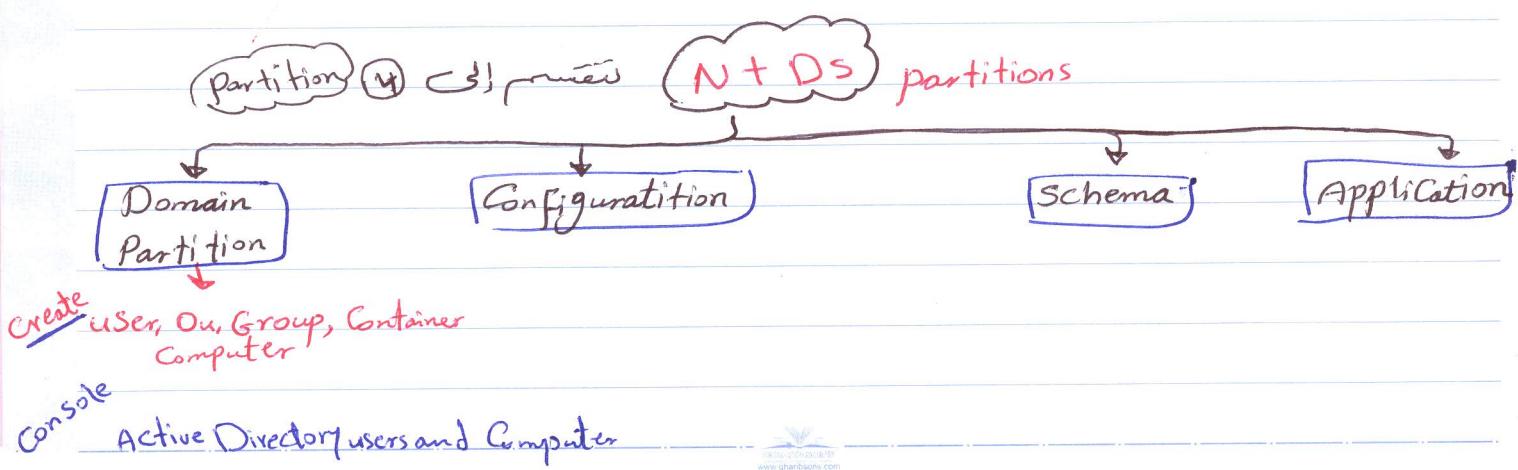
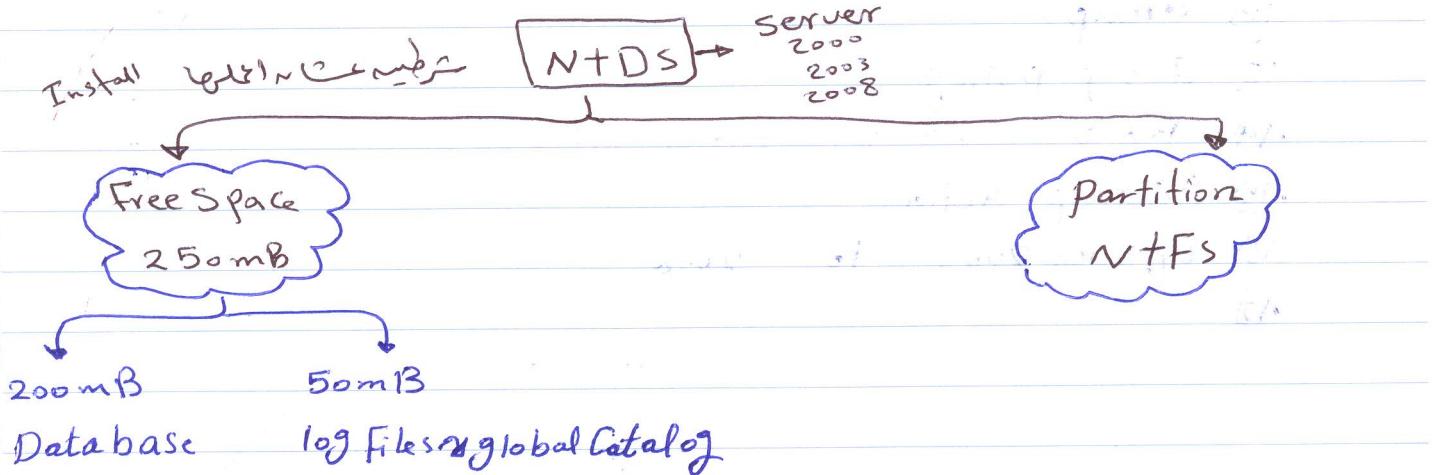
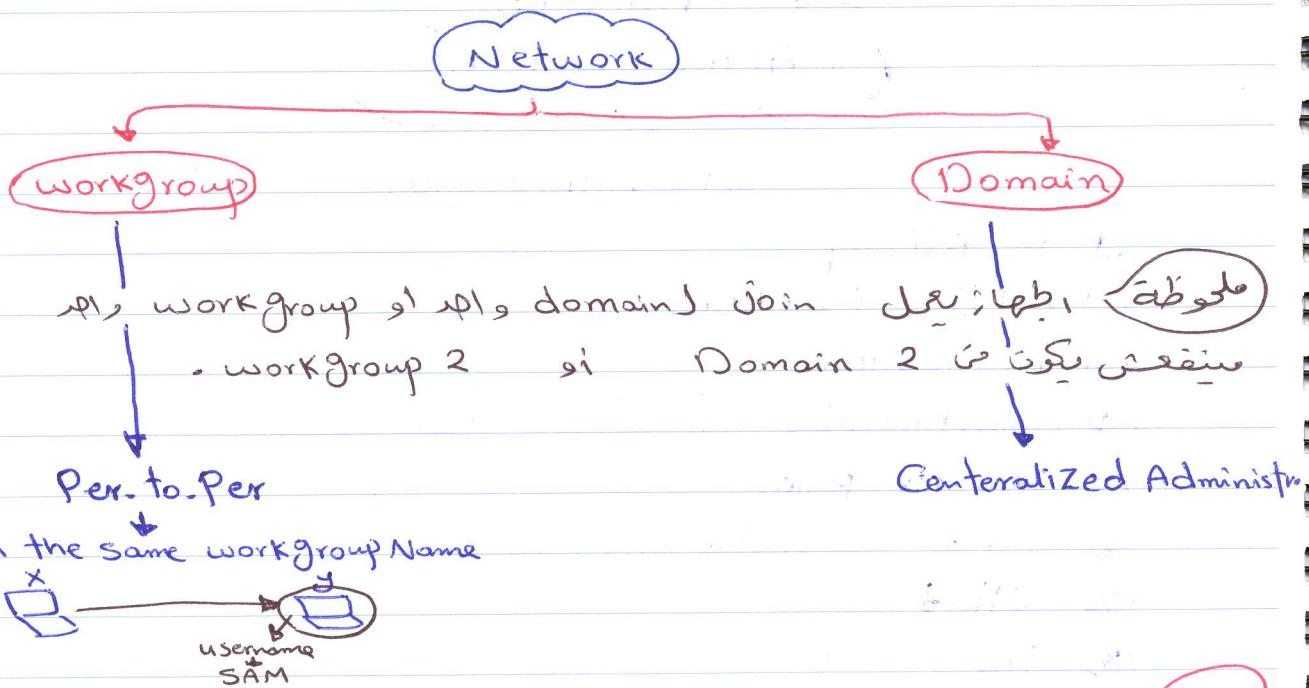




1. Introduction

- ① work Group
- ② NTDS Partitions
- ③ Replication
- ④ Additional → master
→ RODC "Readonly"
- ⑤ master Roles
- ⑥ IFM "Install From primary"
- ⑦ Child
- ⑧ Tree
- ⑨ New Forest, trust
- ⑩ Active Directory migration tool "ADmt"
- ⑪ Create multiple users "Csvde, Ldifde"
- ⑫ Groups
- ⑬ Group Policy
- ⑭ RMS "Rights management Service"
- ⑮ Backup Active
- ⑯ Upgrade 2003 to 2008
- ⑰

"2" N+DS partition



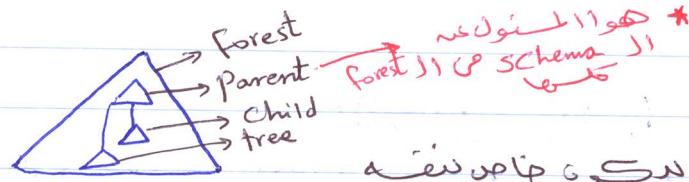
Schema partitions

class

user
ou
Groups

attributes

Properties

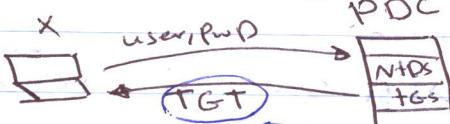


* التوقيع في forest مخصوصاً لل Schema

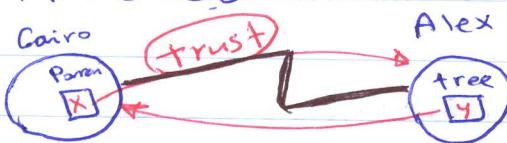
ال ذكر Domain ليس هو خاص بـ forest بل هو مخصوص بالSchema tree .
ال Parent ليس هو Parent tree بل هو Parent forest .
ويقتصر على Parent forest فقط .

Configuration partition

Active directory sites and console to manage sites



Configure partition goes here



جعل لكل واحد ينتمي إلى site

مخصوص لل الموقع X يدخل على Alex وينتقل trust من Cairo بـ Cairo .
و يرسل على Cairo trust .

Forest

كل كلام من نفس ال

Global Catalog

Forest contains all resources in all domains

كلها و ينطوي مع دومين و هي التي تعرف كل

Domain .

كل ما يجد site يجعل معاه * Global Catalog

اللذي يعرف بعدد فيها فقط ال Parent

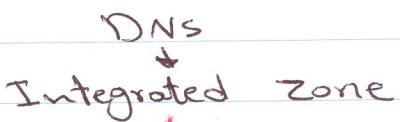
عن replication و ticket

admin هو Enterprise admin → Parent Admin

tree و Parent site

Subject.....

Application partition



التطبيق المحمي

1- نعمل جهاز IP DNS والا IP Server ونرتاحه Domain ونستطي Domains DCPromo Run

ملحوظة اول ما تطلب دفع Configuration Domain لوقت انشاء Domain من هنالك من اصحاب Domain لكن هنالك Local users and groups دفع Active Directory يسقوا في Console دفع Active Directory كـ Domain Partition

لو عملت Domain partition او New user او او عملت Delegate Control على Shared Folder | Publish

ملحوظة active directory sites and services Configuration partition دفع Console دفع Default Site لفتحها هنالك Renew also admin tools → Active directory sites → Default-First-Site Name → Site properties دفع Domain Controller دفع site هنالقي هو Global Catalog

Alex دير نسيمه دفع site

Active directory sites → Sites → New Site → Name [Alex] → OK

ملحوظة Server دفع site لكل subnets فلو لقى جهاز Site دفعها معينة Subnet

لو وقعت على اتصال schema دفع user properties دفع

Active Directory schema and **Schema** نتائج الـ Console ١١

Run → Regsitr32 schmmgmt.dll Register لغایه

Run → mmc → file → add / Remove → Active directory schema

Attributes و classes كنارتها

في DNS هو **Application** نتائج الـ Console ١١

Integrated → zone ١١ في حالة

DC و DNS ١١ Integrated ١١ بـ سرت

على نفس الـ Server

NtDS partition

1- Domain ١١ ادوات ادارة دى جي دى Domain ١١

2- Configuration

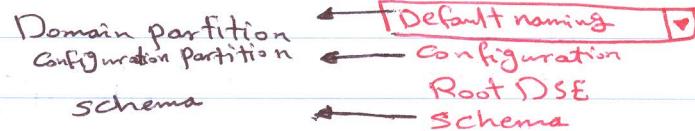
3- Schema

4- Application

} → Parent

ADSI Edit نتائج الـ Console ١١ ملحوظة

Admin tools → ADSI Edit → Connect to → Select a well known Naming



Policy لواد PDC نتائج الـ ADD DC

user ١١ no need to install

ادوات ADSI

2003

ملحوظة

CD → Support → tools → suptools.MSI → Next → Install

Run → adsiedit.msc

3) Replication

A DD DC و PDC ميں Replication Configuration partition

بینیا نہیں بلکہ Physical Connection کو Site میں اسی site میں site خاص ہے وارکر سیٹ میں subnet site وارکر PDC وارکر

PDC DNS یا کامانیلیک PDC Range میں IP یا IP میں Add DC کا مکالمہ

Run → DC promo → Use advanced mode → Next → Add DC to existing Forest

PDC میں

Add DC to existing

→ Next → Name

Alternate credential

PDC میں user pass

→ Next → Next → Select site

Subnet نہیں بلکہ Site

IP address

Cairo

Next → DNS

Global Catalogue

منطقہ کے لئے site

Next →

Replicat over network

Replicat from media Hard و Hard NTDs یا USB → Next

Replicate over the network → Use specific domain Controller

PDC.abc.com

Restor mode

Next → Next → Password Confirm → Next → Reboot on completion

PDC کو دھلتے

Active directory sites → Cairo → Servers → Add DC یا PDC کو

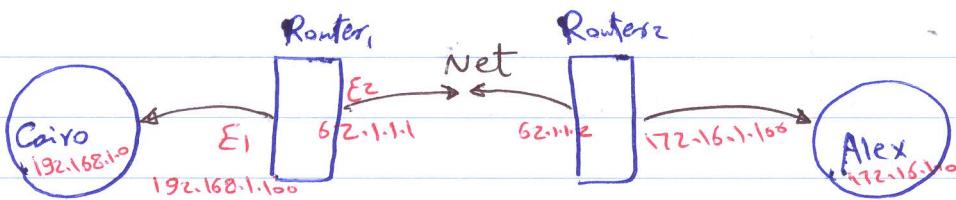
Replication بینیم یعنی منطقہ کے لئے منطقہ کے site میں یعنی اندھر فنکھا.

192.

Subject.....

Date.....

في طيام الفعلية هنالك بيه ال ② روtierين واحد واحد في site Cairo و واحد واحد في site Alex اهنا يعني عاليين نترك ال ADC في site يعني استثنائية.



Router1

CP → network and sharing Center → Change adapter setting

(E1) 192.168.1.100 (E2) 62.1.1.1 network نعمله كارته Routing and Remote

Server manager → Roles → add Role → Network Policy and access → Next →
⇒ Routing and Remote access → Install

Router2

network نعمله كارته

(E3) 62.1.1.2

(E4) 172.16.1.100

Routing and Remote

Server Alex

IP 172.16.1.200

255.255.255.0

Gateway 172.16.1.100

DNS 192.168.1.200

Server Cairo

IP 192.168.1.200

255.255.255.0

Gateway 192.168.1.100

DNS 192.168.1.200

Routing II بدي Router

رجوع

admin tools → Routing and Remote → R. → Configure and enable → Next → LAN routing
Finish

IPv4 → static Router → new static C →

Interface 62.1.1.1
Destin 172.16.1.0
mask 255.255.255.0
Gateway 62.1.1.2

Router2

static Rout

Interface 62.1.1.2
Destin 192.168.1.0
mask 255.255.255.0
Gateway 62.1.1.1

ping ip من المراوتر الثاني

4. Replication

مُلحوظة رهان بطبع في المالي Global Catalogue على windows 2003 على ADC من يسأله لازم أخر مثها أنا

admin tools → active directory sites → Tanta → servers → NTDS → properties →
global Catalogue

في طريقة لعمل Replication يمكن توضيحه هنا
sites → Inter-site transports → IP → RPC over TCP
→ SMTP → SMTP

Certificate Server التي تكون لازم تكون SMTP الفرض يستخدمها

لود خلات على قواعد Default site link IP هتلاتي وائل واتيك كل 180 minutes Replication

عنوان استخراجها لازم أصحى إلها تكون قفلت Default site link IP هتلاتي وائل واتيك القاهرة وأسكندرية

Active sites → Inter-Site transports → IP → New site link →

Name Cairo-alex

sites ② وافتادا

OK ← Add

وائل

بتقدما على Replication خاصتنا لفتحها وتغير موعد Replication كل 10 minutes من 15 minutes لـ 10 minutes

[Change schedule] بحسب انتشار ساعات العمل

apply → OK

* عمل link للقاهرة وطنطا

New site-link → Name Cairo-tanta → Add ونفتحها

Cairo-Alex ونحدد له كل ساعتين برمته بس ليكون متحدين

Alex كـ 1 خطأ يحصل في وقت غير ملحوظة

الوجهة معظم الشركات تتوصل لقرار الفوزي الرئيس لكن حتى يوصل الفوزي الفوزية بعضها مباشرةً



Alex starts Replication

يتم على مر حِلَقٍ فنكتا التَّدْبِيلاتِ سَمِعَ بِهَا بِوقْتٍ كَثِيرٍ

bridge ← Cairo دجیت تکنولوژی Site link bridge

Sites → Inter-site transports → New site link bridge →

Name tanta-Alex

دبي ٢٣ Replication ١١ Cairo وقت الراحة \rightarrow كفاحي

Alex → tanta cas

$$309 = \frac{1024}{\log_{2048}}$$

$$\text{Cost} = \frac{1024}{\log_{BW} k_B}$$

Replication (١) حل tanta , Alex من Replication (٢) *

Cost الباقي من Alex من الأول و tant من الأول .

Replicate Now و صيغت PDC على الوجهات ملحوظة

- Sites → Servers → PDC → NTDS setting → Right click → Replicate Now
هي نفس الوقت Replication جارٍ

Replicate Tanta and Cairo من ADC و PDCapb نباتاتي

Satellite

جـ الـيـ هـمـمـعـيـدـهـ وـلـرـفـهـ آـهـ

Cairo → Servers → **POC** → properties → Ip → **Add** → Apply → **ok**

"5" Replication ③

KCC

اتمام Replications Protocol ॥ ملحوظة

* Replication ي يتم في نفس الوقت بين ADC و PDC .
لكونها في نفس الـ Site

لو عملت user في domain ADC أو PDC أو جهاز Join في نفس الوقت
هسيتم في المقام الثاني . كذا بعده و بعد Replication
Domain Partition ॥ PDC or user ديناع Properties
* لو عدلت في Schema يعني الـ Replication يتم على الـ ADC

* ADC هي مركبة من PDC و عاملات site
و عاملات subnet هي مركبة من ADC و عاملات Configuration
و كذا ॥ Replication ي يتم في Configuration

* عمان Application يستعمل في الـ Replication يعني في DNS
• لازم ذكره ستعالين على Integrated zone

* لو عدلت حماية في Domain DNS هي ملحوظة في DNS

"6" IFM

* عايزين نعمل Replication لـ ADC media طريق



دبي يستعمل على Cmd فقط

C:\>ntdsutil

ntdsutil: ifm

ntdsutil: Activate instance ntds

نعملها

ntdsutil: ifm

ifm: ?

هيسطلع اهتمامات

Create Full %S Policies NTDS نحتاج الى

Create RoDC %S

Create Sysvol Full %S Policies NTDS نحتاج الى

Create Sysvol RoDC %S Readonly NTDS قاعدة NTDS

ifm: Create Full e:\IFM

وهي فضل بحمل طبعان خلوص

لو وقعت الى folder اللي اخوتة احفة ها عليه هتلافق ②

① Active directory

② registry

عن هتلافقه واحد

ifm: Create sysvol Full e:\NTDS

لود فلت على الغول، هتلافق فيه 2 حوالات

③ Active directory

② registry

③ sysvol

فاتح بقى الغول، اللي العقل ونحطه على فلاشة أو هارد

ADC واحظ على

ADC نباً سحب ال

Run → DCPromo → Next → Next → Existing Forest

Domain name

④ Add DC to exist.

→ Next → Name Credential → Next → Next →
 Site, location → DNS Global Catalog → Next → ⑤ Replicate over network
 ⑥ Replicate over media

④ Replicate From media

location [Browse]

لختار ال DC PDC.abc.Com

Replicate من Password Confirm

* دى هحتاجها للباقي عايز نعمل في مساعدة - Ibm 2003 دى مكتبة في يقع بداخلها في

ADC لو دخلت على

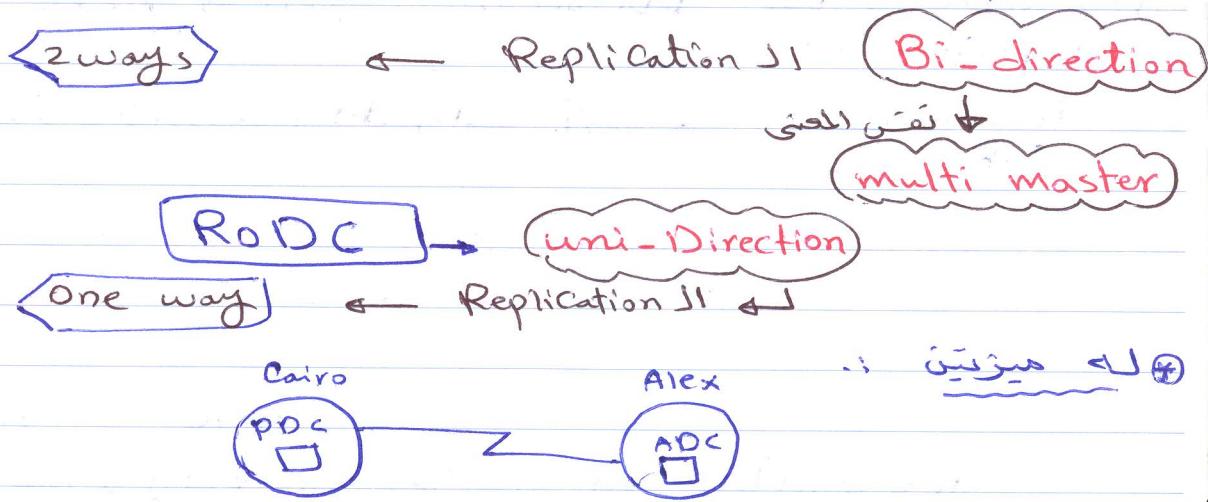
Active directory users → PDC هذان كل ما فيه من

Active directory Site → ↙

Active directory Schema → ↘

⑤ لو عملت اد حاجه في ADC هذان فيها التعولت في PDC برضه

"7" R o D C 2008
"Read only Domain Controller"



- الاجهزه لها اصدار authentication من نوع Alex وهي تعرف الادمن
- يجل او حاجه في اطهار 11AD NDS من تعرف بجمل منها موجه
- دخوله لا users الى يجعل Cache لبيه.
- لو خصل او مشكلة في الماين Add Domain Controller او Reset users والرول Password

ڪسٽان محل RODC لار ۾ من توا فر ③ مشروط :

2008R2 si Win Server 2008 -

2003, 2008, 2008 Re Forest Functional Level - 2

2003, 2008, 2008 Re Domain functional level -3

التطبيق العملي

الجامعة و Aswan Server, Cairo Server على الـ bus-1

- Cairo Server (de P1 Domain) 15

Aswan Server میں تکمیل - ۵

Run → DC promos → Next → Ⓛ Existing Forest

④ Add domain to existing domain

→ Next → Name Credential → next

دی مشکلہ لانی کا امکنہ رہی اک helpdisk اسوناں اور user Pass بتخ

→ Next → DNS

Global Catalog

(ملحوظة هامة)

⇒ Domain Functional level → Assign □ Readonly

~~Server manager~~ → Active directory users and Computer → abc.com →
Raise domain Functional level → Select functional level [2003] [10]

~~Server~~ admin tools → Active directory Domains and trusts →

Raise Forest Functional level → Select Functional Level 2003

☒ Read only domain هنلائمي الفتح ADC في تكميل من

→ Next → Specify Password Replication Policy المفتاح Group

Groups or user Set → Next → ⚡ Replicat over network

→ Next → Use specific DC

PDC.abc.com

→ Next → Next → Pass Confirm → Next → Finish

مسكلاة الطريقة دي إانك لارمى ندى لل pass

مروع لـ PDC وستعمل بالطريقة دي حل المسئللة

admin tools → Active directory users and Computers → abc.com → Domain Controllers

→ Pre-Create Read only Domain Controller account → Next → Next

→ ① My Current logon Credentials → Next → ComputerName

Mount Site B C D E F G H I J K L M N P Q R S T U V W X Y Z

→ Next → Site(s), as Aswan → Next → Global Catalogue → Next →

all group او users لختار add Next → رو الباقي domain بعمل finish → Next → finish

لهم طبّعْتَكْ عَلَيْنِ On وَهُوَ أَهْمَنْ ^{con't}

جامعة أسوان

cmd و دستور RDC - درایو

```
C:\> depromo /useexistingaccount:attach
```

البيانات الخامسة: installation || Interface || delete || add || view

→ Next → Name [abc123] → Use ultrnat credent user aswan-aswin Pass

→ Next → Next → ⚡ Replicate over network → ok

→ Next → Pass Continue → Next → Finish

logon Restart خلصه هيجل RoDC بعد ما ادأ روادرم بعده user pass



switchuser هجتار

uni-Directional هيكلة RoDC Server لوجو *

Active directory users and Computers RoDC → Properties → Connection
uni-direction \leftarrow From PDC to uni-direction

Groups خرى يرجع سهل
المهمة

Gp management → Domain Controllers → Default Domain Controller

Edit → Default → Computer Configuration Policies → Windows Setting

Security setting → Local policies → Security options → User right

assignment → Allow logon locally → account operators
administrators
Backup operators
Print operators
Server operators

RoDC لوعايز دينه بدل DC نصيحت Adduser

* لو دخلت على RoDC وسُوقنا Active directory users and Computer

Domain partition لكن من هى عرض بعض ذي صلاحيه عليها

* لكن هو ايعنى بعنوان IP ديناع DNS او RoDC مع العالم DISKmanagement و Device manager لكن من هى عرض بعض ذي صلاحيه

Configuration لو دخل على

admin tools → Active directory sites → درجه هىستوي كلام لكن من هى عرض بعض ذي صلاحيه

Schema و CNS

مانع DNS بتعالج التغييرات Application

Secondary zone

المحظوظة لونا تحتاج انه يجعل اى مهامه على الـ NtDS يعني اطلب اذن له
لأنك أصلًا عامل او user او في delegation تعلم On

لتفعل على On سطعنه وتحل Delegate Control
Next → Add → aswanadmin → Next → Create, delete and manage user

ذكر 1 هو اهيعرف بجعل كل مهامه في الـ On الى ما عليه
Delegation

Active directory users → Domain Controllers → RoDC → Properties →

Password Replication Policy **كلمات المرور التي تنسخ**

RoDC التي يحتوي على Passwords

هذا من اول user الذي كتبت عاملاته ومتى يستطيها

PDC

On

المحظوظة

Prestonate passwords ← Advanced **تصفح على**

user (اسم) → CheckNone **لعمات اعلى** **المحظوظة**

user (اسم) → OK **ادخل حروف** **لا** **اعدل حروف**

Prepopulatepass **وغير** **Add** **اعمله**

لو اد ادخل على Domain ادخل على PDC وفعلاً اسيب ذكر ا هعرف ادخل على الجهاز

خصوصاً في قماع اسوانه من طريقة اى صناعة فيه في الـ Cache بالمرصاد ، لبيته

RoDC **لعمات اعلى** authentication **ستم عن طريقة**

Domain controller هو وصول للDomain **لوكستي مع ادب**
ما طريقة هي؟

المحظوظة لو حصلت على Maek! **لوكستي** **لوكستي** **لوكستي**

Active directory users and computers → Domain Controllers → RoDC → Delete →

Reset password users

Reset Password Computer

Export

Browse

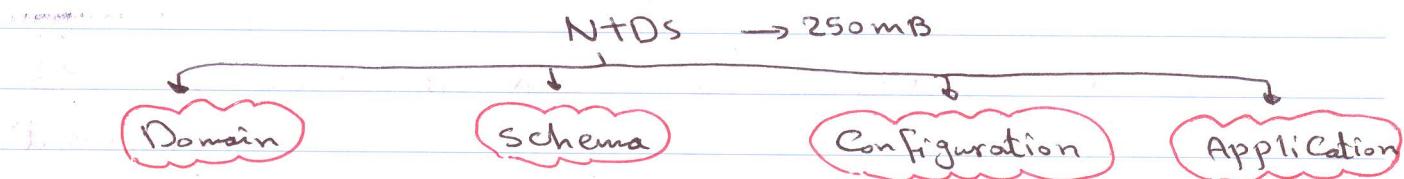
كل الذي عندك **الى محظوظة**

ذكر 1 من على RoDC من هجري يدخل على Admin tools ولا يرى اى مهام

فقط **لا** **طريق** **لوكستي**

"8" Operation Masters"FSOM" Flexibility single operation master

ما يحفلن ADC لوجود PDC يطبق Rules 5 على Rule يدار دى.



* لا يعلم ADC ويتنقل Partitions ④ لـ PDC ويتبع Rules 5 على Rule يدار دى.

S Rules Operation masters for PDC

① Domain naming master Rule. يتابع Name check في services

لـ add unique child Rule في tree أو child Rule في forest.

② Schema master Rule

→ Forest master

يتحقق منExtend Schema لـ Schema objects من forest.

③ RID master Rule

→ Domain master

يتحقق من tickets in pool لـ PDC يتحقق من user ID.

④ PDC emulates Rule

مسؤولة عن GP (Policy) التي من خلالها يتم تطبيق policies على Client (SMBclient).

الثانية (2) المسؤولة عن synchronization between Client (Nonmicro) and Server (Micro).

⑤ Infra structure master Rule.

الثالثة (3) المسؤولة عن permission user على بناء التغريد upgrade.

ملحوظة

- Forest master Rule (الـ PDC أول دولة ينبع لهم)
- Domain master Rule (الـ PDC في كل دولة ينبع لهم)

C:\> netdom query fsmo ← Rule من ينبع بالـ PDC

- * لو عندك ADC وعاليه خلية PDC أولاً، انتي أقدر الـ PDC
- PDC هيتتحول لـ ADC

التطبيق العالمي

PDC شغال

في حالة الـ PDC

- 1- نزوح PDC وتدخل على

admin tools → Active Directory Domains and trusts →

active directory Domains and trusts → Right Click → Change active directory DC

→ ADC.abc.com Add (أختار) → OK

نقطة تأثيرها Active directory DC → Right Click → Operation master →

Domain naming operation master

PDC-ABC-Com
to transfer Domains
ADC-ABC-Com

Change

نقطة تأثيرها

ADC الـ PDC

Domain naming master Rule ← Rule أول دوّي

▪ Schema

▪ نزوح للـ Schema

Run → regsvr32 schmmgmt.dll

ازم تدخلها طبعاً أول Register

▪ نزوح لفتح الـ MMC

Active directory Schema [Add]

وندخل

▪ admin tool → Active directory Schema

وتعدين نزوح عليها

▪ Change Active directory DC → Add ونختار الـ ADC

▪ Active Directory Schema → Operation master → [Change]

Schema master Rule

بـ كـ دـ قـ تـ كـ تـ

▪ نزوح للـ Active directory users

admin tools → Active directory users and Computer → ABC.com → Right click

Change Active directory DC → Add (أختار) →

- Active directory users → abc.com → Right click → Operation masters → RID PDC infrastructure

لائق على كل واحدة دليل Rule لـ Change بيتاعتها

PDC لـ AD DC وـ ⑤ Rules نقلها

* طريقة الثانية لـ PDC اصلاً وقع لوقفتها AD
هتنتقل الـ Rules لا ADC من طريق CmD

ADC نقل على *

CmD →

c:\> ntdsutil

ntdsutil: roles

fsmo maintenance: Connections

Server Connections: set creds administrator abc administrator 123

Server Connections: Connect to server adc-abc.com

Server Connections: Quit

fsmo maintenance: Seize naming master

fsmo maintenance: ?

Rule اينقل اول وتحتاد Interface face

transfer كل اوامر الـ



Global Catalogue يكون ADC في زر

Active directory sites → Default Site-Name → servers → ADC → NTDS
Properties → Global Catalog → OK

* استخدم الـ PDC هيلم الـ seize

الفرق بين seize و transfer من الـ PDC

بـ seize الـ PDC يكتسب سلوك transfer.

يكون المعنون الـ PDC لا seize

DC Rules ارجح PDC و لـ GRS

C:\>ntdsutil

~~ntdsutil:roles~~

Fsmo Connection: Connections

ServerConnections: Connect to Server pdc.abc.com

ServerConnections: quit

Fsmo maintenance: transfer RID master

Yes

RID master lies, ↳
Rule

Domain جسر Forest جسر ایجاد

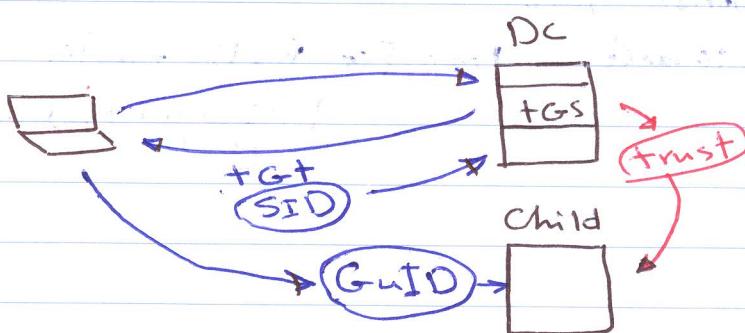
C:\>nlttest /dsgetdc:Site.Com



"g" Child

١١ Child له خصائص :

- ١- يورث الاسم بتابع ال Parent
 - ٢- يكون فيه trust بينه وبين ال Parent
 - ٣- تراث من كل Parent
- (transitive inheritance)



لتحقيق التحول من Domain على مستوى ال access لـ Forest على مستوى ال access

Child لـ Parent لم ينفذه user على مستوى ال access
يُتغير ال SID لأنَّه ينافذه من ال Child أولاً ثمَّ في Forest ثانية على مستوى ال access

- ١- Child من win2003 كان محدوداً بـ DNS خاصته بـ site وـ delegation.
- ٢- Parent : محدوداً بـ DNS يعتمد على بتابع ال site.
- ٣- win2008 أصبح نوع وادره child لـ win2008 خاصته بـ site.

التطبيق العملي

- ١- نعمل Domain Controller على جهاز Server بالطريقة العادي.
- ٢- ندخل على Parent site ونعمل active directory sites.
- ٣- ندخل على Subnet بتابعه.
- ٤- ندخل على child ونعمل لـ child رادر على child.
- ٥- ندخل على IT site ونعمل user لـ create user.
- ٦- ندخل على HR site ونعمل user لـ Active directory users.

Parent ॥ سرطان Child ॥ سرطان Server; لوحات IP نزدیکی
Range of IP & child using domain naming Rule چنانچه
نحوی اینکه child یا site ۱۱
نحوی اینکه child یا site ۱۱

و نهایتی مع اطمینان DC promo & child ۱۱ نزدیکی ۱۱

④ Existing Forest

○ Add domain Controller to existing domain.

○ Create new Domain in Existing Forest. ← Child

□ Create a new domain tree root instead of Child domain tree

→ Next →
Forest

Domain Name [abc.com]

○ Credentials [Set] user Pass > Enterprise admin
(Parent admin)

→ Next →

FQDN : ABC.com

Browse

Child Parent singable DNS

Cairo

→ Next

Domain NetBIOS Name [Cairo] → Next

Domain Functional Level []

→ Next → site []

→ Next → DNS Server

Global Catalog

→ Next → ○ Use Specific PDC
(PDC-ABC.com)

Next → Next → Pass []

→ Next → Reboot on Completion

Restart ← يجيء

لابقنه ۱۱ DNS ۱۱ child ۱۱ لودمیں اسی کیا ۱۱

Schema Active directory users or
Parent ۱۱ قائم نہیں ۱۱ active directory sites ۱۱

trust structures, Parent up لور لایبل

admin tools → active directory domains and trusts → ABC.com →

○ Cairo.abc.com ایجاد

trusts

← ABC.com بحث Properties ۱۱ up لور

Cairo.abc.com

ایجاد ۱۱

209

لهم على الـ Printer I share نعمل Parent

- Start** → Devices and printer → **Add printer** → Add local printer →
 • use existing port **HP** → Next → اختيار نوعها → Next
 → Next → **Share this printer**
- sharename: **HP 910**
 location: **Main office** → Next → Finish

Sharing وختار **Properties** لفتق على **Printer** **локейشن**
 ☐ List in directory → OK

Child دل Join

عن تاجها: نعمل

192.168.1.1 IP دليل

Child DNS ساع 192.168.1.201 DNS

Child ساع DNS 192.168.1.202

DNS 192.168.1.201

Alternate 192.168.1.200

parent ساع

نرجع للجهاز الذي نعمله

- Domain **Cairo.abc.Com** → OK → user **[]** → OK
 → Pass **[]** → OK
 [Restart]

abc.Com طهرا: يفتح هنا التي على تأثيرها ولها

ملحوظة

abc.Com لـ user, pass لـ دليل اديله ← **abc.Com** لـ امنية

Cairo.abc.Com لـ user, pass لـ دليل اديله ← **Cairo.abc.Com** لـ امنية

لـ دليل اديله join Cairo and user

- Start** → Printers and Fax → Add printer → Next → Network printer →
 Next → Find printer in directory → Next → Name **HP** (**FindNow**)
 Share place abc → domain الـ Parent printer الـ مسحوق

Parent الـ Printer: من **Properties** بـ ساع

Forest على الـ Everyone security لـ دليلها يفتحها من جرمه الـ Parent Domain الـ authenticated user

لوحة التحكم \rightarrow sharing \rightarrow Advanced Share \rightarrow Share this folder \rightarrow Permissions \rightarrow Remove everyone, add administrator, full control \rightarrow advanced \rightarrow Find \rightarrow هيسبيلا ABC الموقودة \rightarrow location، يمكن اختيار Parent or Child \rightarrow Cairo.abc.com (أقليها) واصناعه Child if no user واحداً، يفتح على Child if user exists على \rightarrow Run (NFS) لو سنت

SID Pass لا يعلم من غير ما يطلب Shared Folder
من شكله GID \rightarrow شكله GID لفتحه على دخلاتonline

Win 2003 في Parent if Range no IP و Parent if DNS if not (*)

DC Promote \rightarrow Child Domain \rightarrow Next \rightarrow user Pass \rightarrow Next \rightarrow
Parent Domain \rightarrow Browse Child Domain \rightarrow Next \rightarrow Next \rightarrow Next
 Permission Compatible 2000
 Permission Compatible 2000, 2003 \rightarrow Next \rightarrow Restor Pass \rightarrow Confirm \rightarrow Next \rightarrow without Delegation \leftarrow Child is not

Parent is not yet in DNS. حتى لو (with Delegation) لفتح على

DNS \rightarrow ABC.Com \rightarrow Right click \rightarrow New Delegation \rightarrow Next

Delegated Domain (Alex) \rightarrow Next \rightarrow Add IP \rightarrow DN Resolve \rightarrow Next \rightarrow Finish \rightarrow child also will server N

لفتح على child المطلوبات التي تملكها child ولذلك كل المطلوبات

install DNS Server \rightarrow Next

DNS نجحت

في نهاية العملية المفتوحة من DNS بناءً على Child

DNS → Forward lookup zone → New Zone → Secondary → Next →

Zone name [Cairo.abc.com] → Next → IP [192.168.1.20] → Next → finish

نهاية الـ Child

نهاية Child

DNS → Cairo.abc.Com → properties → [Zone transfer]

Allow zone transfer to any server → OK

نهاية Parent

Cairo.abc.Com → transfer from master → refresh

نهاية Parent ، طريقة اهتمام ، موضوع

كمان نعمل هنا Child نفس الكار

New Zone → [abc.com] ونكميل زى السابقة

Parent نعرف نعمل Cairo .
Child الموجود فى Cairo بناءً على DNS بناءً

ممكن طرق تابع لفترة على DNS

Child → Forwarders → Edit → [192.168.1.20] → بناءً على DNS Child
بن كلها بتصدر وقت سوية

ملحوظة

+ مفهوم الـ Alternate DNS الواقع بـ Redhints ولكن الـ forwarders

"10" Tree

trust (tree Root) (transitive)
↓
Parent

domain من يورى اسم ال tree 1, مخطوطة

Ex: Parent ABC.Com

tree Cib.Com

*.Cib.Com trust

Child دكى فقط من tree ال Parent يعمر مخطوطة من أي حاجة.

2003 DNS tree ال ينزله اتصال به سواء 2008 او *

Parent data Access users يفتح tree درجه ليرفوا يجلوا *
عن طريق GUID

Schema وال Configuration ببورث tree ال *

أهمية tree ال لفتح في تأثير الشركة باسم تأثير

"المطلب العملي"

لما زنا سطح ومحترس ال من صلاحي

Existing Forest

Create anew domain in existing Forest.

Create anew domain tree root instead of child.

→ Next → Name Domain Credentials Set enterprise admin

→ Next → (FQDN) tree Cib.Com tree ال

→ Next → Next → Domain Functional level → site ال → Next

→ DNS Server.

Global Catalogue. → Next → Use Specific domain dc=abc.com

→ Next → Next → Confirm Pass Restore → Next →

Restart دخول

- ندخل مهار join parent ونعمل لاجي اعمر logo هنلاجي الميزات تدخل على trust وهي هيحصل اطهارات اللي بينه وبينها

طعاماً على tree لفتح لازم نضج الـ Zone

DNS → Forward lookup Zone → NewZone → Secondary Zone → Next
→ Zone name abc.com → Next → IP 192.168.1.200 → Parent → Next →

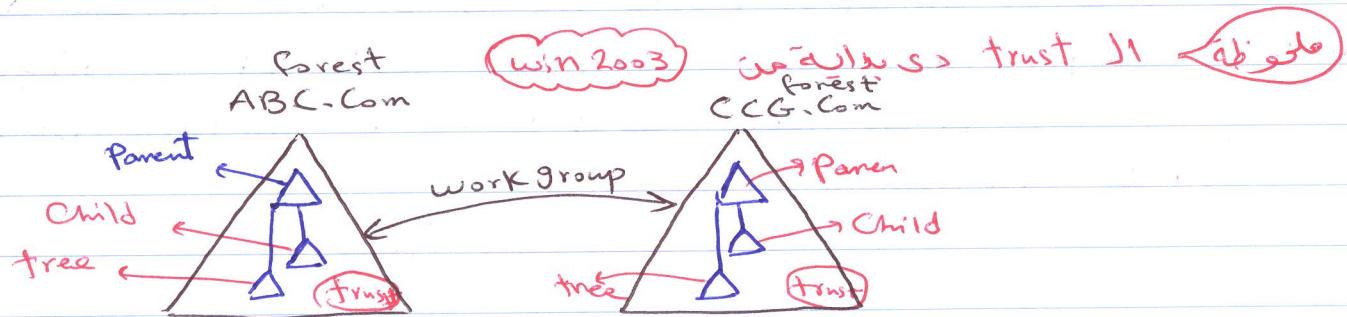
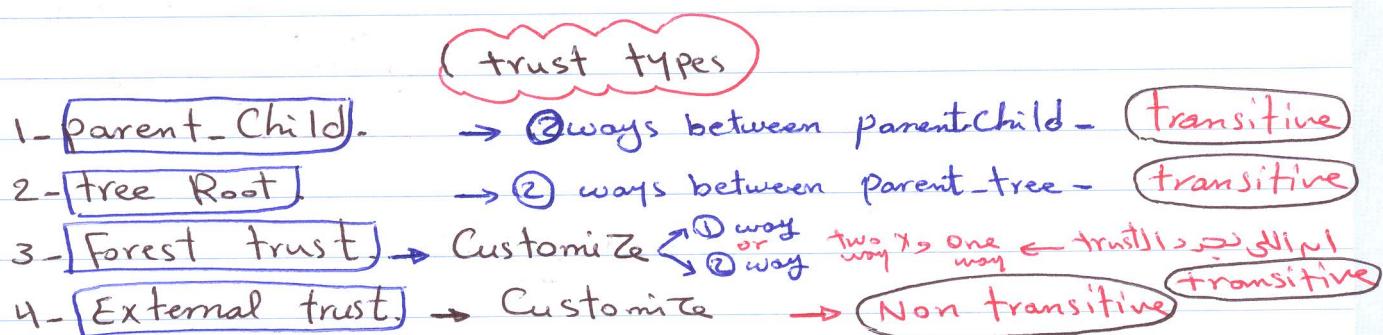
Allow zone transfer ← Parent will always

Dns dns Parent نگزید
tree N Zone ایجاد

trust in "كُوكو" parenting tree if we trust group 
tree if we trust in public child his parent if we
- Child وال

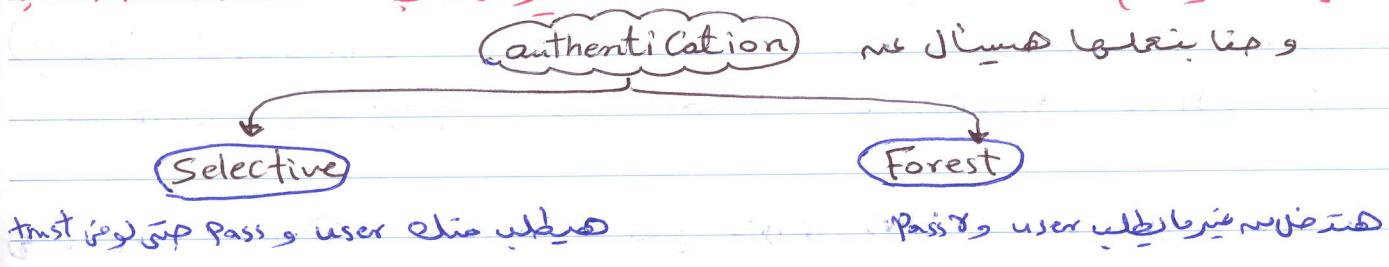
الرسوم بيورى  **Child tree** و **parent tree**  **Root tree**

11. New Forest & trust



5

لأنها تتحقق في forest الابن يثق Parent في forest الأم



tree II access يحاور يصل abc.com II tree II all مجموعات
وـ (trust) كل حره يتم
External trust عن طريق Parent لـ child ما يكرر سوافت افتر عن
عن طريق II tree II كل tree II الثاني على طلبه بعد عاربط

• Parent II
External trust في
Pass user كذا هيلطلب منه *

المطلب الثاني

① حماية Server و راهنها نفس
Routers لكن طبعاً من طبعة لعمليه يكون واحد بينهم IP II Range
Domain & New forest داخل

② Create new domain in newforest.

وتحصل الخطوات على صيغة

tree II Child سواء كان Forest II Domain في كل ما يطلب

Domain II Zone II DNS II التالية

Child II Zone و Parent II Zone مثل tree II

- Zone ما يطلب trust مع

وكان لوصي Newforest trust
Second Zone trust

مجمع اثنين Domain بينها وبين

- Forest وهي

CCG.com لوصي ما يطلب abc.com Join

Forest trust معها II لـ CCG.com

user Pass

وـ (trust)

NewZone DNS يفتح بعد في CCG.com Domain II

ABC.com في II Forest Domain لكل

abc.com و CCG.Com يتابع Parent
 admin tools → active directory Domains trust
 Domains and Services → trusts →

New trust → Next → Domainname abc.com → Next →
 trust over domain

- ④ External trust
- ④ Forest trust → Next → ④ two ways → Next →
 يتابع الشركة整體
 this domain Only Enterprise Pass يتابعها

Both domain and Specific domain
 تكون عارف بالببورد يتابعها Forest التي قد تختلف

- Next → ④ Forest-wide authentication pass user
 من هيكلها ولا يهم
 ④ Selective authentication user pass user
 هيكلها ولا يهم trust

- Next →
 ④ Forest-wide authentication
 من هيكلها ولا يهم
 ④ Selective authentication
 هيكلها ولا يهم forest

→ Next →
 ④ Forest-wide authentication
 من هيكلها ولا يهم

④ Selective authentication
 هيكلها ولا يهم

→ Next →
 ④ Forest-wide authentication
 من هيكلها ولا يهم

④ Selective authentication
 هيكلها ولا يهم

tree من الـ

→ Next → abc.com → Next → Next

لعين من على test فيه
 دلوونت
 ONo, dont Confirm incoming

→ Next → Finish.

*.abc.com هيكلها من النهاية الى المقدمة هي
 * CCG.Com هيكلها من المقدمة الى النهاية

ABC.com يتابع active directory domain and trust ← لو قفت

رجلاً لورقت لـ Domain هي لا

192.168.1.203 IP يتابع CCG.Com ← وفتح هيكله share folder

لـ trust

Active directory domain and trusts → trusts → CCG.Com → Remove
 هل فيها من لا
 ④ Yes, remove trust from both user [] → OK

[CCG.Com] → Remove → ④ Yes, remove → OK

Chane Folder ڪارڈ نڪو ۽ trust لامساوا ملحوظہ

- Pass \rightarrow user

External trust خارجی میانہ

active directory Domains and trusts → trusts → New trust → Next
Name Cib.com → Next → ① two way

Name Cib.com → Next → ○ two way
tree ↗ ↘

External to forest (outside) من خارج الغابة لاحظ

- forest ॥ no deer or tree ॥ time in life

→ @both domain → user pass → Next →

④ Domain-wide authentication → Next →

④ Domain-wide authentication → Next →

④ No, don't Confirm - → Next →

لوجات من CCG.COM

→ Active Directory Sites and Trust → CIB.Com → Properties
→ **Trusts** → CIB.Com (selected) Type: **External**

لورمیت کرے (tree) Cib.Com ne اسی طبقے کے میں Share بنائیں گے CC0.Com میں فتح کرنے والے Child وala جسے Parent کہا جاتا ہے

Forest
trust

www.abc.com مع Newtrust Jet class

"12" Groups

Group type



accept all resources

يتيح لها جميع الموارد وينفع بـ Radio
تعتبر على أنها رسائل بـ Group Type
رسالة يمكن تحميلها Check
رسالة كل الناس whom belong to group



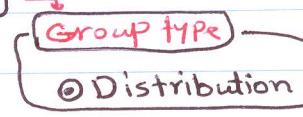
For mail Only

يمكن نفعها على كل الناس
من سهل Check
ولأنها تجاه الجميع يتلقون البريد

التطبيق العملي

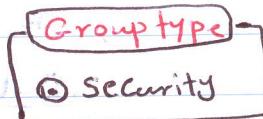
1- active directory users and Comp → New OU → Name **IT**.

IT → New → Group → Group name **IT-D**



عمل جروب ثان

IT → New → Group → Group name **IT-S**



Folder | Share

Data → Properties → Sharing → Share this Folder

Advanced sharing

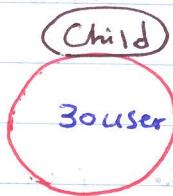
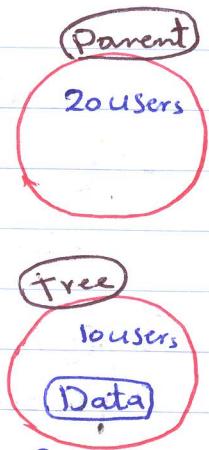
Permissions → **Add** → **Advanced** → Find now →

IT-Security principle ونطويات ونفعها

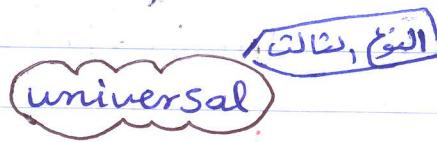
Distributed ← **IT-D** ليس من هيظهر

Permissions, Security من هيتحقق اجل عليها Distributed لا

Group Scope		
Global	Domain Local	Universal
members accept member from it's Domain Only	accept members From it's Domain and all trusted Domain	
Resources accept Resources From it's Domain and all trusted Domain	accept Resources From it's Domain Only	



لوكيز اعلى فيها كل دول users الـ group ويعرفوا بـ hims وaccept members From it's Domain and all trusted Domain



members:

accept members From it's Domain and all trusted Domain

Resources

accept resources From it's Domain and all trusted Domain

at least 2003 → Forest \rightarrow Domain Functional Level \rightarrow universal \rightarrow Rights

Global Catalogue مع الـ Integration يجعل universal !!

سلطة

لو log on Global Catalogue و تعمد عرض ليهل !!
 لذا انما user لا يدخل Global Catalogue !! log on
 group member > user !! user !! NC universal Group

↓ Domain Site في اى ملحوظة لا زم يكون موجود في كل Global Catalogue.

التطبيق العملي

1- لفقي على Parent Domain
 Active directory users and groups → IT → Newgroup →

Name Sales-G

Group Scope

Global

→ OK

→ members → Add → From this location ABC.com
 global من هنا ناخذ ABC.com من هنا location

2- لوقتنا على Child و مثلاً Folder

Data → properties → Sharing → Advanced setting → Share folder

Permissions → Add → Location ABC.com جهازها → trusted
 Cairo.abc.com

advanced → Find now → Sales-G هنالق

member no accept المكان الذي لا يقبل المكان accept global domain

Domain local ← group → Domain local لوركتا

IT → Newgroup → Name Sales-D
 members → Add → Location ABC.com
 trusted Domain Cib.com CCGI.com → OK

لوحة إدارة الموارد (Resource Manager) | شهادة Microsoft Certified Trainer (MCT)

Data → properties → Sharing → Share this Folder → Permission

→ Add → Location [abc.com] → sales-G

لـ Local Domain user بـ Local User sales-G مـ Group

New group → Group scope
Universal

Name [Sales-U]

Share the folder | List Child | Find now

Sales-G و Sales-U ← group child | Shane Permission

Full Control

وهي التي تمنح access لـ user | Shane Folder

Nesting | عناية

لوحة إدارة الموارد (Resource Manager) | شهادة Microsoft Certified Trainer (MCT)

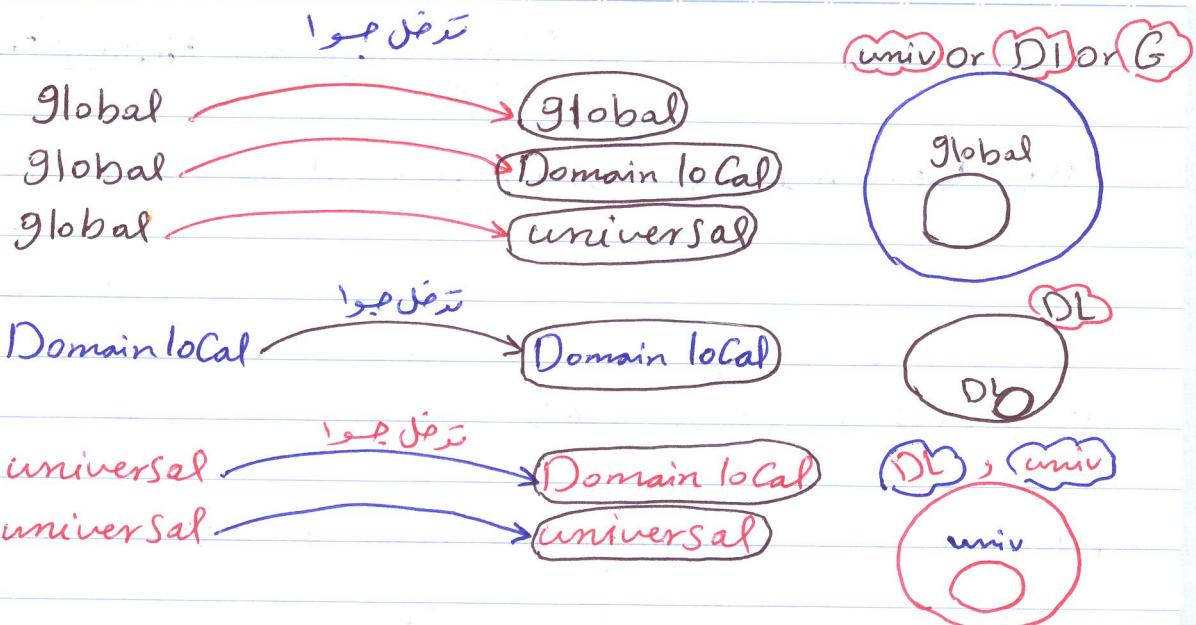
Global Distribution | نعم | Global

Domain local
global

Global | نعم | Domain local
global | نعم | universal

Group | member of | فقط على طرفي التطبيق

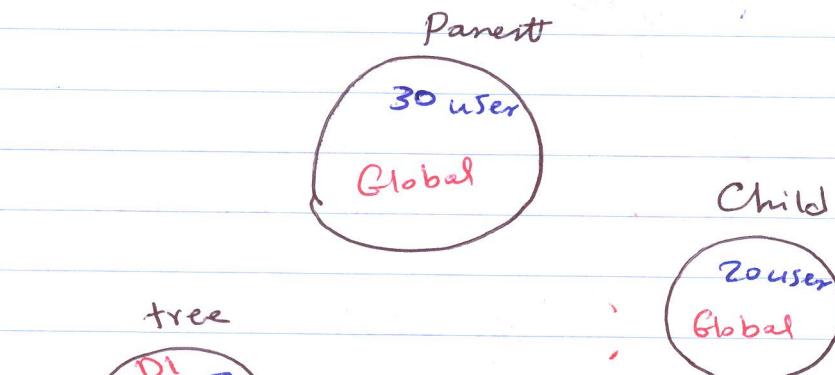
التي غيرت مثلاً جهازاً



advanced → member of group نَفْعُ عَلَى ذَلِكِ وَكَثِيرٌ مُحْكَمٌ

اطرفة دی بتعریف بدل عا اپنیا ایکیا users والد واحد دھینیا groups دھواد

اگر group بسِ الکبیرہ



وامنیتی tree می DL

user حمل کیا access کیا

data لے المزیدہ اگلے

users داحد و امداد

او

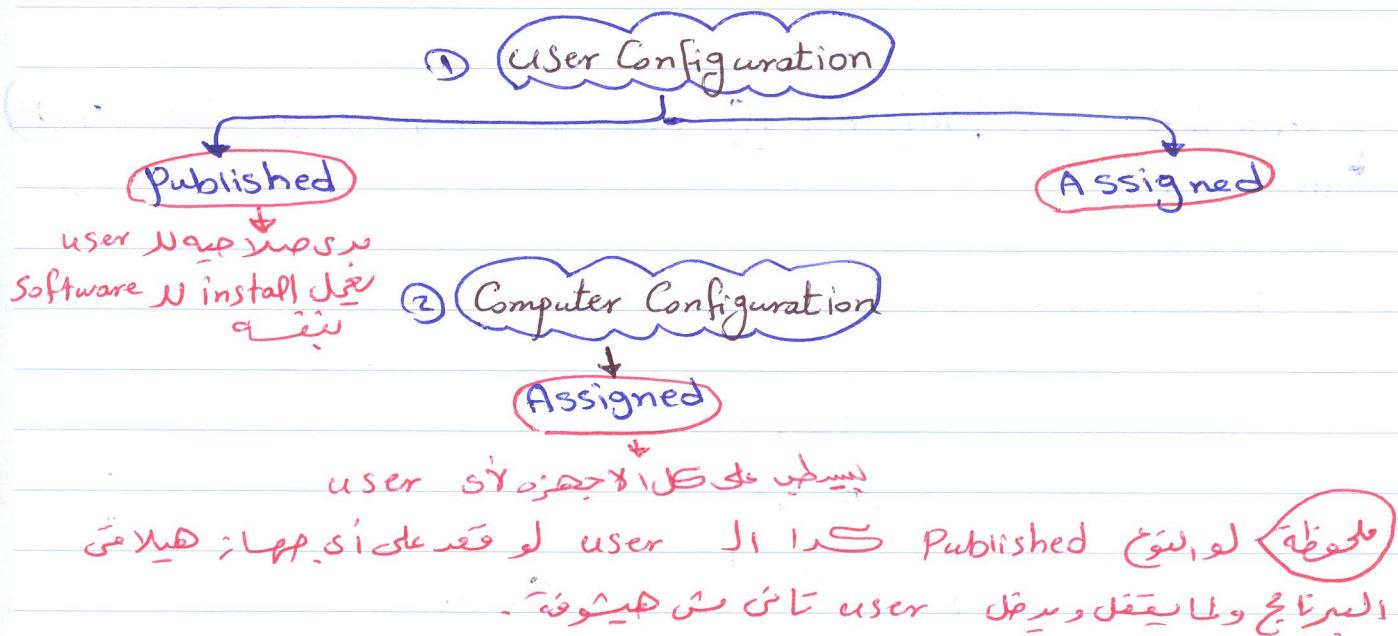
group ② ہے وابط جو ای tree می Domain local ہے
- global ہے

113 Deploy Software by group policy

113 Domain software لوشنی عایزانزلم على الاجهزه المحمول

- Shared لازم يكون ملف Shared
- .msi أو .zip لازم يكون الملفات المحمولة

يمكن اسليم ملف Software على حسابات user Configuration



التطبيق العالمي

1- نعمل On جبده في ال Domain و نعمل فيها

admin tools → gp management → Domains → IT → Creategpo → ..

Name [Deploysoft]

Source Start [] → ok

Deploy Soft → Edit → user Config → policies → Software Setting →

[] Software → New → Package → (كتابات zip / .msi) (يتحمل الملفات)

Lazarus اصلها تكون عاملة الأول وللاختيار (ملحوظة)

مكانة اجياء هي ورقة وارقة my Computer من network

⊗ نکمل می‌آد ۹p بعد مانند رسانه دستار

- لواهتممتها يعني اذا user (مستخدمها) يفتقده
عن على خارجه → **OK**

تَعْلِمُهُ عَسَاهُ تَجْرِيُّ النَّوْمَ الْثَّانِي

Policies → Software setting → software installation → Microsoft office →

Remove →

- ① immediately uninstall Software from users and Computer
- ② Allow users to Continue to use Software, prevent new install

→ OK

لواترنا، لتوح، لئام

New package → **OASSigned** → OK

٠- نزع المخواز Client II

لود فایل Microsoft office کیا ہے مستحبہ

لَا يَعْلَمُهُمْ هُوَ أَبْرَصُهُمْ مِنْ يَأْكُلُونَ حَتَّىٰ يُطْبَقَ طَنَزُهُ هُنَّ عِلْمٌ بِنَفْسِهِ .

* المفروض بين الـ ٦٦ و ٦٧ Published Assigned : بین ۶۷ و ۶۶ مفروض

Published → ينبع من CP او يكتب Software للـ user JI
Assigned → ينبع من All Programs او يكتب Software للـ user JI
فاسدة ينبع من سطح عمال

نقطة ١ خلصت النوح المكان طلب بعمر على مستوى ١١ Computer Config .

Assigned to published user على مستوى 1 **608**
without modification **مُضمنة**

Microsoft office → properties → modifications → **عند تحرير بعد حماية**

يمكن اقتبس البرنامج

Policies → Software setting → Software installation → properties →
Categories → add → Category **[Anti-Spam]** → OK

Categories → Properties ← Microsoft Office الذى عنده **Software** نزول
OK ← apply ← select للقسم جنابه .

add/Remove program → Cp دخل من عنده لوقت Client دخل
هذا في **Category** و يتفق بختار القسم الذى هيبيت حبوه .

Published ← Assigned ← **[Advanced]** و مصوّرها **modification** ← **Computer Configuration** ← **ذى دخل على**
ـ **تحمية تفاصيل** ← **لوعاين العمل** ← **تحمية** ← **ذى دخل على**

يمكن اغلاق **Software** → upgrade **تحفظ**

Properties على **Policy** **تحفظ** ، طبقة **Software** **Policy** **تحفظ**

[add] ← upgrades ← Software installation **فتح**
↓ **[Browse]** → Policy **فتح** → **Uninstall existing packages** → OK

Properties → **Deployment** → Deployment options

Auto install by file extension Serial activate → install **فتح**

Uninstall application when it falls out of Scope management

Software → uninstall **فتح** Policy **فتح** On **الى على** **الى** **user** **لواز**

Don't display packages in add/Remove programs →

install **فتح** **غير المغادرة**

Basic

بيانات توجيه الموجة يستقبل بالرسائل

maximum

بيانات توجيه كل يوم مرادمه ورد

traffic **فتح**

advanced

- ☒ Make 32x86 app
 - ☒ Ignore language

٦٤ → ٣٢ لـ هـ

سُنْهُ يَقِنُونَ بِهِ اللَّهُمَّ إِنَّا نَزَّلْنَاهُ بِرِبِّهَا

Computer Configuration

نذھل علی *

* هیچ نوع داده‌ای در یک Software نباید مستحب باشد اما Assigned و Assigned User می‌توانند مستحب باشند.

طبعاً دى هنڌيڪھا على الـ On اللى طهور جواها .

Computer Configuration → policies → Software → Software installation →
New package → Available → Assigned → OK →

لارم اجل **Lab** هنلاقيه Client لـ Restart وهو يفتح **Software** اطير لـ Install بعمل **Setup**

ل Kumon چنانچه Restart Policy تطبیق نیون نل لوماین ا د administrative templates → system → GP → gp refresh interval → ۱۰ دقیقه بعد وقت دا ۱۰ Policy

لوقت user يفتح Comp على قاعدته و جهاز او معينه Policy مبنية عليهم الى هستيقن

هيطبق عليه الآتي: ليس لـ user جي من Domain ذاتي خلاصه بـ فيه
مع الـ Domain ذاتي يعني هيطبق عليه حالـ الـ delegation
بـ لـ user يـطبق عليه الآتي

Computer Config → policies → admin templates → system → gp →
user gp loopback processing mode → merge [] Replace []
Enable Mode Merge [] (new, different)
Replace [] (existing)
[] (existing)

Subject.....

(227)

Date.....

Connect كائنات Domain no user لبياناتها بـ ID, طلب دعوة
أيضاً GUID of Object ينتمي لـ Domain أو لم ينتمي

«UPN» «user principle Name»

UPN = username @ Domain name

Ex : msarhan @ abc.com

داستنیکلہ علی ال Parent

A Sarhan & user oneq Cairo حمل Child لى لى

Ex: A Sarhan @ Cairo.abc.Com

لحوظة Exchange size ميزة لازم ادمر ال UPN عسان الناس
بتقى كلها @ abc.com عن طريقين ① عن طريق Exchange
② عن طريق DC نفسه او Parent DC

admin tools → Active directory Domains and trusts →
Active DD and T → properties → UPN suffixes

Alternative w/PN Suffixes

ABC-EG-Com

add

لقد علمنا أنها تطبق على $\text{user} \leftarrow \text{user}$ دايركتري

mSarhan → properties → **Account** → user logon name

m Sarhan

© abc.com

حُكْمَنْ نَعِيرُهَا مِنْ هَذَا

ورجته تعلمها على الـ User || Child

ليكدا لايتني تحمل logo ليكدا لايتني تحمل logo ليكدا لايتني تحمل logo

asrarhan @ ABC-EG.Com

نَّكَرْ أَوْ مِدْ يُعْرَفُ بِمِهْلَنَهُ أَذْ حَمَارَ حَمَالَ
دَى سَتَّهَا نَلَّا سَرَّ الَّتِي سَقَلَوْا مِنْ مَكَانِ لَكَاهَ.

"15" Global Catalogue

Services

- * مسئوله عمل الموارد الموجودة في ال Domain resources
- * لهذا تسمى امين المكتبه لوعدها مكتبه لوعاليز كتاب ومسئلتها أمن المكتبه هتفصل دور عليه لكن لوسائل امين المكتبه هيجهوله من الفهرس منه.

- * Exchange o Printer o Shared Folder هكى تكون resources

ملحوظة ال user ينتمي Domain ينما زن ال logon وهو يعمل GUID → SID ID
 Forest ↗ Domain ↗

- * طبعوا ال Domain ينتمي كأن واقع كذا كذا فيكون user ينتمي إلى Domain
- عامل GCache لـ TGT يتحقق بـ Domain ينتمي

أول حاجة Global Catalogue الـ logon يعلم user si ملحوظة universal groups يتحققها بتروج تسلسل الـ

هل الـ user هل الـ user يصنونها ولا لا؟

لو عندك Domain واحد والـ logon وقت من علىه حفظ دردشيف قبل

active users and group او تلعنها من هنا : لوعاليز تفعـد Global Catalogue ملحوظة
 ↳ ABC.Com → Domain Controllers → PDC → properties → NDS setting
 → Global Catalogue → OK

* لودكت على DNS ← -tcp ← Global Catalogue ← هستاري الذي يلغيه

active directory : الـ search المتنول عن الـ Protocols - ldap
 ↳ Global Catalogue → Port 3267 [Port 3267]
 ↳ الـ ldap → Port 389 [Port 389] الـ الذي يدخله بيـ عليه معلومات

مخطوطة لـ Active Directory و فهو يسجل user على المكان الذي يستخدم him global Catalog اقرب و مقدم له .

الارتباط sites ②
- gc - upn - موقع ② بناء Port

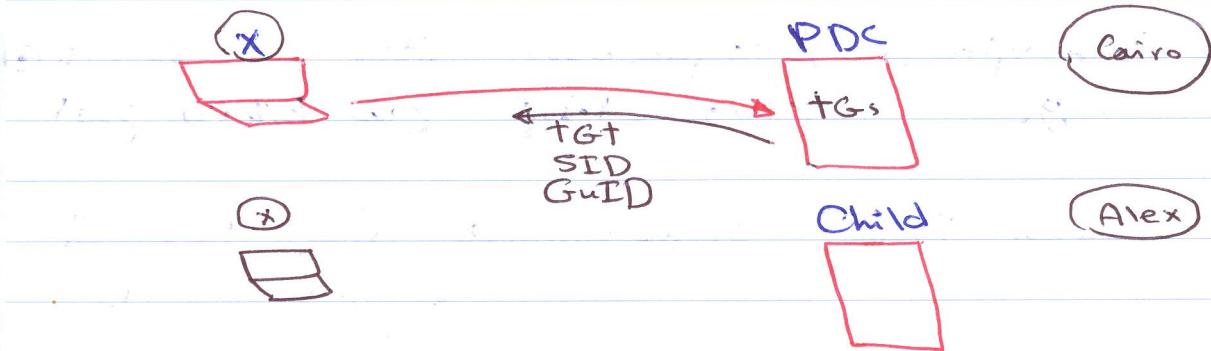
الـ gc بتحل لاحتياط Domain على الـ Connect
- upn ①
- GUID ③

لو عاير امثل بـ universal group N Cache
global Catalog

active directory sites and services → Cairo → NTDS site setting → properties
→ Enable universal group membership Caching → ok
CN=Cairo

دبي من حالة لو ماتن site مفهوم شئ لـ universal group
الـ sites واقعه درجتها حضرت ندخل .

«16» ADMT



اللهم غير لم يرجع ودخل ؛ user (الرجوع الى ظاهره) Cairo

migration tool script microsoft ellis

لاستقلال Alex كـ user لـ SID History يدعى Alex يمتلك Access權利 وكمان الـ Global ID هو من نفس الـ Forest.

• لكي لو انتقل ل Forest تابنه هي تغير عنده ال SID و GUID
• ليس ضعافاً (SID History) بل كانوا في ال Forest
• الطريقة يجري العمل على access في forest القديمة.
• Forest نفس ال Child Parent في user من الترتيب المختلط
• نفس ضعافاً لارسم بضم ال Parent في ال DNS

Forward lookup Zone → New Zone → Next → @Secondary Zone → name

Cairo.abc.Com IP 192.168.1.1 → Next

٦) نزع الـ DNS الخادم وتحل محله New Zone

Subject.....

SID

* الـ SID يُعرف منها 11

* سطحها بالطريقة العاديَّة،
Schema & Extend يُعمل لاحظ أنها لا تستطع العمل

ملحوظة

* عمان نعملها install Parent Domain لكونه شغال

* بعد ما نعملها install Schema الـ SID Register

Run → regsvr32.exe acctinfo.dll

* Add Account info لودكت على user بتابع GUID كاملاً مثيرة لـ SID هنلاؤي الـ GUID

* سطح بقى الـ ADmt دى اللي هعرف انقل فيها الـ user

* سطح الـ Child على الـ rktools ونعملها Register

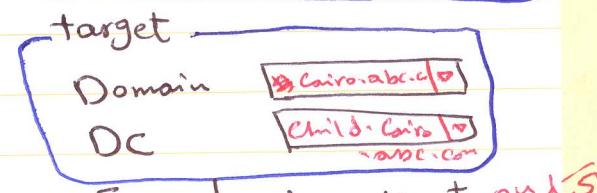
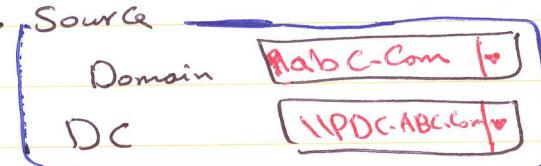
* use local SQL Server → Next → ONo, don't import

→ Next → Finish

* GUID والـ SID بتاعي mSarhan user على الـ mSarhan ننصل

admin tools → Active directory migration tools → Right Click →

user account migration wizard → Next →



→ Next → ① select user from domain → Next → add → mSarhan → OK → Next → target OU [Browse]

→ Next →

translate roaming profile

update user rights

Migrate associated usergroups

لـوـعـاـمـلـاتـ سـتـغـيـعـةـ

لـوـحـوـسـهـاـ لـلـادـمـيـنـ

يـقـلـ الـجـوـيـةـ

→ Next → Next → Finish

لـوـدـخـلـاتـ مـكـانـيـةـ وـدـخـلـاتـ مـكـانـيـةـ

هـنـالـمـوـالـيـلـ مـنـ عـمـلـيـرـ

on active directory users and comp etc وـدـخـلـاتـ مـكـانـيـةـ لـلـادـمـيـنـ



active directory users

Child

هـنـالـمـوـالـيـلـ جـدـيـدـ

Add Account info

لوـسـقـفـ الـأـكـوـنـيـاتـ

هـنـالـقـيـمـهـ اـمـدـ

SID جـدـيـدـ

GUID نـقـصـيـهـ لـلـعـمـلـيـهـ

SID history

لـكـنـ طـبـيـعـاـنـ هـنـالـمـوـالـيـلـ

لـهـ خـاصـيـاتـ جـدـيـدـاـنـ

لـوـاـدـ سـيـرـيـهـ هـنـالـمـوـالـيـلـ

SID history

وـالـ

هـنـالـمـوـالـيـلـ

"17" upgrade From 2003 to 2008

في ملخصتين نعمل بيوم upgrade
△ يجب اسطوانة 2008 وندخلها ونعملها ومتى تطلب النسخة
متى كل منها تأخذ وقت وصالة.

△ نقل 2003 & PDC من 2008 & Add new operation masters
- add → PDC new operation masters

user properties من ملكية هفاعة إدارية 2003
level schema لـ 2003 لـ 2008 migration 2008
المطحنة الأولى (الخطوة الأولى)

Run → DCpromo

* ندخل على جهاز (2003) PDC ← سطيف إداري
وركيمل عادي

→ Parent tree أو Child tree | upgrade (المخطوطة)
متى يكون لوكايزر اجل سطر

2000 ← Forest Function level و 2003 domain function level
levelRaise لزيادة مستوى المطرحة
لبيعاً أهنا لـ 2003 فونجول

Active directory users and Computer → ABC.Com → Raise Functional level

win 2003 → Raise

Active directory Domains and trusts → ABC.Com → Raise Domain functional level
ABC.Com

→ Active directory Domains and trust →
Raise Forest Functional level
win 2003 → Raise

→ open 2008 في حالة
Sources → adprep
Support → adprep

نافذة الملفات
وينفق على
Copy
Partition

Cmd

فتح إداري

C:\> adprep\adprep

٩١

C:\> cd adprep

C:\> adprep> adprep /Forestprep

C

Enter

Schema

کے اکھوں پر بیٹھ دا

C:\adprep /domainprep

Domain

کے اکھیں پر بیٹھ دا

لے گایا اعلیٰ (2008) رکھو ہش پتھر علوی کے اکھوں پر بیٹھ دا

C:\adprep /rodcprep

RODC کے اکھیات دا Domain دا Forest دا

ننھلیں کے اسٹروپہ دا و ننھل windows دا

(C) windows server 2008 R2 Enterprise (full) x64 → Next

upgrade → Check

FreeSpace ← 10GB لے کوئی نہیں على الاقل
2008 R2 کو 2003 R2 لے کوئی نہیں

→ Next →

کے اکھیں پر بیٹھ دا

2008 دا 2003 دا Win اکھوں پر بیٹھ دا

وھتلائی لئے دا Domain دا Users دا Programs دا

7 لا ۷ میں upgrade کے اکھوں پر بیٹھ دا

microSoft tools پر بیٹھ دا

Subject.....

الطريقة الثانية

ممكن نعمل على Server 2003

برضهه هم ينفع تفاصيل ونعمل فيه طفرات على الماكينة

↳ Support → adprep → Copy C: \Temp\adprep

Domain \& Forest \& Raise First User (الأول) *

Cmd →

C:\>adprep\adprep /Forestprep

C Enter

schema \& forest \& upgrade كـ اي جيل *

C:\>adprep\adprep /domainprep domain كـ اعلانات

C:\>adprep\adprep /rodcprep RODC كـ اعانته

add 2008 نعمل عليه *

Run → DC promo → Next → Existing Forest

Add Domain Controller to existing Dom

→ Next → Name ABC.Com

Alternate Credentials

Set

user Pass

→ Next → Next → DNS

Global Catalog

→ Next →

→ Next → Next → Reboot on Completion

Restart

2008

Primary \ add عايز احول على

admin tools → active directory Domains and trusts → Operation masters → Change active DC →

→ ADC-ABC.Com → OK

→ Operation master →

Domain name master transfer (الخطوة最後ة)

schema \ transferred to DC

Run → Regsvr32 schmmgmt.dll → OK

mmc → add/remove snap → Active directory schema → Add → ok

active directory schema → Change active DC → ADC.ABC.Com → OK
 → operation masters → **Change**
 Schema → transfer masters

دوك الاتيم المسؤولين عن ال forest

الثانية Rules ③ على حفظها
 Active directory users and Computers → ABC.Com → Change DC →
 ADC.ABC.Com → OK
 → operation masters → **Change**
 Infrastructure → PDC → RID →

الثالثة Rules → Windows 2003 نرجع له

أخر خطوة هي Active Directory Users & Servers →
 active directory users → Domain Controllers → ADC → properties →
NtDS setting → Global Catalogue

الرابعة، الخطوة تعيين المديرين المسؤولين مع بعضه البعض

نرجع له Windows 2003

Run → DCPromo / Forceremoval **OK**

وتحتى مع الخطوات ونستعرض
 Primary → DNS add اولاً ثم add دلائل كأن وافتتح دلائل

18 Backup & Recovery active

۲۰۰۸ء میں طریقہ

٦٧ صادر Image عن نسخة الوسيط كلها.

(NTDS) . و active directory یا ip cmd ۲

طريقة الـ أولى

1- admin tools → windows Server Backup →

نعملها install اولاً من

Server manager → Features → add → windows Server backup features →

windows Server Backup
 Command-line tools → Next → insta

admin tools → windows Server Backup → **Backup once** → Next →

① Custom → Next → Add items → 日本 local disk (C)

Windows \rightarrow OK

→ Next → ④ local drivers → Next → Backup destination [Drive(D):]

→ Next → **Backup** → Close

کلها win می‌باشد. Image is in US.

٤) لـلسخنه سقط بي ونـايقتح طهرا حـخط اسطوانه، لـعينوز دـاعل Boot

Install Now من اتن سما بتاع

Repair Your Computer → Next

④ Restore Your Comp using system image

→ Next → Select system image

Cmd

الطريقة الثانية

```
C:\> wbadmin start systemStateBackup -backuptarget:e:  
{e:} Enter yes
```

备份恢复：通过启动时选择不同的启动项，从光盘、U 盘或硬盘启动，进入恢复环境，执行恢复操作。

مخطوطة لازم على نفس الجهاز بنفس الاسم ولنفس IP ويندأ سطح Domain نفس الاسم الفاتح بعد ما تفتح F8 ندخل على active directory Restore mode

Restore mode ١١ ٢٢٣٣ Password ٦٦ Reset

C:\>ntdsutil

ntdsutil: reset dsrm password

Restate DSRM administrator password: reset password on
Server pdc.abc.com

Please type password for DS Restore mode Account: * * * * *
Confirm: * * * * *

نکودا امتحانت ۱۱ Password

نکمل: هیو این بینت جهار یعنی IP و نام سرور، طبقاً و این دامنه
Domain نام دارد.

لۇغىت 11 active directory قاپقىنە كېلىرىنىڭ

وهو طهراً يفتح الصيغة f_8 وعدها f_1 من ال Boot عما هي الحال

* Directory Services Restore mode

وَنَعْتَنِي طَرَا حَمْل

و هذہ خلکت علی ال کرنے دیکھاں اور PassWord

ملحوظہ

- admin سے دیکھاں Restore mode اور Password

فیصلہ علی ال Safe mode

C:\> wbadmin get versions Copy & version

C:\> wbadmin start systemStateRecovery -versions: 11/13/2012 8:59 PM
y, y

NTDS ل Recovery کیا گی

و ہتمل Restart کیا گی

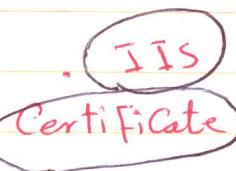
لائقہ حملہ کیلیے Backup کیا گی اور اس کا

«AD-RMS»«Active directory rights management»

في الواقع Microsoft هي التي طورت هذه الميزة فقط.

حيث كل الملفات الموجودة على الـ SQL Server يمكنها Copy ولها هذ صحرافها.

* عسان تنزلها لازم يكون فيه windows internal database . win2008 او في ملخص على Service 2003,xp غيره ونزلتها على الـ Domain Controller.



- ① لازم يكون سيرفر
- ② لازم يكون فيه

الافضل انها تنزل على file server على الـ Domain Controller ويفضل انها تنزل على الـ Domain Controller.

لها شرطين عسان تنزل :

- ① تنزلها ال Database بتابعها .
- ② user لازم يكون له mail address .

التطبيق العملي

Join domain و لازم يكون RMS على نفس الـ Server.

Server manager → Roles → add → Active directory rights management service
→ Next → Add Required Role services

حيثك اد RMS

→ Next → Next → Active directory Rights management

→ Next → Create new AD RMS Cluster → Next →

use windows internal database on this Server

→ Next → Domain user Account

Service will manage the account

Group في member

Enterprise admin

memberof & Properties ← user نعمل على Domain N
Domain admins ← add

AD RMS

نعمل سطح في

الى هتشفر key ne all key

① use AD RMS Centeracy managed Key storage.

→ Next → Password []

Confirm []

رمزها

Next → Next →

② use SSL-encrypted Connections

Internal address

<https://rms.abc.com>

RMS Server

→ Next →

③ Create self sign Certificate → Next

جاء من RMS

or Certificate later

Name [RMS]

→ Next →

④ Register the AD RMS Service Connection point now

→ Next → Next → Install → Restart

mail account roles, users ② نعمل على Domain N ④

share other folder نعمل على RMS

Permission → Add (Domain users, Domain admins)

Full Control

(Domain admins) users inheritance تثبيت security rights

mSarhan & user

نعمل على Client 7 لفتح الملفات

11rms

فتح الملفات

word file ويكمل على folder ال user

الى جواه ويدل على Save حفظ

Prepare → Restrict permission → Restricted Access → Yes

OK → Pass user click

كما يرى لغيرها غير ال user

RMS

لورمجز

admin tools → Active directory Rights management services →

Rights Policy templates → Create distributed rights policy template

Add → Name RMS Desc RMS → Next → Add

كتابات (الى يحق لهم) لـ user

the email

 [Browse]

Rights

Full Control View Document file user following default
لا يحق لهم ما يسمى به
ختار هم يحق لهم؟

لورمجزنال win7 بعد حمايتها تغيرت

☒ Restrict permission

Read رخصة التي ي Authorized

Read

Change رخصة التي ي Authorized

Change

More option

Print (الوظيفة الممنوعة)

Same ، أو

username hali

نفرض بـ hali user كان متواجد على الضوكلر

Full Control

لاظهارها

RMS

Data

file or word

username

لوجين يفتحه

Pass

الى عمل الملف عليه msarhan

RMS

Data

كيفية العمل على الملف

user

pass

يطلب منه

Change permission

Read hali

→ OK

ملحوظة

دوخت لودفل الـ user

11rms → Data

لـ يفتح الملف هيطلب بـ رسمته الـ user وـ الـ Pass

هـ يحصل بيـ نوعه العـ ادـ سـ يـ هـ يـ فـ يـ عـ اـ مـ حـ اـ فـ يـ طـ بـ يـ سـ يـ هـ يـ غـ يـ رـ

يـ جـ لـ Read Print وـ Copy وـ لا فـ يـ طـ

"20. Csvde & ldifde & Dsget"

طريقة لـ users نـ export & import بـ cmd
file لـ active directory
من سـ ID بـ backup بـ restore

Dsget

```
C:\> dsquery user > users حـ يـ مـ
```

```
C:\> dsquery user -name "*" | dsget user > user.txt
```

هـ يـ مـ حـ وـ اـ لـ Cـ مـ لـ فـ بـ الـ سـ مـ <--
هـ يـ مـ جـ وـ اـ لـ users <--

```
C:\> dsquery user -name "*" | dsget user -samid  
-fn -ln -email -upn > x.txt
```

هـ يـ مـ هـ وـ لـ هـ شـ كـ لـ اـ خـ اـ لـ <--

```
C:\> dsquery ou -name "*" | dsget ou > out.txt
```

- حـ يـ مـ حـ وـ اـ لـ ou <--

Csvde

لـ قـ حـ لـ وـ حـ سـ تـ قـ الـ اـ مـ رـ دـ اـ نـ ظـ اـ عـ اـ لـ خـ طـ حـ مـ حـ دـ وـ لـ مـ

```
C:\> Csvde -f user.txt
```

مـ حـ طـ حـ مـ حـ طـ حـ لـ مـ حـ وـ اـ لـ users import بـ يـ هـ مـ حـ وـ اـ لـ

جـ يـ بـ اـ لـ Microsoft mod اـ لـ cmd

DN , objectClass, SAMAccountName, UserPrincipalName, displayName,
UserAccountControl

"CN=Mahmed, DC=abc, DC=com", user, Mahmed, ahmed@abc.com,
OU=HR

Ahmed Sarhan 512 ← Enabled
or
514 ← Disabled

C → designation some thing

C:\> Csude -i -f C:\Csud.txt

Cmd قمّع

import

هذا مفهوم نزلوا بـ cmd active directory users N cups

to Import

الآن يفتح الملف الذي عاشرناه **ملحوظة**
ننشر him Domain

③ Ldifde

dn: Cn=suzan, Ou=HR, dc=abc, dc=com

ChangeType: Add

ObjectClass: user

SamAccountName: suzanf

UserPrincipalName: suzanf @abc.com

displayName: suzan fine

UserAccountControl: 514

C:\> ldiffde

Cmd

C:\> ldiffde -i -f C:\ldifde.txt

لود مفاتيحة active directory users