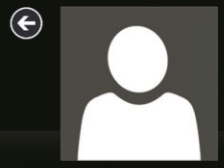
```
C:\>netdom query fsmo
Schema master               dc.target.org
Domain naming master        dc.target.org
PDC                         dc.target.org
RID pool manager            CAIRO-BRANCH.target.org
Infrastructure master       dc.target.org
The command completed successfully.


C:\>ntdsutil
ntdsutil: role
fsmo maintenance: connection
server connections: connect to server dc
Binding to dc ...
Connected to dc using credentials of locally logged on user.
server connections: q
fsmo maintenance: transfer rid master
Server "dc" knows about 5 roles
Schema - CN=NTDS Settings,CN=DC,CN=Servers,CN=HQ-Riyadh,CN=Sites,CN=Configuratio
n,DC=target,DC=org
Naming Master - CN=NTDS Settings,CN=DC,CN=Servers,CN=HQ-Riyadh,CN=Sites,CN=Confi
guration,DC=target,DC=org
PDC - CN=NTDS Settings,CN=DC,CN=Servers,CN=HQ-Riyadh,CN=Sites,CN=Configuration,D
C=target,DC=org
RID - CN=NTDS Settings,CN=DC,CN=Servers,CN=HQ-Riyadh,CN=Sites,CN=Configuration,D
C=target,DC=org
Infrastructure - CN=NTDS Settings,CN=DC,CN=Servers,CN=HQ-Riyadh,CN=Sites,CN=Conf
iguration,DC=target,DC=org
fsmo maintenance: _
```



تطبيقات على الدليل النشط

علاء امين

ISBN 978-1-365-50284-2
90000
9 781365 502842

جميع ما يرد في هذا الكتاب من شروحات
وصور ومعلومات هي متاحة للجميع دون
الرجوع لي ..
كما اني اشركت في اجره كل من ساهم معي
في نشره ... علاء أمين

IN This Part

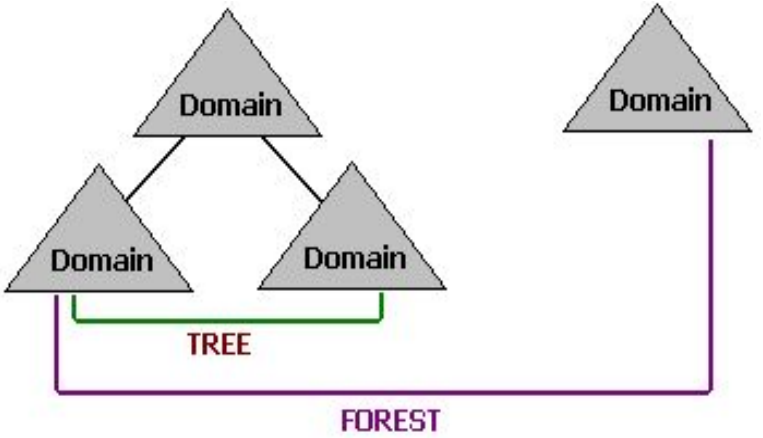
ACTIVE DIRECTORY REPLICATION

سوف نتناول بإذن الله موضوع هام جدا وهو تبادل البيانات بين الشبكات المختلفة والمتباعدة , أي التي لا تقع ضمن نطاق جغرافي واحد والتي تملك عناوين شبكة مختلفة ولكنها تشترك فيما بينها بوجودها داخل نفس الـ Forest

لكننا في البداية سنقف قليلا لاسترجاع بعض المعلومات الهامة في تعريف الـ Forest و الـ Domain والـ Tree

فبعد إجراء أول عملية تنصيب لأول Windows Server و تفعيل الـ Active Directory Role و إنشاء New Domain سوف ينتج عن ذلك تلقائيا

اول Forest و اول Domain وأول Tree كما في الشكل :-



الـ Forest هو المكان الذي يحوي بداخله Tree واحد أو أكثر ويحوي الـ Domain والـ Tree معا ويأخذ إسم أول Domain

الـ Tree هو المكان الذي يحوي بداخلة Domain واحد أو اكثر

الـ Domain أو المجال هو الاداة التي يتم بها إجراء عمليات الربط والتوثيق والصلاحيات والبيانات والضبط والتهيئة وما الى ذلك وهو محور حديثنا وله عده اشكال وأنواع كالتالي :-

1- Root Domain First أو The Primary Domain

وهو أول domain يتم إنشاؤه داخل الـ أول Tree ويتميز عن غيره بالتالي :-

- يكون الاسم الخاص به هو اسم للـ Forest ككل
- هو الوحيد الذي يحتوي على Domain naming Master Role (سنشرح ذلك لاحقا)
- يكون Global Catalog by default

- يصبح Default first site name

2- Additional Domain

هو نسخة من الـ Domain الرئيسي يمكن التعديل عليه بالحذف او الاضافة وما الى ذلك ويستخدم كدومين اضافي او لتخفيف الضغط على الـ Domain الرئيسي .

3- Read Only Domain (RODC)

هو أيضا نسخة من الـ Domain الرئيسي لكن لا يمكن التعديل عليه فهو للقراءة فقط ويستخدم كنوع من انواع الحماية حيث انه لا يقوم بحفظ كلمات المرور عليه بل يقرؤها من الـ Domain الرئيسي .

4 - Child Domain

هو Domain يقع تحت الـ Domain الرئيسي لكنه منفصل عنه في الخصائص و له قاعدة بيانات مستقلة بذاتها عنه ويمكن من خلال الـ Domain الرئيسي التحكم في هذا الـ Child يستخدم في حالة الشركات الكبيرة ذات الافرع والنشاطات المتعددة لكنها جميعا تقع تحت مظلة الشركة الام .

وبهذا نكون قد تعرفنا على الـ Forest و الـ Domain والـ Tree وأيضا أنواع الـ Domain

ملحوظة هامة :-

سنقوم بشرح الـ Replication مباشرة دون التطرق لشرح عملية تنصيب الـ Active Directory لان هذا الكتاب يعد موجها للمتقدمين ومع ذلك وأثناء الشرح سنتعرف على الـ Additional Domain والـ Child Domain وربما أنواع اخرى ولكن دعونا اولا نعرف ما الذي سيتم في عملية تبادل البيانات Replication داخل الـ Active Directory ..؟

و حتى نجيب على هذا السؤال لابد ان نعرف ما هو الـ Active Directory ومما يتكون ؟

الـ Active Directory هو تطبيق من شركة مايكروسوفت موجه لأنظمة التشغيل Windows والغرض الرئيسي منه هو توفير الخدمات المركزية لتحديد الهويات والتوثيق داخل الشبكة وهو يعد قاعدة بيانات مركزية تكون داخل الـ Server يخزن عليها كل المعلومات والبيانات الخاصة بالشبكة مثل المستخدمين والأجهزة والطابعات والملفات المشاركة والخدمات وموارد الشبكة ..... وما الى ذلك ويتيح ايضا لمدير الشبكة Network Administrator تنظيم وإدارة ومراقبة الدخول لموارد الشبكة وكذلك التحكم بها .

وينقسم الـ Active Directory لأربعة اقسام كالتالي :

1- Domain partition
2- Configuration partition
3- Schema partition
4- Application partition

الـ Domain partition

هو الذي يحتوى على كل ما يخص الدومين من Container…. Groups… User Objects ,…. Computer Objects
و كل مكون من هذه المكونات له خصائصه التى تسمى Attributes ويدار بواسطة Active Directory User and Computer Consol

الـ Configuration Partition

هو الذي يحتوى على كافة الإعدادات الخاصة بالـ Active Directory مثل إعدادات الـ Sites و يتم نشر نسخه منه إلى كافة الـ Domain Controllers الموجودة فى الـ Forest ويدار بواسطة Active Directory Site and Services Consol

الـ Schema Partition

هو الذي يحتوي على معلومات كل الـ Objects و الـ Attributes ويدار أيضا بواسطة ADUser and Computer Consol
و يمتلك أول Domain Controller النسخه الوحيدة القابلة للكتابة و يسمى Schema Master و كل الـ Domain Controllers الأخرى تملك نسخه للقراءة فقط من هذه الـ Schema Partition

الـ Application partition

هذا الجزء يوجد اختياريا حسب الحاجة له فالبرامج التى تتكامل مع بيانات الـ Active Directory تقوم باستخدامه فى حفظ بياناتها كخادم البريد Exchange Server مثلا أما التي لا تحتاج Integrated مع الـ Active Directory فلا تحتاجه وهكذا .

Practical Guide

ولتبسيط الامر سوف نقوم بالممارسة العملية على المثال التالي :

لدينا شركة يقع مقرها الرئيسي في مدينة الرياض ولديها أفرع في كلا من القاهرة والدوحة

وبيانات الشبكة كما يلي:

Domain name : target.org (win srvr 2012)

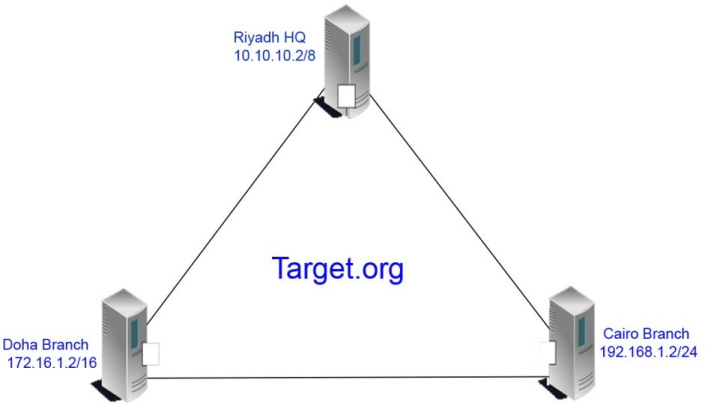
Dns ip is 10.10.10.2 /8

Branch in Cairo has 172.16.1.2/16 (win srvr 2008)

Branch in Doha has 192.168.1.2/24 (win srvr 2008)

Real Ip For Routing is 66.249.64.231/8

شكل الشبكة جغرافياً هو كالتالي:



لاحظنا في الرسم ان هناك ثلاث خطوط اتصال كالتالي :-

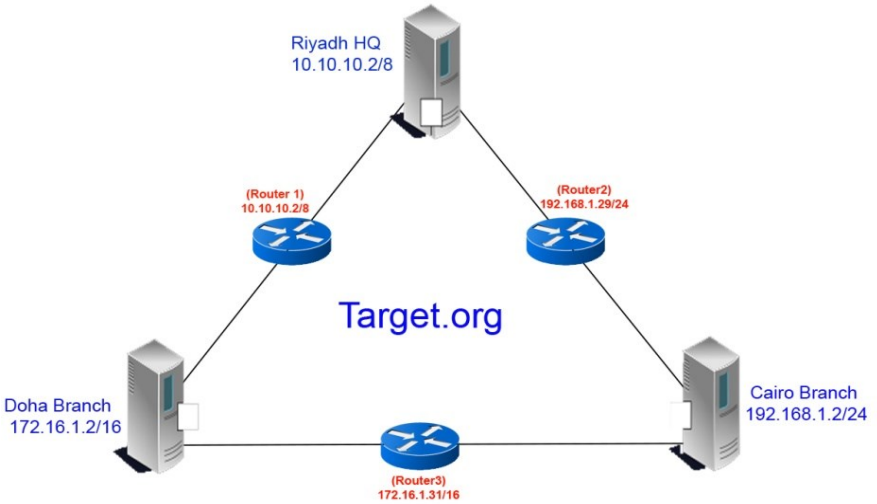
الخط الاول بين الرياض والقاهرة

الخط الثاني بين الرياض والدوحة

الخط الثالث بين الدوحة والقاهرة

ومن المعلوم ان هذه المدن الثلاث متباعدة جغرافيا بل انها تقع في قارتين مختلفتين هما افريقيا واسيا ولكونهما تتبعان معا نفس الشركة الام فلابد ان يتم الربط بينهما ولكن كيف يتم ذلك ؟

الجواب هو اننا نحتاج لتوصيل كل خط داخل كل فرع بواسطة Router عن طريق الانترنت ليصبح شكل الشبكة فيما بعد هو التالي :-



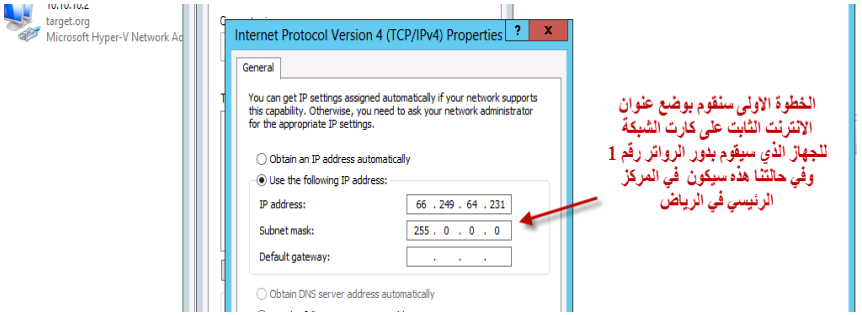
حسنا الان علمنا اننا سنحتاج الى جهاز router في كل فرع وحتى تتمكن الاجهزة من ان ترى بعضها البعض سنحتاج ايضا لعنوان ip ثابت لكل router وهذا العنوان يمكن طلبه من الشركة المزودة لخدمة الانترنت لديك.

والآن هيا بنا لنقوم بعمل هذه الخطوات معا مع العلم أننا سنستخدم في الشرح خدمة Microsoft routing وسيكون الشرح داخل بيئة Hyper V

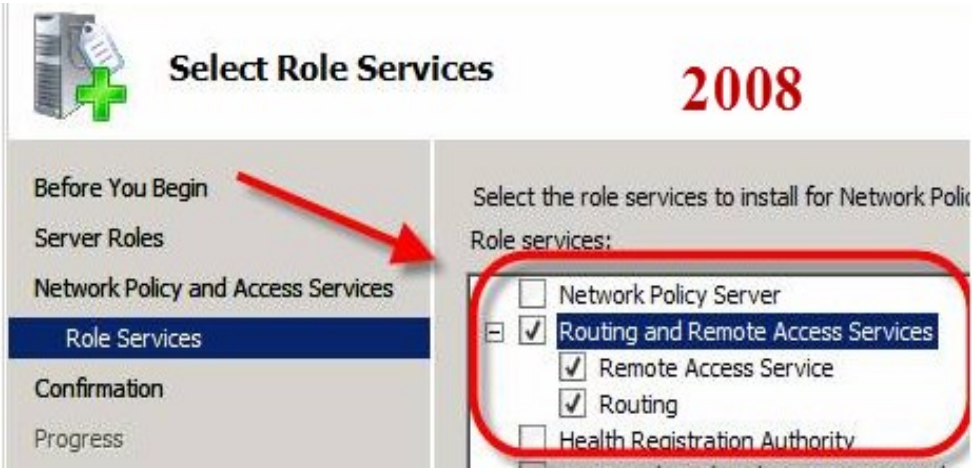
(اضغط هنا للوصول لرابط كتابنا لشرح Hyper V)

ملاحظة مهمة : سيكون ال router عبارة عن جهاز سيرفر أي في بيئة Microsoft وبإمكانك تطبيق الشرح في أي بيئة عمل تفضلها سواء vmware أو Hyper V أو permeatal وأيضا في الواقع بفضل استخدام Cisco router

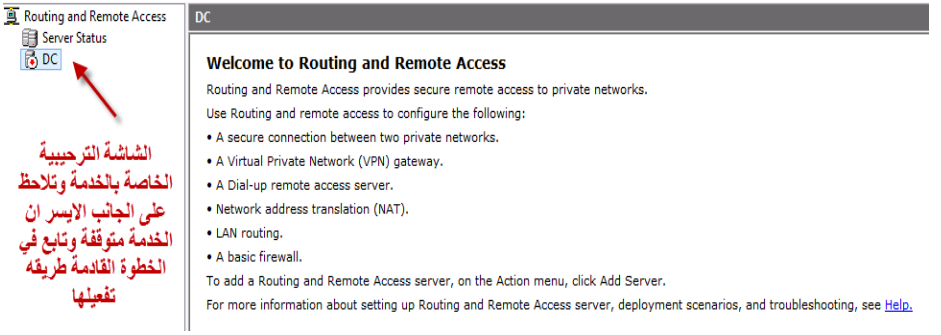
أولا سنقوم بإعداد الـ Routers كما يلي :-

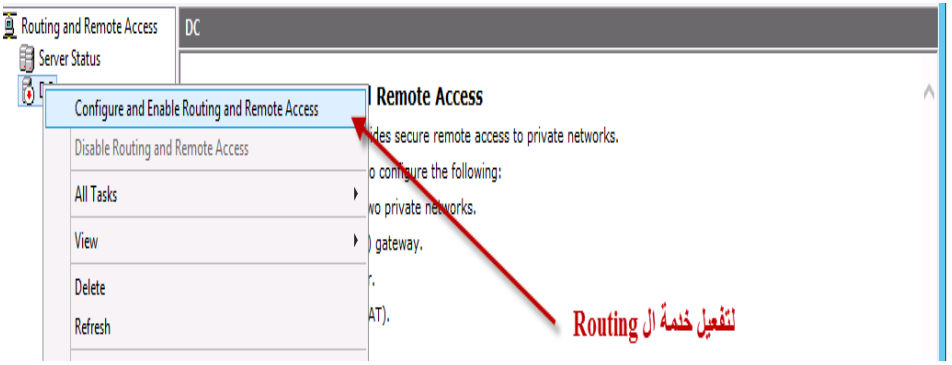


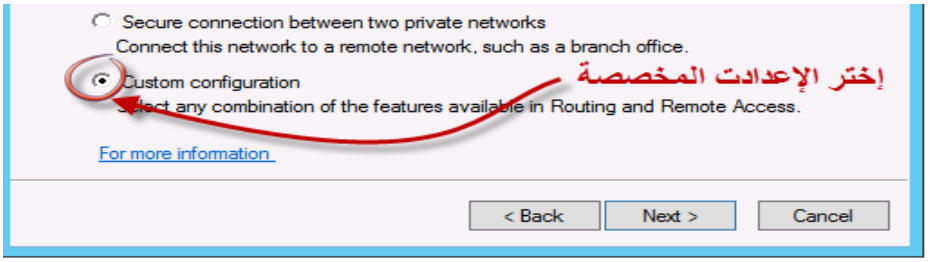

Select server roles
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Remote Access
Role Services
Confirmation
Results
Select one or more roles to install on the selected server.
Roles
Active Directory Federation Services
Active Directory Lightweight Directory Services
Active Directory Rights Management Services
DHCP Server
DNS Server (Installed)
Fax Server
File and Storage Services (2 of 12 installed)
Host Guardian Service
Hyper-V
MultiPoint Services
Network Controller
Network Policy and Access Services
Print and Document Services
Remote Access
Remote Desktop Services
Volume Activation Services
Web Server (IIS)
Windows Deployment Services
Windows Server Essentials Experience
Windows Server Update Services
الخطوة الثانية قم بتفعيل Remote Access Role win2012

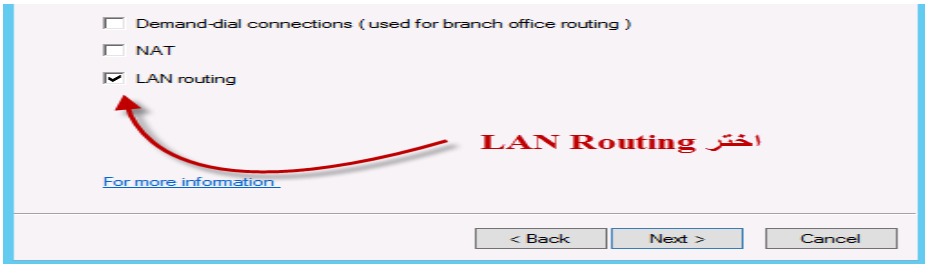

Select Role Services
2008
Before You Begin
Server Roles
Network Policy and Access Services
Role Services
Confirmation
Progress
Select the role services to install for Network Polic
Role services:
Network Policy Server
Routing and Remote Access Services
Remote Access Service
Routing
Health Registration Authority


Start
Administrator
Windows PowerShell
Administrative Tools
Routing and Remote Access
Group Policy Management
DNS
Windows Deployment...
WinRAR
Task Manager
Active Directory Module for...
ADSI Edit
Health Registration...
Internet Information...
Internet Explorer
DHCP
Active Directory Domains and...
Network Policy Server
Remote Access Management
بعد الانتهاء من تفعيل ال role ستظهر الايقونة الخاصة به في قائمة الادوات قم بفتحها الان

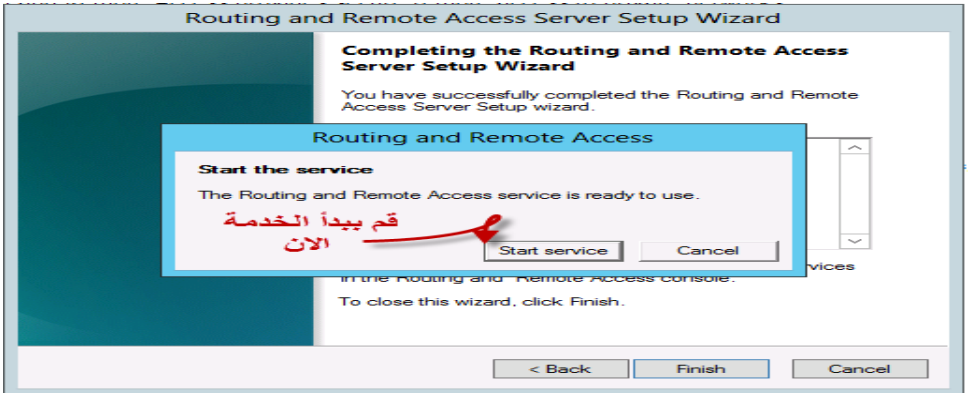

Routing and Remote Access
Server Status
DC
الشاشة الترحيبية الخاصة بالخدمة وتلاحظ على الجانب الايسر ان الخدمة متوقفة وتابع في الخطوة القادمة طريقه تفعيلها
DC
Welcome to Routing and Remote Access
Routing and Remote Access provides secure remote access to private networks.
Use Routing and remote access to configure the following:
• A secure connection between two private networks.
• A Virtual Private Network (VPN) gateway.
• A Dial-up remote access server.
• Network address translation (NAT).
• LAN routing.
• A basic firewall.
To add a Routing and Remote Access server, on the Action menu, click Add Server.
For more information about setting up Routing and Remote Access server, deployment scenarios, and troubleshooting, see Help.

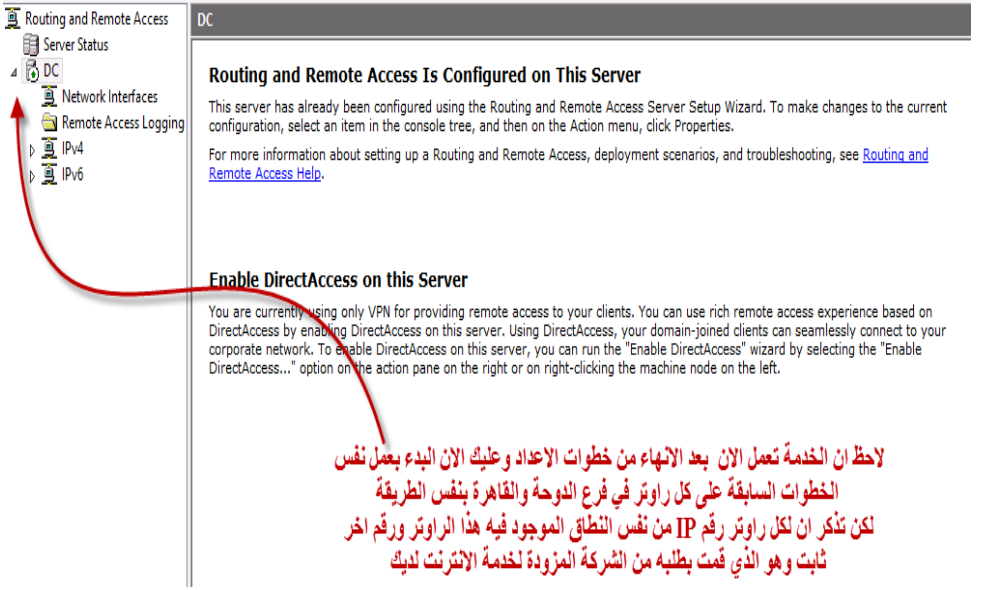

Routing and Remote Access
Server Status
DC
Configure and Enable Routing and Remote Access
Disable Routing and Remote Access
All Tasks
View
Delete
Refresh
Remote Access
لتفعيل خدمة ال Routing


Secure connection between two private networks
Connect this network to a remote network, such as a branch office.
Custom configuration
إختر الإعدادت المخصصة
Select any combination of the features available in Routing and Remote Access.
For more information
< Back
Next >
Cancel


Demand-dial connections (used for branch office routing)
NAT
LAN routing
اختر LAN Routing
For more information
< Back
Next >
Cancel


Routing and Remote Access
Routing and Remote Access has created a default connection request policy called Microsoft Routing and Remote Access Service Policy. To ensure that this new policy does not conflict with existing Network Policy Server (NPS) connection request policies, open the NPS console and verify that it is configured properly.
بعد الانتهاء من الخطوات السابقة ستظهر لك هذه الرساله قم بالموافقة عليها
OK


Routing and Remote Access Server Setup Wizard
Completing the Routing and Remote Access Server Setup Wizard
You have successfully completed the Routing and Remote Access Server Setup wizard.
Routing and Remote Access
Start the service
The Routing and Remote Access service is ready to use.
قم ببدأ الخدمة الان
Start service
Cancel
To close this wizard, click Finish.
< Back
Finish
Cancel


Routing and Remote Access
Server Status
DC
Network Interfaces
Remote Access Logging
IPv4
IPv6
DC
Routing and Remote Access Is Configured on This Server
This server has already been configured using the Routing and Remote Access Server Setup Wizard. To make changes to the current configuration, select an item in the console tree, and then on the Action menu, click Properties.
For more information about setting up a Routing and Remote Access, deployment scenarios, and troubleshooting, see Routing and Remote Access Help.
Enable DirectAccess on this Server
You are currently using only VPN for providing remote access to your clients. You can use rich remote access experience based on DirectAccess by enabling DirectAccess on this server. Using DirectAccess, your domain-joined clients can seamlessly connect to your corporate network. To enable DirectAccess on this server, you can run the "Enable DirectAccess" wizard by selecting the "Enable DirectAccess..." option on the action pane on the right or on right-clicking the machine node on the left.
لاحظ ان الخدمة تعمل الان بعد الانهاء من خطوات الاعداد وعليك الان البدء بعمل نفس الخطوات السابقة على كل راوتر في فرع الدوحة والقاهرة بنفس الطريقة
لكن تذكر ان لكل راوتر رقم IP من نفس النطاق الموجود فيه هذا الراوتر ورقم اخر ثابت وهو الذي قمت بطلبه من الشركة المزودة لخدمة الانترنت لديك

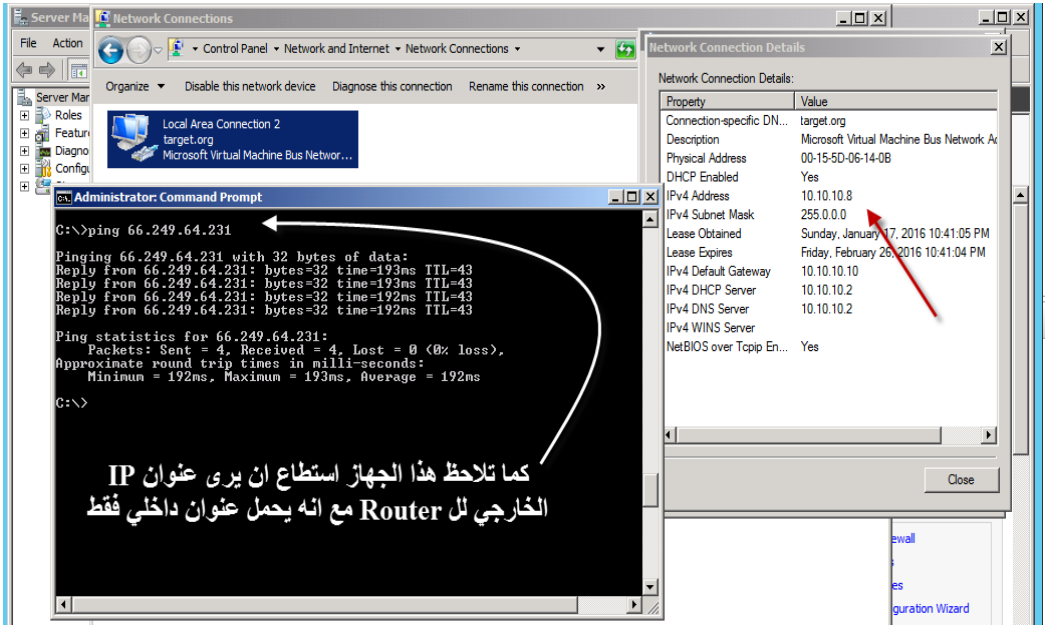
الان دعنا نقف قليلا لنفهم فائدة ما قمنا به :-

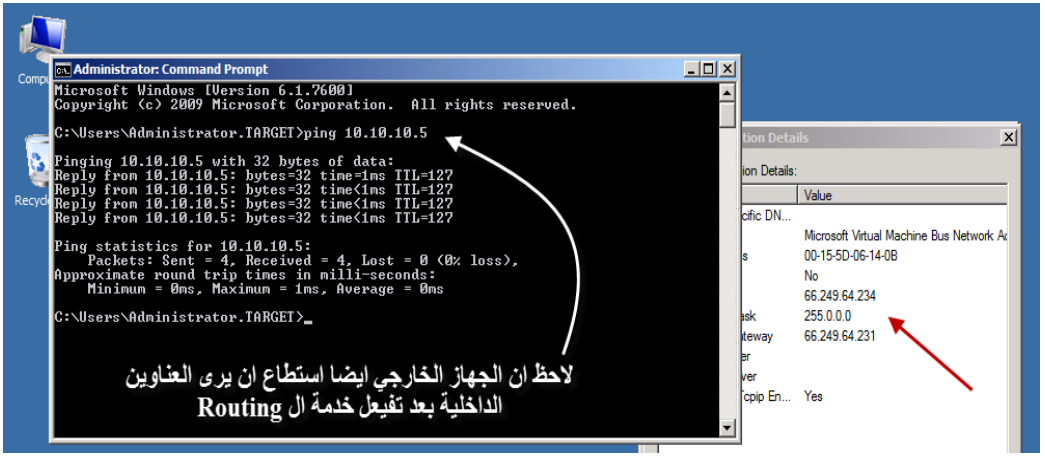
1- قمنا اولا بضبط عناوين ال IP الداخلية والخارجية الخاصة بال router وحيث ان كل router يحتوي على كرتين شبكة على الاقل فقمنا بمنح الكارت الاول (E1) رقم IP داخلي من نفس نطاق الشبكة الموصول عليها والكارت الاخر (E2) قمنا بمنحه الـ Static IP الذي حصلنا عليه من مزود الخدمة

2- قمنا بتفعيل خدمة ال routing واخترنا في الاعدادات ان تكون من نوع LAN Routing وهذا يعني ان كلا الشبكتين المتصليين بال router تستتطيعان الوصول و الاتصال ببعضهما البعض

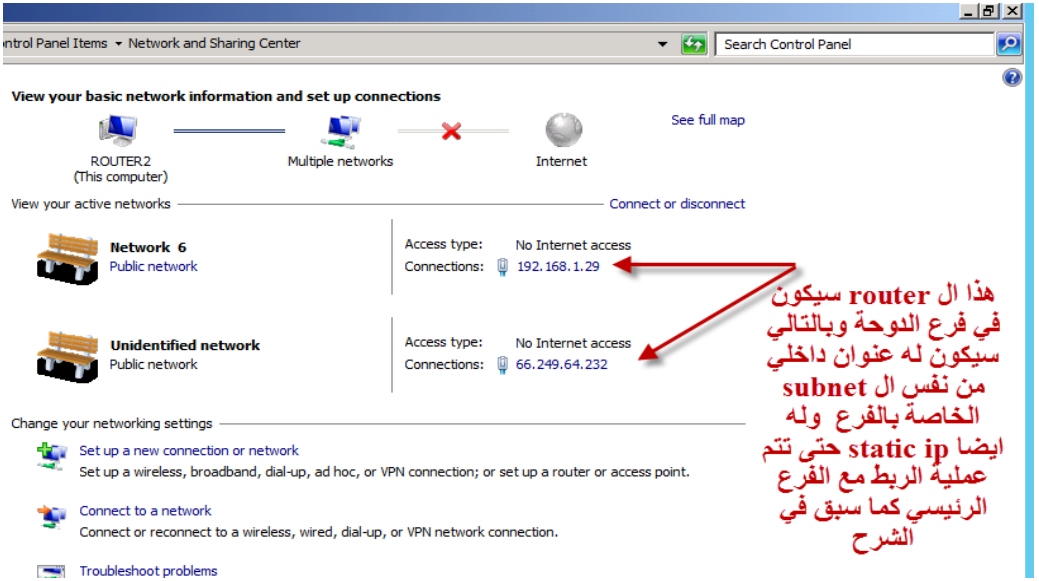
(ان لم يكن هناك اعدادات اخرى تمنع هذا الاتصال بحسب السياسة المعمول بها في المكان)

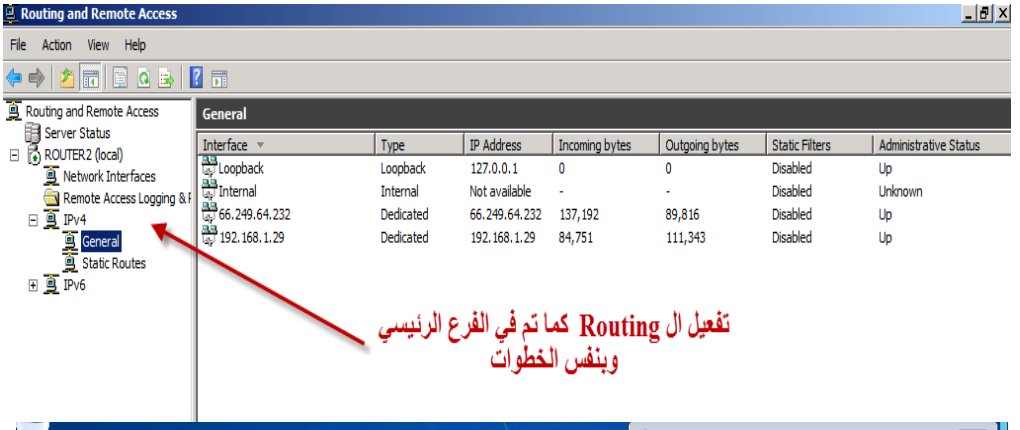
ولتجربة هذا عمليا قم الان بالتوجه الى أي جهاز يحمل عنوانا داخليا من نفس نطاق العنوان الداخلي لل router وحاول ان تتصل به عن طريق عنوانه الخارجي كما في الصورة .

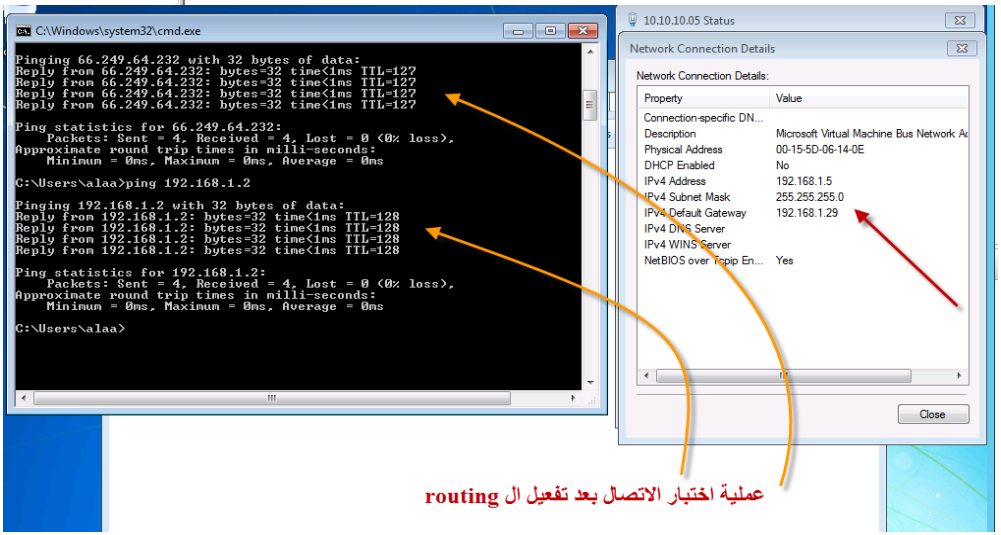




وسنفهم الامر أكثر وأكثر حين نقوم بإعداد الـ router الثاني الخاص بفرع الدوحة وذلك كما قمنا بإعداد الـ router الاول الخاص بالفرع الرئيسي في مدينة الرياض تماما مع اختلاف عناوين الـ IP طبعا فتابع معي :-







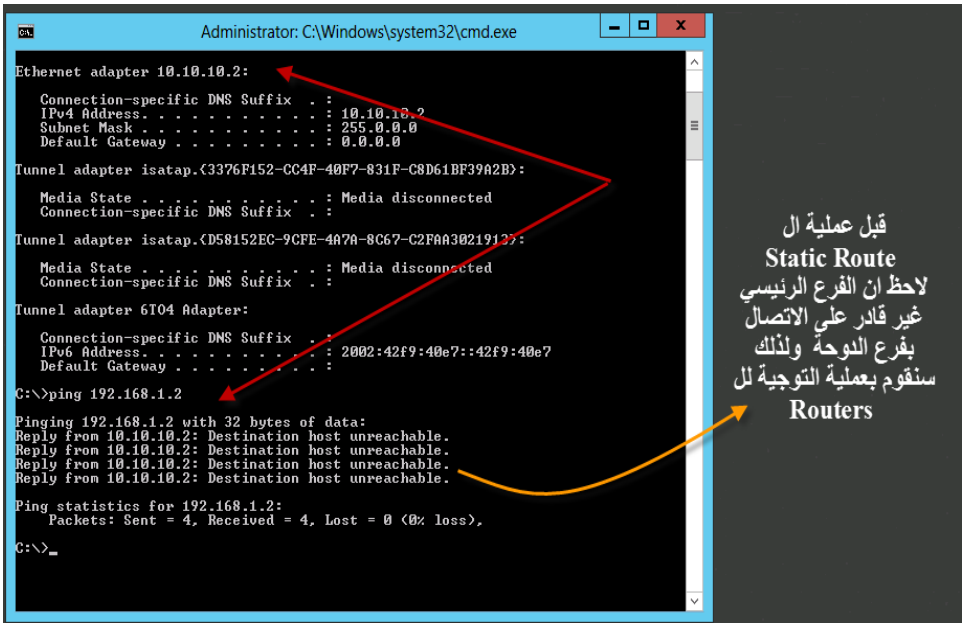
الان لدينا عدد router 2 وعدد subnet 3 كما في الجدول التالي :-

Sub No	Location	IP	Router No
1	Riyadh	10.10.10.2	R1
2	Doha	192.168.1.2	R2
3	Internet	66.249.64.231	Act Link

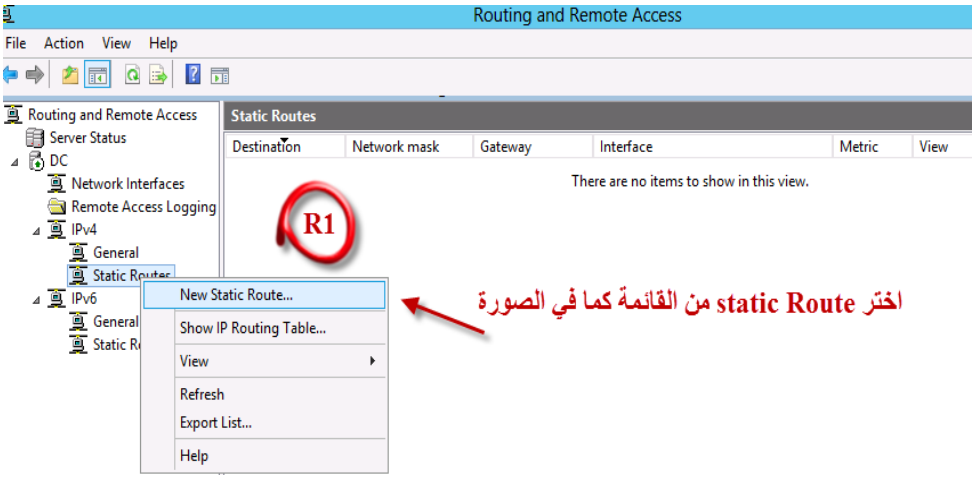
المطلوب الان هو أن يتصل فرع الرياض (R1) وفرع الدوحة (R2) عن طريق الانترنت (Act Link)

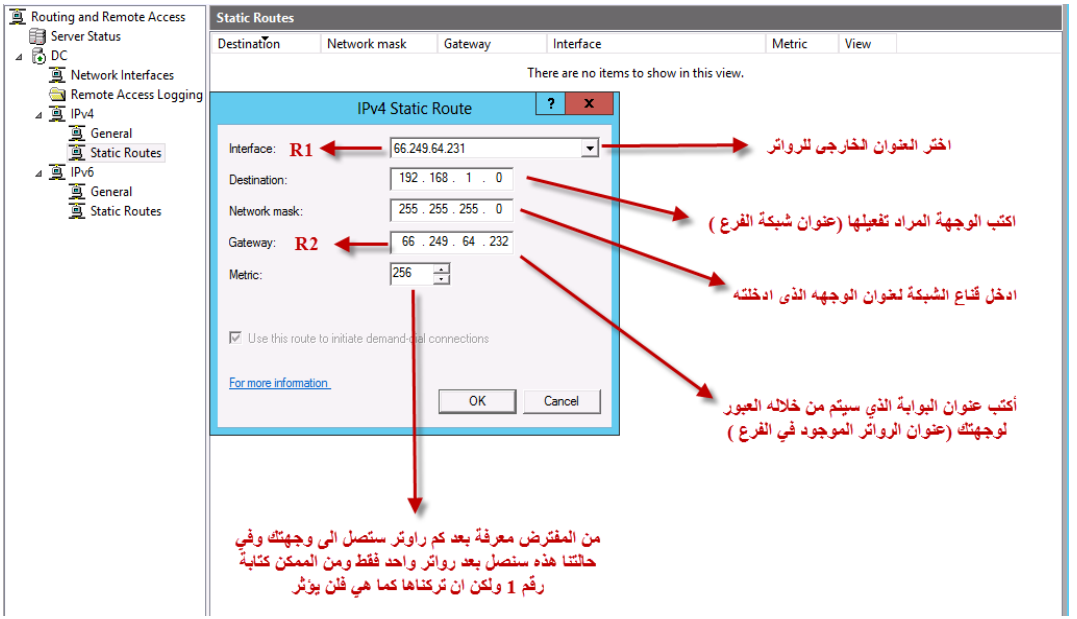
هل تعلم **كيف** يتم ذلك ؟ الجواب في الصفحة التالية :-

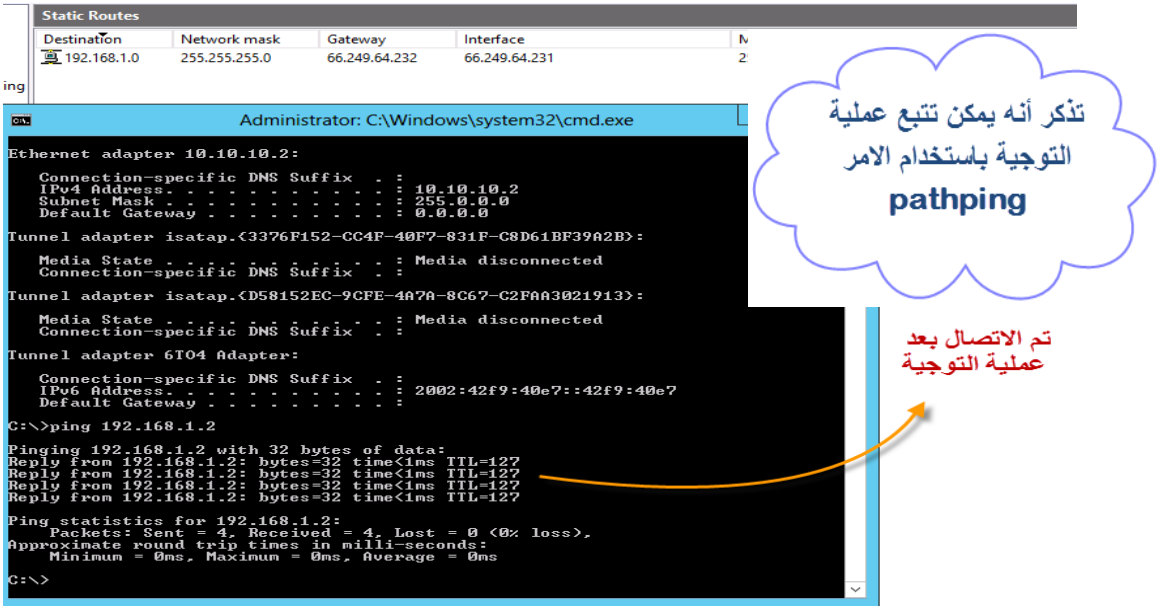
لكي تتم عملية الربط فيجب اولا ان نقوم بعملية توجيه البيانات القادمة من كلا الفرعين عن طريق ال routers أو ما يعرف بالـ Static Route وفيها سوف نجعل ال router رقم 1 الموجود في الرياض يخاطب الـ router رقم 2 الموجود في الدوحة حين يحتاج بيانات من الفرع والعكس ايضا صحيح أي ان كلا منهما سوف يتبادل معلومات الـ Subnet الخاصة به مع الاخر .



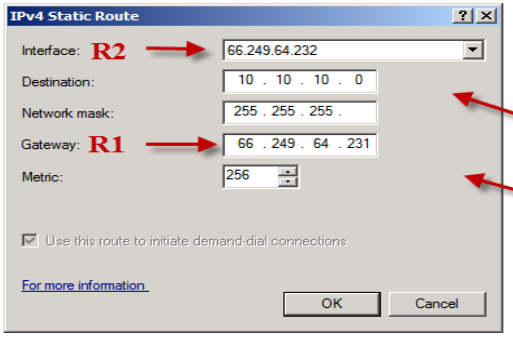
ولعمل هذا التوجيه تابع الآتي :-



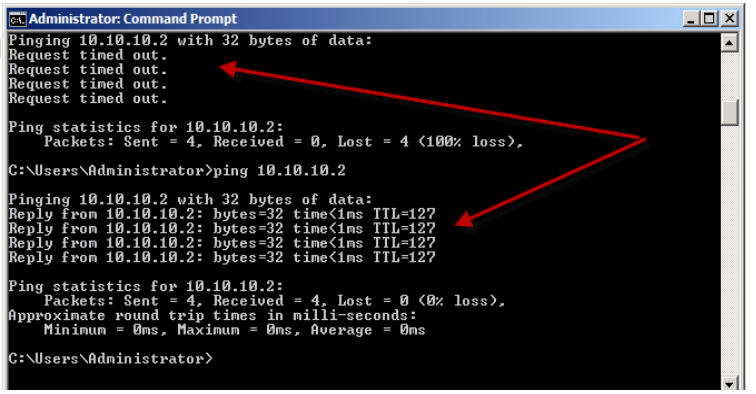




الان سنقوم بالتوجيه من داخل فرع الدوحة فتابع معي :-

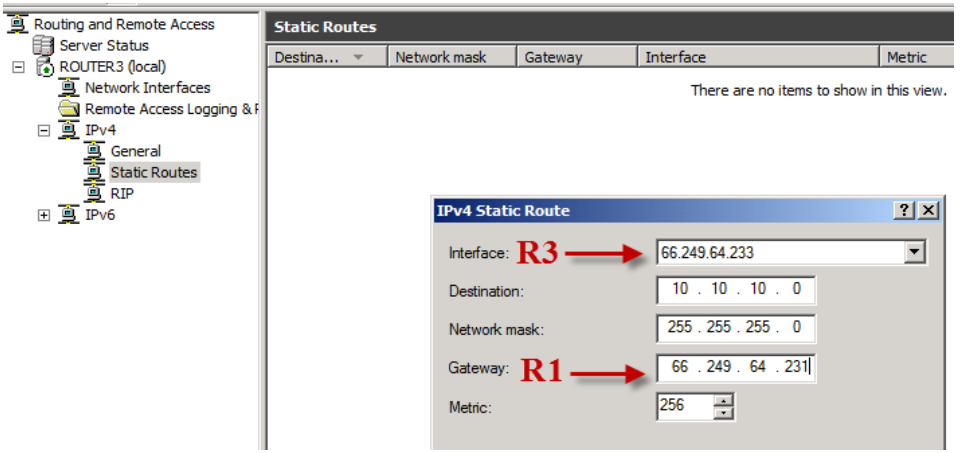


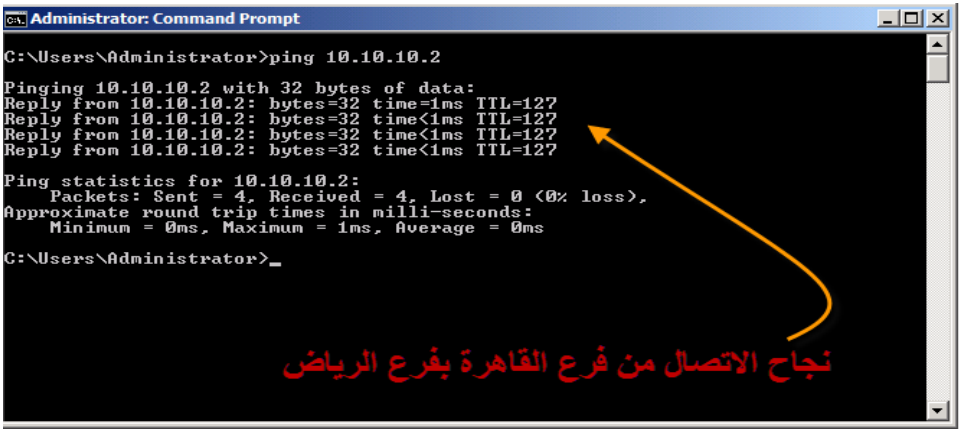
اجراء التوجية للراوتر في فرع الدوحة تماما كما قمنا بها في فرع الرياض



الاتصال قبل وبعد عملية التوجية

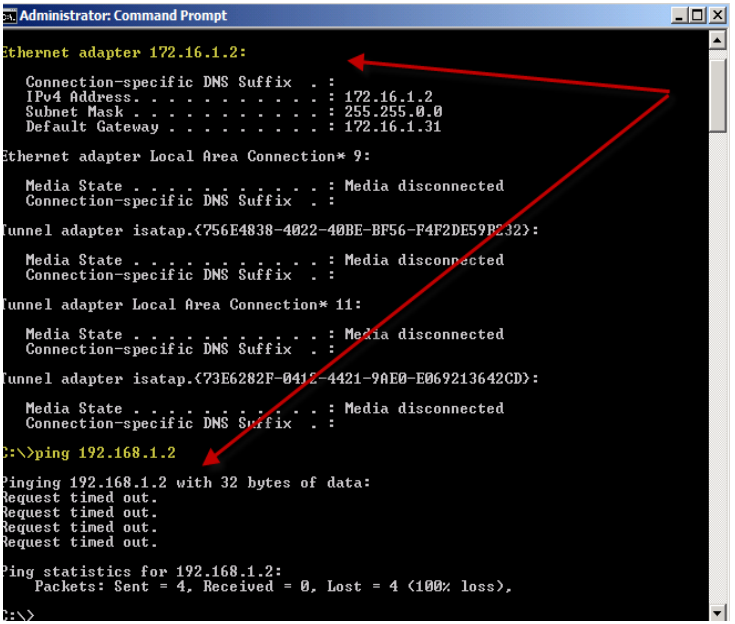
الان بقى ان نقوم بنفس العملية في فرع القاهرة واختبار الاتصال كما سبق





الان لدينا عدد router 3 وعدد subnet 4 كما في الجدول التالي :-

Sub No	Location	IP	Router No
1	Riyadh	10.10.10.2	R1
2	Doha	192.168.1.2	R2
3	Cairo	172.16.1.2	R3
4	Internet	66.249.64.231	Act Link

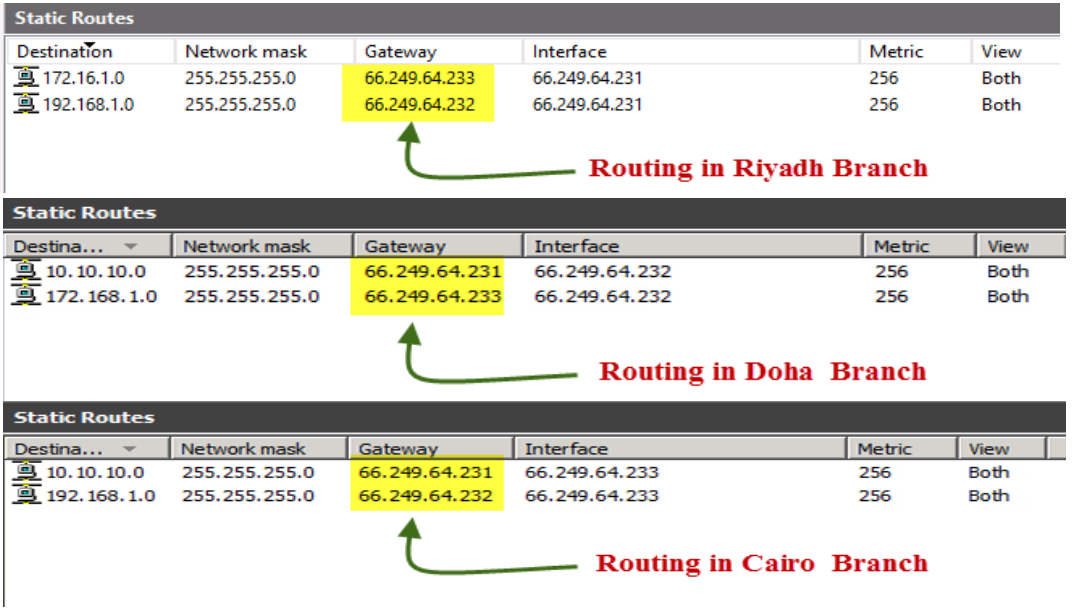


هل تلاحظ ان فرع الدوحة
مازال لا يرى فرع القاهرة ؟
ولكن الحل بسيط جدا لدرجة
انك ستقوم به بنفسك !!

نعم
ستقوم بعمل
Static Route
بين الفرعين كما
تعلمت

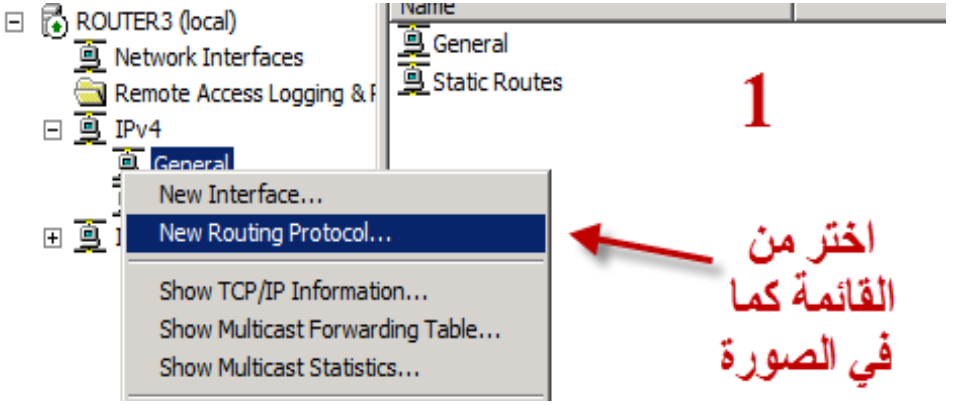
حسنا من المفترض اننا تعلمنا الان طريقة توجيه البيانات بين ال routers والآن اريدك ان تقوم بتوجيه البيانات بين كل router وآخر في اتجاهين كما في الجدول التالي :

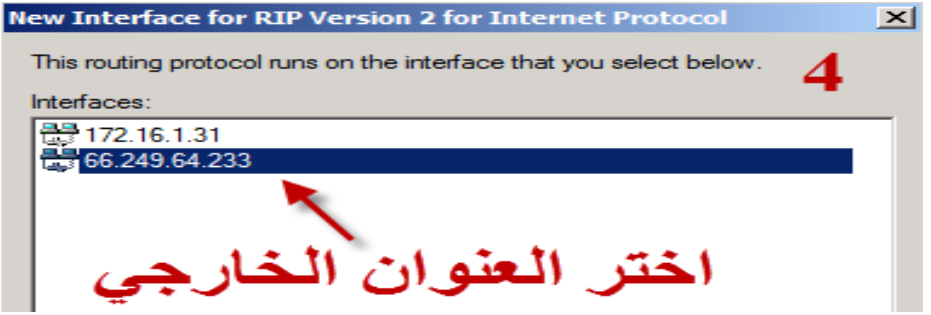
Sub No	Location	IP	Router No	Link with
1	Riyadh	10.10.10.2	R1	R2,R3
2	Doha	192.168.1.2	R2	R1,R3
3	Cairo	172.16.1.2	R3	R1,R2

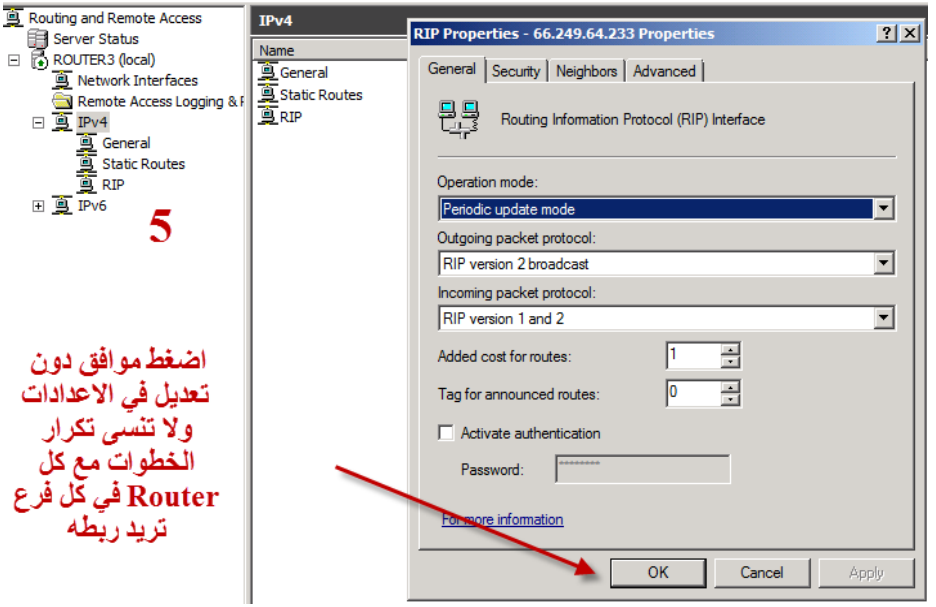


هل وجدت **صعوبة** اثناء عمل ذلك ؟

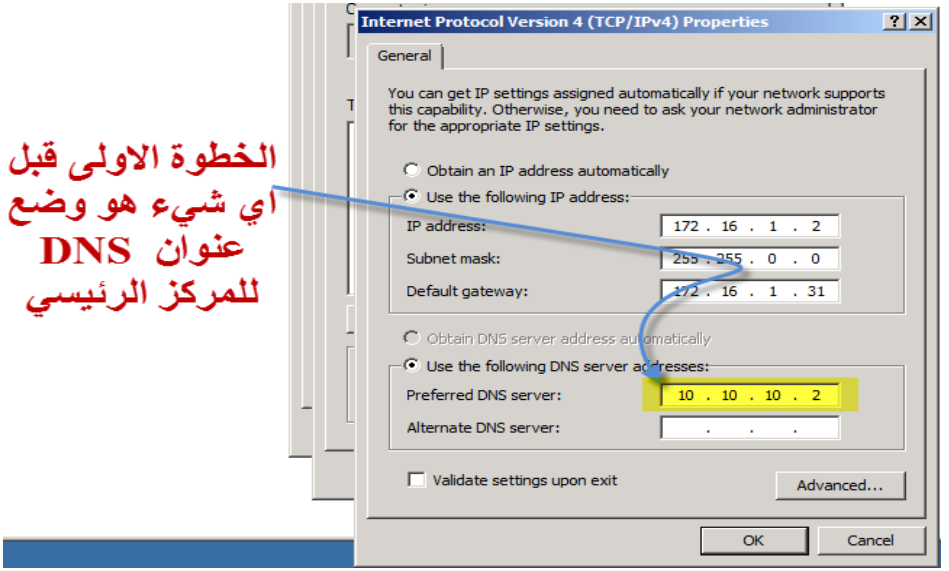
حسنا سنتعلم الان طريقة أسهل بكثير عن طريق بروتوكول الـ RIP v2 (Routing Information Protocol) وهي نفس عملية ال Static Route لكن تتم بشكل سهل وديناميكي وليس بإعداد يدوي كما فعلنا سابقا فتابع معي :-

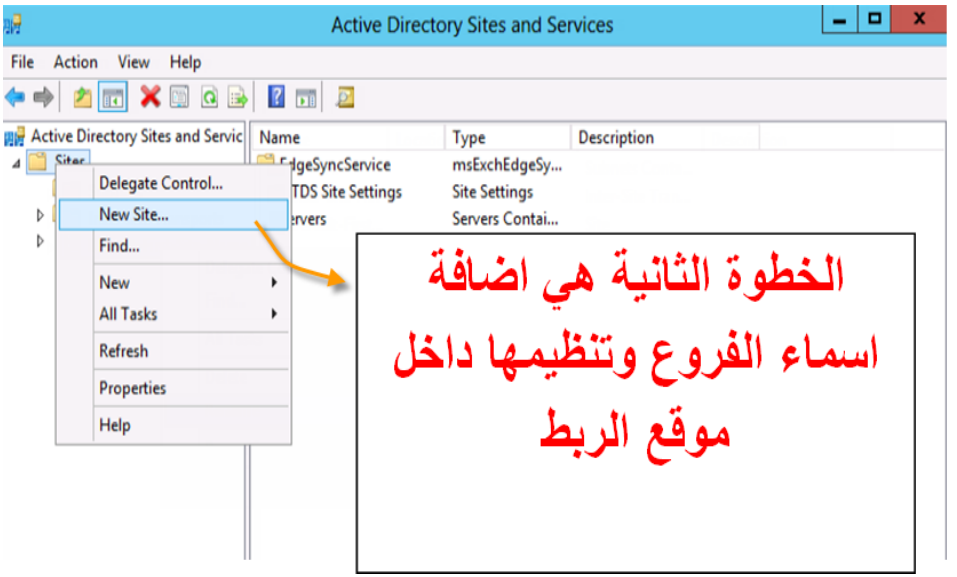




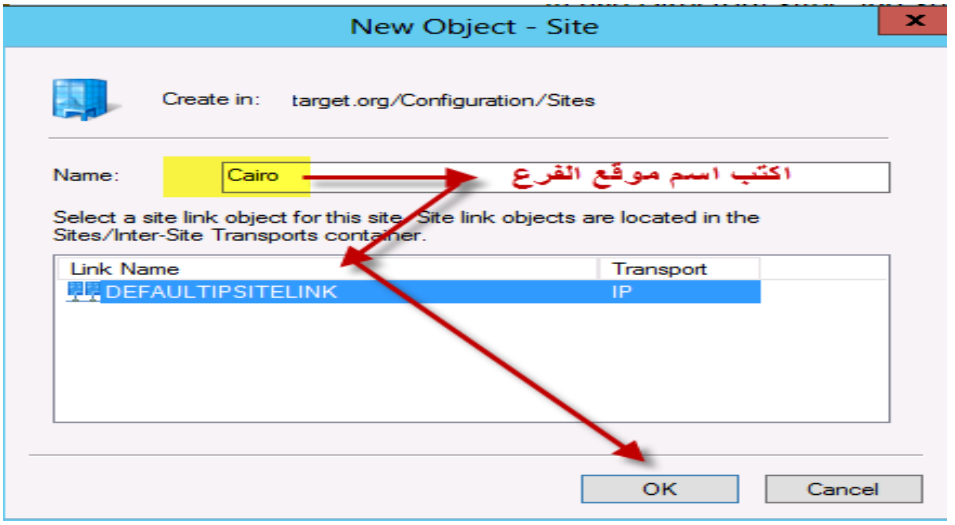


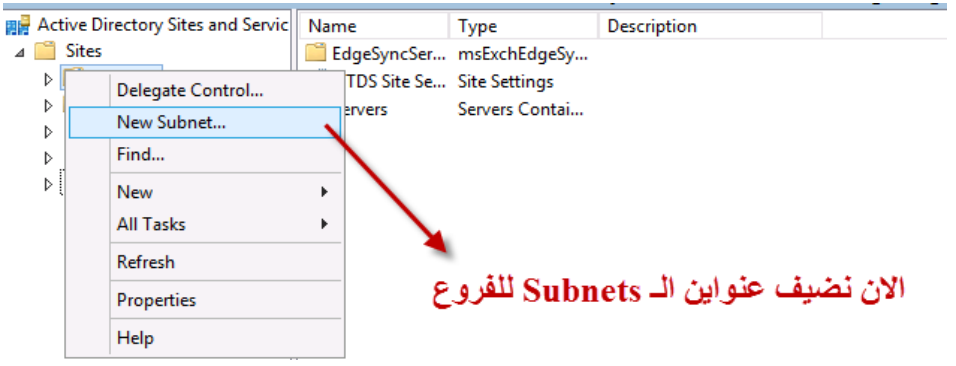
الان قد انتهينا من خطوات اعداد الـ router في الفروع كما سبق في الشرح ونأتي الان لمرحلة انضمام الاجهزة تحت المجال الرئيسي (Join Domain) لكننا قبل هذه الخطوة هناك *خطوتين مهمتين فهيا بنا نقوم بهما معا :-

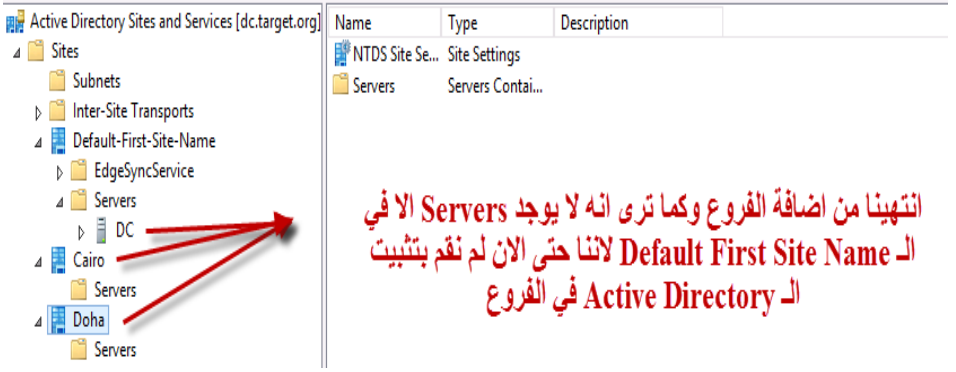


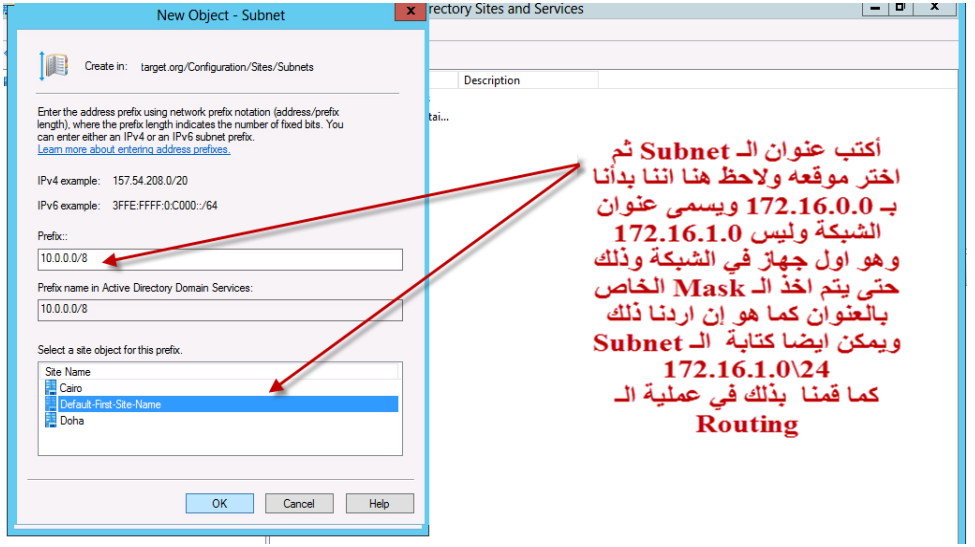


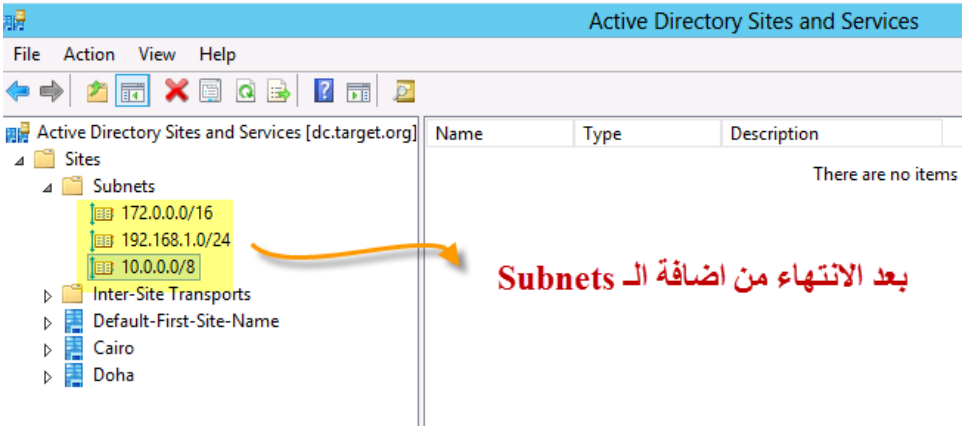
* الخطوة الثانية تتم من داخل AD Sites and Services الذي سنتعرض له بعض الشرح لاحقا


New Object - Site
Create in: target.org/Configuration/Sites
Name:
Cairo
اكتب اسم موقع الفرع
Select a site link object for this site. Site link objects are located in the Sites/Inter-Site Transports container.
Link Name
Transport
DEFAULTIPSITELINK
IP
OK
Cancel


Active Directory Sites and Servic
Sites
Name
Type
Description
EdgeSyncSer...
msExchEdgeSy...
TDS Site Se...
Site Settings
ervers
Servers Contai...
Delegate Control...
New Subnet...
Find...
New
All Tasks
Refresh
Properties
Help
الان نضيف عناوين الـ Subnets للفروع


Active Directory Sites and Services [dc.target.org]
Sites
Subnets
Inter-Site Transports
Default-First-Site-Name
EdgeSyncService
Servers
DC
Cairo
Servers
Doha
Servers
Name
Type
Description
NTDS Site Se...
Site Settings
Servers
Servers Contai...
انتهينا من اضافة الفروع وكما ترى انه لا يوجد Servers الا في الـ Default First Site Name لاننا حتى الان لم نقم بتثبيت الـ Active Directory في الفروع

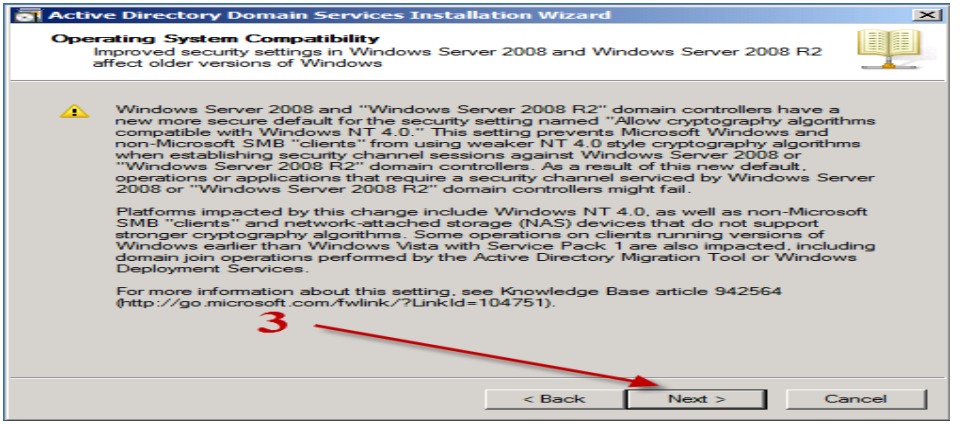


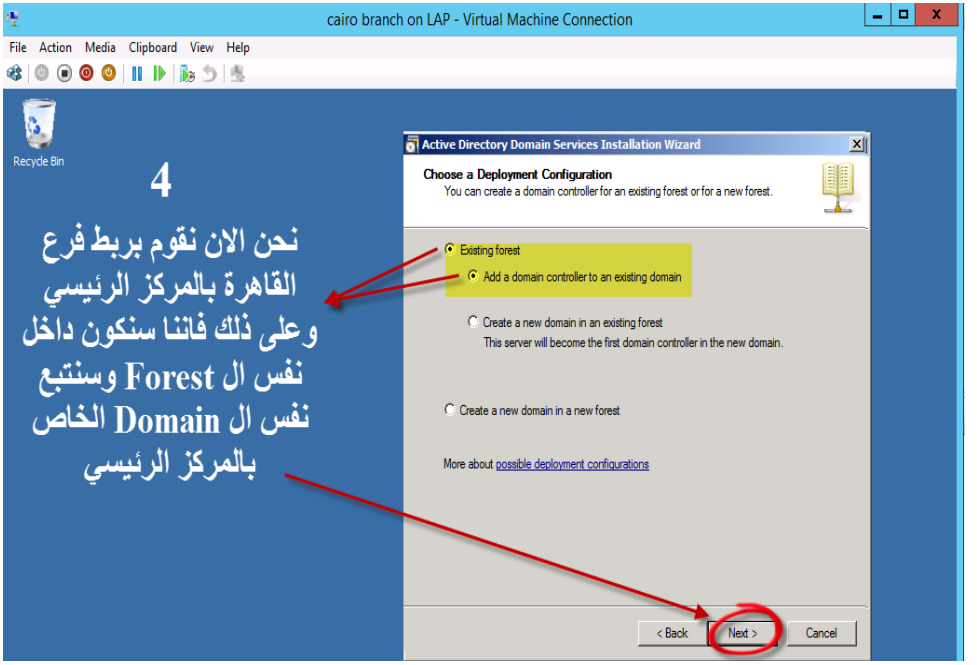


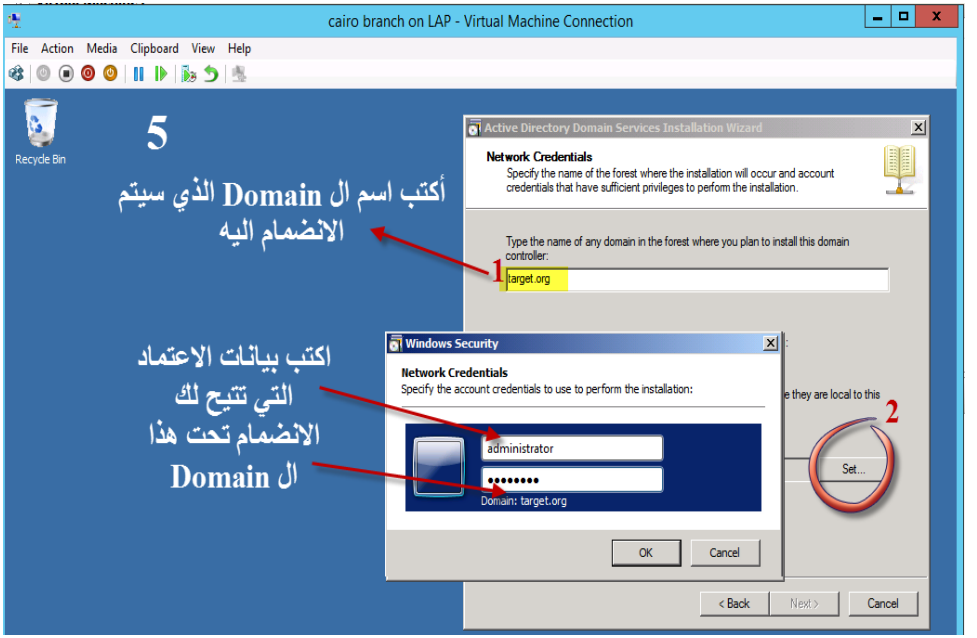
تابع معي الخطوات القادمة حيث سنقوم بالذهاب الى الخوادم الموجودة في الفروع ونبدأ معا ضبط الاعدادات الخاصة بتثبيت **Active Directory** وسنقوم بذلك اولا مع فرع القاهرة باستخدام الوضع العادي فتابع معي:-

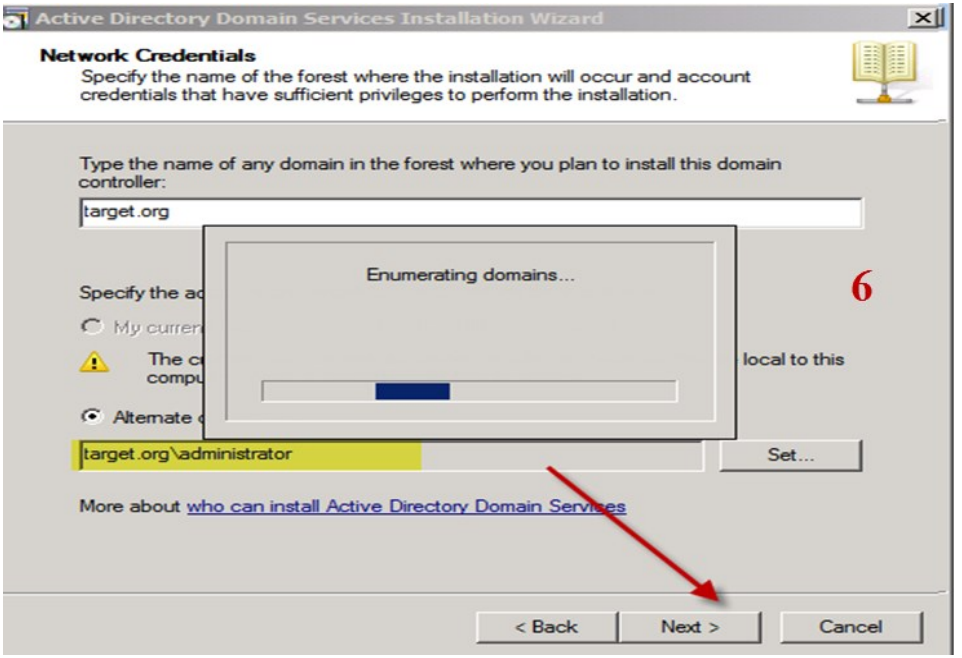

قم بتشغيل معالج تثبيت
Active Directory
1
See more results
dcpromo
Log off
Start


Active Directory Domain Services Installation Wizard
Welcome to the Active Directory Domain Services Installation Wizard
This wizard helps you install Active Directory Domain Services (AD DS) on this server, making the server an Active Directory domain controller. To continue, click Next.
Use advanced mode installation
Learn more about the additional options that are available in advanced mode installation.
More about Active Directory Domain Services
2
< Back
Next >
Cancel

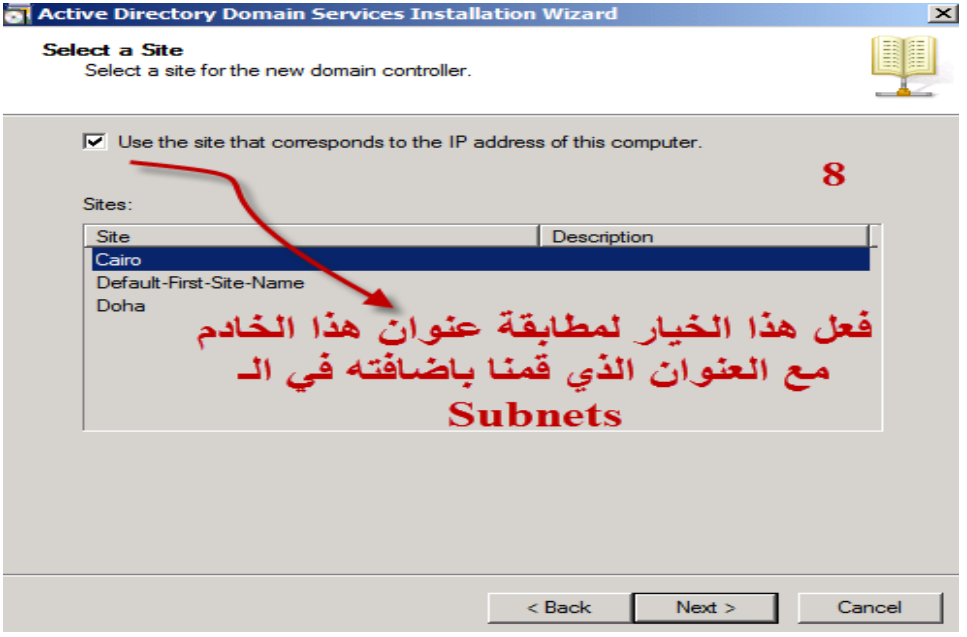

Active Directory Domain Services Installation Wizard
Operating System Compatibility
Improved security settings in Windows Server 2008 and Windows Server 2008 R2 affect older versions of Windows
Windows Server 2008 and "Windows Server 2008 R2" domain controllers have a new more secure default for the security setting named "Allow cryptography algorithms compatible with Windows NT 4.0." This setting prevents Microsoft Windows and non-Microsoft SMB "clients" from using weaker NT 4.0 style cryptography algorithms when establishing security channel sessions against Windows Server 2008 or "Windows Server 2008 R2" domain controllers. As a result of this new default, operations or applications that require a security channel serviced by Windows Server 2008 or "Windows Server 2008 R2" domain controllers might fail.
Platforms impacted by this change include Windows NT 4.0, as well as non-Microsoft SMB "clients" and network-attached storage (NAS) devices that do not support stronger cryptography algorithms. Some operations on clients running versions of Windows earlier than Windows Vista with Service Pack 1 are also impacted, including domain join operations performed by the Active Directory Migration Tool or Windows Deployment Services.
For more information about this setting, see Knowledge Base article 942564 (http://go.microsoft.com/fwlink/?LinkId=104751).
3
< Back
Next >
Cancel

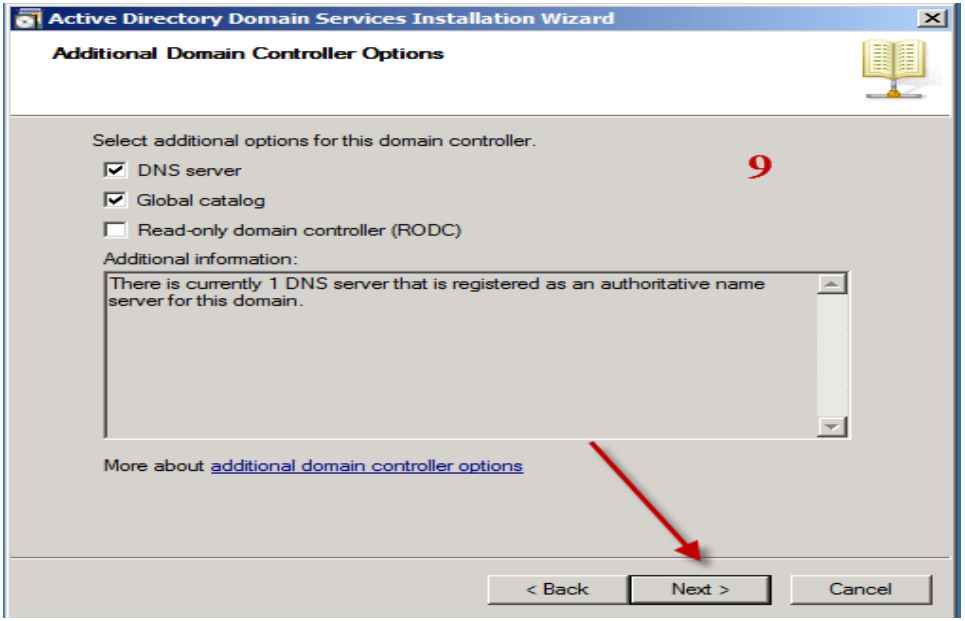

cairo branch on LAP - Virtual Machine Connection
File Action Media Clipboard View Help
Recycle Bin
4
نحن الان نقوم بربط فرع القاهرة بالمركز الرئيسي وعلى ذلك فاننا سنكون داخل نفس ال Forest وسنتبع نفس ال Domain الخاص بالمركز الرئيسي
Active Directory Domain Services Installation Wizard
Choose a Deployment Configuration
You can create a domain controller for an existing forest or for a new forest.
Existing forest
Add a domain controller to an existing domain
Create a new domain in an existing forest
This server will become the first domain controller in the new domain.
Create a new domain in a new forest
More about possible deployment configurations
< Back
Next >
Cancel


cairo branch on LAP - Virtual Machine Connection
File Action Media Clipboard View Help
Recycle Bin
5
أكتب اسم ال Domain الذي سيتم الانضمام اليه
Active Directory Domain Services Installation Wizard
Network Credentials
Specify the name of the forest where the installation will occur and account credentials that have sufficient privileges to perform the installation.
Type the name of any domain in the forest where you plan to install this domain controller:
target.org
1
اكتب بيانات الاعتماد التي تتيح لك الانضمام تحت هذا ال Domain
Windows Security
Network Credentials
Specify the account credentials to use to perform the installation:
administrator
Domain: target.org
OK
Cancel
2
Set...
< Back
Next >
Cancel

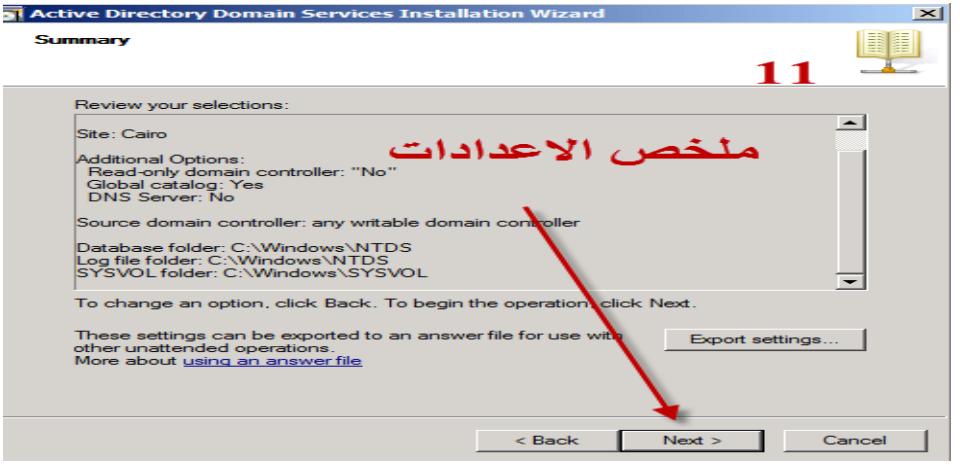

Active Directory Domain Services Installation Wizard
Network Credentials
Specify the name of the forest where the installation will occur and account credentials that have sufficient privileges to perform the installation.
Type the name of any domain in the forest where you plan to install this domain controller:
target.org
Enumerating domains...
6
local to this
target.org\administrator
Set...
More about who can install Active Directory Domain Services
< Back
Next >
Cancel

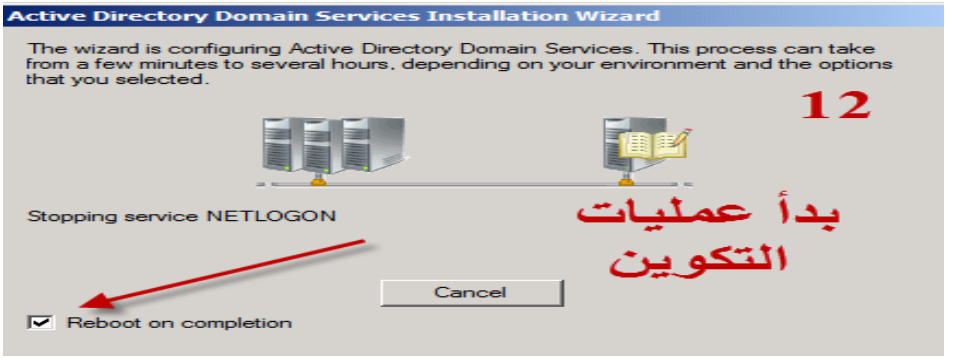

Active Directory Domain Services Installation Wizard
Select a Domain
Select a domain for this additional domain controller.
7
Domains:
target.org (forest root domain)
بعد التوثيق من بيانات الاعتماد
المدخله في الخطوة السابقة
سيظهر لنا اسم الـ Domain
< Back
Next >
Cancel

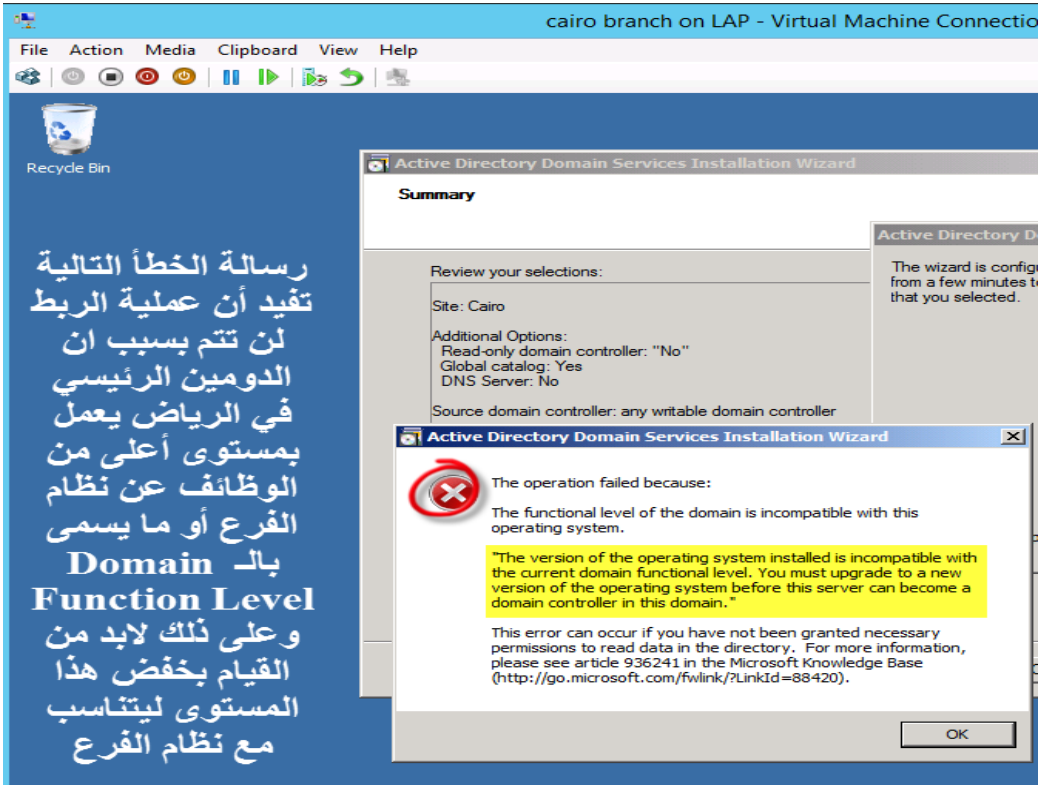

Active Directory Domain Services Installation Wizard
Select a Site
Select a site for the new domain controller.
Use the site that corresponds to the IP address of this computer.
8
Sites:
Site
Description
Cairo
Default-First-Site-Name
Doha
فعل هذا الخيار لمطابقة عنوان هذا الخادم
مع العنوان الذي قمنا باضافته في الـ
Subnets
< Back
Next >
Cancel


Active Directory Domain Services Installation Wizard
Additional Domain Controller Options
Select additional options for this domain controller.
DNS server
Global catalog
Read-only domain controller (RODC)
9
Additional information:
There is currently 1 DNS server that is registered as an authoritative name server for this domain.
More about additional domain controller options
< Back
Next >
Cancel


Active Directory Domain Services Installation Wizard
Directory Services Restore Mode Administrator Password
10
The Directory Services Restore Mode Administrator account is different from the domain Administrator account.
Assign a password for the Administrator account that will be used when this domain controller is started in Directory Services Restore Mode. We recommend that you choose a strong password.
Password:
Confirm password:
More about Directory Services Restore Mode password
تابع الخطوات حتى يطلب منك
ادخال كلمة مرور الـ
Restore Mode
< Back
Next >
Cancel


Active Directory Domain Services Installation Wizard
Summary
11
Review your selections:
Site: Cairo
Additional Options:
Read-only domain controller: "No"
Global catalog: Yes
DNS Server: No
ملخص الاعدادات
Source domain controller: any writable domain controller
Database folder: C:\Windows\NTDS
Log file folder: C:\Windows\NTDS
SYSVOL folder: C:\Windows\SYSVOL
To change an option, click Back. To begin the operation, click Next.
These settings can be exported to an answer file for use with other unattended operations.
More about using an answer file
Export settings...
< Back
Next >
Cancel


Active Directory Domain Services Installation Wizard
The wizard is configuring Active Directory Domain Services. This process can take from a few minutes to several hours, depending on your environment and the options that you selected.
12
Stopping service NETLOGON
بدأ عمليات
التكوين
Cancel
Reboot on completion

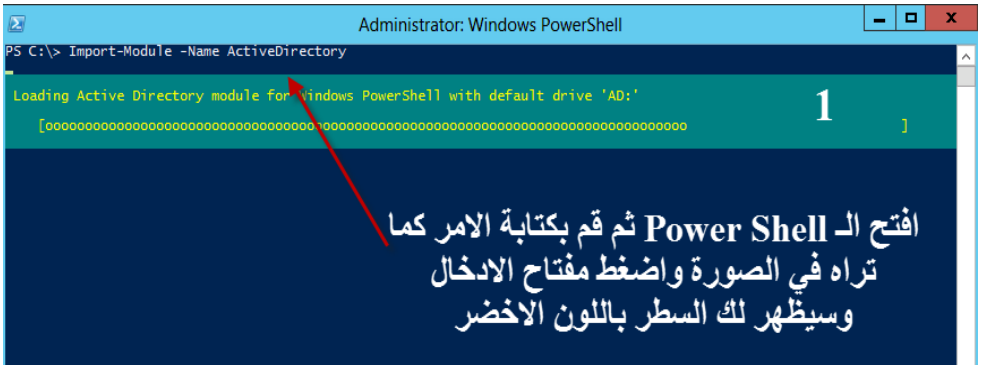


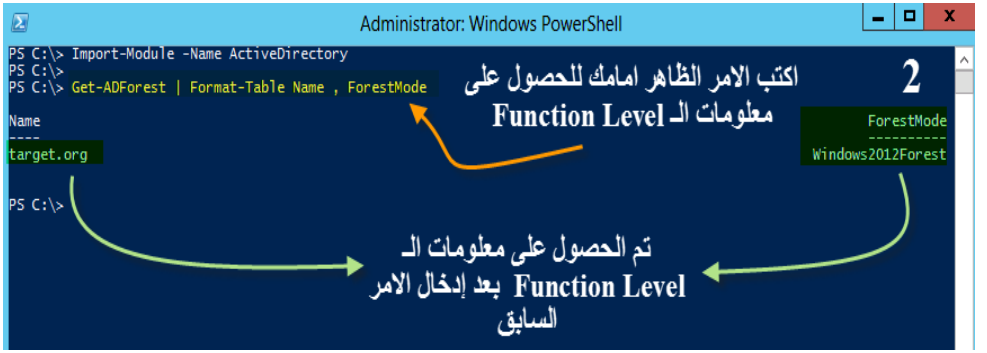
كما نرى فقد ظهرت لنا رسالة **خطأ** تفيد بوجود مشكلة عدم توافق مستوى الوظائف بين كلا من الخادم الموجود في المركز الرئيسي والذي يعمل بنظام التشغيل 2012 وبين هذا الخادم العامل بنظام التشغيل 2008 ولذلك لم يتم اكمال عملية التثبيت

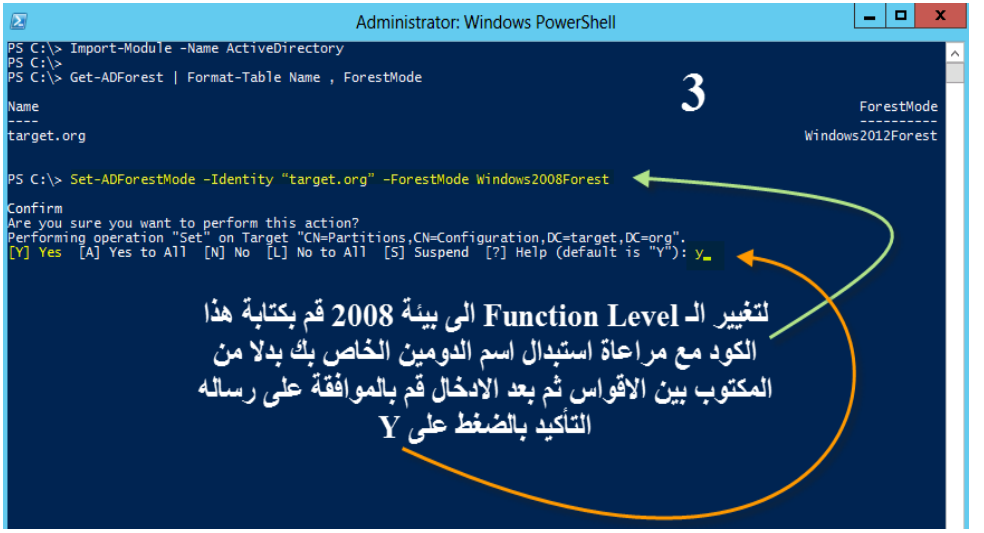
ولحل هذه المشكلة يتوجب علينا إما ترقية نظام التشغيل الخاص بالفروع الى بيئة 2012 أو الطريقة الاسهل وهي الذهاب لخادم الفرع الرئيسي وعمل ما يسمى

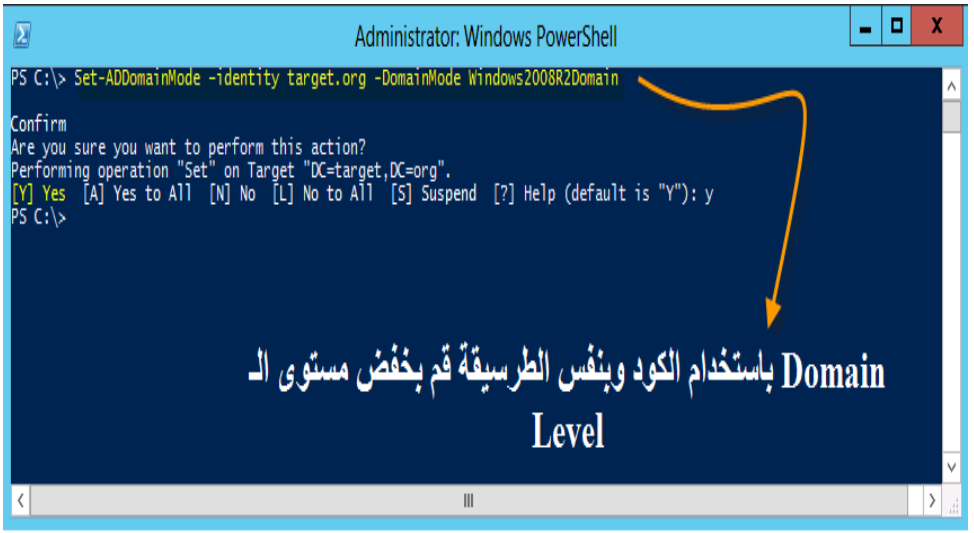
(Raise Domain Function Level)

Raise Domain Function Level









بهذا نكون قد قمنا بخفض مستوى الـ Function level من 2012 الى 2008 والأكواد المستخدمة هي التالية :-

Raise Forest

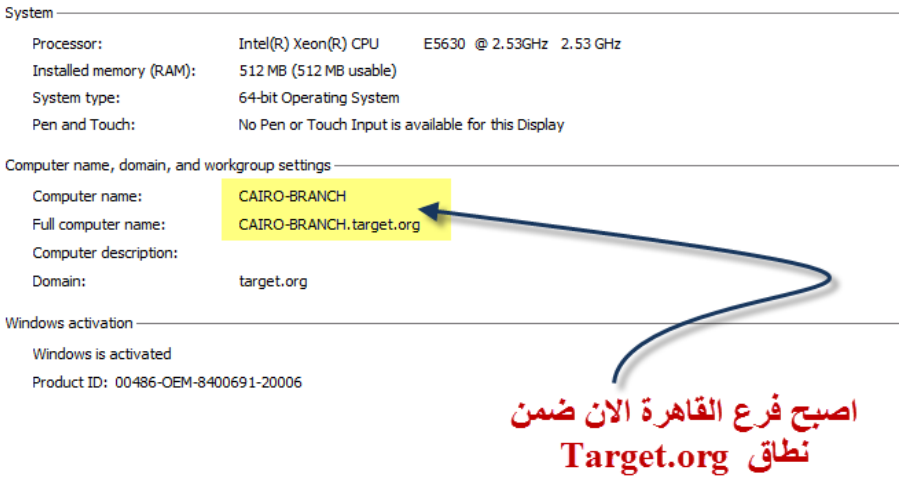
```
Import-Module –Name ActiveDirectory

Get-ADForest | Format-Table Name , ForestMode

Set-ADForestMode –Identity “target.org” –ForestMode Windows2008Forest
```

Raise Domain

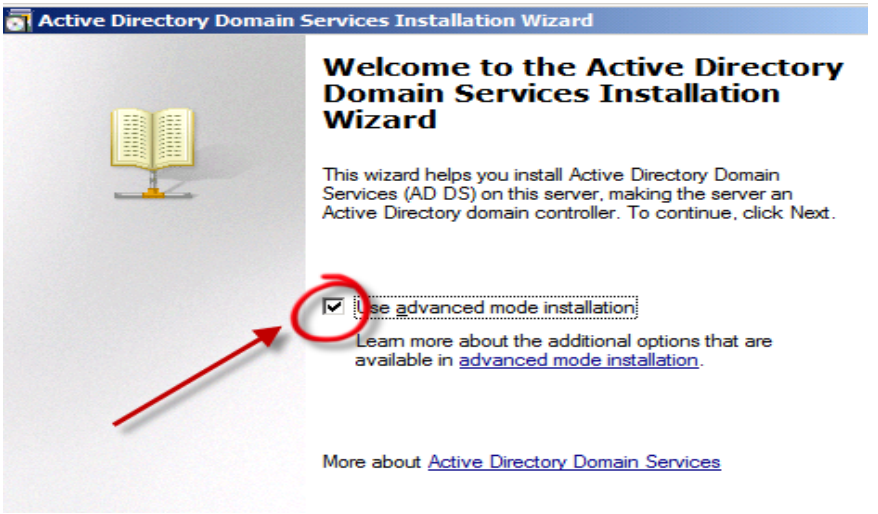
```
Get-ADDomain –identity target.org

Set-ADDomainMode –identity target.org –DomainMode Windows2008Domain
```

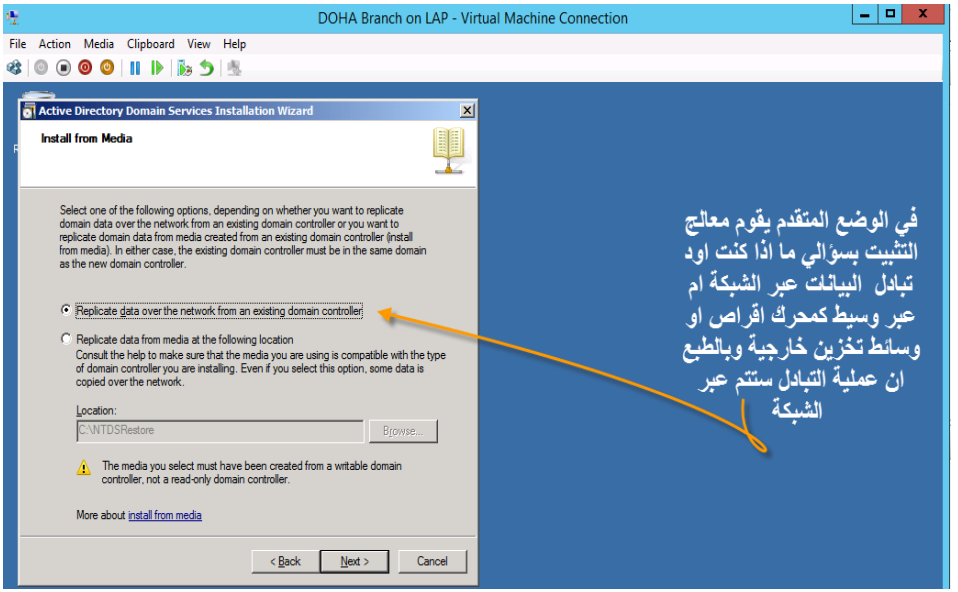
لا تنسى استبدال الكلمات باللون الاحمر باسم Domain/ forest الخاص بك وبالمستوى الذي تود الانتقال اليه .

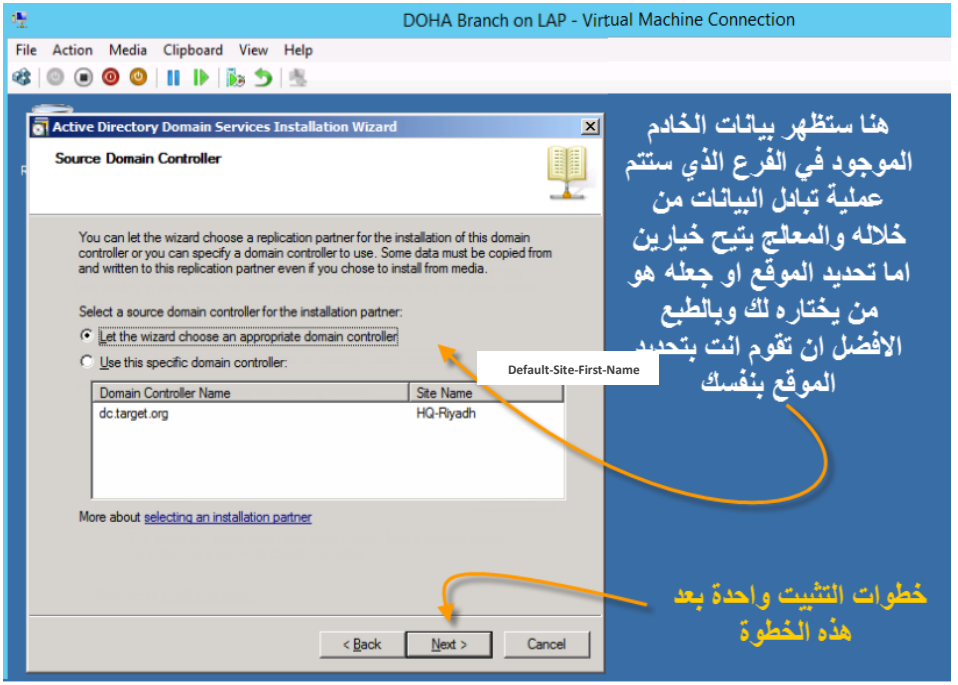
بعد ذلك نتابع تثبيت Active Directory في أجهزة الفروع بدون مشاكل



والآن سنقوم بربط فرع الدوحة كما فعلنا سابقا لكننا الان سنستخدم الوضع المتقدم في التثبيت مع العلم ان خطوات التثبيت نفسها ولكن بزيادة خطوتين فقط




DOHA Branch on LAP - Virtual Machine Connection
File Action Media Clipboard View Help
Active Directory Domain Services Installation Wizard
Install from Media
Select one of the following options, depending on whether you want to replicate domain data over the network from an existing domain controller or you want to replicate domain data from media created from an existing domain controller (install from media). In either case, the existing domain controller must be in the same domain as the new domain controller.
Replicate data over the network from an existing domain controller
Replicate data from media at the following location
Consult the help to make sure that the media you are using is compatible with the type of domain controller you are installing. Even if you select this option, some data is copied over the network.
Location:
C:\NTDSRestore
Browse...
The media you select must have been created from a writable domain controller, not a read-only domain controller.
More about install from media
< Back
Next >
Cancel
في الوضع المتقدم يقوم معالج التثبيت بسؤالي ما اذا كنت اود تبادل البيانات عبر الشبكة ام عبر وسيط كمحرك اقراص او وسائط تخزين خارجية وبالطبع ان عملية التبادل ستتم عبر الشبكة


DOHA Branch on LAP - Virtual Machine Connection
File Action Media Clipboard View Help
Active Directory Domain Services Installation Wizard
Source Domain Controller
You can let the wizard choose a replication partner for the installation of this domain controller or you can specify a domain controller to use. Some data must be copied from and written to this replication partner even if you chose to install from media.
Select a source domain controller for the installation partner:
Let the wizard choose an appropriate domain controller
Use this specific domain controller:
Domain Controller Name
Site Name
dc.target.org
HQ-Riyadh
Default-Site-First-Name
More about selecting an installation partner
< Back
Next >
Cancel
هنا ستظهر بيانات الخادم الموجود في الفرع الذي ستتم عملية تبادل البيانات من خلاله والمعالج يتيح خيارين اما تحديد الموقع او جعله هو من يختاره لك وبالطبع الافضل ان تقوم انت بتحديد الموقع بنفسك
خطوات التثبيت واحدة بعد هذه الخطوة

الان انتهينا من ربط كلا الفرعين بنفس المجال وهذا يعني اننا قمنا بعمل Additional Domain وهو صورة طبق الاصل من الـ Primary Domain الموجود في المركز الرئيسي وحتى يكون صورة طبق الاصل كما قلنا لابد من ان يحصل على كل المعلومات من الـ Primary Domain وهذا ما يمسى بـ عملية الـ Replication أي نسخ البيانات من Server لآخر.

وهناك نوعان من الـ Replication بين الـ Sites وهما:

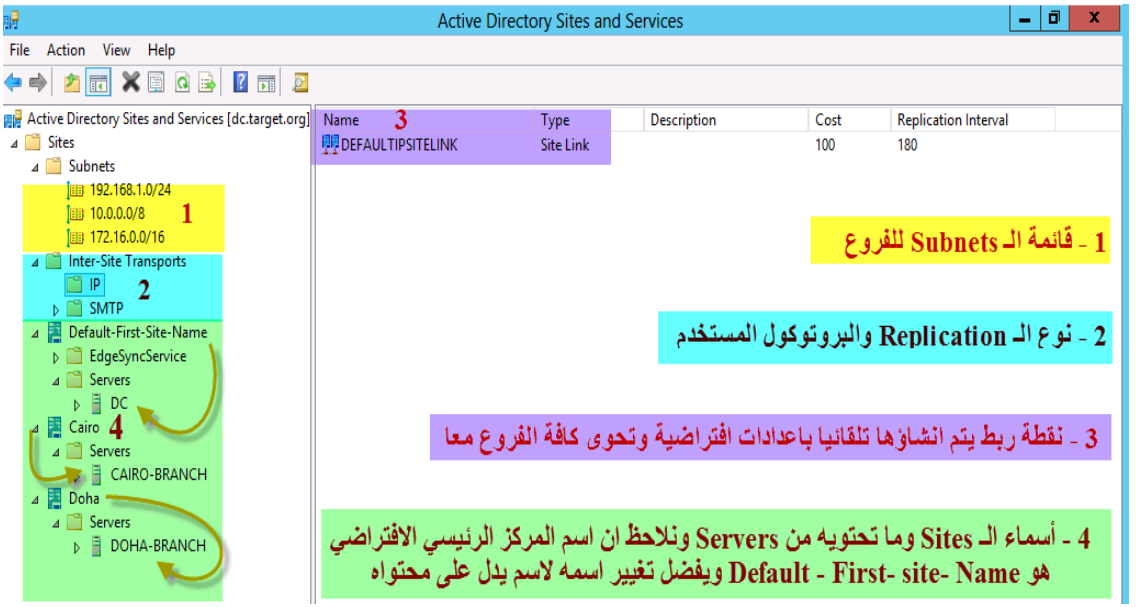
INTRA Site Replication وهي بين السيرفرات في نفس الموقع(Site)

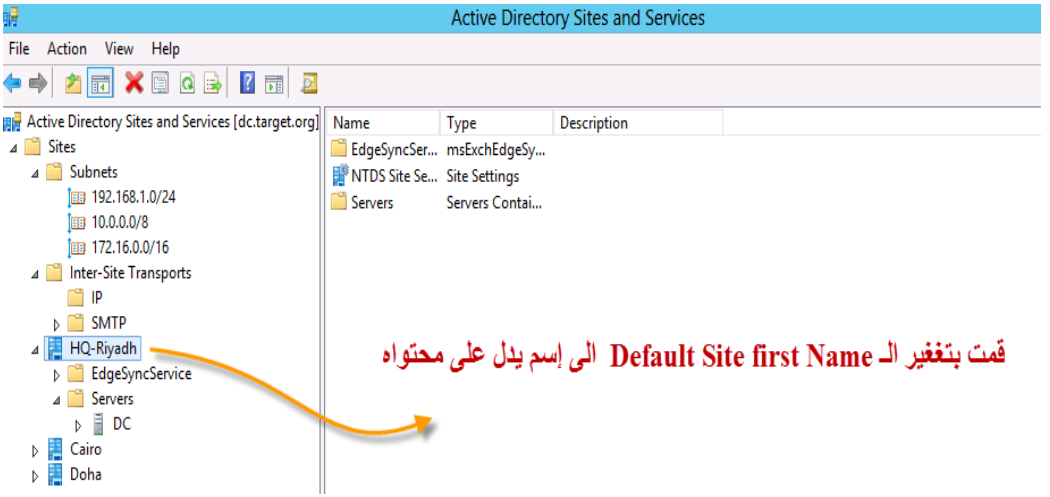
INTER Site Replication وهي بين السيرفرات في مواقع مختلفة وهو الواقع في حالتنا هذه وللتقريب نضرب المثال التالي :-

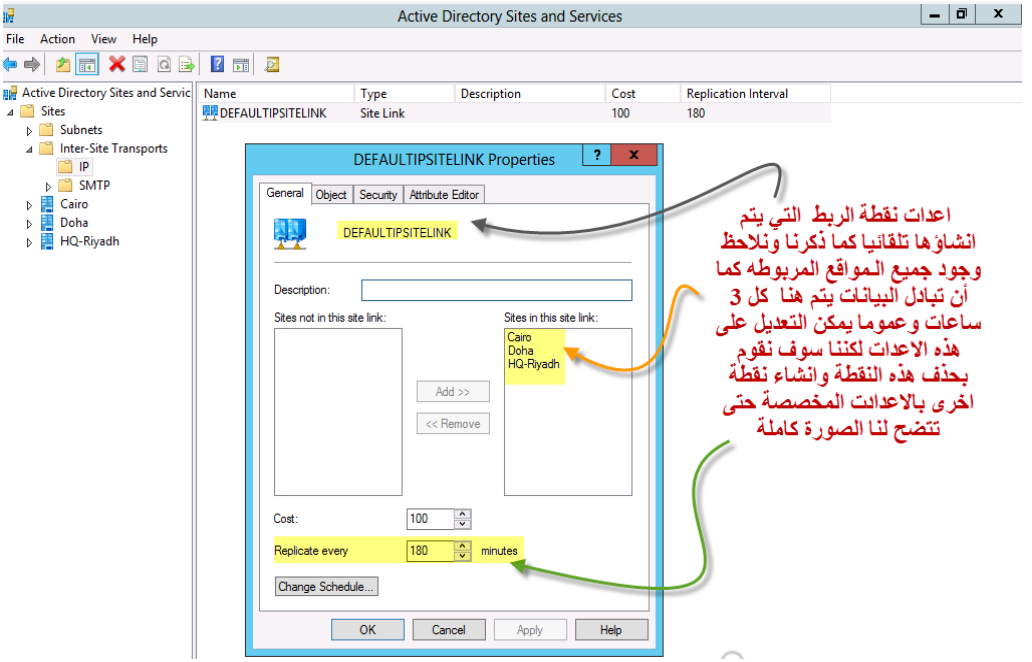
لنفترض أنك أنشأت User جديد في الـ Active Directory من فرع القاهرة وبما ان فرع القاهر موجود في موقع مختلف عن فرع الرياض فسوف يقوم الخادم الموجود في القاهرة بإبلاغ الخادم الموجود في الرياض بان هناك مستخدم جديد وهذا بعد مرور من 15 دقيقة الى 3 ساعات وهذا هو (الوضع الافتراضي) ليقوم بعد ذلك خادم الرياض بنسخ هذا المستخدم إلى قاعدة بياناته و هذه العملية تسمى INTER Site Replication ويستخدم فيها بروتوكول MSTP or RPC

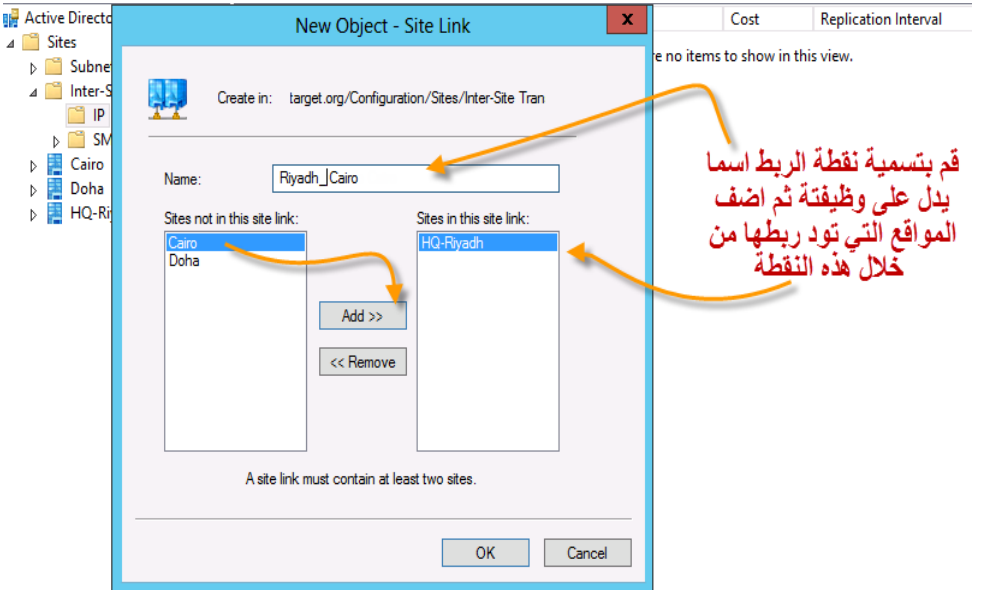
أما اذا كان الخادم في القاهرة والرياض بنفس الموقع وقمت بإنشاء مستخدم جديد فسيقوم الخادم بالإبلاغ ولكن بعد مرور 15 ثانية كحد أقصى وهذه العملية تسمى INTRA Site Replication ويستخدم بروتوكول KCC .

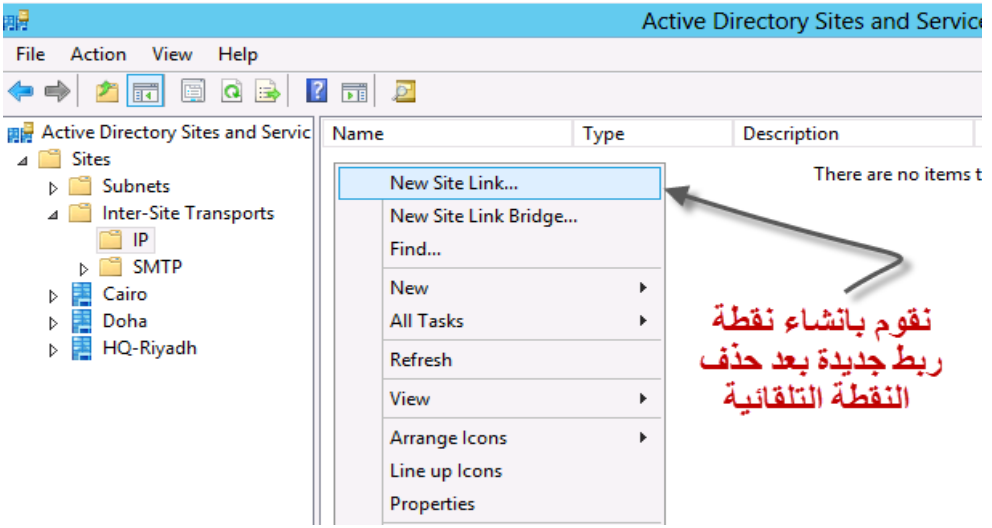
أصبحت الفروع الان متصلة بالمركز الرئيسي وقبل البدء بإدارتها وضبط الاعدادات الخاصة بعمليات الـ Replication دعونا نلقي نظرة على شكل الـ Active Directory Sites and Services وشرح الافتراضيات التي سنعمل عليها لاحقا .

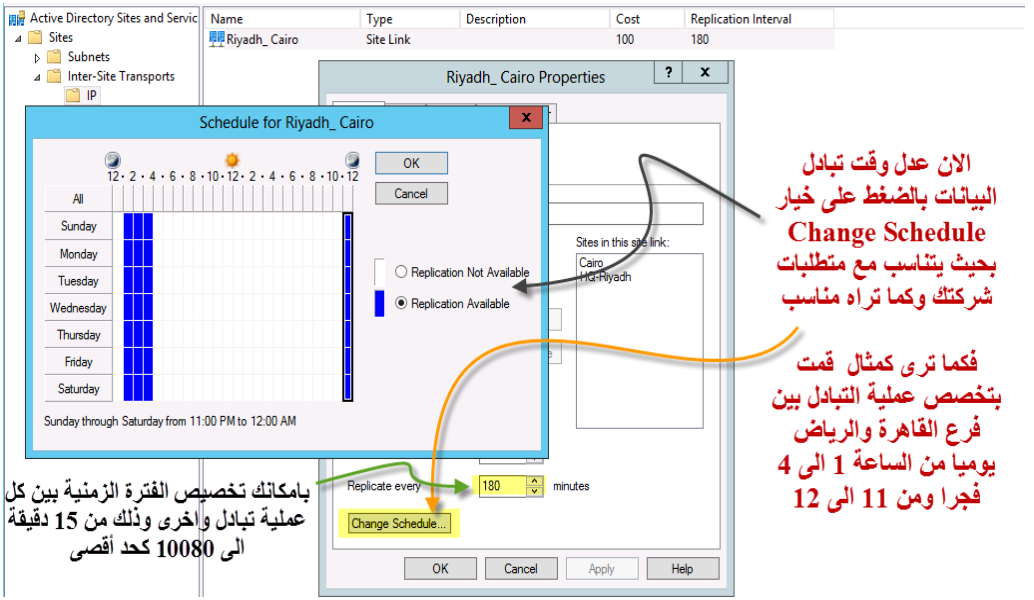


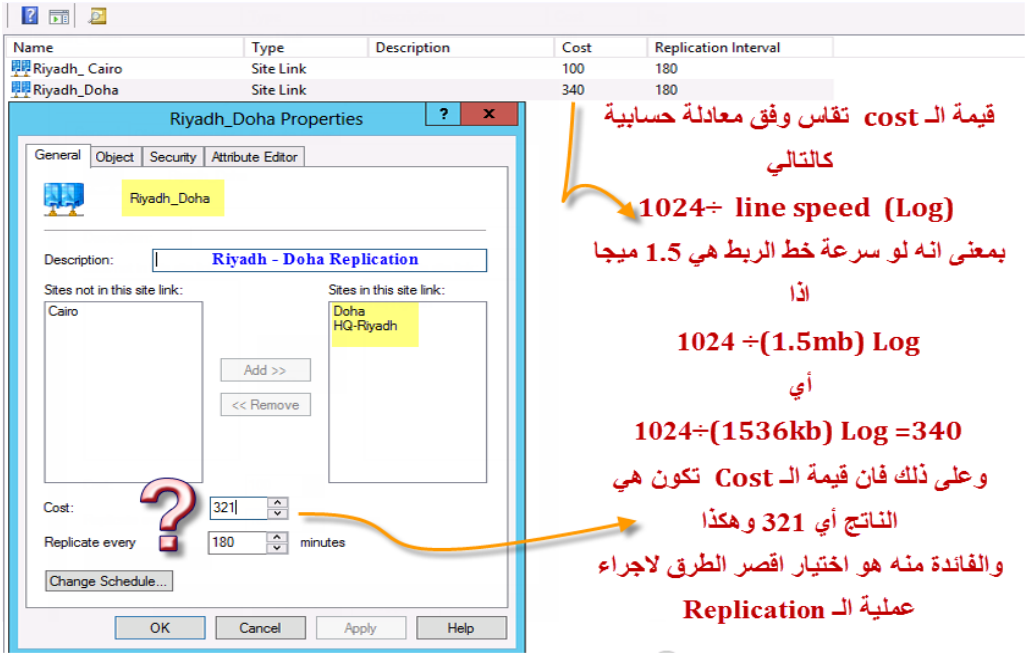

Active Directory Sites and Services
File Action View Help
Active Directory Sites and Services [dc.target.org]
Sites
Subnets
192.168.1.0/24
10.0.0.0/8
172.16.0.0/16
Inter-Site Transports
IP
SMTP
HQ-Riyadh
EdgeSyncService
Servers
DC
Cairo
Doha
Name Type Description
EdgeSyncSer... msExchEdgeSy...
NTDS Site Se... Site Settings
Servers Servers Contai...
قمت بتغيير الـ Default Site first Name الى إسم يدل على محتواه


Active Directory Sites and Services
File Action View Help
Active Directory Sites and Servic
Sites
Subnets
Inter-Site Transports
IP
SMTP
Cairo
Doha
HQ-Riyadh
Name Type Description Cost Replication Interval
DEFAULTIPSITELINK Site Link 100 180
DEFAULTIPSITELINK Properties
General Object Security Attribute Editor
DEFAULTIPSITELINK
Description:
Sites not in this site link:
Sites in this site link:
Cairo
Doha
HQ-Riyadh
Add >>
<< Remove
Cost: 100
Replicate every 180 minutes
Change Schedule...
OK Cancel Apply Help
اعدات نقطة الربط التي يتم انشاؤها تلقائيا كما ذكرنا ونلاحظ وجود جميع المواقع المربوطه كما أن تبادل البيانات يتم هنا كل 3 ساعات وعموما يمكن التعديل على هذه الاعدات لكننا سوف نقوم بحذف هذه النقطة وانشاء نقطة اخرى بالاعدادت المخصصة حتى تتضح لنا الصورة كاملة

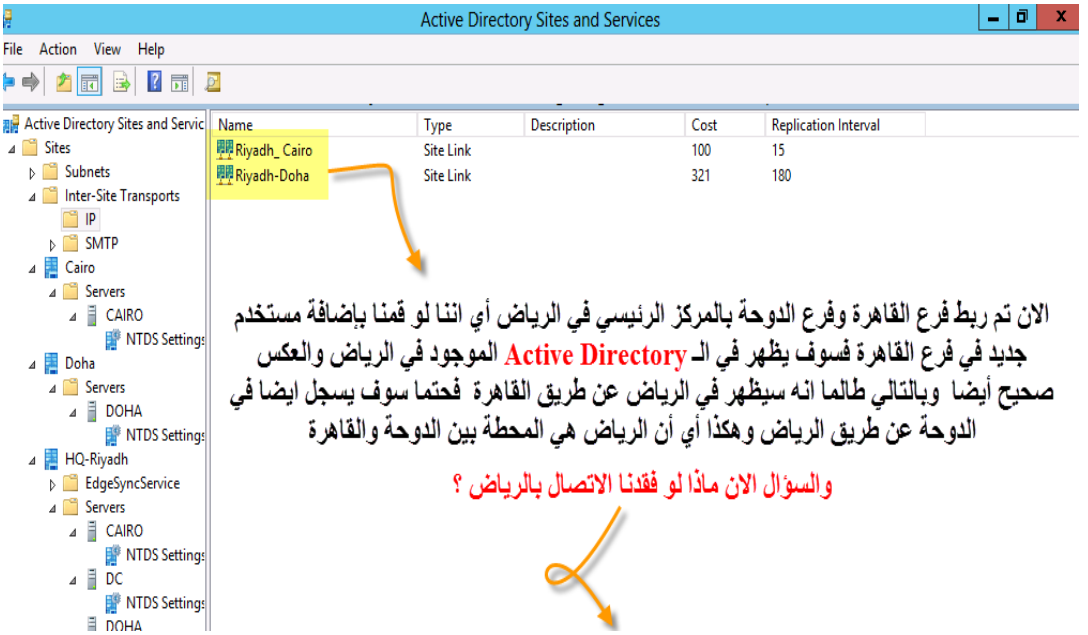

New Object - Site Link
Create in: target.org/Configuration/Sites/Inter-Site Tran
Name: Riyadh_Cairo
Sites not in this site link:
Cairo
Doha
Add >>
<< Remove
Sites in this site link:
HQ-Riyadh
A site link must contain at least two sites.
OK
Cancel
Cost
Replication Interval
no items to show in this view.
قم بتسمية نقطة الربط اسما يدل على وظيفتة ثم اضف المواقع التي تود ربطها من خلال هذه النقطة


Active Directory Sites and Servic
File Action View Help
Active Directory Sites and Servic
Sites
Subnets
Inter-Site Transports
IP
SMTP
Cairo
Doha
HQ-Riyadh
Name
Type
Description
There are no items t
New Site Link...
New Site Link Bridge...
Find...
New
All Tasks
Refresh
View
Arrange Icons
Line up Icons
Properties
نقوم بانشاء نقطة ربط جديدة بعد حذف النقطة التلقائية


Active Directory Sites and Servic
Sites
Subnets
Inter-Site Transports
IP
Name
Type
Description
Cost
Replication Interval
Riyadh_ Cairo
Site Link
100
180
Riyadh_ Cairo Properties
Schedule for Riyadh_ Cairo
OK
Cancel
All
Sunday
Monday
Tuesday
Wednesday
Thursday
Friday
Saturday
Replication Not Available
Replication Available
Sunday through Saturday from 11:00 PM to 12:00 AM
Sites in this site link:
Cairo
HQ-Riyadh
Replicate every
180
minutes
Change Schedule...
OK
Cancel
Apply
Help
الان عدل وقت تبادل البيانات بالضغط على خيار Change Schedule بحيث يتناسب مع متطلبات شركتك وكما تراه مناسب
فكما ترى كمثال قمت بتخصص عملية التبادل بين فرع القاهرة والرياض يوميا من الساعة 1 الى 4 فجرا ومن 11 الى 12
بامكانك تخصيص الفترة الزمنية بين كل عملية تبادل واخرى وذلك من 15 دقيقة الى 10080 كحد أقصى


Name
Type
Description
Cost
Replication Interval
Riyadh_ Cairo
Site Link
100
180
Riyadh_Doha
Site Link
340
180
Riyadh_Doha Properties
General
Object
Security
Attribute Editor
Riyadh_Doha
Description:
Riyadh - Doha Replication
Sites not in this site link:
Cairo
Sites in this site link:
Doha
HQ-Riyadh
Add >>
<< Remove
Cost:
321
Replicate every
180
minutes
Change Schedule...
OK
Cancel
Apply
Help
قيمة الـ cost تقاس وفق معادلة حسابية كالتالي
1024÷ line speed (Log)
بمعنى انه لو سرعة خط الربط هي 1.5 ميجا
اذا
1024 ÷(1.5mb) Log
أي
1024÷(1536kb) Log =340
وعلى ذلك فان قيمة الـ Cost تكون هي الناتج أي 321 وهكذا
والفائدة منه هو اختيار اقصر الطرق لاجراء عملية الـ Replication

حتى تفهم ما هو الـCost وما هي وظيفته فانظر الـ Site Link أعلاه هو بين موقعي الرياض والدوحة وله القيمة 321 وهي ناتج المعادلة (Log) 1024 ÷ line speed ولنفترض الان وجود خط آخر احتياطي ليربط بين نفس الموقعين وهذا الخط بطيء مثلا بسرعة 512 و أنشأنا Site Linkجديد لهذا الخط الاحتياطي وفي هذه الحالة يجب وضع قيمة الـ Cost لهذا الـ Site Linkالجديد ووفقا للقاعدة السابقة سيكون قيمة الـ Cost هي (Log)512 ÷ 1024 = 377



الاجابة هي اننا سنفقد الاتصال بين كل الفروع لان القاهرة والدوحة تتصلان عبر الرياض والرياض اصلا غير متصل .. !

والحل هو :- انشاء موقع ربط بين القاهرة والدوحة ففي حالة تعطل الرياض فأنهما يعملان حتى نقوم بإصلاحه وسيقوم بعمل Replication مع الفروع لاستقبال الـ Updates منهما وكأن شيئا لم يكمن .

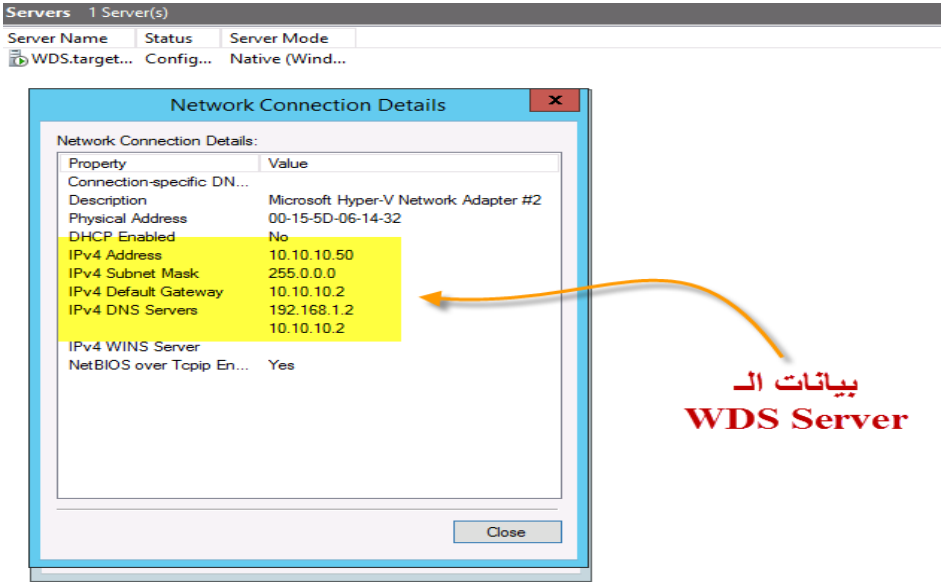
حسنا عليك الان ان تقوم بعمل ذلك **بنفسك** .

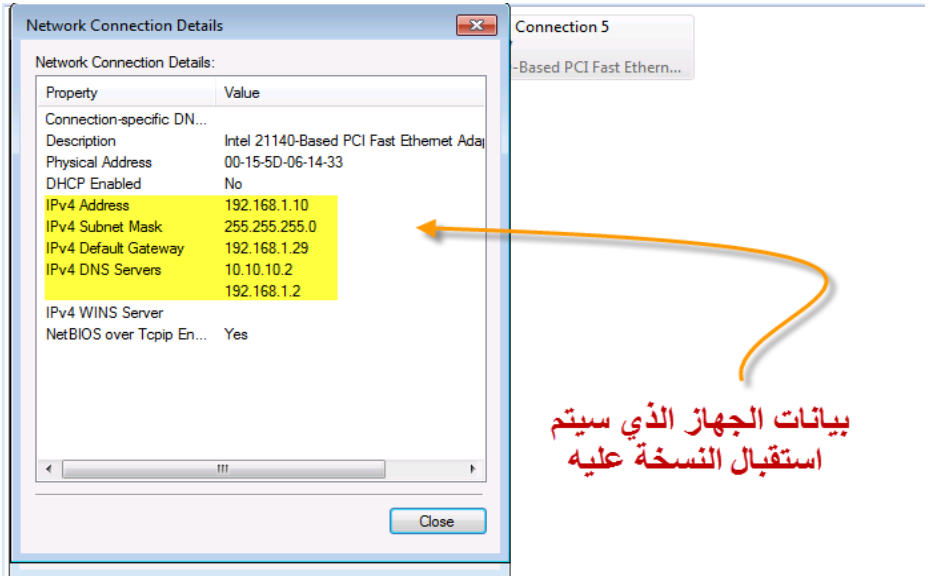
وللتأكيد على ربط الفروع بعضها ببعض دعونا نقوم بعمل Windows Deployment Service (WDS)

كتجربة

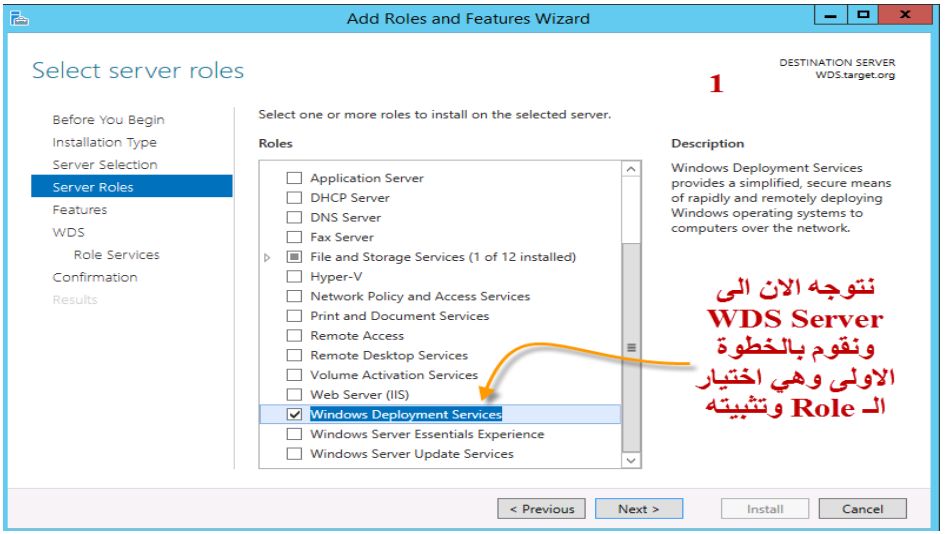
وكما هو معروف فان خدمة الـ Windows Deployment Service هي خدمة لنشر نظام التشغيل من خلال الشبكة وبما ان لدينا شبكة من عدة فروع وفي مدن مختلفة فسيكون من الرائع اختبار اتصال شبكتنا عبر خدمة الـ WDS

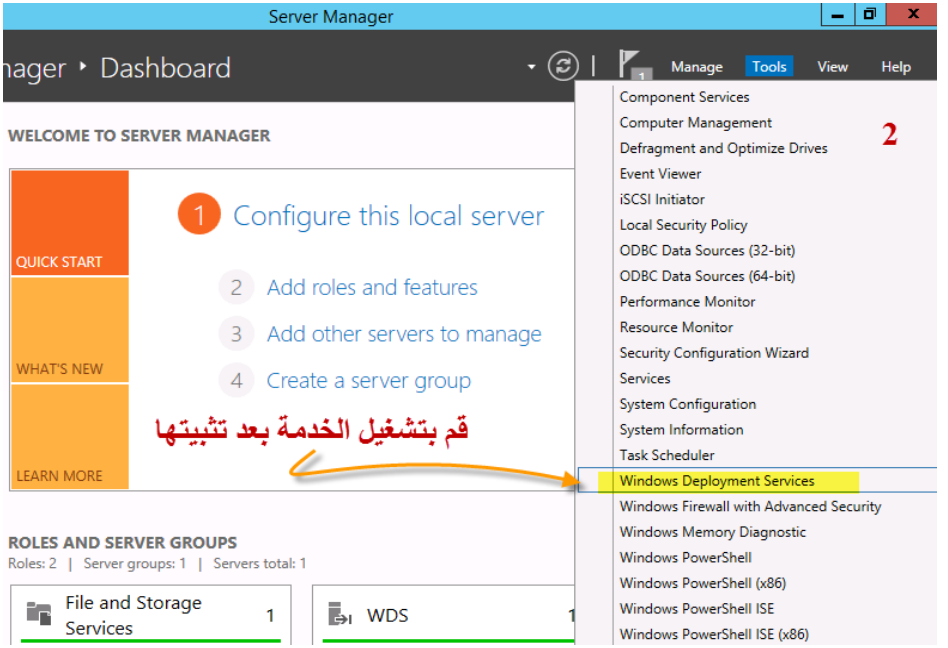
WDS


Servers 1 Server(s)
Server Name
Status
Server Mode
WDS.target...
Config...
Native (Wind...
Network Connection Details
Network Connection Details:
Property
Value
Connection-specific DN...
Description
Microsoft Hyper-V Network Adapter #2
Physical Address
00-15-5D-06-14-32
DHCP Enabled
No
IPv4 Address
10.10.10.50
IPv4 Subnet Mask
255.0.0.0
IPv4 Default Gateway
10.10.10.2
IPv4 DNS Servers
192.168.1.2
10.10.10.2
IPv4 WINS Server
NetBIOS over Tcpip En...
Yes
Close
بيانات الـ
WDS Server


Network Connection Details
Network Connection Details:
Property
Value
Connection-specific DN...
Description
Intel 21140-Based PCI Fast Ethernet Ada
Physical Address
00-15-5D-06-14-33
DHCP Enabled
No
IPv4 Address
192.168.1.10
IPv4 Subnet Mask
255.255.255.0
IPv4 Default Gateway
192.168.1.29
IPv4 DNS Servers
10.10.10.2
192.168.1.2
IPv4 WINS Server
NetBIOS over Tcpip En...
Yes
Close
Connection 5
-Based PCI Fast Ethern...
بيانات الجهاز الذي سيتم
استقبال النسخة عليه

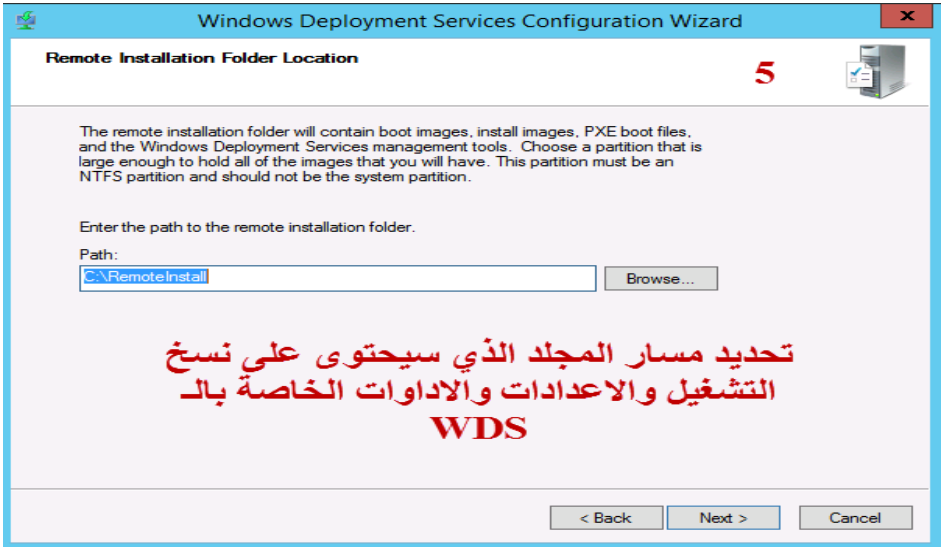
من البيانات السابقة علمنا ان خادم الـ WDS موجود في الرياض وان جهاز المستخدم موجود في الدوحة كما يظهر ذلك من ارقام الـ IP والآن لنفترض ان حالة من سقوط النظام حدثت على هذا الجهاز وبالتالي فانه لابد من اعادة تثبيت نظام التشغيل علية وسنقوم بذلك من خلال خادم الـ WDS الموجود في الرياض فتابع معي .

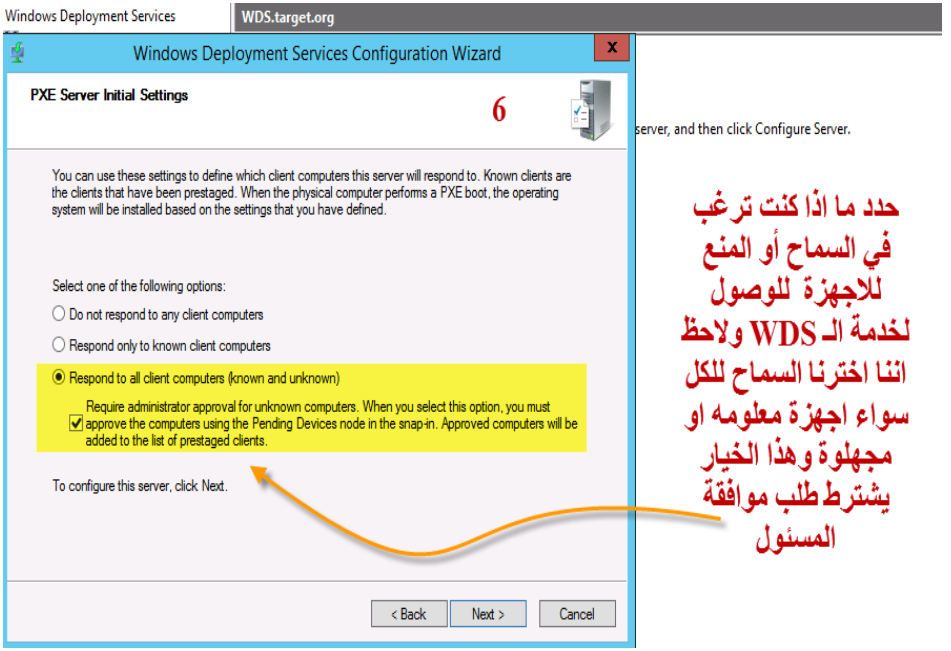





Windows Deployment Services
File Action View Help
3
Windows Deployment Services
Servers
WDS.target.org
Configure Server
Remove Server
View
Refresh
Help
WDS.target.org
Windows Deployment Services is not configured
This server is not configured. To configure this server, right-click the server, and then click Configure Server.
You must be a local administrator to perform this task.
بعد التشغيل لابد ان نقوم الان بضبط اعدادات الـ
WDS Server

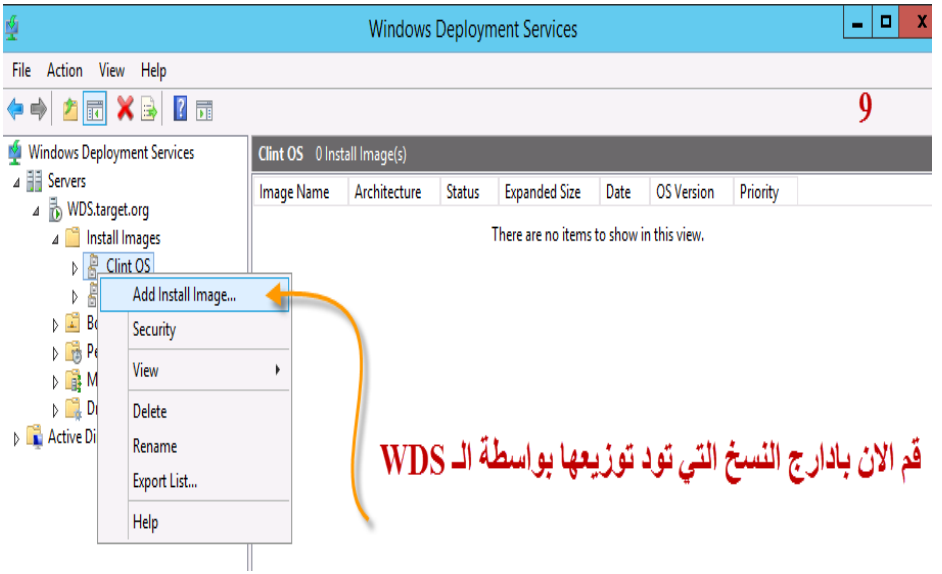

Windows Deployment Services Configuration Wizard
Install Options
4
Select one of the following options:
Integrated with Active Directory
This server is a member of an Active Directory Domain Services (AD DS) domain, or a domain controller for an AD DS domain.
Standalone server
Configure the server so that it is standalone, operating independently of Active Directory.
في اصدار 2012 اصبح بالامكان جعل الـ WDS خارج نطاق الـ AD لكن في حالتنا بالطبع سنختار الخيار الاول
< Back
Next >
Cancel

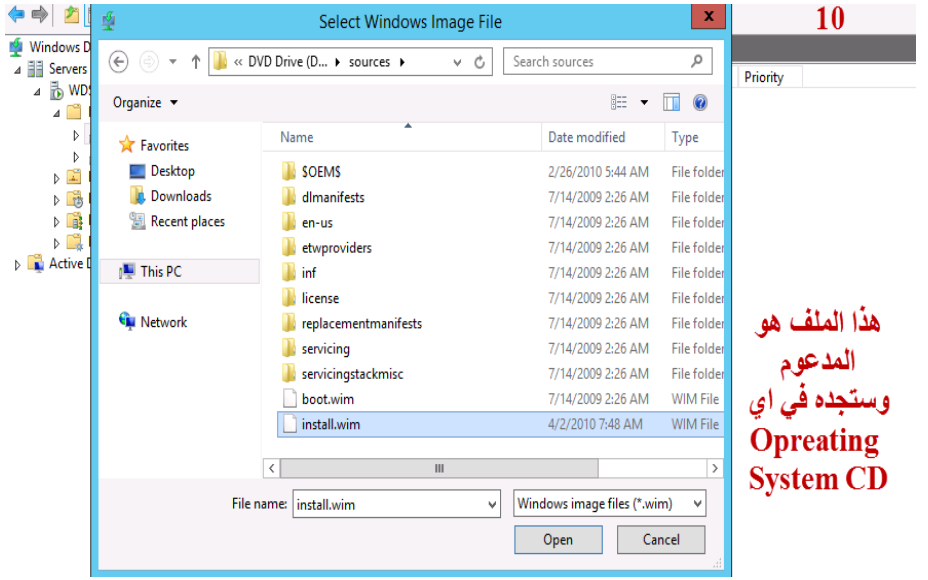

Windows Deployment Services Configuration Wizard
Remote Installation Folder Location
5
The remote installation folder will contain boot images, install images, PXE boot files, and the Windows Deployment Services management tools. Choose a partition that is large enough to hold all of the images that you will have. This partition must be an NTFS partition and should not be the system partition.
Enter the path to the remote installation folder.
Path:
C:\RemoteInstall
Browse...
تحديد مسار المجلد الذي سيحتوى على نسخ التشغيل والاعدادات والاداوات الخاصة بالـ WDS
< Back
Next >
Cancel

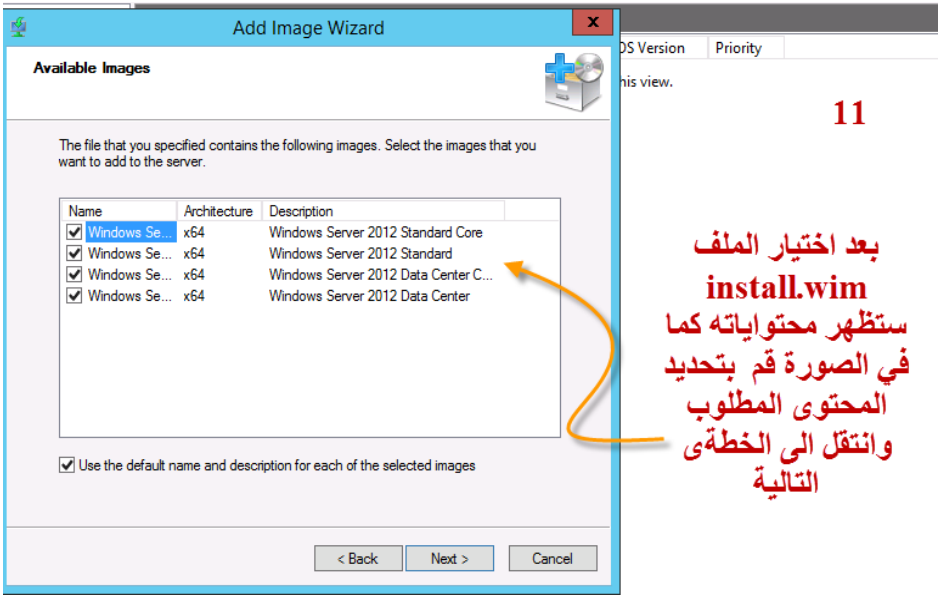

Windows Deployment Services
WDS.target.org
Windows Deployment Services Configuration Wizard
PXE Server Initial Settings
6
server, and then click Configure Server.
You can use these settings to define which client computers this server will respond to. Known clients are the clients that have been prestaged. When the physical computer performs a PXE boot, the operating system will be installed based on the settings that you have defined.
Select one of the following options:
Do not respond to any client computers
Respond only to known client computers
Respond to all client computers (known and unknown)
Require administrator approval for unknown computers. When you select this option, you must approve the computers using the Pending Devices node in the snap-in. Approved computers will be added to the list of prestaged clients.
To configure this server, click Next.
< Back
Next >
Cancel
حدد ما اذا كنت ترغب في السماح أو المنع للاجهزة للوصول لخدمة الـ WDS ولاحظ اننا اخترنا السماح للكل سواء اجهزة معلومه او مجهلوة وهذا الخيار يشترط طلب موافقة المسئول


Windows Deployment Services Configuration Wizard
Task Progress
7
Configuring Windows Deployment Services...
Starting Windows Deployment Services
انتهينا من ضبط الاعدادات وجاري تشغيل الخدمة
< Back
Finish
Cancel


Windows Deployment Services
File Action View Help
8
Windows Deployment Services
Servers
WDS.target.org
Install Images
Boot I
Pendi
Multic
Driver
Active Direct
Add Install Image...
Add Image Group...
View
Export List...
Help
Install Images 0 Image Group(s)
Image Group
There are no items to show in this view.
لانشاء المجموعات واضافة النسخ لها
استخدم الاوامر الموجودة في القائمة

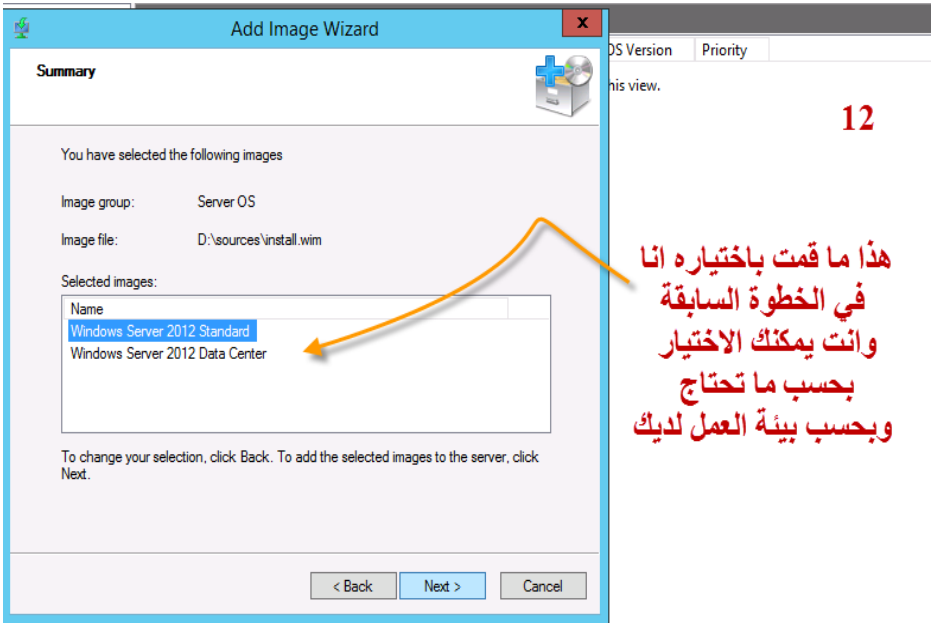

Windows Deployment Services
File Action View Help
9
Windows Deployment Services
Servers
WDS.target.org
Install Images
Clint OS
Active Di
Clint OS 0 Install Image(s)
Image Name
Architecture
Status
Expanded Size
Date
OS Version
Priority
There are no items to show in this view.
Add Install Image...
Security
View
Delete
Rename
Export List...
Help
قم الان بادارج النسخ التي تود توزيعها بواسطة الـ WDS


Select Windows Image File
10
Priority
« DVD Drive (D... ▸ sources ▸
Search sources
Organize
Favorites
Desktop
Downloads
Recent places
This PC
Network
Name
Date modified
Type
OEM 2/26/2010 5:44 AM File folder
dlmanifests 7/14/2009 2:26 AM File folder
en-us 7/14/2009 2:26 AM File folder
etwproviders 7/14/2009 2:26 AM File folder
inf 7/14/2009 2:26 AM File folder
license 7/14/2009 2:26 AM File folder
replacementmanifests 7/14/2009 2:26 AM File folder
servicing 7/14/2009 2:26 AM File folder
servicingstackmisc 7/14/2009 2:26 AM File folder
boot.wim 7/14/2009 2:26 AM WIM File
install.wim 4/2/2010 7:48 AM WIM File
File name: install.wim
Windows image files (*.wim)
Open
Cancel
هذا الملف هو المدعوم وستجده في اي Opreating System CD



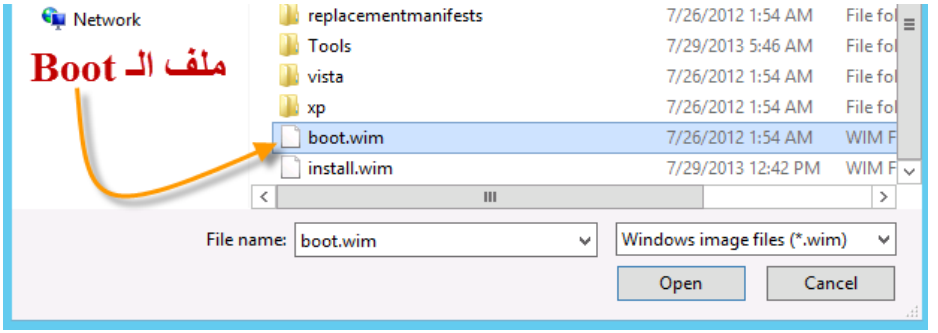
11

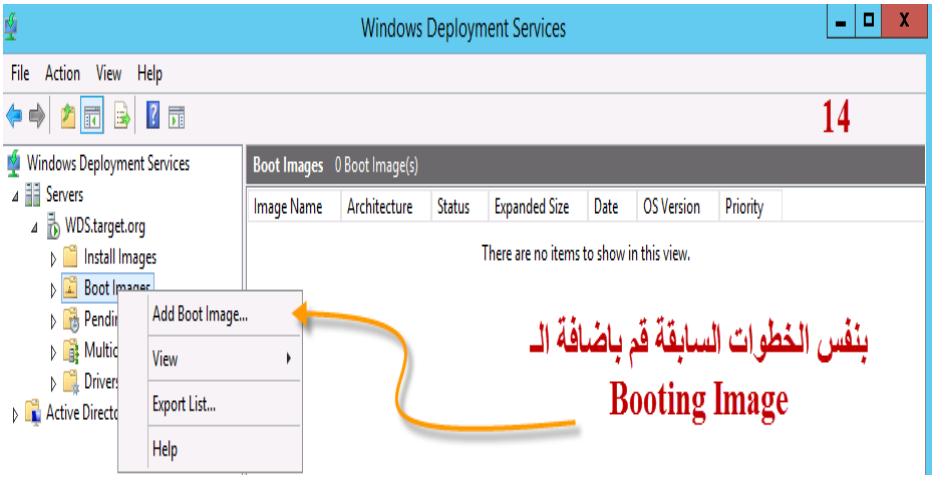
بعد اختيار الملف
install.wim
ستظهر محتوياته كما
في الصورة قم بتحديد
المحتوى المطلوب
وانتقل الى الخطوة
التالية

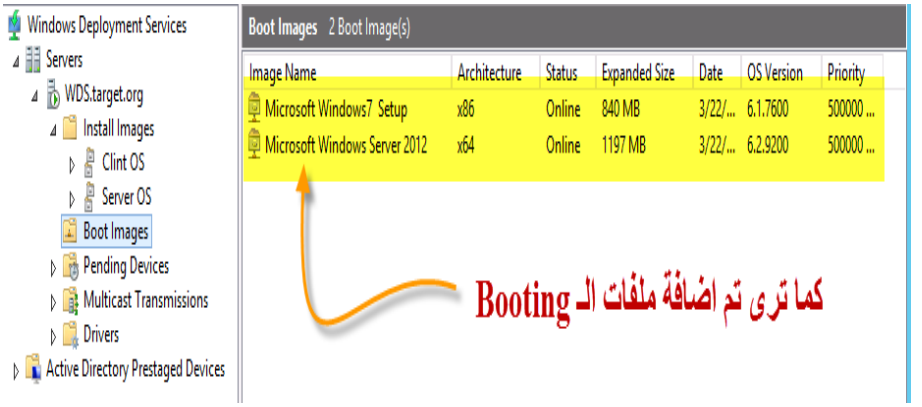


12

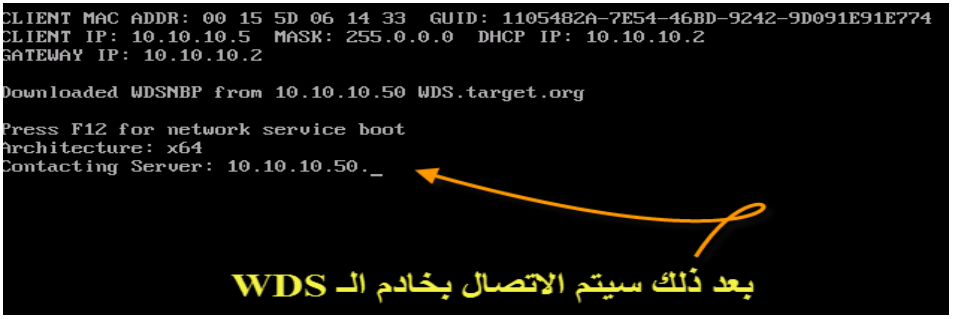
هذا ما قمت باختياره انا
في الخطوة السابقة
وانت يمكنك الاختيار
بحسب ما تحتاج
وبحسب بيئة العمل لديك


Network
ملف الـ Boot
replacementmanifests 7/26/2012 1:54 AM
Tools 7/29/2013 5:46 AM
vista 7/26/2012 1:54 AM
xp 7/26/2012 1:54 AM
boot.wim 7/26/2012 1:54 AM
install.wim 7/29/2013 12:42 PM
File name: boot.wim
Windows image files (*.wim)
Open
Cancel


Windows Deployment Services
File Action View Help
14
Windows Deployment Services
Servers
WDS.target.org
Install Images
Boot Images
Boot Images 0 Boot Image(s)
Image Name Architecture Status Expanded Size Date OS Version Priority
There are no items to show in this view.
Add Boot Image...
View
Export List...
Help
بنفس الخطوات السابقة قم باضافة الـ
Booting Image

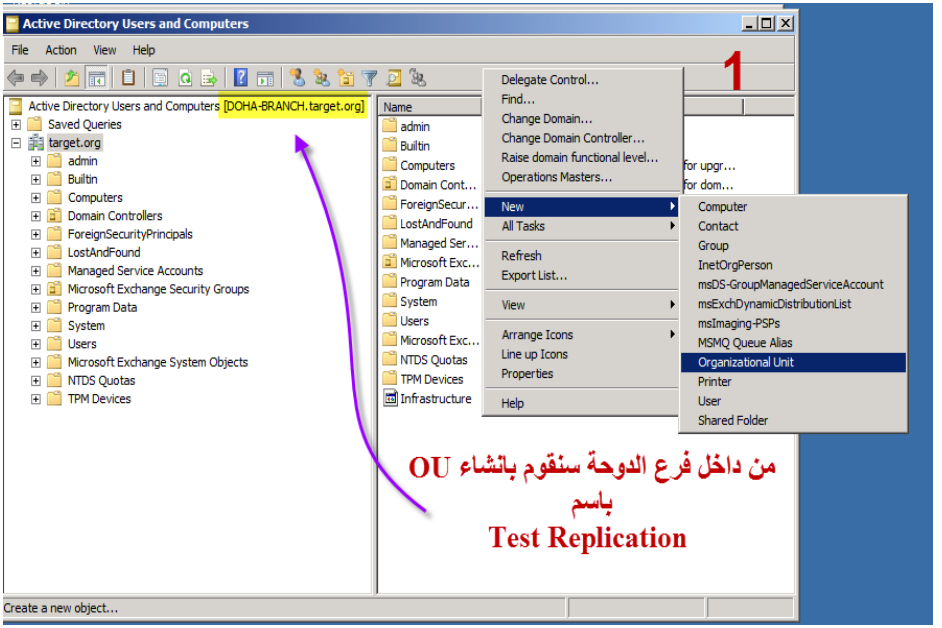

Windows Deployment Services
Servers
WDS.target.org
Install Images
Clint OS
Server OS
Boot Images
Pending Devices
Multicast Transmissions
Drivers
Active Directory Prestaged Devices
Boot Images 2 Boot Image(s)
Image Name Architecture Status Expanded Size Date OS Version Priority
Microsoft Windows7 Setup x86 Online 840 MB 3/22/... 6.1.7600 500000 ...
Microsoft Windows Server 2012 x64 Online 1197 MB 3/22/... 6.2.9200 500000 ...
كما ترى تم اضافة ملفات الـ Booting

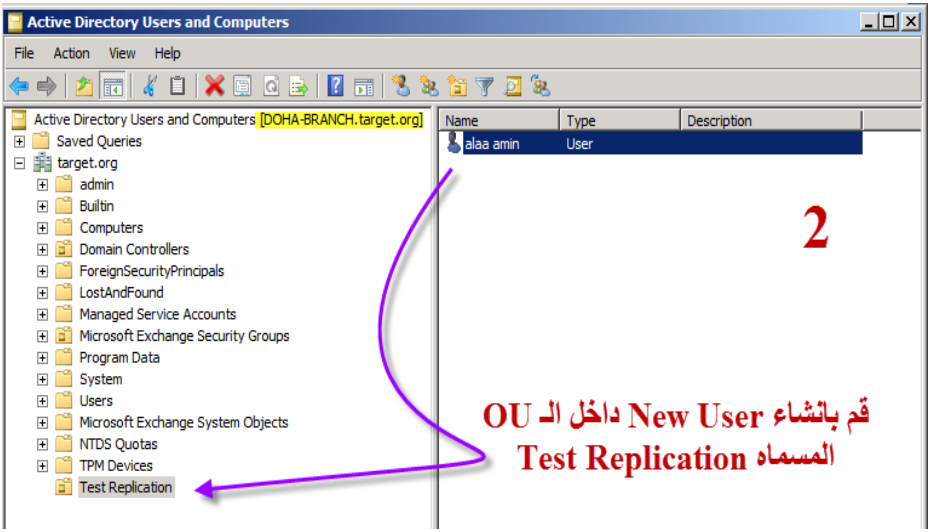

Clint windows 7 on LAP - Virtual Machine Connection
File Action Media Clipboard View Help
Hyper-V
PXE Network Boot 09.14.2011
(C) Copyright 2011 Microsoft Corporation, All Rights Reserved.
CLIENT MAC ADDR: 00 15 5D 06 14 33 GUID: 1105482A-7E54-46BD-9242-9D091E91E774
DHCP.
الان بعد التوجه للجهاز نجعل الاقلاع من الـ PXE حتى
يتمكن من الاتصال بالـ WDS

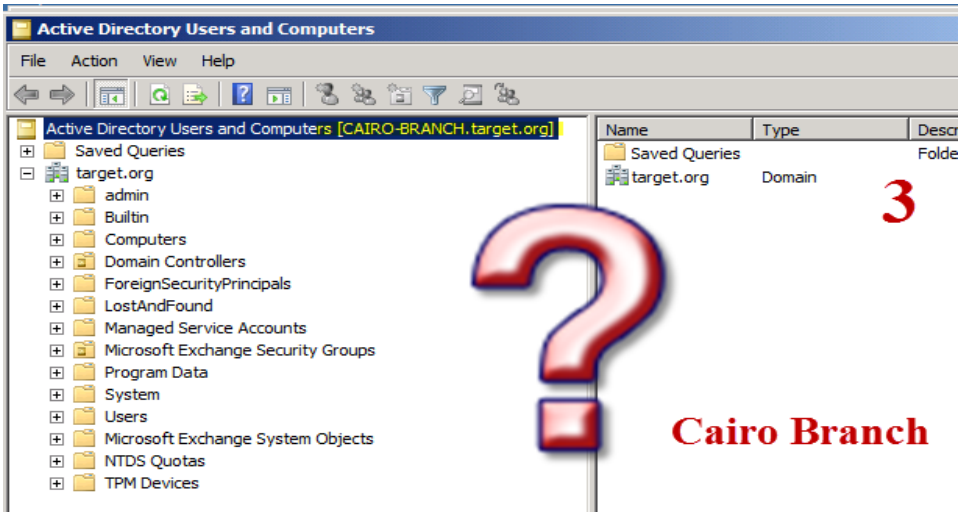

CLIENT MAC ADDR: 00 15 5D 06 14 33 GUID: 1105482A-7E54-46BD-9242-9D091E91E774
CLIENT IP: 10.10.10.5 MASK: 255.0.0.0 DHCP IP: 10.10.10.2
GATEWAY IP: 10.10.10.2
Downloaded WDSNBP from 10.10.10.50 WDS.target.org
Press F12 for network service boot
Architecture: x64
Contacting Server: 10.10.10.50.
بعد ذلك سيتم الاتصال بخادم الـ WDS


Windows Boot Manager (Server IP: 10.10.10.50)
Choose an operating system to start:
(Use the arrow keys to highlight your choice, then press ENTER.)
Microsoft Windows7 Setup
Microsoft Windows Server 2012
كما نرى تم الاتصال وجلب النسخ من داخل الـ WDS الموجود
في الرياض
من خلال الجهاز الموجود في الدوحة

والآن بعد التأكد من اتصال الفروع بشكل تام دعونا نقوم بعملية اختبار للـ Replication

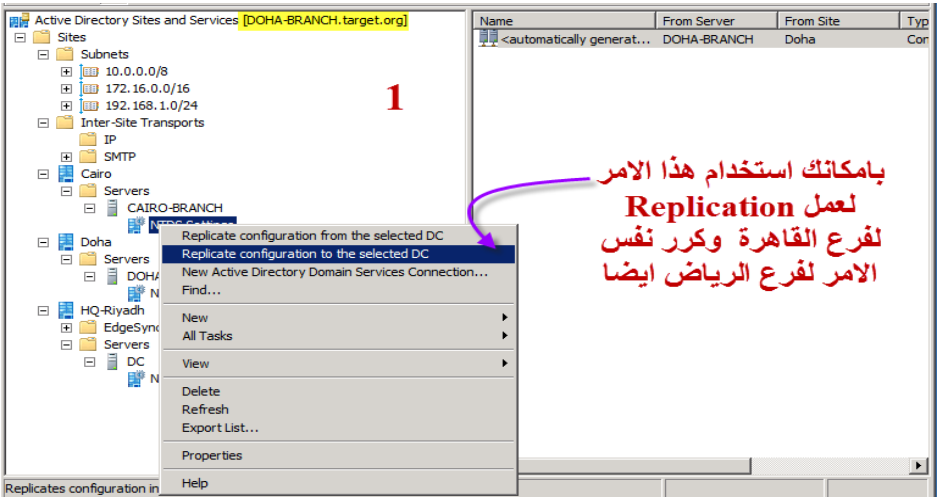




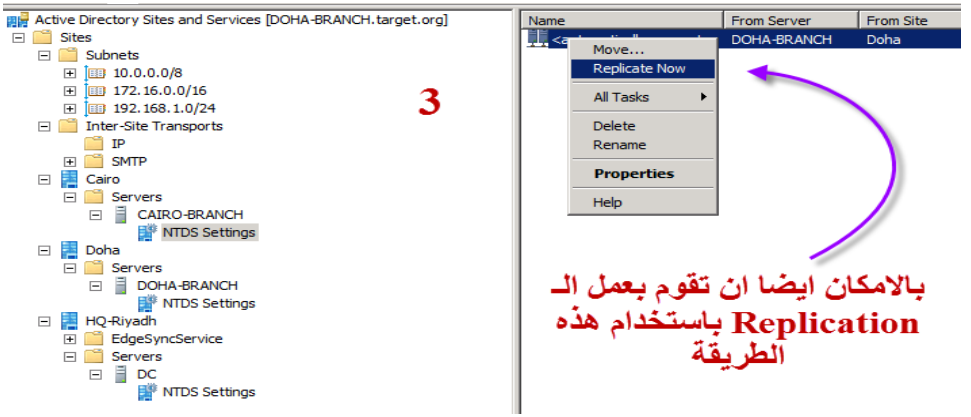


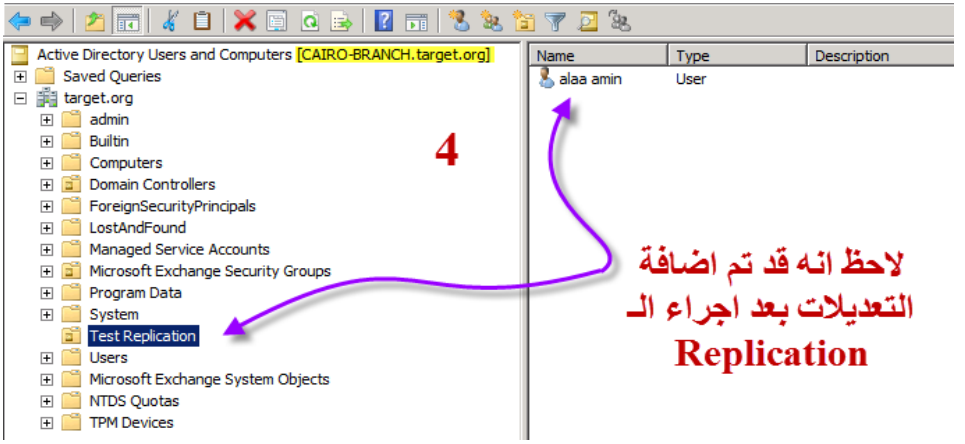
من المفترض ان تظهر التعديلات التي قمنا بها من فرع الدوحة في كلا من القاهرة والرياض لكنها **لم تظهر** والسبب في ذلك هو انه لم يأتي وقت إجراء الـ **Replication** الذي تم تحديده اثناء عمل الـ **Site link** بين كلا من الدوحة والقاهرة والدوحة والرياض .

والحل الان هو عمل الـ **Replication** يدويا دون انتظار الوقت المحدد له مسبقا




Active Directory Sites and Services [DOHA-BRANCH.target.org]
Sites
Subnets
10.0.0.0/8
172.16.0.0/16
192.168.1.0/24
Inter-Site Transports
IP
SMTP
Cairo
Servers
CAIRO-BRANCH
NTDS Settings
Doha
Servers
DOHA-BRANCH
NTDS Settings
HQ-Riyadh
EdgeSyncService
Servers
DC
NTDS Settings
Name
From Server
From Site
<automatically generat...
DOHA-BRANCH
Doha
2
ستظهر لك رساله تفيد باجراء الـ
Replication
Replicate Now
Active Directory Domain Services has replicated the connections.
OK

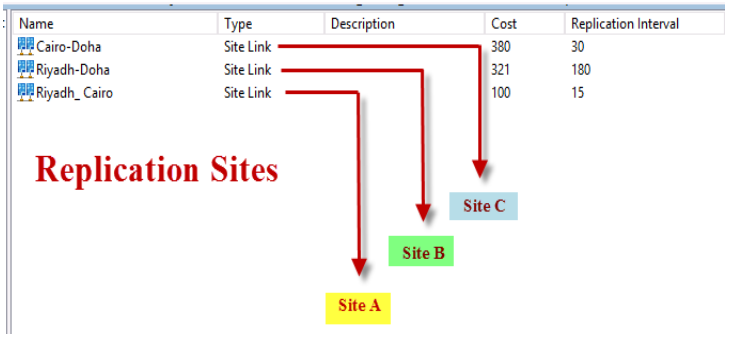

Active Directory Sites and Services [DOHA-BRANCH.target.org]
Sites
Subnets
10.0.0.0/8
172.16.0.0/16
192.168.1.0/24
Inter-Site Transports
IP
SMTP
Cairo
Servers
CAIRO-BRANCH
NTDS Settings
Doha
Servers
DOHA-BRANCH
NTDS Settings
HQ-Riyadh
EdgeSyncService
Servers
DC
NTDS Settings
3
Name
From Server
From Site
DOHA-BRANCH
Doha
Move...
Replicate Now
All Tasks
Delete
Rename
Properties
Help
بالامكان ايضا ان تقوم بعمل الـ
Replication باستخدام هذه
الطريقة


Active Directory Users and Computers [CAIRO-BRANCH.target.org]
Saved Queries
target.org
admin
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
LostAndFound
Managed Service Accounts
Microsoft Exchange Security Groups
Program Data
System
Test Replication
Users
Microsoft Exchange System Objects
NTDS Quotas
TPM Devices
4
Name
Type
Description
alaa amin
User
لاحظ انه قد تم اضافة
التعديلات بعد اجراء الـ
Replication

حسنا بما أننا قمنا في الخطوات السابقة بعمل **Site Link** والذي ينظم عملية ال **Replication** بين فرعين أو أكثر .

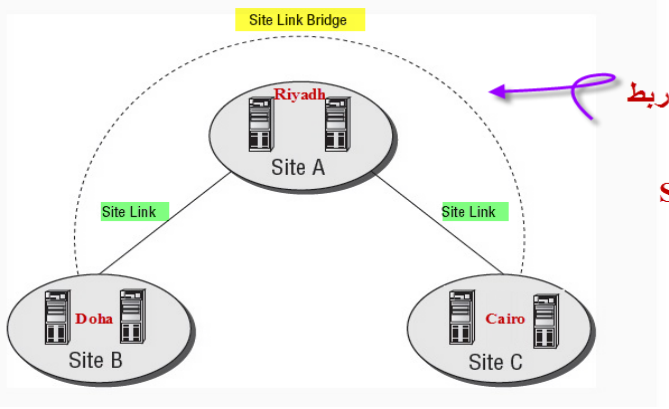
فقد حان لنا الان ان نتعرف على الـ **Site Link Bridge** وهو الذي يربط بين موقعين أو أكثر .

وحتى يتضح الامر أنظر جيدا الى هذا الشكل



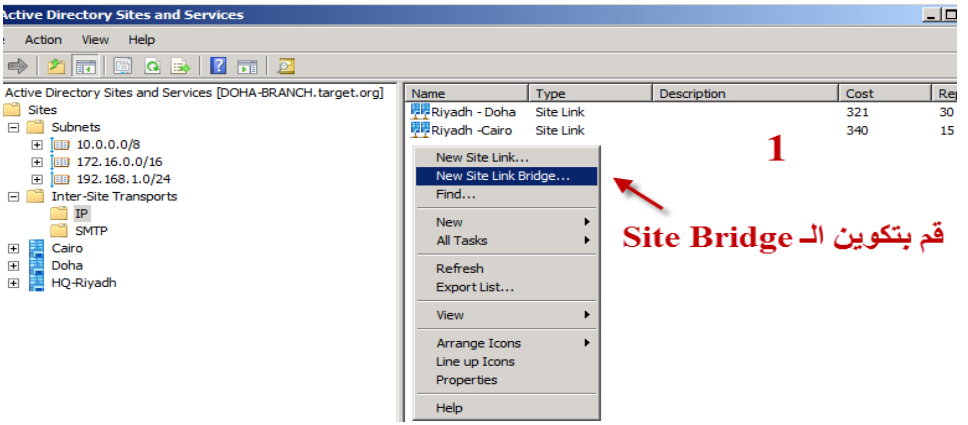
هل تعتقد انه يمكن عمل **Replication** لموقع **C** بطريقة اخرى ؟

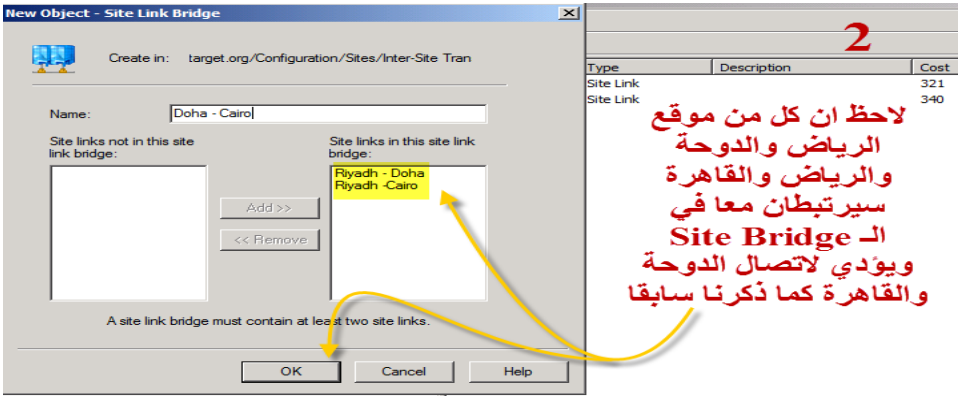
للإجابة على هذا السؤال انظر الرسم التالي :-

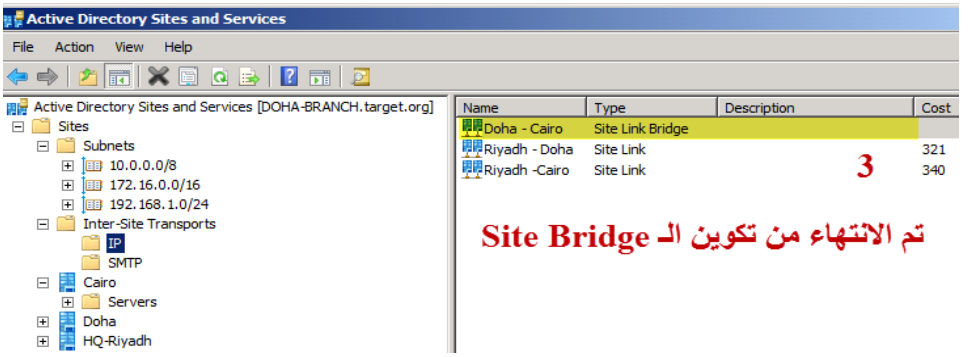


لاحـظنا في الشكل السابق عدم وجود **Link** بين القاهرة والدوحة وحتى يتم عمل **Replication** بينهما سيكون الرياض هو الطرف المشترك فلو تم إجراء أي تعديل في فرع القاهرة مثلا فسيضطر فرع الدوحة الحصول عليه عن طريق الرياض وليس من القاهرة مباشرة لعدم وجود **Link** كما قلنا وسيتوجب أيضا على فرع الدوحة انتظار عملية الـ **Replication** فـي **(Site A)** ومن ثم الحصول على الـ **Updates** فـي عملية الـ **Replication** الخاصة بـ **(Site B)** .

أما في حالة استخدام الـ **Site Link Bridge** فإننا سنتمكن من ربط **Site B/C** معا دون انتظار البيانات في **Site A** .







انتهينا الان من فهم ما هو الـ Replication وطريقة اعداده وإدارته وكموضوع مكمل ومهم سنتعرف على كيفية ادارة المخاطر في حالة فشل الـ Parent Domain

Operations Master Roles

لابد أن نعلم أن في الشبكة توجد خمسة أدوار أو وظائف أو مهام (Roles) اثنين منها على نطاق ال Forest بالكامل تسمى Forest-Wide Operations Master Roles وثلاثة على نطاق الـ Domain تسمى Domain-Wide Operations Master Roles وتسمى في المصادر Flexible Single Master Operation وتختصر الى (FSMO)

إذن الـ Role هو الدور أو الوظيفة أو المهمة التي يقوم بها المتحكم بالمجال DC في المجال أو الـ ... Domain

ولاحظ أن الـ Domain Controllers Servers هي التي تقوم بهذه الأدوار وليس أي Server عادي مثل سيرفر الملفات مثلا .

هذه الـ Rols هي :-

1- Domain naming Master Role
2- Schema Master Role
3- RID Master Role (Relative ID Master Role)
4- PDC Master Role (Primary Domain Controller)
5- Infrastructure Master Role

تذكر أنه في كل Forest يوجد Schema Master واحد فقط و Domain Naming Master واحد فقط انظر الجدول التالي :-

FSMO Role	Number of DCs holding this role	Original DC holding the FSMO role
Schema	One per forest	The first DC in the first domain in the forest (i.e. the Forest Root Domain)
Domain Naming	One per forest	
RID	One per domain	The first DC in a domain (any domain, including the Forest Root Domain, any Tree Root Domain, or any Child Domain)
PDC Emulator	One per domain	
Infrastructure	One per domain	

Domain Naming Master Role

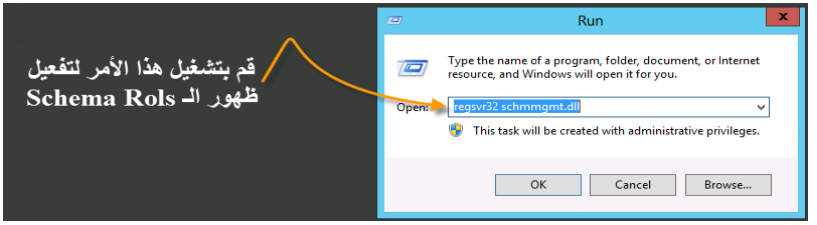
تقع على هذه الـ Role مسئولية مراقبة الـ Domain Name بحيث لا يمكن تكراره ابدا لا على مستوى الـ Forest ولا مستوى الـ Tree أيضا وكما قلنا هي في الـ Forest Level وتحديدا في أول Domain في الـ Forest وبالتالي لو ان هذا الـ Parent Domain أصبح خارج الخدمة لسبب ما فأنني لن استطيع اضافة او حذف أي Domain اخر من أي نوع حتى في وجود Replication لأنه ببساطه هذه الـ Role لم تعد متاحة وهنا يدور محور حديثنا

Schema Master Role

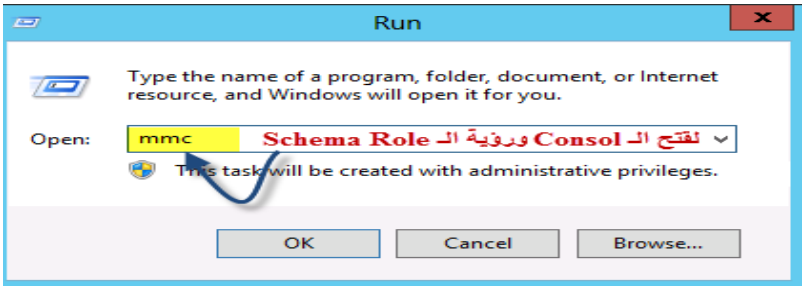
هذه الـ Role لا تقل اهمية ابدا عن سابقتها فهي مسئولة عن كل الـ Clases و الـ Attributes أي على مستوى الـ Forest ككل وبالتالي شأنها شأن الـ Domain naming Master Role ففي حالة عدم وجودها لن استطيع مثلا القيام بتهيئة الـ Domain لاستقبال أي تعديلات ولا تحديثات لأنها هي السجل لكل التحديثات والتغيرات التي تتم على هذه الـ Objects و الـ Attributes .

ويمكن لنا الاطلاع على هذه الـ Role بعد تفعيل ظهورها حيث انها مخفية دخل النظام بالخطوات التالية :-

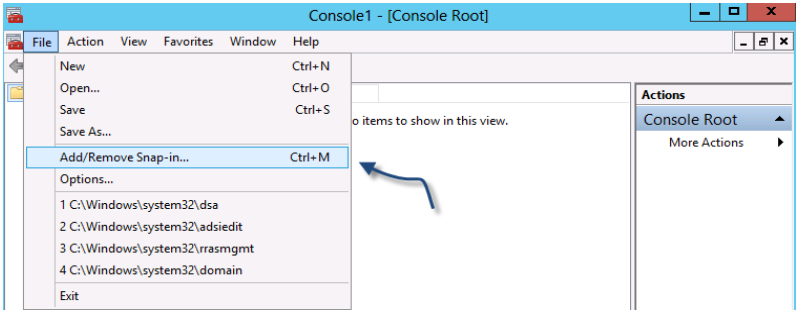
Start → run → regsvr32 schmmgmt.dll

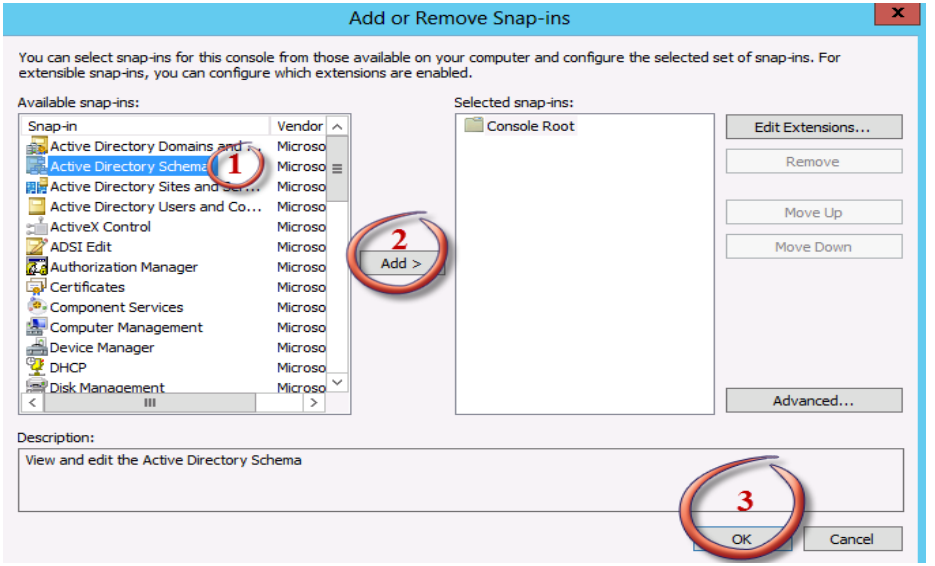


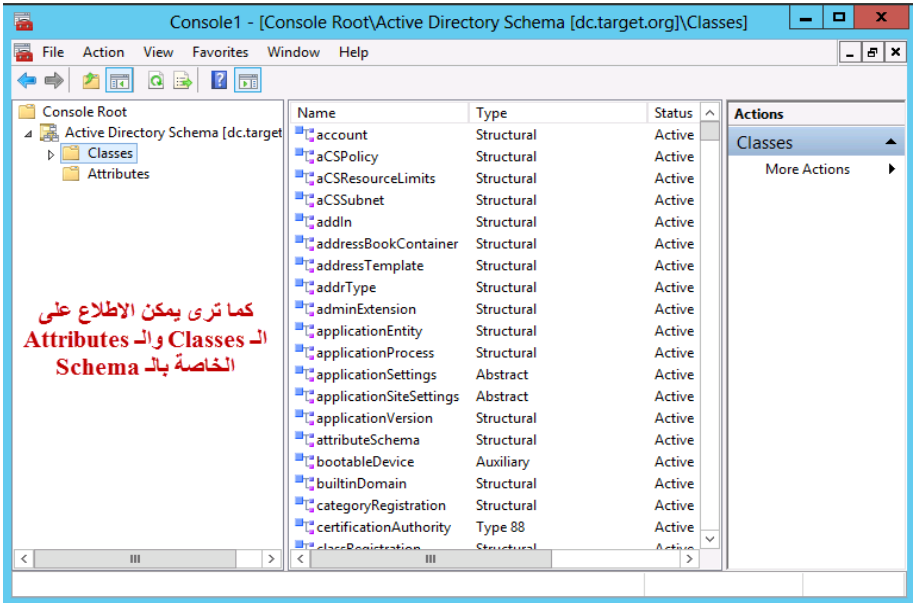
Start → run → mmc



From Consol→ File → add/remove snap in




Add or Remove Snap-ins
You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.
Available snap-ins:
Snap-in
Vendor
Active Directory Domains and ...
Active Directory Schema
Active Directory Sites and Ser...
Active Directory Users and Co...
ActiveX Control
ADSI Edit
Authorization Manager
Certificates
Component Services
Computer Management
Device Manager
DHCP
Disk Management
Microso
1
2
Add >
Selected snap-ins:
Console Root
Edit Extensions...
Remove
Move Up
Move Down
Advanced...
Description:
View and edit the Active Directory Schema
3
OK
Cancel

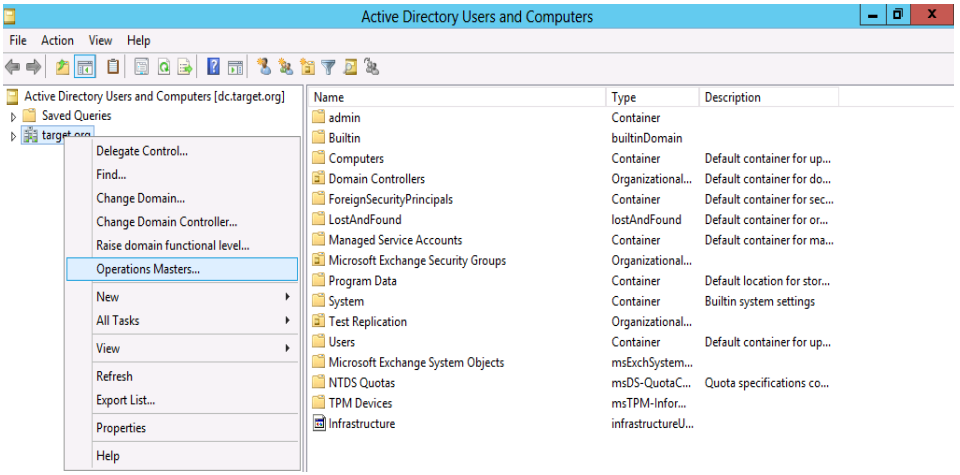

Console1 - [Console Root\Active Directory Schema [dc.target.org]\Classes]
File Action View Favorites Window Help
Console Root
Active Directory Schema [dc.target
Classes
Attributes
كما ترى يمكن الاطلاع على
الـ Classes والـ Attributes
الخاصة بالـ Schema
Name
Type
Status
account Structural Active
aCSPolicy Structural Active
aCSResourceLimits Structural Active
aCSSubnet Structural Active
addIn Structural Active
addressBookContainer Structural Active
addressTemplate Structural Active
addrType Structural Active
adminExtension Structural Active
applicationEntity Structural Active
applicationProcess Structural Active
applicationSettings Abstract Active
applicationSiteSettings Abstract Active
applicationVersion Structural Active
attributeSchema Structural Active
bootableDevice Auxiliary Active
builtinDomain Structural Active
categoryRegistration Structural Active
certificationAuthority Type 88 Active
Actions
Classes
More Actions

RID Master Role

عند عمل أي Object في الـ AD سواءً كان مستخدم user أو مجموعة group أو حتى كمبيوتر computer ، فإن الـ DC الذي يقوم بمهة ال RID Master سيعطي لهذا الـ Object هوية أمنية Security ID خاصة به فمثلاً عند اضافة مستخدم في الـ Active directory فإنك تضع أسما لهذا المستخدم وليكن Alaa لكن الـ RID Master يعطيه ID خاصة به وعادة تكون مثل S-1-5-21-895771394-4047885310-268483753-1006.... لذلك تلاحظ أحياناً عند استعراض صلاحيات الـ NTFS لمجلد أو ملف معين وجود مثل هذا الرقم الطويل وبجانبه أيقونة وجه وعلامة استفهام حمراء وهذا يدل على أن المستخدم قد حذف من ال AD أو ان الكمبيوتر مازال يحاول جلب اسم المستخدم وقد يأخذ ثواني قليلة لجلب البيانات وفي حالة د حذف مستخدم من ال AD فان اعادة انشاؤه بنفس خصائصة السابقة لن تنفع لأن الـ RID Master سوف يعطيه Security ID آخر جديد وهكذا .

ويمكن لنا الاطلاع على هذه الـ Role بالخطوات التالية

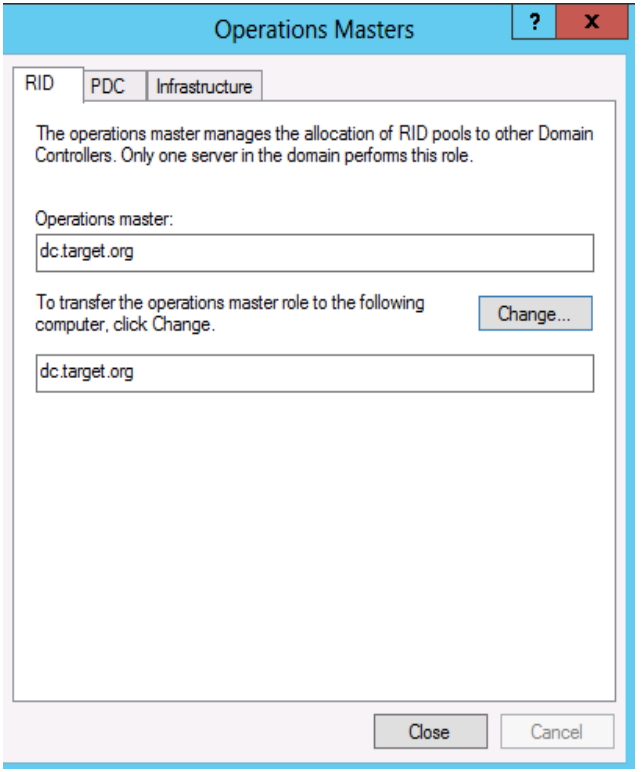
Active Directory Users and Computers → R.click on domain → Operation master



PDC Emulator Role

تقع على هذه الـ Role مسئولية المزامنة بينه وبين الاجهزة Synchronize فمثلا لو تم تغيير الوقت والتاريخ الخاص بالـ Domain ستتغير في كل ال Machine بمجرد عملية الـ Connect كذلك فان أي تغيير في كلمات المرور فإنها توجه إلى الـ PDC Emulator بمعنى أنه يعلم عنها وتسجل عنده وأي ادخال خاطئ لكلمة المرور فأنها توجه له أيضاً وهو يقوم بإجراء اللازم كإظهار نافذة تعلم المستخدم بإدخاله كلمة سر خاطئة بمعنى انه يعد Domain Browser وكذلك تقع عليه مسئولية الـ Domain Group Policy

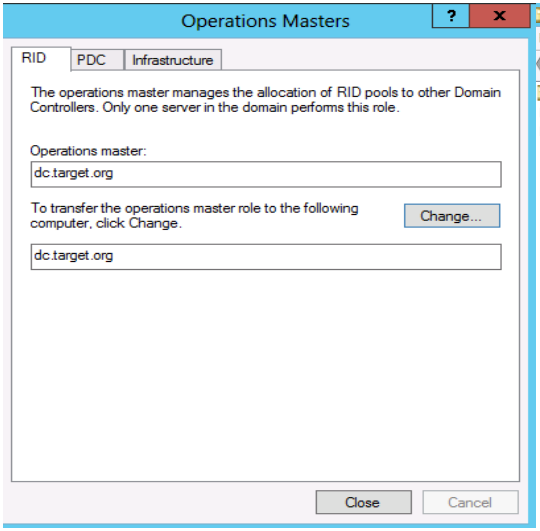
ويمكن الاطلاع على هذه الـ Role بنفس خطوات الـ RID Role

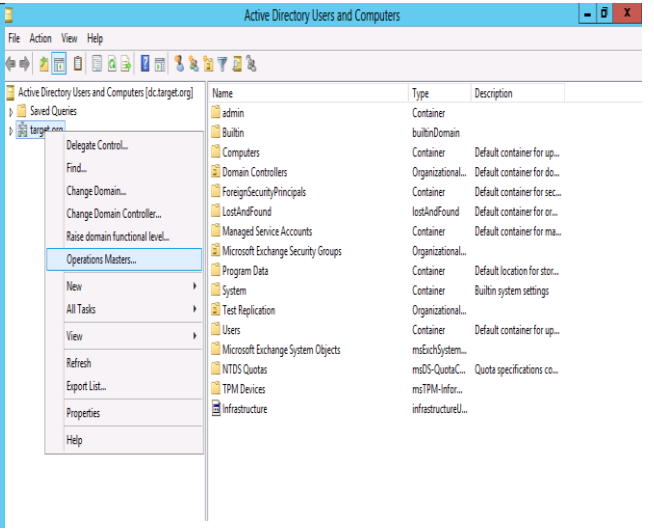


Infrastructure Master Role

هذا الـ Role مسئول عن مصادقة الصلاحيات والتعديلات التي تتم على الـ Objects فاذا تم التعديل على صلاحية مستخدم ما مثلا فان
الـ Infrastructure Master هو الذي يقوم بهذه الـ Modification ومن ثم تحديثها .

أيضا يمكن الاطلاع على هذه الـ Role بنفس خطوات الـ RID Role و الـ PDC Role





والآن بعد أن علمنا أدوار الشبكة ومهام كلا منها واتضح لنا ان هناك Tow Rolls خاصة بالجهاز الذي يكون أول Domain في الـ Forest فقط ولا يمكن تكرارهم أبدا وبالتالي اذا حدثت مشكلة في هذا الجهاز أو حتى قررت شراء أخر بديل فلن يكون هناك إمكانية لاضافة Child او Tree ولا حذف الموجود منهم ولن أستطيع كذلك عمل Additional إذا ما الحل ؟

الحل هو نقل هذه الـ Rolls من الجهاز القديم مثلا الى الجديد او من المتضرر الى السليم وهكذا

وعلى ذلك فهناك احتمالين لا ثالث لهما
الاحتمال الاول هو ان الـ Parent Domain Controller موجود وفي حالة Online
الاحتمال الثاني هو ان الـ Parent Domain Controller غير موجود أو متضرر وفي حالة Offline

وسنقوم بإذن الله تعالى بالتدرب وشرح العمل على كلا الاحتمالين معا .

كيف يتم نقل الـ FSMO Roles من Server الى آخر في حالة ان الـ Parent Domain Controller موجود Online ؟

حسنا سوف نعمل الان على الاحتمال الاول وسنستخدم الـ Domain الذي تدربنا عليه اثناء عمل الـ Replication

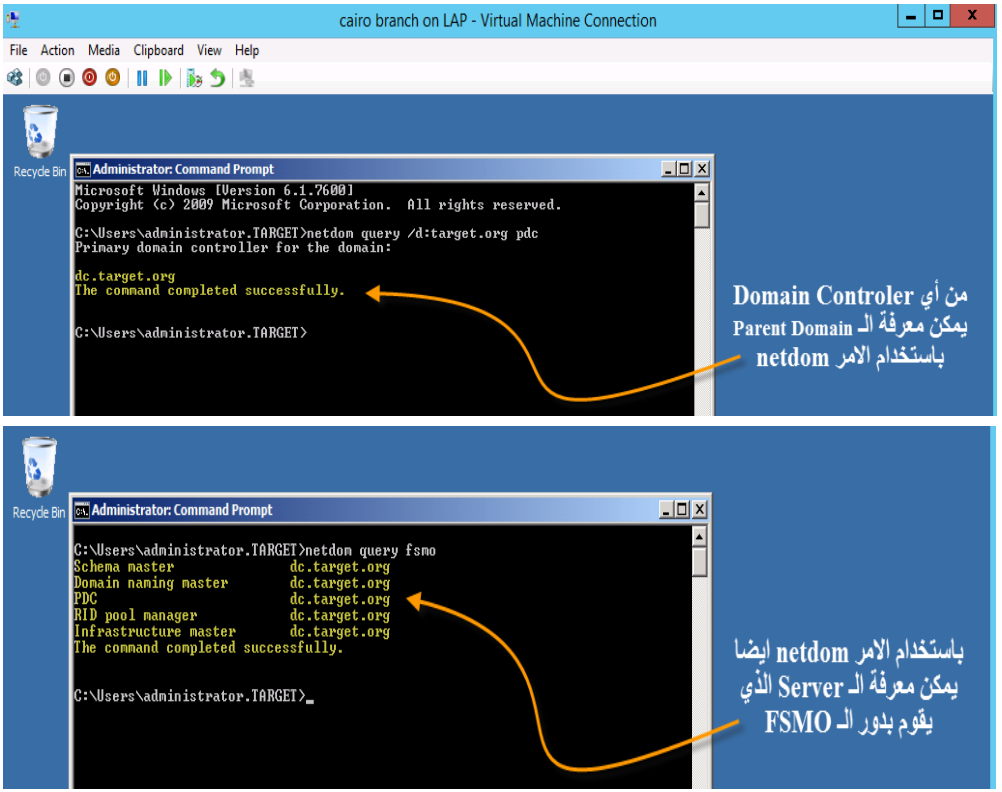
فهل تعرف ما هو الـ Server الذي يقوم بدور الـ Parent Domain في مجال (Target.org) ؟

نعم الاجابة صحيحة الـ Server الذي يقوم بدور الـ Parent Domain Controller في مجال (Target.org) هو الموجود في المركز الرئيسي في الرياض باسم (DC) لأنه ببساطه هو أول Domain في الـ Forest كما علمنا

لكن ماذا لو كنا حقا نجهل هذه المعلومة الاجابة ؟

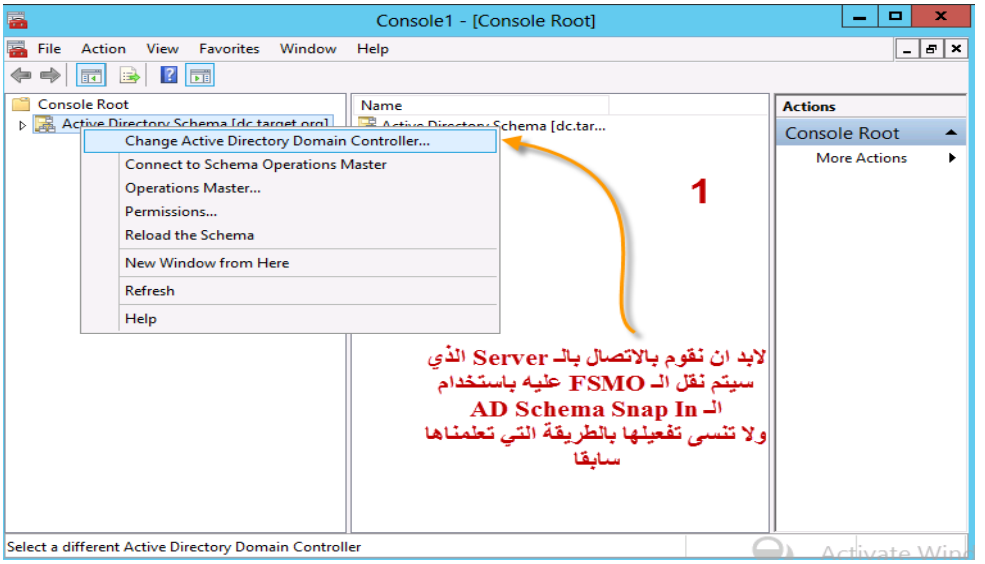
لا تقلق فإننا سنستطيع معرفة ذلك بسهولة باستخدام الاوامر التالية :-

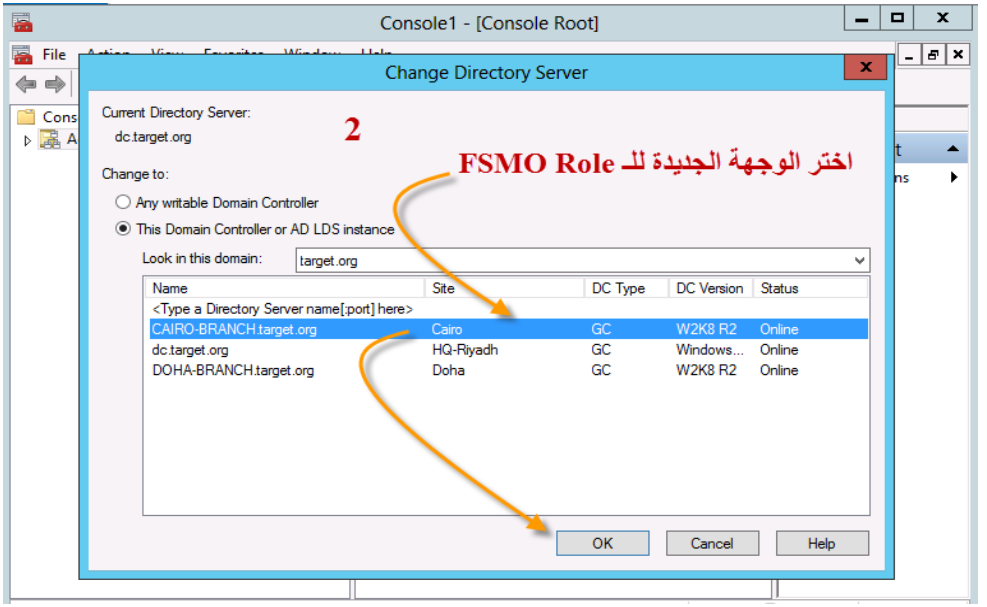
Netdom query /d:your domain name) pdc
Netdom query fsmo

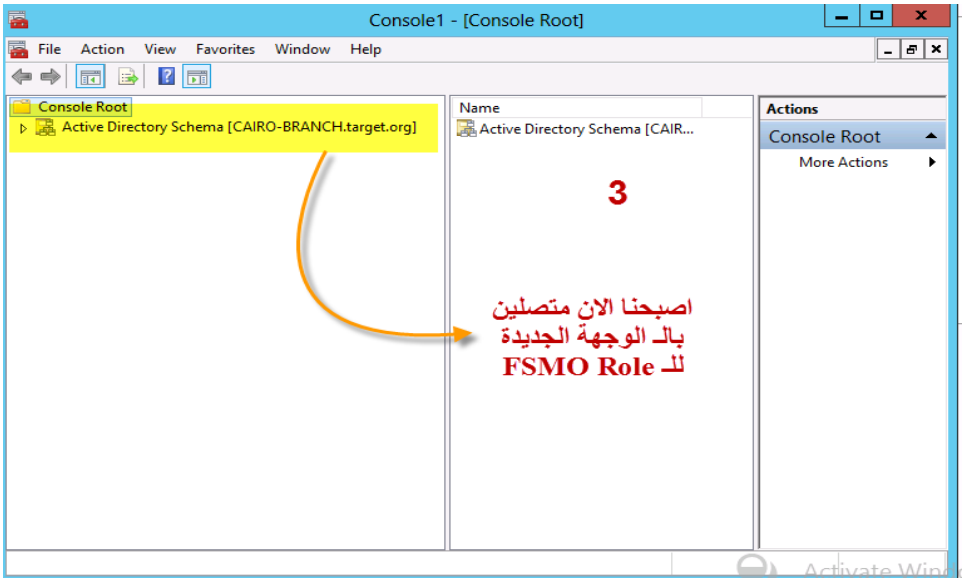


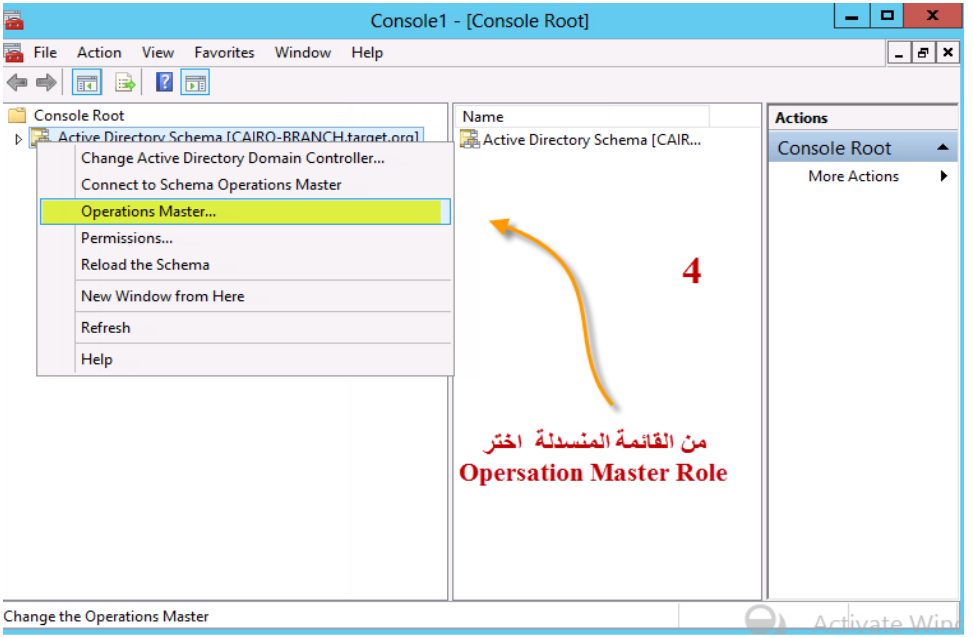
الان بعد أن تأكدنا من ان الـ Parent Domain Controller لمجال (Target.org) هو الموجود في المركز الرئيسي في الرياض باسم (DC) سنقوم الان بنقل الـ FSMO من هذا الـ Server الى الـ Server الموجود في فرع القاهرة .

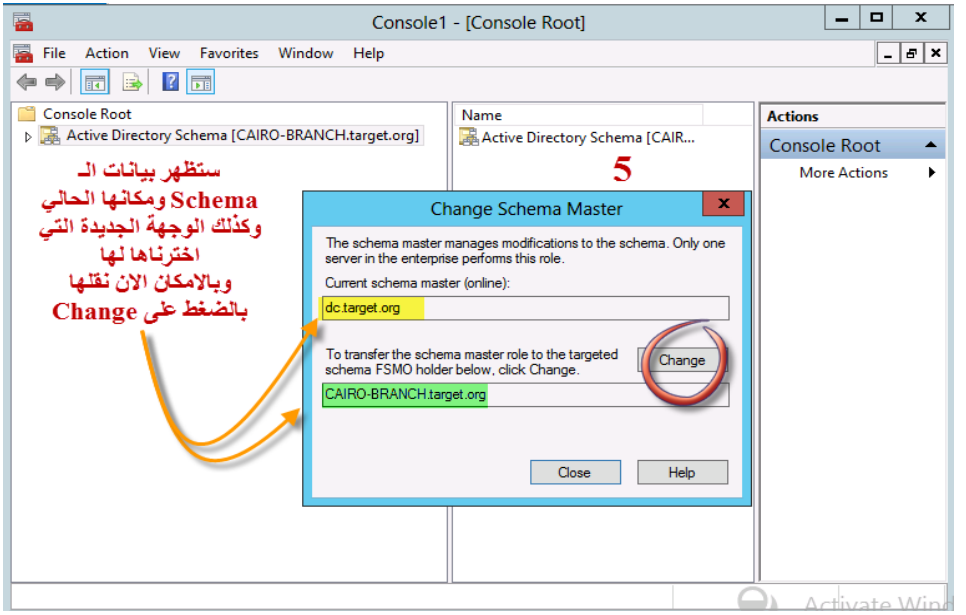
خطوات نقل الـ Schema Role

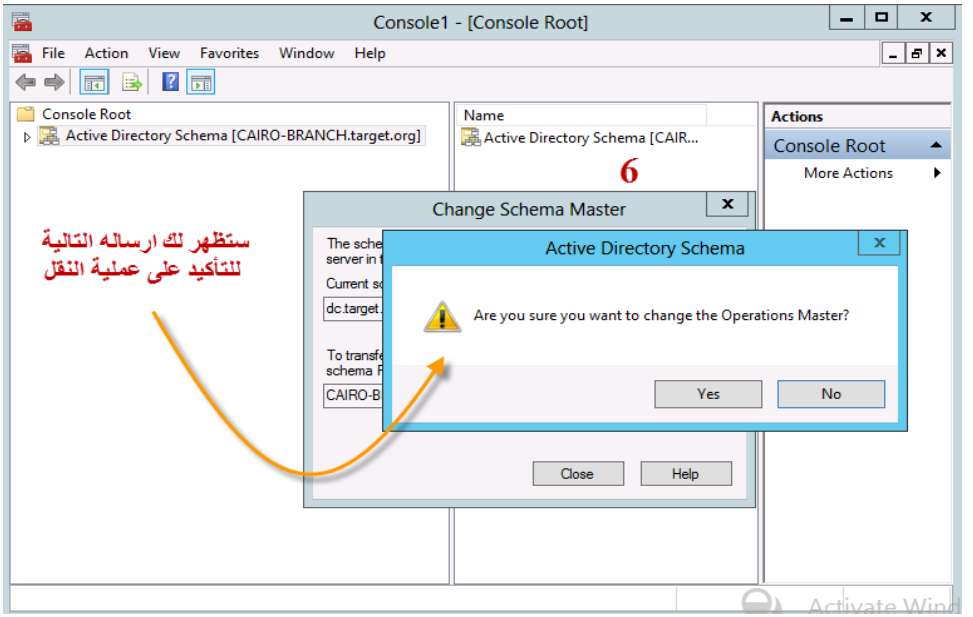


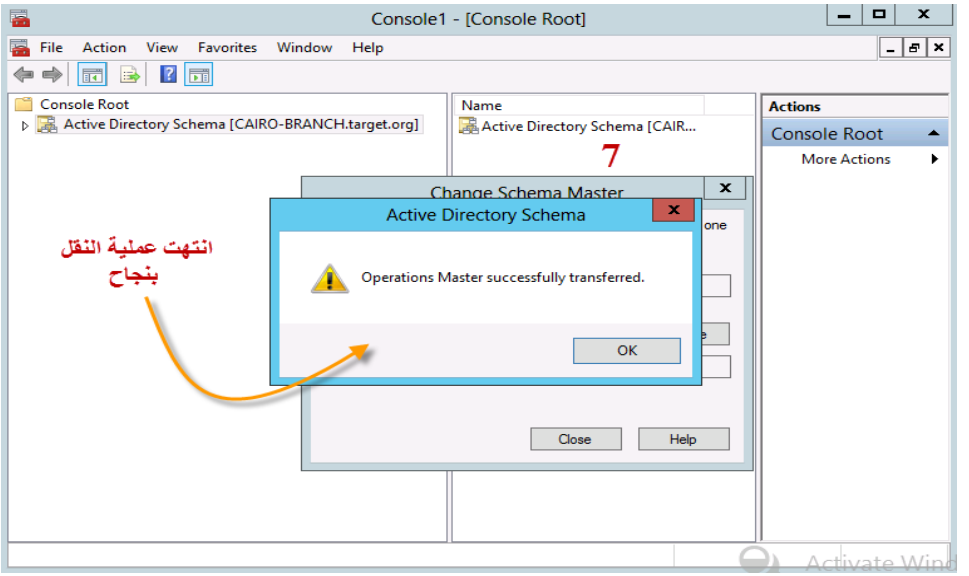


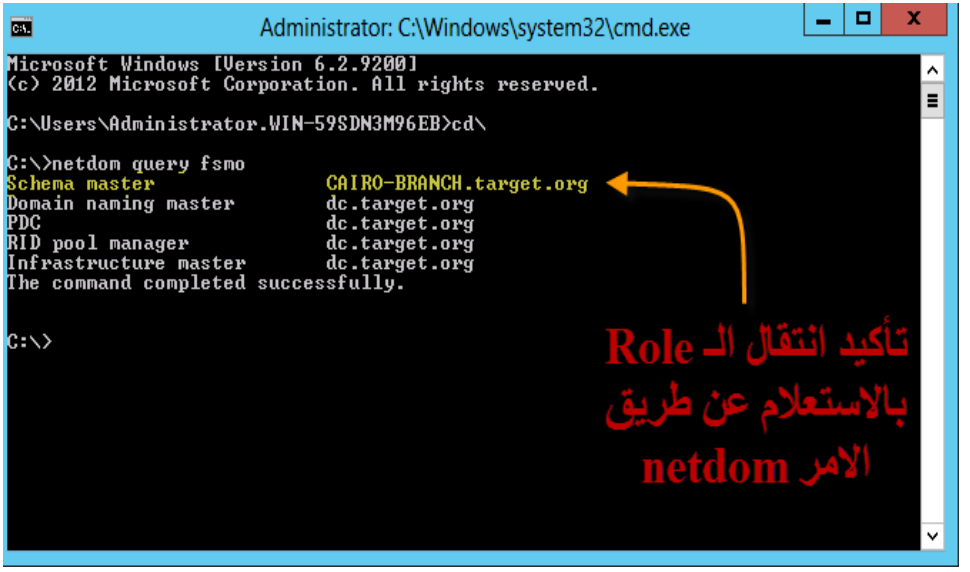

Console1 - [Console Root]
File Action View Favorites Window Help
Console Root
Active Directory Schema [CAIRO-BRANCH.target.org]
Name
Active Directory Schema [CAIR...
Actions
Console Root
More Actions
3
اصبحنا الان متصلين
بالـ الوجهة الجديدة
للـ FSMO Role


Console1 - [Console Root]
File Action View Favorites Window Help
Console Root
Active Directory Schema [CAIRO-BRANCH.target.org]
Change Active Directory Domain Controller...
Connect to Schema Operations Master
Operations Master...
Permissions...
Reload the Schema
New Window from Here
Refresh
Help
Name
Active Directory Schema [CAIR...
Actions
Console Root
More Actions
4
من القائمة المنسدلة اختر
Opersation Master Role
Change the Operations Master


Console1 - [Console Root]
File Action View Favorites Window Help
Console Root
Active Directory Schema [CAIRO-BRANCH.target.org]
Name
Active Directory Schema [CAIR...
Actions
Console Root
More Actions
5
ستظهر بيانات الـ Schema ومكانها الحالي وكذلك الوجهة الجديدة التي اخترناها لها وبالامكان الان نقلها بالضغط على Change
Change Schema Master
The schema master manages modifications to the schema. Only one server in the enterprise performs this role.
Current schema master (online):
dc.target.org
To transfer the schema master role to the targeted schema FSMO holder below, click Change.
Change
CAIRO-BRANCH.target.org
Close
Help

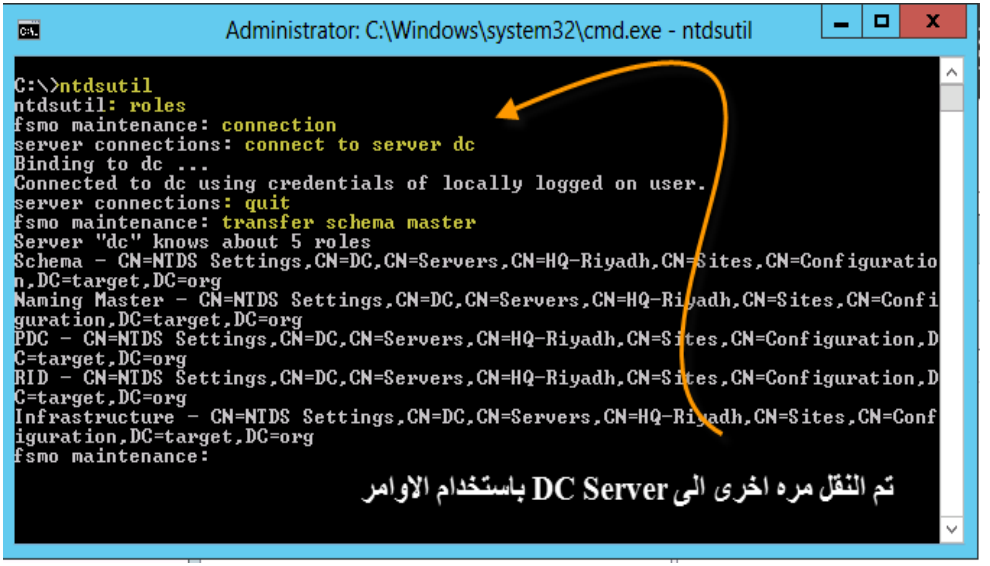

Console1 - [Console Root]
File Action View Favorites Window Help
Console Root
Active Directory Schema [CAIRO-BRANCH.target.org]
Name
Active Directory Schema [CAIR...
Actions
Console Root
More Actions
6
ستظهر لك ارساله التالية للتأكيد على عملية النقل
Change Schema Master
Active Directory Schema
Are you sure you want to change the Operations Master?
Yes
No
Close
Help


Console1 - [Console Root]
File Action View Favorites Window Help
Console Root
Active Directory Schema [CAIRO-BRANCH.target.org]
Name
Active Directory Schema [CAIR...
7
Actions
Console Root
More Actions
Change Schema Master
Active Directory Schema
Operations Master successfully transferred.
OK
Close
Help
انتهت عملية النقل
بنجاح

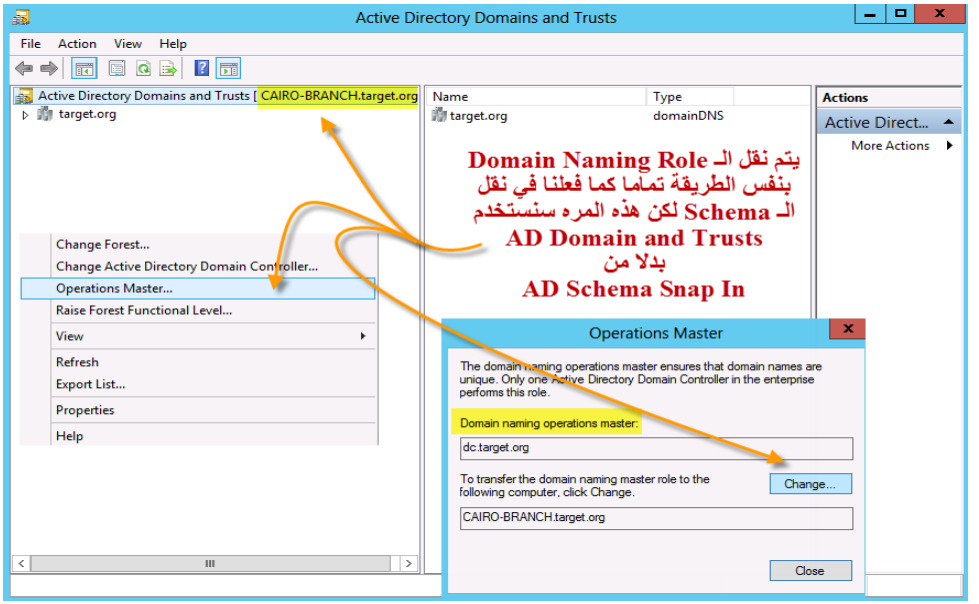

Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.
C:\Users\Administrator.WIN-59SDN3M96EB>cd\
C:\>netdom query fsmo
Schema master CAIRO-BRANCH.target.org
Domain naming master dc.target.org
PDC dc.target.org
RID pool manager dc.target.org
Infrastructure master dc.target.org
The command completed successfully.
C:\>
تأكيد انتقال الـ Role
بالاستعلام عن طريق
الامر netdom

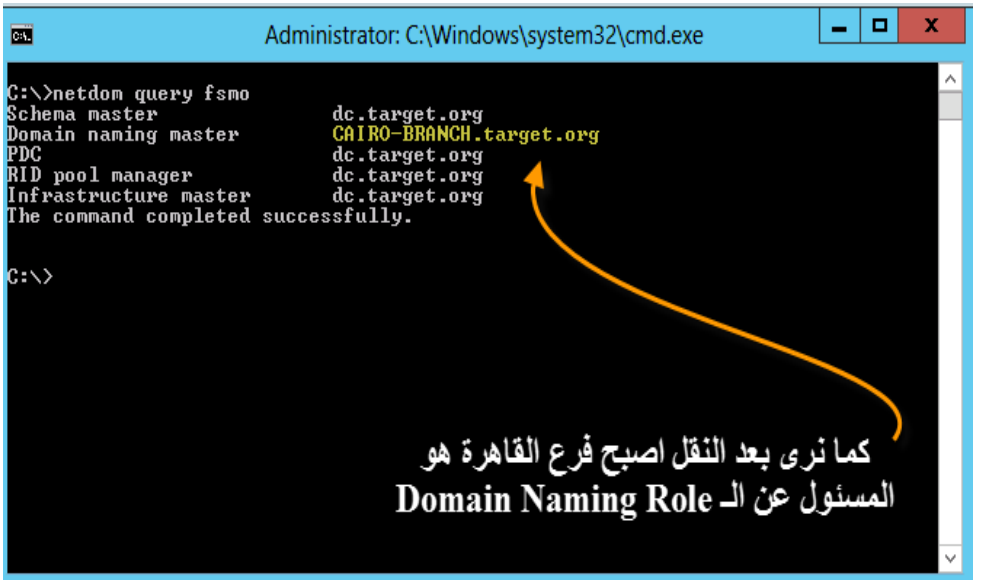
يمكن ايضا ان نقوم بنقل الـ Schema باستخدام سطر الاوامر (CMD) عن طريق الأكواد التالية :-

1. Open Command Prompt.
2. Type: ntdsutil
3. At the ntdsutil command prompt, type: roles
4. At the fsmo maintenance command prompt, type: connection
5. At the server connections command prompt, type: connect to server (type your server name that you want to transfer to him)
6. At the server connections command prompt, type: quit
7. At the fsmo maintenance command prompt, type: transfer schema master



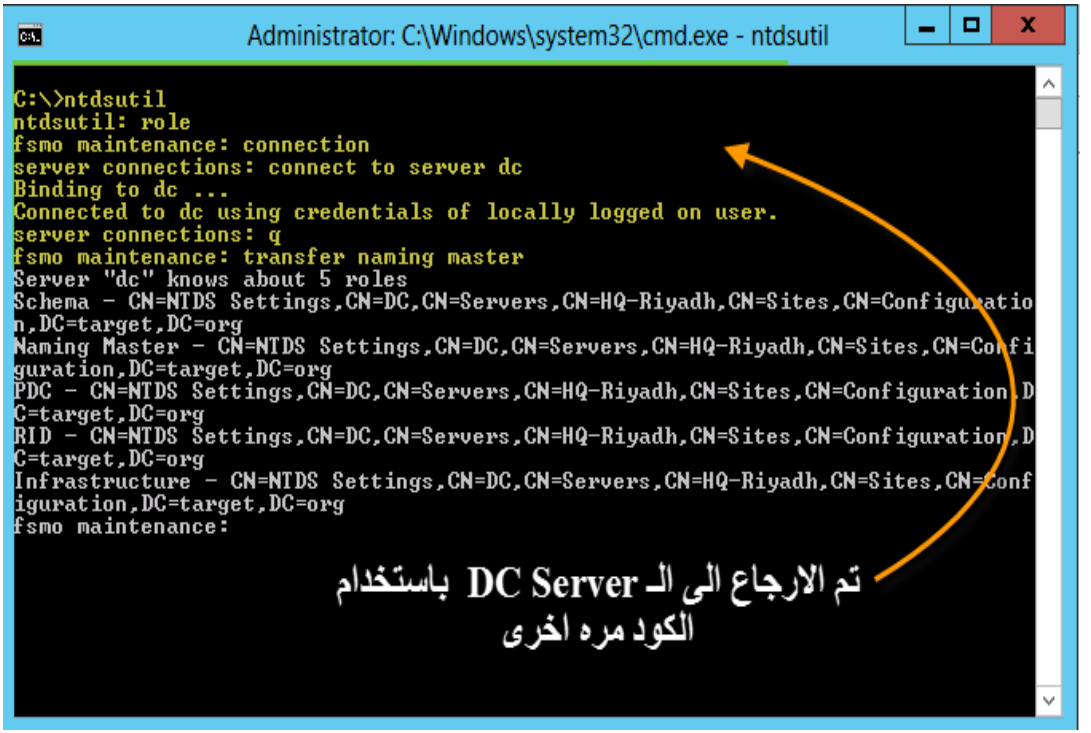
خطوات نقل الـ Domain Naming Master Role



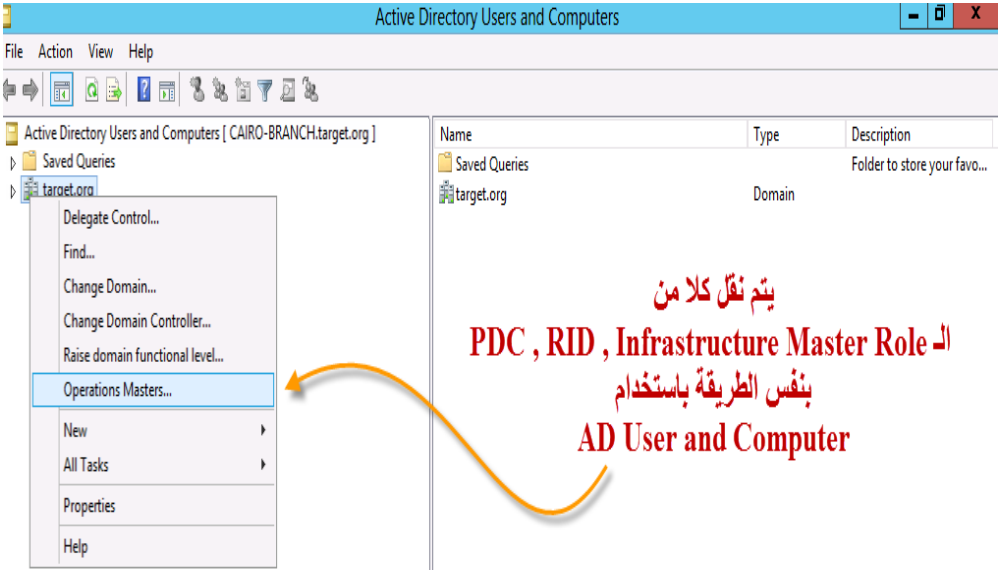


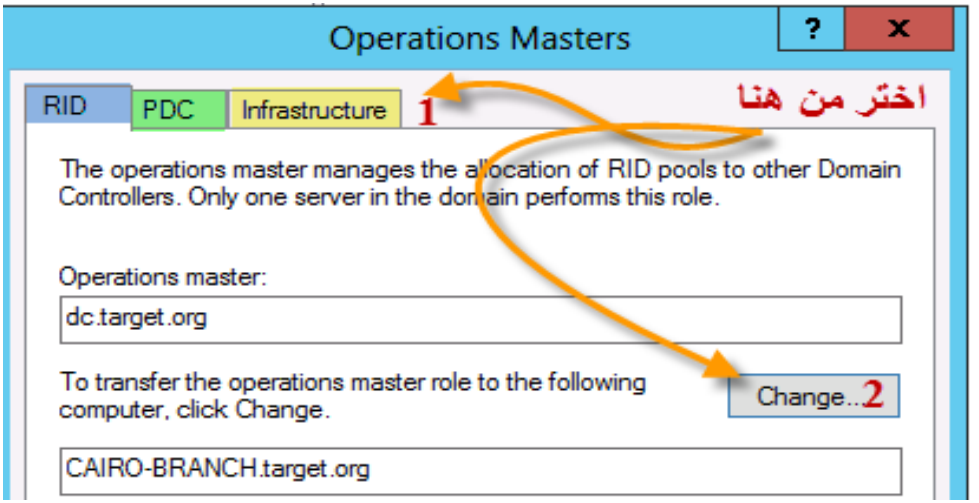
يمكن ايضا ان نقوم بنقل الـ Domain Naming باستخدام سطر الاوامر (CMD) عن طريق الأكواد التالية :-

1. Open Command Prompt.
2. Type: **ntdsutil**
3. At the ntdsutil command prompt, type: **roles**
4. At the fsmo maintenance command prompt, type: **connection**
5. At the server connections command prompt, type: **connect to server** (type your server name that you want to transfer to him)
6. At the server connections command prompt, type: **quit**
7. At the fsmo maintenance command prompt, type: **transfer naming master**



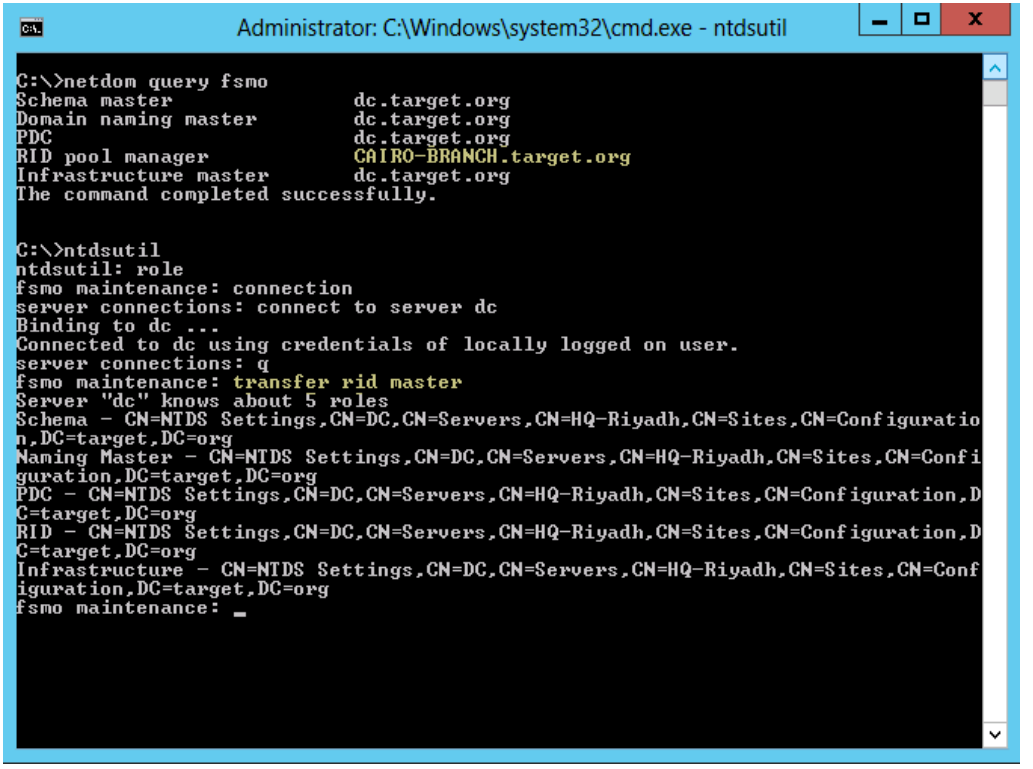
خطوات نقل الـ PDC , RID , Infrastructure Master Role





يمكن ايضا ان نقوم بنقل الـ PDC , RID , Infrastructure باستخدام سطر الاوامر (CMD) عن طريق الأكواد التالية :-

1. Open Command Prompt.
2. Type: **ntdsutil**
3. At the ntdsutil command prompt, type: **roles**
4. At the fsmo maintenance command prompt, type: **connection**
5. At the server connections command prompt, type: **connect to server** (type your server name that you want to transfer to him)
6. At the server connections command prompt, type: **quit**
7. At the fsmo maintenance command prompt, type: **transfer** (RID) or (PDC) or (Ifrastructure)



انتهينا الان من نقل جميع الـ Operation Master Roles عن طريق الـ GUI وباستخدام الكود أيضا من Server الى آخر في حالة ان الـ Parent Domain Controller موجود Online ؟ والان سنتعرف على الاحتمال الثاني هو ان الـ Parent Domain Controller غير موجود أو متضرر

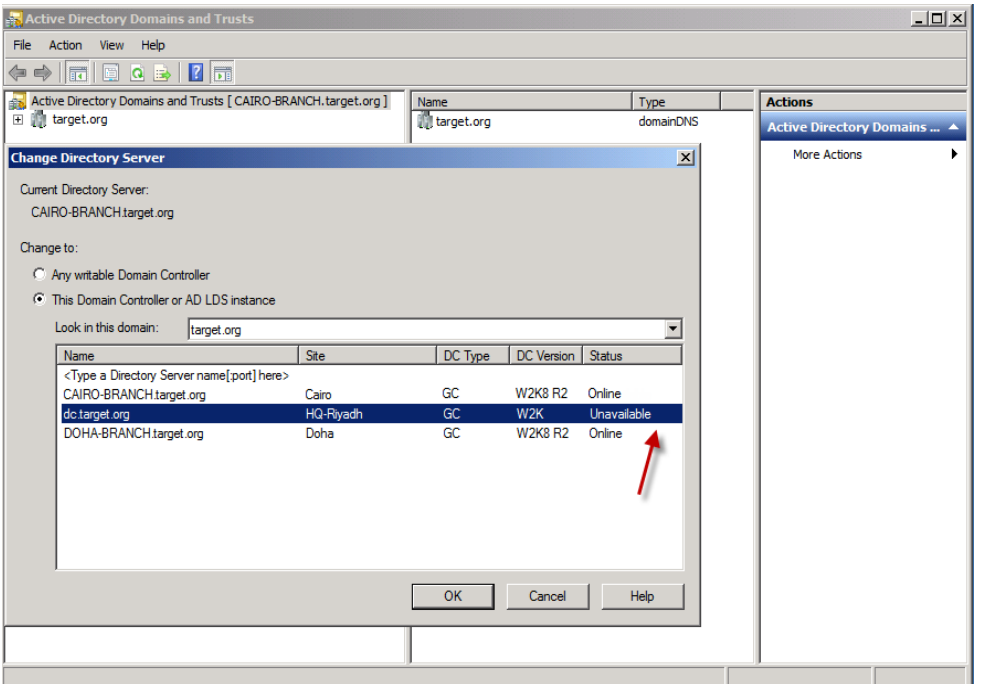
كيف يتم نقل الـ FSMO Roles عندما يكون الـ Parent Domain Controller غير موجود أو Offline ؟

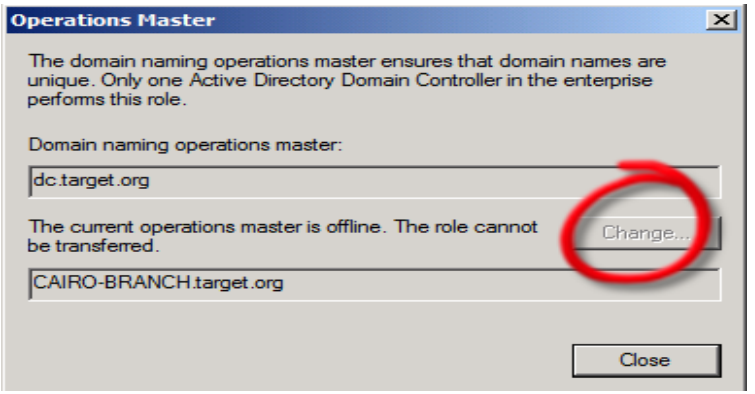
الاجابة هي : استخدام أمر الـ Seize

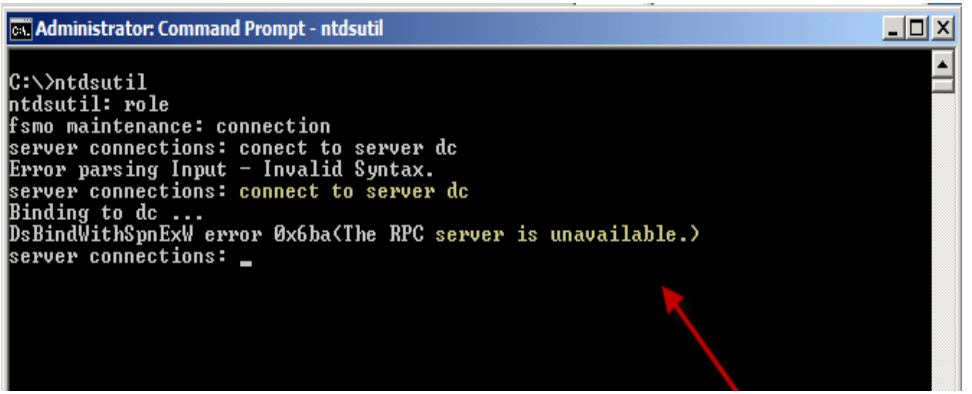
ولكن ماهو الـseize ؟ ومتى يتم عمله؟

الـ Seize هو عملية تصدير الـ role من Domain Controller إلى آخر في حالة إذا كان الـ Domain Controller الذي يقوم بمهمة ما لن يرجع للشبكة أبداً (لعطل في الهاردوير مثلا أو فشل في نظام التشغيل) أو في حال كان معطلاً لفترة لكننا نريد أخذ الـ role لسبب طارئ ففي هذه الحالة يجب تصدير أو عمل seize لـ Domain Controller آخر على الشبكة.

سأقوم الان تعمدا بتعطيل الـ Parent Domain Controller الخاص بشبكتنا Target.org حتى يتثنى لنا اجراء الـ Seize







كما نرى أصبح الـ **Parent Domain Controller** غير متاح والان يأتي دور أمر الـ **Seize**

أمر الـ Seize

1. Open Command Prompt.
2. Type: **ntdsutil**
3. At the ntdsutil command prompt, type: **roles**
4. At the fsmo maintenance command prompt, type: **connection**
5. At the server connections command prompt, type: **connect to server** (type your server name that you want to transfer to him)
6. At the server connections command prompt, type: **quit**
7. At the fsmo maintenance command prompt, type **seize (role name)**

ملاحظة مهمة جداً: بعد عمل **seize** لأي **role** ، يجب بعد اصلاح الخلل في الـ **Server** الأصلي عدم توصيله بالشبكة إلا بعد عمل اعادة تهيئة له **Format** وذلك حتى لا يتسبب بمشكلة لوجود أكثر من **Server** يلعب دور الـ **Domain Naming** .

فعلى سبيل المثال **server1** هو الـ **Domain Naming Master** وقد تعطل فجأة و في هذه الأثناء قمنا بعمل **seize** للـ **role** إلى **server2**

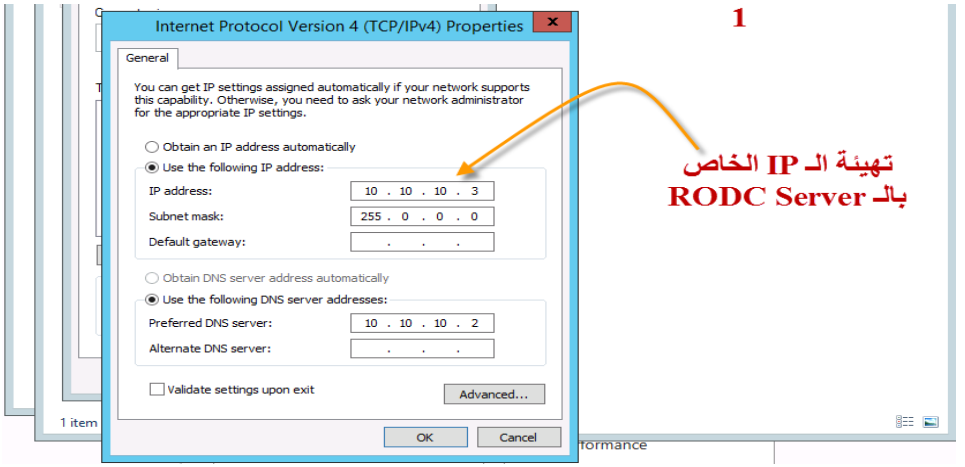
فيجب بعد إصلاح **server1** فورا القيام بعمل **Formatting** له ثم بعد ذلك نقوم بعمل **Transfer** للمهمة أو الـ **role** من من **server2**إلى **server1** مره اخرى اذا دعت الحاجة لذلك .

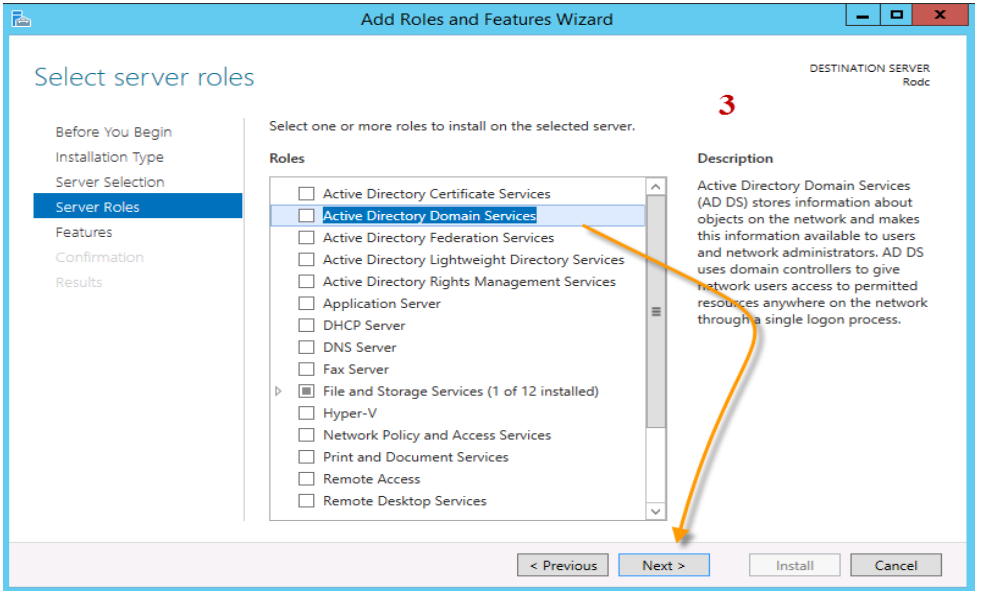
انتهينا الان من عمل الـ Replication وتطرقنا لنوع الـ Additional Domain والآن سنتناول نوع اخر من الـ Domain وهو الـ RODC و الـ RODC وهو نفس فكرة الـ Additional أي انه يعد نسخة طبق الاصل من الـ Domain أيضا غير انه للقراءة فقط ولا يمكن التعديل عليه إلا بمنح تفويض Authorization للقيام بهذا التعديل ويستخدم عادة في الشركات المتوسطة والكبيرة كنوع من انواع الحماية حيث لا تسجل على الـ RODC كلمات المرور وإنما يتم جلبها كما ذكرنا من الـ Domian

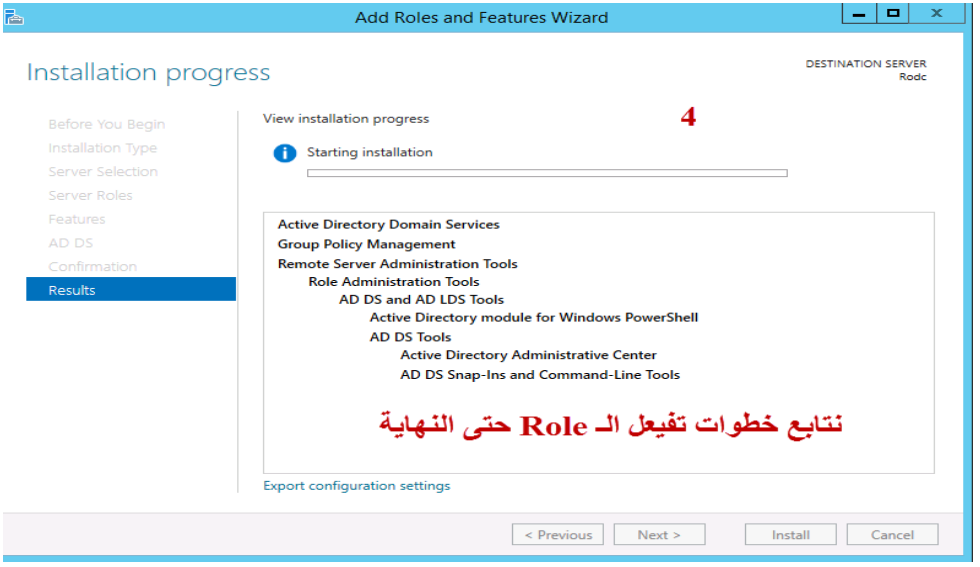
أو بمعنى اخر فان عملية الـ Authentication لا تتم عن طريق الـ RODC كخادم بل تتم عن طريق الـ Domain بواسطة خادم الـ RODC

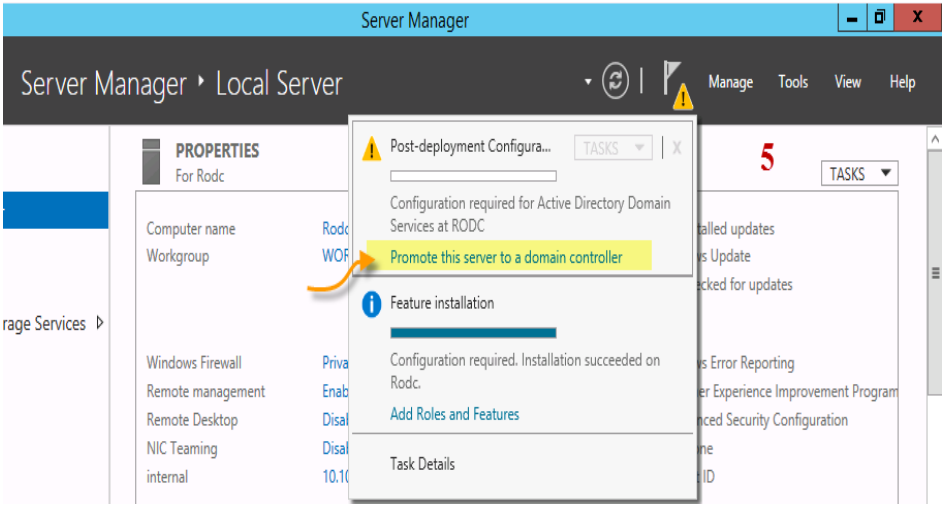
وللتوضيح أكثر فأننا سنفترض ان المركز الرئيسي في الرياض قد افتتح فرعا اخر داخل نفس المدينة وبالتالي فان هذا الفرع حتما سينضم لشبكتنا وكعامل أمان سنفوض أحد الأشخاص بتولى عملية ادارة هذا الفرع تقنيا بحيث يستطيع تولي العمليات المرتبطة بالشبكة بحسب ما يمنح له من صلاحيات ادارية فقط وفي هذه الحالة فان الخيار الافضل هو استخدام الـ RODC

ولعمل الـ RODC Server فسنقوم بضبط اعداد الـ IP والـ Server Name ثم نتابع خطوات التثبيت المعروفة

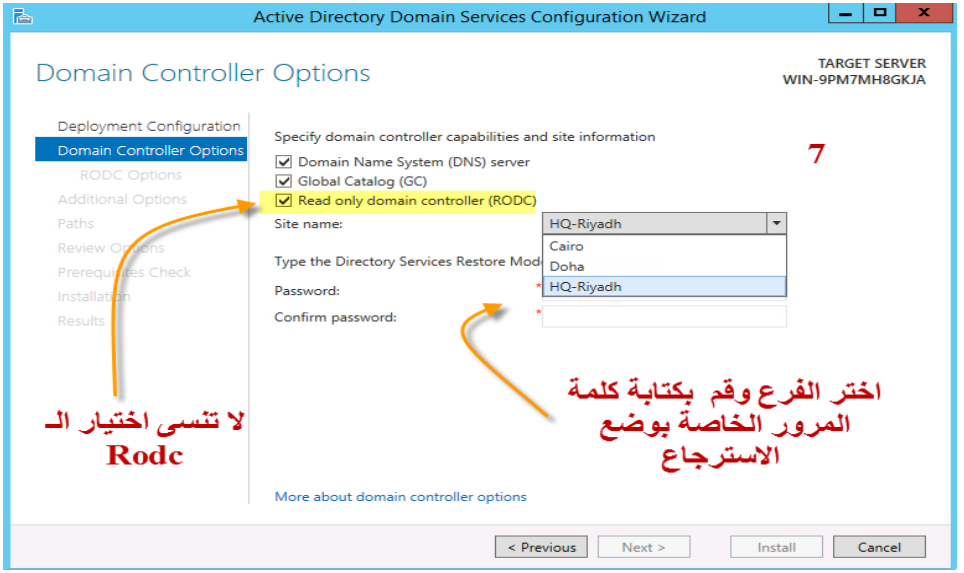


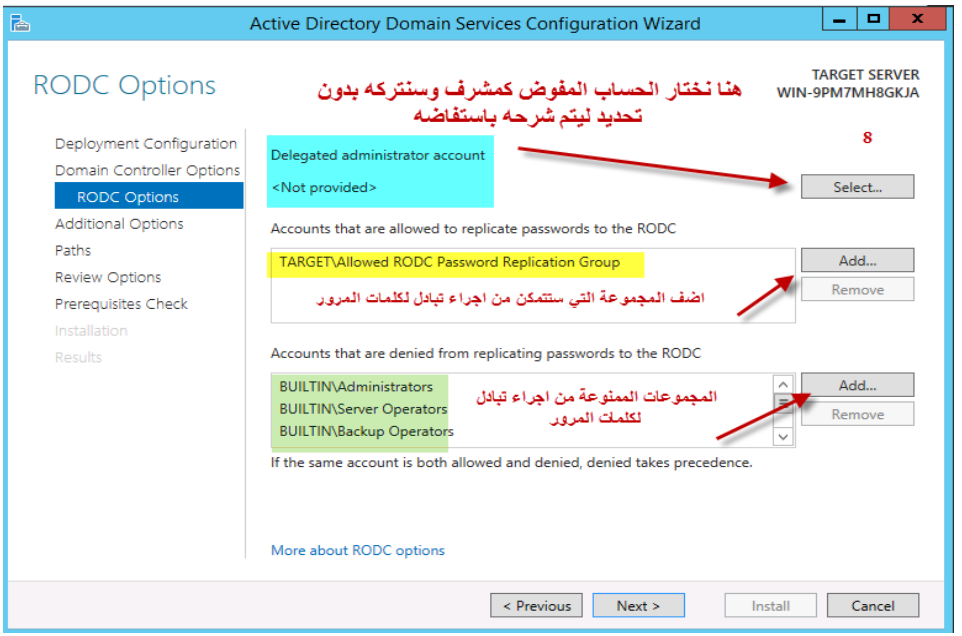

Add Roles and Features Wizard
Select server roles
DESTINATION SERVER
Rodc
3
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select one or more roles to install on the selected server.
Roles
Active Directory Certificate Services
Active Directory Domain Services
Active Directory Federation Services
Active Directory Lightweight Directory Services
Active Directory Rights Management Services
Application Server
DHCP Server
DNS Server
Fax Server
File and Storage Services (1 of 12 installed)
Hyper-V
Network Policy and Access Services
Print and Document Services
Remote Access
Remote Desktop Services
Description
Active Directory Domain Services (AD DS) stores information about objects on the network and makes this information available to users and network administrators. AD DS uses domain controllers to give network users access to permitted resources anywhere on the network through a single logon process.
< Previous
Next >
Install
Cancel

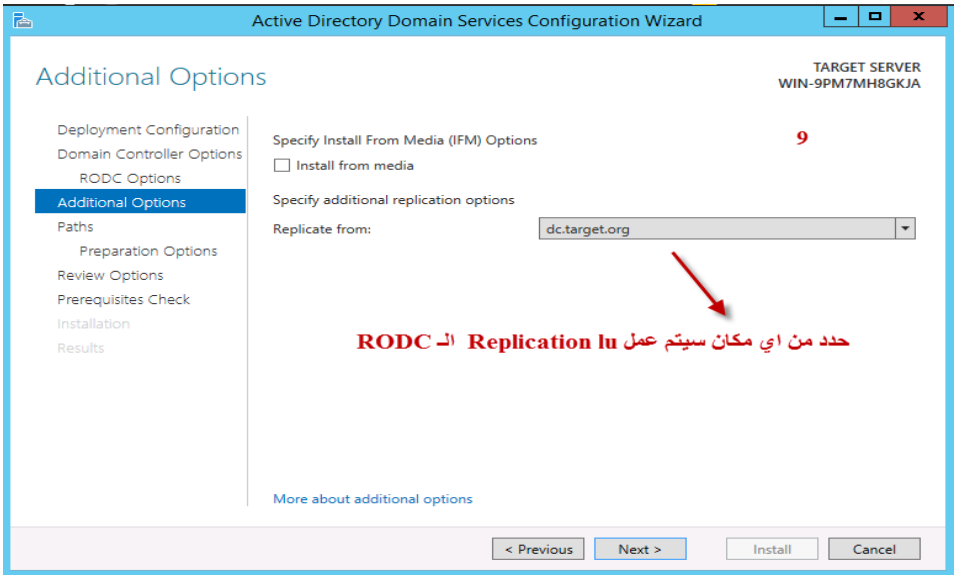

Add Roles and Features Wizard
Installation progress
DESTINATION SERVER
Rodc
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
Confirmation
Results
View installation progress
4
Starting installation
Active Directory Domain Services
Group Policy Management
Remote Server Administration Tools
Role Administration Tools
AD DS and AD LDS Tools
Active Directory module for Windows PowerShell
AD DS Tools
Active Directory Administrative Center
AD DS Snap-Ins and Command-Line Tools
نتابع خطوات تفيعل الـ Role حتى النهاية
Export configuration settings
< Previous
Next >
Install
Cancel

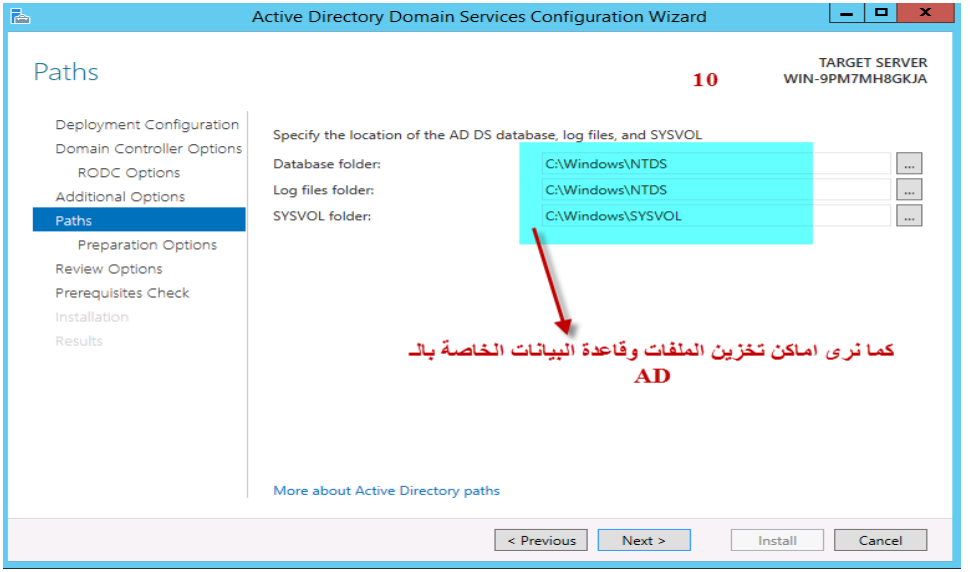

Server Manager
Server Manager ‣ Local Server
Manage
Tools
View
Help
PROPERTIES
For Rodc
Computer name
Workgroup
Post-deployment Configura...
TASKS
Configuration required for Active Directory Domain Services at RODC
Promote this server to a domain controller
Feature installation
Configuration required. Installation succeeded on Rodc.
Add Roles and Features
Task Details
5
TASKS
rage Services
Windows Firewall
Remote management
Remote Desktop
NIC Teaming
internal

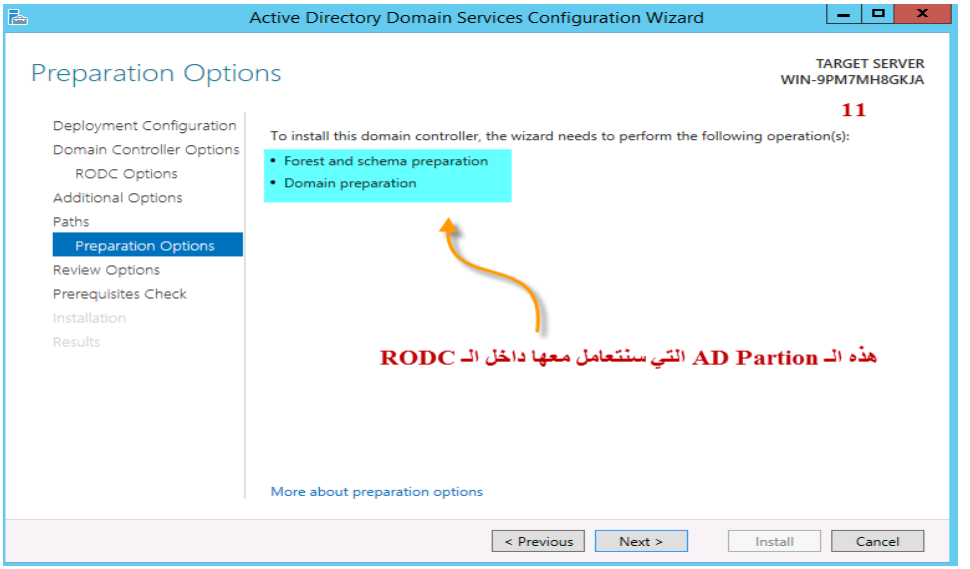

Active Directory Domain Services Configuration Wizard
Deployment Configuration
6
TARGET SERVER
Rodc
Deployment Configuration
Domain Controller Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Select the deployment operation
Add a domain controller to an existing domain
Add a new domain to an existing forest
Add a new forest
Specify the domain information for this operation
Domain:
Select...
Change...
Windows Security
Credentials for deployment operation
Supply credentials for the deployment operation
target.org\administrator
Domain: target.org
OK
Cancel
ادخل بيانات الاعتماد
Next >
Install
Cancel

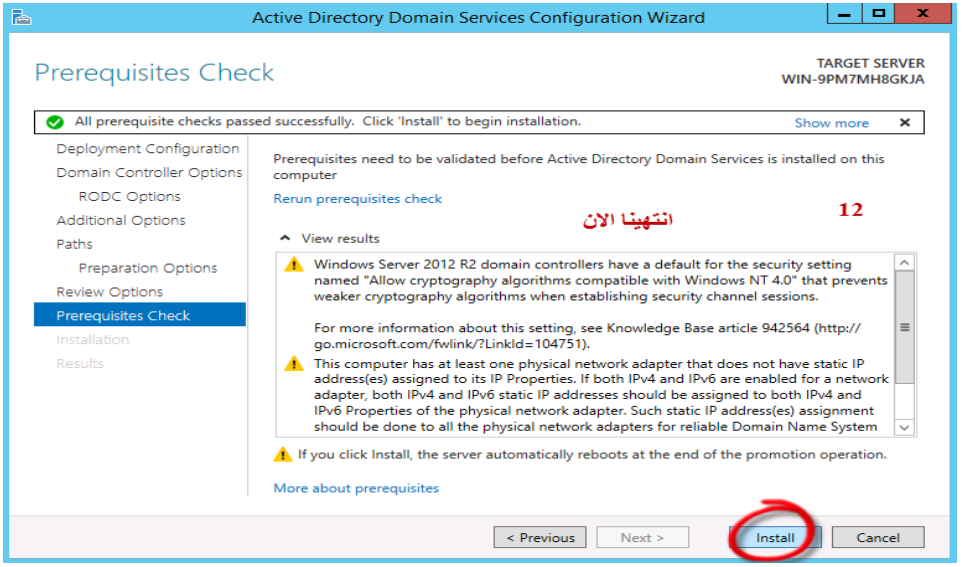

Active Directory Domain Services Configuration Wizard
Domain Controller Options
TARGET SERVER
WIN-9PM7MH8GKJA
Deployment Configuration
Domain Controller Options
RODC Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Specify domain controller capabilities and site information
7
Domain Name System (DNS) server
Global Catalog (GC)
Read only domain controller (RODC)
Site name:
HQ-Riyadh
Cairo
Doha
HQ-Riyadh
Type the Directory Services Restore Mod
Password:
Confirm password:
لا تنسى اختيار الـ
Rodc
اختر الفرع وقم بكتابة كلمة
المرور الخاصة بوضع
الاسترجاع
More about domain controller options
< Previous
Next >
Install
Cancel

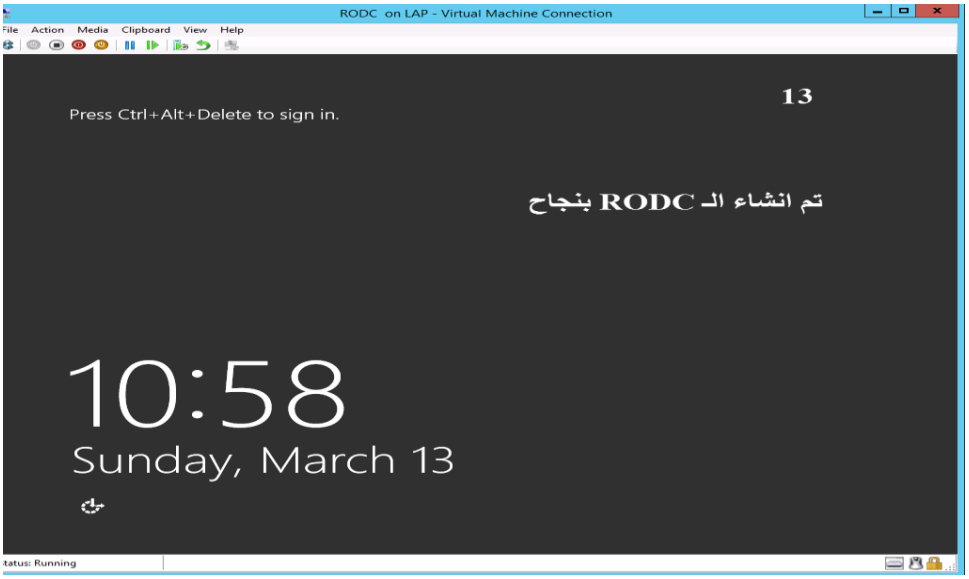

Active Directory Domain Services Configuration Wizard
RODC Options
TARGET SERVER
WIN-9PM7MH8GKJA
هنا نختار الحساب المفوض كمشرف وسنتركه بدون
تحديد ليتم شرحه باستفاضه
8
Deployment Configuration
Domain Controller Options
RODC Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Delegated administrator account
<Not provided>
Select...
Accounts that are allowed to replicate passwords to the RODC
TARGET\Allowed RODC Password Replication Group
Add...
Remove
اضف المجموعة التي ستتمكن من اجراء تبادل لكلمات المرور
Accounts that are denied from replicating passwords to the RODC
BUILTIN\Administrators
BUILTIN\Server Operators
BUILTIN\Backup Operators
المجموعات الممنوعة من اجراء تبادل
لكلمات المرور
Add...
Remove
If the same account is both allowed and denied, denied takes precedence.
More about RODC options
< Previous
Next >
Install
Cancel

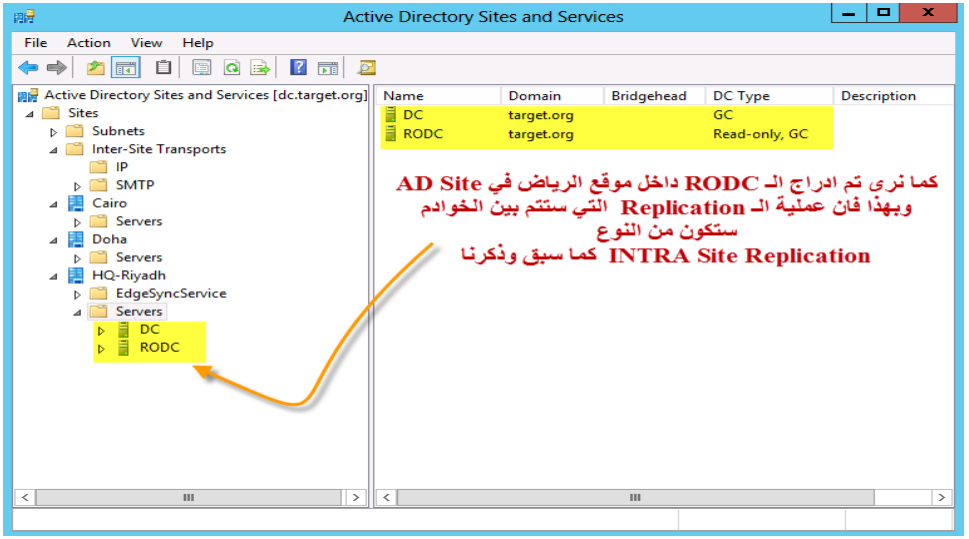

Active Directory Domain Services Configuration Wizard
Additional Options
TARGET SERVER
WIN-9PM7MH8GKJA
Deployment Configuration
Domain Controller Options
RODC Options
Additional Options
Paths
Preparation Options
Review Options
Prerequisites Check
Installation
Results
Specify Install From Media (IFM) Options
9
Install from media
Specify additional replication options
Replicate from:
dc.target.org
حدد من اي مكان سيتم عمل Replication lu الـ RODC
More about additional options
< Previous
Next >
Install
Cancel


Active Directory Domain Services Configuration Wizard
Paths
10
TARGET SERVER
WIN-9PM7MH8GKJA
Deployment Configuration
Domain Controller Options
RODC Options
Additional Options
Paths
Preparation Options
Review Options
Prerequisites Check
Installation
Results
Specify the location of the AD DS database, log files, and SYSVOL
Database folder:
C:\Windows\NTDS
Log files folder:
C:\Windows\NTDS
SYSVOL folder:
C:\Windows\SYSVOL
كما نرى اماكن تخزين الملفات وقاعدة البيانات الخاصة بالـ AD
More about Active Directory paths
< Previous
Next >
Install
Cancel

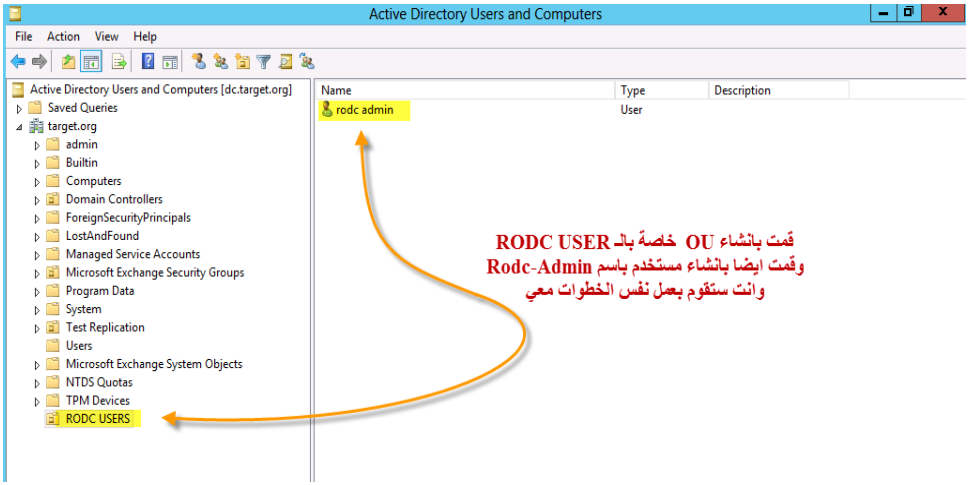

Active Directory Domain Services Configuration Wizard
Preparation Options
TARGET SERVER
WIN-9PM7MH8GKJA
11
Deployment Configuration
Domain Controller Options
RODC Options
Additional Options
Paths
Preparation Options
Review Options
Prerequisites Check
Installation
Results
To install this domain controller, the wizard needs to perform the following operation(s):
• Forest and schema preparation
• Domain preparation
هذه الـ AD Partion التي سنتعامل معها داخل الـ RODC
More about preparation options
< Previous
Next >
Install
Cancel


Active Directory Domain Services Configuration Wizard
Prerequisites Check
TARGET SERVER
WIN-9PM7MH8GKJA
All prerequisite checks passed successfully. Click 'Install' to begin installation.
Show more
Deployment Configuration
Domain Controller Options
RODC Options
Additional Options
Paths
Preparation Options
Review Options
Prerequisites Check
Installation
Results
Prerequisites need to be validated before Active Directory Domain Services is installed on this computer
Rerun prerequisites check
انتهينا الان
12
View results
Windows Server 2012 R2 domain controllers have a default for the security setting named "Allow cryptography algorithms compatible with Windows NT 4.0" that prevents weaker cryptography algorithms when establishing security channel sessions.
For more information about this setting, see Knowledge Base article 942564 (http://go.microsoft.com/fwlink/?LinkId=104751).
This computer has at least one physical network adapter that does not have static IP address(es) assigned to its IP Properties. If both IPv4 and IPv6 are enabled for a network adapter, both IPv4 and IPv6 static IP addresses should be assigned to both IPv4 and IPv6 Properties of the physical network adapter. Such static IP address(es) assignment should be done to all the physical network adapters for reliable Domain Name System
If you click Install, the server automatically reboots at the end of the promotion operation.
More about prerequisites
< Previous
Next >
Install
Cancel

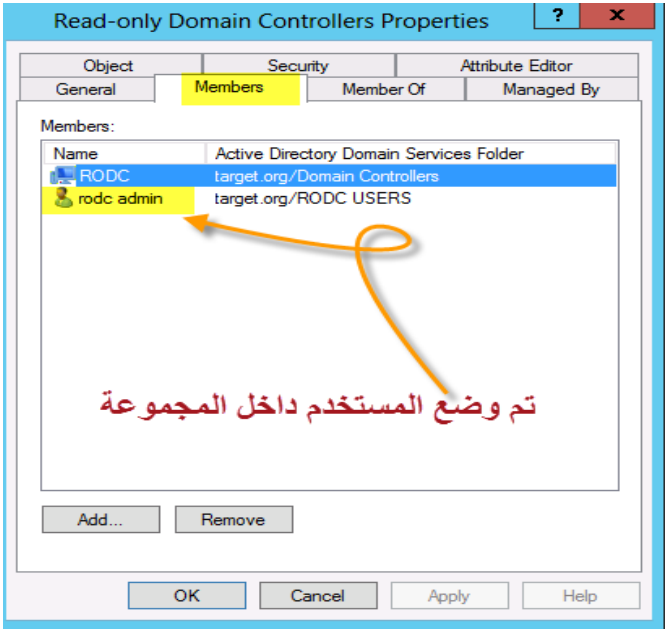




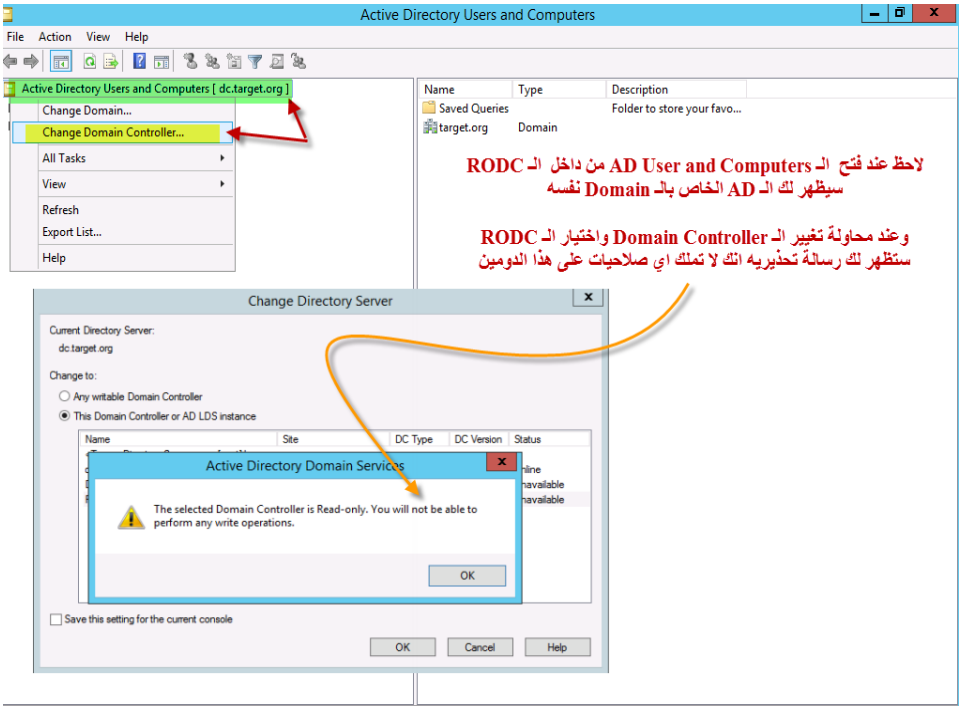
الان دعونا نكمل خطواتنا ونقوم **بتفويض** الشخص المسئول عن خادم الـ RODC

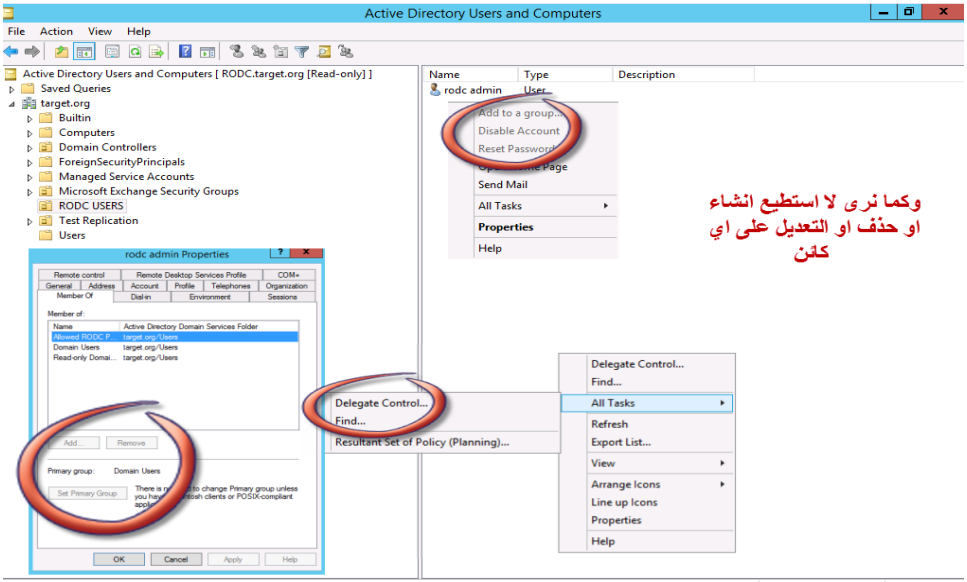

Active Directory Users and Computers
File Action View Help
Active Directory Users and Computers [dc.target.org]
Saved Queries
target.org
admin
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
LostAndFound
Managed Service Accounts
Microsoft Exchange Security Groups
Program Data
System
Test Replication
Users
Microsoft Exchange System Objects
NTDS Quotas
TPM Devices
RODC USERS
Name
Type
Description
rodc admin
User
قمت بانشاء OU خاصة بالـ RODC USER
وقمت ايضا بانشاء مستخدم باسم Rodc-Admin
وانت ستقوم بعمل نفس الخطوات معي


Other user
The sign-in method you're trying to use isn't allowed. For more info, contact your network administrator.
OK
لاحظ انه عند محاولة الدخول على الـ RODC بالمستخدم الذي
تم انشاؤه تظهر رسالة تفيد بعدم السماح بالدخول كما نرى
وحتى نستطيع فعل ذلك فانه لابد من وضع المستخدم في الـ
Read Only Domain Group
Windows Server 2012 R2

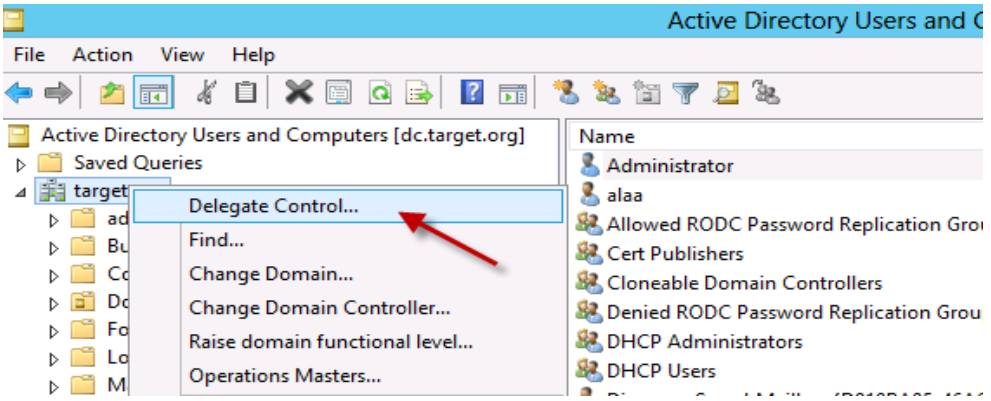

Read-only Domain Controllers Properties
Object
Security
Attribute Editor
General
Members
Member Of
Managed By
Members:
Name
Active Directory Domain Services Folder
RODC
target.org/Domain Controllers
rodc admin
target.org/RODC USERS
تم وضع المستخدم داخل المجموعة
Add...
Remove
OK
Cancel
Apply
Help

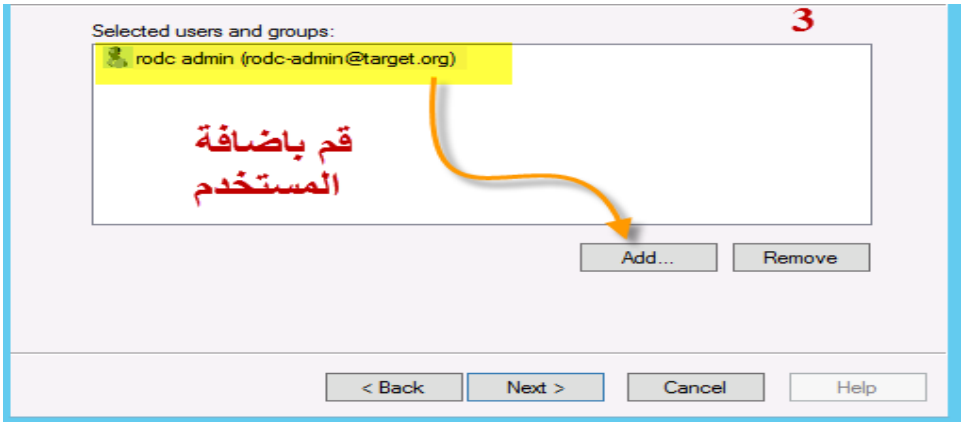

rodc admin
TARGET\rodc-admin
Applying user settings
والان نستطيع الدخول
Windows Server 2012 R2

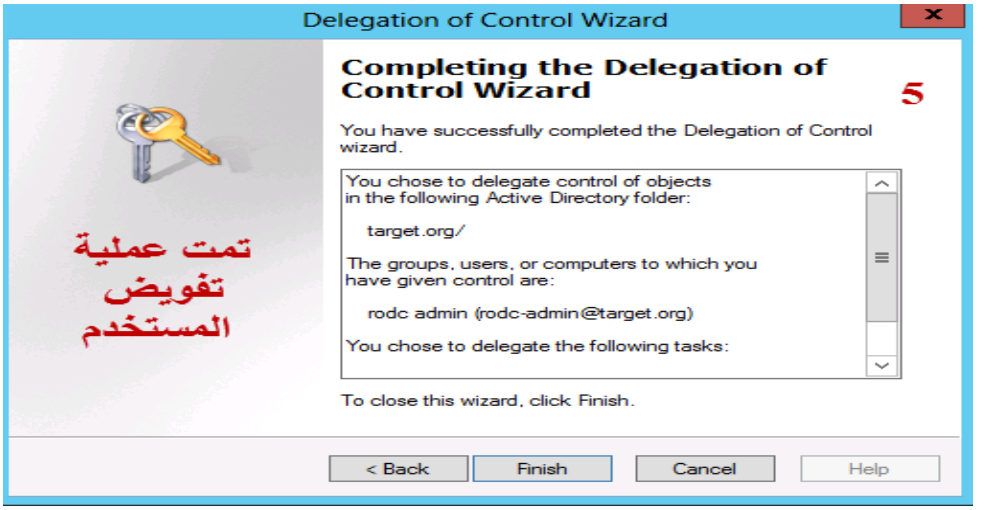

Active Directory Users and Computers
File Action View Help
Active Directory Users and Computers [dc.target.org]
Change Domain...
Change Domain Controller...
All Tasks
View
Refresh
Export List...
Help
Name Type Description
Saved Queries Folder to store your favo...
target.org Domain
لاحظ عند فتح الـ AD User and Computers من داخل الـ RODC
سيظهر لك الـ AD الخاص بالـ Domain نفسه
وعند محاولة تغيير الـ Domain Controller واختيار الـ RODC
ستظهر لك رسالة تحذيريه انك لا تملك اي صلاحيات على هذا الدومين
Change Directory Server
Current Directory Server:
dc.target.org
Change to:
Any writable Domain Controller
This Domain Controller or AD LDS instance
Name Site DC Type DC Version Status
Active Directory Domain Services
The selected Domain Controller is Read-only. You will not be able to perform any write operations.
OK
Save this setting for the current console
OK Cancel Help


Active Directory Users and Computers
File Action View Help
Active Directory Users and Computers [RODC.target.org [Read-only]]
Saved Queries
target.org
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Managed Service Accounts
Microsoft Exchange Security Groups
RODC USERS
Test Replication
Users
Name Type Description
rodc admin User
Add to a group...
Disable Account
Reset Password...
Send Mail
All Tasks
Properties
Help
وكما نرى لا استطيع انشاء
او حذف او التعديل على اي
كائن
rodc admin Properties
Delegate Control...
Find...
Resultant Set of Policy (Planning)...
Delegate Control...
Find...
All Tasks
Refresh
Export List...
View
Arrange Icons
Line up Icons
Properties
Help

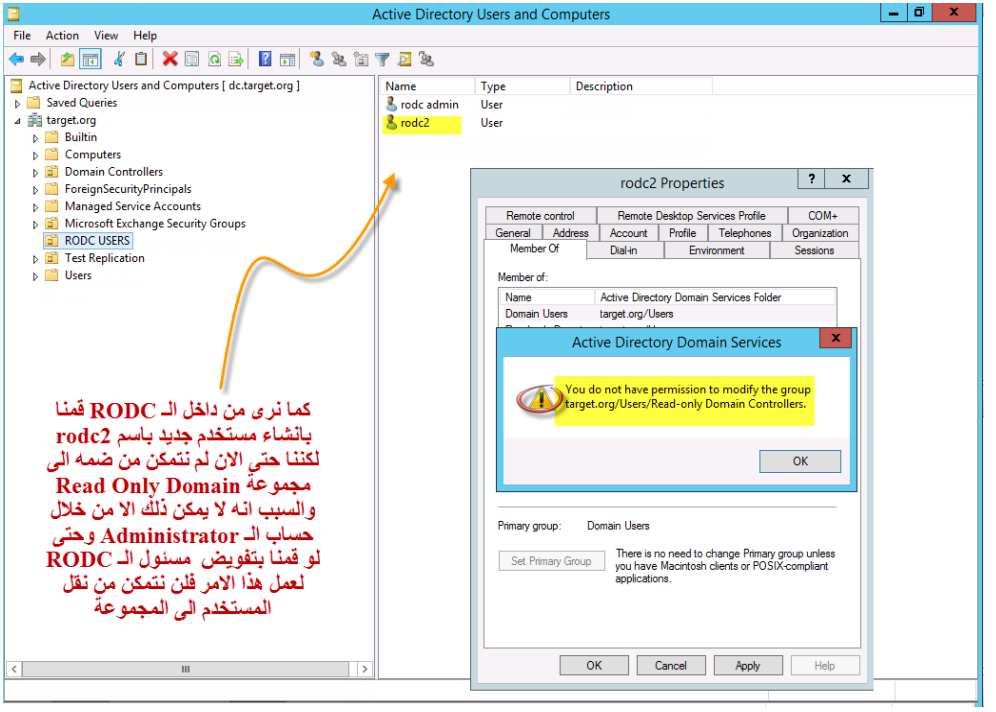
الان سنقوم بعمل الـ Delegation للمستخدم







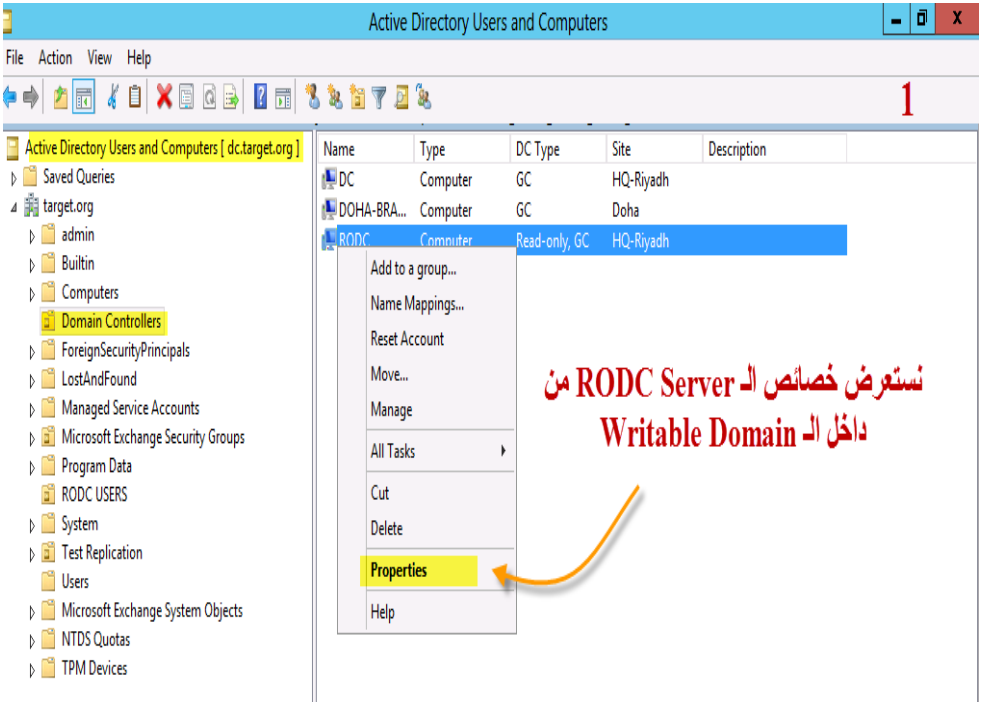
قمنا في الخطوات السابقة بتفويض المستخدم rodc-admin بحذف وإنشاء المستخدمين والآن سنجرب العملية من داخل الـ RODC

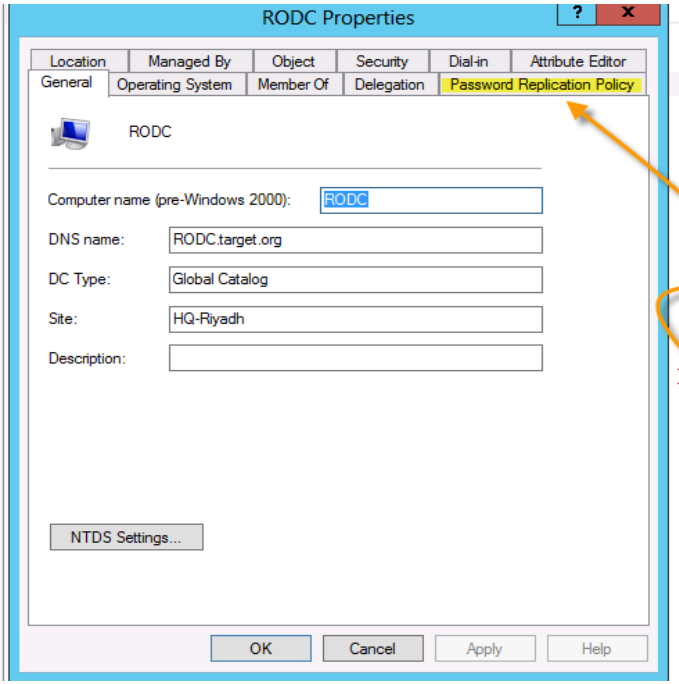


اذا من الصورة السابقة تتضح فكرة عمل الـ Rodc حيث لا يقوم بحفظ كلمات المرور عليه بل يجلبها من الـ Writable Domain وحتى يتستطيع المستخدم الدخول علي الـ RODC سيتم الاتصال أولا بهذا الـ Writable Domain لكي يحصل علي تصريح الدخول منه

وطبعا اذا لم يكن الـ Domain الرئيسي متاحا فلن يتمكن المستخدم العادي ولا حتى المستخدم المفوض من الدخول على الـ RODC لأنه ببساطة لا يوجد تصريح للدخول . **إذا فما الحل ؟**

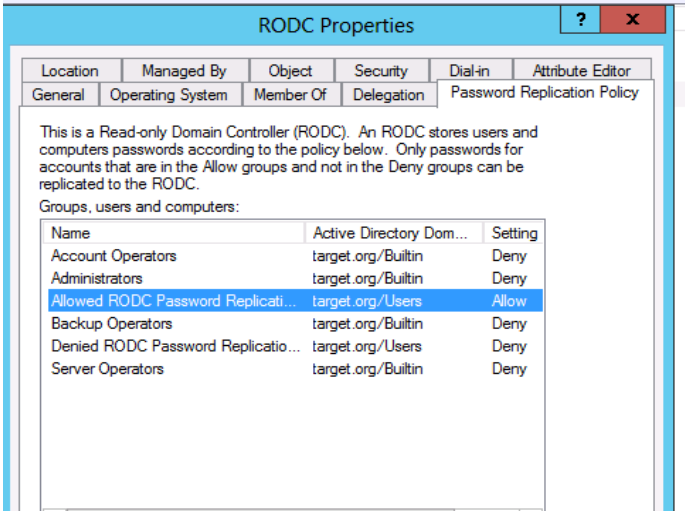
الحل هو ان نقوم بالسماح للمستخدمين بعمل تخزين Cache لكلمه المرور الخاصة بهم علي الـ RODC وبهذه الطريقة سيتمكن الـ RODC Users من الدخول عليه دون انتظار التصريح من الدومين الرئيسي والخطوات كالتالي :-



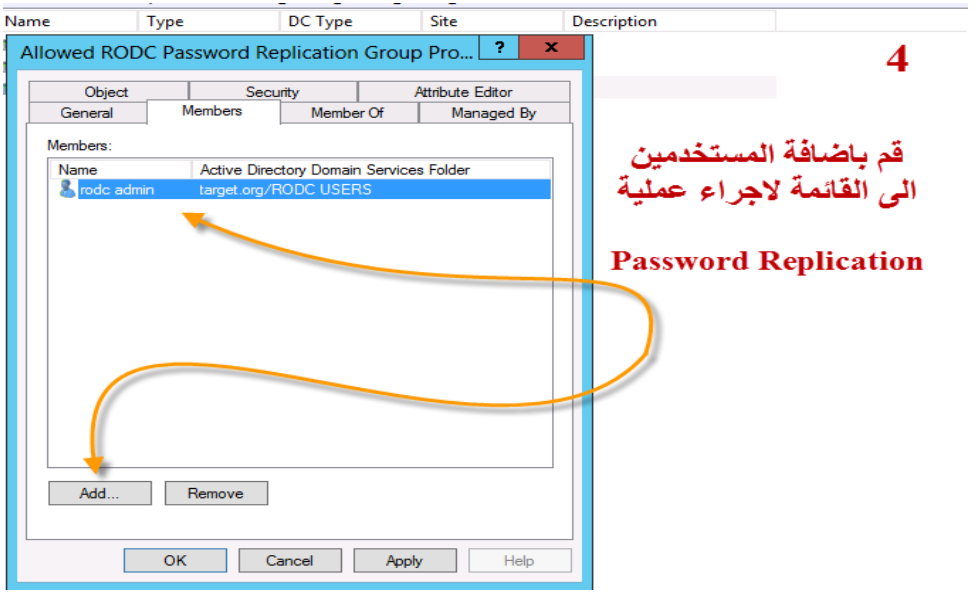


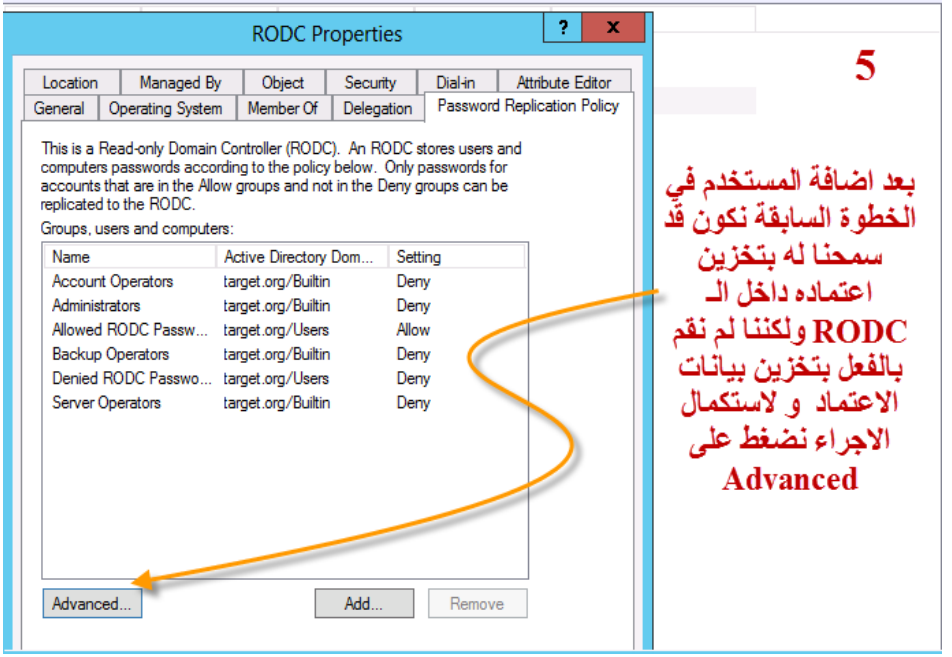
من خصائص الـ RODC
نذهب الى
Passord Replication
Policy

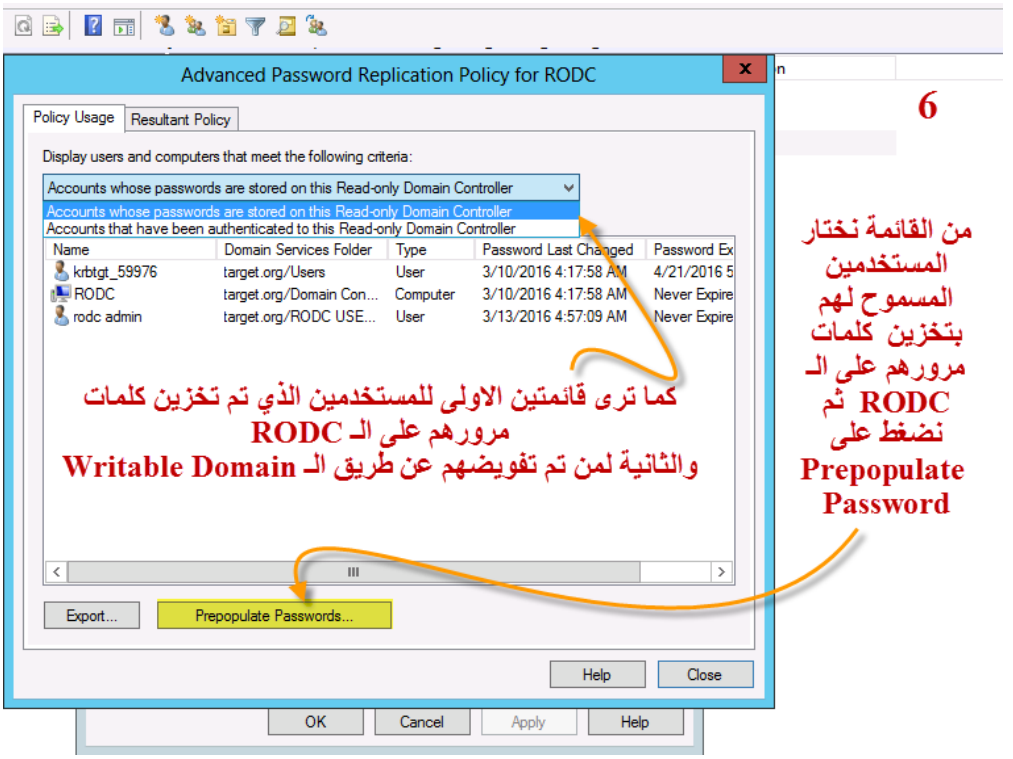
3



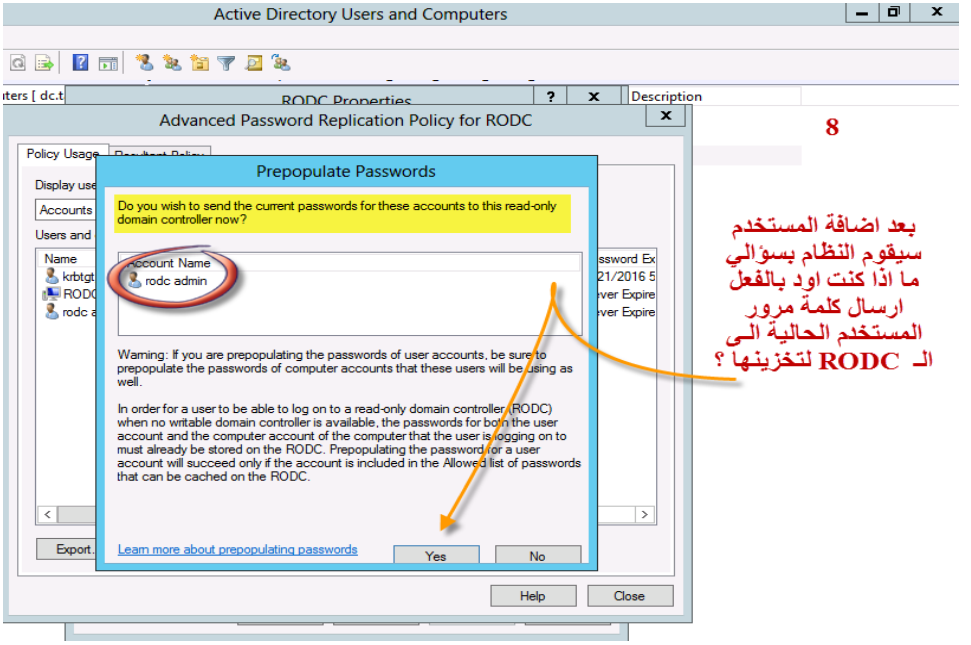
أختر مجموعة
Allowd Password
Replication


Name
Type
DC Type
Site
Description
Allowed RODC Password Replication Group Pro...
Object
Security
Attribute Editor
General
Members
Member Of
Managed By
Members:
Name
Active Directory Domain Services Folder
rodc admin
target.org/RODC USERS
Add...
Remove
OK
Cancel
Apply
Help
4
قم باضافة المستخدمين
الى القائمة لاجراء عملية
Password Replication


RODC Properties
Location
Managed By
Object
Security
Dial-in
Attribute Editor
General
Operating System
Member Of
Delegation
Password Replication Policy
This is a Read-only Domain Controller (RODC). An RODC stores users and computers passwords according to the policy below. Only passwords for accounts that are in the Allow groups and not in the Deny groups can be replicated to the RODC.
Groups, users and computers:
Name
Active Directory Dom...
Setting
Account Operators
target.org/Builtin
Deny
Administrators
target.org/Builtin
Deny
Allowed RODC Passw...
target.org/Users
Allow
Backup Operators
target.org/Builtin
Deny
Denied RODC Passwo...
target.org/Users
Deny
Server Operators
target.org/Builtin
Deny
Advanced...
Add...
Remove
5
بعد اضافة المستخدم في
الخطوة السابقة نكون قد
سمحنا له بتخزين
اعتماده داخل الـ
RODC ولكننا لم نقم
بالفعل بتخزين بيانات
الاعتماد و لاستكمال
الاجراء نضغط على
Advanced


Advanced Password Replication Policy for RODC
Policy Usage
Resultant Policy
Display users and computers that meet the following criteria:
Accounts whose passwords are stored on this Read-only Domain Controller
Accounts whose passwords are stored on this Read-only Domain Controller
Accounts that have been authenticated to this Read-only Domain Controller
Name
Domain Services Folder
Type
Password Last Changed
Password Ex
krbtgt_59976
target.org/Users
User
3/10/2016 4:17:58 AM
4/21/2016 5
RODC
target.org/Domain Con...
Computer
3/10/2016 4:17:58 AM
Never Expire
rodc admin
target.org/RODC USE...
User
3/13/2016 4:57:09 AM
Never Expire
Export...
Prepopulate Passwords...
Help
Close
OK
Cancel
Apply
Help
6
من القائمة نختار المستخدمين المسموح لهم بتخزين كلمات مرورهم على الـ RODC ثم نضغط على Prepopulate Password
كما ترى قائمتين الاولى للمستخدمين الذي تم تخزين كلمات مرورهم على الـ RODC
والثانية لمن تم تفويضهم عن طريق الـ Writable Domain

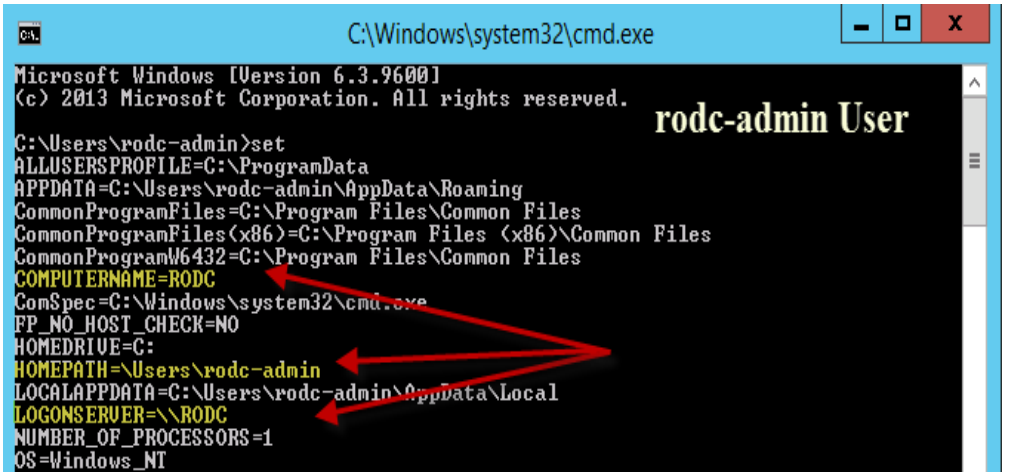

Advanced Password Replication Policy for RODC
Select Users or Computers
Select this object type:
Users or Computers
Object Types...
From this location:
target.org
Locations...
Enter the object names to select (examples):
rodc admin (rodc-admin@target.org)
Check Names
Advanced...
OK
Cancel
7
Password Ex
4/21/2016 5
Never Expire
Never Expire
قم باضافة المستخدم

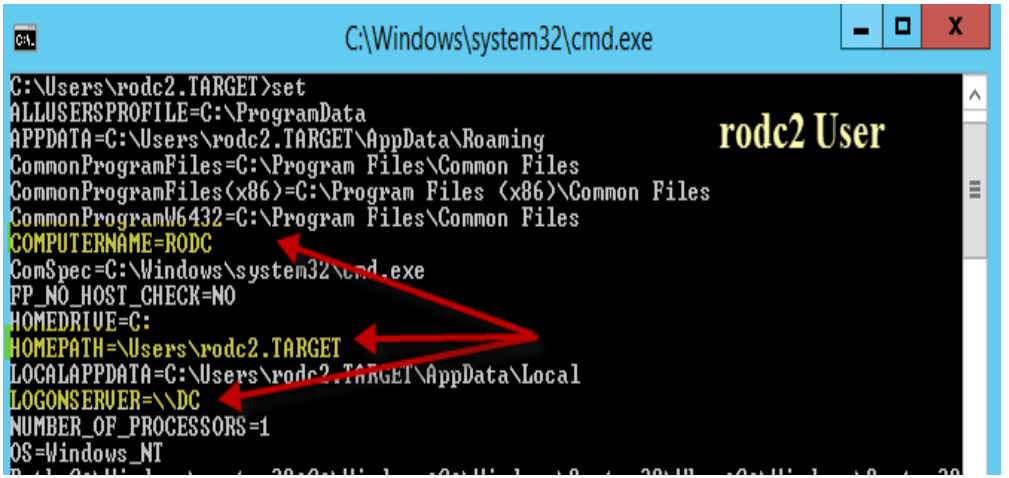

Active Directory Users and Computers
RODC Properties
Description
Advanced Password Replication Policy for RODC
Policy Usage
Prepopulate Passwords
Do you wish to send the current passwords for these accounts to this read-only domain controller now?
Account Name
rodc admin
Warning: If you are prepopulating the passwords of user accounts, be sure to prepopulate the passwords of computer accounts that these users will be using as well.
In order for a user to be able to log on to a read-only domain controller (RODC) when no writable domain controller is available, the passwords for both the user account and the computer account of the computer that the user is logging on to must already be stored on the RODC. Prepopulating the password for a user account will succeed only if the account is included in the Allowed list of passwords that can be cached on the RODC.
Learn more about prepopulating passwords
Yes
No
Help
Close
Export...
8
يعد اضافة المستخدم سيقوم النظام بسؤالي ما اذا كنت اود بالفعل ارسال كلمة مرور المستخدم الحالية الى الـ RODC لتخزينها ؟


Name
Domain Services Folder
Type
Password Last Changed
Password Ex
krbtgt_59976
RODC
rodc admin
4/21/2016 5
Never Expire
Never Expire
Prepopulating Passwords...
Processing item 1 out of 1...
Prepopulate Password Success
Passwords for all accounts were successfully prepopulated.
والان تمت العملية بنجاح
OK
Export...
Prepopulate Passwords...

الان سنجرب العملية معا وللتذكير فان لدينا عدد User 2 كالتالي :-

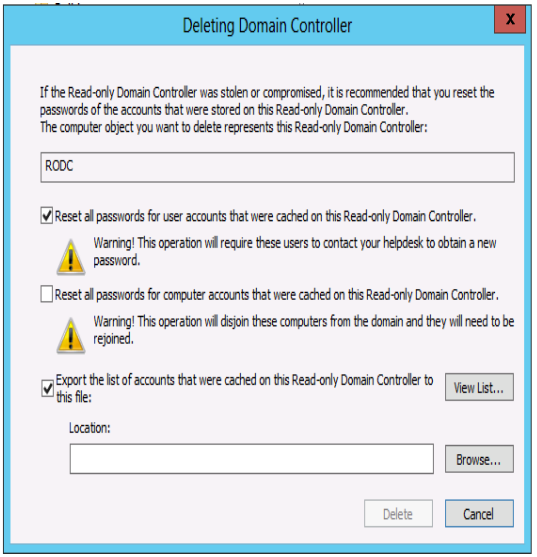
- Rodc-admin وهذا المستخدم تم تخزين بيانات اعتماده على الـ RODC في السابق
- Rodc2 وهذا المستخدم لم يتم تخزين بيانات اعتماده على الـ RODC وما زال يطلب التصريح من الـ Writable Domain





كما نرى الان طريقة الدخول على الـ RODC بالنسبة لكلا المستخدمين

الخطوة القادمة والمهمة هي معرفة كيفية مسح او استرجاع بيانات الاعتماد التي قمنا بتخزينها عند حدوث امور طارئة كعمليات القرصنة او محاولة سرقة كلمات المرور ففي هذه الحالة نقوم فورا بالتالي :-



كما نرى خيارات الاستعادة لكلمات المرور الخاصة بالمستخدم والخاصة بالاجهزة
كما يمكن تصدير كلمات المرور كملف يمكن الاستعانه به لاحقا

وبهذا نكون قد انتهينا من الـ RODC هل تعتقد أن الموضع كان صعبا ؟

Child Domain

الغرض من انشاء الـ Child هو إيجاد Domain صغير من ال Domain الرئيسي
أو ما يسمى بالـ Sub-Domain فقد تكون مؤسستي تزايد عدد ال Users بها وتنوعت النشاطات وزادت التخصصات , في هذه الحاله اقوم بإنشاء Domain فرعي من ال Domain الرئيسي يكون المتحكم فيه هو ال Enterprise Administrator

وما يميز الـ Child Domain

- له قاعدة بيانات Database منفصلة عن الدومين الرئيسي وخاصة به
- ليس كحال الـ Additional or RODC فيما يتعلق بالـ Replication فحينما اقوم بإنشاء اي Object لا يتم تبادل بياناته تلقائيا مع المواقع الاخرى داخل الـ Forest
- يكون التحكم فيه عن طريق الـ Enterprise Administrator الخاص بالدومين الرئيسي
- يرث اسم الدومين الرئيسي
- يمكن عمل Child Domain من Child Domain آخر ويسمى في هذه الحالة Grand Child
- مدير نظام الـ Child domain لا يستطيع ان يقوم بالتحكم في الـ Domain الرئيسي انما يحدث العكس

أمثله على الـ Child Domain

Parent Domian is : Yahoo.com

Child domain is : mail.yahoo.com

Parent Domian is : google.com

Child domain is : paly.google.com

Parent Domian is : icrosoft.com

Child domain is : windows. microsoft.com

الان سوف نقوم بعمل child من الدومين الخاص بنا وانا اخترت اسم Europe على اعتبار ان شركتنا توسعت وصولا الى أوروبا

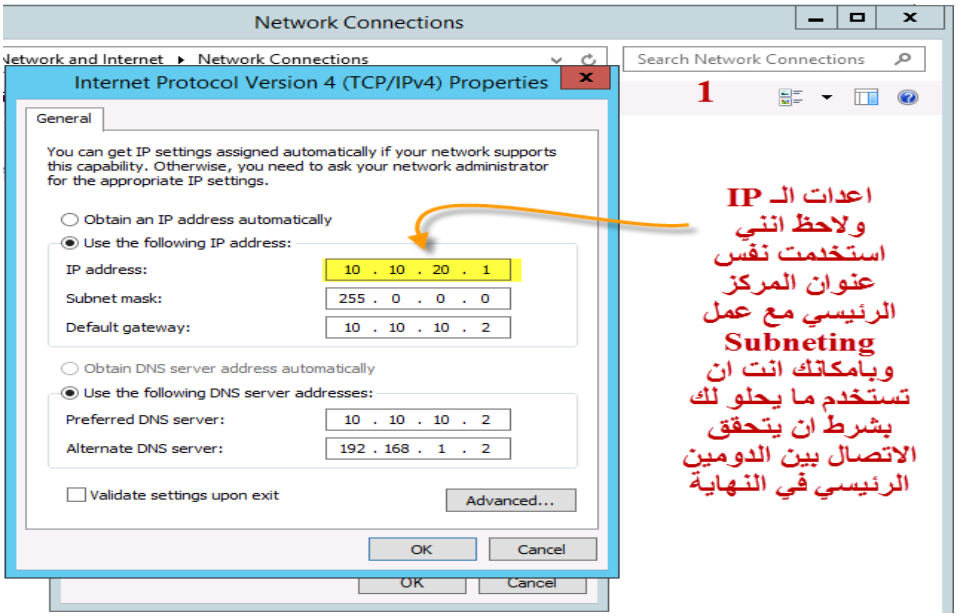
وعلى ذلك فسيكون الـ Child Domain Name هو **Eu.target.org**

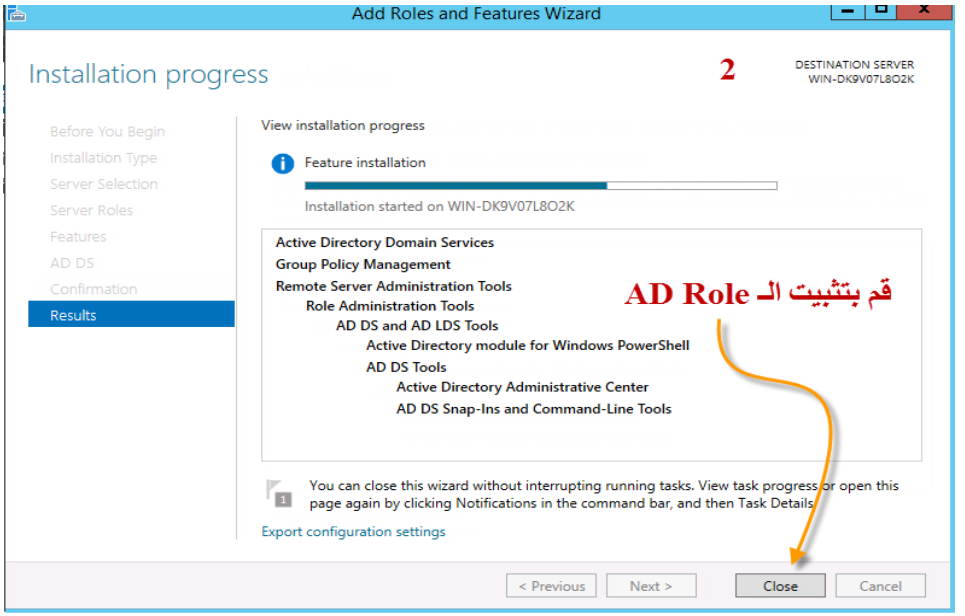
ولا ننسى قبل القيام بخطوات العمل أننا سنضع **router** بين المركز الرئيسي وبين المدينة التي سيكون فيها الـ **Server** الخاص بالـ Child ان كان في مدينة اخرى غير التي في المركز الرئيسي وسوف نقوم ايضا بعمل **Site** و **Subnet** كذلك كما تعلمنا

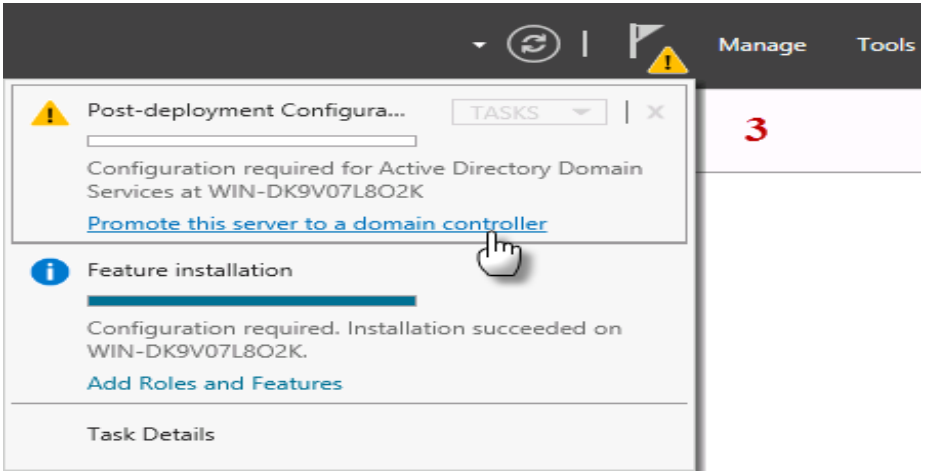
والان سنبدأ معا عمل الـ Child Domain

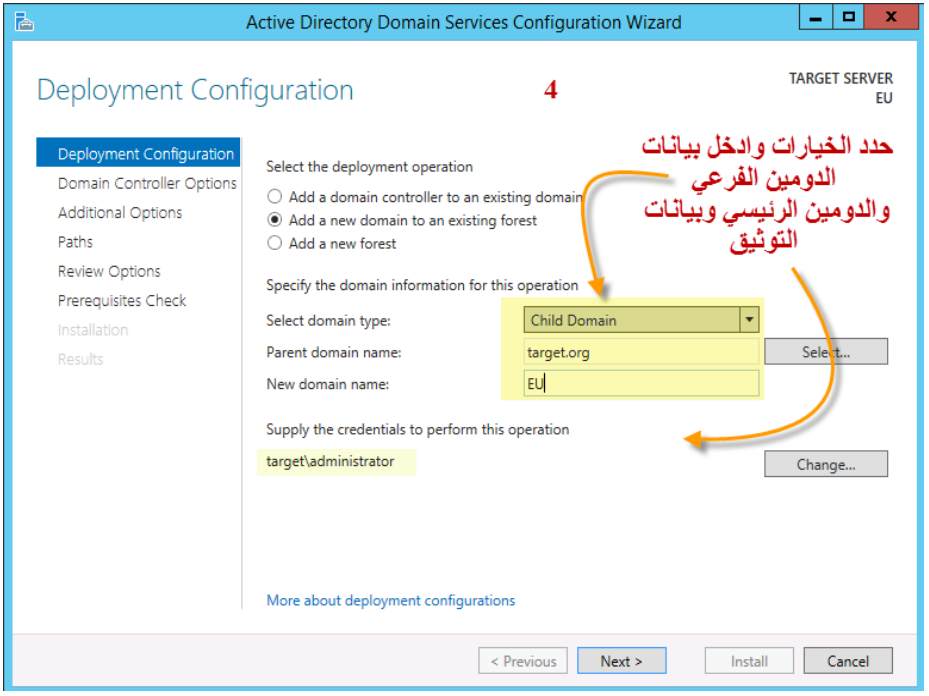
- **ملحوظة مهمه**

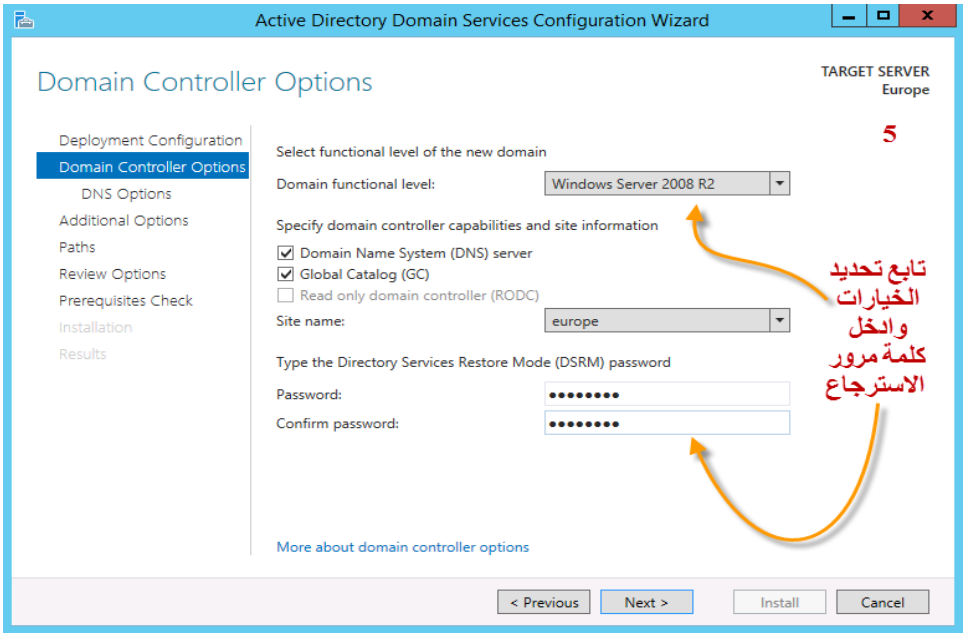
تم استخدام نفس نطاق الـ **IP** الخاص بالمركز الرئيسي وعلى ذلك فان الـ **Child** سيكون داخل نفس المدينة لكنني اردت تذكيرك في حال كونه يحمل **IP** مختلف أو يوجد في **Deferent Site**

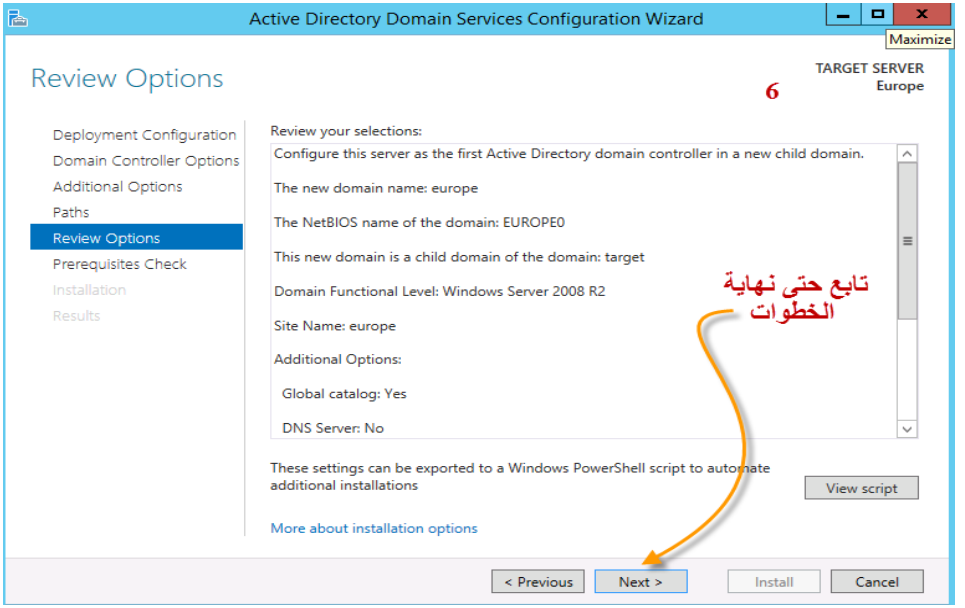

Network Connections
Network and Internet ▸ Network Connections
Search Network Connections
1
Internet Protocol Version 4 (TCP/IPv4) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 10 . 10 . 20 . 1
Subnet mask: 255 . 0 . 0 . 0
Default gateway: 10 . 10 . 10 . 2
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server: 10 . 10 . 10 . 2
Alternate DNS server: 192 . 168 . 1 . 2
Validate settings upon exit
Advanced...
OK
Cancel
اعدات الـ IP
ولاحظ انني
استخدمت نفس
عنوان المركز
الرئيسي مع عمل
Subneting
وبامكانك انت ان
تستخدم ما يحلو لك
بشرط ان يتحقق
الاتصال بين الدومين
الرئيسي في النهاية

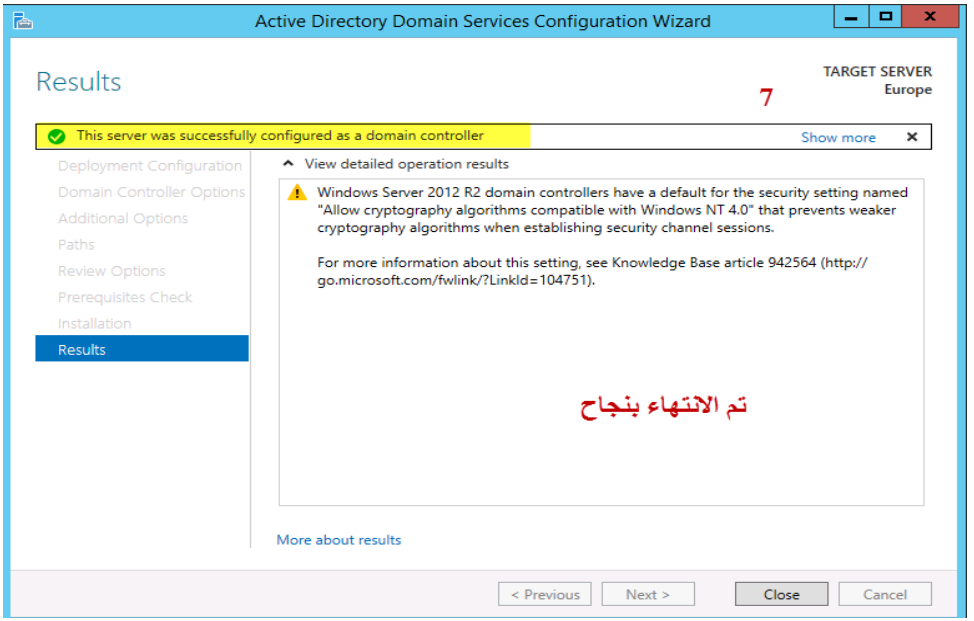

Add Roles and Features Wizard
Installation progress
2
DESTINATION SERVER
WIN-DK9V07L8O2K
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
Confirmation
Results
View installation progress
Feature installation
Installation started on WIN-DK9V07L8O2K
Active Directory Domain Services
Group Policy Management
Remote Server Administration Tools
Role Administration Tools
AD DS and AD LDS Tools
Active Directory module for Windows PowerShell
AD DS Tools
Active Directory Administrative Center
AD DS Snap-Ins and Command-Line Tools
قم بتثبيت الـ AD Role
You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.
Export configuration settings
< Previous
Next >
Close
Cancel

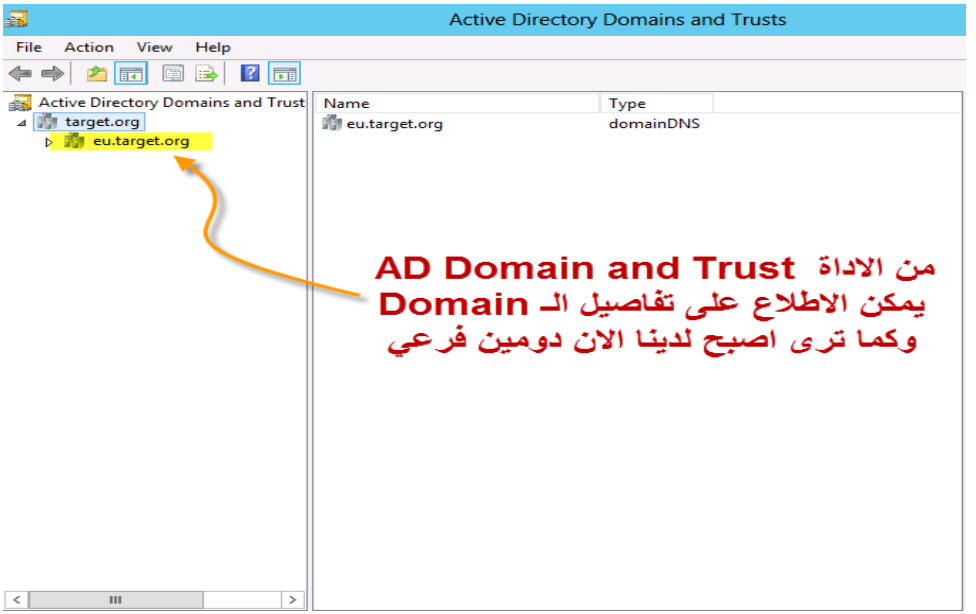

Manage
Tools
Post-deployment Configura...
TASKS
3
Configuration required for Active Directory Domain Services at WIN-DK9V07L8O2K
Promote this server to a domain controller
Feature installation
Configuration required. Installation succeeded on WIN-DK9V07L8O2K.
Add Roles and Features
Task Details


Active Directory Domain Services Configuration Wizard
Deployment Configuration
4
TARGET SERVER
EU
Deployment Configuration
Domain Controller Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Select the deployment operation
Add a domain controller to an existing domain
Add a new domain to an existing forest
Add a new forest
حدد الخيارات وادخل بيانات الدومين الفرعي والدومين الرئيسي وبيانات التوثيق
Specify the domain information for this operation
Select domain type:
Child Domain
Parent domain name:
target.org
Select...
New domain name:
EU
Supply the credentials to perform this operation
target\administrator
Change...
More about deployment configurations
< Previous
Next >
Install
Cancel


Active Directory Domain Services Configuration Wizard
Domain Controller Options
TARGET SERVER
Europe
5
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Select functional level of the new domain
Domain functional level:
Windows Server 2008 R2
Specify domain controller capabilities and site information
Domain Name System (DNS) server
Global Catalog (GC)
Read only domain controller (RODC)
Site name:
europe
Type the Directory Services Restore Mode (DSRM) password
Password:
Confirm password:
More about domain controller options
< Previous
Next >
Install
Cancel
تابع تحديد الخيارات وادخل كلمة مرور الاسترجاع


Active Directory Domain Services Configuration Wizard
Maximize
Review Options
TARGET SERVER
Europe
6
Deployment Configuration
Domain Controller Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Review your selections:
Configure this server as the first Active Directory domain controller in a new child domain.
The new domain name: europe
The NetBIOS name of the domain: EUROPE0
This new domain is a child domain of the domain: target
Domain Functional Level: Windows Server 2008 R2
Site Name: europe
Additional Options:
Global catalog: Yes
DNS Server: No
These settings can be exported to a Windows PowerShell script to automate additional installations
View script
More about installation options
< Previous
Next >
Install
Cancel
تابع حتى نهاية الخطوات


Active Directory Domain Services Configuration Wizard
Results
TARGET SERVER
Europe
7
This server was successfully configured as a domain controller
Show more
Deployment Configuration
Domain Controller Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
View detailed operation results
Windows Server 2012 R2 domain controllers have a default for the security setting named "Allow cryptography algorithms compatible with Windows NT 4.0" that prevents weaker cryptography algorithms when establishing security channel sessions.
For more information about this setting, see Knowledge Base article 942564 (http://go.microsoft.com/fwlink/?LinkId=104751).
تم الانتهاء بنجاح
More about results
< Previous
Next >
Close
Cancel

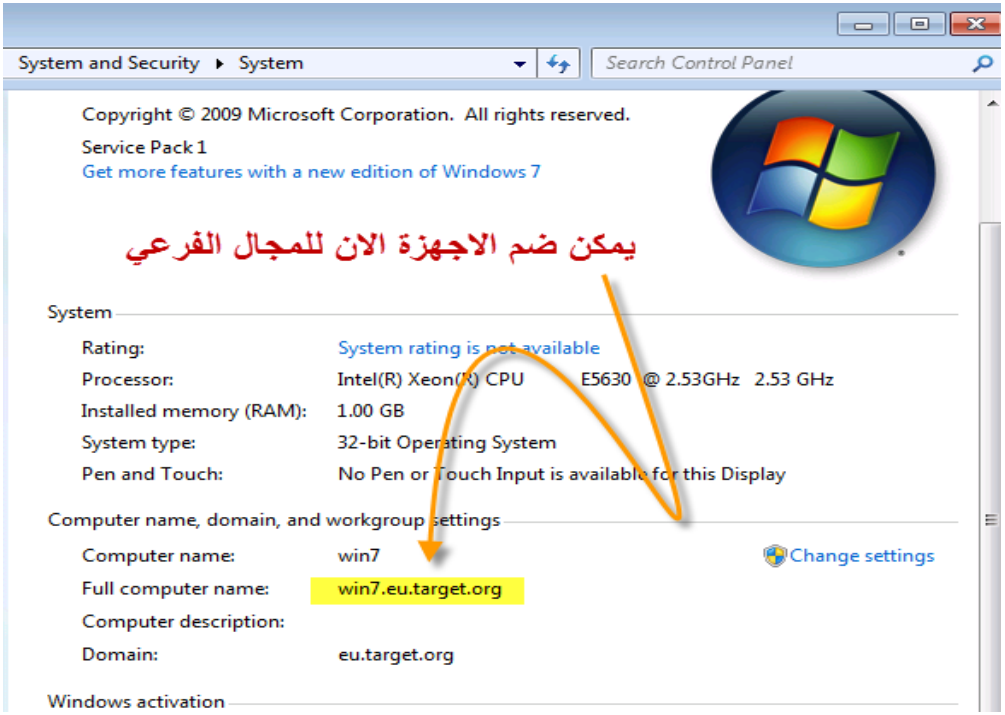

Active Directory Domains and Trusts
File
Action
View
Help
Active Directory Domains and Trust
target.org
eu.target.org
Name
Type
eu.target.org
domainDNS
AD Domain and Trust من الاداة
يمكن الاطلاع على تفاصيل الـ Domain
وكما ترى اصبح لدينا الان دومين فرعي

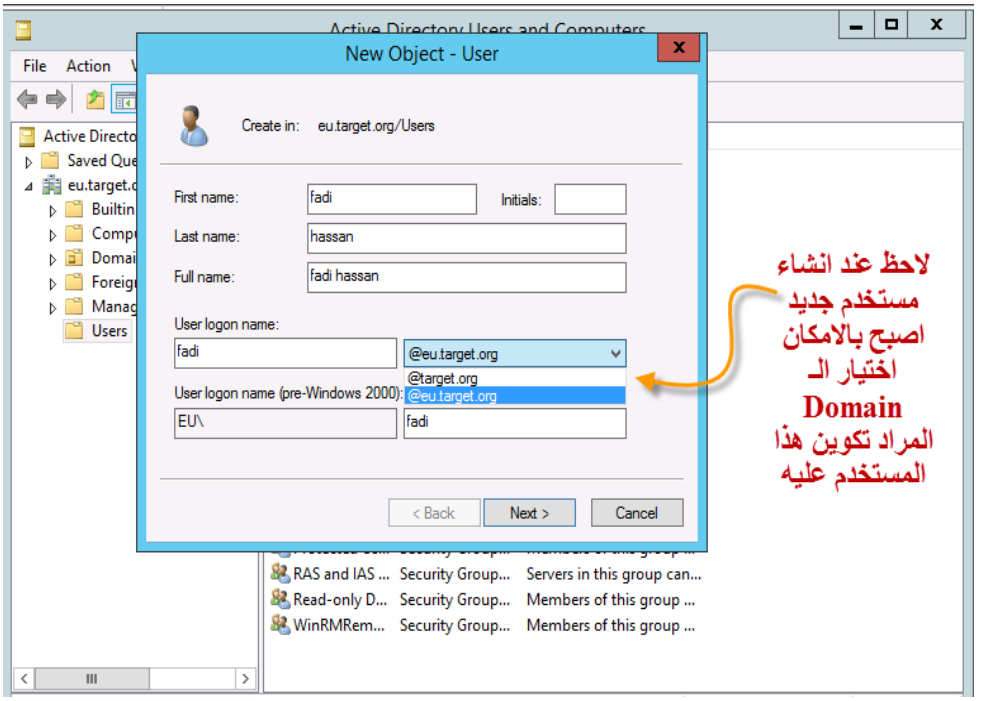
حسنا أصبحنا الان نملك Domain فرعي من الـ Domain الرئيسي الخاص بنا وكما ذكرنا هو domain خاص بذاته له خصوصياته وقاعدة بياناته وبيئته المنفصلة عن الـ parent domain لكن يستطيع الـ Domain الرئيسي التحكم الكامل به

والسؤال هنا

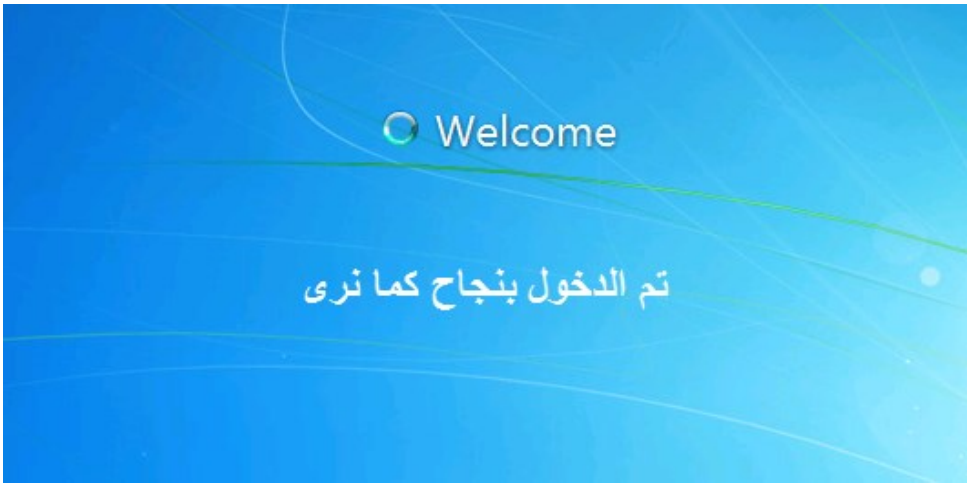
هل لو قمنا بإنشاء مستخدم على دومين الـ Eu يمكن لهذا المستخدم الدخول على دومين ال Target والعكس ؟

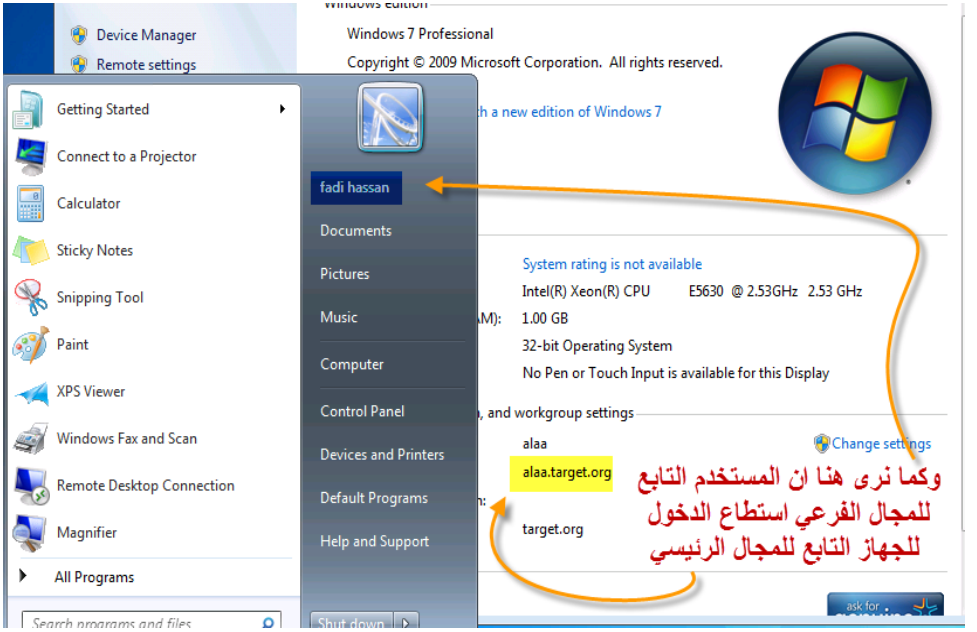
هيا لنتعرف على الاجابة عمليا في الخطوات التالية :-




Active Directory Users and Computers
File Action
New Object - User
Create in: eu.target.org/Users
First name: fadi
Initials:
Last name: hassan
Full name: fadi hassan
User logon name:
fadi
@eu.target.org
@target.org
@eu.target.org
User logon name (pre-Windows 2000):
EU\
fadi
< Back
Next >
Cancel
RAS and IAS ... Security Group... Servers in this group can...
Read-only D... Security Group... Members of this group ...
WinRMRem... Security Group... Members of this group ...
لاحظ عند انشاء مستخدم جديد اصبح بالامكان اختيار الـ Domain المراد تكوين هذا المستخدم عليه


على الجهاز التابع للمجال الفرعي سنحاول الدخول بمستخدم تابع للمجال الرئيسي
alaa@target.org
Log on to: target.org
How do I log on to another domain?





هل عرفنا الاجابة ؟ حسنا السؤال التالي هو لماذا ؟ وما الذي يجعل هذا يحدث ؟

تابع لتعرف الجواب .....

ACTIVE DIRECTORY TRUST RELATIONSHIP

حسنا كنا نتساءل ما الذي يجعل المستخدمين في كلا من الـ Parent OR Child يستطيعون الدخول بحساباتهم دون شرط او قيد ؟

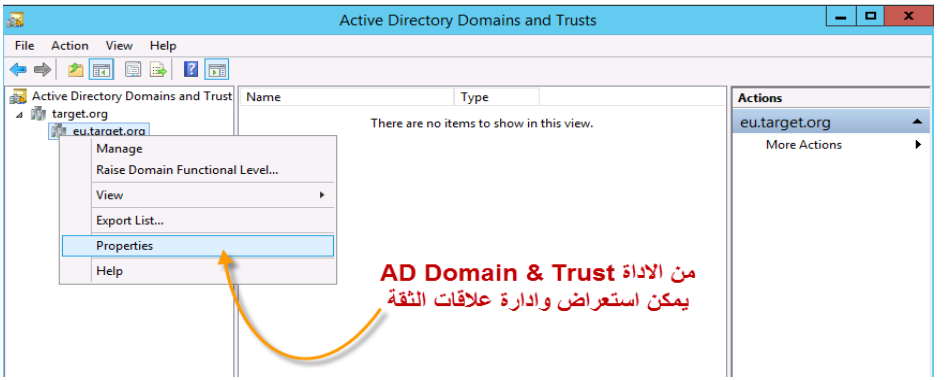
الجواب هو اننا حينما انشانا مجالا فرعيا من المجال الرئيسي فقد نشأت بينهما مباشرة علاقة ثقة TRUST RELATIONSHIP

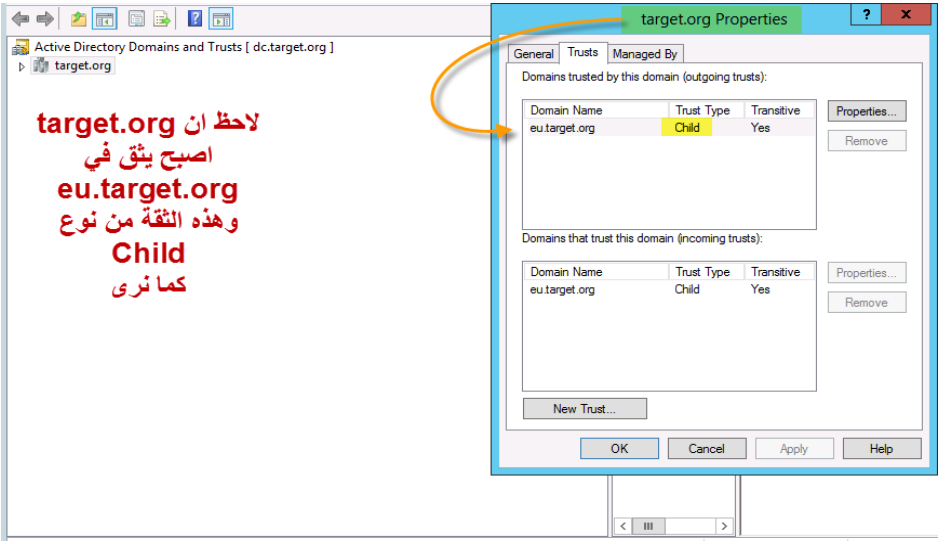
وعلاقات الثقة بين الـ DOMAIN وبين الـ CHILD تنشأ تلقائيا تماما كما يحدث هذا بين علاقة الاب وابنه في حياتنا وتسمى هذه العلاقة IMPLICIT

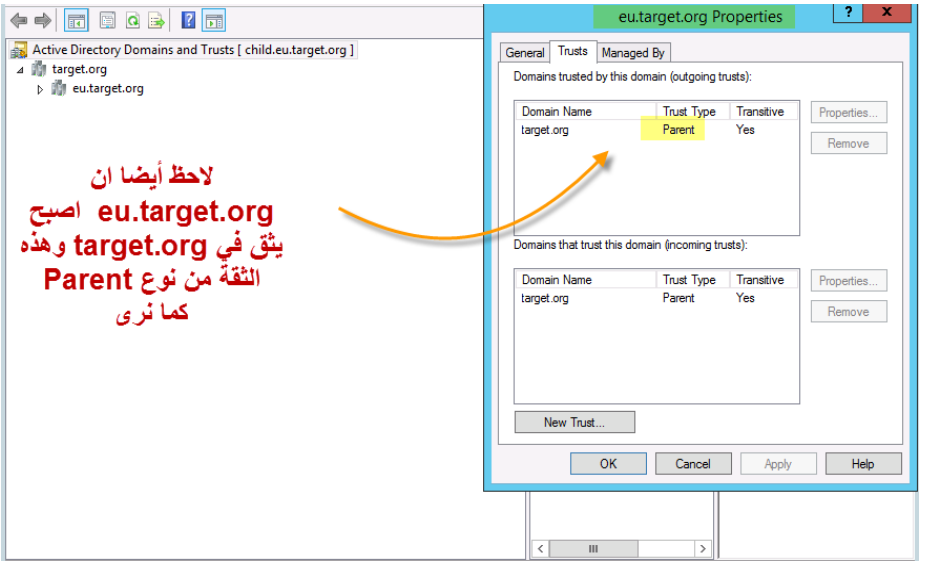
وهذا النوع ينشئ آليا بين المجالات الموجودة فى نفس الـ Forest

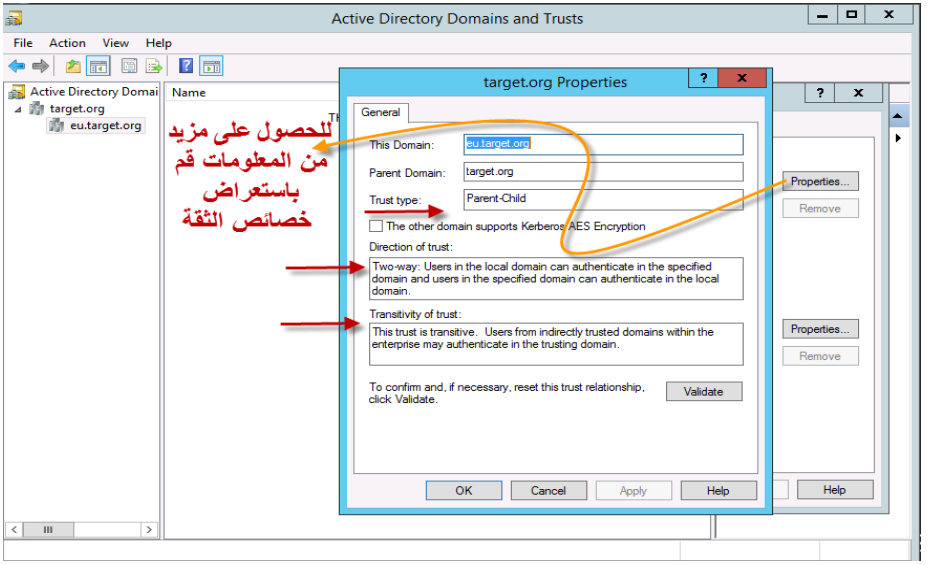
أما ما ينشأ بواسطة مسؤول الشبكة او مدير النظام فيسمى EXPLICIT

ويمكن بواسطة الأداة (AD DOMAIN AND TRUSTS) معاينة هذه العلاقة والتعرف عليها كما يلي :-









وبواسطة (AD DOMAIN AND TRUSTS) نستطيع أيضا التحكم بالعلاقات القائمة وإنشاء علاقة ثقة جديدة بين المجالات بعضها البعض .

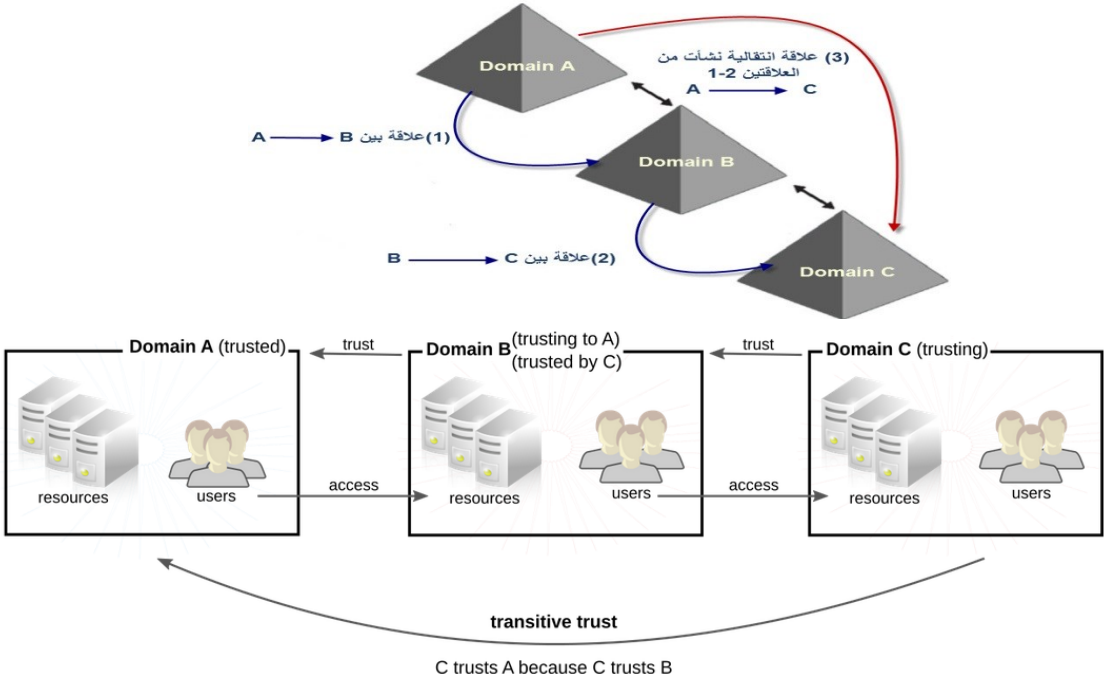
ويمكن تقســـيم **أنواع** علاقات الثقة لنوعين - :

1 - TRANSITIVE TRUSTS (علاقات منتقلة) وهذا النوع من الثقة يمرر علاقة الثقة من خلال كل مجال موثوق إلى آخر

مثال : إذا كان لدينا تسلسل هرمي بين الدومين A والدومين B والدومين C .....

و كان هناك علاقة ثقة بين الدومين A والدومين B .... و هناك علاقة ثقة بين الدومين B والدومين C

فستؤدى هذه العلاقة (B/C) إلى تخليق علاقة ثقة بين كلا من (A/C) وهكذا (انظر الشكل)



2- NON TRANSITIVE TRUSTS (علاقات غير منتقلة)

وهنا العلاقة تقف عند حد معين ألا وهو الثقة بين المجالات المنشأ بينها ثقة فقط .

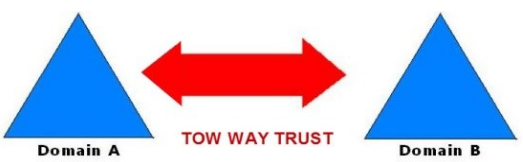
ويمكن تقســـيم طرق انشاء علاقات الثقة لنوعين أيضا - :

TRUST TWO WAY -1

معنى ذلك ان يستطيع المستخدمين في الدومين A الوصول لمصادر الدومين B والعكس كما رأينا في المثال صفحة 100 -101

TRUST ONE WAY -2

معنى ذلك ان يحدد اتجاه واحد فقط للثقة فمثلا يستطيع المستخدمين في الدومين A الوصول لمصادر الدومين B اذا كانت علاقة الثقة في اتجاه B بينما لن يستطيع مستخدم الدومين B الوصول لمصادر الدومين A اذا لم يكن هناك اتجاه ثقة لهذا الدومين



أما الثقة نفسها فيمكن تقسيمها الى ستة أنواع اقسام كالتالي :-

A PARENT AND CHILD TRUST -1

وهذا النوع هو ما تم شرحه باستخدام المثال الوارد في صفحة 100 -101

TREE ROOT TRUST -2

عندما يتم إنشاء New Tree داخل نفس الـ Forest يتكون شجرة من المجالات ويتم خلق ثقة تلقائيا بينهم وهذا النوع يكون TRANSITIVE ويكون أيضا TWO WAY افتراضيا .

SHORTCUT TRUST -3

كما ذكرنا في الـ TRANSITIVE TRUSTS فان المستخدم من الدومين A اذا اراد الوصول الى مصادر الدومين C فسيتوجب عليه المروربالدومين B في المثال أو بكل المجالات التى تربط بينهما علاقة ثقة كما فى أمثله أخرى لكن علاقة الثقة من النوع SHORTCUT توفر المسافة والوقت الازم لذلك من خلال تحديد اقصر الطرق للوصول . هذا النوع يكون TRANSITIVE ويكون أيضا TWO WAY افتراضيا ولكن الحرية في جعله ONE WAY كما نشاء .

REALM TRUST -4

هذا النوع هو المختص بعمل TRUST بين السيرفر الذى يستخدم البرتوكول KERBEROS V5 فى عملية التوثيق مع اى نظام آخر لا يستخدم هذا النوع من البروتوكول مثل نظام اللـ Unix .

EXTERNAL TRUST -5

هذا النوع مخصص لعمل TRUST بين مجالات خارج نطاق الـ Forest هذا النوع من ال TRUST قد يكون ONE WAY أو TWO WAY ودائما هذا النوع ... TRANSITIVE وبعد إنشاء هذه العلاقة يستطيع المجال الموجود خارج الـ Forest أن يصل إلى كل المصادر الموجودة داخل الـ Forest طبعا بعد توافر التراخيص الازمة لذلك كما نعلم .

FOREST TRUST -6

في حالة اندماج شركتين معا كما حدث مع شركة HP و Compaq فانه بالطبع كلا الشركتين لهما Tow Domain and Two Forests وبالتالي كانت الحاجة لهذا النوع من ال TRUST لانه ينشئ فقط بين ROOT DOMAIN IN TWO FORESTS

ويجب أن يكون كلا الـ FOREST المراد عمل بينهم علاقة الثقة من النوع ويندوز سيرفر

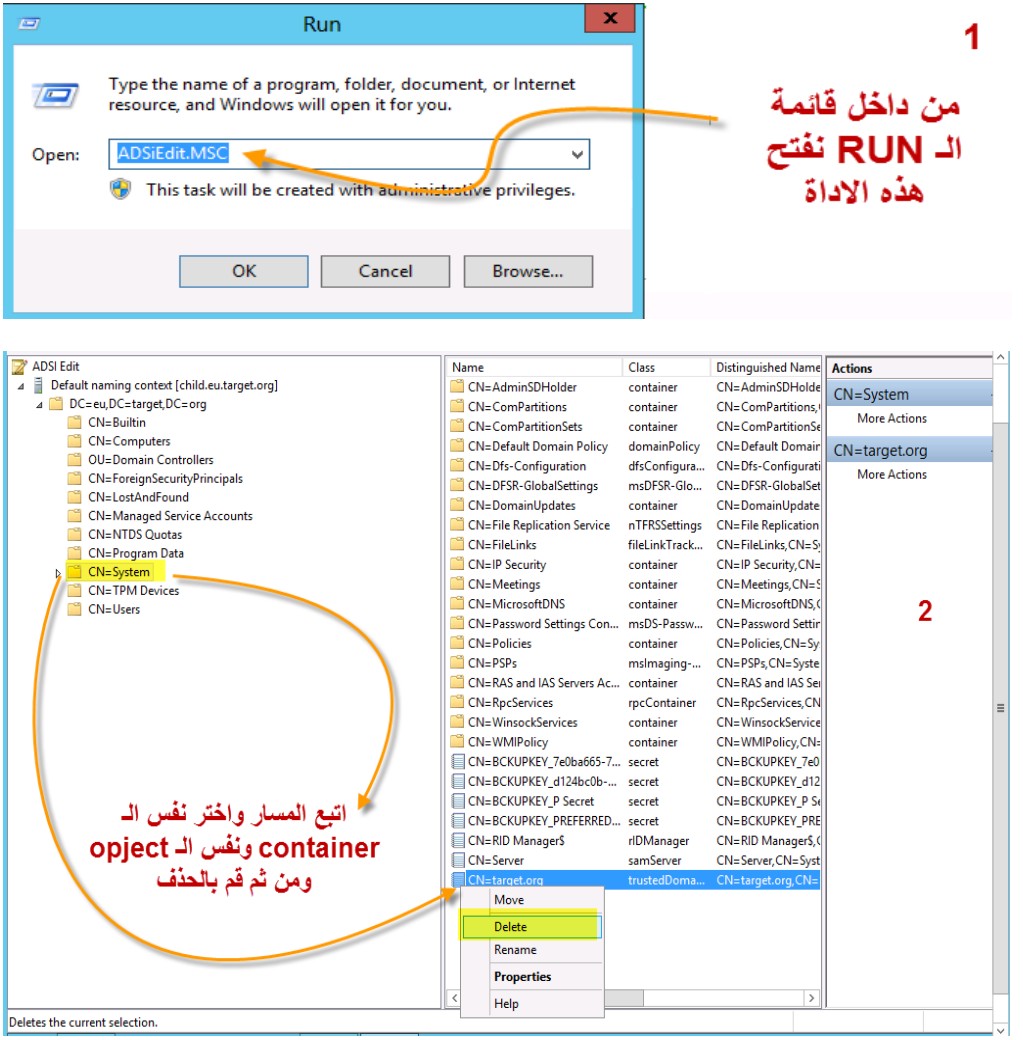
و هذا النوع من الثقه قد يكون من حيث الإتجاه ONE WAY أو TWO WAY و هذا النوع يعتبر TRANSITIVE TRUST

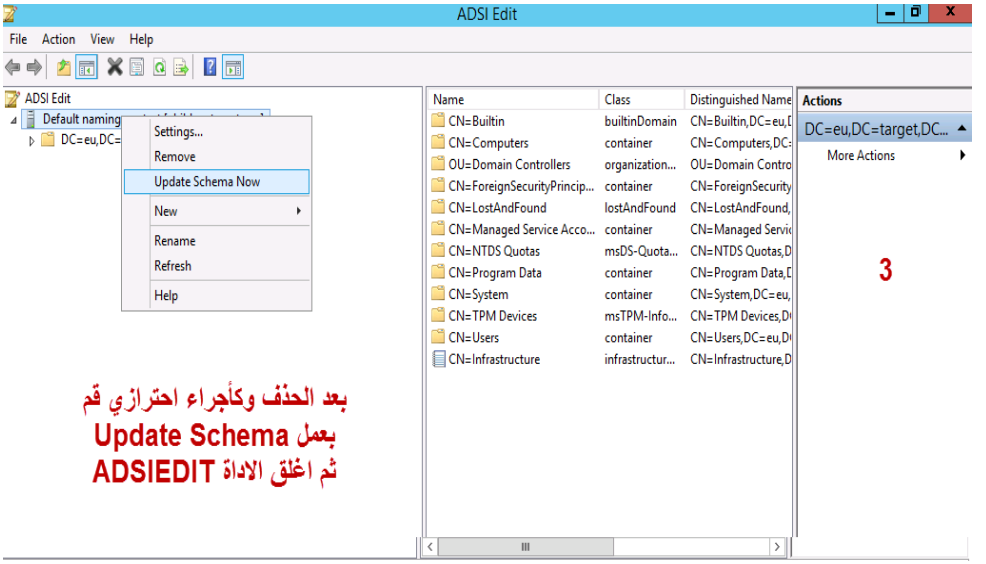
والان بعدما تعرفنا على ما هي الثقة وانواعها وطرقها يجب ان نتعلم الان كيفية انشاء الثقة وادارتها وفق ما تم ذكره .

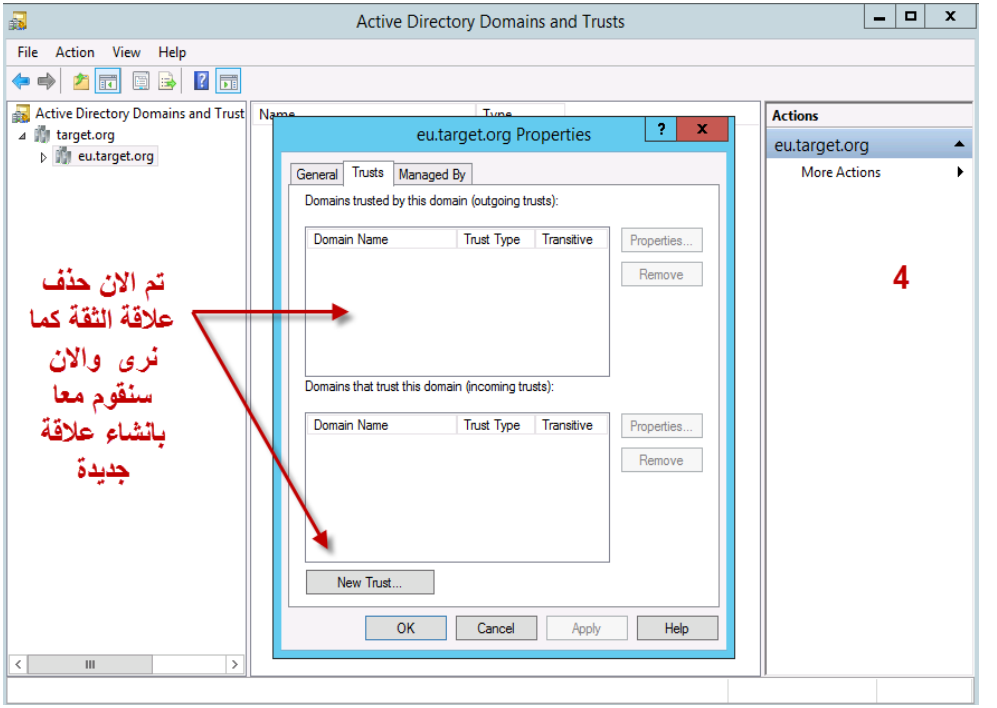
انتبه

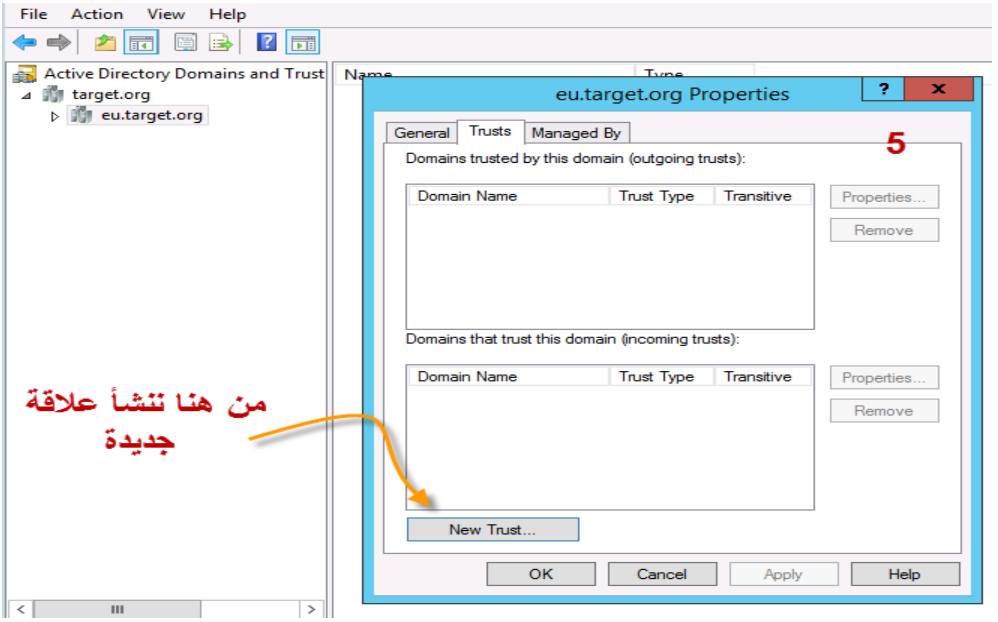
قلنا سابقا ان PARENT AND CHILD TRUST علاقة تنشأ تلقائيا أي هي من النوع Built in لذلك فانك لن تستطيع حذفها بالطريقة العادية وعلى ذلك فإننا سنقوم بحذفها يدويا واعادة انشاؤها من جديد فتابع معي

كيف نقوم بحذف Built in Trust

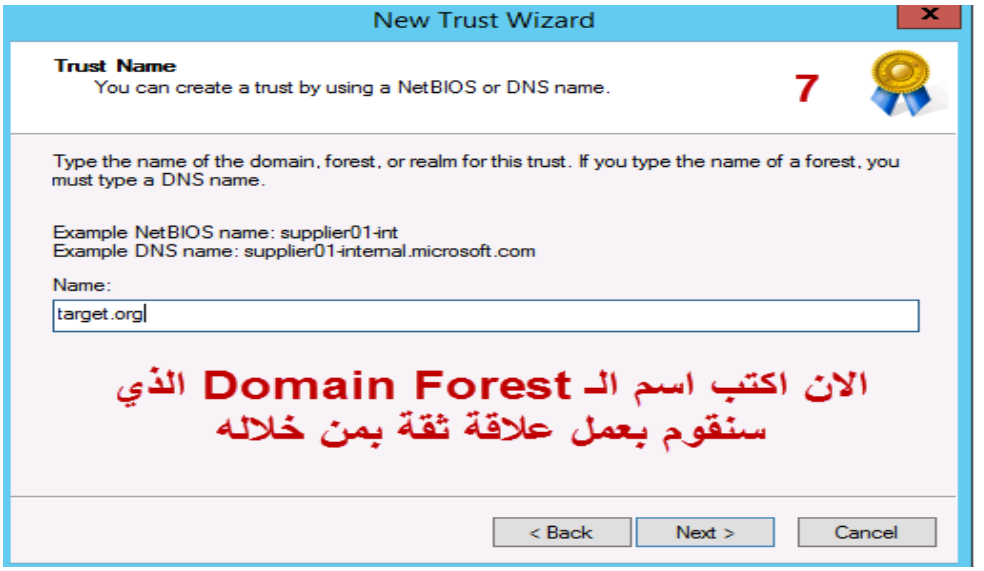


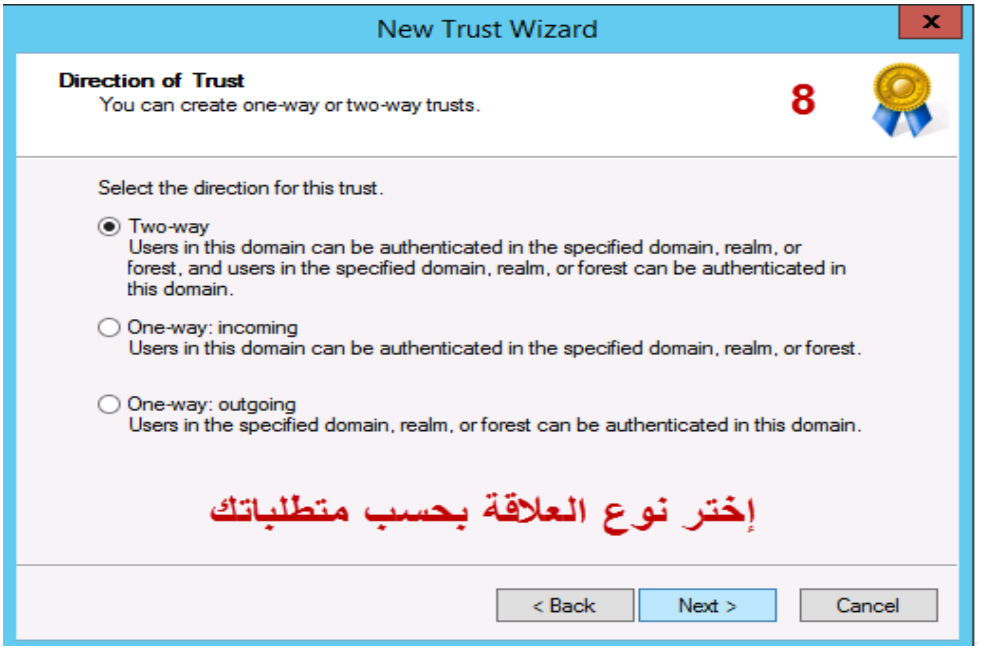

ADSI Edit
File Action View Help
ADSI Edit
Default naming
DC=eu,DC=
Settings...
Remove
Update Schema Now
New
Rename
Refresh
Help
Name
Class
Distinguished Name
CN=Builtin
builtinDomain
CN=Builtin,DC=eu,D
CN=Computers
container
CN=Computers,DC=
OU=Domain Controllers
organization...
OU=Domain Contro
CN=ForeignSecurityPrincip...
container
CN=ForeignSecurity
CN=LostAndFound
lostAndFound
CN=LostAndFound,
CN=Managed Service Acco...
container
CN=Managed Servic
CN=NTDS Quotas
msDS-Quota...
CN=NTDS Quotas,D
CN=Program Data
container
CN=Program Data,D
CN=System
container
CN=System,DC=eu,
CN=TPM Devices
msTPM-Info...
CN=TPM Devices,D
CN=Users
container
CN=Users,DC=eu,D
CN=Infrastructure
infrastructur...
CN=Infrastructure,D
Actions
DC=eu,DC=target,DC...
More Actions
3
بعد الحذف وكأجراء احترازي قم
بعمل Update Schema
ثم اغلق الاداة ADSIEDIT

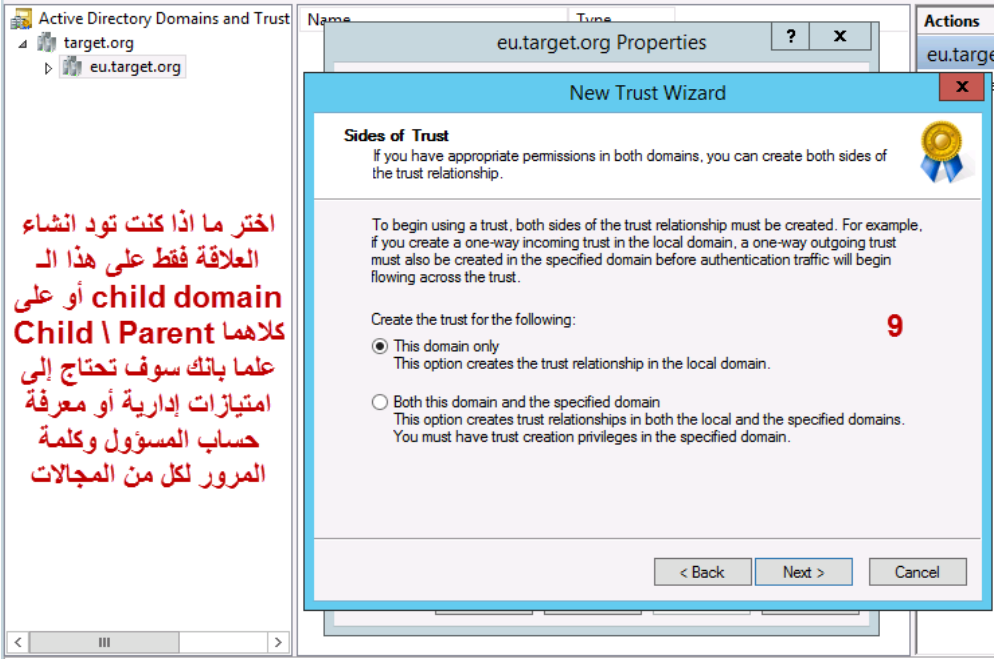

Active Directory Domains and Trusts
File Action View Help
Active Directory Domains and Trust
target.org
eu.target.org
Name
Type
eu.target.org Properties
General
Trusts
Managed By
Domains trusted by this domain (outgoing trusts):
Domain Name
Trust Type
Transitive
Properties...
Remove
Domains that trust this domain (incoming trusts):
Domain Name
Trust Type
Transitive
Properties...
Remove
New Trust...
OK
Cancel
Apply
Help
Actions
eu.target.org
More Actions
4
تم الان حذف
علاقة الثقة كما
نرى والان
سنقوم معا
بانشاء علاقة
جديدة

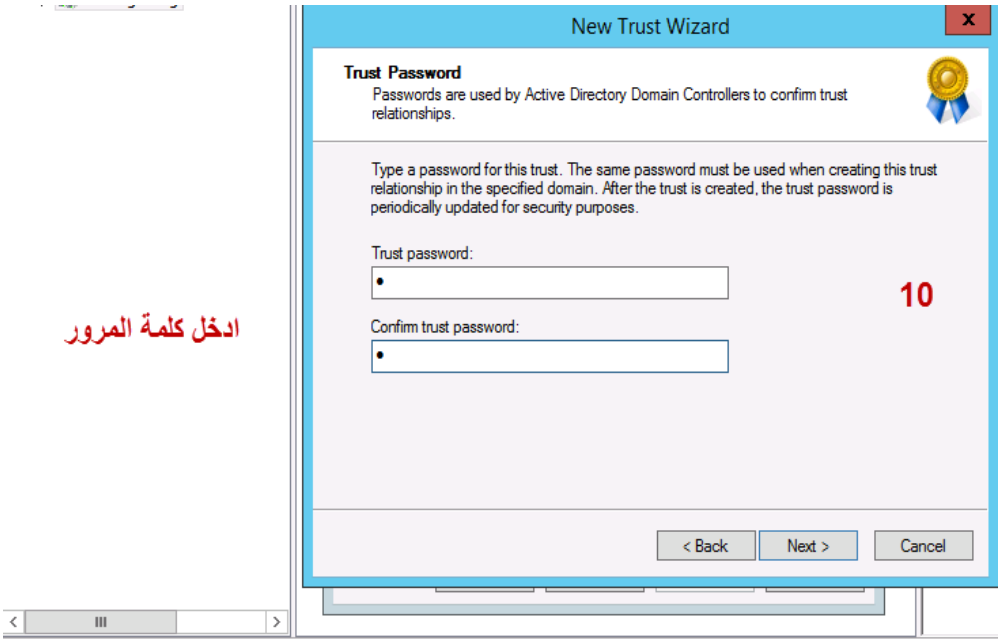

File Action View Help
Active Directory Domains and Trust
target.org
eu.target.org
eu.target.org Properties
General Trusts Managed By
5
Domains trusted by this domain (outgoing trusts):
Domain Name Trust Type Transitive
Properties...
Remove
Domains that trust this domain (incoming trusts):
Domain Name Trust Type Transitive
Properties...
Remove
New Trust...
OK Cancel Apply Help
من هنا ننشأ علاقة جديدة

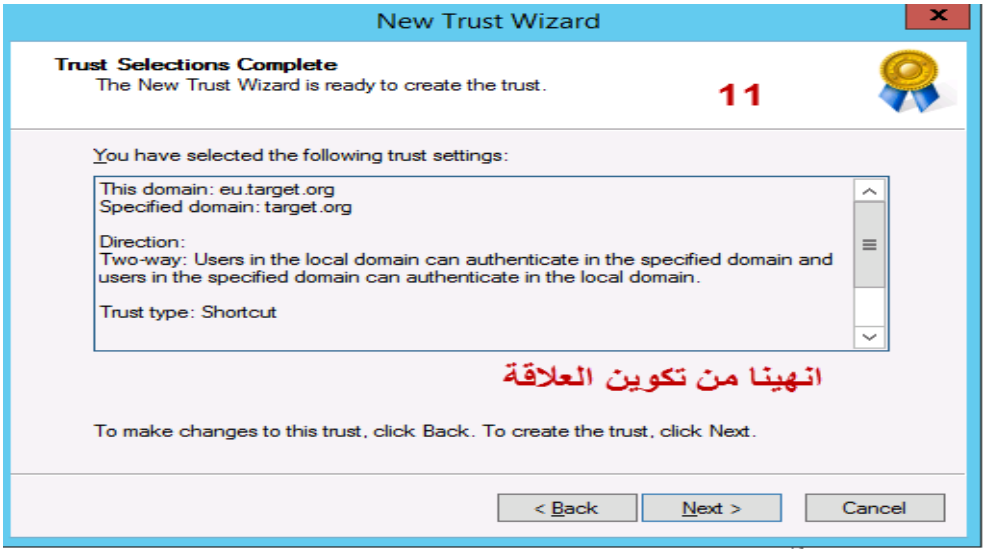

New Trust Wizard
Welcome to the New Trust Wizard
6
This wizard helps you create a trust between this domain and any of the following:
A Windows domain in this forest or in another forest.
A Windows NT 4.0 domain.
A Kerberos V5 realm trust.
ابدأ خطواتك
A trust is a relationship that enables users in one domain, forest, or realm to be authenticated in a specified domain, forest, or realm.
To continue, click Next.
< Back Next > Cancel

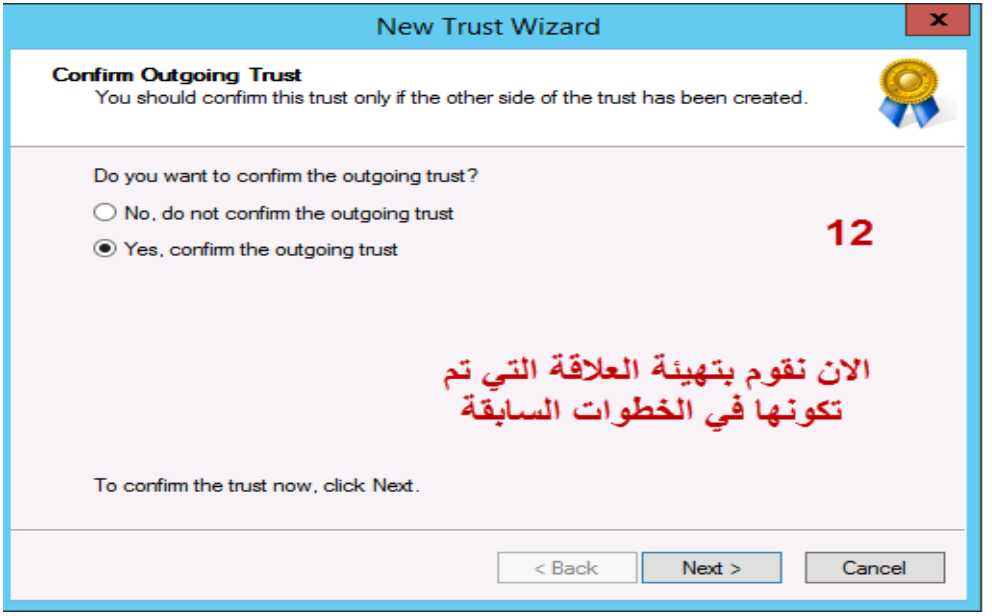

New Trust Wizard
Trust Name
You can create a trust by using a NetBIOS or DNS name.
7
Type the name of the domain, forest, or realm for this trust. If you type the name of a forest, you must type a DNS name.
Example NetBIOS name: supplier01-int
Example DNS name: supplier01-internal.microsoft.com
Name:
target.org
الان اكتب اسم الـ Domain Forest الذي
سنقوم بعمل علاقة ثقة بمن خلاله
< Back
Next >
Cancel

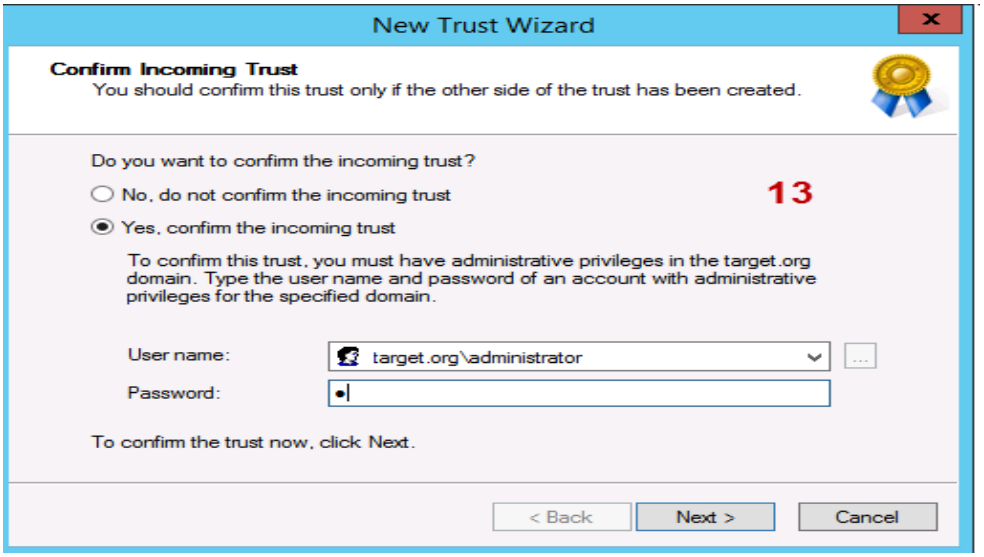

New Trust Wizard
Direction of Trust
You can create one-way or two-way trusts.
8
Select the direction for this trust.
Two-way
Users in this domain can be authenticated in the specified domain, realm, or forest, and users in the specified domain, realm, or forest can be authenticated in this domain.
One-way: incoming
Users in this domain can be authenticated in the specified domain, realm, or forest.
One-way: outgoing
Users in the specified domain, realm, or forest can be authenticated in this domain.
إختر نوع العلاقة بحسب متطلباتك
< Back
Next >
Cancel

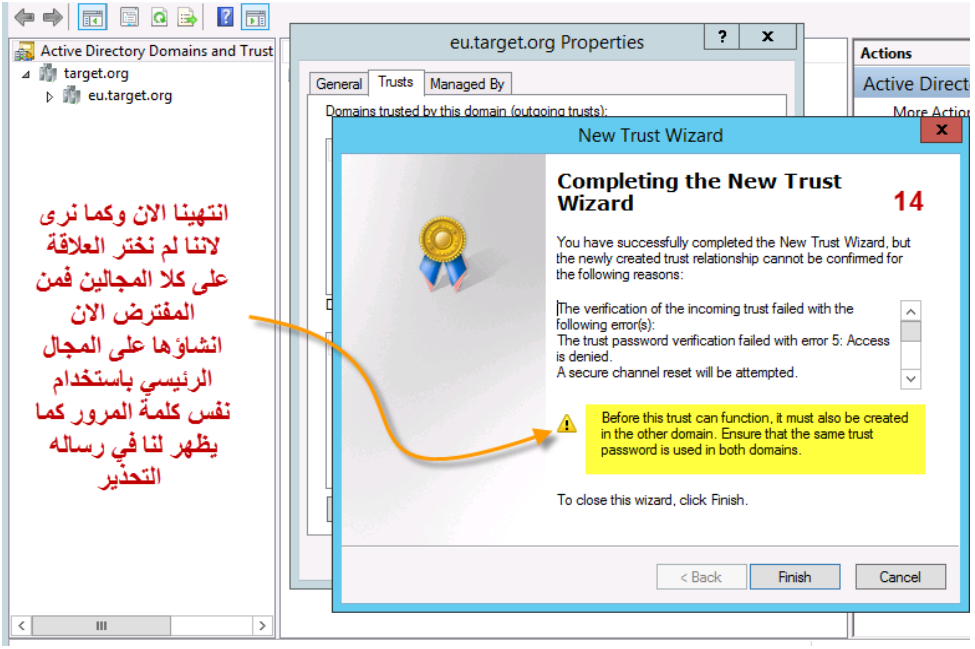

Active Directory Domains and Trust
target.org
eu.target.org
Name
Type
Actions
eu.targe
eu.target.org Properties
New Trust Wizard
Sides of Trust
If you have appropriate permissions in both domains, you can create both sides of the trust relationship.
To begin using a trust, both sides of the trust relationship must be created. For example, if you create a one-way incoming trust in the local domain, a one-way outgoing trust must also be created in the specified domain before authentication traffic will begin flowing across the trust.
Create the trust for the following:
9
This domain only
This option creates the trust relationship in the local domain.
Both this domain and the specified domain
This option creates trust relationships in both the local and the specified domains.
You must have trust creation privileges in the specified domain.
< Back
Next >
Cancel
اختر ما اذا كنت تود انشاء العلاقة فقط على هذا الـ child domain أو على كلاهما Child \ Parent علما بانك سوف تحتاج إلى امتيازات إدارية أو معرفة حساب المسؤول وكلمة المرور لكل من المجالات

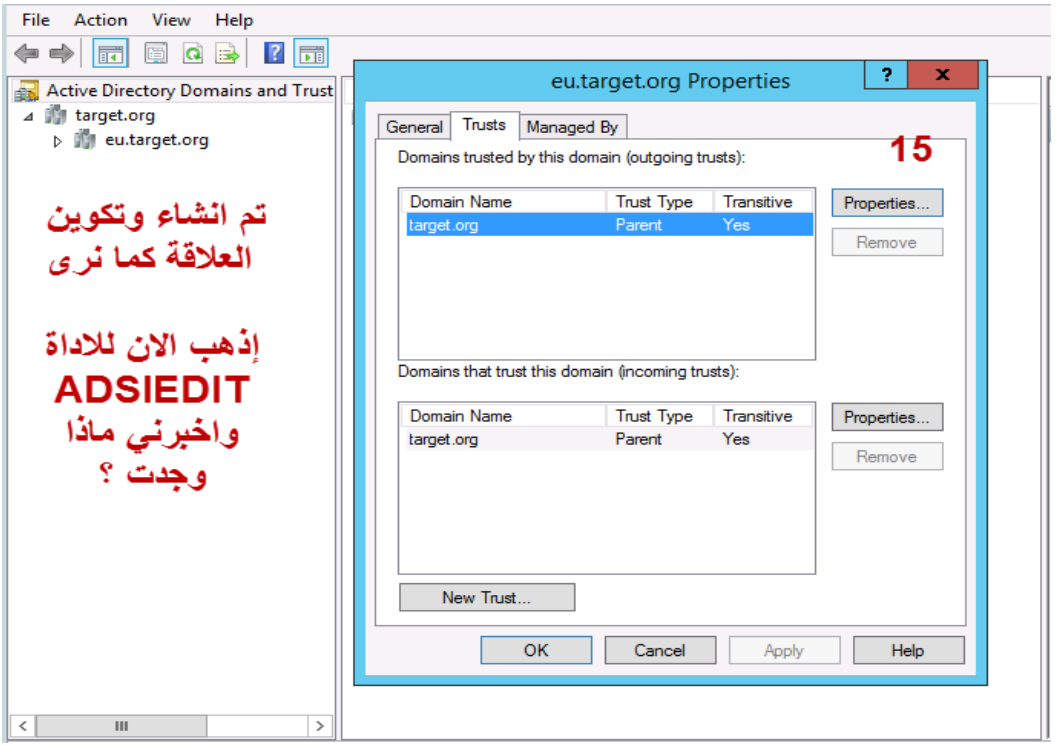

New Trust Wizard
Trust Password
Passwords are used by Active Directory Domain Controllers to confirm trust relationships.
Type a password for this trust. The same password must be used when creating this trust relationship in the specified domain. After the trust is created, the trust password is periodically updated for security purposes.
Trust password:
Confirm trust password:
10
< Back
Next >
Cancel
ادخل كلمة المرور


New Trust Wizard
Trust Selections Complete
The New Trust Wizard is ready to create the trust.
11
You have selected the following trust settings:
This domain: eu.target.org
Specified domain: target.org
Direction:
Two-way: Users in the local domain can authenticate in the specified domain and users in the specified domain can authenticate in the local domain.
Trust type: Shortcut
انهينا من تكوين العلاقة
To make changes to this trust, click Back. To create the trust, click Next.
< Back
Next >
Cancel


New Trust Wizard
Confirm Outgoing Trust
You should confirm this trust only if the other side of the trust has been created.
Do you want to confirm the outgoing trust?
No, do not confirm the outgoing trust
Yes, confirm the outgoing trust
12
الان نقوم بتهيئة العلاقة التي تم
تكونها في الخطوات السابقة
To confirm the trust now, click Next.
< Back
Next >
Cancel


New Trust Wizard
Confirm Incoming Trust
You should confirm this trust only if the other side of the trust has been created.
Do you want to confirm the incoming trust?
No, do not confirm the incoming trust
13
Yes, confirm the incoming trust
To confirm this trust, you must have administrative privileges in the target.org domain. Type the user name and password of an account with administrative privileges for the specified domain.
User name:
target.org\administrator
Password:
To confirm the trust now, click Next.
< Back
Next >
Cancel


Active Directory Domains and Trust
target.org
eu.target.org
eu.target.org Properties
General
Trusts
Managed By
Domains trusted by this domain (outgoing trusts):
Actions
Active Direct
New Trust Wizard
Completing the New Trust Wizard
14
You have successfully completed the New Trust Wizard, but the newly created trust relationship cannot be confirmed for the following reasons:
The verification of the incoming trust failed with the following error(s):
The trust password verification failed with error 5: Access is denied.
A secure channel reset will be attempted.
Before this trust can function, it must also be created in the other domain. Ensure that the same trust password is used in both domains.
To close this wizard, click Finish.
< Back
Finish
Cancel
انتهينا الان وكما نرى لاننا لم نختر العلاقة على كلا المجالين فمن المفترض الان انشاؤها على المجال الرئيسي باستخدام نفس كلمة المرور كما يظهر لنا في رساله التحذير



حسنا بما اننا قد تعلمنا معا حذف وانشاء العلاقة من نوع **Parent / Child** وقمنا بعمل الخطوات من داخل الـ **Child Domain** أطلب منك الان ان تتوجه للـ **Parent Domain** وانشاء نفس العلاقة عليه ...

هيا **نراجع** معا مخطط شبكتنا

لاحظ أن مخطط الـ Forest يحتوى على مجال رئيسي واحد Parent Domain وعدة مجالات فرعية Additional كما يوجد Child Domain و RODC Domain ولان الـ Tree تحتوى على Domain واحد أو أكثر وقد طبقنا ذلك عمليا

فان كل هذا يعتبر Tree

وقد ذكرنا سابقا أن الـ Forest تحتوى على Tree واحد أو أكثر .

لكننا لم نقوم بعمل أكثر من Tree داخل نفس الـ Frost فهيا الان نقوم بتطبيق ذلك عمليا .

Tree Root Domain

ماذا لو إنقسمت شركتنا الى شركتين أو أكثر ؟ و لكل منها شبكتها ومجالها الخاص لكنهما حتما سيقعان تحت مظلة واحدة هي target.org ؟
هل تذكر كلامي لك في الصفحة رقم 4 من هذا الكتاب ؟

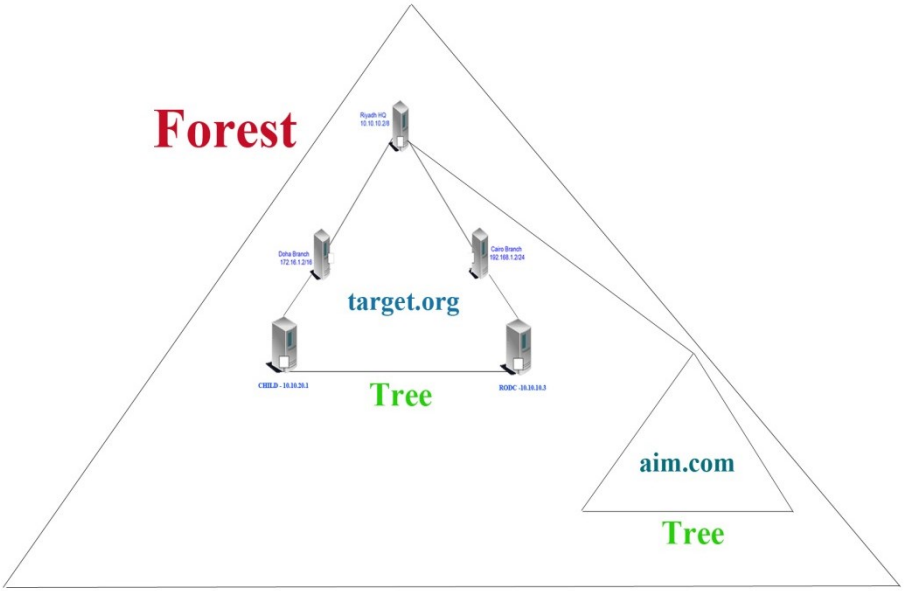
رائع جدا الـ Tree هو المكان الذي يحوي بداخلة Domain واحد أو اكثر كما قلنا

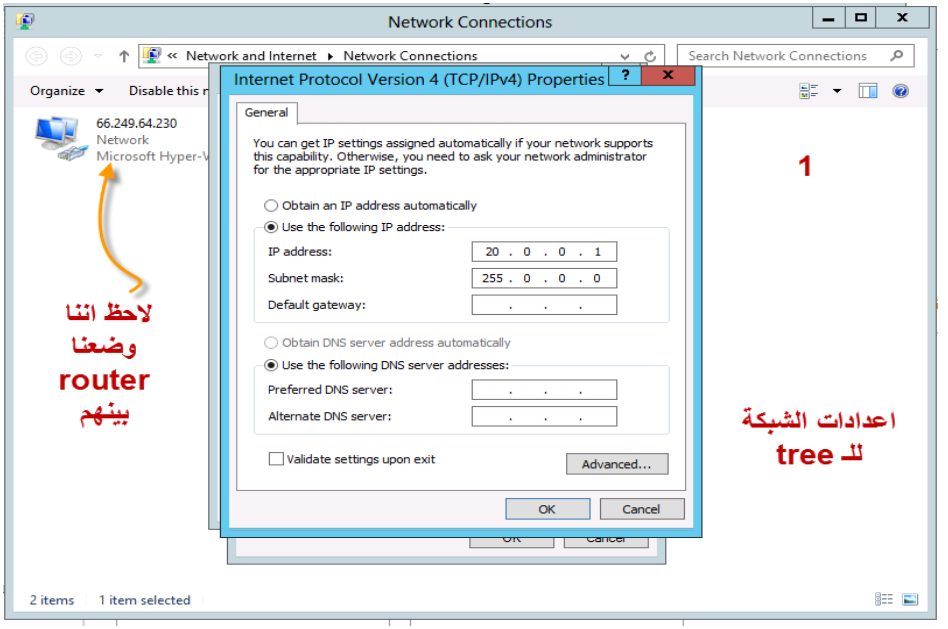
والغرض من انشاء الـ Tree هو عمل Domain جديد داخل ال Forest الرئيسية

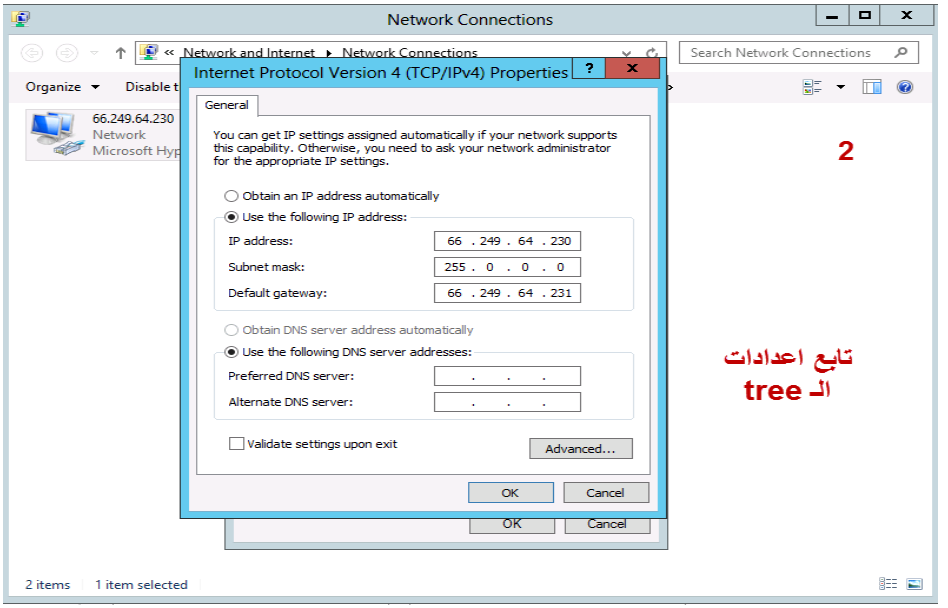
وما يميز الـ TREE

- لها قاعدة بيانات Database منفصلة تماما عن أي Tree أو Domain داخل الـ Forest
- لا ترث اسم الدومين الرئيسي مطلقا
- أيضا يمكن عمل Additional / Child / RODC داخلها على اعتبار انها مجال منفصل تماما
- يكون التحكم فيها عن طريق الـ Enterprise Administrator الخاص بالـ Forest (وهو اول Administrator لأول Domain داخل الـ Forest)

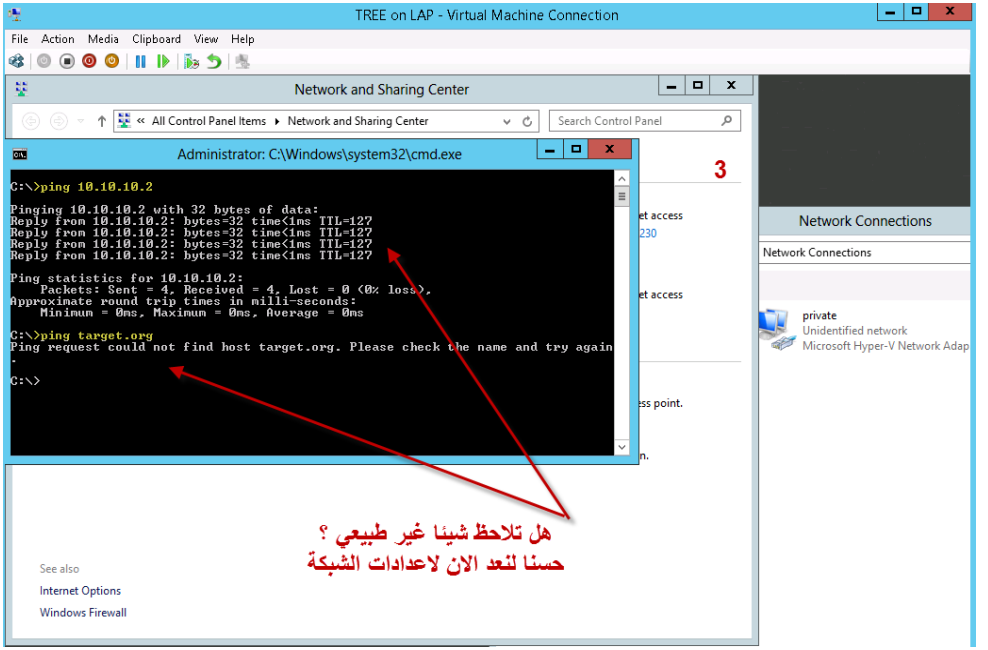
حسنا سنقوم بعمل Tree وسوف أقوم بتسميتها Aim.com وانت قم بتسميه شبكتك التي ستتدرب على انشاؤها كما يحلو لك .
وسوف يصبح مخطط العمل كالتالي :-

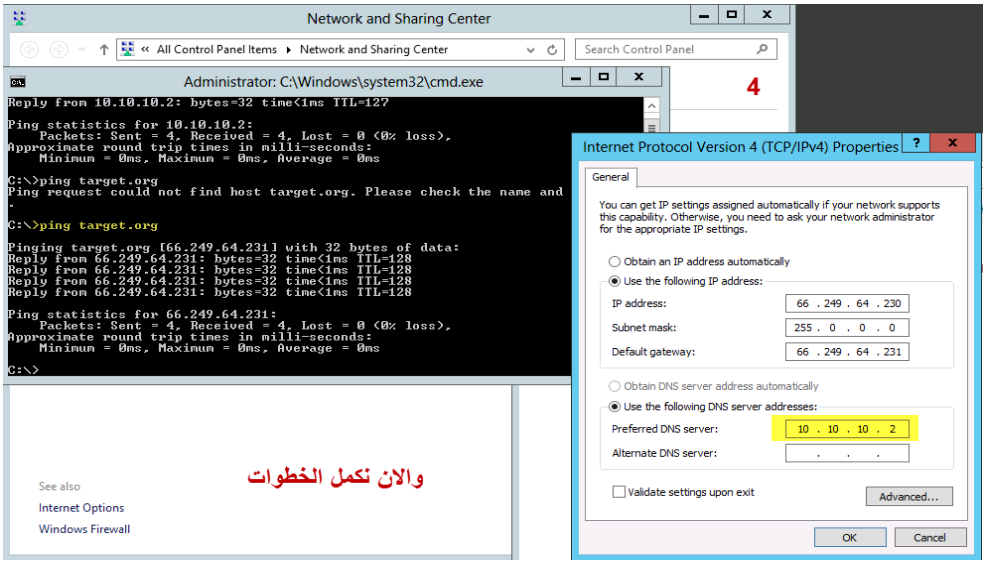


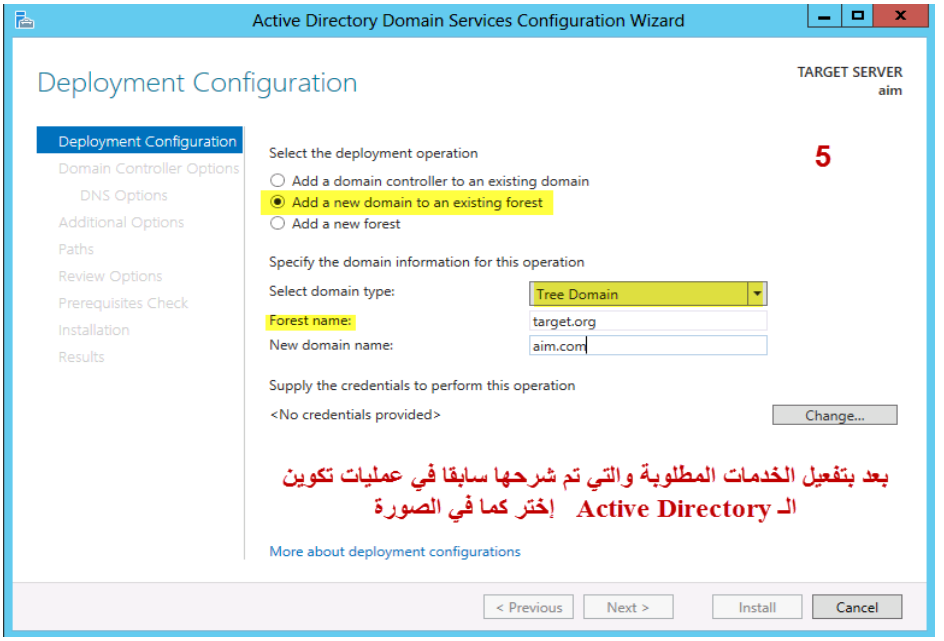


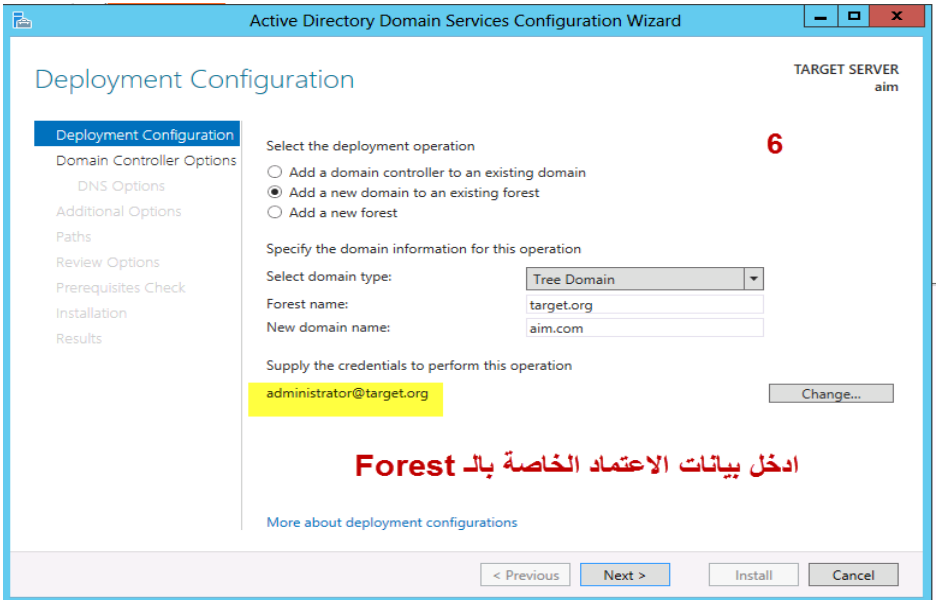


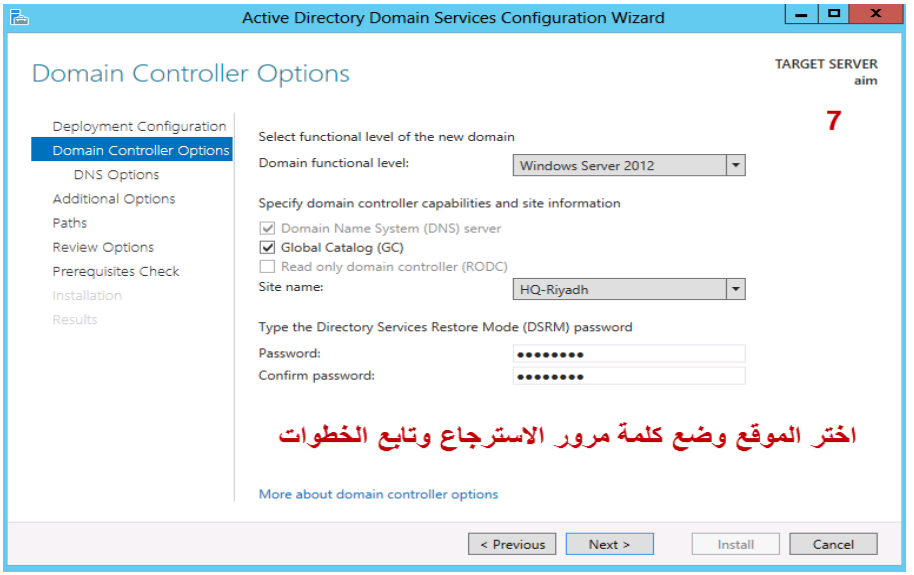
ولا تنسى ان تقوم بتفعيل خدمة الـ Routing لتتمكن من تحقيق الاتصال بين الـ Tree داخل الـ Forest

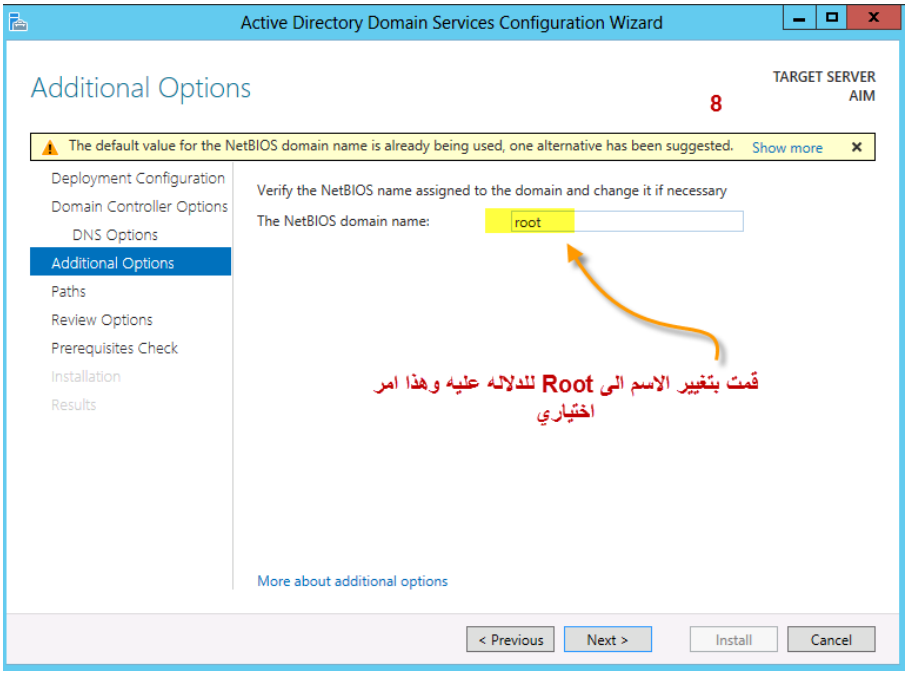

TREE on LAP - Virtual Machine Connection
File Action Media Clipboard View Help
Network and Sharing Center
« All Control Panel Items ▸ Network and Sharing Center
Search Control Panel
Administrator: C:\Windows\system32\cmd.exe
C:\>ping 10.10.10.2
Pinging 10.10.10.2 with 32 bytes of data:
Reply from 10.10.10.2: bytes=32 time<1ms TTL=127
Reply from 10.10.10.2: bytes=32 time<1ms TTL=127
Reply from 10.10.10.2: bytes=32 time<1ms TTL=127
Reply from 10.10.10.2: bytes=32 time<1ms TTL=127
Ping statistics for 10.10.10.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping target.org
Ping request could not find host target.org. Please check the name and try again
C:\>
3
Network Connections
Network Connections
private
Unidentified network
Microsoft Hyper-V Network Adap
هل تلاحظ شيئا غير طبيعي ؟
حسنا لنعد الان لاعدادات الشبكة
See also
Internet Options
Windows Firewall

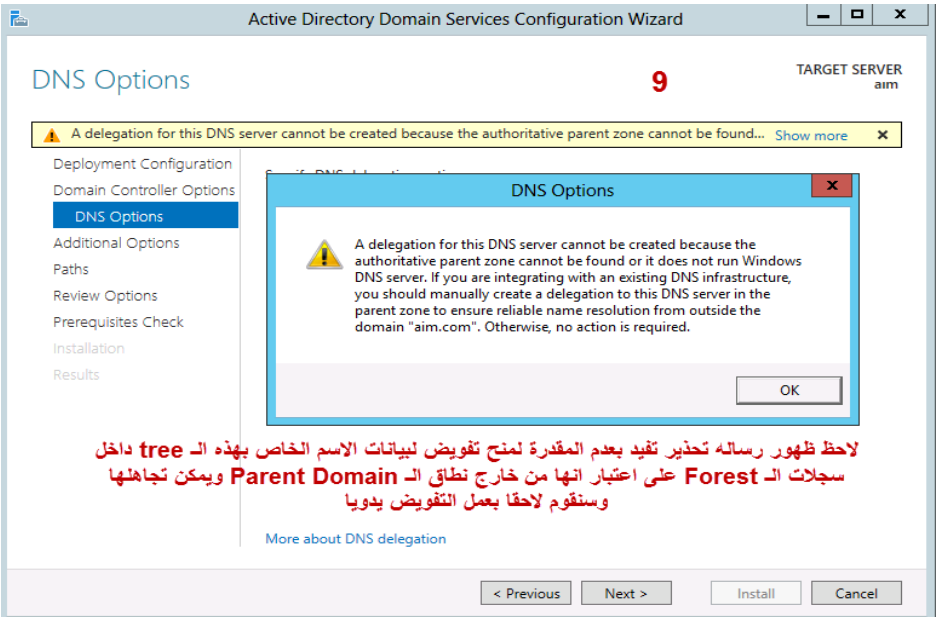

Network and Sharing Center
« All Control Panel Items ▸ Network and Sharing Center
Search Control Panel
Administrator: C:\Windows\system32\cmd.exe
Reply from 10.10.10.2: bytes=32 time<1ms TTL=127
Ping statistics for 10.10.10.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping target.org
Ping request could not find host target.org. Please check the name and
C:\>ping target.org
Pinging target.org [66.249.64.231] with 32 bytes of data:
Reply from 66.249.64.231: bytes=32 time<1ms TTL=128
Reply from 66.249.64.231: bytes=32 time<1ms TTL=128
Reply from 66.249.64.231: bytes=32 time<1ms TTL=128
Reply from 66.249.64.231: bytes=32 time<1ms TTL=128
Ping statistics for 66.249.64.231:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>
4
Internet Protocol Version 4 (TCP/IPv4) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 66 . 249 . 64 . 230
Subnet mask: 255 . 0 . 0 . 0
Default gateway: 66 . 249 . 64 . 231
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server: 10 . 10 . 10 . 2
Alternate DNS server:
Validate settings upon exit
Advanced...
OK
Cancel
والان نكمل الخطوات
See also
Internet Options
Windows Firewall

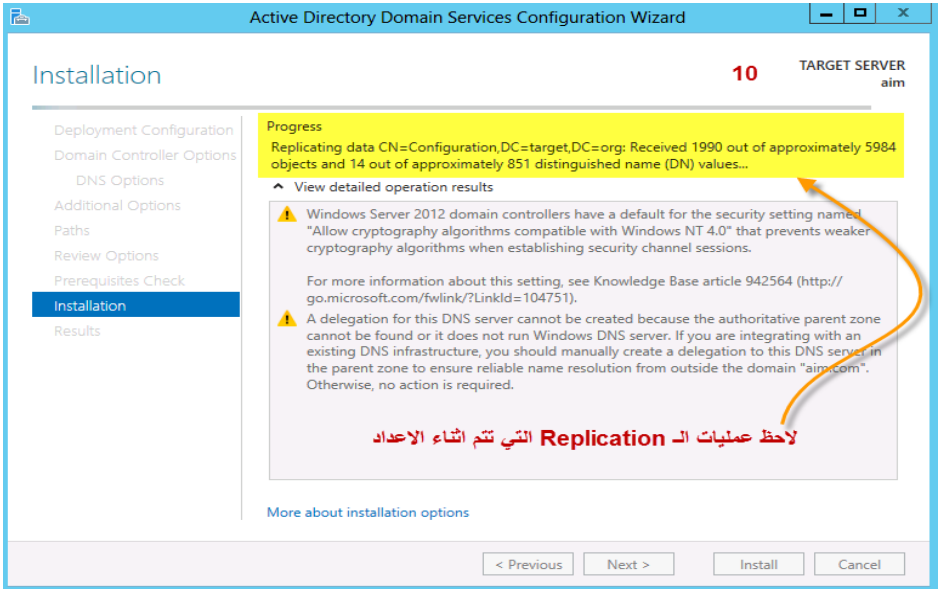

Active Directory Domain Services Configuration Wizard
Deployment Configuration
TARGET SERVER
aim
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Select the deployment operation
5
Add a domain controller to an existing domain
Add a new domain to an existing forest
Add a new forest
Specify the domain information for this operation
Select domain type:
Tree Domain
Forest name:
target.org
New domain name:
aim.com
Supply the credentials to perform this operation
<No credentials provided>
Change...
بعد بتفعيل الخدمات المطلوبة والتي تم شرحها سابقا في عمليات تكوين الـ Active Directory إختر كما في الصورة
More about deployment configurations
< Previous
Next >
Install
Cancel

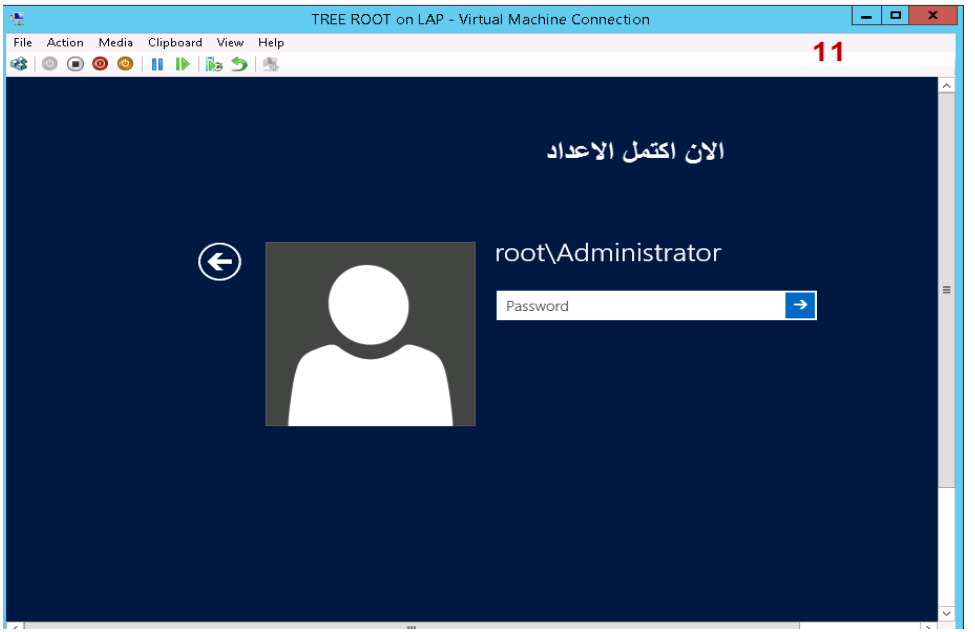

Active Directory Domain Services Configuration Wizard
Deployment Configuration
TARGET SERVER
aim
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Select the deployment operation
6
Add a domain controller to an existing domain
Add a new domain to an existing forest
Add a new forest
Specify the domain information for this operation
Select domain type:
Tree Domain
Forest name:
target.org
New domain name:
aim.com
Supply the credentials to perform this operation
administrator@target.org
Change...
ادخل بيانات الاعتماد الخاصة بالـ Forest
More about deployment configurations
< Previous
Next >
Install
Cancel

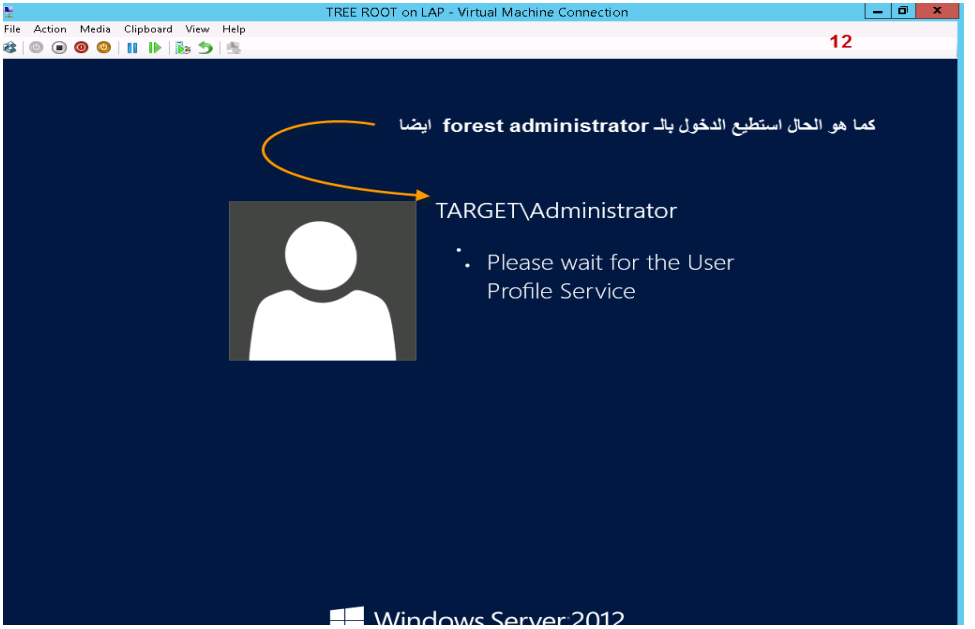

Active Directory Domain Services Configuration Wizard
Domain Controller Options
TARGET SERVER
aim
7
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Select functional level of the new domain
Domain functional level:
Windows Server 2012
Specify domain controller capabilities and site information
Domain Name System (DNS) server
Global Catalog (GC)
Read only domain controller (RODC)
Site name:
HQ-Riyadh
Type the Directory Services Restore Mode (DSRM) password
Password:
Confirm password:
اختر الموقع وضع كلمة مرور الاسترجاع وتابع الخطوات
More about domain controller options
< Previous
Next >
Install
Cancel

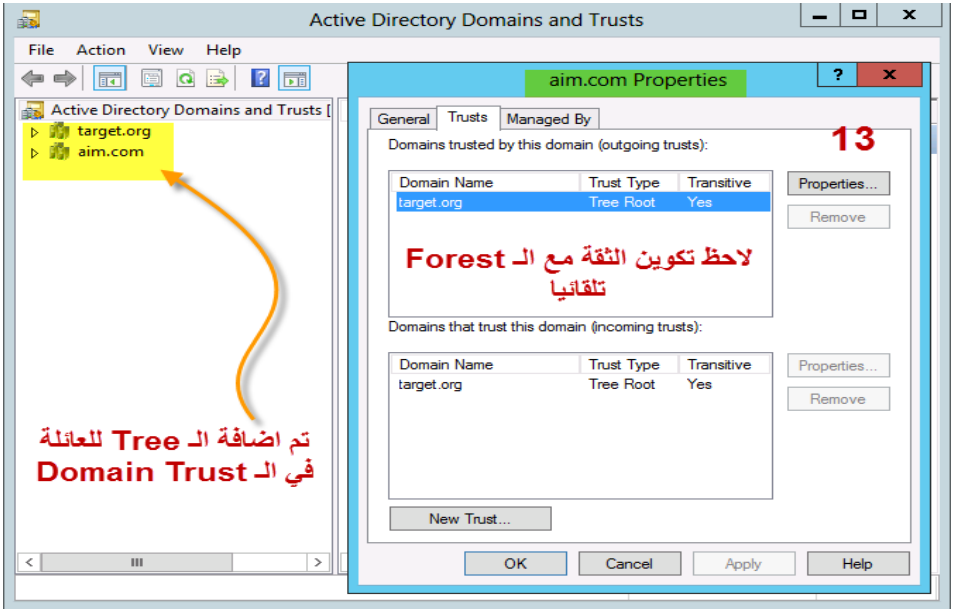

Active Directory Domain Services Configuration Wizard
Additional Options
TARGET SERVER
AIM
8
The default value for the NetBIOS domain name is already being used, one alternative has been suggested.
Show more
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Verify the NetBIOS name assigned to the domain and change it if necessary
The NetBIOS domain name:
root
قمت بتغيير الاسم الى Root للدلاله عليه وهذا امر اختياري
More about additional options
< Previous
Next >
Install
Cancel

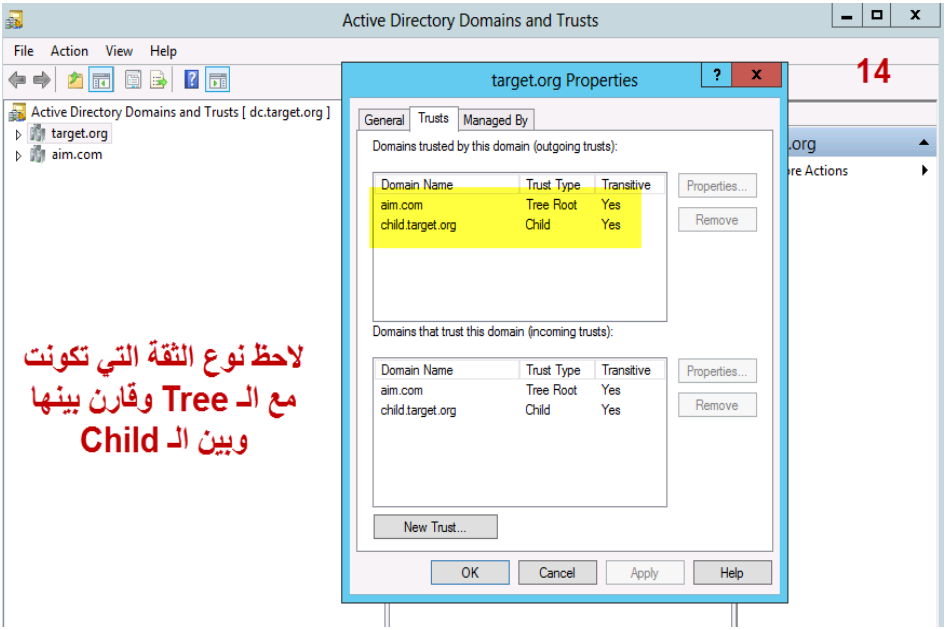

Active Directory Domain Services Configuration Wizard
DNS Options
9
TARGET SERVER
aim
A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found...
Show more
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
DNS Options
A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found or it does not run Windows DNS server. If you are integrating with an existing DNS infrastructure, you should manually create a delegation to this DNS server in the parent zone to ensure reliable name resolution from outside the domain "aim.com". Otherwise, no action is required.
OK
لاحظ ظهور رساله تحذير تفيد بعدم المقدرة لمنح تفويض لبيانات الاسم الخاص بهذه الـ tree داخل سجلات الـ Forest على اعتبار انها من خارج نطاق الـ Parent Domain ويمكن تجاهلها وسنقوم لاحقا بعمل التفويض يدويا
More about DNS delegation
< Previous
Next >
Install
Cancel


Active Directory Domain Services Configuration Wizard
Installation
10
TARGET SERVER
aim
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Progress
Replicating data CN=Configuration,DC=target,DC=org: Received 1990 out of approximately 5984 objects and 14 out of approximately 851 distinguished name (DN) values...
View detailed operation results
Windows Server 2012 domain controllers have a default for the security setting named "Allow cryptography algorithms compatible with Windows NT 4.0" that prevents weaker cryptography algorithms when establishing security channel sessions.
For more information about this setting, see Knowledge Base article 942564 (http://go.microsoft.com/fwlink/?LinkId=104751).
A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found or it does not run Windows DNS server. If you are integrating with an existing DNS infrastructure, you should manually create a delegation to this DNS server in the parent zone to ensure reliable name resolution from outside the domain "aim.com". Otherwise, no action is required.
لاحظ عمليات الـ Replication التي تتم اثناء الاعداد
More about installation options
< Previous
Next >
Install
Cancel


TREE ROOT on LAP - Virtual Machine Connection
File Action Media Clipboard View Help
11
الان اكتمل الاعداد
root\Administrator
Password


TREE ROOT on LAP - Virtual Machine Connection
File Action Media Clipboard View Help
12
كما هو الحال استطيع الدخول بالـ forest administrator ايضا
TARGET\Administrator
Please wait for the User Profile Service
Windows Server 2012

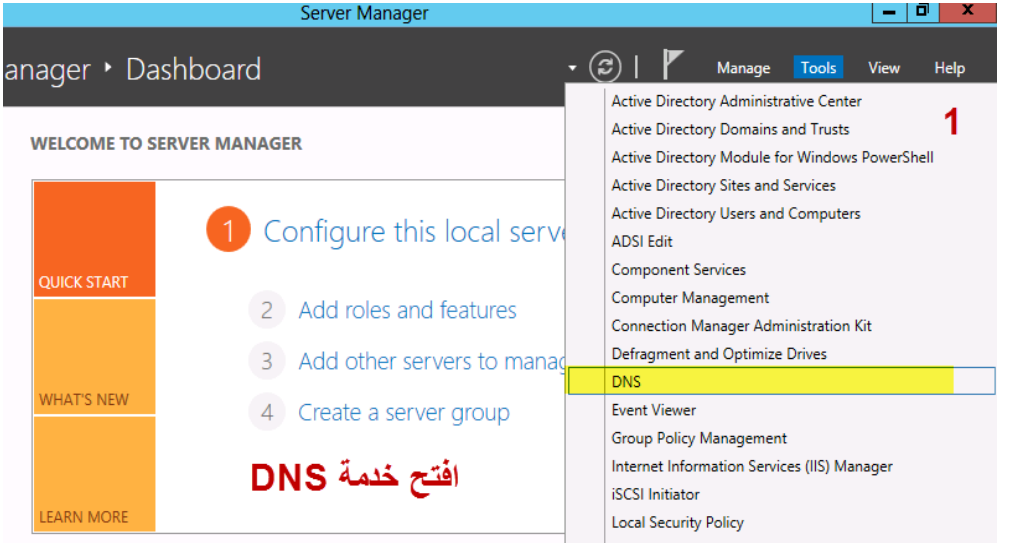

Active Directory Domains and Trusts
File Action View Help
Active Directory Domains and Trusts [
target.org
aim.com
تم اضافة الـ Tree للعائلة
في الـ Domain Trust
aim.com Properties
General Trusts Managed By
13
Domains trusted by this domain (outgoing trusts):
Domain Name Trust Type Transitive
target.org Tree Root Yes
Properties...
Remove
لاحظ تكوين الثقة مع الـ Forest
تلقائيا
Domains that trust this domain (incoming trusts):
Domain Name Trust Type Transitive
target.org Tree Root Yes
Properties...
Remove
New Trust...
OK Cancel Apply Help

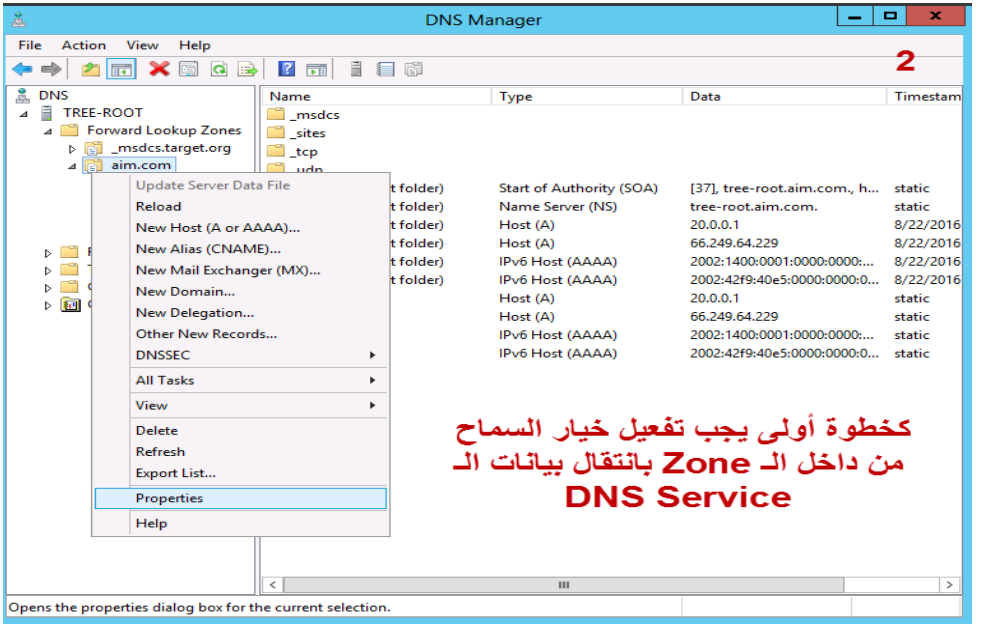

Active Directory Domains and Trusts
File Action View Help
Active Directory Domains and Trusts [dc.target.org]
target.org
aim.com
target.org Properties
14
General Trusts Managed By
Domains trusted by this domain (outgoing trusts):
Domain Name Trust Type Transitive
aim.com Tree Root Yes
child.target.org Child Yes
Properties...
Remove
Domains that trust this domain (incoming trusts):
Domain Name Trust Type Transitive
aim.com Tree Root Yes
child.target.org Child Yes
Properties...
Remove
New Trust...
OK Cancel Apply Help
لاحظ نوع الثقة التي تكونت
مع الـ Tree وقارن بينها
وبين الـ Child

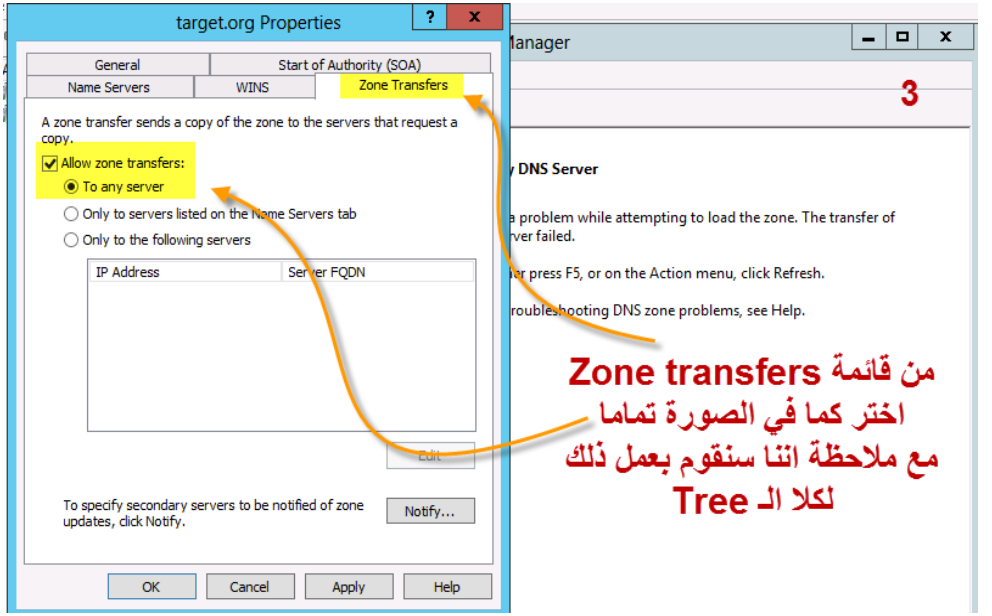
الان تم تكوين الـ Tree داخل الـ Forest واصبح لدي عدد 2 tree هما target.org و aim.com وتكونت بينهما علاقة تلقائية من نوع TREE ROOT TRUST ويستطيع الان المستخدمين في كلا الـ root الوصول الى مصادر بعضهما البعض ما دامت هذه العلاقة قائمة فلو كان لدي مستخدم باسم khaled@aim.com وهناك مجلد او طابعه متاحة للتشارك على جهاز تابع لمستخدم باسم yahya@target.org فان خالد يستطيع الوصول الى هذا المجلد أو الطابعة والعكس صحيح أيضا .

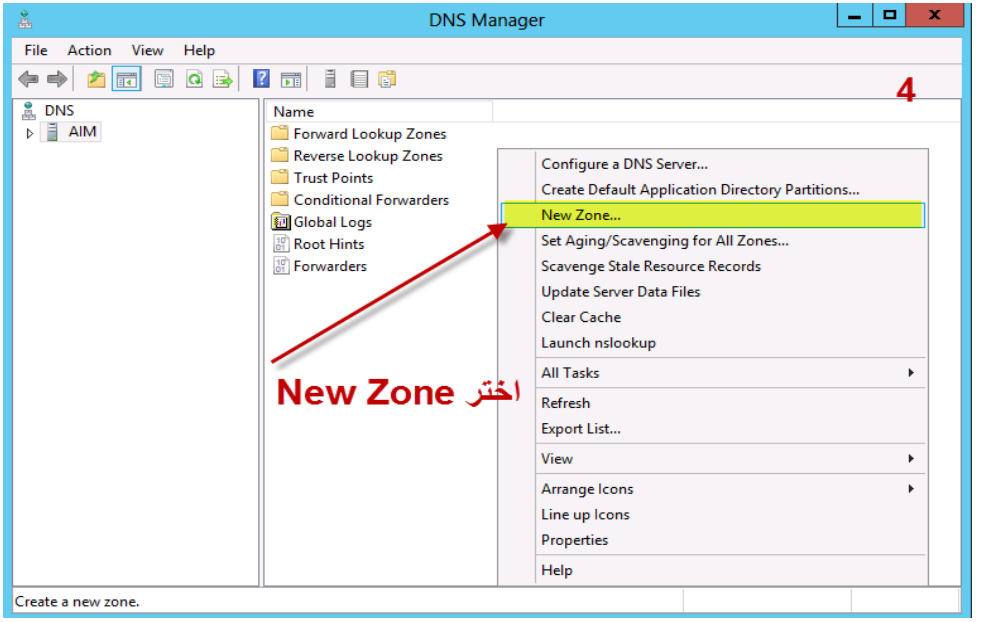
ويتم ذلك عن طريق ارسال طلب استعلام من جهاز خالد الى قاعدة بيانات DNS التابعة لمجال aim.com وبالطبع فان قاعدة البيانات تلك لا تحتوي على معلومات جهاز yahya فترد بعدم القدرة على التعرف على هذه البيانات ومن ثم تطلبها من قاعدة البيانات الخاصة بمجال Target.org فيرد الـ DNS الخاص بالـ Target Tree على هذا الاستعلام ويمنح aim.com البيانات الخاصة بالجهاز والمجلد ليوصلها في النهاية الى من طلبها وهو khaled وهذه العملية تسمى broadcast request

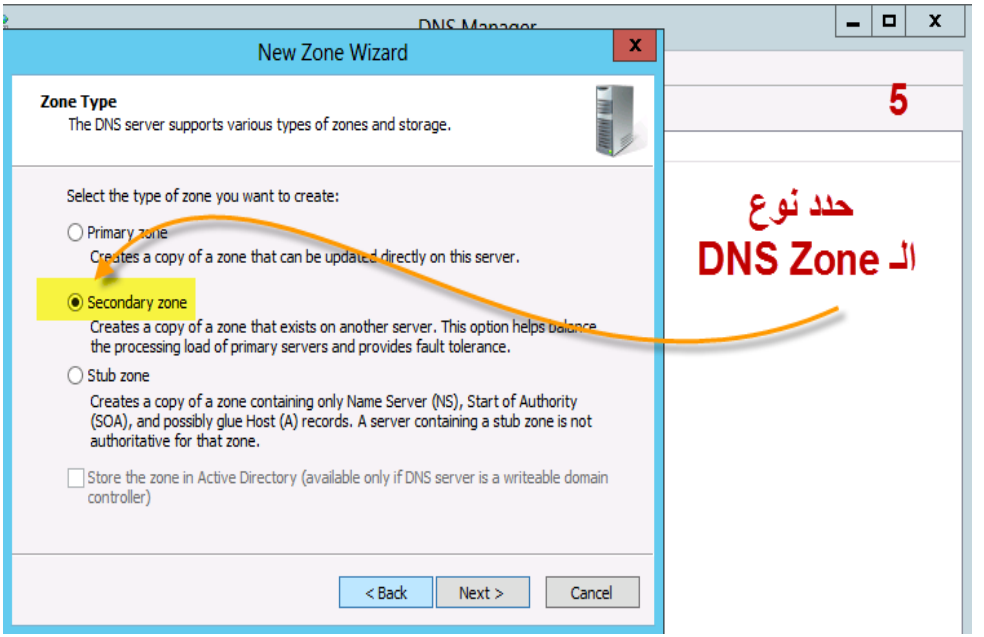
لكننا نستطيع توفير كل هذا الامر بالحصول على نسخة من قاعدة بيانات DNS الخاص بالـ Target Tree وتخزينها مع قاعدة بيانات DNS التابعة لمجال aim.com والعكس أيضا وبذلك سيتمكن كلا المستخدمين في كلا المجالين من الحصول على البيانات من نفس الـ DNS التبع لهم والطريقة تتم كالتالي :

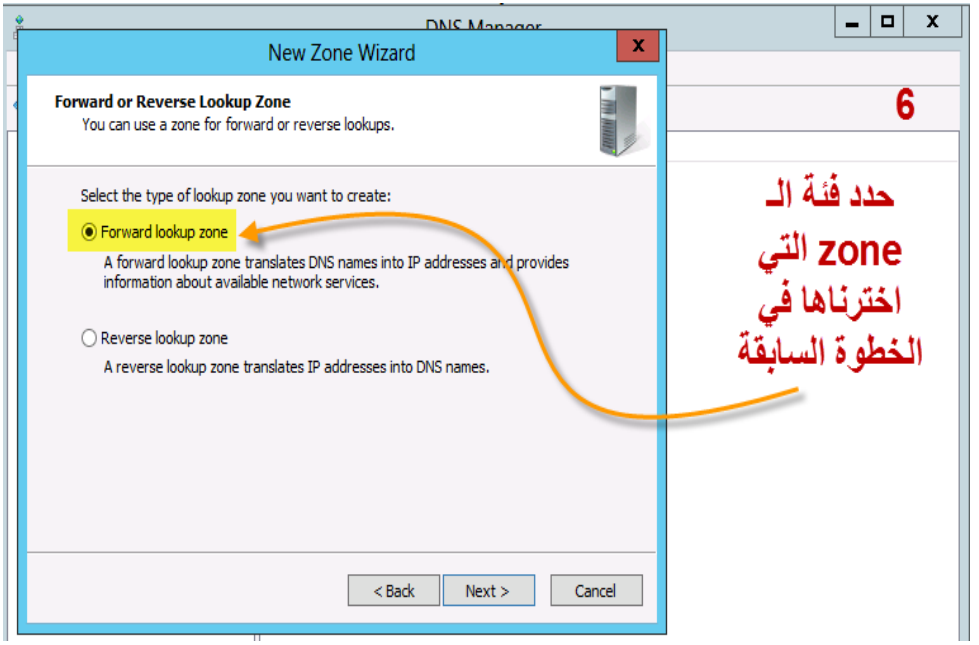


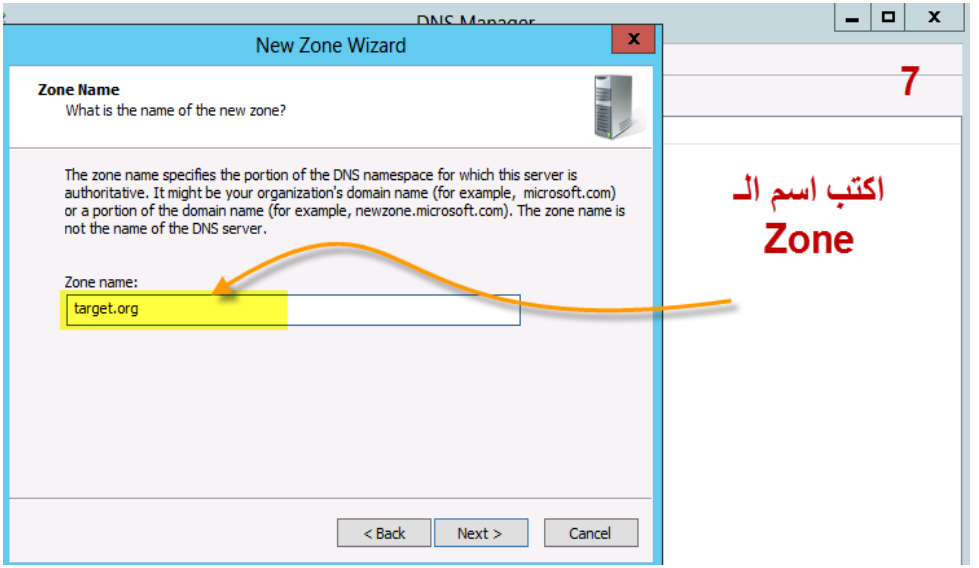

DNS Manager
File Action View Help
2
DNS
TREE-ROOT
Forward Lookup Zones
_msdcs.target.org
aim.com
Name
Type
Data
Timestam
_msdcs
_sites
_tcp
Update Server Data File
Reload
New Host (A or AAAA)...
New Alias (CNAME)...
New Mail Exchanger (MX)...
New Domain...
New Delegation...
Other New Records...
DNSSEC
All Tasks
View
Delete
Refresh
Export List...
Properties
Help
Start of Authority (SOA) [37], tree-root.aim.com., h... static
Name Server (NS) tree-root.aim.com. static
Host (A) 20.0.0.1 8/22/2016
Host (A) 66.249.64.229 8/22/2016
IPv6 Host (AAAA) 2002:1400:0001:0000:0000:... 8/22/2016
IPv6 Host (AAAA) 2002:42f9:40e5:0000:0000:0... 8/22/2016
Host (A) 20.0.0.1 static
Host (A) 66.249.64.229 static
IPv6 Host (AAAA) 2002:1400:0001:0000:0000:... static
IPv6 Host (AAAA) 2002:42f9:40e5:0000:0000:0... static
كخطوة أولى يجب تفعيل خيار السماح
من داخل الـ Zone بانتقال بيانات الـ
DNS Service
Opens the properties dialog box for the current selection.

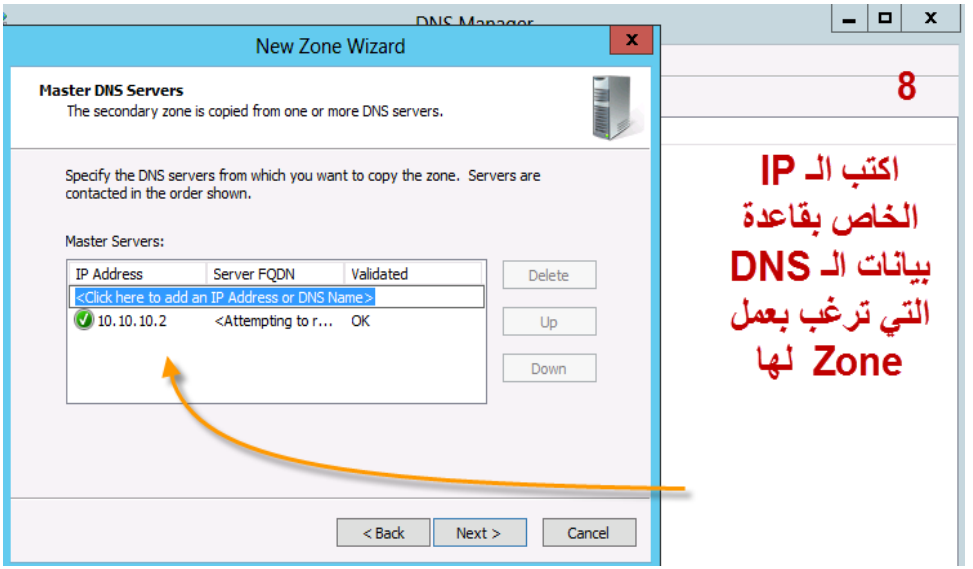

target.org Properties
General
Start of Authority (SOA)
Name Servers
WINS
Zone Transfers
A zone transfer sends a copy of the zone to the servers that request a copy.
Allow zone transfers:
To any server
Only to servers listed on the Name Servers tab
Only to the following servers
IP Address
Server FQDN
Edit...
To specify secondary servers to be notified of zone updates, click Notify.
Notify...
OK
Cancel
Apply
Help
anager
3
DNS Server
a problem while attempting to load the zone. The transfer of rver failed.
er press F5, or on the Action menu, click Refresh.
roubleshooting DNS zone problems, see Help.
من قائمة Zone transfers
اختر كما في الصورة تماما
مع ملاحظة اننا سنقوم بعمل ذلك
لكلا الـ Tree


DNS Manager
File Action View Help
4
DNS
AIM
Name
Forward Lookup Zones
Reverse Lookup Zones
Trust Points
Conditional Forwarders
Global Logs
Root Hints
Forwarders
Configure a DNS Server...
Create Default Application Directory Partitions...
New Zone...
Set Aging/Scavenging for All Zones...
Scavenge Stale Resource Records
Update Server Data Files
Clear Cache
Launch nslookup
All Tasks
Refresh
Export List...
View
Arrange Icons
Line up Icons
Properties
Help
New Zone اختر
Create a new zone.

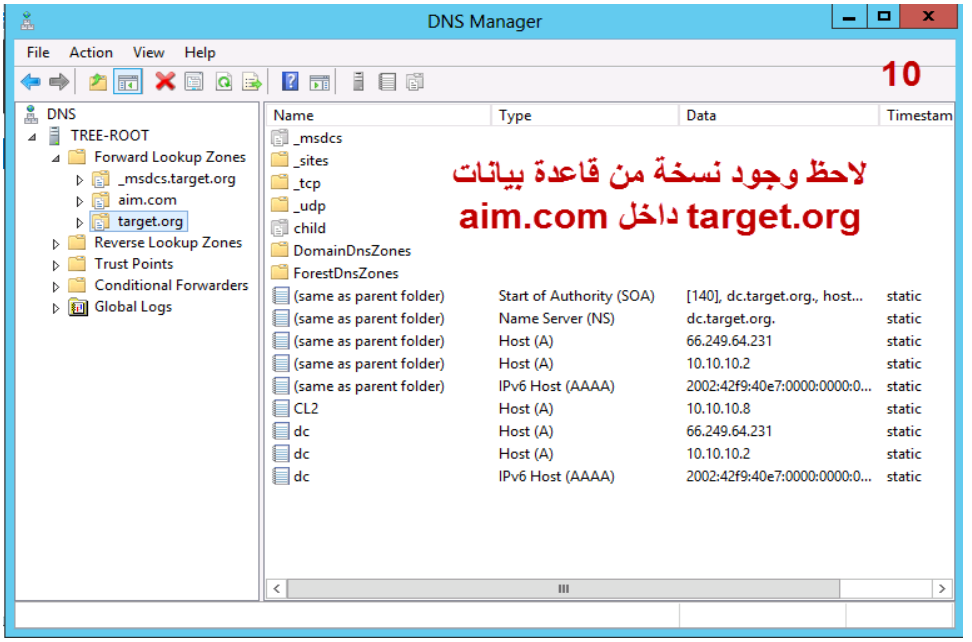

New Zone Wizard
Zone Type
The DNS server supports various types of zones and storage.
Select the type of zone you want to create:
Primary zone
Creates a copy of a zone that can be updated directly on this server.
Secondary zone
Creates a copy of a zone that exists on another server. This option helps balance the processing load of primary servers and provides fault tolerance.
Stub zone
Creates a copy of a zone containing only Name Server (NS), Start of Authority (SOA), and possibly glue Host (A) records. A server containing a stub zone is not authoritative for that zone.
Store the zone in Active Directory (available only if DNS server is a writeable domain controller)
< Back
Next >
Cancel
5
حدد نوع
الـ DNS Zone

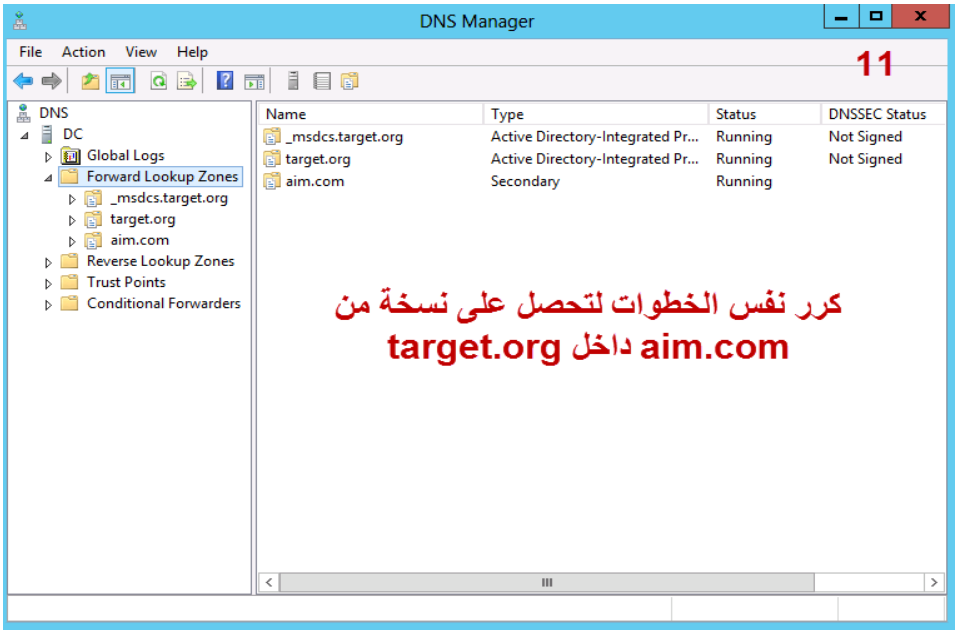

New Zone Wizard
Forward or Reverse Lookup Zone
You can use a zone for forward or reverse lookups.
Select the type of lookup zone you want to create:
Forward lookup zone
A forward lookup zone translates DNS names into IP addresses and provides information about available network services.
Reverse lookup zone
A reverse lookup zone translates IP addresses into DNS names.
< Back
Next >
Cancel
6
حدد فئة الـ
zone التي
اخترناها في
الخطوة السابقة


New Zone Wizard
Zone Name
What is the name of the new zone?
The zone name specifies the portion of the DNS namespace for which this server is authoritative. It might be your organization's domain name (for example, microsoft.com) or a portion of the domain name (for example, newzone.microsoft.com). The zone name is not the name of the DNS server.
Zone name:
target.org
< Back
Next >
Cancel
7
اكتب اسم الـ
Zone


New Zone Wizard
Master DNS Servers
The secondary zone is copied from one or more DNS servers.
Specify the DNS servers from which you want to copy the zone. Servers are contacted in the order shown.
Master Servers:
IP Address
Server FQDN
Validated
<Click here to add an IP Address or DNS Name>
10.10.10.2
<Attempting to r...
OK
Delete
Up
Down
< Back
Next >
Cancel
8
اكتب الـ IP الخاص بقاعدة بيانات الـ DNS التي ترغب بعمل Zone لها


New Zone Wizard
Completing the New Zone Wizard
You have successfully completed the New Zone Wizard. You specified the following settings:
Name: target.org
Type: Secondary
Lookup type: Forward
File name: target.org.dns
Note: You should now add records to the zone or ensure that records are updated dynamically. You can then verify name resolution using nslookup.
To close this wizard and create the new zone, click Finish.
< Back
Finish
Cancel
9
تهانينا تم الانتهاء


DNS Manager
File Action View Help
10
DNS
TREE-ROOT
Forward Lookup Zones
_msdcs.target.org
aim.com
target.org
Reverse Lookup Zones
Trust Points
Conditional Forwarders
Global Logs
Name Type Data Timestam
_msdcs
_sites
_tcp
_udp
child
DomainDnsZones
ForestDnsZones
(same as parent folder) Start of Authority (SOA) [140], dc.target.org., host... static
(same as parent folder) Name Server (NS) dc.target.org. static
(same as parent folder) Host (A) 66.249.64.231 static
(same as parent folder) Host (A) 10.10.10.2 static
(same as parent folder) IPv6 Host (AAAA) 2002:42f9:40e7:0000:0000:0... static
CL2 Host (A) 10.10.10.8 static
dc Host (A) 66.249.64.231 static
dc Host (A) 10.10.10.2 static
dc IPv6 Host (AAAA) 2002:42f9:40e7:0000:0000:0... static
لاحظ وجود نسخة من قاعدة بيانات
aim.com داخل target.org


DNS Manager
File Action View Help
11
DNS
DC
Global Logs
Forward Lookup Zones
_msdcs.target.org
target.org
aim.com
Reverse Lookup Zones
Trust Points
Conditional Forwarders
Name Type Status DNSSEC Status
_msdcs.target.org Active Directory-Integrated Pr... Running Not Signed
target.org Active Directory-Integrated Pr... Running Not Signed
aim.com Secondary Running
كرر نفس الخطوات لتحصل على نسخة من
target.org داخل aim.com

FOREST TRUST

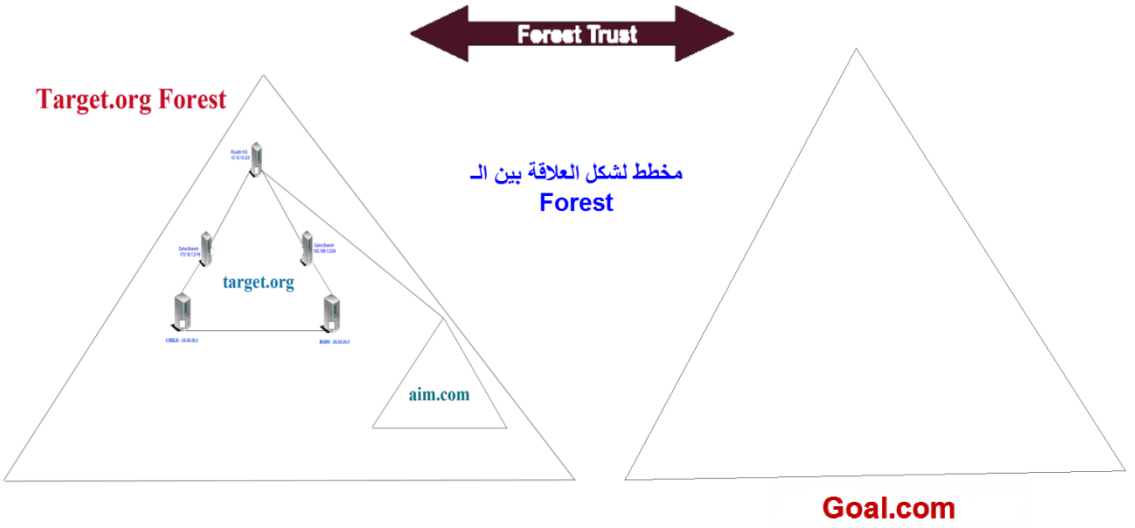
موضوعنا الاخير في هذا الجزء من الكتاب هو اجراء الثقة بين أكثر من Forest لذلك سوف نقوم بعمل New Forest ثم نحاول تكوين علاقة ثقة فيما بينها وبين الـ Target.org Forest

وبما انك الان أصبحت مؤهلا لعمل الـ New Forest فلن اتطرق معك لشرح هذه العملية ولكني سأعرض عليك فقط اعدادات الـ Network Connection حتى أساعدك في تكوين الـ New Forest

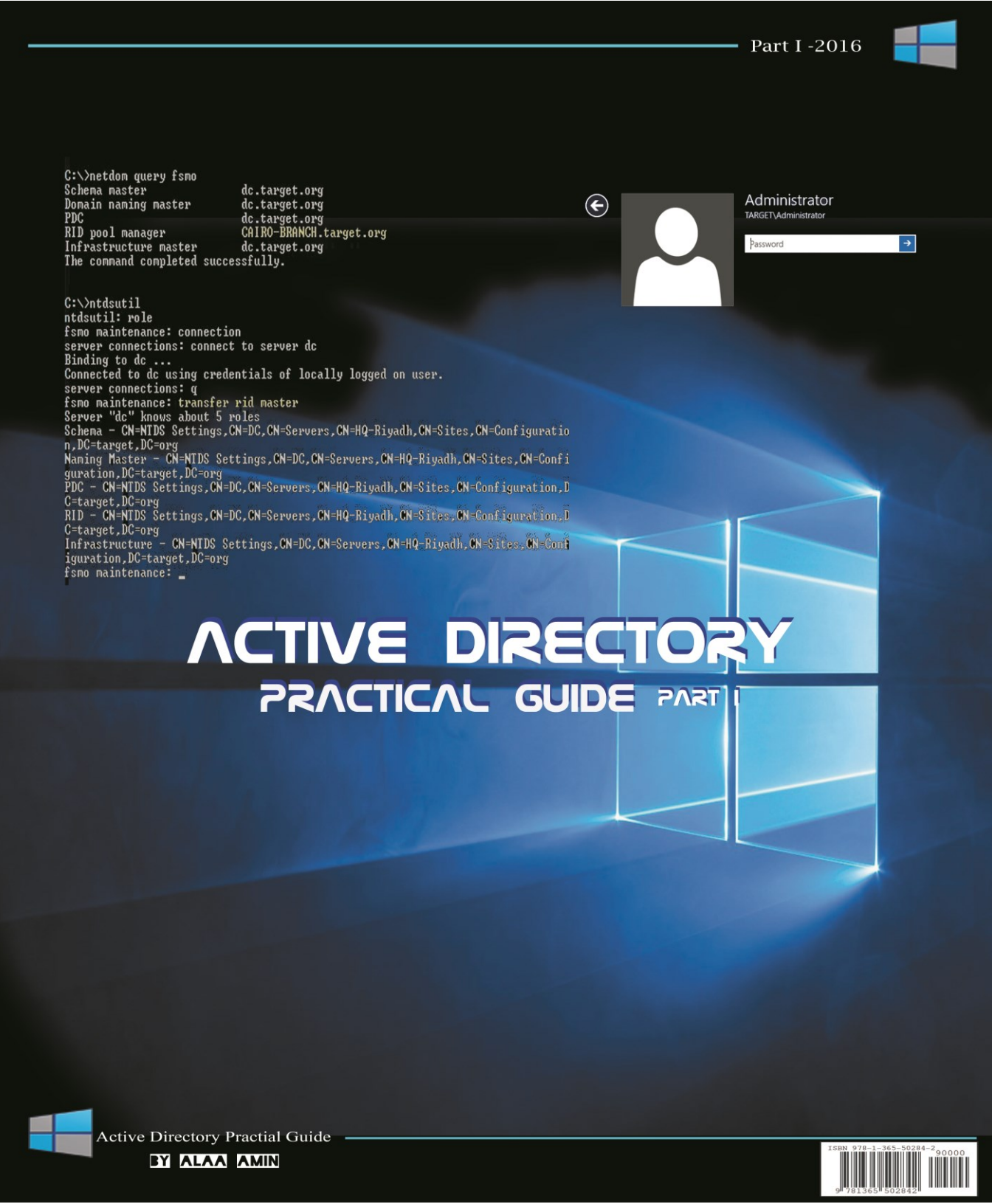
Domain name : ACS.com (win srvr 2012)

local ip is 96.10.20.10 /24

Real Ip For Routing is 66.249.64.228/8



انتهى الجزء الاول



ACTIVE DIRECTORY

PRACTICAL GUIDE PART I

ISBN 978-1-365-50284-2