi à restreindre une règle intégrée, on crée des règles dédiées et on
désactive l'intégrée
if (-not $tcpRestricted) {
    Write-Host "==> Création d'une règle dédiée TCP 3389 restreinte, et désactivation de la règle
intégrée." -ForegroundColor Yellow
    if (-not (Get-NetFirewallRule -Name 'RDP-In-TCP-3389-LANs' -ErrorAction SilentlyContinue)) {
        New-NetFirewallRule -Name 'RDP-In-TCP-3389-LANs' -DisplayName 'RDP (TCP 3389) - LANs
pédagogiques' `

        -Direction Inbound -Protocol TCP -LocalPort 3389 -Action Allow `

        -RemoteAddress $AllowedSubnets -Profile Any | Out-Null
    } else {
        Enable-NetFirewallRule -Name 'RDP-In-TCP-3389-LANs'
        Set-NetFirewallRule -Name 'RDP-In-TCP-3389-LANs' -RemoteAddress $AllowedSubnets -`

        Profile Any
    }
    if ($tcpRule) { Disable-NetFirewallRule -Name $tcpRuleName }
}

if (-not $udpRestricted) {
    Write-Host "==> Création d'une règle dédiée UDP 3389 restreinte, et désactivation de la règle
intégrée." -ForegroundColor Yellow
    if (-not (Get-NetFirewallRule -Name 'RDP-In-UDP-3389-LANs' -ErrorAction SilentlyContinue)) {
        New-NetFirewallRule -Name 'RDP-In-UDP-3389-LANs' -DisplayName 'RDP (UDP 3389) -`

        LANs pédagogiques' `

        -Direction Inbound -Protocol UDP -LocalPort 3389 -Action Allow `

        -RemoteAddress $AllowedSubnets -Profile Any | Out-Null
    } else {
        Enable-NetFirewallRule -Name 'RDP-In-UDP-3389-LANs'
        Set-NetFirewallRule -Name 'RDP-In-UDP-3389-LANs' -RemoteAddress $AllowedSubnets -`

        Profile Any
    }
    if ($udpRule) { Disable-NetFirewallRule -Name $udpRuleName }
}

Write-Host "==> Vérifications..." -ForegroundColor Cyan
Get-NetFirewallRule | Where-Object { $_.Name -match 'RemoteDesktop|RDP-In' } |`

Select-Object Name, DisplayName, Enabled, Direction

Write-Host "==> Test du port 3389 en local :" -ForegroundColor Cyan
Test-NetConnection -ComputerName localhost -Port 3389

```

## 12. Conclusion

Avec cette configuration, le serveur Windows 2025 agit comme contrôleur de domaine, DNS, DHCP et fournit des accès sécurisés à distance (SSH et RDP).

### \*NLA : Network Level Authentication

---

#### 1. Définition

**NLA (Network Level Authentication)** est une **technologie de sécurité de Remote Desktop Protocol (RDP)** introduite par Microsoft à partir de Windows Vista / Server 2008.

Avant que la session graphique RDP ne s'ouvre, l'utilisateur doit d'abord s'authentifier.

Sans NLA :

- Le serveur ouvre la session graphique **avant l'authentification**.
- Résultat : le serveur consomme des ressources inutilement et reste exposé aux attaques (bruteforce, DoS).

Avec NLA :

- L'utilisateur s'authentifie **avant l'établissement de la session RDP**.
- Si l'authentification échoue → la session RDP n'est jamais ouverte.

#### 2. Technologie utilisée

NLA s'appuie sur :

- **CredSSP (Credential Security Support Provider)**
  - Un fournisseur de sécurité Windows qui permet de déléguer les identifiants de manière chiffrée.
  - Il utilise **Kerberos** (si le client et le serveur sont dans le même domaine) ou **NTLM** comme mécanisme d'authentification.
- **TLS (Transport Layer Security)**
  - Chiffrement des communications RDP.
  - Empêche l'interception des données (mot de passe, session).

#### 3. Avantages pédagogiques

- Réduit les risques d'attaque brute-force (pas de session ouverte si échec d'authentification).
- Économie de ressources côté serveur (pas de bureau chargé pour rien).
- Authentification **intégrée à Active Directory** (Kerberos si dispo).
- Communication sécurisée par **TLS**.

#### 4. Exemple concret

- Sans NLA :
  - Un pirate lance un client RDP → le serveur crée une session graphique → tentative d'attaque par mot de passe.
- Avec NLA :
  - Le pirate doit s'authentifier **avant** la création de la session → la surface d'attaque est réduite.

**NLA = Authentification préalable à la session RDP, basée sur CredSSP (Kerberos/NTLM) et TLS.**

Cela rend RDP plus sûr et plus léger en empêchant toute ouverture de session sans authentification valide.