Nicolas Yang

Active Directory

Contexte :
Active Directory est un service annuaire d'entreprise qui existe depuis 1996 et est utilisable depuis Windows 2000 Server Edition sorti en 1999. Il s'agit donc d'un produit éprouvé par les années. Cet annuaire d'entreprise vient en remplacement des bases SAM (Security Account Manager) qui étaient exploitées avec NT4 et les groupes de travail. Ces bases présentaient notamment des limitations d'administration. L'arrivée d'Active Directory a permis de passer des groupes de travail aux domaines Active Directory et ainsi de centraliser toute l'administration et la gestion des droits dans un annuaire de type LDAP. Tout logiciel utilisant LDAP sera capable de communiquer avec Active Directory : on peut, par exemple, gérer (partiellement) des postes Linux à partir d'un Active Directory.

Il étend les fonctionnalités des services d'annuaire précédemment fournis avec Windows et offre en outre des fonctionnalités entièrement nouvelles. Active Directory est sécurisé, distribué, partitionné et dupliqué. Il a été conçu pour fonctionner correctement quelle que soit la taille de l'installation, d'un serveur unique comportant quelques centaines d'objets à un ensemble de milliers de serveurs et de millions d'objets.

Prérequis :
La configuration matérielle minimale :
Processeur : Architecture 64 bits uniquement, cadencé à 1,4 GHz au minimum (il est recommandé d’avoir un processeur multicœur).

Mémoire vive : 512 Mo au minimum (il est recommandé d’avoir au moins 1024 Mo).

Disque dur : 32 Go au minimum (l’installation réelle prenant environ 10 Go, il faut que le système ait de la place pour gérer la mémoire sur le disque).

Nicolas Yang

Tutoriel :
Installer Active Directory

Utilisez les commandes de base de PowerShell
Vous avez :

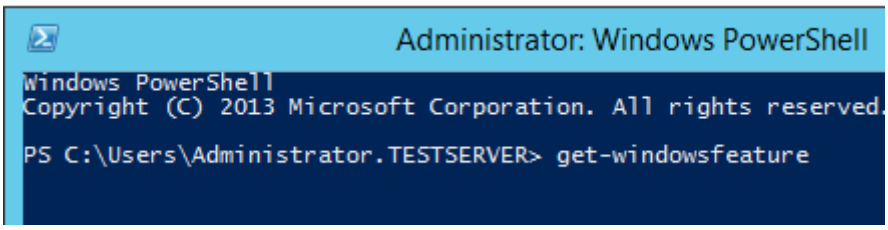
C:\Users\Administrateur>

Tapez « powershell » puis « validez ».

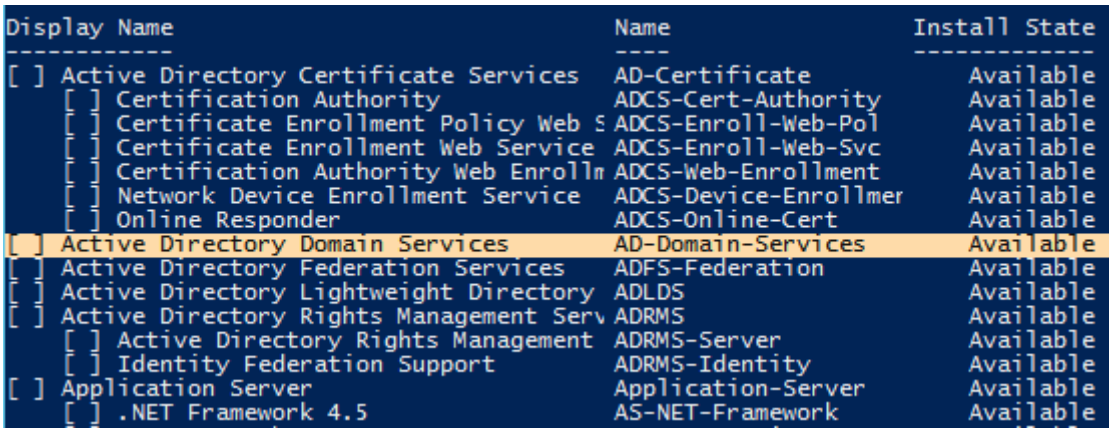
Si vous regardez votre prompt, il a changé, il est passé de C:\Users\Administrateur> à PS C:\Users\Administrateur>.

Vous êtes maintenant en mode PowerShell.

Obtenir le nom du service AD
Pour commencer l'installation d'AD à partir de la ligne de commande, nous devons connaître le nom exact du service Active Directory que nous devons installer.
Tout d'abord, exécutez la commande «get-windowsfeature» à partir du PowerShell Windows.



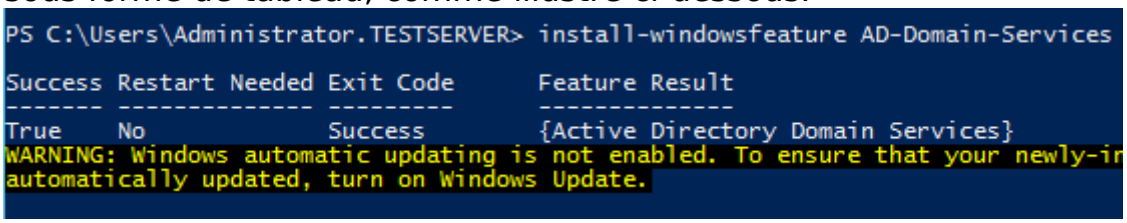
Cela répertoriera toutes les fonctionnalités du serveur Windows comme indiqué ci-dessous. Comme vous le voyez dans cette liste, le nom du service AD est «AD-Domain-Services».



Installer le service de domaine AD
Pour installer Active Directory à partir de la ligne de commande, utilisez la commande «install-windowsfeature» comme indiqué ci-dessous.

```
C: \> Install-windowsfeature AD-Domain-Services
```

Cette commande va extraire tous les fichiers binaires requis et démarrer l'installation AD.
Une fois l'installation d'Active Directory terminée, il affichera le résultat sous forme de tableau, comme illustré ci-dessous.



Importer le module ADDSDeployment
Pour augmenter les performances du serveur, tous les modules et commandes ne sont pas chargés par défaut sur le serveur. Nous devons importer les modules selon nos besoins.
Pour poursuivre l'installation et la configuration d'AD, nous avons besoin du module ADDSDeployment. Importez ce module comme indiqué ci-dessous à l'aide de la commande powershell d'import-module.

```
C: \> Import-Module ADDSDeployment
```

Commandes pour promouvoir le serveur en tant que contrôleur de domaine
Ensuite, promouvez votre serveur en tant que contrôleur de domaine en fonction de vos besoins à l'aide de l'une des commandes suivantes.

Commander	**La description**
Add-ADDSReadOnlyDomainControllerAccount	Installer un contrôleur de domaine en lecture seule
Install-ADDSDomain	Installer le premier contrôleur de domaine dans un domaine enfant ou arborescent
Install-ADDSDomainController	Installer un contrôleur de domaine supplémentaire dans le domaine
Install-ADDSForest	Installer le premier contrôleur de domaine dans une nouvelle forêt
Test-ADDSDomainControllerInstallation	Vérifier les prérequis pour installer un contrôleur de domaine supplémentaire

	dans le domaine
Test-ADDSDomainControllerUninstallation	Désinstaller le service AD du serveur
Test-ADDSDomainInstallation	Vérifier les prérequis pour installer le premier contrôleur de domaine dans un domaine enfant ou arborescent
Test-ADDSForestInstallation	Installer le premier contrôleur de domaine dans une nouvelle forêt
Test-ADDSReadOnlyDomainControllerAccountCreation	Vérifier les prérequis pour installer le contrôleur de domaine en lecture seule
Uninstall-ADDSDomainController	Désinstaller le contrôleur de domaine du serveur

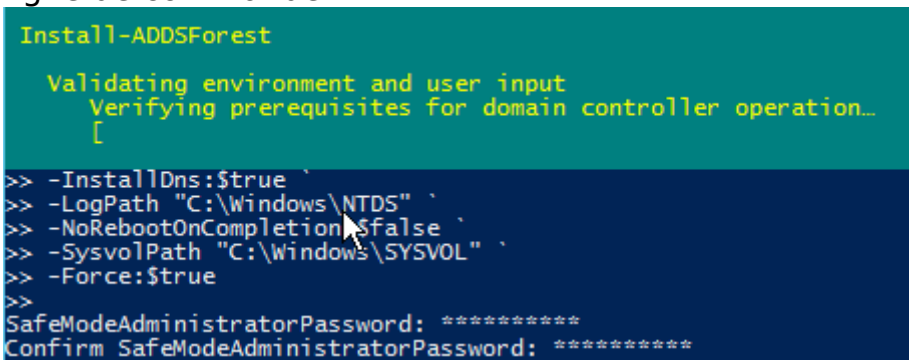
Installez le premier contrôleur de domaine dans la forêt
Dans cet exemple, nous installons le premier contrôleur de domaine dans la forêt.
Pour installer Active Directory avec la configuration par défaut, exécutez la commande «Install-AddsForest»:

```
C: \> Install-AddsForest
```

Pour installer Active Directory avec des options personnalisées, transmettez les paramètres appropriés comme indiqué ci-dessous. Dans cet exemple, nous définissons plusieurs paramètres de configuration pour notre AD, y compris le DomainName.

```
C: \> Install-ADDSForest
 -CreateDnsDelegation: $ false `
 -DatabasePath "C: \ Windows \ NTDS" `
 -DomainMode "Win2012R2" "
 -DomainName "thegeekstuff.com" "
 -DomainNetbiosName "THEGEEKSTUFF" `
 -ForestMode "Win2012R2" "
 -InstallDns: $ true `
 -LogPath "C: \ Windows \ NTDS" "
 -NoRebootOnCompletion: $ false `
 -SysvolPath "C: \ Windows \ SYSVOL" `
 -Force: $ true
```

Terminez l'installation d'AD
Enfin, cela vous demandera SafeModeAdministratorPassword. Ce mot de passe correspond au mode de restauration des services d'annuaire (DSRM).
Définissez ici votre mot de passe DSRM, qui terminera l'installation et la configuration d'AD sur votre serveur Windows à l'aide des utilitaires de ligne de commande.



Nicolas Yang

Utilisation :
Automatisez la configuration d’Active Directory avec PowerShell
La commande **New-ADUser** permet de créer un utilisateur avec PowerShell.

Comment gérer les utilisateurs

Création d'un nouveau compte utilisateur

Tapez la commande suivante :

dsadd user **userdn** -samid **sam_name**

Les valeurs suivantes sont utilisées dans cette commande :

- **userdn** spécifie le nom unique (également connu sous le nom de DN) de l'objet utilisateur que vous souhaitez ajouter.
- **sam-name** spécifie le nom de gestionnaire de compte de sécurité (SAM) utilisé comme nom de compte SAM unique pour cet utilisateur (par exemple, Linda).

Pour spécifier le mot de passe du compte utilisateur, tapez la commande suivante, où **le mot de passe** est le mot de passe qui doit être utilisé pour le compte utilisateur :

dsadd user userdn -pwd **mot de passe**

REMARQUE Pour afficher la syntaxe complète pour cette commande, et pour obtenir plus d'informations sur la saisie de plus d'informations sur le compte d'utilisateur, à une invite de commande, tapez dsadd user /?.

Réglage d'un mot de passe utilisateur

Tapez la commande suivante :

dsmod user **user_dn** -pwd **nouveau mot de passe**

Cette commande utilise les valeurs suivantes :

- **user_dn** spécifie le nom unique de l'utilisateur pour lequel le mot de passe sera réinitialisé.
- **new_password** spécifie le mot de passe qui remplacera le mot de passe utilisateur actuel

2. Si vous souhaitez demander à l'utilisateur de modifier ce mot de passe lors du prochain processus de connexion, tapez la commande suivante :

dsmod user **user_dn** -mustchpwd {yes|no}

REMARQUE Si un mot de passe n'est pas attribué, la première fois que l'utilisateur tente de se connecter (en utilisant un mot de passe vierge), le message de connexion suivant s'affiche :
Vous devez changer votre mot de passe à la première ouverture de session

Une fois que l'utilisateur a changé le mot de passe, le processus de connexion continue.

Vous devez réinitialiser les services qui sont authentifiés avec un compte utilisateur si le mot de passe du compte utilisateur du service est modifié.

REMARQUE Pour afficher la syntaxe complète pour cette commande, et pour obtenir plus d'informations sur la saisie de plus d'informations sur le compte d'utilisateur, à une invite de commande, tapez dsmod user /?.

Désactivation ou activation d'un compte utilisateur

T*apez la commande suivante :*

dsmod user **user_dn** -disabled {yes|no}

Cette commande utilise les valeurs suivantes :

- **user_dn** spécifie le nom unique de l'objet utilisateur à désactiver ou à activer.
- **{yes|no}** précise si le compte utilisateur est désactivé pour se connecter (oui) ou non (non).

REMARQUE Par mesure de sécurité, au lieu de supprimer le compte de cet utilisateur, vous pouvez désactiver les comptes d'utilisateurs pour empêcher un utilisateur particulier de se connecter. Si vous désactivez les comptes d'utilisateurs qui ont des adhésions de groupe communes, vous pouvez utiliser les comptes d'utilisateur désactivés comme modèles de compte pour simplifier la création de compte d'utilisateur.

Suppression d'un compte utilisateur

Tapez la commande suivante, où
user_dn spécifie le nom unique de l'objet utilisateur à supprimer :

dsrm **user-dn**

Après avoir supprimé un compte d'utilisateur, toutes les autorisations et les adhésions associées à ce compte d'utilisateur sont définitivement supprimées. Étant donné que l'identifiant de sécurité (SID) pour chaque

compte est unique, si vous créez un nouveau compte d'utilisateur qui a le même nom qu'un compte d'utilisateur précédemment supprimé, le nouveau compte n'assume pas automatiquement les autorisations et les adhésions du compte d'utilisateur supprimé. Pour dupliquer un compte d'utilisateur supprimé, vous devez recréer manuellement toutes les autorisations et les adhésions.

REMARQUE Pour afficher la syntaxe complète pour cette commande, et pour obtenir plus d'informations sur la saisie de plus d'informations sur le compte d'utilisateur, à une invite de commande, tapez dsrm /?.

Comment gérer les groupes

Création d'un nouveau groupe

T*apez la commande suivante :*

dsadd group **group_dn** -samid **sam_name** -secgrp yes | no -scope l | g | u

Cette commande utilise les valeurs suivantes :

- **group-dn** spécifie le nom unique de l'objet du groupe que vous souhaitez ajouter.
- **sam-name** spécifie le nom SAM qui est le nom du compte SAM unique pour ce groupe (par exemple, les opérateurs).
- yes | no spécifie si le groupe que vous souhaitez ajouter est un groupe de sécurité (oui) ou un groupe de distribution (non).
- l | g | u spécifie la portée du groupe que vous souhaitez ajouter (domaine local [l], global [g], ou universel [u]).

Si le domaine dans lequel vous créez le groupe est réglé au niveau fonctionnel de domaine de Windows 2000 mixed, vous pouvez sélectionner uniquement les groupes de sécurité avec des étendues locales ou globales de domaine.

Pour afficher la syntaxe complète pour cette commande, et pour obtenir plus d'informations sur la saisie de plus d'informations sur le groupe, à une invite de commande, tapez dsadd group /?.

Ajout d'un membre à un groupe

Tapez la commande suivante :

dsmod group **group_dn** -addmbr **member_dn**

Cette commande utilise les valeurs suivantes :

- **group-dn** spécifie le nom unique de l'objet du groupe que vous souhaitez ajouter.
- **member_dn** spécifie le nom unique de l'object que vous souhaitez ajouter au groupe.

En plus des utilisateurs et des ordinateurs, un groupe peut contenir des contacts et d'autres groupes.

Pour afficher la syntaxe complète pour cette commande, et pour obtenir plus d'informations sur la saisie de plus d'informations sur le compte d'utilisateur et le groupe, à une invite de commande, tapez dsmod group /?.

Conversion d'un groupe en un autre type de groupe

Tapez la commande suivante :

dsmod group **group_dn** -secgrp {yes|no}

Cette commande utilise les valeurs suivantes :

- **group_dn** spécifie le nom unique de l'objet du groupe pour lequel vous souhaitez modifier le type de groupe.
- {yes|no} spécifie que le type de groupe est réglé sur le groupe de sécurité (oui) ou le groupe de distribution (non).

Pour convertir un groupe, la fonctionnalité du domaine doit être réglée sur Windows 2000 Native ou supérieur. Vous ne pouvez pas convertir les groupes lorsque la fonctionnalité du domaine est réglée sur Windows 2000 Mixed.

Pour afficher la syntaxe complète de cette commande, à une invite de commandes, tapez dsmod group /?.

Modification de l'étendue du groupe

Tapez la commande suivante :

dsmod group **group_dn** -scope l|g|u

Cette commande utilise les valeurs suivantes :

- **group_dn** spécifie les noms uniques de l'objet du groupe auquel la portée sera modifiée.

- l|g|u spécifie la portée à laquelle le groupe doit être fixé (local, global ou universel). Si le domaine est toujours réglé sur Windows 2000 mixed, la portée universelle n'est pas pris en charge. En outre, il n'est pas possible de convertir un groupe local de domaine en groupe global ou vice versa.

Suppression d'un groupe

Tapez la commande suivante :

dsrm **group_dn**

Cette commande utilise les valeurs suivantes :

- **group_dn** spécifie le nom unique de l'objet du groupe à supprimer.

REMARQUE Si vous supprimez le groupe, le groupe est définitivement supprimé.

Pour afficher la syntaxe complète de cette commande, à une invite de commandes, tapez dsrm /?.

Recherche d'un groupe dont un utilisateur est membre

Tapez la commande suivante :

dsget user **user_dn** -memberof

Cette commande utilise les valeurs suivantes :

- **user_dn** spécifie le nom unique de l'objet utilisateur pour lequel vous souhaitez afficher l'adhésion au groupe.

Pour afficher la syntaxe complète de cette commande, à une invite de commandes, tapez dsget user /?.

Comment gérer les ordinateurs

Création d'un nouveau compte d'ordinateur

Tapez la commande suivante :

dsadd computer **computer_dn**

Cette commande utilise les valeurs suivantes :

- **computer_dn** spécifie le nom unique de l'ordinateur que vous souhaitez ajouter. Le nom unique indique l'emplacement du dossier.

Pour afficher la syntaxe complète de cette commande, à une invite de commandes, tapez dsadd computer /?.

Pour modifier les propriétés d'un compte d'ordinateur, utilisez la commande dsmod computer.

Ajout d'un compte d'ordinateur à un groupe

Tapez la commande suivante :

dsmod group **group_dn** -addmbr **computer_dn**

Cette commande utilise les valeurs suivantes :

- **group_dn** spécifie le nom unique de l'objet du groupe auquel vous souhaitez ajouter l'objet d'ordinateur.
- **computer_dn** spécifie le nom unique de l'objet d'ordinateur à ajouter au groupe. Le nom unique spécifie l'emplacement du dossier.

L'ajout d'un ordinateur à un groupe vous permet d'accorder des autorisations à tous les comptes d'ordinateur de ce groupe, puis de filtrer des paramètres de stratégie de groupe sur tous les comptes de ce groupe.

Pour afficher la syntaxe complète de cette commande, à une invite de commandes, tapez dsmod group /?.

Réinitialisation d'un compte d'ordinateur

Tapez la commande suivante :

dsmod computer **computer_dn** -reset

Cette commande utilise les valeurs suivantes :

- **computer_dn** spécifie les noms uniques d'un ou plusieurs objets d'ordinateur que vous souhaitez réinitialiser.

REMARQUE Lorsque vous réinitialisez un compte d'ordinateur, vous arrêtez la connexion de l'ordinateur au domaine. Vous devez rejoindre le compte d'ordinateur du compte de domaine d'ordinateur après l'avoir réinitialisé.

Pour afficher la syntaxe complète de cette commande, à une invite de commandes, tapez dsmod computer /?.

Désactivation ou activation d'un compte d'ordinateur

Tapez la commande suivante :

dsmod computer **computer_dn** -disabled {yes|no}

Cette commande utilise les valeurs suivantes :

- **computer_dn** spécifie le nom unique de l'objet d'ordinateur que vous souhaitez activer.
- {yes|no} précise si l'ordinateur est désactivé pour se connecter (oui) ou non (non).

Lorsque vous désactivez un compte d'ordinateur, vous arrêtez la connexion de l'ordinateur avec le domaine et l'ordinateur ne peut pas s'authentifier au domaine.

Pour afficher la syntaxe complète de cette commande, à une invite de commandes, tapez dsmod computer /?.

Comment gérer les unités d'organisation

Création d'une nouvelle unité d'organisation

Tapez la commande suivante :

dsadd ou **organizational_unit_dn**

Cette commande utilise les valeurs suivantes :

- **organizational_unit_dn** spécifie le nom unique de l'unité d'organisation à ajouter.

Pour afficher la syntaxe complète de cette commande, à une invite de commandes, tapez dsadd ou /?.

REMARQUE Pour modifier les propriétés d'un compte d'ordinateur, utilisez la commande dsmod ou.

Suppression d'une unité d'organisation

Tapez la commande suivante :

dsrm **organizational_unit_dn**

Cette commande utilise les valeurs suivantes :

- **organizational_unit_dn** spécifie le nom unique de l'unité d'organisation à supprimer.

Pour afficher la syntaxe complète de cette commande, à une invite de commandes, tapez dsrm /?.

REMARQUE Si vous supprimez une unité d'organisation, tous les objets qu'elle contient sont supprimés.

Comment effectuer une recherche dans Active Directory

Comment trouver un compte utilisateur

Tapez la commande suivante :

dsquery user **parameter**

Cette commande utilise les valeurs suivantes :

- **parameter** spécifie le paramètre à utiliser. Pour la liste des paramètres, consultez l'aide en ligne pour la commande dsquery user.

Pour afficher la syntaxe complète de cette commande, à une invite de commandes, tapez dsquery user /?.

Comment chercher un contact

Tapez la commande suivante :

dsquery contact **parameter**

Cette commande utilise les valeurs suivantes :

- **parameter** spécifie le paramètre à utiliser. Pour la liste des paramètres, consultez l'aide en ligne pour la commande dsquery user.

Recherche d'un groupe

Tapez la commande suivante :

dsquery group **parameter**

Cette commande utilise les valeurs suivantes :

- **parameter** spécifie le paramètre à utiliser. Pour la liste des paramètres, consultez l'aide en ligne pour la commande dsquery user.

Nicolas Yang

Recherche d'un compte d'ordinateur

Tapez la commande suivante :

dsquery computer -name **name**

Cette commande utilise les valeurs suivantes :

- **name** spécifie le nom de l'ordinateur que la commande recherche. Cette commande recherche des ordinateurs dont les attributs de nom (valeur de l'attribut CN) correspondent à **name**.

Pour afficher la syntaxe complète de cette commande, à une invite de commandes, tapez dsquery computer /?.

Recherche d'une unité d'organisation

Tapez la commande suivante :

dsquery ou **parameter**

Cette commande utilise les valeurs suivantes :

- **parameter** spécifie le paramètre à utiliser. Pour la liste des paramètres, consultez l'aide en ligne pour dsquery ou.

Pour afficher la syntaxe complète de cette commande, à une invite de commandes, tapez dsquery ou /?.

Recherche d'un contrôleur de domaine

Tapez la commande suivante :

dsquery server **parameter**

Cette commande utilise les valeurs suivantes :

- **parameter** spécifie le paramètre à utiliser. Il existe plusieurs attributs d'un serveur que vous pouvez rechercher en utilisant cette commande. Pour la liste des paramètres, consultez l'aide en ligne pour dsquery server.

Exécution d'une recherche personnalisée

Tapez la commande suivante :

dsquery * **parameter.**