إيه هو الـ Active Directory (AD)؟

الـ Active Directory (AD) هو نظام بيخلّي إدارة الشبكات الكبيرة أسهل. بدل ما تعدي على كل جهاز في الشبكة وتضبط إعداداته يدوي، AD بيخلّيك تدير كل حاجة من مكان واحد.

الجهاز اللي بيشغل الـ Active Directory اسمه **Domain Controller (DC)**، وده زي "المخ" بتاع الشبكة.

ليه بنحتاج AD؟

تخيّل إنك عندك شركة صغيرة فيها 5 أجهزة و5 موظفين. تقدر بسهولة تضبط كل جهاز يدوي، لكن لو الشركة كبرت وبقى عندك 320 مستخدم و157 جهاز في 4 مكاتب، هتبقى كارثة لو بتديرهم كل واحد لوحده.

هنا الـ AD بيحل المشكلة، وده اللي بيعمله:

1. **إدارة مركزية للهويات:** المستخدمين بيتسجلوا في مكان واحد، وبيقدروا يدخلوا على أي جهاز في الشبكة بحسابهم.
2. **إدارة السياسات الأمنية:** زي منع الموظفين من فتح الـ Control Panel على أجهزة الشركة.
3. **توفير وقت ومجهود:** بدل ما تعدي على كل جهاز، كل حاجة بتضبطها من السيرفر.

أهم مكونات الـ AD:

1. Users (المستخدمين):

- كل موظف في الشركة بيكون ليه حساب مستخدم. الحساب ده بيتيح له الدخول على الشبكة، استخدام الملفات المشتركة، والطابعات.
- ممكن كمان تعمل حسابات لخدمات زي قواعد البيانات.

2. Machines (الأجهزة):

- لما جهاز ينضم للدومين، بيتسجل في الـ AD كـ "Machine Account".
- اسم الجهاز في الدومين بيبقى اسمه العادي + "$" (مثال: DC01$).

3. Security Groups (مجموعات الأمان):

- بدل ما تضبط صلاحيات لكل مستخدم لوحده، بتجمع المستخدمين في مجموعة (Group) وتدي المجموعة دي الصلاحيات.
- زي إنك تعمل مجموعة "Sales" وتديهم صلاحية الوصول لطابعة معينة.

4. Organizational Units (OUs):

- دول زي "فروع" جوا AD بتصنف المستخدمين والأجهزة حسب الأقسام (زي Sales، IT).
- كل قسم ممكن يكون ليه سياسات (Policies) مختلفة.

الفرق بين الـ OUs والـ Groups؟

- الـ OUs: لتطبيق سياسات (Policies) على المستخدمين أو الأجهزة، وكل مستخدم ينتمي لـ OU واحدة بس.
- الـ Groups: لإعطاء صلاحيات على الموارد (زي الملفات والطابعات)، والمستخدم ممكن ينتمي لأكتر من Group.

مثال عملي:

الشركة عندها الأقسام دي:

- IT
- Sales
- Marketing
- Management

السيناريو:

1. **تنظيم المستخدمين:**
   - تضيف حساب لكل موظف في القسم بتاعه (Sales ،IT... إلخ).
   - تدي صلاحيات للمجموعات زي السماح لقسم IT بالدخول على السيرفرات.
2. **ضبط السياسات:**
   - تمنع قسم Sales من فتح الـ Control Panel.
   - تسمح لقسم IT بتغيير باسوردات الموظفين.
3. **إدارة الموارد:**
   - عندك طابعة مشتركة، تعمل مجموعة اسمها "Printer Users" وتضيف اللي هيستخدموا الطابعة.
4. **النتيجة:**
   - الموظف يقدر يدخل بأي جهاز في الشركة بحسابه.
   - السياسات مطبقة تلقائي على حسب القسم.
   - الموارد (زي الطابعة) متاحة بس للمستخدمين اللي عندهم صلاحية.

Your first task

إيه المطلوب؟

إحنا شغالين على Active Directory (AD) وعايزين نعمل شوية تعديلات عشان نطابق الهيكل التنظيمي بتاع الشركة.
الخطوات اللي هنعملها تشمل:

1. حذف الأقسام (OUs) اللي مش مطلوبة.
2. حذف وإضافة المستخدمين عشان يطابقوا الهيكل الجديد.
3. تفويض (Delegation) صلاحيات لفيلبس (Phillip) عشان يقدر يغير باسوردات المستخدمين اللي في الأقسام اللي بيشرف عليها.
4. تجربة تفويض الصلاحيات باستخدام PowerShell.

الخطوات بالتفصيل وبالعامية

1. حذف الـ OU اللي مش مطلوبة

- افتح Active Directory Users and Computers.
- هتلاقي إن الأقسام (OUs) محمية ضد الحذف عشان ما تتلغبش بالغلط. عشان نلغي الحماية:
  1. من قايمة **View**، فعل **Advanced Features**.

2. كليك يمين على الـ OU اللي عايز تحذفها، واختار **Properties**.
3. في التبويب **Object**، شيل علامة الصح من "Protect object from accidental deletion".
4. دلوقتي احذف الـ OU بكل بساطة، وهيمسح كل اللي جواها (مستخدمين أو OUs تانية).

---

2. تعديل المستخدمين

- عشان تضيف أو تحذف مستخدمين:
  1. كليك يمين على القسم (OU) اللي عايز تعدل فيه.
  2. لو عايز تضيف مستخدم جديد: اختر **New > User** وامشي مع الخطوات.
  3. لو عايز تحذف: كليك يمين على المستخدم واختر **Delete**.

---

3. تفويض الصلاحيات (Delegation)

- فيليبس مسؤول عن الـ IT Support وعايزينه يقدر يغير باسوردات الناس اللي في الأقسام: **Marketing**، **Sales**، و**Management**.
- خطوات التفويض:
  1. كليك يمين على القسم (زي Sales) واختر **Delegate Control**.
  2. في النافذة اللي هتفتح، اختار المستخدم (Phillip).
     - اكتب اسمه "phillip"، واضغط **Check Names**.
  3. اختر المهمة اللي هتفوّضها له: **Reset user passwords and force password change at next logon**.
  4. اضغط **Finish**.

---

4. تجربة تفويض الصلاحيات

- هنستخدم حساب فيليبس ونجرب نغير باسورد Sophie اللي في قسم Sales باستخدام PowerShell.

تغيير الباسورد:

1. افتح PowerShell كفيليبس.

اكتب الأمر ده:
powershell
نسخ الكود
```
Set-ADAccountPassword sophie -Reset -NewPassword (Read-Host
-AsSecureString -Prompt 'New Password') -Verbose
```

2.
   - لما يطلب منك، اكتب الباسورد الجديد.

إجبار المستخدم على تغيير الباسورد عند أول دخول:

اكتب الأمر ده:
powershell

نسخ الكود

```
Set-ADUser -ChangePasswordAtLogon $true -Identity sophie -Verbose
```

.1

---

5. الدخول بحساب Sophie

- بعد ما تغير الباسورد، ادخل على جهاز Sophie باستخدام RDP.
  - اسم المستخدم: `THM\sophie`.
  - الباسورد: الباسورد الجديد اللي حطيته.
- هتلاقي علم (flag) على سطح المكتب، انسخه.

مثال عملي

1. في AD، شيل الـ OU اللي اسمها "Old Department" بنفس الخطوات.
2. عدل المستخدمين في قسم Sales. لو Sophie مش موجودة، أضفها، ولو في حد مش موجود في الهيكل امسحه.
3. فوض فيلبس لصلاحيات تغيير الباسوردات على قسم Sales.
4. استخدم PowerShell كفيلبس وغير باسورد Sophie.
5. ادخل بحساب Sophie وشوف العلم.

ملخص شرح الـ Active Directory وإعداد الـ GPOs والسياسات الأمنية

1. الـ Organizational Units (OUs):

- **OUs** هي وحدات تنظيمية تُستخدم لتقسيم الأجهزة والمستخدمين داخل الشبكة.
- عند انضمام أي جهاز للشبكة، يُوضع افتراضيًا داخل **Computers Container**.
- يفضل إنشاء **OUs** لفصل الأجهزة بناءً على الاستخدام:
  1. **Workstations:** للأجهزة التي يستخدمها الموظفون يوميًا.
  2. **Servers:** للخوادم التي تقدم خدمات الشبكة.
  3. **Domain Controllers (DCs):** للتحكم في الدومين.

---

2. Group Policy Objects (GPOs):

- الـ **GPO** هي مجموعات من السياسات تُطبق على الـ **OUs** لتخصيص الإعدادات الأمنية والوظيفية.
- تُدار عبر أداة **Group Policy Management** الموجودة في قائمة **Start**.

---

3. أمثلة على إعداد GPOs:

1. **تقييد الوصول للـ Control Panel:**

- أنشئ GPO جديد باسم "Restrict Control Panel Access".
- اذهب إلى:
  - **User Configuration > Policies > Administrative Templates > Control Panel**
  - قم بتفعيل **Prohibit Access to Control Panel and PC settings**.
- اربط هذا الـ GPO مع الـ OUs للمستخدمين مثل **Marketing** و **Sales**.

2. **قفل الشاشة التلقائي:**
   - أنشئ GPO جديد باسم "Auto Lock Screen".
   - اذهب إلى:
     - **Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options**
     - قم بتحديد الوقت بـ 5 دقائق لقفل الشاشة عند عدم النشاط.
   - اربط الـ GPO بالجذر (Root Domain) لتطبيقه على جميع الأجهزة.

---

4. تطبيق وتحديث الـ GPOs:

- التحديث التلقائي للـ GPOs قد يستغرق ساعتين.

لتطبيق السياسات فورًا، استخدم الأمر التالي في **PowerShell**:
powershell
نسخ الكود
```
gpupdate /force
```

---

5. بروتوكولات المصادقة في Windows Domains:

البروتوكولات في ويندوز دومين

عندك نوعين أساسيين من بروتوكولات المصادقة في شبكات الويندوز:

- **Kerberos**: البروتوكول الحديث والمعتمد بشكل افتراضي في جميع الإصدارات الحديثة من ويندوز.
- **NetNTLM**: بروتوكول قديم، بيستخدم فقط للتوافق مع الأنظمة القديمة.

أولاً: Kerberos Authentication

Kerberos بيشتغل بفكرة "التذاكر" (Tickets)، وده معناه إنك لما تدخل الشبكة مرة، مش محتاج تدخل بياناتك في كل مرة عايز تستخدم خدمة.

كيف يعمل Kerberos؟

1. **طلب التذكرة (TGT):**
   - المستخدم يبعت اسمه و"توقيت مشفر" باستخدام مفتاح مستخرج من كلمة السر الخاصة بيه إلى **Key Distribution Center (KDC)**.
   - الـ KDC يرد عليه بـ **TGT (Ticket Granting Ticket)**، اللي هو تذكرة تسمح له يطلب تذاكر أخرى.
   - مع التذكرة دي، المستخدم بياخد كمان مفتاح اسمه **Session Key**.

2. **طلب الوصول لخدمة معينة:**
   - لما يحتاج المستخدم يدخل خدمة (مثلاً قاعدة بيانات)، يبعت الـ TGT للـ KDC ومعاه اسم الخدمة.
   - الـ KDC يرد عليه بتذكرة اسمها **TGS (Ticket Granting Service)** مخصصة للخدمة المطلوبة.
3. **الاتصال بالخدمة:**
   - المستخدم يبعث الـ TGS للخدمة اللي عايز يدخلها.
   - الخدمة تتحقق من التذكرة وتسمح له بالوصول.

المميزات:

- المستخدم مش بيحتاج يبعت كلمة سره كل مرة.
- العملية سريعة وآمنة.

ثانياً: NetNTLM Authentication

NetNTLM بيستخدم طريقة اسمها **Challenge-Response**، وده نظام يعتمد على توليد تحديات عشوائية والتحقق من الإجابة عليها.

كيف يعمل NetNTLM؟

1. **طلب المصادقة:**
   - المستخدم يبعث طلب دخول للخادم.
2. **إرسال التحدي:**
   - الخادم يرد عليه بتحدي (رقم عشوائي).
3. **حل التحدي:**
   - الجهاز الخاص بالمستخدم ياخد كلمة السر المُشفرة بتاعته ويستخدمها مع التحدي لحساب رد (Response).
   - الرد يتبعت للخادم.
4. **التحقق:**
   - الخادم يبعت التحدي والرد للـ Domain Controller.
   - الـ Domain Controller يتحقق إذا الرد صحيح من خلال حساب نفس العملية ومقارنة النتيجة.
5. **إرسال النتيجة:**
   - إذا كانت الإجابة صح، المستخدم يتصل بالخدمة. لو غلط، يتم رفض الدخول.

المميزات والعيوب:

- **ميزة:** كلمة السر نفسها عمرها ما تتبعت على الشبكة.
- **عيب:** أقل أمانًا من Kerberos وممكن يتعرض لهجمات مثل Pass-the-Hash

---

1. الشجرة (Tree)

لما الشركة تكبر وتفتح في بلاد تانية، هنا الموضوع بيبقى معقد شوية.

- لو مثلًا فتحنا فرع في **إنجلترا** وفرع في **أمريكا**، وكل فرع ليه قوانين وسياسات مختلفة، ساعتها هنحتاج نقسم الدومين لعدة دومينات فرعية (Subdomains) زي:
  - `uk.thm.local` (لإنجلترا)
  - `us.thm.local` (لأمريكا)
- كده كل فرع هيبقى ليه **Domain Controller** خاص بيه، وفريق IT في كل فرع يقدر يدير أموره من غير ما يتدخل في فرع تاني.

- فيه مجموعتين مهمين هنا:
  - **Domain Admins**: مسئولين عن الدومين الفرعي بتاعهم بس.
  - **Enterprise Admins**: دول بقى اللي عندهم صلاحيات على كل الدومينات في الشجرة.

---

2. الغابة (Forest)

بفرض إن شركتك اشترت شركة تانية زي **MHT Inc.**، والشركتين ليهم دومينات مختلفة (زي `thm.local` و `mht.com`).

- ممكن توحد الشغل كله في **Forest** بحيث كل شجرة تحتفظ بهويتها (اسمها) بس كلهم بيتشاركوا نفس الشبكة.
- كده كل شركة تقدر تدير شغلها وفي نفس الوقت فيه إمكانية للتواصل بينهم عند اللزوم.

---

3. العلاقات بين الدومينات (Trust Relationships)

لو في موظف من فرع إنجلترا محتاج يدخل على ملفات موجودة في سيرفر فرع أمريكا، لازم يكون فيه **Trust** بين الدومينات.

- **علاقة الثقة (Trust)** معناها إن دومين بيسمح لدومين تاني إنه يستخدم موارده.

أنواع الثقة:

1. **ثقة في اتجاه واحد (One-Way Trust)**:
   - لو دومين A وثق في دومين B، يبقى المستخدمين في B يقدروا يدخلوا على موارد A، لكن العكس مش هيحصل.
2. **ثقة متبادلة (Two-Way Trust)**:
   - هنا الدومينات بتثق في بعض، وكل واحد يقدر يدخل على موارد التاني.
   - ده بيبقى الوضع الطبيعي لما يكونوا تحت شجرة أو غابة واحدة.

ملحوظة مهمة

الثقة مش معناها السماح التلقائي!

- يعني حتى لو فيه Trust بين دومينين، لازم مسؤول النظام (Admin) يحدد مين مسموح له يدخل على إيه

---

1. الدومين (Domain)

- **إيه هو الدومين؟**
تخيل شركة كبيرة، وكل الموظفين فيها ليهم حسابات على نفس الشبكة عشان يقدروا يدخلوا على السيرفرات أو الطابعات أو الملفات. الـ **Domain** ده بمثابة قلب الشبكة اللي بيجمع المعلومات عن كل المستخدمين والأجهزة اللي تحت مظلته.
- **مثال:**
عندك موظف اسمه أحمد. أول ما يحاول يدخل على الكمبيوتر في الشركة، بيطلب منه اليوزر نيم والباسورد. الدومين بيشوف لو أحمد موجود فعلاً ومصرح ليه، ويقول للكمبيوتر "أيوة ده أحمد بتاعنا، سيبه يدخل".

---

2. الدومين كونترولر (Domain Controller)

- **إيه وظيفته؟**
  ده بمثابة العقل المدبر للدومين.
  هو اللي بيدير كل حاجة:
  - مين يدخل.
  - مين ليه صلاحيات على إيه.
  - بيتأكد إن كله ماشي صح.
- **مثال:**
  لو أحمد عايز يفتح ملف خاص بالمدير، الدومين كونترولر هيقول له: "استنى، الملف ده مش ليك، دي صلاحيات المدير".

---

3. الشجر والغابات (Trees & Forests)

- **الشجرة (Tree):**
  دي لما يكون عندك أكتر من دومين جوه نفس الشركة. يعني لو الشركة ليها فرع في مصر وفرع في السعودية، كل فرع ممكن يبقى ليه دومين مختلف، لكن الدومينات دي بتتواصل مع بعض بسهولة عن طريق **Trust**.
  - **مثال:**
    لو فيه دومين اسمه `egypt.company.local` ودومين تاني `ksa.company.local`، الموظفين في مصر يقدروا يشوفوا الملفات اللي في السعودية والعكس صحيح.
- **الغابة (Forest):**
  لو عندك أكتر من شجرة (يعني أكتر من شركة كبيرة)، وكل شجرة ليها دومیناتها، الغابة هي اللي بتجمع الشجر ده كله تحت مظلة واحدة.
  - **مثال:**
    شركة A اشترت شركة B، وكل شركة ليها دومينات مختلفة. الغابة تخلي الشركتين يشتغلوا مع بعض بسهولة من غير ما يغيروا دومیناتهم.

---

4. الثقة (Trust)

- دي العلاقة بين الدومينات عشان يقدروا يشاركوا الموارد.
  - **مثال:**
    لو فيه **One-Way Trust** بين مصر والسعودية، يبقى موظفي مصر يقدروا يدخلوا على موارد السعودية، لكن موظفي السعودية ما يقدروش يدخلوا على موارد مصر إلا لو عملنا **Two-Way Trust**.

---

5. الحاويات والأوراق (Containers & Leaves)

- **الحاوية (Container):**
  لو عندك حاجة جوه حاجة. زي فولدر فيه ملفات.
  - **مثال:**
    القسم المالي عنده فولدر فيه كل ملفات الموظفين. الفولدر هنا حاوية.
- **الورقة (Leaf):**
  لو عندك حاجة لوحدها. زي ملف Excel مثلاً مش جوه فولدر.

---

6. تخزين الـ LM Hash (LAN Manager Hash)

- **إيه ده؟**
الباسورد بتاعك ما بيتخزنش بنصه، بيتخزن كأنه مشفر بحاجة اسمها **Hash**. الـ LM Hash ضعيف، والمهاجمين ممكن يكسروا التشفير بسهولة.
- **الحل:**
تلغي تخزين الـ LM Hash وتستخدم NT Hash الأقوى.
- **مثال عملي:**
في الـ Group Policy، تختار:
Computer Configuration > Policies > Security Options > Do not store LM hash.

---

7. SMB Signing

- **إيه فايدته؟**
الـ SMB بيستخدم لنقل الملفات. لو مش مأمن، ممكن حد يعدل الملفات وهي بتتنقل.
الـ SMB Signing بيأكد إن الملفات ما اتعدلتش.
- **مثال عملي:**
في الـ Group Policy:
Computer Configuration > Security Settings > Microsoft network server: Digitally sign communication.

---

8. LDAP Signing

- **إيه ده؟**
ده بروتوكول بيستخدم لتحديد الموارد في الشبكة. لو مش مؤمن، ممكن حد يبعث طلبات وهمية.
- **مثال عملي:**
في الـ Group Policy:
Domain controller: LDAP server signing requirements > Require signing.

---

9. سياسة الباسورد (Password Policy)

- **إزاي تعملها؟**
  - الطول الأدنى: 10-14 حرف.
  - لازم يكون معقد (حروف كبيرة وصغيرة وأرقام ورموز).
  - ما تستخدمش نفس الباسورد القديم.
- **مثال عملي:**
Account Policies > Password Policy > Set maximum password age.

---

10. نموذج الوصول المتدرج (Tiered Access Model)

- **إيه هو؟**
تقسيم الشبكة لمستويات:
  - **Tier 0:** المديرين والدومين كونترولر.
  - **Tier 1:** السيرفرات المهمة.
  - **Tier 2:** أجهزة المستخدمين العادية.

- **فايدته؟**
بيقلل المخاطر لو حصل اختراق في أي مستوى.

---

11. الحماية من الهجمات المشهورة (Kerberoasting)

- **إيه المشكلة؟**
المهاجمين ممكن يكسروا كلمات السر بتاعة السيرفرات باستخدام تذاكر Kerberos.
- **الحل:**
  - استخدم MFA.
  - غير الباسوردات بشكل دوري.