Gestion de l'Active Directory avec PowerShell

Création de domaine, groupes, utilisateurs, jonction de poste et déploiement logiciel

1. Contexte et objectif

L'Active Directory (AD) est le service d'annuaire de Microsoft. Il centralise la gestion des utilisateurs, des groupes, des ordinateurs et des politiques de sécurité au sein d'un domaine Windows. Il permet à une entreprise de gérer finement les droits d'accès, d'authentifier les utilisateurs sur n'importe quel poste du domaine et de déployer des configurations ou des logiciels à distance.

Cette documentation présente les opérations AD réalisées en PowerShell : création du domaine, des unités organisationnelles, des groupes de sécurité, des comptes utilisateurs, la jonction d'un poste client au domaine, et le déploiement d'un logiciel à distance via PSSession.

2. Création du domaine Active Directory

Le rôle AD DS (Active Directory Domain Services) est d'abord installé sur le serveur Windows, avec les outils de gestion inclus :

```
Install-WindowsFeature AD-Domain-Services -IncludeManagementTools
```

Une fois le rôle installé, le module ADDSDeployment est importé et la forêt Active Directory est créée. Le domaine lucas.local est configuré avec le nom NetBIOS LUCAS, le DNS intégré est activé, et un mot de passe de mode restauration est défini :

```
Import-Module ADDSDeployment
Install-ADDSForest `
    -DomainName "lucas.local" `
    -DomainNetbiosName "LUCAS" `
    -InstallDNS `
    -Force
```

```
PS C:\Users\Administrateur> Install-WindowsFeature AD-Domain-Services -IncludeManagementTools

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             Success        {Services AD DS, Gestion de stratégie de g...


PS C:\Users\Administrateur> Import-Module ADDSDeployment
PS C:\Users\Administrateur> Install-ADDSForest `
>>     -DomainName "lucas.local" `
>>     -DomainNetbiosName "LUCAS" `
>>     -InstallDNS `
>>     -Force
SafeModeAdministratorPassword: ********
Confirmer SafeModeAdministratorPassword: ********
```

L'installation valide l'environnement, crée la partition d'annuaire et applique la configuration. Des avertissements informatifs apparaissent (chiffrement NT 4.0, délégation DNS) mais n'empêchent pas la création. Le serveur redémarre automatiquement à l'issue.

```
AVERTISSEMENT : Cet ordinateur contient au moins une carte réseau physique pour laquelle aucune adresse IP statique n'a
 été attribuée à ses propriétés IP. Si IPv4 et IPv6 sont tous deux activés pour une carte réseau, vous devez attribuer

 Install-ADDSForest

   Validation d'environnement et d'entrée utilisateur
      Tous les tests ont réussi
      [oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo]
   Installation d'une nouvelle forêt
      Création en cours de la partition d'annuaire : CN=Configuration,DC=lucas,DC=local; 787 objets restants

AVERTISSEMENT : Les contrôleurs de domaine Windows Server 2022 offrent un paramètre de sécurité par défaut nommé
« Autoriser les algorithmes de chiffrement compatibles avec Windows NT 4.0 ». Ce paramètre empêche l'utilisation
d'algorithmes de chiffrement faibles lors de l'établissement de sessions sur canal sécurisé.

Pour plus d'informations sur ce paramètre, voir l'article 942564 de la Base de connaissances
(http://go.microsoft.com/fwlink/?LinkId=104751).

AVERTISSEMENT : Cet ordinateur contient au moins une carte réseau physique pour laquelle aucune adresse IP statique n'a
 été attribuée à ses propriétés IP. Si IPv4 et IPv6 sont tous deux activés pour une carte réseau, vous devez attribuer
des adresses IP statiques IPv4 et IPv6 aux propriétés IPv4 et IPv6 de la carte réseau physique. Ces affectations
d'adresses IP statiques doivent être effectuées sur toutes les cartes réseau physiques pour que l'opération DNS soit
fiable.

AVERTISSEMENT : Il est impossible de créer une délégation pour ce serveur DNS car la zone parente faisant autorité est
introuvable ou elle n'exécute pas le serveur DNS Windows. Si vous procédez à l'intégration avec une infrastructure DNS
existante, vous devez manuellement créer une délégation avec ce serveur DNS dans la zone parente pour activer une
résolution de noms fiable en dehors du domaine « lucas.local ». Sinon, aucune action n'est requise.
```

3. Création des groupes de sécurité

Les groupes de sécurité permettent d'organiser les utilisateurs par service et de leur attribuer des droits collectifs. La cmdlet New-ADGroup crée un groupe dans l'annuaire :

Creates an Active Directory group.

Syntax

Default (Default)

Syntax — Copy

```
New-ADGroup
    [-WhatIf]
    [-Confirm]
    [-AuthType <ADAuthType>]
    [-Credential <PSCredential>]
    [-Description <String>]
    [-DisplayName <String>]
    [-GroupCategory <ADGroupCategory>]
    [-GroupScope] <ADGroupScope>
    [-HomePage <String>]
    [-Instance <ADGroup>]
    [-ManagedBy <ADPrincipal>]
    [-Name] <String>
    [-OtherAttributes <Hashtable>]
    [-PassThru]
    [-Path <String>]
    [-SamAccountName <String>]
    [-Server <String>]
    [<CommonParameters>]
```

Description

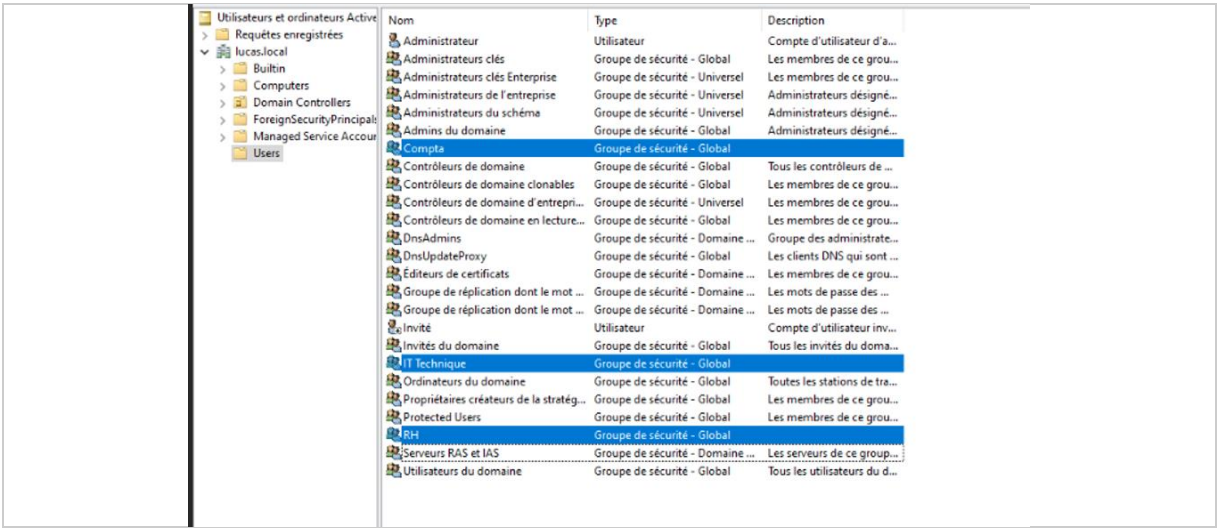
The **New-ADGroup** cmdlet creates an Active Directory group object. Many object properties are defined by setting cmdlet parameters. Properties that cannot be set by cmdlet parameters can be set using the **OtherAttributes** parameter.

Trois groupes de sécurité globaux sont créés, correspondant aux services de l'entreprise :

```
New-ADGroup -Name "RH" -GroupScope Global -GroupCategory Security -Path
"CN=Users,DC=lucas,DC=local"
New-ADGroup -Name "Compta" -GroupScope Global -GroupCategory Security -Path
"CN=Users,DC=lucas,DC=local"
New-ADGroup -Name "IT Technique" -GroupScope Global -GroupCategory Security -Path
"CN=Users,DC=lucas,DC=local"
```

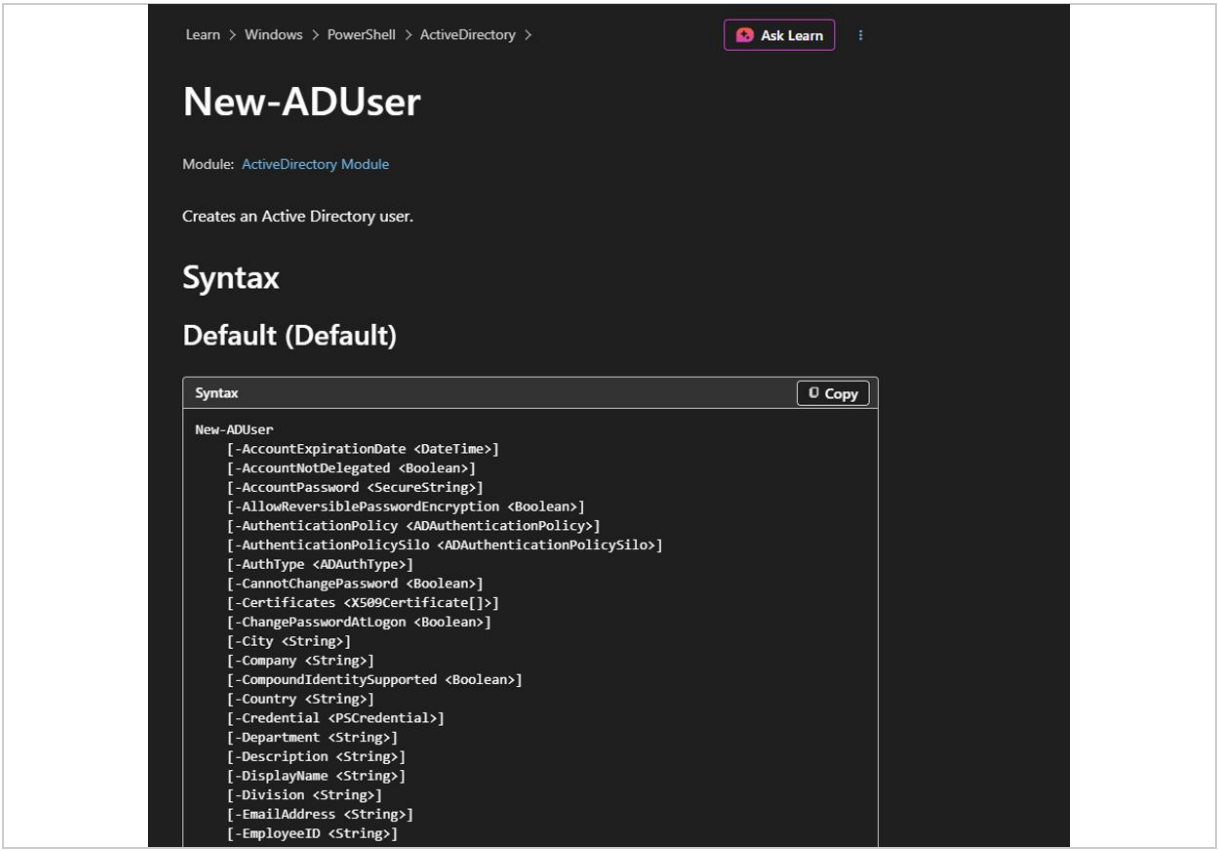
```
PS C:\Users\Administrateur> New-ADGroup -Name "RH" -GroupScope Global -GroupCategory Security -Path "CN=Users,DC=lucas,DC=local"
PS C:\Users\Administrateur> New-ADGroup -Name "Compta" -GroupScope Global -GroupCategory Security -Path "CN=Users,DC=lucas,DC=local"
PS C:\Users\Administrateur> New-ADGroup -Name "IT Technique" -GroupScope Global -GroupCategory Security -Path "CN=Users,DC=lucas,DC=local"
```

Les groupes créés (RH, Compta, IT Technique) apparaissent dans la console "Utilisateurs et ordinateurs Active Directory" aux côtés des groupes système du domaine :

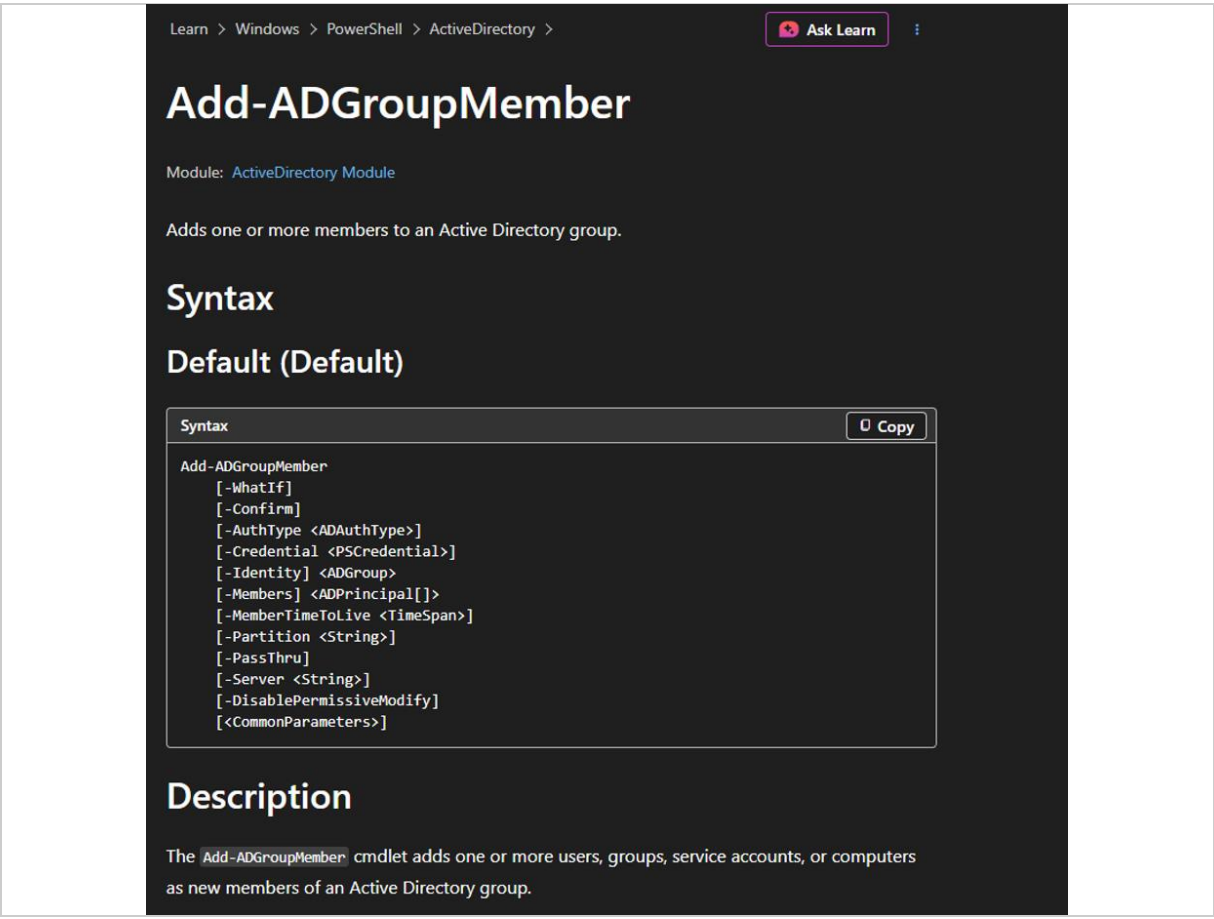


4. Création des comptes utilisateurs et attribution aux groupes

La cmdlet New-ADUser crée un compte utilisateur dans l'annuaire Active Directory. Elle accepte de nombreux paramètres (nom, prénom, UPN, mot de passe, statut d'activation, chemin OU, etc.) :



La cmdlet Add-ADGroupMember ajoute un ou plusieurs utilisateurs à un groupe existant :



Learn > Windows > PowerShell > ActiveDirectory > Ask Learn

Add-ADGroupMember

Module: ActiveDirectory Module

Adds one or more members to an Active Directory group.

Syntax

Default (Default)

Syntax — Copy

```
Add-ADGroupMember
    [-WhatIf]
    [-Confirm]
    [-AuthType <ADAuthType>]
    [-Credential <PSCredential>]
    [-Identity] <ADGroup>
    [-Members] <ADPrincipal[]>
    [-MemberTimeToLive <TimeSpan>]
    [-Partition <String>]
    [-PassThru]
    [-Server <String>]
    [-DisablePermissiveModify]
    [<CommonParameters>]
```

Description

The `Add-ADGroupMember` cmdlet adds one or more users, groups, service accounts, or computers as new members of an Active Directory group.

Trois comptes utilisateurs sont créés et immédiatement affectés à leur groupe de service respectif. Les comptes sont activés (Enabled $true), le mot de passe est défini de manière sécurisée avec ConvertTo-SecureString, et le changement de mot de passe à la prochaine connexion est désactivé (AsPlainText) :

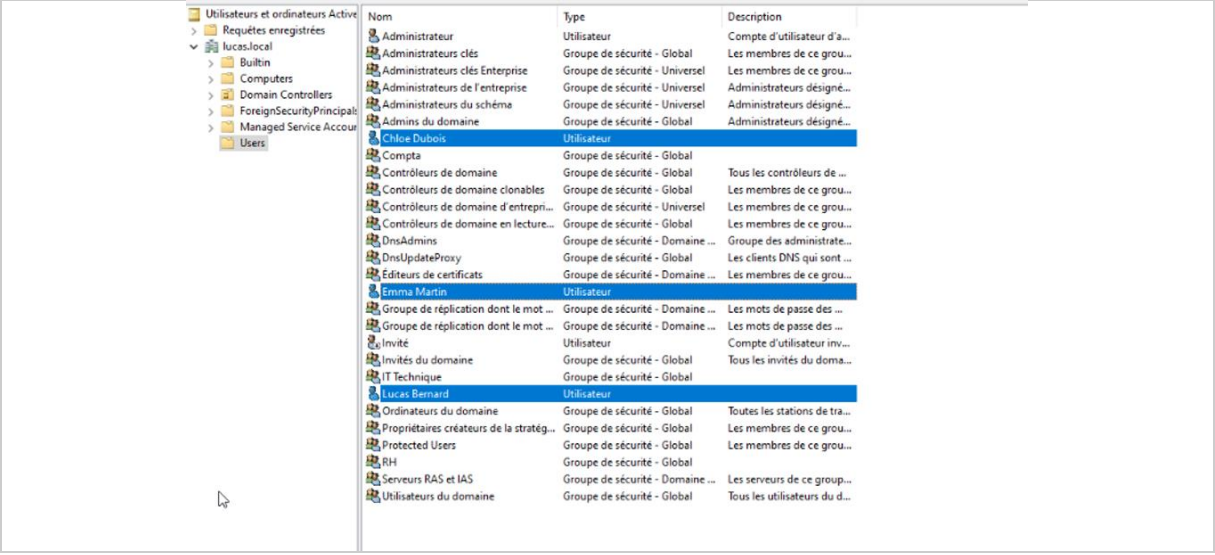
```
New-ADUser -Name "Emma Martin" -GivenName "Emma" -Surname "Martin" -SamAccountName "emartin" \
  -UserPrincipalName "emartin@lucas.local" -AccountPassword (ConvertTo-SecureString
"P@ssw0rd123!" -AsPlainText -Force) \
  -Enabled $true -Path "CN=Users,DC=lucas,DC=local"
Add-ADGroupMember -Identity "RH" -Members "emartin"

New-ADUser -Name "Lucas Bernard" -GivenName "Lucas" -Surname "Bernard" -SamAccountName
"lbernard" \
  -UserPrincipalName "lbernard@lucas.local" -AccountPassword (...) -Enabled $true -Path ...
Add-ADGroupMember -Identity "Compta" -Members "lbernard"

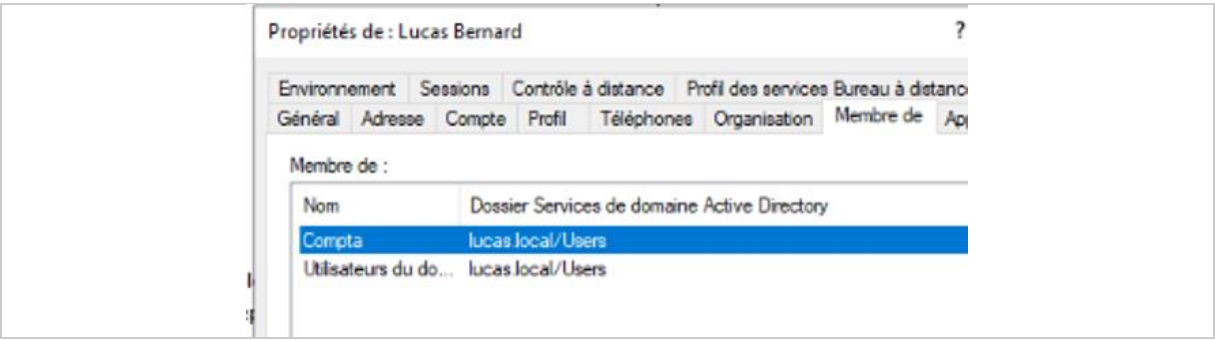
New-ADUser -Name "Chloe Dubois" -GivenName "Chloe" -Surname "Dubois" -SamAccountName "cdubois" \
  -UserPrincipalName "cdubois@lucas.local" -AccountPassword (...) -Enabled $true -Path ...
Add-ADGroupMember -Identity "IT Technique" -Members "cdubois"
```



La console AD affiche les trois utilisateurs créés (Chloe Dubois, Emma Martin, Lucas Bernard) parmi les objets du domaine :



La vérification des propriétés d'un utilisateur (ici Lucas Bernard) confirme son appartenance au groupe Compta et au groupe Utilisateurs du domaine :



5. Jonction d'un poste client au domaine

5.1 Configuration du DNS sur le poste client

Pour rejoindre un domaine Active Directory, le poste client doit utiliser le serveur AD DS comme serveur DNS. Sans cela, il ne peut pas résoudre le nom de domaine lucas.local. La cmdlet Set-DnsClientServerAddress configure le DNS sur l'interface réseau :



Set-DnsClientServerAddress

Module: DnsClient Module

Sets DNS server addresses associated with the TCP/IP properties on an interface.

Syntax

ByAlias (Default)

Syntax — Copy

```
Set-DnsClientServerAddress
    [-InterfaceAlias] <String[]>
    [-ServerAddresses <String[]>]
    [-Validate]
    [-ResetServerAddresses]
    [-CimSession <CimSession[]>]
    [-ThrottleLimit <Int32>]
    [-AsJob]
    [-PassThru]
    [-WhatIf]
    [-Confirm]
    [<CommonParameters>]
```

ByName

Syntax — Copy

```
Set-DnsClientServerAddress
    -InterfaceIndex <UInt32[]>
    [-ServerAddresses <String[]>]
    [-Validate]
    [-ResetServerAddresses]
    [-CimSession <CimSession[]>]
    [-ThrottleLimit <Int32>]
    [-AsJob]
    [-PassThru]
    [-WhatIf]
    [-Confirm]
    [<CommonParameters>]
```

```
Set-DnsClientServerAddress -InterfaceAlias "Ethernet" -ServerAddresses "192.168.108.119"
```

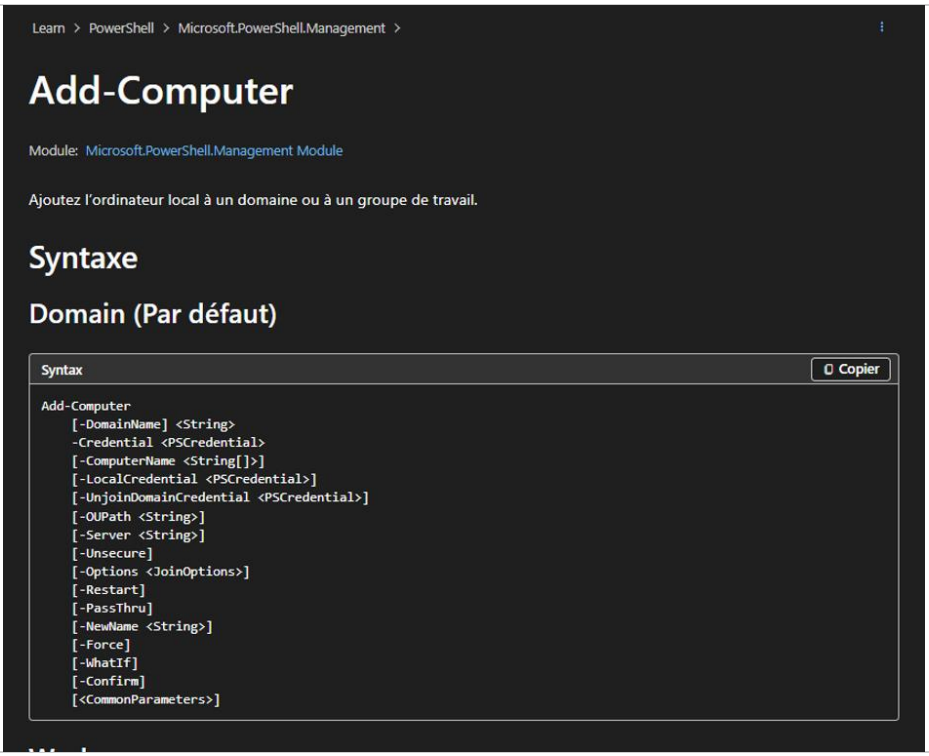
La résolution DNS est vérifiée avec nslookup, qui doit retourner l'adresse IP du contrôleur de domaine pour lucas.local :

```
PS C:\Users\lucas> Set-DnsClientServerAddress -InterfaceAlias "Ethernet" -ServerAddresses "192.168.108.119"
PS C:\Users\lucas> nslookup lucas.local
Serveur :   UnKnown
Address:  192.168.108.119

Nom :    lucas.local
Address:  192.168.108.119
```

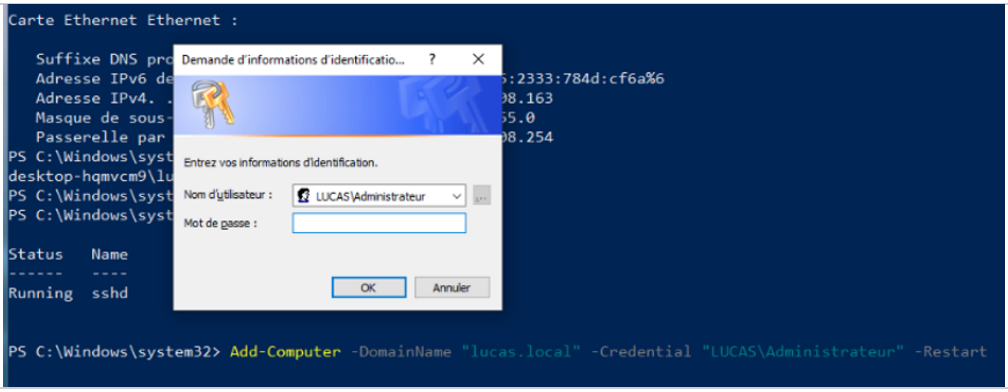
5.2 Jonction du poste au domaine

La cmdlet Add-Computer joint le poste local au domaine Windows. Elle requiert les identifiants d'un administrateur du domaine et déclenche un redémarrage :



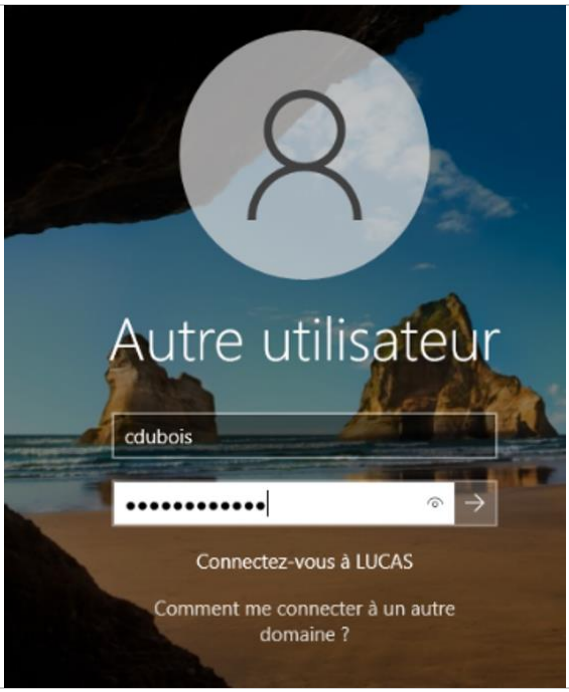

```
Add-Computer -DomainName "lucas.local" -Credential "LUCAS\Administrateur" -Restart
```

Une fenêtre de saisie des identifiants s'affiche. Les informations de l'administrateur du domaine sont saisies, puis le poste redémarre automatiquement pour finaliser la jonction :



5.3 Connexion avec un compte du domaine

Après redémarrage, l'écran de connexion Windows propose l'option "Autre utilisateur" et affiche "Connectez-vous à LUCAS", confirmant la jonction au domaine. L'utilisateur peut désormais se connecter avec n'importe quel compte du domaine (ici cdubois) :

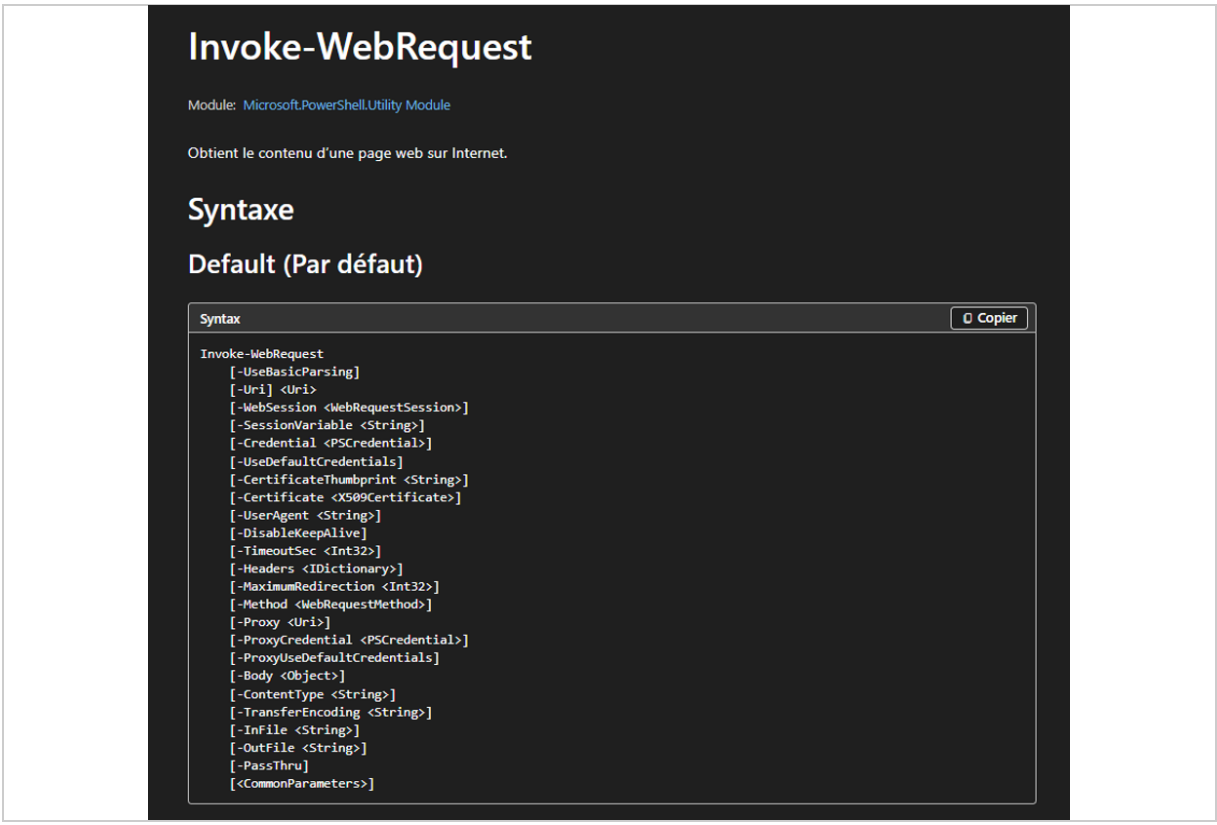


6. Déploiement de Firefox depuis le serveur vers un poste client

PowerShell permet d'administrer des postes à distance via des sessions PSSession. Cette fonctionnalité est utilisée ici pour déployer Firefox sur le poste client de Nicolas Joret (groupe RH) depuis le serveur, sans intervention manuelle sur le poste.

6.1 Téléchargement du fichier MSI sur le serveur

L'installeur Firefox au format MSI est téléchargé sur le serveur via la cmdlet Invoke-WebRequest, qui effectue une requête HTTP pour récupérer un fichier distant :

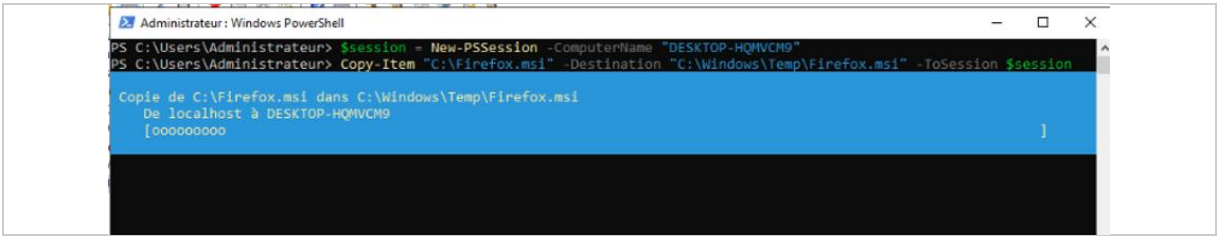



```
Invoke-WebRequest "https://download.mozilla.org/?product=firefox-msi-latest-
ssl&os=win64&lang=fr" -OutFile "C:\Firefox.msi"
```

6.2 Copie du MSI vers le poste client

Une session PowerShell distante (PSSession) est ouverte vers le poste client DESKTOP-HQMVCM9. Le fichier MSI est copié depuis le serveur vers le dossier temporaire du poste client :

```
$session = New-PSSession -ComputerName "DESKTOP-HQMVCM9"
Copy-Item "C:\Firefox.msi" -Destination "C:\Windows\Temp\Firefox.msi" -ToSession $session
```



6.3 Installation silencieuse à distance

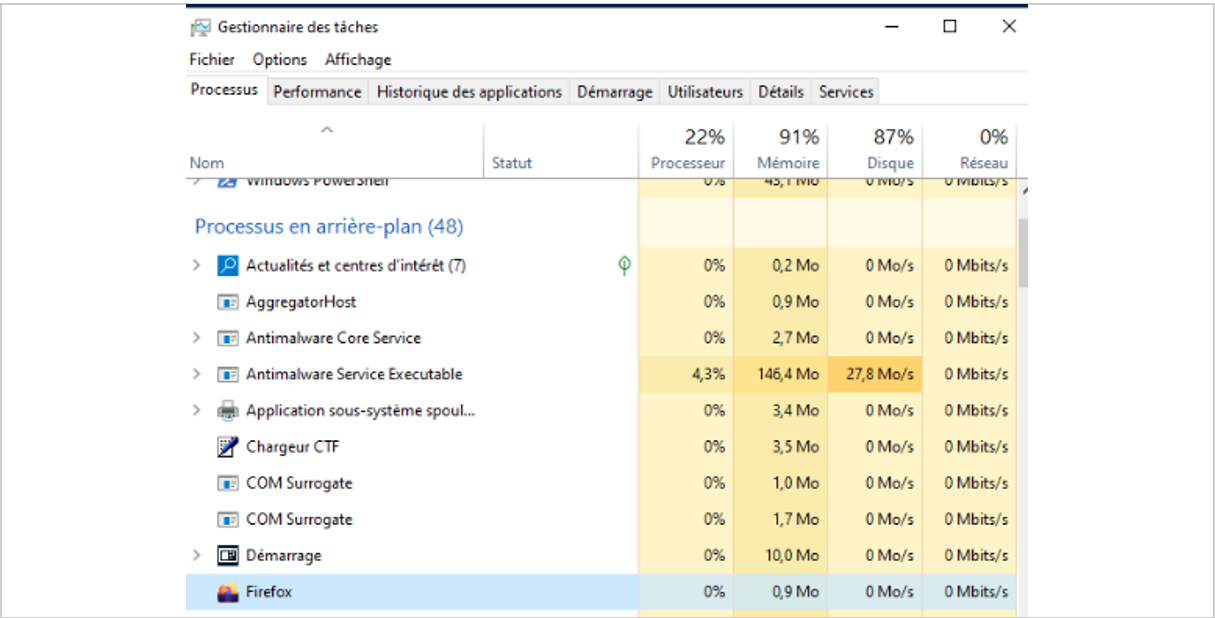
L'installation est déclenchée à distance via Invoke-Command, qui exécute un bloc de script sur la session distante. L'installeur msiexec est lancé en mode silencieux (/qn) sans redémarrage (/norestart) :

```
$session = New-PSSession -ComputerName DESKTOP-HQMVCM9
Invoke-Command -Session $session -ScriptBlock {
    Start-Process msiexec.exe -ArgumentList '/i "C:\Windows\Temp\Firefox.msi" /qn /norestart' -
Wait
}
```



6.4 Vérification côté poste client

Sur le poste client, le Gestionnaire des tâches confirme que le processus Firefox est présent en arrière-plan, indiquant que l'installation s'est déroulée avec succès :



Après environ une minute, Firefox apparaît sur le bureau du poste client, installé sans aucune intervention de l'utilisateur :

