

ACTIVE DIRECTORY

L'ADMINISTRER AVEC POWERSHELL

1ERE ÉDITION



IT-CONNECT
FLORIAN BURNEL



© Florian Burnel, 2021

ISBN numérique : 979-10-262-8465-9

Librinova”

Courriel : contact@librinova.com

Internet : www.librinova.com

Le Code de la propriété intellectuelle interdit les copies ou reproductions destinées à une utilisation collective. Toute représentation ou reproduction intégrale ou partielle faite par quelque procédé que ce soit, sans le consentement de l’auteur ou de ses ayants cause, est illicite et constitue une contrefaçon sanctionnée par les articles L335-2 et suivants du Code de la propriété intellectuelle.



Table des matières

A propos de cet eBook	4
A propos de l'auteur : Florian Burnel	4
Module 1 - Introduction et prérequis	5
1. Prérequis Active Directory et PowerShell	5
2. Présentation du Lab'	6
3. Créer un domaine Active Directory via PowerShell	7
I. Nom d'hôte.....	7
II. Configuration réseau	7
III. Installation des rôles.....	8
IV. Créer le domaine Active Directory	9
4. Installer le module Active Directory sur Windows 10 et Windows Server	10
V. Installer le module Active Directory sur Windows Server.....	10
VI. Installer le module Active Directory sur Windows 10	11
Module 2 - Gérer les utilisateurs AD avec PowerShell.....	13
1. Récupérer des informations sur les utilisateurs avec PowerShell	13
I. Syntaxe de Get-ADUser	13
II. Rechercher des utilisateurs dans une OU avec SearchBase.....	16
III. Obtenir la liste des adresses e-mails des utilisateurs	17
IV. Afficher la date de création des comptes.....	17
V. Récupérer la liste des utilisateurs créés à une date précise	18
VI. Quels sont les groupes dont l'utilisateur est membre ?	19
VII. Coupler l'utilisation du Filter et du Like	19
VIII. Récupérer la liste des comptes utilisateurs désactivés.....	20
IX. Récupérer la liste des comptes où le mot de passe est expiré.....	20
X. Compter le nombre d'utilisateurs dans l'Active Directory.....	21
XI. Exporter les utilisateurs dans un fichier CSV	22
2. Créer un utilisateur dans l'AD avec PowerShell	24
I. Premiers pas avec New-ADUser	24
II. Créer un utilisateur AD : découverte d'une autre syntaxe.....	26
III. New-ADUser : les paramètres additionnels.....	27
3. Créer des utilisateurs dans l'AD à partir d'un CSV	28
I. Le fichier CSV avec les utilisateurs.....	28
II. Importer le fichier CSV dans un script.....	29
III. Créer les utilisateurs AD en masse	29
4. Modifier le mot de passe d'un compte AD avec PowerShell	33
I. Réinitialiser un mot de passe d'un utilisateur Active Directory	33

II.	Modifier des mots de passe en lot	34
III.	Demander à l'utilisateur de changer son mot de passe	35
5.	Modifier des comptes AD en lot avec PowerShell	36
I.	Ajouter une valeur dans un attribut en masse à partir d'un CSV	36
II.	Modifications en masse via Get-ADUser et Set-ADUser	37
Module 3 - Gérer les groupes AD avec PowerShell		39
1.	Créer un groupe Active Directory avec PowerShell	39
I.	Récupérer les informations sur un groupe.....	39
II.	Créer un groupe AD avec PowerShell.....	40
III.	Créer un groupe de distribution	40
2.	Ajouter ou retirer des membres d'un groupe AD	41
I.	Ajouter un utilisateur dans un groupe AD.....	41
II.	Ajouter un utilisateur dans un groupe : autres exemples.....	42
III.	Retirer un utilisateur d'un groupe AD	42
IV.	Mettre à jour la liste des groupes dont un utilisateur est membre	43
V.	Précisions sur les cmdlets.....	43
3.	Récupérer la liste des membres d'un groupe AD	44
I.	Utiliser « Get-ADGroupMember »	44
II.	Utiliser « Get-ADPrincipalGroupMembership »	44
III.	Compter le nombre de membres dans un groupe	45
IV.	Récupérer la liste des groupes vides	45
V.	La notion de rechercher récursive.....	46
4.	Modifier et supprimer un groupe AD avec PowerShell.....	47
I.	Modifier un groupe AD avec PowerShell	47
II.	Comment changer le type de groupe et son étendue ?.....	47
III.	Renommer un groupe AD avec PowerShell.....	48
IV.	Supprimer un groupe AD	49
Module 4 - Analyser et maintenir l'Active Directory		50
1.	Obtenir des informations sur les contrôleurs de domaine	50
I.	Lister les contrôleurs de domaine avec PowerShell	50
II.	Vérifier la disponibilité des contrôleurs de domaine	51
2.	Lister les rôles FSMO en PowerShell	52
3.	Troubleshooting de la réplication Active Directory.....	55
I.	Get-ADReplicationFailure	55
II.	Get-ADReplicationPartnerMetadata	56
III.	Get-ADReplicationAttributeMetadata.....	57
IV.	Informations sur les sites Active Directory.....	57
4.	Obtenir des informations sur les ordinateurs avec PowerShell.....	58

I.	Get-ADComputer : nom, OS et adresse IP.....	58
II.	Combien est-ce qu'il y a de machines Windows 10 dans mon AD ?.....	58
III.	Quelle est la date de dernière connexion au domaine d'une machine ?.....	59
5.	Utiliser PowerShell pour identifier les ordinateurs et utilisateurs inactifs	60
I.	Comment identifier les utilisateurs inactifs ?.....	60
II.	Comment identifier les ordinateurs inactifs ?.....	61
III.	Les options complémentaires de Search-ADAccount.....	62
IV.	Search-ADAccount : comment exclure les nouveaux objets ?	63
V.	Retirer l'utilisateur des groupes dont il est membre	63
VI.	Désactiver l'utilisateur et le déplacer	64
VII.	Script de gestion des comptes inactifs	65
6.	Gérer la corbeille Active Directory avec PowerShell.....	67
I.	Activer la corbeille Active Directory	67
II.	Restaurer un objet de la corbeille Active Directory	67
III.	Purger la corbeille Active Directory	68
7.	Activer la protection contre la suppression accidentelle sur vos objets.....	70
I.	Lister les OU non protégées	71
II.	Activer la protection sur toute les OU de l'annuaire.....	71
III.	Protéger un autre objet : utilisateur, ordinateur, etc.....	72
8.	Apprendre PowerShell grâce au Centre d'administration Active Directory.....	73
I.	L'historique PowerShell d'ADAC.....	73
Conclusion.....		76

A propos de cet eBook

Ce cours au format livre numérique a pour objectif de vous apprendre à administrer votre annuaire Active Directory à l'aide de PowerShell, ce dernier étant devenu incontournable pour l'administration système dans un environnement Microsoft.

Grâce aux différents sujets abordés dans ce cours, que ce soit la gestion des utilisateurs, des ordinateurs ou des groupes, vous serez en mesure d'automatiser certaines tâches du quotidien à l'aide de scripts PowerShell. En complément, vous serez en mesure d'analyser et de maintenir votre annuaire Active Directory en lui-même grâce à différentes commandes qui servent à récolter des informations.

Ce cours s'adresse aux administrateurs système, aux étudiants en informatique, et plus généralement aux personnes qui souhaitent prendre en main l'Active Directory avec PowerShell.

Des scripts associés à ce livre numérique sont disponibles à l'adresse suivante :

<https://github.com/florianburnel/PowerShell/tree/master/EBOOK-ActiveDirectory-PowerShell>

A propos de l'auteur : Florian Burnel

Véritable passionné par l'informatique et les nouvelles technologies, j'ai près de 10 ans d'expérience dans l'administration système et réseau. Généraliste, je maîtrise particulièrement les technologies Microsoft, y compris l'Active Directory et PowerShell. Le langage PowerShell m'accompagne au quotidien depuis des années, et je ne manque jamais l'opportunité de dégainer une console pour exécuter une commande ou créer un script pour automatiser la moindre tâche !

J'ai écrit et publié de nombreux articles au sujet de l'Active Directory et de PowerShell. Ces articles sont disponibles, comme tous les autres, sur le site IT-Connect, en libre accès.

J'en profite pour remercier Thibault Baheux pour sa relecture technique.

Bonne lecture !

Module 1 - Introduction et prérequis

1. Prérequis Active Directory et PowerShell

Avant de commencer à suivre ce cours, il est préférable de prendre connaissance des prérequis ci-dessous, à la fois pour l'Active Directory et pour PowerShell.

- **Active Directory**

Dans ce cours, nous allons manipuler les objets de l'Active Directory les plus courants, à savoir les utilisateurs, les ordinateurs et les groupes. Par ailleurs, nous allons évoquer à plusieurs reprises les attributs constituant ces objets, notamment le `sAMAccountName` correspondant à l'identifiant de connexion (login).

Au niveau de l'annuaire Active Directory en lui-même, nous allons récupérer des informations sur le niveau fonctionnel, les rôles FSMO, la réplication, etc.

Je vous invite à lire mon cours sur les bases théoriques de l'Active Directory avant de commencer ce cours si les notions évoquées ci-dessus sont abstraites pour vous.

- **PowerShell**

PowerShell nous accompagnera dans chacun des chapitres de ce cours, nous allons utiliser notamment les notions suivantes :

- Les boucles, notamment `ForEach`
- Le pipeline
- Manipuler un fichier CSV
- Chaîne de caractères sécurisée

Pour suivre ce cours, vous devez disposer de Windows PowerShell 5.1, une version native sur les systèmes d'exploitation Microsoft les plus récents.

Nous découvrirons ensemble les commandes du module Active Directory pour PowerShell, mais si vous avez des bases, la compréhension sera plus facile.

2. Présentation du Lab'

Avant de commencer le cours, je vais décrire le Lab utilisé afin que vous puissiez en avoir connaissance d'une part, mais aussi que vous puissiez mettre en place quelque chose d'équivalent.

Le Lab à mettre en place est relativement simple puisqu'il repose sur une seule machine virtuelle (4 Go de RAM). En effet, il est nécessaire de disposer d'un serveur virtuel qui sera contrôleur de domaine suite au déploiement du rôle Active Directory Domain Services (ADDS).

Voici quelques informations au sujet de ce serveur virtuel :

Caractéristiques	Valeurs
Nom du système	SRV-ADDS-01
Système d'exploitation	Windows Server 2016
Nom de domaine Active Directory	it-connect.local
Nom de domaine NETBIOS	IT-CONNECT

Ce cours s'applique aussi bien à Windows Server 2012, Windows Server 2012 R2, Windows Server 2016 qu'à Windows Server 2019.

Si vous le souhaitez, vous pouvez opérer depuis un poste sous Windows 10, intégré à ce même domaine et sur lequel vous serez connecté avec une session ayant des droits « Admin du domaine ».

Prêt ? Alors allons-y !

3. Créer un domaine Active Directory via PowerShell

Pour mettre en place les services de domaine Active Directory, il est bien entendu possible de le faire par l'interface graphique, mais aussi en ligne de commande par PowerShell. Ceci sera utile notamment sur un serveur en mode core, mais également pour **automatiser la création d'un domaine**, que ce soit pour votre lab perso ou pour une mise en œuvre.

Pour rappel, un serveur en mode core est une machine installée sous Windows Server sans interface graphique. En local, la gestion d'une machine installée en mode core s'effectue uniquement à partir de la console.

Des outils d'automatisation, comme PowerShell DSC pourront vous permettre de déployer ADDS ou un contrôleur de domaine rapidement en s'appuyant sur PowerShell. Pour cet exemple, on utilisera simplement des commandes PowerShell qu'il est tout à fait possible de mettre dans un script.

Pour préparer notre lab' dans le cadre de ce cours, voyons ensemble **comment déployer Active Directory avec PowerShell**.

Alternative - créer un domaine Active Directory via l'interface graphique :

<https://www.it-connect.fr/creer-un-domaine-ad-avec-windows-server-2016/>

I. Nom d'hôte

Commençons par renommer le serveur, dans cet exemple « SRV-ADDS-01 » puis redémarrons le serveur. Ce qui nous donne ces deux commandes :

```
Rename-Computer -NewName SRV-ADDS-01 -Force  
Restart-Computer
```

Lorsque le serveur aura redémarré, il aura son joli petit nom !

II. Configuration réseau

Maintenant, on va définir la configuration réseau du serveur, toujours via PowerShell. Dans cet exemple, j'attribue l'adresse IP 192.168.1.10 en IP, avec un masque 255.255.255.0 (/24) et une passerelle par défaut 192.168.1.1.

```
New-NetIPAddress -IPAddress "192.168.1.10" -PrefixLength "24" -InterfaceIndex (Get-NetAdapter).ifIndex -DefaultGateway "192.168.1.1"
```

Pour définir le serveur DNS, il faut utiliser un autre cmdlet, ce qui nous donne :

```
Set-DnsClientServerAddress -InterfaceIndex (Get-NetAdapter).ifIndex -ServerAddresses ("127.0.0.1")
```

Pour terminer la configuration réseau, on va renommer notre carte réseau. Le nom actuel est "Ethernet0" que l'on va renommer en "LAN".

```
Rename-NetAdapter -Name Ethernet0 -NewName LAN
```

Si tout va bien, votre serveur a un nom définitif et une configuration réseau adéquate. Nous pouvons passer à la phase la plus intéressante : la mise en place du domaine Active Directory.

III. Installation des rôles

Pour cette installation, nous aurons besoin de trois fonctionnalités : les services de domaine Active Directory (AD-Domain-Services), le DNS (DNS) et les outils d'administration graphique (RSAT-AD-Tools), mais ceci est facultatif.

```
$FeatureList = @("RSAT-AD-Tools","AD-Domain-Services","DNS")
Foreach($Feature in $FeatureList){
    if(((Get-WindowsFeature -Name $Feature).InstallState) -eq "Available"){
        Write-Output "Feature $Feature will be installed now !"
        Try{
            Add-WindowsFeature-Name $Feature -IncludeManagementTools -
            IncludeAllSubFeature
            Write-Output "$Feature : Installation is a success !"
        }Catch{
            Write-Output "$Feature : Error during installation !"
        }
    } # if(((Get-WindowsFeature -Name $Feature).InstallState) -eq "Available")
} # Foreach($Feature in $FeatureList)
```

Vous pourrez réutiliser le bloc de code ci-dessus, il va installer les trois fonctionnalités une à une, et vous indiquer le résultat à chaque fois. Si vous ne rencontrez pas d'erreur, vous pouvez passer à la suite.