

## Administration sécurisée et efficace d'Active Directory

Présenté par :

➤ Pr. Nordine ZIDANE

Creative Commons



MICROSOFT OFFICIAL COURSE

## Module 2

# Administration sécurisée et efficace d'Active Directory®

Diapositive annexe de la page Commentaires. Ne pas imprimer la diapositive. Voir le volet Commentaires.



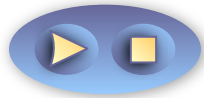
## Vue d'ensemble du module

- Utilisation des composants logiciels enfichables Active Directory
- Consoles personnalisées et privilèges minimum
- Rechercher des objets dans Active Directory
- Utiliser les commandes DS pour administrer Active Directory

# Leçon 1 : Utilisation des composants logiciels enfichables Active Directory

- La console MMC
- Les composants logiciels enfichables Active Directory
- Recherche des composants logiciels enfichables Active Directory
- Démonstration : administration de base avec Utilisateurs et ordinateurs Active Directory

# La console MMC



**Afficher/masquer  
l'arborescence de  
la console**

**Afficher/  
masquer le volet  
Actions**

Utilisateurs et ordinateurs Active Directory

Fichier Action Affichage ?

Utilisateurs et ordinateurs Active Directory

- Requêtes sauvegardées
- contoso.com
  - Admins
  - Builtin
  - Client Computers
  - Computers
  - Disabled Accounts
  - Domain Controllers
  - ForeignSecurityPrincipals
  - Groups
  - Kiosks
  - New Computers
  - New Users
  - Servers
  - User Accounts
    - Contractors
    - Employees**
    - Users

Nom	Type
Nurhan Güran	Utilisateur
Nuria Gonzalez	Utilisateur
Ofer Daliot	Utilisateur
Ole Gotfred	Utilisateur
Oleg Anashkin	Utilisateur
Olinda Turner	Utilisateur
Oliver Kiel	Utilisateur
Oliver Lee	Utilisateur
Oliver Szimmetat	Utilisateur
Olivier Fontana	Utilisateur
Olivier Renaud	Utilisateur
Olya Veselova	Utilisateur
Omri Kiesler	Utilisateur
Osama Shabaneh	Utilisateur
Ovidiu Burlacu	Utilisateur
Pablo Rovira Diez	Utilisateur
Palle Petersen	Utilisateur
Parry Bedi	Utilisateur
Parul Manek	Utilisateur
<b>Pat Coleman</b>	Utilisateur
Patricia Doyle	Utilisateur
Patrick M. Cook	Utilisateur
Patrick Sands	Utilisateur
Patrick Shortt	Utilisateur
Paul Koch	Utilisateur
Paul Shakespear	Utilisateur

**Actions**

- Employees**
  - Autres actions
- Pat Coleman**
  - Autres actions

**Arborescence  
de la console**

**Volet  
d'informations**

**Volet Actions**

# Composants logiciels enfichables Active Directory

- Utilisateurs et ordinateurs Active Directory
  - Gérer au quotidien les objets les plus courants, dont les utilisateurs, les groupes, les ordinateurs, les imprimantes et les dossiers partagés
- Sites et services Active Directory
  - Gérer la réplication, la topologie du réseau et les services associés
- Domaines et approbations Active Directory
  - Configurer et gérer les relations d'approbation et le niveau fonctionnel du domaine et de la forêt
- Schéma Active Directory
  - Administrer le schéma



# Recherche des composants logiciels enfichables

## Active Directory

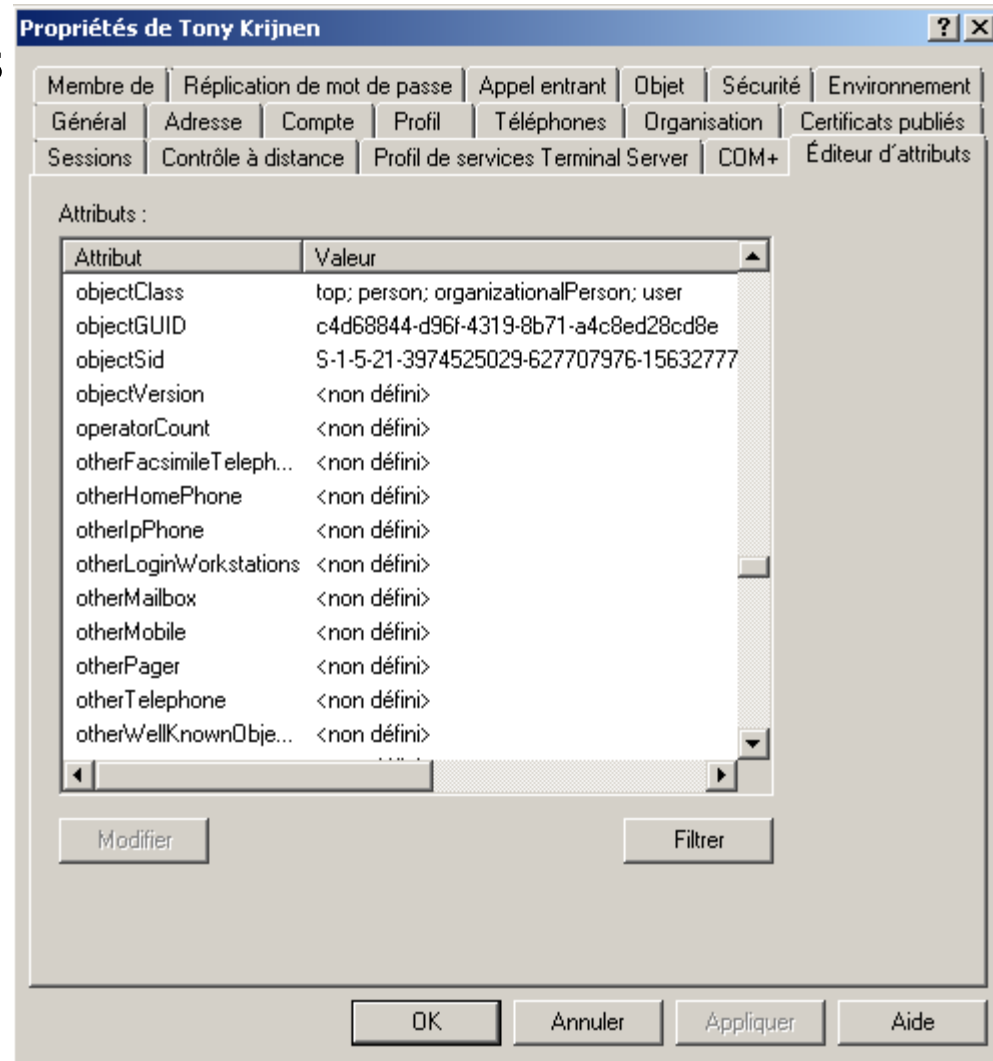
- Les composants logiciels enfichables Active Directory sont installés dans un contrôleur de domaine.
  - Gestionnaire de serveur : Utilisateurs et ordinateurs, Sites et services
  - Dossier des outils d'administration
- Installer les Outils d'administration de serveur distant sur un serveur ou un client membre
  - Windows Server® 2022
    - Gestionnaire de serveur → Fonctionnalités → Ajout de fonctionnalités → Outils d'administration de serveur distant
  - Windows Vista® SP1, Windows 7
    - Télécharger les Outils d'administration de serveur distant à l'adresse [www.microsoft.com/downloads](http://www.microsoft.com/downloads)
    - Double-cliquer sur le fichier, puis suivre les instructions de l'Assistant Installation.
    - Panneau de configuration → Programmes et fonctionnalités → Activer ou désactiver des fonctionnalités Windows → Outils d'administration de serveur distant



# Démonstration : Administration de base avec Utilisateurs et ordinateurs Active Directory

Cette démonstration explique :

- Comment afficher des objets dans Utilisateurs et ordinateurs Active Directory
- Comment actualiser la vue
- Comment créer des objets
- Comment configurer les attributs d'un objet
- Comment afficher tous les attributs d'un objet



Diapositive annexe de la page Commentaires. Ne pas imprimer la diapositive. Voir le volet Commentaires.



## Leçon 2 : Consoles personnalisées et privilèges minimum

- Démonstration : création d'une console MMC personnalisée pour administrer Active Directory
- Administration sécurisée avec des privilèges minimum, Exécuter en tant qu'administrateur et Contrôle de compte d'utilisateur
- Démonstration : administration sécurisée avec Contrôle de compte d'utilisateur et Exécuter en tant qu'administrateur
- Démonstration : « super consoles »

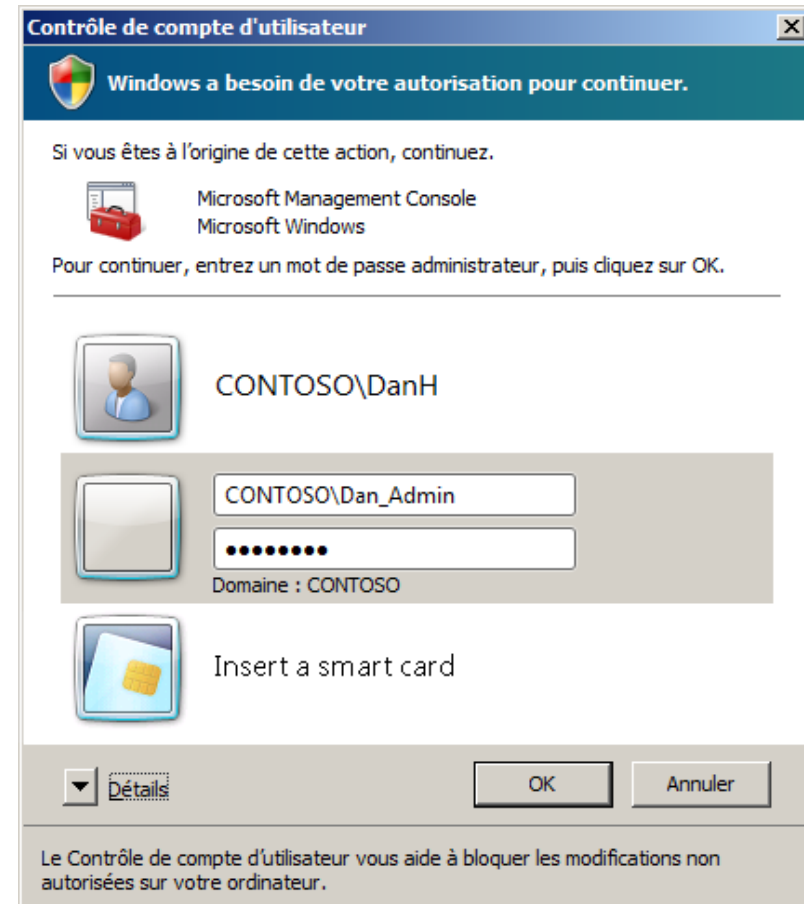
# Démonstration : création d'une console MMC personnalisée pour administrer Active Directory

Cette démonstration explique :

- Comment créer une console MMC personnalisée avec plusieurs composants logiciels enfichables
- Comment enregistrer le composant logiciel enfichable Schéma Active Directory
- Où enregistrer une console personnalisée

# Administration sécurisée avec des privilèges minimum, Exécuter en tant qu'administrateur et Contrôle de compte d'utilisateur

- Conserver au moins deux comptes
  - Un compte d'utilisateur standard
  - Un compte avec des privilèges d'administration
- Ouvrir une session sur votre ordinateur en tant qu'utilisateur standard
  - Ne pas ouvrir une session sur votre ordinateur avec des informations d'identification d'administrateur
- Lancer des consoles d'administration avec Exécuter en tant qu'administrateur
  1. Cliquer du bouton droit sur la console et sélectionner **Exécuter en tant qu'administrateur**
  2. Cliquer sur **Utiliser un autre compte**
  3. Entrer le nom d'utilisateur et le mot de passe de votre compte d'administrateur



# Démonstration : administration sécurisée avec Contrôle de compte d'utilisateur et Exécuter en tant qu'administrateur

Cette démonstration explique :

- Comment exécuter une console d'administration personnalisée en tant qu'administrateur
- Pourquoi il est important d'enregistrer une console personnalisée dans un emplacement partagé

# Démonstration : « super consoles »

Cette démonstration explique :

- Comment ajouter la vue d'un partage de fichiers à une console personnalisée
  - La vue se sert des informations d'identification (élevées) utilisées pour lancer la console.
- Comment créer une « zone de lancement » d'administration
  - Ouvrir des outils externes avec les informations d'identification (élevées) de la console



Diapositive annexe de la page Commentaires. Ne pas imprimer la diapositive. Voir le volet Commentaires.



# Atelier pratique A : Création et exécution d'une console d'administration personnalisée

- Exercice 1 : exécuter des tâches d'administration de base en utilisant le composant logiciel enfichable Utilisateurs et ordinateurs Active Directory
- Exercice 2 : créer une console d'administration Active Directory personnalisée
- Exercice 3 : exécuter des tâches d'administration avec des privilèges minimum et utiliser Exécuter en tant qu'administrateur et Contrôle de compte d'utilisateur
- Exercice 4 (facultatif avancé) : personnalisation avancée de la console MMC et administration à distance

## Informations de connexion

Ordinateur virtuel	6238B-HQDC01-A
Nom d'ouverture de session utilisateur	Pat.Coleman
Nom d'utilisateur administrateur	Pat.Coleman Admin
Mot de passe	Pa\$\$w0rd

**Durée approximative : 20 minutes**

Diapositive annexe de la page Commentaires. Ne pas imprimer la diapositive. Voir le volet Commentaires.



# Scénario de l'atelier pratique

- Dans cet exercice, vous vous appelez Pat Coleman et êtes administrateur chez Contoso, Ltd. Vous êtes responsable de diverses tâches de support Active Directory et vous ouvrez constamment plusieurs consoles depuis le dossier Outils d'administration dans le Panneau de configuration. Vous avez décidé de créer une seule console qui contient tous les composants logiciels enfichables dont vous avez besoin. En outre, la stratégie de sécurité informatique de Contoso change et vous ne pouvez plus ouvrir une session sur un système avec les informations d'identification disposant des privilèges d'administration, sauf en cas d'urgence. Vous devez désormais ouvrir une session avec des informations d'identification sans privilèges.

# Récapitulatif

- Quel composant logiciel enfichable êtes-vous le plus susceptible d'utiliser tous les jours pour administrer Active Directory ?
- Lorsque vous créez une console MMC personnalisée dans votre entreprise, quels composants logiciels enfichables ajoutez-vous ?

## Leçon 3 : Recherche d'objets dans Active Directory

- Recherche d'objets dans Active Directory
- Démonstration : utilisation de la boîte de dialogue Sélectionner des utilisateurs, des contacts, des ordinateurs ou des groupes
- Options de recherche d'objets dans Utilisateurs et ordinateurs Active Directory
- Démonstration : contrôler l'affichage des objets dans Utilisateurs et ordinateurs Active Directory
- Démonstration : utiliser la commande Rechercher
- Déterminer l'emplacement d'un objet
- Démonstration : utiliser des requêtes enregistrées

# Recherche d'objets dans Active Directory

- Lorsque vous affectez des autorisations à un dossier ou un fichier
  - Sélectionnez le groupe ou l'utilisateur auquel les autorisations sont affectées.
- Lorsque vous ajoutez des membres à un groupe
  - Sélectionnez l'utilisateur ou le groupe qui sera ajouté en tant que membre.
- Lorsque vous configurez un attribut lié tel que Géré par
  - Sélectionnez l'utilisateur ou le groupe qui sera affiché dans l'onglet Géré par.
- Lorsque vous devez administrer un utilisateur, un groupe ou un ordinateur
  - Effectuez une recherche pour trouver l'objet dans Active Directory, au lieu de le rechercher manuellement.



# Démonstration : utilisation de la boîte de dialogue Sélectionner des utilisateurs, des contacts, des ordinateurs ou des groupes

Cette démonstration explique :

- Comment sélectionner des utilisateurs avec la boîte de dialogue Sélectionner

# Options de recherche d'objets dans Utilisateurs et ordinateurs Active Directory

- **Tri :** utiliser les en-têtes de colonne dans Utilisateurs et ordinateurs Active Directory pour localiser des objets dans une colonne



- **Recherche :** fournir vos critères de recherche



# Démonstration : contrôler l'affichage des objets dans Utilisateurs et ordinateurs Active Directory

Cette démonstration explique :

- Comment ajouter ou supprimer des colonnes dans le volet d'informations
- Comment trier des objets dans des colonnes dans le volet d'informations

# Démonstration : utiliser la commande Rechercher

Cette démonstration explique :

- Comment rechercher des objets dans Active Directory à l'aide de la commande Rechercher

# Détermination de l'emplacement d'un objet

1. Vérifiez que l'option **Fonctionnalités avancées** est sélectionnée dans le menu **Affichage** de la console MMC.
2. Recherchez l'objet.
3. Ouvrez sa boîte de dialogue **Propriétés**.
4. Ouvrez l'onglet **Objet**.
5. Affichez le **Nom canonique de l'objet**

*ou*

- Dans la boîte de dialogue Rechercher, **Affichage** → **Choisir les colonnes** et ajoutez la colonne **Publié à**.

# Démonstration : utiliser des requêtes enregistrées

Cette démonstration explique :

- Comment créer une requête sauvegardée
- Comment distribuer une requête sauvegardée
- Pourquoi les requêtes sauvegardées constituent un outil efficace pour l'administration

Diapositive annexe de la page Commentaires. Ne pas imprimer la diapositive. Voir le volet Commentaires.





# Atelier pratique B : Recherche d'objets dans Active Directory

- Exercice 1 : Rechercher des objets dans Active Directory
- Exercice 2 : Utiliser des requêtes enregistrées
- Exercice 3 (facultatif avancé) : Explorer des requêtes enregistrées

## Informations de connexion

Ordinateur virtuel	6238B-HQDC01-A
Nom d'ouverture de session utilisateur	Pat.Coleman
Nom d'utilisateur administrateur	Pat.Coleman Admin
Mot de passe	Pa\$\$w0rd

**Durée approximative : 20 minutes**

# Scénario de l'atelier pratique

- Contoso couvre maintenant cinq sites géographiques dans le monde et compte plus de 1 000 employés. Maintenant que le domaine contient un grand nombre d'objets, il est plus difficile de rechercher des objets en le parcourant. On vous demande de définir des pratiques recommandées pour rechercher des objets dans Active Directory pour le reste de l'équipe d'administrateurs. Il vous est également demandé de contrôler l'intégrité de certains types de comptes.

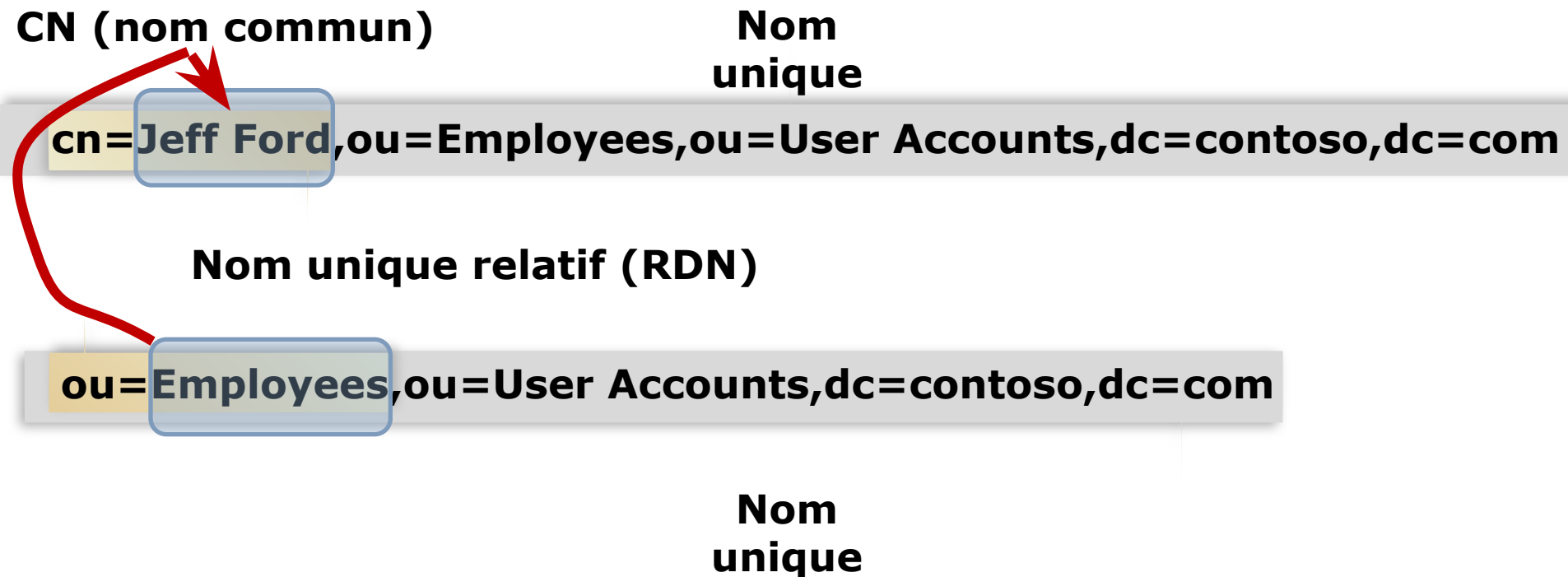
# Récapitulatif

- Dans le cadre de votre travail, quand êtes-vous amené à effectuer des recherches dans Active Directory ?
- Quels types de requêtes enregistrées pouvez-vous créer pour exécuter les tâches d'administration plus efficacement ?

## Leçon 4 : Utilisation des commandes DS pour administrer Active Directory

- Noms uniques, Noms uniques relatifs (RDN) et Noms communs
- Les commandes DS
- Recherche d'objets avec DSQuery
- Extraction des attributs des objets avec DSGet
- Envoi de noms uniques à d'autres commandes DS
- Modification des attributs des objets avec DSMod
- Suppression d'un objet avec DSRm
- Transfert d'un objet avec DSMove
- Ajout d'un objet avec DSAdd
- Administration sans l'interface utilisateur graphique

# Noms uniques, Noms uniques relatifs (RDN) et Noms communs



- Il ne doit pas y avoir deux noms uniques
- Le RDN doit donc être unique au sein du conteneur parent

# Commandes DS

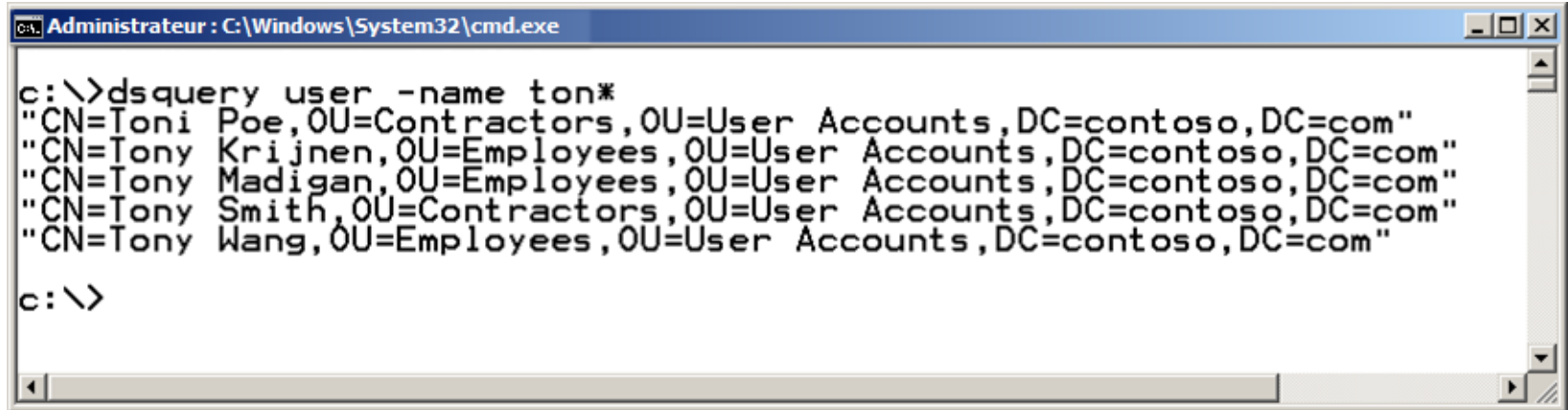
- **DSQuery.** Exécute une requête en fonction des paramètres définis sur la ligne de commande et renvoie la liste des objets correspondants.
- **DSGet.** Renvoie les attributs définis d'un objet.
- **DSMod.** Modifie les attributs définis d'un objet.
- **DSMove.** Transfère un objet vers un nouveau conteneur ou une nouvelle UO.
- **DSAdd.** Crée un objet dans l'annuaire.
- **DSRm.** Supprime un objet ou tous les objets dans l'arborescence sous un objet conteneur ou les deux.
- **DScommand /?**  
Exemple : dsquery /?

# Recherche d'objets avec DSQuery

- `dsquery objectType`
  - *objectType* : utilisateur, ordinateur, groupe, unité d'organisation
  - Par défaut, l'étendue de la recherche est l'ensemble du domaine.
  - **-limit** commutateur pour spécifier le nombre de résultats
    - 100 est la valeur par défaut
    - 0 signifie « renvoyer tous les résultats »
- `dsquery objectType -attribut "critères"`
  - *attribut* est spécifique à *objectType* : **dsquery objectType /?**
  - Exemples pour utilisateur : -name, -samid, -office, -desc
  - *critères* entre guillemets s'il y a un espace. Les caractères génériques (\*) sont autorisés.
- `dsquery objectType BaseDN`  
`-scope {subtree|onelevel|base}`
  - Spécifier le début et l'étendue de la recherche



# Recherche d'objets avec DSQuery



```
Administrateur : C:\Windows\System32\cmd.exe
c:\>dsquery user -name ton*
"CN=Toni Poe,OU=Contractors,OU=User Accounts,DC=contoso,DC=com"
"CN=Tony Krijnen,OU=Employees,OU=User Accounts,DC=contoso,DC=com"
"CN=Tony Madigan,OU=Employees,OU=User Accounts,DC=contoso,DC=com"
"CN=Tony Smith,OU=Contractors,OU=User Accounts,DC=contoso,DC=com"
"CN=Tony Wang,OU=Employees,OU=User Accounts,DC=contoso,DC=com"
c:\>
```

# Extraction des attributs des objets avec DSGet

- **`dsget objectType objectDN -attribut`**
  - **Syntaxe courante pour de nombreuses commandes DS**
- **`dsget user "cn=Jeff Ford,ou=Employees,ou=User Accounts,dc=contoso,dc=com" -email`**
- Quelle différence existe-t-il entre DSGet et DSQuery ?

# Envoi des noms DN à d'autres commandes DS

- Il est difficile de saisir des noms DN !
  - `dsget user "cn=Jeff Ford,ou=Employees,ou=User Accounts,dc=contoso,dc=com" -email`
- DSQuery revoie des noms DN
  - **`dsquery user -name "Jeff Ford"`**  
> `"cn=Jeff Ford,ou=Employees,ou=User Accounts,dc=contoso,dc=com"`
- Envoyer les noms DN de la commande DSQuery à la commande DSGet avec |
  - **`dsquery user -name "Jeff Ford" | dsget user -email`**
  - Ou plusieurs résultats :  
**`dsquery user -name "Dan*" | dsget user -email`**
- DSGet peut renvoyer des noms DN à partir de certains attributs également.
  - **`dsget group groupDN -members | dsget user -samid`**

# Modification des attributs des objets avec DSMod

- `dsmod objectType "objectDN" -attribut "nouvelle valeur"`
- `dsmod user "cn=Jeff Ford,ou=Employees,ou=User Accounts,dc=contoso,dc=com" -dept "Information Technology"`
- `dsquery user "ou=Admins,dc=contoso,dc=com" | dsmod user -department "Information Technology"`

# Suppression d'un objet avec DSRm

- `dsrm objectDN`
  - Notez que DSRm n'a pas besoin de *objectType*
- `dsrm "cn=DESKTOP234,ou=Client Computers,dc=contoso,dc=com"`
- `dsquery computer -stalepwd 90 | dsrm`

# Transfert d'un objet ave DSMove

- **dsmove *objectDN* –newparent *targetOUDN***
  - *objectDN* : objet à déplacer
  - *targetOUDN* : unité d'organisation cible (destination)
- **dsmove *objectDN* –newname *nouveauNom***
  - *objectDN* : objet à déplacer
  - *nouveauNom* : nouveau nom de l'objet (utilisé dans le RDN)

# Ajout d'un objet avec DSAdd

- `dsadd objectType objectDN -attribut "valeur"`
  - *objectType* : classe d'objet à ajouter
  - *objectDN* : unité d'organisation dans laquelle créer l'objet
  - *-attribut "valeur"* : attributs à renseigner
    - Chaque classe d'objet requiert des attributs.
- `dsadd ou "ou=Lab,dc=contoso,dc=com"`

# Administration sans l'interface graphique utilisateur

- Invite de commandes
  - Commandes DS
  - csvde.exe et ldifde.exe
- LDAP
  - ldp.exe
- Windows PowerShell
- Scripts
  - Scripts Windows PowerShell
  - VBScript



# Atelier pratique C : Utilisation des commandes DS pour administrer Active Directory

- Exercice 1 : Utilisation des commandes DS pour administrer Active Directory

## Informations de connexion

Ordinateur virtuel	6238B-HQDC01-A
Nom d'ouverture de session utilisateur	Pat.Coleman
Nom d'utilisateur administrateur	Pat.Coleman Admin
Mot de passe	Pa\$\$w0rd

**Durée approximative : 15 minutes**

# Scénario de l'atelier pratique

- La société Contoso se développe et il est nécessaire de modifier des objets dans Active Directory. Vous êtes administrateur d'AD DS et vous savez que vous pouvez simplifier la création, la suppression et la modification des objets en utilisant l'invite de commande plutôt que Utilisateurs et ordinateurs Directory.

# Récapitulatif

- Que pouvez-vous faire pour ne pas avoir à taper les noms uniques des utilisateurs, des groupes et des ordinateurs dans DSGet et les autres commandes de DS ?
- Quelle est la différence entre des recherches exécutées avec DSQuery en utilisant des caractères génériques et des recherches effectuées avec la commande Rechercher dans Utilisateurs et ordinateurs Active Directory ? En d'autres termes, quel type de recherche avez-vous exécuté dans cet atelier que vous n'auriez pas pu effectué en utilisant l'interface de base de la commande Rechercher ?