

Ports réseau requis pour l'ajout d'un contrôleur de domaine à une forêt Active Directory

Pour permettre l'ajout d'un contrôleur de domaine à une forêt Active Directory existante, il est essentiel d'ouvrir certains ports réseau sur le pare-feu entre le nouveau contrôleur et les contrôleurs de domaine existants.

Ports TCP/UDP à ouvrir

Service	Port(s)	Protocole	Description
DNS	53	TCP/UDP	Résolution de noms
Kerberos	88	TCP/UDP	Authentification
LDAP	389	TCP/UDP	Annuaire AD
LDAP sur SSL (LDAPS)			
Global Catalog	3268	TCP	Requêtes LDAP sur le catalogue global
Global Catalog (SSL)	3269	TCP	
Netlogon	445, 135, 139	TCP	
RPC (Remote Procedure Call)	135	TCP	Communication entre services AD
RPC dynamique	49152-65535	TCP	
WMI	135 + dynamiques	TCP	Utilisé pour la gestion à distance
SMB	445 TCP Partage de fichiers et communication AD		
FRS / DFSR	445, 135 + dynamiques	TCP	Réplication de fichiers AD

Recommandations

- RPC dynamique : Par défaut, Windows utilise des ports dynamiques entre 49152 et 65535. Il est possible de restreindre cette plage pour faciliter la configuration du pare-feu.
- Test de connectivité : Utilisez PortQry ou Test-NetConnection pour vérifier l'ouverture des ports.
- Pare-feu Windows : Assurez-vous que les règles de pare-feu locales permettent aussi ces communications.

Script PowerShell pour tester les ports

Ce script utilise Test-NetConnection pour chaque port et affiche les résultats dans la console.

Test-ADPorts.ps1

```
# Script PowerShell pour tester les ports nécessaires à l'ajout d'un contrôleur de domaine
$Target = Read-Host 'Entrez le nom ou l'adresse IP du contrôleur de domaine existant'

Write-Host 'Test DNS (TCP 53)'
Test-NetConnection -ComputerName $Target -Port 53 | Format-Table -AutoSize

Write-Host 'Test DNS (UDP 53)'
Test-NetConnection -ComputerName $Target -Port 53 -InformationLevel Detailed -UdpPort 53 | Format-Table -AutoSize

Write-Host 'Test Kerberos (TCP 88)'
Test-NetConnection -ComputerName $Target -Port 88 | Format-Table -AutoSize

Write-Host 'Test Kerberos (UDP 88)'
Test-NetConnection -ComputerName $Target -Port 88 -InformationLevel Detailed -UdpPort 88 | Format-Table -AutoSize

Write-Host 'Test LDAP (TCP 389)'
Test-NetConnection -ComputerName $Target -Port 389 | Format-Table -AutoSize

Write-Host 'Test LDAP (UDP 389)'
Test-NetConnection -ComputerName $Target -Port 389 -InformationLevel Detailed -UdpPort 389 | Format-Table -AutoSize

Write-Host 'Test LDAPS (TCP 636)'
Test-NetConnection -ComputerName $Target -Port 636 | Format-Table -AutoSize

Write-Host 'Test Global Catalog (TCP 3268)'
```

```
Test-NetConnection -ComputerName $Target -Port 3268 | Format-Table -AutoSize
Write-Host 'Test Global Catalog SSL (TCP 3269)'
Test-NetConnection -ComputerName $Target -Port 3269 | Format-Table -AutoSize
Write-Host 'Test RPC (TCP 135)'
Test-NetConnection -ComputerName $Target -Port 135 | Format-Table -AutoSize
Write-Host 'Test NetLogon (TCP 139)'
Test-NetConnection -ComputerName $Target -Port 139 | Format-Table -AutoSize
Write-Host 'Test SMB / Netlogon / FRS (TCP 445)'
Test-NetConnection -ComputerName $Target -Port 445 | Format-Table -AutoSize
Write-Host 'Test RPC dynamique (TCP 49152)'
Test-NetConnection -ComputerName $Target -Port 49152 | Format-Table -AutoSize
Write-Host 'Test RPC dynamique (TCP 49153)'
Test-NetConnection -ComputerName $Target -Port 49153 | Format-Table -AutoSize
Write-Host 'Test RPC dynamique (TCP 49154)'
Test-NetConnection -ComputerName $Target -Port 49154 | Format-Table -AutoSize
Write-Host 'Test RPC dynamique (TCP 49155)'
Test-NetConnection -ComputerName $Target -Port 49155 | Format-Table -AutoSize
Write-Host 'Test RPC dynamique (TCP 49156)'
Test-NetConnection -ComputerName $Target -Port 49156 | Format-Table -AutoSize
Write-Host 'Test RPC dynamique (TCP 49157)'
Test-NetConnection -ComputerName $Target -Port 49157 | Format-Table -AutoSize
Write-Host 'Test RPC dynamique (TCP 49158)'
Test-NetConnection -ComputerName $Target -Port 49158 | Format-Table -AutoSize
Write-Host 'Test RPC dynamique (TCP 49159)'
Test-NetConnection -ComputerName $Target -Port 49159 | Format-Table -AutoSize
Write-Host 'Test RPC dynamique (TCP 49160)'
Test-NetConnection -ComputerName $Target -Port 49160 | Format-Table -AutoSize
Write-Host 'Test RPC dynamique (TCP 49161)'
Test-NetConnection -ComputerName $Target -Port 49161 | Format-Table -AutoSize
Write-Host 'Test RPC dynamique (TCP 49162)'
Test-NetConnection -ComputerName $Target -Port 49162 | Format-Table -AutoSize
```

From:
/ - Les cours du BTS SIO

Permanent link:
</doku.php/systeme/windows/server/port?rev=1759417767>

Last update: 2025/10/02 17:09

