

الباب الثالث

Active Directory Service الدليل النشط

س1: عرف الدليل النشط Active Directory وماهى الوظائف التى يقوم بها فى شبكة الاتصال؟
الدليل النشط : عبارة عن خدمة موجودة داخل نظام التشغيل لخدمة وتكون من مجموعة كبيرة من العناصر وتم تقسيمها فى شكل هرمى لتسهيل التعامل مع الدليل وتصحيح اى اخطاء ومشاكل قد تحدث .

يقوم الدليل النشط بالوظائف الاتية فى شبكة الاتصال

- 1- توفير دليل (يحتوى على قائمة هيكلية) بكل الكائنات الموجودة فى شبكة مثل المستخدمين users والمجموعات groups واجهزة devices
- 2- توفير نقطة واحدة لادارة الكائنات (من المستخدمين - اجهزة الكمبيوتر والموارد)
- 3- توفير خدمة التوثيق والامن التى توفر امكانية الوصول الى موارد الشبكة والتحكم فيها .
- 4- تفويض من الادارة للسماح بالادارة الغير مركزية لكائنات الدليل النشط (users and group)

س2: ماهو التخطيط المستخدم فى الدليل النشط ؟

- 1- يتم تخطيط الدليل النشط على عدة مستويات بحيث يتضمن كل مستوى مجموعة من الكائنات وسهل التحكم فيها .
- 2- يتم تقسيم عناصر الدليل فى شكل هرمى (لتسهيل التعامل معها - وتسهيل تصحيح الاخطاء)

س3: اشرح البنية الهرمية للدليل النشط ؟

التقسيم الهرمى للدليل النشط A.D Logical structure

- 1- المجال domain وحدات التنظيم OU
- 2- التفرعات Tree ومجموعات التفرع forest
- 3- A global catalog

اولاً: المجال domain وحدات التنظيمية

1- كائنات الدليل النشط :

كلمة كائن تطلق على اى عنصر من موارد الشبكة مثل المستخدم user ، مجموعة group ولاجهزة

2- وحدات تنظيمية (OU) Organizational unit (OU) هي عبارة عن تجمع تنظمى لكائنات

3- المجال او النطاق Domain معين هو عبارة عن مجموعة من اجهزة ومستفيدين ومجموعات تربط بينها علاقة ثقة من نوع ما وتتشارك في بعض الخصائص المشتركة ولها قاعدة بيانات واحدة

ثانياً: التفرع Forest

التفرع هو مجموعة من domain التي تربط بينها لها اسم مشترك وغالباً ما تتكون من Parent domain , sub domain or child domain

علاقة الثقة المتعددة

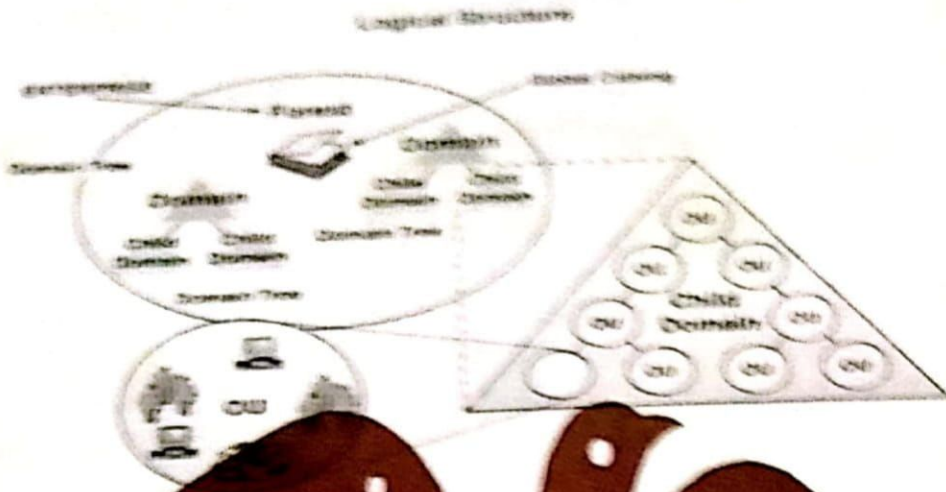
هي عبارة عن علاقة ثقة تربط بين اثنين Domain مختلفين من بعض وتسمح بتحويل اى مستخدم من احد ال Domain الى Domain اخر

مجموعة التفرع Forest

هي مجموعة من الأشجار tree مرتبطة مع بعضها البعض عن طريق علاقات الثقة المتعددة بينهم

ثالثاً : خادم الكتالوج العام GC

هو عبارة عن نوع جديد من قواعد البيانات يحتوى على قائمة بالخدمات التي يمكن الوصول اليها من داخل شبكة الاتصال و يتم تثبيته على وحدة تحكم واحدة DC
مميزاته: تسجيل الدخول - الاستعلام (البحث عن موارد محددة)



س٤: عرف محفظ البيانات وذكر أهميته ؟

محفظ البيانات هي مجموعة من البيانات التي يتم تخزينها في قاعدة البيانات. من خلاله يمكن التعرف على البيانات وخصائصها الموجودة في قاعدة البيانات. يقدم المعلومات المخزنة في قاعدة البيانات بصورة متكاملة لجميع كائنات

أهمية محفظ البيانات

- يحدد مخطط البيانات Schema المعلومات المخزنة والتي يوفرها دليل النشط بصورة متكاملة لكل كائناته

- إنشاء الحقول المحددة لكل كائن من قبل مدير الشبكة

- يوفر أرقام لكل الكائنات الموجودة في الدليل النشط كذلك النوار الوحدات التي تتصل بها وتتصل

س٥: المعلومات التي يقوم الدليل النشط بتخزينها لادخال دليل (خدمات الدليل)؟

● اسم المستخدم ومعلومات جهات الاتصال

(مثل العنوان المادي - أرقام الهاتف - البريد الإلكتروني - جهات اتصال إنترنت والملكيات) - سمات الكائنات

س6: ما المقصود بشر عناصر الى الدليل؟ وماهى عيوبه؟

هى عملية توزيع معلومات عن الكائنات المستضافة على خوادم المستخدمين الموجودة فى انحاء شبكة الاتصال

عيوبها:
زيادة تدفق تكرار المجال لضمان ان كل جهاز لديه أحدث المعلومات

س7: عرف متحكم الميدان *domain controller DC*؟ التكرار؟ وكيف يتم استخدامه؟

متحكم الميدان

هو عبارة عن جهاز يدير ويندوز معروف ثم تنصيب *ACTIVE directory* فيه وهو المسئول الرئيسى عن عمل الشبكة من حيث تصحيح المستخدمين والاجهزة وعمليات تسجيل الدخول والوصول لكثير من المهام المشابهة على الشبكة

التكرار

يعنى نسخ معلومات الدليل من وحدات التحكم فى الشبكة حتى يكون لديها نفس المعلومات ويمكن استعمال اى من وحدات التحكم عن جهاز او مستخدم معين

فى مجال الدليل النشط يتطلب 4 فئات اساسية من المعلومات للتكرار هم:

1- التوصيف

2- مخطط البيانات

3- المجال

4- معلومات عن الكتالوج العام (معلومات عن كل كائن فى الدليل)

س8: عرف المجال وأسباب استخدام مجالات متعددة فى شبكة الاتصال؟

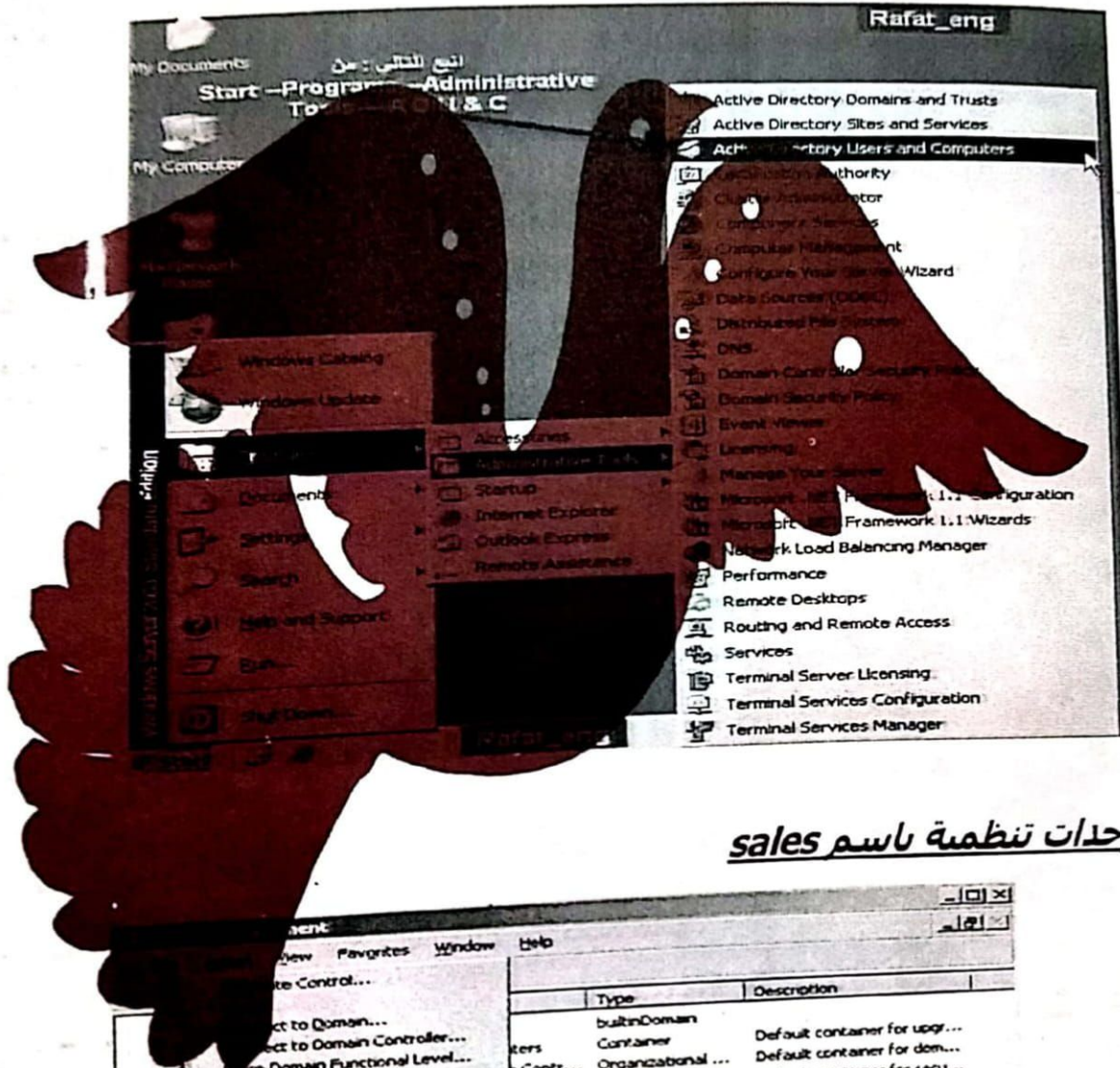
المجال او النطاق Domain

هو عبارة عن مجموعة من اجهزة ومستخدمين ومجموعات تربط بينها علاقة ثقة من نوع ما وتتشارك فى بعض الخصائص المشتركة ولها قاعدة بيانات واحدة.

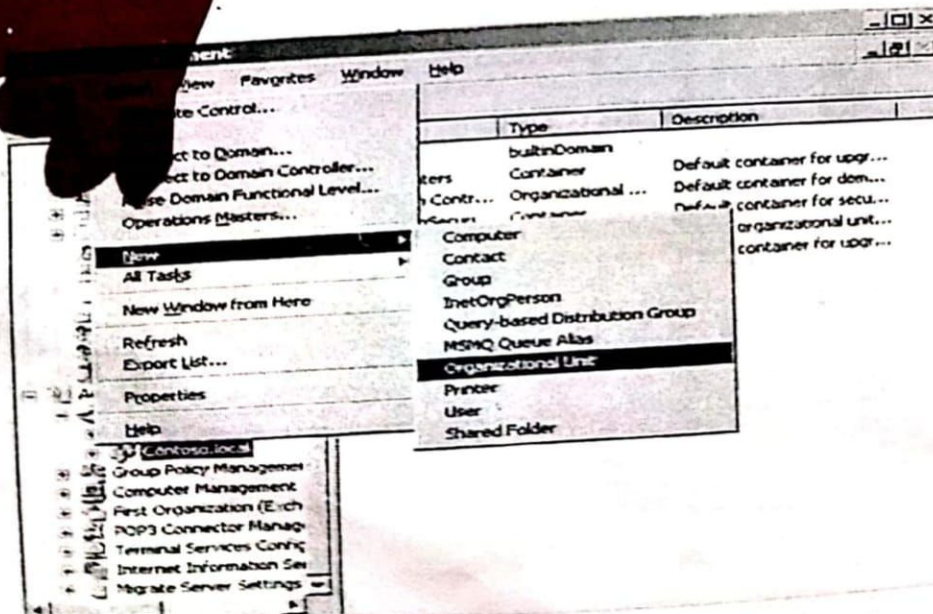
أسباب استخدام مجالات متعددة في شبكة الاتصال

- 1- توفير بنية شبكة الاتصال
- 2- التكرار وذلك نتيجة لوجود خوادم كتالوج العام يقوم بنشر المعلومات بين المجالات من أجل وصول المستخدمين إليها
- 3- الأمن والإدارة
- 4- تفويض الإدارة

إدارة المستخدمين ومجموعات العمل



إنشاء وحدات تنظمية باسم sales



New Object - Organizational Unit

Create in: ISA-SERVER.COM/

Name: Sales

OK

Active Directory Users and Computers (version 3.0) - ISA-SERVER.COM/

Saved Queries

ISA-SERVER.COM

Builtin

Computers

Domain Controllers

ForeignSecurityPrincipals

Users

Sales

Delegate Control...

Move...

Find...

Computer

Contact

Group

InetOrgPerson

MSMQ Queue Alias

Organizational Unit

Printer

User

Shared Folder

OK

New User Wizard

Create in: ISA-SERVER.COM/Sales

First name: Rafat Initials:

Last name: Salah

Full name: Rafat Salah

User logon name: rafat_eng @ISA-SERVER.COM

User logon name (pre-Windows 2000): ISA-SERVER\ rafat_eng

Next > Cancel

New Object - User Rafat_eng

Create in: ISA-SERVER.COM/Sales

Password: اكتب كلمة المرور هنا

Confirm password: اكتب كلمة المرور مرة أخرى

☒ User must change password at next logon هذا الخيار يضمن للمستخدم من تغير كلمة المرور في أو مستعمل في النظام

☐ User cannot change password. ☐ Password never expires ☐ Account is disabled

هذا الخيار يمنع المستخدم من تغير كلمة المرور
كل أربعين يوم يطلب النظام تغير كلمة المرور
هذا الخيار يقوم بإلغاء طلب تغير كلمة المرور

اسم المستخدم لا يعمل من الممكن إعطاء
اسم مستخدم وعدم سحبه من الدخول إلى النظام

Back Next > Cancel

س9: ماهي عناصر إنشاء مستخدم جديد؟

الاسم الأول
أول حرف في الاسم الوسط للمستخدم
الاسم الأخير
الاسم الكامل للمستخدم
اسم دخول في المجال للمستخدم
اسم دخول غير متكرر في المجال للإصدارات السابقة

س10: ماهي الشروط المقترحة لكلمة السر التي تجعلها قوية؟

- يجب أن يبلغ طولها 7 أحرف أو أكثر على الأقل .
- يجب أن تكون مزجا من الأحرف و الأرقام
- يجب أن تشمل على أحرف كبيرة وصغيرة A,B,a,b
- يجب أن تشمل على رمز خاص واحد أو أكثر \$,%,&
- لا يجب أن تشكل كلمة محجوزة مثل (Administrator)
- لا يجب أن تكون الأحرف والأرقام مرتبطة .

س11: ماهي حالات كلمة المرور
● إزام المستخدم بتغير كلمة السر في المرة التالية لدخوله الى التومين

● المستخدم لا يستطيع تغير كلمة السر

● يعني كلمة المرور لا تفقد صلاحيتها بمرور الوقت

● يعني انه تم انشاء حساب مستخدم ولكن لم يتم ايجين استخدامه

~~~~~

### التحكم في صلاحيات المستخدم

نلاحظ من خلال النافذة أننا دخلنا على قائمه account وتحتوي الخيارات التالية:-

-الاختيار الأول هو تحديد ساعات الدخول

-الاختيار الثاني هو السماح أو منعه

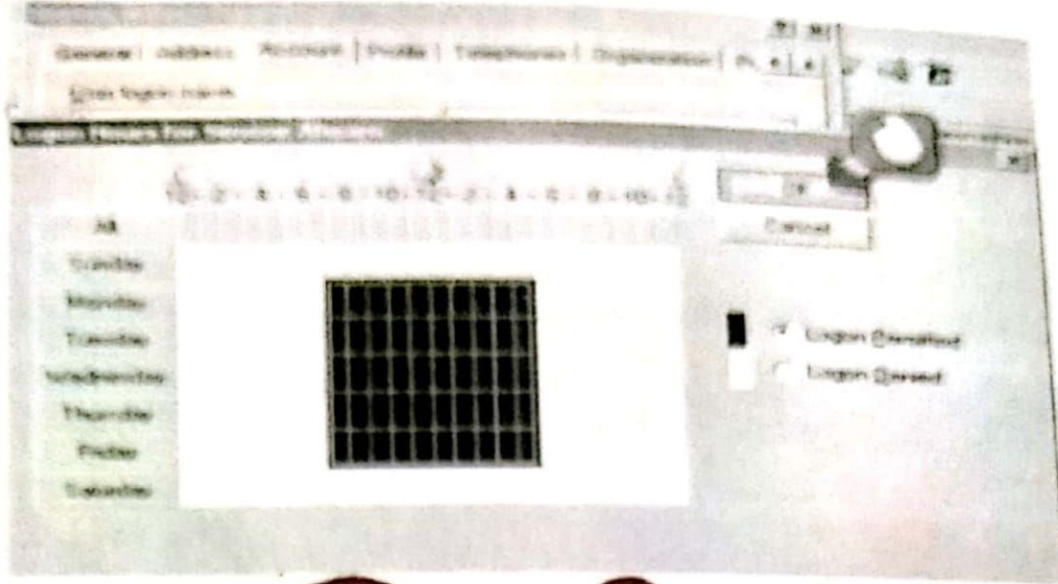
الحاسوب أو السماح الدخول من الخوادم والعمل أم لا

-الاختيار الثالث هو تحديد متى انتهاء الحساب للمستخدم.

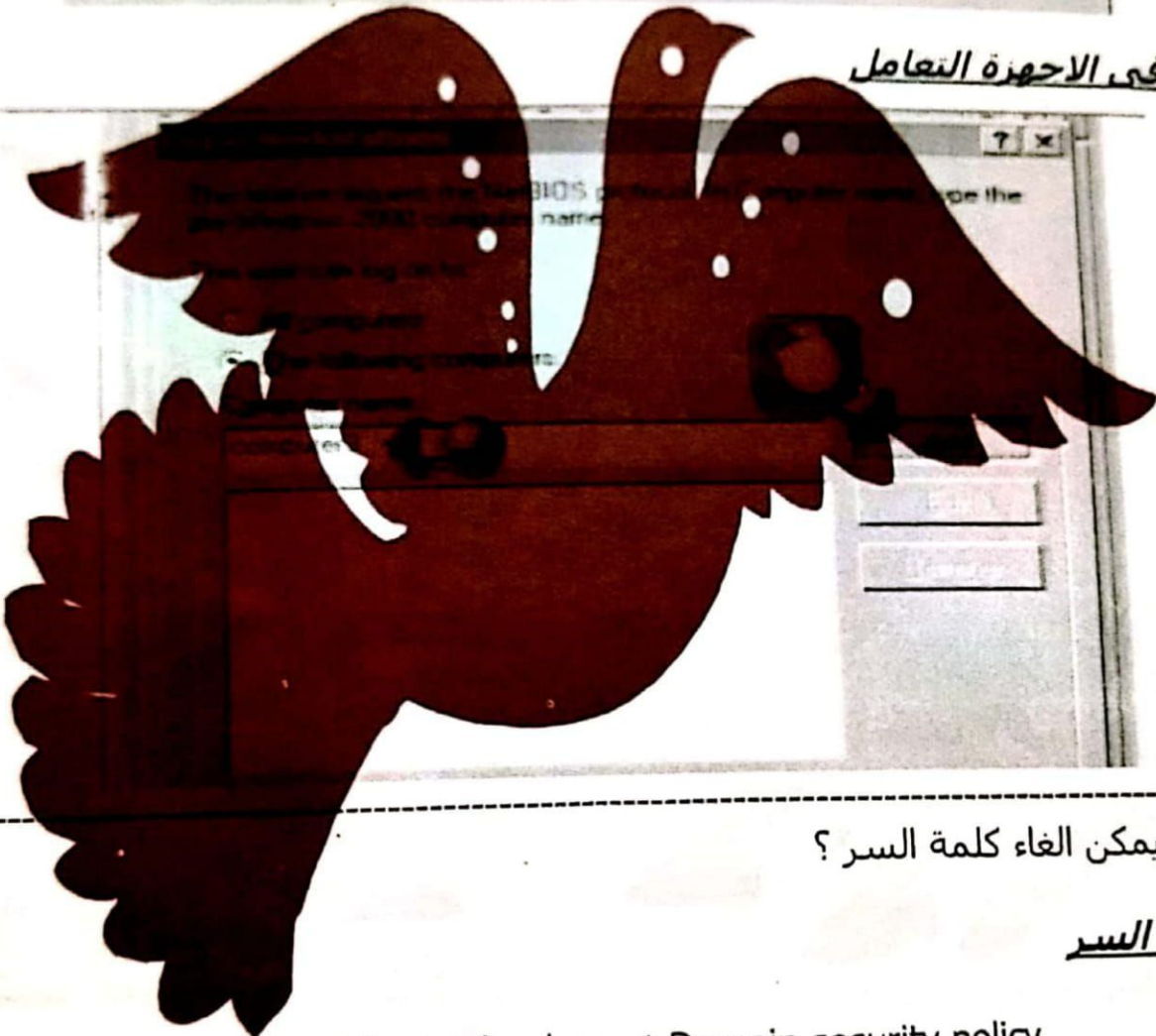
-الاختيار الرابع هو صلاحيات المستخدم.

### تحكم في الوقت مستخدم





## التحكم في الاجهزة التعامل



س12: كيف يمكن الغاء كلمة السر ؟

## لإلغاء كلمة السر

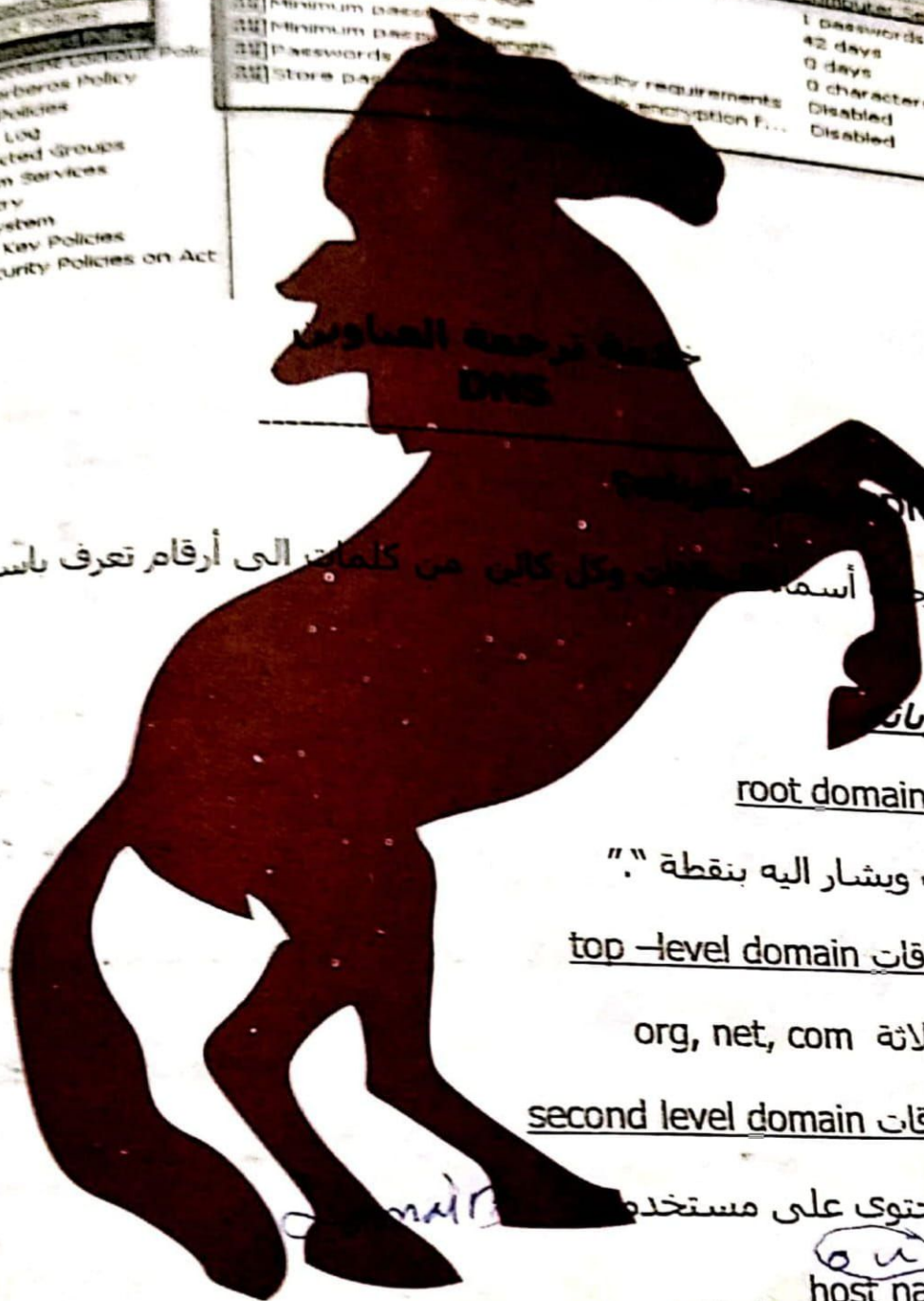
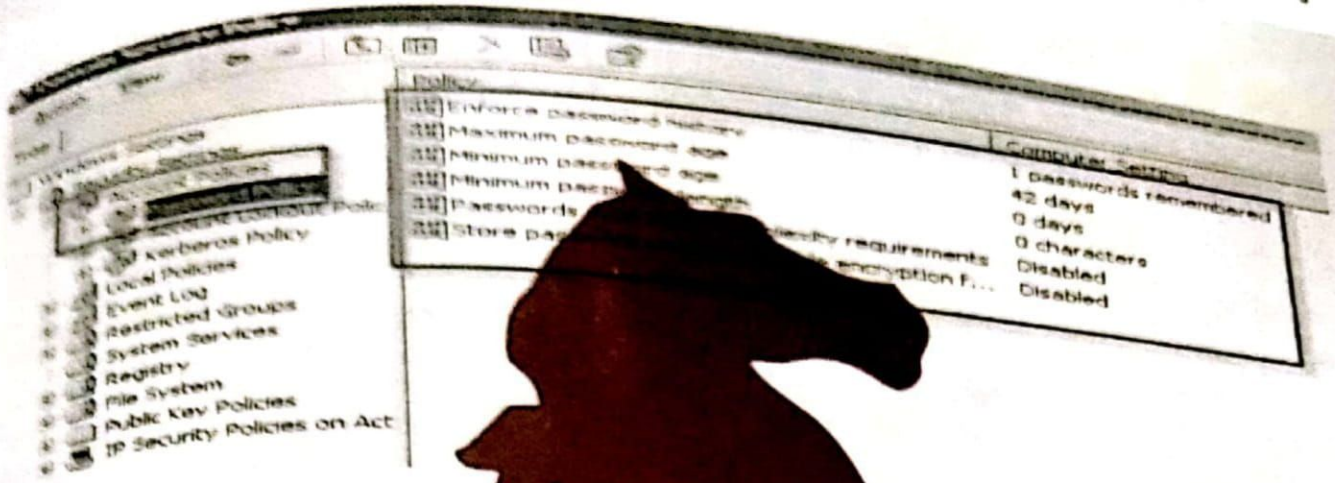
- Start administrative tools ثم نختار Domain security policy ومنها نختار account polices ثم password policy

• نقوم بتقليل طول الكلمة والغاء تعقيدها

Minimum password length (0)

Password must meet complexity require met **Disable**

نشأ حساباً باستخدام اسمه بالكامل على احد



خدمة ترجمة العناوين  
DNS

س13: عرف DNS  
يقوم بترجمة أسماء العناوين وكل كلمة من كلمات الـ IP إلى أرقام تعرف باسم IP Address

مكوناته او مستوياته

النطاق الجذري root domain

يمثل أعلى مستوى ويشار إليه بنقطة "."

مستوى القمة للنطاقات top-level domain

يمثل من رمزين او ثلاثة org, net, com

مستوى الثاني للنطاقات second level domain

تمثل sub domain يحتوي على مستخدم

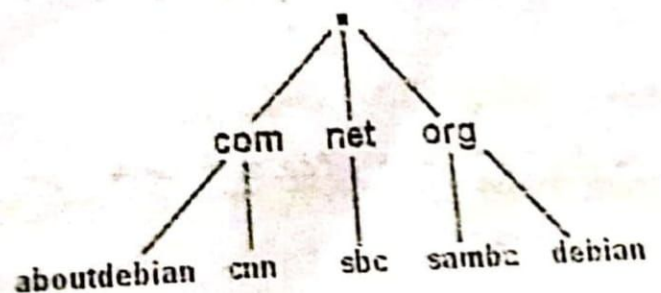
host names سماء المضيفين

مارة الى اجهزة الكمبيوتر الموجودة على الانترنت

Namespace Root

Top Level Domains

Second Level Domains





- ممكن ان :  
 1- DNS, AD لا بد ان يشتركا في نفس الوحدة التنظيمية المركزية domain  
 2- لا يقوم بتخزين كائنات ولكنه يقوم بتخزين مجالات ومعلومات  
 3- يقوم بتخزين FQDN وعنوان IP المرتبط به  
 4- DNS لا يتطلب وجود خدمة AD ولكن العكس صحيح

س14: المقصود بـ FQDN - DDNS : وظيفة DNS : FQDN

تعني اسم نطاق موزع بالكامل أي يحتوي على اسم الجهاز واسم المجالات التابعة له

وظيفة الـ DNS :

- 1- تحويل FQDN إلى عنوان IP .
- 2- تيسر خدمة DNS لكل أجهزة المجال استخدام نفس قاعدة البيانات ويتم تحديثها تلقائياً عند إضافة أي كائن .
- 3- تيسر DNS بالعمل على شبكة اتصال قائمة على DHCP ويتم تغير عنوان الكائن بشكل أوتوماتيكي .

(DDNS)

وهي خدمة تيسر لكل وحدات التحكم في المجال باستخدام نفس قاعدة البيانات التي يتم تحديثها تلقائياً عند إضافة أجهزة كمبيوتر جديدة إلى شبكة الاتصال وإزالتها منها أي يقوم DDNS بربط DSN , DHCP معاً

كيفية ترجمة العناوين

- يطلب المستخدم من أقرب DNS عنوان رقمي لإسم نطاق معين وعادة يكون معروف بالنسبة لإعدادات الشبكة .
- يقوم خادم المترجم بالبحث عن خادم رئيسي لإسم النطاق ويسئل الخادمت إلى أن يصل إلى الخادم المسئول عن النطاق ويرسل له الإستفسار .
- خادم أسماء النطاقات يبحث عن ملف النطاق المتوفر عنده المعلومة المطلوبة ثم يرد بإستفسار بالعنوان الرقمي للنطاق .
- المقرر يرد على إستفسار المستخدم بالنتيجة التي حصل عليها ويخزنها في السجلات إلى أن يطلب أي مستخدم نفس الإستفسار

كيفية انشاء منحكم مجال ونفعل خدمة الدليل النشط  
ادارة المستخدمين والنحكم في صلاحيات المستخدم

## أسئلة الباب الثالث :

- 1- عرف الدليل النشط مع ذكر وظيفته في شبكة الاتصال ؟
- 2- اذكر تخطيط الدليل النشط؟
- 3- اذكر تقسيم الدليل النشط في ويندوز سيرفر 2003؟
- 4- عرف مخطط البيانات وما أهميته ؟
- 5- عرف المجال والمنحكم الميدان واسطى استخدام مجالات منظمة في شبكة الاتصال ويندوز سيرفر 2003
- 6- عرف التفرع مع تعريف العلاقة المتعدية ؟
- 7- عرف مجموعة التفرع وخادم الكتالوج ؟
- 8- ما المقصود بالتكرار الدليل النشط بين المواقع ؟
- 9- ما المقصود بنشر عناصر الدليل وأهميته مع ذكر عيوبه ؟
- 10- اذكر ماتعرفه عن DNS ومكوناته وعلاقته بالدليل النشط ؟
- 11- اذكر ماتعرفه عن DDNS-FONS ؟
- 12- ماهى الشروط لانشاء لكلمة السر وحالات كلمة المرور والقاء كلمة السر ؟
- 12- ماهى عناصر انشاء المنحكم ؟
- 13- عرف كلا من : (DNS)-الوحدات التنظيمية (TTL)-مخطط الوقت (sales) وحدة تنظيمية Arab
- 14- أنشئ حساب مستخدم باسم أول Mohamed Ali واسم دخول Ali-eng وله الحسابات الآتية  
واسم الدخول Ali-eng وله الحسابات الآتية
- كلمة السر %2sf4YK و لابد من تغير كلمة السر .
- على جهاز أسم PC1 , PC5 , PC6 .
- السماح بالدخول من 9 ص حتى 2 مساء ماعدا جميع الايام ماعدا يوم الاثنين .
- 15- أنشئ حساب باسم أول ALI وله الصلاحيات الآتية
- كلمة السر (Ali101) و الحساب ملغى مؤقتا .
- الدخول على جهازى (Lab5-Lab 6) .