installation du service DNS

Ressources

Les enregistrements DNS nécessaires au service Active Directory :

- https://www.it-connect.fr/active-directory-les-enregistrements-dns-indispensables/

Utiliser Active Directory avec Bind9 :

- https://www.serverlab.ca/tutorials/linux/network-services/using-linux-bind-dns-servers-for-active-directory-domains/
- https://social.technet.microsoft.com/wiki/contents/articles/7608.srv-records-registered-by-net-logon.aspx
- https://learn.microsoft.com/fr-fr/troubleshoot/windows-server/networking/verify-srv-dns-records-have-been-created

Installation du rôle DNS

- Ouvrez une session sur votre serveur Windows Core.
- Utilisez PowerShell pour installer le rôle DNS. Exécutez la commande suivante :

```
Install-WindowsFeature DNS -IncludeManagementTools
```

Configuration du service DNS

Après l'installation, vous pouvez configurer le service DNS à l'aide de PowerShell ou de l'outil de gestion DNS distant.

- Pour configurer une zone de recherche directe, utilisez la commande :

```
Add-DnsServerPrimaryZone -Name "example.com" -ZoneFile "example.com.dns"
```

- Pour ajouter un enregistrement A, utilisez la commande :

```
Add-DnsServerResourceRecordA -Name "www" -ZoneName "example.com" -IPv4Address "192.168.1.1"
```

- Ajouter une zone de recherche inverse

```
Add-DnsServerPrimaryZone -NetworkID "192.168.1.0/24" -ZoneFile "1.168.192.in-addr.arpa.dns"
```

- Ajouter un enregistrement PTR

```
Add-DnsServerResourceRecordPtr -Name "100" -ZoneName "1.168.192.in-addr.arpa" -PtrDomainName
"www.exemple.local"
```

- Vérification de la configuration : Utilisez la commande nslookup pour vérifier que le serveur DNS répond correctement aux requêtes. Vous pouvez également utiliser la commande Resolve-DnsName pour tester la résolution de noms.

Configuration du pare-feu

Assurez-vous que le pare-feu Windows autorise le trafic DNS (port 53).

Utilisez la commande suivante pour autoriser le trafic DNS entrant :

```
# Autoriser le trafic DNS entrant sur le port 53
New-NetFirewallRule -Name "DNS-in-udp" -DisplayName "Autoriser DNS Inbound" -Direction Inbound -Protocol
UDP -LocalPort 53 -Action Allow
New-NetFirewallRule -Name "DNS-in-tcp" -DisplayName "Autoriser DNS Inbound" -Direction Inbound -Protocol
TCP -LocalPort 53 -Action Allow

# Autoriser le trafic DNS sortant sur le port 53
New-NetFirewallRule  -Name "DNS-out-udp" -DisplayName "Autoriser DNS Outbound" -Direction Outbound -
Protocol UDP -LocalPort 53 -Action Allow
New-NetFirewallRule  -Name "DNS-out-tcp" -DisplayName "Autoriser DNS Outbound" -Direction Outbound -
Protocol TCP -LocalPort 53 -Action Allow
```

Serveur Core Windows Server