Active Directory

تعريف :

قاعدة بيانات مركزية داخل Domain Controller تحتوي على:

1. المستخدمين Users
2. الأجهزة Computers
3. المجموعات Groups
4. الوحدات التنظيمية(Organizational Units (OU
5. الصلاحيات والسياسات

" الـ Active Directory هو النظام المسؤول عن إدارة الشبكة بالكامل.."

هيكلية الدومين داخل Active Directory :

تعريف الدومين Domain

هو نطاق أو اسم خاص بالشركة او المؤسسة ويُكتب بصيغة **FQDN**، يمكن أن يكون اسما داخليا مثل: Alhwash.local أو اسما عاما مثل: Google.com

يسمح بربط الأجهزة والمستخدمين ضمن بيئة عمل موحدة وإدارتهم مركزياً

الشجرة (Tree)

- كل Domain مرتبط مع دومينات أخرى من خلال بنية هرمية تسمى **Tree**.
- أي دومين جديد ينضم إلى دومين أكبر يُعتبر جزءا من الشجرة.

Forest

- إذا كان لدينا أكثر من Tree داخل شبكة واحدة، فإن جميعها تكون ما يُسمى Forest
- كل Forest يمكن أن تضم أكثر من Tree ، وكل Tree يمكن أن تضم أكثر من Domain

Child Domain

هو دومين فرعي تابع لدومين رئيسي.

مثال : domain.com child.domain.com

العلاقة بين Domain – Tree – Forest

Domain

- وحدة أساسية داخل Active Directory
- يحتوي مستخدمين، أجهزة، مجموعات، وسياسات.

Tree

- مجموعة من الدومينات المرتبطة بهيكل تسلسلي واحد.

Forest

- تضم أكثر من Tree
- أعلى مستوى تنظيمي داخل Active Directory

أنواع Domain Controller :

1. Read-Only Domain Controller (RODC)

- نسخة من الـ Domain Controller مخصصة للقراءة فقط (Read Only)
- لا تسمح بالتعديل على بيانات Active Directory
- تُستخدم عادةً في الفروع البعيدة أو الأماكن ذات الأمان الأقل التي لا نريد تخزين كامل قاعدة البيانات فيها.
- تستطيع تخزين نسخة من المستخدمين، ولكن حفظ كلمات المرور يكون محدودًا لزيادة الأمان.

2. Additional Domain Controller (ADC)

- Domain Controller إضافي يعمل كنسخة احتياطية من الـ Primary DC
- يحتوي نفس قاعدة البيانات الخاصة بالدومين.
- يتم تحديث بياناته من خلال عملية Replication بينه وبين الـ Primary DC
- يتم استخدامه لضمان استمرارية العمل في حال سقوط الـ DC الرئيسي ولموازنة تحميل تسجيل الدخول (بدلا من تسجيل الدخول من مكان واحد يتم استخدامه لتخفيف الضغط عن ال DC الرئيسي وبالتالي تحسين سرعة الاستجابة في الشبكات الكبيرة).

القسم العملي :

إعداد بيئة العمل (VMware – Client – Server – Domain Controller)

- **مكونات البيئة :**
  - لدينا جهازان على VMware :

Server سيصبح Domain Controller + **client**

- **إعداد عنوان IP لكل جهاز**

1. عنوان الـServer

- ندخل إلى **Windows Server** ونضيف IP ثابت عبر:
  - Control Panel → Network and Sharing Center
  - Change Adapter Settings
  - Properties
  - IPv4
  - Use the following IP Address

2. عنوان الـClient

- نحول إعداد الشبكة بحيث يكون متوافقًا مع نوع الشبكة التي اخترناها للـ Server
- نضبط IP ، DNS

ملاحظة : DNS يجب أن يكون عنوان الـ Server لأنه الـ Domain Controller في تطبيقنا.

- **اختبار الاتصال بين الأجهزة**
  - من جهاز Client ننفذ أمر ping لعنوان السيرفر

إذا لم ينجح الاتصال ❌ غالباً يكون السبب الـ Firewall مفعل على أحد الجهازين.

الحل:

- إطفاء Windows Firewall على كل من Server و Client مؤقتا.

• إعداد DNS وDomain Controller

1.مفهوم DNS في الشبكة الخاصة بالـDomain

- DNSمهم جدا لأنه يمكن الأجهزة من العثور على الـ Domain داخل الشبكة.
- عند استخدام Domain Controller يجب أن يشير الـ DNS في الأجهزة الأخرى إلى IPالخاص بال -Domain Controller **(في تطبيقنا هو نفسه IP السيرفر) .**

2.تثبيت DNS داخل الـServer

- عندما نقوم بإنشاء Domain جديد داخل Windows Server ، فإن النظام يقوم تلقائيا بتنصيب DNS وربطه بالـ Domain

ملاحظة هامة ☜: بدون DNS صحيح، ❌ لا يمكن لأي جهاز Client الانضمام إلى الدومين.

• خطوات الانضمام إلى الـ Domain من الـClient

1. التأكد من:
   - IP صحيح
   - DNS يشير إلى الـServer
2. التأكد من نجاح Ping بين الجهازين.
3. الذهاب إلى:
   - System Properties → Rename this PC → Change → Domain
4. إدخال اسم الـDomain
5. إدخال **Username + Password**الخاصة بالـDomain Controller
6. إعادة تشغيل الجهاز.

ملاحظات هامة :

- الـ Domain لا يعمل إذا لم يكن DNS مضبوطا بشكل صحيح.
- الـ Client يجب أن يقرأ DNS من الـ Domain Controller ليتمكن من العثور على الـ Domain في الشبكة.
- أي خطأ في IP أو Subnet أو DNS يؤدي إلى فشل كامل في الاتصال أو الانضمام.

خطوات تحويل الخادم إلى Domain Controller :

(Promote Server to Domain Controller)

- **المتطلبات الأساسية قبل البدء**

  - يجب ضبط Static IP Address على السيرفر.
  - ضبط DNS بحيث يشير إلى نفس السيرفر.
  - التأكد من أن السيرفر قابل للوصول عبر الشبكة (نجاح الاتصال مع الاجهزة).

- **خطوات تثبيت دور Active Directory Domain Services**

  - بدء العمل من .Server Manager
  - الذهاب إلى : Add Roles and Features
  - اختيار نوع التثبيت : Role-based or feature-based installation
  - اختيار الخادم
  - اختيار الـ Role المطلوب : Active Directory Domain Services (AD DS)
    سيظهر طلب اضافة بعض الميزات Features المرتبطة ب AD DS
  - تثبيت ال Role (اي الضغط على install) والانتظار حتى اكتمال التثبيت .

- **ترقية السيرفر ليصبح Domain Controller**

1. بدء عملية الترقية : بعد التثبيت يظهر تنبيه أصفر في Server Manager
   Promote this server to a domain controller
2. اختيار نوع الدومين : إنشاء Domain جديد في Forest جديد (New Forest) وتحديد اسمه مثل : Alhwash.edu .
3. ادخال كلمة مرور لاستعادة النظام (Restore Mode) في حال حصول خلل مفاجئ DSRM Password .
4. الفحص والتهيئة : سيقوم النظام بفحص إعدادات DNS وNetBIOS ، ثم بناء الدومين.

NetBios Name هو اسم قصير Short Name مقابل اسم الدومين الطويل.(FQDN)

FQDN: ALHWASH.Local NetBIOS: ALHWASH

5. اعادة التشغيل بشكل تلقائي .

يصبح السيرفر الآن Domain Controller كامل.

6. بعد الترقية يصبح تسجيل الدخول

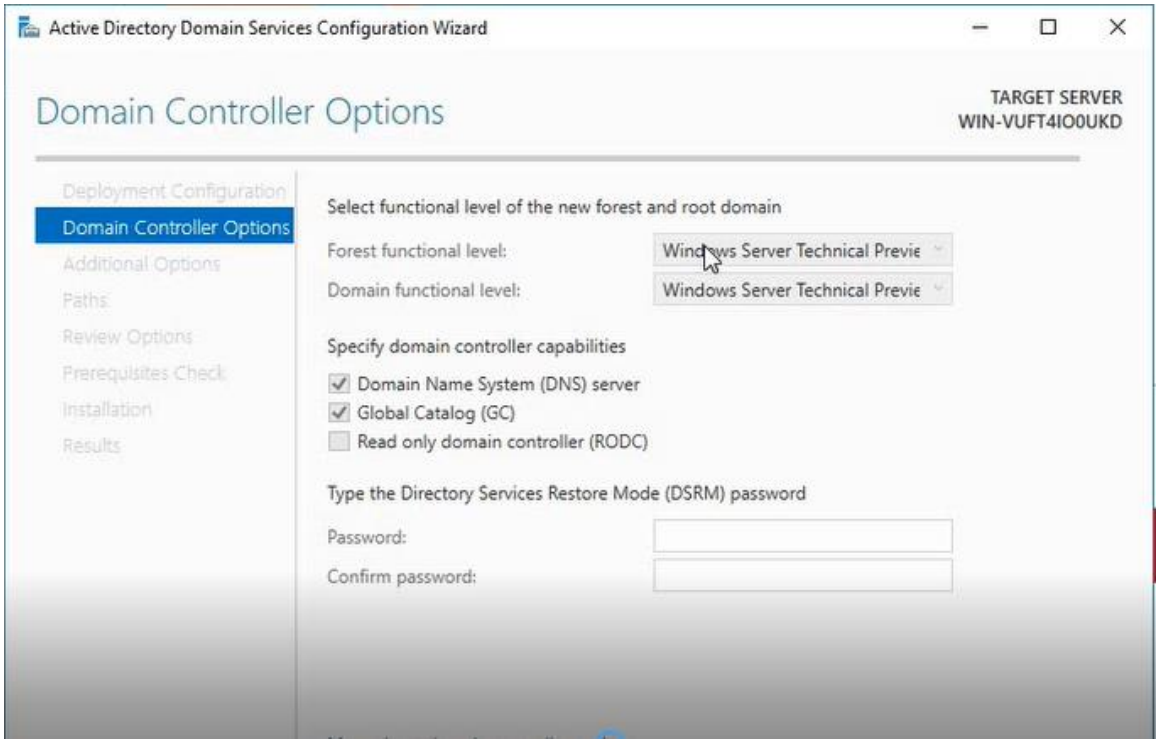
إما باستخدام:

- Administrator
- أو اسم الدومين الجديد متبوعاً بالـ backslash مثل:
  ALHWASH \Administrator

ملاحظات :

- يجب تعيين Password قوية لحساب Administrator تحقق الشروط التالية:
  - أحرف كبيرة وصغيرة
  - أرقام
  - رموز
  - طول مناسب
- DNS يجب أن يشير إلى السيرفر نفسه قبل الترقية.
- أثناء عملية الـPromote ، النظام يضبط DNS تلقائياً.
- تثبيت Active Directory Domain Services هو مجرد Role.
- عملية **Promote** هي التي تنشئ الدومين فعلياً وتحول السيرفر إلى Domain Controller
- يمكن تثبيت Active Directory Domain Services على:
  - Windows Server 2008
  - Windows Server 2012

عند الترقية من 2008 إلى 2012 أو العكس، يجب الانتباه لإصدارات الـ Domain Functional Level.



لماذا نحتاج DNS معActive Directory وما هو Global Catalog ؟

- يعمل DNS كخريطة تساعد الأجهزة على معرفة أماكن الخدمات داخل الدومين.
- بدون DNS : ❌ لا يمكن لـ Domain Controller التعرف على الأجهزة أو المصادقة عليها.
- لذلك أثناء إعداد AD يجب:
  - تثبيتDNS
  - ربطه بالدومين
  - إن لم يكن موجودا، يقوم النظام بتثبيته تلقائيا.

Global Catalog (GC) : هو عنصر مهم داخلActive Directory ، وظيفته الأساسية:

- تسريع عملية البحث Search داخل الدومين.
- حفظ نسخة جزئية من كائنات الدومين.

- يجب وجود Global Catalog واحد على الأقل في كل Forest حيث يتم تفعيله مباشرة أثناء إعداد Domain Controller

ملخص الخطوات السابقة:

- يجب تحديد:
  - Domain Name
  - NetBIOS
  - DNS
  - Password
- بعد اختيار Domain Name سيتم إنشاء:
  - DNS Zone
  - SYSVOL Folder (يحتوي على الاعدادات المشتركة مثل السياسات الامنية للنطاق وغيرها)
  - Active Directory Database

بعد الانتهاء: نعيد تشغيل السيرفر ليصبح Domain Controller جاهز للعمل

إضافة المستخدم (User) داخل الدومين واستعماله لتسجيل الدخول من جهاز العميل (Client)

1.إنشاء مستخدم جديد داخل الدومين

- ندخل إلى: **Active Directory Users and Computers**
- نختار **Users → New User** :
- نقوم بكتابة:
  - **Username**
  - **Password**
- يصبح المستخدم تحت الدومين:

ALHWASH.edu

2.تسجيل الدخول من جهاز Client باستخدام User من الدومين

- جهاز الـ Client يعمل بنظام **Windows 7** أو أي نسخة أخرى.
- يجب أولًا **ضم الجهاز إلى الدومين** حتى نتمكن من تسجيل الدخول بالمستخدم الجديد.

بعد إعادة التشغيل:

- نذهب لشاشة تسجيل الدخول.
- نضغط **Switch User**.

- نختار تسجيل الدخول من الدومين وليس الـ.Local
- نكتب:
  - **Username: user الذي أنشأناه**
  - **Password** الخاصة به.
- سيتم تسجيل الدخول بواسطة الدومين.

..... انتهت الجلسة مع تمنياتي لكم بالتوفيق والنجاح .....