# 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) 636 TCP LDAP sécurisé Global Catalog 3268 TCP Requêtes LDAP sur le catalogue global Global Catalog (SSL) 3269 TCP Catalogue global sécurisé Netlogon 445, 135, 139 TCP Authentification et scripts de connexion RPC (Remote Procedure Call) 135 TCP Communication entre services AD RPC dynamique 49152–65535 TCP Ports dynamiques RPC (à adapter selon configuration) 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 Un script PowerShell est disponible pour tester l’ouverture des ports nécessaires à l’ajout d’un contrôleur de domaine. Ce script utilise Test-NetConnection pour chaque port et affiche les résultats dans la console. Lien vers le script : Test-ADPorts.ps1

From:
/ - **Les cours du BTS SIO**

Permanent link:
**/doku.php/systeme/windows/server/port?rev=1759417595**

Last update: **2025/10/02 17:06**