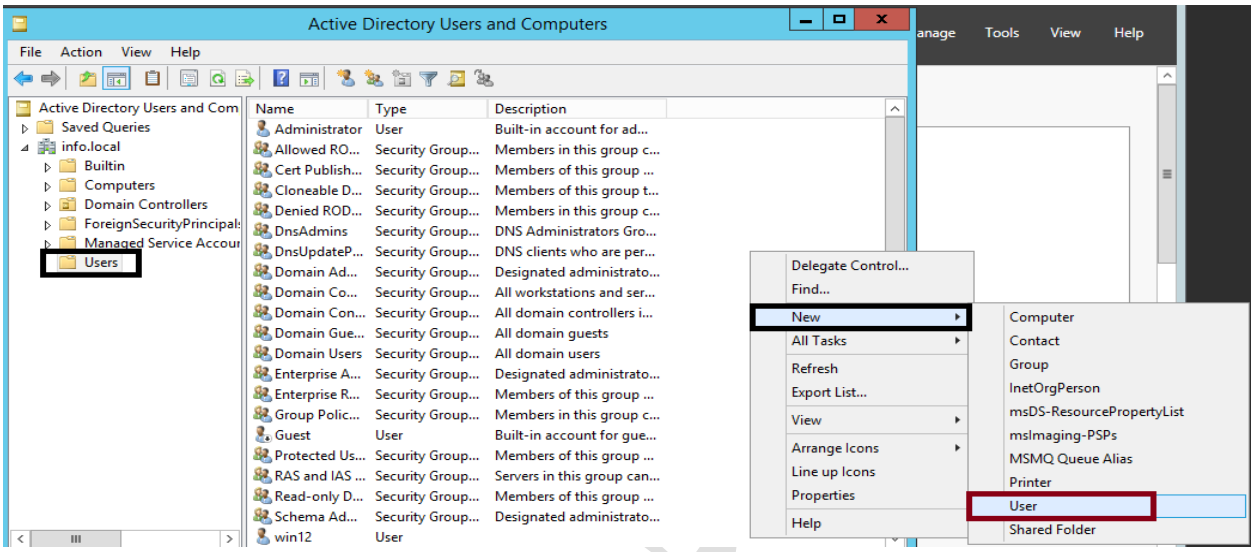
# بدء التعامل مع بيئة ال Active Directory (Domain Controller)

- كما علمنا أن محتويات ملف ال **SAM** الذي يحتوي على حسابات المستخدمين (**Accounts**) المخزنة بشكل محلي على النظام , سيتم تخزينها في قاعدة البيانات الخاصة بال **Active Directory** (**NTDS**).
- وبالتالي لإدارة ال ( **Users And Computers**) على مستوى ال **Domain** , يتم من خلال الأداة (**Active Directory Users And computers**) , وأي تعديل عليها , يتم التعديل على قاعدة البيانات (**NTDS**), الموجودة في المسار التالي (القرص **C** <<<< **Windows** <<<< **NTDS Folder** <<<< نجلد ملف بإسم (**NTDS.dit**) يحتوي على قاعدة البيانات الخاصة بال **Active Directory**.
- ندخل الى **Active Directory Users And Computers** , نجد إسم ال **Domain** الذي تم إنشائه , سنجد أسفل إسم ال **Domain** وضمنه مجموعة من الحاويات (**Containers**) , منها ال **Users** الذي يحتوي على جميع ال **users** التي تم إنشائها , بالإضافة الى جميع ال **Users** التي كانت موجودة في ملف ال **SAM** , بالإضافة الى جميع ال **Groups** الموجودة.

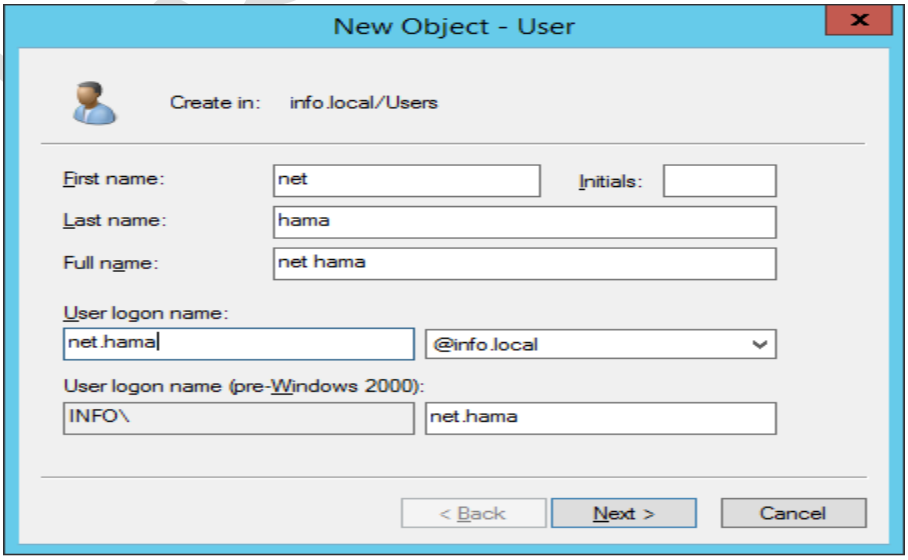
## لإنشاء حساب جديد :

- ننتقل الى ال **Users** <<<< ننقر الزر اليميني بالماوس <<<< **new** <<<<< **User** <<<

تظهر نافذة إنشاء **user** كما يلي :

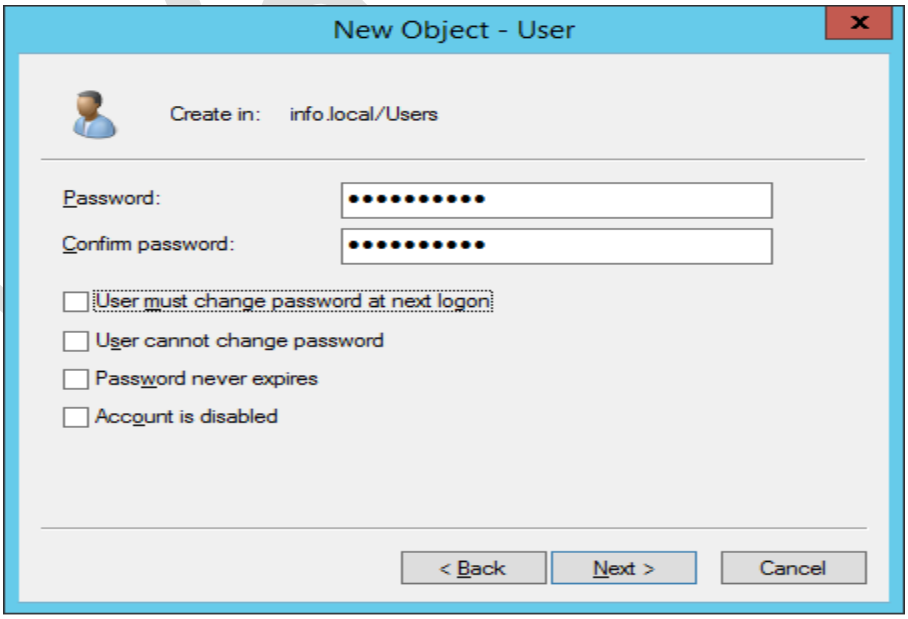



في هذه النافذة يتم تحديد كلا من المعلومات التالية , حيث أن ال **User logon Name** هو الأسم الذي يتم تسجيل الدخول به الى المستخدم على جهاز ال **client**, وال **User logon name (pre-Windows 2000)** وهو الاسم الذي يتم تسجيل الدخول فيه عندما يكون نظام تشغيل ال **Client** (**Windows 2000**) وما قبل وهو عبارة عن (**Netbios Domain name /User logon name**).

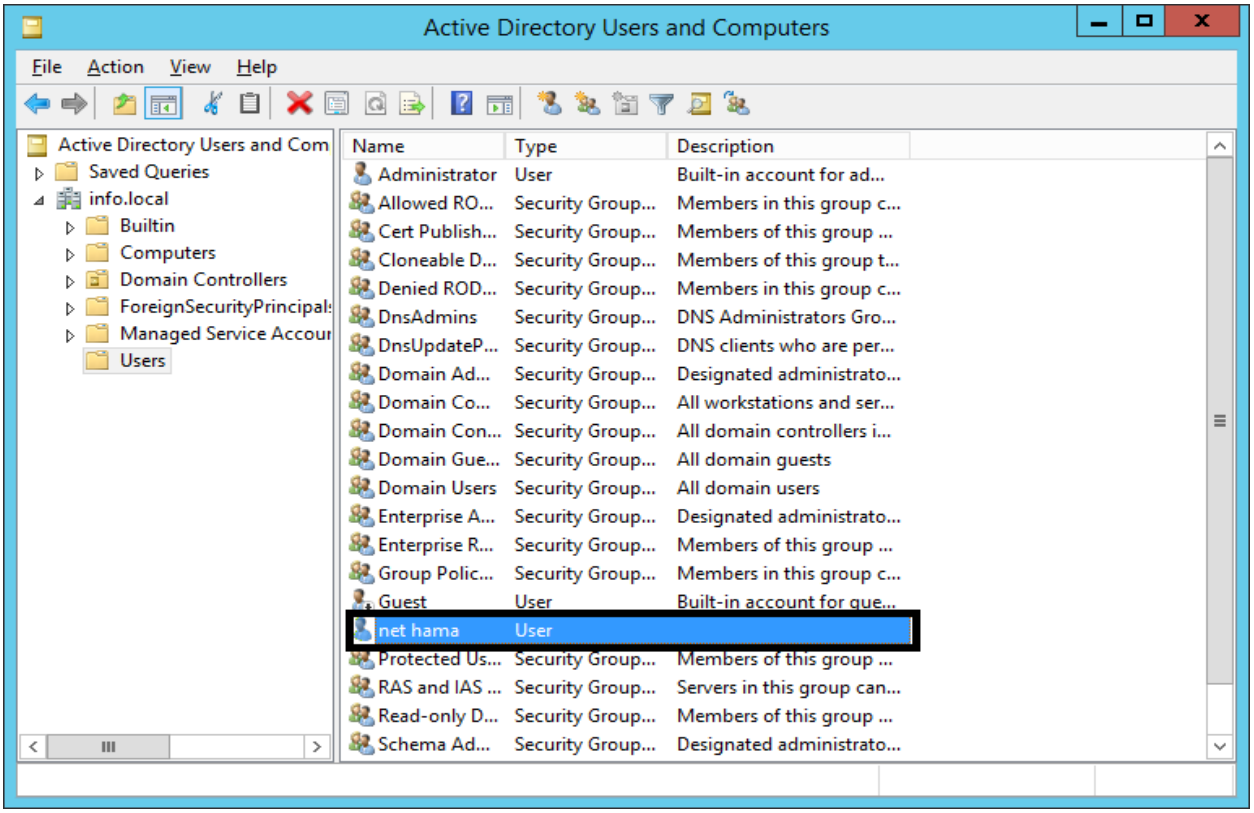


- في النافذة التالية يتم إسناد **password** لإسم المستخدم ويجب أن تكون معقدة حسب السياسات الأمنية المطبقة بشكل إفتراضي على ال **Domain**, أيضا يمكننا تحديد أربع من الخيارات لهذا المستخدم :

- ✓ **user must change password at next logon**: في حال تحديد هذا الخيار يجب على المستخدم تغيير ال **password** بعد تسجيل الدخول لأول مرة على هذا الحساب .
- ✓ **user cannot change password**: حيث من الممكن للمستخدم أن يقوم بتغيير كلمة المرور الخاصة به, في حال تحديد هذا الخيار المستخدم لا يمكنه أبدا تغيير كلمة المرور الخاصة به.
- ✓ **Password never expires** :حيث أن حساب المستخدم بشكل افتراضي له مدة صلاحية بعد إنتهائها يتم تعطيل الحساب ويجب على ال **Admin** أن يقوم بتفعيله من جديد, في حال تحديد هذا الخيار المستخدم لا تنتهي صلاحية حسابه أبدا.
- ✓ **Account Is Disabled**: تعطيل الحساب الى أن يقوم ال**Admin** بتفعيل هذا الحساب.



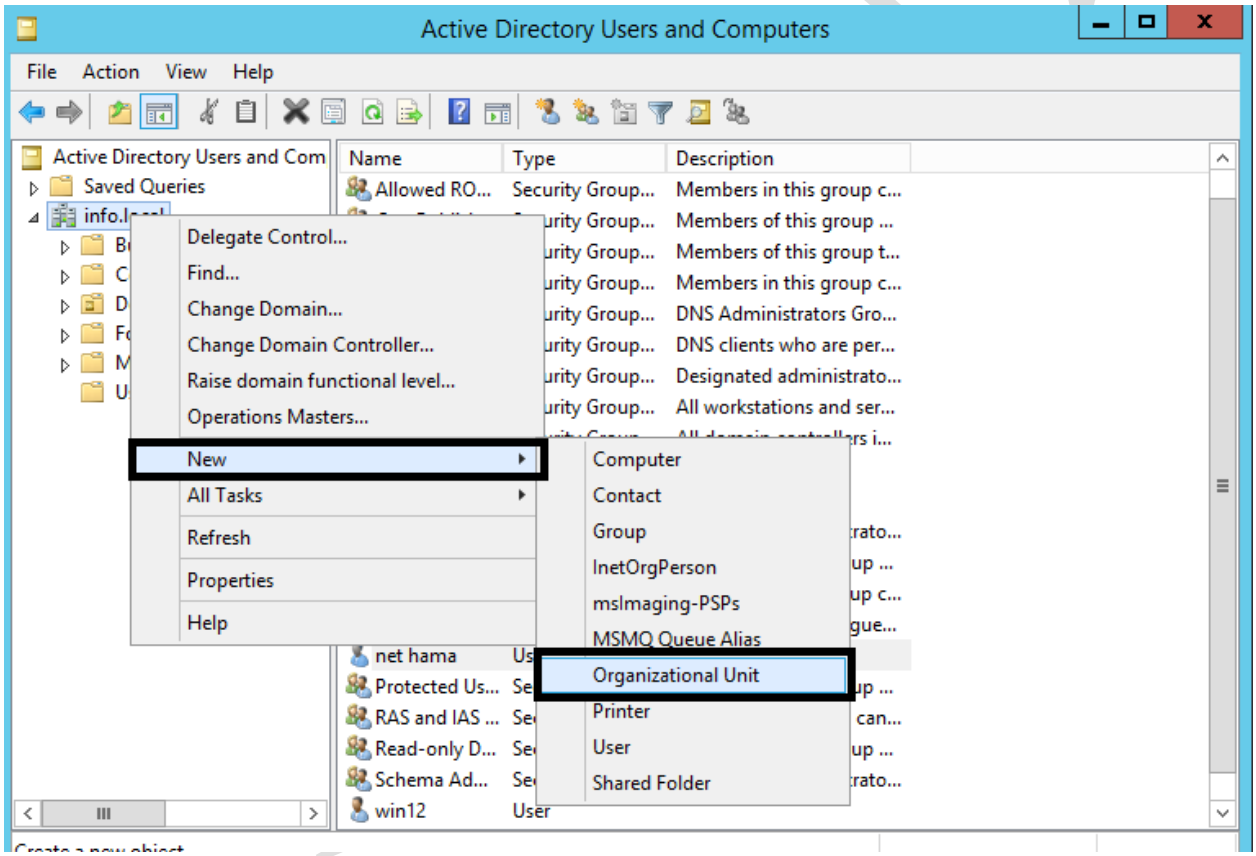
➢ **بعد الانتهاء من إنشائه يظهر كما يلي :**



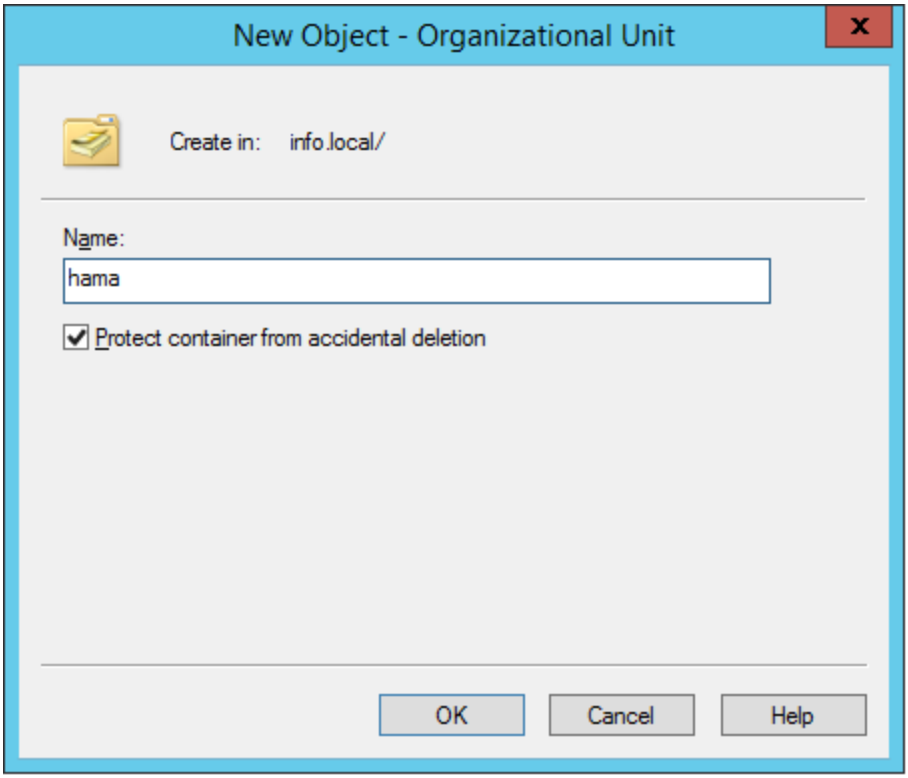
- في حال تم إنشاء الكثير من حسابات المستخدمين , وبالتالي ستظهر بشكل غير منظم ويصعب البحث عنها , لهذا السبب سنقوم بإنشاء وحدات تنظيمية (**organization Units**), لنقوم بتنظيم ال **user** ضمنها .

➢ نقوم بإنشائها كما يلي:

✓ يتم إنشاء ال **OU** على مستوى ال **Domain** , ننقر يميني على إسم ال **Domain** <<<< **new** >>>> **organization unit** <<< لتظهر نافذة نحدد إسم هذه ال **Ou** :



- ✓ في النافذة التالية في حال تم تحديد الخيار ( **Protect Container from accidental deletion**) , فإن هذه ال **ou** لا يمكننا حذفها أبدا .



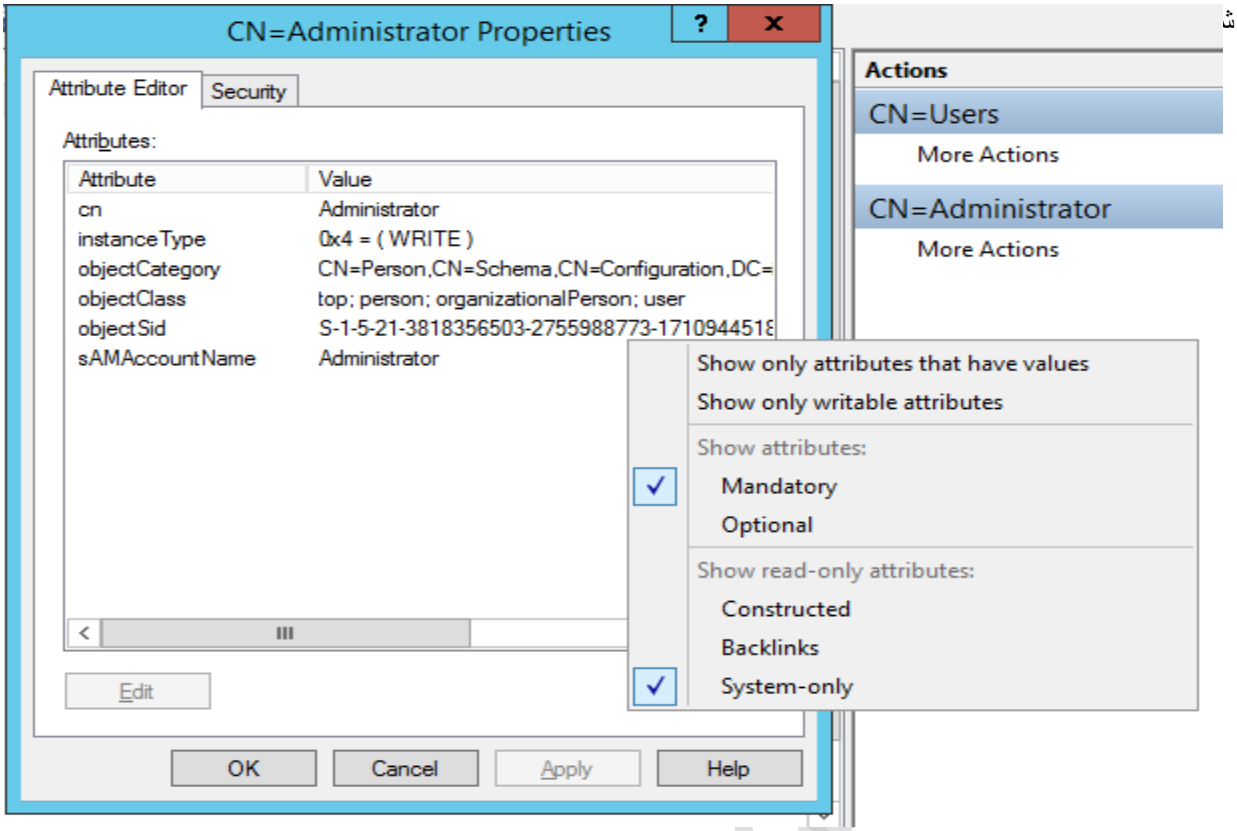

- ✓ لنأخذ مثال يوضح إستخدام ال **OU** : لنفرض لدينا شركة في أكثر من موقع, وبالتالي نقوم بإنشاء **ou** خاص بكل موقع , وأيضا في كل موقع هناك مجموعة من الأقسام , وبالتالي نقوم بإنشاء **ou** خاصة بكل قسم ضمن هذا الموقع , حيث يمكننا إنشاء **ou** ضمن **ou** أخرى, وبالتالي نحصل على نظام هرمي منظم.

- ➢ يمكننا ضمن ال **ou** مباشرة أنشاء حساب مستخدم , أو يمكننا نقل **user** من أي موقع ال **ou** معينة وذلك بالسحب والإفلات , أو ( **Cut**) و **Copy** للحساب.
- ➢ لحذف **Ou** معينة , يميني على هذه ال **Ou** <<<< **delete**.

- **في حال كانت هذه ال ou محمية من الحذف , لإزالة هذه الحماية , ننتقل الى قائمة View <<<< Advanced features <<<< ثم يميني على إسم ال ou >>>> properties <<<< ثم Tap >>>> object <<<< ونزيل ال Check عن الخيار ( Protect object from accidental deletion) >>> Apply <<<< OK.**
- **يتم تميز ال ou عن غيره من ال containers أن ال ou يكون عليها علامة صفراء, وأيضا تسمح ال OU بأن نقوم بتطبيق policies سياسات أمنية على مستوى ال OU, لا يمكن تطبيقها على مستوى ال Containers الأخرى.**

- **Security Identifier (SID): جميع الموارد التي يتم إضافتها من نوع ( Security Principals) مثل (User, Computer, Group), يكون لكل منها (SID) فريد على مستوى ال forest بشكل كامل.**

- **يتم معرفة ال SID الخاصة ب User معين بعدة طرق منها >>>> ننتقل ال server manager >>>> Tools >>>> ADSI Edi >>>>> يميني على ADSI Edit >>>>> connect to >>>> للاتصال مع الجهاز الحالي نقبل الاعدادات الافتراضية >>>>> OK< >>>> يظهر ال Domain >>>> ننتقل الى موقع ال User >>>>> يميني على ال User >>>>> properities >>>>> filter >>>> نظهر الخيارات الأساسية فقط (Mandatory), فإنه يظهر ال SID لهذا ال User.**




- ملاحظة : ال **SID** للمستخدم ال **Administrator** تنتهي بالرقم (**500**) وبالتالي حتى لو تم تغيير ال (**logon name**) له, سيبقى ال **SID** ذاته وبالتالي يشكل هذا نقطة ضعف , وبالتالي ينصح بأن يتم إنشاء **User** جديد له كامل صلاحيات ال **Administrator**, ومن ثم تعطيل حساب ال **Adminisrator** , يتم ذلك<<<< يميني على حساب ال **Administrator** <<<< **copy** <<< نقوم بإنشائه <<<< أخيرا نقوم بتعطيل حساب ال **Administrator**.

- **جعل حاسب أو مكنة عضو في ال Domain:**

1. **نقوم بإعداد ال IP لهذه المكنة من الشبكة ذاتها لل DC.**
2. **نضع ال DNS Server هو عنوان ال Domain Controller الذي تم تثبيت خدمة ال DNS Server عليه, وذلك لأن الجهاز سيم ضمه الى ال domain من خلال الاسم.**
3. **بعد ذلك نبدأ بضم الجهاز الى ال Domain <<<< يمني على جهاز ال computer <<<< change setting <<< change <<<< نضع الخيار على Domain ونكتب إسم ال Domain , مثلا (INFO.local) , يطلب إدخال ( User Account) عبارة عن Username و Password لمستخدم تم إنشائه على ال Domain , نقوم بإدخالها, في حال النجاح يطلب إعادة إقلاع الجهاز.**

- **بعد إعادة الإقلاع أصبح بإمكاننا تسجيل الدخول الى هذا الجهاز إما Locally بإستخدام الحسابات التي كانت موجودة مسبقا كما يلي (Computer name / Username) و أو بإستخدام حساب مستخدم على ال domain كما يلي ( Domain name /logon name) و أيضا يمكننا تسجيل الدخول الى ال Domain بإسم المستخدم فقط ( logon name).**
- **بعد ضم الجهاز الى ال Domain وتسجيل الدخول , ننتقل ال Domain controller <<<<< server manager <<<< DNS <<<<< نلاحظ أن تم إضافة سجل جديد خاص بال client, وبالتالي أصبح بإمكاننا الوصول اليه بإستخدام اسم الحاسب .**

- **أي Computer يصبح عضو من ال Domain, فإنه بشكل إفتراضي يتم إنشاء Computer Account له , ويوضع في ال Container بإسم computers, ونصل اليه من >>>> Server manager <<<< Active Directory Users And Computers >>>>> computers, حيث يمننا نقله إلى موقع أخر مثلا ال OU معينة , وذلك عند الحاجة لتطبيق Policies عليه مثلا.**
- **ملاحظة : ال Computer Account يمكن الدخول عليه بأكثر من User Account.**

**لإخراج جهاز ما من ال Domain وإرجاعه الى شبكة ال Workgroup أو حتى لتغيير إسمه :**

- **يميني على جهاز الكمبيوتر >>>> خصائص (Properties) >>>> تغير الإعدادات (Change settings)>>>>> في حال كان المستخدم عادي , لن يتمكن من إخراج الجهاز من ال domain, عندها سيطلب حساب ال Adminstator, نقوم بإدخال حساب (local administrator) أو حساب ال (domain Adminstrator) >>>>> تقتح نافذة نختار (Change)>>>> نختار workgroup ونحدد إسمها مثلا (WORKGROUP), سيطلب إعادة إقلاع الجهاز.**