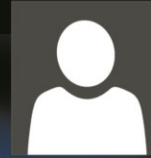




```
C:\>netdom query fsmo
Schema master          dc.target.org
Domain naming master   dc.target.org
PDC                   dc.target.org
RID pool manager       CAIRO-BRANCH.target.org
Infrastructure master   dc.target.org
The command completed successfully.
```

```
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=Configuration,DC=target,DC=org
Naming Master - CN=NTDS Settings,CN=DC,CN=Servers,CN=HQ-Riyadh,CN=Sites,CN=Configuration,DC=target,DC=org
PDC - CN=NTDS Settings,CN=DC,CN=Servers,CN=HQ-Riyadh,CN=Sites,CN=Configuration,DC=target,DC=org
RID - CN=NTDS Settings,CN=DC,CN=Servers,CN=HQ-Riyadh,CN=Sites,CN=Configuration,DC=target,DC=org
Infrastructure - CN=NTDS Settings,CN=DC,CN=Servers,CN=HQ-Riyadh,CN=Sites,CN=Configuration,DC=target,DC=org
fsmo maintenance: _
```



Administrator
TARGET\Administrator

password



ACTIVE DIRECTORY

PRACTICAL GUIDE PART I



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

AD Replication	3
AD Partition	4
Practical Guide	6
Routing	7
Domain Function Level	29
Additional Domain Controller	32
Working With AD Sites and Services	34
Windows Deploying Service	40
Operations Master Roles	54
Read Only Domain Controller	73
Child Domain	92
AD Trust And Relationship	101
Tree Root Domain	115
Forest Trust	129

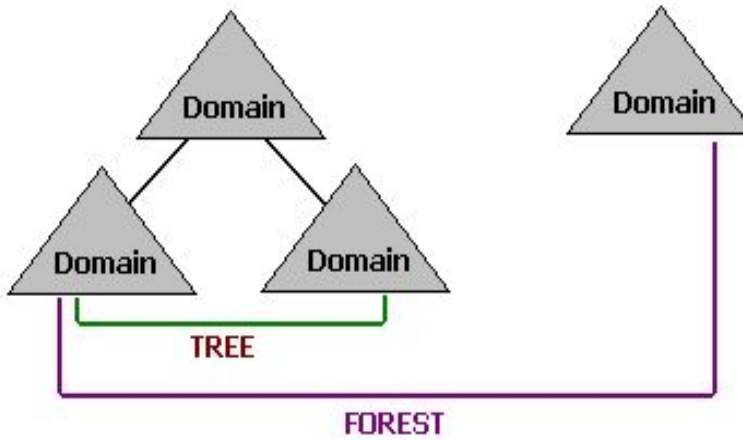
ACTIVE DIRECTORY REPLICATION

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** والـ **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

أول **Forest** و أول **Domain** وأول **Tree** كما في الشكل :-



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

الـ **Tree** هو المكان الذي يحوي بداخله **Domain** واحد أو أكثر

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

The Primary Domain أو Root Domain First -1

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

- يكون الاسم الخاص به هو اسم الـ Forest ككل
- هو الوحيد الذي يحتوي على Domain naming Master Role (سنشرح ذلك لاحقا)
- يكون Global Catalog by default
- يصبح Default first site name

Additional Domain -2

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 .

(RODC) Read Only Domain -3

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 يقرأها من الـ **Domain** الرئيسي .

Child Domain - 4

هو **Domain** يقع تحت الـ **Domain** الرئيسي لكنه منفصل عنه في الخصائص وله قاعدة بيانات مستقلة بذاتها عنه ويمكن من خلل 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** و الـ **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** و الـ **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

الدومين Partition

هو الذي يحتوي على كل ما يخص الدومين من **Computer Objects** ,... **User Objects** ...**Groups**.... **Container** و كل مكون من هذه المكونات له خصائصه التي تسمى **Attributes** و يدار بواسطة **Active Directory User and Computer Consol**

الدومين Configuration Partition

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

الدومين Schema Partition

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

الدومين Application partition

هذا الجزء يوجد اختياريًا حسب الحاجة له فالبرامج التي تتكامل مع بيانات الـ **Active Directory** تقوم باستخدامه في حفظ بياناتها كخادم البريد Exchange Server مثلًا 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:

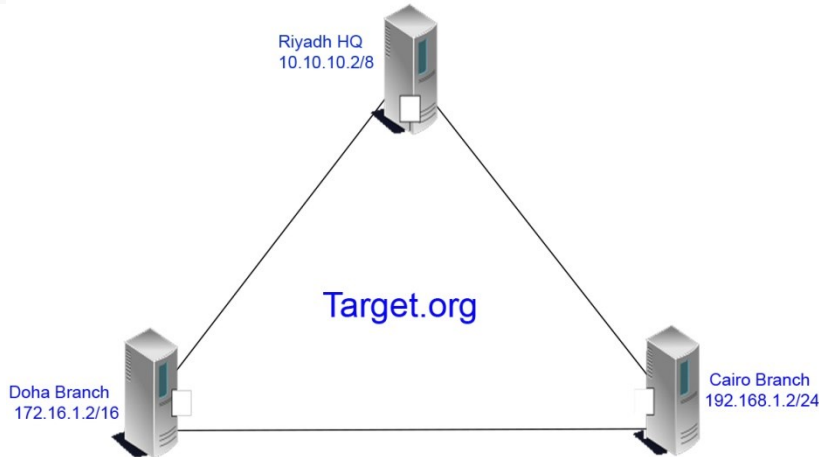
Domain name : target.org (win svr 2012)

Dns ip is 10.10.10.2 /8

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

Branch in Doha has 192.168.1.2/24 (win svr 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 :-

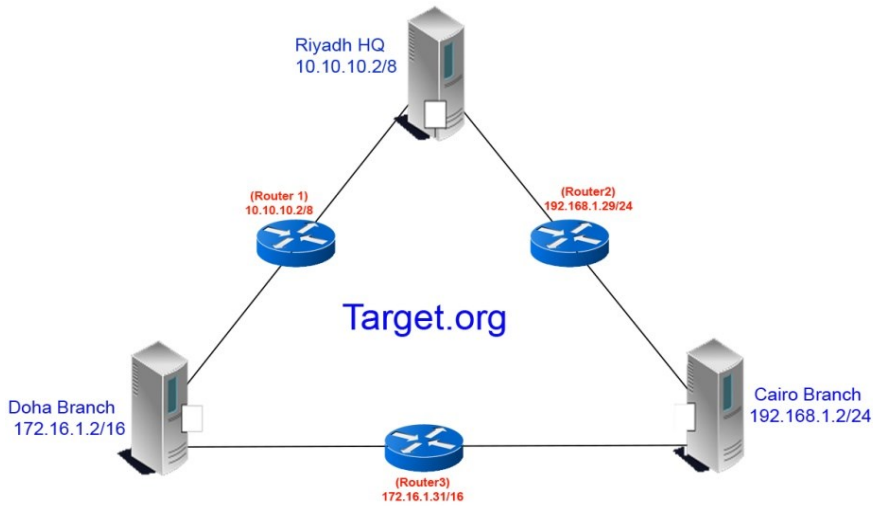
الخط الاول بين الرياض والقاهرة

الخط الثاني بين الرياض والدوحة

الخط الثالث بين الدوحة والقاهرة

ومن المعلوم ان هذه المدن الثلاث متباعدة جغرافياً بل انها تقع في قارتين مختلفتين هما أفريقيا واسيا ولكونهما تتبعان معا نفس الشركة الام فلا بد 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 :-

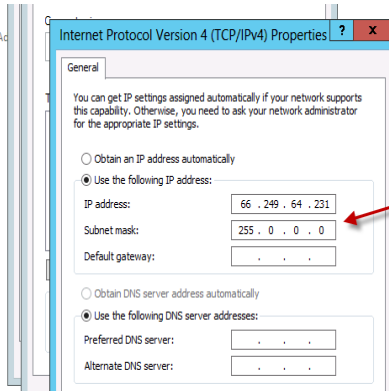
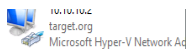


حسنا الان علمنا اننا سنحتاج الى جهاز router في كل فرع وحتى تتمكن الاجهزة من ان ترى بعضها البعض سنحتاج ايضا لعنوان ip ثابت لكل router وهذا العنوان يمكن طلبه من الشركة المزودة لخدمة الانترنت لديك

والآن هيا بنا لنقوم بعمل هذه الخطوات معا مع العلم اننا سنستخدم في الشرح خدمة Microsoft routing وسيكون الشرح داخل بيئة Hyper V (اضغط هنا للوصول لرابط كتابتنا لشرح Hyper V)

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

أولا سنقوم باعداد ال Routers كما يلي :-



الخطوة الاولى سنقوم بوضع عنوان الانترنت الثابت على كارت الشبكة للجهاز الذي سيقوم بدور الرواثر رقم 1 وفي حالتنا هذه سيكون في المركز الرئيسي في الرياض

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 Policy

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
Task Manager
Internet Explorer

Group Policy Management
DNS
Windows Deployment...
WinRAR
Active Directory Module for...
ADSI Edit
Health Registration...
Internet Information...
DHCP
Active Directory Domains and...
Network Policy Server
Remote Access Management

بعد الانتهاء من تفعيل ال role سنظهر الأيقونة الخاصة به في قائمة الأدوات قم بفتحها الآن

Routing and Remote Access
Server Status
DC

الشاشة الرئيسية الخاصة بالخدمة وتلاحظ على الجانب الأيسر أن الخدمة متوقفة وتابع في الخطوة القادمة طريقه تفعيلها

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

Configure and Enable Routing and Remote Access
Disable Routing and Remote Access
All Tasks
View
Delete
Refresh

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).

لتفعيل خدمة ال Routing

Secure connection between two private networks
Connect this network to a remote network, such as a branch office.

Custom configuration
Select any combination of the features available in Routing and Remote Access.

[For more information.](#)

< Back Next > Cancel

اختر الإعدادات المخصصة

Demand-dial connections (used for branch office routing)

NAT

LAN routing

[For more information.](#)

< Back Next > Cancel

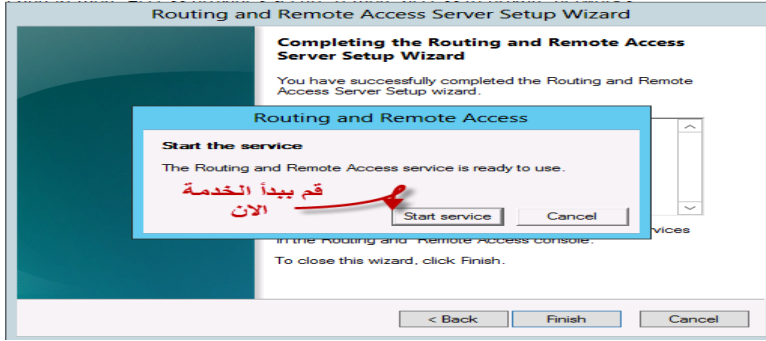
اختر LAN Routing

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 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 الانتهاء من خطوات الاعداد و عليك 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 اولاً 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 المتصل بها والكارت الاخر (E2) قمنا بمنحه ال Static IP الذي حصلنا عليه من مزود الخدمة
- 2- قمنا بتفعيل خدمة ال routing واختارنا في الاعدادات ان تكون من نوع LAN Routing وهذا يعني ان كلا الشبكتين المتصلتين بال router تستطيعان 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 .

The screenshot shows the Windows Network Connections window with 'Local Area Connection 2' selected. The 'Network Connection Details' window is open, showing the IPv4 Address as 10.10.10.8. A red arrow points to this address. Below, the 'Administrator: Command Prompt' window shows the command 'C:\>ping 66.249.64.231' and its output, which includes 'Reply from 66.249.64.231: bytes=32 time=193ms TTL=43'. A white arrow points from the text below to the 'Reply from' line in the Command Prompt output.

كما تلاحظ هذا الجهاز استطاع ان يرى عنوان IP الخارجي لل Router مع انه يحمل عنوان داخلي فقط

The screenshot shows the 'Administrator: Command Prompt' window with the command 'C:\Users\Administrator.TARGET>ping 10.10.10.5' and its output, which includes 'Reply from 10.10.10.5: bytes=32 time<1ms TTL=127'. A white arrow points from the text below to the 'Reply from' line in the Command Prompt output. To the right, the 'Network Connection Details' window is open, showing the IPv4 Address as 10.10.10.5. A red arrow points to this address.

لاحظ ان الجهاز الخارجي ايضا استطاع ان يرى العناوين الداخلية بعد تفعيل خدمة ال Routing

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

View your basic network information and set up connections

ROUTER2 (This computer) Multiple networks Internet

View your active networks

Network 6 Public network

Unidentified network Public network

Access type: No Internet access
Connections: 192.168.1.29

Access type: No Internet access
Connections: 66.249.64.232

Change your networking settings

Set up a new connection or network
Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.

Connect to a network
Connect or reconnect to a wireless, wired, dial-up, or VPN network connection.

Troubleshoot problems

هذا ال router سيكون في فرع الدوحة وبالتالي سيكون له عنوان داخلي من نفس ال subnet الخاصة بالفرع وله ايضا static ip حتى تتم عملية الربط مع الفرع الرئيسي كما سبق في الشرح

Routing and Remote Access

File Action View Help

Routing and Remote Access

Server Status

ROUTER2 (local)

Network Interfaces

Remote Access Logging & Settings

IPv4

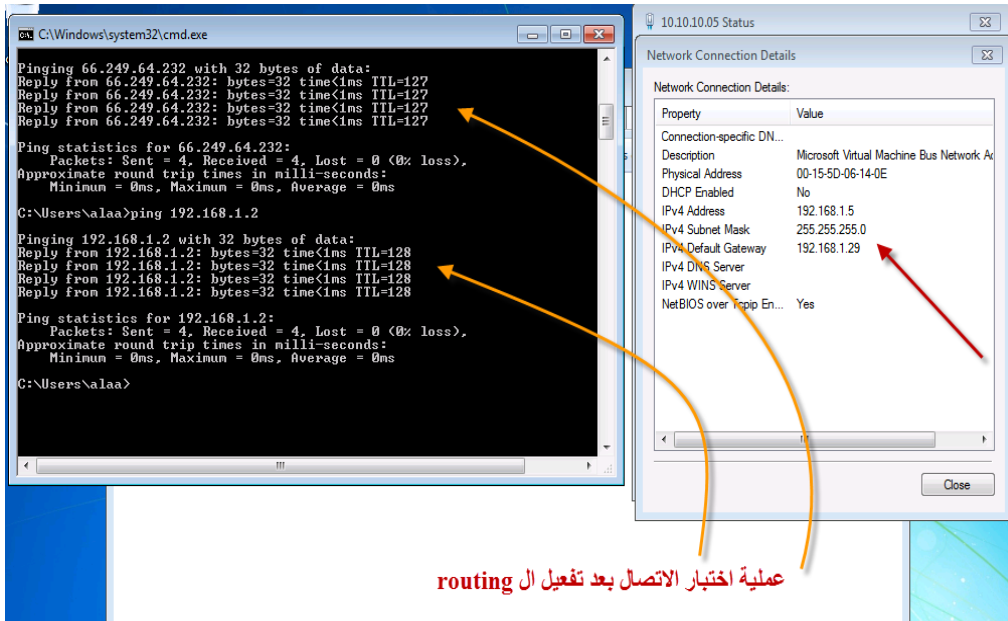
General

Static Routes

IPv6

Interface	Type	IP Address	Incoming bytes	Outgoing bytes	Static Filters	Administrative Status
Loopback	Loopback	127.0.0.1	0	0	Disabled	Up
Internal	Internal	Not available	-	-	Disabled	Unknown
66.249.64.232	Dedicated	66.249.64.232	137,192	89,816	Disabled	Up
192.168.1.29	Dedicated	192.168.1.29	84,751	111,343	Disabled	Up

تفعيل ال Routing كما تم في الفرع الرئيسي وبنفس الخطوات



الان لدينا عدد 2 router وعدد 3 subnet 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 اولاً ان نقوم بعملية توجيه البيانات القادمة من كلا الفرعين عن طريق ال routers أو ما يعرف بال Static Route وفيها سوف نجعل ال router رقم 1 الموجود في الرياض يخاطب ال router رقم 2 الموجود في الدوحة حين يحتاج بيانات من الفرع والعكس ايضاً صحيح أي ان كلا منهما سوف يتبادل معلومات ال Subnet الخاصة به مع الاخر .

```

Administrator: C:\Windows\system32\cmd.exe

Ethernet adapter 10.10.10.2:
    Connection-specific DNS Suffix  . : 
    IPv4 Address. . . . . : 10.10.10.2
    Subnet Mask . . . . . : 255.0.0.0
    Default Gateway . . . . . : 0.0.0.0

Tunnel adapter isatap.{3376F152-CC4F-40F7-831F-C8D61BF39A2B}:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Tunnel adapter isatap.{D58152EC-9CFE-4A7A-8C67-C2FAA3021913}:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Tunnel adapter 6T04 Adapter:
    Connection-specific DNS Suffix  . : 
    IPv6 Address. . . . . : 2002:42f9:40e7::42f9:40e7
    Default Gateway . . . . . : 

C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:
Reply from 10.10.10.2: Destination host unreachable.
Reply from 10.10.10.2: Destination host unreachable.
Reply from 10.10.10.2: Destination host unreachable.
Reply from 10.10.10.2: Destination host unreachable.

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 0 (0% loss),
C:\>_
  
```

قبل عملية ال Static Route لاحظ ان الفرع الرئيسي غير قادر علي الاتصال بفرع الدوحة ولذلك سنقوم بعملية التوجيه لل Routers

ولعمل هذا التوجيه تابع الآتي :-



Routing and Remote Access

Server Status

DC

Network Interfaces

Remote Access Logging

IPv4

General

Static Routes

IPv6

General

Static Routes

Static Routes

Destination	Network mask	Gateway	Interface	Metric	View
There are no items to show in this view.					

IPv4 Static Route

Interface: R1

66.249.64.231

اختر العنوان الخارجي للراوتر

Destination: 192.168.1.0

اكتب الوجهة المراد تفعيلها (عنوان شبكة الفرع)

Network mask: 255.255.255.0

ادخل قناع الشبكة لعنوان الوجهة الذي ادخلته

Gateway: R2

66.249.64.232

أكتب عنوان البوابة الذي سيتم من خلاله العبور
لوجهتك (عنوان الراوتر الموجود في الفرع)

Metric: 256

Use this route to initiate demand-dial connections

For more information.

OK Cancel

من المقترض معرفة بعد كم راوتر سنصل الى وجهتك وفي حالتنا هذه سنصل بعد راوتر واحد فقط ومن الممكن كتابة رقم 1 ولكن ان تركناها كما هي فلن يؤثر

Destination	Network mask	Gateway	Interface	Metric
192.168.1.0	255.255.255.0	66.249.64.232	66.249.64.231	256

ing

```
Administrator: C:\Windows\system32\cmd.exe

Ethernet adapter 10.10.10.2:
    Connection-specific DNS Suffix  . : 
    IPv4 Address. . . . . : 10.10.10.2
    Subnet Mask . . . . . : 255.0.0.0
    Default Gateway . . . . . : 0.0.0.0

Tunnel adapter isatap.{3376F152-CC4F-40F7-831F-C8D61BF39A2B}:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Tunnel adapter isatap.{D58152EC-9CFE-4A7A-8C67-C2FAA3021913}:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Tunnel adapter 6T04 Adapter:
    Connection-specific DNS Suffix  . : 
    IPv6 Address. . . . . : 2002:42f9:40e7::42f9:40e7
    Default Gateway . . . . . : 

C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:
Reply from 192.168.1.2: bytes=32 time<1ms TTL=127
Reply from 192.168.1.2: bytes=32 time<1ms TTL=127
Reply from 192.168.1.2: bytes=32 time<1ms TTL=127
Reply from 192.168.1.2: bytes=32 time<1ms TTL=127

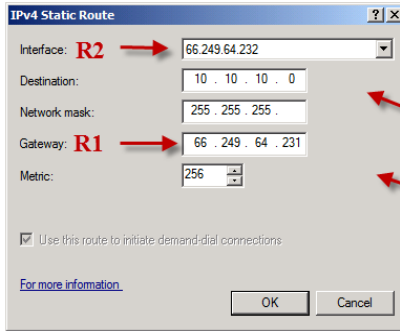
Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

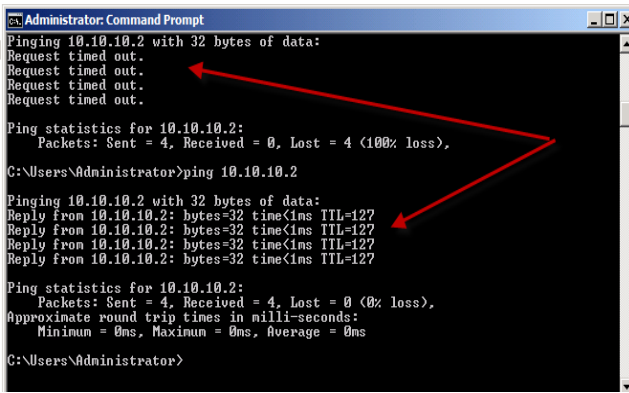
تذكر أنه يمكن تتبع عملية التوجيه باستخدام الامر pathping

تم الاتصال بعد عملية التوجيه

الان سنقوم بالتوجيه من داخل فرع الدوحة فتابع معي :-

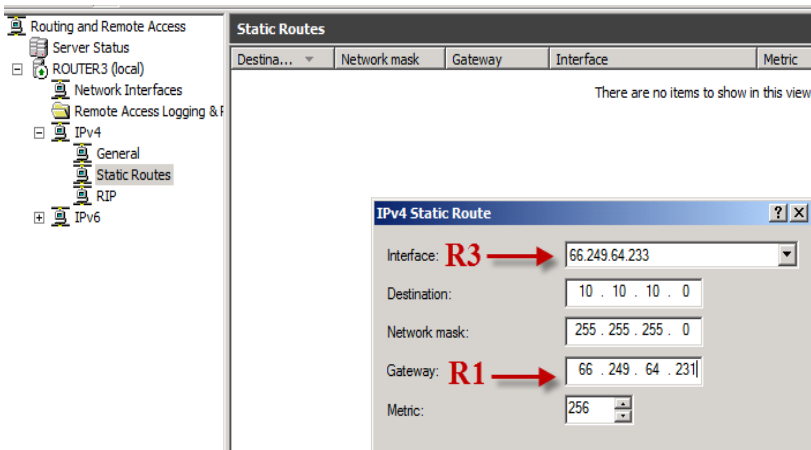


إجراء التوجيه للراوتر في فرع
الدوحة تماما كما قمنا بها في فرع
الرياض



الاتصال قبل
ويعد عملية
التوجيه

الآن بقي ان نقوم بنفس العملية في فرع القاهرة واختبار الاتصال كما سبق



```

Administrator: Command Prompt
C:\Users\Administrator>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 = 1ms, Average = 0ms
C:\Users\Administrator>_

```

نجاح الاتصال من فرع القاهرة بفرع الرياض

الآن لدينا عدد 3 router وعدد 4 subnet 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

```

Administrator: Command Prompt
Ethernet adapter 172.16.1.2:
    Connection-specific DNS Suffix  . :
    IPv4 Address. . . . . : 172.16.1.2
    Subnet Mask . . . . . : 255.255.0.0
    Default Gateway . . . . . : 172.16.1.31

Ethernet adapter Local Area Connection* 9:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Tunnel adapter isatap.{756E4838-4022-40BE-BF56-F4F2DE59E232}:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Tunnel adapter Local Area Connection* 11:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Tunnel adapter isatap.{73E6282F-0412-4421-9AE0-E069213642CD}:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

C:\>ping 192.168.1.2
Pinging 192.168.1.2 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
    :>

```


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


حسننا 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


Static Routes					
Destination	Network mask	Gateway	Interface	Metric	View
172.16.1.0	255.255.255.0	66.249.64.233	66.249.64.231	256	Both
192.168.1.0	255.255.255.0	66.249.64.232	66.249.64.231	256	Both

 **Routing in Riyadh Branch**

Static Routes					
Destina...	Network mask	Gateway	Interface	Metric	View
10.10.10.0	255.255.255.0	66.249.64.231	66.249.64.232	256	Both
172.168.1.0	255.255.255.0	66.249.64.233	66.249.64.232	256	Both

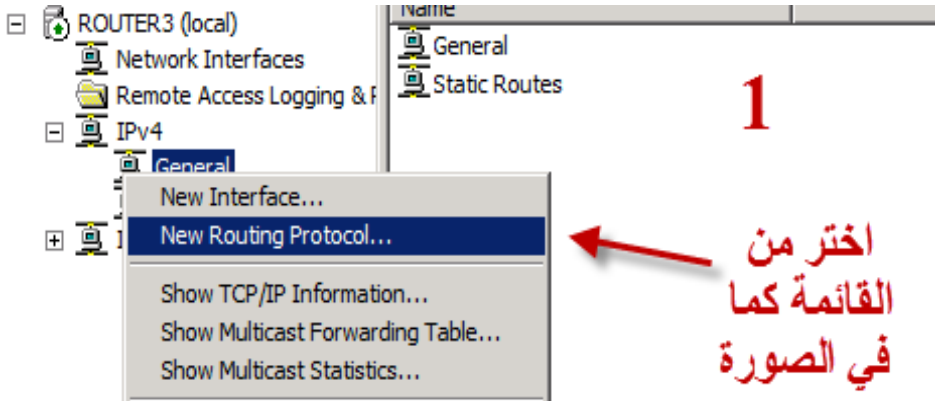
 **Routing in Doha Branch**

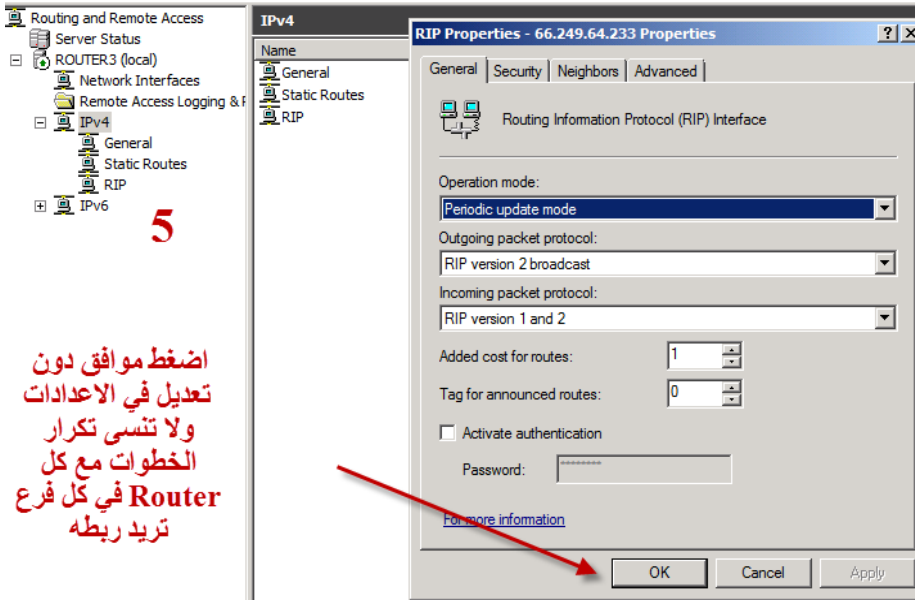
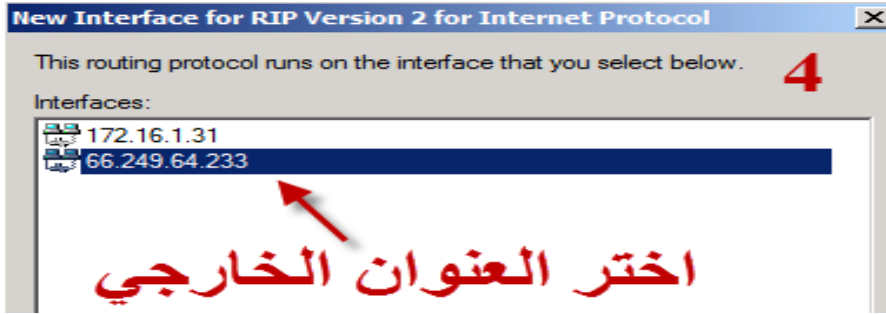
Static Routes					
Destina...	Network mask	Gateway	Interface	Metric	View
10.10.10.0	255.255.255.0	66.249.64.231	66.249.64.233	256	Both
192.168.1.0	255.255.255.0	66.249.64.232	66.249.64.233	256	Both

 **Routing in Cairo Branch**

هل وجدت صعوبة اثناء عمل ذلك ؟

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

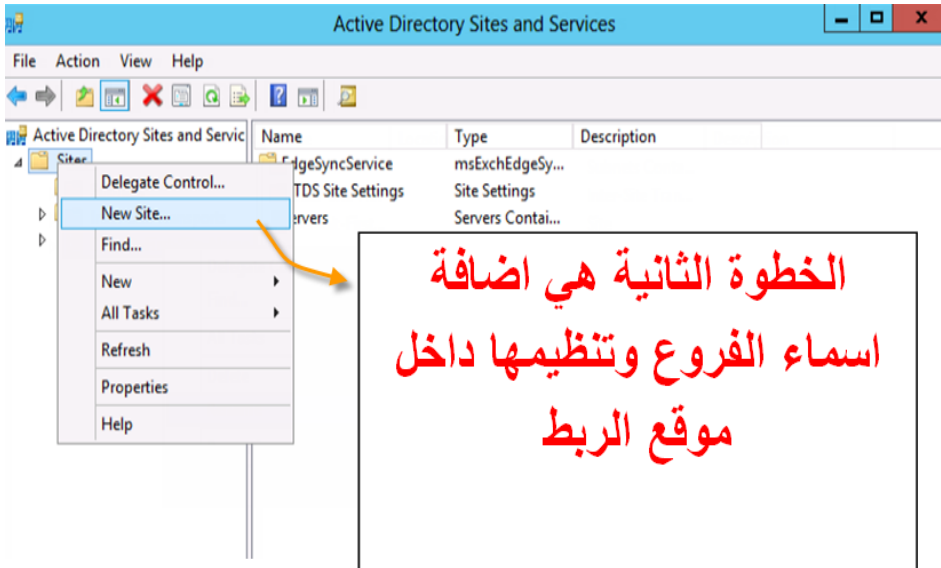
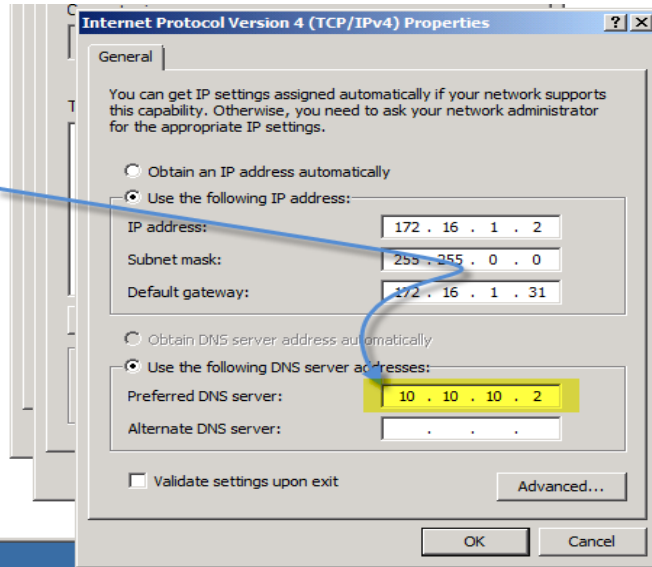




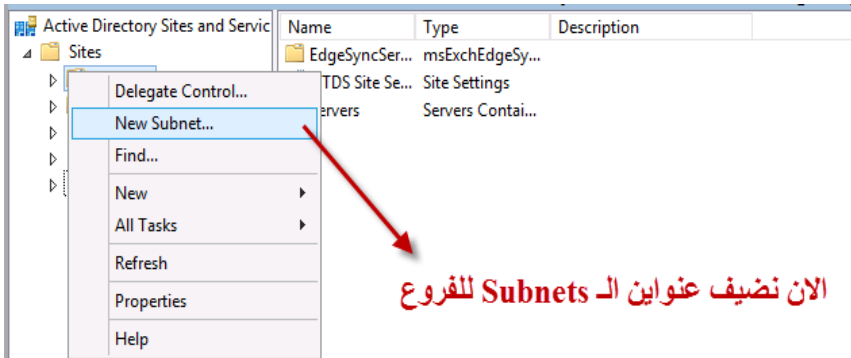
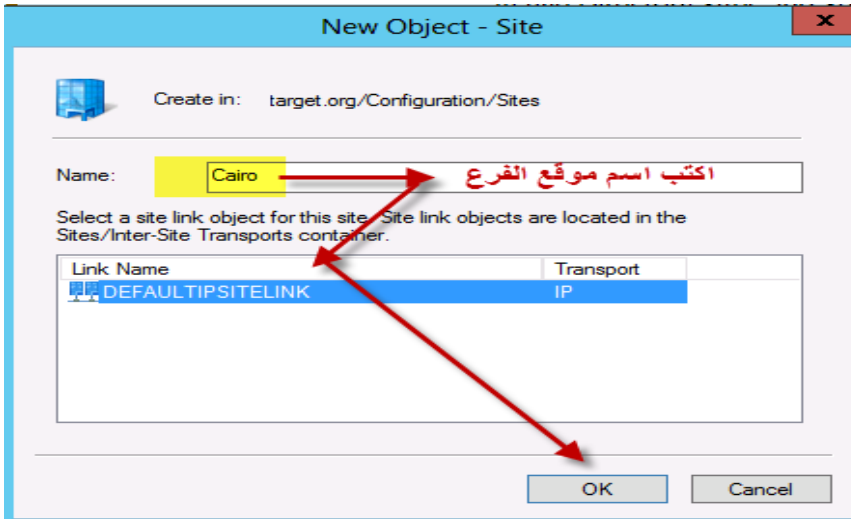
اضغط موافق دون
تعديل في الاعدادات
ولا تنسى تكرار
الخطوات مع كل
Router في كل فرع
تريد ربطه

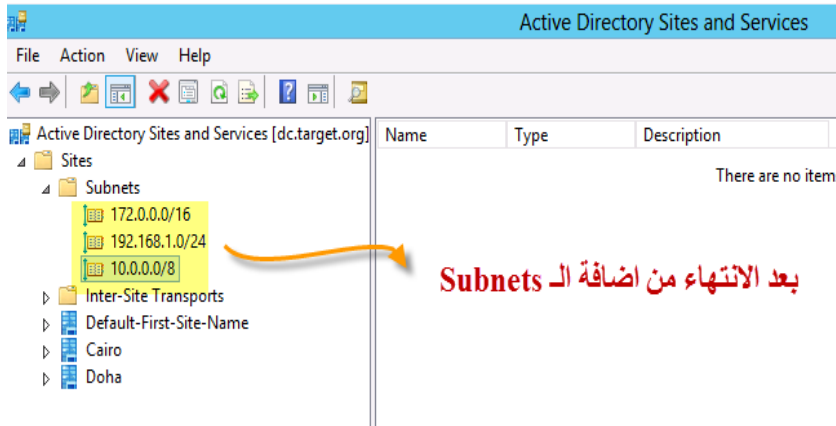
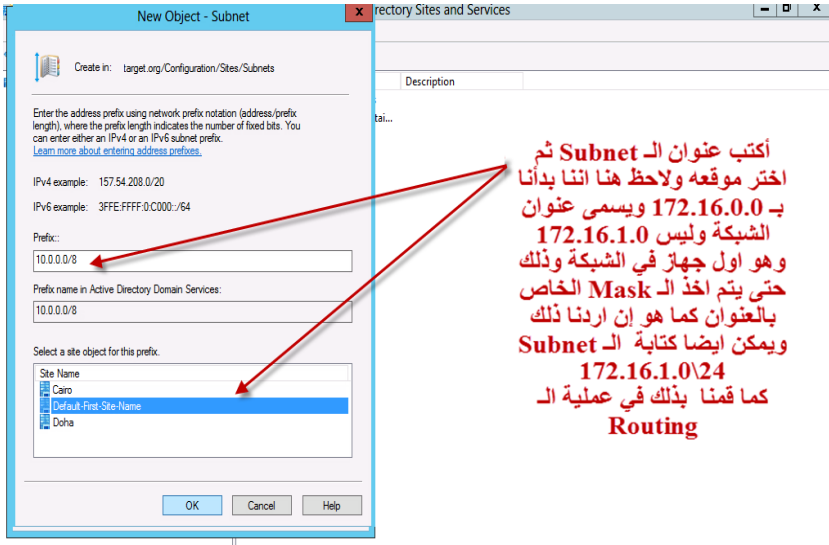
الآن قد انتهينا من خطوات اعداد ال router في الفروع كما سبق في الشرح ونأتي الان لمرحلة انضمام الاجهزة تحت المجال الرئيسي (Join Domain) لكننا قبل هذه الخطوة هناك خطوتين مهمتين فها بنا نقوم بهما معا :-

الخطوة الاولى قبل
اي شيء هو وضع
عنوان DNS
للمركز الرئيسي



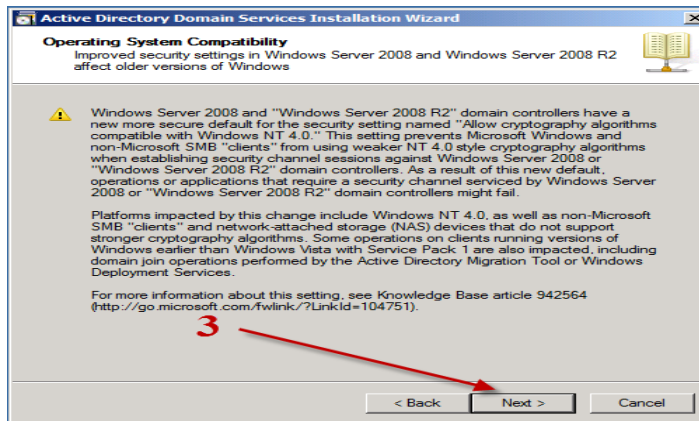
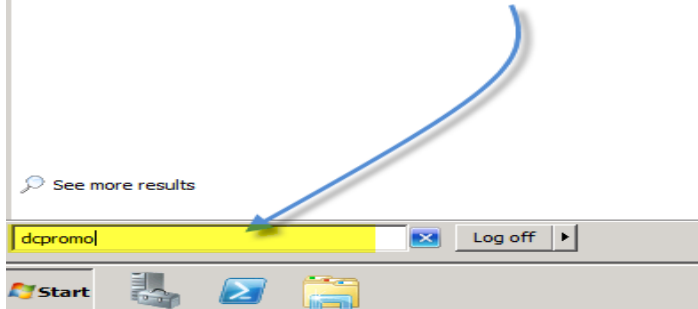
الخطوة الثانية تتم من داخل AD Sites and Services الذي سنتعرض له بعض الشرح لاحقا

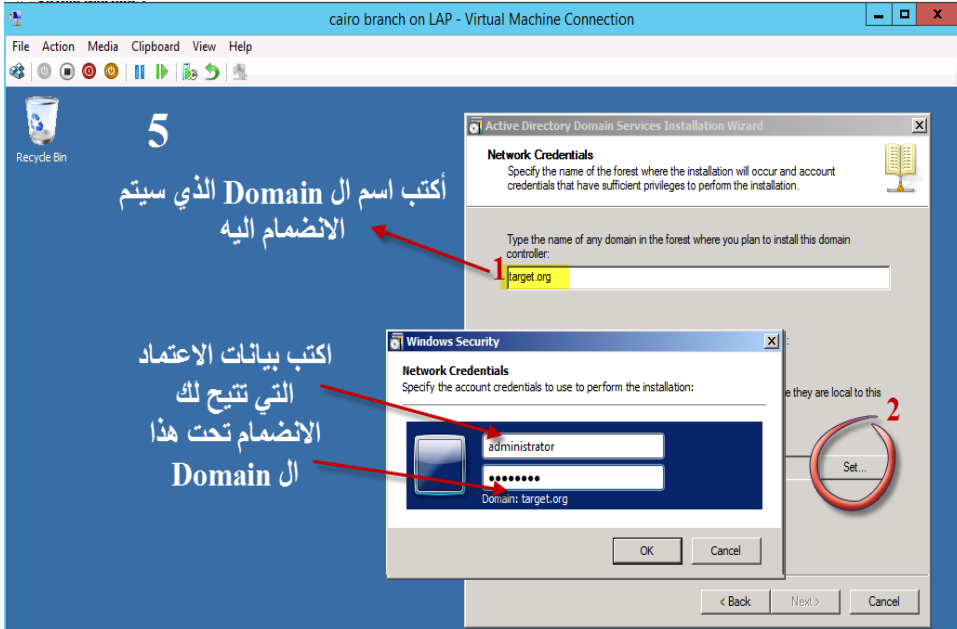
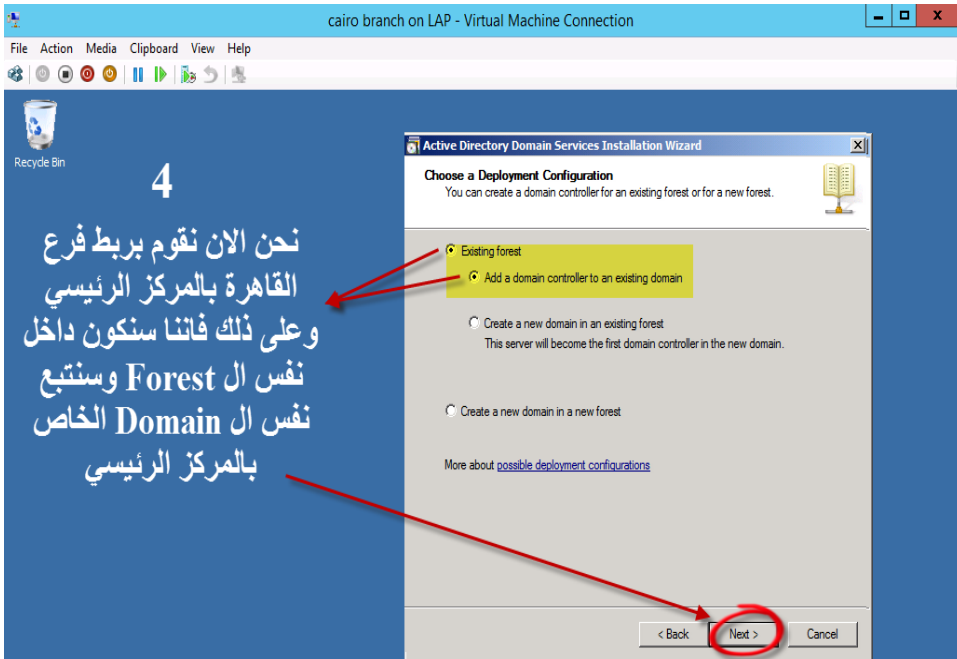


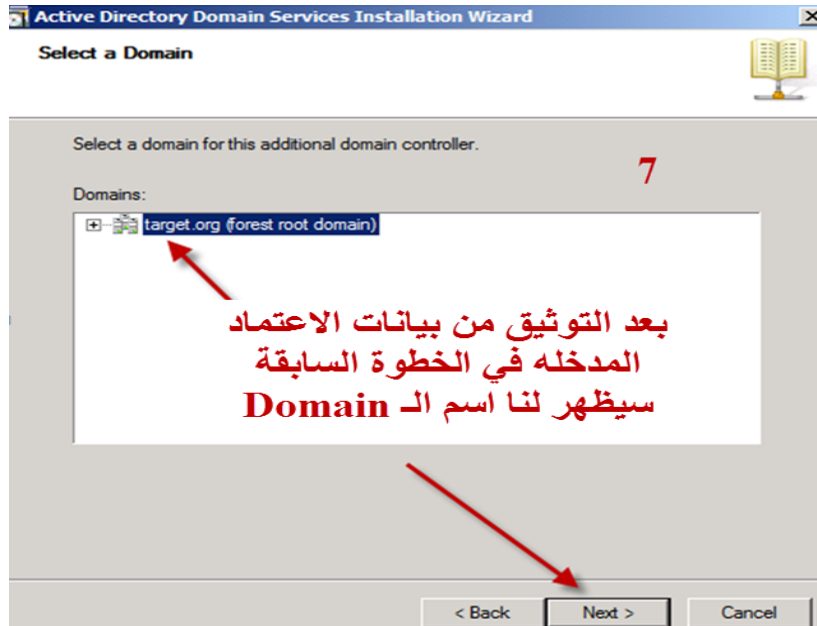
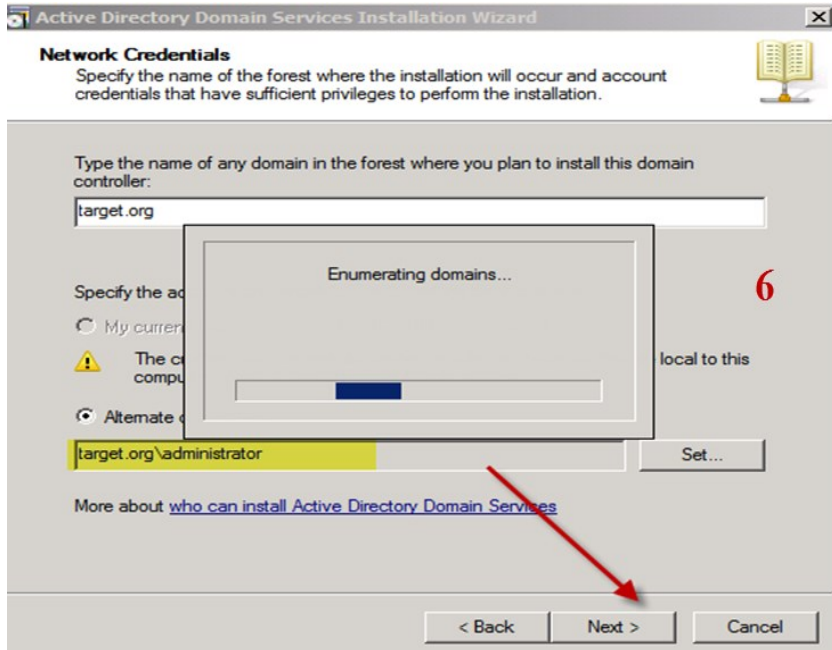


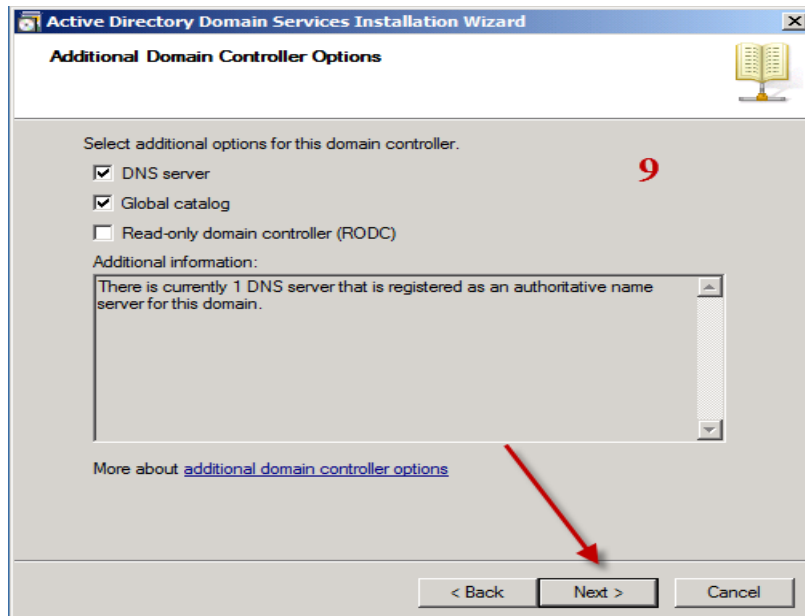
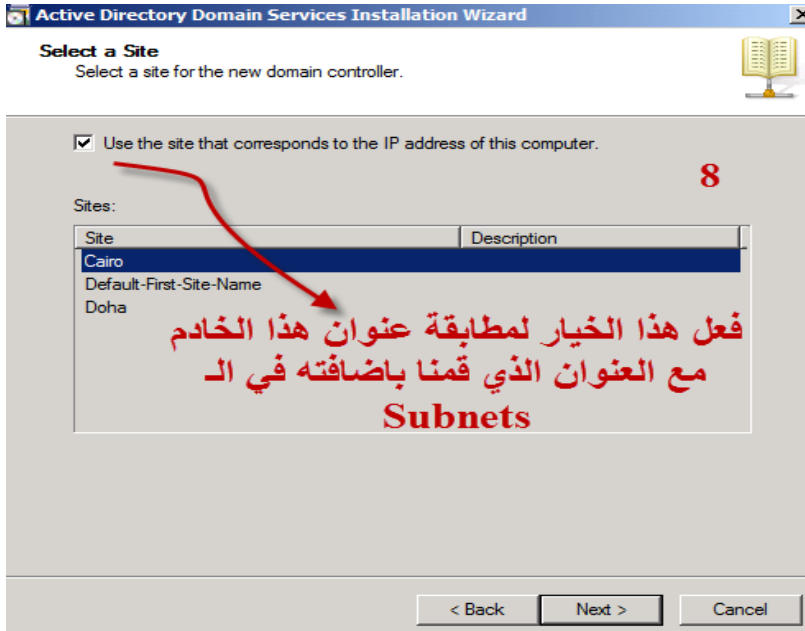
تابع معي الخطوات القادمة حيث سنقوم بالذهاب الى الخوادم الموجودة في الفروع ونبدأ معا ضبط الاعدادات الخاصة بتثبيت Active Directory وسنقوم بذلك اولاً مع فرع القاهرة باستخدام الوضع العادي فتابع معي:-

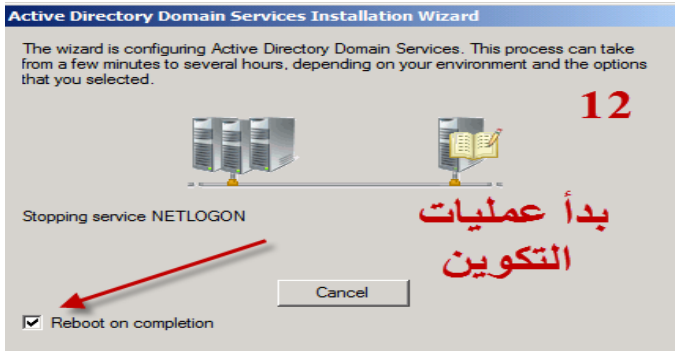
قم بتشغيل معالج تثبيت Active Directory 1

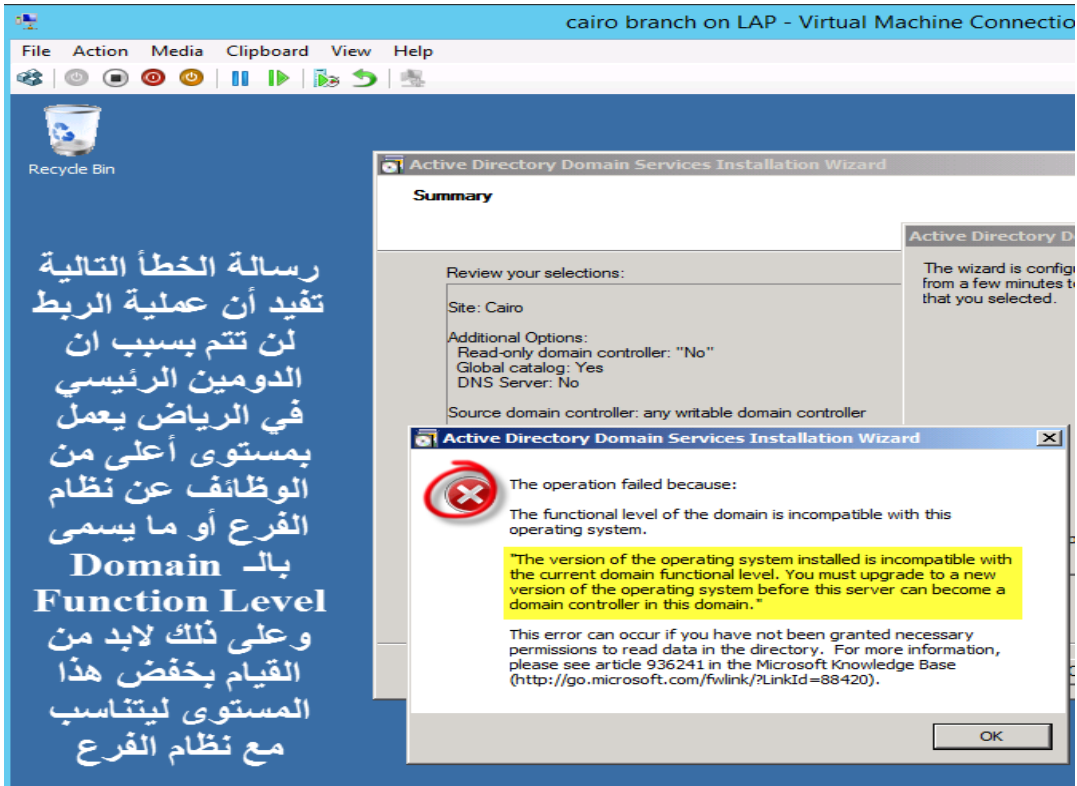












رسالة الخطأ التالية
تفيد أن عملية الربط
لن تتم بسبب ان
الدومين الرئيسي
في الرياض يعمل
بمستوى أعلى من
الوظائف عن نظام
الفرع أو ما يسمى
بالـ **Domain
Function Level**
وعلى ذلك لابد من
القيام بخفض هذا
المستوى ليتناسب
مع نظام الفرع

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

```
Administrator: Windows PowerShell
PS C:\> Import-Module -Name ActiveDirectory

Loading Active Directory module for Windows PowerShell with default drive 'AD:'
[ooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo] ]
```

1

افتح الـ Power Shell ثم قم بكتابة الامر كما تراه في الصورة واضغط مفتاح الادخال وسيظهر لك السطر باللون الاخضر

```
Administrator: Windows PowerShell
PS C:\> Import-Module -Name ActiveDirectory
PS C:\>
PS C:\> Get-ADForest | Format-Table Name , ForestMode
```

Name	ForestMode
target.org	Windows2012Forest

2

اكتب الامر الظاهر امامك للحصول على معلومات الـ Function Level

تم الحصول على معلومات الـ Function Level بعد إدخال الامر السابق

```
Administrator: Windows PowerShell
PS C:\> Import-Module -Name ActiveDirectory
PS C:\>
PS C:\> Get-ADForest | Format-Table Name , ForestMode
```

Name	ForestMode
target.org	Windows2012Forest

```
PS C:\> Set-ADForestMode -Identity "target.org" -ForestMode Windows2008Forest

Confirm
Are you sure you want to perform this action?
Performing operation "Set" on Target "CN=Partitions,CN=Configuration,DC=target,DC=org".
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "Y"): y_
```

3

لتغيير الـ Function Level الى بيئة 2008 قم بكتابة هذا الكود مع مراعاة استبدال اسم الدومين الخاص بك بدلا من المكتوب بين الاقواس ثم بعد الادخال قم بالموافقة على رساله التأكيد بالضغط على Y

```

Administrator: Windows PowerShell
PS C:\> Set-ADDomainMode -identity target.org -DomainMode Windows2008R2Domain
Confirm
Are you sure you want to perform this action?
Performing operation "Set" on Target "DC=target,DC=org".
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "Y"): y
PS C:\>

```

Domain باستخدام الكود وبنفس الطريقة قم بخفض مستوى الـ 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**

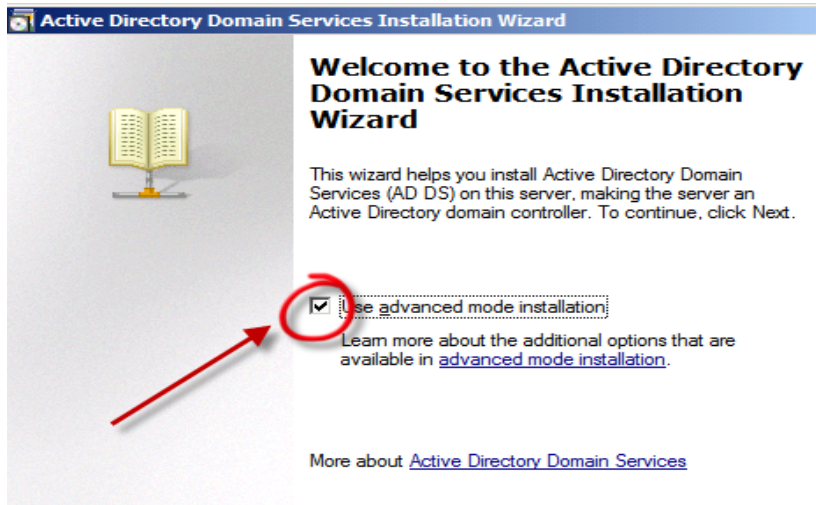
لا تنسى استبدال الكلمات باللون الاحمر باسم Domain/ forest الخاص بك وبالمستوى الذي تود الانتقال اليه .

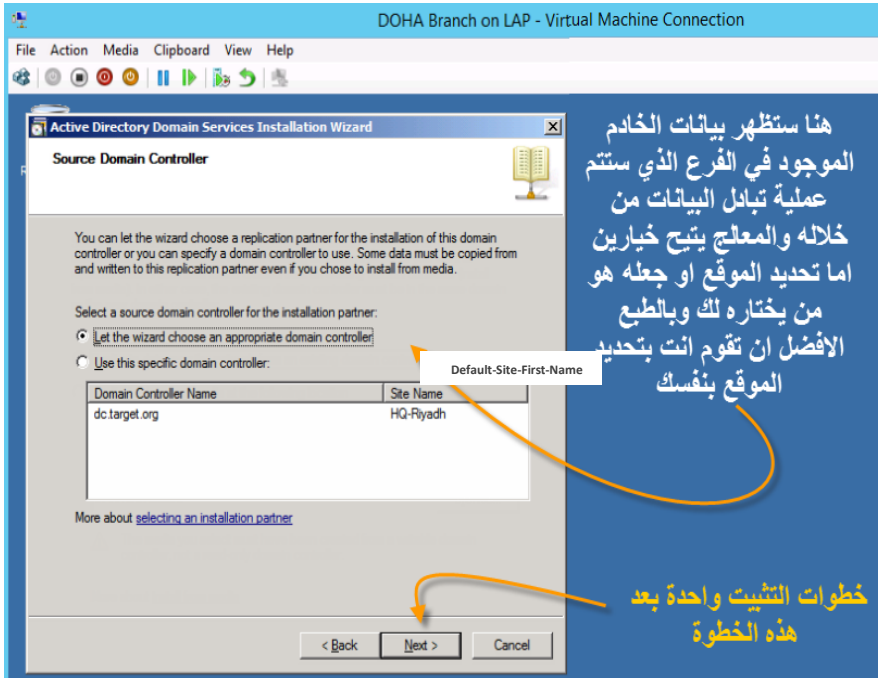
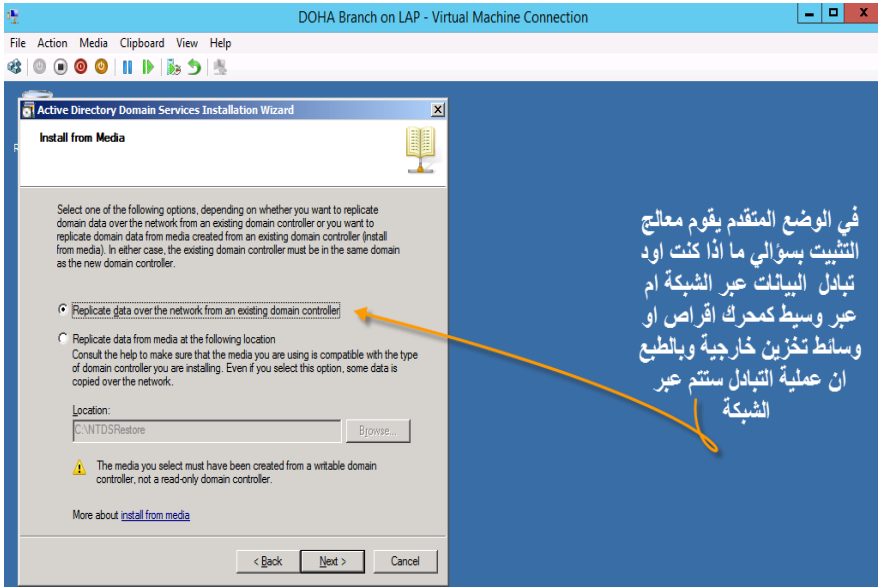
بعد ذلك نتابع تثبيت Active Directory في أجهزة الفروع بدون مشاكل

System		
Processor:	Intel(R) Xeon(R) CPU	E5630 @ 2.53GHz 2.53 GHz
Installed memory (RAM):	512 MB	(512 MB usable)
System type:	64-bit Operating System	
Pen and Touch:	No Pen or Touch Input is available for this Display	
Computer name, domain, and workgroup settings		
Computer name:	CAIRO-BRANCH	
Full computer name:	CAIRO-BRANCH.target.org	
Computer description:		
Domain:	target.org	
Windows activation		
Windows is activated:	Yes	
Product ID:	00486-OEM-8400691-20006	

اصبح فرع القاهرة الان ضمن
نطاق Target.org

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





الآن انتهينا من ربط كلا الفرعين **بنفس المجال** وهذا يعني أننا قمنا بعمل **Additional Domain** وهو صورة طبق الاصل من الـ **Primary Domain** الموجود في المركز الرئيسي وحتى يكون صورة طبق الاصل كما قلنا لا بد من ان يحصل على كل المعلومات من الـ **Primary Domain** وهذا ما يسمى بعملية 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 القاهرة 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 وهذه العملية تسمى **INTER Site Replication** ويستخدم فيها بروتوكول **MSTP or RPC**

أما إذا 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 الآن متصلة بالمركز الرئيسي وقبل البدء بإدارتها وضبط الإعدادات الخاصة بعملية الـ **Replication** دعونا نلقي نظرة على شكل الـ **Active Directory Sites and Services** وشرح الافتراضيات التي سنعمل عليها لاحقاً .

Active Directory Sites and Services

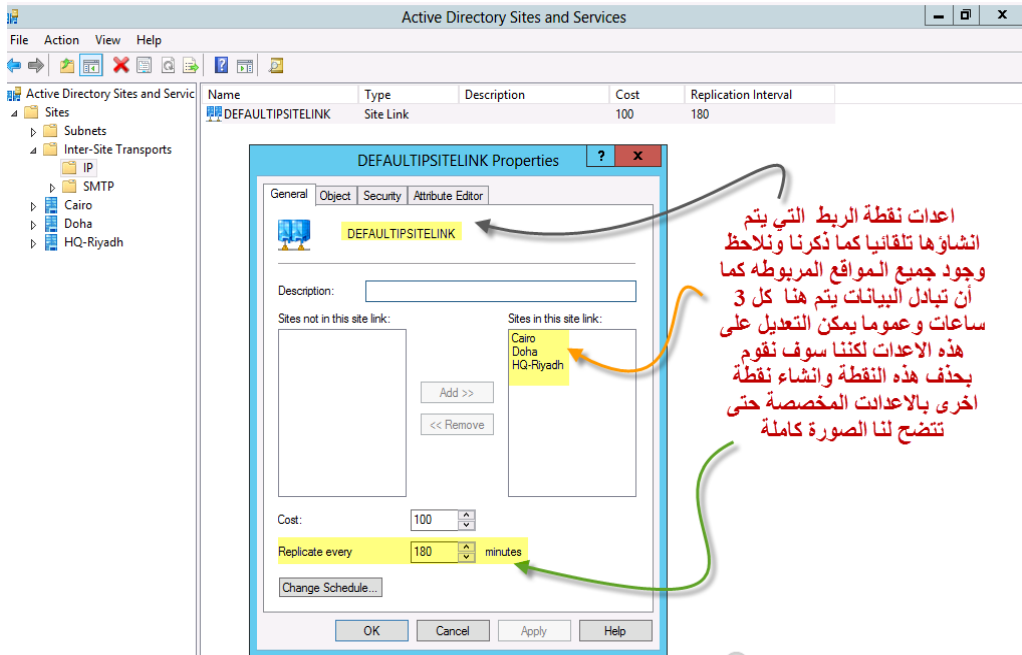
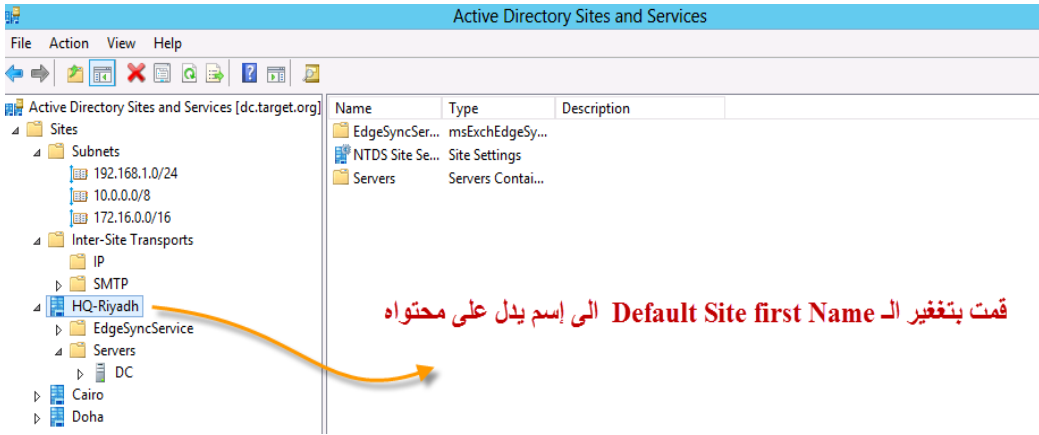
Name	Type	Description	Cost	Replication Interval
3	Site Link		100	180

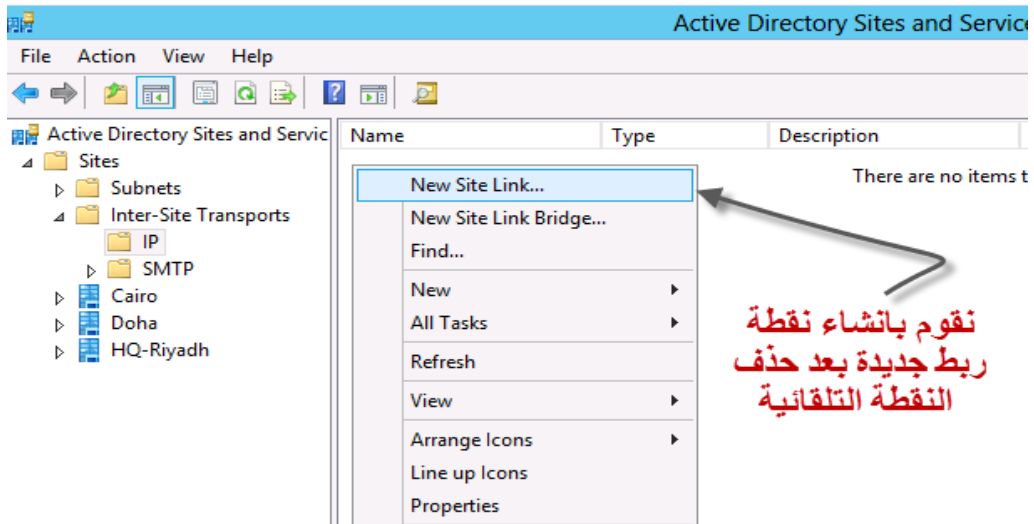
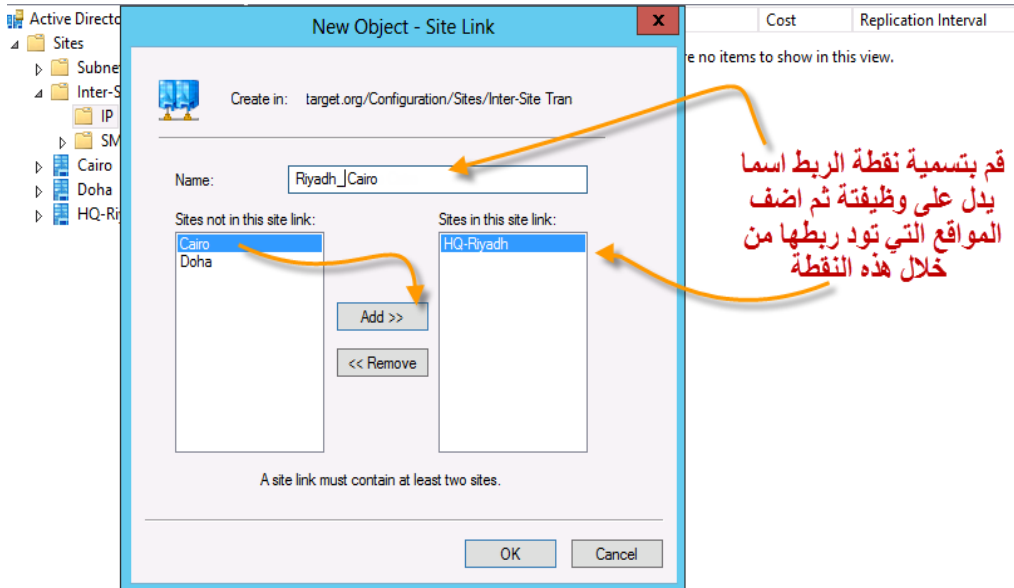
1 - قائمة الـ **Subnets** للفروع

2 - نوع الـ **Replication** والبروتوكول المستخدم

3 - نقطة ربط يتم إنشاؤها تلقائياً بإعدادات افتراضية وتحوى كافة الفروع معا

4 - أسماء الـ **Sites** وما تحتويه من **Servers** ونلاحظ ان اسم المركز الرئيسي الافتراضي هو **Default - First- site- Name** ويفضل تغيير اسمه لاسم يدل على محتواه





الآن 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 إلى 4 فجرا ومن 11 إلى 12

بإمكانك تخصيص الفترة الزمنية بين كل عملية تبادل وأخرى وذلك من 15 دقيقة إلى 10080 كحد أقصى

قيمة الـ **cost** تقاس وفق معادلة حسابية كالتالي

1024 ÷ line speed (Log)

بمعنى انه لو سرعة خط الربط هي 1.5 ميجا إذا

1024 ÷ (1.5mb) Log

أي

1024 ÷ (1536kb) Log = 340

وعلى ذلك فإن قيمة الـ **Cost** تكون هي الناتج أي 321 وهكذا والفائدة منه هو اختيار اقصر الطرق لاجراء عملية الـ **Replication**

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

Name	Type	Description	Cost	Replication Interval
Riyadh_Cairo	Site Link		100	15
Riyadh-Doha	Site Link		321	180


الان تم ربط فرع القاهرة وفرع الدوحة بالمركز الرئيسي في الرياض أي اننا لو قمنا بإضافة مستخدم جديد في فرع القاهرة فسوف يظهر في الـ **Active Directory** الموجود في الرياض والعكس صحيح أيضا وبالتالي طالما انه سيظهر في الرياض عن طريق القاهرة فحنما سوف يسجل ايضا في الدوحة عن طريق الرياض وهكذا أي أن الرياض هي المحطة بين الدوحة والقاهرة

والسؤال الان ماذا لو فقدنا الاتصال بالرياض ؟

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 وكان شينا لم يكمن .

حسنا عليك الان ان تقوم بعمل ذلك بنفسك .



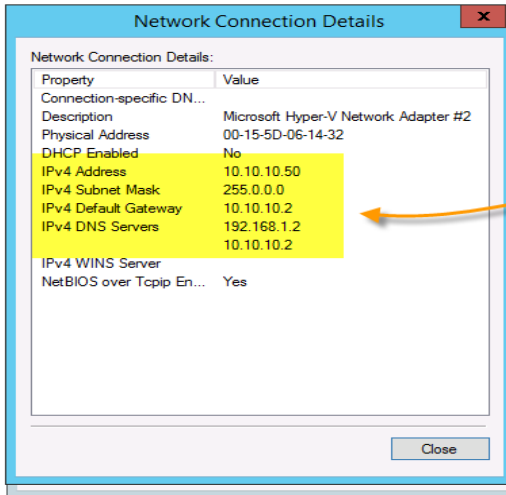
Active Directory Sites and Services [dc.target.org]

Name	Type	Description	Cost	Replication Interval
Cairo - Doha	Site Link		100	180
Riyadh - Cairo	Site Link		340	15
Riyadh - Doha	Site Link		321	30

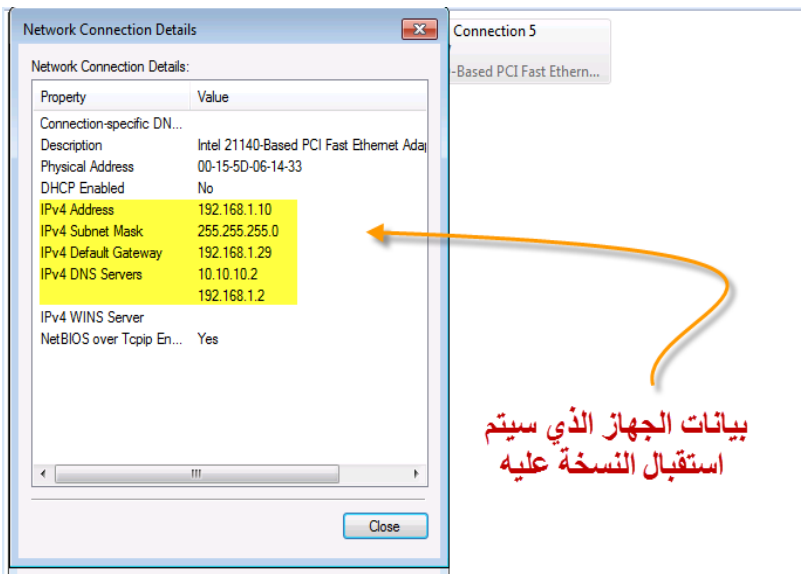
انتهينا الان من عمل Site link للفروع كما يظهر وبذلك تكون جميع المواقع الان بينهما Replication ويمكن التواصل مع بعضهم البعض عن طريق الـ IP لوجود Routing بينهم

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

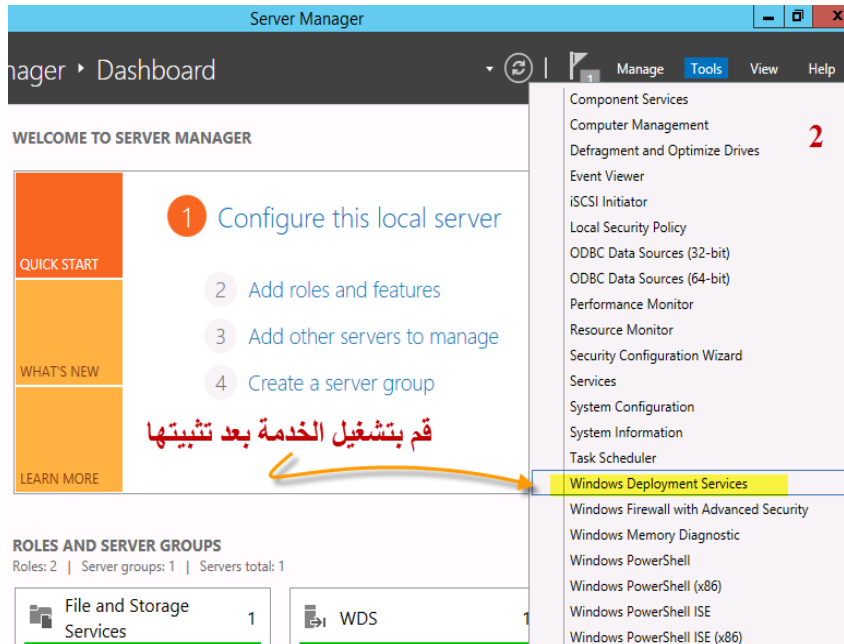
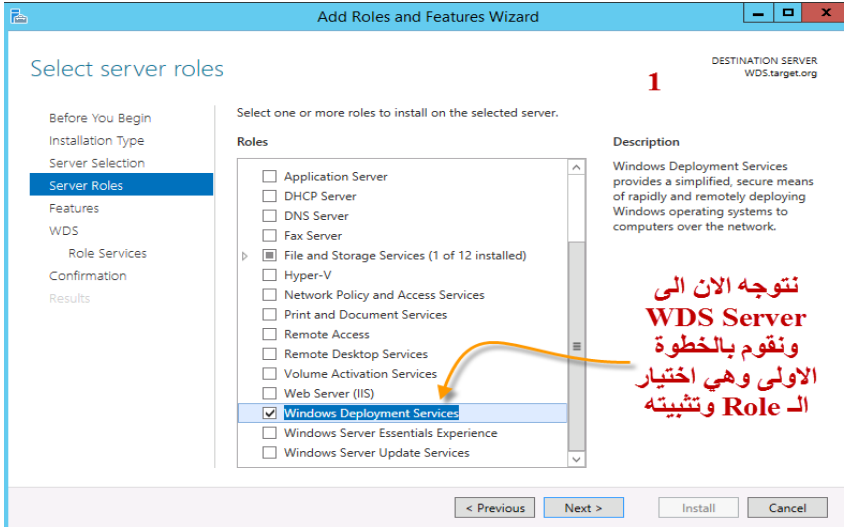


بيانات الـ
WDS Server

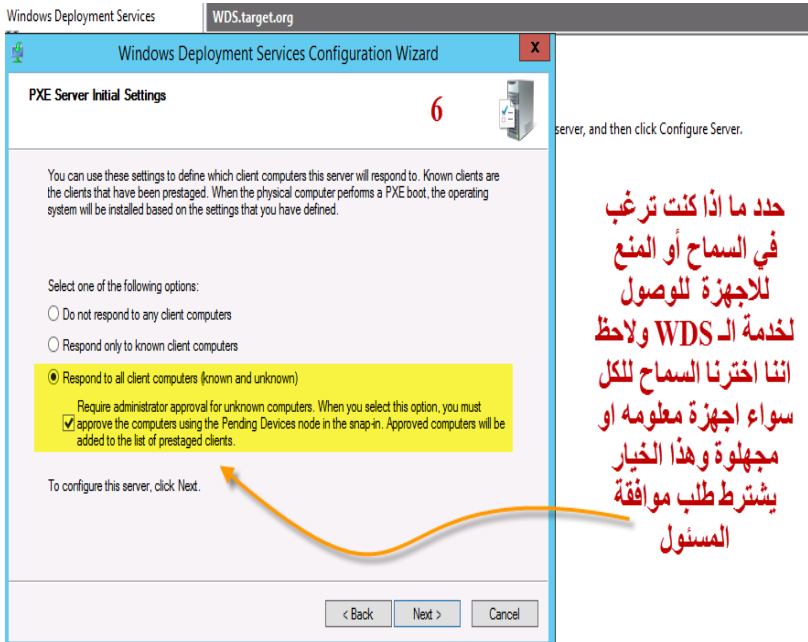


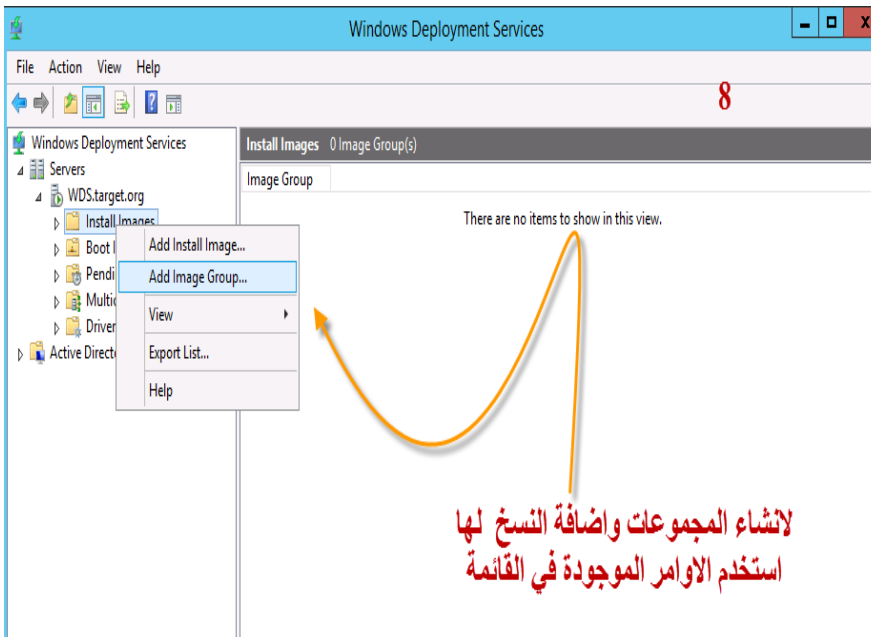
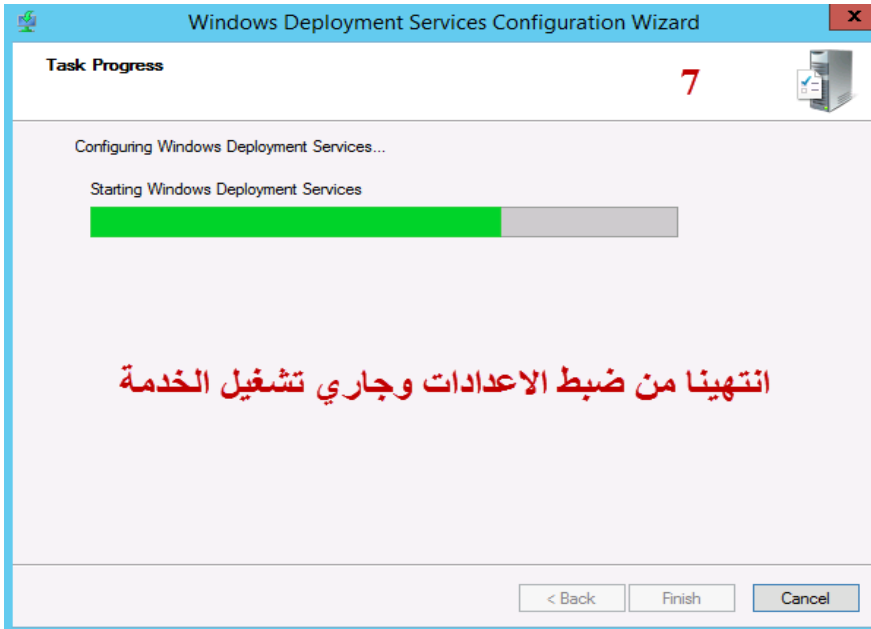
بيانات الجهاز الذي سيتم
استقبال النسخة عليه

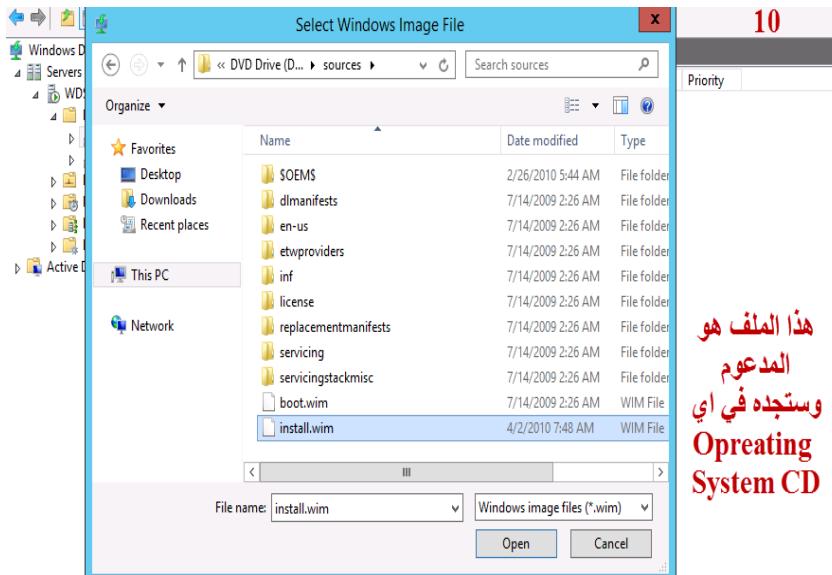
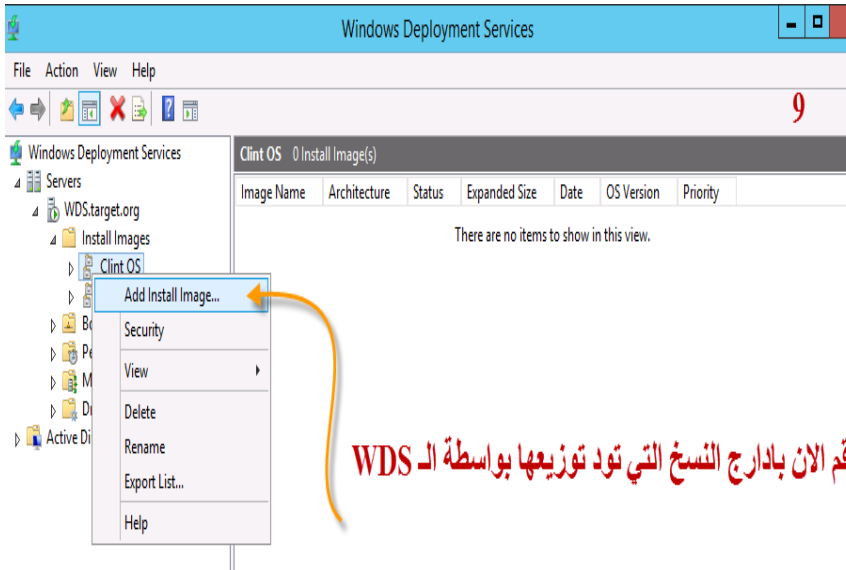
من البيانات السابقة علمنا ان خادم الـ WDS موجود في الرياض وان جهاز المستخدم موجود في الدوحة كما يظهر ذلك من ارقام الـ IP والآن لنفترض ان حالة من سقوط النظام حدثت على هذا الجهاز وبالتالي فانه لا بد من اعادة تثبيت نظام التشغيل عليه وسنقوم بذلك من خلال خادم الـ WDS الموجود في الرياض فتابع معي .

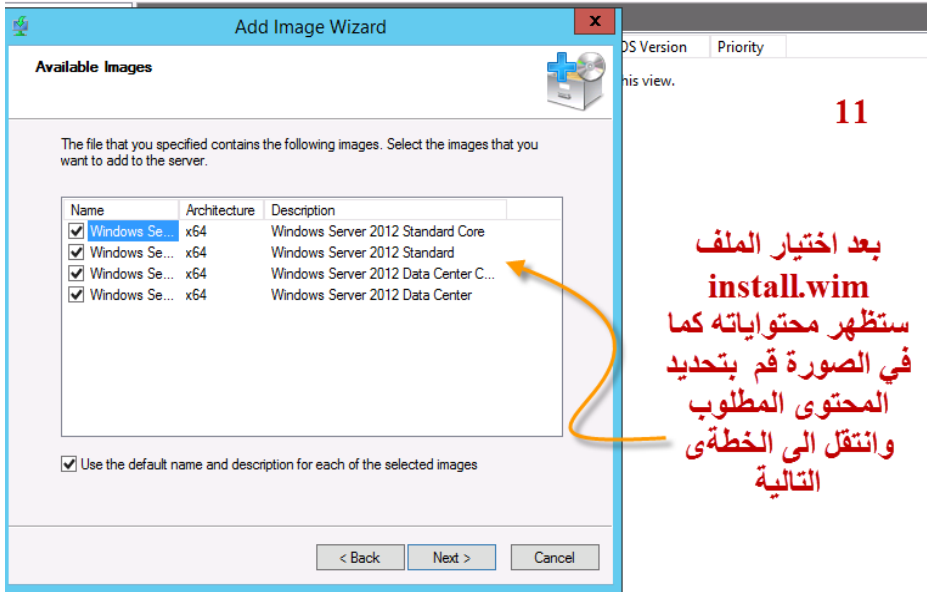






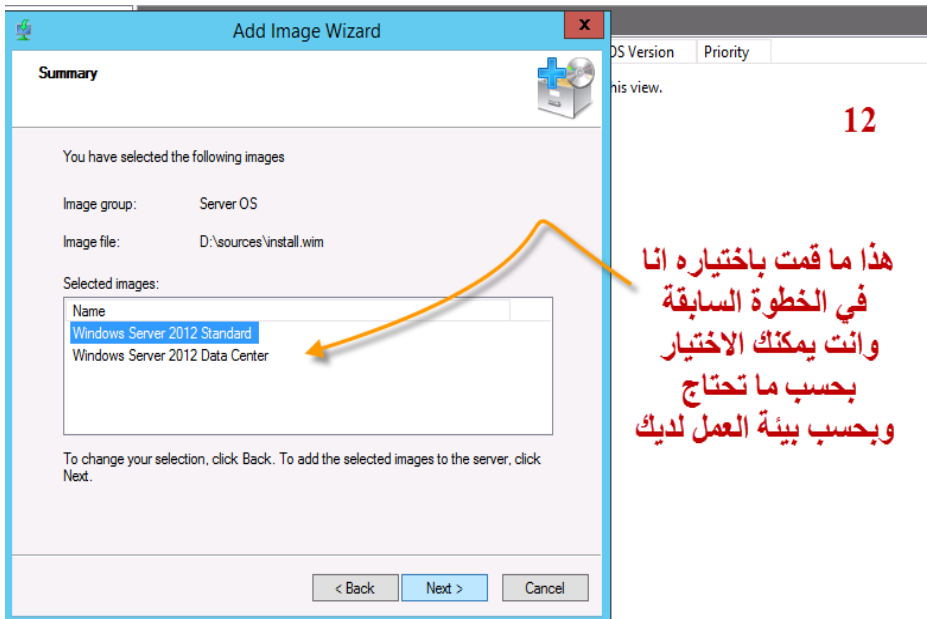






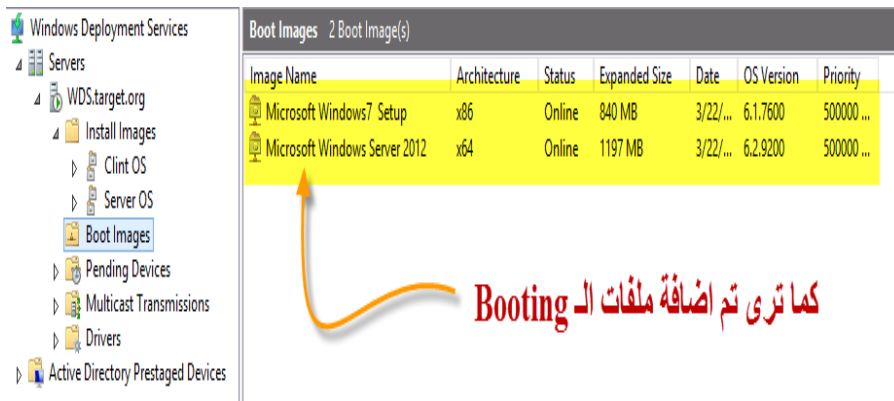
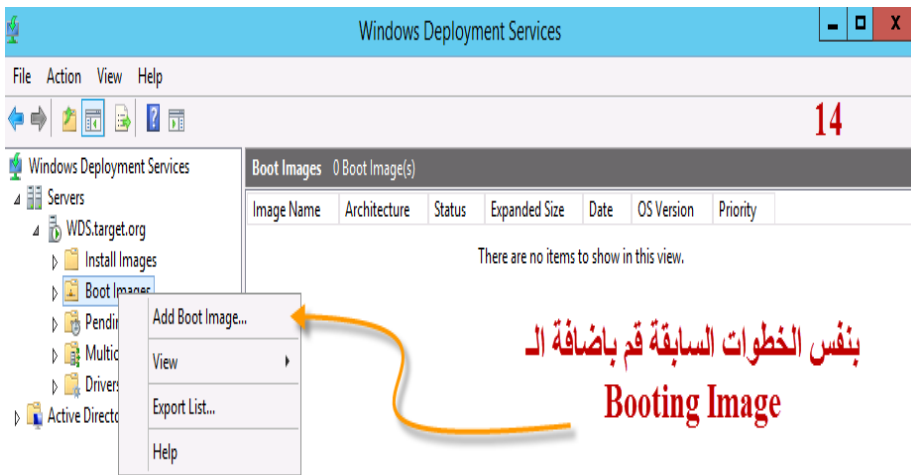
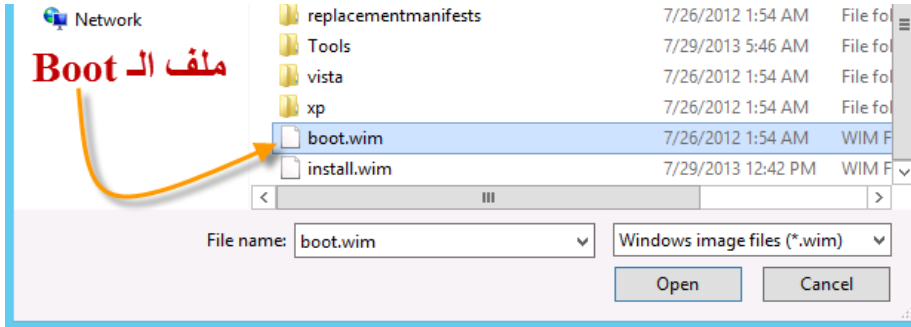
11

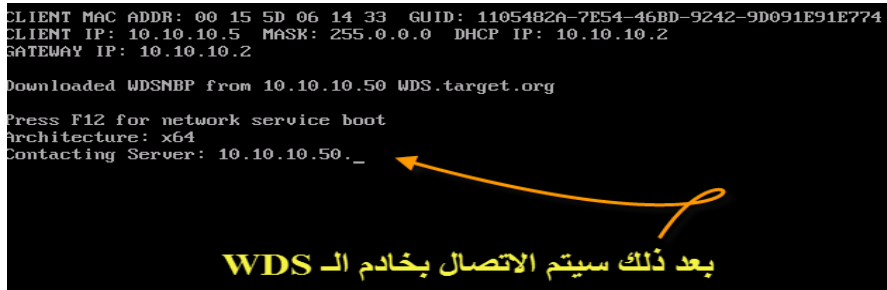
بعد اختيار الملف
install.wim
ستظهر محتوياته كما
في الصورة قم بتحديد
المحتوى المطلوب
وانتقل الى الخطوة
التالية



12

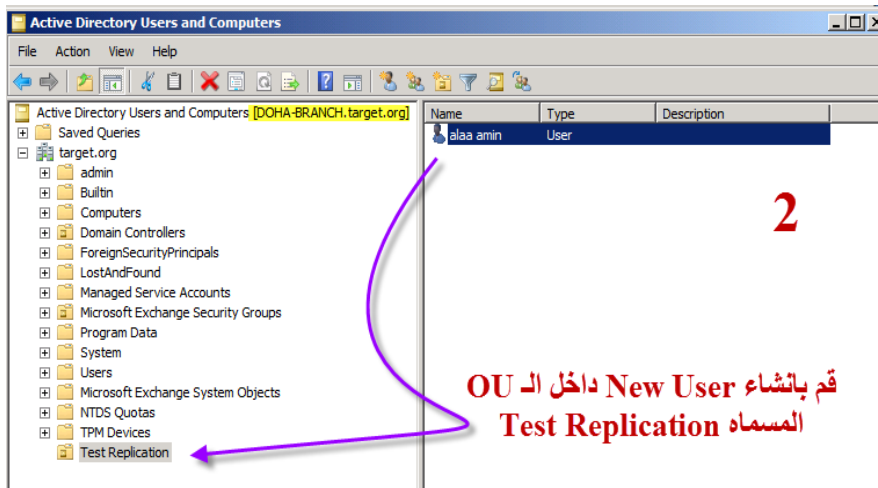
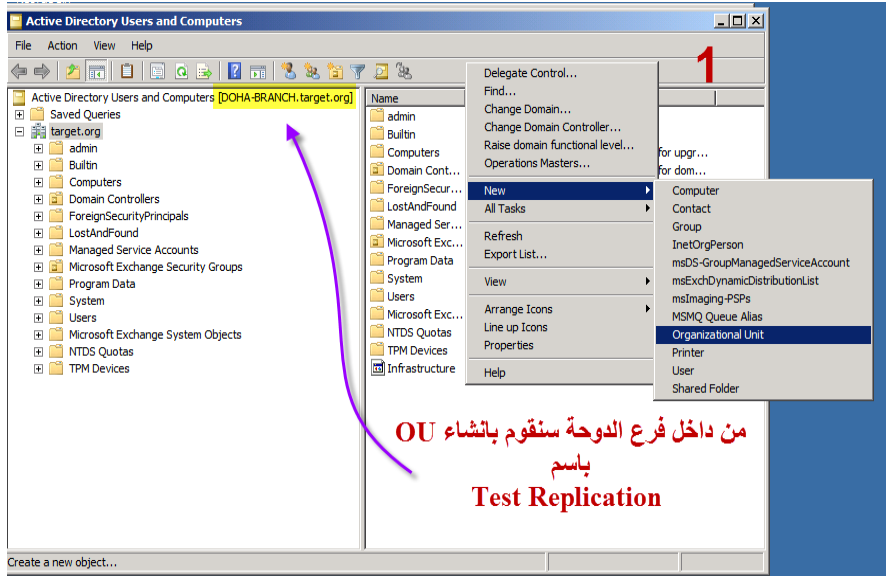
هذا ما قمت باختياره انا
في الخطوة السابقة
وانت يمكنك الاختيار
بحسب ما تحتاج
وبحسب بيئة العمل لديك

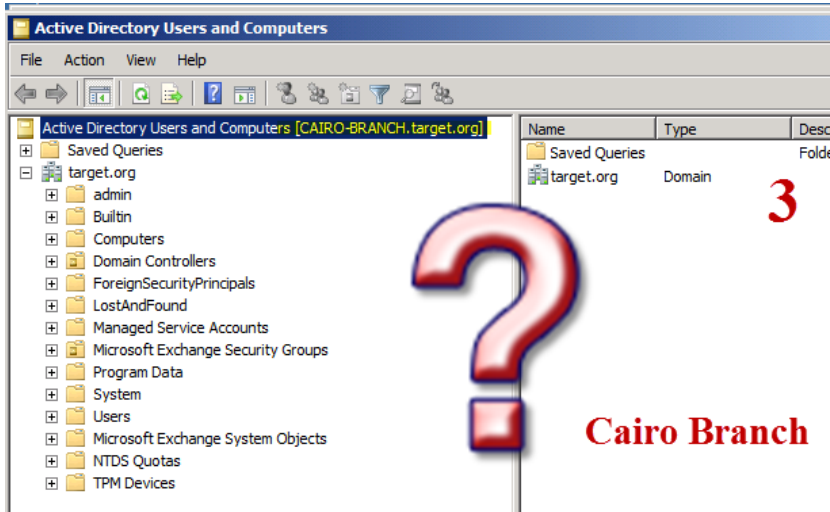




والآن بعد التأكد من اتصال الفروع بشكل تام دعونا نقوم بعملية اختبار للـ

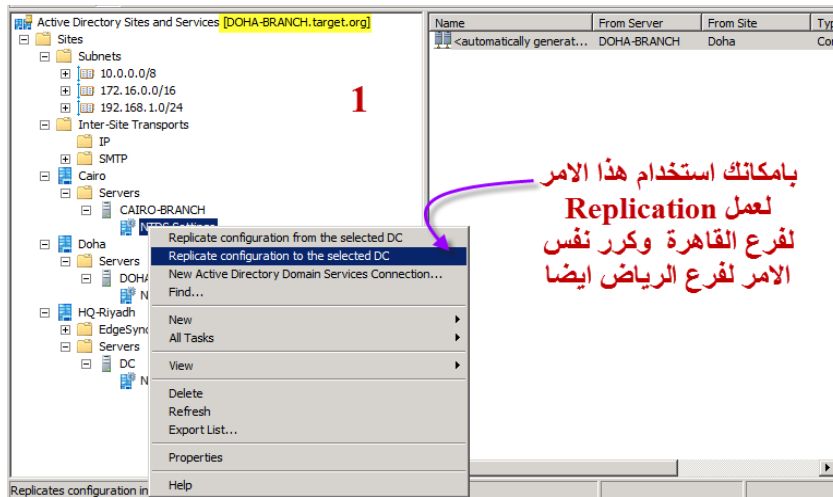
Replication

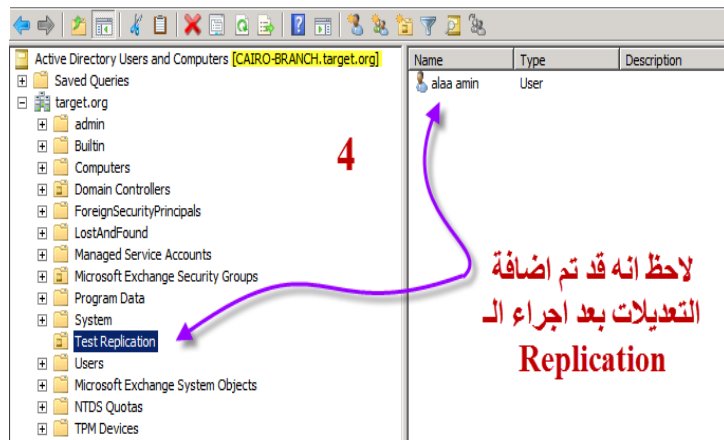
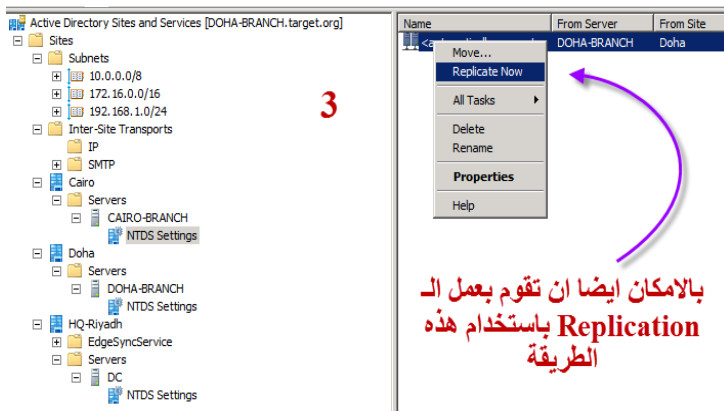
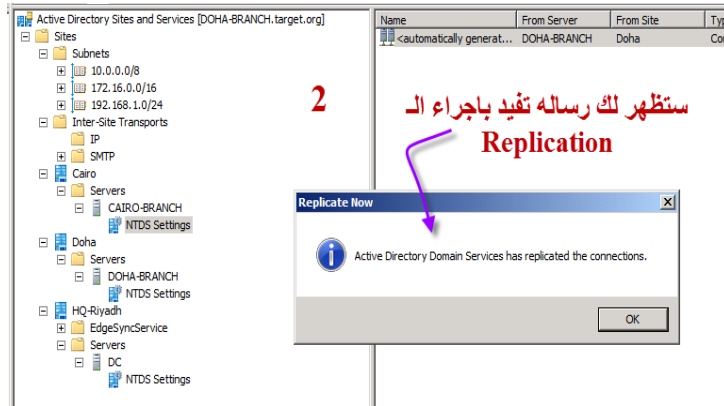




من المفترض ان تظهر التعديلات التي قمنا بها من فرع الدوحة في كلا من القاهرة والرياض لكنها لم تظهر والسبب في ذلك هو انه لم يأتي وقت إجراء الـ **Replication** الذي تم تحديده اثناء عمل الـ **Site link** بين كلا من الدوحة والقاهرة والدوحة والرياض .

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





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 ال **Site Link Bridge** وهو الذي يربط بين موقعين أو أكثر .

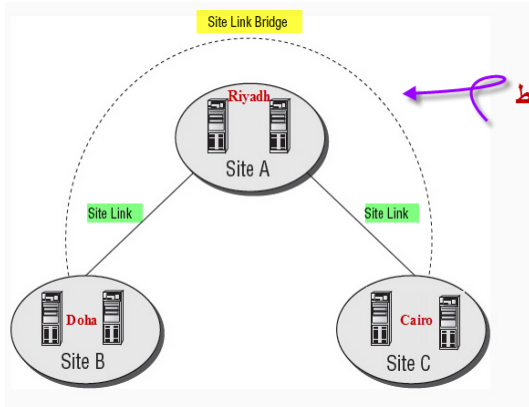
وحتى يتضح الامر أنظر جيدا الى هذا الشكل

Name	Type	Description	Cost	Replication Interval
Cairo-Doha	Site Link		380	30
Riyadh-Doha	Site Link		321	180
Riyadh_ Cairo	Site Link		100	15

Replication Sites

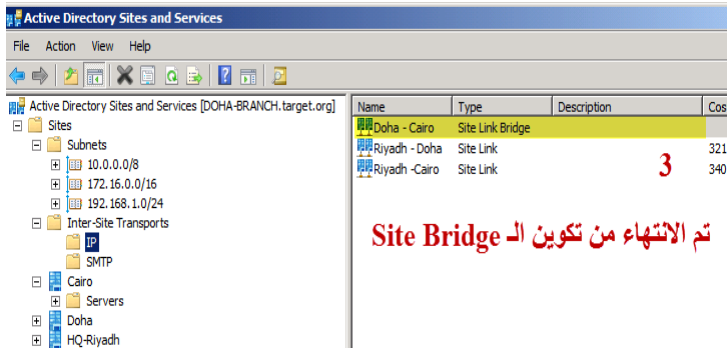
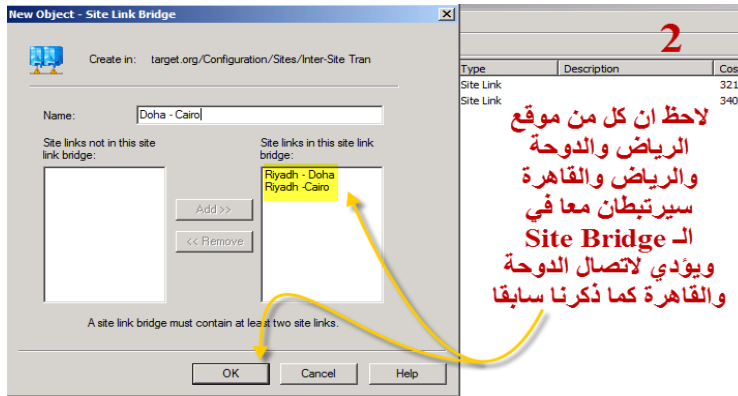
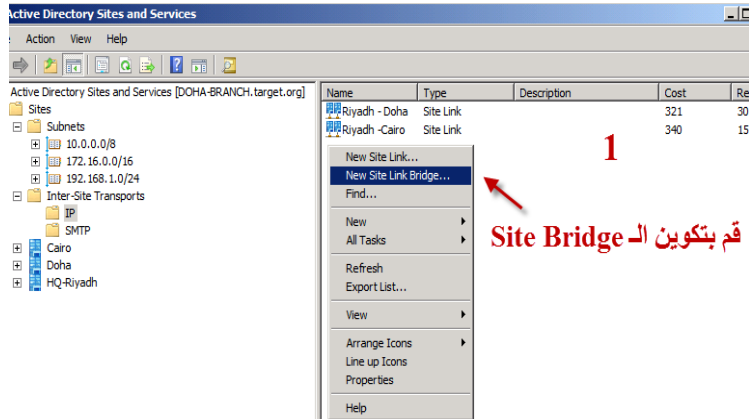
هل تعتقد انه يمكن عمل **Replication** لموقع **C** بطريقة اخرى ؟

للإجابة على هذا السؤال انظر الرسم التالي :-



لاحظنا 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 وستوجب أيضا على فرع الدوحة انتظار عملية ال **Replication** في (Site A) ومن ثم الحصول على ال **Updates** في عملية ال **Replication** الخاصة بـ (Site B) .

أما في حالة استخدام ال **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

لا بد 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 ال **Domain** تسمى **Domain-Wide Operations Master Roles** وتسمى في المصادر **Flexible Single Master Operation (FSMO)** وتختصر الى

إن ال **Role** هو الدور أو الوظيفة أو المهمة التي يقوم بها المتحكم بالمجال **DC** في المجال أو ال **Domain ...**

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

هذه ال **Roles** 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

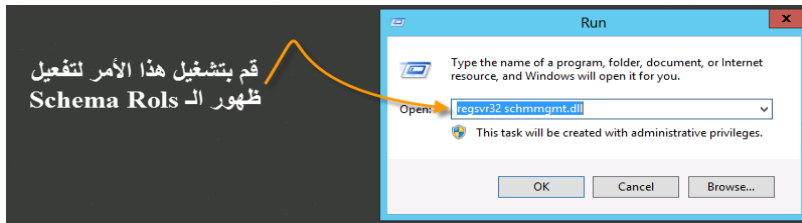
تقع على هذه ال **Role** مسنولية مراقبة ال **Domain Name** بحيث لا يمكن تكراره ابدا لا على مستوى ال **Forest** ولا مستوى ال **Tree** أيضا وكما قلنا هي في ال **Forest Level** وتحديدًا في أول **Domain** في ال **Forest** وبالتالي لو ان هذا ال **Parent Domain** أصبح خارج الخدمة لسبب ما فأنني لن استطيع اضافة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

Schema Master Role

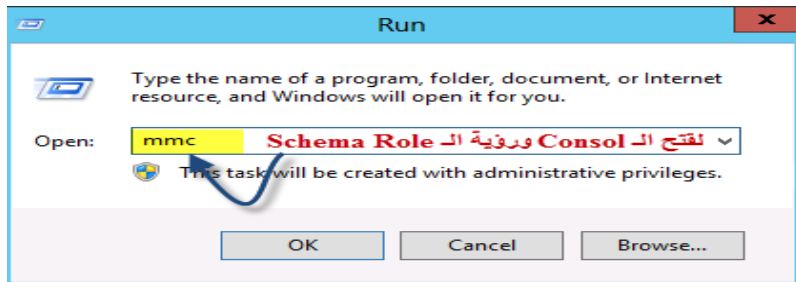
هذه ال **Role** لا تقل أهمية ابدا عن سابقتها فهي مسنولة عن كل ال **Classes** و ال **Attributes** أي على مستوى ال **Forest** ككل وبالتالي شأنها شأن ال **Domain naming Master Role** ففي حالة عدم وجودها لن استطيع مثلا القيام بتهيئة ال **Domain** لاستقبال أي تعديلات ولا تحديثات لأنها هي السجل لكل التحديثات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

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

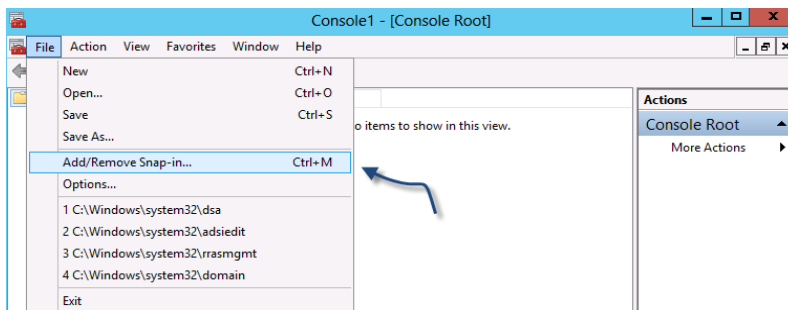
Start → run → regsvr32 schmmgmt.dll

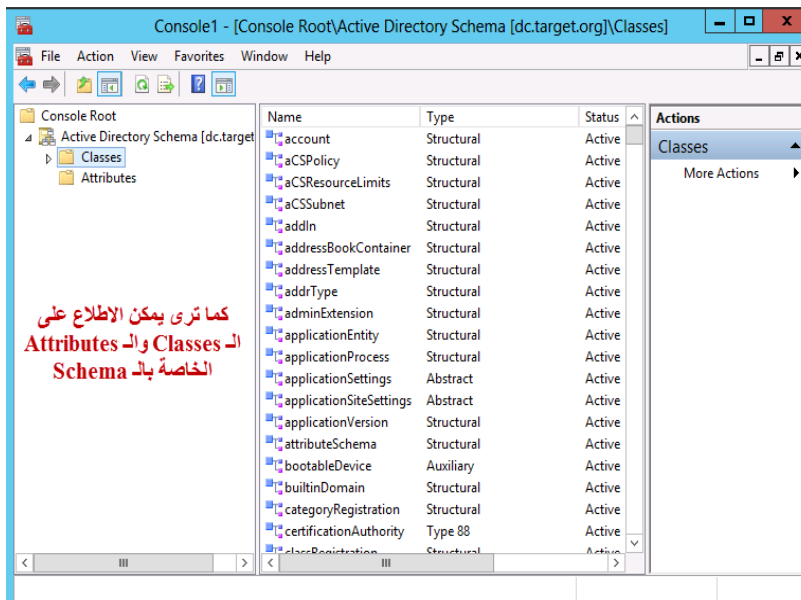
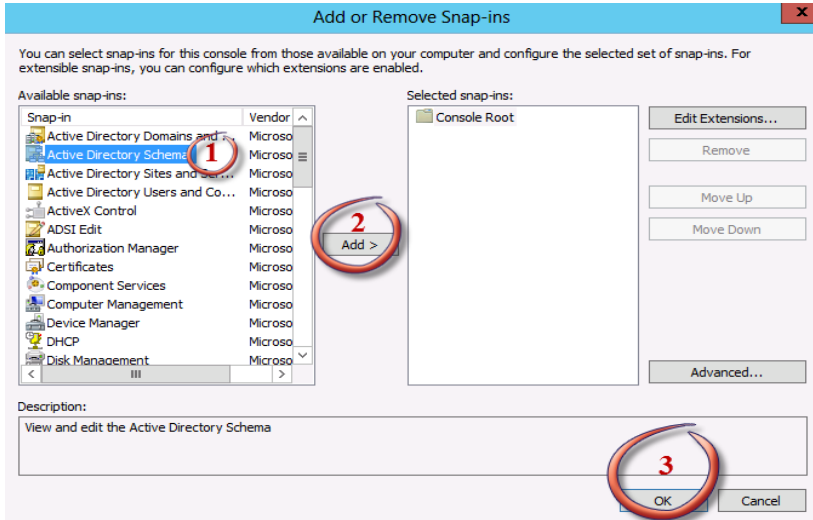


Start → run → mmc



From Consol → File → add/remove snap in



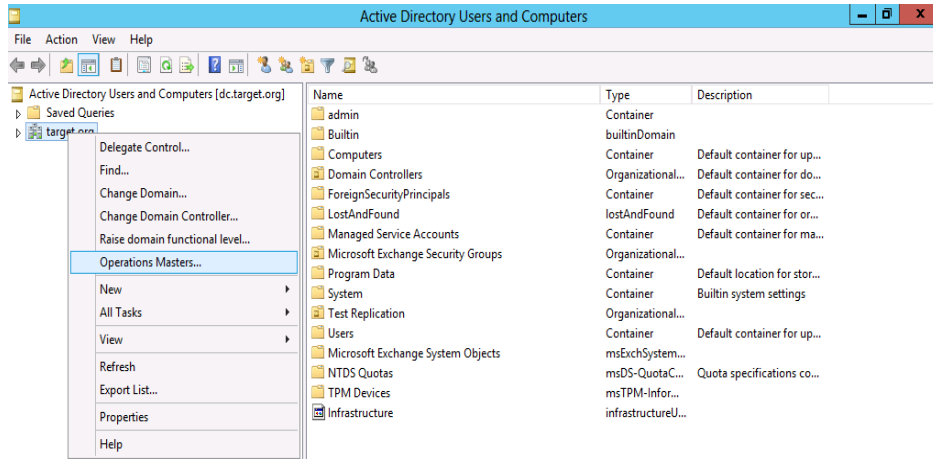


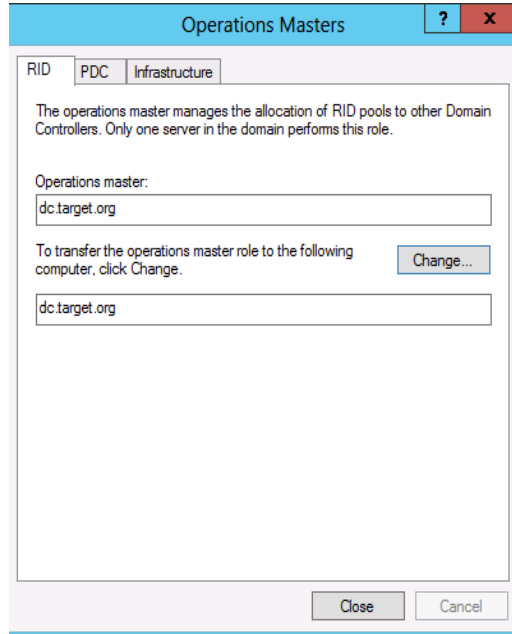
RID Master Role

عند عمل أي **Object** في الـ **AD** سواء كان مستخدم **user** أو مجموعة **group** أو حتى كمبيوتر **computer** ، فإن الـ **DC** الذي يقوم بمهمة الـ **RID Master** سيعطي لهذا الـ **Object** هوية أمنية **Security ID** خاصة به فمثلاً عند إضافة مستخدم في الـ **Active directory** فإنك تضع أسماً لهذا المستخدم وليكن **Alaa** لكن الـ **RID Master** يعطيه **ID** خاصة به وعادة تكون مثل **S-1-5-21-895771394-4047885310-268483753-1006....** ان 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 الـ **AD** أو ان الكمبيوتر مازال يحاول جلب اسم المستخدم وقد يأخذ ثواني قليلة لجلب البيانات وفي حالة د حذف مستخدم من الـ **AD** فإن إعادة انشاؤه بنفس خصائصه 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

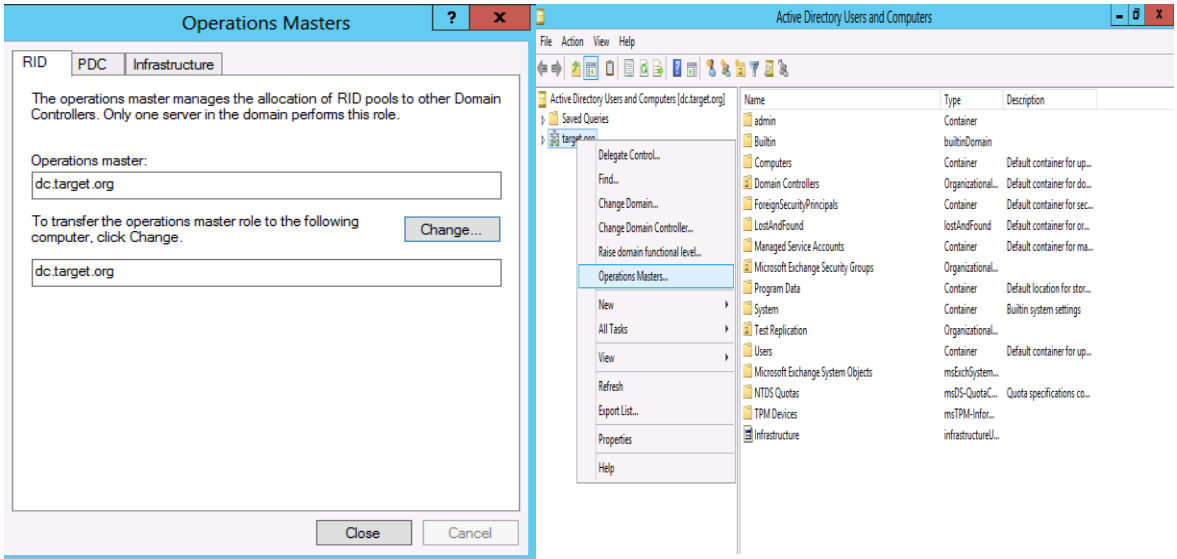




PDC Emulator Role

تقع على هذه الـ **Role** مسؤولية المزامنة بينه وبين الاجهزة **Synchronize** فمثلا لو تم تغيير الوقت والتاريخ الخاص بالـ **Domain** ستتغير في كل الـ **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 فإنها توجه له أيضاً وهو يقوم بإجراء اللازم كإظهار نافذة تعلم المستخدم بإدخاله كلمة سر خاطئة بمعنى انه يعد **Domain Browser** وكذلك تقع عليه مسؤولية الـ **Domain Group Policy**

ويمكن الاطلاع على هذه الـ **Role** بنفس خطوات الـ **RID Role**



Infrastructure Master Role

هذا الـ **Role** مسنول عن مصادقة الصلاحيات والتعديلات التي تتم على الـ **Objects** فإذا تم التعديل على صلاحية مستخدم ما مثلاً فإن الـ **Infrastructure Master** هو الذي يقوم بهذه الـ **Modification** ومن ثم تحديثها .

أيضاً 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 أبداً وبالتالي إذا حدثت مشكلة في هذا الجهاز أو حتى قررت شراء آخر بديل فلن يكون هناك إمكانية لإضافة **Child** أو **Tree** ولا حذف الموجود منهم ولن أستطيع كذلك عمل **Additional** إذا ما الحل ؟

الحل هو نقل هذه الـ **Rolls** من الجهاز القديم مثلاً 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 ؟

حسنًا سوف نعمل الآن على الاحتمال الاول وسنستخدم الـ Domain الذي تدريبنا 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 حقًا نجهل هذه المعلومة الاجابة ؟

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

Netdom query /d:(your domain name) pdc

Netdom query fsmo

```

Administrator: Command Prompt
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\administrator.TARGET>netdom query /d:target.org pdc
Primary domain controller for the domain:

dc.target.org
The command completed successfully.

C:\Users\administrator.TARGET>
  
```

من أي Domain Controller يمكن معرفة الـ Parent Domain باستخدام الامر netdom

```

Administrator: Command Prompt

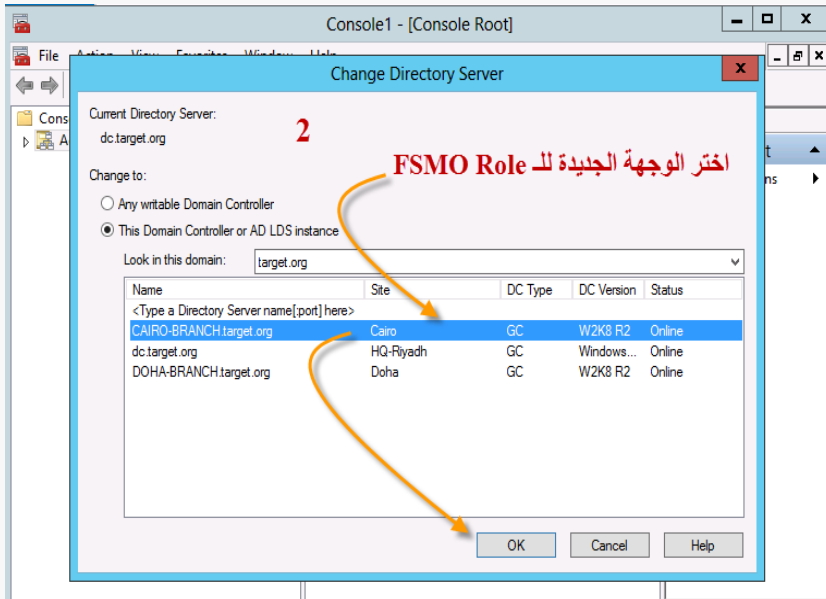
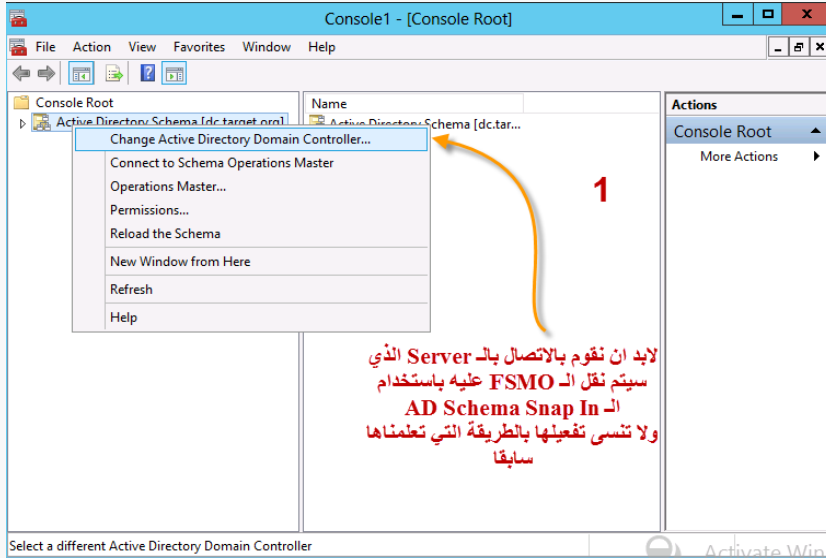
C:\Users\administrator.TARGET>netdom query fsmo
Schema master          dc.target.org
Domain naming master   dc.target.org
PDC                    dc.target.org
RID pool manager       dc.target.org
Infrastructure master  dc.target.org
The command completed successfully.

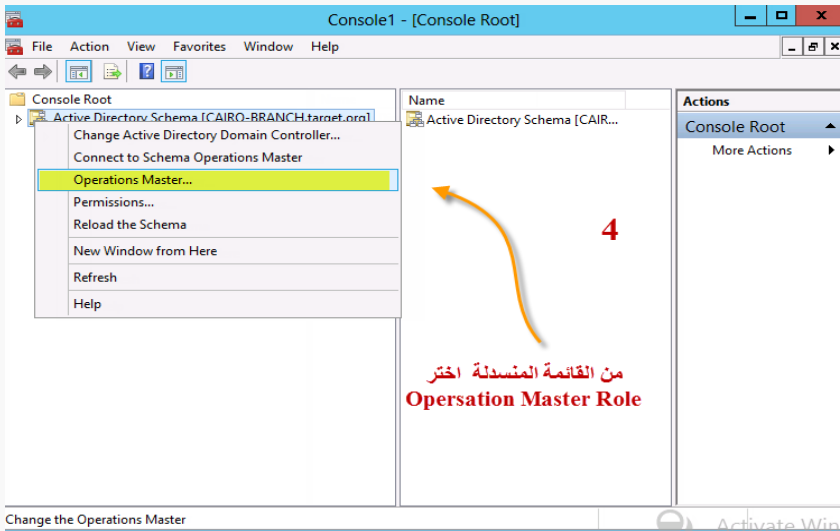
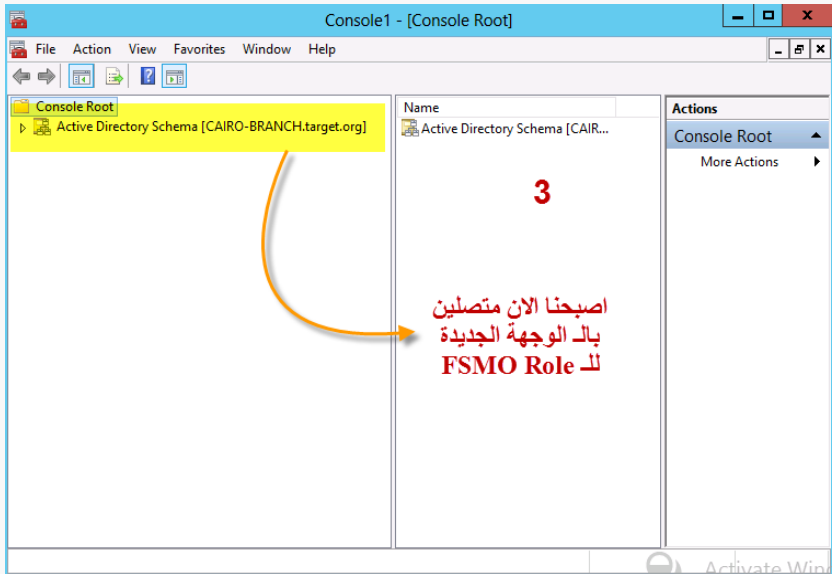
C:\Users\administrator.TARGET>
  
```

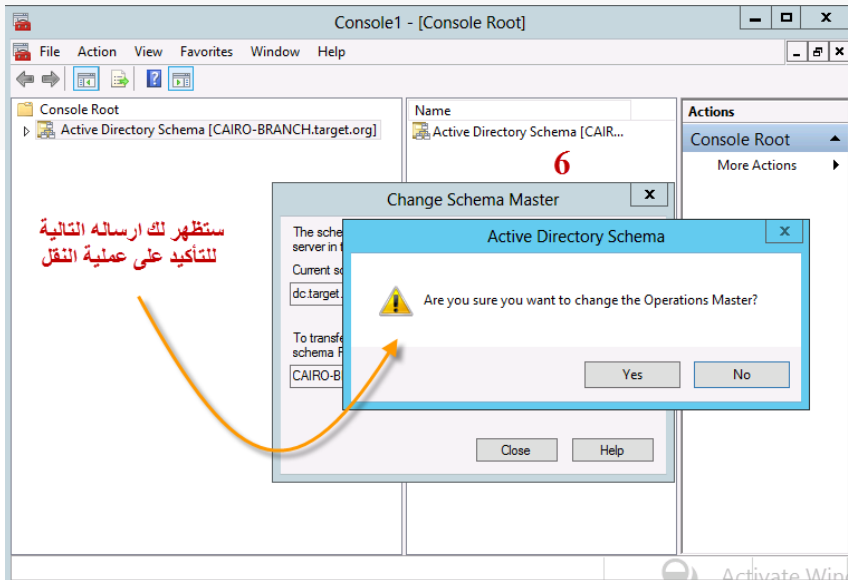
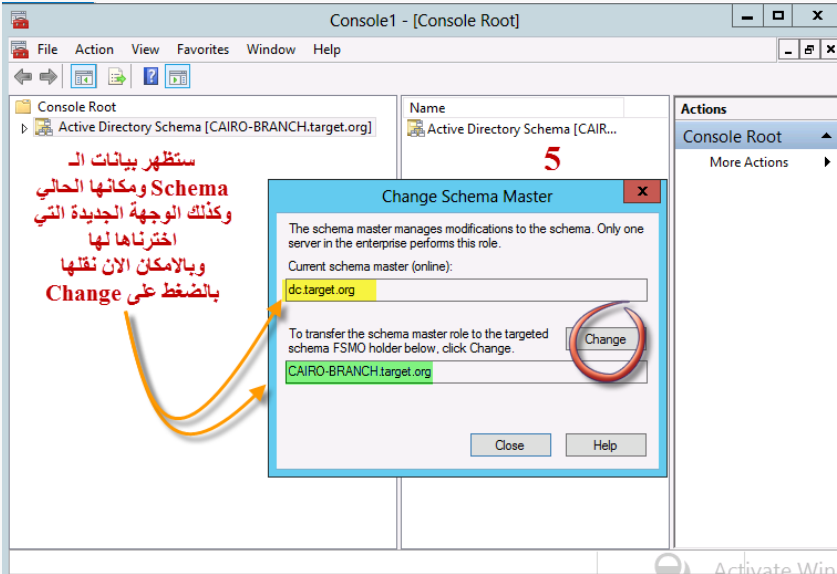
باستخدام الامر netdom ايضا يمكن معرفة الـ Server الذي يقوم بدور الـ FSMO

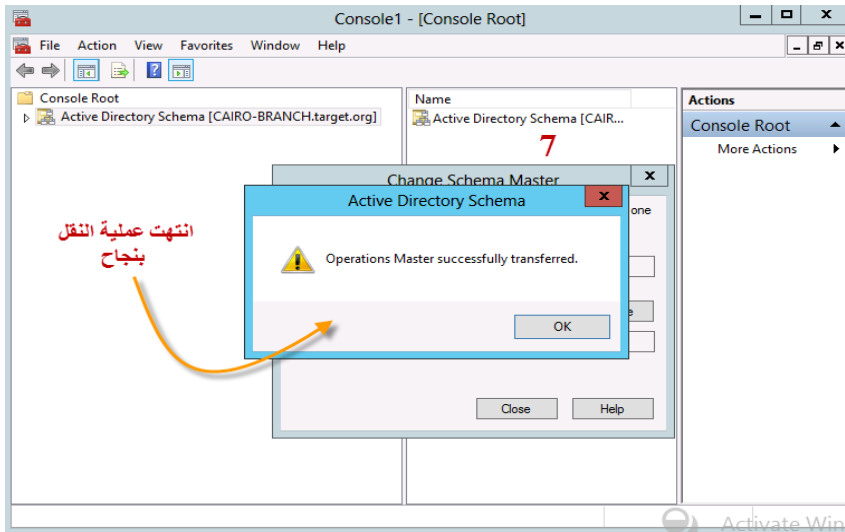
الآن بعد أن تأكدنا من أن الـ **Parent Domain Controller** لمجال **(Target.org)** هو الموجود في المركز الرئيسي في الرياض باسم **(DC)** سنقوم الآن بنقل الـ **FSMO** من هذا الـ **Server** إلى الـ **Server** الموجود في فرع القاهرة .

(1) خطوات نقل الـ Schema Role







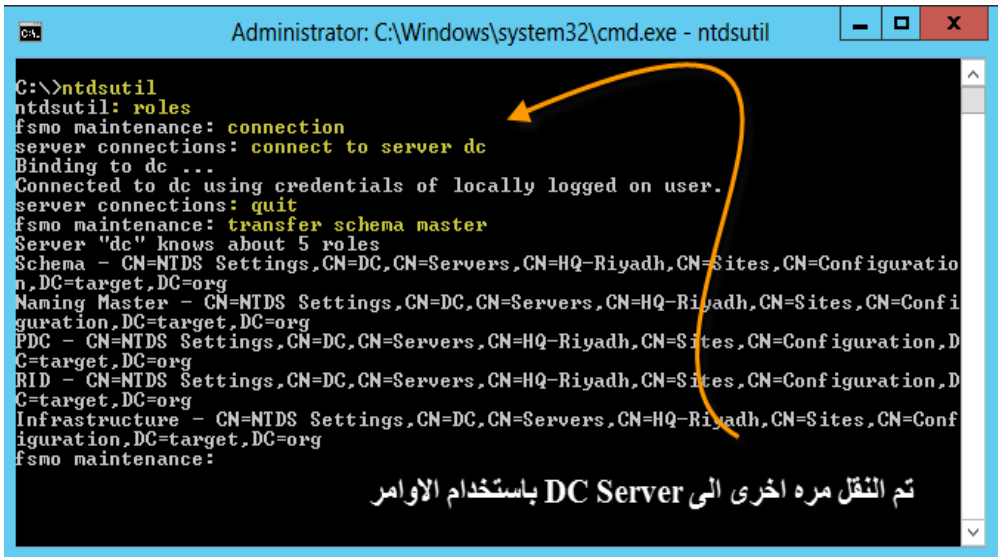


```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.
C:\Users\Administrator.WIN-59SDN3M96EB>cd\
C:\>netdom query fsmo
Schema master          CAIRO-BRANCH.target.org
Domain naming master  dc.target.org
PDC                   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 أيضا ان نقوم بنقل الـ Schema باستخدام سطر الاوامر (CMD) عن طريق الاكواد 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



```

Administrator: C:\Windows\system32\cmd.exe - ntdsutil

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

تم النقل مره اخرى الى DC Server باستخدام الاوامر

(2) خطوات نقل الـ Domain Naming Master Role

The screenshot shows the 'Active Directory Domains and Trusts' console. The left pane shows the tree structure with 'target.org' selected. The right pane shows the properties for 'target.org', with the 'Operations Master...' button highlighted. A yellow box highlights 'CAIRO-BRANCH.target.org' in the tree. A yellow arrow points from this box to the 'Operations Master...' button. Another yellow arrow points from the 'Operations Master...' button to the 'Operations Master' dialog box.

Domain Naming Role الـ يتم نقل الـ بنفس الطريقة تماما كما فعلنا في نقل الـ Schema لكن هذه المرة سنستخدم الـ AD Domain and Trusts بدلا من AD Schema Snap In

Operations Master

The domain naming operations master ensures that domain names are unique. Only one Active Directory Domain Controller in the enterprise performs this role.

Domain naming operations master:
dc.target.org

To transfer the domain naming master role to the following computer, click Change.
CAIRO-BRANCH.target.org

Change... Close

Administrator: C:\Windows\system32\cmd.exe

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

C:\>
```

كما نرى بعد النقل اصبح فرع القاهرة هو المسئول عن الـ Domain Naming Role

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

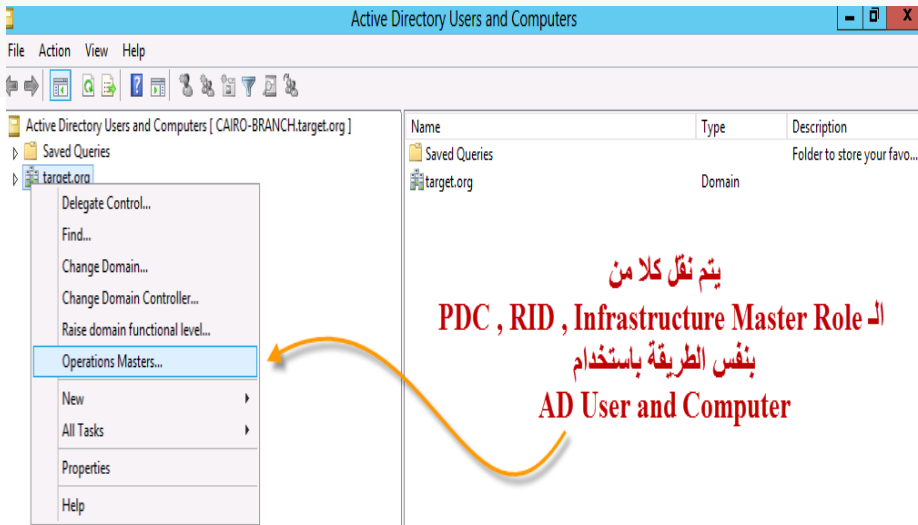
1. Open Command Prompt.
2. Type: **ntdsutil**
3. At the ntdsutil command prompt, type: **roles**
4. At the fsmo maintenance command prompt, type: **connection**
5. At the server connections command prompt, type: **connect to server** (type your server name that you want to transfer to him)
6. At the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

```

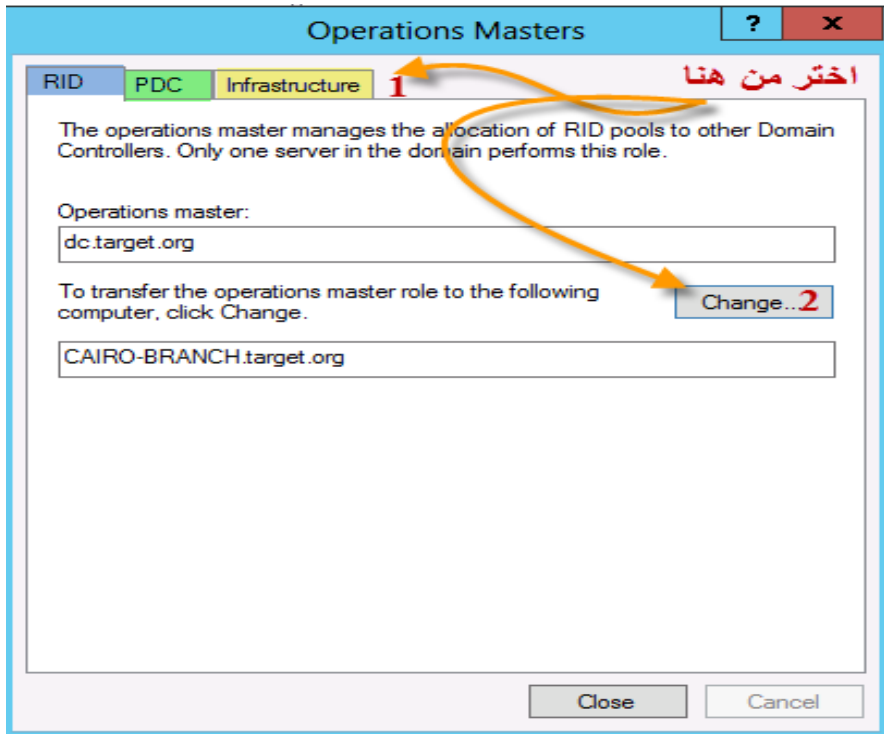
Administrator: C:\Windows\system32\cmd.exe - ntdsutil
C:\>ntdsutil
ntdsutil: role
fsmo maintenance: connection
server connections: connect to server dc
Binding to dc ...
Connected to dc using credentials of locally logged on user.
server connections: q
fsmo maintenance: transfer naming master
Server "dc" knows about 5 roles
Schema - CN=NTDS Settings,CN=DC,CN=Servers,CN=HQ-Riyadh,CN=Sites,CN=Configuration,DC=target,DC=org
Naming Master - CN=NTDS Settings,CN=DC,CN=Servers,CN=HQ-Riyadh,CN=Sites,CN=Configuration,DC=target,DC=org
PDC - CN=NTDS Settings,CN=DC,CN=Servers,CN=HQ-Riyadh,CN=Sites,CN=Configuration,DC=target,DC=org
RID - CN=NTDS Settings,CN=DC,CN=Servers,CN=HQ-Riyadh,CN=Sites,CN=Configuration,DC=target,DC=org
Infrastructure - CN=NTDS Settings,CN=DC,CN=Servers,CN=HQ-Riyadh,CN=Sites,CN=Configuration,DC=target,DC=org
fsmo maintenance:
  
```

تم الارجاع الى الـ DC Server باستخدام الكود مره اخرى

(3) خطوات نقل الـ PDC , RID , Infrastructure Master Role



يتم نقل كلاً من
 الـ PDC , RID , Infrastructure Master Role
 بنفس الطريقة باستخدام
 AD User and Computer



يمكن أيضا 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 (Infrastructure)**

```

Administrator: C:\Windows\system32\cmd.exe - ntdsutil

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=Configuration,DC=target,DC=org
Naming Master - CN=NTDS Settings,CN=DC,CN=Servers,CN=HQ-Riyadh,CN=Sites,CN=Configuration,DC=target,DC=org
PDC - CN=NTDS Settings,CN=DC,CN=Servers,CN=HQ-Riyadh,CN=Sites,CN=Configuration,DC=target,DC=org
RID - CN=NTDS Settings,CN=DC,CN=Servers,CN=HQ-Riyadh,CN=Sites,CN=Configuration,DC=target,DC=org
Infrastructure - CN=NTDS Settings,CN=DC,CN=Servers,CN=HQ-Riyadh,CN=Sites,CN=Configuration,DC=target,DC=org
fsmo maintenance: _
  
```

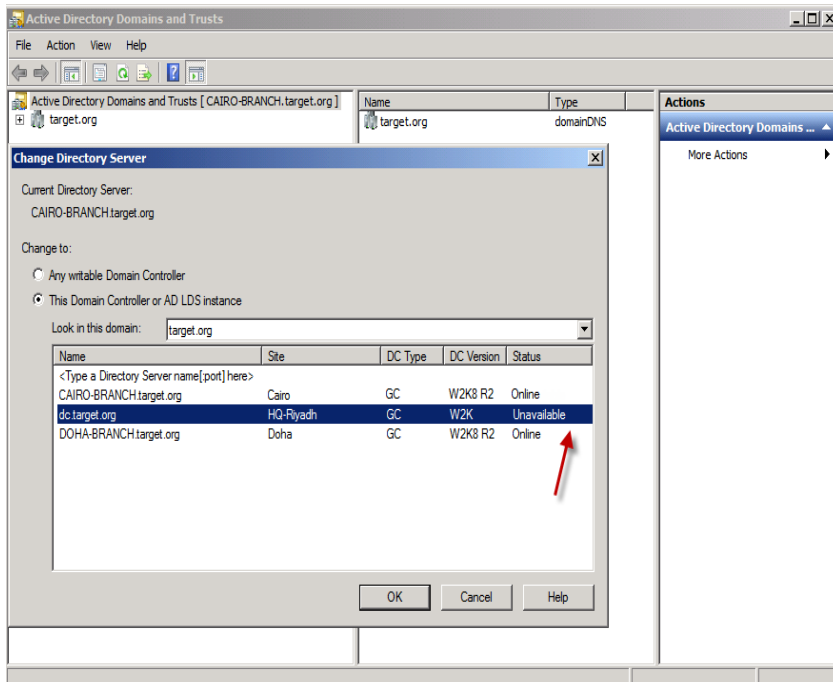
انتهينا الان من نقل جميع الـ **Operation Master Roles** عن طريق الـ **GUI** وباستخدام الكود أيضا من **Server** الى آخر في حالة ان الـ **Parent Domain Controller** موجود **Online** ؟ والان سنتعرف على الاحتمال الثاني هو ان الـ **Parent Domain Controller** غير موجود أو متضرر

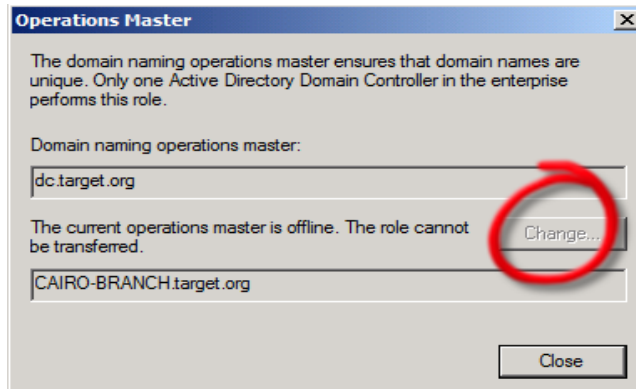
كيف يتم نقل الـ **FSMO Roles** عندما يكون الـ **Parent Domain Controller** غير موجود أو **Offline** ؟

الاجابة هي : استخدام أمر الـ **Seize** ولكن ماهو الـ **seize** ؟ 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 تعمداً بتعطيل الـ **Parent Domain Controller** الخاص بشبكتنا **Target.org** حتى يتبنى لنا اجراء الـ **Seize**





```

C:\>ntdsutil
ntdsutil: role
fsmo maintenance: connection
server connections: connect to server dc
Error parsing Input - Invalid Syntax.
server connections: connect to server dc
Binding to dc ...
DsBindWith$pnExW error 0x6ba(The RPC server is unavailable.)
server connections: _
  
```

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)**


```

Administrator: Command Prompt - ntdsutil
C:\>ntdsutil
ntdsutil: role
fsmo maintenance: connection
server connections: connect to server doha-branch
Binding to doha-branch ...
Connected to doha-branch using credentials of locally logged on user.
server connections: q
fsmo maintenance: seize schema master
Attempting safe transfer of schema FSMO before seizure.
FSMO transferred successfully - seizure not required.
Server "doha-branch" knows about 5 roles
Schema - CN=NTDS Settings,CN=DOHA-BRANCH,CN=Servers,CN=Doha,CN=Sites,CN=Configuration,DC=target,DC=org
Naming Master - CN=NTDS Settings,CN=DOHA-BRANCH,CN=Servers,CN=Doha,CN=Sites,CN=Configuration,DC=target,DC=org
PDC - CN=NTDS Settings,CN=DC,CN=Servers,CN=HQ-Riyadh,CN=Sites,CN=Configuration,DC=target,DC=org
RID - CN=NTDS Settings,CN=DC,CN=Servers,CN=HQ-Riyadh,CN=Sites,CN=Configuration,DC=target,DC=org
Infrastructure - CN=NTDS Settings,CN=DC,CN=Servers,CN=HQ-Riyadh,CN=Sites,CN=Configuration,DC=target,DC=org
fsmo maintenance: _

```

كما ترى يمكن القيام بنقل الـ Roles باستخدام أمر Seize في حالة فشل الـ Parent Domain Controller هل يمكنك نقل باقي الـ Roles ؟

ملاحظة مهمة جداً: بعد عمل **seize** لأي **role** ، يجب بعد إصلاح الخلل في الـ **Server** الأصلي عدم توصيله بالشبكة إلا بعد عمل إعادة 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 server2** إلى

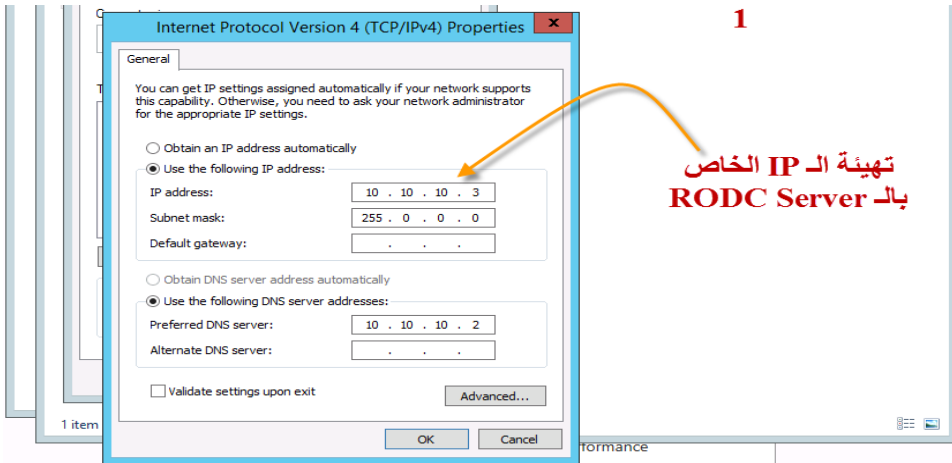
فيجب بعد إصلاح **server1** فوراً القيام بعمل **Formatting** له ثم بعد ذلك نقوم بعمل **Transfer** للمهمة أو الـ **role** من **server2** إلى **server1** مره اخرى اذا دعت الحاجة لذلك .

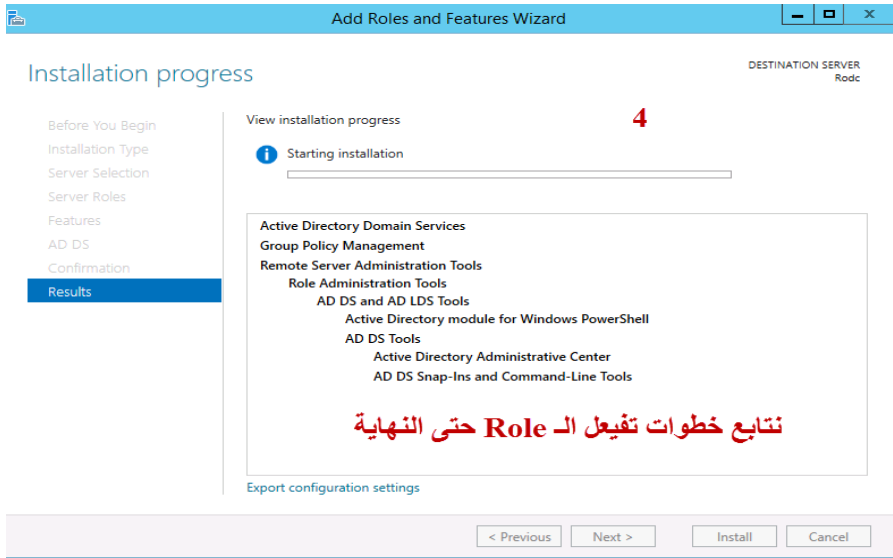
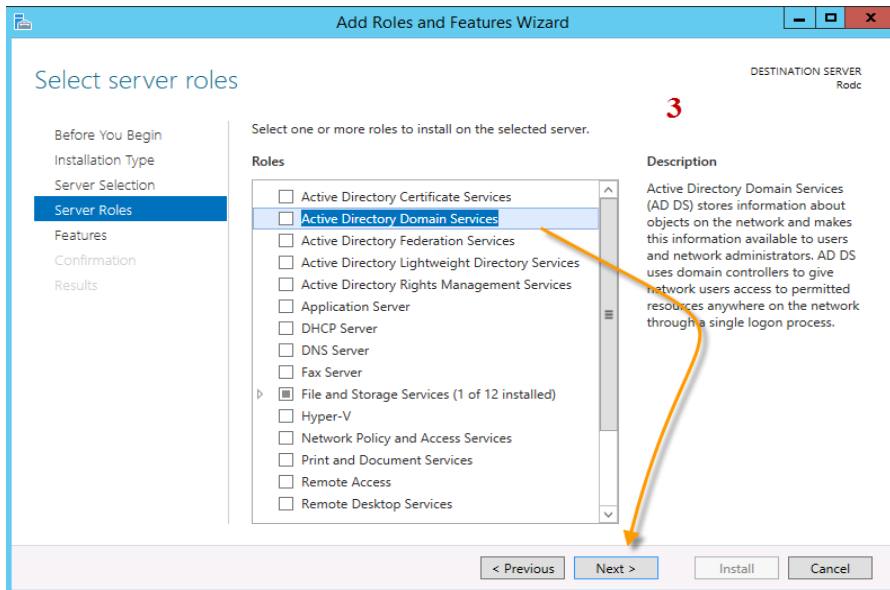
انتهينا الان من عمل الـ **Replication** وتطرقنا لنوع الـ **Additional Domain** والآن سنتناول نوع اخر من الـ **Domain** وهو الـ **RODC** و الـ **RODC** وهو نفس فكرة الـ **Additional** أي انه يعد نسخة طبق الاصل من الـ **Domain** أيضا غير انه للقراءة فقط ولا يمكن التعديل عليه إلا بمنح تفويض **Authorization** 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**

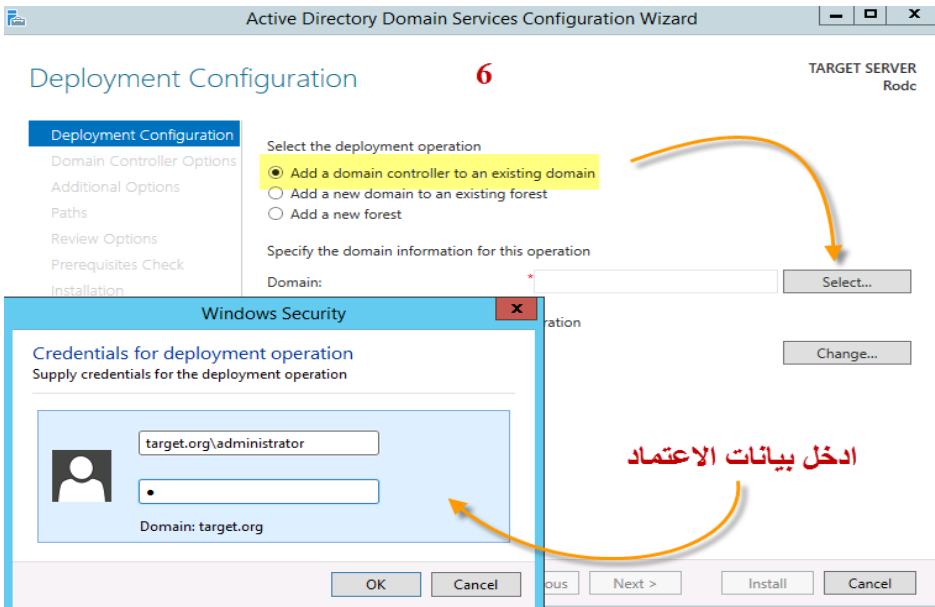
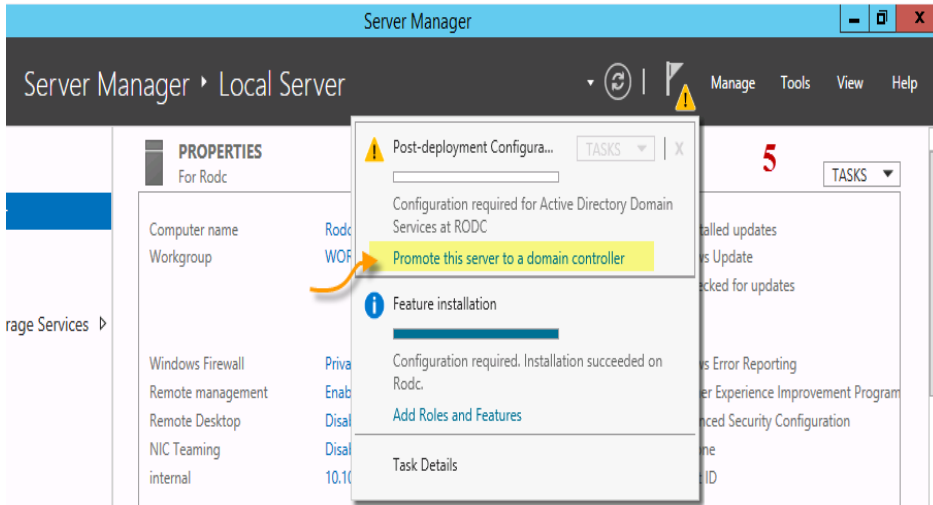
أو بمعنى اخر فان عملية الـ **Authentication** لا تتم عن طريق الـ **RODC** كخادم بل تتم عن طريق الـ **Domain** بواسطة خادم الـ **RODC**

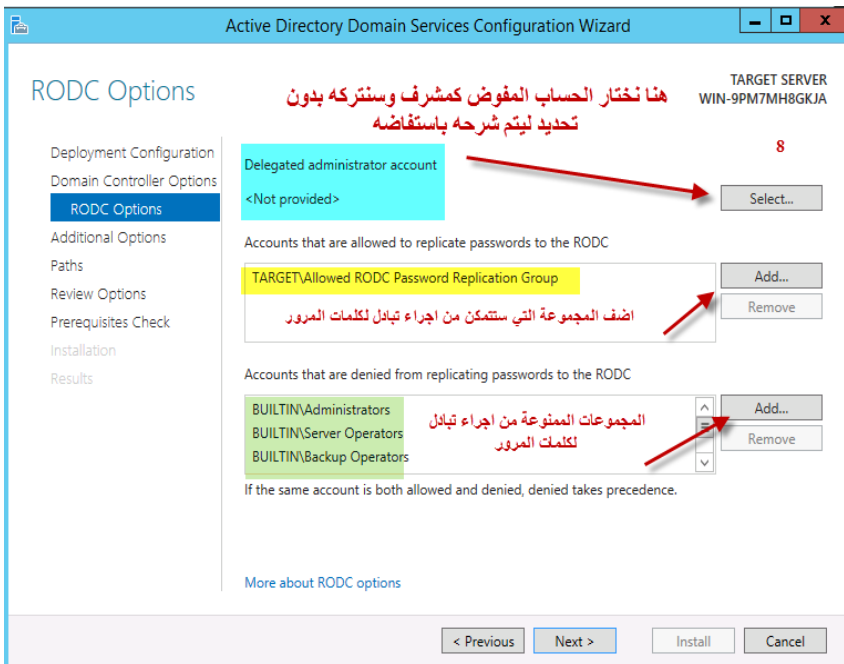
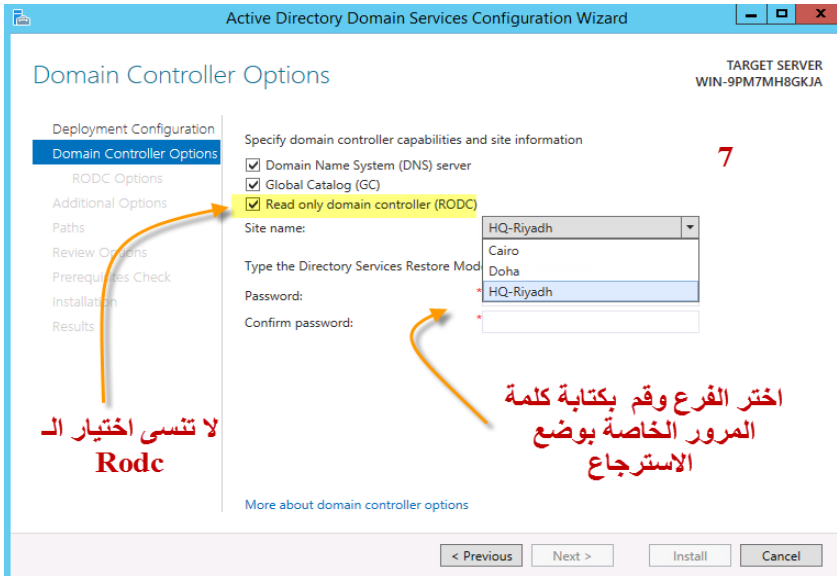
وللتوضيح أكثر فأننا سنفترض ان المركز الرئيسي في الرياض قد افتتح فرعا اخر داخل نفس المدينة وبالتالي فان هذا الفرع حتما سينضم لشبكتنا وكعامل أمان سنفوض أحد الأشخاص بتولي عملية ادارة هذا الفرع تقنيا بحيث يستطيع تولي العمليات المرتبطة بالشبكة بحسب ما يمنح له من صلاحيات ادارية فقط وفي هذه الحالة فان الخيار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

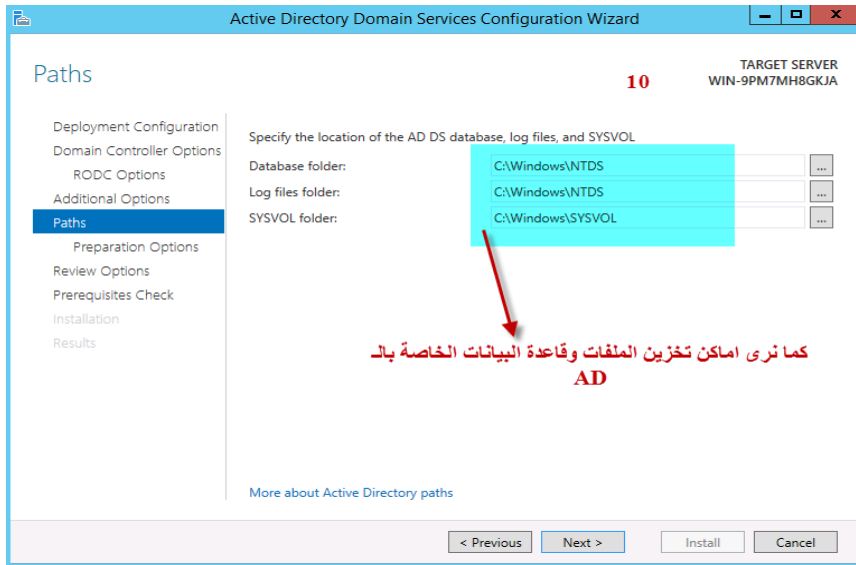
ولعمل الـ **RODC Server** فسنقوم بضبط اعداد الـ **IP** والـ **Server Name** ثم نتابع خطوات التثبيت المعروفة

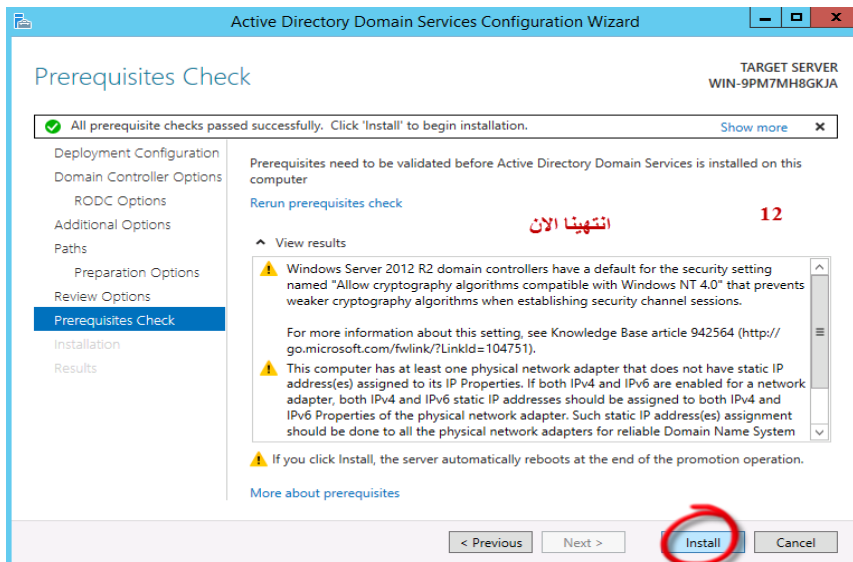
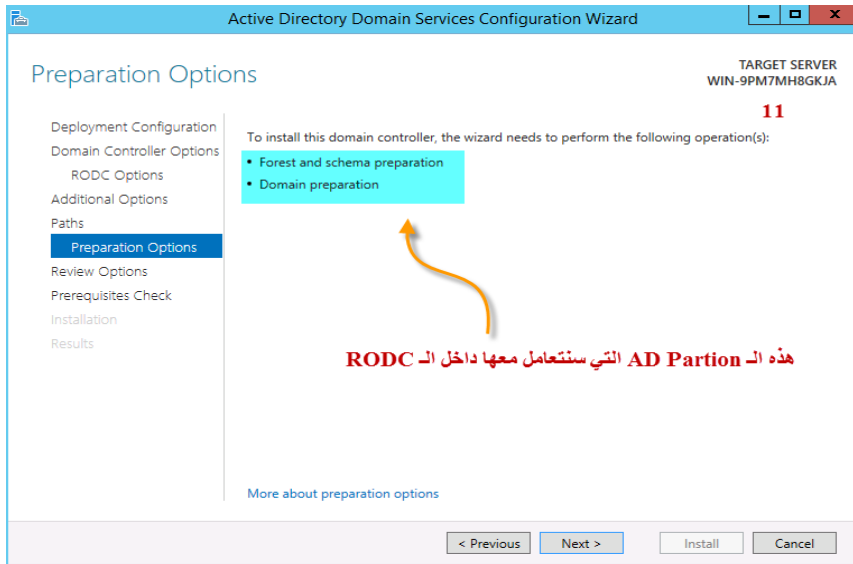


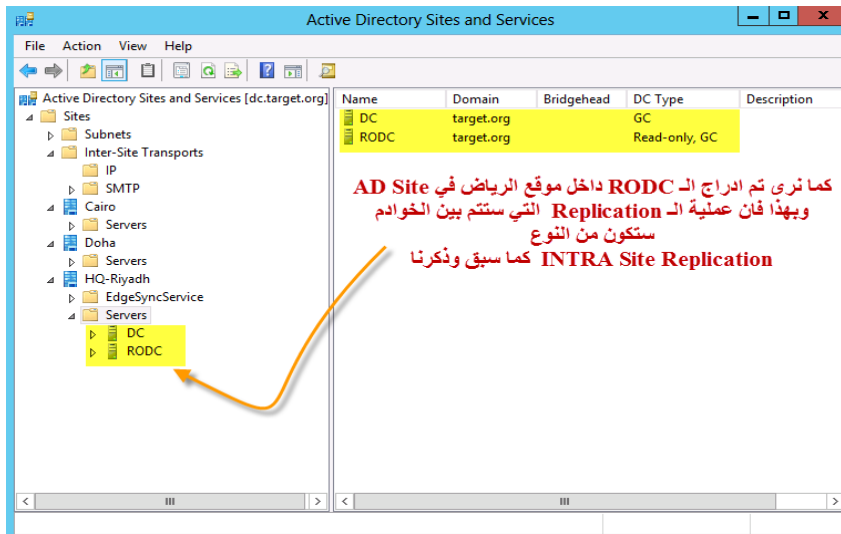
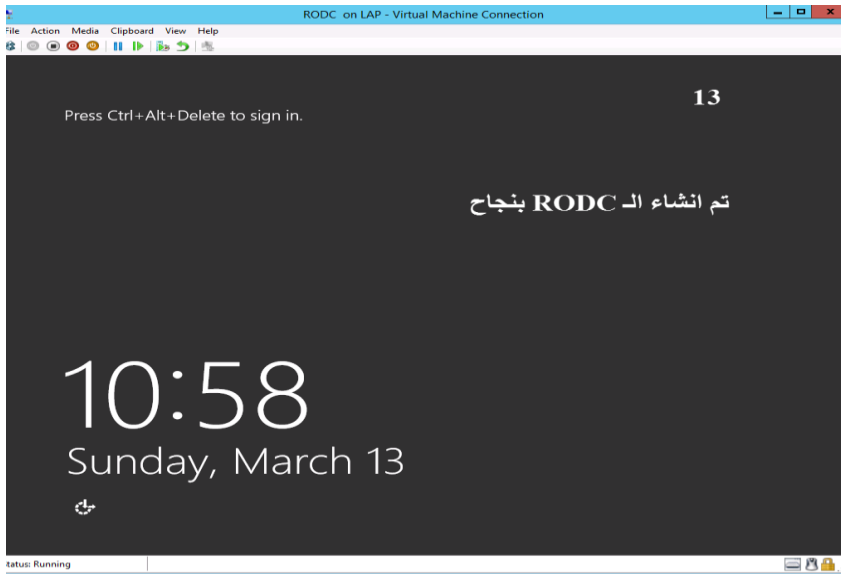




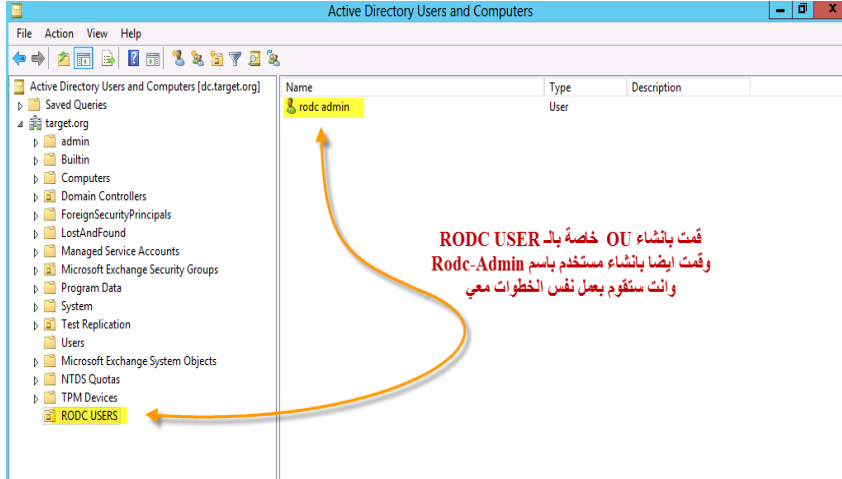


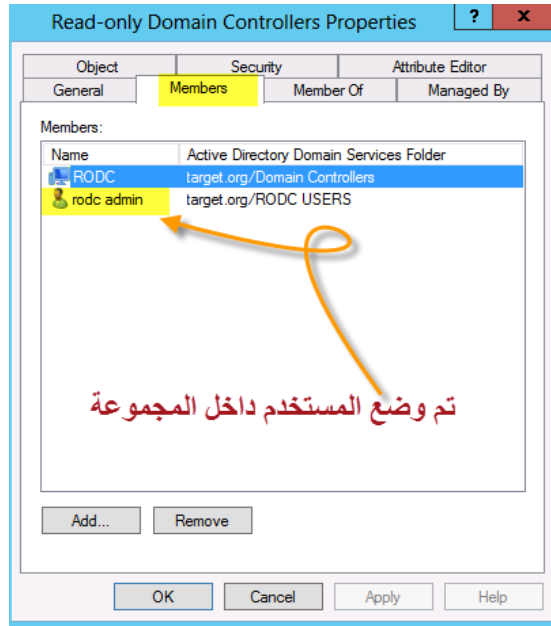






الآن دعونا نكمل خطواتنا ونقوم بتفويض الشخص المسنول عن خادم الـ **RODC**





Active Directory Users and Computers [dc.target.org]

Change Domain...
Change Domain Controller...
 All Tasks
 View
 Refresh
 Export List...
 Help

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
				Line Unavailable Unavailable

The selected Domain Controller is Read-only. You will not be able to perform any write operations.

Save this setting for the current console

OK Cancel Help

RODC عند فتح الـ Active Directory Users and Computers من داخل الـ AD سيظهر لك الـ Domain الخاص بالـ Domain نفسه

وعند محاولة تغيير الـ Domain Controller واختيار الـ RODC ستظهر لك رسالة تحذيرية أنك لا تملك أي صلاحيات على هذا الدومين

Active Directory Users and Computers [RODC.target.org [Read-only]]

rodadmin Properties

Members of:

Name	Active Directory Domain Services Folder
Domain Users	target.org/Users
Read-only Domain...	target.org/Users

Primary group: Domain Users

Set Primary Group There is a problem with this change Primary group unless you have the appropriate permissions on both clients or POSIX-compliant applications.

OK Cancel Apply Help

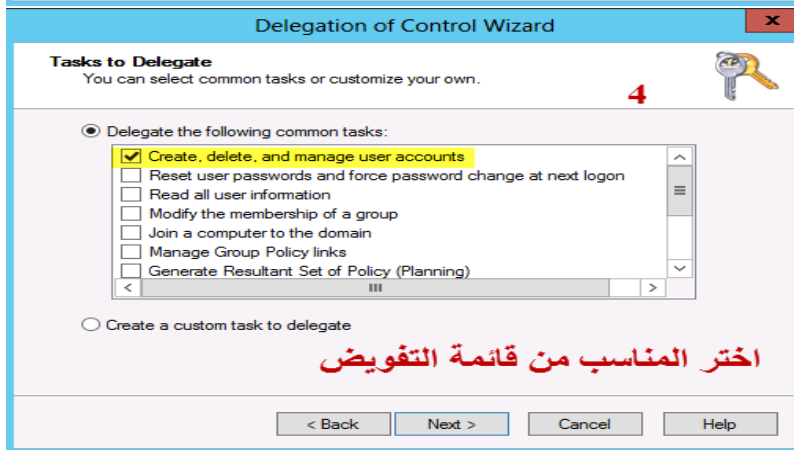
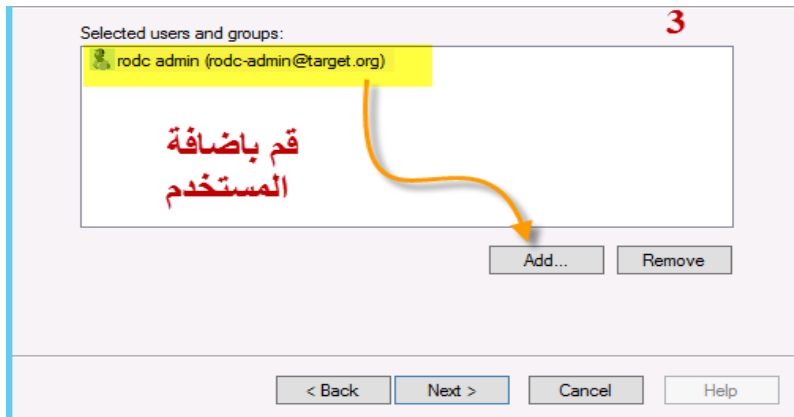
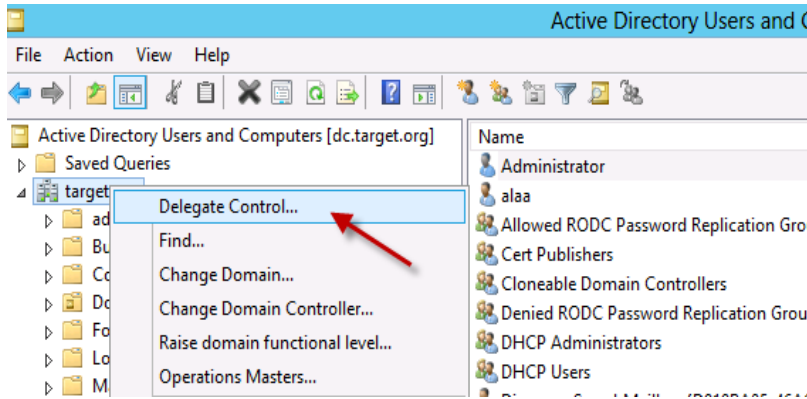
rodadmin User

Add to a group...
 Disable Account
 Reset Password
 Send Mail
 All Tasks
 Properties
 Help

Delegate Control...
 Find...
 Resultant Set of Policy (Planning)...

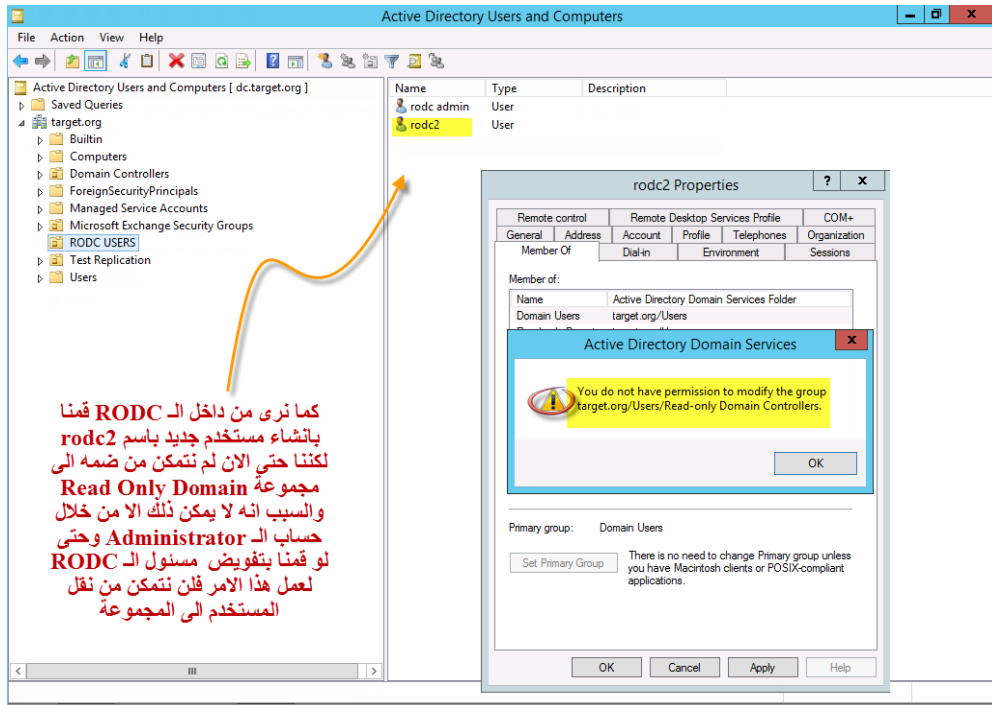
وكما نرى لا نستطيع انشاء او حذف او التعديل على اي كائن

الآن سنقوم بعمل الـ **Delegation** للمستخدم





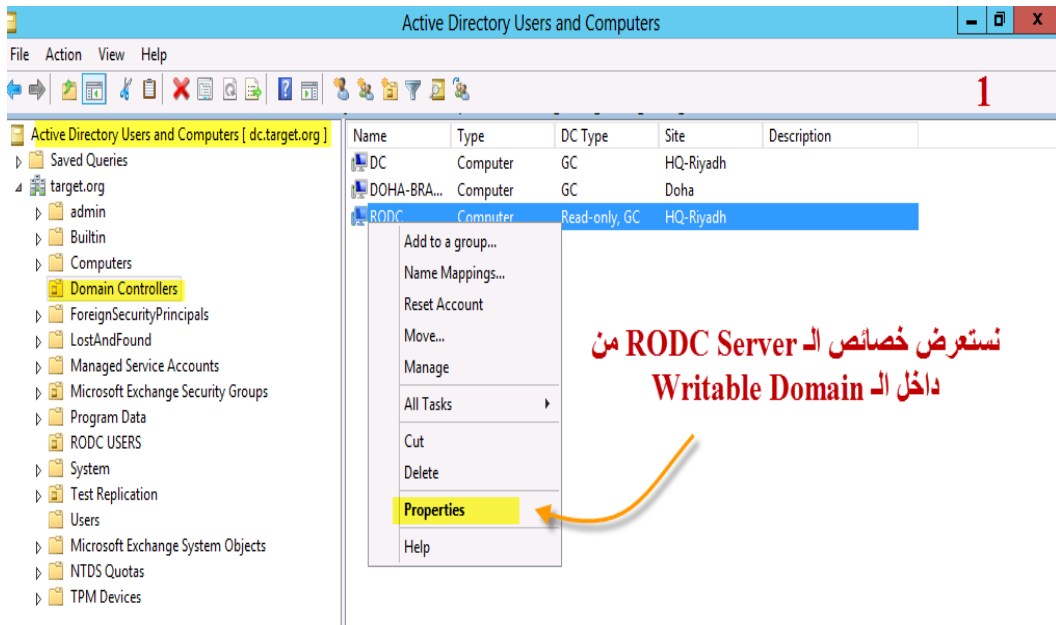
قمنا في الخطوات السابقة بتفويض المستخدم **rodc-admin** بحذف وإنشاء المستخدمين والآن سنجرّب العملية من داخل الـ **RODC**

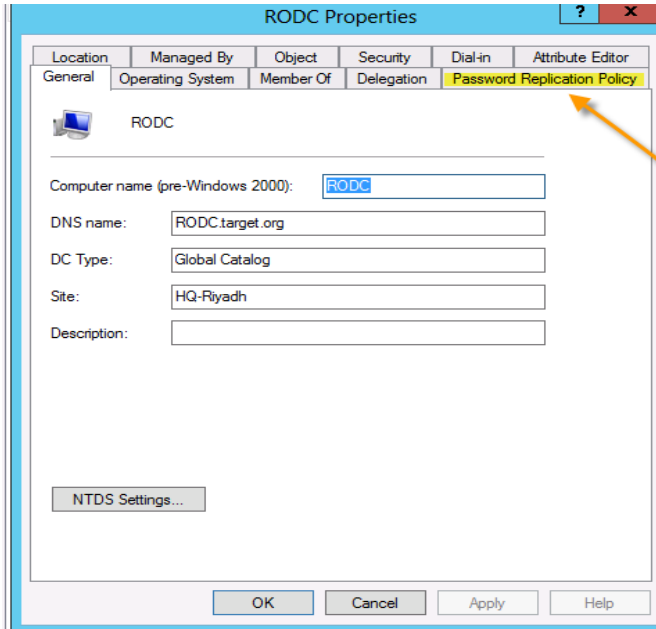


إذا من الصورة السابقة تتضح فكرة عمل الـ **Rodc** حيث لا يقوم بحفظ كلمات المرور عليه بل يجلبها من الـ **Writable Domain** وحتى يستطيع المستخدم الدخول على الـ **RODC** سيتم الاتصال أولاً بهذا الـ **Writable Domain** لكي يحصل على تصريح الدخول منه

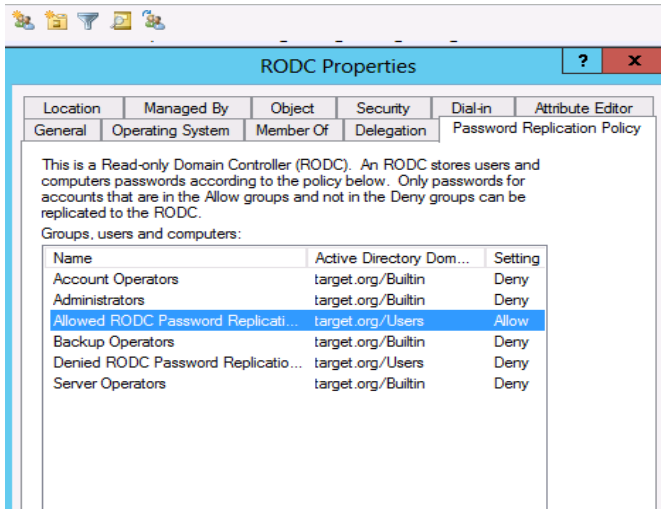
وطبعاً إذا لم يكن الـ **Domain** الرئيسي متاحاً فلن يتمكن المستخدم العادي ولا حتى المستخدم المفوض من الدخول على الـ **RODC** لأنه ببساطة لا يوجد تصريح للدخول. **إذا فما الحل؟**

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

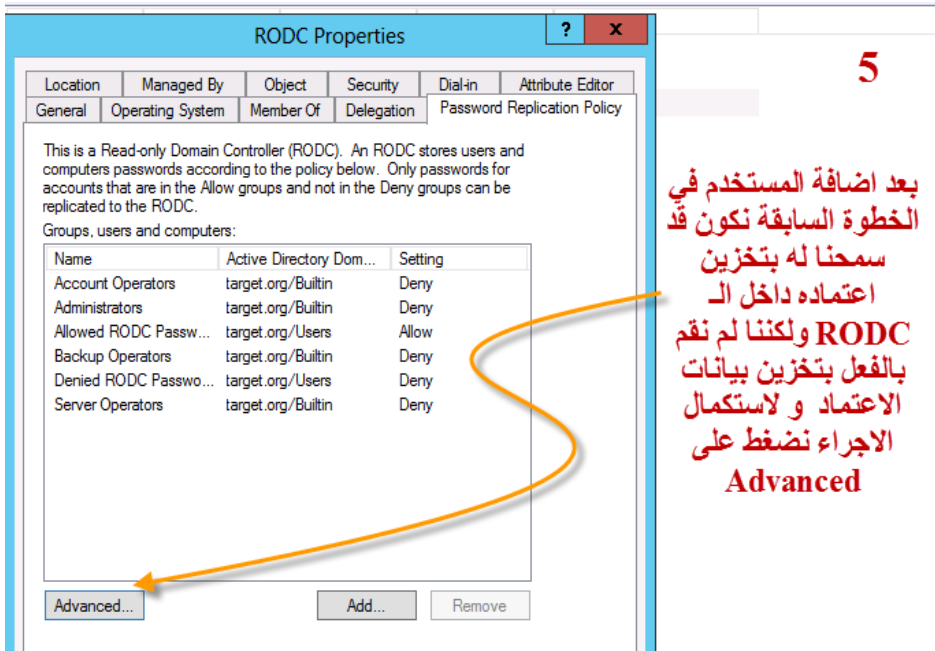




من خصائص الـ RODC
تذهب الي
Password Replication
Policy



أختر مجموعة
Allow Password
Replication



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

كما ترى قائمتين الاولى للمستخدمين الذي تم تخزين كلمات مرورهم على الـ RODC والثانية لمن تم تفويضهم عن طريق الـ Writable Domain

من القائمة نختار المستخدمين المسموح لهم بتخزين كلمات مرورهم على الـ RODC نضغط على Prepopulate Password

6

Advanced Password Replication Policy for RODC

Select Users or Computers

Select this object type:

Users or Computers

From this location:

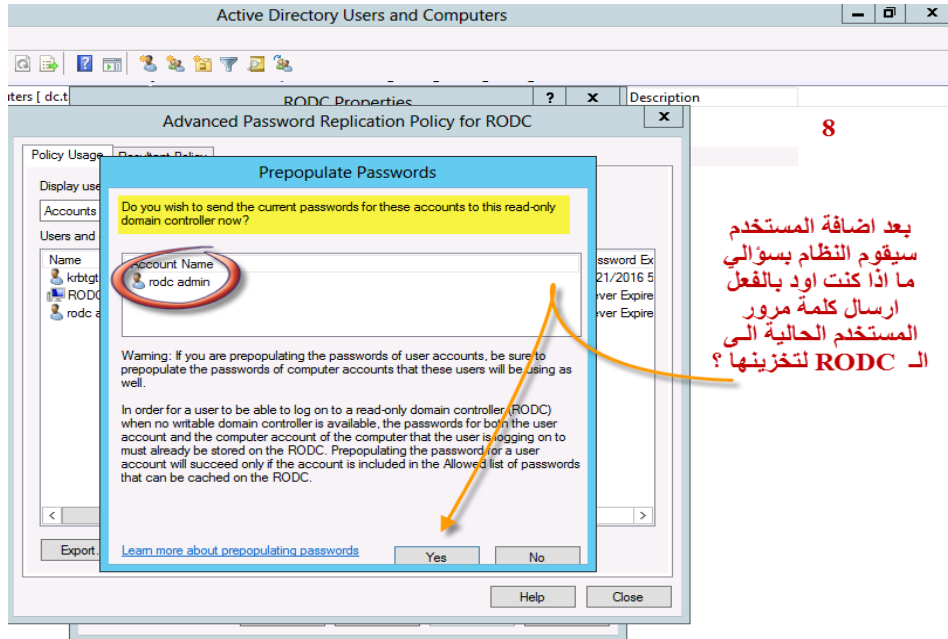
target.org

Enter the object names to select (examples):

rodc admin (rodc-admin@target.org)

7

قم باضافة المستخدم



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

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

```

C:\Windows\system32\cmd.exe

Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\rodc-admin>set
ALLUSERSPROFILE=C:\ProgramData
APPDATA=C:\Users\rodc-admin\AppData\Roaming
CommonProgramFiles=C:\Program Files\Common Files
CommonProgramFiles(x86)=C:\Program Files (x86)\Common Files
CommonProgramW6432=C:\Program Files\Common Files
COMPUTERNAME=RODC
ComSpec=C:\Windows\system32\cmd.exe
FP_NO_HOST_CHECK=NO
HOMEDRIVE=C:
HOMEPATH=\Users\rodc-admin
LOCALAPPDATA=C:\Users\rodc-admin\AppData\Local
LOGONSERVER=\RODC
NUMBER_OF_PROCESSORS=1
OS=Windows_NT
  
```

```

C:\Windows\system32\cmd.exe

C:\Users\rodc2.TARGET>set
ALLUSERSPROFILE=C:\ProgramData
APPDATA=C:\Users\rodc2.TARGET\AppData\Roaming
CommonProgramFiles=C:\Program Files\Common Files
CommonProgramFiles(x86)=C:\Program Files (x86)\Common Files
CommonProgramW6432=C:\Program Files\Common Files
COMPUTERNAME=RODC
ComSpec=C:\Windows\system32\cmd.exe
FP_NO_HOST_CHECK=NO
HOMEDRIVE=C:
HOMEPATH=\Users\rodc2.TARGET
LOCALAPPDATA=C:\Users\rodc2.TARGET\AppData\Local
LOGONSERVER=\DC
NUMBER_OF_PROCESSORS=1
OS=Windows_NT
  
```

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 فوراً بالتالي :-

Name	Type	DC Type	Site	Description
DC	Computer	GC	HQ-Riyadh	
DOHA-BRA...	Computer	GC	Doha	
RODC	Computer	Read-only, GC	HQ-Riyadh	

1

الخطوة الاولى لمحو بيانات الاعتماد المخزنة على الـ
RODC

Delete

Deleting Domain Controller

If the Read-only Domain Controller was stolen or compromised, it is recommended that you reset the passwords of the accounts that were stored on this Read-only Domain Controller.
The computer object you want to delete represents this Read-only Domain Controller:

RODC

Reset all passwords for user accounts that were cached on this Read-only Domain Controller.
Warning! This operation will require these users to contact your helpdesk to obtain a new password.

Reset all passwords for computer accounts that were cached on this Read-only Domain Controller.
Warning! This operation will disjoin these computers from the domain and they will need to be rejoined.

Export the list of accounts that were cached on this Read-only Domain Controller to this file: View List...

Location: Browse...

Delete Cancel

كما نرى خيارات الاستعادة لكلمات
المرور الخاصة بالمستخدم والخاصة
بالأجهزة
كما يمكن تصدير كلمات المرور كملف
يمكن الاستعانة به لاحقاً

وبهذا نكون قد انتهينا من الـ RODC هل تعتقد أن الموضوع كان صعباً ؟

Child Domain

الغرض من انشاء الـ **Child Domain** هو إيجاد **Domain** صغير من الـ **Domain** الرئيسي أو ما يسمى بالـ **Sub-Domain** فقد تكون مؤسستي تزايد عدد الـ **Users** بها وتنوعت النشاطات وزادت التخصصات , في هذه الحالة أقوم بإنشاء **Domain** فرعي من الـ **Domain** الرئيسي يكون المتحكم فيه هو الـ **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 أقوم بإنشاء اي **Object** لا يتم تبادل بياناته تلقائياً مع المواقع الأخرى 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

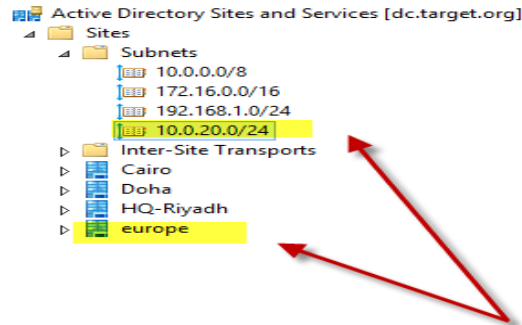
Child domain is : **paly.google.com**

Parent Domian is : microsoft.com

Child domain is : **windows.microsoft.com**

الآن سوف نقوم بعمل **child** من الدومين الخاص بنا وأنا 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

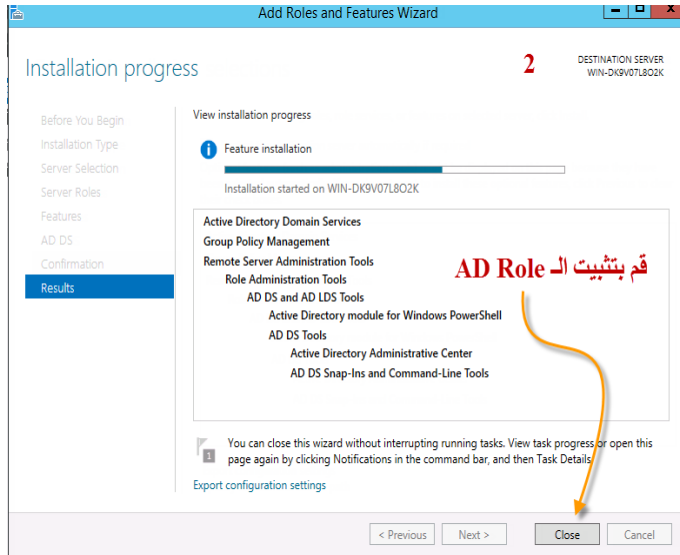
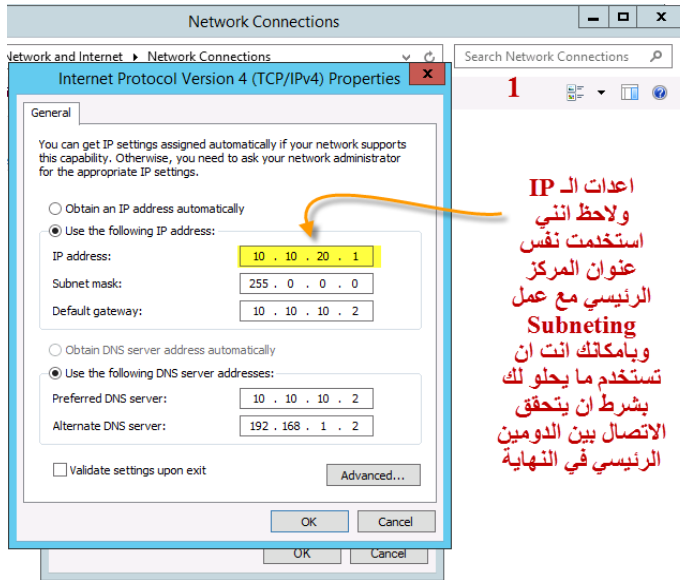
والآن سنبدأ معا عمل الـ **Child Domain**

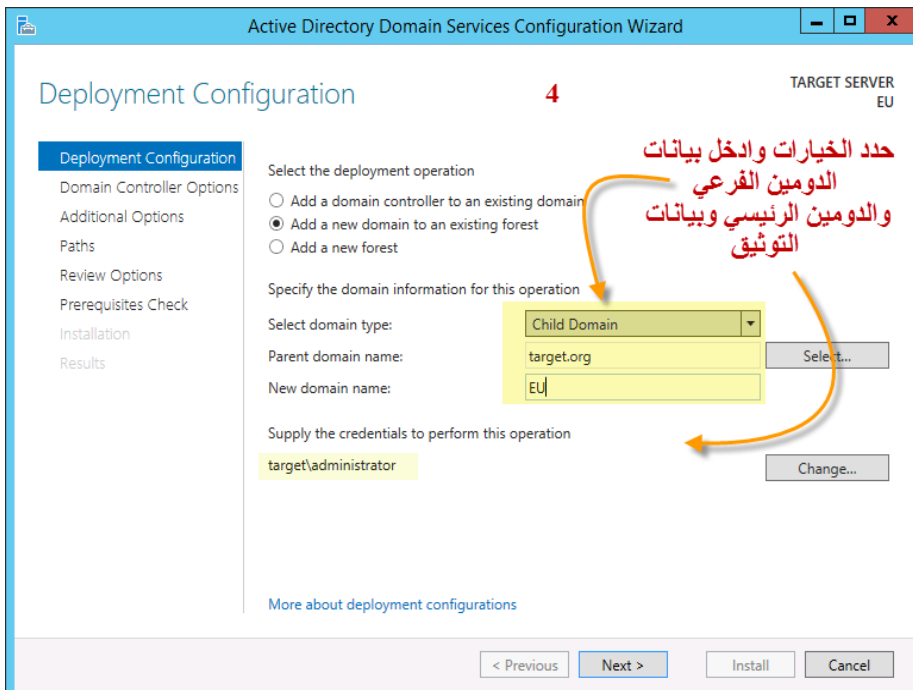
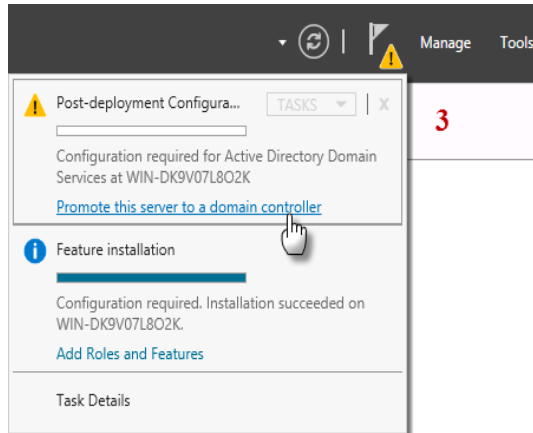


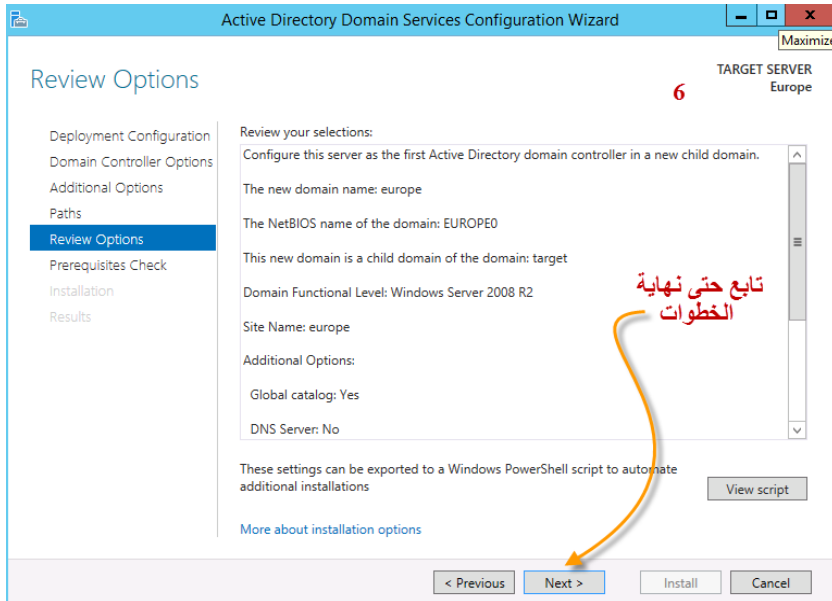
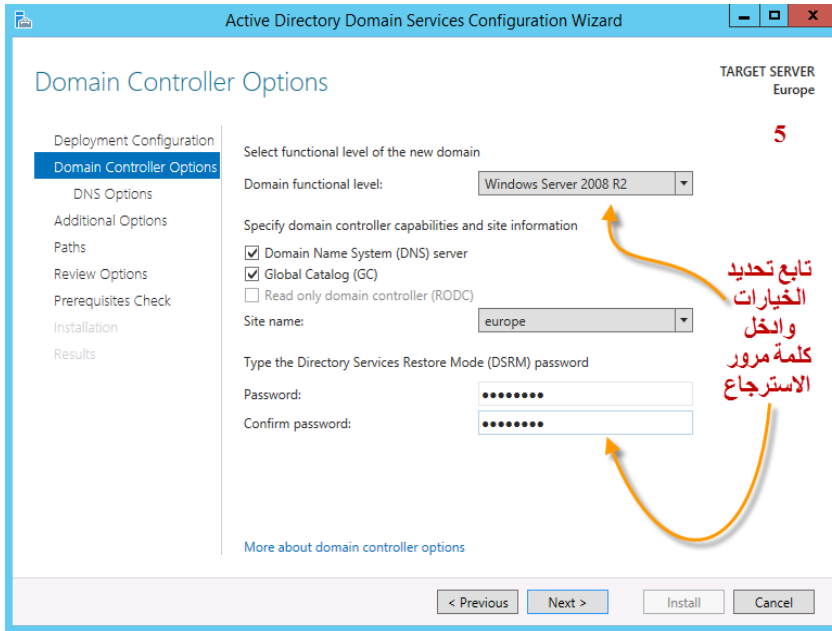
لا تنسى اضافة الموقع
والـ **Subnet** قبل عمل
الـ **Child**

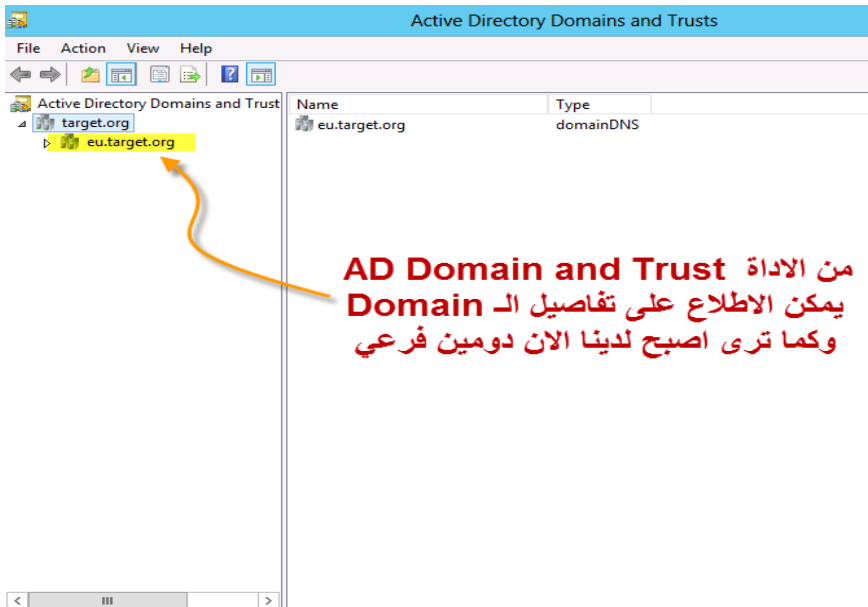
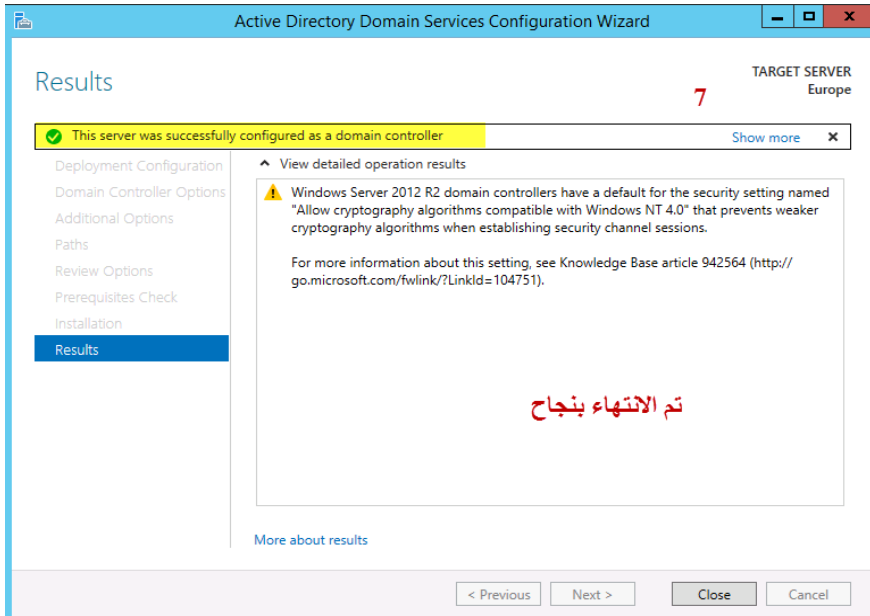
• ملحوظة مهمة

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**









حسنًا أصبحنا الآن نملك **Domain** فرعي من الـ **Domain** الرئيسي الخاص بنا وكما ذكرنا هو **domain** خاص بذاته له خصائصه 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 الـ **Target** والعكس؟
هيا لنتعرف على الإجابة عمليًا في الخطوات التالية :-

The screenshot shows the Windows 7 System Control Panel window. The title bar reads "System and Security > System". The main content area displays system information and domain settings. A red Arabic text overlay reads "يمكن ضم الاجهزة الان للمجال الفرعي" (It is possible to add devices to the sub-domain). An orange arrow points from this text to the "Full computer name" field, which is highlighted in yellow and contains "win7.eu.target.org".

Copyright © 2009 Microsoft Corporation. All rights reserved.
Service Pack 1
Get more features with a new edition of Windows 7

يمكن ضم الاجهزة الان للمجال الفرعي

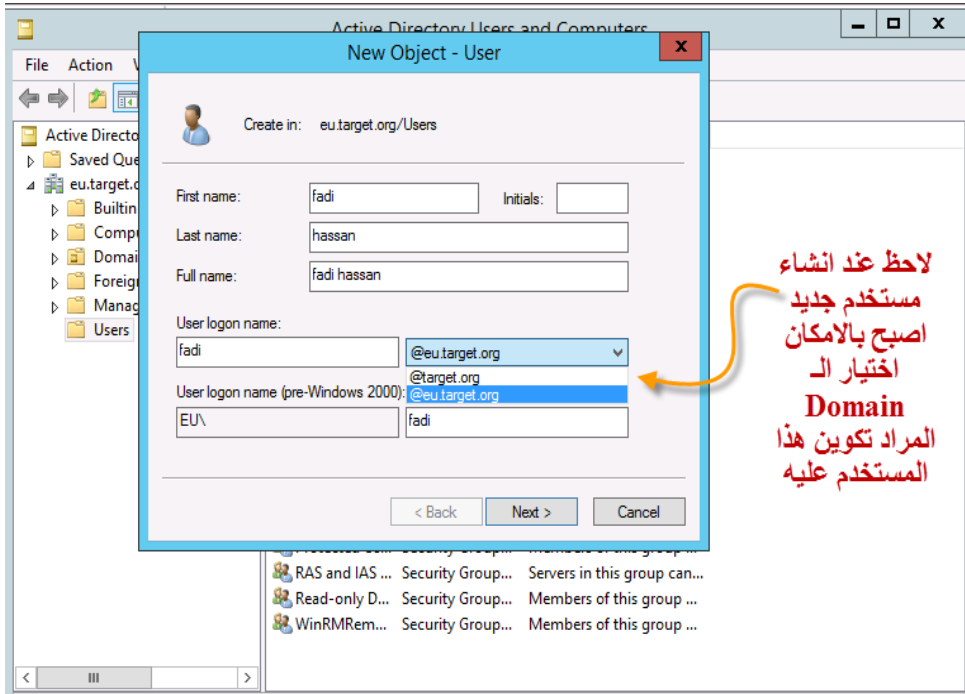
System

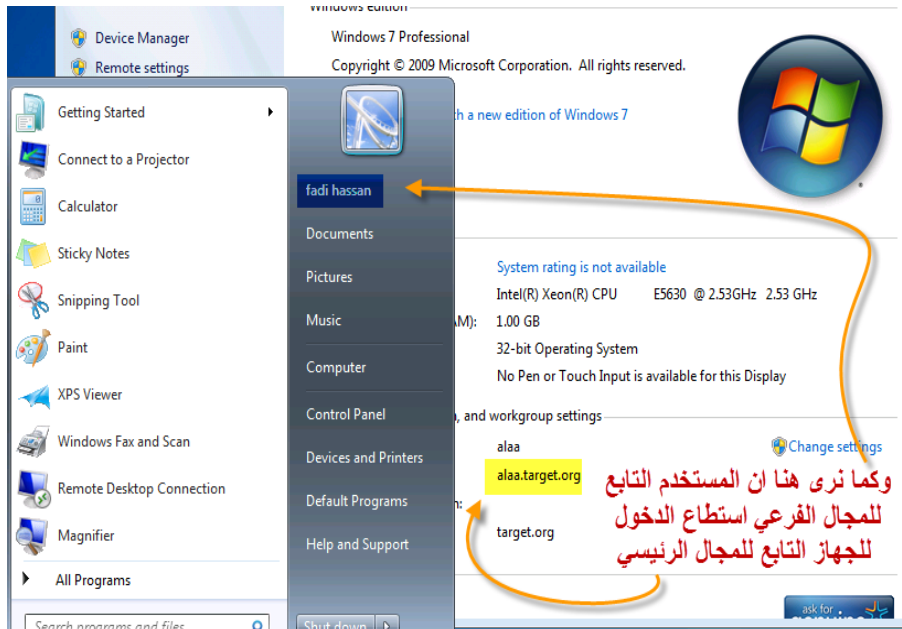
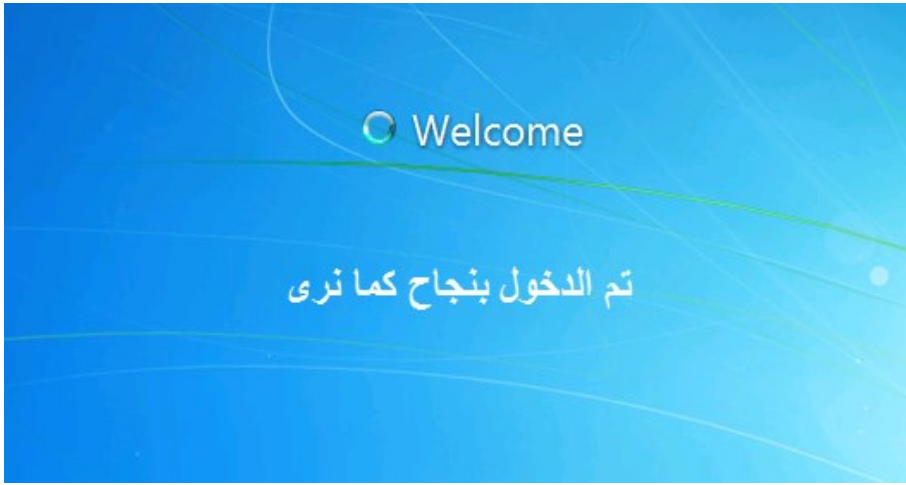
Rating:	System rating is not available
Processor:	Intel(R) Xeon(TM) CPU E5630 @ 2.53GHz 2.53 GHz
Installed memory (RAM):	1.00 GB
System type:	32-bit Operating System
Pen and Touch:	No Pen or Touch Input is available for this Display

Computer name, domain, and workgroup settings

Computer name:	win7	Change settings
Full computer name:	win7.eu.target.org	
Computer description:		
Domain:	eu.target.org	

Windows activation





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

ACTIVE DIRECTORY TRUST RELATIONSHIP

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

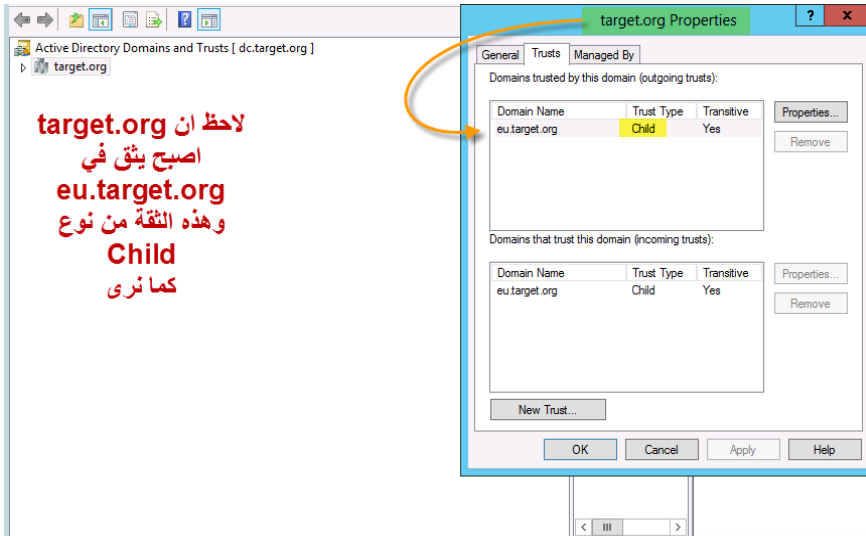
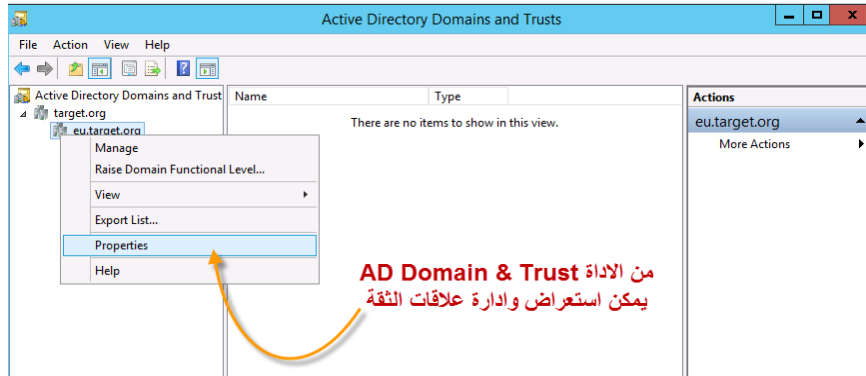
الجواب هو أننا حينما انشأنا مجالاً فرعياً من المجال الرئيسي فقد نشأت بينهما مباشرة علاقة ثقة **TRUST RELATIONSHIP**

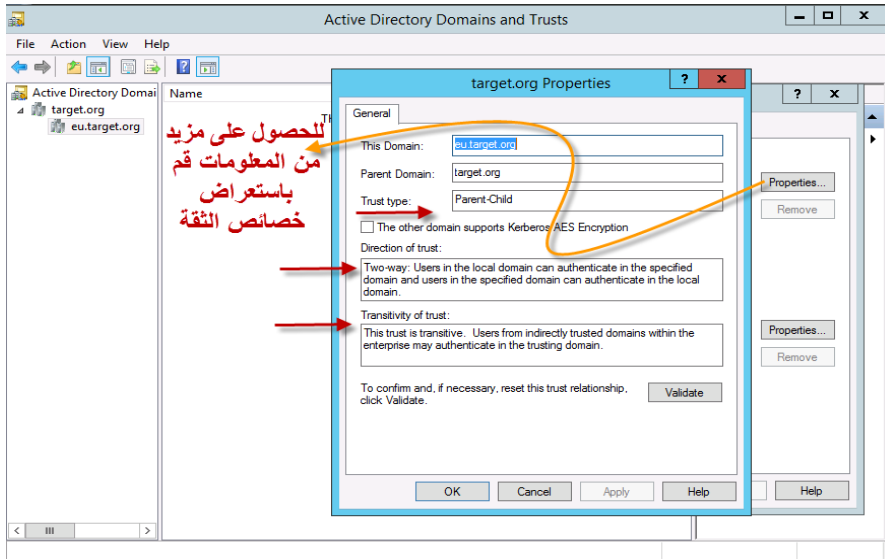
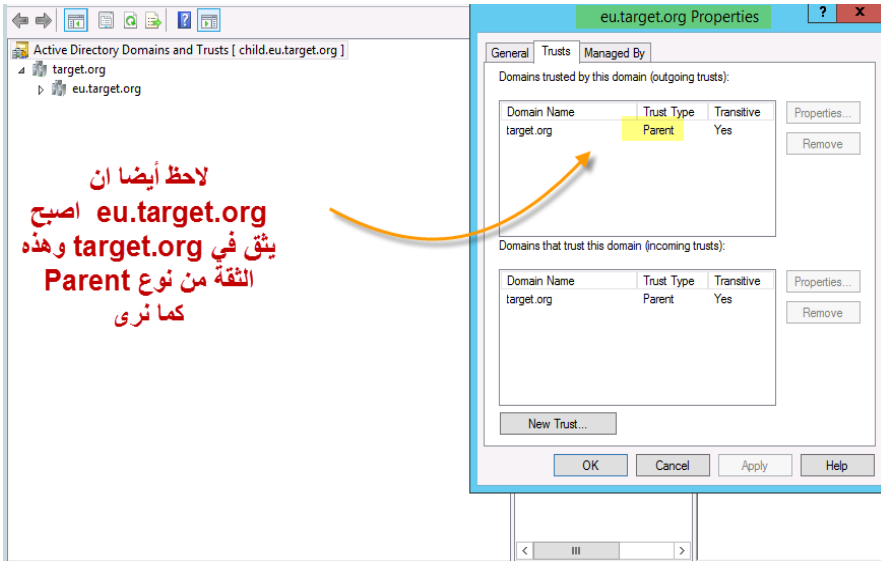
وعلاقات الثقة بين الـ **DOMAIN** وبين الـ **CHILD** تنشأ تلقائياً تماماً كما يحدث هذا بين علاقة الأب وابنه في حياتنا وتسمى هذه العلاقة **IMPLICIT**

وهذا النوع ينشأ ألياً بين المجالات الموجودة في نفس الـ **Forest**

أما ما ينشأ بواسطة مسؤول الشبكة أو 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 .

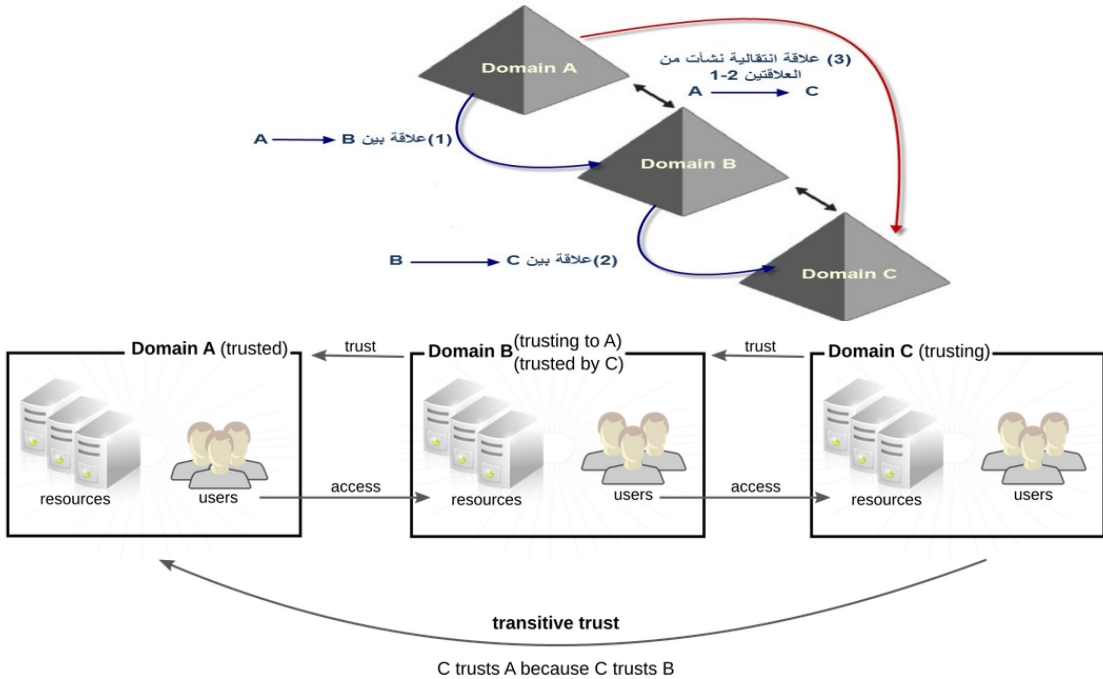
ويمكن تقسيم أنواع علاقات الثقة لنوعين - :

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 تقسيم طرق انشاء علاقات الثقة لنوعين أيضا - :

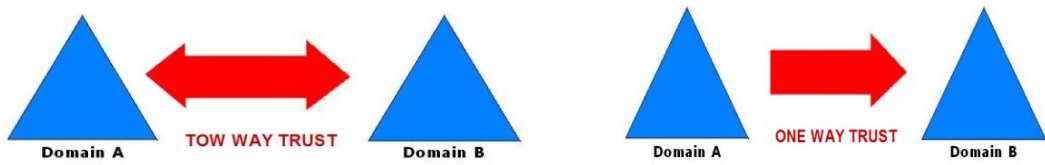
TRUST TWO WAY -1

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** فإن المستخدم من الدومين **A** إذا اراد الوصول الى مصادر الدومين **C** فسيحتاج عليه المرور بالدومين **B** في المثال أو بكل المجالات التي تربط بينهما علاقة ثقة كما في 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 البروتوكول **KERBEROS V5** فى عملية التوثيق مع أى نظام آخر لا يستخدم هذا النوع من البروتوكول مثل نظام الـ **Unix** .

EXTERNAL TRUST -5

هذا النوع مخصص لعمل **TRUST** بين مجالات خارج نطاق الـ **Forest** هذا النوع من الـ **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** طبعاً بعد توافر التراخيص اللازمة لذلك كما نعلم .

FOREST TRUST -6

فى حالة اندماج شركتين معا كما حدث مع شركة **HP** و **Compaq** فإنه بالطبع كلا الشركتين لهما **Two Domain and Two Forests** وبالتالي كانت الحاجة لهذا النوع من الـ **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

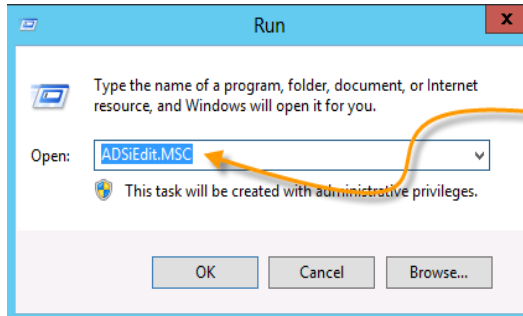
و هذا النوع من الثقة قد يكون من حيث الإتجاه **ONE WAY** أو **TWO WAY** و هذا النوع يعتبر **TRANSITIVE TRUST**

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

إنتبه

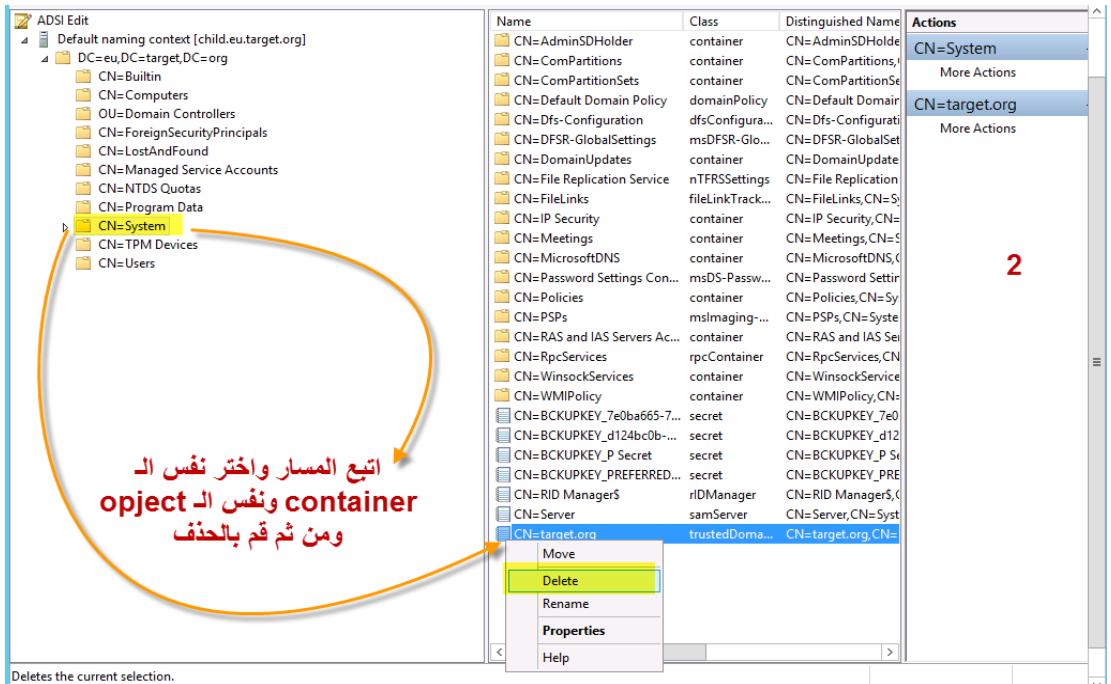
قلنا سابقا ان **PARENT AND CHILD TRUST** علاقة تنشأ تلقائيا أي هي من النوع **Built in** لذلك فانك لن تستطيع حذفها بالطريقة العادية وعلى ذلك فإننا سنقوم بحذفها يدويا وإعادة انشاؤها من جديد فتابع معي

كيف نقوم بحذف Built in Trust



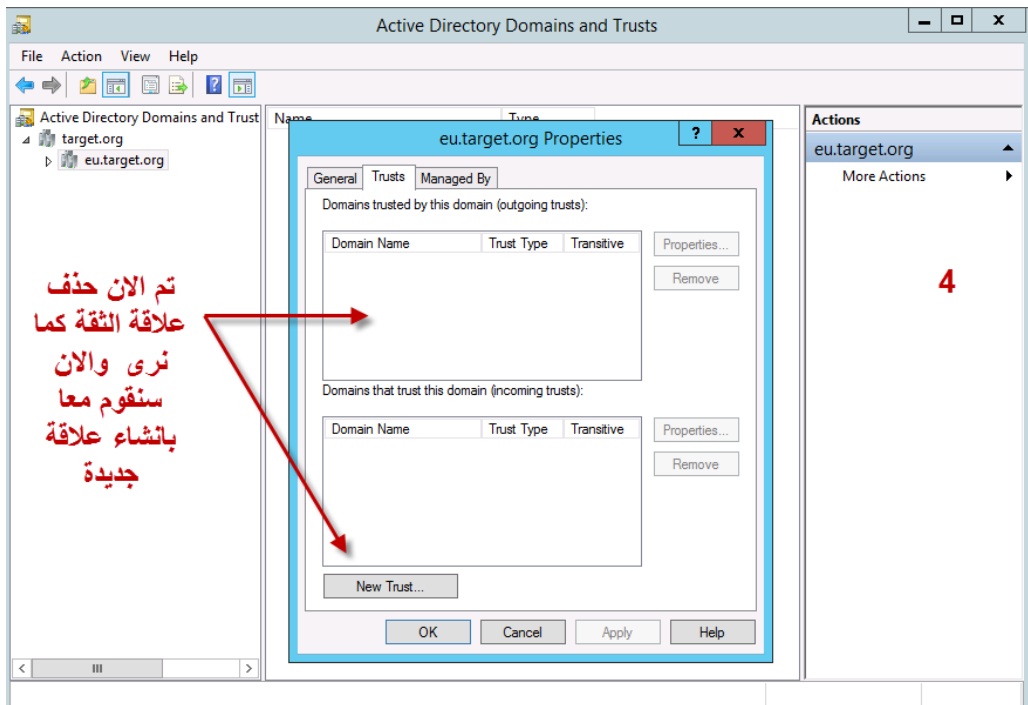
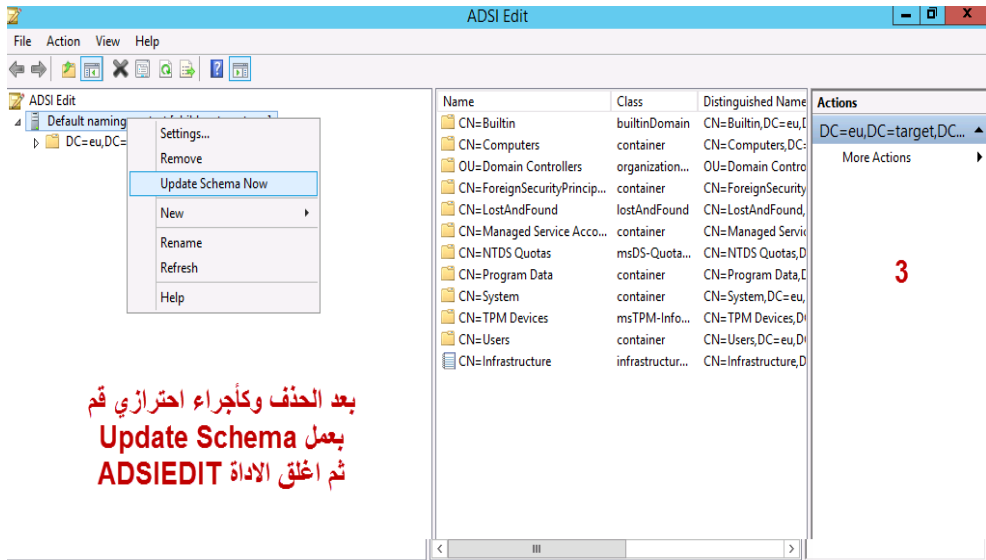
1

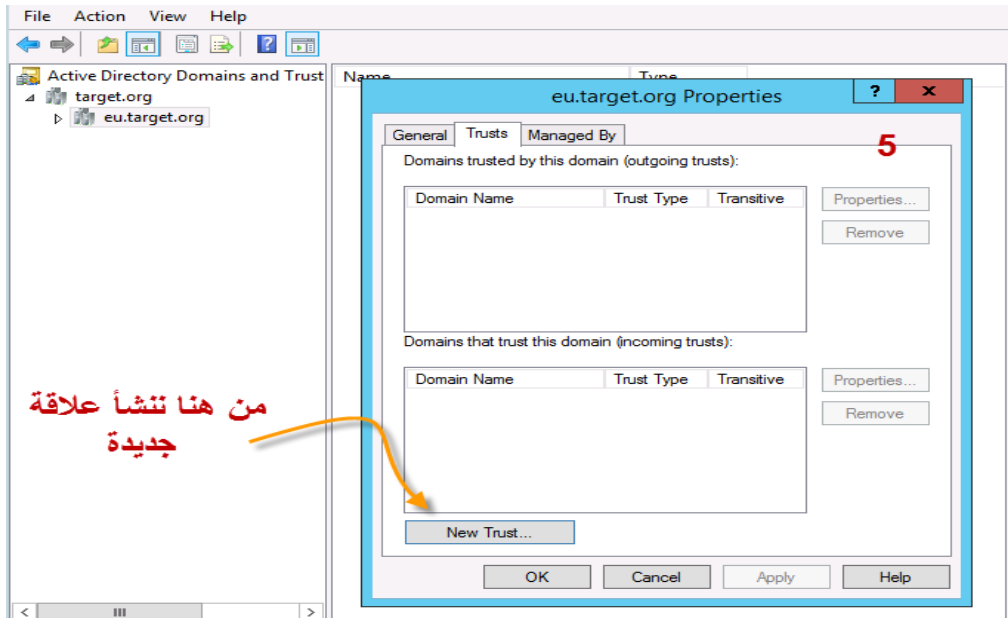
من داخل قائمة
الـ RUN الـ
هذه الاداة



اتبع المسار واختر نفس الـ
object container ونفس الـ
object ونفس الـ object
ومن ثم قم بالحذف

2





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:

الآن اكتب اسم الـ Domain Forest الذي سنقوم بعمل علاقة ثقة بمن خلاله

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

Active Directory Domains and Trusts
target.org
eu.target.org

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:

- 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
Child \ Parent كلاهما
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.

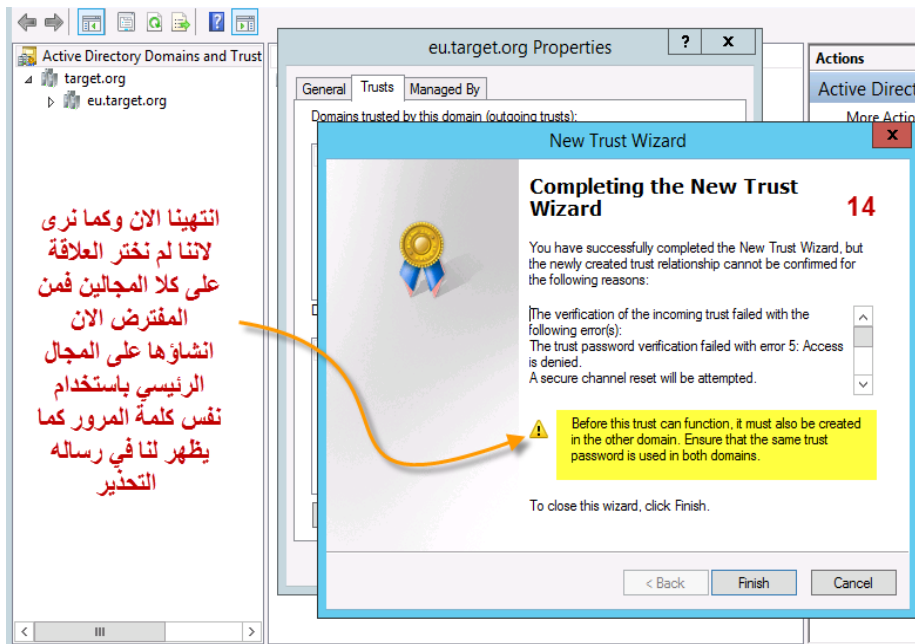
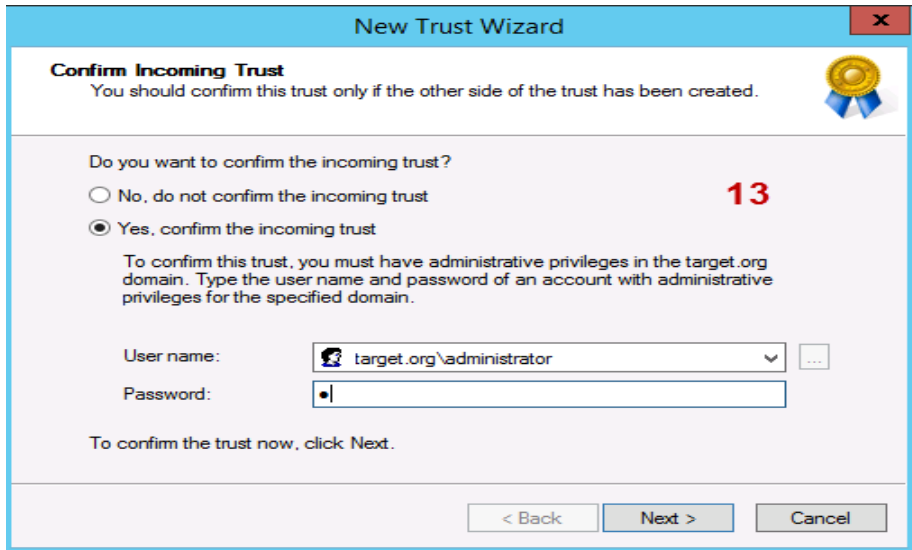
Trust password:

Confirm trust password:

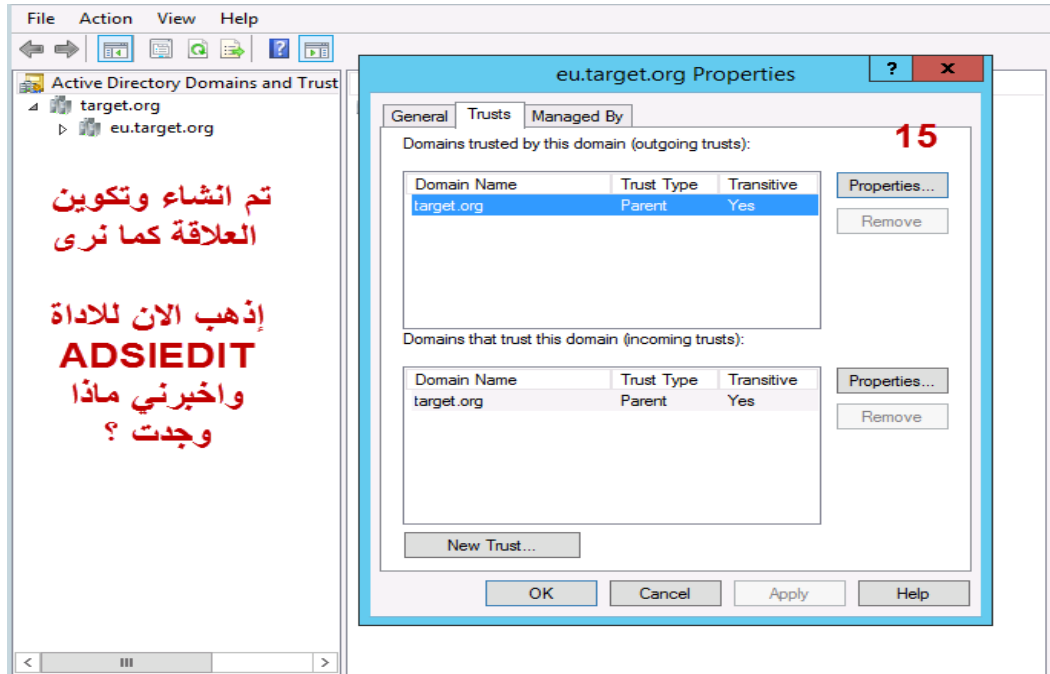
< Back Next > Cancel

ادخل كلمة المرور





انتبهنا الان وكما نرى
لاتنا لم نختر العلاقة
على كلا المجالين فمن
المفترض الان
انشاؤها على المجال
الرئيسي باستخدام
نفس كلمة المرور كما
يظهر لنا في رساله
التحذير



حسناً 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 تراجع معا مخطط شبكتنا



لاحظ أن مخطط الـ **Forest** يحتوى على مجال رئيسي واحد **Parent Domain** و عدة 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؟

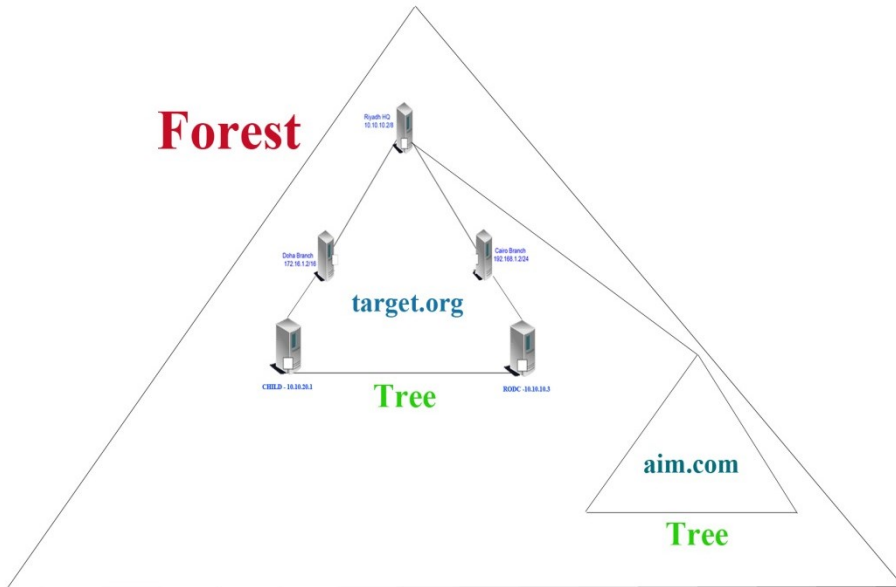
رائع جدا الـ **Tree** هو المكان الذي يحوي بداخله **Domain** واحد أو اكثر كما قلنا

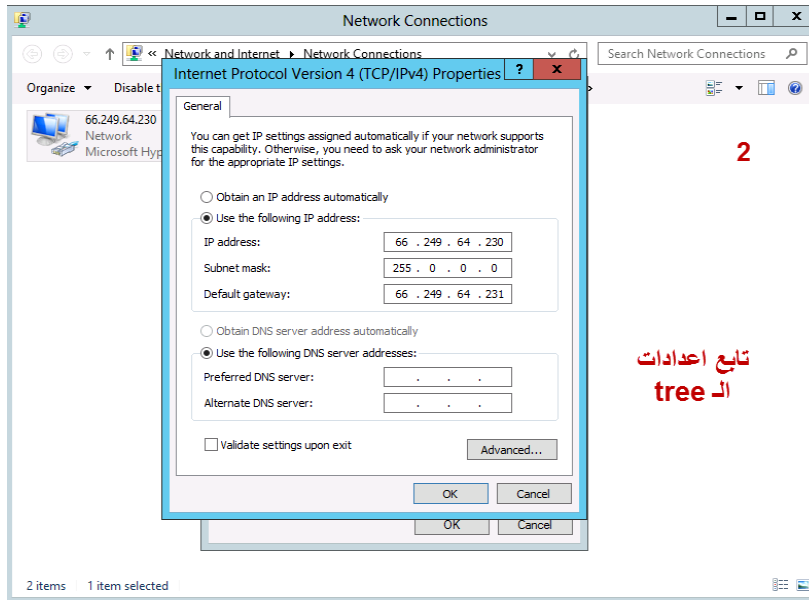
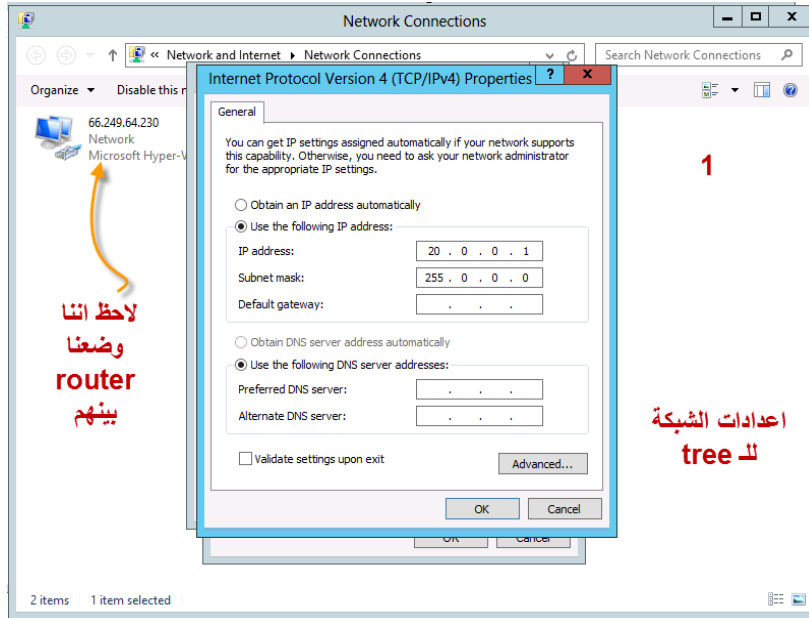
والغرض من انشاء الـ **Tree** هو عمل **Domain** جديد داخل الـ **Forest** الرئيسية

وما يميز الـ **TREE**

- لها قاعدة بيانات **Database** منفصلة تماما عن أي **Tree** أو **Domain** داخل الـ **Forest**
- لا تترث اسم الدومين الرئيسي مطلقا
- أيضا يمكن عمل **RODC / Child / Additional** 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**

Network and Sharing Center

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:\>

```

هل تلاحظ شيئا غير طبيعي ؟
حسنًا لنعد الآن لاعدادات الشبكة

See also
Internet Options
Windows Firewall

Network and Sharing Center

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:\>

```

والآن تكمل الخطوات

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

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

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 سابقاً في عمليات تكوين الـ Active Directory. إختار 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

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

Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results

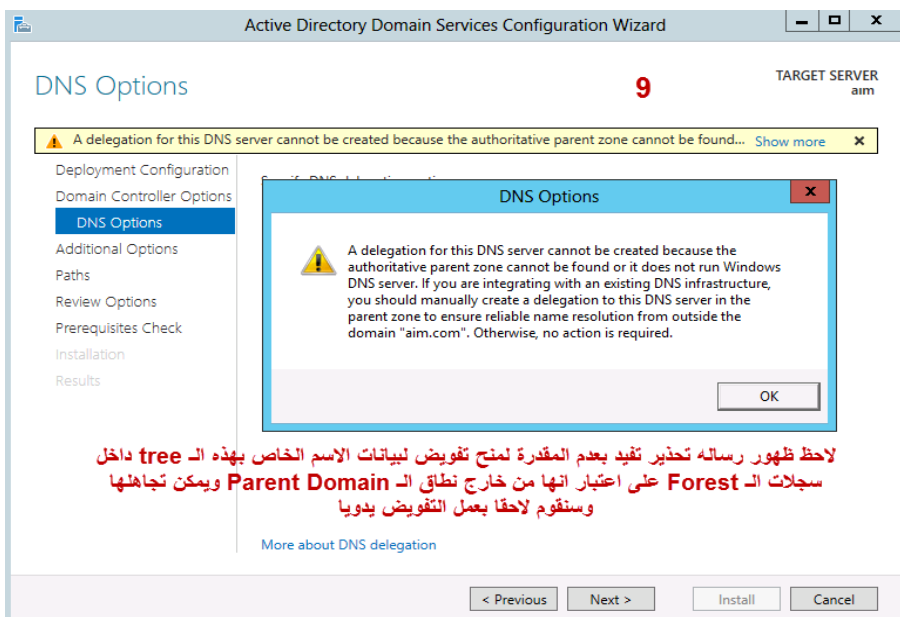
The default value for the NetBIOS domain name is already being used, one alternative has been suggested. [Show more](#)

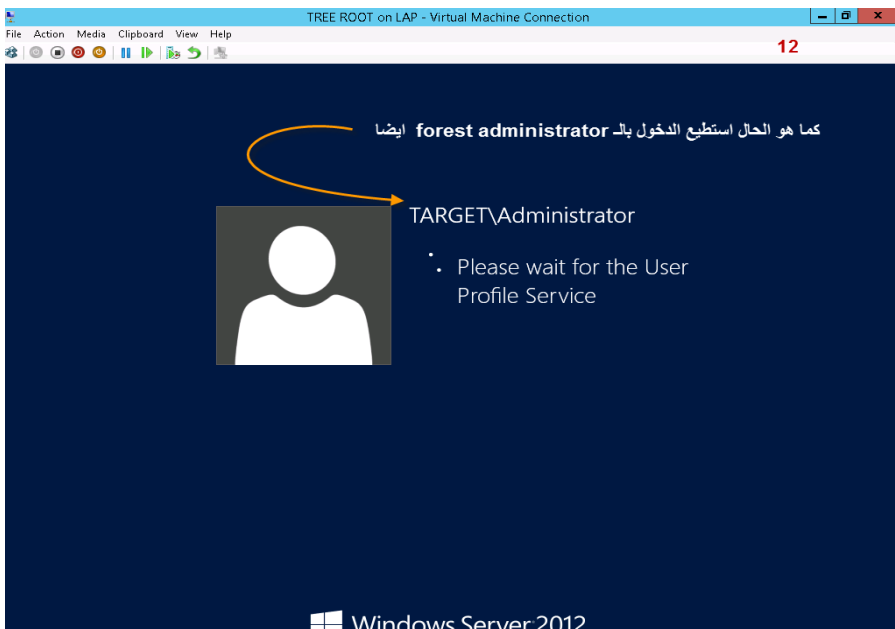
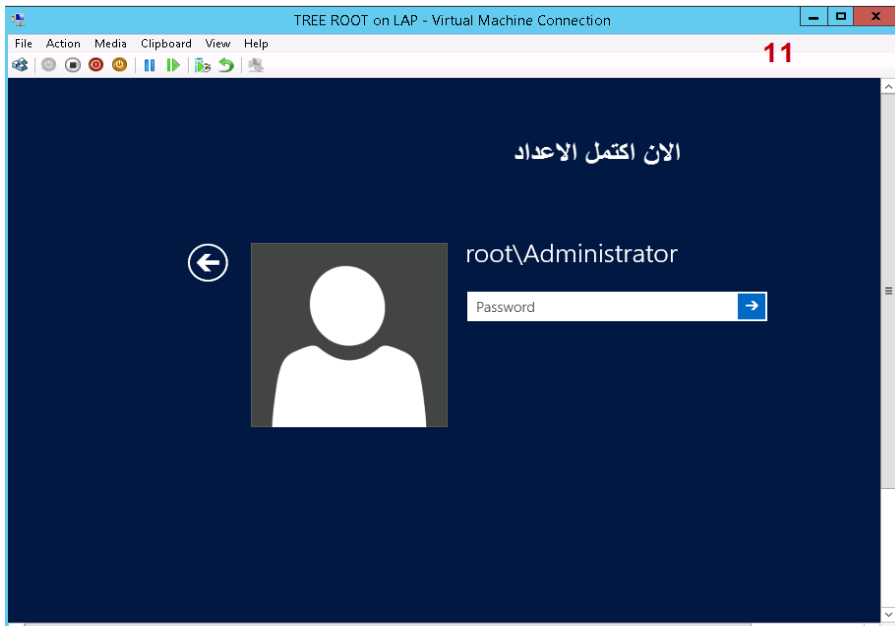
Verify the NetBIOS name assigned to the domain and change it if necessary
The NetBIOS domain name: root

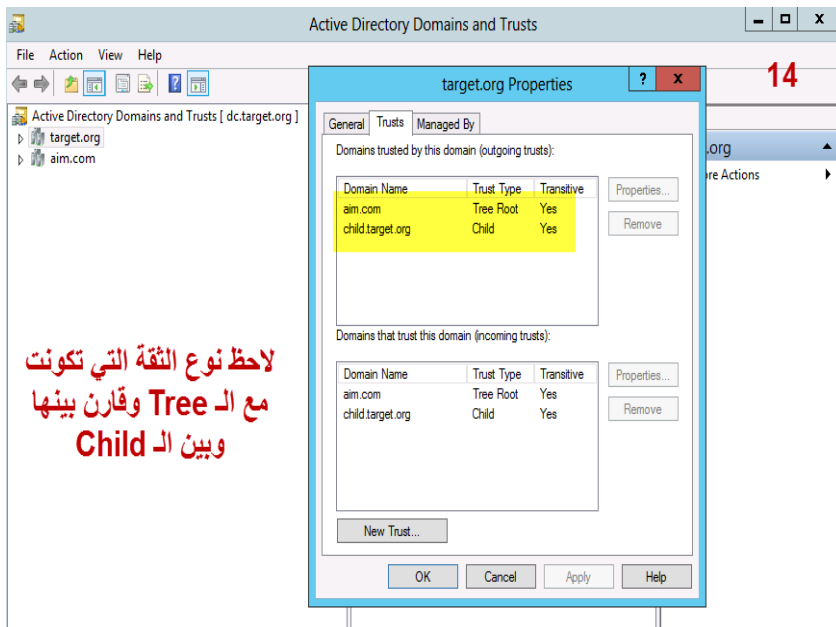
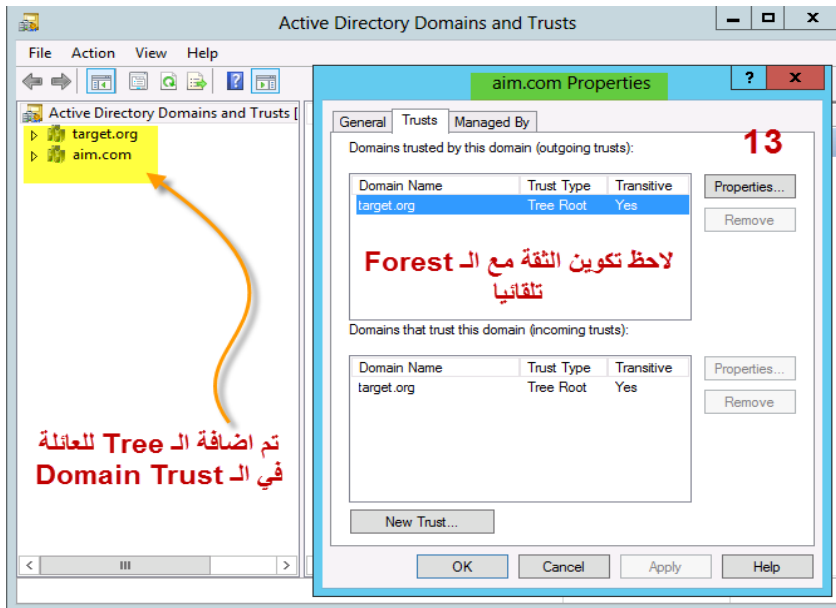
قمت بتغيير الاسم الى Root للدلالة عليه وهذا امر اختياري

[More about additional options](#)

< Previous Next > Install Cancel



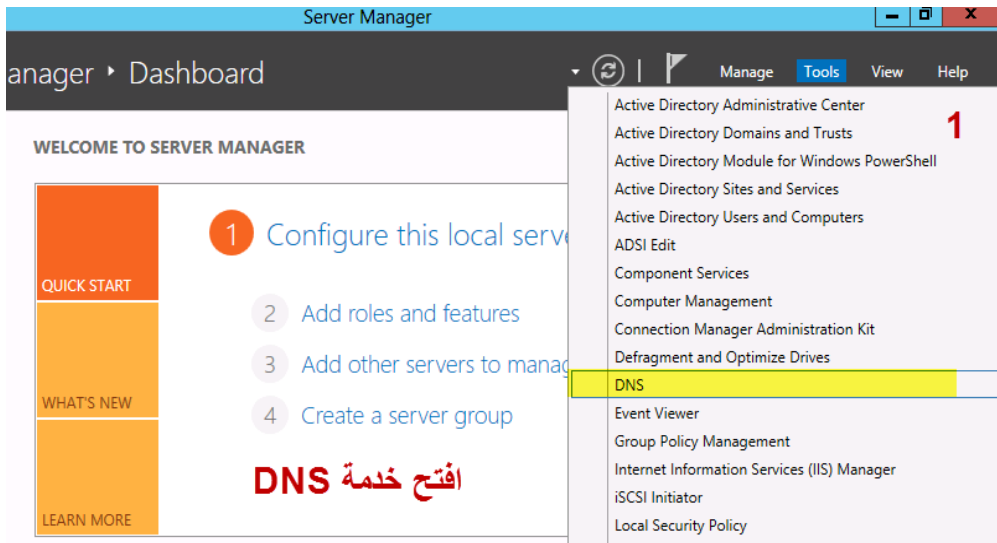


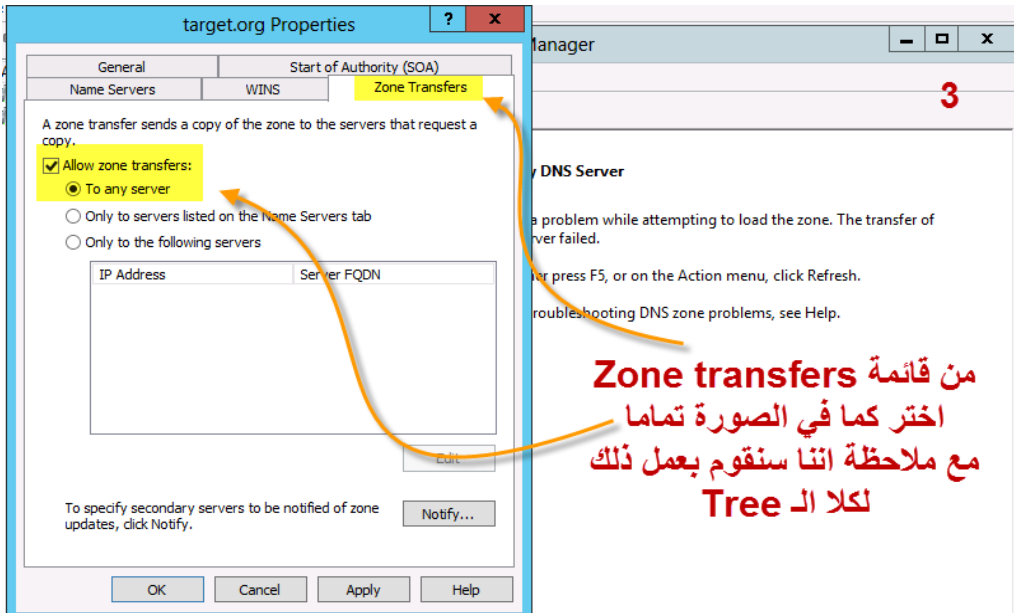
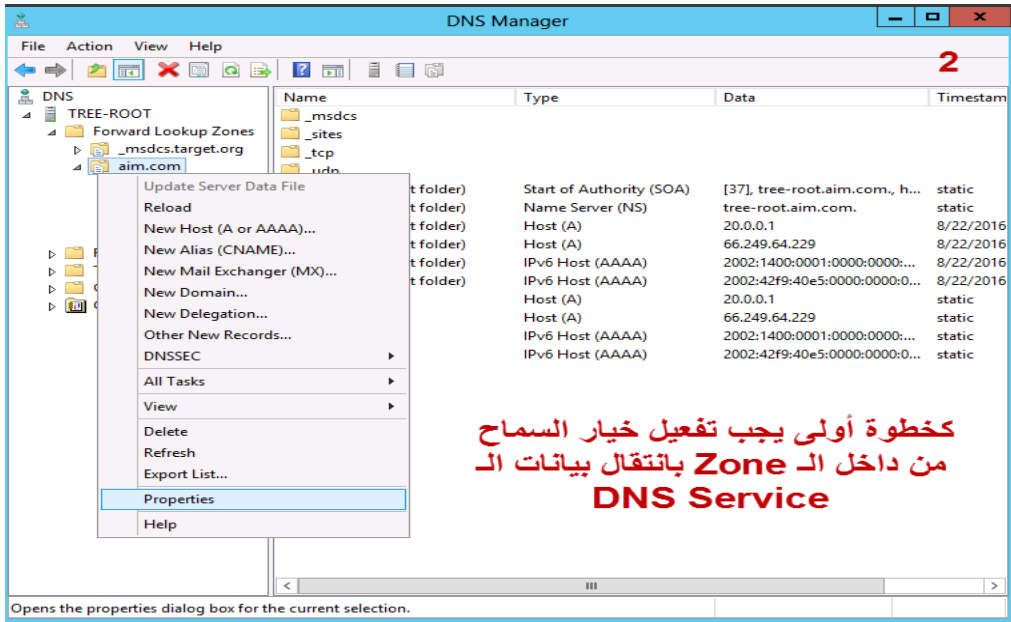


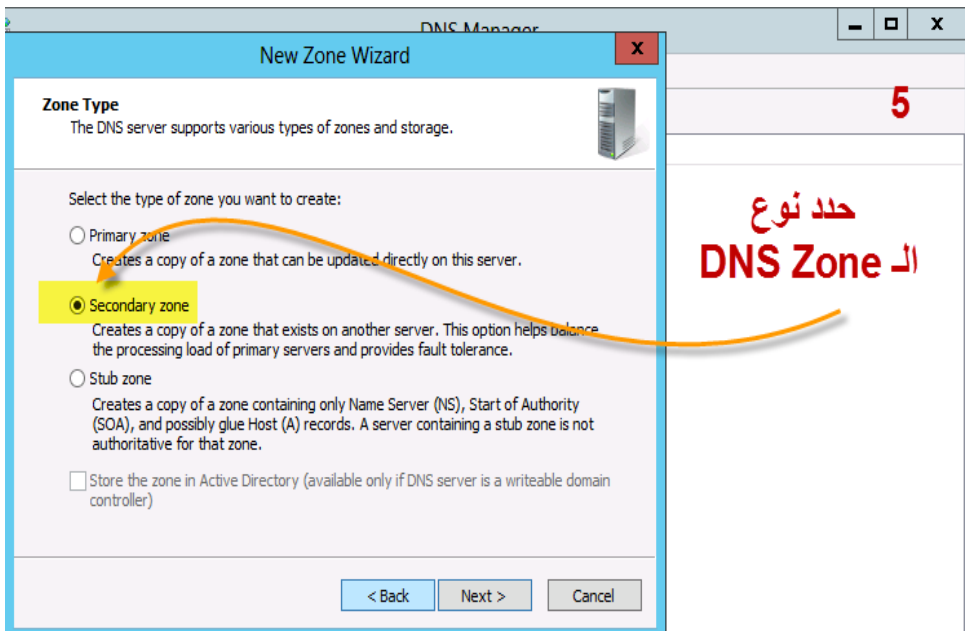
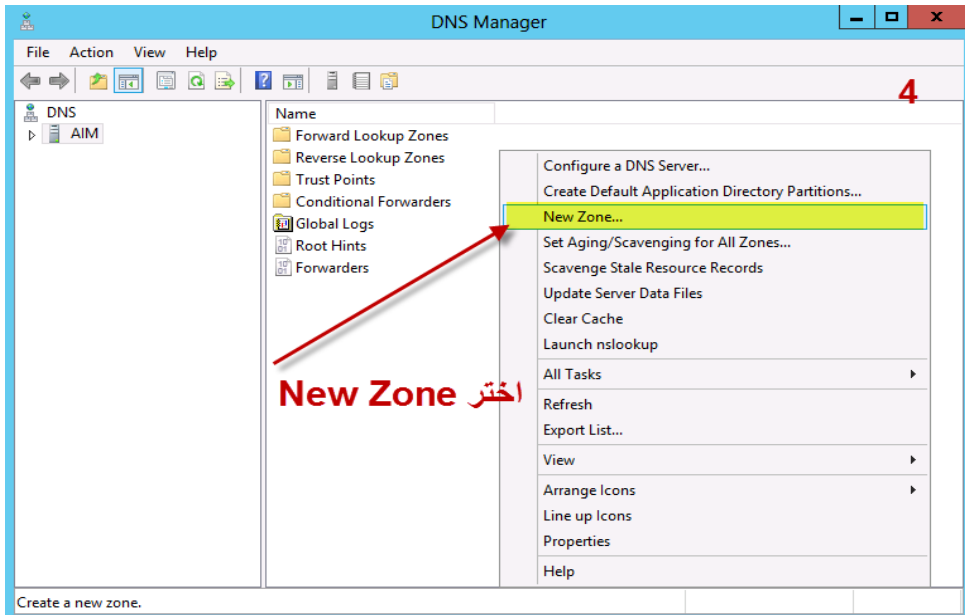
الان تم تكوين الـ **Tree** داخل الـ **Forest** واصبح لدي عدد 2 **tree** هما **target.org** و **aim.com** وتكونت بينهما علاقة تلقائية من نوع **TREE ROOT TRUST** ويستطيع الان المستخدمين في كلا الـ **root** الوصول الى مصادر بعضهما البعض ما دامت هذه العلاقة قائمة فلو كان لدي مستخدم باسم **khaled@aim.com** 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

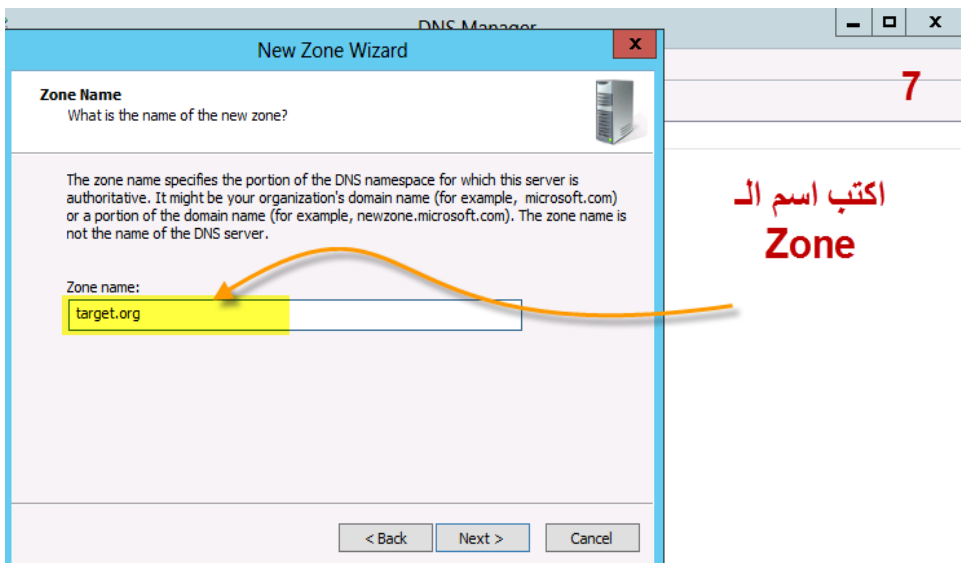
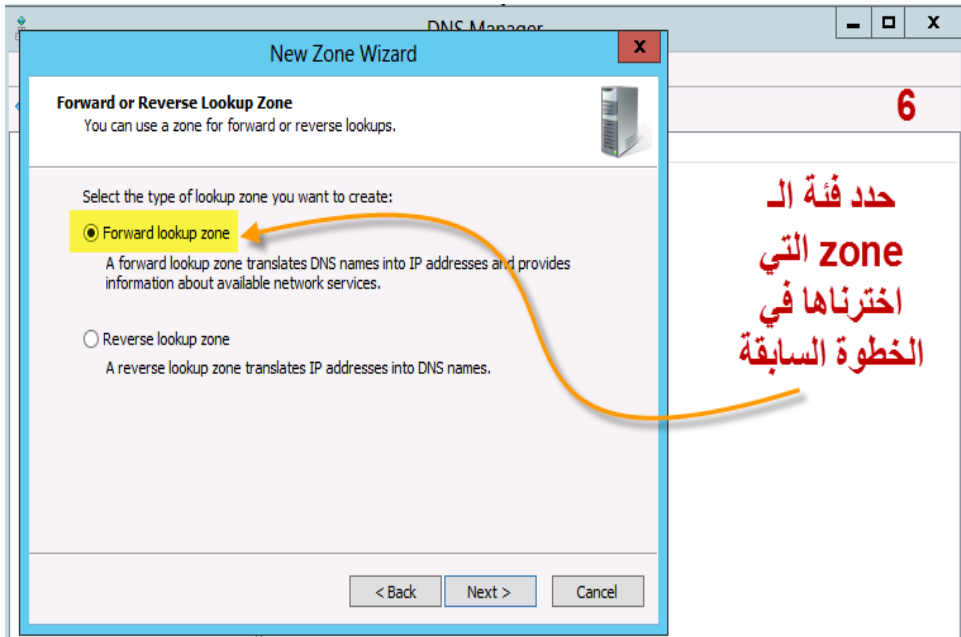
ويتم ذلك عن طريق ارسال طلب استعلام من جهاز خالد الى قاعدة بيانات **DNS** التابعة لمجال **aim.com** وبالطبع فان قاعدة البيانات تلك لا تحتوي على معلومات جهاز **yahya** فتترد بعدم القدرة على التعرف على هذه البيانات ومن ثم تطلبها من قاعدة البيانات الخاصة بمجال **Target.org** فيرد الـ **DNS** الخاص بالـ **Target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

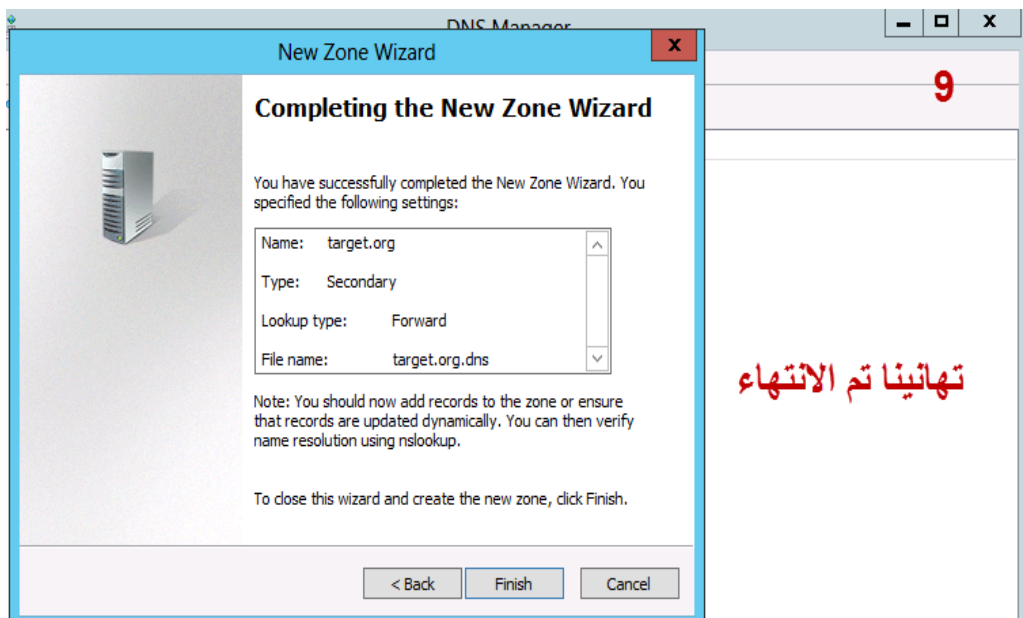
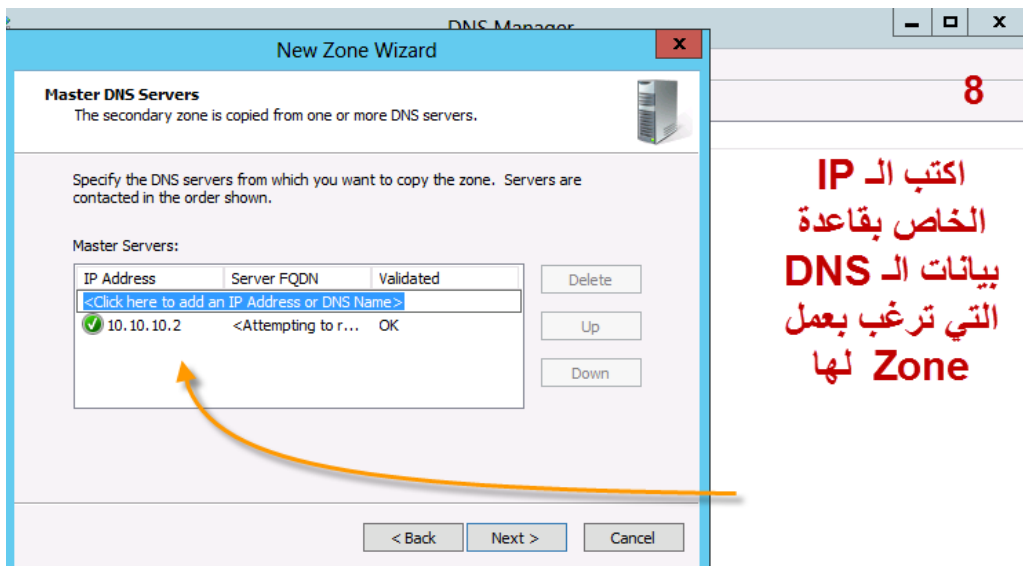
لكننا نستطيع توفير كل هذا الامر بالحصول على نسخة من قاعدة بيانات **DNS** الخاص بالـ **Target Tree** وتخزينها مع قاعدة بيانات **DNS** التابعة لمجال **aim.com** والعكس أيضا وبذلك سيتمكن كلا المستخدمين في كلا المجالين من الحصول على البيانات من نفس الـ **DNS** التابع لهم والطريقة تتم كالتالي :











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	Timestamp
_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)	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

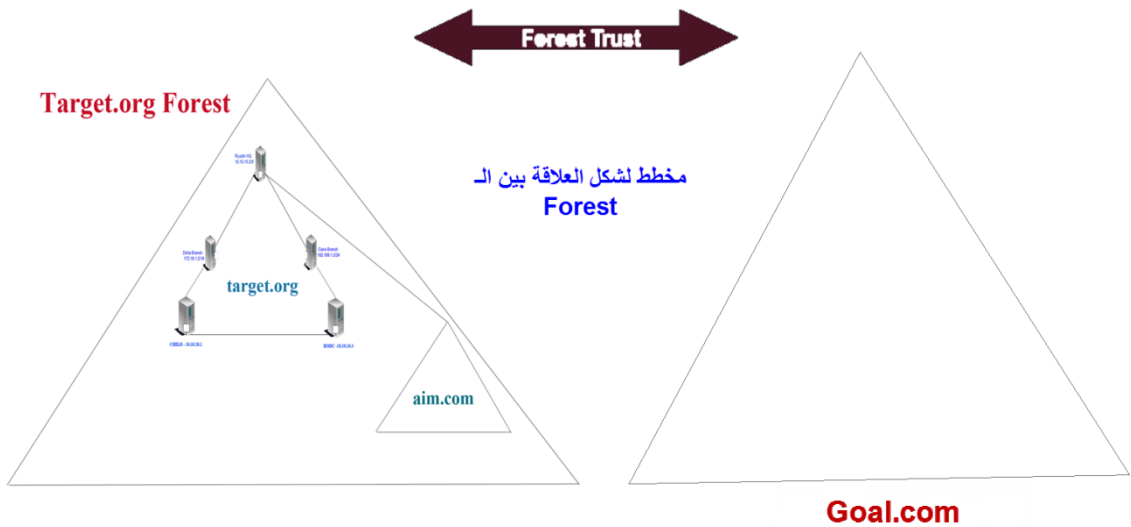
موضوعنا الاخير في هذا الجزء من الكتاب هو اجراء الثقة بين أكثر من Forest لذلك سوف نقوم بعمل **New Forest** ثم نحاول تكوين علاقة ثقة فيما بينها وبين الـ **Target.org Forest**

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 svr 2012)

local ip is 96.10.20.10 /24

Real Ip For Routing is 66.249.64.228/8

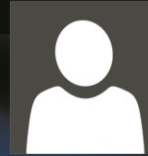


انتهى الجزء الاول



```
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=Conf i
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: _
```



Administrator
TARGET\Administrator



ACTIVE DIRECTORY

PRACTICAL GUIDE PART I

