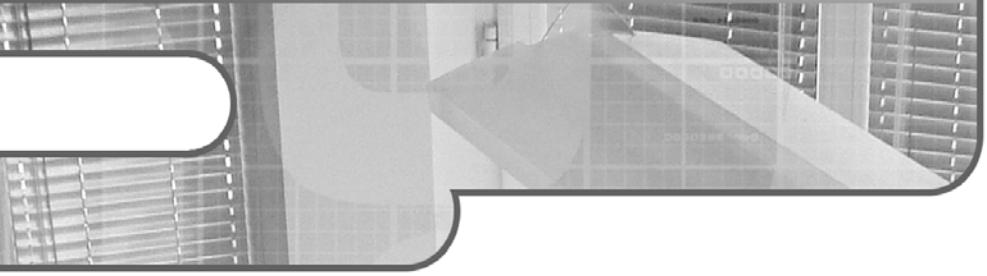

Chapitre 3
Active Directory

1. Définition

Active Directory (AD) est le service d'annuaire développé par Microsoft pour l'administration des environnements Windows. Il centralise les informations relatives aux utilisateurs, aux ordinateurs, aux groupes ainsi qu'aux autres ressources du réseau, offrant ainsi un point d'administration unique pour la gestion des identités et des accès.

Active Directory assure les fonctions d'authentification et d'autorisation. Il vérifie l'identité des utilisateurs et des ordinateurs lors de leur connexion, puis détermine les ressources auxquelles ils sont autorisés à accéder en fonction des autorisations qui leur sont attribuées.

Les objets gérés par Active Directory sont organisés selon une structure hiérarchique reposant sur les notions de domaines, d'arbres et de forêts. Cette organisation facilite l'administration des ressources et la mise en œuvre de délégations administratives à différentes échelles de l'infrastructure.

Par ailleurs, Active Directory s'appuie sur les stratégies de groupe *Group Policy Objects* (GPO) pour déployer et appliquer de manière centralisée des paramètres de configuration et de sécurité aux utilisateurs et aux ordinateurs d'un domaine.

2. Le protocole DNS

Le *Domain Name System* (DNS) est un service indispensable au fonctionnement des réseaux IP et d'Internet. Son rôle est d'assurer la résolution de noms en traduisant des noms de domaine compréhensibles par l'utilisateur, tels que www.google.com, en adresses IP numériques, telles que 192.0.2.1, utilisées pour identifier et localiser les hôtes sur le réseau.

Le système DNS repose sur une architecture hiérarchique composée de domaines de premier niveau *Top-Level Domain* (TLD), tels que .com ou .org, auxquels sont rattachés des domaines et des sous-domaines. Cette organisation garantit une gestion distribuée de l'espace de noms tout en assurant l'unicité des enregistrements DNS.

L'infrastructure DNS s'appuie sur plusieurs catégories de serveurs, notamment les serveurs racine, les serveurs des domaines de premier niveau TLD et les serveurs de noms faisant autorité (*authoritative name servers*). Chacun de ces serveurs remplit une fonction spécifique dans le processus de résolution des noms.

Afin d'améliorer les performances et de réduire le nombre de requêtes adressées aux serveurs distants, les serveurs DNS mettent en œuvre un mécanisme de cache. Les résultats des résolutions de noms sont ainsi conservés temporairement, ce qui accélère les consultations ultérieures et diminue la charge de l'infrastructure DNS.

2.1 Le rôle d'un serveur DNS

Sous Windows Server, le rôle Serveur DNS assure la gestion des espaces de noms DNS et la résolution des noms de domaine en adresses IP. Il constitue un composant essentiel de l'infrastructure réseau en permettant aux ordinateurs et aux applications de localiser les ressources disponibles sur un réseau local ou sur Internet.

Le serveur DNS héberge et administre des zones DNS contenant différents types d'enregistrements, tels que A, AAAA, CNAME, MX, NS, PTR ou SRV, qui établissent les correspondances entre les noms de domaine et les informations nécessaires à leur résolution. Il prend également en charge un mécanisme de mise en cache des réponses afin d'accélérer les résolutions ultérieures et de limiter le nombre de requêtes adressées aux serveurs distants.

Lorsqu'une requête concerne un domaine qui n'est pas administré localement, le serveur DNS peut la transmettre à des redirecteurs (*forwarders*), tels que des serveurs DNS publics ou ceux du fournisseur d'accès à Internet, afin d'obtenir la réponse appropriée.

Dans un environnement *Active Directory Domain Services* (AD DS), le serveur DNS joue un rôle fondamental. Il participe notamment à la localisation des contrôleurs de domaine et des différents services d'annuaire grâce aux enregistrements SRV, indispensables au fonctionnement des mécanismes d'authentification et de découverte des services. Le rôle DNS permet également de renforcer la sécurité de l'infrastructure en prenant en charge des fonctionnalités telles que DNSSEC (*Domain Name System Security Extensions*), destinées à protéger les échanges DNS contre des attaques telles que l'usurpation de réponses (DNS spoofing) ou l'empoisonnement du cache (*cache poisoning*).

2.2 Gérer le DNS avec PowerShell

PowerShell permet d'installer, de configurer et d'administrer le rôle Serveur DNS au moyen des cmdlets du module DnsServer. Si le rôle n'est pas encore installé sur le serveur, il peut être ajouté à l'aide de la cmdlet `Install-WindowsFeature` :

```
    PS C:\> Install-WindowsFeature -Name DNS -
IncludeManagementTools
```

2.2.1 Créer une zone DNS primaire

La cmdlet `Add-DnsServerPrimaryZone` permet de créer une zone DNS primaire, qu'elle soit intégrée à Active Directory ou basée sur un fichier.

Syntaxe

Les syntaxes les plus courantes sont les suivantes :

```
Add-DnsServerPrimaryZone
   -Name <String>
   -ReplicationScope <String>
   [-DynamicUpdate <String>]
   [-ComputerName <String>]
   [-PassThru]
```

```
Add-DnsServerPrimaryZone
   -Name <String>
   -ZoneFile <String>
   [-DynamicUpdate <String>]
   [-ComputerName <String>]
   [-PassThru]
```

```
Add-DnsServerPrimaryZone
   -NetworkId <String>
   -ZoneFile <String>
```

Paramètres principaux

Paramètre	Description
`-Name`	Spécifie le nom de la zone de recherche directe à créer.
`-NetworkId`	Indique le préfixe réseau utilisé lors de la création d'une zone de recherche inversée.
`-ReplicationScope`	Définit l'étendue de réplication d'une zone intégrée à Active Directory (Forest, Domain, Legacy ou Custom).
`-Directory PartitionName`	Précise la partition d'annuaire utilisée lorsque l'étendue de réplication est définie sur Custom.

Paramètre	Description
-ZoneFile	Indique le nom du fichier utilisé pour stocker une zone DNS basée sur un fichier.
-DynamicUpdate	Configure le mode de mise à jour dynamique de la zone (None, Secure ou NonsecureAndSecure).
-ComputerName	Exécute la commande sur un serveur DNS distant.
-LoadExisting	Charge un fichier de zone existant au lieu de créer une nouvelle zone.
-ResponsiblePerson	Renseigne la personne responsable de la zone dans l'enregistrement SOA.
-Virtualization Instance	Ajoute la zone dans une instance de virtualisation DNS spécifique.
-PassThru	Retourne l'objet représentant la zone créée.

Exemple 1 : création d'une zone primaire intégrée à Active Directory

La commande suivante crée une zone de recherche directe nommée domainepoc.fr. Cette zone est intégrée à Active Directory et répliquée sur l'ensemble des contrôleurs de domaine de la forêt. Le paramètre -PassThru affiche les informations relatives à la zone créée.

```
PS C:\> Add-DnsServerPrimaryZone -Name "domainepoc.fr"
-ReplicationScope "Forest" -PassThru
```

Exemple 2 : création d'une zone de recherche directe basée sur un fichier

Cette commande crée une zone de recherche directe nommée domainepoc.fr dont les données sont stockées dans le fichier domainepoc.fr.dns, plutôt que dans Active Directory.

```
PS C:\> Add-DnsServerPrimaryZone -Name "domainepoc.fr" -ZoneFile
"domainepoc.fr.dns"
```

Exemple 3 : création d'une zone de recherche inversée intégrée à Active Directory

La commande suivante crée une zone de recherche inversée correspondant au réseau 10.1.0.0/24. Cette zone est intégrée à Active Directory et répliquée à l'échelle de la forêt.

```
PS C:\> Add-DnsServerPrimaryZone -NetworkID "10.1.0.0/24"
-ReplicationScope "Forest"
```

Exemple 4 : création d'une zone de recherche inversée basée sur un fichier

Cette commande crée une zone de recherche inversée pour le réseau 10.3.0.0/24. Les données de la zone sont enregistrées dans le fichier 0.3.10.in-addr.arpa.dns.

```
PS C:\> Add-DnsServerPrimaryZone -NetworkID 10.3.0.0/24
-ZoneFile "0.3.10.in-addr.arpa.dns"
```

2.2.2 Ajouter un enregistrement A

La cmdlet `Add-DnsServerResourceRecordA` permet d'ajouter un enregistrement de ressource de type A dans une zone DNS. Un enregistrement A associe un nom d'hôte à une adresse IPv4 et constitue l'un des enregistrements les plus couramment utilisés dans une infrastructure DNS.

Syntaxe

Les formes les plus courantes de la cmdlet sont les suivantes :

```
Add-DnsServerResourceRecordA
    -Name <String>
    -ZoneName <String>
    -IPv4Address <IPAddress>
    [-TimeToLive <TimeSpan>]
    [-CreatePtr]
    [-AllowUpdateAny]
    [-PassThru]
```

```
Add-DnsServerResourceRecordA
    -Name <String>
    -ZoneName <String>
    -IPv4Address <IPAddress>
    [-ComputerName <String>]
```

Paramètres principaux

Paramètre	Description
`-Name`	Spécifie le nom d'hôte de l'enregistrement à créer.
`-ZoneName`	Indique la zone DNS dans laquelle l'enregistrement est ajouté.
`-IPv4Address`	Définit l'adresse IPv4 associée au nom d'hôte.
`-TimeToLive`	Configure la durée de vie (*Time To Live* – TTL) de l'enregistrement dans les caches DNS.
`-CreatePtr`	Crée automatiquement l'enregistrement PTR correspondant dans la zone de recherche inversée.
`-AllowUpdateAny`	Autorise tout utilisateur authentifié à mettre à jour l'enregistrement.
`-AgeRecord`	Applique un horodatage à l'enregistrement afin de permettre son nettoyage automatique (aging/scavenging).
`-ComputerName`	Exécute la commande sur un serveur DNS distant.
`-ZoneScope`	Ajoute l'enregistrement dans une étendue de zone DNS spécifique.
`-Virtualization Instance`	Cible une instance de virtualisation DNS particulière.
`-PassThru`	Retourne l'objet représentant l'enregistrement créé.

Exemple 1 : ajout d'un enregistrement A

La commande suivante crée un enregistrement de type A pour l'hôte SERVEURWPOC2K25 dans la zone domainepoc.fr. L'adresse IPv4 associée est 192.168.1.5 et la durée de vie de l'enregistrement est fixée à trois heures.

```
PS C:\> Add-DnsServerResourceRecordA -Name "SERVEURWPOC2K25" -
ZoneName "domainepoc.fr" -AllowUpdateAny -IPv4Address
"192.168.1.5" -TimeToLive 03:00:00
```

Exemple 2 : ajout d'un enregistrement A avec création automatique de l'enregistrement PTR

La commande suivante crée un enregistrement A pour l'hôte SERVEURFICHIERS dans la zone domainepoc.fr. Le paramètre `-CreatePtr` génère automatiquement l'enregistrement PTR correspondant dans la zone de recherche inversée, ce qui facilite la résolution inverse des noms.

```
PS C:\> Add-DnsServerResourceRecordA -Name "SERVEURFICHIERS" `
   -ZoneName "domainepoc.fr" `
   -IPv4Address "192.168.1.20" `
   -CreatePtr
```

2.2.3 Obtenir les détails d'une zone DNSt

La cmdlet `Get-DnsServerZone` permet d'interroger un serveur DNS afin d'obtenir des informations sur les zones qu'il héberge. Elle peut être utilisée pour afficher la liste de toutes les zones configurées ou pour consulter les propriétés d'une zone spécifique, telles que son type, son état, son mode de stockage ou son étendue de réplication.

Syntaxe

La syntaxe la plus couramment utilisée est la suivante :

```
Get-DnsServerZone
     [[-Name] <String[]>]
     [-ComputerName <String>]
     [-VirtualizationInstance <String>]
```

Paramètres principaux

Paramètre	Description
`-Name`	Spécifie le nom de la ou des zones DNS à afficher. Si ce paramètre est omis, toutes les zones du serveur sont retournées.
`-ComputerName`	Exécute la commande sur un serveur DNS distant. En son absence, la commande s'exécute sur le serveur local.

Paramètre	Description
`-Virtualization Instance`	Limite la recherche à une instance de virtualisation DNS donnée.

Exemple 1 : afficher toutes les zones DNS

Cette commande retourne en détail l'ensemble des zones configurées sur le serveur DNS local.

```
PS C:\> Get-DnsServerZone
```

Exemple 2 : afficher les informations d'une zone DNS

La commande suivante affiche les propriétés de la zone domainepoc.fr, notamment son type, son état, son mode de stockage et, lorsqu'elle est intégrée à Active Directory, son étendue de réplication.

```
PS C:\> Get-DnsServerZone -Name "domainepoc.fr"
```

2.2.4 Supprimer un enregistrement DNS

La cmdlet `Remove-DnsServerResourceRecord` permet de supprimer un ou plusieurs enregistrements de ressources d'une zone DNS. La suppression peut s'effectuer à partir d'un objet retourné par la cmdlet `Get-DnsServer-ResourceRecord` ou en spécifiant les caractéristiques de l'enregistrement à supprimer, telles que son nom, son type et si nécessaire, ses données.

Lorsque plusieurs enregistrements possèdent le même nom et le même type, le paramètre `-RecordData` permet de cibler précisément celui à supprimer. En son absence, tous les enregistrements correspondant au nom et au type indiqués sont supprimés.

Syntaxe

Les syntaxes les plus courantes sont les suivantes :

```
Remove-DnsServerResourceRecord
    -ZoneName <String>
    -RRType <String>
    -Name <String>
    [-RecordData <String[]>]
    [-ComputerName <String>]
```