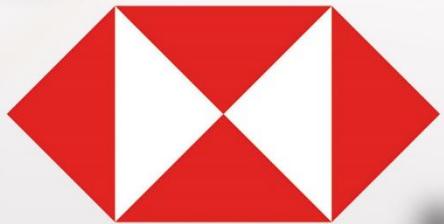


HSBC



The Hongkong & Shanghai International Banking Corporation



BASSEL AFLAK
ABDULRAHMANA AKKAD
FARES HADDAD
HAMZE ALHARSTANI
HASAN ALMUNAJED
FIRAS SHAHER
MOHAMMAD AODEH
FARES BASALE

SUPERVISOR:
ENG. SHEREEN ASSAF



فكرة المشروع:

بناء شبكة لبنك HSBC (The Hong Kong & Shanghai International Banking Corporation) تؤمن الاتصال الدائم ما بين الفرع الرئيسي في دمشق مع بقية الأفرع في سوريا، كما تؤمن الربط بالإنترنت للاتصال مع بقية الأفرع في جميع أنحاء العالم؛ بالإضافة إلى الربط مع شركة WU (Western Union) للصرافة وتحويل الأموال وذلك لتسهيل عملية إدارة حسابهم بسماحيات محدودة.

أهداف المشروع:

- الهدف الرئيسي بناء الشبكة بموثوقية عالية تضمن الاتصال الدائم من خلال تأمين خطط ربط بديلة احتياطية محكمة
- في حال انقطاع الاتصال جزئياً أو كلياً سواء ما بين الأفرع أو ضمن الفرع الواحد، وضمان الأمان العالي للبيانات الحساسة من التلف أو الضياع باستخدام تقنيات التخزين والنسخ الاحتياطي المناسبة.
- تأمين الأجهزة الاحتياطية على كل المستويات من تجهيزات شبكة ووصلات احتياطية بينها واعتماد بروتوكولات تعمل على توزيع الحمل والربط الاحتياطي على كل المستويات كما تأمين وسائل التخزين الاحتياطية والخدمات الاحتياطية لضمان عدم توقف الخدمات إلا لفترة محدودة من الزمن.
- استخدام أحدث الطرق والتقنيات والتجهيزات المتوفرة من أجل ضمان السرعة والأداء العالي مع مراعاة التكلفة المناسبة.
- تمركز التجهيزات والأجهزة التي تدير الشبكة ضمن الفرع الرئيسي في دمشق ضمن غرفة الشبكة ذات الجاهزية العالية لضمان البيئة المناسبة لعمل هذه التجهيزات لتعود بأعلى مردودية عمل ممكنة.
- ربط الأفرع عبر الـ WAN باستخدام تقنيات متعددة مع ضمان إتاحة التجهيزات المستخدمة للربط بين الأفرع.
- استخدام تجهيزات مناسبة على حسب الضغط ضمن الفرع لضمان تكلفة منخفضة بأداء عالي.
- ضمان سهولة ادرأه الشبكة بتنبيه الخدمات التي تساهم وتساعد في تسهيل عملية الإدارة والمراقبة للشبكة على فريق الإدارة الرئيسي المتواجد في الفرع الرئيسي في دمشق حيث تتم إدارة الأفرع في سوريا بشكل مركزي من دمشق بالتنسيق مع الفنيين في بقية الأفرع.
- اعتماد سياسة امنية صارمة للشبكة للعمل على تأمين الشبكة من الخروقات على جميع المستويات داخلياً وخارجياً.
- تأمين مصادر الطاقة الكهربائية ودورات عدم انقطاع التيار لضمان عدم توقف التجهيزات والخدمات والحواسيب عن العمل في حال انقطاع التيار الكهربائي.



القسم النظري
Theoretical Division



Network Design

تقسيم طبقات الشبكة:

Routers والمتمثلة بال Edge Layer

Multilayer Switches ممثلة ب Core Layer + Distribution Layer

L2 Access Switches والمتمثلة ب Access Layer

MSTP (Multiple Spanning Tree Protocol)

وهو أفضل بروتوكول مطور من بروتوكول spanning tree حيث يتيح لنا جمع أكثر من VLAN ضمن Instance بحيث يكون لكل Instance طريق منطقي خاص به، على عكس PVST+ الذي يوفر طريق منطقي لكل VLAN على حدي، فهذا يوفر من استهلاك موارد المعدلات من CPU cycle & RAM Memory ويعطي أداءً أفضل حيث أن هذه الآلية سوف يتم تطبيقها نفسها بالفرعين.

تقسيم ال VLANs على ال Instances ضمن الفرع الرئيسي

Instance 1 :

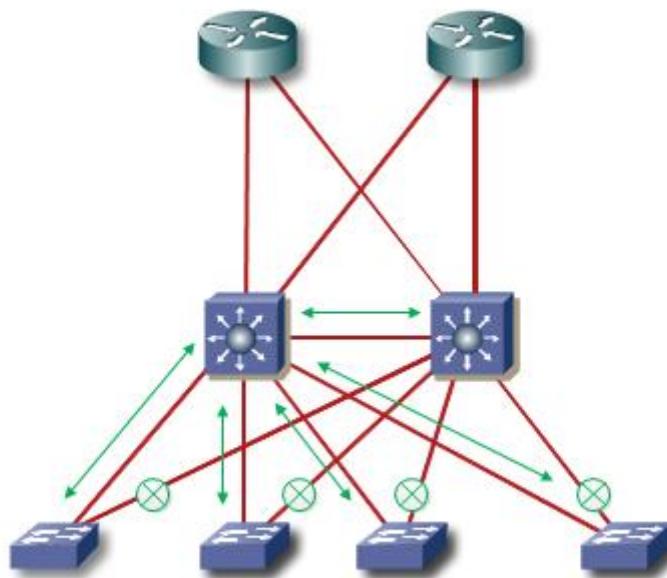
Management VLAN

IT-technical VLAN

IT-Network VLAN

IT-Administration VLAN

Servers VLAN



Instance 2:

Costumer-serv VLAN

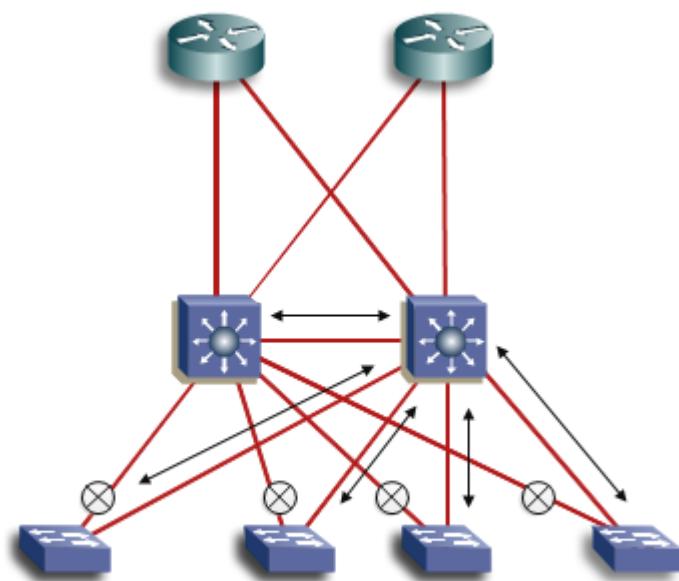
Accounting VLAN

Security VLAN

HR VLAN

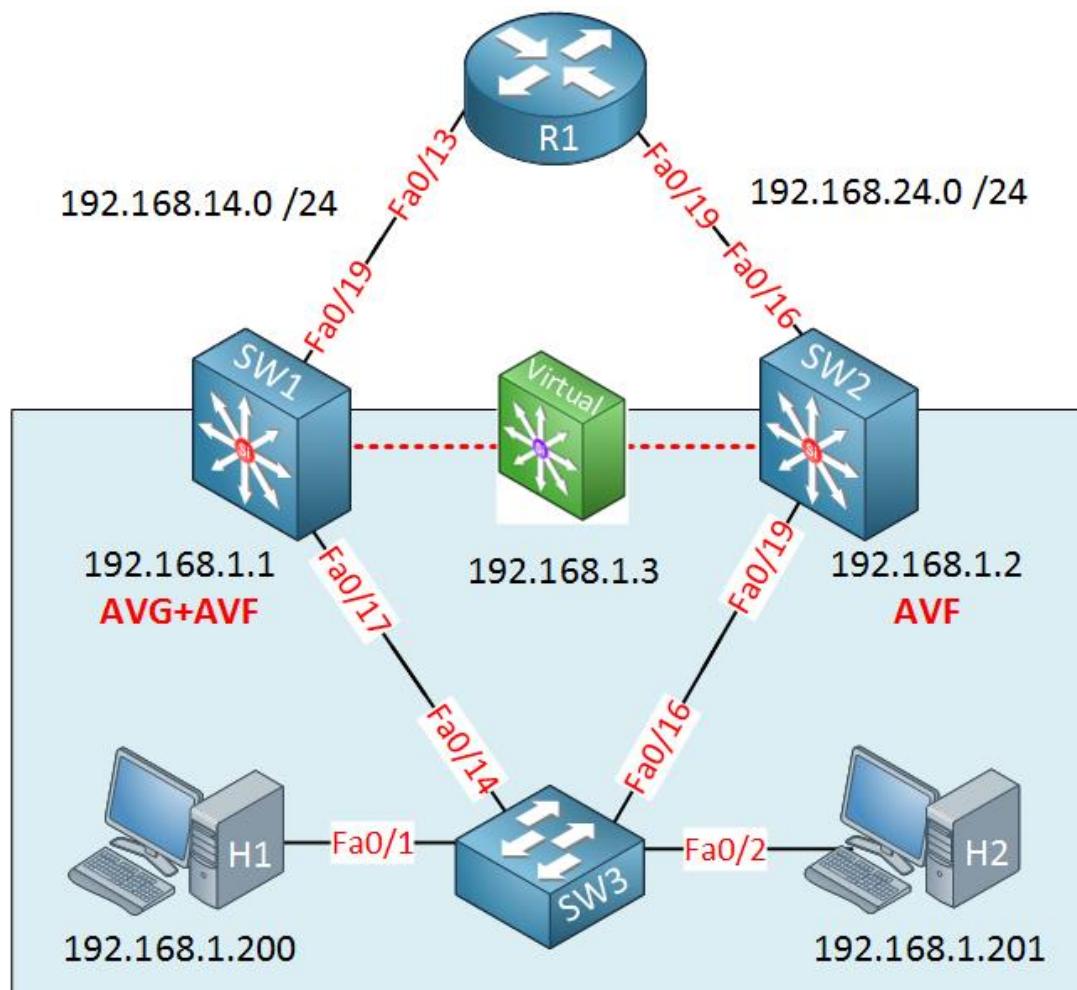
Internal-Tran VLAN

National-Tran VLAN



GLBP (Gateway Load Balancing Protocol)

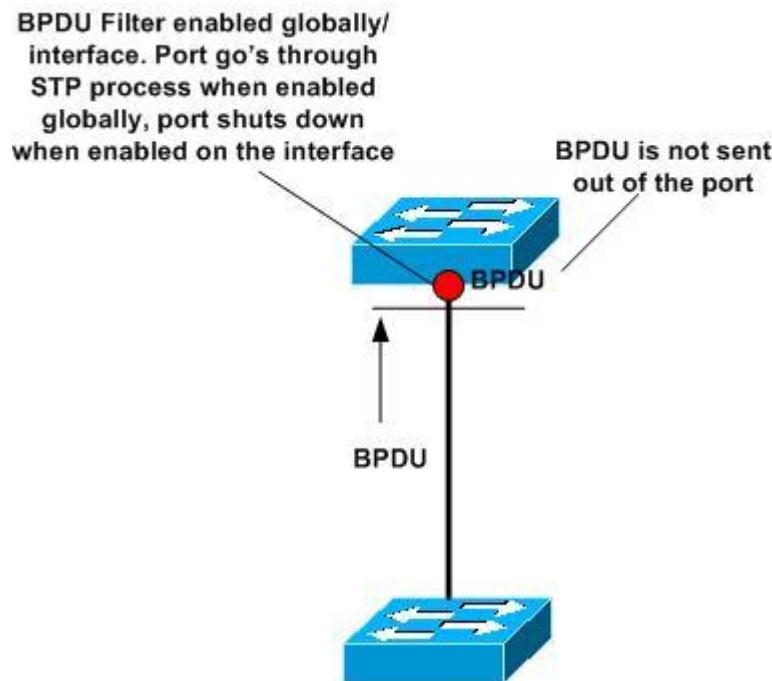
ملکية شركة Cisco ويؤدي نفس مهمة HSRP بالإضافة إلى Load Balancing حيث تصبح التجهيزات المشتركة بالخدمة والمطبقة عليها إعدادات هذه الخدمة في حالة Active – Active وليس Active – standby.





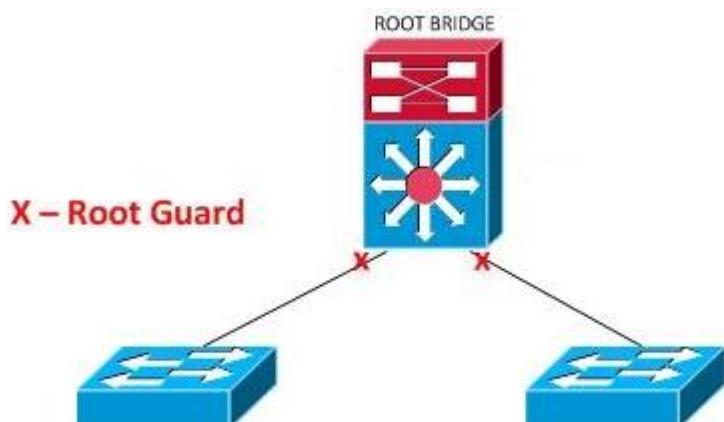
BPDU Filter

هي خاصية تستعمل لحماية spanning tree من أي تأثير خارجي ويتم تفعيلها على المنفذ المتصلة مع end points (hosts) والمفعول عليها خاصية port fast حيث تمنع المنفذ من استقبال أو إرسال BPDU أي بمعنى آخر تعطل خدمة spanning tree على المنفذ في حال تم وصل مبدل على هذا المنفذ فأن المبدل الجديد سوف يقوم بإرسال BPDU ويتفاوض مع باقي المبدلات لانتخاب Root Bridge جديد ويمكن أن يتسبب بloop في الشبكة ويقوم بتغيير spanning tree topology.



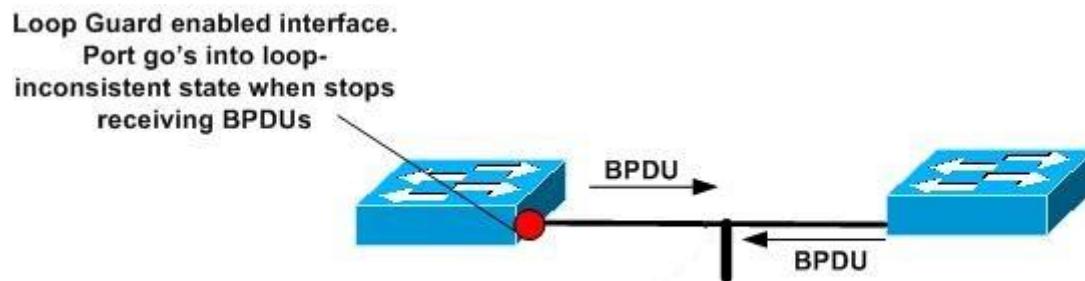
Root Guard

وهو خاصية تقوم بتفعيلها على منافذ Flapping interface في حال إصابة مشكلة Root Bridge للأحد منافذ non Root Bridge فحسب سلوك المبدلات يمكن أن يجعل Root Bridge بالاعتقاد أن Root Bridge أصبح خارج الخدمة وبالتالي سوف تقوم المبدلات بالدخول في حالة انتخاب Spanning tree جديداً والتسبب بتغيير Root Bridge Topology، وهذه الخاصية تسمح بالإبقاء على Bridges كما هي.



Loop Guard

وهي خاصية تسمح بتتبع BPDUs على المنفذ المفعة على عليها هذه الخاصية ونقوم بتفعيلها على Non Root ففي حالة قد تتسبب بضياع Flapping interface BPDUs وفي هذه الحالة سيعتقد المبدل Non Root بأن الوصلة بينه وبين أصبحت خارج الخدمة وسوف يقوم بوضع المنفذ الذي حاليته Blocking Forwarding بحالة Root Bridge في الشبكة ولكن هذه الخاصية سوف تقوم بوضع المنفذ بحالة Loop-inconsistent إلى حين استقبال .Root Bridge من BPDUs

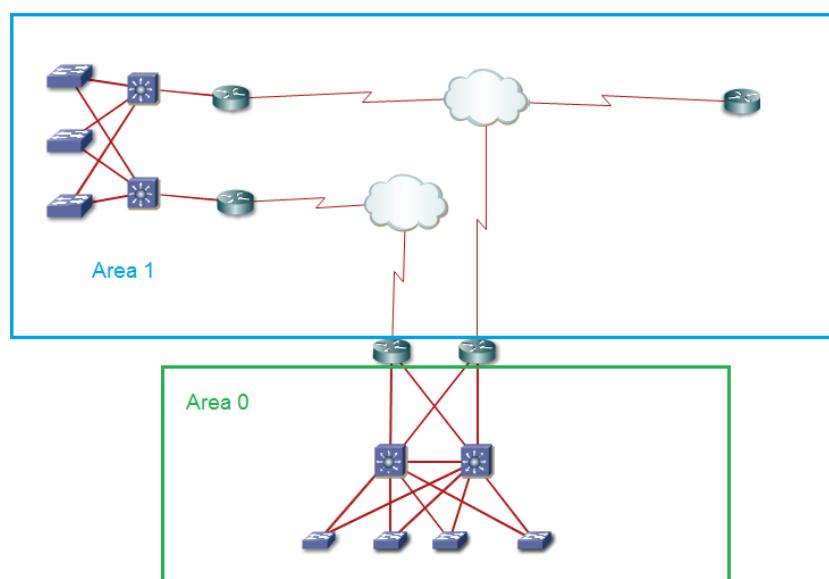


Port Fast

وهي خاصية نقوم بتفعيلها على المنفذ الموصولة مع End Points(hosts) حيث تضع المنفذ مباشرة في حالة دون المرور بحالي Listening and Learning والتي تستغرق 30 ثانية. Forwarding

OSPF (Open Shortest Path First)

وهو بروتوكول توجيه لبروتوكول IP، يتبع خوارزمية Link State Routing (LSR) ويصنف من مجموعة Interior Gateway Protocols (IGPs) مفرد التمثيل على المخطط:





SSH (Secure Shell)

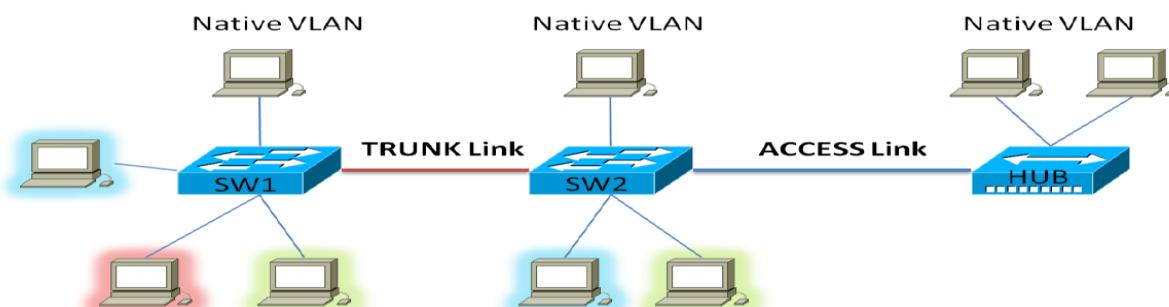
وهو بروتوكول لتشغيل خدمات الشبكة بشكل آمن عن طريق شبكة غير آمنة والاستخدام الشائع لها هو Remote Login للأجهزة وتنفيذ الأوامر عليها وفي شبكة سوف يتم تفعيل هذه الخدمة على كل الموجهات والمبدلات.

Banner

وهي رسالة توضيحية وتحذيرية تظهر عند فتح جلسة SSH أو Telnet مع التجهيز المراد الدخول إليها في حال أراد الـ Hacker الدخول إلى التجهيز واستطاع الدخول دون أن تظهر له رسالة تحذيرية فلا يمكن اعتبارها جريمة إلكترونية ولكن في حال تم تحذيره ومع ذلك اخترق الشبكة فإنها تعتبر جريمة إلكترونية ويمكن محاسبته عليها.

Trunk

عندما يقوم جهاز بإرسال packet إلى جهاز آخر ضمن الشبكة يقوم الـ switch بإضافة tag على الـ packet حسب الـ trunk protocol وهذا عمل الـ Vlan الذي يتمنى إليه مما يسمح بمرور الـ Vlan



:trunking protocol

: ISL(inter-switch link) -1

هو Cisco protocol خاص به يقوم بإعادة تغليف packet ووضع header وفوس من FCS جديد

-2 هو 802.1Q: هو protocol standard حتى

بالنسبة لـ Cisco يقوم الـ switch بوضع tag على الرسالة عند تلقيه من الـ host وعندما تصل الرسالة للـ host يقوم بإزالة هذا الـ tag لأن الأجهزة لا تفهم معنى tag وهذه الخاصية تستخدم حصر ضمن الـ switch

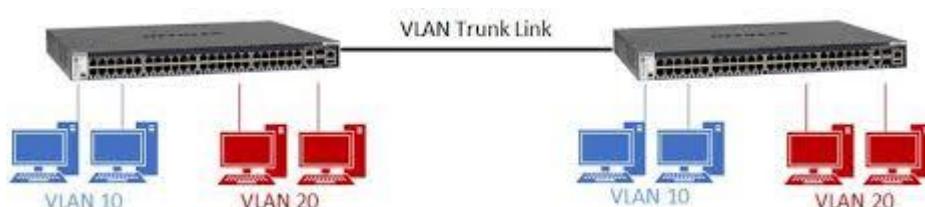
Vlan (Virtual LAN)

- مبدأ عملها نقوم بتجمیع المستخدمین فی مجموعات ضمن الـ switch الواحد
- نقوم بتقسیم الـ Vlan على حسب عدد الـ broadcast
- كل Vlan منفصلة عن الأخرى ولا يمكن الوصول لها من قبل Vlan أخرى
- استخدام الـ Vlan يحسن من أداء الشبکة على عکس ذلك نقوم بتحفیض مدى انتشار الـ broadcast في الشبکة
- إذا أردنا تقسیم الشبکة بدون استخدام الـ router نحتاج إلى Vlan للتوجیه بين الشبکة والأخرى مما یسبب التکلفة العالية

DAMASCUSE	
Vlan id	Name Vlan
5	servers
10	Network_Administration
20	IT
30	Technical_Administration
40	Technical_support
50	management
60	HR
70	internal_trades
80	international_trades
90	Customer_Services
100	Accounting
110	Security

- نستطيع من خلالها فصل الأقسام المهمة في الشبکة عن الأقسام الغیر مهمۃ يمكن إعطاء أولوية عالیة للبيانات الحساسة
- نذكر الـ Vlans الموجودة في شبکتنا في كلا الفرعین:

HOMS	
Vlan id	Name Vlan
115	Servers_homs
120	IT_homs
130	HR_homs
140	Network_Department
150	Accounting_homs
160	network_room
170	mangment_homs
180	Customer_Services_homs

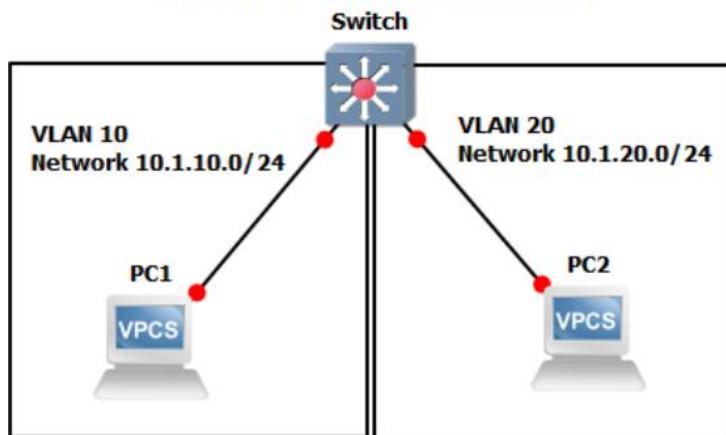




Inter Vlan routing

للتوجيه بين الـ VLANs التي هي شبكات وهمية على switch واحد نحتاج إلى router ليصل بينهما sub لـ switch layer 3 الذي يعمل عمل الـ router بينما يتوجه لنا باستخدام شيء مشابه لـ

RVI Address 10.1.10.1 /24 for Vlan 10
RVI Address 10.1.20.1 /24 for Vlan 20



بينما في شبكة استخدمنا switch interface لكن ليس على port محدد وإنما داخل الـ SVI (switched virtual interface) تسمى switch L3 interface

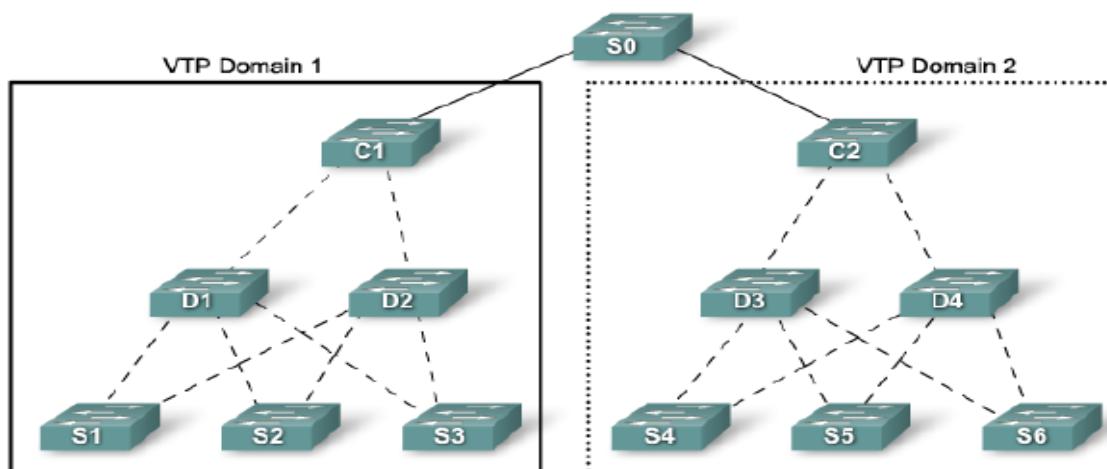
- خطوات الانشاء على switch L3
 - إنشاء SVI على كل Vlan
 - إعطاء عنوان لكل SVI حسب عنوان الـ Vlan
 - تفعيل استخدام الطبقة الثالثة على الـ switch
 - جعل الـ default-gateway للحاسوب الموصول على الـ Vlan هي SVI المخصصة لكل Vlan

VTP

هو protocol خاص بشركة Cisco وهذا الـ protocol يعمل على أجهزة الـ switch وفكرةه يقوم بإنشاء الـ VLAN بطريقة أوتوماتيكية على الـ switch واحد ومن ثم يقوم بتوزيعه على باقي الـ switches الموجودة في الشبكة

يعتمد بـ protocol vtp على الـ revision number وهو رقم يمثل حالة الـ switch vtp قبل تفعيل الـ vtp على الـ switch يكون $vtp = 0$ وعند تفعيله يصبح واحد عند كل تعديل على معلومات الـ VLAN يرتفع الـ revision number

معلومات الـ VLAN تكون مخزنة في flash الخاص بالـ switch vlan.net الذي يتم تبادله بين الـ switches عند ارتفاع الـ revision number





Vtp mode

يوجد ثلاثة حالات لـ switch بالنسبة لـ protocol vtp

: Vtp server -1

نستطيع إضافة VLAN وتعديل عليها وحذفها أو إعدادات الـ switch الأخرى كما يقوم بإرسال واستقبال تحديثات الـ VLAN من الـ switches ذات الـ revision number الأعلى

: Vtp client -2

يشابه vtp server لكن الاختلاف الوحيد لا يسمح بالتعديل أو إضافة وحذف الـ VLAN

: Vtp transparent -3

يختلف عن النوعين السابقين بعدة أمور:

- يسمح بتعديل الـ vlans عليه

- الـ VLAN التي تضاف لا تنشر إلى الشبكة

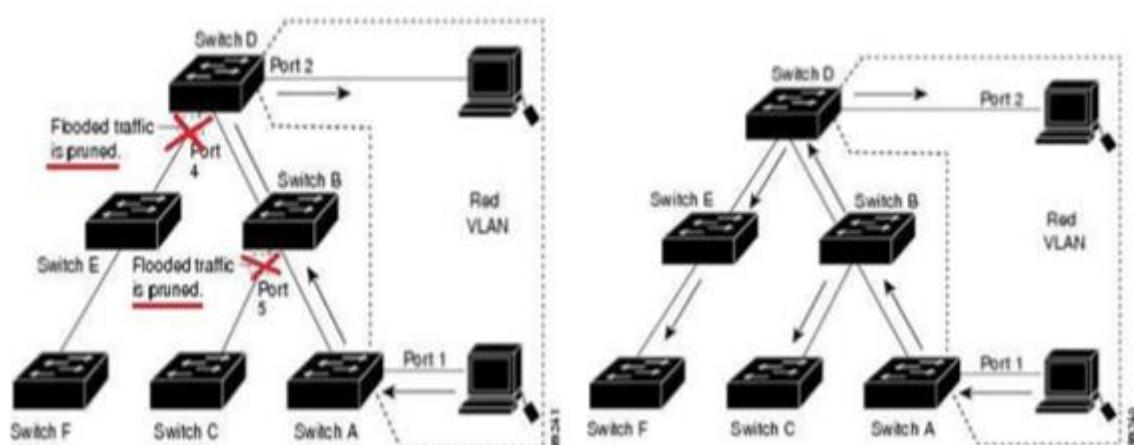
- في حال كان 1 vtp version يقوم بتحديث الـ VLAN من الـ switch ذات الرقم الأعلى

- في حال كان 2 vtp version يقوم بأخذ تحديثه الـ vtp وإرسالها للـ switches الموصولة عليه لا يأخذ التحديثات لنفسه

VTP pruning

سنستخدمها في حالة نريد إيقاف إرسال البيانات بشكل broadcast في حال كان لا يوجد أي PC من VLAN معينة لا يقوم بتمرير رسالة الـ broadcast إلى الـ VLAN

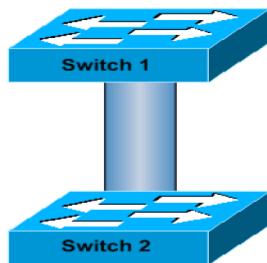
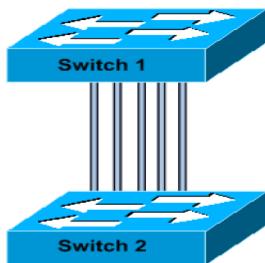
تكون موجودة على الـ VTP server لأنها هو الذي سيقوم بحجب الرسائل بعد التفعيل الـ pruning الشبكة قبل تفعيل الـ pruning





Ether channel

هي تقنية يتم فيها دمج أكثر من منفذ موجودين على نفس الـ switch ليتم العمل وكأنهم منفذ واحد بسرعة عالية جدا يجب أن تكون جميع المنافذ في الـ switch من نوع واحد وشرط أن تكون trunk ويكونوا سرعة واحد لا تختلف من إلى آخر في نفس الـ port



التي تدعم هذه التقنية: Protocols

Port aggregation -1
cisco (PAGP) protocol

وهو بروتوكول من مؤسسة IEEE وهو يعمل مع جميع Link aggregation control protocol (lacp) -2
الأجهزة

وهنا جدول يوضح الفرق بين البروتوكولات في عملية الاتصال بين المنافذ :

protocol	Link A mode	Link B mode	Negotiation result
PAGP	Auto	Auto	No negotiation
	Auto	Desirable	Negotiation successful
	Auto	On	No negotiation
	Desirable	Desirable	Negotiation successful
LACP	Passive	Passive	No negotiation
	Passive	Active	Negotiation successful
	Passive	On	No negotiation
	Active	Active	Negotiation successful

فوائد التقنية:

- الحصول على bandwidth عريض يقوم بجمع 4 links متساوي ممكّن أن تصل إلى 80 gig
- يقوم بتوزيع الحمل متساوياً
- يوفر الـ redundancy أي عطل في أحد physical links يتم تحويل الـ frame إلى آخر في نفس الثانية



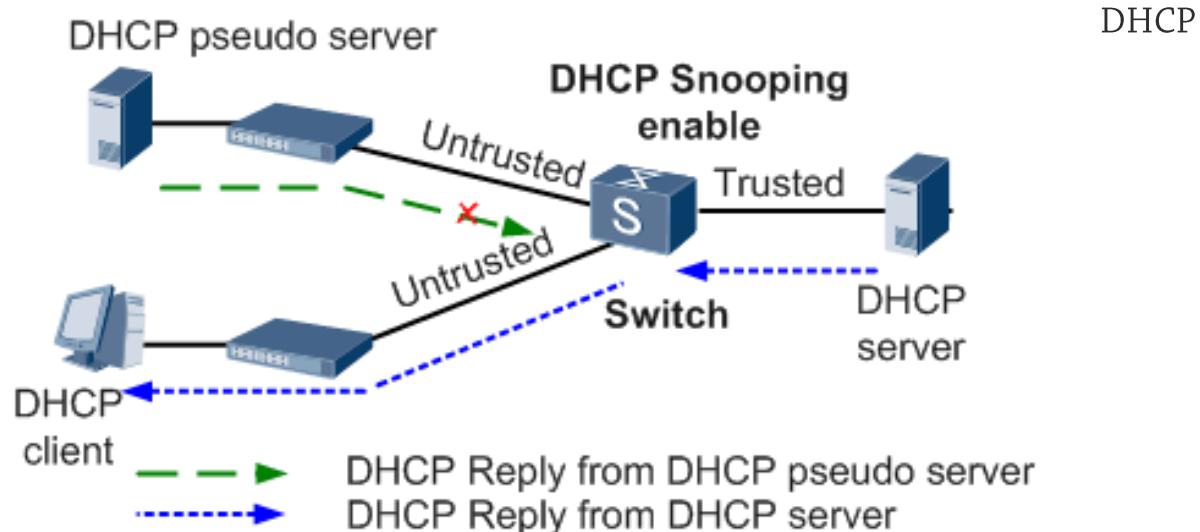
IP Helper

للحصول على معلومات من قبل DHCP server يجب أن يتوفر DHCP client مثبت ولكي يتصل مع الـ server ويقوم بإرسال الـ broadcast على الشبكة لكي يحدد مكان الـ server ولكن ضمن شبكة واحدة أي أن تكون جميع الأجهزة ضمن شبكة واحدة.

أما في شبكة البنك في يوجد أكثر من فرع وكل فرع في شبكة مختلفة أي لا يمكن تمرير رسائل الـ broadcast حيث قامت cisco router بعمل خاصية مميزة ip helper address تقوم بتحويل الـ broadcast القادمة من أحد الـ ports إلى عنوان أقوم بوضعه ويرسله على شكل unicast يصل للـ server DHCP ويقوم بعدها الـ server بالرد على طلب IP helper وإيصال المعلومات للجهاز الـ source في شبكتنا سنقوم بوضع الـ ip helper على كل interface Vlan في كل فرع على الـ distribution الموجدة في كل فرع

DHCP SNOOPING

أدت هذه الآلية من أجل حل الكثير من الهجمات منها هجوم spoofing أو العديد من المهدومات التي تقوم بإرسال الكثير من رسائل discover إلى server DHCP مما يسبب الحمل الكبير على الـ server فكان الـ snooping حل لمثل هذه الهجمات او لهجوم spoofing الذي هو احد الهجمات التي تستهدف server DHCP يقوم الجهاز المهاجم بعمل جهاز مخادع على انه مخدم DHCP ويقوم بتوزيع عناوين مختلفة غير العناوين المستخدمة في الشبكة يقوم بتغيير عنوان البوابة الافتراضية DG وذلك باستخدام برنامج يقوم بإجراء sniffing على الشبكة ويقوم بإعادة توجيه البيانات باستخدام برنامج تحليل البيانات wirshrek ويتمكن الهجوم من معرفة كل البيانات في الشبكة حيث أتى الـ snooping حل لجميع المشاكل حيث يقوم بتحديد الـ port الموثوقة على الـ switch التي تستطيع إرسال رسائل الـ DHCP وتمرير إعدادات offer في مخطط شبكتنا سنقوم بتفعيل الـ DHCP snooping على جميع المسارات المسموح لها تمرير رسائل DHCP في حال تفعيل خدمة snooping على احدى الـ port سيقوم بجعل الـ port وحده موثوق ويمكن أن يمرر رسائل DHCP





NTP: (Network time protocol)

هو protocol مؤقت الشبكة يقوم بتوحيد الوقت على جميع التجهيزات يستخدم port رقم 123 من بروتوكول UDP ويعد من أقدم البروتوكولات الموجودة يمكن تعريفها عبر الإنترنت ولكن يعتبر ثغرة أمنية لأنه يفتح منفذ يمكن للمهاجم أن يستغلها. لذا الحل الأمثل أن نقوم بتعريف محيي وهو عبارة عن واحد من التجهيزات مثل router يمكن أن يتواجد أكثر من server والرقم يدل على أولوية المخدم وكلما كان الرقم أقل كلما كانت وثيقته أعلى Syslog

هي عبارة عن تطبيق يمكن من خلاله مراقبة الأجهزة التي تضمنها الشبكة من أجهزة وطابعات تقوم بإرسال log إلى السيرفر المخصص لاستقبال البيانات وتقوم هذه الخدمة بتسجيل كل الأوامر التي تنفذ على التجهيزات الشبكية بشكل يتم معالجتها بسهولة، مما يساعد في عمليات الصيانة وكشف الأخطاء وإصلاحها في الشبكة وتعقب محاولات الاختراق.

SysLog

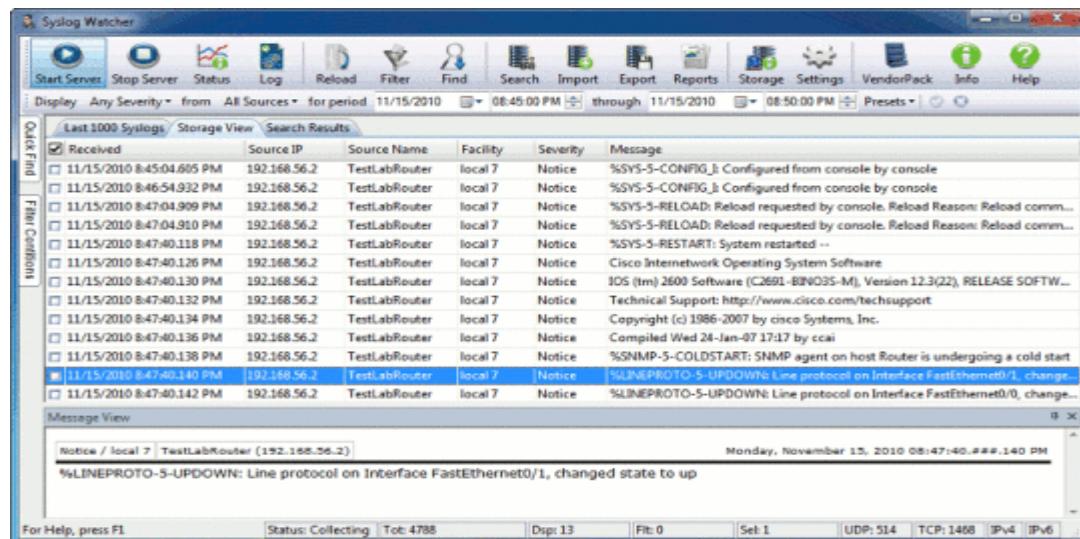
تقوم هذه الخدمة بتسجيل كل الأوامر التي تنفذ على التجهيزات ويساعد في عملية كشف الخطأ ومعرفة الوقت عند حدوث المشكلة والتخلص من المشكل قبل حدوثها وهي عبارة ثمانية رسائل لكل رسالة مستوى خطورة معين

Syslog Event Levels





يجب تنصيب برنامج يعمل ك syslog watcher يدعم خاصية تسجيل الأحداث سنقوم باستخدام برنامج sys log watcher أن يتم إعداده على syslog server



IP SLA (IP services level agreement)

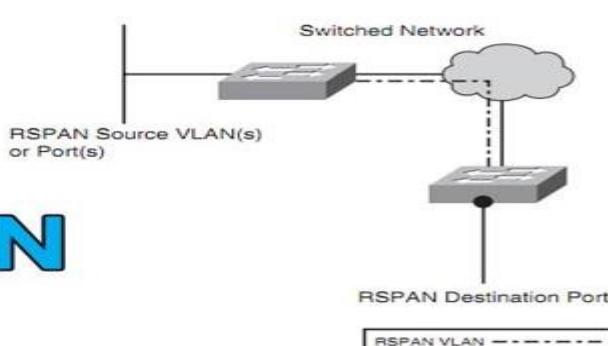
هي اتفاقية تفاوض بين طرفين أحدهم يكون العميل والأخر هو مزود الخدمة. ويمكن أن يكون هذا العقد بطريقة رسمية أو غير رسمية وهي خدمة تعمل مع Cisco operation center فقط تحوي على أكثر من 10 operation center منها في الشبكة

تستخدم لفحص الاتصال بشكل مستمر لمرة يتم تحديدها إلى port echo operation يقوم بعمل ping وفحص الاتصال بشكل مستمر لمرة يتم تحديدها إلى port echo operation يقوم بفحص الاتصال بشكل مستمر و دائم و فحص الشبكة

Rspan

يستخدم لمراقبة port معين في الـ switch وذلك بأخذ نسخة من الـ traffic وتمريرها إلى port معين في آخر وذلك بدون تغيير محتوى البيانات أو التعديل عليها وذلك باختصار عملية capture للـ configuration الموجدة

RSPAN



وتستخدم الـ Rspan عندما يكون جهاز على switch معين والجهاز الذي يريد مراقبة الـ traffic الخاصة به على آخر ويمكن عمل capture على مستوى Vlan وليس فقط على مستوى port



Network Security

الشبكة الافتراضية VPN

هي نوع من الشبكات المصممة لتقديم الشركات الكبيرة والمكاتب التي لديها فروع وأقسام في مناطق مختلفة، تؤمن للمشتركيين شبكة افتراضية منه للاتصال بغض النظر عن أماكنهم الجغرافية.

Port Security

وهو نوع من الأمان يعمل على الطبقة الثانية ويقييد الوصول إلى المنفذ عن طريق العنوان الفيزيائي MAC address حيث يتم تحديد العناوين المسموح لها باستخدام المنفذ باقي العناوين لا تستطيع استخدام المنفذ ويوجد أربع طرق لتفعيل امن المنفذ

- Dynamic: يمكنك تحديد عدد عناوين MAC المسموح بها لاستخدام منفذ في وقت واحد نستخدم هذا النهج لتحديد عدد العناوين بدلاً من تحديد عناوين المسموح بها هذه العناوين المتعلمة هذه العناوين (تنتهي صلاحيتها).
- Static: تقوم بإعداد العنوان المحدد المسموح له باستخدام المنفذ (لا تنتهي صلاحيتها)
- Combination: يمكنك الاختيار لتحديد بعضاً من العناوين المسموح بها وترك المبدل يتعلم البقية من العناوين (دمج لطريقتين static / dynamic العناوين المختارة static لا تنتهي صلاحيتها أما الأخرى تنتهي صلاحيتها)
- Sticky Learning: عند تفعيل هذه الخاصية على المنفذ سوف يقوم المنفذ بتحويل العناوين المتعلمة بشكل ديناميكي إلى النوع Sticky Secure وكأنها وضعت بشكل يدوي (لا تنتهي صلاحيتها).

Access Control List

يطبق الـ ACL على كل interface على حدا عند تطبيق الـ ACL على interface يمكن تحديد اتجاه البيانات التي ستقوم الـ ACL بفحصه حيث يمكن (تمثيل الـ ACL بانها فلتر يقوم بترشيح البيانات حسب الجهة التي تقوم بتحديدها) يمكن أن تكون جهة الفلترة هي للبيانات الداخلة إلى interface أو للبيانات الخارجة من interface ويمكن منع وصول إلى set محدد أو السماح لها.

IPsec

يعمل على أرسال البيانات من الجهاز الأول إلى الجهاز الثاني بطريقه موثوقة ومشفره باستخدام مفتاح مشترك

:Authentication Head (AH) يملك هذا البروتوكول ثلاثة بروتوكولات رئيسية

يستخدم في توقيع الرسائل والبيانات ولا يعمل على تشفيرها يحقق (وثوقيه، تكامليه وعدم أعاده الأرسال وحماية ضد الخداع).

Encapsulating Security Payload (ESP)

يوفر هذا البروتوكول تشفير وتوقيع للبيانات ويتحقق (مصادقه المرسل، تشفير البيانات، عدم أعاده الأرسال، حماية ضد الخداع) Internet Key Exchange(IKE) ضمان مشاركه وتوزيع المفاتيح بين المستخدمين، بروتوكول مصادقه في النظام، الموثوقية.

Leased line

أحد أنواع الربط بواسطة الـ WAN وهو عباره عن خط محجوز بشكل كامل غير مشارك مع أي جهة أخرى له سرعات عديدة يستخدم للربط بين أفرع شبكه خاصه بك حيث يؤمن وثوقيه عاليه للمعلومات وضمان عدم انقطاع بين أفرع الموصولة يتم الربط بين أفرع الشبكة بواسطة خط leased line عن طريق المخدم حيث يؤمن هذا المخدم خط موصول بشكل مباشر إلى الطرف الآخر ثم تحديد السرعة التي نريدها عن طريق المخدم يتم الربط الفيزيائي بواسطة وصلات الـ serial.

TMG

Microsoft Forefront Threat Management Gateway

وهو عبارة عن البرمجيات التي أصدرتها شركة مايكروسوفت والتي دورها الأساسي حماية نطاق الحواسيب من أي هجمات خارجية كانت من الأنترنت، يعد سيرفر ال TMG هو النسخة المطورة من سيرفر ال ISA (اختصاراً لـ Internet Security and Acceleration).

الهدف من استخدام سيرفر TMG :

1) يقدم الحماية عند الخروج إلى الأنترنت من أي اختراق أو فيروسات بحيث يجعل أي مستخدم يدخل إلى الأنترنت بشكل آمن

2) يقوم بالعمل على طبقات ISO جميعها مما يؤمن فلترة من مستوى أعلى تصل لمستوى التطبيقات

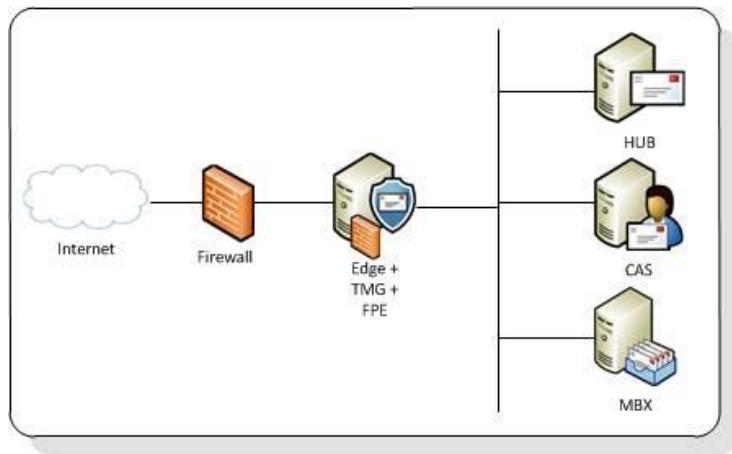
3) يقوم بتسريع عملية الدخول الشبكة عن طريق ضغط الملفات وعملية ال cashing (تخزين عناوين المواقع في الكاش الخاصة به في حال طلبها مرة أخرى)

4) يقوم بالتحكم بحجم ال traffic الداخلة أو الخارجة من الأنترنت

5) عمل للحزم ال HTTPS inspection لمنع وصول الفيروسات عن طريقها مع إمكانية استثناء بعض المواقع من عملية inspection (التفتيش)

6) عمل فلترة للروابط: بحيث انه يقوم بحظر المواقع بحسب تصنيفها (مثلا المواقع ذات محتوى العنف) دون الحاجة لحظرها كل موقع على حدى

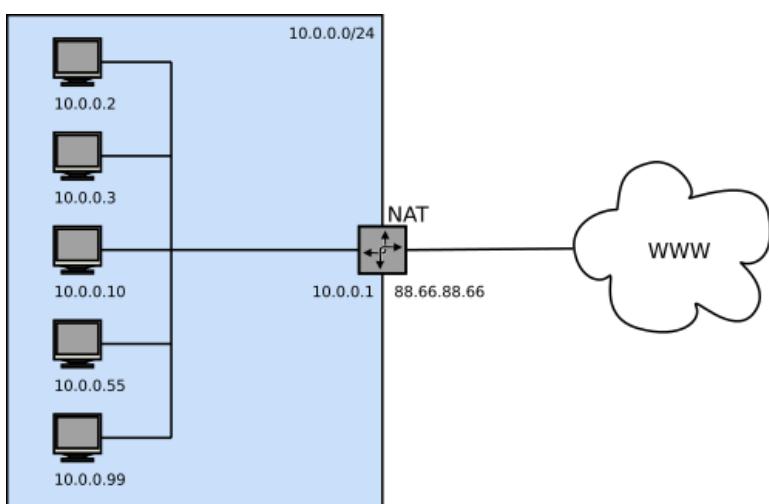
7) يدعم تعدد الوصلات مع الأنترنت للقيام بتوزيع الحمل أو عدم التوقف في حال وقوع احدى الوصلات



AAA

وهي خدمة تسجيل أسماء وكلمات سر وصلاحيات المستخدمين على سيرفر واحد بدل إنشائهم على كل تجهيزه أي أن الدور الأساسي لهذه الخدمة هي تشكيل data base توضع فيها أسماء وكلمات وصلاحيات المستخدمين ترجع إليها التجهيزة عند كل عملية تسجيل دخول لتحقق من وجود المستخدم وصلاحياته

أن AAA هي اختصاراً لـ Authentication Authorization Accounting ومن هنا نستنتج وظائفه:



(1) التحقق من اسم المستخدم Authentication وكلمة مروره

(2) الموثوقية أو إعطاء الصلاحيات للمستخدم Authorization

(3) جمعية الصلاحيات المستخدمة من قبل نفس المستخدم Accounting يمكننا تطبيق خدمة AAA عن طريق أحد بروتوكولين + Tacacs أو RADUIS

يكون الفرق الأساسي بين البروتوكولين في أن بروتوكول radius يقوم بعملية Authentication وAuthorization وبخطوة واحدة

بين ما يقوم بهما بروتوكول Tacacs + بخطوة منفردة لكل منها



وهذا ما يعطي بروتوكول Tacacs+ إمكانية تعقب كامل للمستخدم بحيث انه في كل مرة يقوم المستخدم باستخدام صلاحية معينة سيتم العودة لسيرفر AAA لسؤاله إذا كانت صالحه له أم لا.

Management security

للوصول لأي تجهيز سيسكو للقيام بعمليات الأعداد عليها تحتاج للوصول إلى ما يسمى بالmanagement plane

ويمكن الوصول لهذه الـ management plane بأكثر من طريقة:

إما console أو Aux أو line vty إن عمل هذه الخدمة الأساسي هو قفل طرق الوصول هذه بكلمات سر حتى لا يتم الدخول إليها إلا عن طريق أشخاص مخولين بذلك.

NAT

مع التزايد الكبير لعدد مستخدمي شبكة الإنترنت أصبحت مشكلة توزيع عناوين IP تمثل قضية مهمة حيث أن مجال عناوين IPv4 لم يعد كافياً لاستيعاب العدد الهائل من المستخدمين مما دعا الحاجة لاقتراح طريقة NAT حيث يتم حجز عنوان IP وحيد لكل شبكة داخلية من مزود الخدمة بدلاً من حجز عنوان لكل مستخدم وإذا أراد مستخدم ما الاتصال إلى الإنترنت من هذه الشبكة يتم التحويل من عنوان Private IP إلى Public IP.

أنواع NAT:

(1) Static NAT: يستخدم هذا النوع في المخدمات حيث يتم فيه ترجمة Public IP إلى Private IP.

(2) Dynamic NAT: في هذا النوع يتم تحديد مجموعة من عناوين Public IP. ويتم ترجمة مجموعة عناوين Private IP إلى عناوين من هذه المجموعة وعند استخدام جميع عناوين Public IP الموجودة ضمن المجموعة وأراد مستخدم ما الاتصال بالإنترنت فإنه ينتظر حتى يصبح أحد هذه العناوين متاحاً.

(3) NAT Overload: يتم استخدام هذه الطريقة من قبل DSL Router حيث يتم إضافة مفهوم رقم المنفذ Port Number إلى عناوين Public IP لتخديم أكبر عدد ممكن من المستخدمين.



Network Administration

Dynamic Host Configuration Protocol (DHCP)

هو بروتوكول يعتمد على مبدأ client / Server يقوم بتزويد الأجهزة التي تتصل على الشبكة بعنوان IP يأخذ من يكون الـ Admin Scope قد قام بإعداداته بالإضافة إلى أي إعدادات أخرى قد يحتاجها الجهاز عند الاتصال بالشبكة مثل عنوان DNS Server وعنوان Default Gateway.

DHCP Failover

هي خاصية موجودة ضمن Windows Server 2012 DHCP Server Role تقوم بعمل DHCP Server احتياطي بحال وقوع السيرفر الأساسي يقوم السيرفر الاحتياطي باستلام عملية توزيع عناوين IP وذلك مع المحافظة على العناوين المؤجرة مسبقاً من قبل الـ DHCP Server الأساسي حيث ستتضمن لنا وجود DHCP Server احتياطي بحال سقوط الأساسي دون حدوث انقطاع بالشبكة.

DHCP Policies

وهي ميزة تمت إضافتها إلى Windows Server 2012 DHCP Role تسمح لنا بتحديد سياسات معينة للأجهزة معينة تبعاً لحقول تكون موجودة ضمن الـ DHCP Client Packets التي يرسلها إلى الـ DHCP Server هذا الأمر الذي سيمكنا من حماية الشبكة من أي جهاز خارجي من الممكن أن يتصل عليها.

Enabling Audit Logging

عند تفعيل Audit Logging لكل DHCP Server على الشبكة سيتمكن الـ Admin المسؤول بالحصول والاطلاع على تاريخ حركة الـ DHCP Packets على الشبكة مما يفيد في الحماية ومتابعة المشاكل والأخطاء التي قد تحصل وهي خاصية مفعولة افتراضياً بكل DHCP Server ويتوضع الملف الذي يحفظه الـ DHCP Server في المسار C:\window\system\dhcp حيث يكون اسم الملف DhcpSrvLog-XYZ.log حيث XYZ هو كود ثلثي يمثل اليوم الذي حفظ فيه.

Domain Name System (DNS)

هي خدمة تعتمد على مبدأ Client / Server تستخد لربط عناوين IP الخاصة بالأجهزة أو الخدمات الموجودة ضمن الشبكة مع أسماء ذو بنية هرمية بهدف الوصول إلى الجهاز عن طريق الاسم المرتبط بعنوان IP الخاص بالجهاز وهو



مكون رئيسي لشبكة الأنترنت ويعتمد بشكل كبير على DHCP حيث ستحقق لنا هذه الخدمة سهولة الوصول إلى موارد الشبكة من سيرفرات وخدمات وتجهيزات.

Conditional Forwarder

وهي إحدى خصائص DNS Server حيث يتم توجيه الـ Domain بحسب اسم الـ Domain الموجود ضمن الـ Query ما يؤدي إلى سرعة أكبر في حل الأسماء وأيضاً ستفي في عملية الربط مع شركة Western Union للصرافة حيث سيتم توجيه الطلبات الخاصة بها إلى الـ DNS Server الخاص بهم مباشرة.

Secure Dynamic Updates

إحدى أهم الخصائص في DNS حيث تقوم بالتعديل على الـ DNS Record معين عندما يتم تغيير عنوان الـ IP الخاص به مما يسهل عملية إدارة الأسماء المعطاة للتجهيزات وعند استخدام الـ DNS Sever مع بيئة ADDS تصبح عملية الـ Dynamic Updates محصورة فقط على الأجهزة المتصلة.

Resource Records Aging & Scavenging

مع الوقت قد تصبح بيانات الـ DNS قديمة وغير صالحة للاستخدام وهو الأمر الذي يولد مشكلة مساحة زائدة على Hard Disk وبحال بقيت دون تعامل معها قد تؤدي إلى عدة مشاكل ولتفاديها سنقوم بتنشيط خاصية Aging & Scavenging في الـ DNS Server حيث سيتم وضع طابع زمني لكل DNS Record يتم إنشاؤه ديناميكياً ويدخل السجل بحالة No-Refresh Interval لمدة يتم تحديدها حيث لا يمكن عمل تحديث للطابع الزمني وإنما فقط المعلومات الأخرى المتعلقة بالسجل ثم يدخل السجل بحالة Refresh Interval حيث يمكن تحديث أي معلومة من السجل من ضمنها الطابع الزمني وعند انتهاء مدة الـ Refresh Interval للطابع الزمني سيتم حذف السجل.

Active Directory Integrated Zone

حيث سيتم حفظ سجلات الـ Active Directory ضمن قاعدة بيانات DNS مما يعطينا عدة ميزات منها الأمان العالي وسهولة التعديل على الـ Records من أي Domain Controller يحتوي على الـ DNS Role.

DNS Socket Pool

هي خاصية تسمح لـ DNS Server باستخدام Port عشوائي للمصدر وPort عشوائي للوجهة بدلاً من استخدام Port DNS Spoofing Queries مما يجعلها منيعة ضد هجمات.



DNS Cache Locking

خاصية يتم تفعيلها لمنع استبدال الـ Record لفترة معينة من TTL وهو موجود ضمن الـ Cache.

DNSSEC

وهو نظام حماية قامت شركة Microsoft بتطويره ضمن نظام Windows Server 2012 مهمته حماية الـ DNS Queries عن طريق إضافة توقيع مشفر لعمل Authentication كي يتم التحقق من هوية الجواب على الـ DNS Server من قبل الـ DNS Server.

Active Directory Domain Services

هي خدمة أساسية لكل Windows Domain يقوم بتخزين كل أعضاء الـ Domain من تجهيزات ومستخدمين Users ويقوم بتحديد سمات الوصول واستخدام موارد الشبكة كما يسمح لنا بتأمين إدارة مركبة لها.

تستخدم خدمة ADDS بروتوكول Lightweight Directory Access Protocol (LDAP) بالإضافة إلى بروتوكول Kerberos كما تعتمد بشكل أساسي على DNS.

Logical Active Directory

يعتمد على:

- OU: وهي عبارة عن وحدة تنظيمية تستخدم لتنظيم الـ Objects ضمن الـ Domain لتسهيل إدارتهم وتطبيق سياسات أمنية على أعضائهم.
- Domain: وهي مجموعة من المستخدمين، الحواسيب، والمجموعات التي تشارك بعض الخصائص وبقاعدتها بيانات واحدة توجد نسخة منها على كل Domain Controller في الـ Domain.
- Tree: مجموعة من Domain واحد أو أكثر وتشارك ب مجال اسمي واحد وتمتلك علاقة Parent / Child وليس لها أي أهداف إدارية.
- Forest: مجموعة من Tree واحدة أو أكثر لها خصائص واحدة متصلة مع بعضها بعلاقة ثقة متبادلة وهي أعلى حد للحماية والإدارة.



Physical Active Directory

من أهم مفاهيمه:

- Domain Controller (DC) هو الـ Server الذي تم تنزيل ADDS Role عليه وترقيته إلى Domain Controller ما يمكنه من التحكم بالـ Domain واستضافة قاعدة بيانات ADDS ويمكن وجود أكثر من DC واحد في الـ Domain.
- Site: وهو المكان الفيزيائي الذي يتواجد به الـ DC حيث يمثل الشبكة الفيزيائية من مكان توضع الـ Server إلى الكبار.

Recycle Bin

هي خدمة اختيارية يتم تشغيلها على الـ ADDS حيث ستتمكن الـ Admins من استعادة الـ Objects بعد حذفها مع استعادة وظائفها كاملة دون الحاجة لعمل Restore من الـ Backups الخاصة بـ ADDS ثم إعادة تشغيل الـ ADDS مما سيمكنا من استعادة أي حساب قد يتم حذفه عن طريق الخطأ بأبسط الطرق.

Password Policies

وهي شروط معينة يجب مراعاتها عند تعيين الـ Password الخاص بالـ User مثل عمر الـ Password ، طوله، وتعقيده حيث ستمكننا من تحديد شروط صارمة للـ Password الذي سيستخدمه الـ User للدخول إلى حسابه مما يوفر الأمان العالي.

Account Lock out Policy

هي سياسة تسمح لنا بتحديد متى يتم قفل حساب المستخدم حال تم إدخال الـ Password بشكل خاطئ عدة مرات.

Fine-Grained Password Policy

تسمح لنا بوضع Account Lock Out Policies و Password Policies مختلفة وتعيينها لمجموعة معينة من المستخدمين.



Group Policy Object (GPO)

وهي عبارة عن Object تحتوي على عدة سياسات من أجل إعداد حسابات المستخدمين أو الـ Computers على الشبكة. يستطيع الـ Administrator عن طريق الـ GPO فرض الإعدادات عن طريق تعديل الإعدادات المخصصة للـ Computer أو المخصصة للمستخدم مما يمكننا مثلاً من منع المستخدم من تشغيل برامج معينة قد يكون ليس له عمل بها.

Redircmp & Rediusr

Redircmp: تقوم نقل موضع الحاوية الافتراضية للـ Computer Obj إلى OU من اختيارنا حيث تمكنا من تطبيق Group Policy معينة عليها ريثما يتم التأكد من مصدر الجهاز الجديد ونقله إلى الـ Ou المناسبة Redirusr: نفس عمل redircmp لكنها تغير موضع الـ User Object

RAID Technology

بهدف تأمين وسط تخزين بسرعة عالية وكلفة منخفضة بالإضافة إلى الحفاظ على المعلومات والتأكد على عدم انقطاع (RAID) Redundant Array of Independent Disk الخدمة بسبب عطب في وسط تخزين يتم بناء المخدم بتقنية RAID

وبما يخدم أهداف المشروع سيتم البناء على RAID 0+1 والتي تمتاز بـ:

- سرعة أداء عالية أثناء القراءة من الأقراص الصلبة أو الكتابة عليها

- تقسيم البيانات عبر عدة أقراص

- وجود أقراص Mirror وهي عبارة عن أقراص احتياطية يساوي عددها عدد الأقراص الأصلية التي تقسم عليها البيانات ففي حال تعطل أي قرص أو حدوث خلل في بياناته يتم استرداد البيانات من القرص الاحتياطي.

Exchange

عبارة عن مخدم لتبادل الرسائل والتعاون من Microsoft ، وهو برنامج يتم تشغيله على المخدمات ويمكنك من إرسال وتلقي البريد الإلكتروني ونماذج أخرى من التواصل التفاعلي من خلال شبكات أجهزة الكمبيوتر. ولقد تم تصميم Exchange Server للتعامل مع تطبيق برمجي عميل مثل Microsoft Outlook ، وهو يتعامل أيضاً مع Express ومع تطبيقات عميل البريد الإلكتروني الأخرى.

NAP (Network Access Management)

وهي عبارة عن خدمة تقوم بفحص الـ Computer Health وفق المعايير الموضوعة لها ومنه لتسمح او تمنع هذا الجهاز من الوصول إلى موارد الشبكة أو إلى جزء منها.

WSUS

وهو عبارة عن مخدم يقوم بتأمين آخر التحديثات للأجهزة الموجودة في الشبكة وذلك لضمان عدم وجود أي ثغرات أمنية في نظام التشغيل أو برامجية من برمجياته.

Manage Disk Quote

وهي عبارة عن أداة تسمح بتحديد أنواع الملفات التي يمكن وجودها على الأقراص لكل من للزبائن والخدمات وحجوم الملفات الأعظمية كما تحديد المساحة التخزينية التي يمكن استخدامها.

RSAT (Microsoft Remote Server Administration Tools)

وهي عبارة عن حزمة برمجية تعمل على تسهيل إدارة الخدمات عن بعد دون الاتصال بسطح المكتب البعيد حيث يتم التعامل مع الـ Server Manager, AD و غيرها لمخدم واحد أو لعدة مخدمات بسهولة ومن مكان واحد.

RDS (Remote Desktop Connection)

وهي خدمة يتم تفعيلها عند الـ Clients و الـ Servers وذلك بهدف الوصول إليها من منصة حاسوب آخر مما يفيد بالدعم عن بعد ويؤمن سهولة وسرعة حل المشاكل في مختلف أقسام الشركة.

SharePoint

مخدم تطبيقات الويب المطور من مايكروسوفت، يعمل على تسهيل عملية تبادل الوثائق والملفات والسجلات بين موظفين المؤسسة الواحدة وبين أفرع المؤسسة عبر صفحات الويب، يعتمد على بروتوكول Http و Https، وبحيوي قوالب تطبيقات وصفحات ويب جاهزة مما يمكن كل موظف في الشركة من عمل صفحة شخصية وتتبادل البيانات مع باقي الموظفين. كما كل تطبيقات الويب تعتمد على قاعدة بيانات لتخزين بياناتها عليها، يعتمد الـ SharePoint على نظام قواعد البيانات SQL المطور من مايكروسوفت أيضاً، حيث ينشئ قاعدة بيانات خاصة له.

SQL Server

مخدم قواعد البيانات المطور من مايكروسوفت، يستخدم مع الـ SharePoint بشكل أساسي وأيضاً لتقديم البرامج الأخرى التي تعتمدها الشركة مثل برامج المحاسبة للبنوك وغيرها وتحتوي بيانات الموظفين والعملاء.



Web server

مخدم يستخدم لتقديم صفحات الويب يعتمد ببروتوكولي Http وHttps، ويستخدم كمخدم محلي يمكن تصفحها عبر متصفحات الويب، ويحوي صفحة الويب المحلية للشركة والموقع الرسمي للشركة كما يمكنه تقديم تطبيقات الويب التي تعتمد على الشركة وربطها مع قاعدة البيانات.

File server

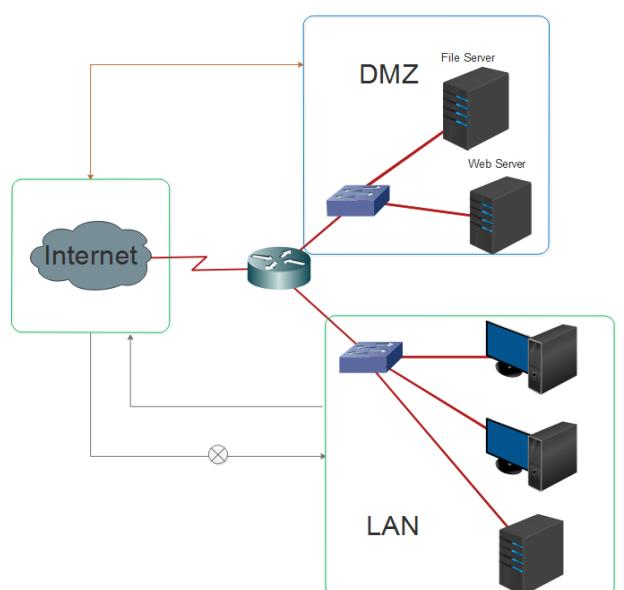
مخدم يقوم بتأمين نقل وحفظ البيانات ويعتمد على بروتوكول FTP، يمكن الشركة من تناقل البيانات بين موظفيها بشكل سهل، ويمكن الوصول إليها بوضع Ftp:// قبل اسم الـ Domain الذي اعتمده الشركة، أو عبر برامج خاصة تسمى FTPClient يمكن المستخدم أو الموظف من رفع وتنزيل وتعديل البيانات على المخدم.

DMZ

تسمى أي المنطقة منزوعة السلاح وتعني تقنية المنطقة المحايدة أي لا هي محمية بشكل كامل مثل شبكة الـ LAN ولا ضعيفة الحماية مثل شبكة الـ Internet، وتوضع دعماً للجدار الناري، تمثل طريقة لعزل الشبكة المحلية للشبكة عن الأخطار الخارجية في حال ما أردنا تمكين الوصول للمخدمات من خارج الشبكة المحلية وتوضع

سياسات على كل منفذ مثلاً تمكّن مستخدمي الـ LAN من تصفح الإنترنت فقط، والتعديل والقراءة عالـ DMZ.

يتم تمكين الخدمات الآتية في الـ DMZ :



لحاجة هذه المخدمات للوصول إليها من خارج الشبكة المحلية.

Backup Server

هي ميزة تقدمها شركة مايكروسوف特 لإجراء النسخ الاحتياطي للمخدم بشكل كامل أو لأقسام معينة منه، وتمكننا من استعادة هذه البيانات عند الحاجة إليها.

إن وجود النسخ الاحتياطي ضرورة لا يمكن الاستغناء عنها، فهي توفر الكثير من الوقت والجهد في حال فقدان البيانات أو فشل النظام.



تمكننا ميزة النسخ الاحتياطي من إجراء نسخ لكامل المخدم أو لاقسام معينة منه أو حتى لتطبيقات محددة، كما يمكن استخدام ميزة النسخ الاحتياطي لإجراء backup لجهاز حاسوب محلي أو لجهاز بعيد، كما يمكن جدولة عملية النسخ الاحتياطي كي تعمل بشكل أوتوماتيكي.

VSS (Volume Shadow copy Service)



- هي خدمة من شركة Microsoft تسمح بإجراء نسخ احتياطي للملفات المفتوحة واستعادة البيانات إلى درجة معينة.
- طرحت هذه الخدمة للمرة الأولى مع إصدار windows XP
- تقوم بإنشاء snapshot للقرص
- لا تعتبر بديلا عن النسخ الاحتياطي الطبيعي regular backup لأن
- 1. snapshot تقوم بتسجيل الملفات التي تم تعديلها فقط، أما في حال فقدان ملف لم يتم التعديل عليه فلا بد من الرجوع للنسخ الاحتياطي العادي لاستعادته
- 2. Snapshot تكون محدودة بعدد ومساحة معينين، يحدث انه عندما تكون مساحة التخزين ممتلئة، تمحى الsnapshot القديمة
- 3. يحدد المشرف مساحة التخزين الخاصة بال snapshot على ألا تقل عن 300 ميغا بايت.
- 4. تخزن 64 نسخة من كل ملف مع كل تعديل، وعند بلوغ هذا العدد تمحى النسخ القديمة.



Windows Deployment Services

هي عبارة عن منتج مايكروسوفت، يمكننا من توزيع أنظمة التشغيل على أجهزة الكمبيوتر عن بعد عبر الشبكة دون الحاجة إلى تثبيت نظام التشغيل على كل حاسوب على حدة باستخدام قرص DVD، CD

:WDS فوائد خدمة

- 1 تسمح بتنصيب أنظمة التشغيل عبر الشبكة، وهو أقل تكلفة وتعقيداً من تنصيب الأجهزة اليدوي.
- 2 يدعم توزيع أنظمة التشغيل مختلفة عند العمل في بيئة عمل فيها أنظمة تشغيل مختلفة "غير موحدة" من نظام windows server حتى ويندوز 8.1 وأنظمة تشغيل windows server 2003 مروراً بناظمة تشغيل windows 7 2008 R2
- 3 يستخدم تقنيات التنصيب القياسية(standard)
- 4 استخدام تقنية multicast لنقل البيانات وصور أنظمة التشغيل.
- 5 تسمح بإنشاء صورة نظام لجهاز حاسوب مرجعى، والذي سيكون بدليلاً tool ImageX
- 6 تسمح بتوزيع كافة المكونات البرمجية اللازمة على أجهزة الـ client واللازمة لعمل الأجهزة على أنظمة تشغيل windows

سبب استخدام WDS ضمن شبكة HSBC هو تنصيب أنظمة التشغيل على أجهزة الكمبيوتر عن بعد وذلك لتوفير وقت وجهد فريق الدعم الفني المسؤول عن الشبكة، كما تسهل عملية الإدارة وتصحيح الأخطاء كتهيئة جهاز حاسوب عند انضمام موظف بديل على الشبكة، وهي لا تلغي تدخل المشرف بشكل كامل.

المطلبات الأساسية التي تعمل خدمة WDS:

- 1 DC in ADDS domain أو أن يكون عضواً في ADDS domain يجب على WDS server ولا علاقة لمستوى forest أو domain بوجود WDS server حيث أن جميع الإصدارات تدعمه.
- 2 لابد من وجود DHCP server وله مجال فعال من عناوين IP في الشبكة كي تعمل خدمة WDS لأنها تستعمل (PXE) Pre-execution Environment من أجل العونة المنطقية.
- 3 لابد من وجود مخدم DNS في الشبكة قبل تشغيل خدمة WDS.
- 4 يتطلب مخدم WDS وجود نظام ملفات NTFS لتخزين صور النظام image NTFS volume
- 5 لتنصيب وظيفة WDS على المخدم لابد أن تكون عضواً في مجموعة administration group ولهيئة المخدم لابد أن تكون عضواً في مجموعة domain admins group



ملاحظة: لتهيئة المخدم للعمل ك standalone mode لست مضطراً أن تكون عضواً في مجموعة domain users group

ADCS (Active Directory certificate services)

في أي بيئة عمل كبيرة نحن بحاجة إلى جهة تقوم بتوثيق المستخدمين وأجهزة الحاسوب والمُخدمات، خدمة ADCS من مايكروسوفت تقدم خدمة التوثيق لموارد الشبكة السابقة إضافة إلى توثيق صفحة الويب الخاصة بالبيئة وال Emails التي يتبادلها المستخدمون ضمنها.

تقديم ADCS خدمات مخصصة لإنشاء وإدارة شهادات التوثيق والتي تستخدمن من قبل برامج الأنظمة الأمنية التي تستخدم تقنيات المفتاح العام.

قمنا باستخدام ADCS ضمن بيئة HSBC كي يكون المرجع في إعطاء الشهادات الرقمية للموارد المذكورة وإدارتها.

أهم الخدمات التي تقدمها ADCS:

• هي هيئة إصدار الشهادات الرقمية: Certification authority(CAs)

أول CA يتم إنشاؤه في البيئة يسمى root CA ويقوم بتشكيل أساس الـ PKI، ويقوم بإعطاء الصلاحية للـ CAs الأخرى في البيئة، ويعتبر الأعلى موثوقية في البنية الهرمية لبيئة ADCS، كما لا يقوم بإعطاء الشهادات للمستخدمين، إنما تقوم الـ subordinate التي يقوم الـ root بإنشائهما بإعطاء الشهادات للمستخدمين.

ولها نوعان، CA داخلية لتامين شهادات ضمن المؤسسة، وهي ما تقدمه خدمة ADCS والتي سنقوم بتنصيبها، وCA خارجية عند الحاجة لتامين الشهادات بين المؤسسات وليس ضمن المؤسسة ذاتها.

محطويات الشهادة الرقمية: تحوي على اسم المستخدم ورقم الهوية الخاص به، وتاريخ المنح وتاريخ انتهاء الصلاحية إضافة إلى التوقيع الخاص بمانح الشهادة CA، وتستخدم هذه الشهادة في التوثيق والتشفير.

تقسم الـ CA إلى نوعين هما enterprise و standalone



يتميز بـ enterprise

.1 متكامل مع بيئة AC

.2 يوافق على الطلب إذا كان متطابقاً مع certificate template موجودة لديه

.3 يوافق على الطلبات أتوماتيكياً

أما standalone :

.1 يعمل ضمن workgroup

.2 لا يحتوي على certificate template

.3 ينتظر الأدمين ليوافق على الطلب

Dynamic Access Control

هي خدمة حديثة من مايكروسوفت لتحسين عمل الدليل النشط AD، تمت إضافتها مع إصدار windows server 2012، وهي خدمة تعتمد على الـ domain، وتسمح للمشرفين أن يطبقوا قيوداً وأذونات للتحكم بالوصول إلى الموارد بناءً على قواعد واضحة والتي يمكن أن تتضمن دور أو وظيفة المستخدم، وإعدادات الجهاز المستخدم من أجل الوصول إلى تلك الموارد الخ...

كمثال على ذلك، إذا حاول موظف أن يصل إلى أحد الموارد باستخدام الحاسب الموجود في مكتبه أو باستخدام حاسوب محمول فقد يواجهه أذونات مختلفة.



القسم العملي
Practical Division



Network Design

Trunk protocol

Configuration:

```
Daccsw-vlans >enable
Daccsw-vlans #> configuration terminal
Daccsw-vlans (config)# interface fastethernet 0/1
Daccsw-vlans (config-if)# switchport trunk encapsulation dot1Q
Daccsw-vlans (config-if)#switchport mode trunk
Daccsw-vlans (config-if)# switchport trunk allowed vlan all
```

VLAN

switch على الـ **vlan** الـ **switch**

Configuration:

```
Daccsw-vlans>enable
Daccsw-vlans#> configuration terminal
Daccsw-vlans (config)# interface range fastethernet 0/1-3
Daccsw-vlans (config-if)# switchport access
Daccsw-vlans (config-if)# switchport access Vlan 10
```

VLAN Name	Status	Ports
1 default	active	Gi1/1
10 Network_Admin	active	
20 IT	active	
30 Tech_Admin	active	
40 Tech_support	active	
50 management	active	
60 HR	active	
70 inter_trades	active	
80 interna_trades	active	
90 Cust_Services	active	
100 Accounting	active	
110 Security	active	
1002 fddi-default	act/unsup	
1003 trcrf-default	act/unsup	
1004 fdnet-default	act/unsup	
1005 trbrf-default	act/unsup	

عرض الـ **Vlans** الموجودة على الـ **switch** الموجودة في الشبكة:

Daccsw-vlans>enable



Daccsw-vlans#> show Vlan brief

Inter Vlan routing

سنقوم بتوجيه الـ Vlan عن طريق switch layer 3

Configuration in switch L3 :

```
damas-des2>enable
damas-des2#> configuration terminal
damas-des2 (config)# interface Vlan 10
damas-des2 (config-if)#ip address 192.168.0.16 255.255.255.128
damas-des2 (config-if)#no shutdown
damas-des2 (config)# interface Vlan 20
damas-des2 (config-if)#ip address 192.168.0.145 255.255.255.128
damas-des2 (config-if)#no shutdown
damas-des2 (config)#ip routing
```

Configuration in switch L3 :

```
damas-des1>enable
damas-des1#> configuration terminal
damas-des1 (config)# interface Vlan 10
damas-des1 (config-if)#ip address 192.168.0.17 255.255.255.128
damas-des1 (config-if)#no shutdown
damas-des1 (config)# interface Vlan 20
damas-des1 (config-if)#ip address 192.168.0.146 255.255.255.128
damas-des1 (config-if)#no shutdown
damas-des1 (config)#ip routing
```

Vlan trunking protocol (vtp)

سنقوم بتفعيل الـ vtp server وتفعيله كـ 2 domain version وضع اسم domain وكلمة سر

Configuration:

```
damas-des2# configuration terminal
damas-des2 (config)# Vtp domain HSBC
damas-des2 (config)# Vtp version 2
damas-des2 (config)# Vtp mode server
damas-des2 (config)# Vtp password HSBC
damas-des2 (config)# Vtp pruning
```

سنقوم بإنشاء الـ Vlan على الـ Vtp client ومن ثم تلقائيا يأخذ الـ الموجدة على الـ Vlan

```
damas-des2 (config)# Vlan 5
damas-des2 (config)# servers
damas-des2 (config)# Vlan 10
damas-des2 (config)# Network Administration
```



```

damas-des2 (config)# Vlan 20
damas-des2 (config)# IT
damas-des2 (config)# Vlan 30
damas-des2 (config)# Technical_Administration
damas-des2 (config)# Vlan 40
damas-des2 (config)# Technical_support
damas-des2 (config)# Vlan 50
damas-des2 (config)# management
damas-des2 (config)# Vlan 60
damas-des2 (config)#HR
damas-des2 (config)# Vlan 70
damas-des2 (config)# internal_trades
damas-des2 (config)# Vlan 80
damas-des2 (config)#international_trades
damas-des2 (config)# Vlan 90
damas-des2 (config)# Customer_Services
damas-des2 (config)# Vlan 100
damas-des2 (config)# Accounting
damas-des2 (config)# Vlan 110
damas-des2 (config)# Security

```

ونطبق نفس التعليمات على الـ switch الاحتياطي BKHQ

ونعيد التعليمات على HQ , HOMS ونطبقها في كل طابق في الفرعين switches VTP client

Configuration on VTP client:

```

Daccsw-vlans # configuration terminal
Daccsw-vlans (config)# Vtp domain VLANs
Daccsw-vlans (config)# Vtp version 2
Daccsw-vlans (config)# Vtp mode client
Daccsw-vlans (config)# Vtp password HSBC

```

لمعرفة حالة الـ Vtp نستخدم

Daccsw-vlans >enable

Daccsw-vlans # show Vtp status

```

damas-des2#show vtp status
VTP Version capable      : 1 to 3
VTP version running      : 2
VTP Domain Name          : HSBC
VTP Pruning Mode         : Enabled
VTP Traps Generation    : Disabled
Device ID                : 0000.ab98.2000
Configuration last modified by 172.16.1.5 at 5-23-17 13:58:31
Local updater ID is 172.16.1.5 on interface V11 (lowest numbered VLAN interface found)

Feature VLAN:
-----
VTP Operating Mode       : Server
Maximum VLANs supported locally : 1005
Number of existing VLANs   : 16
Configuration Revision    : 16
MD5 digest               : 0xF2 0xFD 0xA3 0xDD 0x68 0xB3 0x48 0x23
                           0xF2 0x9E 0xB8 0xE7 0x49 0x4E 0x85 0xC4

damas-des2#

```



Daccsw-vlans # show Vtp password

ولمعرفة كلمة السر

Etherchannel

سنقوم بتفعيل الـ link distribution switch على etherchannel فيما بينهم من توزيع الحمل على الـ source ipحسب

Configuration:

```
damas-des1 #> configuration terminal
damas-des1 (config)# interface range fastethernet 0/1-3
damas-des1 (config-if)#channel-group 1 mode auto
damas-des1 (config-if)#exit
damas-des1 (config)# port-channel load-balance src-ip
```

```
damas-des2 #> configuration terminal
damas-des2 (config)# interface range fastethernet 0/1-3
damas-des2 (config-if)#channel-group 2 mode desirable
damas-des2 (config-if)#exit
damas-des2 (config)# port-channel load-balance src-ip
```

IP-helper

في شبكة سنقوم بوضع الـ helper على كل فرع على الـ distribution interface Vlan الموجودة في كل فرع في الفرع الأساسي HQ

Configuration:

```
damas-des1 #configuration terminal
damas-des1 (config)#interface rang vlan 10
الموارد في الفرع الأساسي سنتقوم بضع عنوان DHCP server
damas-des1 (config-if)#ip helper-address 192.168.0.1
```

نضع عنوان DHCP في حال وقوع الـ server الأساسي سيتتم توجيه الـ DHCP من الـ server الاحتياطي

```
damas-des1 (config-if)#ip helper-address 192.168.0.2
```

في الفرع الثاني HOMS

```
homs-des1 #configuration terminal
```

```
homs-des1 (config)#interface vlan 120
```

الموارد في الثاني سنتقوم بضع عنوان DHCP server

```
homs-des1 (config-if)#ip helper-address 192.168.6.129
```

نضع عنوان DHCP في حال وقوع الـ server الأساسي سيتتم توجيه الـ DHCP من الـ server الاحتياطي

```
homs-des1 (config-if)#ip helper-address 192.168.0.2
```

```
damas-des2#show vtp password
```

```
VTP Password: HSBC
```

```
damas-des2#
```



DHCP snooping

في مخطط شبكة سنقوم بتفعيل DHCP snooping على جميع المسارات المسموح لها تمرير رسائل DHCP في حال تفعيل خدمة snooping على أحدى ports سنقوم بجعل port وحده موثوق ويمكن أن يمرر رسائل DHCP

Configuration:

نقوم بتفعيل snooping على switch ونقوم بتحديد VLAN التي نريد من الهجوم عليها

```
damas-des2 (config)# ip dhcp snooping
damas-des2 (config)# ip dhcp snooping vlan 10, 20 30
damas-des2 (config)# interface range fastethernet 0/0-2
```

نقوم بتحديد عدد معين من الطلبات التي يسمح للجهاز بطلباتها ونقوم بجعل port المحددة موثوقة وهي التي يمكن ان ترسل رسائل DHCP offer لطلباتها

```
damas-des2 (config-if)# ip dhcp snooping limit rate 3
damas-des2 (config-if)# ip dhcp snooping trust
```

Network time protocol (ntp)

Configuration:

نقوم بوضع ntp server

```
ISP1 (config)# ntp master 1
```

ومن ثم نعطي جميع التجهيزات عنوان NTP server

```
damas-des2 (config)# ntp server 55.100.3.2.
```

Sys log

الأوامر اللازمة لتطبيق sys log server

```
damas-des2 (config)# logging host 192.168.0.8
```

ظهور فقط الرسائل من المستوى الرابع

```
damas-des2 (config)# logging trap 7
```

Standard Services Agreement

نقوم بتطبيقها على الـ ISP على الـ router المتصل مع

```
damas-edge2>enable
damas-edge2# configuration terminal
damas-edge2(config)# ip sla 1
damas-edge2 (config-ip-sla)# icmp-echo 188.80.60.2
damas-edge2 (config-ip-sla-icmp-echo) # frequency 300
```



```
damas-edge2 (config-ip-sla- icmp-echo) # timeout 3000
damas-edge2 (config-ip-sla- icmp-echo) #exit
damas-edge2 (config-ip-sla)#exit
damas-edge2 (config)# ip sla schedule 1 start-time now forever
```

Rspan

Configuration:

نريد مراقبة الـ Traffic تنقل الى VLAN 20 إلى السويفتش الثاني والذي يحوي نظام تحليل البيانات وكشف الفيروسات

```
damas-des2 (config)#vlan 20
damas-des2 (config-vlan)#remot-span
damas-des2 (config-vlan)#exit
damas-des2 (config)#monitor session 1 source interface fastethernet 1/1
damas-des2 (config)#monitor session 1 destination remot vlan 20
```

على الـ switch الثاني

```
damas-des1 (config)#monitor session 1 source remot vlan 20
damas-des1 (config)#monitor session 1 destination interface fastethernet 1/1
```

OSPF

سوف نقوم بتفعيل هذا البروتوكول على التجهيزات الآتية

Distribution Switches

Edge Routers

ISP Routers

Western Union Router

التجهيزات المشتركة بـ: Area 0 (backbone area)

Damas-edge1

Damas-edge2

Damas-des1

Damas-des2

التجهيزات المشتركة بـ: Area 1

Damas-edge1

Damas-edge2

ISP 1

ISP2

Western Union

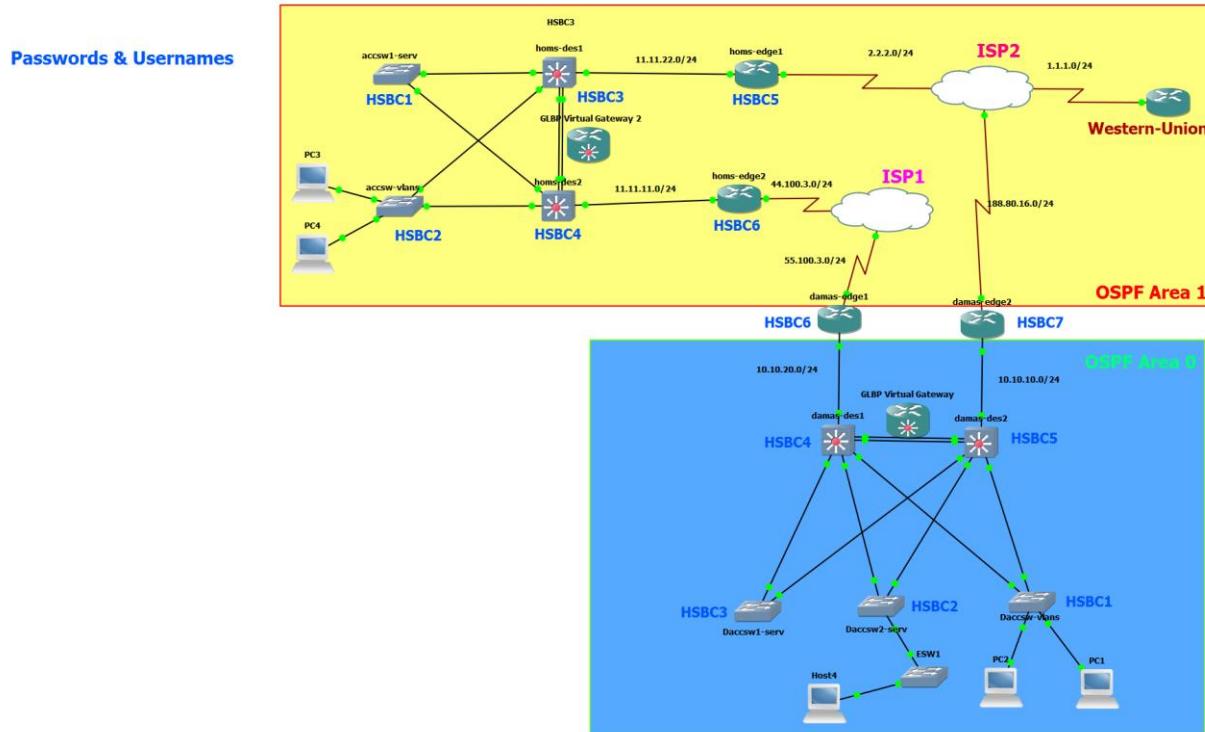
Homs-edge1

Homs-edge2

Homs-des1
Homs-des2

في حالتنا سوف يكون ABRs (Area Border Router) هما Damas-edge1 & Damas-edge2
Router وهو الـ ABR الوحيد الذي يكون مشترك بـ Area 0 & Area 1

توضيح الـ Areas



damas-des2

```

interface gig 0/0
no swithcport
no negotiation auto
duplex full
ip address 10.10.10.1 255.255.255.0
exit
router ospf 1
network 10.10.10.0 0.0.0.255 area 0
network 192.168.0.0 0.0.0.127 area 0
network 192.168.0.128 0.0.0.127 area 0
network 172.16.1.0 0.0.0.255 area 0
exit

```



damas-des1

```
interface gig 0/0
no swithcport
no negotiation auto
duplex full
ip address 10.10.20.1 255.255.255.0
exit
router ospf 1
network 10.10.20.0 0.0.0.255 area 0
network 192.168.0.0 0.0.0.127 area 0
network 192.168.0.128 0.0.0.127 area 0
network 172.16.1.0 0.0.0.255 area 0
exit
```

damas-edge2

```
interface fa0/0
no shutdown
duplex full
ip address 10.10.10.2 255.255.255.0
exit
interface serial 1/1
no shutdown
ip address 188.80.16.1 255.255.255.0
exit
router ospf 1
network 10.10.10.0 0.0.0.255 area 0
network 188.80.16.0 0.0.0.255 area 1
exit
```

damas-edge1

```
interface fa0/0
no shutdown
duplex full
ip address 10.10.20.2 255.255.255.0
exit
interface serial 1/1
no shutdown
ip address 55.100.3.1 255.255.255.0
exit
router ospf 1
```

```
network 10.10.20.0 0.0.0.255 area 0
network 55.100.3.0 0.0.0.255 area 1
exit
```

ISP2

```
interface serial 1/1
no shutdown
ip address 188.80.16.2 255.255.255.0
exit
interface serial 1/0
no shutdown
ip address 2.2.2.2 255.255.255.0
exit
interface serial 1/7
no shutdown
ip address 1.1.1.2 255.255.255.0
exit
router ospf 1
network 188.80.16.0 0.0.0.255 area 1
network 2.2.2.0 0.0.0.255 area 1
network 1.1.1.0 0.0.0.255 area 1
exit
```

ISP1

```
interface serial 1/0
no shutdown
ip address 44.100.3.2 255.255.255.0
```

exit

interface serial 1/1

no shutdown

ip address 55.100.3.2 255.255.255.0

exit

router ospf 1

network 44.100.3.0 0.0.0.255 area 1

network 55.100.3.0 0.0.0.255 area 1

exit

western-union

interface serial 1/7

no shutdown

ip address 1.1.1.1 255.255.255.0

exit

router ospf 1

network 1.1.1.0 0.0.0.255 area 1

exit

homs-edge1

interface serial 1/0

no shutdown

ip address 2.2.2.1 255.255.255.0

exit

interface fa0/0

no shutdown

duplex full

ip address 11.11.22.2 255.255.255.0

exit

router ospf 1

network 2.2.2.0 0.0.0.255 area 1

network 11.11.22.0 0.0.0.255 area 1

exit

homs-edge2

interface serial 1/0

no shutdown

ip address 44.100.3.0 255.255.255.0

exit

interface fa0/0

no shutdown

duplex full

ip address 11.11.11.2 255.255.255.0

exit

router ospf 1

network 44.100.3.0 0.0.0.255 area 1

network 11.11.11.0 0.0.0.255 area 1

exit

homs-des1

interface gig 0/0

no swithcport

no negotiation auto

duplex full

ip address 11.11.22.1 255.255.255.0

exit



```
router ospf 1  
network 11.11.22.0 0.0.0.255 area 1  
network 192.168.5.128 0.0.0.127 area 1  
network 192.168.6.128 0.0.0.127 area 1  
exit
```

homs-des2

```
interface gig 0/0  
no swithcport  
no negotiation auto  
duplex full  
ip address 11.11.11.1 255.255.255.0  
exit  
router ospf 1  
network 11.11.11.0 0.0.0.255 area 1  
network 192.168.5.128 0.0.0.127 area 1  
network 192.168.6.128 0.0.0.127 area 1  
exit
```

لتسهيل الأعلان عن الشبكات

بعد كتابة الأمر router ospf do show ip interface brief نفذ الأمر التالي network command

Verifying OSPF commands
Show ip ospf database
show ip ospf topology-info
Show ip ospf neighbor

SSH

configuration-damascus

damas-des1

```
hostname damas-des1
ip domain-name HSBC
username HSBC4 secret HSBC4
enable secret HSBC4
crypto key generate rsa modulus 1024
line vty 0 4
login local
transport input ssh
exit
ip ssh version 2
interface vlan 1
no shutdown
ip address 172.16.1.4 255.255.255.0
exit
```

damas-des2

```
hostname damas-des2
ip domain-name HSBC
username HSBC5 secret HSBC5
enable secret HSBC5
crypto key generate rsa modulus 1024
line vty 0 4
login local
```

```
transport input ssh  
exit  
ip ssh version 2  
interface vlan 1  
no shutdown  
ip address 172.16.1.5 255.255.255.0  
exit
```

Daccsw-vlans

```
hostname vlans  
ip domain-name HSBC  
username HSBC1 secret HSBC1  
enable secret HSBC1  
crypto key generate rsa modulus 1024  
line vty 0 4  
login local  
transport input ssh  
exit  
ip ssh version 2  
interface vlan 1  
no shutdown  
ip address 172.16.1.1 255.255.255.0  
exit
```

Daccsw2-serv

```
hostname accsw-serv2  
ip domain-name HSBC  
username HSBC2 secret HSBC2
```

```
enable secret HSBC2
crypto key generate rsa modulus 1024
line vty 0 4
login local
transport input ssh
exit
ip ssh version 2
interface vlan 1
no shutdown
ip address 172.16.1.2 255.255.255.0
exit
```

Dacsw-serv

```
hostname accsw-serv1
ip domain-name HSBC
username HSBC3 secret HSBC3
enable secret HSBC3
crypto key generate rsa modulus 1024
line vty 0 4
login local
transport input ssh
exit
ip ssh version 2
interface vlan 1
no shutdown
ip address 172.16.1.3 255.255.255.0
exit
```

damas-edge1

```
hostname damas-edge1
ip domain-name HSBC
username HSBC6 secret HSBC6
enable secret HSBC6
crypto key generate rsa modulus 1024
line vty 0 4
login local
transport input ssh
exit
ip ssh version 2
```

damas-edge2

```
hostname damas-edge2
ip domain-name HSBC
username HSBC7 secret HSBC7
enable secret HSBC7
crypto key generate rsa modulus 1024
line vty 0 4
login local
transport input ssh
exit
ip ssh version 2
```

ssh configuration-homs

homs-des1

```
hostname homs-des1
ip domain-name HSBC
username HSBC3 secret HSBC3
enable secret HSBC3
crypto key generate rsa modulus 1024
line vty 0 4
login local
transport input ssh
exit
ip ssh version 2
interface vlan 1
no shutdown
ip address 172.16.2.3 255.255.255.0
exit
```

homs-des2

```
hostname homs-des2
ip domain-name HSBC
username HSBC4 secret HSBC4
enable secret HSBC4
crypto key generate rsa modulus 1024
line vty 0 4
login local
transport input ssh
```

```
exit  
ip ssh version 2  
interface vlan 1  
no shutdown  
ip address 172.16.2.4 255.255.255.0  
exit
```

accesw-serv

```
hostname accesw-serv1  
ip domain-name HSBC  
username HSBC1 secret HSBC1  
enable secret HSBC1  
crypto key generate rsa modulus 1024  
line vty 0 4  
login local  
transport input ssh  
exit  
ip ssh version 2  
interface vlan 1  
no shutdown  
ip address 172.16.2.1 255.255.255.0  
exit
```

accesw-vlans

```
hostname accesw-vlans  
ip domain-name HSBC  
username HSBC2 secret HSBC2  
enable secret HSBC2
```

```
crypto key generate rsa modulus 1024
```

```
line vty 0 4
```

```
login local
```

```
transport input ssh
```

```
exit
```

```
ip ssh version 2
```

```
interface vlan 1
```

```
no shutdown
```

```
ip address 172.16.2.2 255.255.255.0
```

```
exit
```

homs-edge1

```
hostname homs-edge1
```

```
ip domain-name HSBC
```

```
username HSBC5 secret HSBC5
```

```
enable secret HSBC5
```

```
crypto key generate rsa modulus 1024
```

```
line vty 0 4
```

```
login local
```

```
transport input ssh
```

```
exit
```

```
ip ssh version 2
```

homs-edge2

```
hostname accsw-vlans
```

```
ip domain-name HSBC
```

```
username HSBC6 secret HSBC6
```

```
enable secret HSBC6
```

```
crypto key generate rsa modulus 1024
```

line vty 0 4

login local

transport input ssh

exit ip ssh version 2

Banner

وهي خدمة تعمل مع خدمتي telnet & SSH

نفعها على كافة تجهيزات الشركة ولتفعيلها نقوم بالآتي

```
damas-edge1(config)#line vty 0 4
damas-edge1(config-line)#banner login c WARNING DO NOT ENTER HSBC NETWORK c
damas-edge1(config)#
```

حيث حرف ، الأول لتحديد بداية الرسالة المراد اظهارها و الثاني لتحديد نهايتها

Multiple Spanning Tree Protocol (MST)

نقوم بتضمين الـ Vlans المراده الى الـ Instance المحدد ليكون لكل Instance طريق افتراضي مخصص ضمن الـ

Spanning tree

في مشروعنا تم التقسيم الى Two Instances

Instance 1

يضم :

Network_Admin VLAN

IT VLAN

Tech_Admin VLAN

Tech_support VLAN

Management VLAN

Instance 2

يضم

HR VLAN

inter_trades VLAN

Internal_trades VLAN
Cust_Services VLAN

Accounting VLAN

Security VLAN

الآن لتفعيل البروتوكول نقوم بكتابة الأوامر التالية على جميع الـ switches المشتركة بهذا البروتوكول

اعدادات فرع دمشق



```

damas-des2(config)#spanning-tree mode ms
damas-des2(config)#spanning-tree mode mst
damas-des2(config)#spanning-tree mst configuration
damas-des2(config-mst)#instance 1 vlan 10,20,30,40,50
damas-des2(config-mst)#instance 2 vlan 60,70,80,90,100,110
damas-des2(config-mst)#revision 1
damas-des2(config-mst)#

```

والآن لتحديد الـ Alternative Root Bridge و Root Bridge على الأوصياء Distribution Switches

```

damas-des1(config)#spanning-tree mst 1 root primary
damas-des1(config)#spanning-tree mst 2 root secondary
damas-des1(config)#

```

وعلى الـ Distribution Switch يقوم بكتابة الأوامر التالية:

```

damas-des2(config)#spanning-tree mst 1 root secondary
damas-des2(config)#spanning-tree mst 2 root primary
damas-des2(config)#

```

Verifying Mst commands:

```

Switch(config-mst)# show pending
Switch# show spanning-tree mst
Switch# show spanning-tree mst [instance number]
Switch# show spanning-tree mst configuration
Switch# show spanning-tree summary

```

Bpdu Filter

نقوم بالدخول للمنفذ المراد تطبيق الخدمة عليه وكتابة الأمر التالي:

```
spanning-tree bpdufilter enable
```

Root Guard

نقوم بالدخول للمنفذ المراد تطبيق الخدمة عليه وكتابة الأمر التالي:

```
Spanning-tree guard root
```

Loop Guard

نقوم بالدخول للمنفذ المراد تطبيق الخدمة عليه وكتابة الأمر التالي:

```
spanning-tree guard loop
```



GLBP (Gateway Load Balancing Protocol)

بما ان كل Vlan لها Distribution Switch واحده على كل Two Default Gateways فكل زوج من هذه البوابات الأفتراضية والتي تحمل نفس id VLAN سوف يكون لها نفس id VLAN سوف نرد مثال لكيفية تفعيل الخدمة على interface VLAN على التجهيز الأولى :

```
damas-des1(config)#interface vlan 10
damas-des1(config-if)#glbp 1 ip 192.168.0.126
damas-des1(config-if)#glbp 1 priority 1
damas-des1(config-if)#glbp 1 load-balancing round-robin
damas-des1(config-if)#glbp 1 preempt
damas-des1(config-if)#exit
damas-des1(config)#interface vlan 20
damas-des1(config-if)#glbp 2 ip 192.168.0.223
damas-des1(config-if)#glbp 2 priority 1
damas-des1(config-if)#glbp 2 load-balancing round-robin
damas-des1(config-if)#glbp 2 preempt
damas-des1(config-if)#exit
damas-des1(config)#[
```

على التجهيز الثانية :

```
damas-des2(config)#interface vlan 10
damas-des2(config-if)#glbp 1 ip 192.168.0.126
damas-des2(config-if)#glbp 1 priority 100
damas-des2(config-if)#glbp 1 load-balancing round-robin
damas-des2(config-if)#glbp 1 preempt
damas-des2(config-if)#exit
damas-des2(config)#interface vlan 20
damas-des2(config-if)#glbp 2 ip 192.168.0.223
damas-des2(config-if)#glbp 2 priority 100
damas-des2(config-if)#glbp 2 load-balancing round-robin
damas-des2(config-if)#glbp 2 preempt
damas-des2(config-if)#exit
damas-des2(config)#[
```

وهكذا على باقي interfaces VLAN

GLBP Verifying commands

Show glbp

Show glbp active

Show glbp standby

Show glbp listen

Show glbp brief

Show glbp detail

OSPF (Open Shortest Path First Protocol)



Network Security

VPN and IPSec

1- نقوم لتحديد السياسة الأمنية:

- تحديد رقم الـ (policy)

○ نوع (authentication)

○ نوع التشفير (encryption)

○ رقم الـ (group)

○ نوع الـ (hash)

2- نقوم بتحديد مفتاح المستخدم وتحديد عنوان

3- نقوم بصنع access list لتحديد ما هي البيانات المراد تشفيرها

4- تحديد الـ map

○ الأجهزة المراد تشفيرها

○ تحديد عنوان الجهاز المقابل

○ تحديد طريقة التشفير للمفتاح

5- نطبق الـ Map على الـ Interface

6- زمن بين كل مره يقوم الـ router بتغيير كلمه المرور (lifetime)



damas-edge2

```

www.zeallsoft.com
crypto isakmp policy 10
  encr aes
  authentication pre-share
  lifetime 63000
crypto isakmp key 6 cisco address 2.2.2.1
!
!
crypto ipsec transform-set set1 esp-aes esp-sha-hmac
!
crypto map map1 100 ipsec-isakmp
  set peer 2.2.2.1
  set transform-set set1
  match address vpndamas
!
!
!
!
interface FastEthernet0/0
  ip address 10.10.10.2 255.255.255.0
  duplex full
!
interface Serial1/0
  no ip address
  shutdown
  serial restart-delay 0
!
www.zeallsoft.com
  list extended vpnhoms
    permit ip 11.11.22.0 0.0.0.255 any
    permit ip 11.11.11.0 0.0.0.255 any
!

```

```

www.zeallsoft.com
  ip access-list extended vpndamas
    permit ip 10.10.10.0 0.0.0.255 any
    permit ip 10.10.20.0 0.0.0.255 any
!

```

homs-edge1

```

www.zeallsoft.com
crypto isakmp policy 10
  encr aes
  authentication pre-share
  lifetime 63000
crypto isakmp key 6 cisco address 188.80.16.1
!
!
crypto ipsec transform-set set1 esp-aes esp-sha-hmac
!
crypto map map1 110 ipsec-isakmp
  set peer 188.80.16.1
  set transform-set set1
  match address vpnhoms
!
!
!
!
interface FastEthernet0/0
  ip address 11.11.22.2 255.255.255.0
  duplex full
!
interface Serial1/0
  ip address 2.2.2.1 255.255.255.0
  serial restart-delay 0
  crypto map map1

```

Port Security

ويوجد أربع طرق لتفعيل امن المنفذ عند تنفيذ الإعدادات التالي

سيتم منع المتسللين من الدخول واستخدم المنفذ المخصصة للموظفين

من اجل تحديد عدد الأجهزة التي يتعلّمها السويفت

switchport portsecurity maximum 1



من أجل تحديد عنوان الـ Mac أو جعل الجهاز يتعلم الـ Mac

switchport portsecurity mac-address sticky

رفض الرسالة (من أجل تحديد السلوك الذي سيقوم به الـ Interface)

switchport portsecurity violation restrict

هذا فرع دمشق نطبق فقط على الـ Interface

0/0&0/1&0/2&1/0&1/2&1/3

```
www.zeallsoft.com
vlans#conf t
Enter configuration commands, one per line. End with CNTL/Z.
vlans(config)#int r gig 0/0-2
vlans(config-if-range)#switchport mode access
vlans(config-if-range)#switchport port-security maximum 1
vlans(config-if-range)#switchport port-security mac-address sticky
vlans(config-if-range)#switchport port-security violation restrict
vlans(config-if-range)#switchport port-security
vlans(config-if-range)#exit
vlans(config)#int gig 1/0
vlans(config-if)#switchport mode access
vlans(config-if)#switchport port-security maximum 1
vlans(config-if)#switchport port-security mac-address sticky
vlans(config-if)#switchport port-security violation restrict
vlans(config-if)#switchport port-security
vlans(config-if)#exit
vlans(config)#int r gig 1/2-3
vlans(config-if-range)#switchport mode access
vlans(config-if-range)#switchport port-security maximum 1
vlans(config-if-range)#switchport port-security mac-address sticky
vlans(config-if-range)#switchport port-security violation restrict
vlans(config-if-range)#switchport port-security
vlans(config-if-range)#exit
vlans(config)#
```

```
www.zeallsoft.com
vlans(config)#INT R GIG 1/2-3
vlans(config-if-range)#Switchport Mode ACcess
vlans(config-if-range)#SWitchport POrt-security MAXimum 1
vlans(config-if-range)#SWitchport POrt-security MAC-address Sticky
vlans(config-if-range)#SWitchport POrt-security VIolation Restrict
vlans(config-if-range)#SWitchport POrt-security
vlans(config-if-range)#EX
vlans(config)#INT R GIG 1/0
vlans(config-if-range)#SWitchport POrt-security MAXimum 1
vlans(config-if-range)#SWitchport POrt-security MAC-address Sticky
vlans(config-if-range)#SWitchport POrt-security VIolation Restrict
vlans(config-if-range)#SWitchport POrt-security
vlans(config-if-range)#EX
vlans(config)#DO SHOW PO
vlans(config)#DO SHOW POR
vlans(config)#DO SHOW PORT-security
vlans(config)#DO SHOW PORT-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
          (Count)      (Count)      (Count)
-----
    Gi0/0        1           0           0       Restrict
    Gi0/1        1           0           0       Restrict
    Gi0/2        1           0           0       Restrict
    Gi1/0        1           0           0       Restrict
    Gi1/2        1           0           0       Restrict
    Gi1/3        1           0           0       Restrict
```

هذا فرع حمص نطبق على الـ Interface

0/0&0/1&1/0&1/1&1/2&1/3

```
www.zealsoft.com
vlans>en
Password:
Password:
vlans#conf t
Enter configuration commands, one per line. End with CNTL/Z.
vlans(config)#
vlans(config)#int r gig 0/0-1
vlans(config-if-range)#
vlans(config-if-range)#switchport mode access
vlans(config-if-range)#switchport port-security maximum 1
vlans(config-if-range)#switchport port-security mac-address sticky
vlans(config-if-range)#switchport port-security violation restrict
vlans(config-if-range)#switchport port-security
vlans(config-if-range)#ex
vlans(config)#int r gig 1/0-3
vlans(config-if-range)#switchport mode access
vlans(config-if-range)#switchport port-security maximum 1
vlans(config-if-range)#switchport port-security mac-address sticky
vlans(config-if-range)#switchport port-security violation restrict
vlans(config-if-range)#switchport port-security
vlans(config-if-range)#ex
vlans(config)#

```

```
www.zeallsoft.com
127.0.0.1:8080

vlans(config-if-range)#switchport port-security violation restrict
vlans(config-if-range)#switchport port-security
vlans(config-if-range)#exit
vlans(config)#ex
% Ambiguous command: "ex"
vlans(config)#exit
vlans#
*May 23 18:29:46.676: %SYS-5-CONFIG_I: Configured from console by console
vlans#show po
vlans#show por
vlans#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
          (Count)      (Count)      (Count)
-----
  G10/0        1           0           0       Restrict
  G10/1        1           0           0       Restrict
  G11/0        1           0           0       Restrict
  G11/1        1           0           0       Restrict
  G11/2        1           0           0       Restrict
  G11/3        1           0           0       Restrict
-----
Total Addresses in System (excluding one mac per port) : 0
Max Addresses limit in System (excluding one mac per port) : 4096
vlans#
```

Control Access List

السماح للعنوان 192.168.0.16 بالوصول إلى 1.1.1.0

```
www.zeallsoft.com  
ip access-list extended damas  
 permit ip host 192.168.0.16 1.1.1.0 0.0.0.255  
 deny   ip host 192.168.0.145 1.1.1.0 0.0.0.255
```

منع للعنوان 192.168.0.145 بالوصول إلى

نطيقها على المنفذ (الخارج من الـ interface)

```
www.zeallsoft.com  
interface Serial1/1  
 ip address 188.80.16.1 255.255.255.0  
 ip access-group damas out
```

السماح للعنوان 192.168.5.148 بالوصول إلى 1.1.1.0

منع للعنوان 192.168.6.145 بالوصول إلى

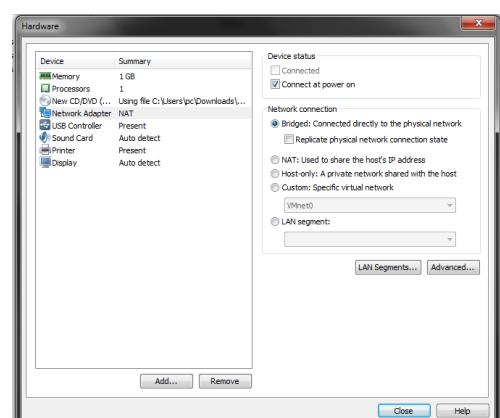
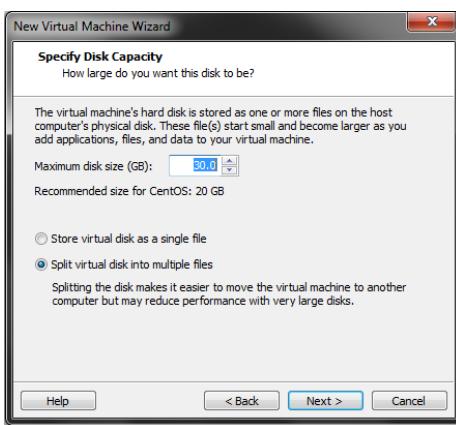
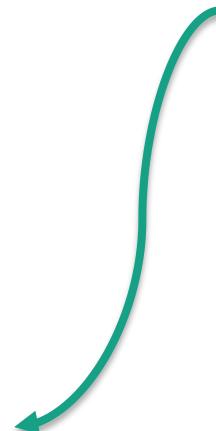
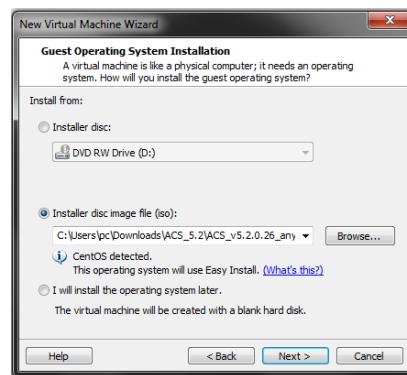
```
www.zeallsoft.com  
ip access-list extended homse  
 permit ip host 192.168.5.148 1.1.1.0 0.0.0.255  
 deny ip host 192.168.6.145 1.1.1.0 0.0.0.255
```

نطيقها على المنفذ (الخارج من الـ interface) (

```
www.zeallsoft.com Serial1/0  
 ip address 2.2.2.1 255.255.255.0  
 ip access-group homs out
```

AAA

(server acs) - تثبيت 1



```
GNU GRUB version 0.95 (638K lower / 2766784K upper MEMORY)

ADE-OS-1.2 (2.6.18.8-ADEUM)

Use the ↑ and ↓ keys to select which entry is highlighted.
Press enter to boot the selected OS or 'p' to enter a
password to unlock the next set of features.

The highlighted entry will be booted automatically in 2 seconds.
```

Booting 'ADE-OS-1.2 (2.6.18.8-ADEUM)'

```
root (hd0,8)
Filesystem type is ext2fs, partition type 0x83
kernel /boot/vmlinuz-2.6.18.8-ADEUM ro root=LABEL=/ selinux=0 quiet
[Linux-bzImage, setup=0x1e00, size=0x17d5c1]
initrd /boot/initrd-2.6.18.8-ADEUM.img
[Linux-initrd @ 0x37f30000, 0xbff8df bytes]

Uncompressing Linux... Ok, booting the kernel.
Red Hat nash version 4.2.1.13 starting
sda: assuming drive cache: write through
sda: assuming drive cache: write through
INIT: version 2.85 booting
Booting Cisco ADE-OS Version: 1.2.0.182 ...
INIT: Entering runlevel: 3
```

```
*****
Please type 'setup' to configure the appliance
*****
localhost login: setup_
```

Press 'Ctrl-C' to abort setup

```
Enter hostname[acs]: acs
Enter IP default netmask[1]: 192.168.0.4
Enter IP default netmask[1]: 192.168.0.15
Invalid Netmask
Enter IP default netmask[1]: 255.255.255.128
Enter IP default gateway[1]: 192.168.0.15
Enter default DNS domain[1]: HSBC.LO
Enter Primary nameserver[1]: 192.168.0.1
Add/Edit another nameserver? Y/N : N
Enter username[admin]: ACS
Enter password:
Enter password again:
Error: password cannot contain user name
Enter password:
Enter password again:
Passwords do not match
Enter password:
Enter password again:
Error: password must have at least one lower case letter
Enter password:
Enter password again:
Bringing up network interface...
Pinging the gateway...
```

```
Booting 'ADE-OS-1.2 (2.6.18.8-ADEUM)'

root (hd0,8)
Filesystem type is ext2fs, partition type 0x83
kernel /boot/vmlinuz-2.6.18.8-ADEUM ro root=LABEL=/ selinux=0 quiet
[Linux-bzImage, setup=0x1e00, size=0x17d5c1]
initrd /boot/initrd-2.6.18.8-ADEUM.img
[Linux-initrd @ 0x37f30000, 0xbff8df bytes]

Uncompressing Linux... Ok, booting the kernel.
Red Hat nash version 4.2.1.13 starting
sda: assuming drive cache: write through
sda: assuming drive cache: write through
INIT: version 2.85 booting
```

```
acs login: acs
Password: _
```

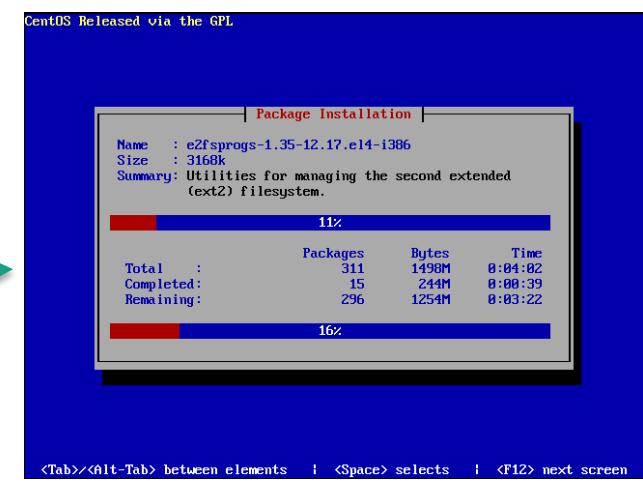
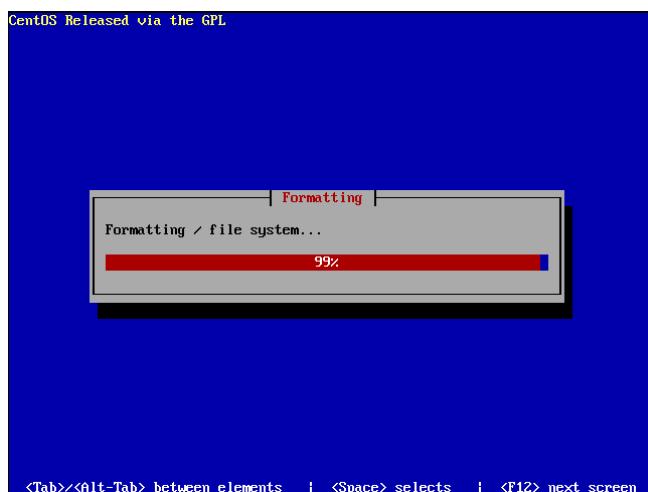
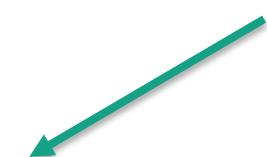
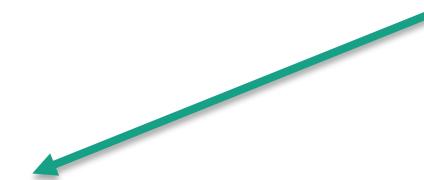
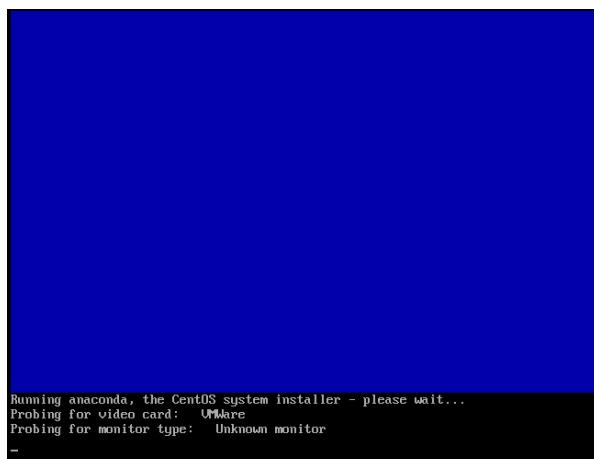
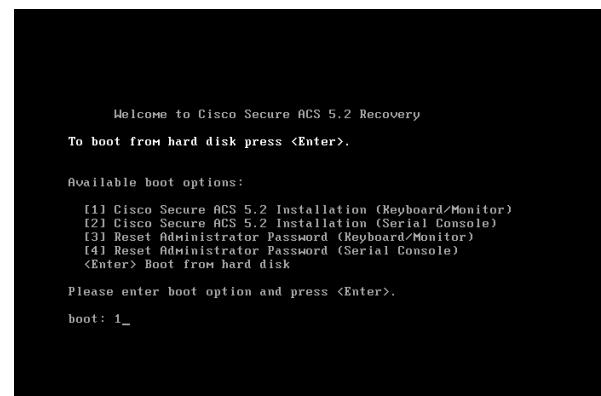
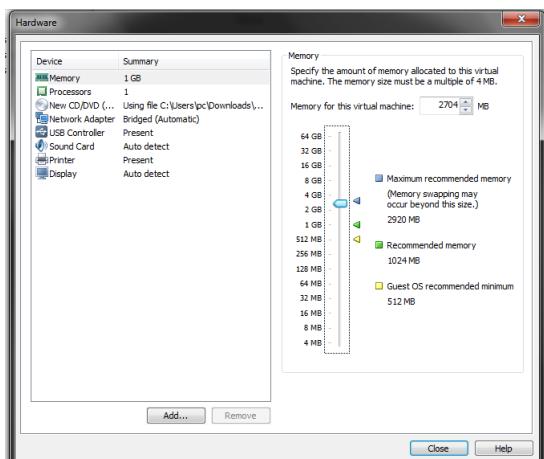
```
acs login: acs
Password:
Login incorrect

login: ACS
Password:
acs/ACS# show app status acs

ACS role: PRIMARY

Process 'database'                                running
Process 'management'                             running
Process 'runtime'                                 running
Process 'view-database'                           running
Process 'view-jobmanager'                         running
Process 'view-alertmanager'                      running
Process 'view-collector'                          running
Process 'view-logprocessor'                      running

acs/ACS# _
```





www.zealsoft.com ACS Login - Windows Internet Explorer
https://192.168.0.4/acsadmin/login.htm
Favorites Cisco Secure ACS Login

Cisco Secure ACS
Version 5.2.0.26
Hostname: acs (Primary)
Welcome to Cisco Secure ACS
For Authorized Use Only

Copyright 2009 Cisco Systems Inc
All rights reserved

Username: acsadmin
Password:
Log In | Reset

Internet | Protected Mode: On 100%

www.zealsoft.com ACS - Windows Internet Explorer
https://192.168.0.4/acsadmin/
Favorites Cisco Secure ACS

Cisco Secure ACS
EVAL(Days left: 90)

Welcome to Cisco Secure Access Control System

Before You Begin
Essential Reading to Get Started
ACS Policy Model & Terminology

Getting Started
Let ACS guide you through these tasks
Quick Start
Initial System Setup
Policy Setup Steps

New in ACS 5
Managing Network Devices
Managing Users & Identities
Creating & Maintaining Policies

Tutorials & Other Resources
Introduction & Overview Video
Common Scenarios

Cisco Secure ACS Online Resources: Product & Support Information, Forums, WWW.CISCO.COM

Internet | Protected Mode: On 100%

www.zealsoft.com ACS - Windows Internet Explorer
https://192.168.0.4/acsadmin/
Favorites Cisco Secure ACS

Cisco Secure ACS
EVAL(Days left: 90)

Network Resources > Network Device Groups > Location > Create

Device Group - General

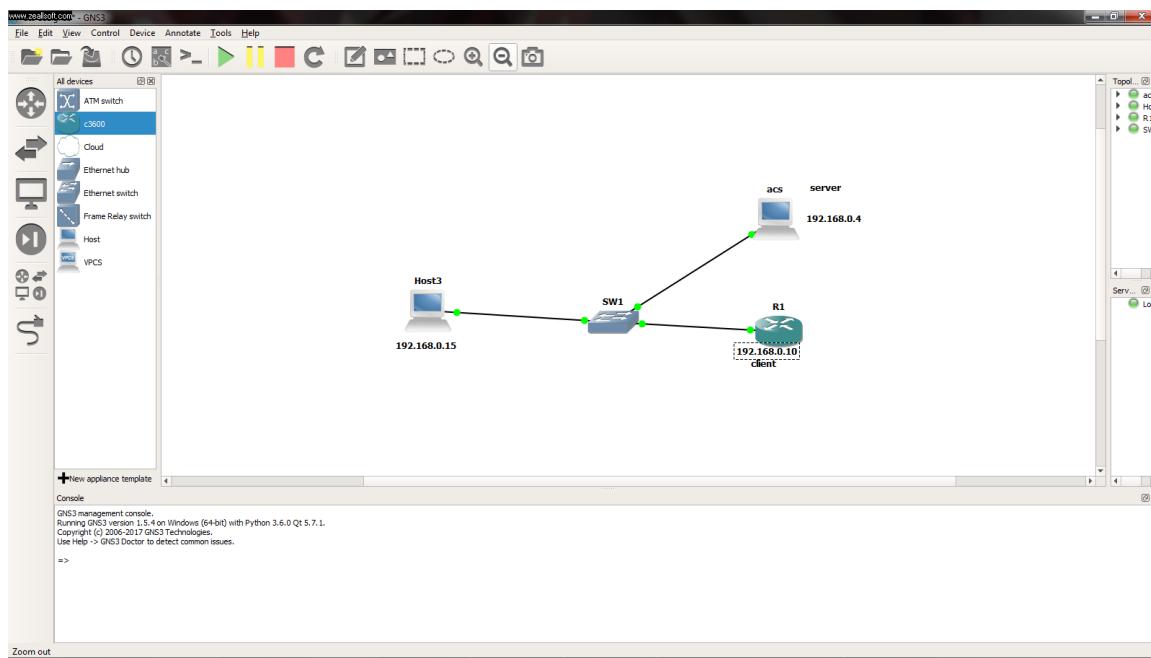
Name: HSBC
Description: HSBC-L1
Parent: All Locations
Required fields

Submit | Cancel

Policy Setup Steps
Follow the steps listed below to build ACS access control policies. Clicking on any of the links will navigate the main web console to the appropriate configuration page. For more information, please refer to online help.

- Define Policy Elements
Policy Elements are the building blocks of policy rules. >
Time & Date Conditions
Custom Conditions
Network Access Authorization Profiles
Device Shell Profiles
Device Command Sets
- Create a new Access Service
An ACS Access Service is the basic access policy

Internet | Protected Mode: On 100%



2- تحديد اعدادات السيرفر AAA

ce0ctrl.com|ACS - Windows Internet Explorer
192.168.0.4

Favorites | Cisco Secure ACS

Cisco Secure ACS
EVAL(days left: 87)

acadmin acc (Primary) Log Out About Help

My Workspace

Network Resources

- Network Device Groups
- Location
- Device Type
- Hosted Services and AAA Clients
- Default Network Device
- External RADIUS Servers

Users and Identity Stores

Policy Elements

Access Policies

Monitoring and Reports

System Administration

Network Resources > Network Devices and AAA Clients > Create

Name: R1
Description: RAAA
Network Device Groups

Location: All Locations Habc [Select]
Device Type: All Device Types lab1-device [Select]

IP Address

Single IP Address [Selected] IP Range(s)
IP: 192.168.0.10

Authentication Options

TACACS+ [Selected]
Shared Secret: admin
Single Connect Device
Legacy TACACS+ Single Connect Support
TACACS+ Draft Compliant Single Connect Support

RADIUS [Selected]
Shared Secret
CoA port: 1700
Enable KeyWrap
Key Encryption Key
Message Authenticator Code Key
Key Input Format: ASCII [Selected] HEXADECIMAL

Submit Cancel

www.zealsoft.com/ACS - Windows Internet Explorer
192.168.0.4 Cisco Secure ACS

Cisco Secure ACS
EVAL(Days left: 87)

My Workspace Network Resources Network Device Groups Network Devices and AAA Clients Default Network Device External RADIUS Servers Users and Identity Stores Policy Elements Access Policies Monitoring and Reports System Administration

Network Resources > Network Devices and AAA Clients Network Devices

Name	IP / Mask	NDG Location	NDG Device Type	Description
R1	192.168.0.10/32	All Locations: Hsbc	All Device Types: lab1-device	RAAA

Show 1-1 of 1 50 per page Go

Create Duplicate Edit Delete File Operations Export Page 1 of 1

Internet | Protected Mode: On 100%

www.zealsoft.com/ACS - Windows Internet Explorer
192.168.0.4 Cisco Secure ACS

Cisco Secure ACS
EVAL(Days left: 87)

My Workspace Network Resources Users and Identity Stores Identity Groups Internal Identity Stores Hosts External Identity Stores LDAP Active Directory RSA SecurID Token Servers RADIUS Identity Servers Certificate Authorities Certificate Authentication Profile Identity Store Sequences Policy Elements Access Policies Monitoring and Reports System Administration

Users and Identity Stores > Internal Identity Stores > Users > Create

General

Name: mohamad Status: Enabled

Description: it

Identity Group: All Groups:it

Password Information

Password must:

- Contain 4 - 32 characters

Password: Confirm Password:

Change password on next login

User Information

There are no additional identity attributes defined for user records

= Required fields

Enable Password Information

Password must:

- Contain 4 - 32 characters

Enable Password: Confirm Password:

Submit Cancel

www.zealsoft.com/ACS - Windows Internet Explorer
192.168.0.4 Cisco Secure ACS

Cisco Secure ACS
EVAL(Days left: 87)

My Workspace Network Resources Users and Identity Stores Identity Groups Internal Identity Stores Hosts External Identity Stores LDAP Active Directory RSA SecurID Token Servers RADIUS Identity Servers Certificate Authorities Certificate Authentication Profile Identity Store Sequences Policy Elements Access Policies Monitoring and Reports System Administration

Users and Identity Stores > Internal Identity Stores > Users > Create

General

Name: admin strator Status: Enabled

Description: it&hr

Identity Group: All Groups

Password Information

Password must:

- Contain 4 - 32 characters

Password: Confirm Password:

Change password on next login

User Information

There are no additional identity attributes defined for user records

= Required fields

Enable Password Information

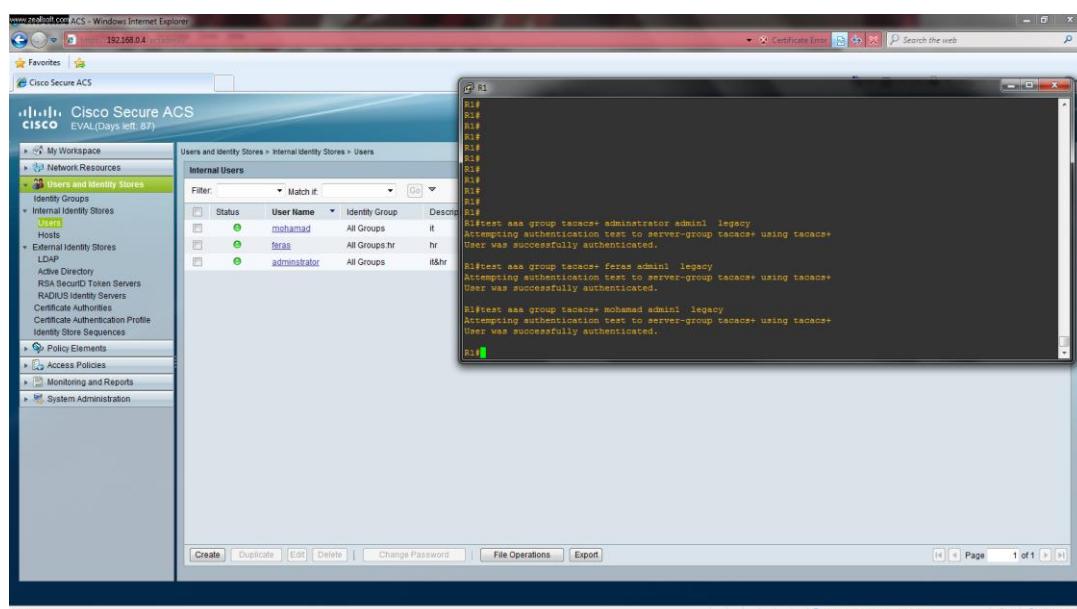
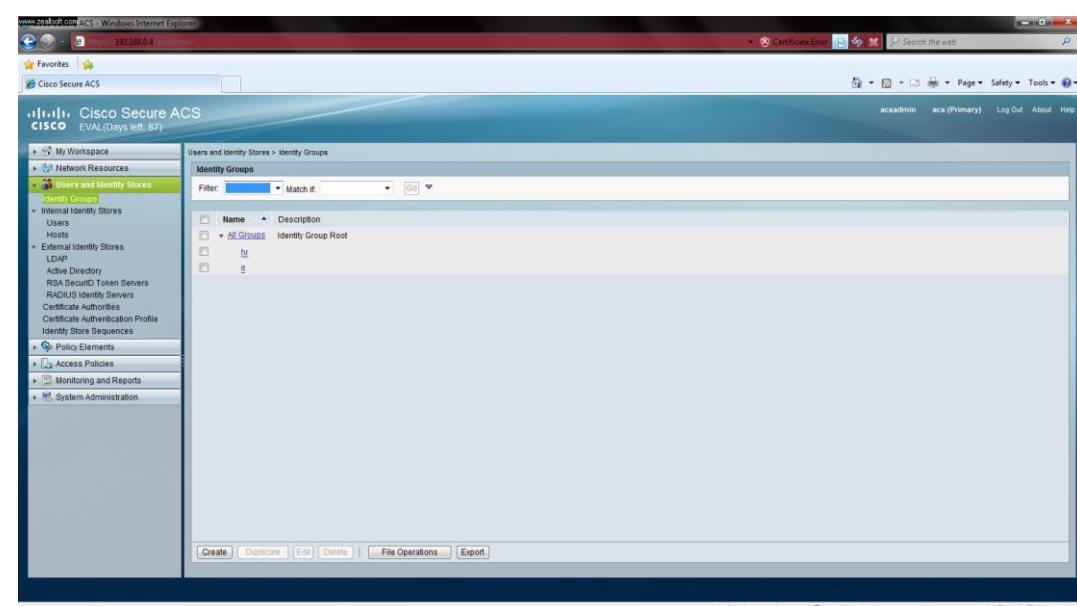
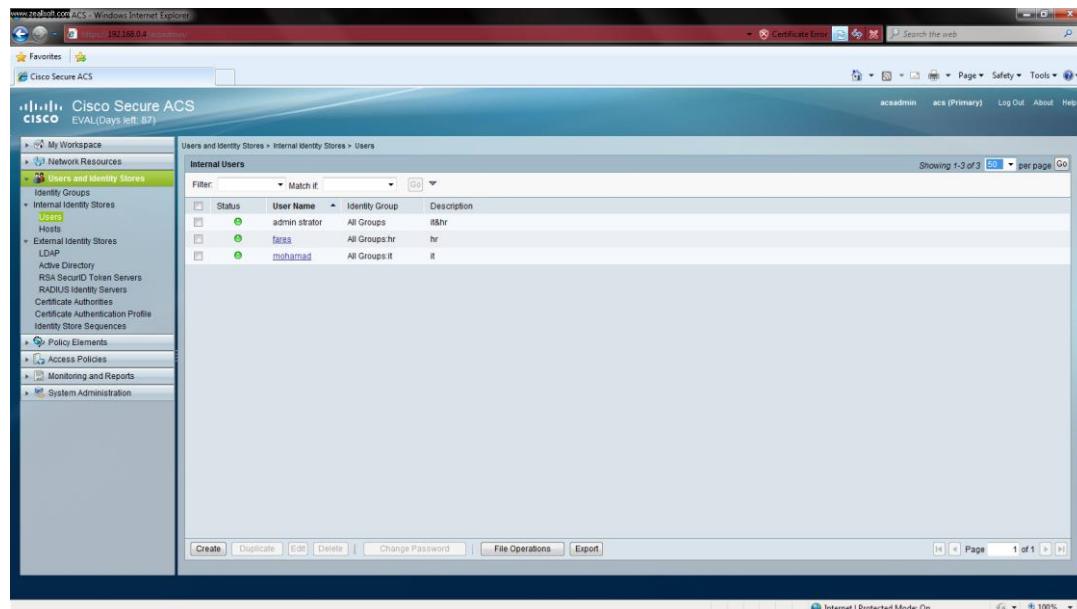
Password must:

- Contain 4 - 32 characters

Enable Password: Confirm Password:

Submit Cancel

Done Internet | Protected Mode: On 100%





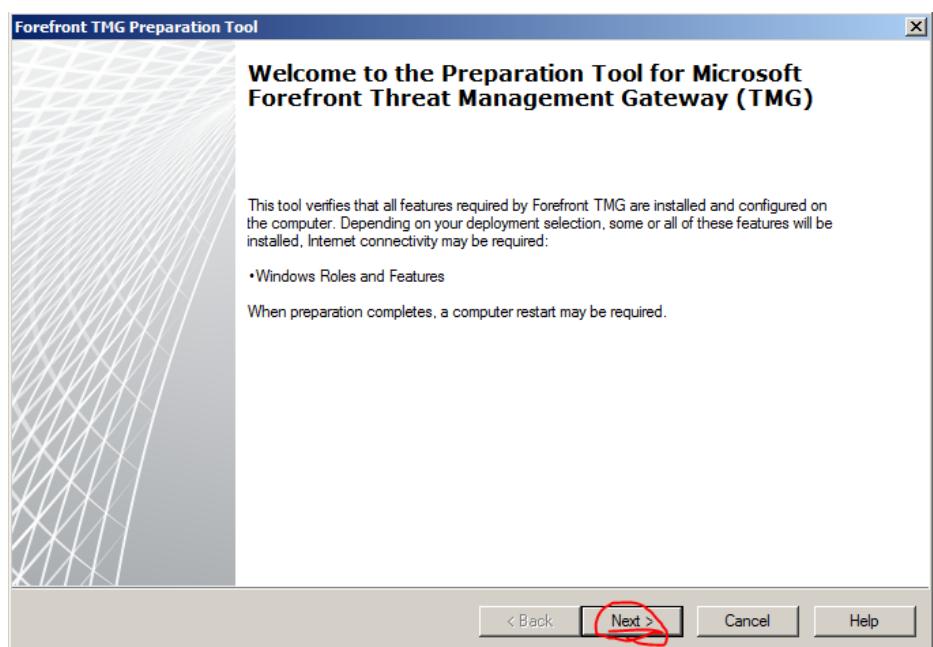
اعدادات سيرفر الـ TMG

(1) تنصيب السيرفر :

بداية يجب ان يتوفّر لدينا في السيرفر كرتين شبكة على الاقل

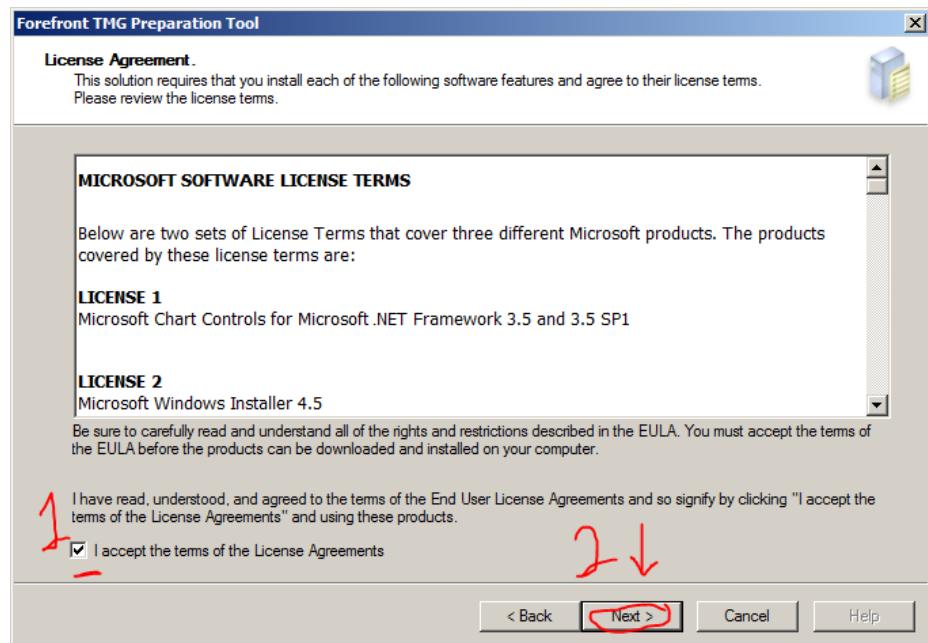
ثم نبدأ بتشغيل ملف التنصيب ثم نتبع الخطوات التالية:

بداية نشغل اداة الاعداد للتجهيز للتنصيب

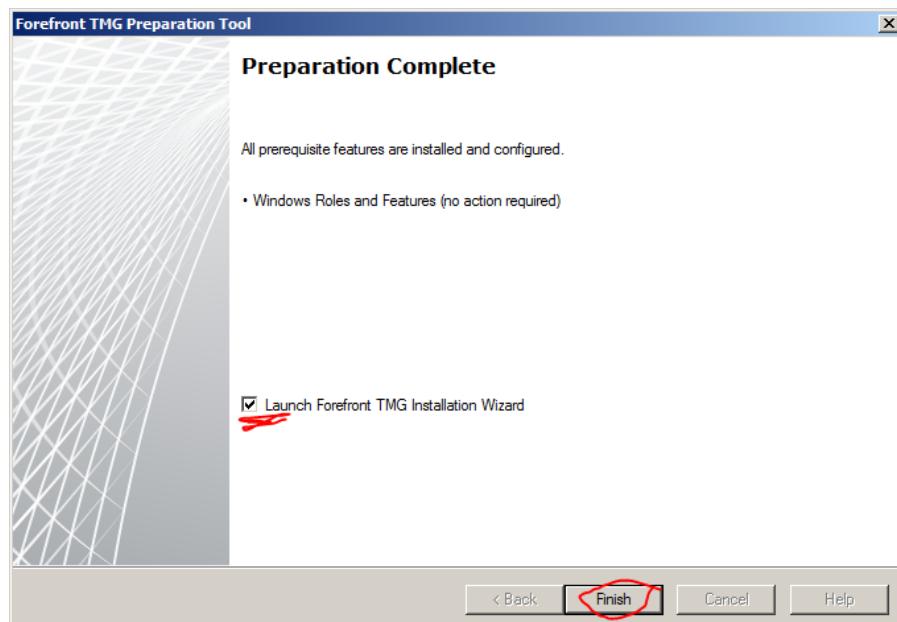




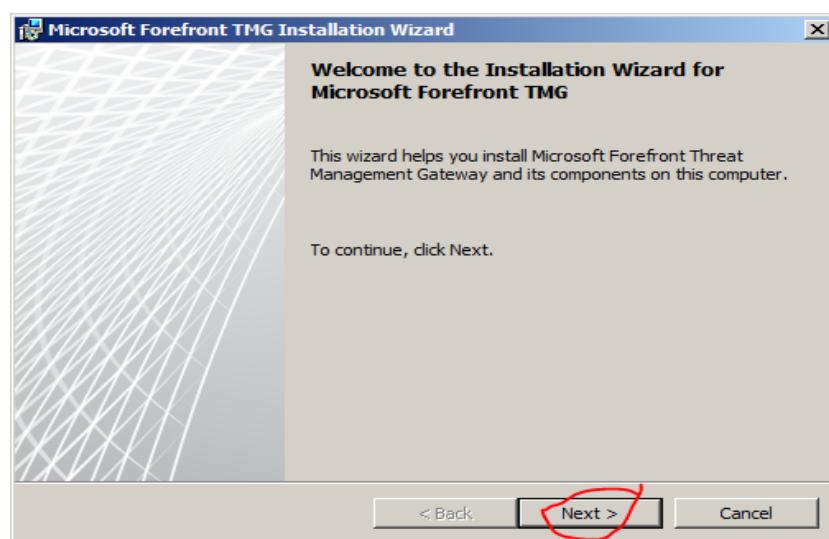
نوافق على الشروط



نختار نوع الـ TMG المراد تنصيبه في حالتنا هنا الخيار الاول لأننا نريد تنصيب السيرفر مع عمل ادارة عليه



بمجرد ضغطنا على زر الانتهاء، سوف يبدأ معالج الأعداد لتنصيب الـ TMG

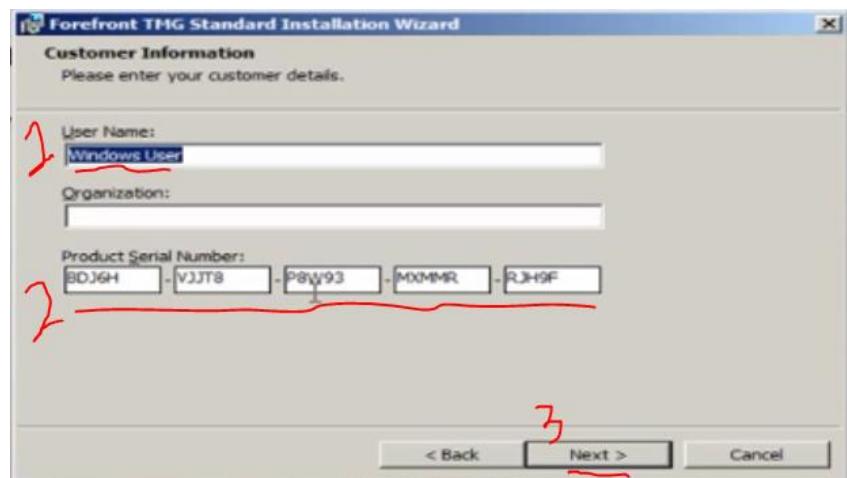


نوفق على الشروط

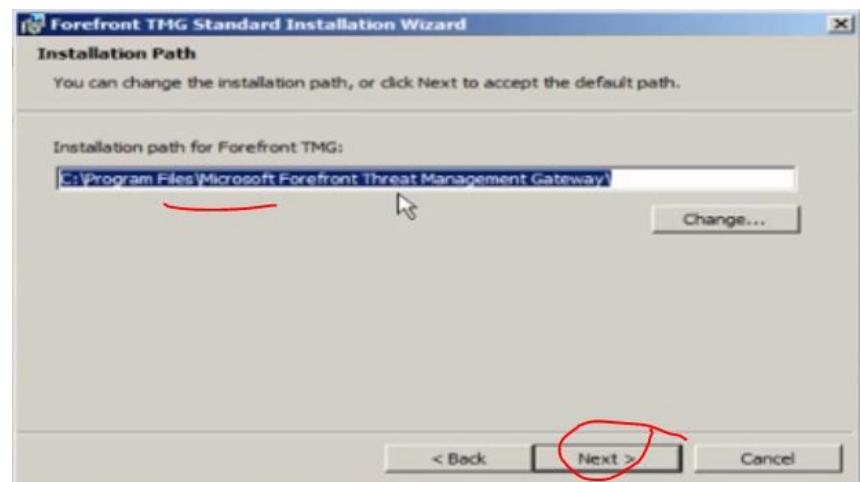




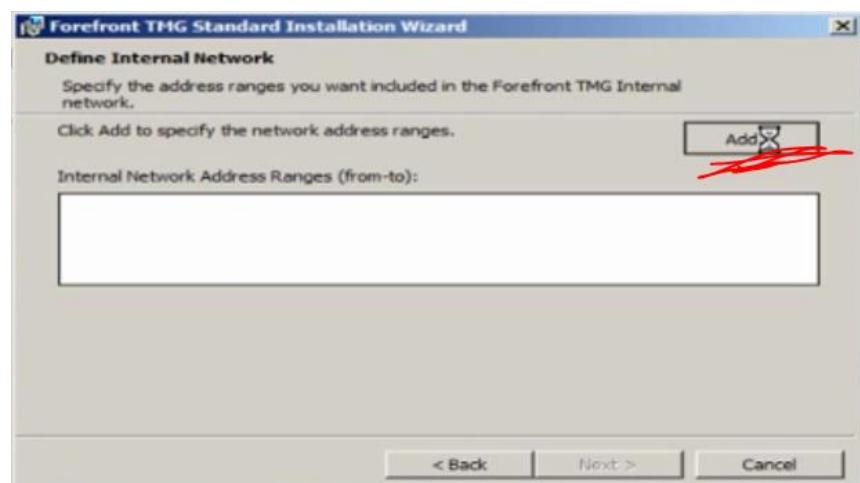
ندخل السيريرال



نختار مكان التنصيب بشرط ان يكون نظام الملفات للهارد المراد التنصيب عليه من نوع NTFS

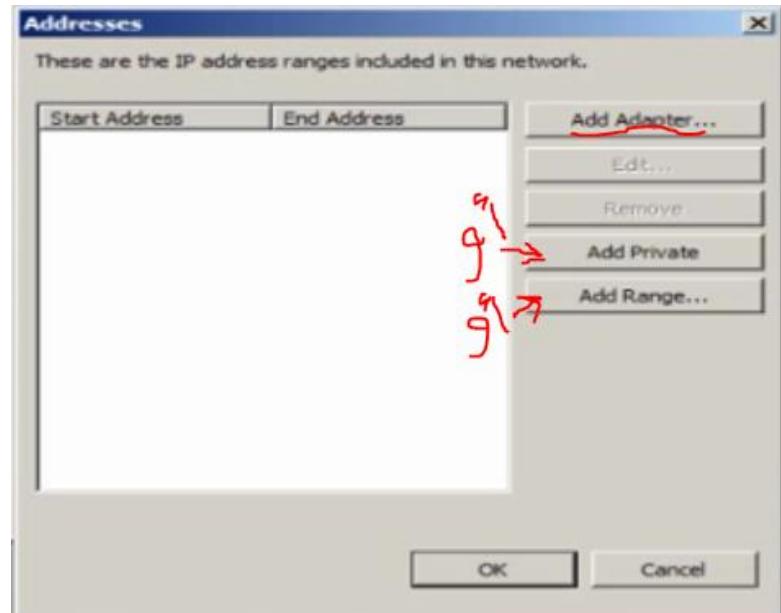


بعد ذلك سوف يطلب منا تحديد الشبكة الداخلية المرتبطة مع السيرفر فنضغط على اضافة

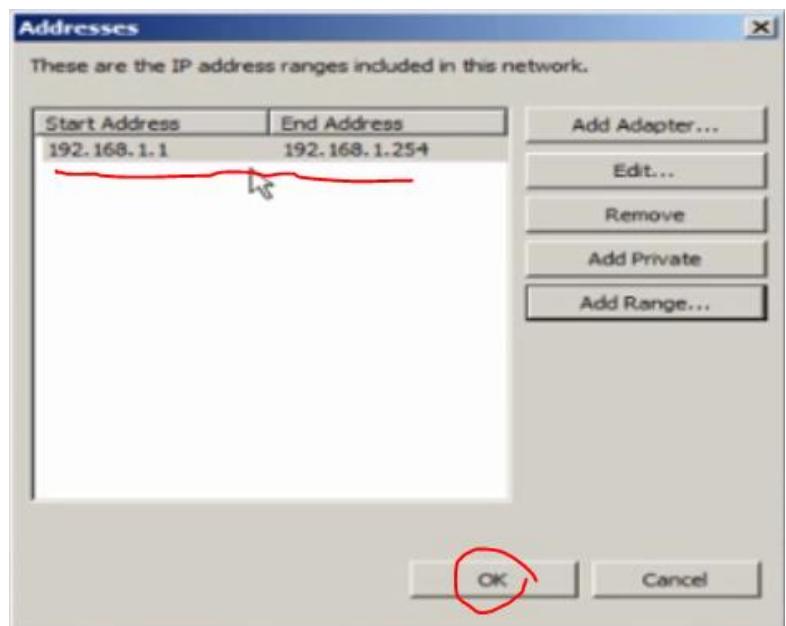
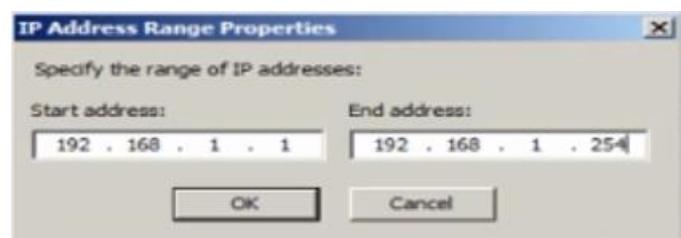




هنا يكون لدينا ثلاثة طرق لاضافة الشبكة الداخلية :
 اما عن طريق اضافة محول شبكة فنختار المحول المرتبط بالشبكة الداخلية فيقوم بوضع المجال المشكل لشبكته
 او عن طريق اضافة عنوان شبكة خاصة بحيث يتيح لنا الاختيار من بين اي شبكة خاصة
 او عن طريق اضافة مجال ندخله يدويا بتحديد عنوان بداية ونهاية له

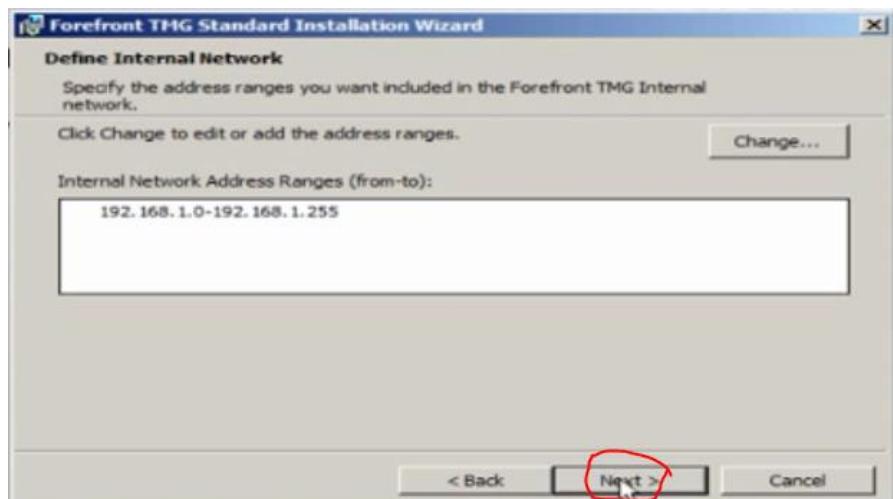


هنا اخترت تمrir مجال

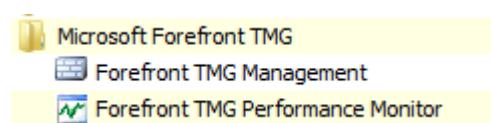




بعد تمرير المجال نكمل عملية التنصيب



وبهذا تكون قد نصبنا السيرفر





بعد التنصيب يكون لدينا في السيرفر سياسة امنية افتراضية تقول بمنع اي مستخدم قادم من اي شبكة بالولوج الى اي

شبكة في اي وقت

(2) TMG Client

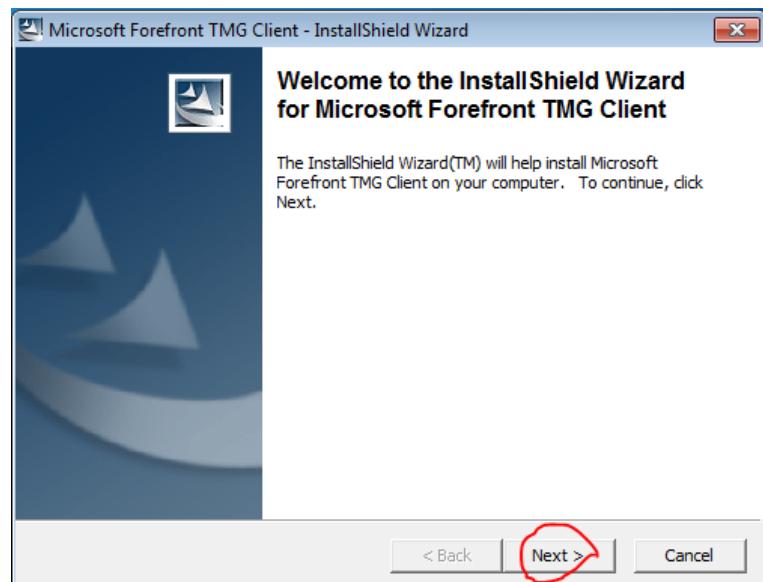
كيفية اعداد جهاز ليكون جهاز زبون لل TMG اي يعتمد في اتصاله على السيرفر

هنا لدينا يجب علينا نصيف برنامج على الجهاز الزبون ليكون اتصاله عن طريق ال TMG حسب الخطوات التالية :

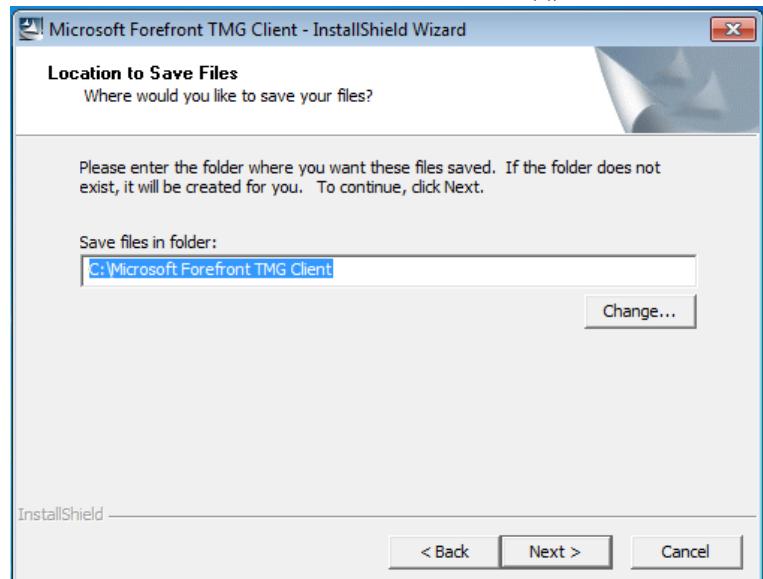
البرنامج المراد تنصيبه :

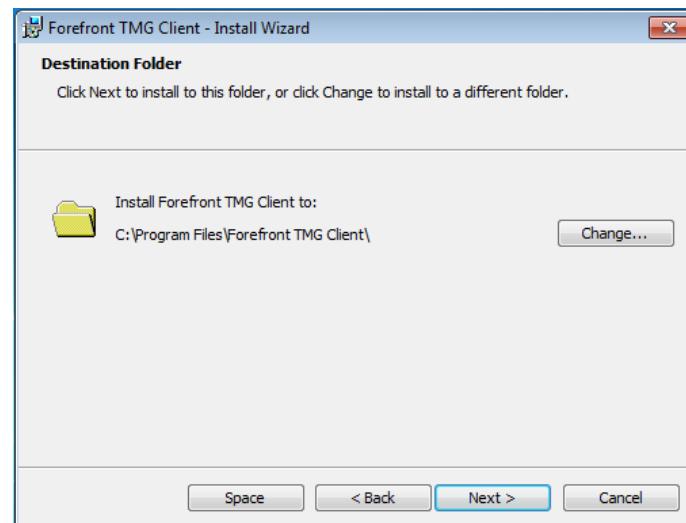


نشغله ثم نتبع الخطوات التالية :



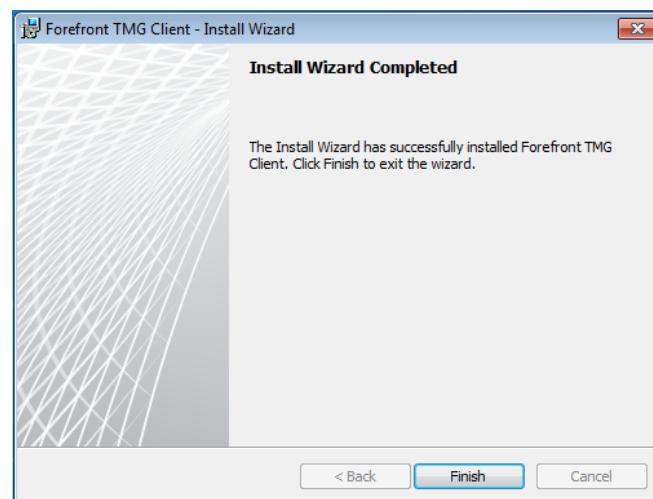
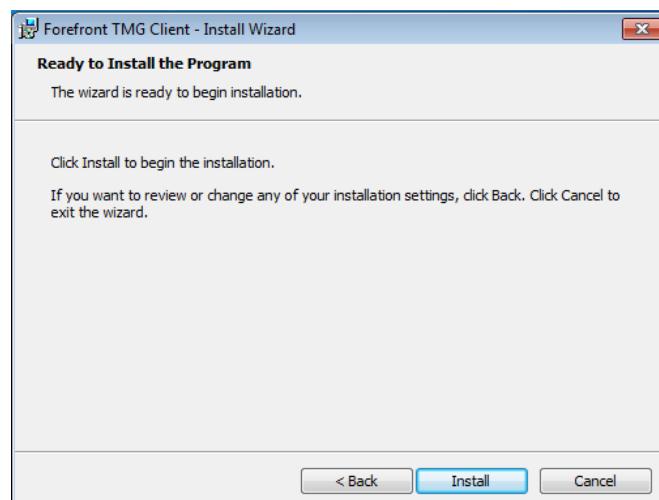
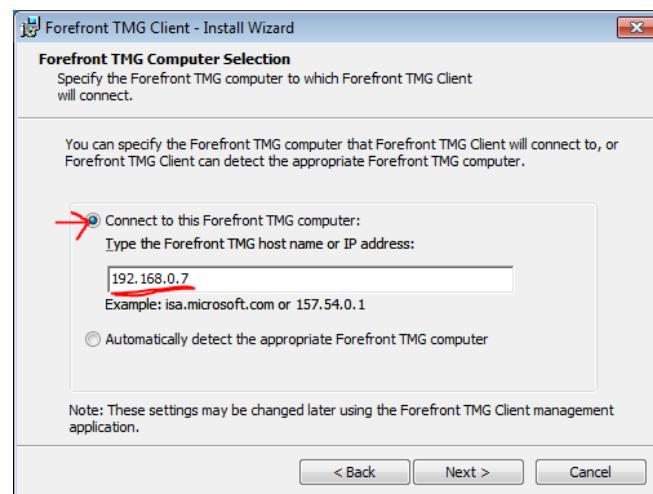
نختار مكان التنصيب





هنا يطلب منا ادخال عنوان السيرفر بشكل يدوي او الاتصال به بشكل اتوماتيكي

وانا هنا اخترت الاتصال بالسيرفر بشكل يدوي



ISP Redundancy (3

هي عملية تعددية الوصلات مع الانترنت وهذا لدينا نوعين

اما عن طريق fail over اي تفعيل وصلة والاعتماد عليها في الاتصال مع الانترنت وفي حال وقوعها الاعتماد على الوصلة الثانية لتحمل محلها



او عن طريق (load balancing) non fail over اي توزيع الحمل بين الوصلتين بحيث ان مستخدمين معينين يستخدمون الوصلة الاولى في حين ان الباقي يستخدمون الوصلة الاخرى وفي حال وقوع احد الوصلات يمكننا الاعتماد على الوصلة الاخرى ليعمل عليها كافة المستخدمين

سوف اقوم بتطبيق طريقة الـ load balancing لاحق عملية توزيع الحمل بين الوصلات

وذلك عن طريق الخطوات التالية :

بداية يجب اضافة كرت شبكة ثالث للسيرفر واعطائه public ip لوصول الوصلة الاحتياطية مع الانترنت

عليه

Name	Type	IP Addresses	Subnets	Status
WIN-PUES3Q57VKO				
External 2 (62.1.1.1)	Static	62.1.1.1	255.255.255.248	Connected
External1 (61.1.1.1)	Static	61.1.1.1	255.255.255.248	Connected
Internal (192.168.0.7)	Static	192.168.0.7	255.255.255.0	Connected

ثم ندخل اي معالج ادارة الـ TMG ونختار الخيار networking ثم نختار التاب ISP Redundancy ثم الخيار configure ISP Redundancy

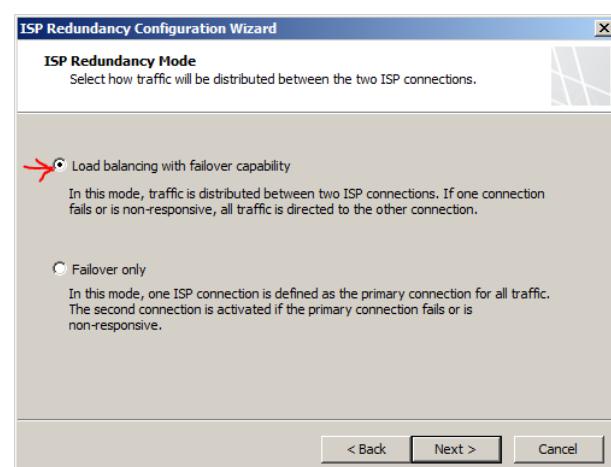
The screenshot shows the Microsoft Forefront Threat Management Gateway 2010 interface. On the left, there is a navigation pane with various icons and a tree view showing 'Forefront TMG (WIN-PUES3Q57VKO)' under 'Microsoft Forefront Threat Management'. A red arrow points from the text 'Then enter any management device' to this pane. On the right, the main window displays the 'ISP Redundancy' configuration page. The title bar says 'Microsoft Forefront Threat Management Gateway 2010'. Below it, a banner says 'Click here to learn about the Customer Experience Improvement Program.' The top menu bar includes 'File', 'Action', 'View', 'Help', and several icons. The main content area has tabs: 'Networks', 'Network Sets', 'Network Rules', 'Network Adapters', 'Routing', 'Web Chaining', and 'ISP Redundancy'. A red arrow points from the text 'Select the ISP redundancy tab' to the 'ISP Redundancy' tab. Below the tabs, the section 'ISP Redundancy' is described with the text: 'You can configure ISP redundancy to distribute outbound traffic between two ISP connections using failover between a primary and backup link, or load balancing and failover. To define the ISP connections and the distribution mode, on the task pane, click Configure ISP Redundancy.' A red arrow points from the text 'Configure the ISP connections' to the 'Configure ISP Redundancy' link.



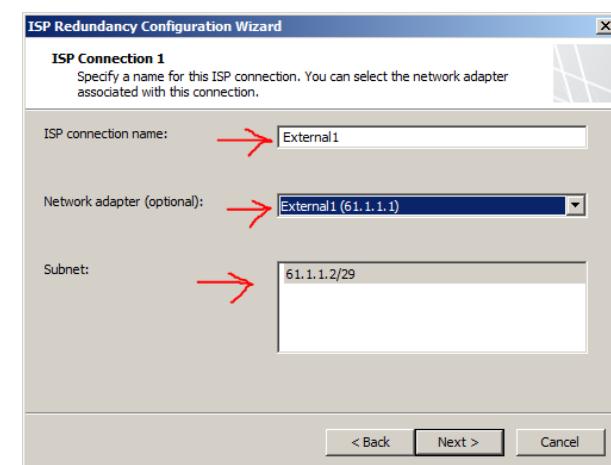
بعد ذلك نكمل خطوات الاعداد حسب التالي :



نختار الخيار الاول (load balancing+failover) من اجل توزيع الحمل وعمل وصلة احتياطية



ثم نختار محول الشبكة الاول بعد وضع اسم له





ISP Redundancy Configuration Wizard

ISP Connection 1 - Configuration
Modify or enter the details for this ISP.

Gateway address:	51 . 1 . 1 . 2	/ Mask	29
Subnet:	255 . 255 . 255 . 248		
Primary DNS server:	8 . 8 . 8 . 8		
Alternate DNS server:	. . .		

< Back Next > Cancel

ISP Redundancy Configuration Wizard

ISP Connection 1 - Dedicated Servers
Traffic to the servers specified here will be routed through this ISP connection only.

Dedicated servers:	External1 Primary DNS Server	Add
		Edit
		Remove

Examples: ISP-specific DNS servers, mail servers.

< Back Next > Cancel

نختار محول الشبكة الثاني بعد وضع اسم له

ISP Redundancy Configuration Wizard

ISP Connection 2
Specify a name for this ISP connection. You can select the network adapter associated with this connection.

ISP connection name:	External2
Network adapter (optional):	External 2 (62.1.1.1)
Subnet:	62.1.1.2/29

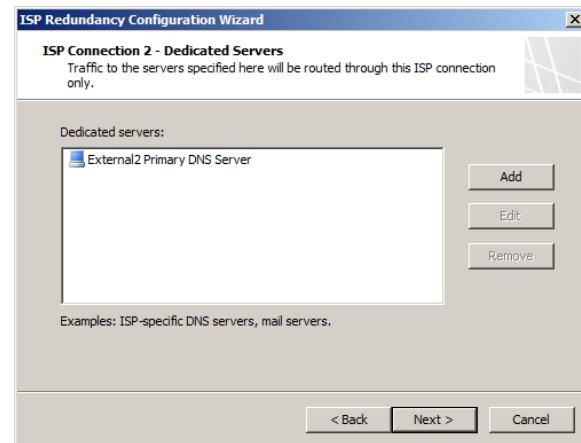
< Back Next > Cancel

ISP Redundancy Configuration Wizard

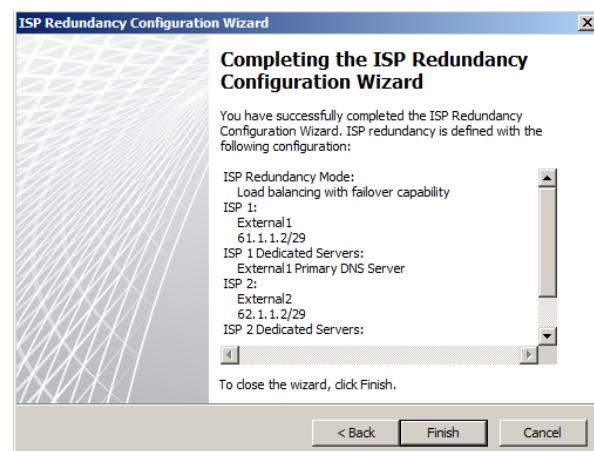
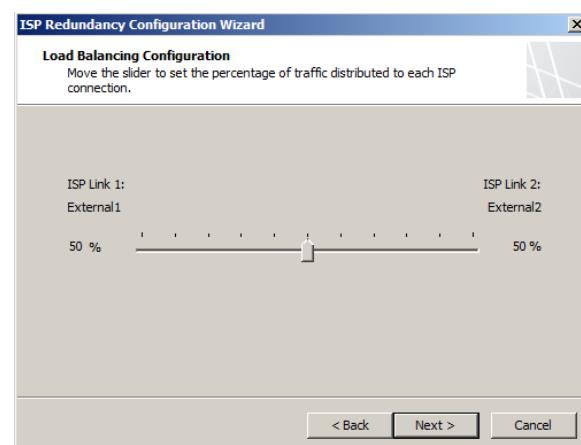
ISP Connection 2 - Configuration
Modify or enter the details for this ISP.

Gateway address	52 . 1 . 1 . 2	/ Mask	29
Subnet:	255 . 255 . 255 . 248		
Primary DNS server:	8 . 8 . 4 . 4		
Alternate DNS server:	. . .		

< Back Next > Cancel



ثم نختار توزيع الحمل بين الوصلتين بحيث اخترت انا ان يكون مناصفة



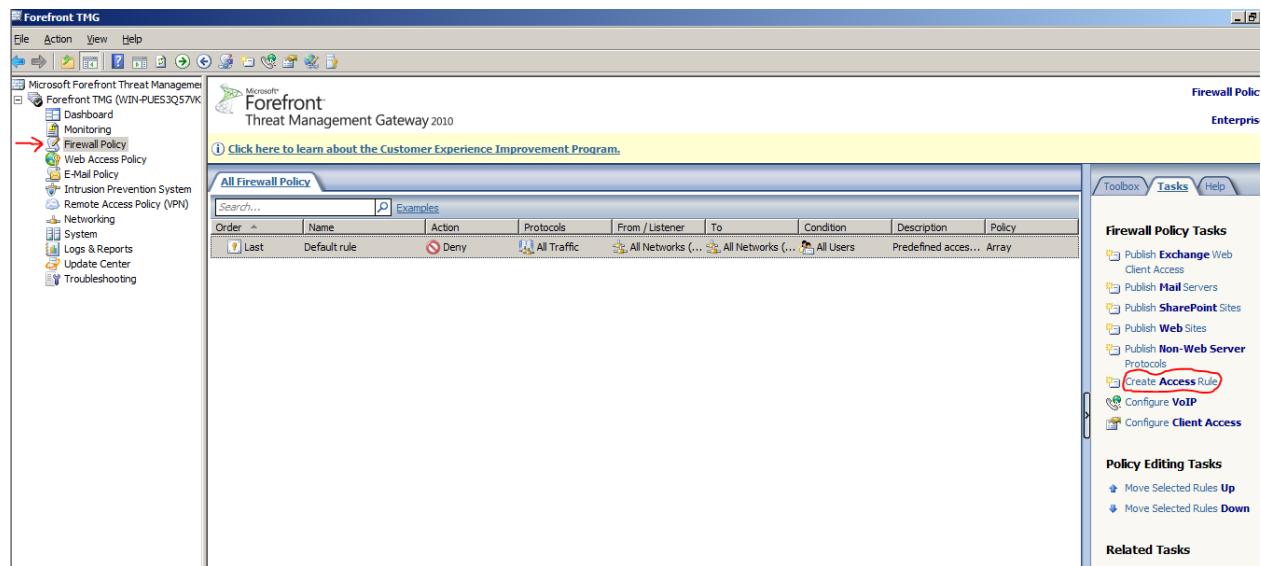
وبهذا يكون اصبح لدينا وصلتين مع الانترنت يستخدمهما السيرفر لتوزيع الحمل بينهما ول تقوم احداهما محل الاخرة في حال وقوعها



firewall rules (4

وهي عبارة عن السياسة الآمنية للسماح او المنع للمستخدمين بمرور البيانات

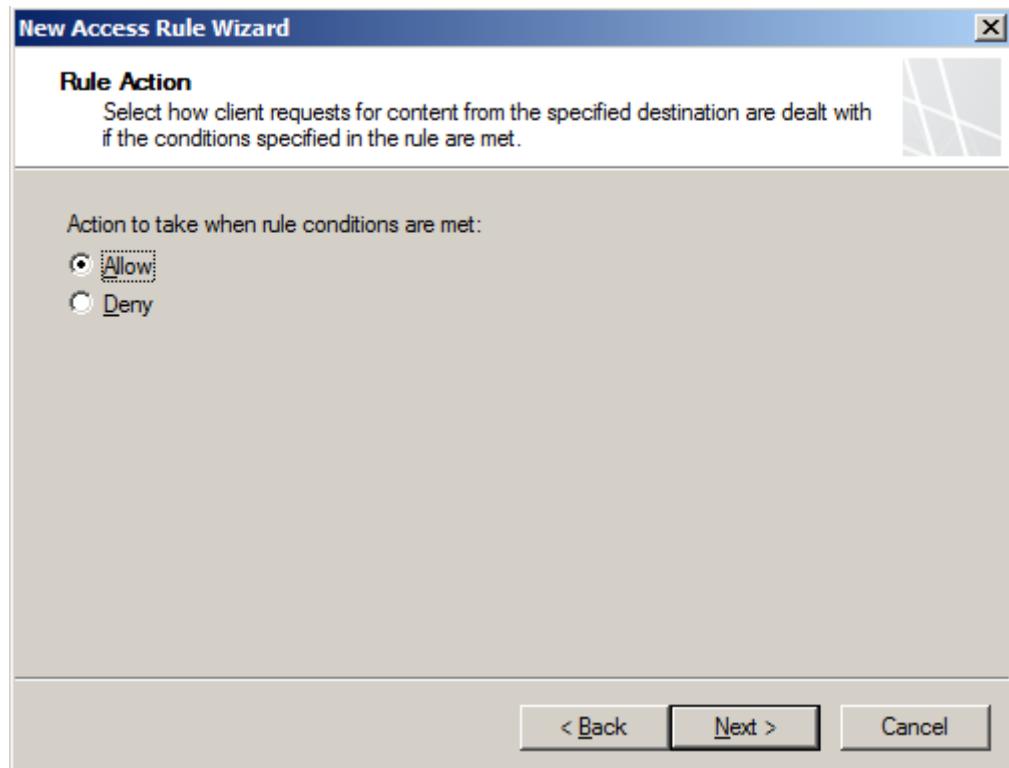
بداية لانشاء اي سياسية تتبع الخطوات التالية :



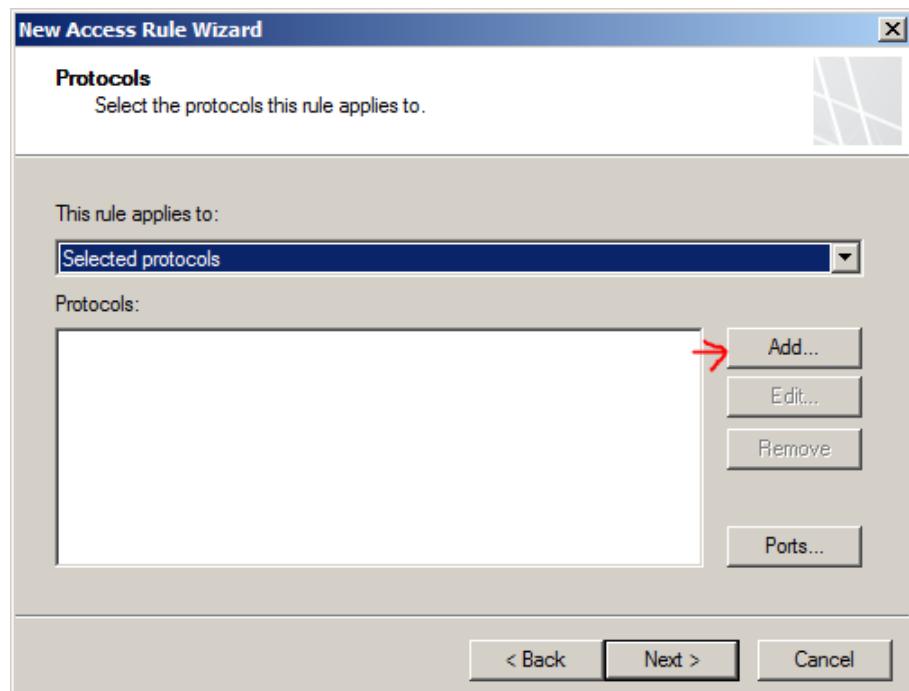
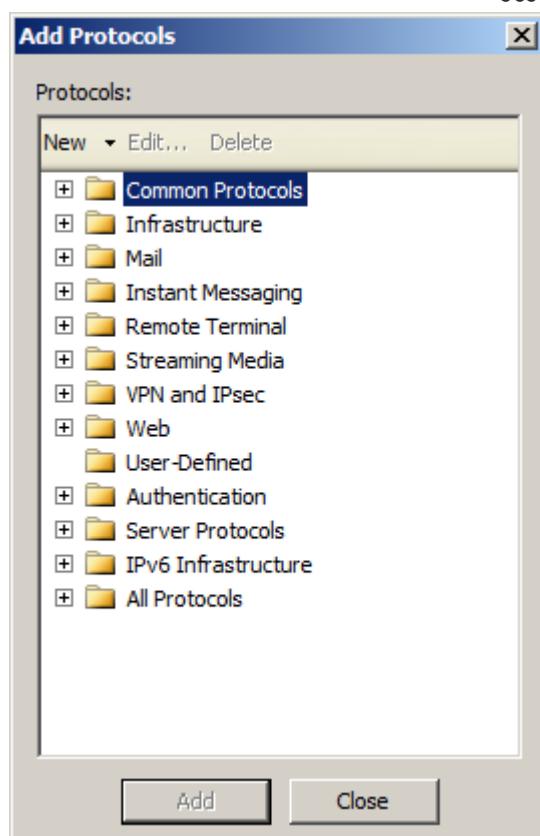
نختار اسم لل access rule التي نريد تطبيقها

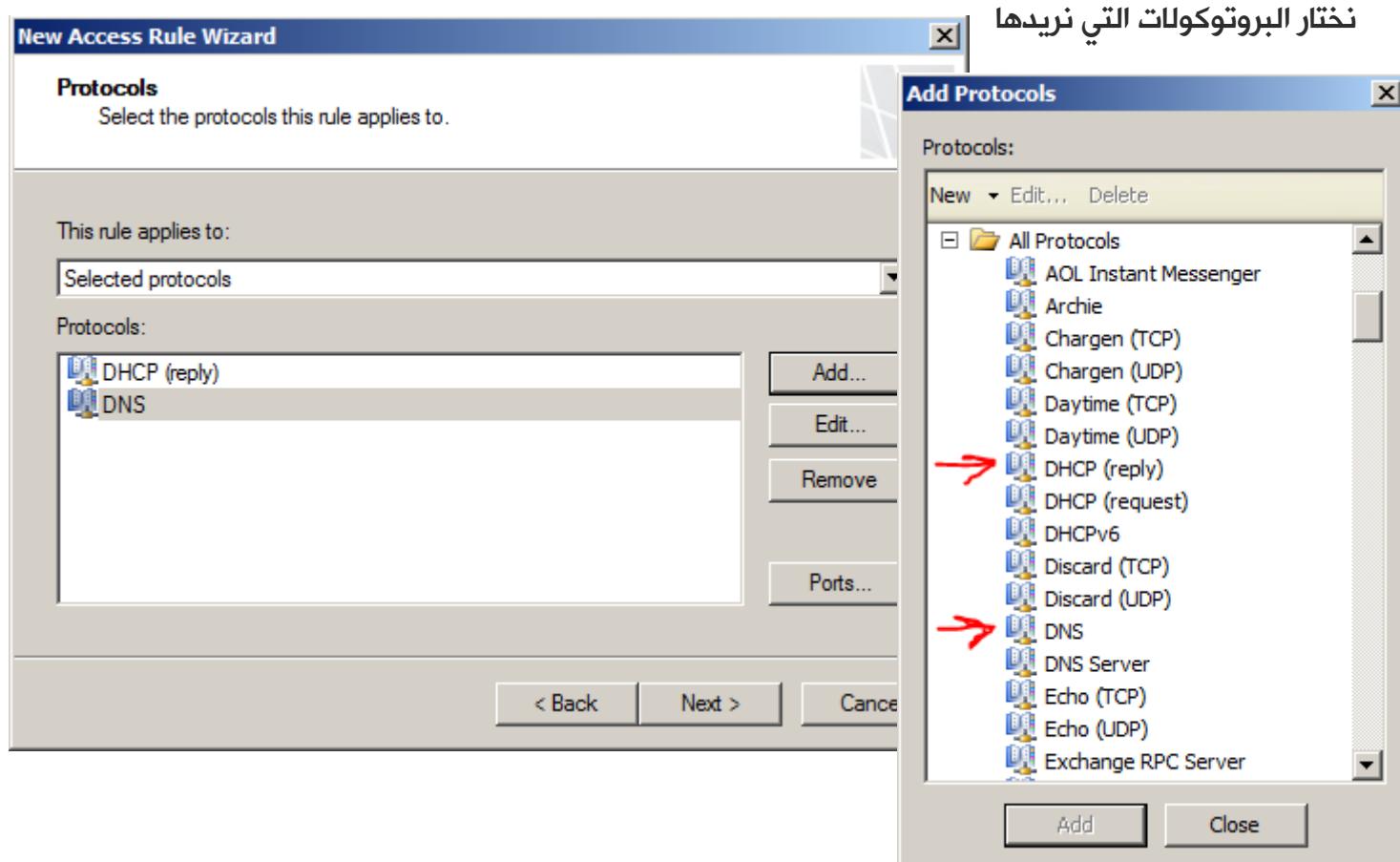


نختار نوع هذه السياسة اذا كانت بالسماح او الرفض

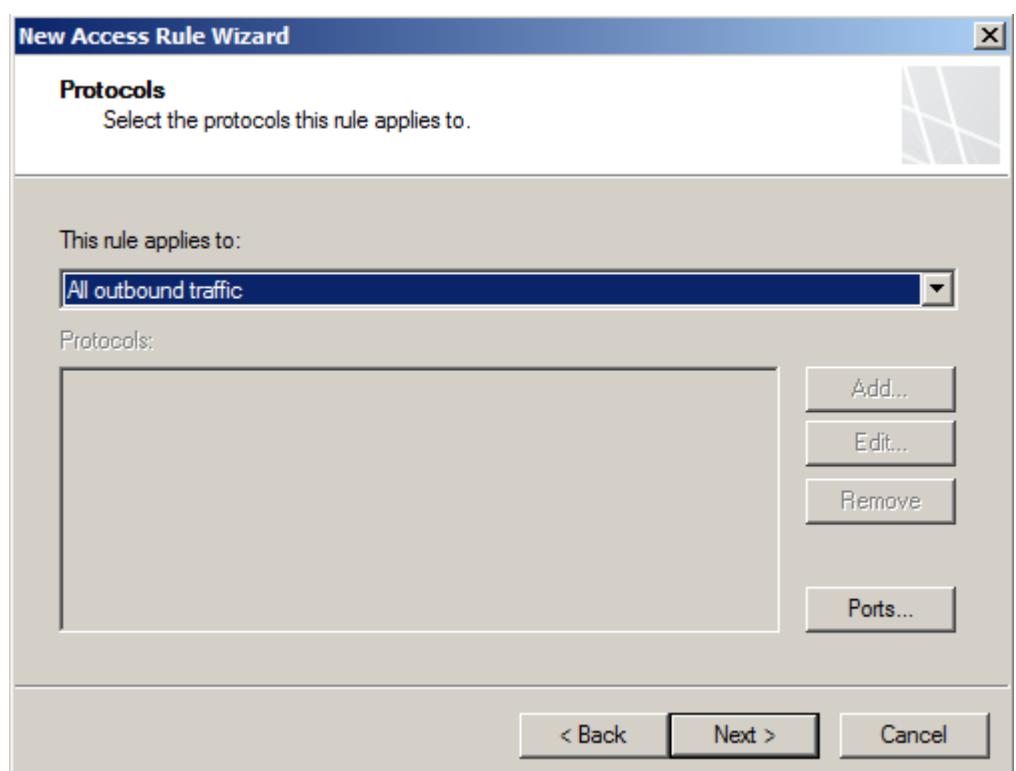


نختار نوع البروتوكول (البورت) المراد تطبيق السياسة عليه (منع او السماح بعموره)

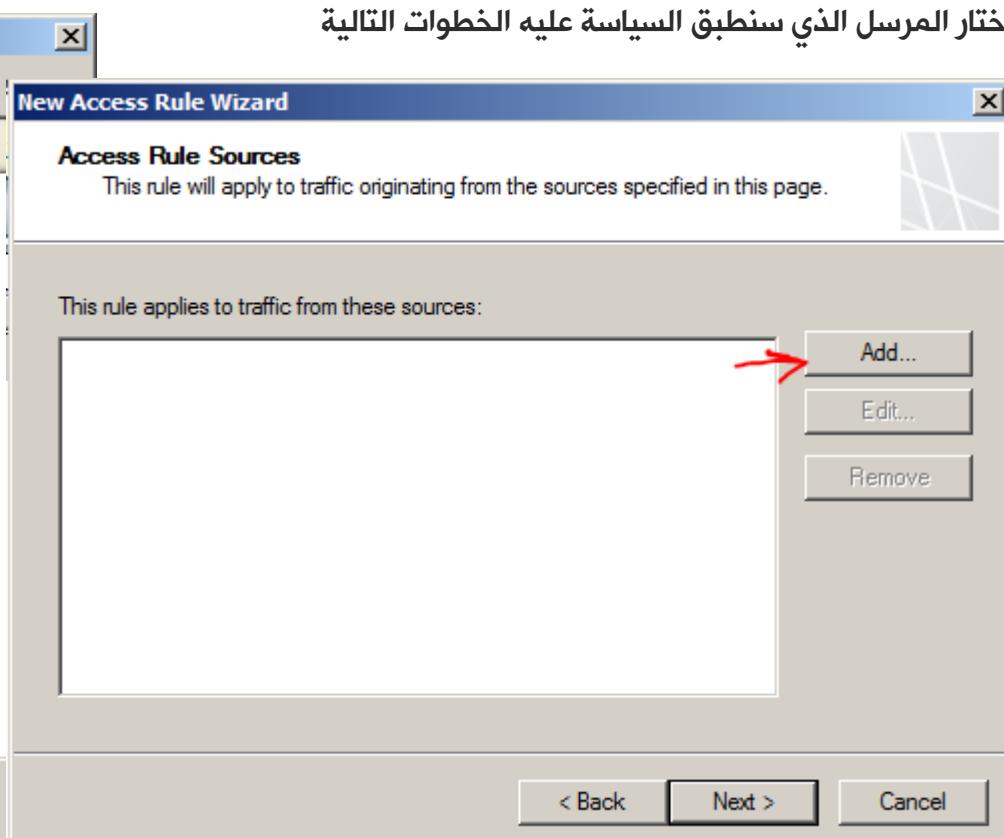
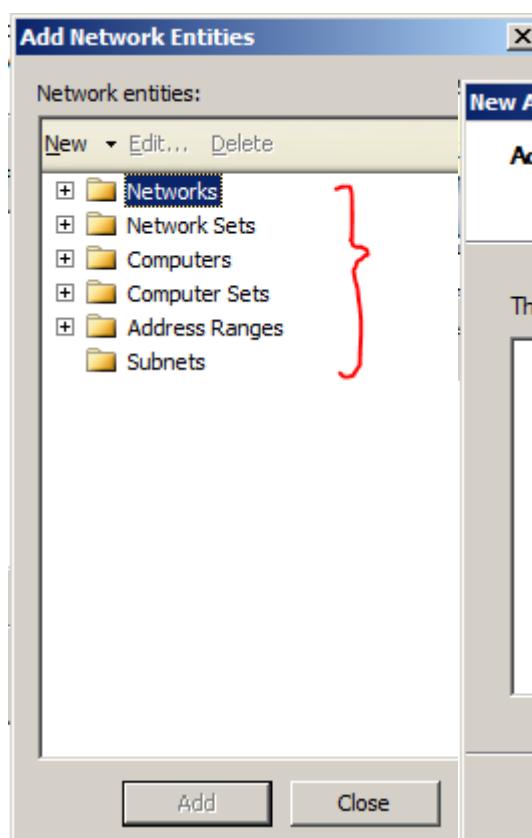
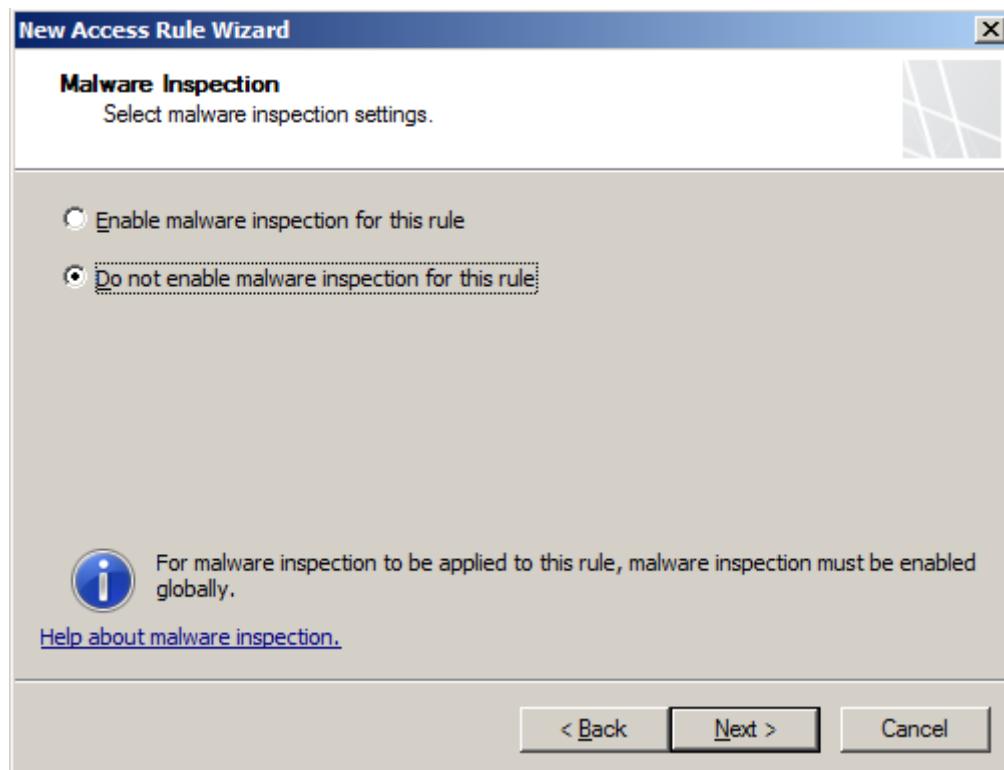




أو يمكننا اختيار جميع البروتوكولات (جميع المنافذ)



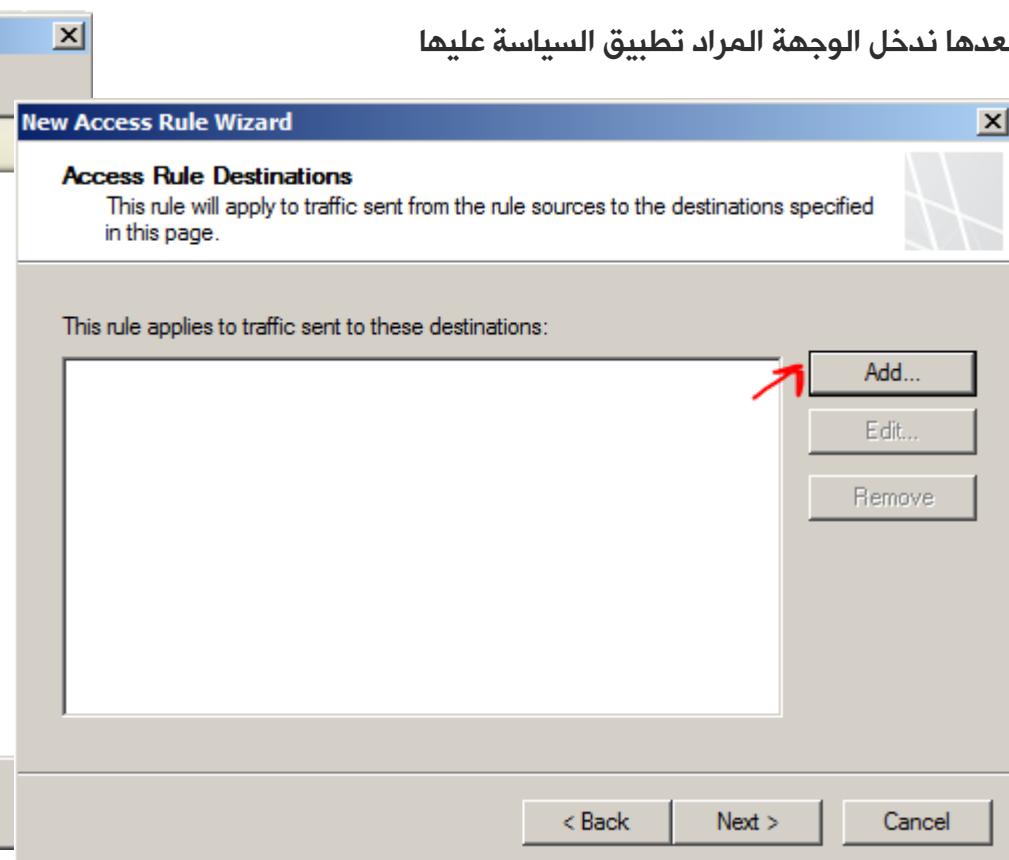
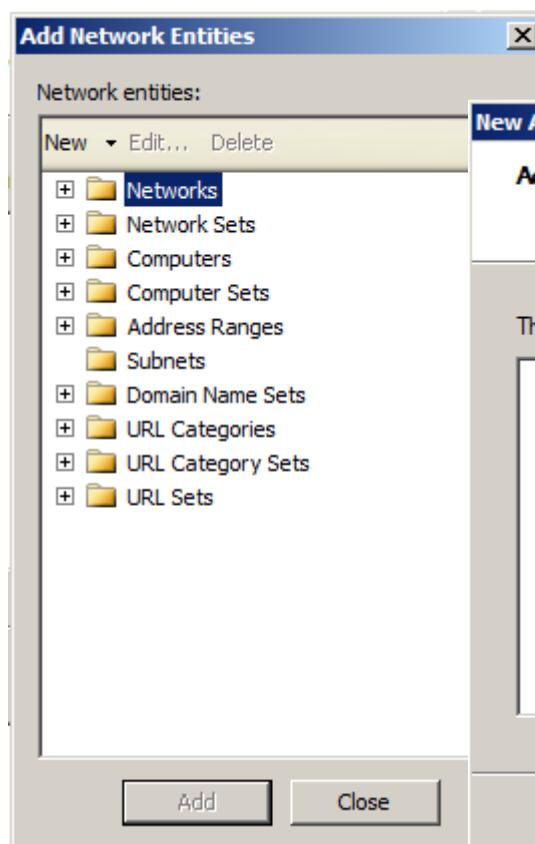
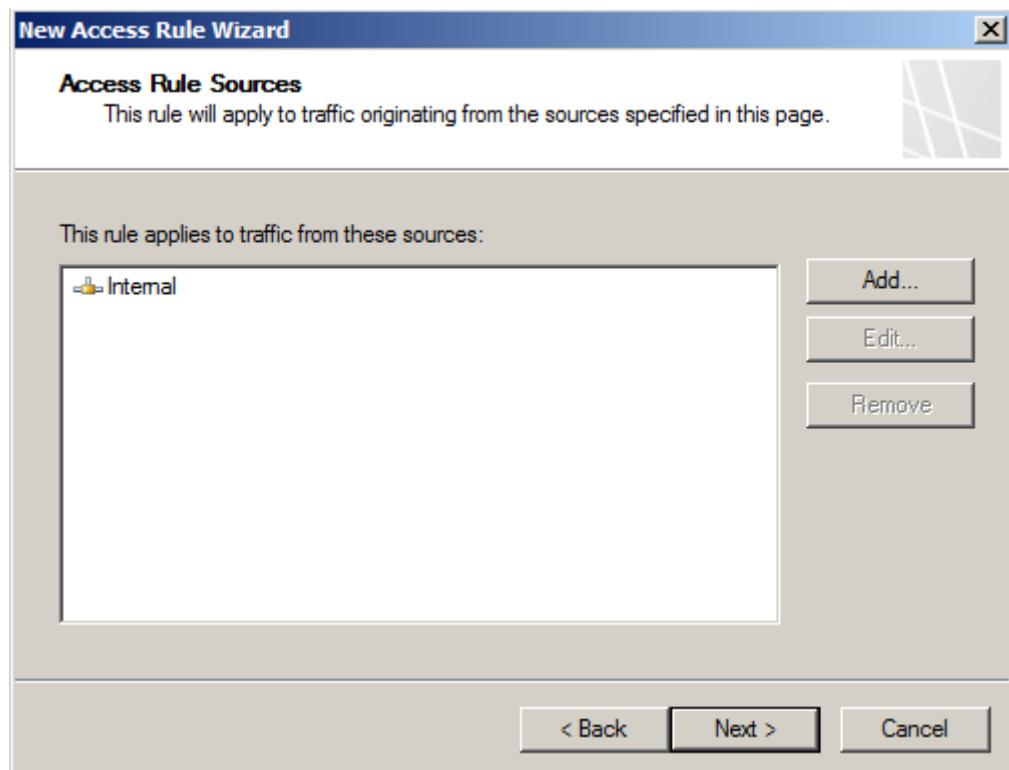
نختار في اذا ماكنا نريد التفتيش في هذه السياسة عن ال malware



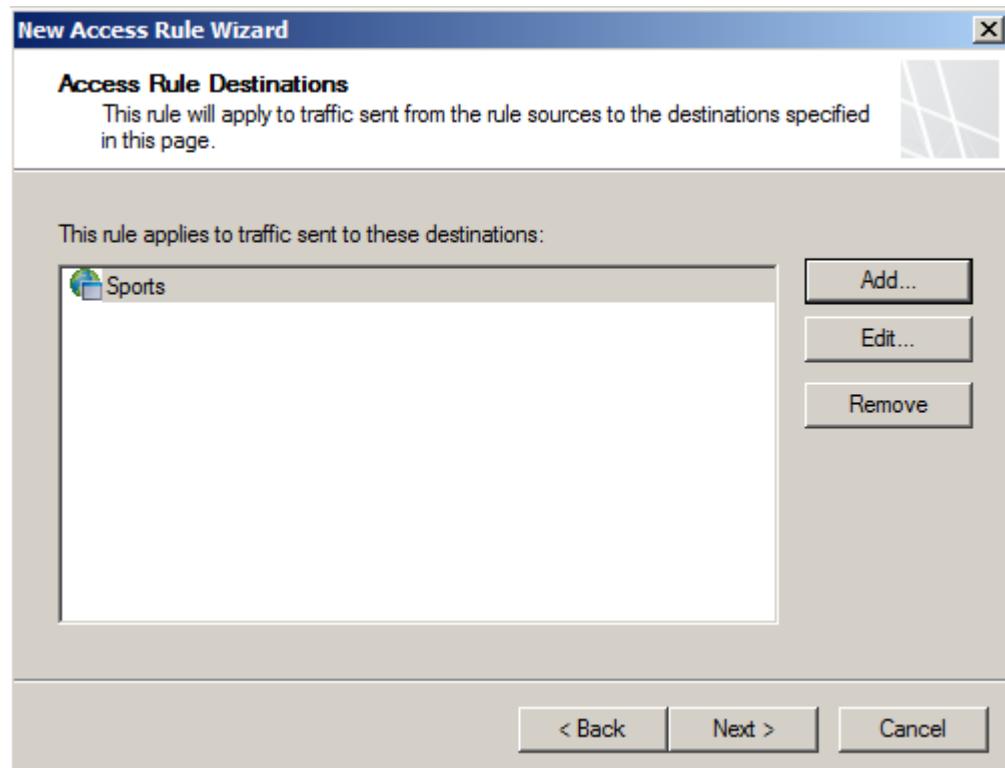
وهنا يمكننا اختيار المرسل بعده طرق اما عن طريق اضافة شبكة كاملة (-vpn-external-internal-localhost) او عن طريق (quarantine)

او عن طريق اضافة حاسب بعينه عن طريق عنوانه (او عدة حواسب)

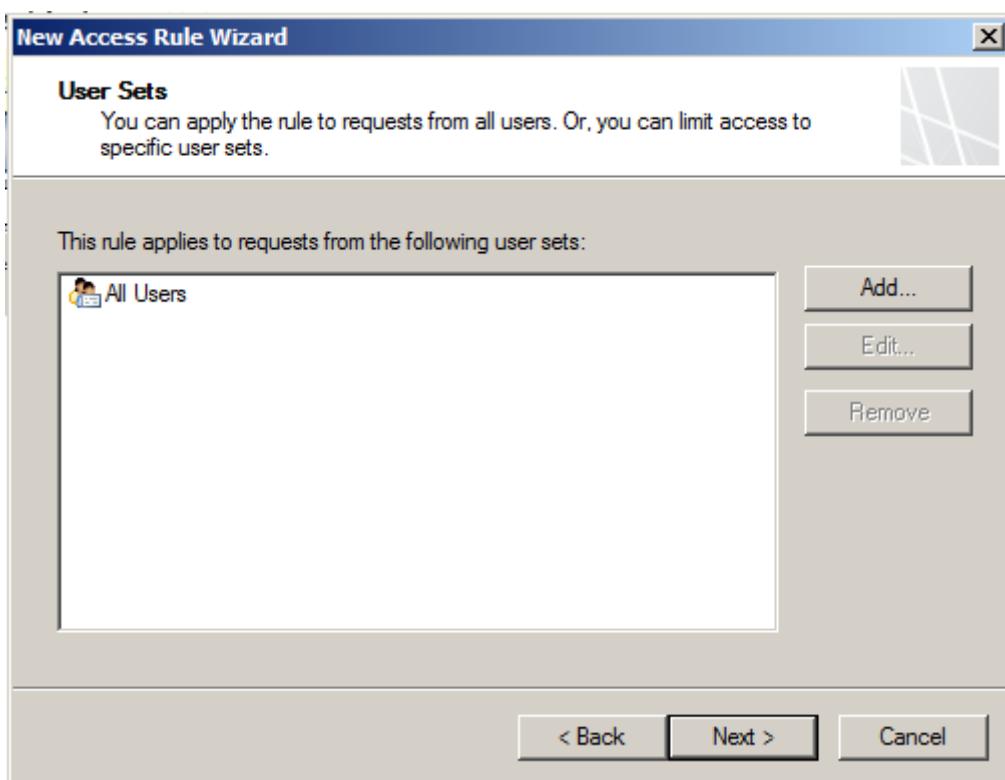
او عن طريق اضافة مسار من العنوانين المنطقية يتم ادخاله مسبقا ... الخ



بعدها ندخل الوجهة المراد تطبيق السياسة عليها
 هنا يمكننا الاضافة نفس طريقة اضافة المرسل يضاف عليها امكانية اضافة الوجهة عن طريق اضافة رابط موقع او عدة مواقع بحسب تصنيفها (categorys) بدلا من ادخالها رابط رابط (sport) فعلى فرض يمكننا اختيار موقع الرياضة جميعها حسب تصنيفها



ثم نقوم بإضافة حسابات المستخدمين الذين نريد أن يتم تطبيق السياسة عليهم





URL filtering (5)

وهي عملية فلترة الروابط القادمة من الانترنت

لتفعيل هذه الميزة على السيرفر من ادارة السيرفر

The screenshot shows the Microsoft Forefront Threat Management Gateway 2010 interface. On the left, there's a 'URL Filtering Settings' dialog box with tabs for General, Category Query, URL Category Override, and License Details. Under the General tab, there's a checkbox for 'Enable URL filtering' which is checked. Below it, there's a note about using Microsoft Reputation Service for categorization. At the bottom of the dialog are OK, Cancel, and Apply buttons.

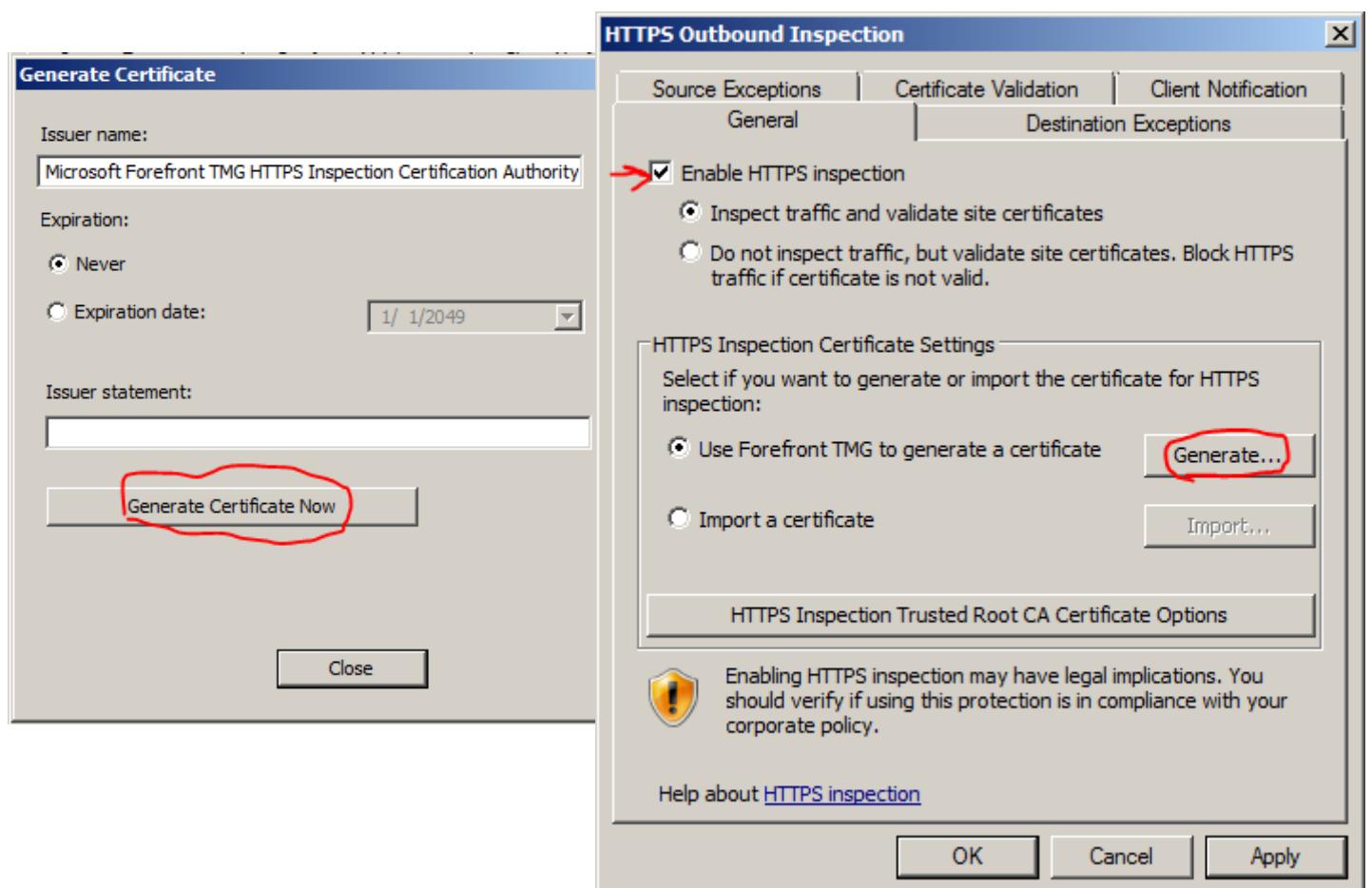
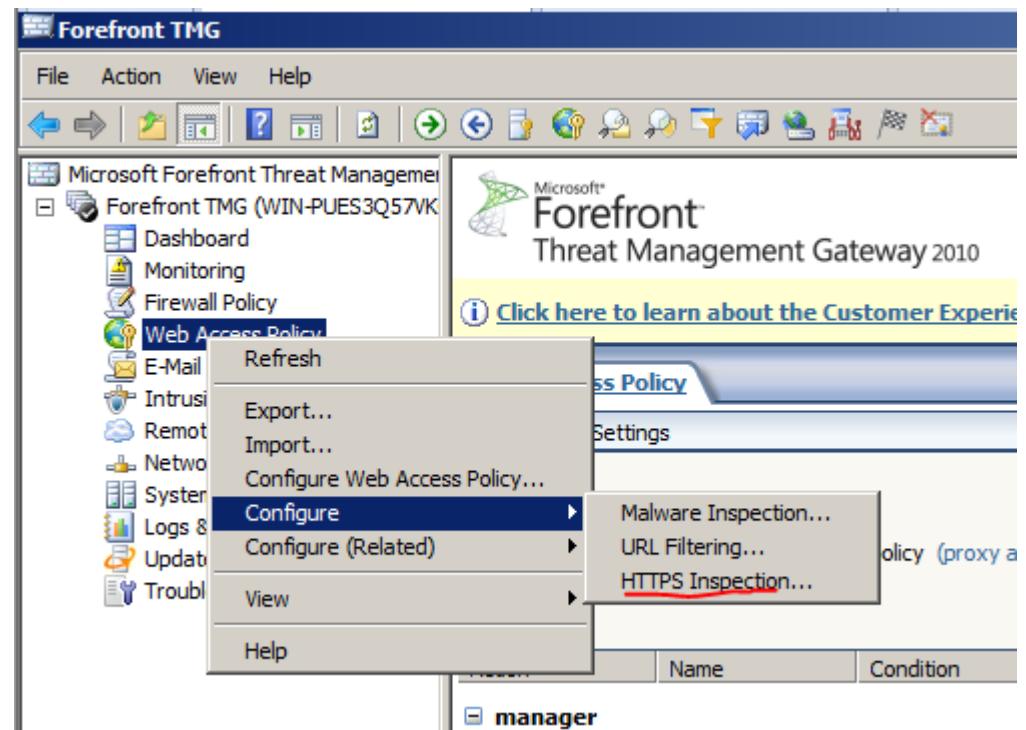
The main window shows a navigation pane with items like Threat Management, TMG (WIN-PUES3Q57VK), Dashboard, Monitoring, Firewall Policy, Web Access Policy, Mail Policy, Fusion Prevention, Remote Access, Working Environment, Reports & Analytics, Update Center, and Troubleshooting. A context menu is open over the 'Web Access Policy' item, with options like Refresh, Export..., Import..., Configure Web Access Policy..., Configure (Related)..., View, and Help. The 'Configure (Related)...' option has a submenu with Malware Inspection..., URL Filtering..., and HTTPS Inspection... highlighted in red.

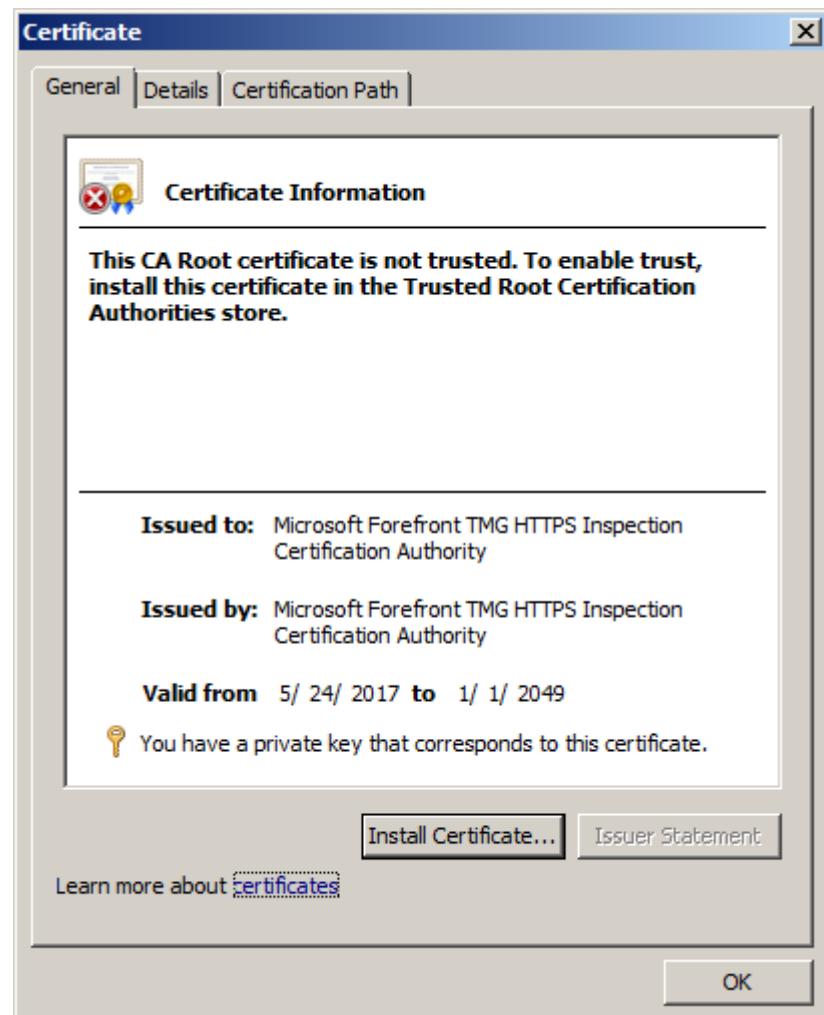


6) https incpections

وهي عملية تفتيش الروابط ال https والتتأكد من موظقيتها

للتفعيل:





anti spam (7)

وهي عملية حذف الاعلانات من الايميلات القادمة من الانترنت بالإضافة لامكانية حظر ايميلات معينة

**E-Mail Policy Wizard****Welcome to the E-Mail Policy Wizard**

This wizard helps you define SMTP routes between mail servers and Forefront TMG.

After defining these routes, you can configure Forefront TMG e-mail protection features to filter mail messages for potentially

E-Mail Policy Wizard**Internal Mail Server Configuration**

Specify your internal mail servers and the domains from which these servers accept mail messages (accepted authoritative domains).

Internal mail servers:

Computer Name	IP Address	Add...
mail	192.168.0.8	Remove

Accepted authoritative domains:**E-Mail Policy Wizard****Internal E-Mail Listener Configuration**

The internal e-mail listener accepts mail traffic from the networks and IP addresses specified here.

Networks:

Name	Selected IPs
<input type="checkbox"/> External	<All IP addresses>
<input checked="" type="checkbox"/> Internal	<All IP addresses>
<input type="checkbox"/> Local Host	<All IP addresses>
<input type="checkbox"/> Quarantined VPN Clients	<All IP addresses>
<input type="checkbox"/> VPN Clients	<All IP addresses>

Select Addresses...**< Back** **Next >** **Cancel**



E-Mail Policy Wizard

External E-Mail Listener Configuration

The external e-mail listener accepts inbound mail traffic from the networks and IP addresses specified here.

Networks:

Name	Selected IPs
<input checked="" type="checkbox"/> External	<All IP addresses>
<input type="checkbox"/> Internal	<All IP addresses>
<input type="checkbox"/> Local Host	
<input type="checkbox"/> Quarantine	
<input type="checkbox"/> VPN Client	

E-Mail Policy Wizard

E-Mail Policy Configuration

Forefront TMG leverages the mail protection provided by Microsoft Forefront Protection 2010 for Exchange Server and Exchange Edge Transport server role to provide an integrated mail protection policy

Enable spam filtering

FPES's antispam technology uses multiple filters to scan for unsolicited mail traffic.

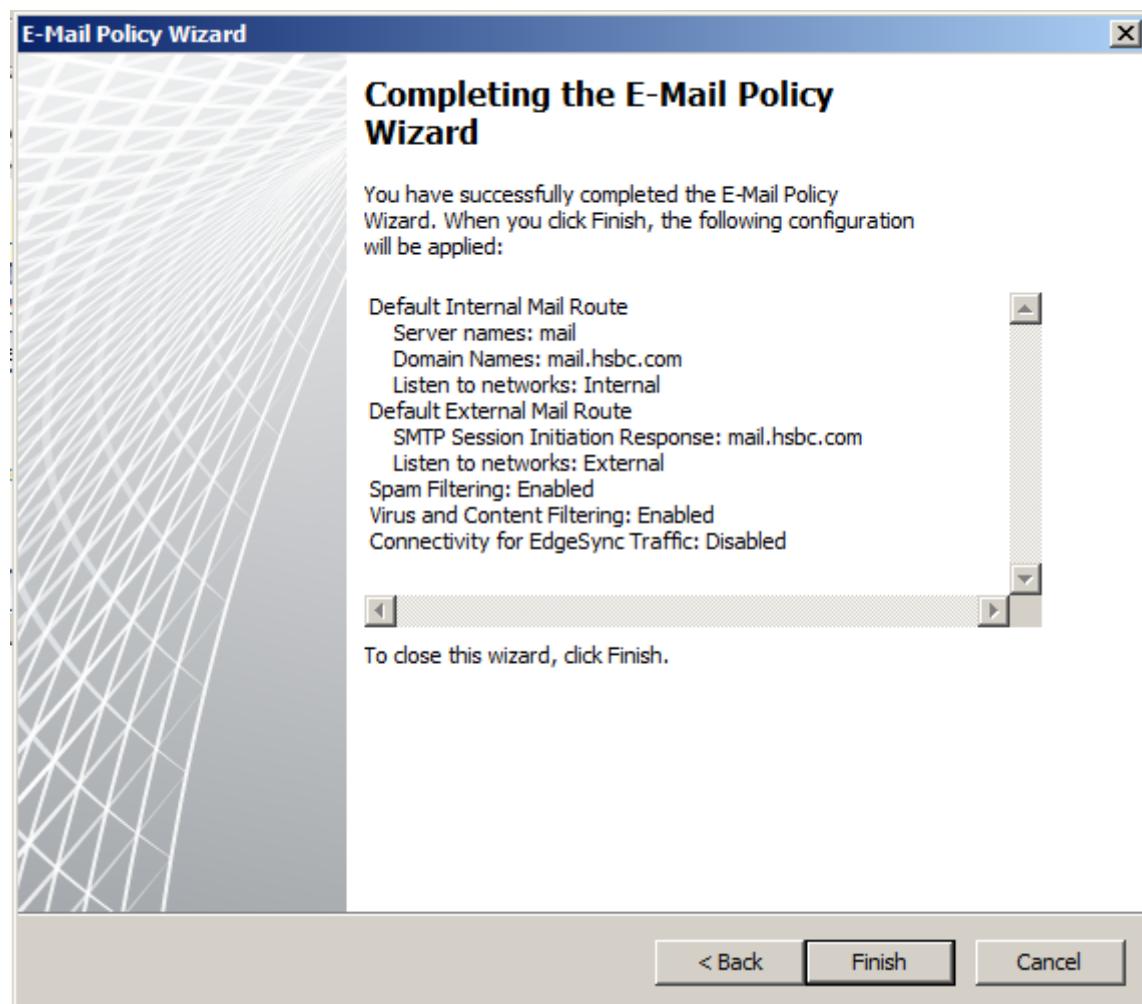
Enable virus and content filtering

Virus filters scan mail traffic for viruses and other malware in attached files. Content filters allow you to search for specific words within e-mail messages, and for attachments with specific names and types.

Enable connectivity for EdgeSync traffic

Subscribe to your Microsoft Exchange messaging organization for enhanced anti-spam features. After enabling connectivity, read about the next steps in [Configuring Edge Subscriptions](#).

[**< Back**](#) [**Next >**](#) [**Cancel**](#)



anti malware & virus (8)

Microsoft Forefront Threat Management Gateway 2010

[Click here to learn about the Customer Experience Improvement Program.](#)

Web Access Policy

Web Access Settings

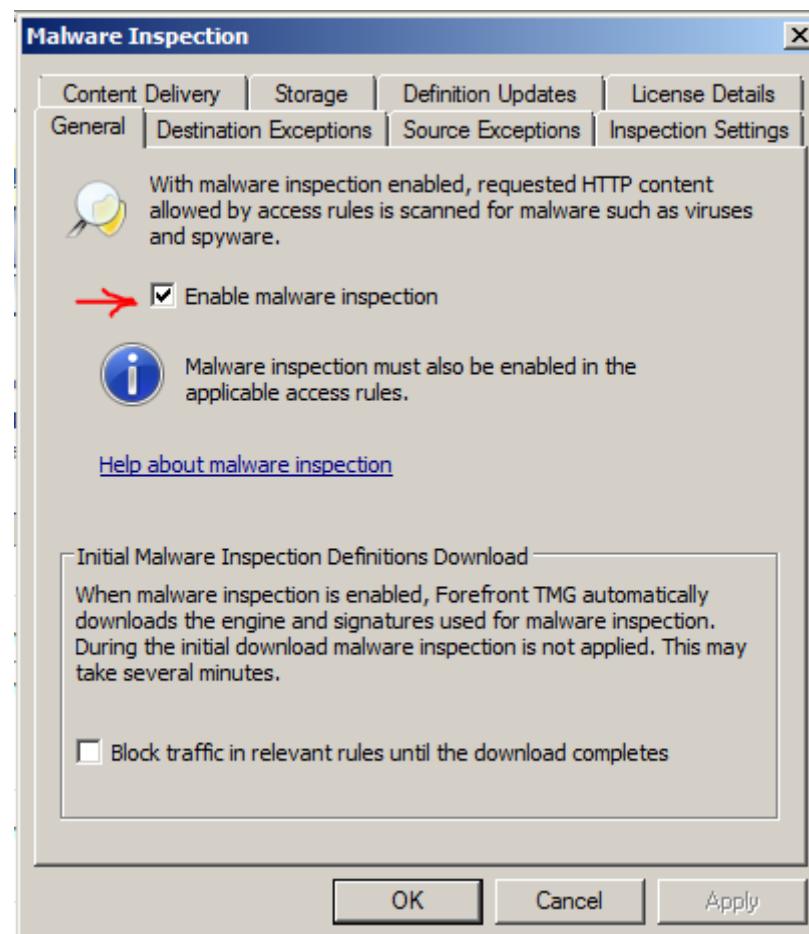
Action	Name	Condition	From	To
manager	Allow	All Users	manager	Internal
marketing	Allow	All Users	marketing	External Hacking/Com...
IT	Allow	All Users	IT	web server

Access Policy Tasks

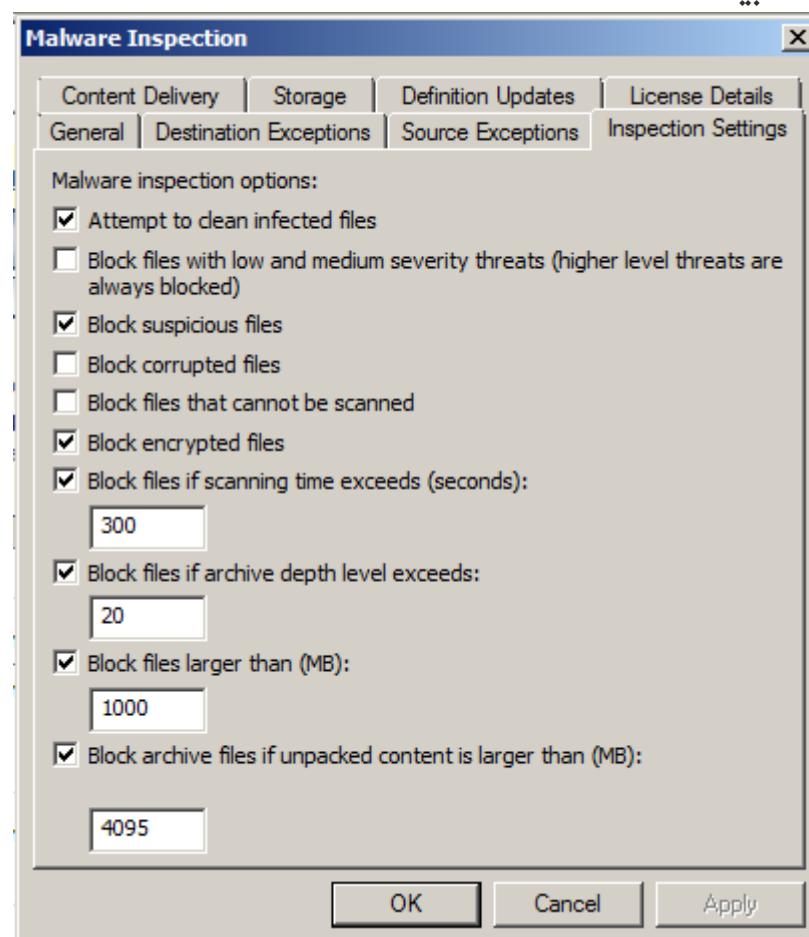
- Configure Web Access Policy
- Create Access Rule

Web Protection Tasks

- Configure HTTPS Inspection
- Configure Malware Inspection
- Configure URL Filtering
- Configure URL Category Overrides
- Query for URL Category



نختار السياسات التي نريد تطبيقها

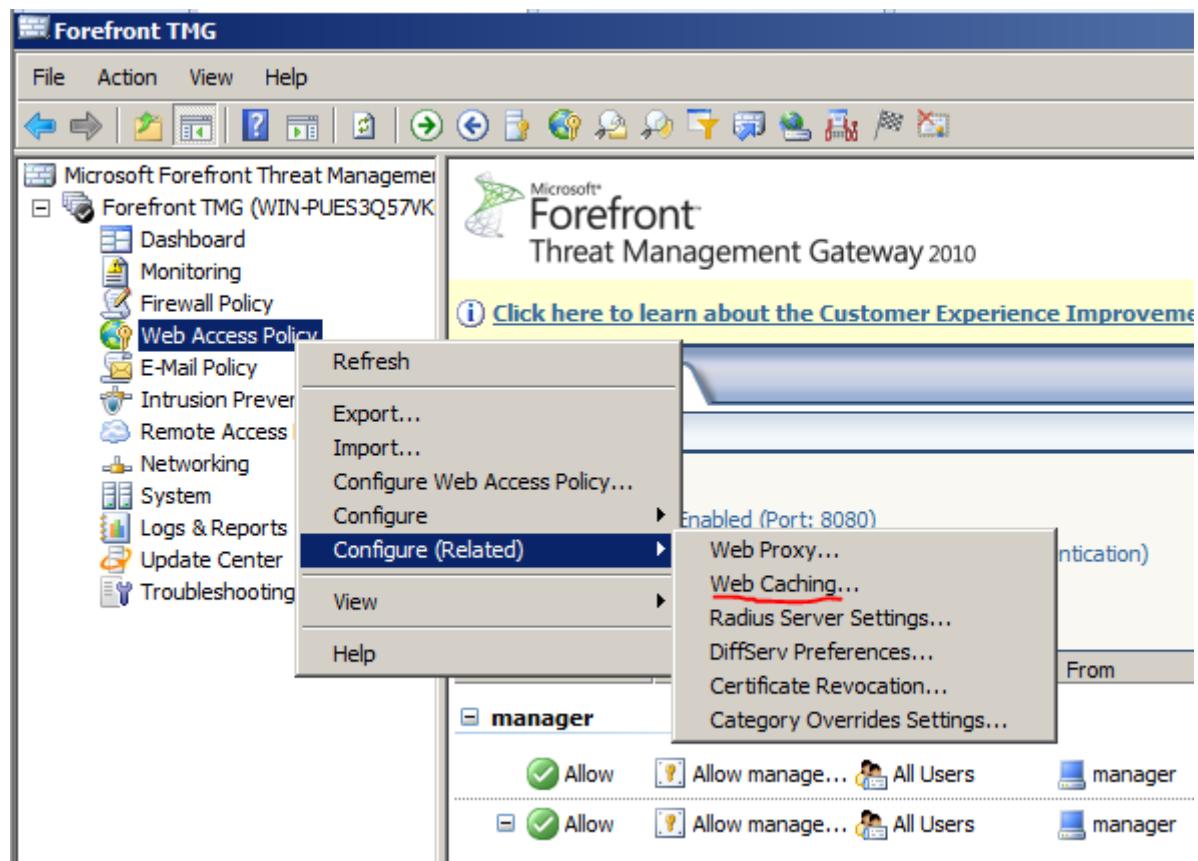




Web Caching (9)

يمكنا تسريع تصفح الانترنت عن طريق هذه الخدمة بحيث يخزن السيرفر الصفحات التي يتم الولوج اليها بحيث لو طلب مستخدم اخر موقعا سبق الولوج اليه فان السيرفر يقوم باحضاره من مخزنه بدل الذهاب الى الانترنت مما يوفر الوقت والحمل على الشبكة

يتم تطبيق الخدمة عن طريق الخطوات التالية :



بداية نقوم باختيار القرص الذي سوف نخزن عليه والحجم الذي سوف نخزن فيه

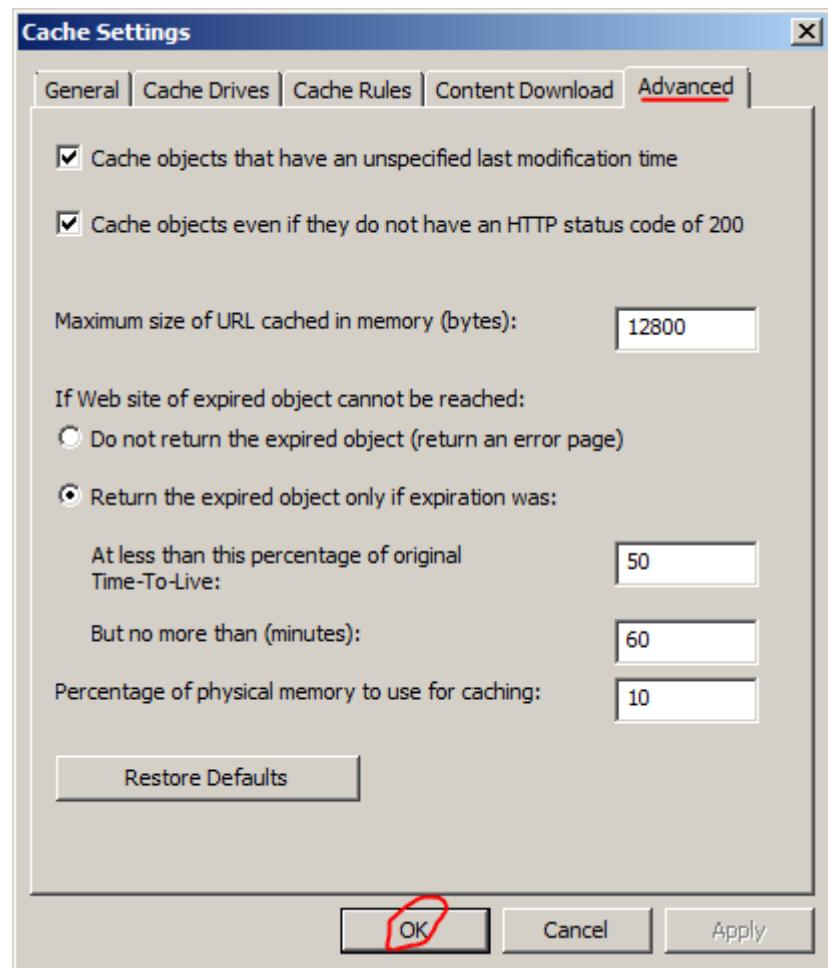
The image contains two side-by-side screenshots of the 'Cache Settings' dialog box from the Forefront TMG interface.

Left Screenshot (Cache Rules Tab):

- Tab: Cache Rules
- Table Headers: O., Name, Description, To
- Items:
 - cache rule (External)
 - Microsoft Update... (Microsoft Update...)
 - Default rule (All Networks (an...))
- Buttons: New..., Edit..., Delete, OK, Cancel, Apply

Right Screenshot (Cache Drives Tab):

- Tab: Cache Drives
- Table Headers: Cache Size (MB), Total Disk Size (MB), Free Space (MB)
- Items:
 - (WIN-PUES3Q57VKO...) 20985 1300
- Buttons: Help about configuring cache drives, Configure..., OK, Cancel, Apply



بعد الضغط على ok يكون السيرفر جاهز لعملية ال web caching

NAT

وهي الخدمة التي تمكنت من الخروج الى الانترنت بالعنوان المحلي لجهازي وذلك بتحويله الى عنوان محلي عند خروجه الى الانترنت وذلك باستخدام الراوتر الذي سوف اطبق عليه الخدمة وذلك عن طريق التعليمات التالية :

```
Router>en
Router#conf t
```

.Enter configuration commands, one per line. End with CNTL/Z

نطبق السياسة التي من خلالها نسمح للأشخاص المخولين بالولوج الى الانترنت بتطبيق الخدمة عليهم:

```
Router(config)#ip access-list extended NATACL
Router(config-ext-nacl)#permit ip 192.168.0.0 0.0.255.255 any
Router(config-ext-nacl)#exit
```

نختار في اذا ما كنا نريد تطبيق الخدمة للحزم الخارجية او الداخلة للتجهيزه ثم نختار السياسة التي نريد تطبيقها (التي سبق وعرفناها) وبعد ذلك نختار العنفذ الذي نريد تطبيقها عليه ثم نختار نوع الخدمة (هنا استخدمت NAT overload)

```
Router(config)#ip nat inside source list NATACL interface fastEthernet 0/0 overload
```



Management Security

: 1) قفل منفذ ال consle

```
Router>en
```

```
Router#conf t
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Router(config)#line console 0
```

```
Router(config-line)#password cisco@123
```

```
Router(config-line)#login
```

```
Router(config-line)#exit
```

: 2) قفل منفذ ال AUX

```
Router(config)#line aux 0
```

```
Router(config-line)#password cisco@123
```

```
Router(config-line)#login
```

```
Router(config-line)#exit
```

: 3) قفل منفذ ال VTY

```
Router(config)#line vty 0 15
```

```
Router(config-line)#password cisco@123
```

```
Router(config-line)#login
```

```
Router(config-line)#exit
```

ويمكننا ايضاً قفل اي مستوى privilege نريد بكلمة سر :

```
Router(config)#enable secret password level 15 pass@15
```

```
Router(config)#enable secret password level 7 pass@7
```

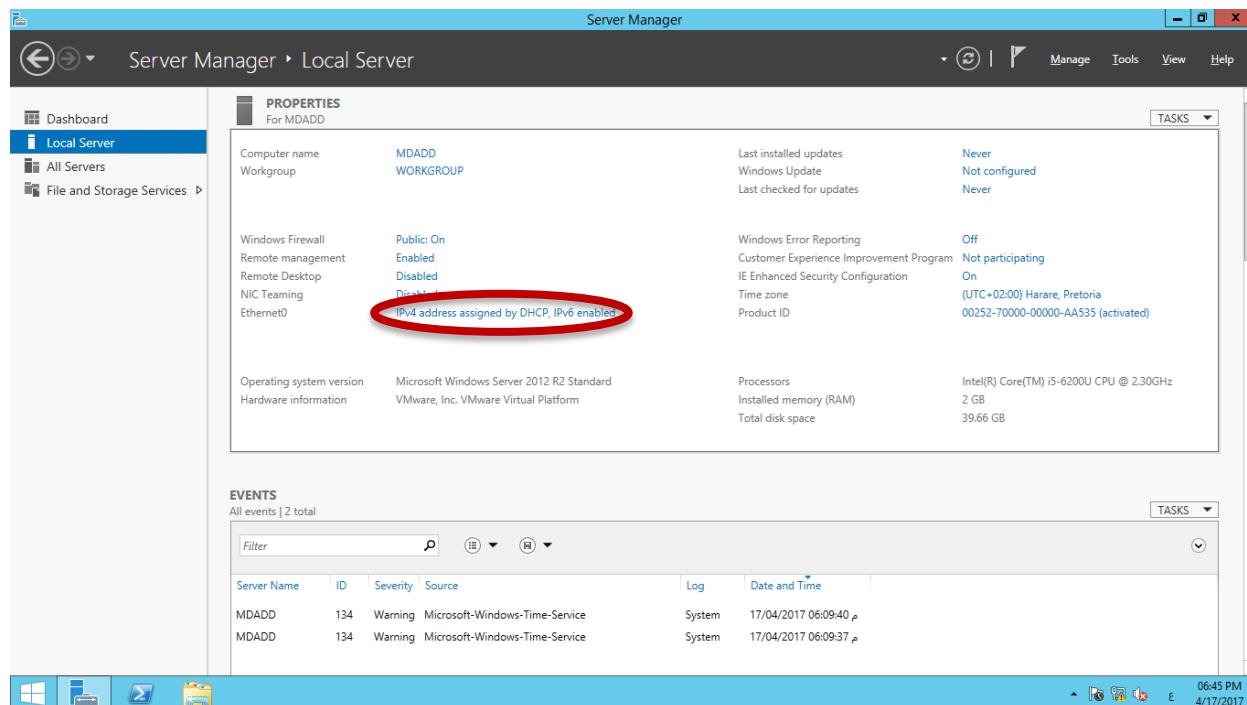
```
Router(config)#enable secret password level 3 pass@3
```



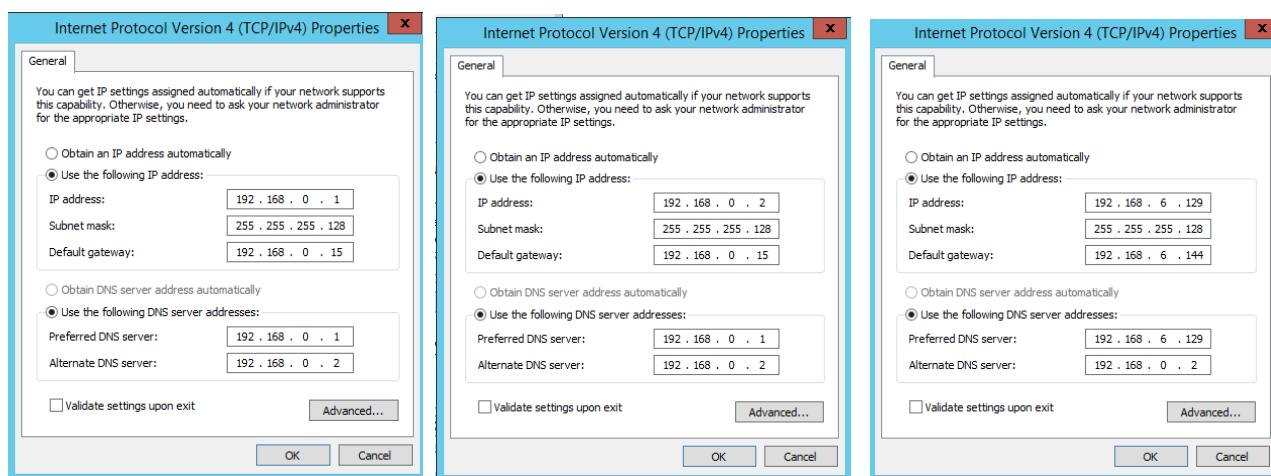
Network Administration

DHCP, DNS, ADDS الخاصة بـ Binaries

أولاً يجب وضع Static IP للأجهزة التي سيتم تنزيل الملفات عليها ويمكن عمل ذلك من Local Server → IPv4 address assigned by DHCP,IPv6 Enabled

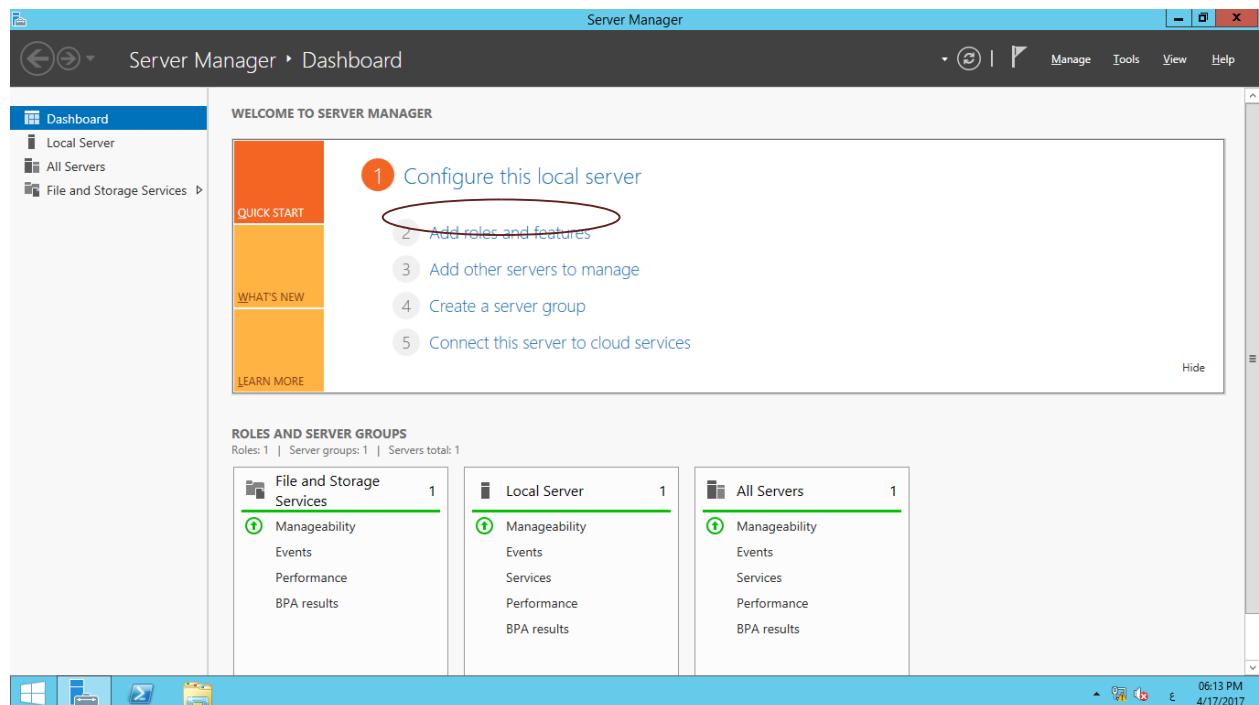


فيتم فتح الـ Network Connections الموجودة على الجهاز ومنها نقوم بالضغط مرتين على الـ Adapter Use Properties → Internet Protocol Version 4 (TCP/IPv4) ونقوم بتحديد the following IP address.



الآن سنقوم بتنصيب ملفات الـ Binaries الخاصة بـ DHCP, DNS, ADDS

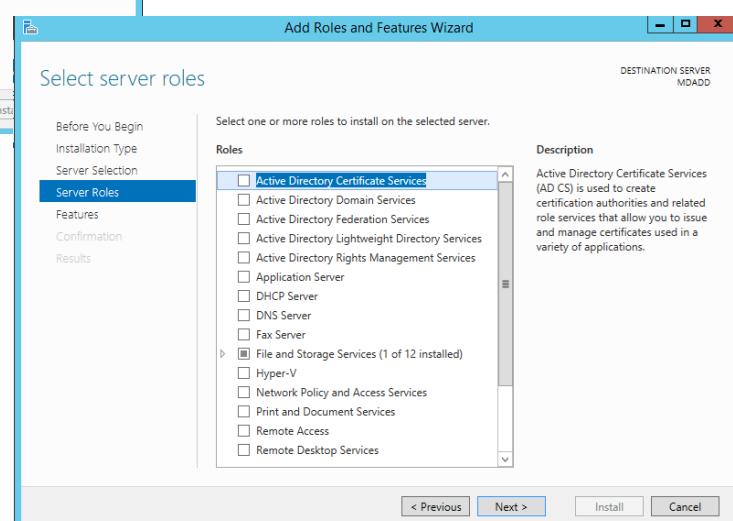
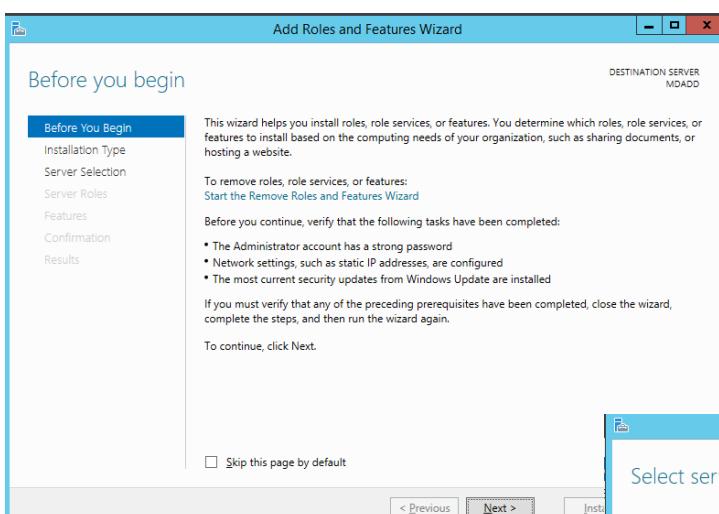
Add Roles Or Features نختار Server Manager من

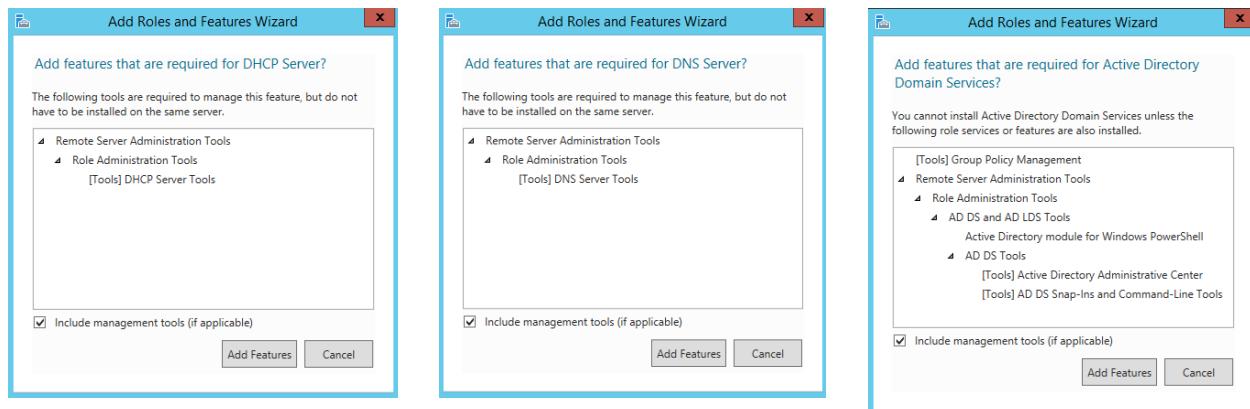


نقوم بالضغط على Next ثم نختار Role-Based or Feature-based installation

بعدها نختار المراد تنزيله عليه

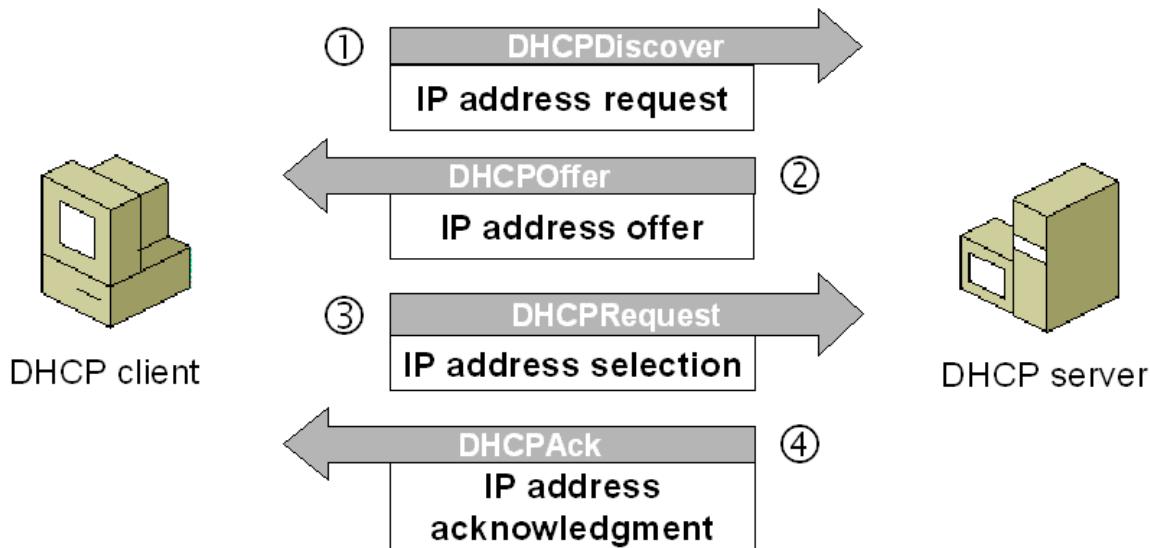
وبعدها نختار المراد تثبيتها وهي DHCP، Active Directory Domain Services و DNS





ثم نقوم بالضغط على زر Next ونتابع تعليمات التنزيل.

DHCP



DHCP Scopes

سنقوم بإضافة الـ DHCP Scopes والـ Exclusion Range والـ Options لكل Scope الخاصة بها عن طريق الـ PowerShell وذلك باستخدام Import-Csv

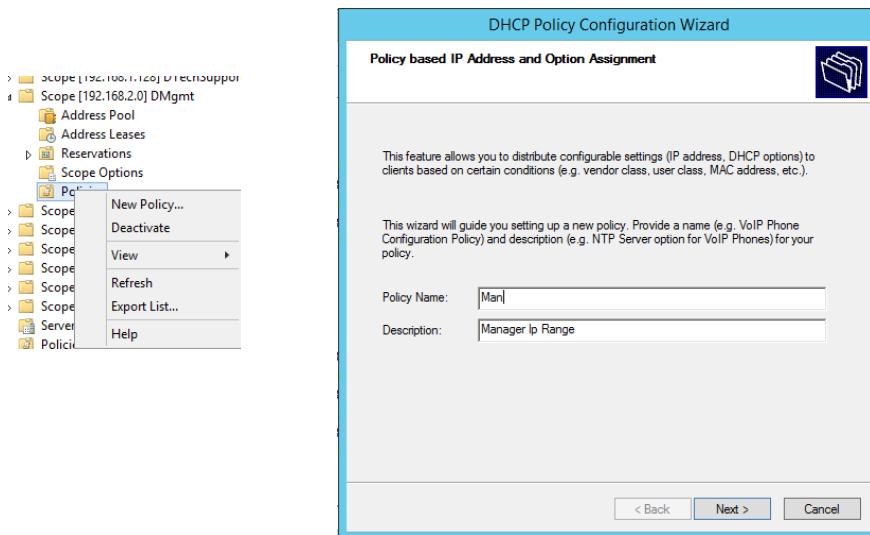
The image shows three separate windows of Windows PowerShell running under 'Administrator' mode. Each window displays the command being run and its output.

- Top Window:** Runs `PS C:\Users\Administrator\Desktop\Csv> Import-Csv .\DRanges.csv | Add-DhcpServerv4Scope`
- Middle Window:** Runs `PS C:\Users\Administrator\Desktop\Csv> Import-Csv .\DExcl.csv | Add-DhcpServerv4ExclusionRange`
- Bottom Window:** Runs `PS C:\Users\Administrator\Desktop\Csv> import-csv .\DScopOpt.csv | Set-DhcpServerv4OptionValue`



DHCP Policies

من DHCP Manager نختار الـ Scope ثم نضغط على مجلد Policies ونختار New

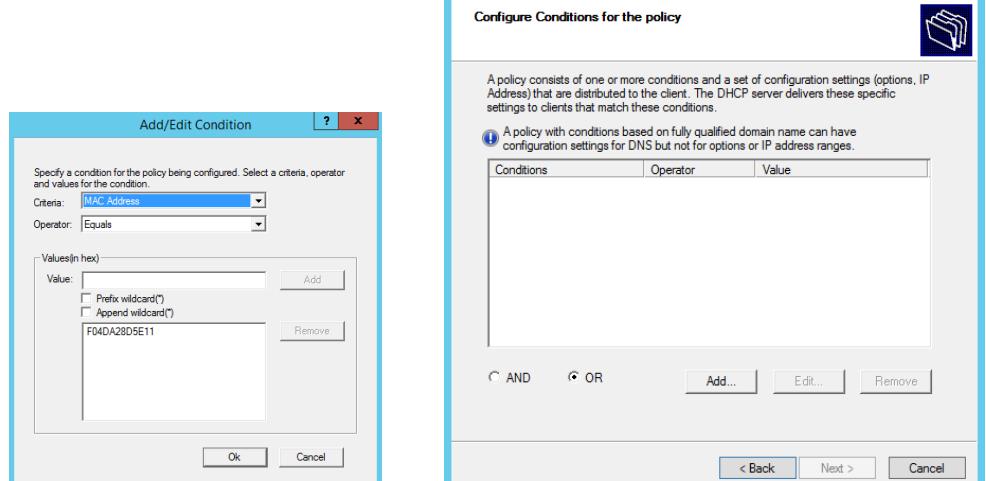


ندخل اسم الـ Policy وشرح ثم نضغط Next

نضغط على Add لنضيف الشرط المراد تحقيقه كي يأخذ الجهاز عنوان IP من المجال المحدد حيث سيكون هذا الشرط هو الـ Mac Address

المدير ثم نضغط على Ok وثم

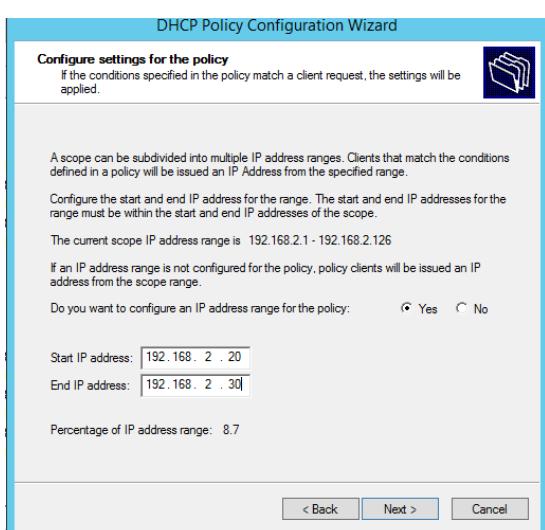
Next ثم نضغط على Ok وثم



نضيف مجال من الـ Scope كي يوزع منه العناوين الخاصة لهذه الـ

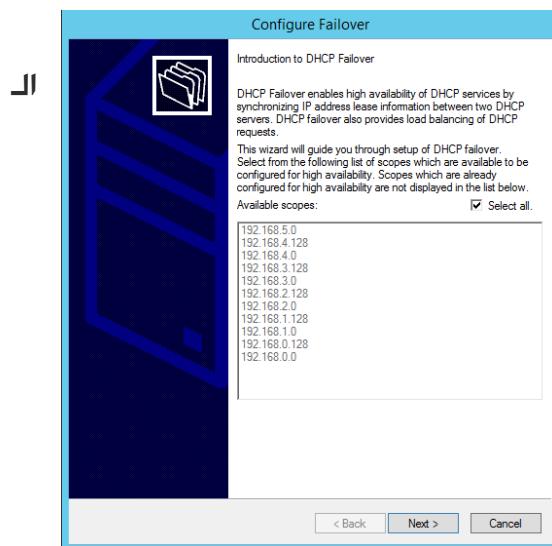
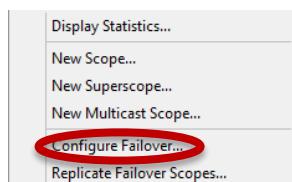
Policy ثم نضغط على Next

نضيف أي معلومات إضافية نريد أن يوزعها الـ DHCP Server لهذا الجزء من الـ Scope ونضغط Finish ثم Next



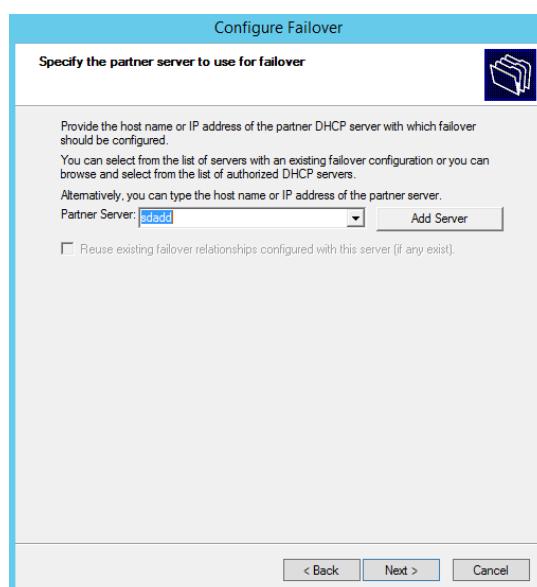
DHCP Failover

1- من DHCP manager نضغط بالزر اليمين على IPv4 ونختار Configure Failover

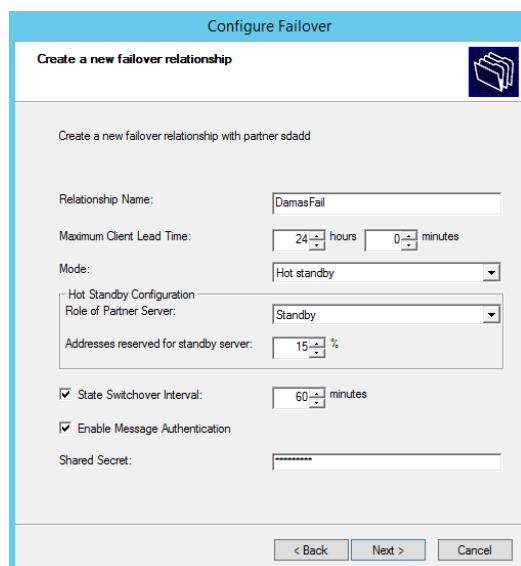


2- نختار Scopes التي نريد أن يتم عمل لها إلى Replicate Scopes الاحتيطي ثم نضغط على Next Server

3- نختار Server الاحتياطي الذي تم تثبيت ملفات DHCP الخاصة بـ Binaries ونضغط على Next



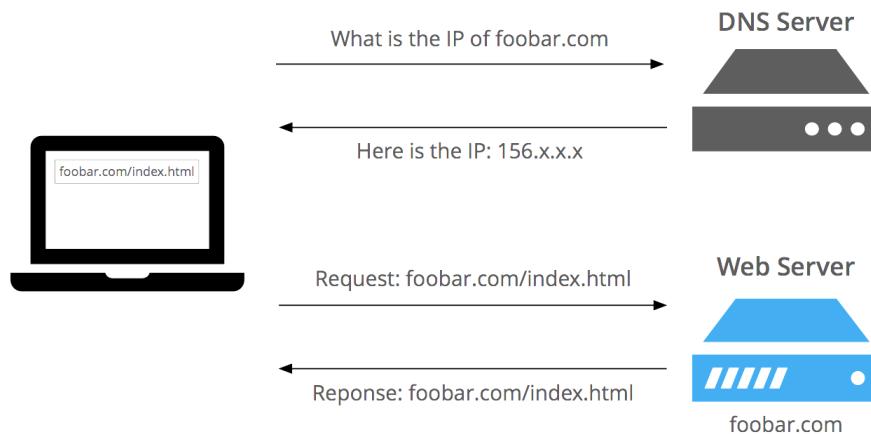
4- نقوم بتحديد نمط العلاقة بين Servers وتحديد



خياراتها



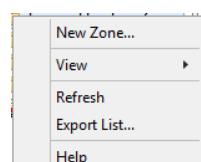
DNS



DNS Zone Creation

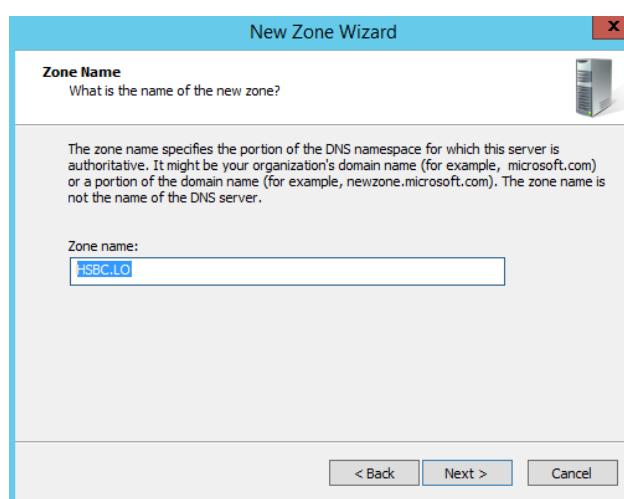
Server Manager → Tools → DNS -1

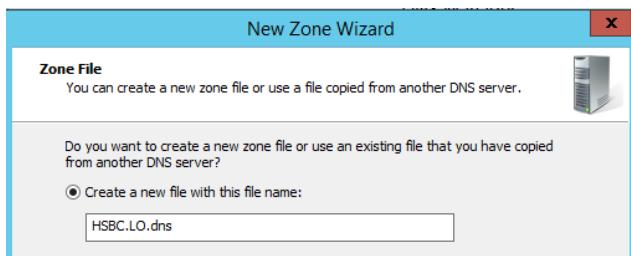
2- نضغط بالزر اليمين على New Zone فتظهر لنا نافذة Forward Lookup Zones ثم نضغط



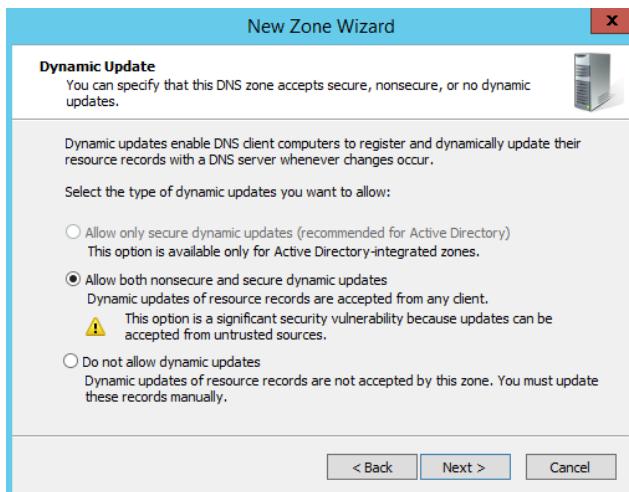
على وختار Next علی

3- ندخل اسم الـ Zone اعتماده ونضغط على Next





4- في الصفحة التالية نختار إما أن نحفظ إلـ DNS Records في ملف موجود مسبقاً أو أن ننشأ ملف جديد وسنختار إنشاء ملف جديد ونضغط على Next



5- خاصية Dynamic Update التي تمكنا من تحديث إلـ Records ديناميكياً عندما يتم تغيير إلـ ip الخاص بجهاز ما وسنختار Allow both nonsecure and secure dynamic updates كي نستطيع تحويل إلـ Zone إلى Active Directory integrated zone Domain Controller إلى Server

6- نضغط على Finish ثم Next

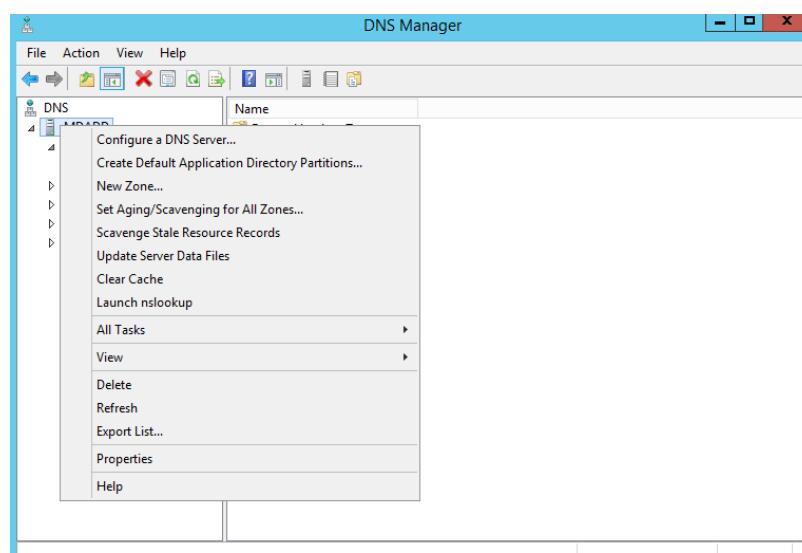
Adding resource records

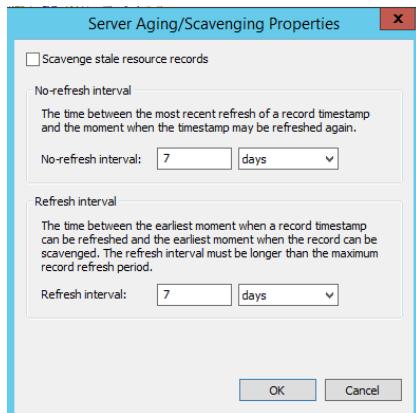
وسيتم ذلك عن طريق امر PowerShell التالي:

```
Import-csv .\servers | Add-DnsServerResourceRecordA
```

Aging and Scavenging

1- من Server Manager → Tools → Dns نضغط بالزر اليمين على اسم إلـ Server ونختار Set Aging/Scavenging for All Zones



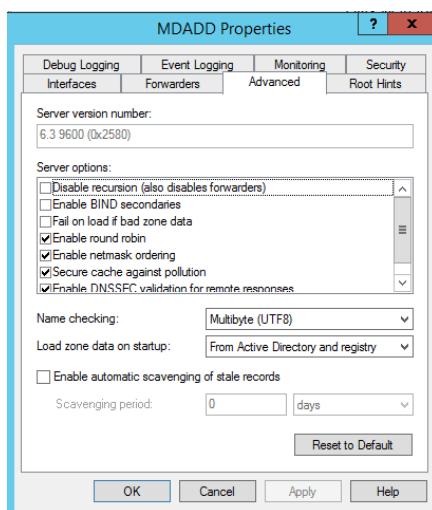


2- نعلم خيار ثم نضغط Scavenge Stale resource records Ok

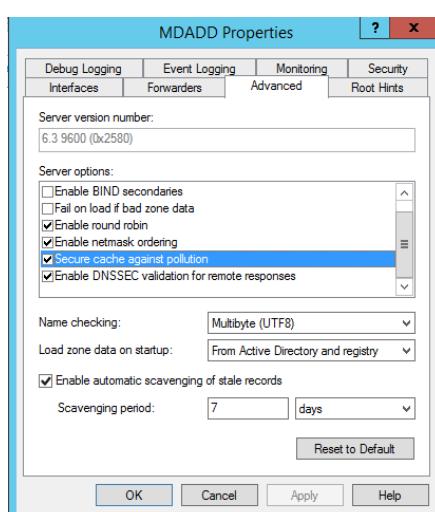
3- نعلم خيار ثم نضغط Apply these setting to existing Active Directory integrated Zones Ok

4- ثم نضغط بالزر اليمين على الـ Server ونختار Properties ومنها نتجه إلى تبويبه Advanced ونعلم خيار

Enable Automatic Scavenging of stale records Ok



DNS Cache Locking



تكون مفعولة افتراضياً وللتتأكد من ذلك نضغط على الـ Server بالزر اليمين

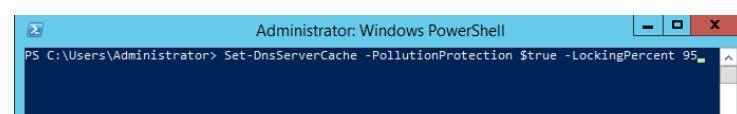
من الـ DNS Manager Properties ثم نفتح تبويبه Advanced فنجد أن خاصية Secure cache against pollution مفعولة فنضغط على OK

ولتعديل نسبة قفل الـ Record يقوم بفتح الـ PowerShell وإدخال

Set-DnsServerCache -PollutionProtection \$true الأمر –

وهكذا تكون قد وتوضع قيمة النسبة مكان الـ # حيث

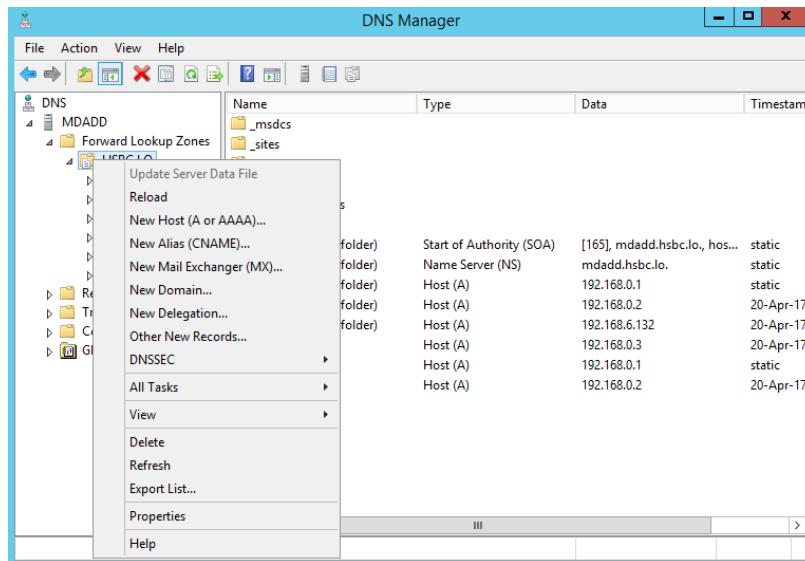
تكون افتراضياً 100٪.





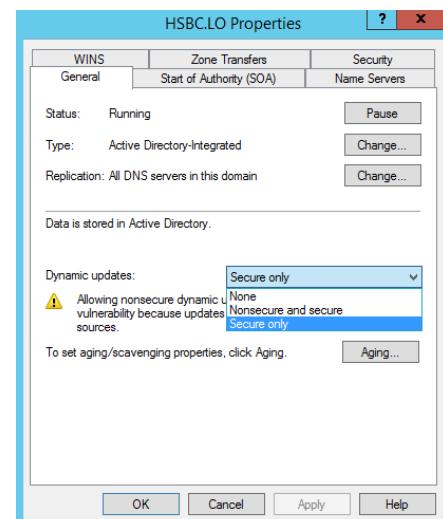
Secure Dynamic Updates

يجب أن يكون الـ Server قد تمت ترقيته إلى Domain Controller كي نستطيع تفعيل الخاصية



من DNS Manager نضغط بالزر اليمين على
المراد تفعيل الخاصية لها ثم نختار
Zone Properties

ثم من قائمة Dynamic Updates نختار
Ok ونضغط Secure Only





Socket Pool

و تكون مفعلاً افتراضياً بقيمة port 2500 ويمكن التعديل عليها من خلال أمر cmd التالي:

DnsCmd /Config /SocketPoolSize 5000

حيث سنزيد عدد الـ Ports العشوائية إلى Port 5000 ويمكننا أن نتأكد من خلال الأمر /info

```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>dnsCmd /info /socketpoolsize
Query result:
Dword: 2500 (000009C4)
Command completed successfully.

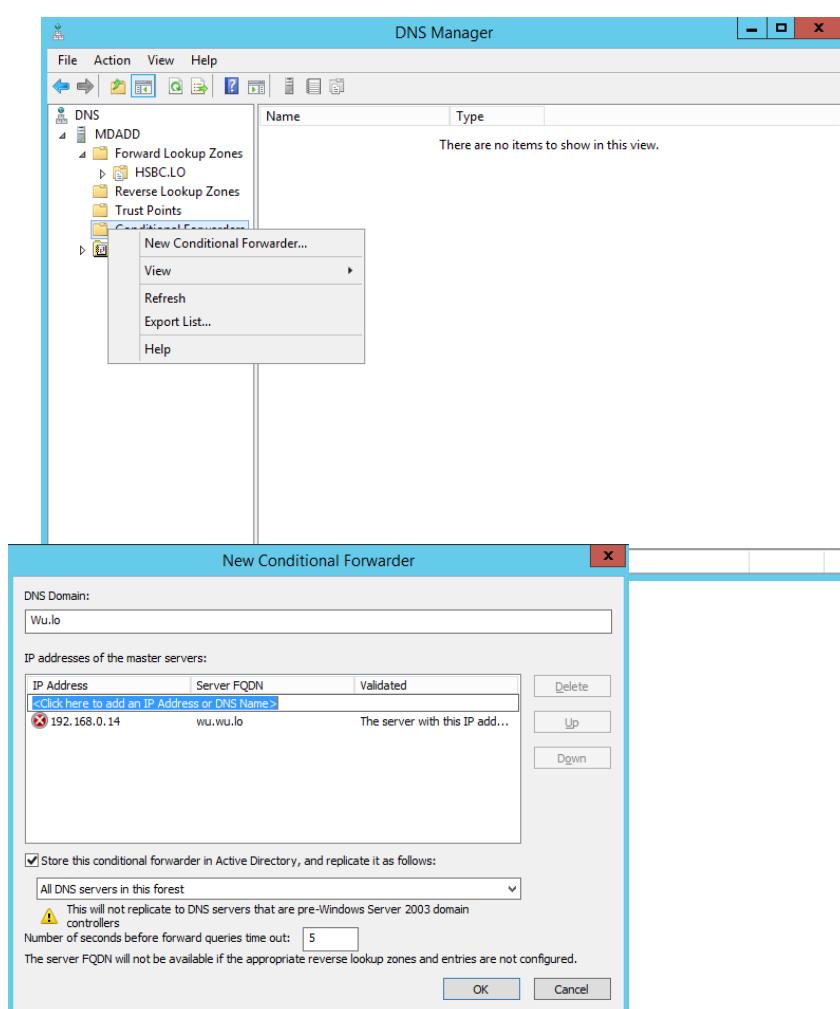
C:\Users\Administrator>dnsCmd /Config /SocketPoolSize 5000
Registry property SocketPoolSize successfully reset.
Command completed successfully.

C:\Users\Administrator>dnsCmd /info /socketpoolsize
Query result:
Dword: 5000 (00001388)
Command completed successfully.
```

Conditional Forwarder

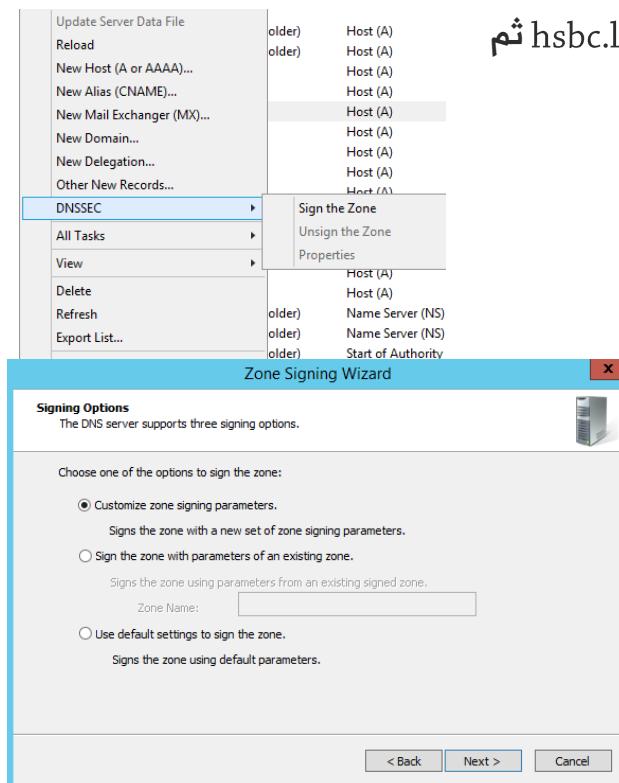
1- من DNS Manager نضغط على Conditional Forwarders بالزر اليمين ونختار Forwarder... Forwarder...

2- نضع الـ Dns domain الذي نريد أن نمرر طلباته وعنوان الـ Authoritative Dns Server الخاص به ونعلم خيار ثم نضغط Store this conditional forwarder in active directory and replicate it as follows Ok





DNSSEC



1- من DNS Manager نضغط بالزر اليمين على `hsbc.lo zone` ثم
DNSSEC → Sign the Zone

فيتم تشغيل الـ Zone Signing Wizard

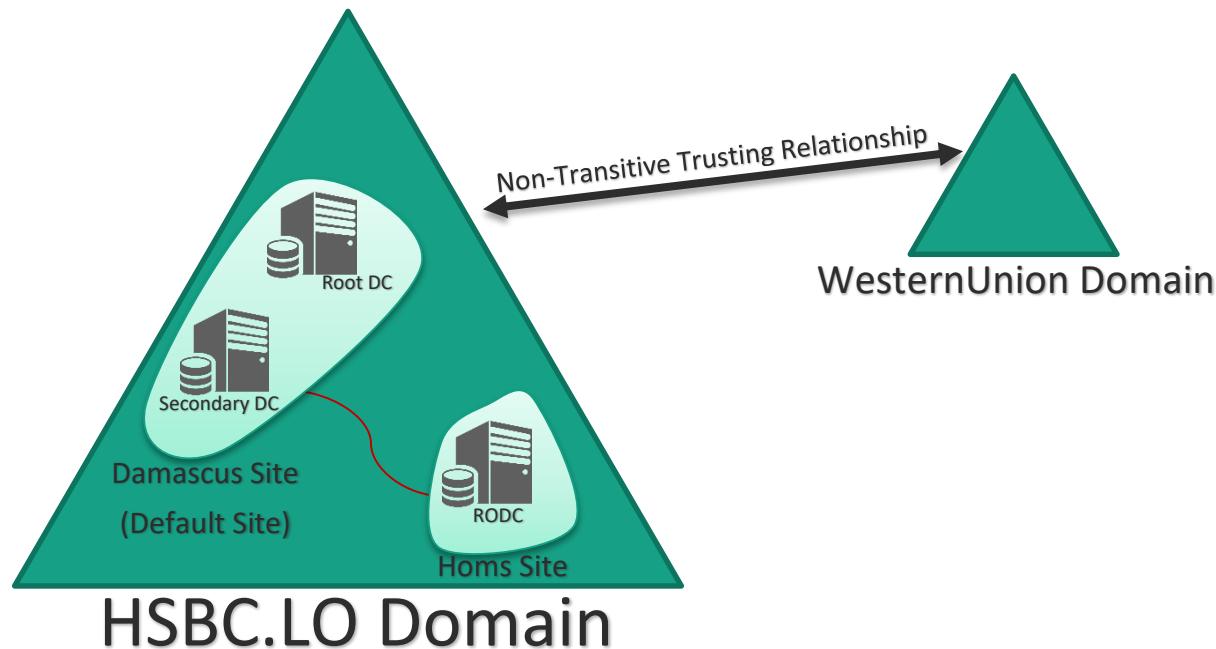
2- نقوم بتحديد Use default settings to sign ثم Next → Next ثم نضغط على the zone

حيث ستكون الإعدادات كما يلي:

Group	Setting	Value	Description
Key Signing key (KSK)	Algorithm	RSA/SHA-256	نوع خوارزمية التشفير المستخدمة لتشغيل الـ Keys التي سيتم توليدها لتوقيع الـ Zone
	Key Length	2048 bits	حجم الـ KSK
	KSP	Microsoft Software Key Storage Provider	مكان حفظ الـ Keys
	DNSKEY signature validity	168 hours	المدة التي سيبيقي الـ KSK فعالةً قبل تغييره
	Replication	Enabled	لنقل الإعدادات عبر الـ ADDS
Zone Signing Key (ZSK)	Algorithm	RSA/SHA-256	نوع خوارزمية التشفير المستخدمة لتشغيل الـ Zone
	Key Length	1024 bits	حجم الـ ZSK
	KSP	Microsoft Software Key Storage Provider	مكان حفظ الـ Keys
	DNSKEY signature validity	168 hours	المدة التي سيبيقي الـ ZSK فعالةً قبل تغييره
	DS Signature validity	168 hours	المدة التي سيبيقي الـ DS فعالةً خلالها
Authenticated Denial of Existence	Zone Resource record signature validity	240 hours	المدة التي سيبيقي تشفير الـ Resource Record فعالةً خلالها قبل تغييره
	Replication	Enabled	لنقل الإعدادات عبر الـ ADDS
Authenticated Denial of Existence	Authenticated Denial of Existence	NSEC3	النمط المستخدم لتشغيل الرد على الـ query عند عدم إيجاد جواب لها
Trust Anchor	Trust Anchor	Enabled	لتحديد نقطة البداية الخاصة بتوليد الـ ADDS عند استخدام بيئة Keys

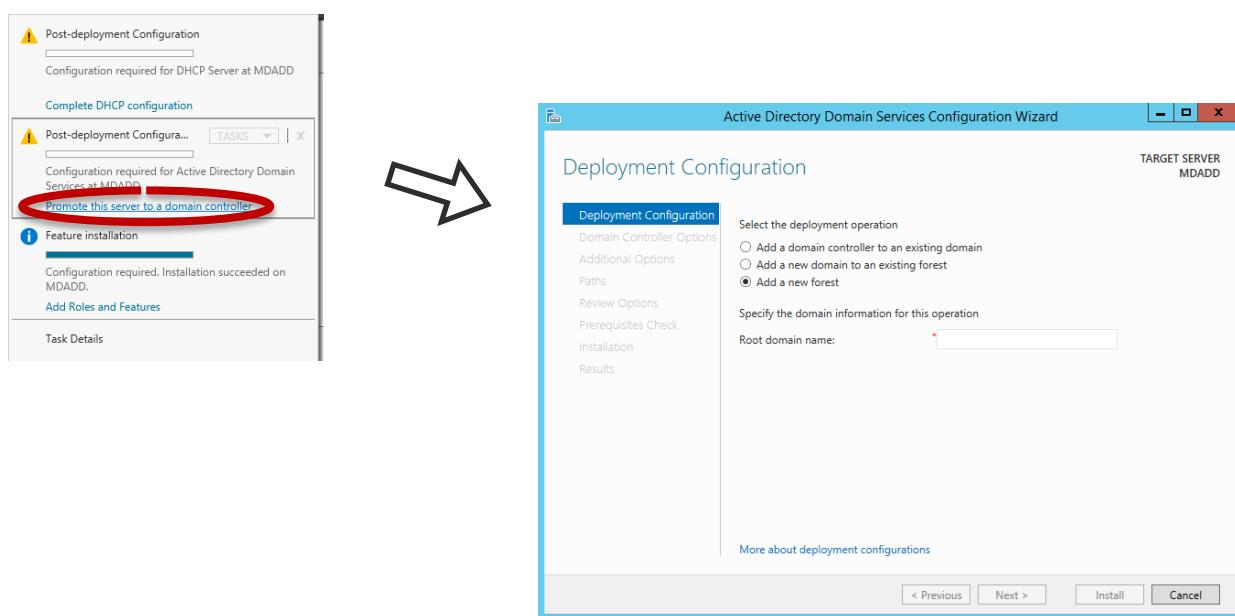


ADDS

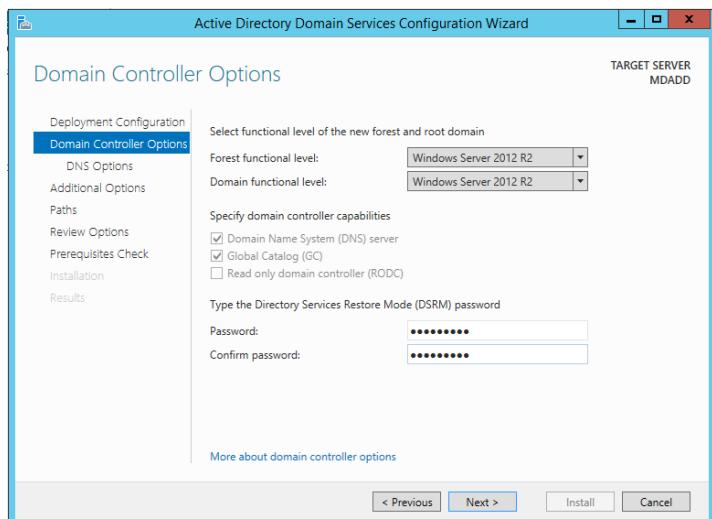


Domain Creation

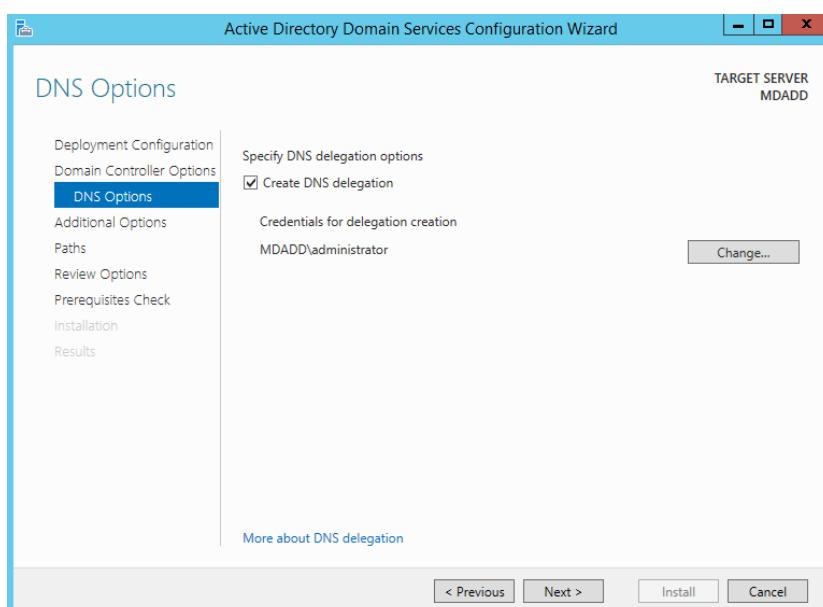
MDADD (Main Damascus DC)



تسألنا النافذة السابقة إذا أردنا أن ننشأ Domain Controller موجودة مسبقاً أو إضافة إلى Forest Domain منشأ مسبقاً أو إنشاء Forest جديدة في حالتنا سنقوم بإنشاء Forest جديد تحتوي على الـ domain الجديد ثم نحدد اسم الـ domain حيث سيكون HSBC.LO



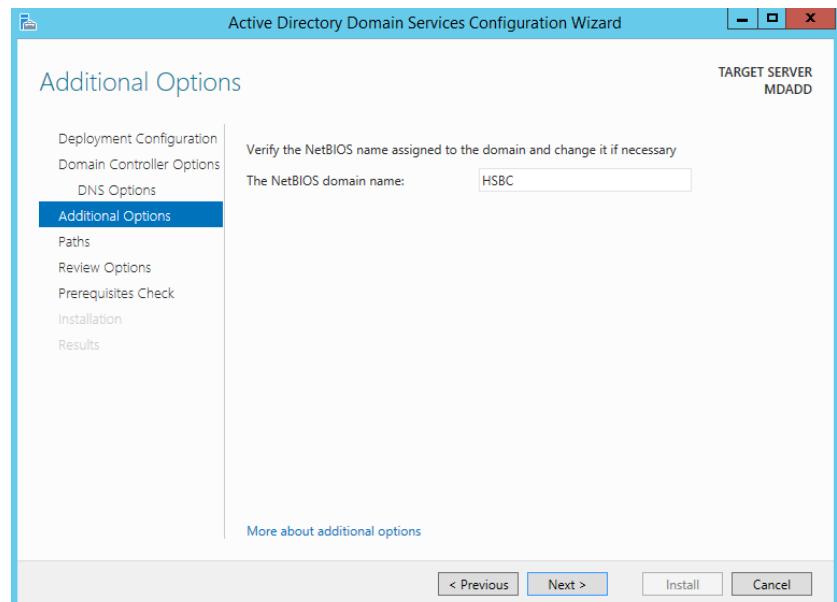
في النافذة التالية سنقوم باختيار الـ Forest Functional Lever حيث سيكونان Windows Server 2012 R2 هيكل سيرفر 2012 R2 حيث ستكون Level بالإضافة إلى Domain Password خاص بالـ Domain.



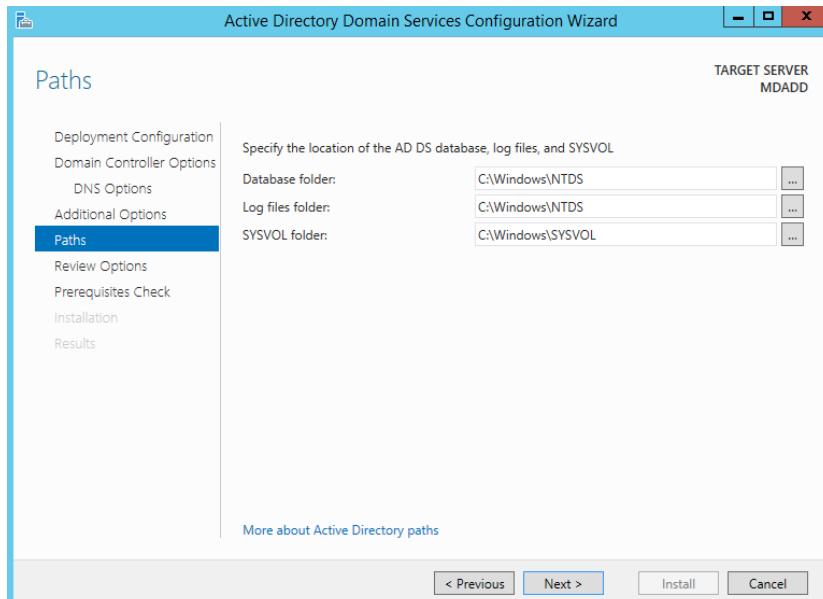
ثم نضغط على Next وضمن النافذة التالية نقوم بتحديد Create DNS Delegation لتحويل الـ Dns Zone الخاصة بالـ Domain إلى Active Directory Integrated Zone.

ثم نقوم من خلال الضغط على زر change... بتحديد هوية الـ local administrator الخاص بهذا الجهاز للسماح بهذه العملية ونضغط على Next.

نتحقق من الـ NetBIOS Name الخاص بالـ Domain ونضغط على Next.

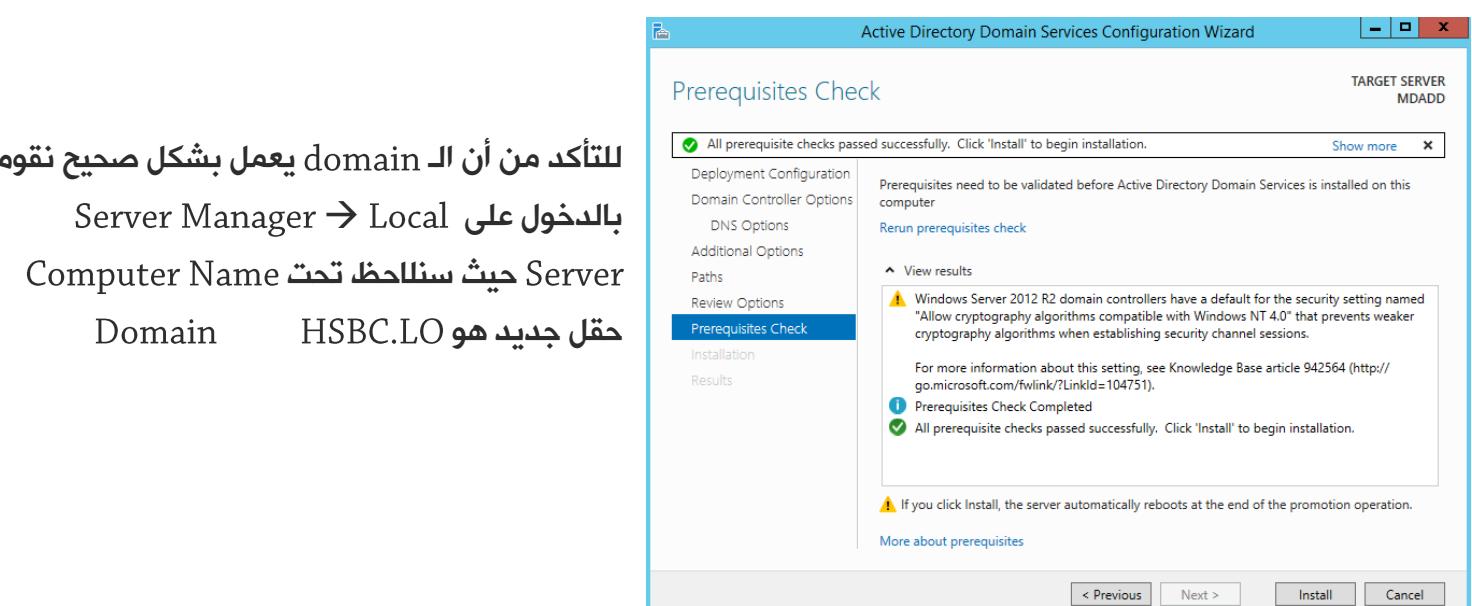


بعدها نقوم بتحديد مكان حفظ الملفات الخاصة بال Active Directory Database وملفات ال Log بالإضافة إلى مجلد SYSVOL الذي يحتفظ بالملفات public التحرّكات التي تحصل على الـ domain controller بالإضافة إلى الملفات الخاصة بال domain clients والتي يحتاج الـ clients إلى نصّفها.



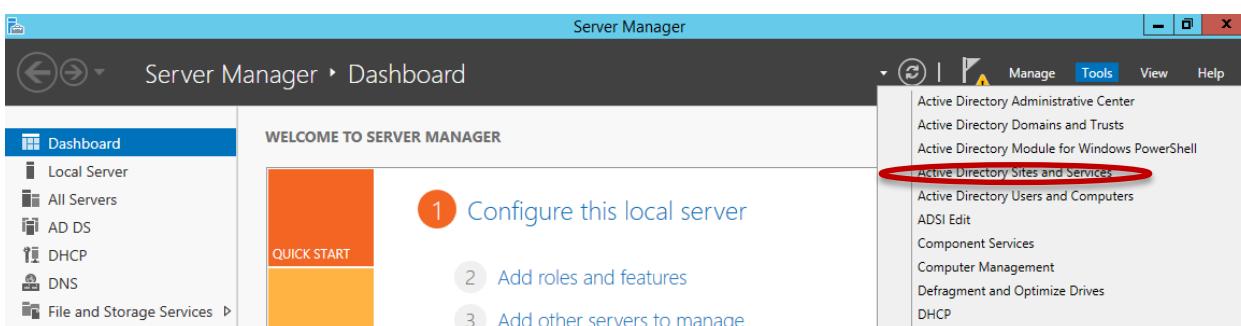
ننتظر ريثما يتم التحقق من وجود كافة المتطلبات لتشغيل الـ Domain Controller ثم نضغط على Install وعند الانتهاء سيقوم الـ Server بعمل Restart.

لتتأكد من أن الـ domain يعمل بشكل صحيح نقوم بالدخول على Local Computer Name حيث سنلاحظ تحت Server Domain هو HSCB.LOCAL جيد.

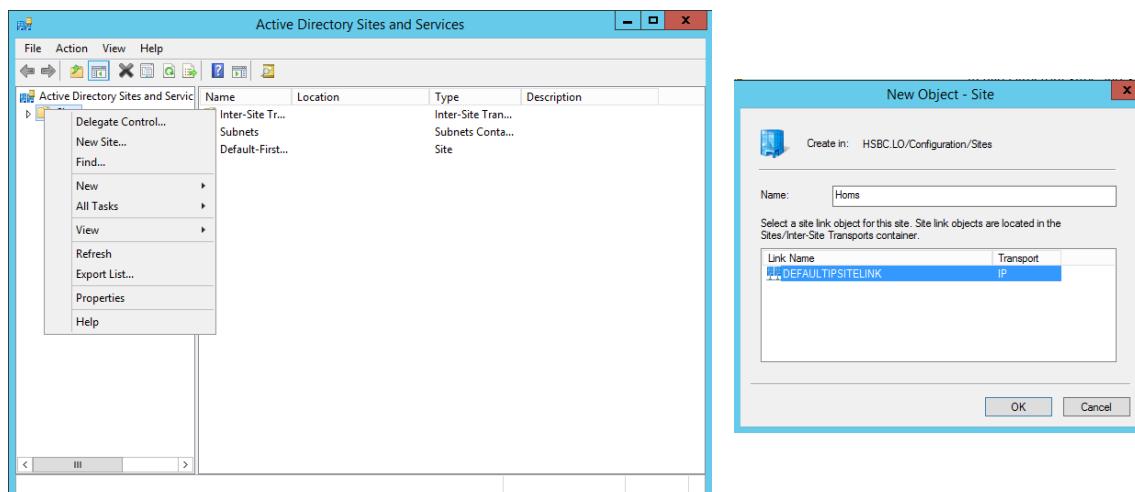


ذكرنا سابقاً وجود AD Objects تدل على التموضع الفيزيائي للشبكة ومن أبرزها الـ Sites وبما أن بنك HSBC له فرعين فستقوم بإنشاء Site آخر يعبر عن فرع دمشق وسنقوم بتغيير اسم Site الأساسي إلى Damascus.

Sites Creation



نضغط بالزر اليمين على اسم الـ Domain ثم من قائمة Site New نختار



عند الانتهاء من الخطوات السابقة ستظهر رسالة تخبر بضرورة إضافة Site Subnets لكل Site والتأكد من أن الـ Site مرتبطين بـ Links وأنه يجب إضافة إلى Site الجديد.

لإنشاء الـ Subnets سنستخدم ملف بصيغة csv بالإضافة إلى تعليمات في PowerShell هما New-Import-Csv AdReplicationSubnet

Name	Site
192.168.0.0/25	Damascus
192.168.0.128/25	Damascus
192.168.1.0/25	Damascus
192.168.1.128/25	Damascus

وسيكون ملف الـ csv على الشكل التالي

حيث حقل الـ Name يدل على عنوان الـ subnet والحقل Site يدل على Site التابع الذي يتبع لها

بعد إنشاء الـ Sites وإضافة الـ Subnets سنقوم بإضافة سيرفري HADD (وهو سيرفر فرع حمص) وـ SDADD (وهو السيرفر الاحتياطي للشبكة كل) إلى الـ Domain Controllers ثم ترقيتهما إلى Domain حيث سيكون HADD عبارة عن RODC وـ SDADD سيكون DC.

```

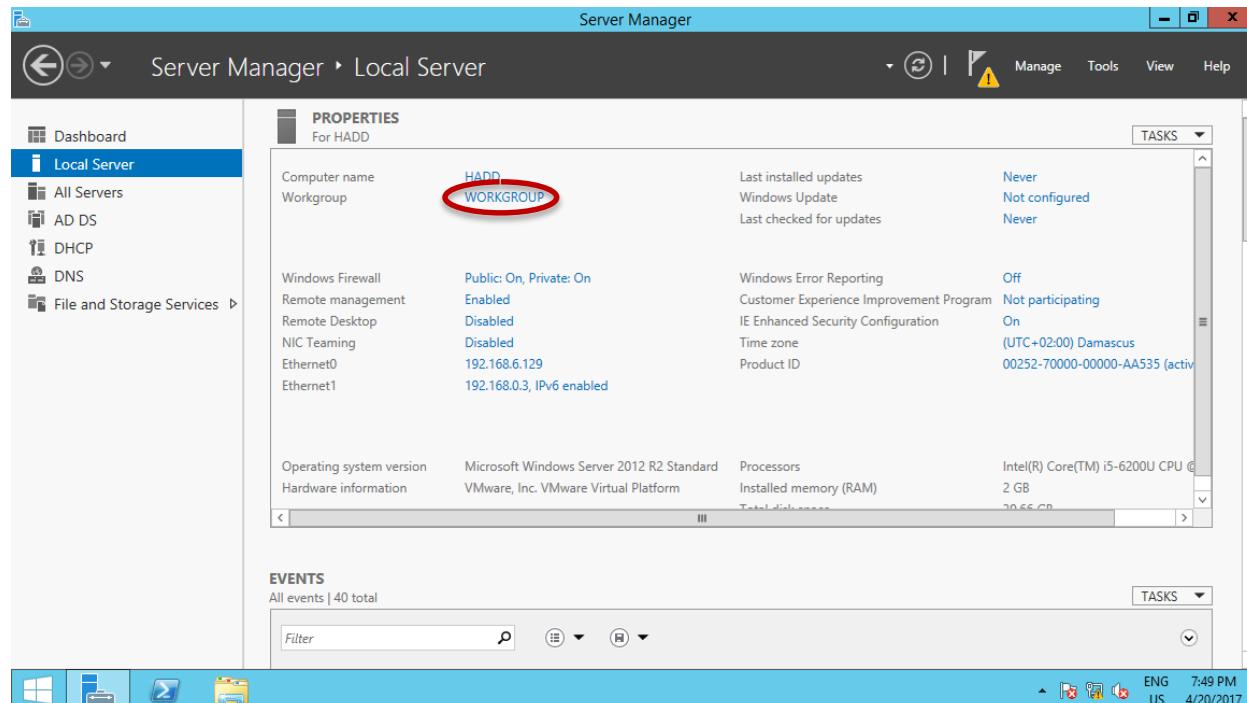
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2014 Microsoft Corporation. All rights reserved.

C:\Users\Administrator> cd .\Desktop
C:\Users\Administrator\Desktop> cd .\Csv
C:\Users\Administrator\Desktop\Csv> Import-Csv .\Subnets.csv | New-ADReplicationSubnet

```

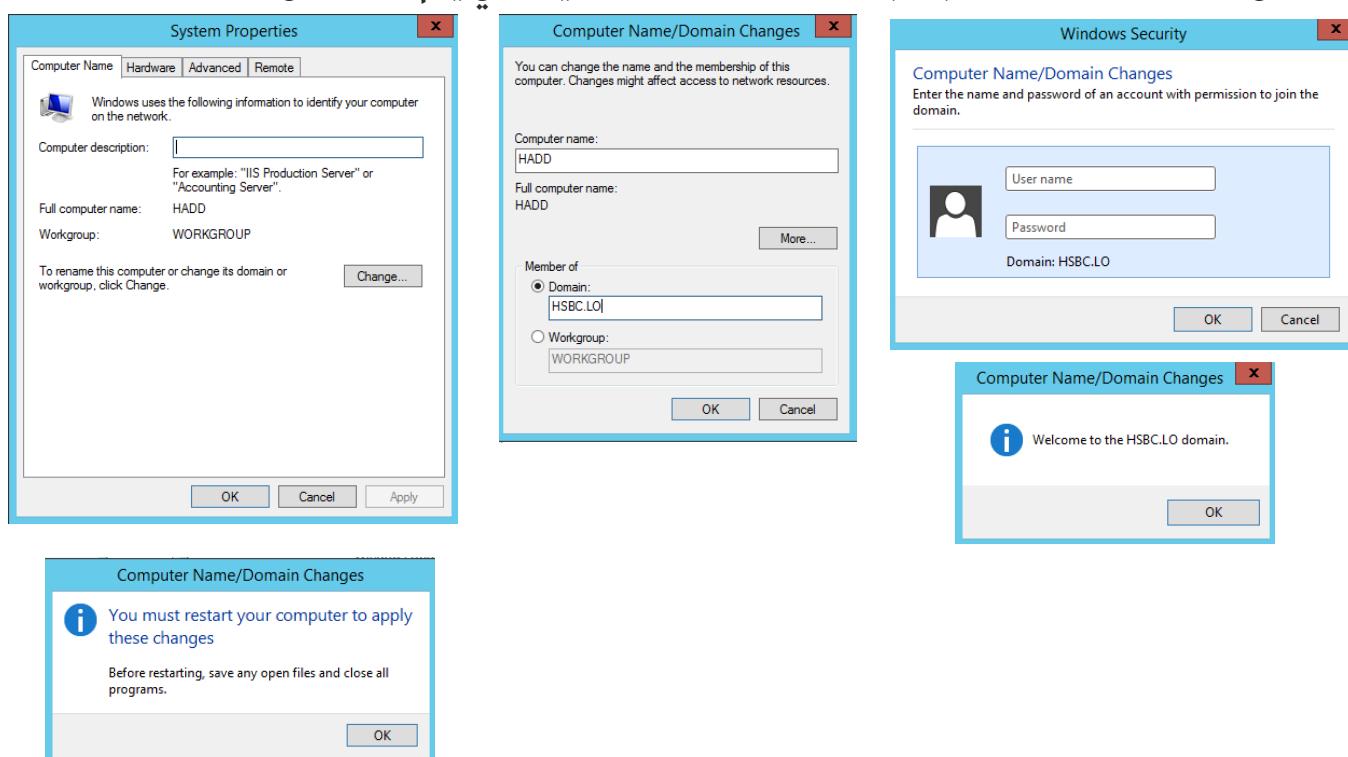


لإضافة السيرفرات إلى الـ Domain تقوم بالدخول من كل سيرفر على حداً إلى Local Server → WORKGROUP



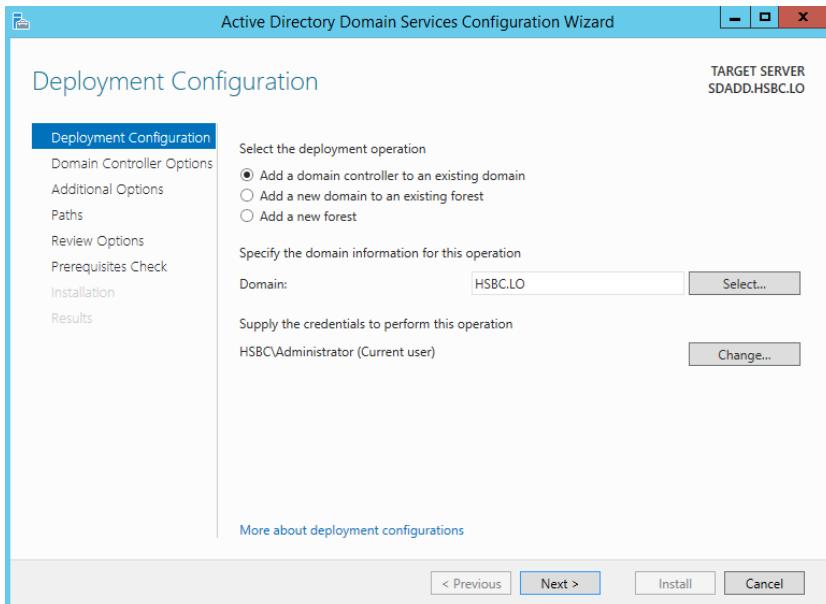
نضغط على Change فتظهر لنا نافذة نختار منها الخيار Domain ونضع في المستطيل اسم الـ Domain ثم نضغط OK فتظهر لنا رسالة تطلب اسم وكلمة سر الـ Domain Admin ندخلهما ونضغط على OK ثم تظهر لنا رسالة ترحيب في الـ Domain.

. domain . نضغط على OK فتظهر لنا رسالة تخبرنا بضرورة عمل Restart للسيرفر كي يتم إضافته إلى الـ Domain

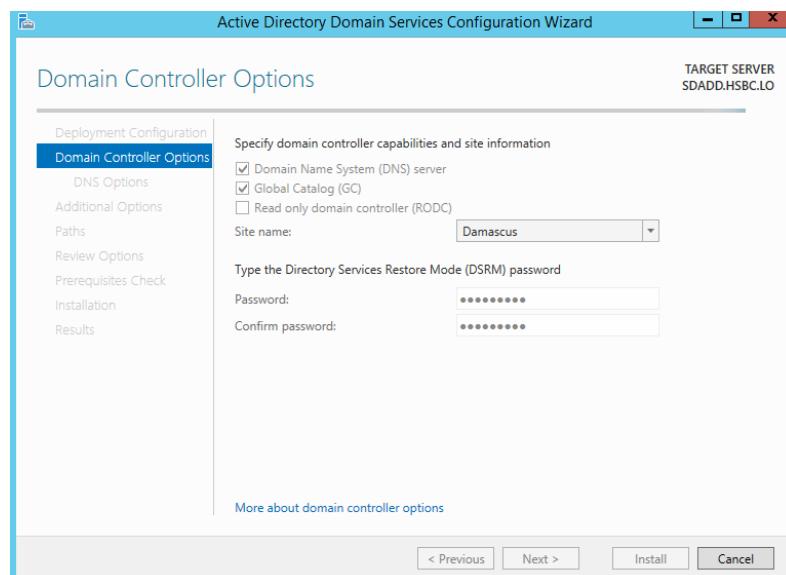




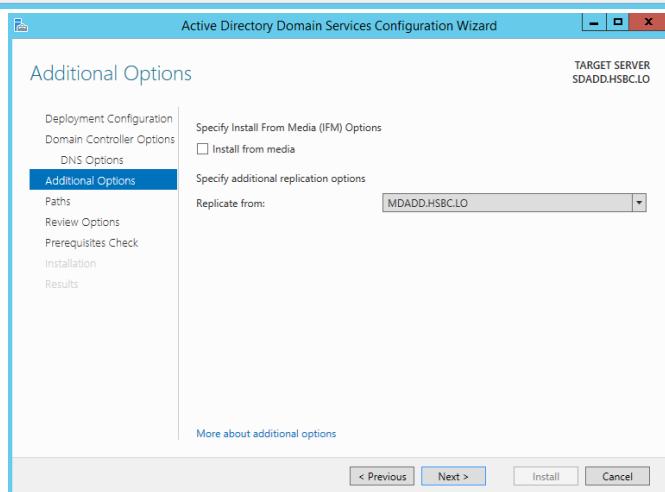
Promoting SDADD to a Domain Controller



بعد عمل Log in على السيرفر من حساب الـ Server Manager ندخل على Domain Admin ونضغط على Notification ومنها نختار Promote this server to a domain Add a domain controller نختار controller فنلاحظ أنه قد تم إدخال اسم الـ domain والصلاحيات تلقائياً فنضغط على Next .



بما أن هذا السيرفر سيكون بهدف تخفيف الحمل عن السيرفر الأساسي وللحافظة على عمل الشبكة بحال حدوث ضرر للسيرفر الرئيسي فسيكون هذا السيرفر كـ Password أيضاً لذا ندخل الـ Global Catalog ونضغط على Next .



عند ظهور النافذة التالية نضغط أيضاً على Next .

نختار الـ Domain Controller الذي سيقوم Replicate من هو MDADD.HSBC.LO .

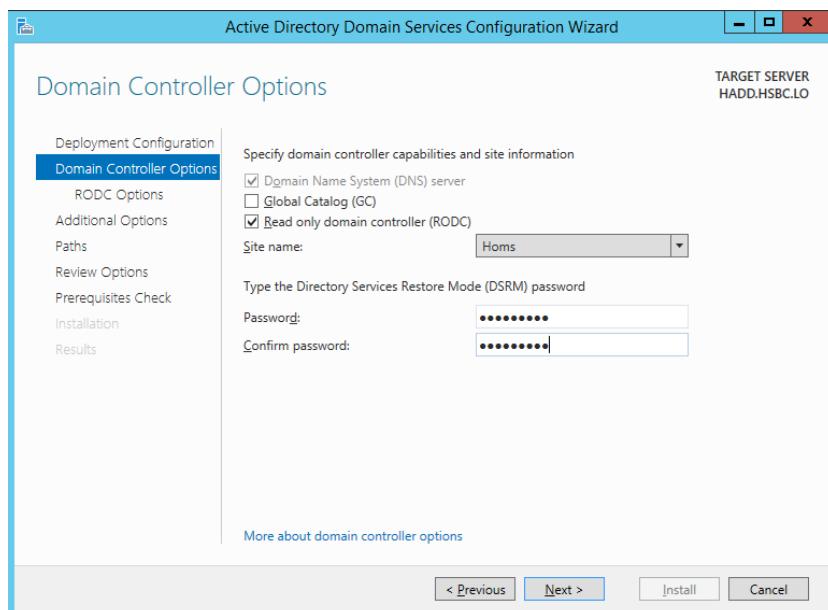
ثم نضغط على Next → Next → Install .

وبعد عمل Restart للسيرفر يكون قد أصبح Controller .



Promoting HADD to a Read-Only Domain Controller

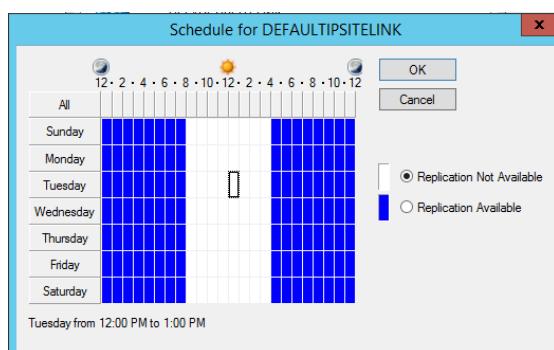
بعد عمل Log In على السيرفر من حساب الـ Domain Admin → نقوم بالضغط على Add a domain controller to an نختار Notification → Promote this server to a domain controller Next ونضغط على existing domain



في النافذة التالية نلغي تحديد Read only domain controller (GC) ومن ثم نضع Site Name Homs (RODC) في النافذة التالية تمكنا من اختيار حساب الـ Domain Controller المسئول عن إدارة هذا الـ Domain Controller بالإضافة إلى الـ Users المسموح حفظه، بالإضافة إلى الـ Users الخاص بهم في الـ cache والـ Password الغير مسموح حفظه الـ Password الخاص بهم سنضغط على Next حيث سنقوم بتحديدهم لاحقاً

في النافذة التالية نضغط على Next → Next → Next → Install وبعد عمل Restart يكون قد أصبح RODC.

Replication Policy



لتخفيف الحمل على الشبكة في أوقات الدوام سيكون الـ Replication مسموح فقط بعد انتهاء دوام الموظفين أي كل يوم من الساعة 5 وحتى 8 صباحاً ما عدا أيام العطل سيكون مسموح طول اليوم ولعمل ذلك من Server Manager → AD Sites and services → Default Inter-Site Transports → IP Change Schedule على ونختار Site Link ونقوم بالتعديل بحسب ما يناسب ثم نضغط على ok ثم ok مرة أخرى.



OU Design and Creation

HSBC.LO

Damascus	Accounting	Users Computers Groups
Branch	Security	Users Computers Groups
	Customer Service	Users Computers Groups
	Internal Trades	Users Computers Groups
	International Trades	Users Computers Groups
	HR	Users Computers Groups
	Management	Users Computers Groups
	Technical Support	Users Computers Groups
	Technical Administration	Users Computers Groups
	IT	Users Computers Groups
	Network Admin	Users Computers Groups

Homs

Branch

Accounting	Users Computers Groups
Customer Service	Users Computers Groups
HR	Users Computers Groups
Management	Users Computers Groups
Network Dep	Users Computers Groups
IT	Users Computers Groups
Net Room	Users Computers Groups

سيتم إنشاء الـ Ou's عن طريق دمج أمرا PowerShell import-csv هما (التي تقوم بإدخال الإعدادات من ملف csv) و

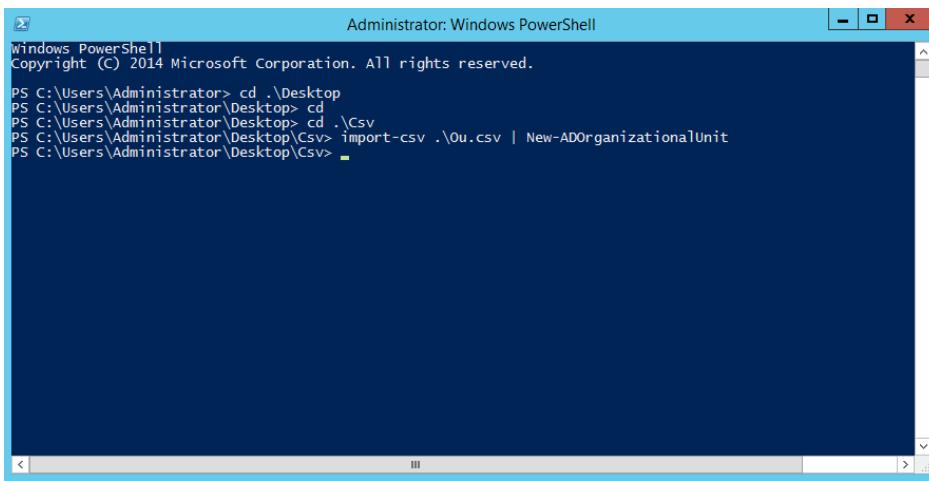
Path	Name
DC=HSBC,DC=LO	DamascusBranch
DC=HSBC,DC=LO	HomsBranch
OU=DamascusBranch,DC=HSBC,DC=LO	Accounting
OU=DamascusBranch,DC=HSBC,DC=LO	Security
OU=DamascusBranch,DC=HSBC,DC=LO	CustomerService

New-ADOrganizationalUnit
الذي يقوم بإنشاء (Ou) عن طريق الـ Pipeline (|) حيث سيكون ملف الـ csv كالتالي:

عمود الـ Path يمثل Parameter –Path الذي يعطي لتعليمات إنشاء الـ Ou ويمثل مسار الـ Ou ضمن الـ Domain

عمود الـ Name هو أيضًا Parameter يمثل اسم الـ Ou

نقوم بفتح الـ PowerShell والتوجه إلى مكان تمويع ملف الـ csv الذي يحتوي على الإعدادات عن طريق استخدام تعليمة cd يمكننا أن نعطي التعليمية import-csv ونحدد مسار تمويع parameter –Path الملف. ثم ندخل الأمر المراد تنفيذه ونضغط Enter



```

Windows PowerShell
Administrator: Windows PowerShell
Copyright (C) 2014 Microsoft Corporation. All rights reserved.

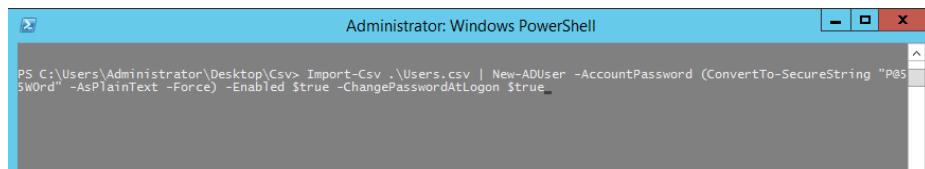
PS C:\Users\Administrator> cd ..\Desktop
PS C:\Users\Administrator\Desktop> cd ..
PS C:\Users\Administrator\Desktop> cd ..\Csv
PS C:\Users\Administrator\Desktop\Csv> import-csv .\Ou.csv | New-ADOrganizationalUnit
PS C:\Users\Administrator\Desktop\Csv>

```

Users Addition

وسيتم ذلك عن طريق ملف csv وأمر PowerShell التالي:

Import-Csv .\Users.csv | New-ADUser –AccountPassword (ConvertTo-SecureString "P@55W0rd" –AsPlainText –Force) –Enabled \$true –ChangePasswordAtLogon \$true



```

Administrator: Windows PowerShell
PS C:\Users\Administrator\Desktop\Csv> Import-Csv .\Users.csv | New-ADUser -AccountPassword (ConvertTo-SecureString "P@55W0rd" -AsPlainText -Force) -Enabled $true -ChangePasswordAtLogon $true

```

: لتخزين الكلمة المدخلة في متغير من النمط secure string كي يتم محياها من ذاكرة الجهاز عند الانتهاء من تنفيذ الأمر

: كي لا يعامل الكلمة المدخلة على أنها متتحول إذا حوت على \$

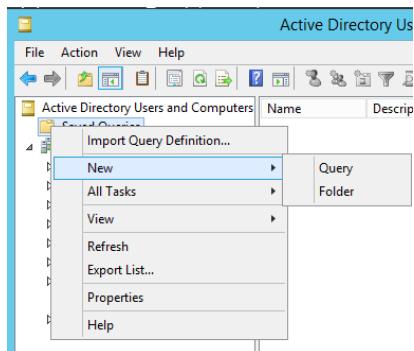
: لإجبار التنفيذ –Force

: ليتم تفعيل الحساب –Enabled

: لتغيير كلمة المرور عند أول استخدام للحساب –ChangePasswordAtLogon

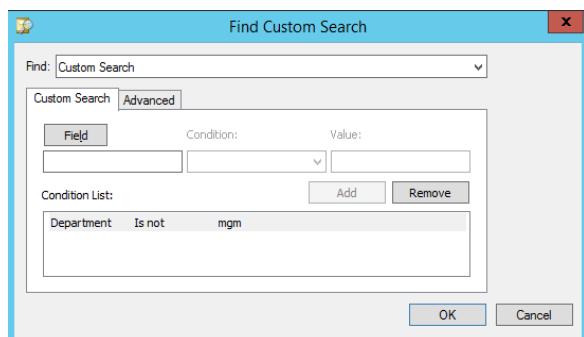
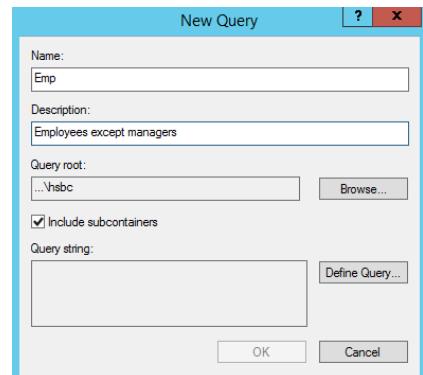


LogOn Hours

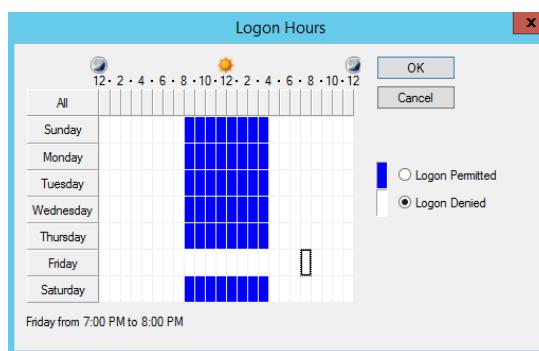
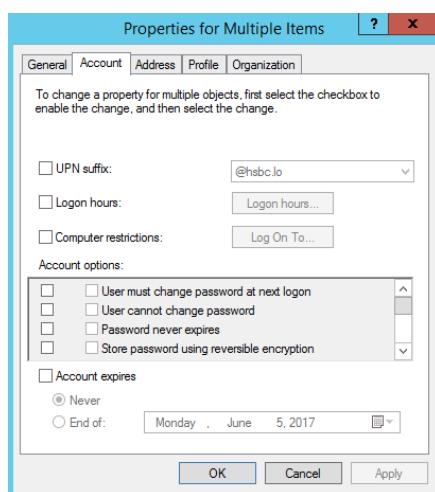


لتحديد الوقت المسموح فيه استخدام الحساب الخاص بكل موظف من Active Directory Users and Computers نضغط بالزر اليمين على Query New ثم وختار Saved Queries.

من النافذة الظاهرة نضغط على Define Query



ثم نضغط على ok فنجد جميع الحسابات المطبقة عليها شروطنا فنقوم بتحديد الكل ثم نضغط بالزر اليمين وختار Properties ومنها نعلم المربع بجانب Logon Hours ونضغط على ... لتحديد الأوقات المناسبة



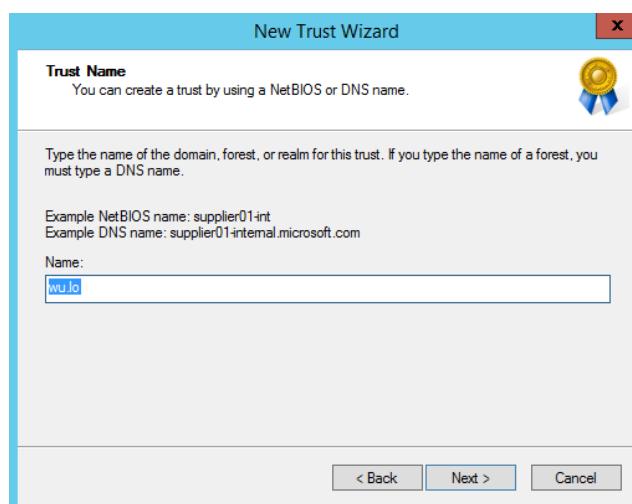


Trust Relationship

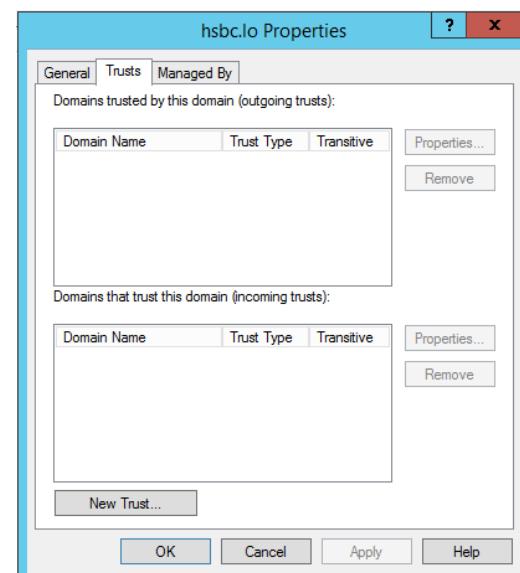
1- من Active Directory Domains and Trusts نضغط بالزر اليمين ونختار Domain

2- من تبوية Trusts نختار New Trust

ندخل اسم الـ Domain الذي نريد إنشاء العلاقة معه



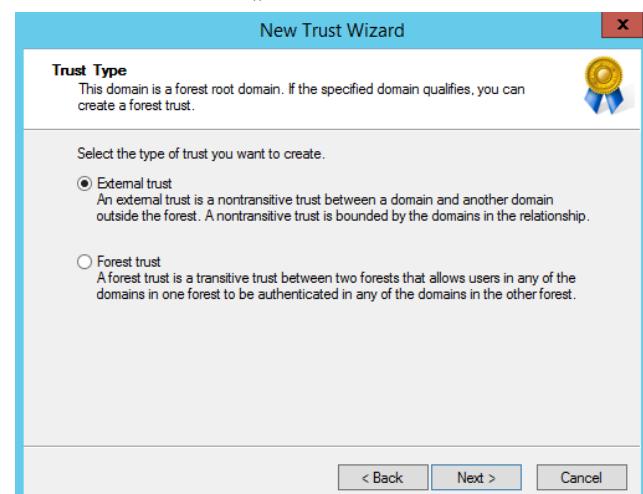
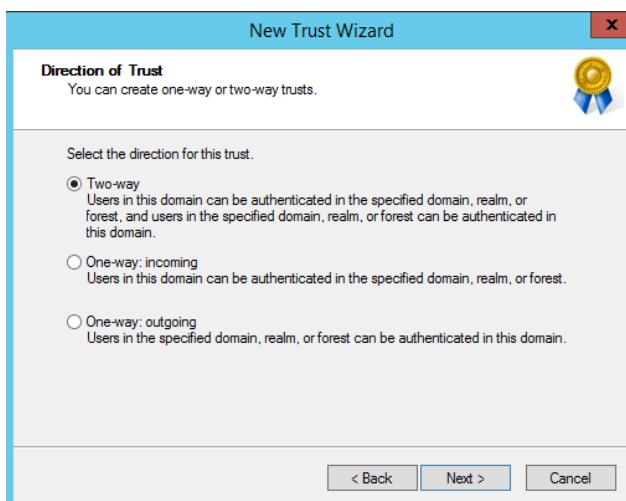
-3



4- نختار نمط العلاقة هل هي مع Forest من نفس الـ Domain أو من خارجها

نختار اتجاه العلاقة

-5



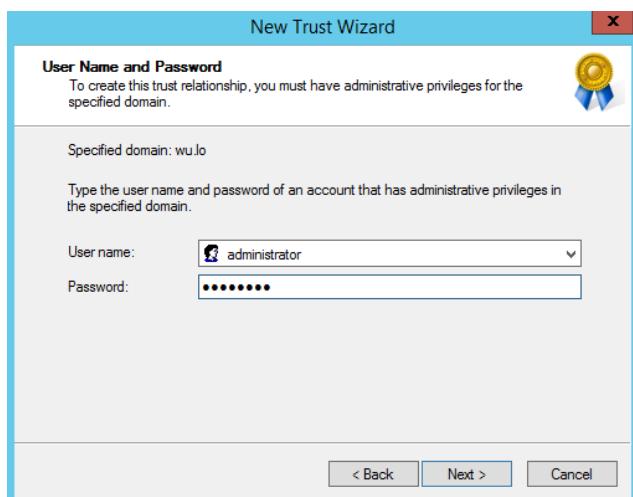
نختار الجهة التي يتم إنشاء العلاقة فيها

-6

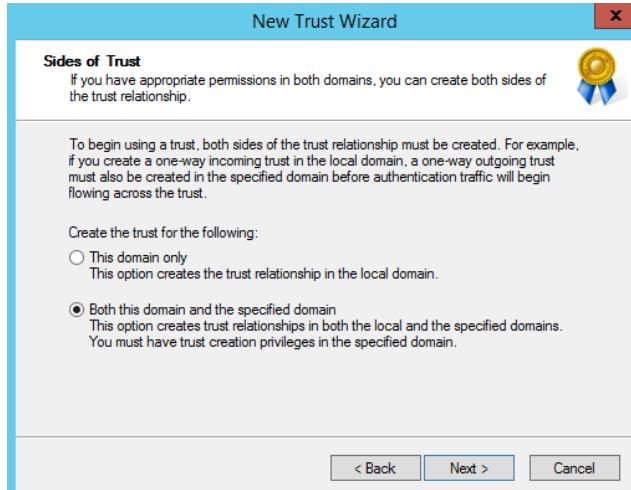
ندخل الـ Username and Password الخاصين بـ

-7

WU. LO Domain Administrator

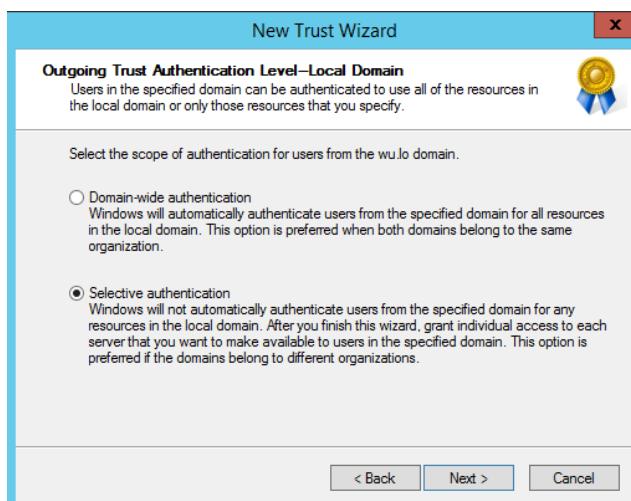
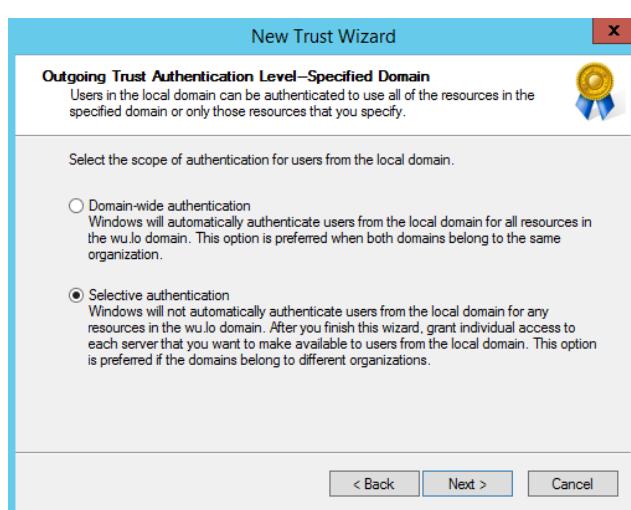


نختار نمط الـ Authentication للاتصالات الصادرة إلى



8- نختار نمط الـ Authentication للاتصالات

الواردة من



نقوم بتأكيد العلاقة ونضغط على

-10

AGDLA

Global Groups

_Inten	_NetAdmin
_Interna	_IT
_CustServ	_TechAdmin
_Acc	_TechSup
_Sec	_Mgmt
_HR	

Group	Members	Type	Permissions
_Employees	All Employees	Security	Read
_Damas	Damascus Employees	Security	Read
_Homs	Homs Employees	Security	Read
_Decisions-W	_mgmt	Security	Write
_Decisions-R	_employees	Security	Read
_News-R	_employees	Security	Read
_News-W	_Mgmt	Security	Write
_Prg-R	_Employees	Security	Read
_Prg-W	_NetAdmin _IT	Security	Write
_NetAdminDR-r	_NetAdmin,_Mgmt	Security	Read
_ITDR-r	_IT,_Mgmt	Security	Read
_TechAdminDR-r	_TechAdmin,_Mgmt	Security	Read
_TechSupDR-r	_TechSup,_Mgmt	Security	Read
_MgmtDR-r	_Mgmt,_Mgmt	Security	Read
_HRDR-r	_HR,_Mgmt	Security	Read
_IntenDR-r	_Inten,_Mgmt	Security	Read
_InternaDR-r	_Interna,_Mgmt	Security	Read
_CustServDR-r	_CustServ,_Mgmt	Security	Read
_AccDR-r	_Acc,_Mgmt	Security	Read
_SecDR-r	_Sec,_Mgmt	Security	Read
_NetAdminDR-w	NET-Maya-01	Security	Write
_ITDR-w	IT-Stieve-04,IT-Bassel-01	Security	Write
_TechAdminDR-w	TADM-Lara-01	Security	Write
_TechSupDR-w	TSUP-Leen-01	Security	Write
_MgmtDR-w	MGM-Carl-03,MGM-Zena-01	Security	Write
_HRDR-w	HR-Roni-04,HR-Samar-01	Security	Write
_IntenDR-w	INT-Abdulrahman-01	Security	Write
_InternaDR-w	INTR-Shadi-01	Security	Write
_CustServDR-w	CUS-Mary-04,CUS-Fares-01	Security	Write
_AccDR-w	ACC-Yara-03,ACC-Mohamad-01	Security	Write
_SecDR-w	SEC-Hassan-01	Security	Write



Domain Local Groups

Groups Creation

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2014 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator\Desktop\Csv> cd Desktop\Csv
PS C:\Users\Administrator\Desktop\Csv> Import-Csv .\Groups.csv | New-ADGroup
PS C:\Users\Administrator\Desktop\Csv>
```

سنقوم بإنشاء الـ groups objects عن طريق أمر PowerShell التالي:

Import-Csv .\Groups.csv | New-ADGroup

Group Members Addition

لإضافة أعضاء إلى المجموعات سنقوم باستخدام أمر PowerShell التالي:

Import-Csv .\GrpMem.csv | ForEach-Object {Add-ADGroupMember -Identity \$_.Id -Members \$_.Mem}

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2014 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator\Desktop\Csv> Import-Csv .\GrpMem.csv | ForEach-Object{ Add-ADGroupMember -Identity $_.Id -Members $_.Mem }
PS C:\Users\Administrator\Desktop\Csv>
```

PSO

Employees PSO

Attribute	Value
Cn	Emp
msDS-PasswordSettingsPrecedence	2
msDSPasswordReversibleEncryptionEnabled	False
msDS-PasswordHistoryLength	30
msDS-PasswordComplexityEnabled	TRUE
msDS-MinimumPasswordLength	10
msDS-MinimumPasswordAge	45:00:00:00
msDS-MaximumPasswordAge	60:00:00:00
msDS-LockoutThreshold	3
msDS-LockoutObservationWindow	00:00:30:00
msDS-LockoutDuration	(Never)
msDS-PSOAppliesTo	All Employees Except (Management ,IT, and Tech support)

Management and IT PSO

Attribute	Value
Cn	Man
msDS-PasswordSettingsPrecedence	3
msDSPasswordReversibleEncryptionEnabled	False
msDS-PasswordHistoryLength	70
msDS-PasswordComplexityEnabled	TRUE
msDS-MinimumPasswordLength	10
msDS-MinimumPasswordAge	20:00:00:00
msDS-MaximumPasswordAge	30:00:00:00
msDS-LockoutThreshold	3
msDS-LockoutObservationWindow	00:00:30:00
msDS-LockoutDuration	(Never)
msDS-PSOAppliesTo	Management ,IT, and Tech support

Default Domain PSO

Attribute	Value
Enforce Password History	24
Minimum Password Length	8
Minimum Password Age	45 Days
Maximum Password Age	90 Days
Account Lockout Threshold	3
Reset Account Lockout Counter After	30 min
Account Lockout Duration	0

GPO

Normal Employees

- Folder Redirection:
 - o AppData(Roaming) → User's Desktop
- Policies:
 - o Control Panel:
 - Hide the “Add a program from CD-ROM or floppy disk” Option
 - o Prohibit access to Control Panel
 - o Display:
 - Hide Settings Tab

- Programs:
 - Hide “Installed Updates” Page
 - Hide “Programs and Features” Page
 - Hide “Windows Features”
- Desktop:
 - Remove Properties from the Computer icon context menu
- System:
 - Remove Task Manager
 - CD and DVD : Deny Read and Write Access
 - Floppy Drives: Deny Read and Write Access
 - Removable Disks: Deny Read and Write Access
 - All Removable Storage Classes: Deny All Access
 - Prevent Access to the Command Prompt
 - Prevent Access to registry editing tools
- Windows Components:
 - Turn off Autoplay
 - Notify Antivirus programs when opening attachments
 - Restrict unpacking and installation of gadgets that are not digitally signed
 - Turn off “Windows + X”

Management

- Folder Redirection:
 - AppData(Roaming) → User’s Desktop
- Policies:
 - Control Panel:
 - Hide the “Add a program from CD-ROM or floppy disk” Option
 - Display:



- Hide Settings Tab
- Programs:
 - Hide “Installed Updates” Page
 - Hide “Programs and Features” Page
 - Hide “Windows Features”
- Desktop:
 - Remove Properties from the Computer icon context menu
- System:
 - Remove Task Manager
 - Prevent Access to the Command Prompt
 - Prevent Access to registry editing tools
- Windows Components:
 - Turn off Autoplay
 - Notify Antivirus programs when opening attachments
 - Restrict unpacking and installation of gadgets that are not digitally signed
 - Turn off “Windows + X”

IT Staff

Full Control

Redircmp & Redirusr

يتم تفعيل الأداة عبر PowerShell بـإدخال الأمر `Redircmp -Name Ou -DistinguishedName Ou -WillBeUsed` الخاص بالـOU المراد وضعها لذلك أولاً سنقوم بإنشاء الـOU ثم تحويلها وإنشاء الـOU نقوم بـإدخال أمر الـPowerShell التالي:

```
New-ADOrganizationalUnit –Path “DC=HSBC,DC=LO” –Name New
```



ثم نقوم بتحويلها عن طريق الأمران

```

Administrator: Windows PowerShell
Copyright (C) 2014 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> redircmp "ou=new,dc=hsbc,dc=lo"
Redirection was successful.
PS C:\Users\Administrator> redirusr "ou=new,dc=hsbc,dc=lo"
Redirection was successful.
PS C:\Users\Administrator>

```

بعدها نقوم بتطبيق الـ GPO المراد استخدامها على الـ OU عن طريق الـ OU

Recycle Bin

ولتفعيلها نقوم بإدخال أمر PowerShell التالي:

```

Administrator: Windows PowerShell
PS C:\Users\Administrator> Enable-ADOptionalFeature 'Recycle Bin Feature' -Scope ForestOrConfigurationSet -Target "HSBC,LO"
WARNING: Enabling 'Recycle Bin Feature' on 'CN=Partitions,CN=Configuration,DC=hsbc,DC=lo' is an irreversible action!
You will not be able to disable 'Recycle Bin Feature' on 'CN=Partitions,CN=Configuration,DC=hsbc,DC=lo' if you proceed.

Confirm
Are you sure you want to perform this action?
Performing the operation "Enable" on target "Recycle Bin Feature".
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "Y"): y
PS C:\Users\Administrator>

```

حيث الـ Scope تحدد مجال الميزة (..... domain, forest و الـ Target تحدد اسم الـ domain, forest التي ستُفعَّل عليها

Backup Server

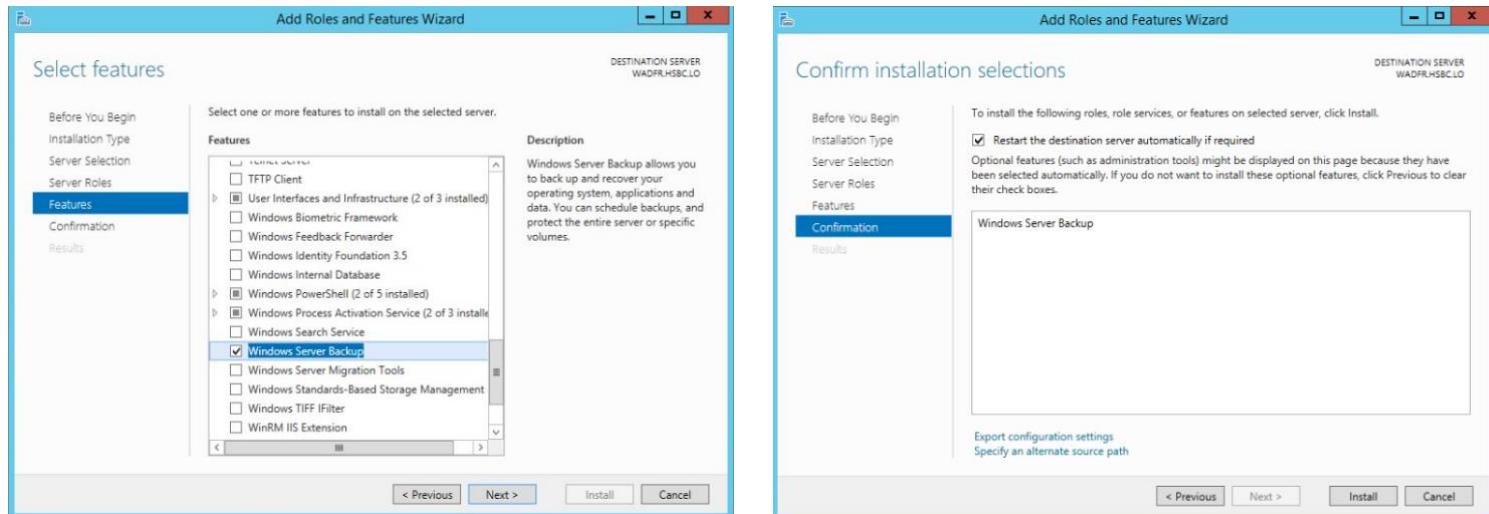


وهي عبارة عن feature يتم تنصيبها على المخدم المُراد إجراء النسخ الاحتياطي له.



تنصيب خدمة النسخ الاحتياطي

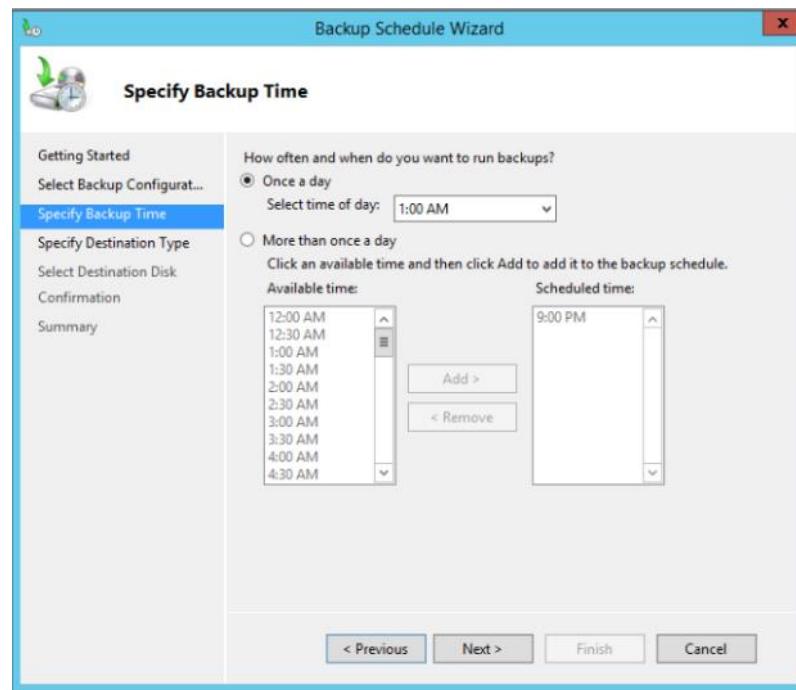
Server Manager → Add roles and features → Windows server backup → install



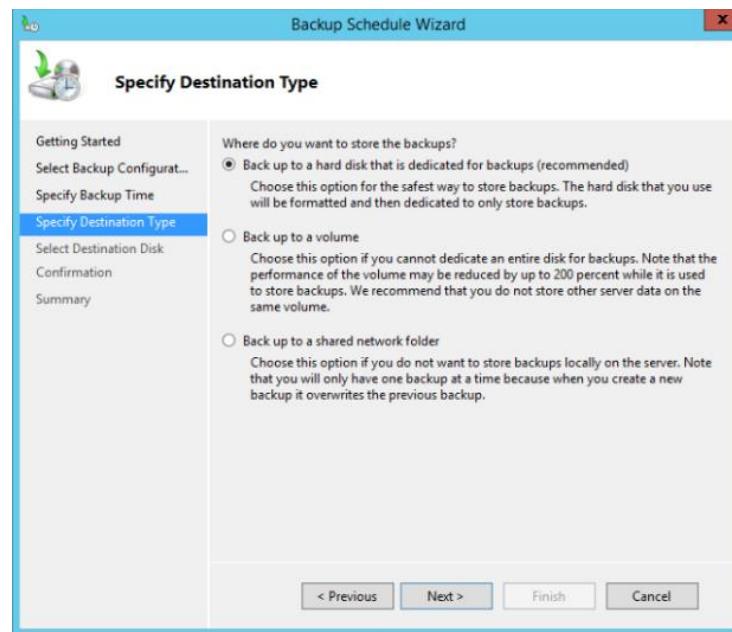
إعداد جدولة النسخ الاحتياطي

Tools → windows server backup → local backup → backup schedule

١- نقوم بتحديد إجراء النسخ لمرة واحدة في اليوم خارج أوقات عمل البنك، لأن عملية النسخ الاحتياطي تؤدي إلى بطيء في أداء المخدم



2- نقوم بتحديد المكان الذي سنحتفظ به بالنسخ الاحتياطية، حيث يوجد ثلاثة خيارات



النسخ الاحتياطي على قرص خاص لعملية النسخ الاحتياطي

النسخ الاحتياطي على قرص عام (غير مخصص للنسخ الاحتياطي)

النسخ الاحتياطي في مكان غير الجهاز المحلي.

قمنا بإجراء النسخ الاحتياطي كما في الخيار الثالث

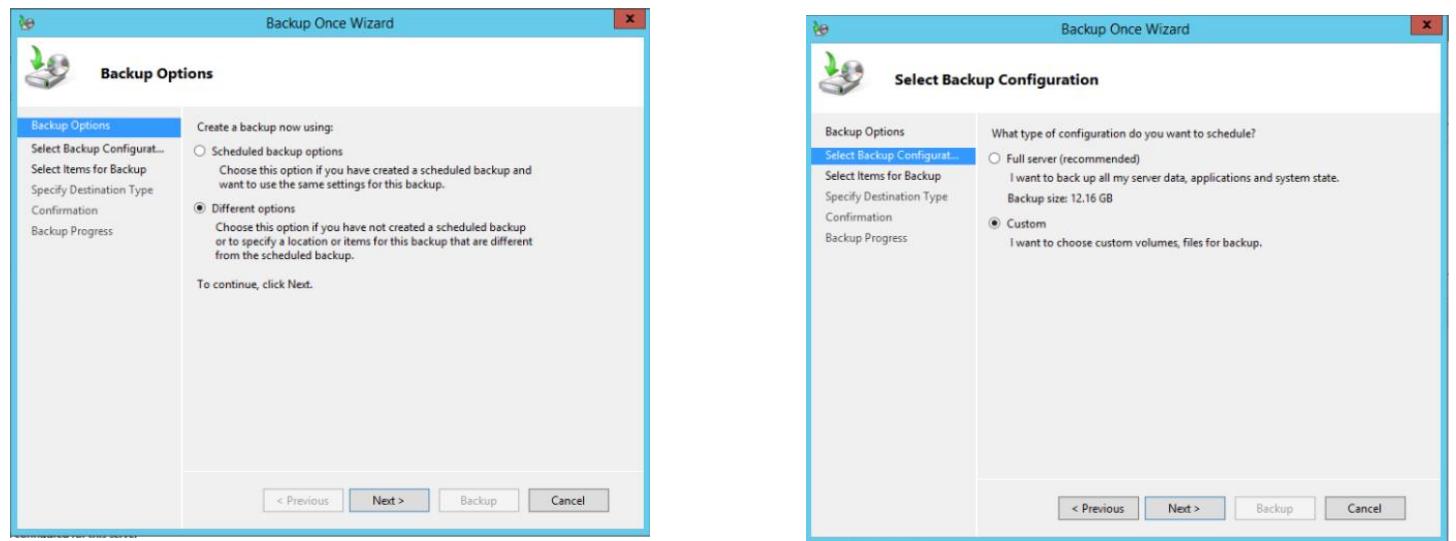
نقوم باختيار اسم الجهاز الذي سنحتفظ فيه بالنسخ الاحتياطي واسم المجلد على الشبكة





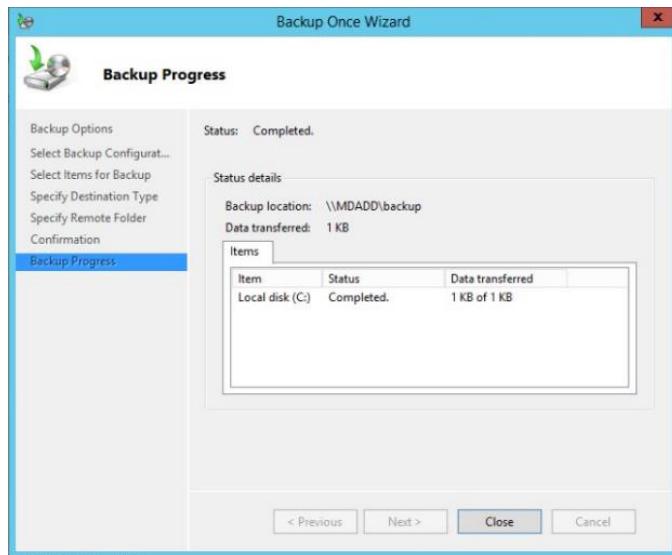
لإجراء النسخ الاحتياطي مباشرة دون الجدولة:

Tools → windows server backup → local backup → backup once



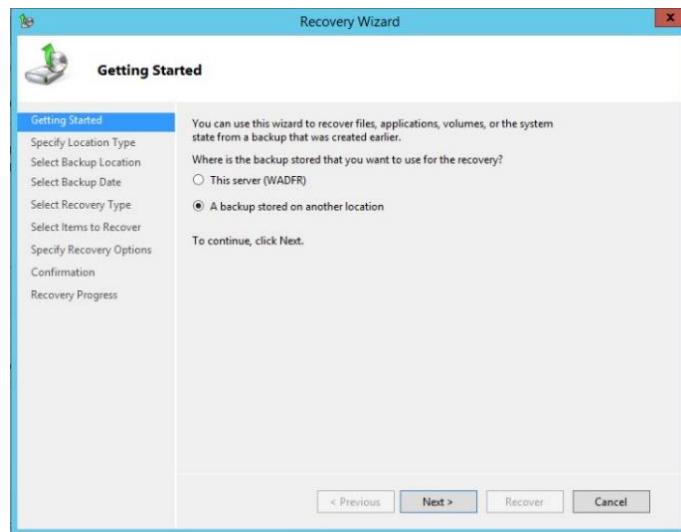
نقوم بالضغط على add items لتحديد العناصر المراد نسخها احتياطيا، ثم تحدد مكان تخزين النسخة المطلوبة

عند انتهاء عملية النسخ الاحتياطي بنجاح تظهر النافذة التالية



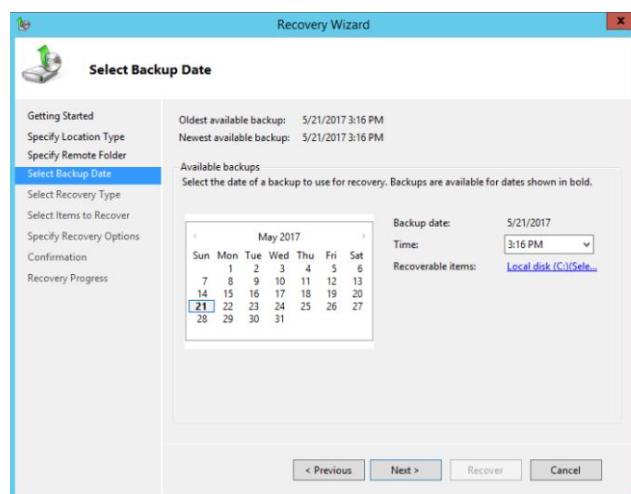
استعادة البيانات

Tools → windows server backup → local backup → recover



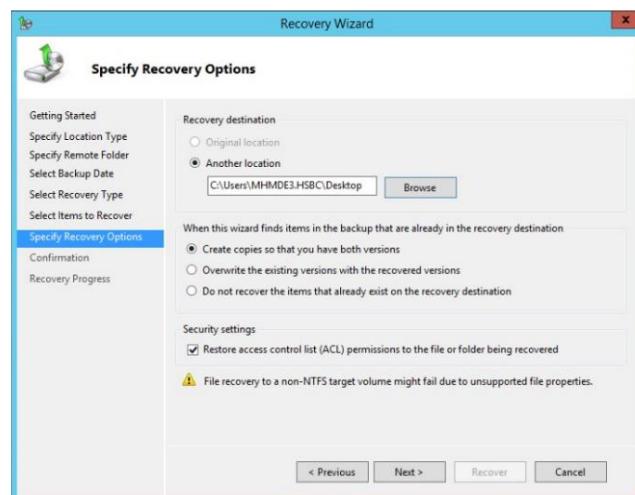
نقوم بتحديد تاريخ النسخة الاحتياطية التي نريد استعادتها

نختار الاستعادة من جهاز بعيد لأننا قمنا بإجراء النسخ على جهاز غير الجهاز المحلي



نقوم بتحديد إذا ما كنا نريد استعادة volume أو مجلد ثم نحدد اسم المجلد الذي نريد استعادته

نقوم بتحديد مكان حفظ المسخة المستعادة من عملية النسخ الاحتياطي



VSS (Volume Shadow copy Service)

- تفعيل VSS على قرص صلب:

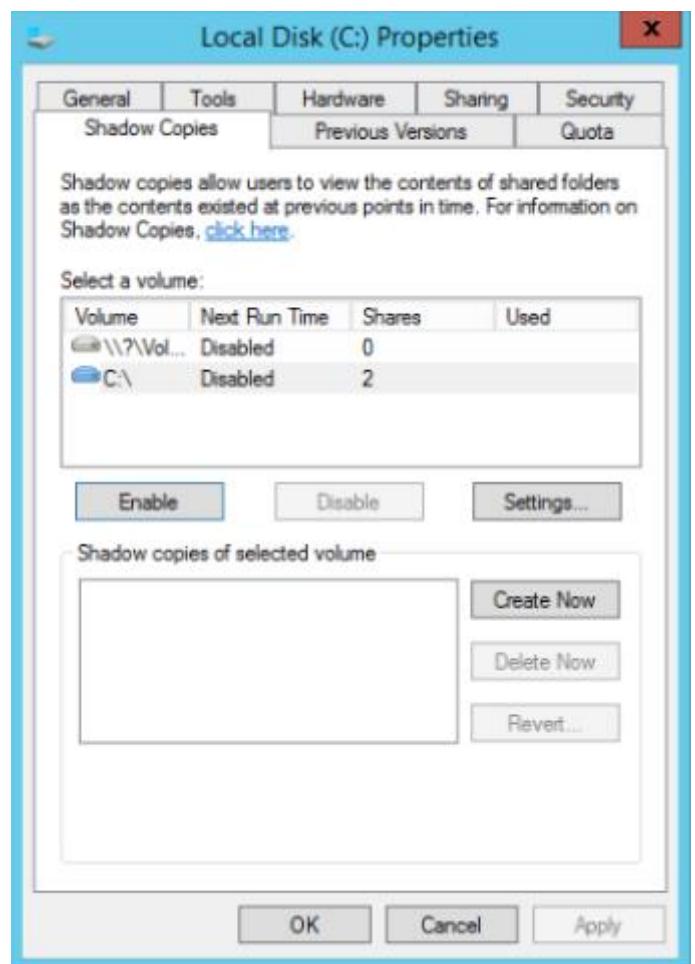
Properties → shadow copies → Enable

- لالتقاط نسخة مباشرة بغض النظر عن الجدولة:

Properties → shadow copies → create new

- لضبط جدول التقاط النسخ الاحتياطية الدورية:

Properties → shadow copies → setting





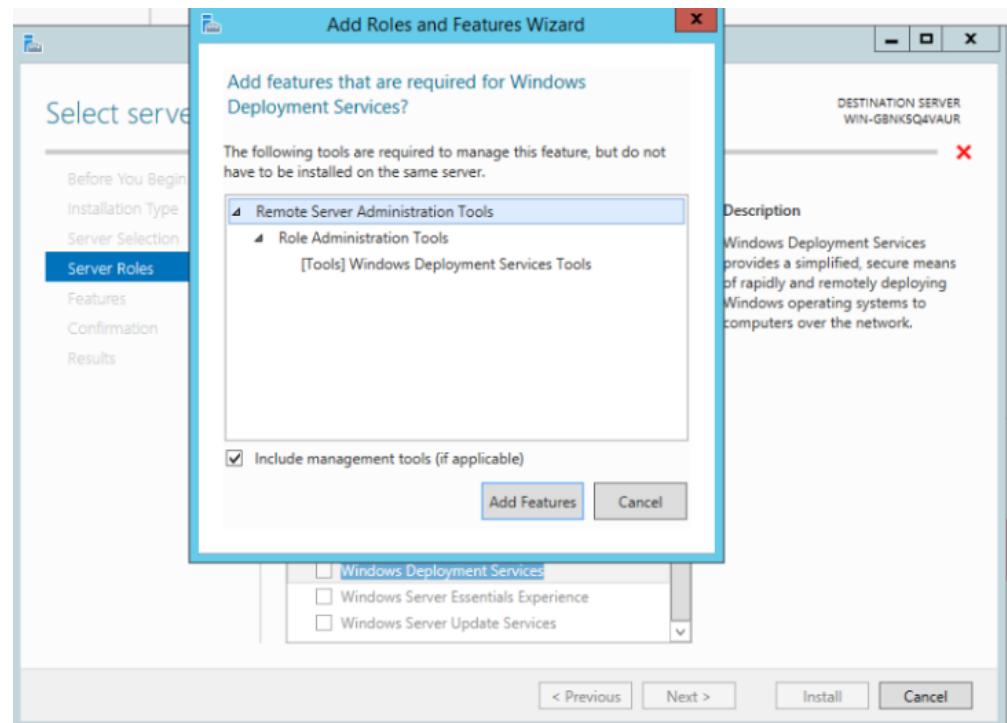
WDS

تعتبر قضية اعداد أجهزة الحاسوب بأنظمة التشغيل المناسبة وتهيئتها عند الحاجة من أهم متطلبات عمل الشبكة، وان القيام بتلك المهمة بشكل يدوي يستهلك الكثير من الوقت والجهد، لذلك قمنا بتنصيب مخدم

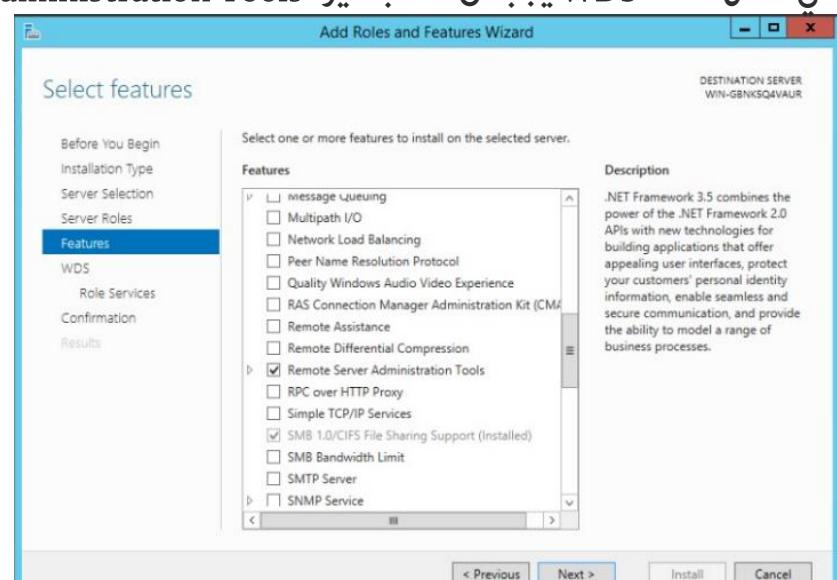
Windows Deployment Services (WDS) والذي سيقوم بعملية توزيع أنظمة تشغيل ويندوز على أجهزة المصرف عن بعد.

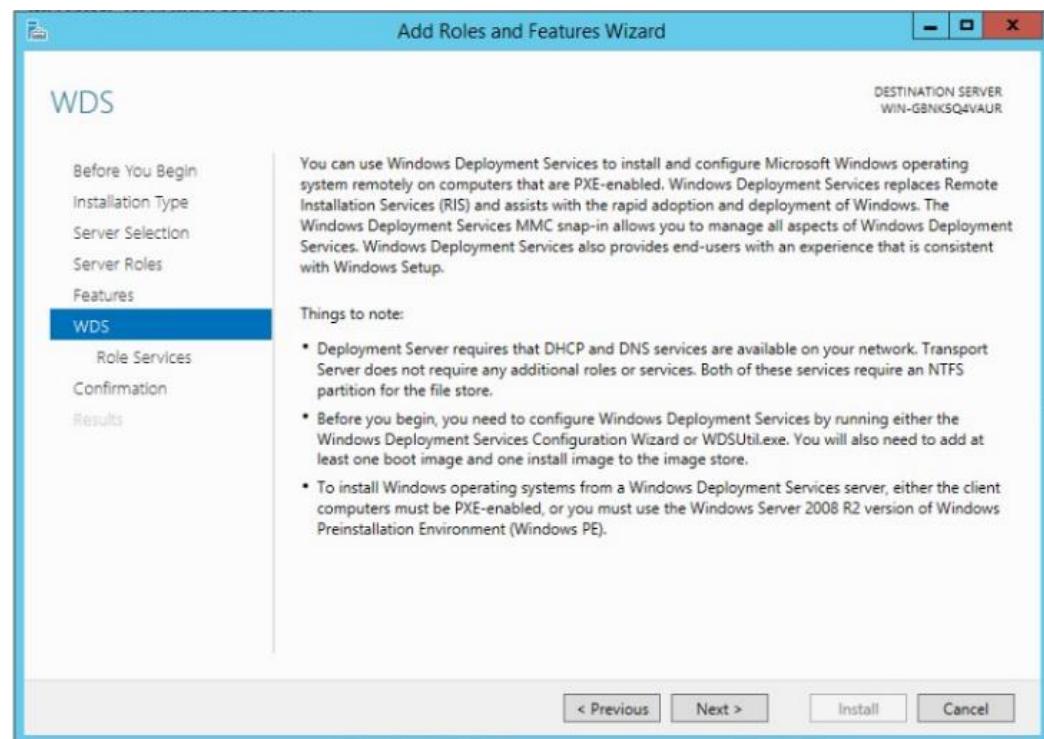
طريقة تنصيب خدمة WDS ضمن أنظمة تشغيل Windows server 2012 R2

Start _ Administrative tools _ Server Manager _ Add Roles and features _ Windows Deployment Services

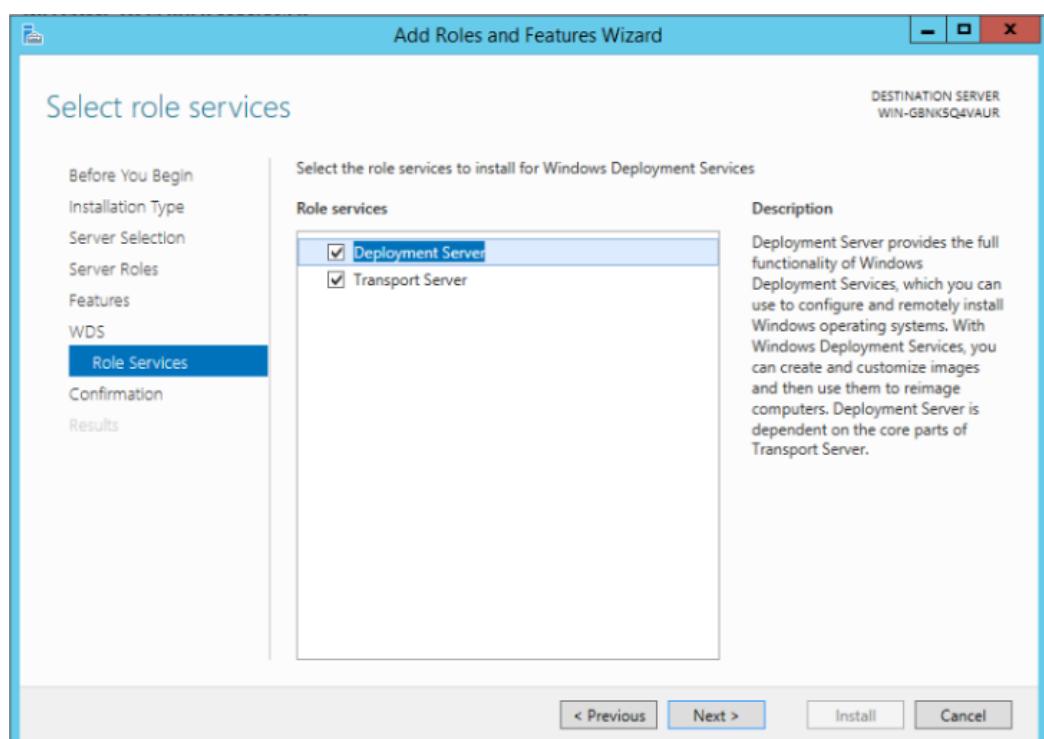


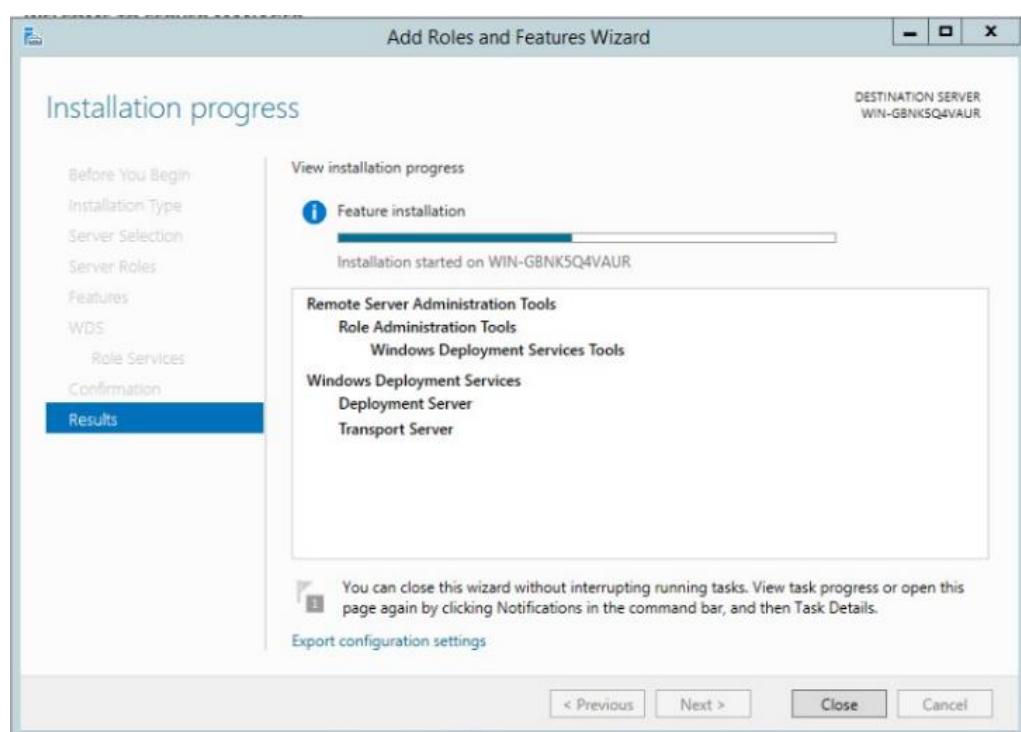
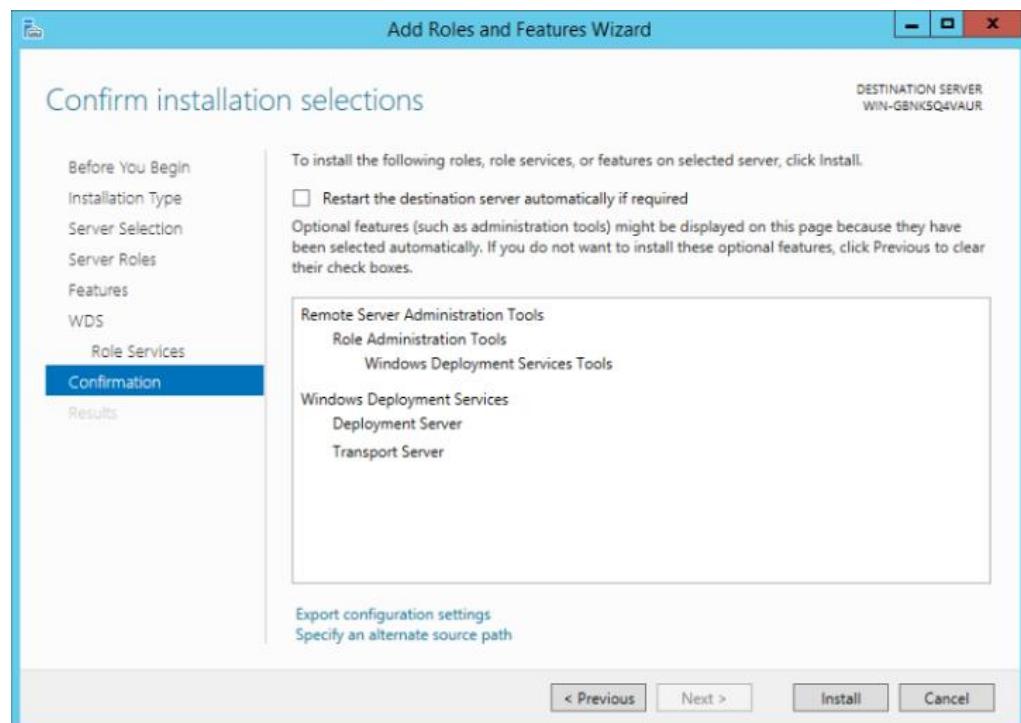
كي تعمل خدمة WDS يجب ان ننصب ميزة Remote Server Administration Tools





نختار :Deployment Server / Transport Server





اكتمال التنصيب.



DAC

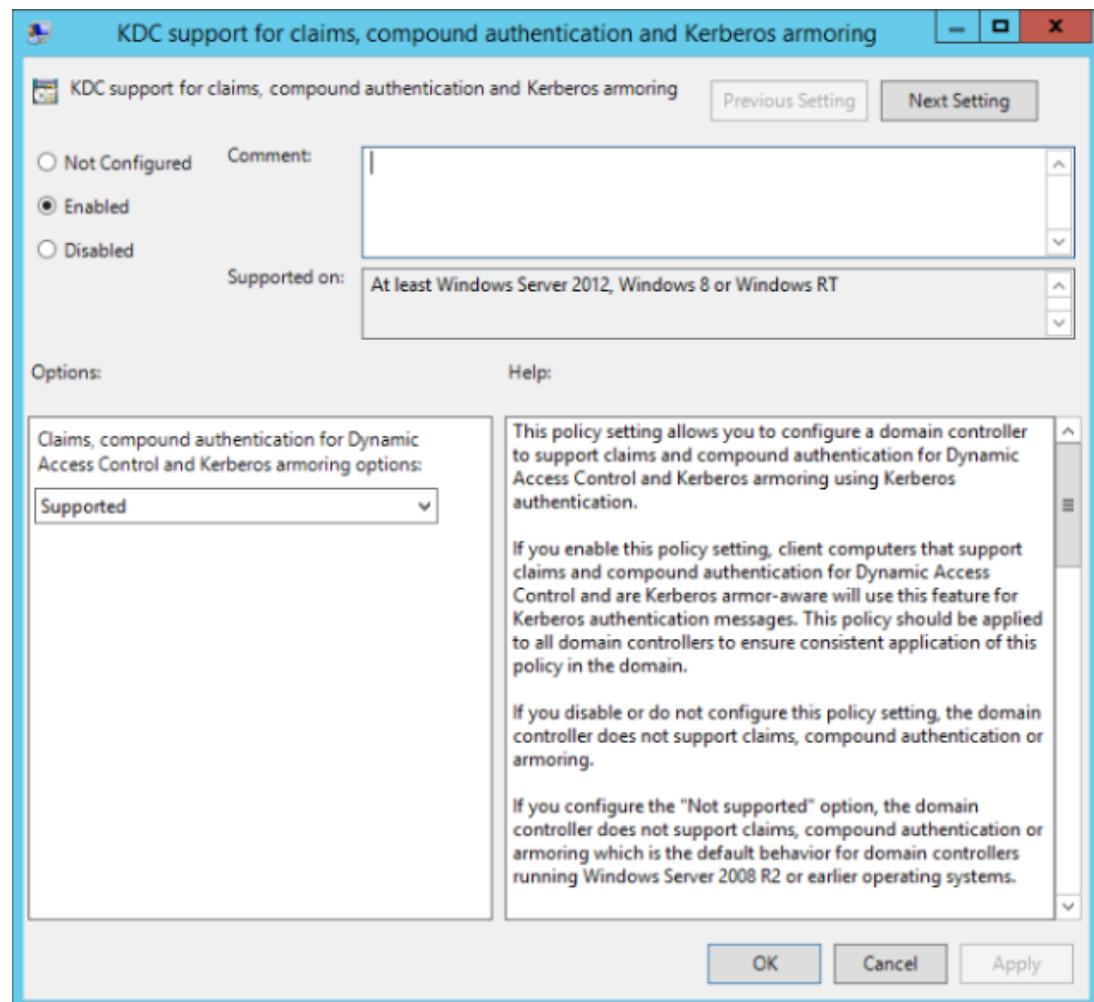
Dynamic Access Control

هي خدمة جديدة أضيفت الى windows server 2012, وهي تمنح تحكم إضافي وأكثر مرونة بالموارد وكيفية الوصول إليها وتساعد على وضع قواعد وصول أكثر دقة الى موارد البيئة.

كيفية اعداد DAC:

Group policy management → Domain controllers → Default domain controller policy → edit → computer → policies → administrative template: policy definition (ADMX files) retrieved from local computer → system → KDC → KDC support for claims

نقوم بتفعيل الخدمة





Create Claim Type: accountExpires

Source Attribute	Display Name	Value Type	Belongs To (CL...)	ID
accountExpires	Integer	user, computer	Account-Expires	
accountName...	Multi-Valued S...	user, computer	Account-Name-History	
aCSPolicyName	String	user, computer	ACS-Policy-Name	
streetAddress	String	user, computer	Address	
homePostalAd...	String	user, computer	Address-Home	
adminCount	Integer	user, computer	Admin-Count	
adminDescripti...	String	user, computer	Admin-Description	
adminDisplayN...	String	user, computer	Admin-Display-Name	

Display name: * accountExpires
Description: Account-Expires

Claims of this type can be issued for the following classes:
 User
 Computer

Set ID to a semantically identical claim type in a trusted forest:
 Protect from accidental deletion

More Information OK Cancel

Create claim

Active directory administrative center → Dynamic access control → new → claim type

- Claim: هي المتطلبات التي يجب ان تكون موجودة لدى المستخدم او الكمبيوتر كي يتمكن من الوصول الى الملف.
1. نقوم بتحديد اسم ال claim
 2. نقوم بتحديد على من ستطبق قاعدة الوصول "مستخدم او كومبيوتر"
 3. نحدد ماهية الصفة التي يجب ان تكون موجودة لدى المستخدم او الكمبيوتر كي يتمكن من الوصول.
- (3) انشاء resource properties

Dynamic access control → resource properties → confidentiality → enable

Create Claim Type: accountExpires

Source Attribute	Display Name	Value Type	Belongs To (CL...)	ID
accountExpires	Integer	user, computer	Account-Expires	
accountName...	Multi-Valued S...	user, computer	Account-Name-History	
aCSPolicyName	String	user, computer	ACS-Policy-Name	
streetAddress	String	user, computer	Address	
homePostalAd...	String	user, computer	Address-Home	
adminCount	Integer	user, computer	Admin-Count	
adminDescripti...	String	user, computer	Admin-Description	
adminDisplayN...	String	user, computer	Admin-Display-Name	

Display name: * accountExpires
Description: Account-Expires

Claims of this type can be issued for the following classes:
 User
 Computer

Set ID to a semantically identical claim type in a trusted forest:
 Protect from accidental deletion

More Information OK Cancel



create central access role

من واجهة DAC

New → central access policy

Create Central Access Policy:

General

Name: *

Description:

Protect from accidental deletion

Member Central Access Rules

Name	Permissions St...

Add... Remove

OK Cancel

1. تحديد اسم central access policy
2. تحديد الملفات او المجلدات التي ستطبق عليها القاعدة.

ثم نقوم بتحديد السماحيات على المجلد الهدف

Permission Entry for Current Permissions

Principal: IT (HSBCIT) Select a principal

Type: Allow

Basic permissions:

Full Control
 Modify
 Read and Execute
 Read
 Write
 Special permissions

Show advanced permissions

Add a condition to limit access. The principal will be granted the specified permissions only if conditions are met.

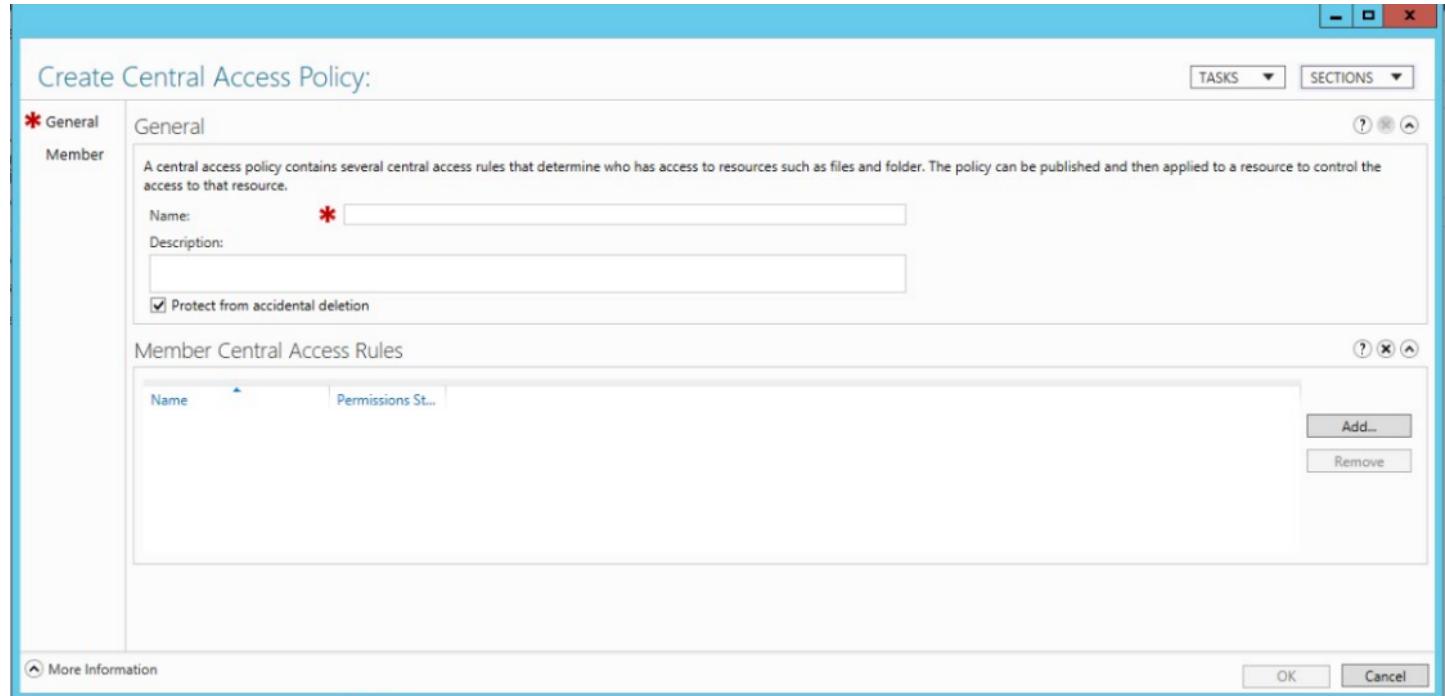
User Group Not member of any Value 2 item(s) selected Add items Remove

Add a condition

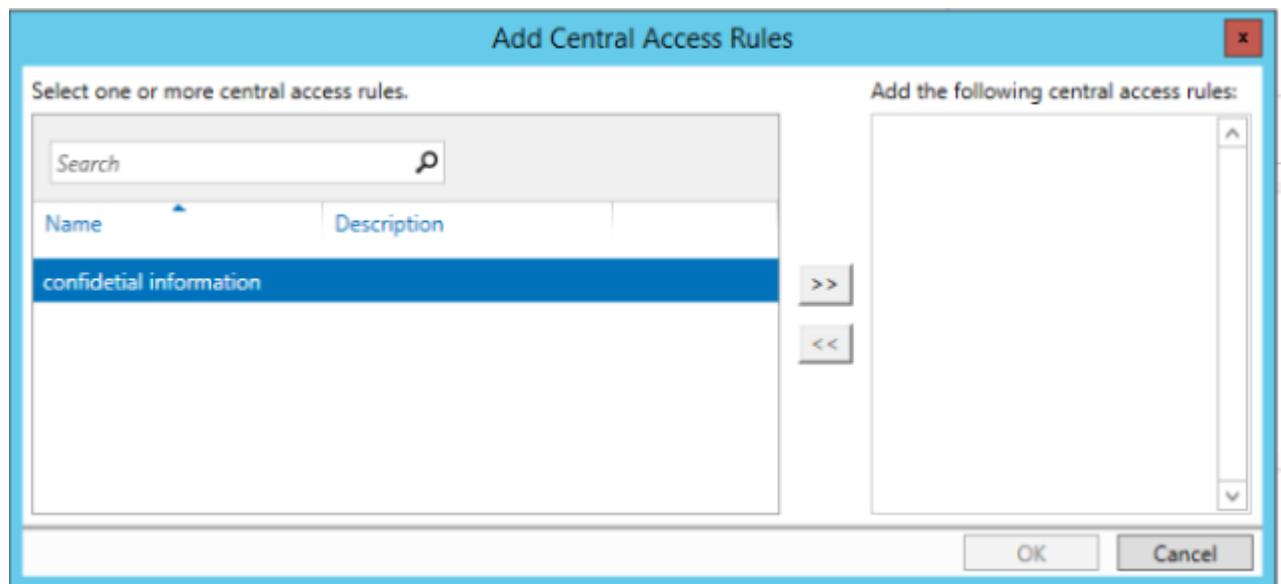
OK Cancel

إنشاء central access policy

Dynamic access control → central access policy → new → central access policy

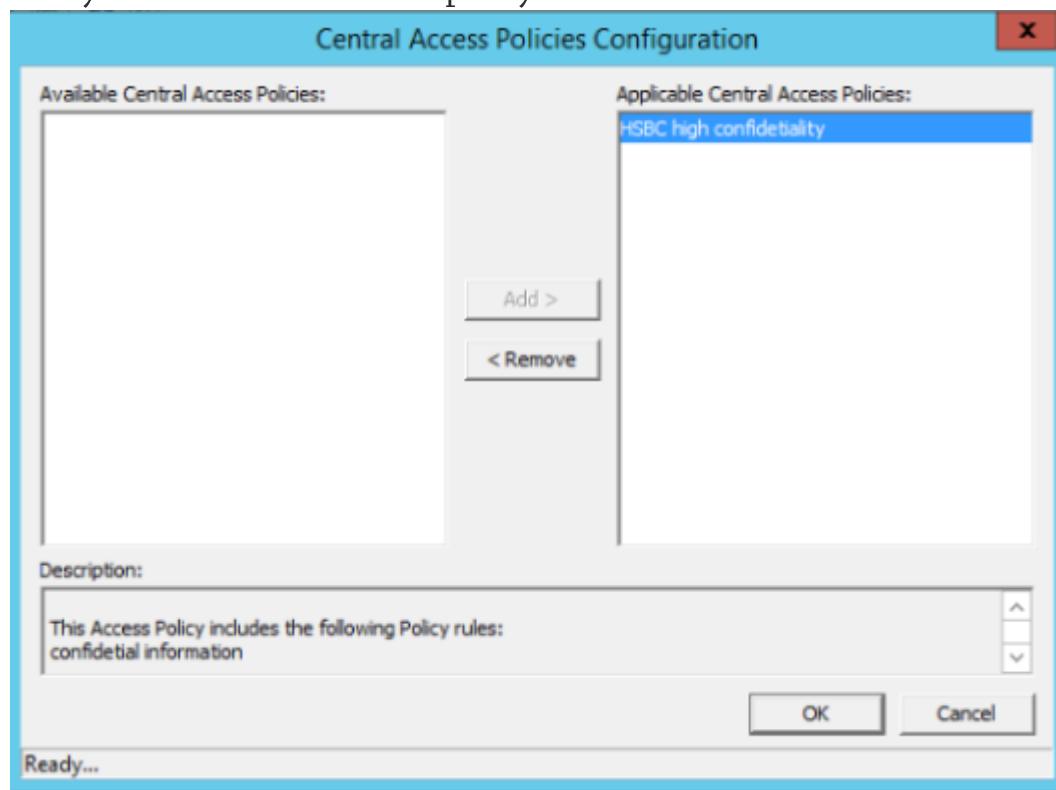


- .1 .نحدد اسم central access policy
- .2 .نقوم بإضافة central access role التي أنشأناها سابقا





Group policy management → default domain policy → policy → windows settings → security settings → file system → central access policy



ADCSs Active Directory Certificate Services

Certificate Authority



ضمن أي مؤسسة تحتاج الى جهة تقوم بتوثيق كل من الـ emails، computers، users، servers وتحتى صفحة الانترنت الخاصة بالشركة.



لتقدیم خدمة التوثیق قمنا بتنصیب Certificate Server ليقوم بتوثیق جميع الموارد المذکورة، ويكون هو مرجع الشهادات الخاص بـ HSBC.

تم العمل على الخدمة المقدمة من Microsoft وهي ADCS ما هو Certificate Authority؟

هو الجهة الموثوقة المانحة للشهادات ضمن المؤسسة، وهو جهاز كومبيوتر يعمل بأحد أنظمة تشغيل windows وتم تثبيت خدمة ADCS server عليه.

ما هي محتويات الشهادة وكيف يمكن الاستفادة منها؟

تحتوي الشهادة على اسم المشترك ورقم الهوية الخاصة به وتاريخ المنح وتاريخ انتهاء الصلاحية، ويتم توقيع الشهادة بمقتني خاص private key ، يستفاد من الشهادة في عمليات التشفير والتوثيق.

ما تتألف هرمية CA؟

1_root CA

2_subordinate CA

يكون الـ root هو رأس الهرم وهو أول CA يتم إنشاؤه، أما subordinate CA فهو خيار إضافي ويوجد العديد من الأسباب لاستخدامه :

1. استخدام الشهادات لأغراض مختلفة مثل توثيق مخدم web وتوثيق الزبائن، الخ... وبالتالي يمكن فصل الـ CA لهذا الغرض.

2. توزيع الحمل

3. التوزع الجغرافي

4. تأمين الاتاحية العالية high availability

عند تطبيق الـ CA ضمن بيئة معينة يوجد خيارات :

• Internal private CA

• External public CA

لتوسيع الفرق بينهما: يوجد العديد من المؤسسات العالمية التجارية المانحة للشهادات الرقمية، ويمكنني كزبون ان أقدم طلب حصول على شهادة رقمية من احدى هذه المؤسسات لغرض ما، وأقدم المعلومات المتعلقة بالشهادة وما هييتها ومدى أهميتها، أي سأقوم بالاعتماد على جهة خارجية للتوثيق، كل جهاز حاسوب يحتوي مسبقاً على قائمة بهذه المؤسسات العالمية والتي سيثق بالجهاز او الزبون الذي يحمل شهادة من احدى هذه المؤسسات، وبالتالي لا أقوم بإدارة هذه الشهادات انما اكتفي بطلبها فقط.

اما عند العمل على internal private CA فلو قمت مثلاً بتصميم موقع على الانترنت ومنته شهادة ثقة من CA داخلي خاص فان هذا الموقع سيكون موثوقاً بالنسبة لأعضاء المؤسسة التابعة لي ولن يكون موثوقاً خارجها.

اما مميزات كل منهما فان تكلفة الحصول على شهادة داخلية اقل من تكلفة الحصول على شهادة خارجية، كما يمكنني إدارة الشهادة الممنوحة داخلياً ولا أستطيع إدارة الشهادة الممنوحة من طرف خارجي.

عند إنشاء CA داخلي خاص امامنا خيارات لإتمام العمل:

1. Standalone

2. Enterprise



اما ال standalone فهو جهاز حاسوب تم تثبيت خدمة ADCS عليه ويستخدم لمن الشهادات ويعمل بشكل مستقل عن ADDS أي انه لا يكون عضوا في نطاق ما (domain)

Aهم الفوارق بين: Standalone & Enterprise

1) Standalone: لا يوجد به group policy أي لا نستطيع تطبيق trusted root propagation, بإصدار شهادة داخلية تكون باقي الأجهزة ضمن المؤسسة لا تعلم بها، وبالتالي لا نستطيع استخدام ال group policy لنشر القوائم الموثوقة بينما استطيع استخدامها في enterprise وبالتالي فإنني اخبر العملاء بان الشهادات الممنوعة من قبل موثوقة.

2) enterprise CA وهي خدمة موجودة ضمن CA Publishes Certificates and URLs to ADDS: يوجد لديه قائمة بالشهادات التي تم رفضها، ويقوم العملاء بالتحقق من هذه القوائم بأنهم عندما يحصلون على هذه الشهادات بأنها مازالت صالحة او لا، ويمكن نشر هذه القوائم بين أجهزة المؤسسة عن طريق ADDS و تكون هذه القائمة بعكس قائمة الشهادات الصالحة.

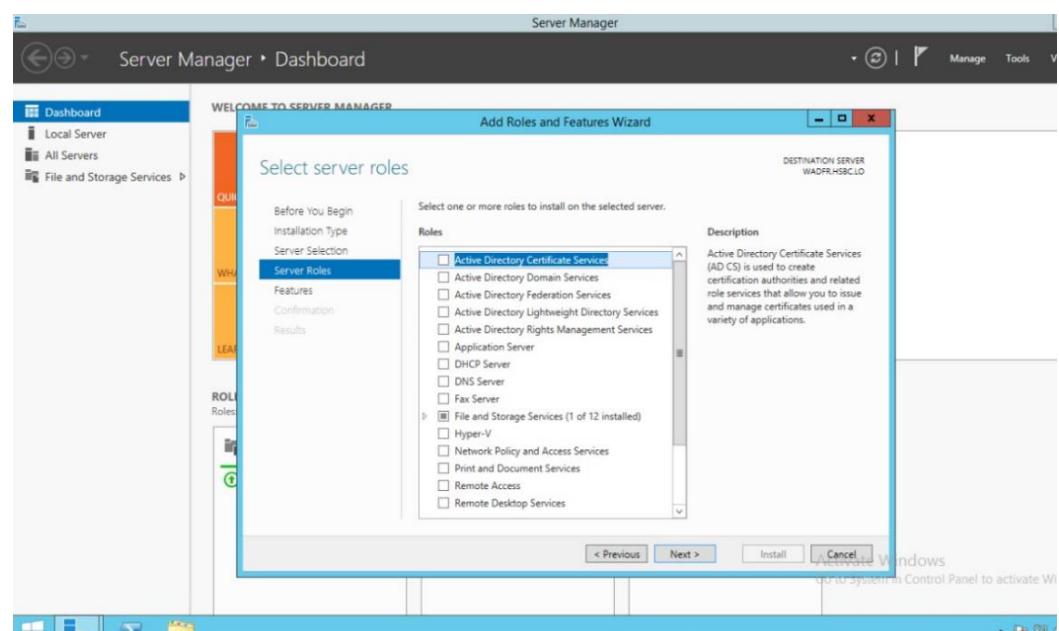
3) Can enforce credential check during enrollment: وهي خدمة تمكّنني من التحقق من شخصية من يطلب الشهادة قبل منحها له.

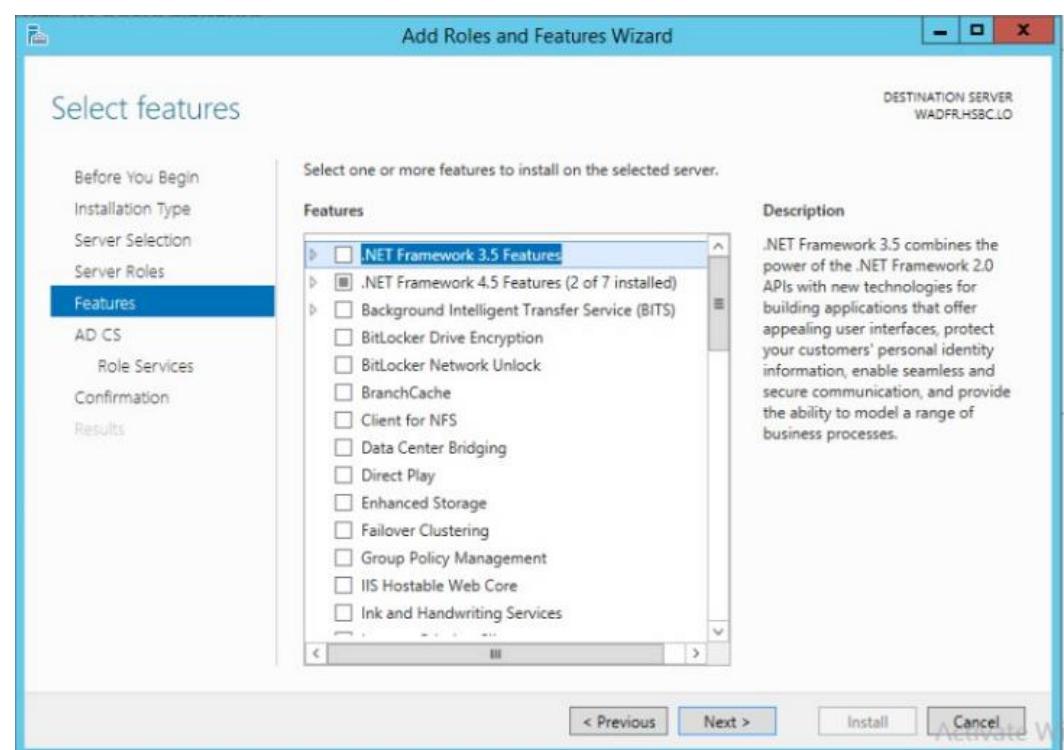
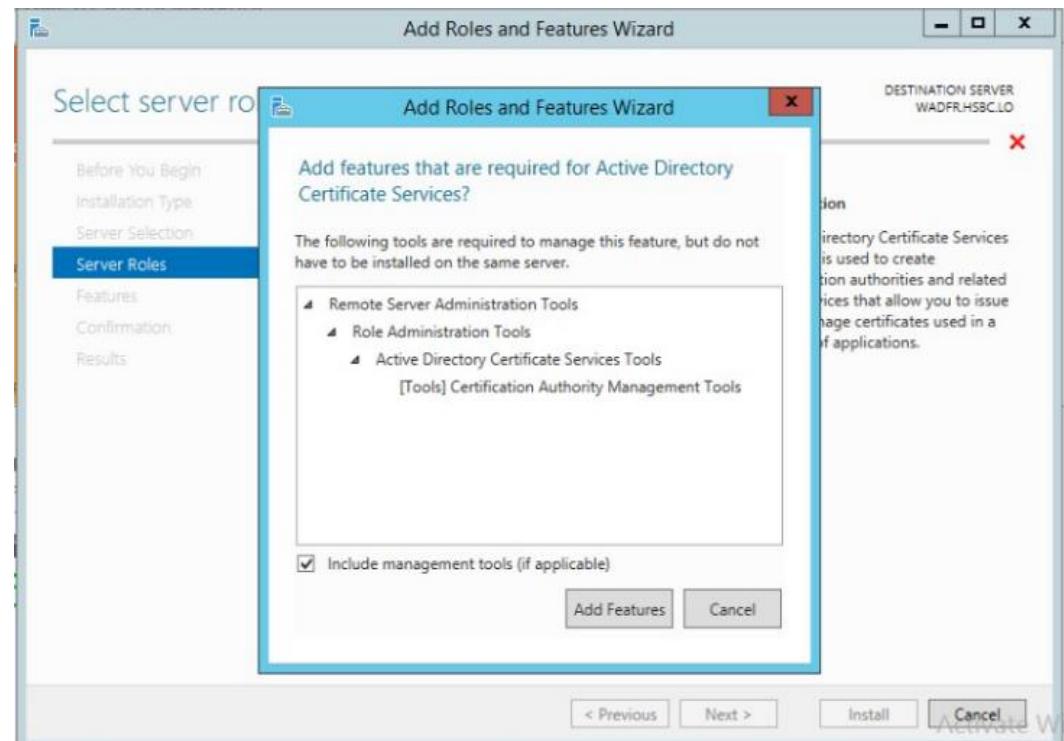
4) Can have subject name generated automatically from logon credentials: وهي ميزة تسمح بإنشاء subject name يولد تلقائيا عند منح الشهادة، أي ان الاسم الذي سيصبح صالحا يجب ان يتواافق مع name الخاص بالشهادة.

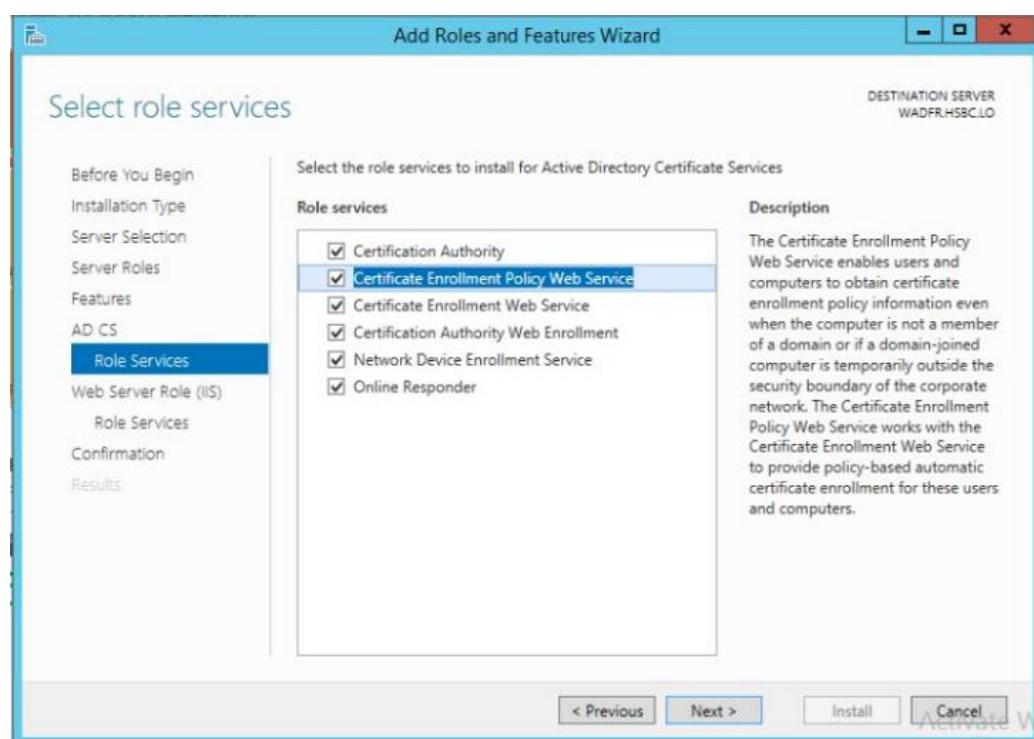
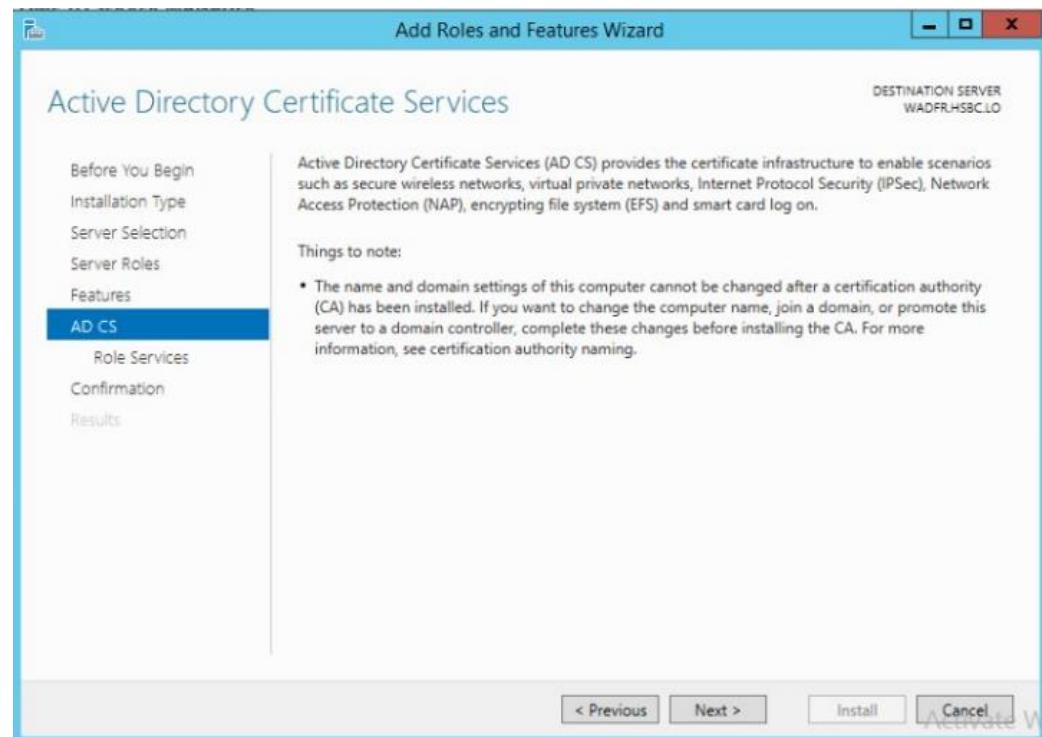
5) Can use certificate template: وهي قوالب محدّدة مسبقاً ضمن CA و يقوم ال admin بإدارتها و تعديلها و منها للمستخدمين.

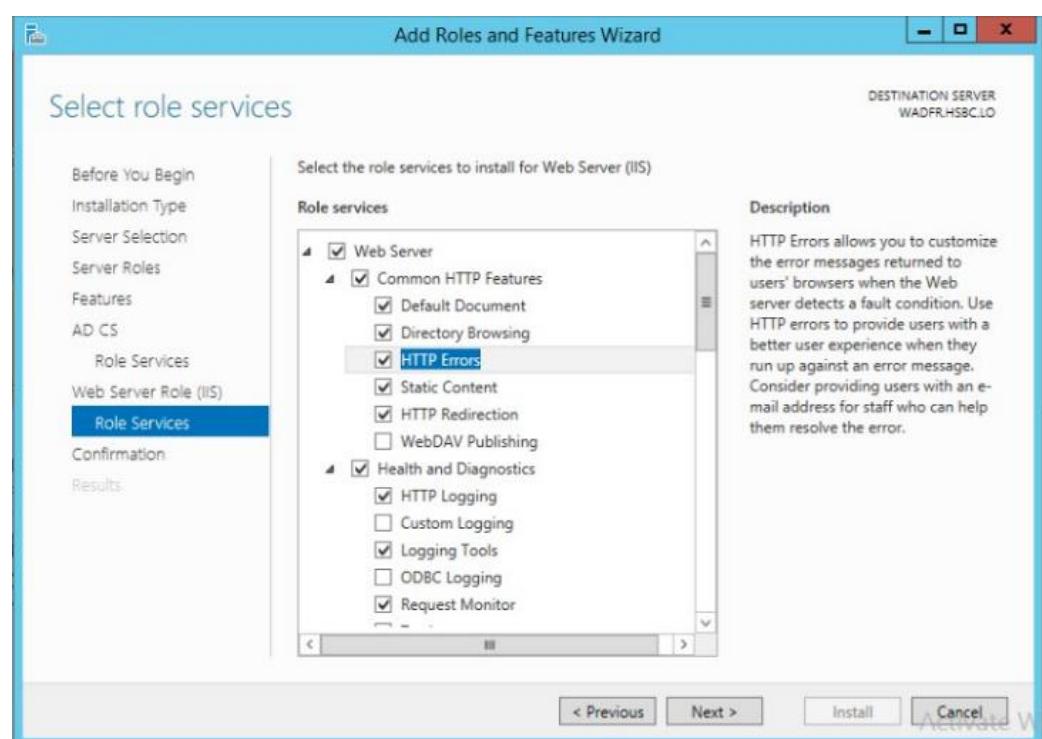
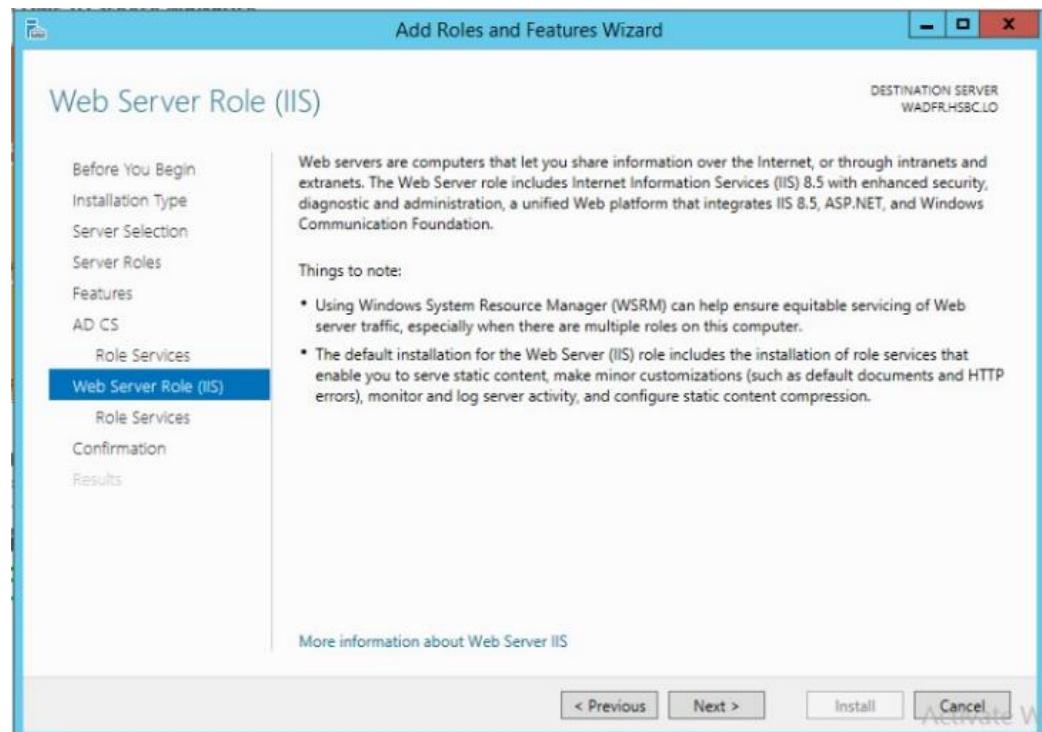
6) Can be used to generate smart card windows domain authentication certificates: توجد فقط online CA وتمكن من المنح التلقائي للشهادة، كمثال: يمكن تعين بانه حالما يصبح جهاز الحاسوب فإنه يحصل على شهادة تلقائية لأي غرض يحتاجه.

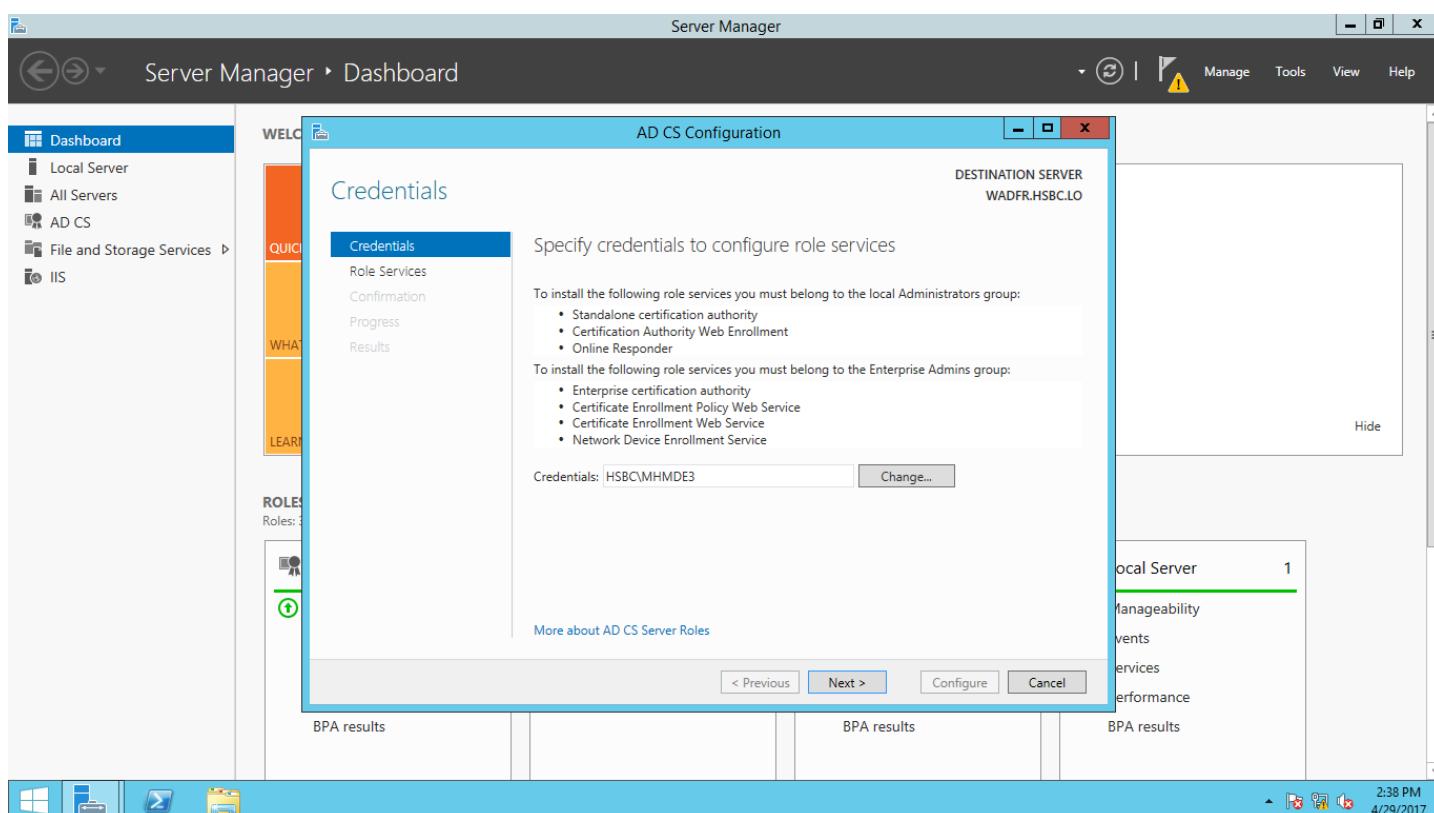
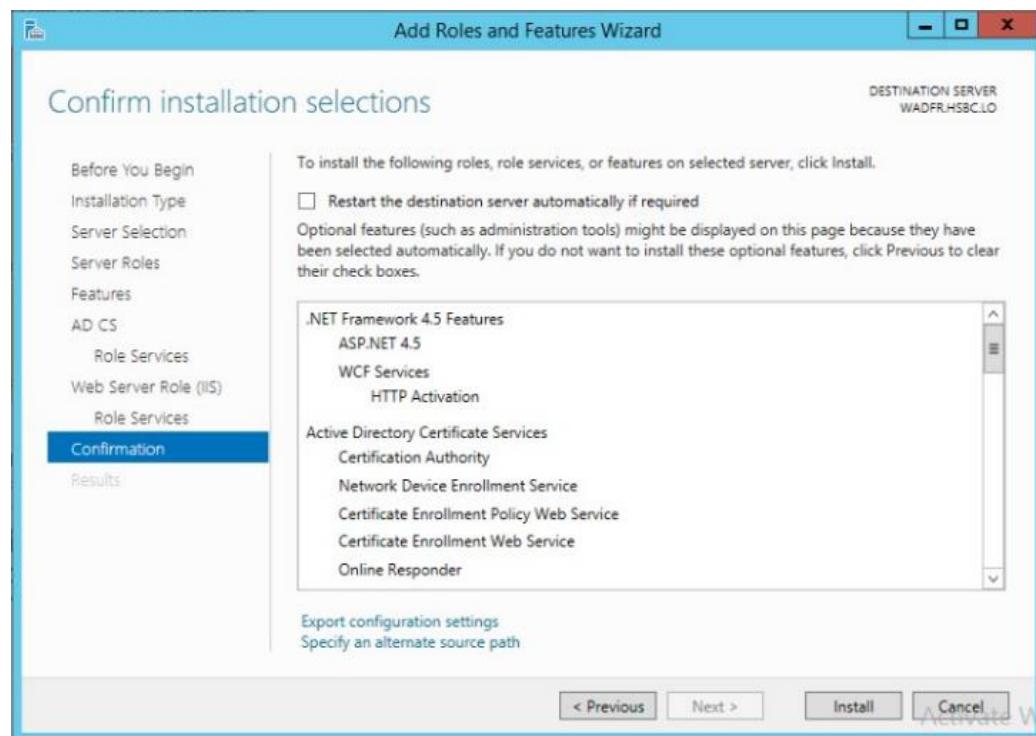
Configuration













Server Manager

Server Manager > Dashboard

AD CS Configuration

Role Services

DESTINATION SERVER
WADFR.HSBC.LO

Select Role Services to configure

Credentials

Certification Authority

Certification Authority Web Enrollment

Online Responder

Network Device Enrollment Service

Certificate Enrollment Web Service

Certificate Enrollment Policy Web Service

More about AD CS Server Roles

< Previous Next > Configure Cancel

BPA results BPA results BPA results BPA results

Local Server 1

Manageability Events Services Performance

2:39 PM 4/29/2017

Server Manager

Server Manager > Dashboard

AD CS Configuration

Setup Type

DESTINATION SERVER
WADFR.HSBC.LO

Specify the setup type of the CA

Credentials

Role Services

Setup Type

CA Type

Private Key

Cryptography

CA Name

Validity Period

Certificate Database

Confirmation

Progress

Results

Enterprise certification authorities (CAs) can use Active Directory Domain Services (AD DS) to simplify the management of certificates. Standalone CAs do not use AD DS to issue or manage certificates.

Enterprise CA
Enterprise CAs must be domain members and are typically online to issue certificates or certificate policies.

Standalone CA
Standalone CAs can be members or a workgroup or domain. Standalone CAs do not require AD DS and can be used without a network connection (offline).

More about Setup Type

< Previous Next > Configure Cancel

BPA results BPA results BPA results BPA results

Local Server 1

Manageability Events Services Performance

2:39 PM 4/29/2017



Server Manager

Server Manager > Dashboard

WELCOME TO SERVER MANAGER

Dashboard Local Server All Servers AD CS File and Storage Services IIS

QUICK START WADFR.HSBC.LO LEARN MORE ROLES Roles: 3

CA Type

DESTINATION SERVER WADFR.HSBC.LO

Specify the type of the CA

When you install Active Directory Certificate Services (AD CS), you are creating or extending a public key infrastructure (PKI) hierarchy. A root CA is at the top of the PKI hierarchy and issues its own self-signed certificate. A subordinate CA receives a certificate from the CA above it in the PKI hierarchy.

Root CA
Root CAs are the first and may be the only CAs configured in a PKI hierarchy.

Subordinate CA
Subordinate CAs require an established PKI hierarchy and are authorized to issue certificates by the CA above them in the hierarchy.

More about CA Type

< Previous Next > Configure Cancel

BPA results BPA results BPA results BPA results

local Server 1 Manageability Events Services Performance

2:39 PM 4/29/2017

Server Manager

Server Manager > Dashboard

WELCOME TO SERVER MANAGER

Dashboard Local Server All Servers AD CS File and Storage Services IIS

QUICK START WADFR.HSBC.LO LEARN MORE ROLES Roles: 3

Private Key

DESTINATION SERVER WADFR.HSBC.LO

Specify the type of the private key

To generate and issue certificates to clients, a certification authority (CA) must have a private key.

Create a new private key
Use this option if you do not have a private key or want to create a new private key.

Use existing private key
Use this option to ensure continuity with previously issued certificates when reinstalling a CA.

Select a certificate and use its associated private key
Select this option if you have an existing certificate on this computer or if you want to import a certificate and use its associated private key.

Select an existing private key on this computer
Select this option if you have retained private keys from a previous installation or want to use a private key from an alternate source.

More about Private Key

< Previous Next > Configure Cancel

BPA results BPA results BPA results BPA results

local Server 1 Manageability Events Services Performance

2:39 PM 4/29/2017



Server Manager

Server Manager > Dashboard

WELCOME TO SERVER MANAGER

Dashboard Local Server All Servers AD CS File and Storage Services IIS

QUICK START WHAT'S NEW LEARN MORE ROLES Roles: 3

Cryptography for CA

AD CS Configuration

DESTINATION SERVER: WADFR.HSBC.LO

Specify the cryptographic options

Select a cryptographic provider: RSA#Microsoft Software Key Storage Provider Key length: 2048

Select the hash algorithm for signing certificates issued by this CA:

- SHA256
- SHA384
- SHA512
- SHA1
- MD5

Allow administrator interaction when the private key is accessed by the CA.

More about Cryptography

< Previous Next > Configure Cancel

BPA results BPA results BPA results BPA results

local Server 1 Manageability Events Services Performance

2:39 PM 4/29/2017

Server Manager

Server Manager > Dashboard

WELCOME TO SERVER MANAGER

Dashboard Local Server All Servers AD CS File and Storage Services IIS

QUICK START WHAT'S NEW LEARN MORE ROLES Roles: 3

CA Name

AD CS Configuration

DESTINATION SERVER: WADFR.HSBC.LO

Specify the name of the CA

Type a common name to identify this certification authority (CA). This name is added to all certificates issued by the CA. Distinguished name suffix values are automatically generated but can be modified.

Common name for this CA: HSBC-WADFR-CA

Distinguished name suffix: DC=HSBC,DC=LO

Preview of distinguished name: CN=HSBC-WADFR-CA,DC=HSBC,DC=LO

More about CA Name

< Previous Next > Configure Cancel

BPA results BPA results BPA results BPA results

local Server 1 Manageability Events Services Performance

2:39 PM 4/29/2017



Server Manager

Server Manager > Dashboard

AD CS Configuration

Validity Period

DESTINATION SERVER
WADFR.HSBC.LO

Specify the validity period

Select the validity period for the certificate generated for this certification authority (CA):
1 Years

CA expiration Date: 4/29/2018 2:39:00 PM

The validity period configured for this CA certificate should exceed the validity period for the certificates it will issue.

< Previous Next > Configure Cancel

BPA results BPA results BPA results

More about Validity Period

Local Server 1 Manageability events services performance

2:40 PM 4/29/2017

Server Manager

Server Manager > Dashboard

AD CS Configuration

CA Database

DESTINATION SERVER
WADFR.HSBC.LO

Specify the database locations

Certificate database location:
C:\Windows\system32\CertLog

Certificate database log location:
C:\Windows\system32\CertLog

< Previous Next > Configure Cancel

BPA results BPA results BPA results

More about CA Database

Local Server 1 Manageability events services performance

2:40 PM 4/29/2017



Server Manager

Server Manager ▶ Dashboard

Dashboard Local Server All Servers AD CS File and Storage Services IIS

WELCOME TO SERVER MANAGER

QUICK START LEARN MORE

ROLES Roles: 3

Progress Results

AD CS Configuration

Confirmation

DESTINATION SERVER WADFR.HSBC.LO

To configure the following roles, role services, or features, click Configure.

Active Directory Certificate Services

Certification Authority

CA Type:	Enterprise Root
Cryptographic provider:	RSA#Microsoft Software Key Storage Provider
Hash Algorithm:	SHA1
Key Length:	2048
Allow Administrator Interaction:	Disabled
Certificate Validity Period:	4/29/2018 2:39:00 PM
Distinguished Name:	CN=HSBC-WADFR-CA,DC=HSBC,DC=LO
Certificate Database Location:	C:\Windows\system32\CertLog
Certificate Database Log Location:	C:\Windows\system32\CertLog

Certification Authority Web Enrollment

Online Responder

< Previous Next > Configure Cancel

BPA results BPA results BPA results

local Server 1 Manageability events services performance

2:41 PM 4/29/2017

Server Manager

Server Manager ▶ Dashboard

Dashboard Local Server All Servers AD CS File and Storage Services IIS

WELCOME TO SERVER MANAGER

QUICK START LEARN MORE

ROLES Roles: 3

Progress Results

AD CS Configuration

Results

DESTINATION SERVER WADFR.HSBC.LO

The following roles, role services, or features were configured:

Active Directory Certificate Services

Certification Authority More about CA Configuration	Configuration succeeded
Certification Authority Web Enrollment More about Web Enrollment Configuration	Configuration succeeded
Online Responder More about OCSP Configuration	Configuration succeeded

< Previous Next > Close Cancel

BPA results BPA results BPA results

local Server 1 Manageability events services performance

2:41 PM 4/29/2017



Screenshot of the Windows Administrative Tools - Certificates (Local) window.

The left pane shows a tree view with the root "Certification Authority (Local)" expanded, showing "HSBC-WADFR-CA" which has subfolders: "Revoked Certificates", "Issued Certificates", "Pending Requests", "Failed Requests", and "Certificate Templates".

The right pane displays a table with one entry:

Name	Description
HSBC-WADFR-CA	Certification Authority

Screenshot of the Local Group Policy Editor window.

The left pane shows the navigation tree under "Computer Configuration" and "User Configuration".

The right pane shows the "Object Type" section with three policy entries: "Certificate Services Client - Certificate Enrollment Policy", "Certificate Services Client - Credential Roaming", and "Certificate Services Client - Auto-Enrollment".

A detailed configuration dialog box is open for "Certificate Services Client - Auto-Enrollment Pr...".

Enrollment Policy Configuration

Enroll user and computer certificates automatically

Configuration Model: Enabled

Renew expired certificates, update pending certificates, and remove revoked certificates

Update certificates that use certificate templates

Log expiry events and show expiry notifications when the percentage of remaining certificate lifetime is

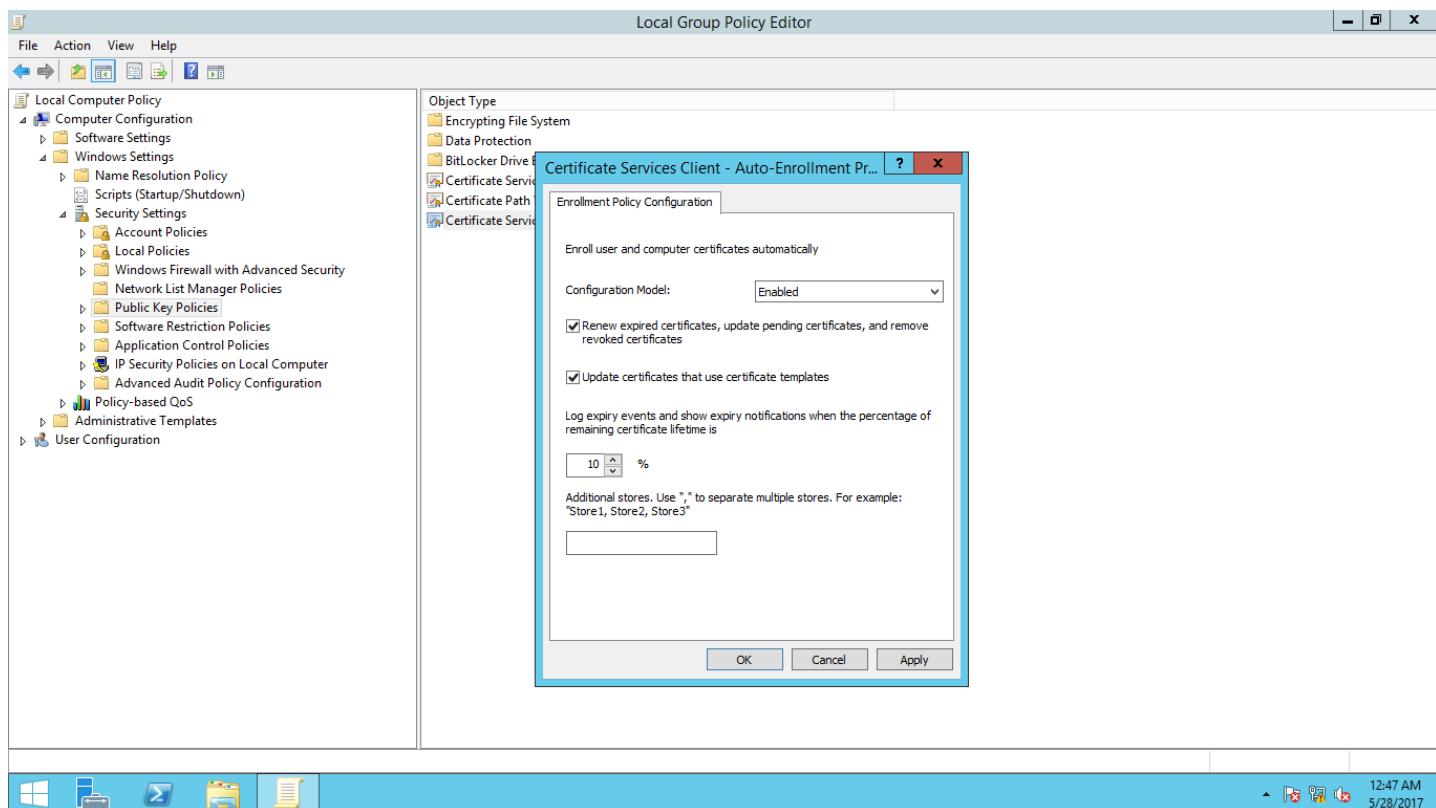
10 %

Additional stores. Use "*" to separate multiple stores. For example: "Store1, Store2, Store3"

MY store

Display user notifications for expiring certificates in user and machine

OK Cancel Apply



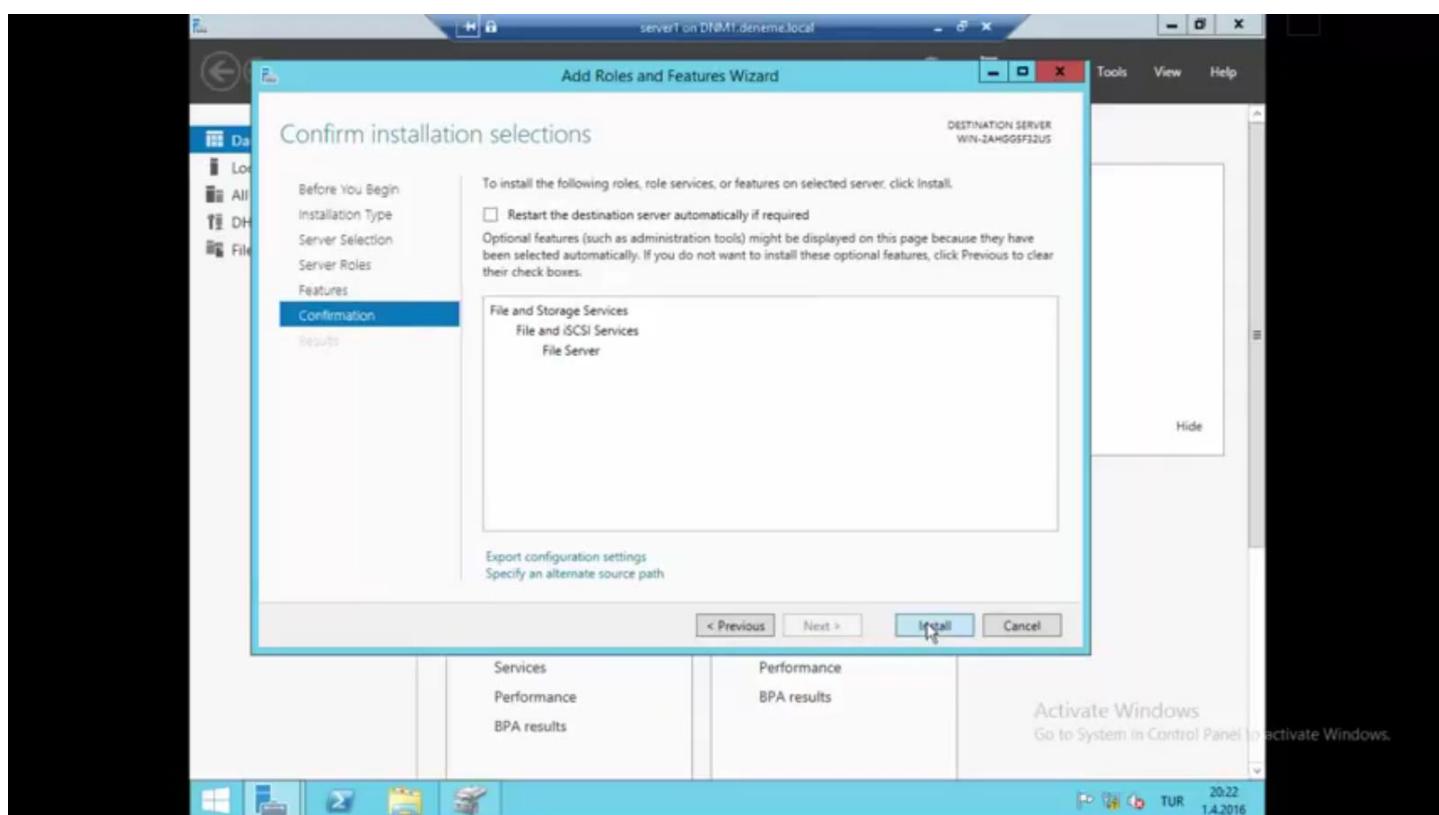
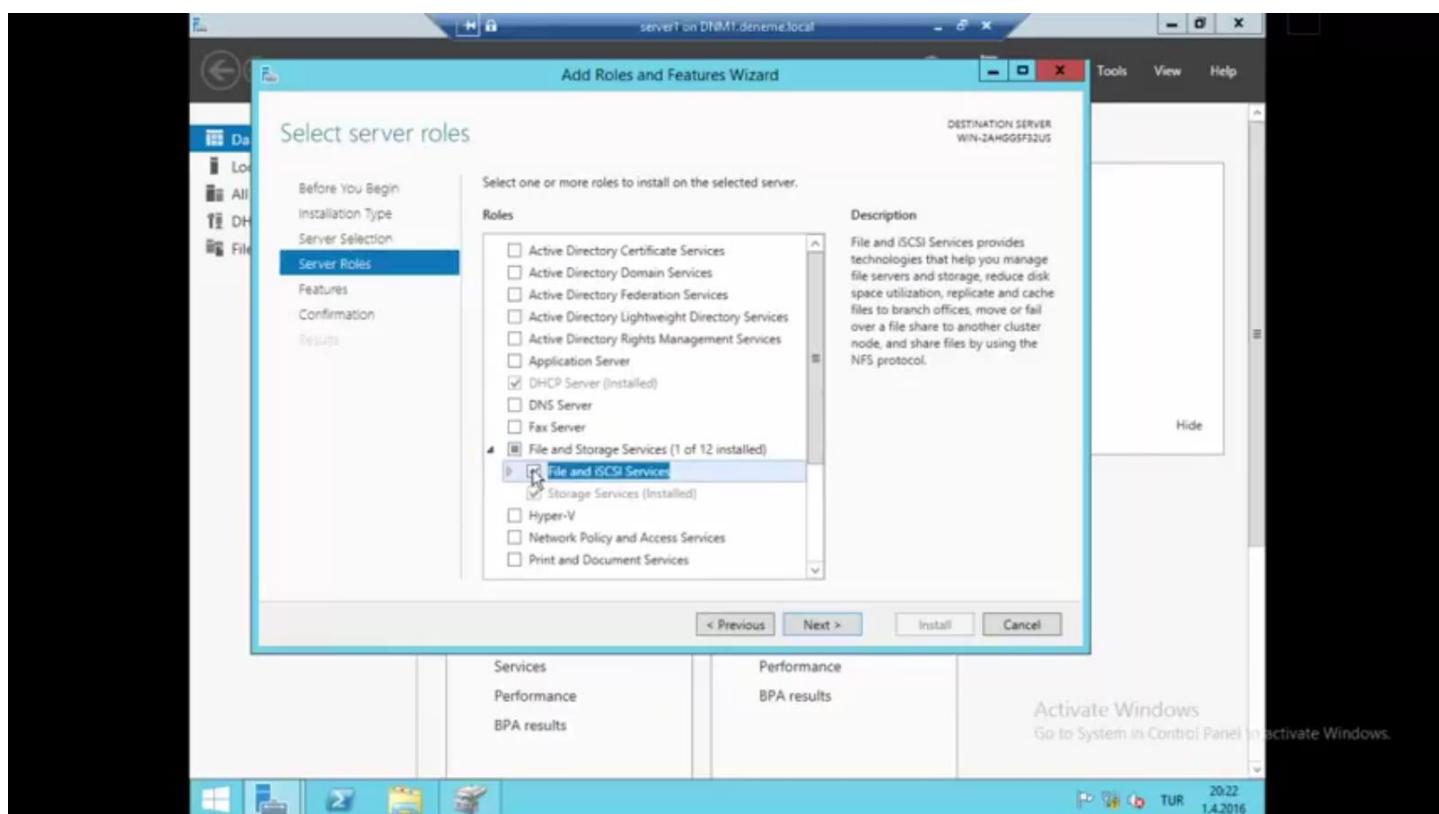
RAID Redundant Array of Independent Disks

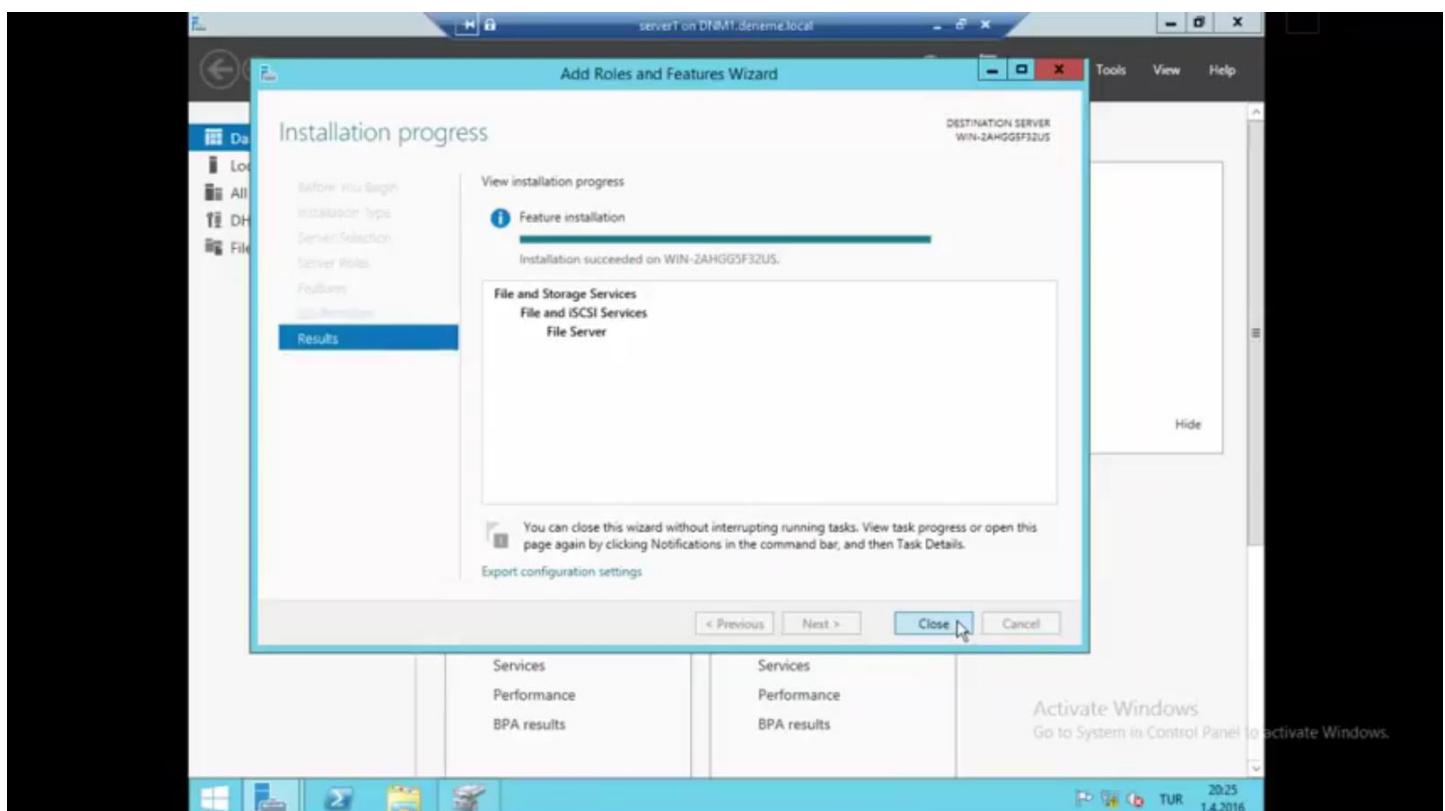
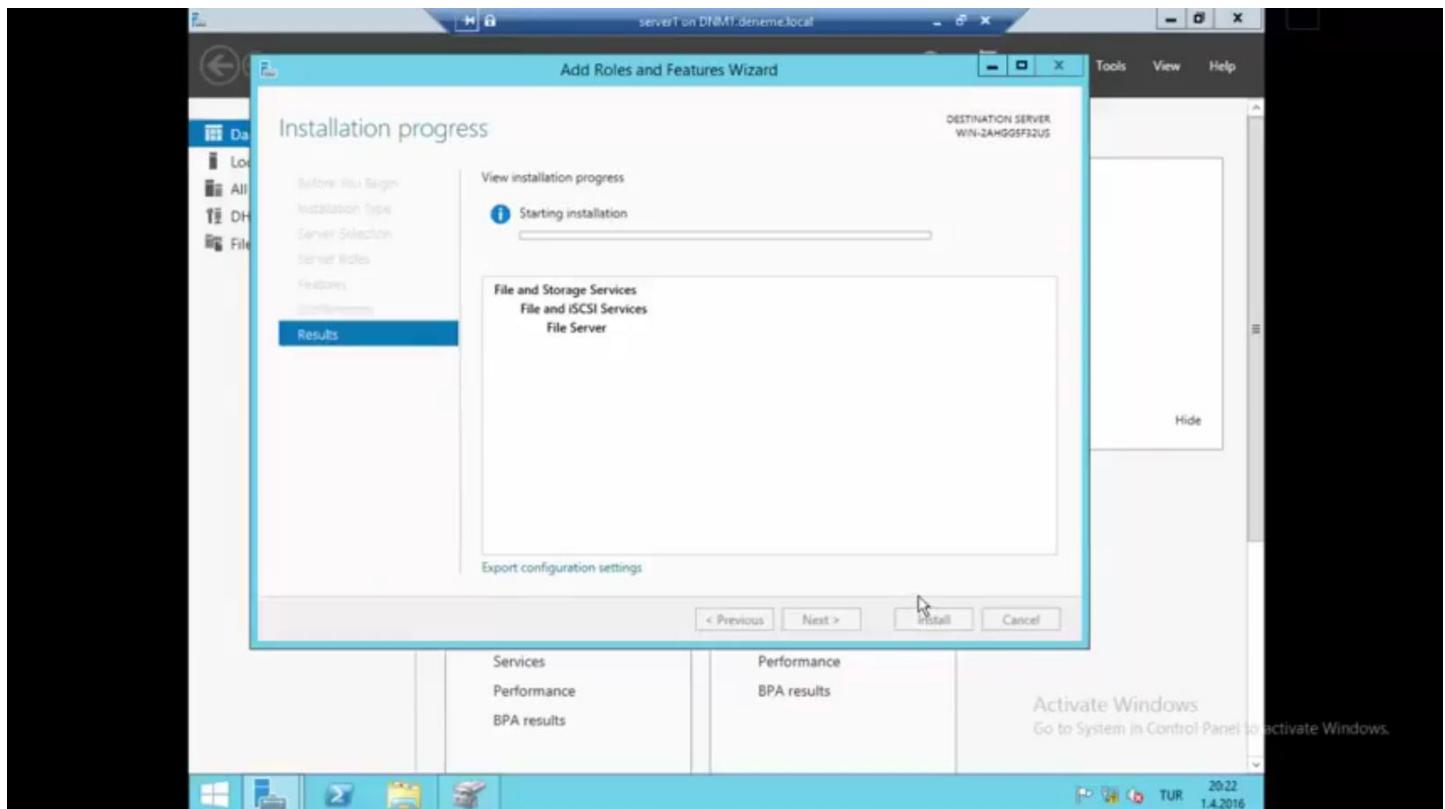
RAID 10

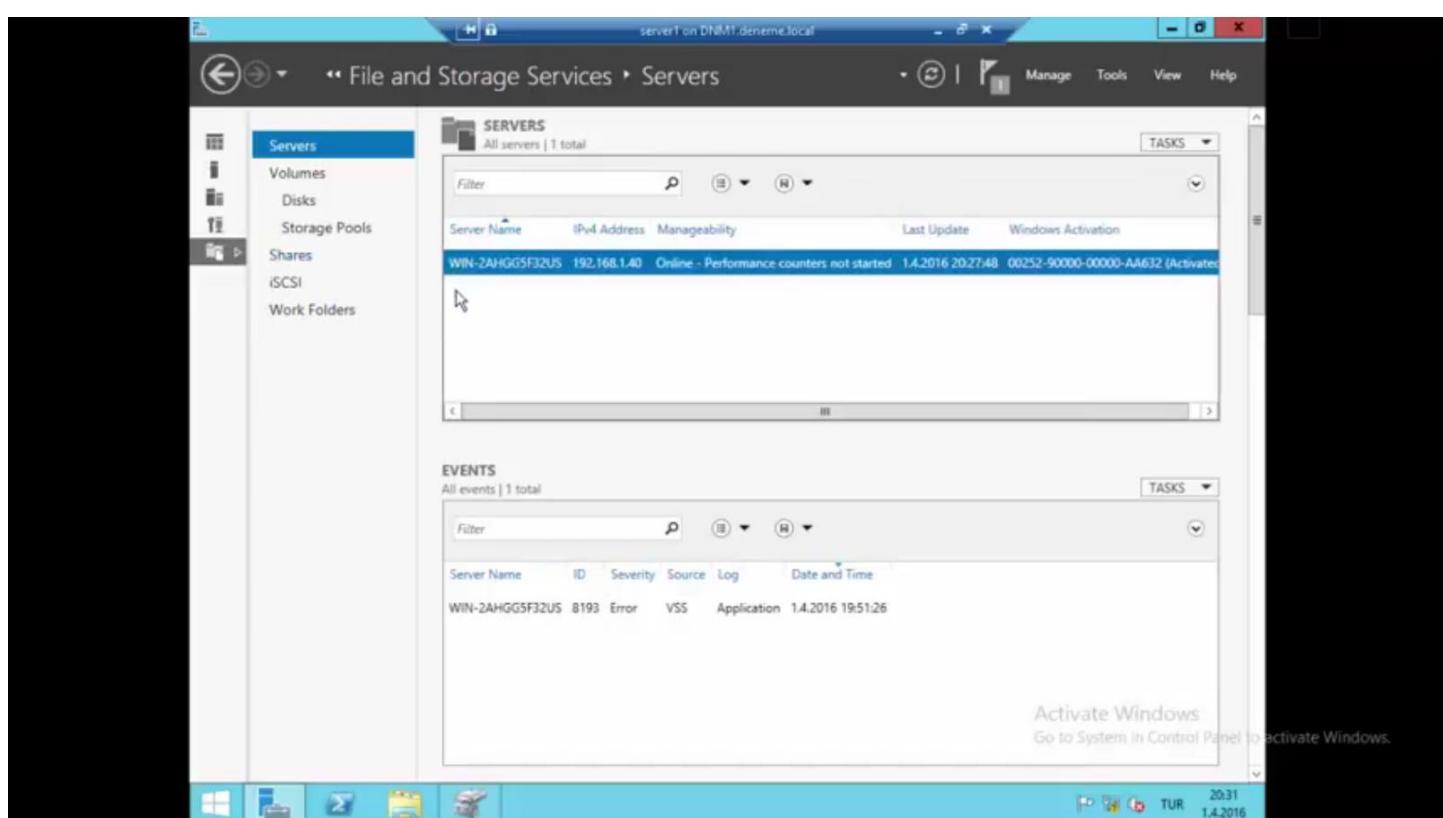
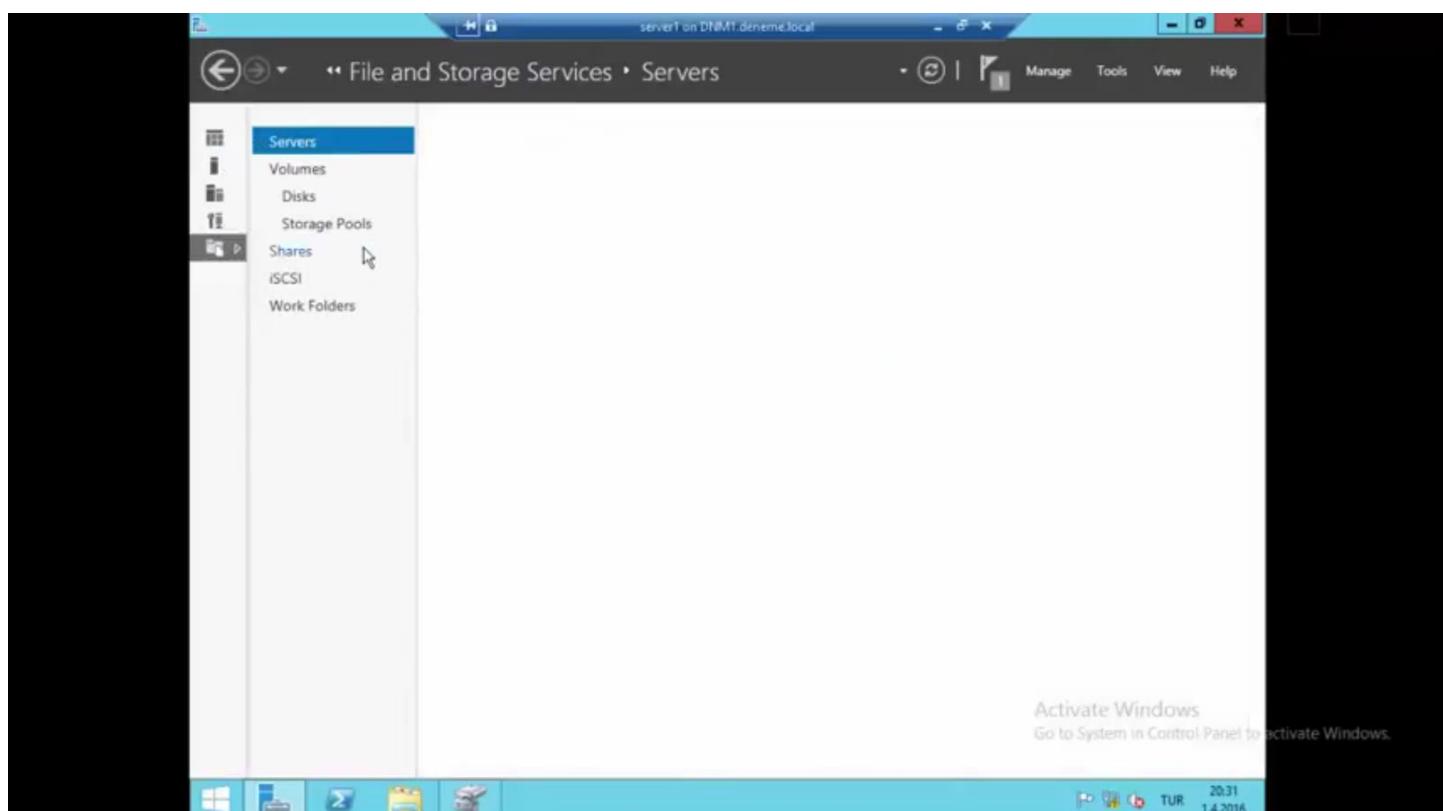
لتطبيق RAID 10 يحتاج إلى أربعة أقراص صلبة على الأقل ولتفعيل آلية العمل وفقا لنظام هذه البنية يحتاج إلى أداتين:

File and storage

وهي إداة تمكينا من إدارة الأقراص وتجميعها ضمن مجالات كما انشاء أقراص افتراضية عن الأقراص الفيزيائية وهو ما نحتاجه للدمج ما بين RAID 0&1









File and Storage Services > Volumes > Disks

DISKS
All disks | 5 total

Number	Virtual Disk	Status	Capacity	Unallocated	Partition	Read Only	Clustered	Subsystem	Bus Type
0		Online	60,0 GB	0,00 B	MBR				ATA
1		Online	10,0 GB	9,97 GB	GPT				SAS
2		Online	10,0 GB	9,97 GB	GPT				SAS
3		Online	10,0 GB	9,97 GB	GPT				SAS
4		Online	10,0 GB	9,97 GB	GPT				SAS

Last refreshed on 1.4.2016 20:31:58

VOLUMES
Related Volumes | 2 total

Volume	Status	Provisioning	Capacity	Free Space
\\\Volume\b6...	Fixed	350 MB	87,9 MB	
C:	Fixed	59,7 GB	51,2 GB	

STORAGE POOL
Virtual HD ATA Device on WIN-2AHGG5F32US

No related storage pool exists.

Activate Windows
Go to System in Control Panel to activate Windows.

20:32 TUR 1.4.2016

File and Storage Services > Volumes > Storage Pools

STORAGE POOLS
All storage pools | 1 total

Name	Type	Managed by	Available to	Read-Write Server
Storage Spaces (1)				
Primordial	Available Disks	WIN-2AHGG5F32US	WIN-2AHGG5F32US	WIN-2AHGG5F32US

Last refreshed on 1.4.2016 20:32:11

VIRTUAL DISKS
No related data is available.

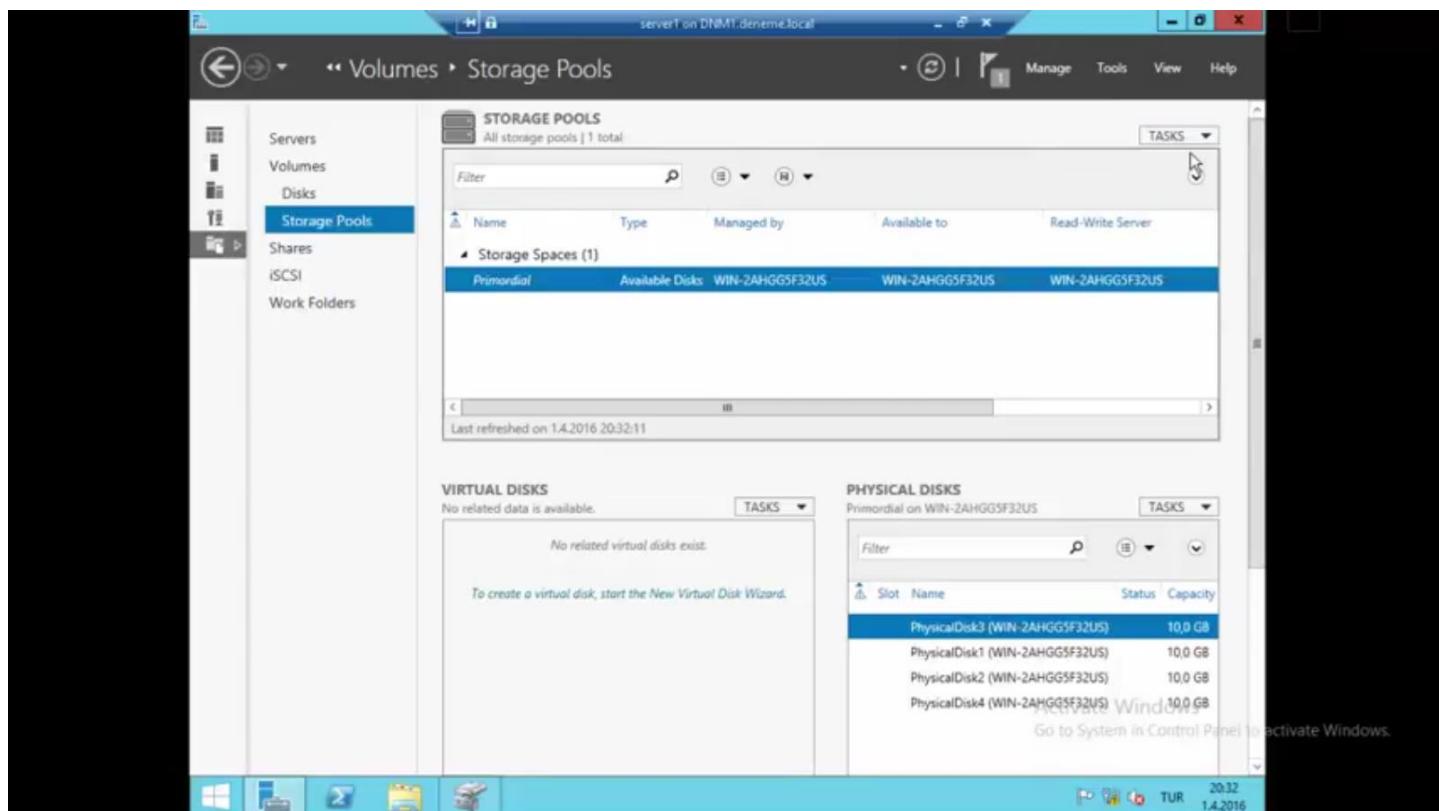
No related virtual disks exist.
To create a virtual disk, start the New Virtual Disk Wizard.

PHYSICAL DISKS
Primordial on WIN-2AHGG5F32US

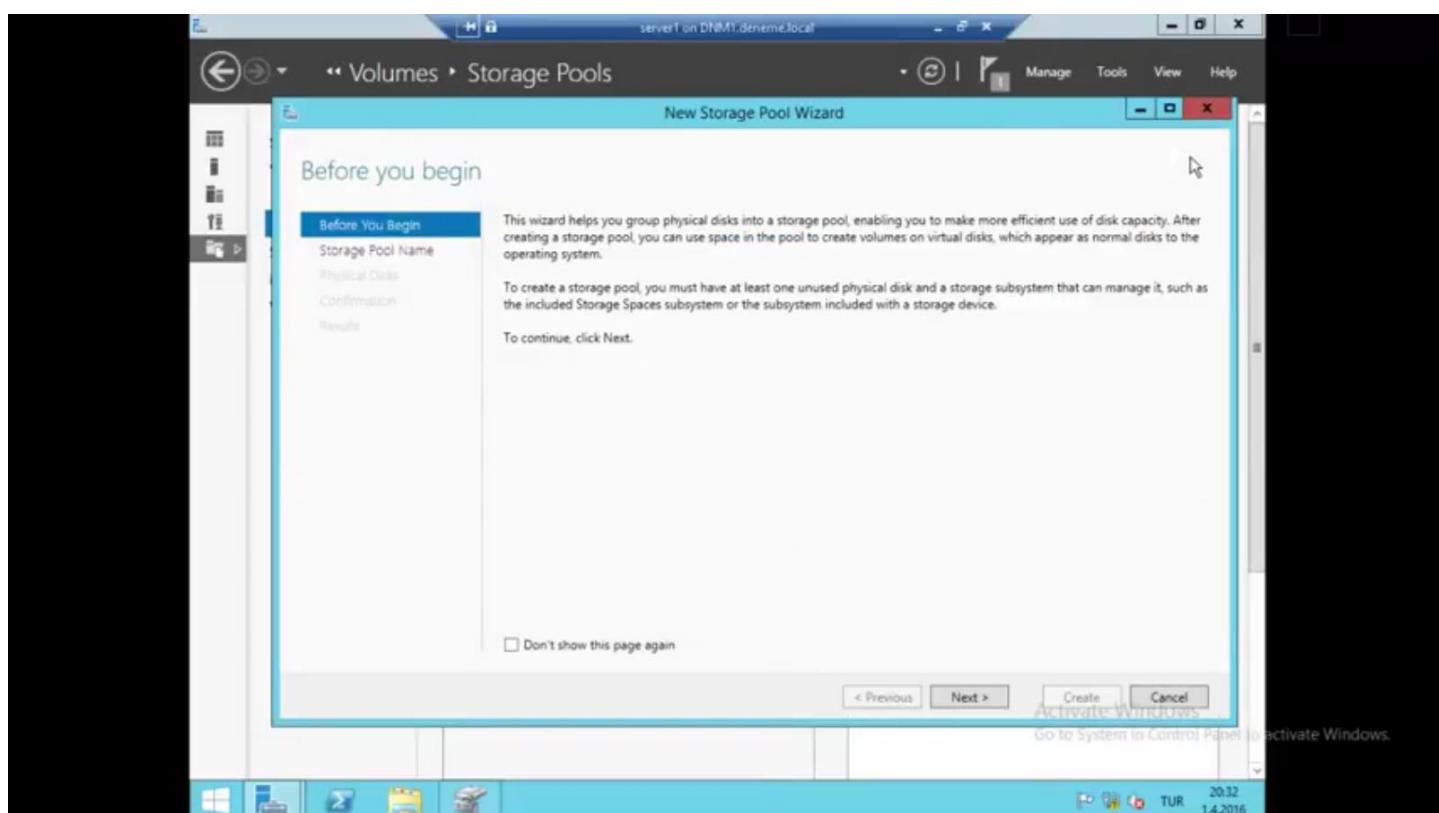
Slot	Name	Status	Capacity
PhysicalDisk3 (WIN-2AHGG5F32US)		10,0 GB	
PhysicalDisk1 (WIN-2AHGG5F32US)		10,0 GB	
PhysicalDisk2 (WIN-2AHGG5F32US)		10,0 GB	
PhysicalDisk4 (WIN-2AHGG5F32US)		10,0 GB	

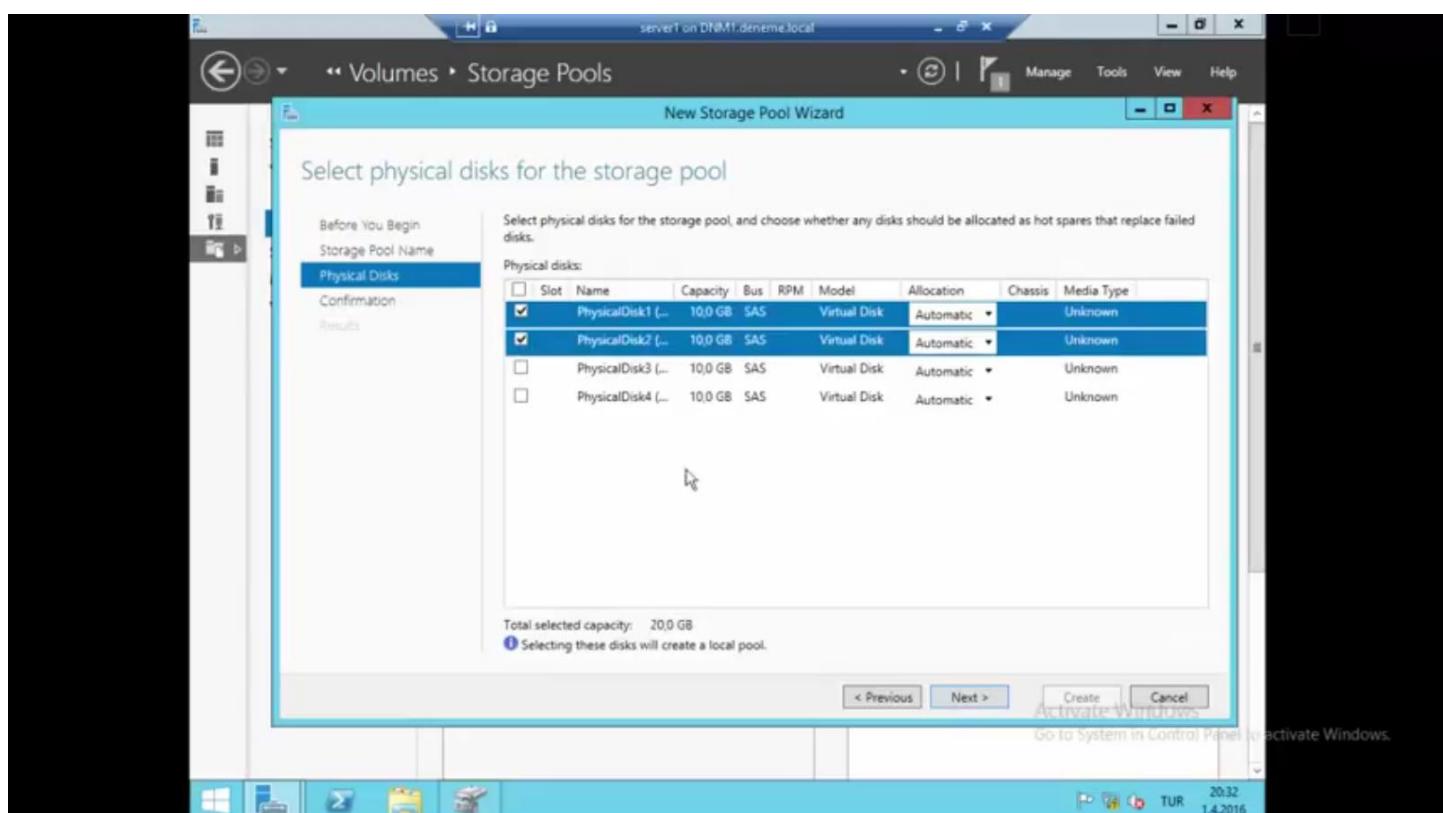
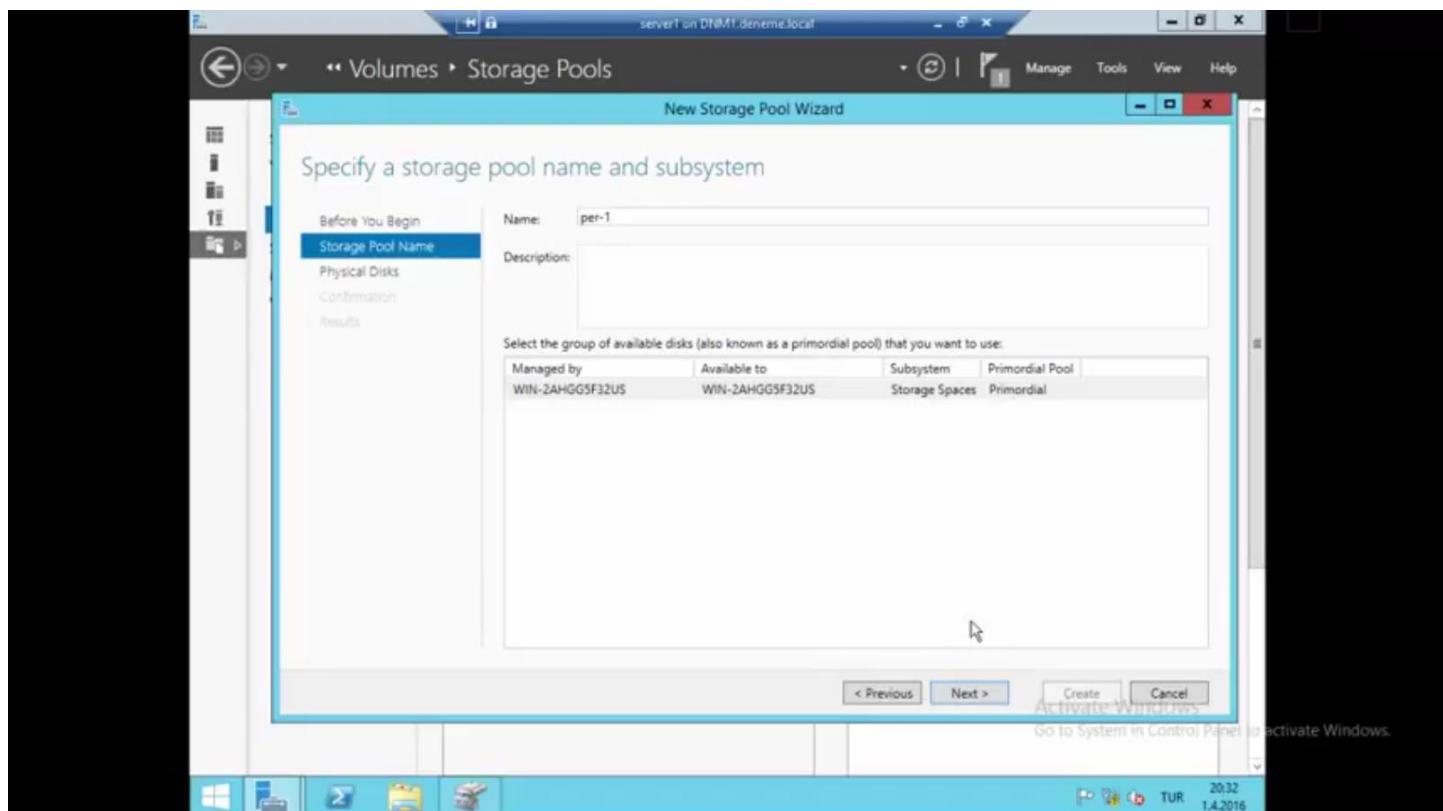
Activate Windows
Go to System in Control Panel to activate Windows.

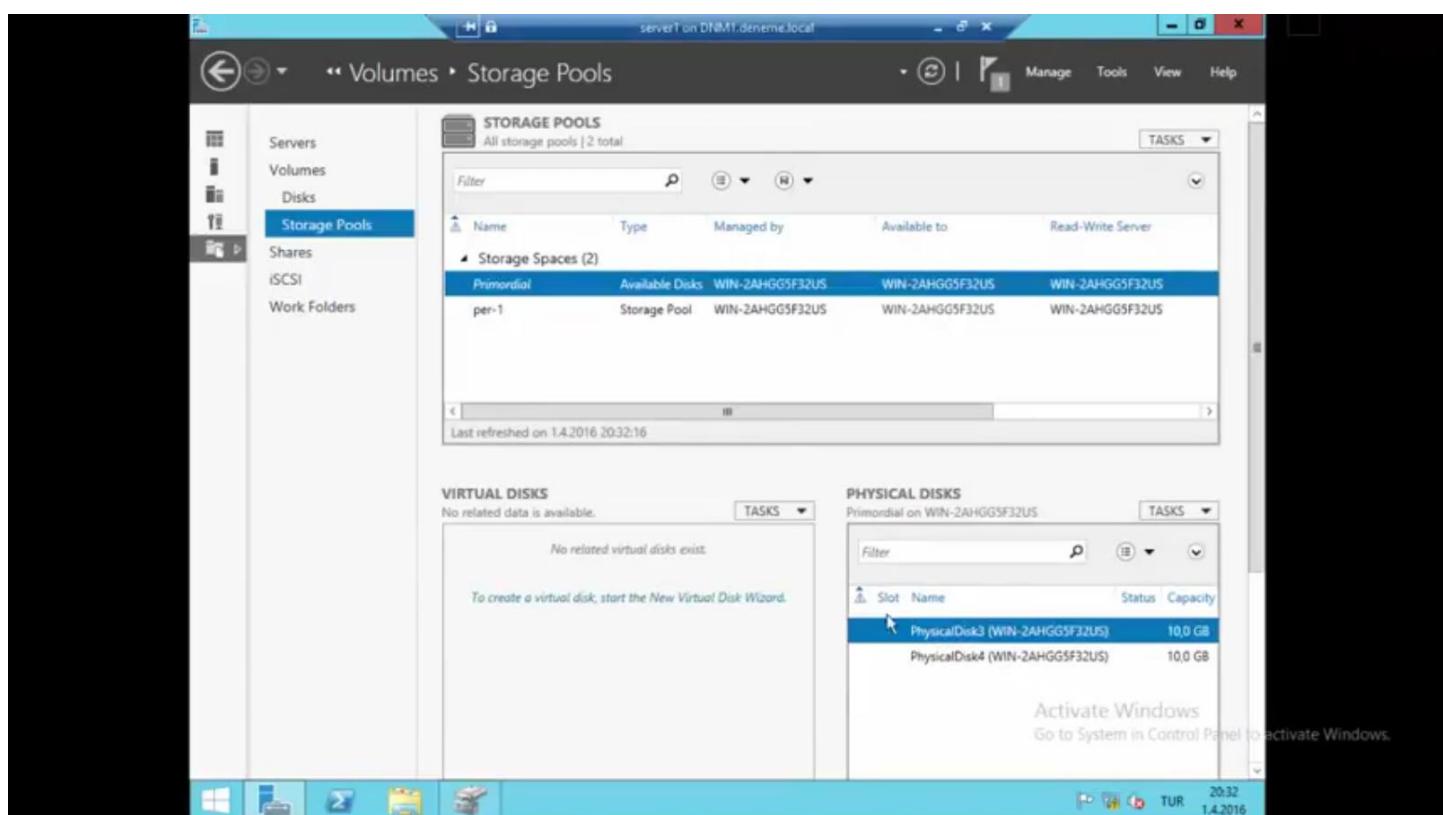
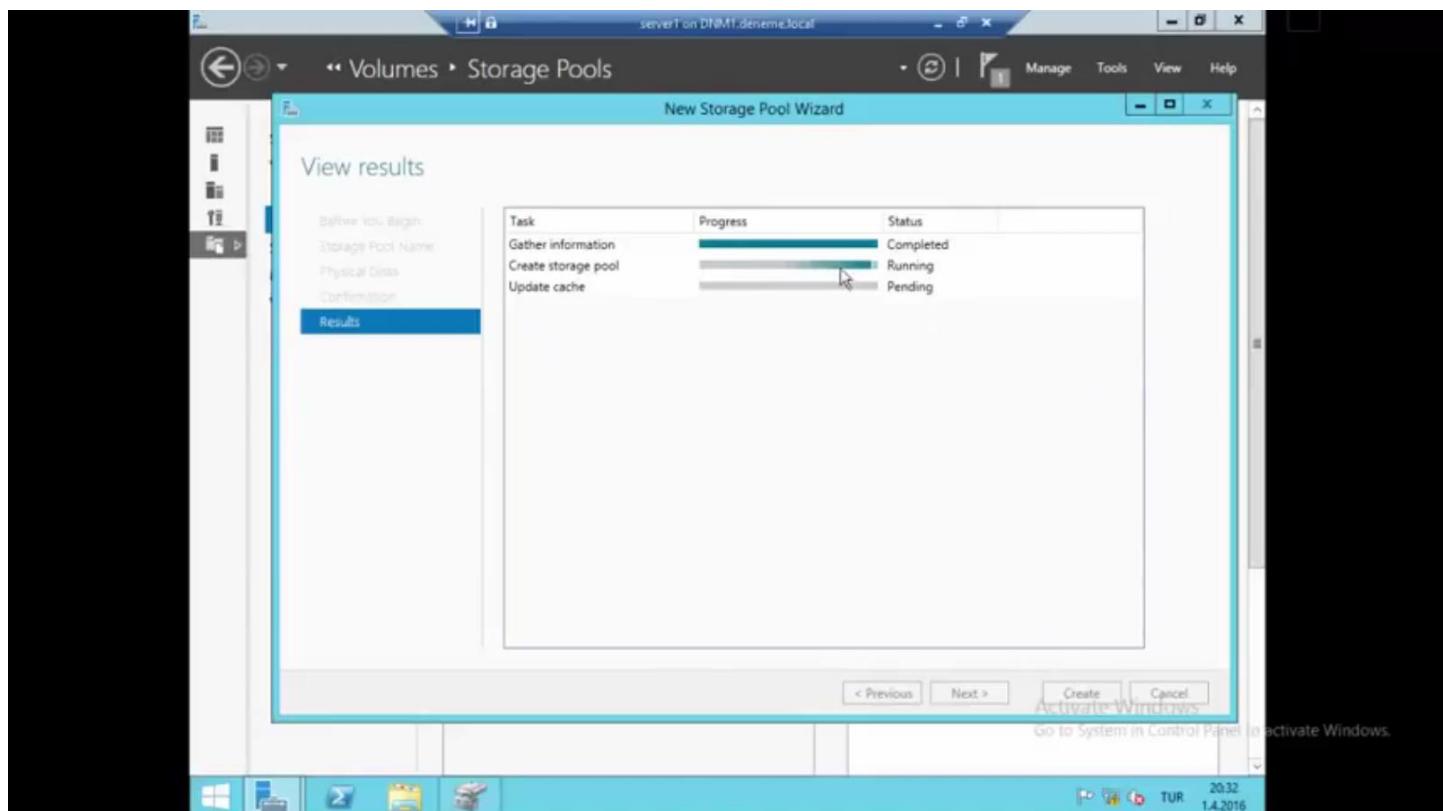
20:32 TUR 1.4.2016



إنشاء المجال الأول للاول قرصين









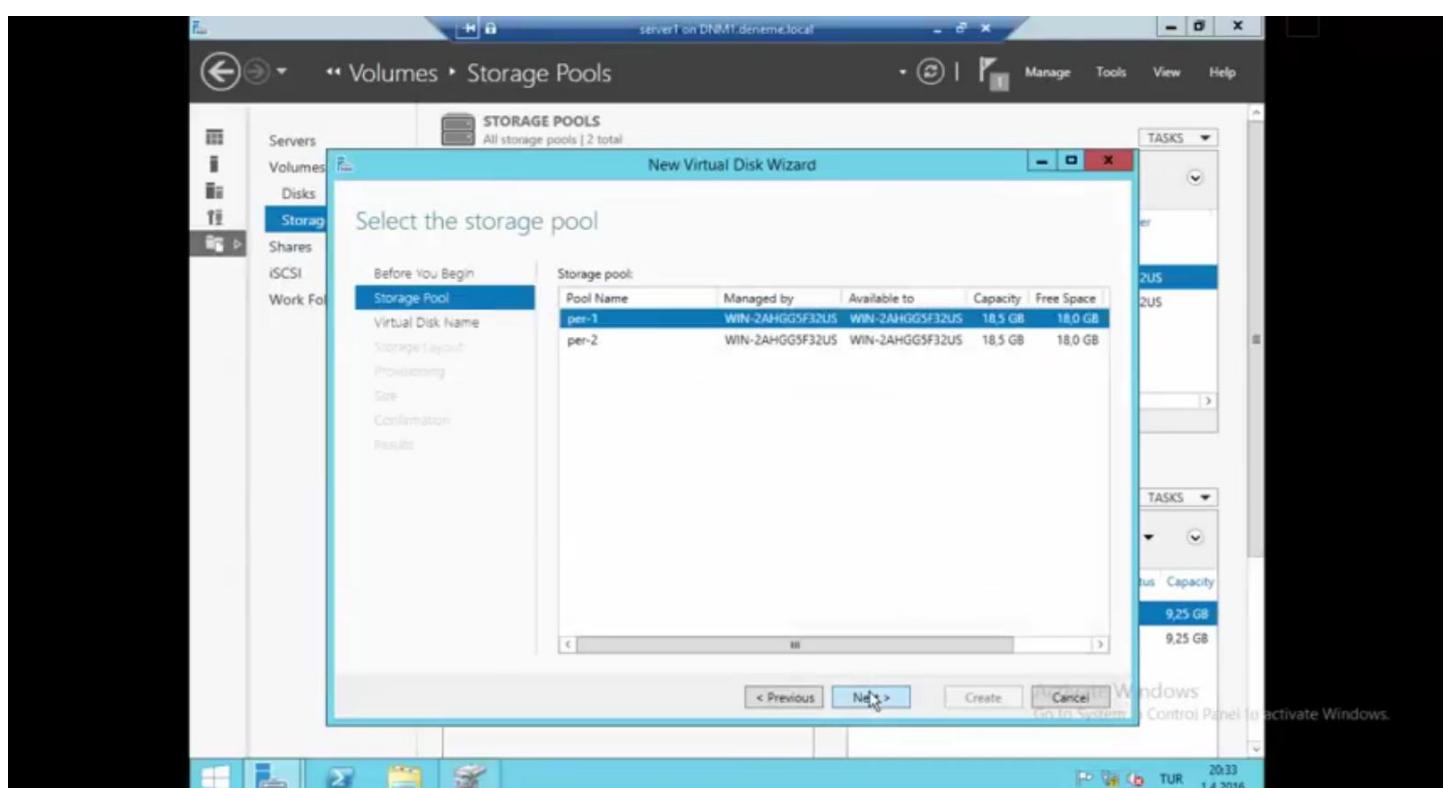
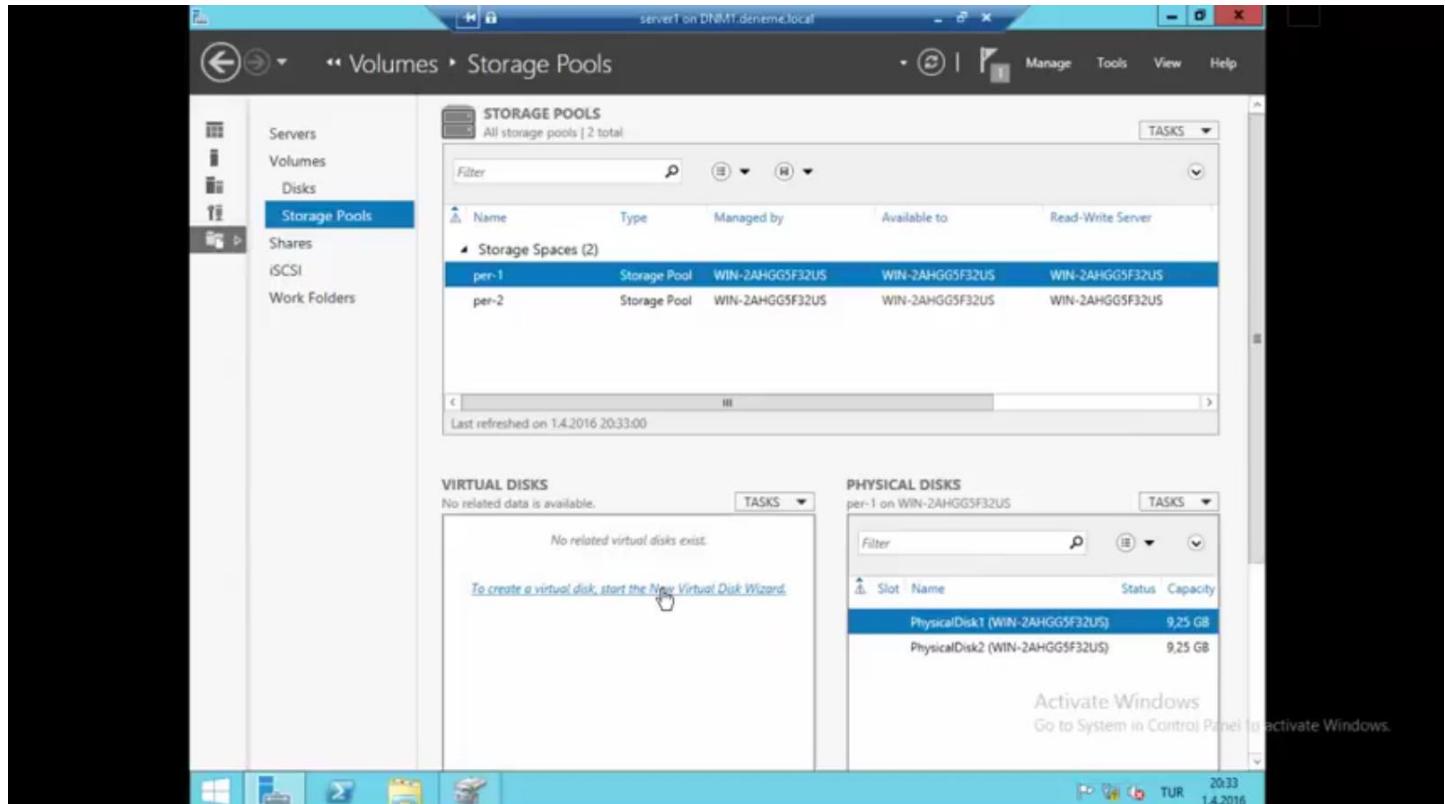
The screenshot shows the 'Storage Pools' section of a server management interface. The left sidebar lists 'Servers', 'Volumes', 'Disks', 'Storage Pools' (which is selected), 'Shares', 'iSCSI', and 'Work Folders'. The main area displays 'STORAGE POOLS' with two entries: 'Primordial' (Available Disks: WIN-2AHGG5F32US) and 'per-1' (Storage Pool: WIN-2AHGG5F32US). Below this is a 'VIRTUAL DISKS' section stating 'No related data is available.' and a 'PHYSICAL DISKS' section listing 'PhysicalDisk1 (WIN-2AHGG5F32US)' and 'PhysicalDisk2 (WIN-2AHGG5F32US)' both with 9.25 GB capacity. A message at the bottom right says 'Activate Windows Go to System in Control Panel to activate Windows.' The taskbar at the bottom includes icons for Start, File Explorer, Mail, File History, Task View, and TUR, with the date and time showing 1.4.2016 20:32.

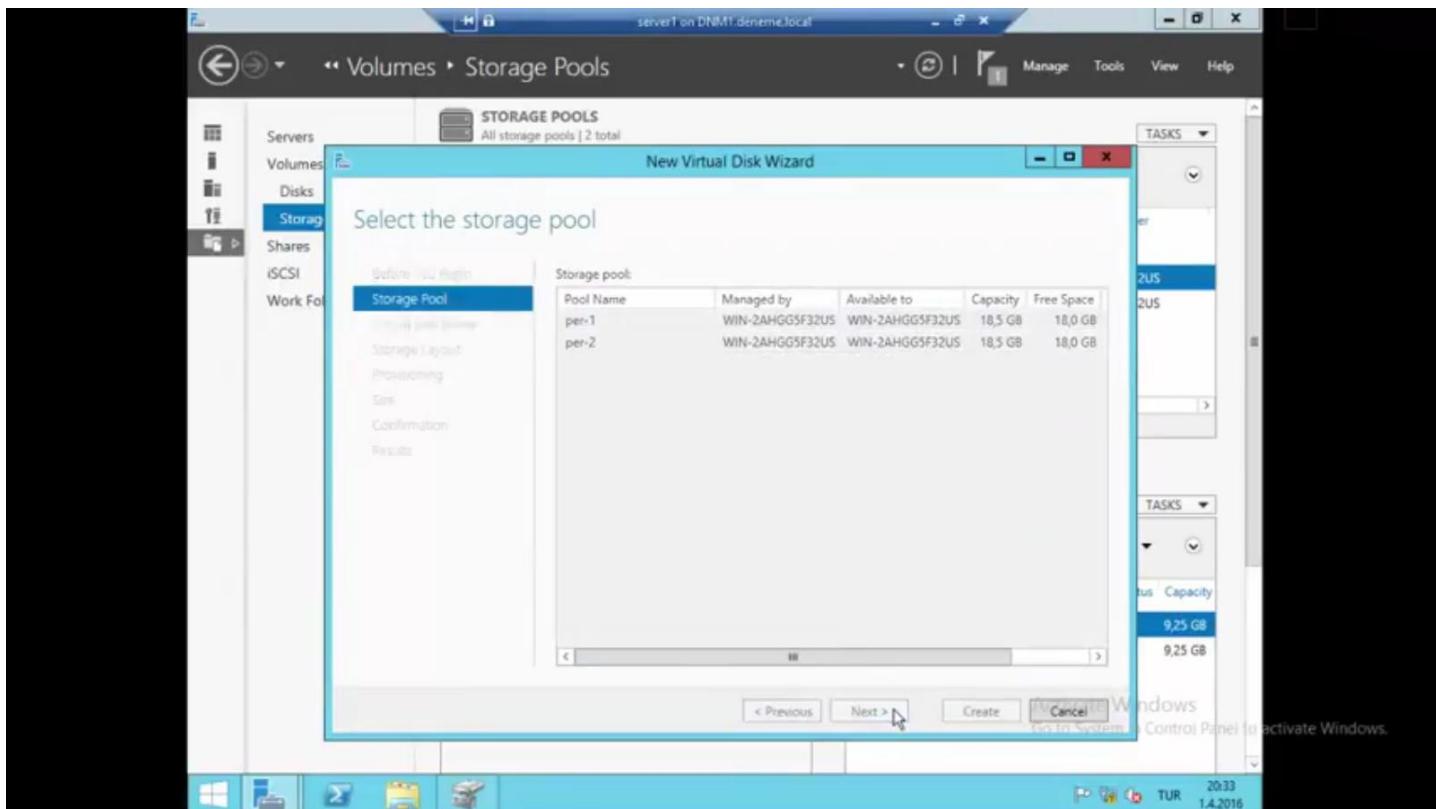
بنفس الطريقة ننشئ المجال الثاني للقرصين الآخرين



إنشاء الأقراص الـ Mirrror من المجالين السابقين

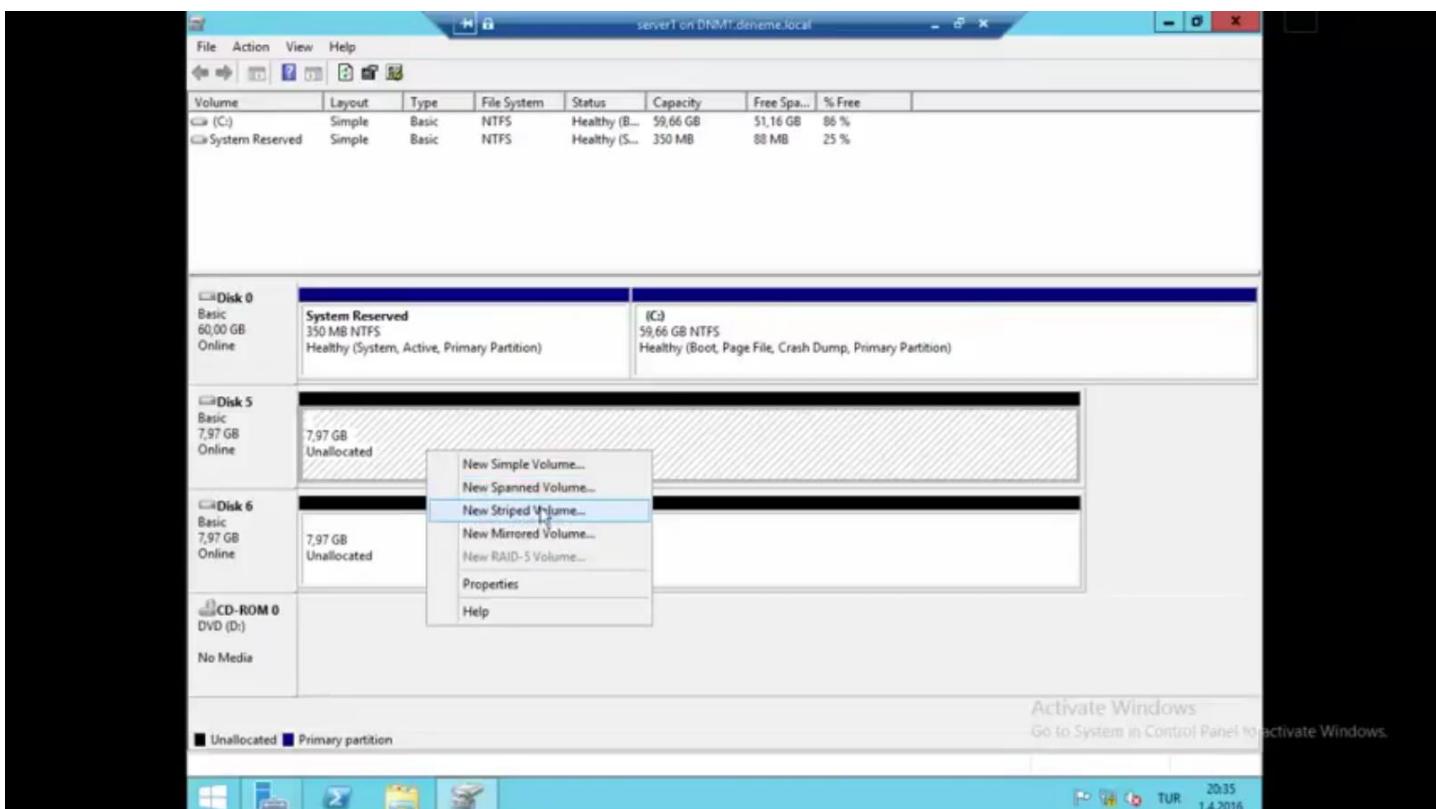
وهنا نأخذ المجالين الاول والثاني ونحو كل من هما الى قرص افتراضي من نوع Mirrror بشكل منفصل مما يؤدي الى ظهور قرصين فقط من 4 للنظام في اداة ادارة الأقراص ما يمكننا من اعدادهما ليكونا Stripp Volume خلال الخطوات التالية:

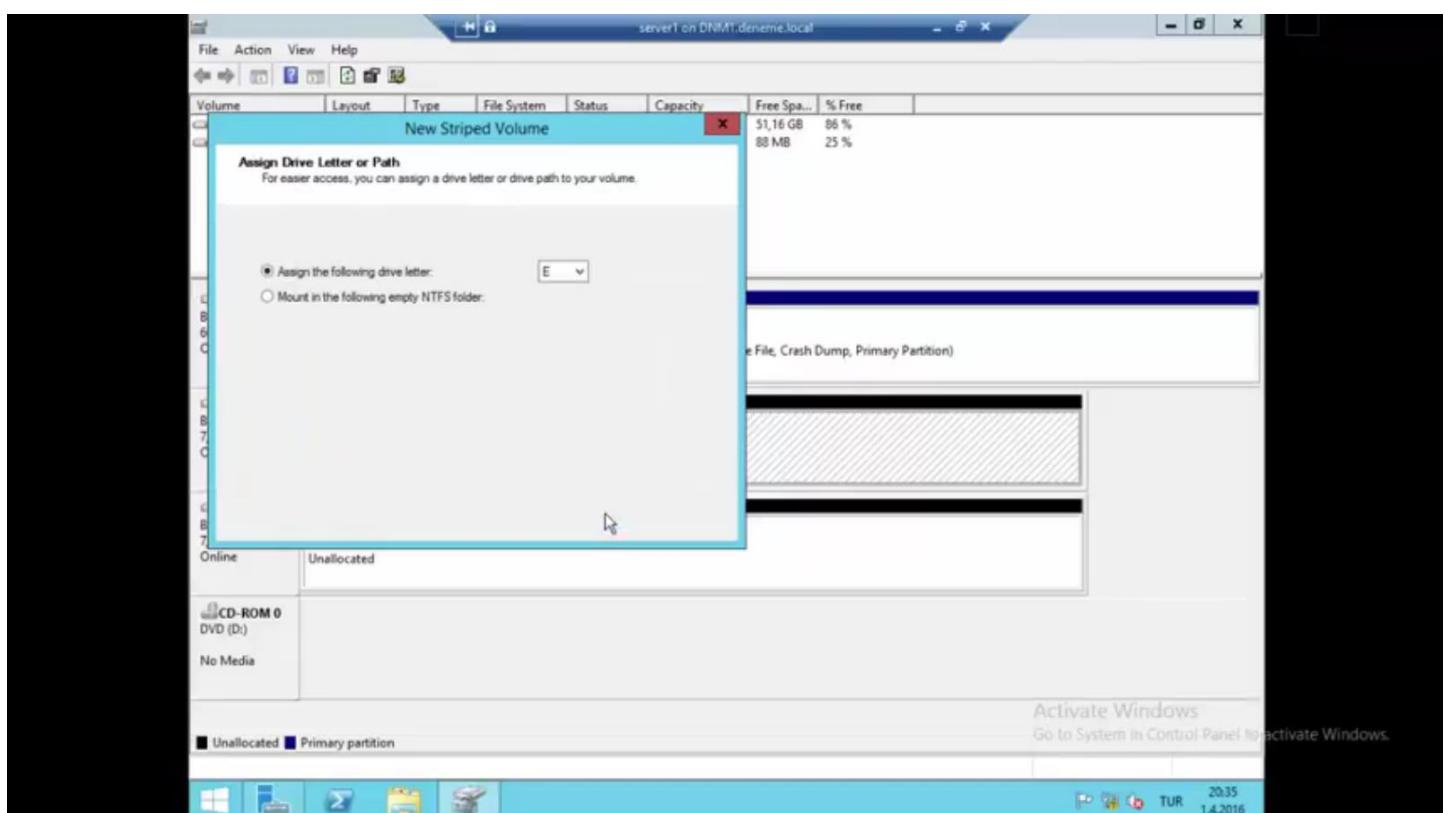
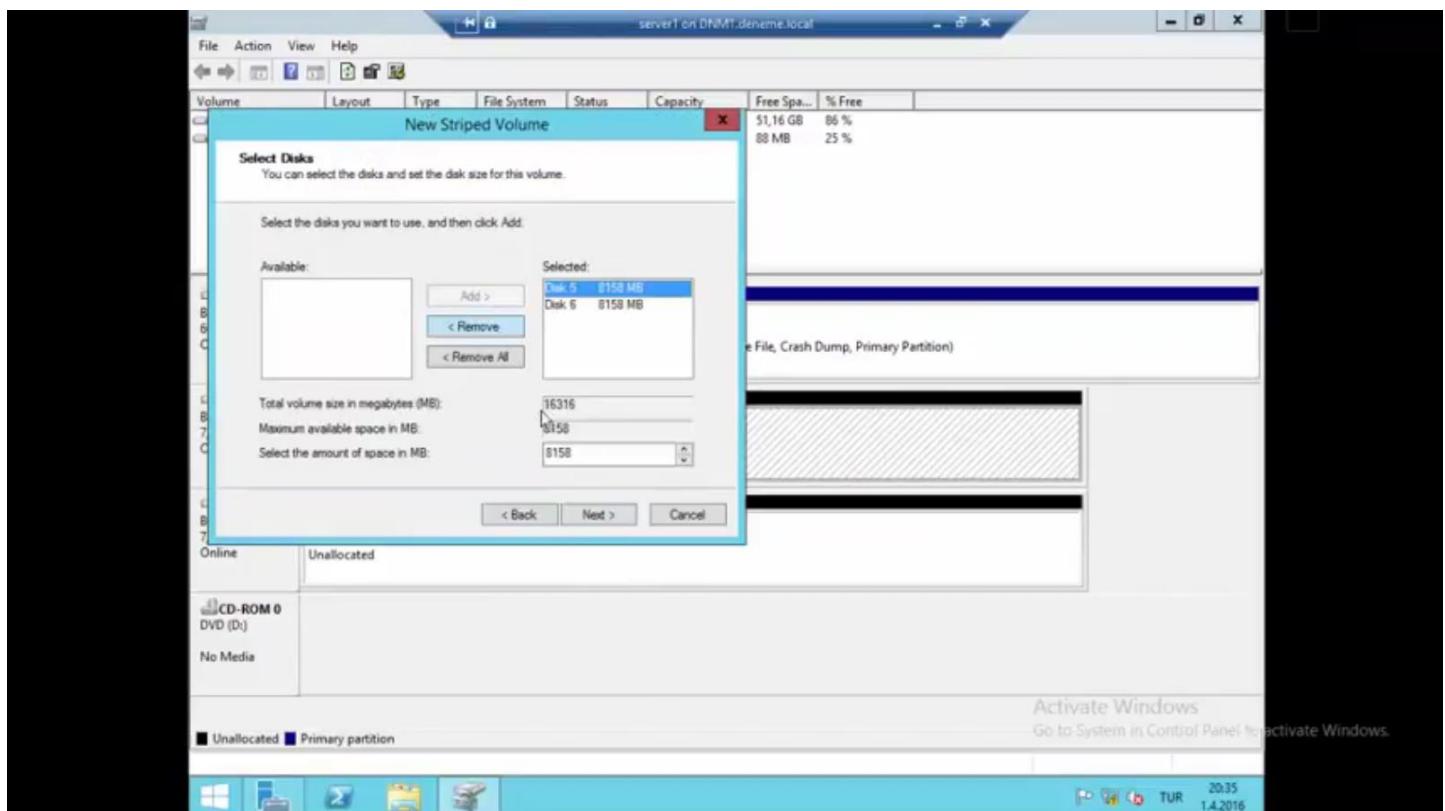


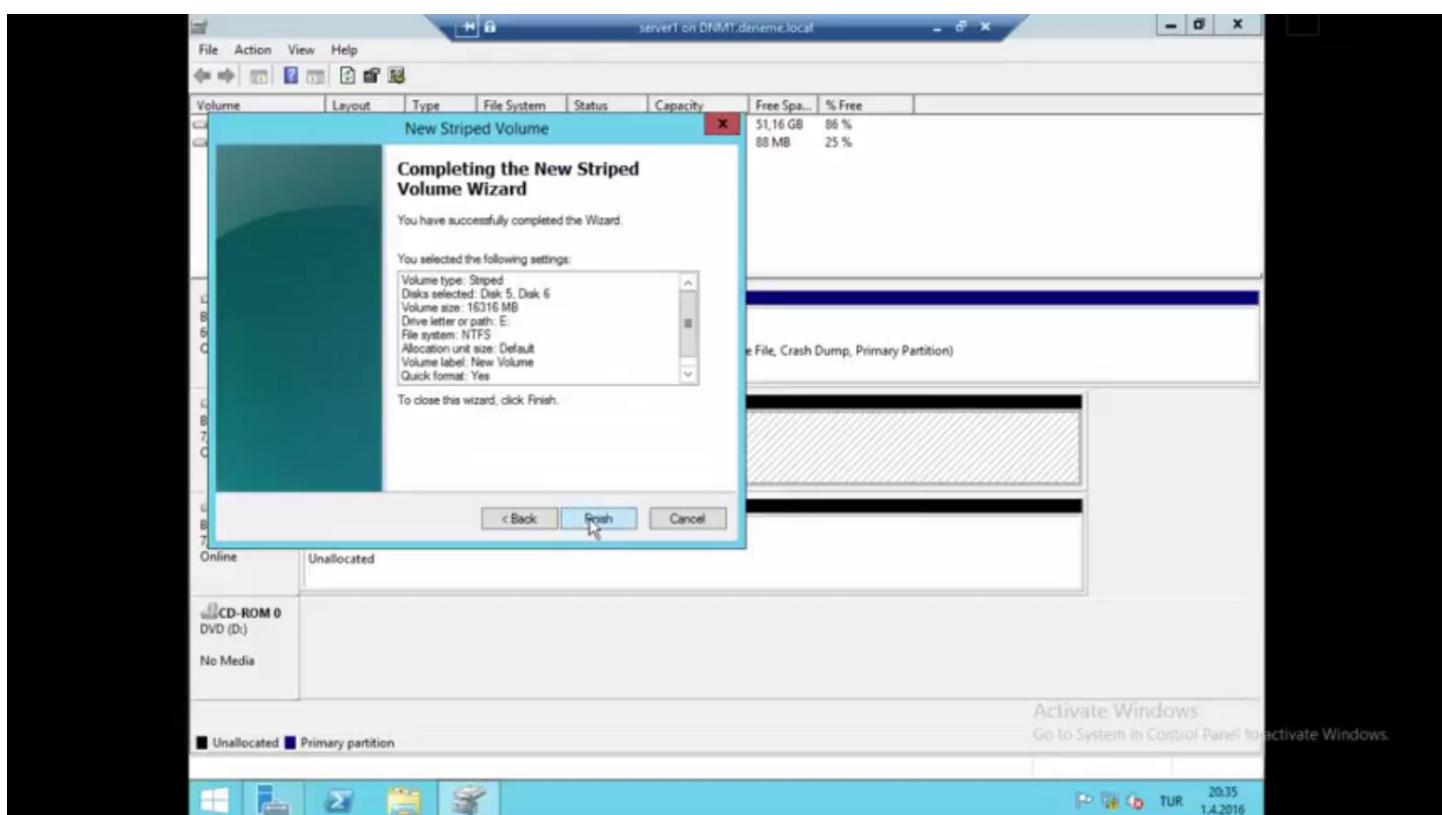
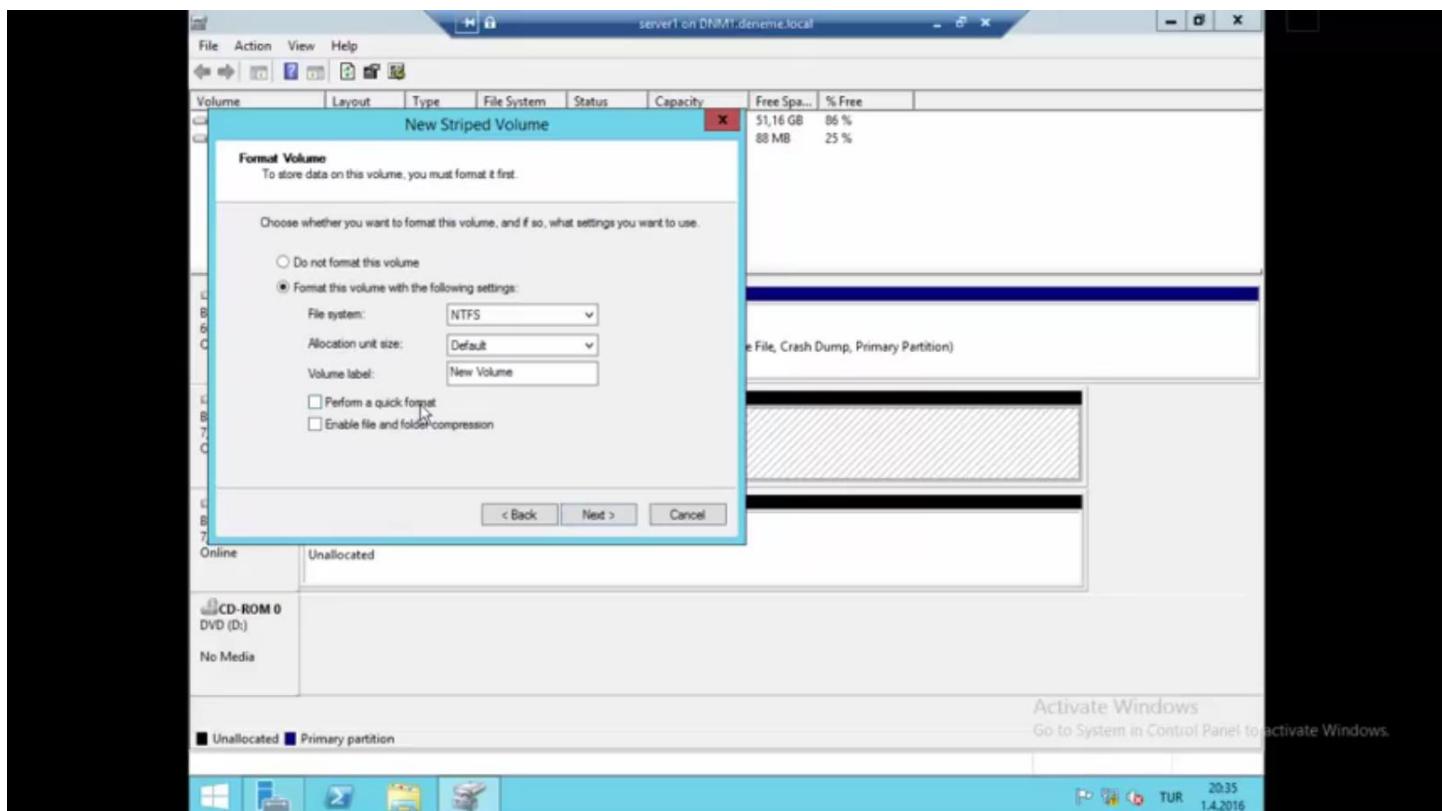


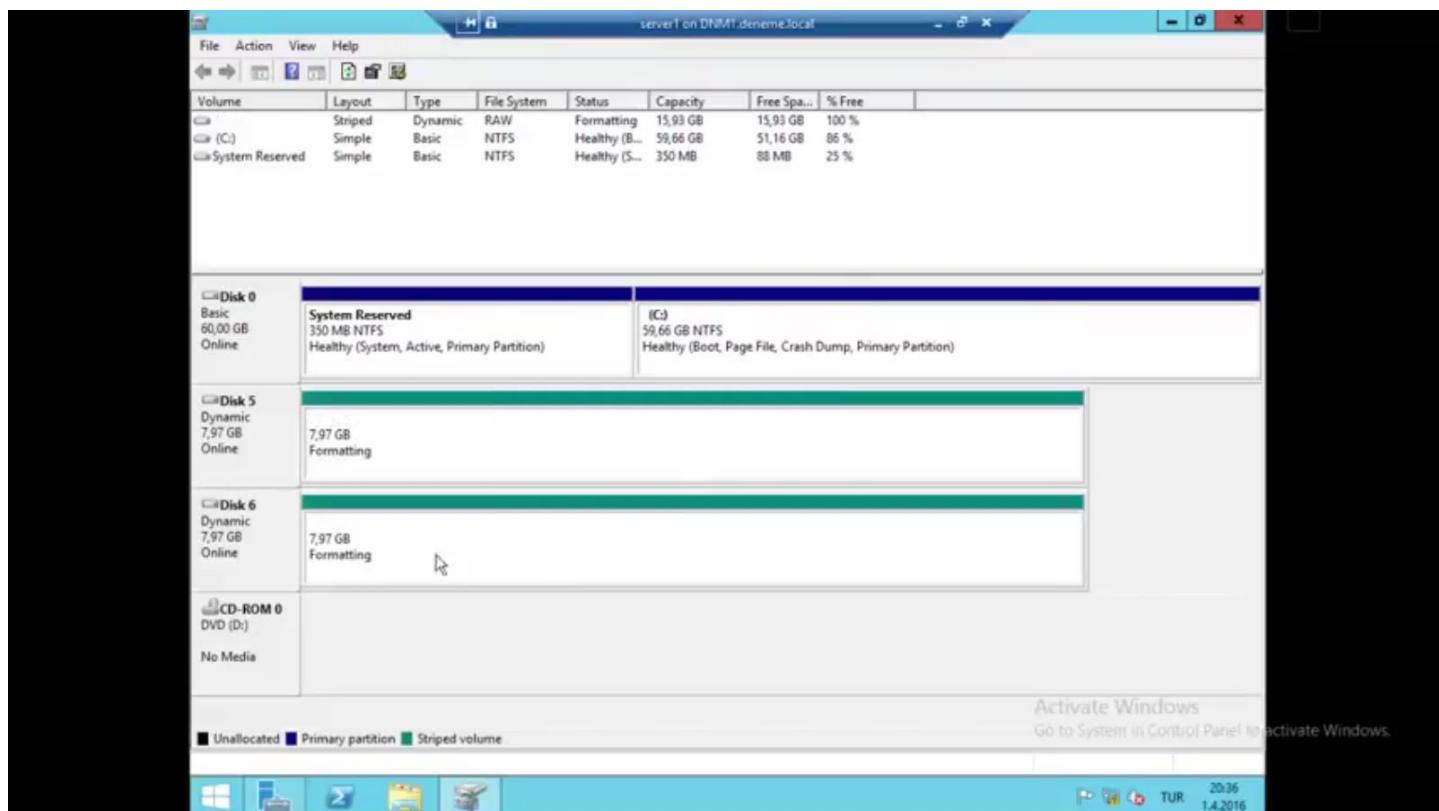
وبنفس الطريقة ننشئ القرص الافتراضي الآخر للمجال الآخر.

الخطوة الأخيرة وهي إنشاء الـ Strip volume









وبهذا تكون قد حققنا الدمج ما بين الـ RAID 0&1 وفي النتيجة هنا حلصنا على قرص واحد منطقي مؤلف من قرصين افتراضيين بنائًّا على أربعة أقراص اثنان منها مرآة للآخر.

الفوائد المحققة:

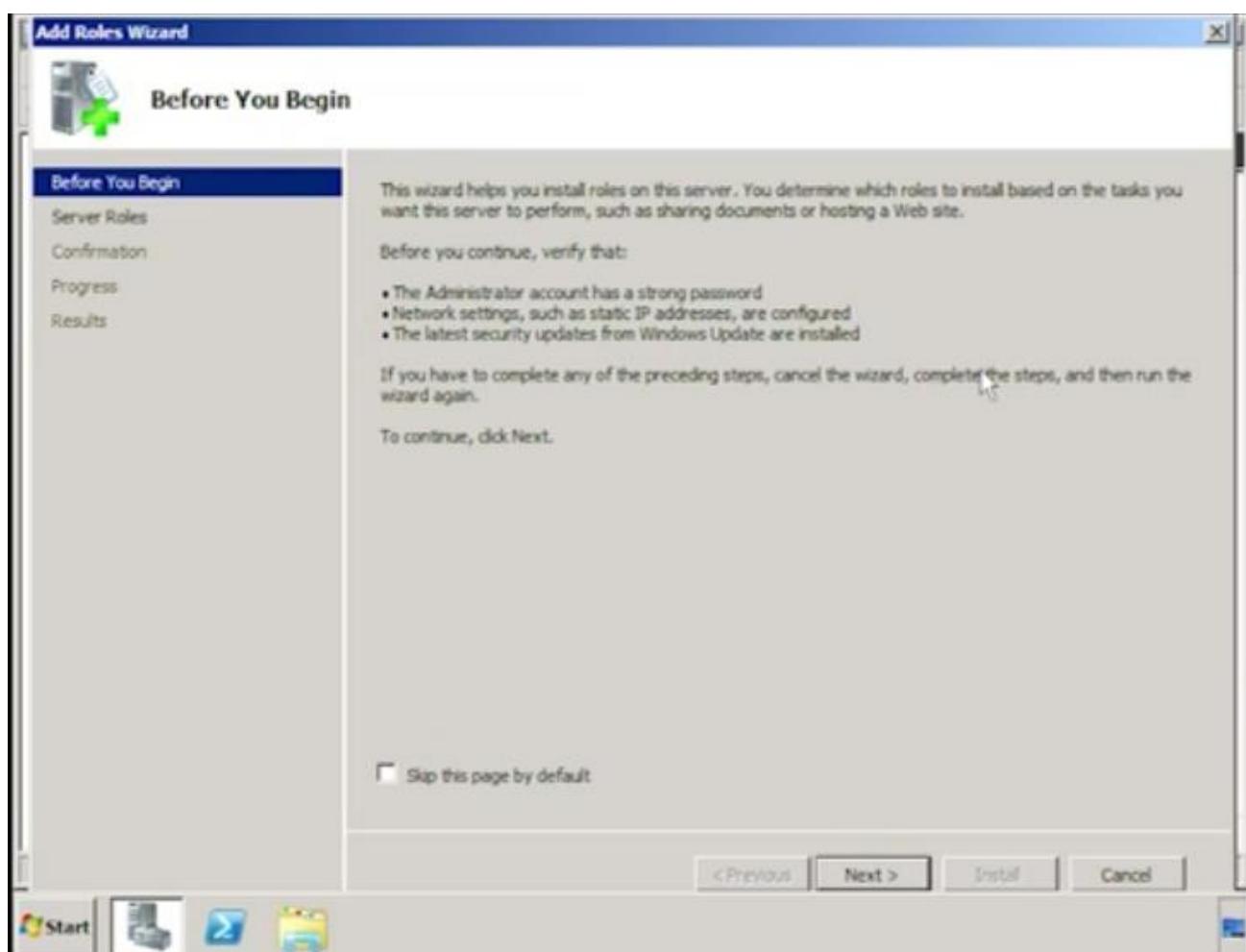
- سرعة عالية في كتابة واسترداد البيانات من الأقراص
- حدوث عطب في أي من الأقراص لا يؤدي لا إلى توقف العمل ولا إلى فقدان البيانات
- استمرار العمل دون أي خلل في البيانات أو أي انقطاع طالما هناك $\frac{1}{2}$ أقراص في الخدمة
- في حال عطب أي قرص أو انتهاء عمره الافتراضي يمكن ببساطة تغييره ليدخل في المنظومة تلقائياً

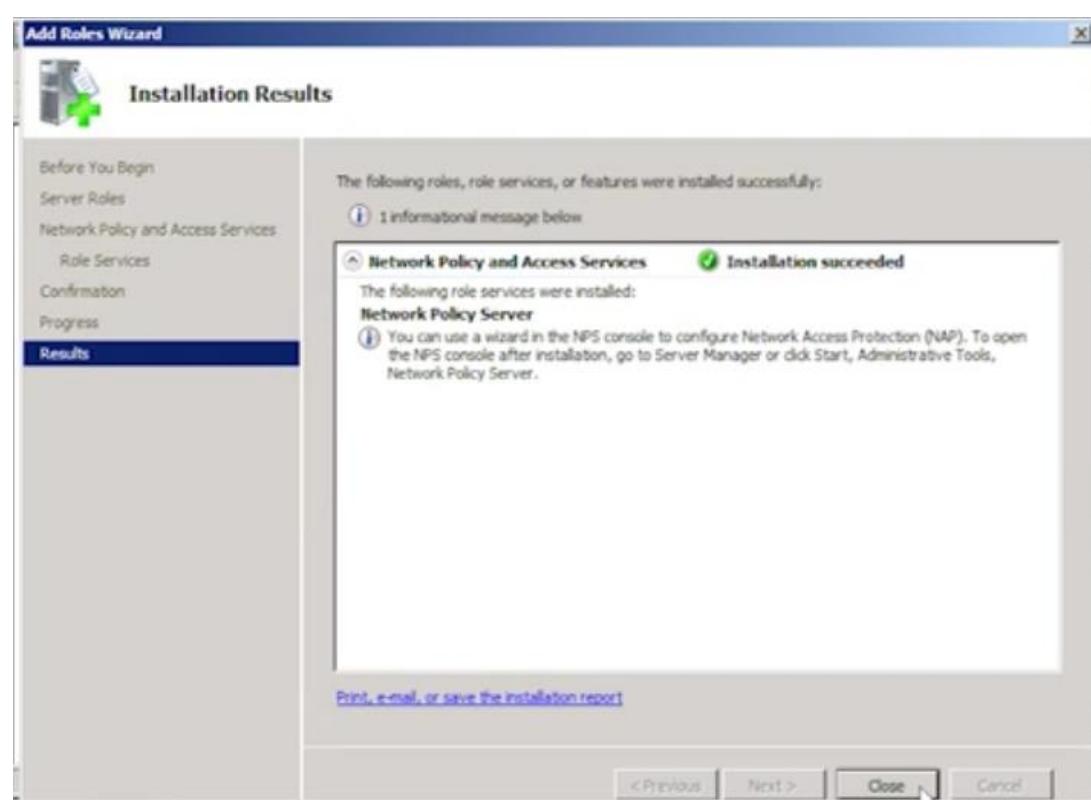
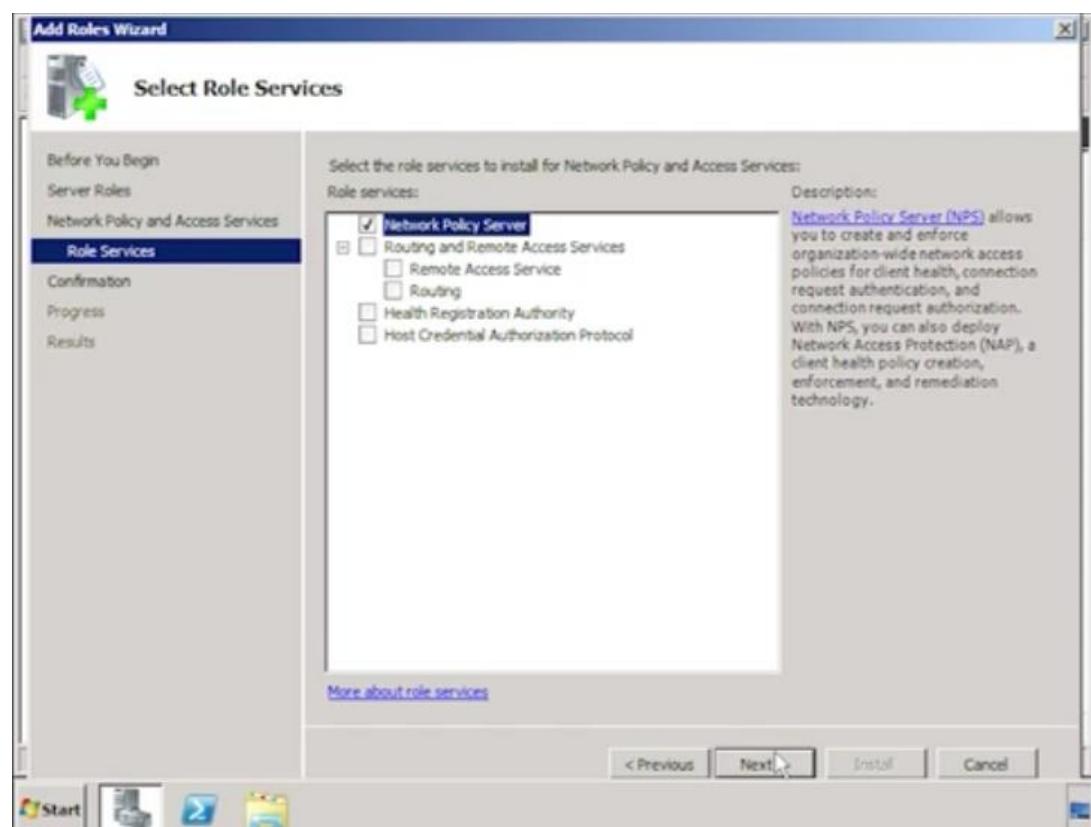
NAP Network Access Protection

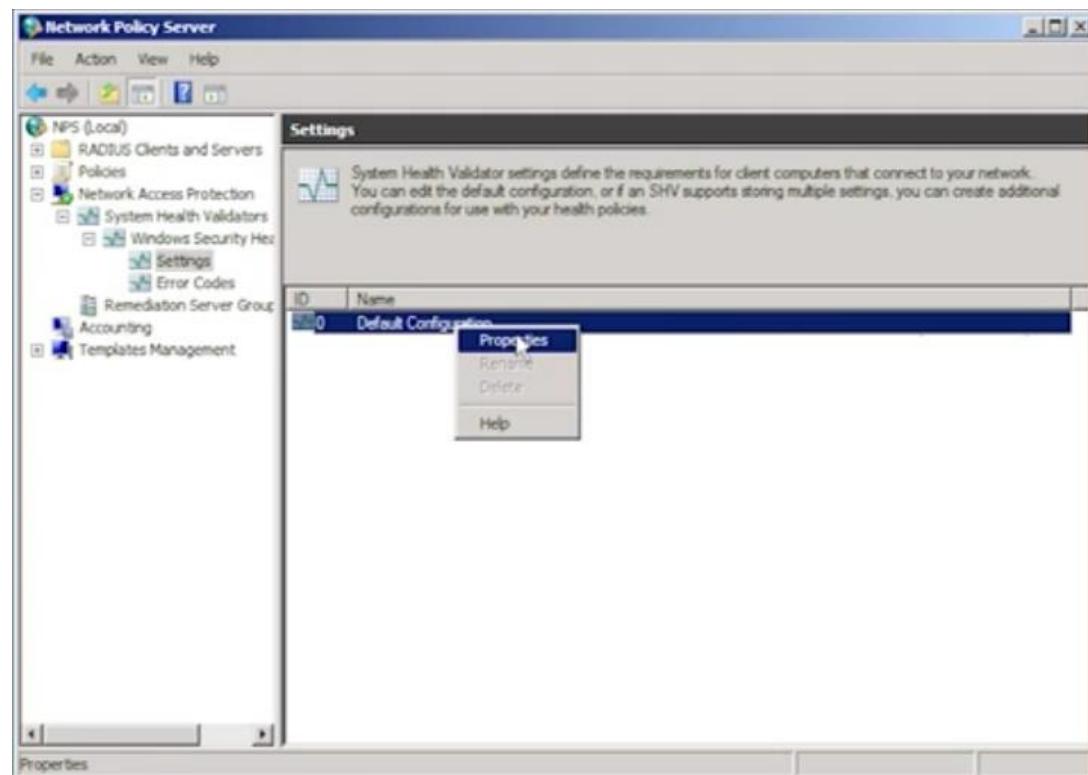
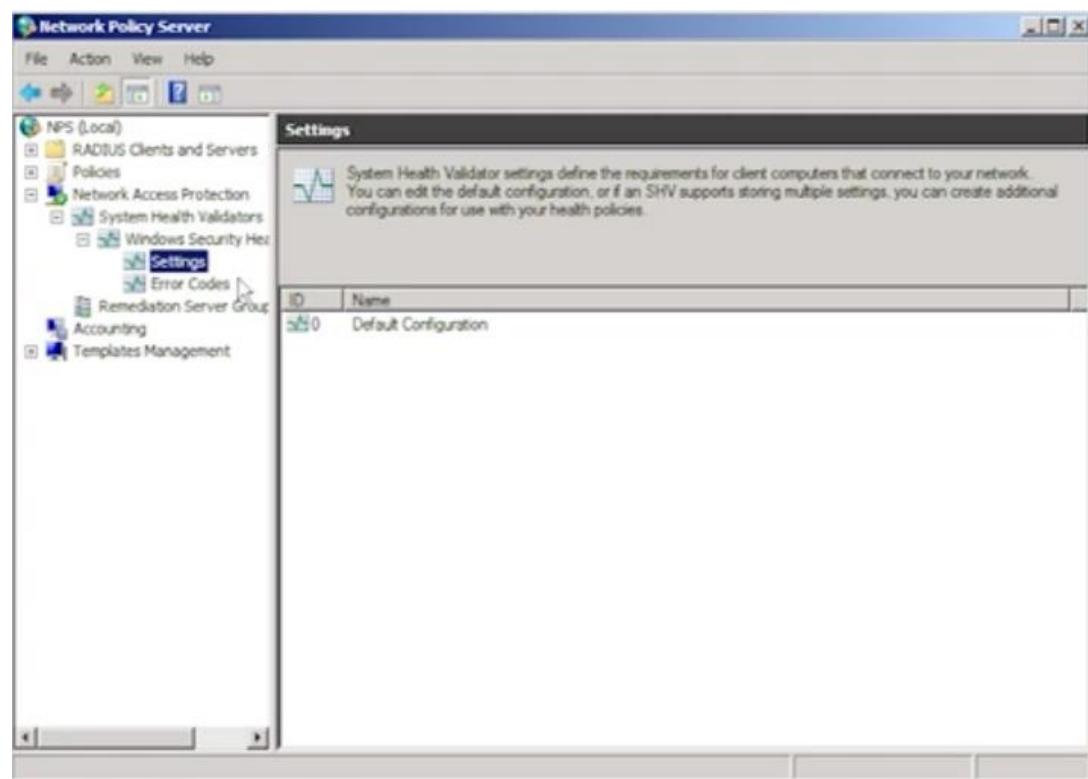
الخطوات:

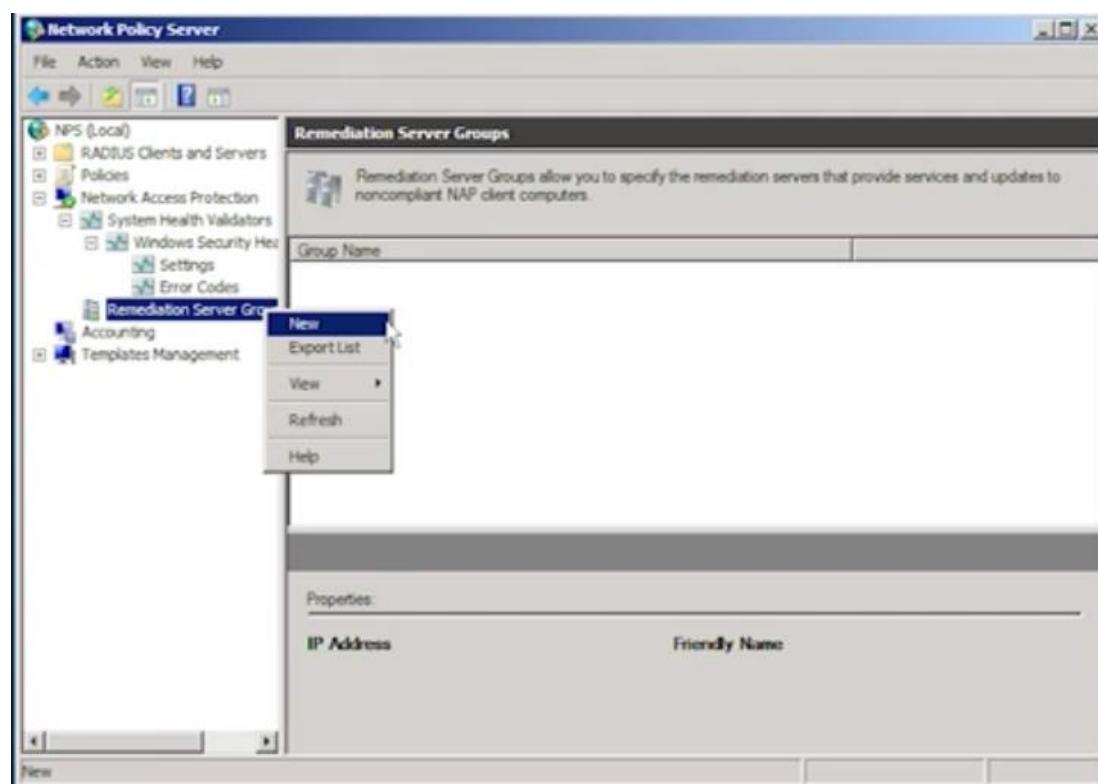
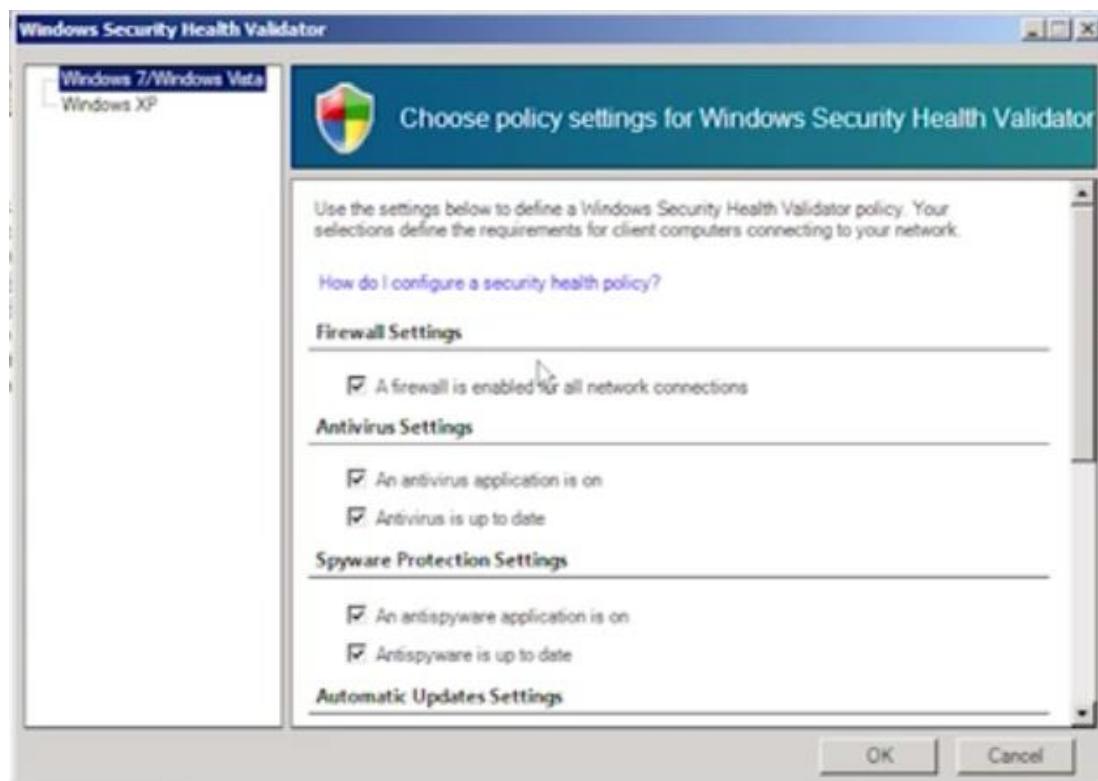
- تثبيت الـ NAP على كل من الـ DHCP Server والـ NAP Server الخاص بالـ NAP Server.
- اعداد الـ NAP Server.
- اضافة الـ WSUS الى مجموعة الـ Clients Remediation Server Group وذلك للسماح للـ Clients الذي يحتاج الى Update لكي يتمكن من الاتصال بالشبكة.
- انشاء الاتصال بين كلا من الـ NPS و الـ NPS.

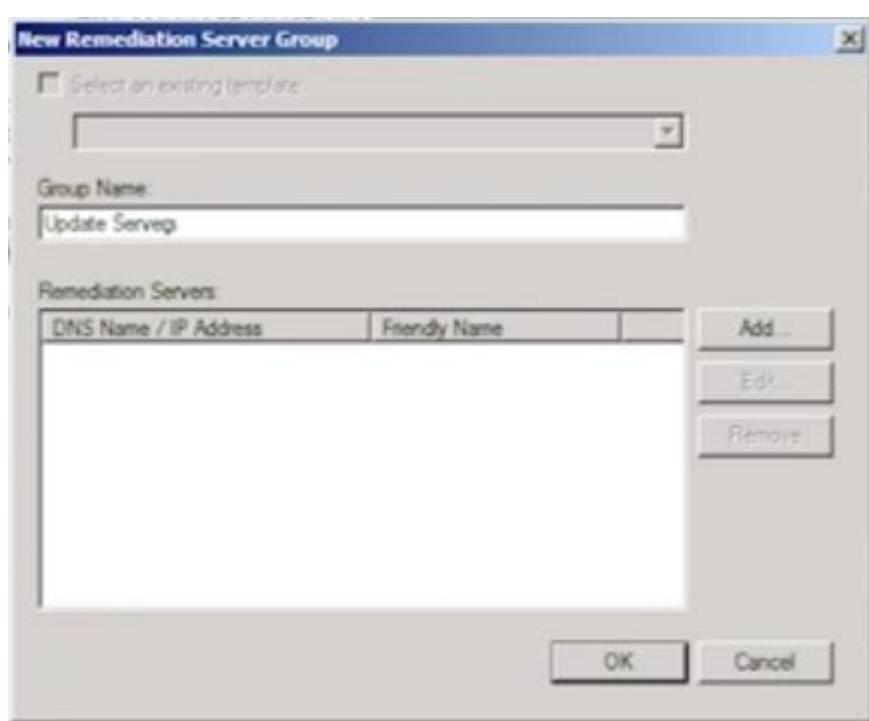
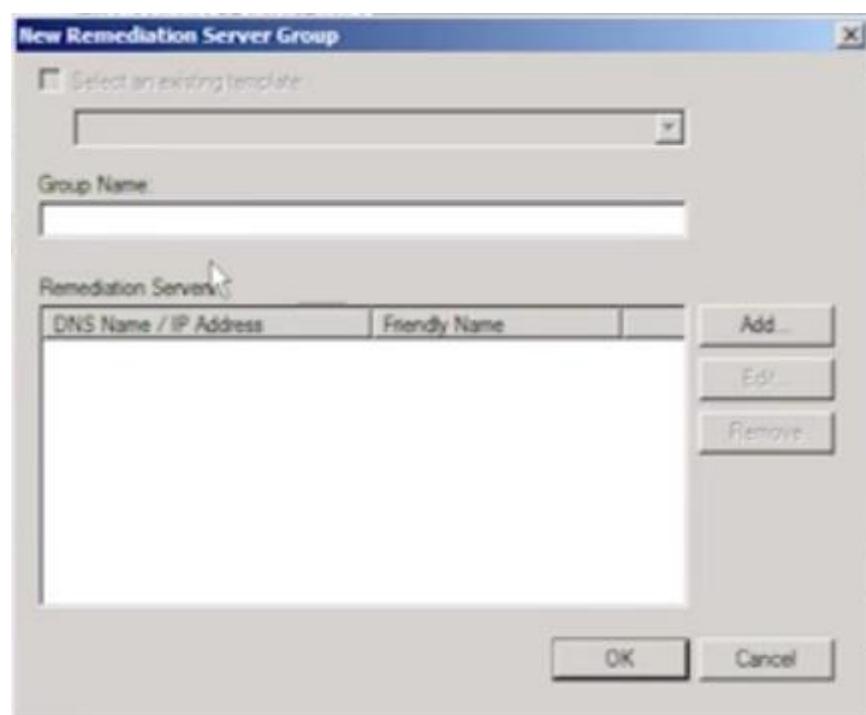
يتم ذلك على النحو التالي:

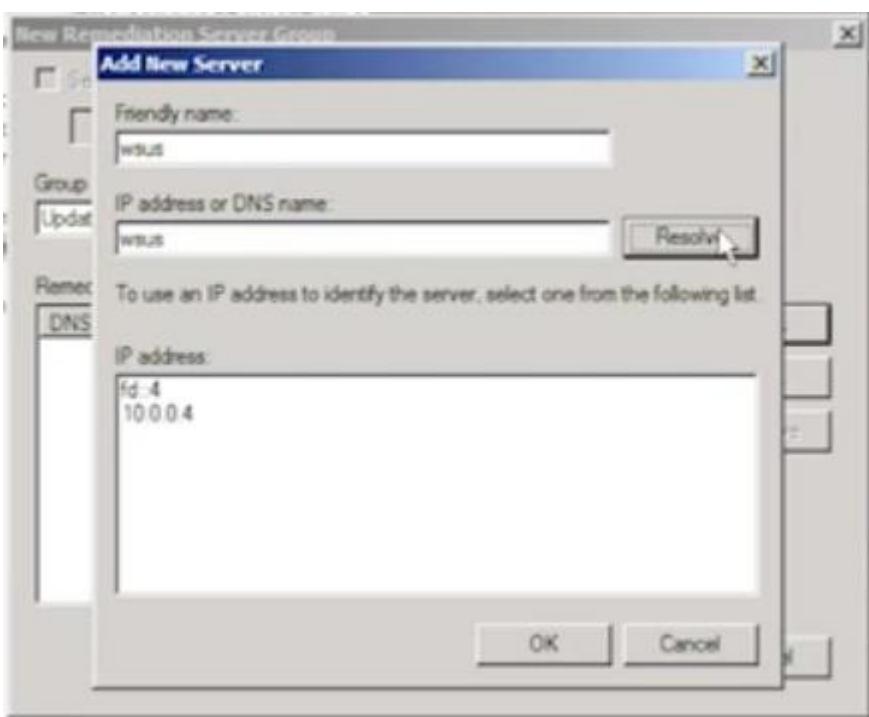
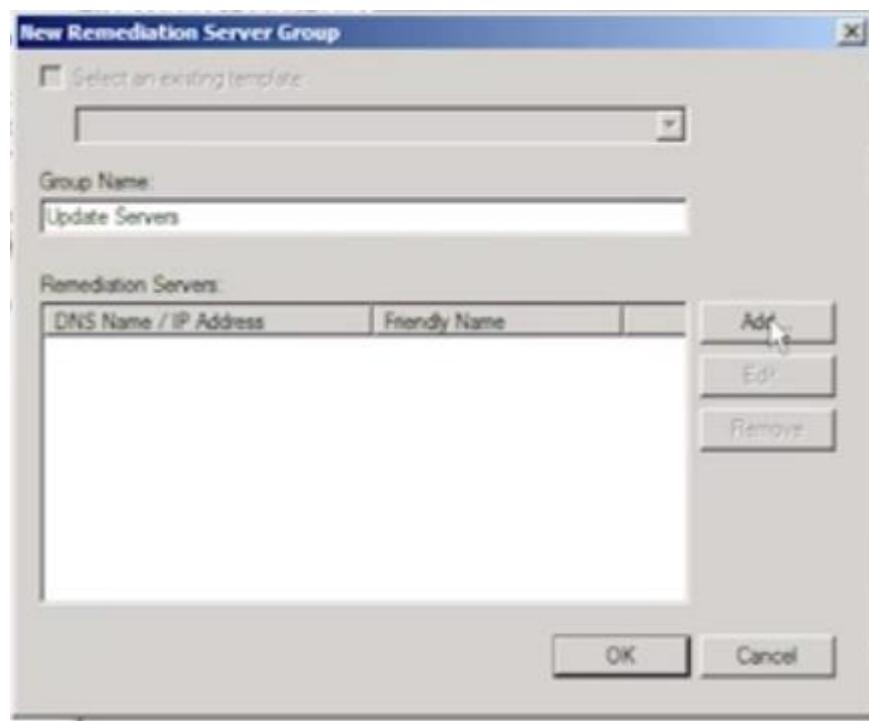














Network Policy Server

File Action View Help

NPS (Local)

Getting Started

Network Policy Server (NPS) allows you to create and enforce organization-wide network access policies for client health, connection request authentication, and connection request authorization.

Standard Configuration

Select a configuration scenario from the list and then click the link below to open the scenario wizard.

Network Access Protection (NAP)

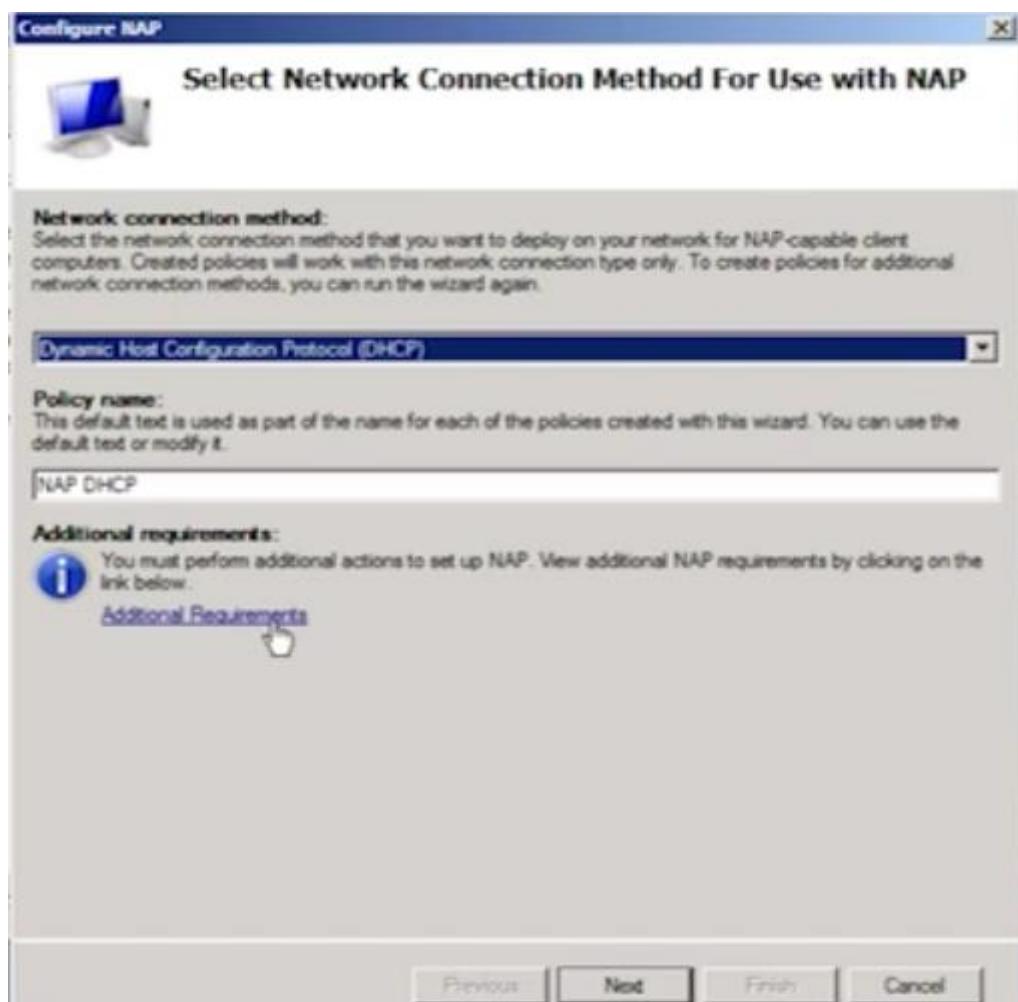
Network Access Protection (NAP)

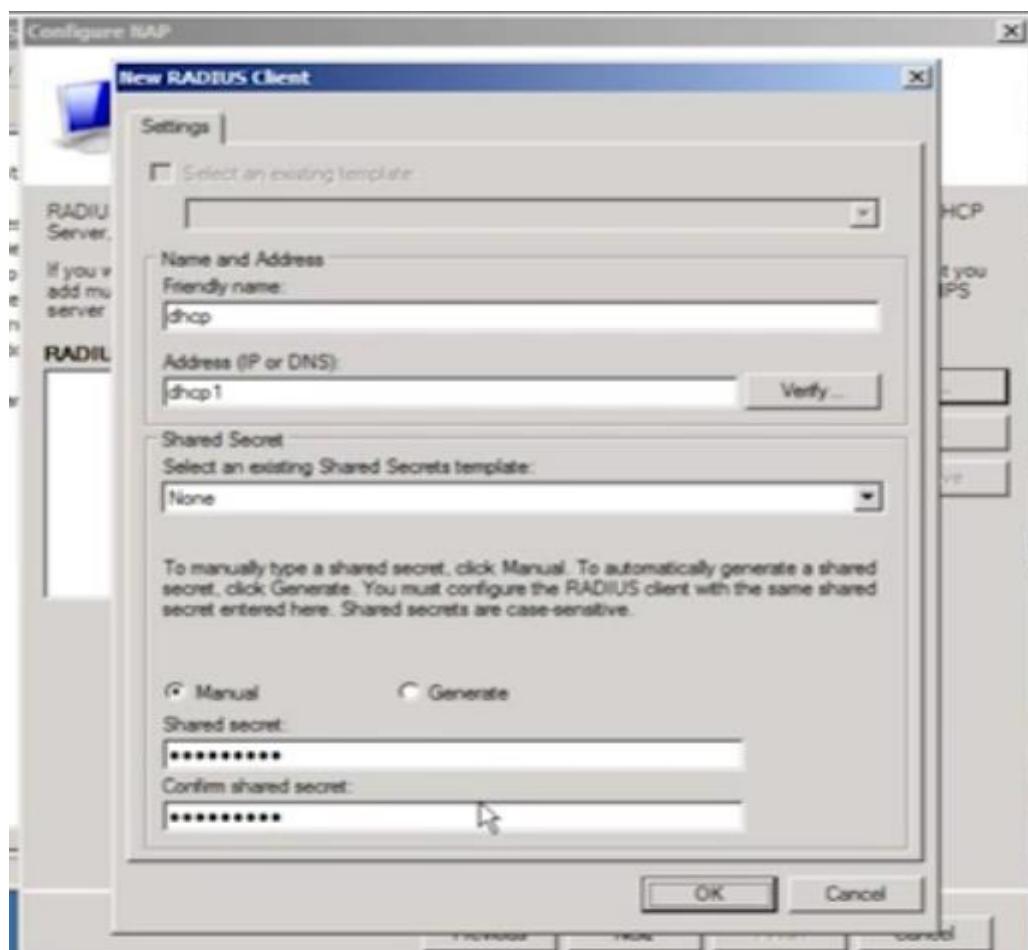
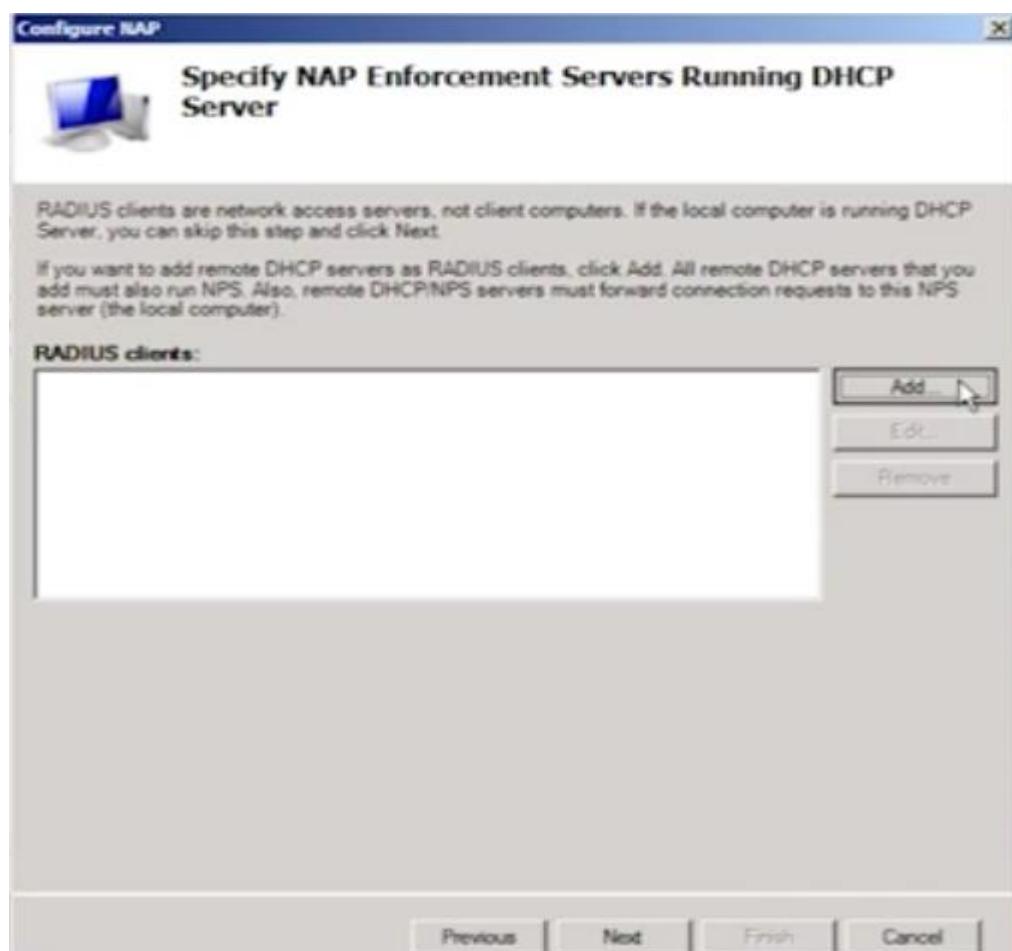
When you configure NPS as a NAP health policy server, you create health policies that allow NPS to validate the configuration of NAP-capable client computers before they connect to your network. Clients that are not compliant with health policy can be placed on a restricted network and automatically updated to bring them into compliance.

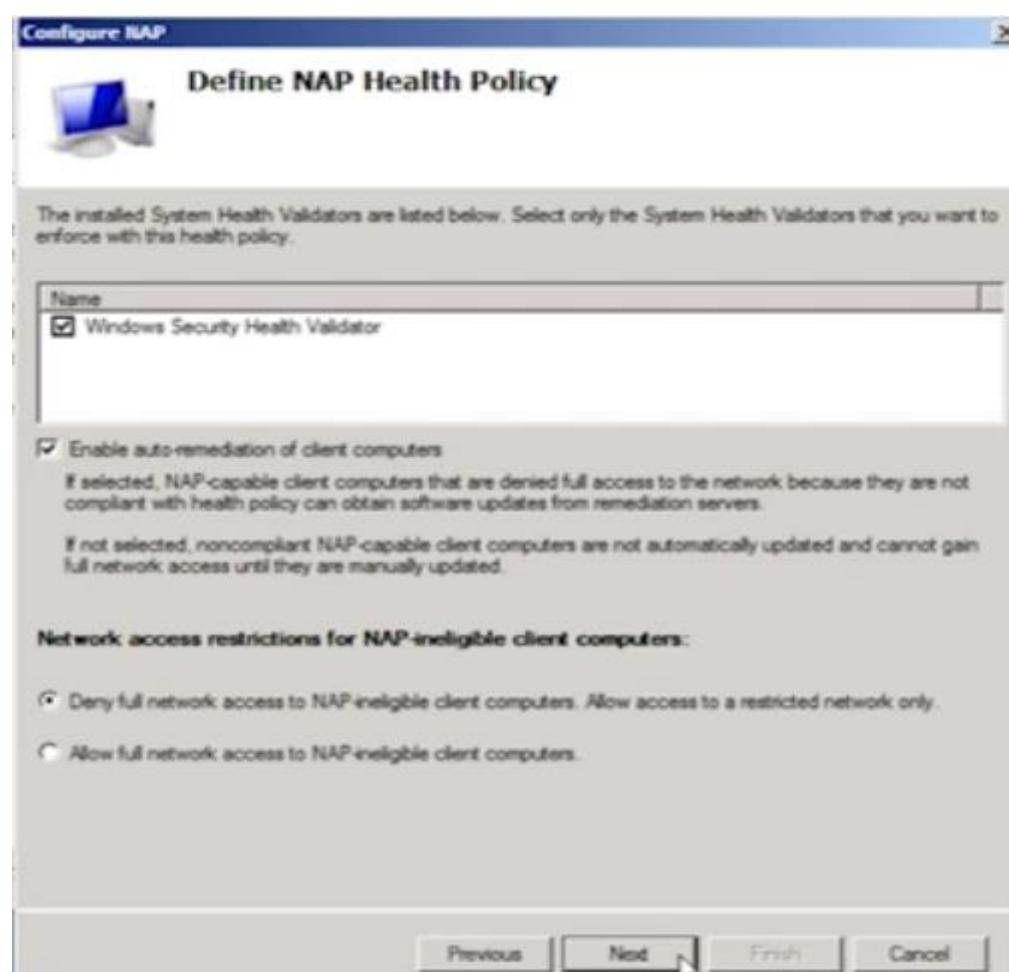
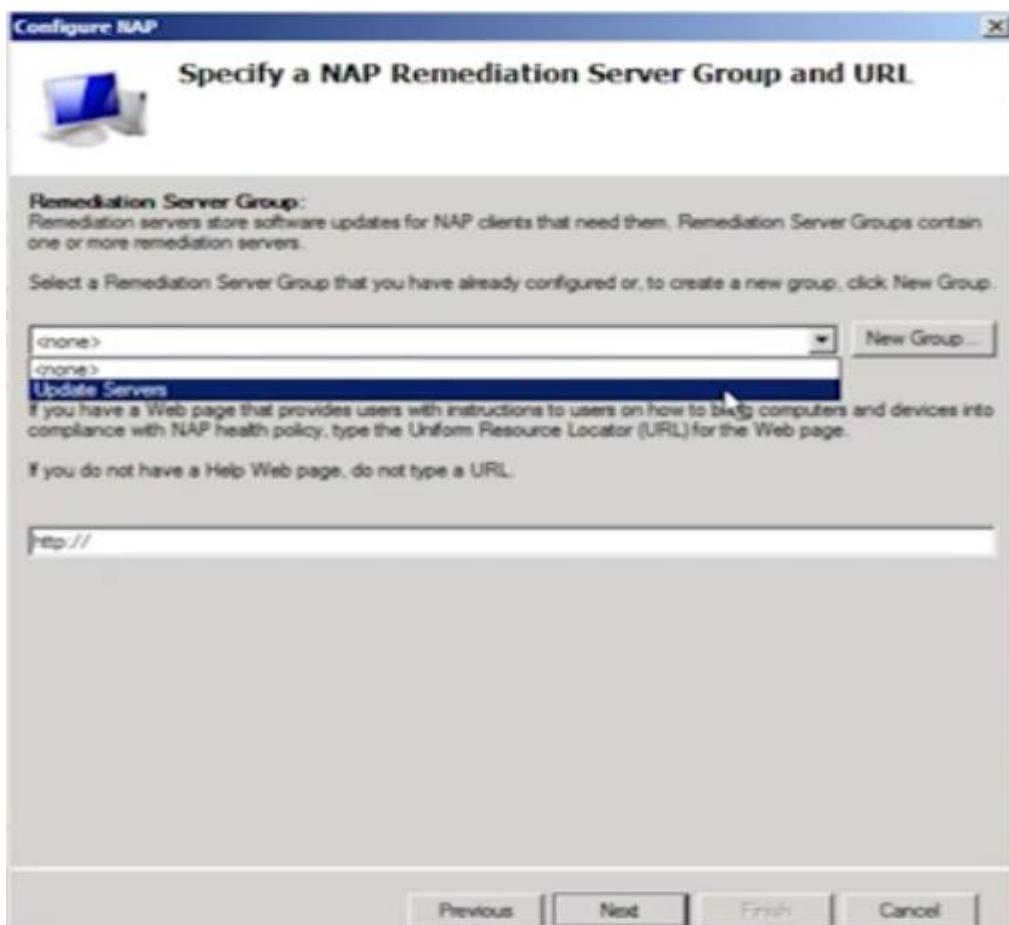
[Configure NAP](#) Learn more

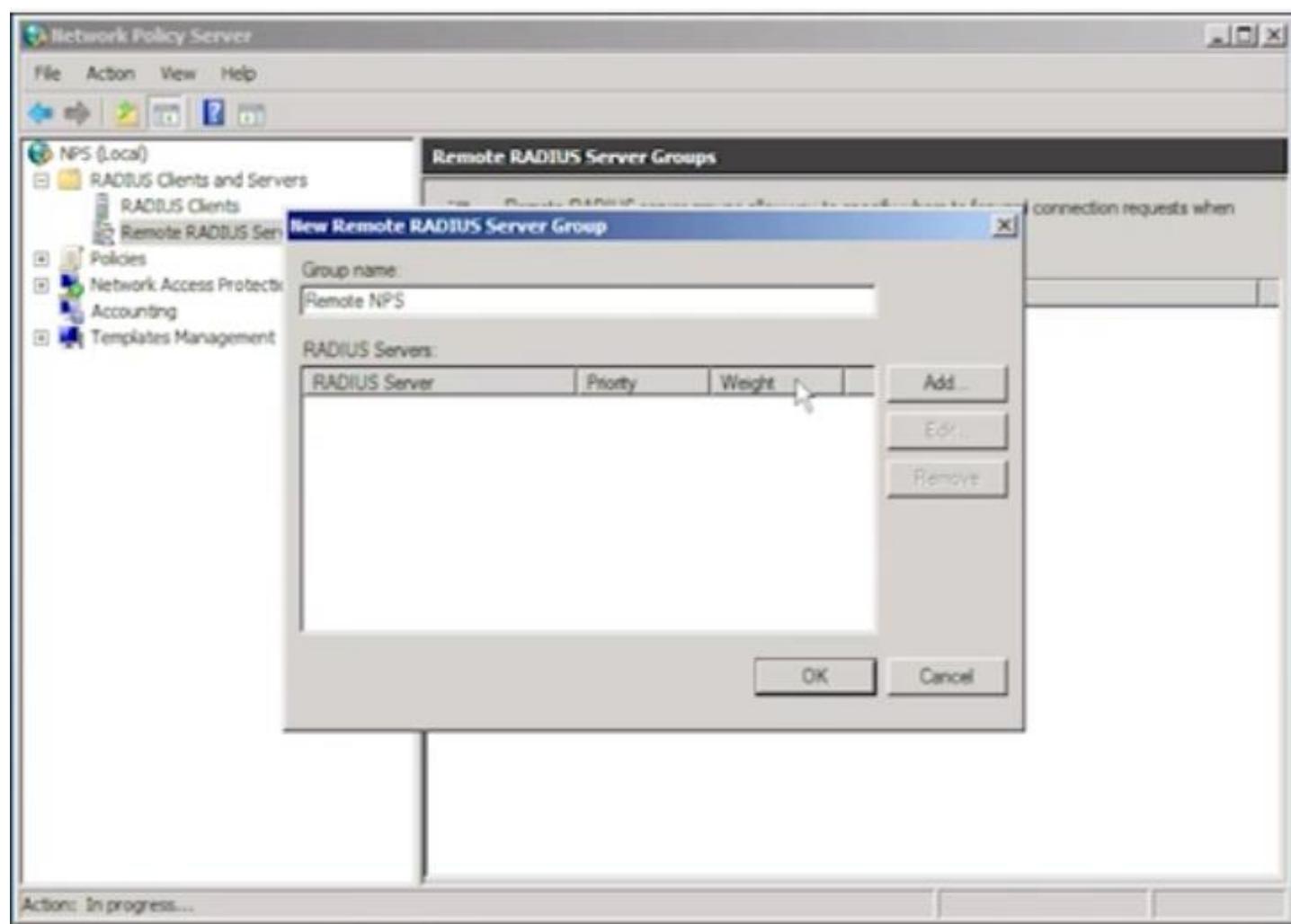
Advanced Configuration

Templates Configuration









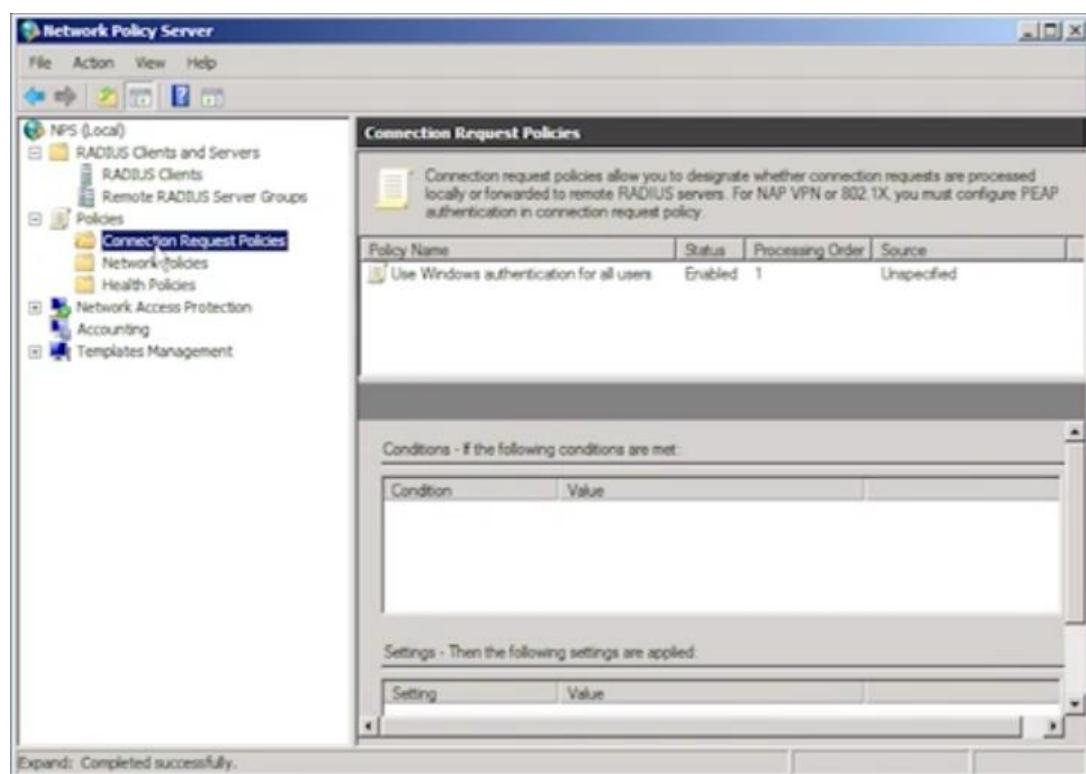
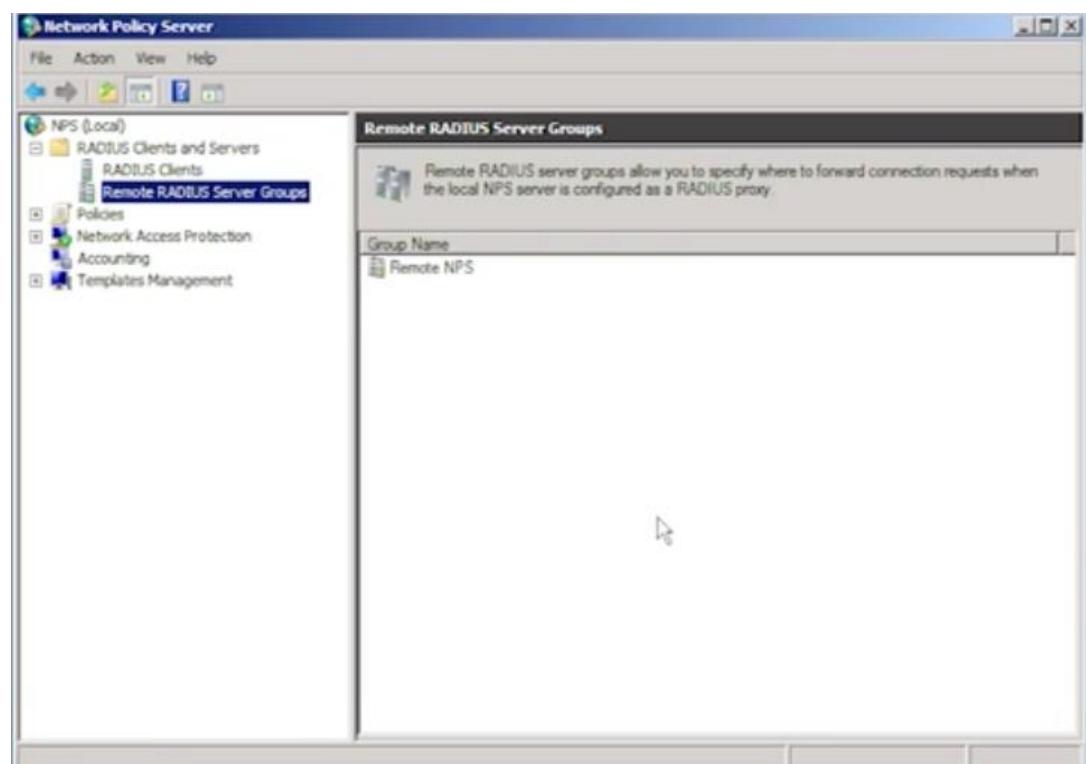
Add RADIUS Server

Address	Authentication/Accounting	Load Balancing
Authentication port: 1812		
Select an existing Shared Secrets template: None		
Shared secret:		
Confirm shared secret:		
<input type="checkbox"/> Request must contain the message authenticator attribute		
Accounting		
Accounting port: 1813		
<input checked="" type="checkbox"/> Use the same shared secret for authentication and accounting.		
Select an existing Shared Secrets template: None		
Shared secret:		
Confirm shared secret:		
<input checked="" type="checkbox"/> Forward network access server start and stop notifications to this server		

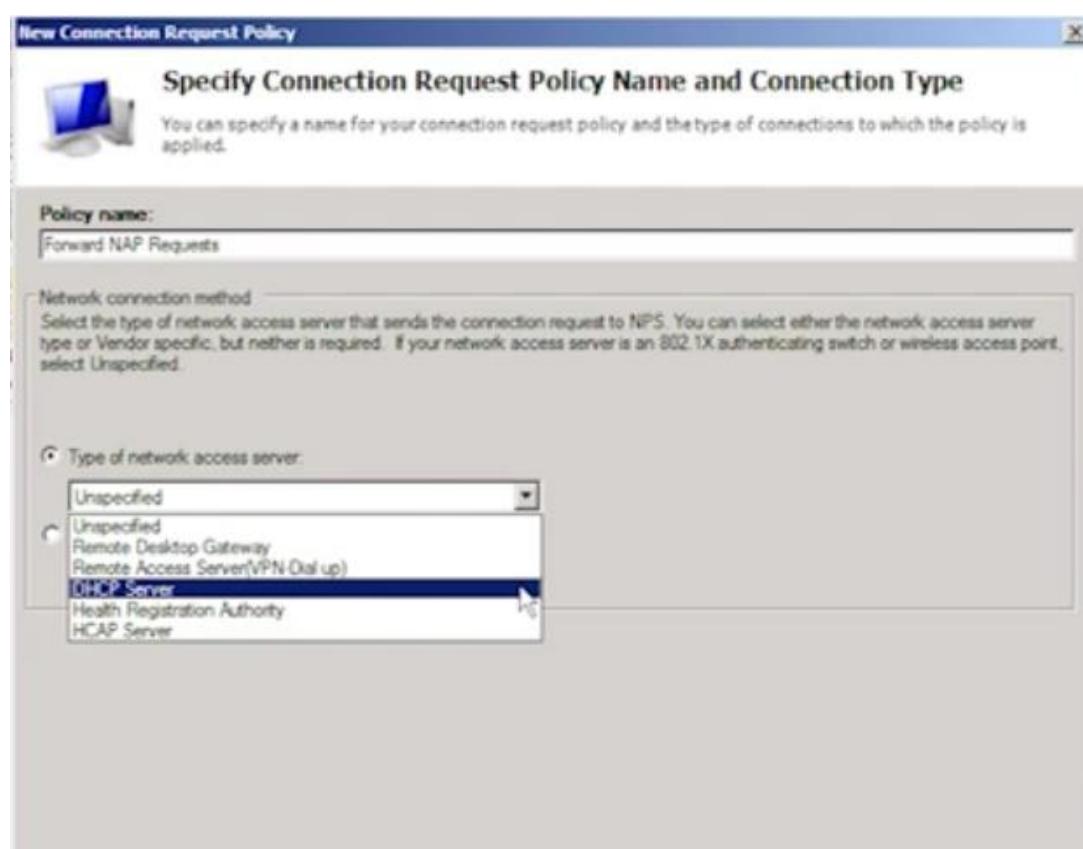
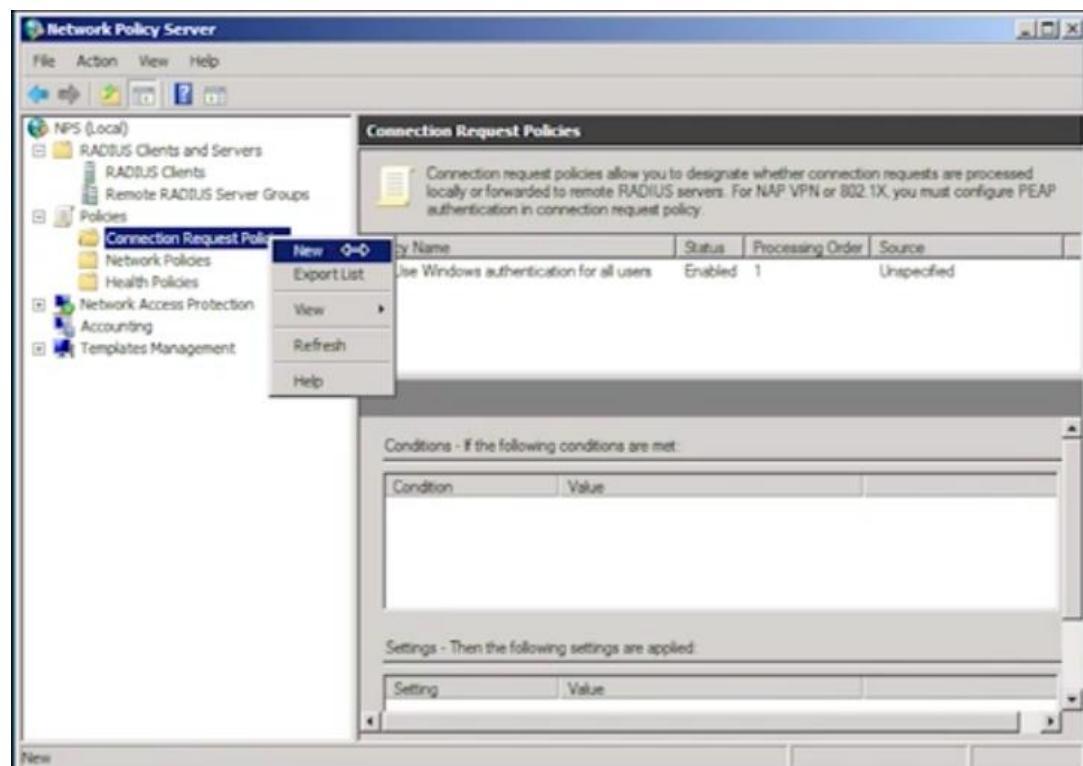
New Remote RADIUS Server Group

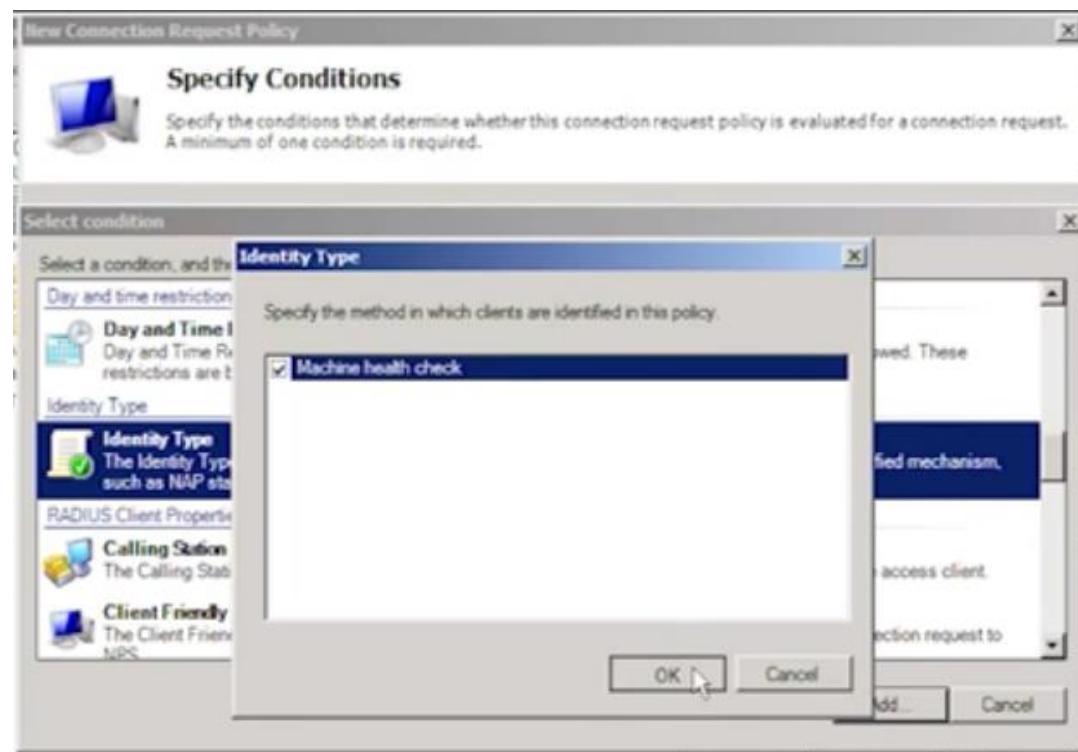
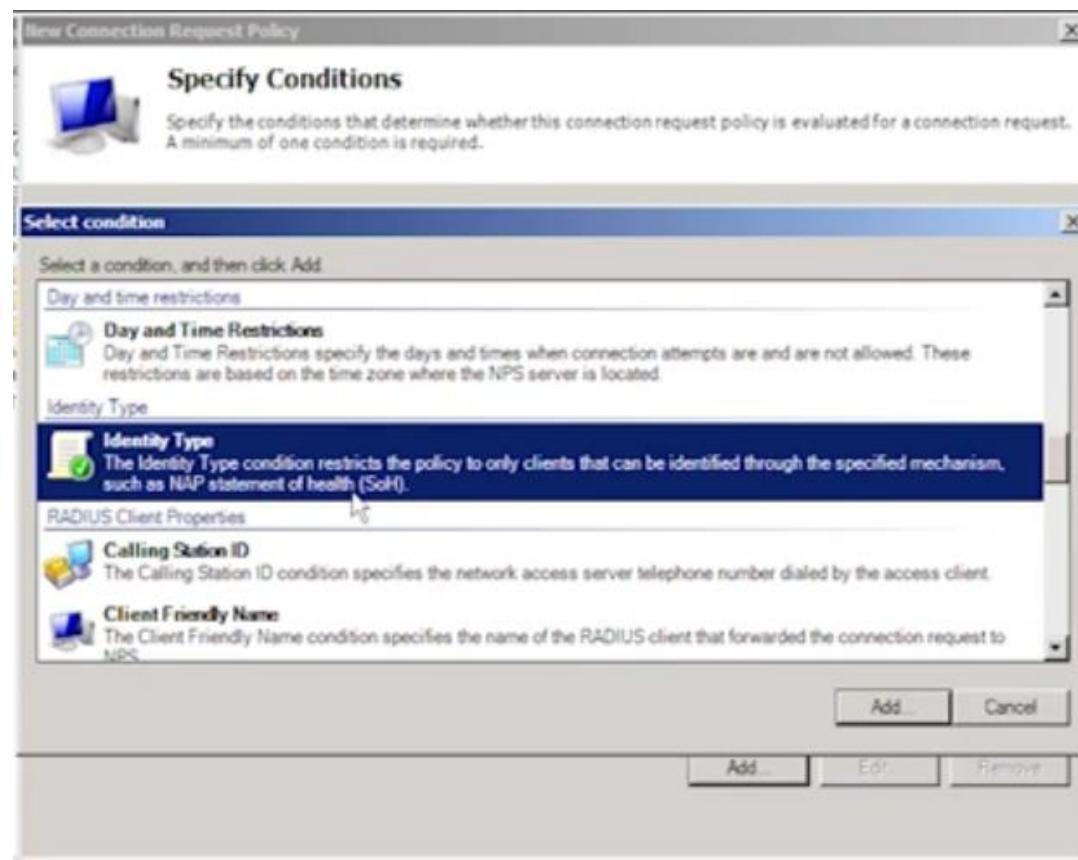
Group name: Remote NPS	Add...						
RADIUS Servers:	Edit...						
<table border="1"> <thead> <tr> <th>RADIUS Server</th> <th>Priority</th> <th>Weight</th> </tr> </thead> <tbody> <tr> <td>nip</td> <td>1</td> <td>50</td> </tr> </tbody> </table>	RADIUS Server	Priority	Weight	nip	1	50	Remove
RADIUS Server	Priority	Weight					
nip	1	50					

OK Cancel



[Expand] Completed successfully.







New Connection Request Policy

Specify Conditions

Specify the conditions that determine whether this connection request policy is evaluated for a connection request. A minimum of one condition is required.

Conditions:

Condition	Value
Identity Type	Machine health check

Condition description:

Add... Edit... Remove

New Connection Request Policy

Specify Connection Request Forwarding

The connection request can be authenticated by the local server or it can be forwarded to RADIUS servers in a remote RADIUS server group.

If the policy conditions match the connection request, these settings are applied.

Settings:

Forwarding Connection Request

- Authentication
- Accounting

Specify whether connection requests are processed locally, are forwarded to remote RADIUS servers for authentication, or are accepted without authentication.

Authenticate requests on this server

Forward requests to the following remote RADIUS server group for authentication:

Remote NPS

Accept users without validating credentials

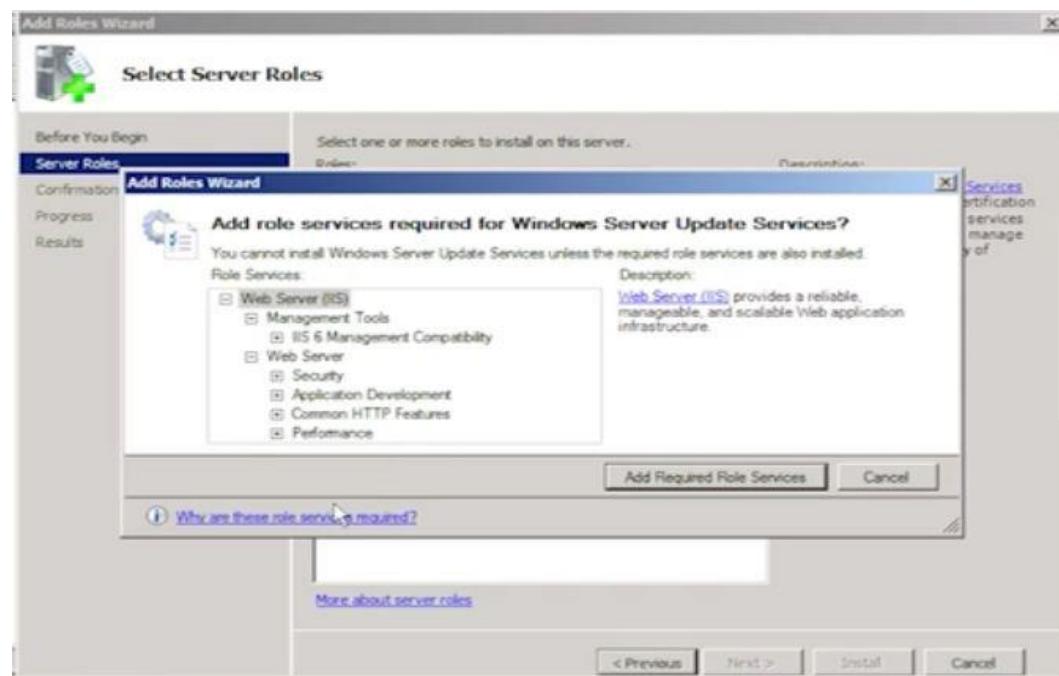
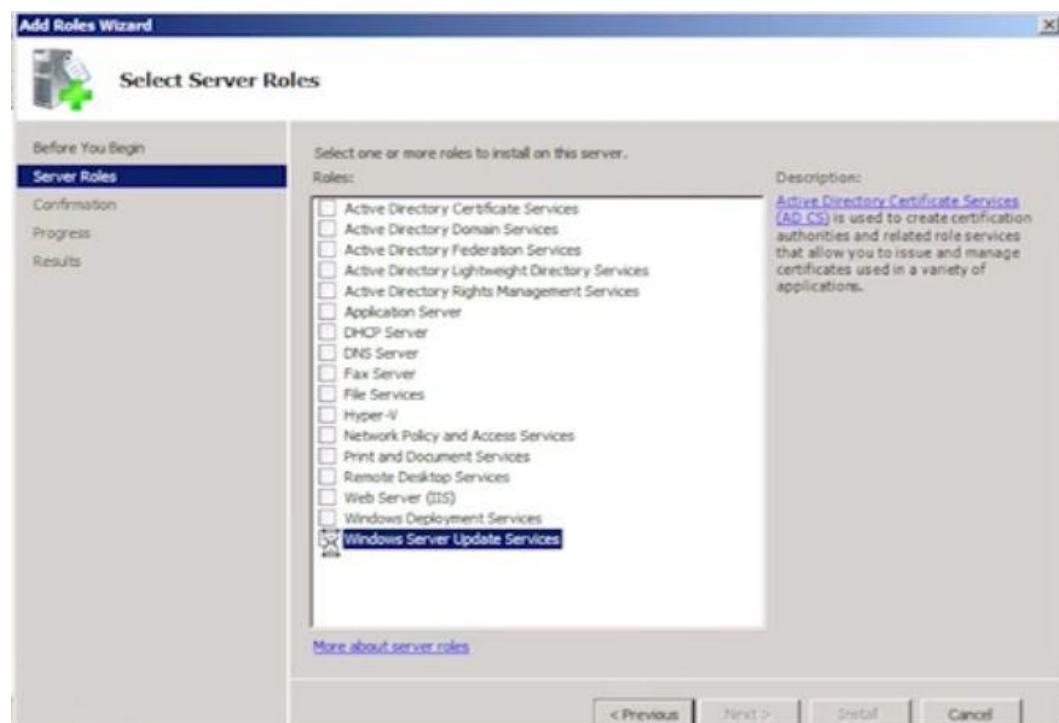


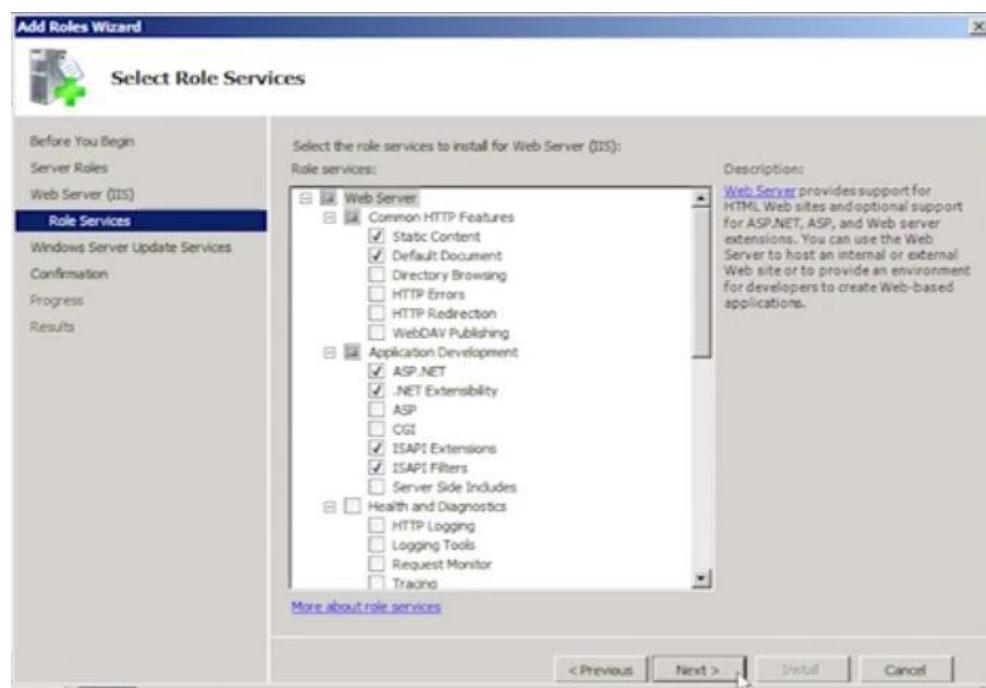
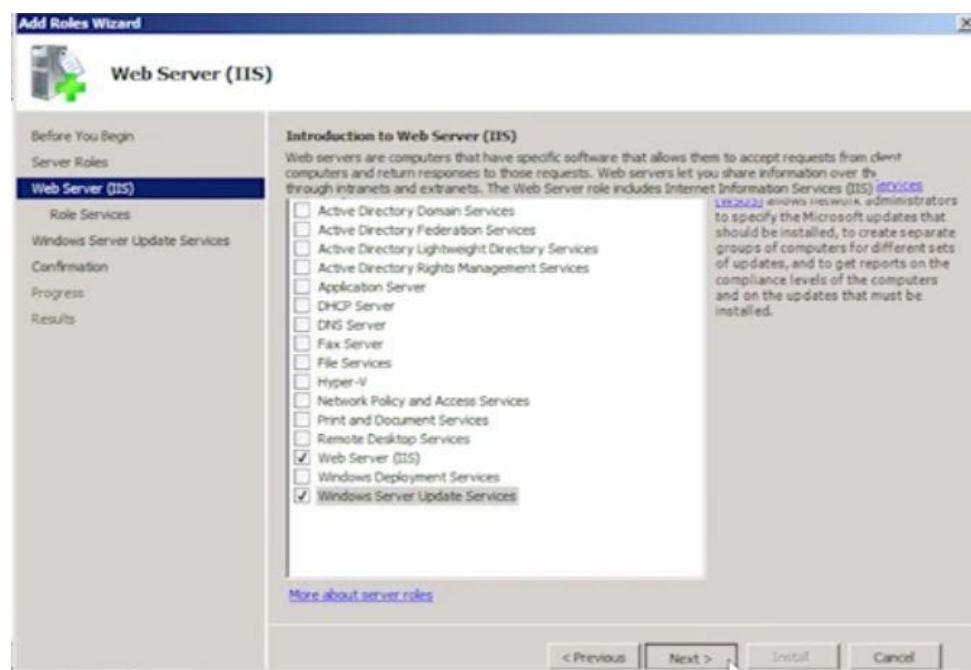
WSUS Windows Software Update Server

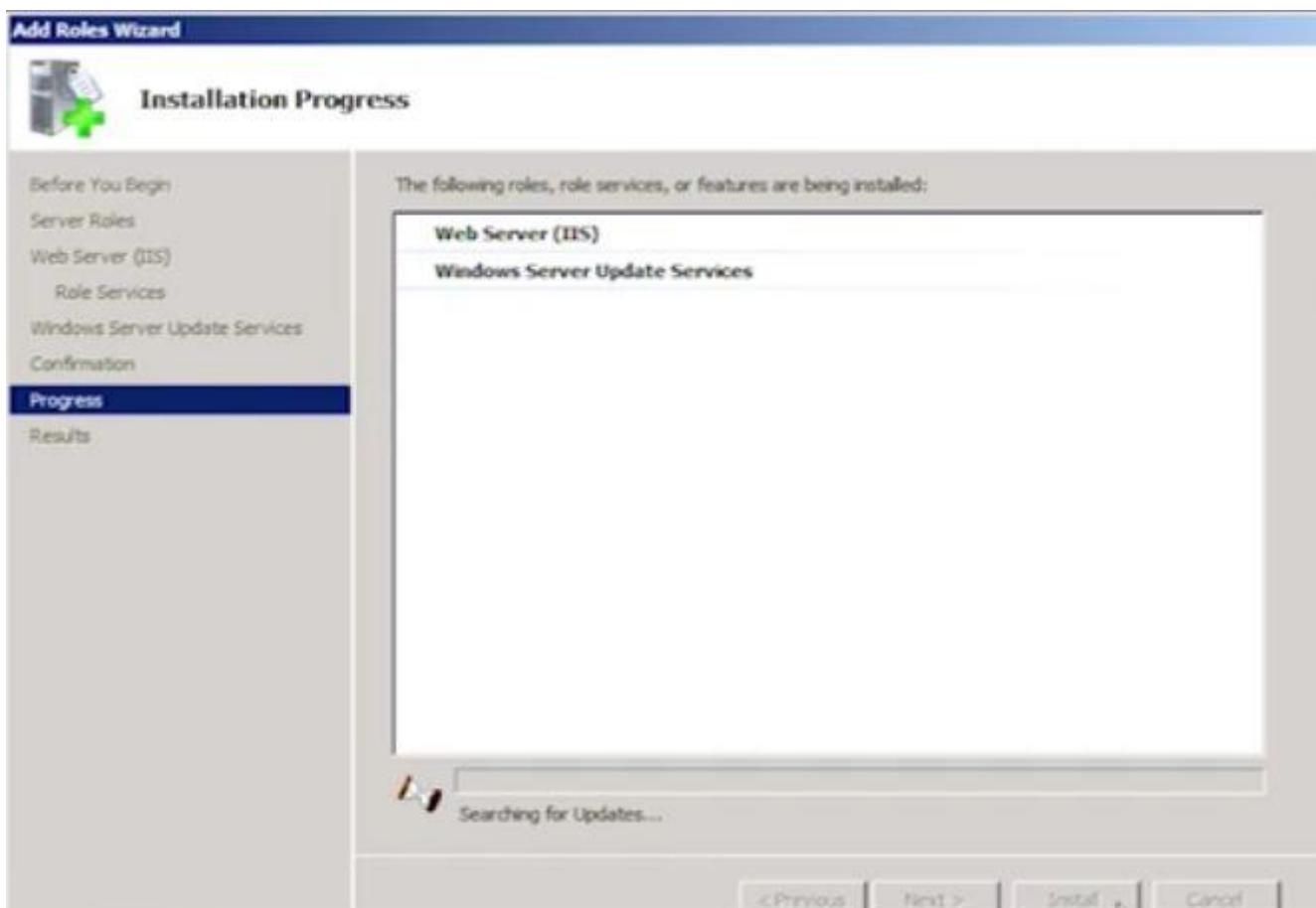
يتم اعداد هذا المخدم على مراحلتين:

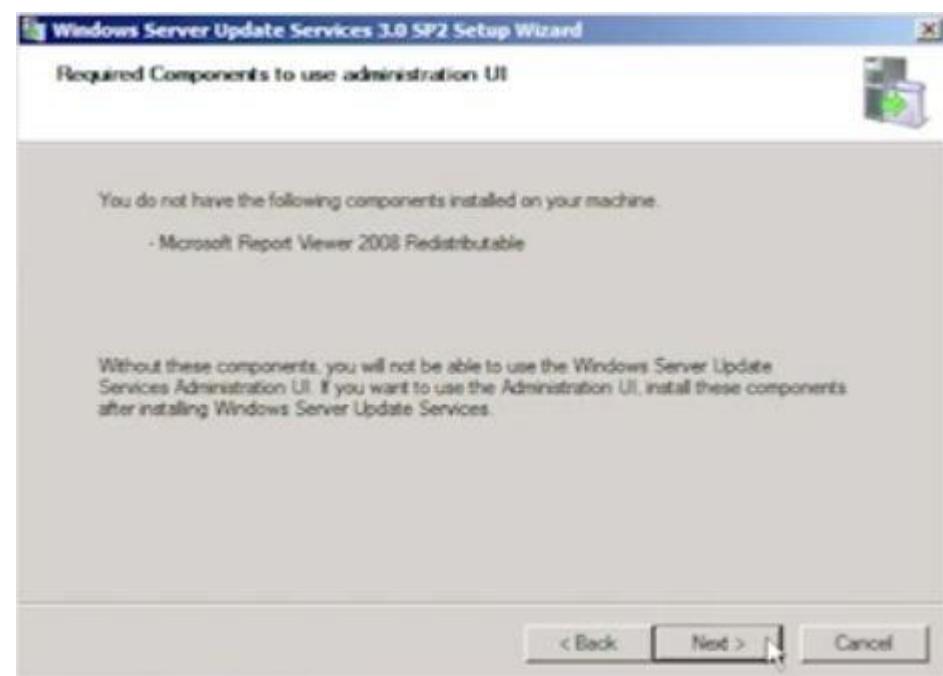
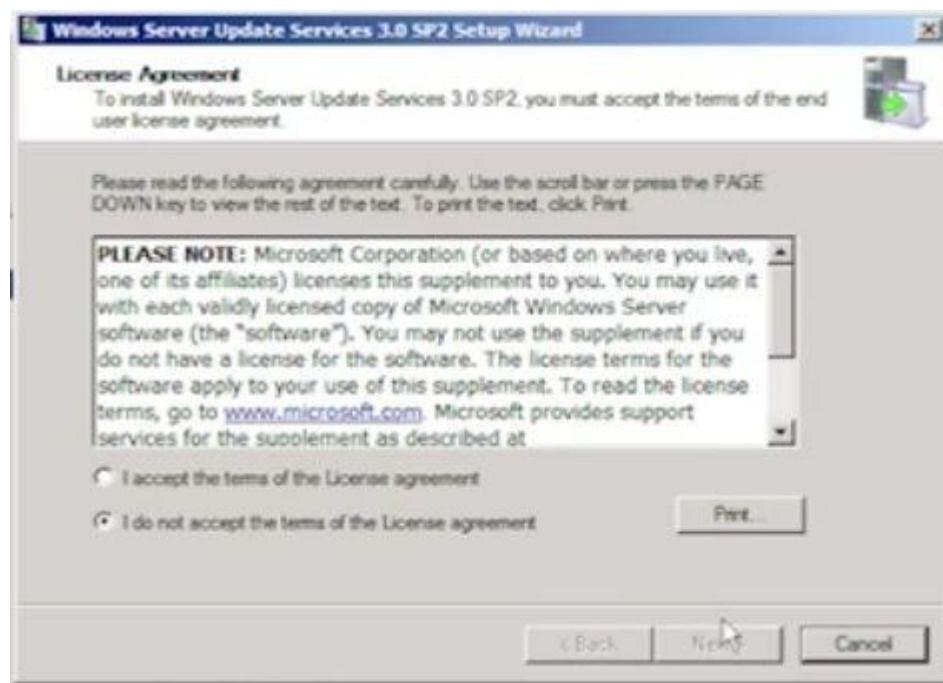
- 1- التنصيب: ويتم فيها تنصيب الخدمات والميزات التي يحتاجها WSUS ليعمل
- 2- الاعداد: اعداد WSUS لتحديد ما البرامج والأنظمة التي سوف يحمل لها تحديثات كما كيفية تنزيل التحديثات وكيفية ايصالها للClient.

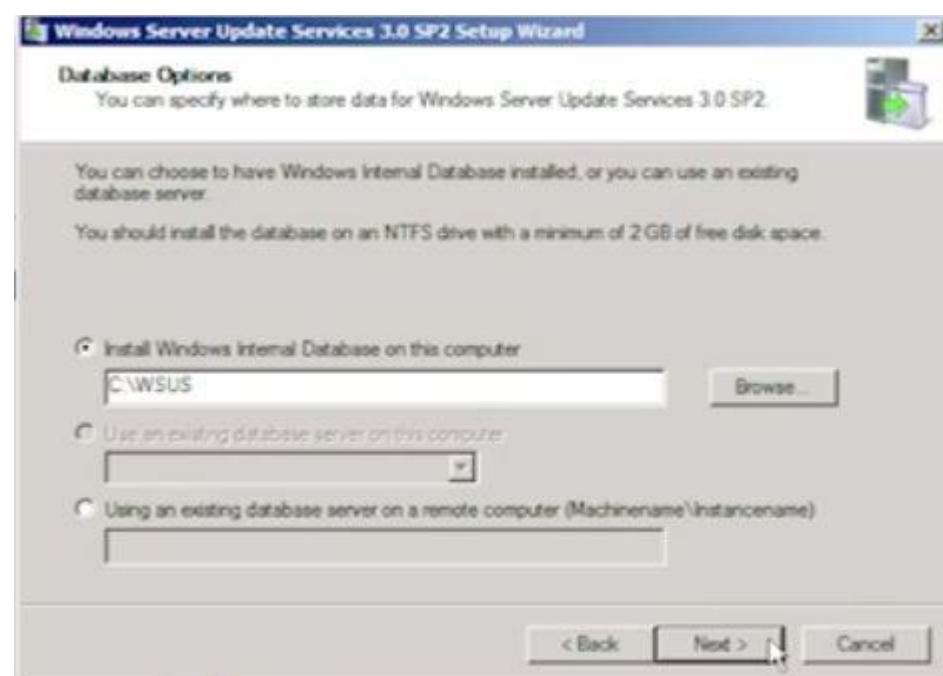
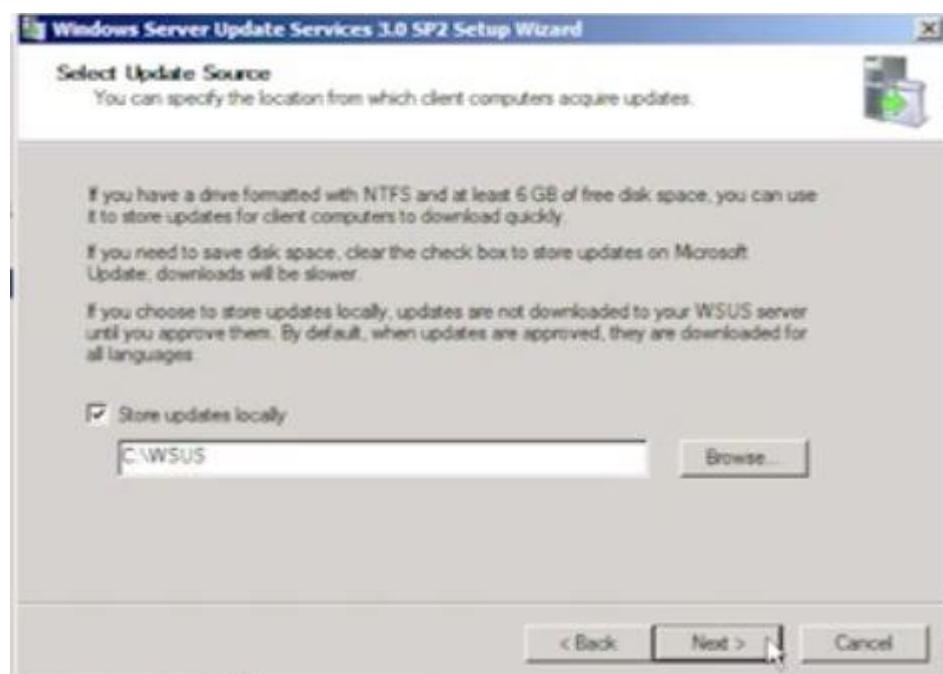
يتم ذلك على الشكل التالي:

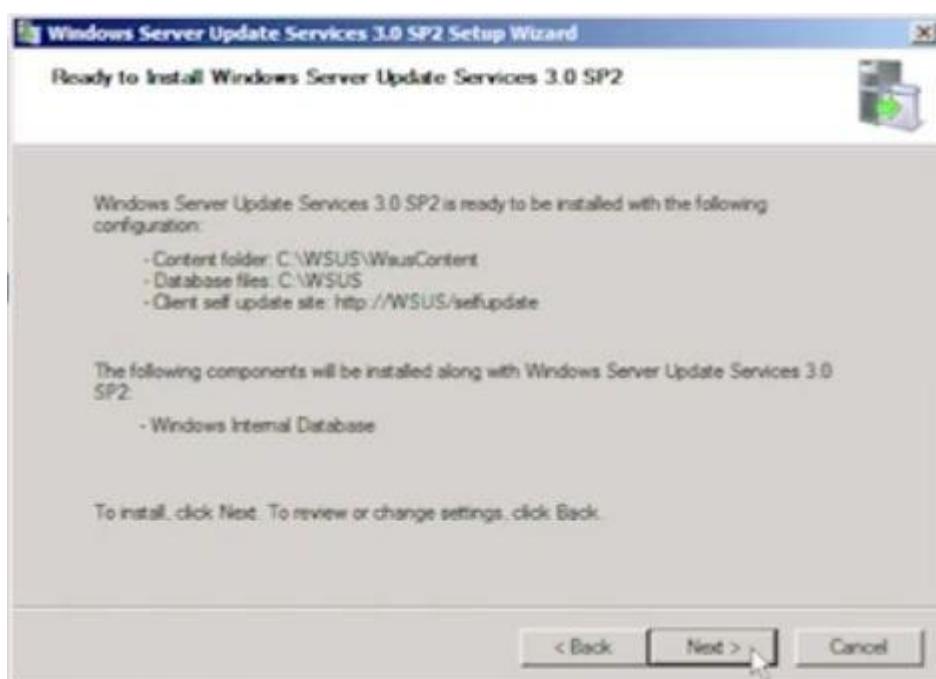
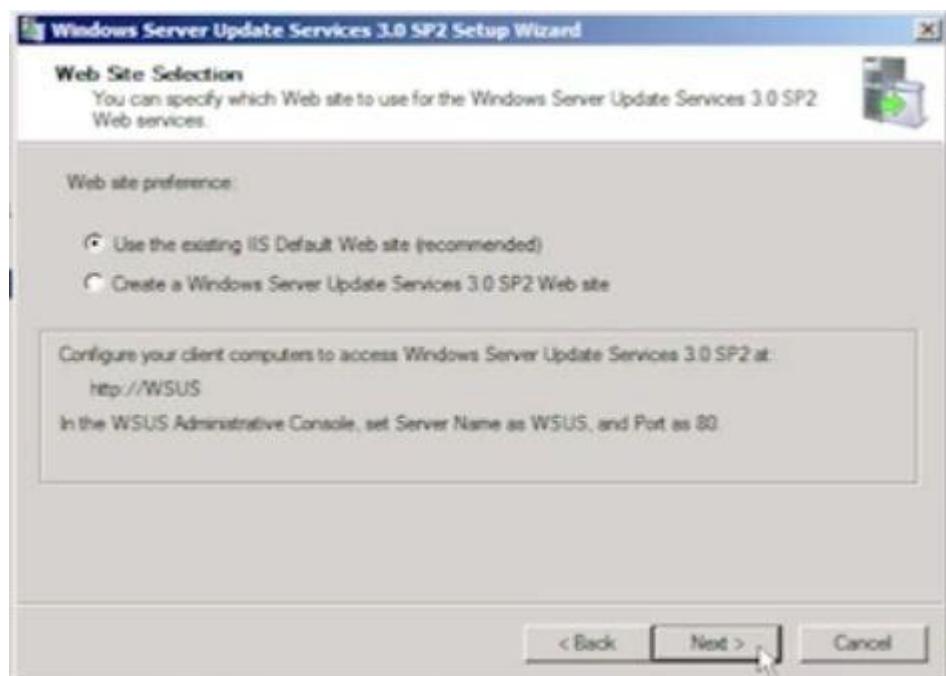


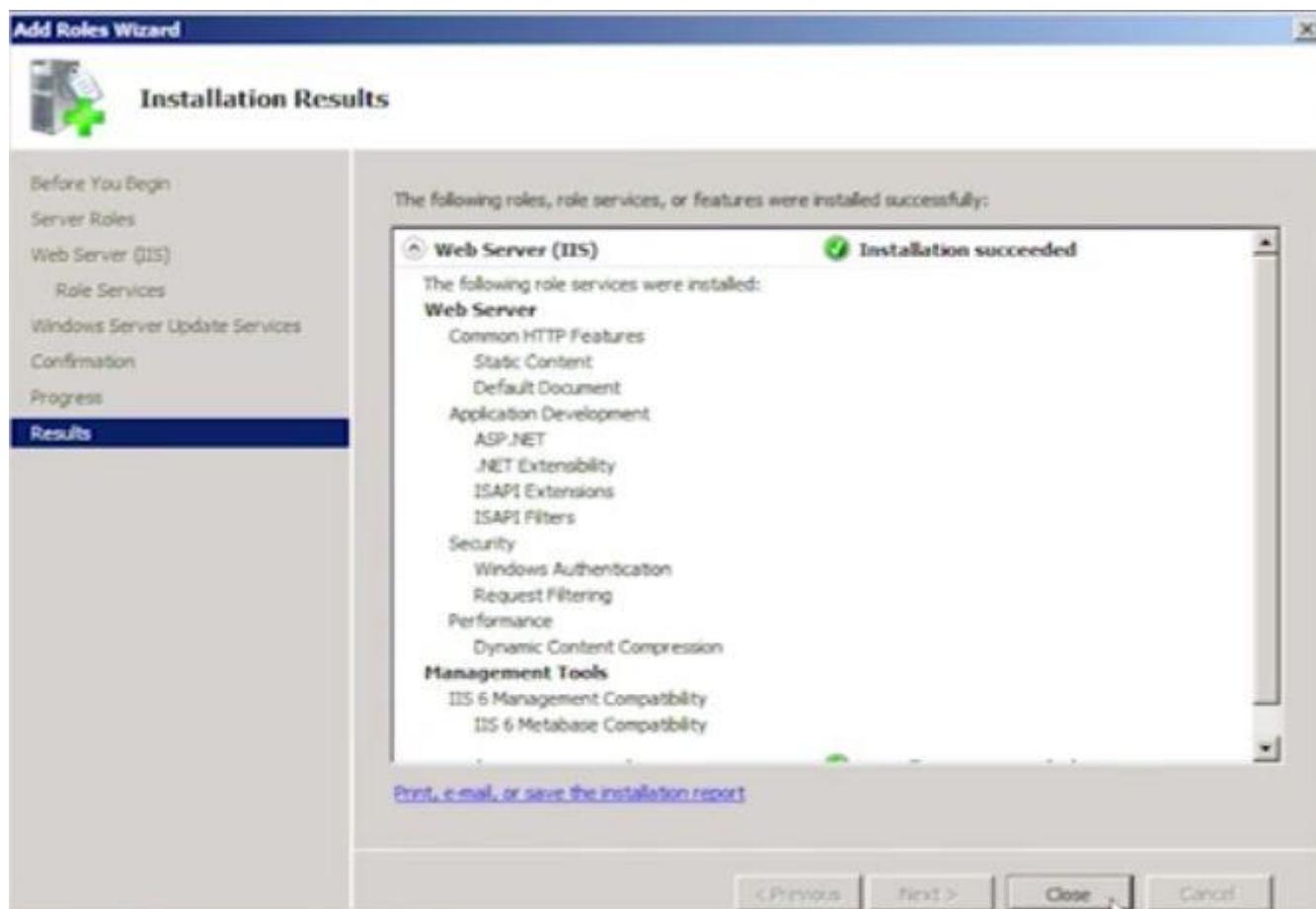
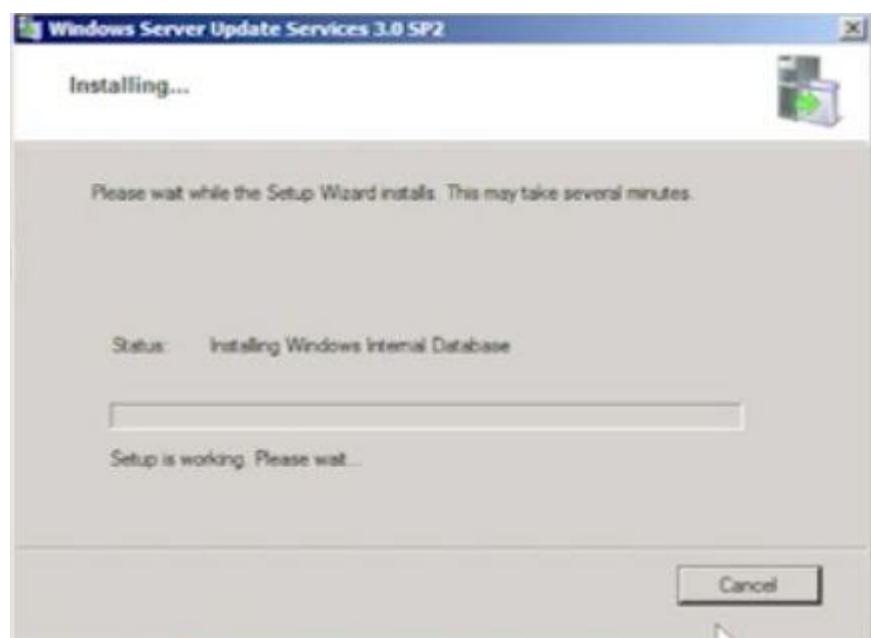


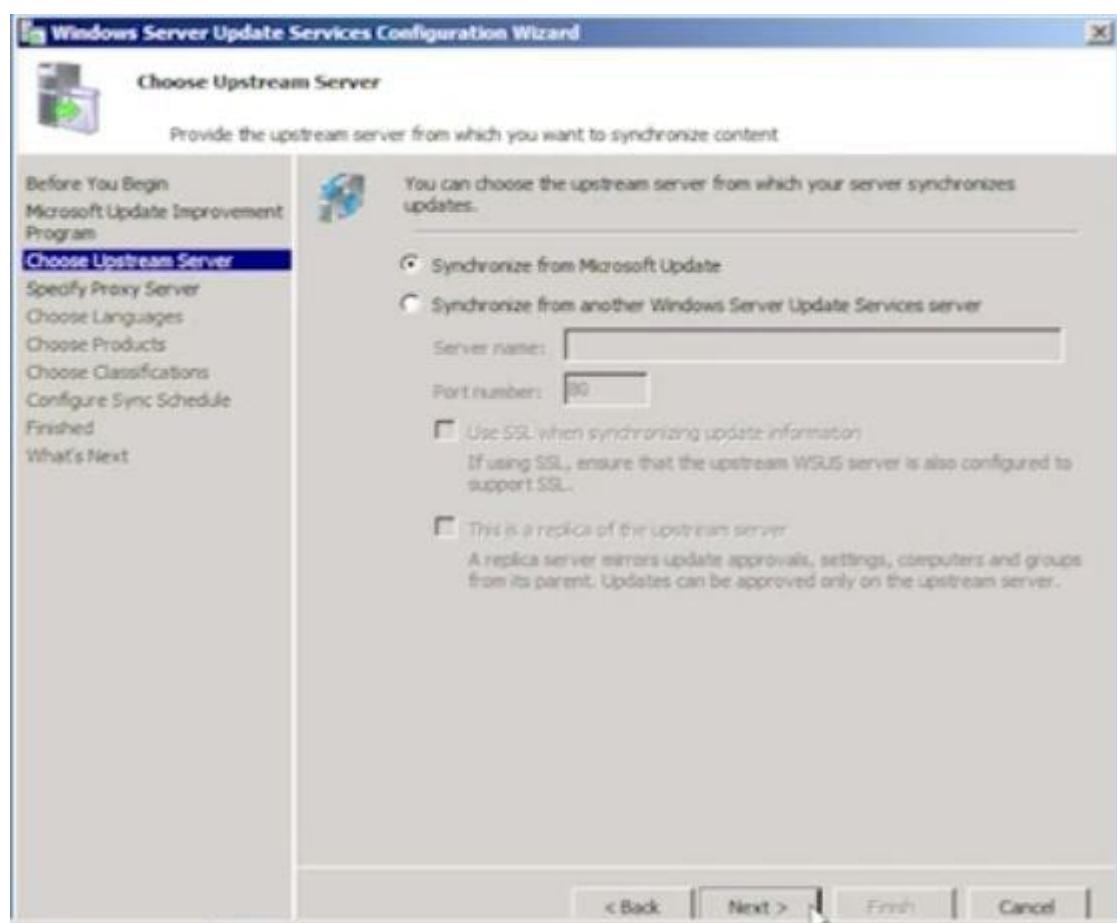
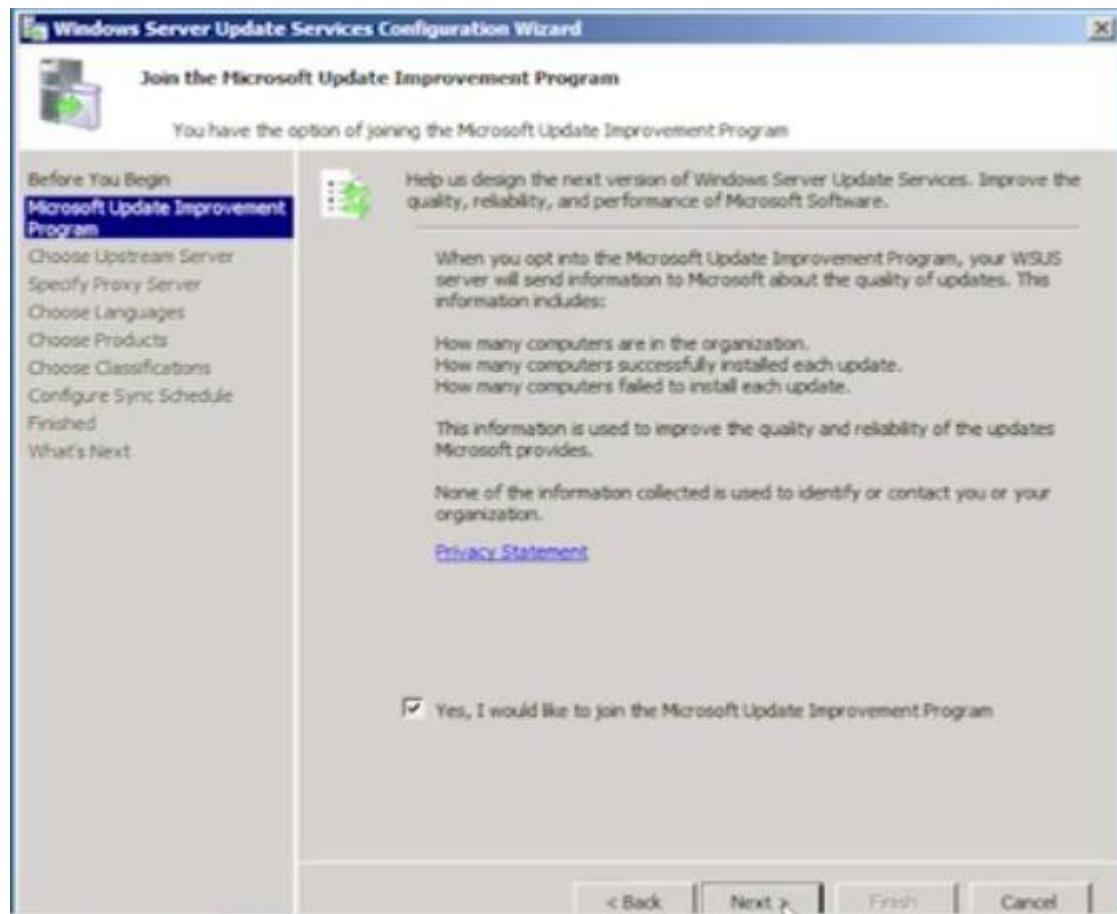


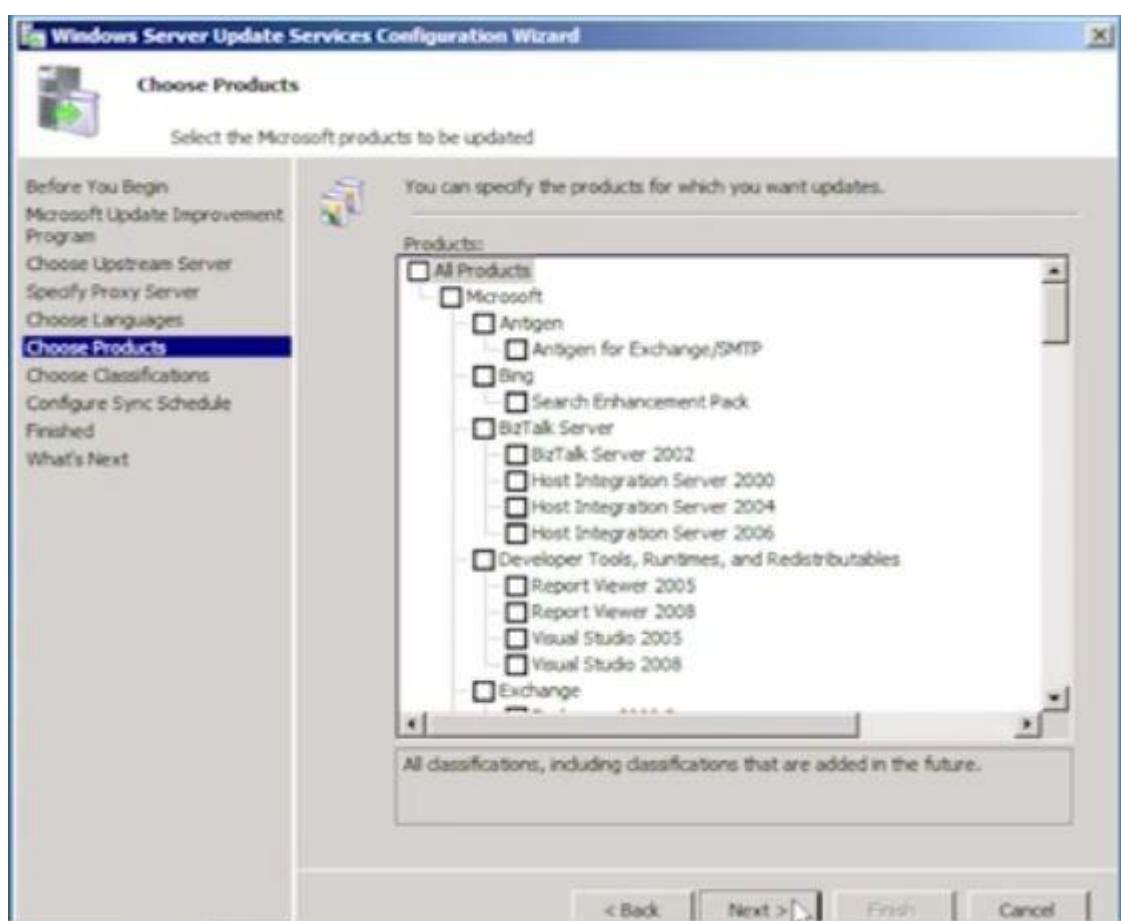
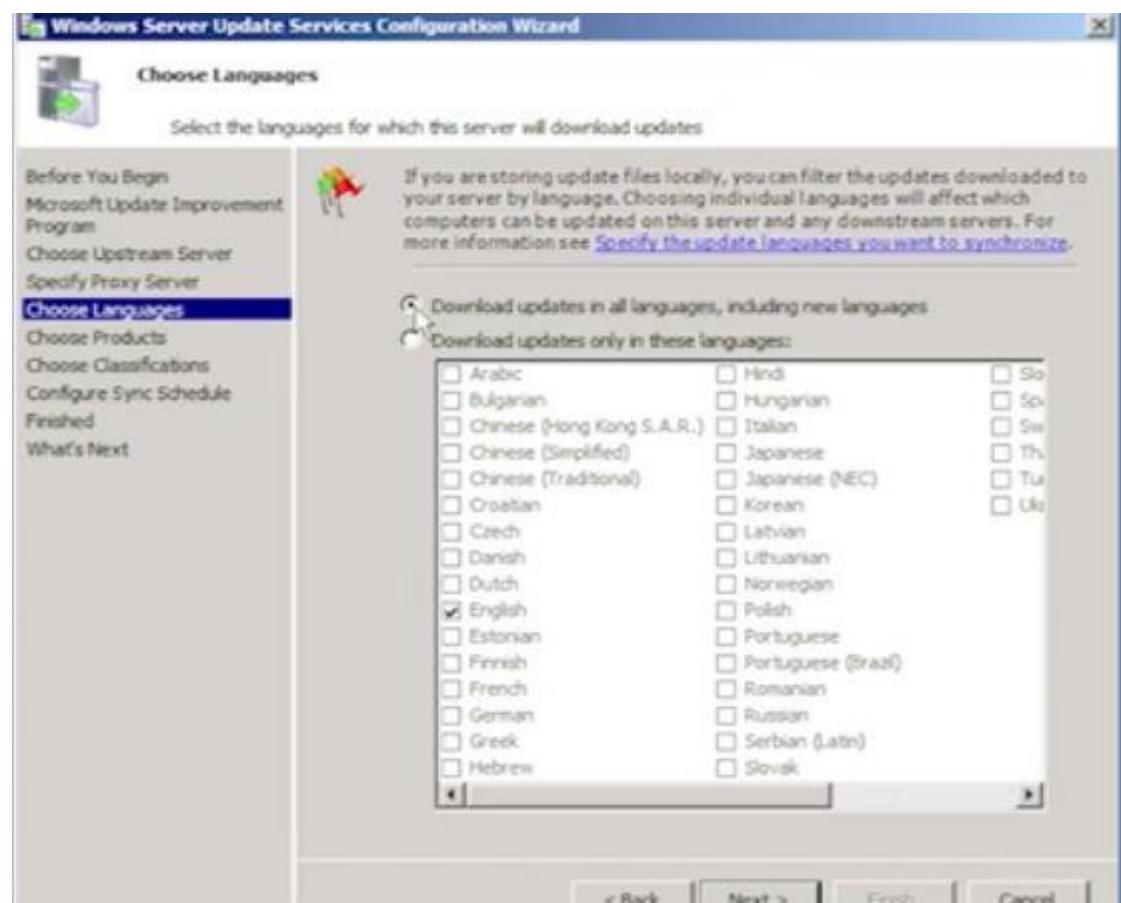


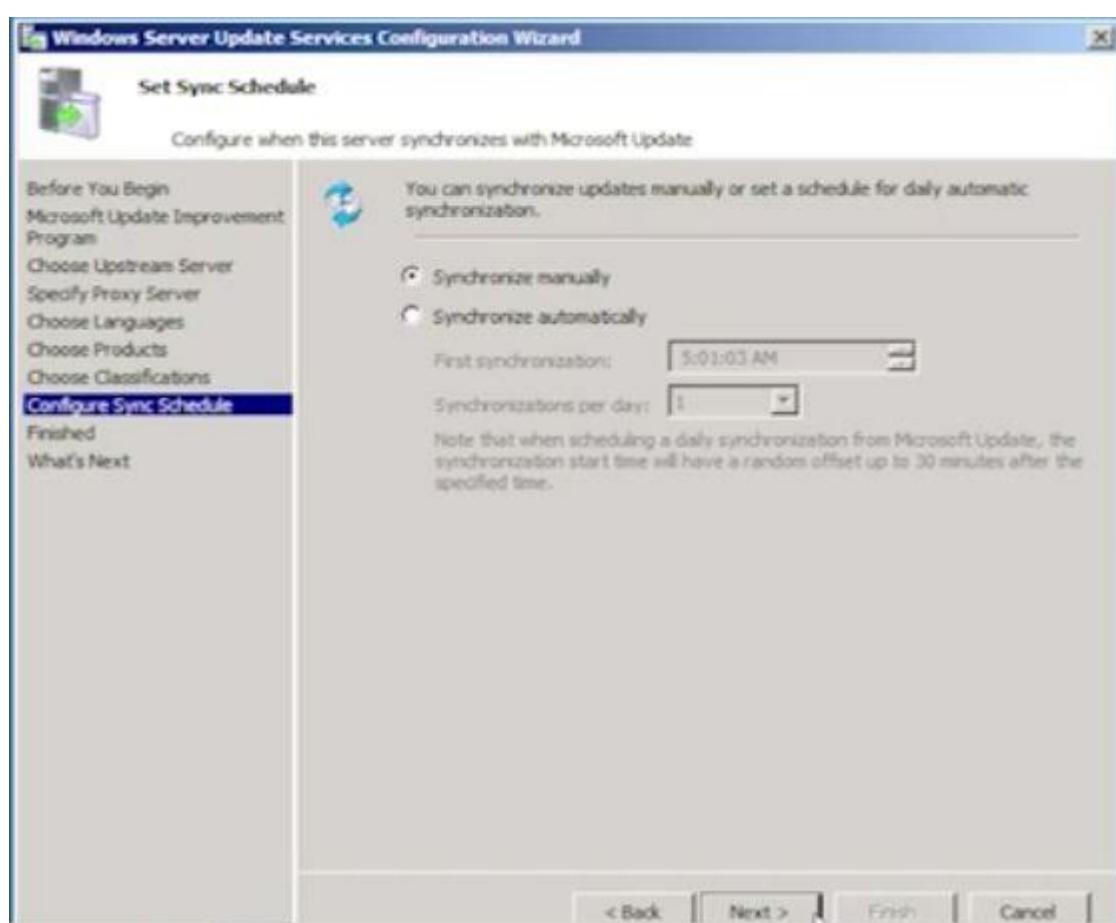
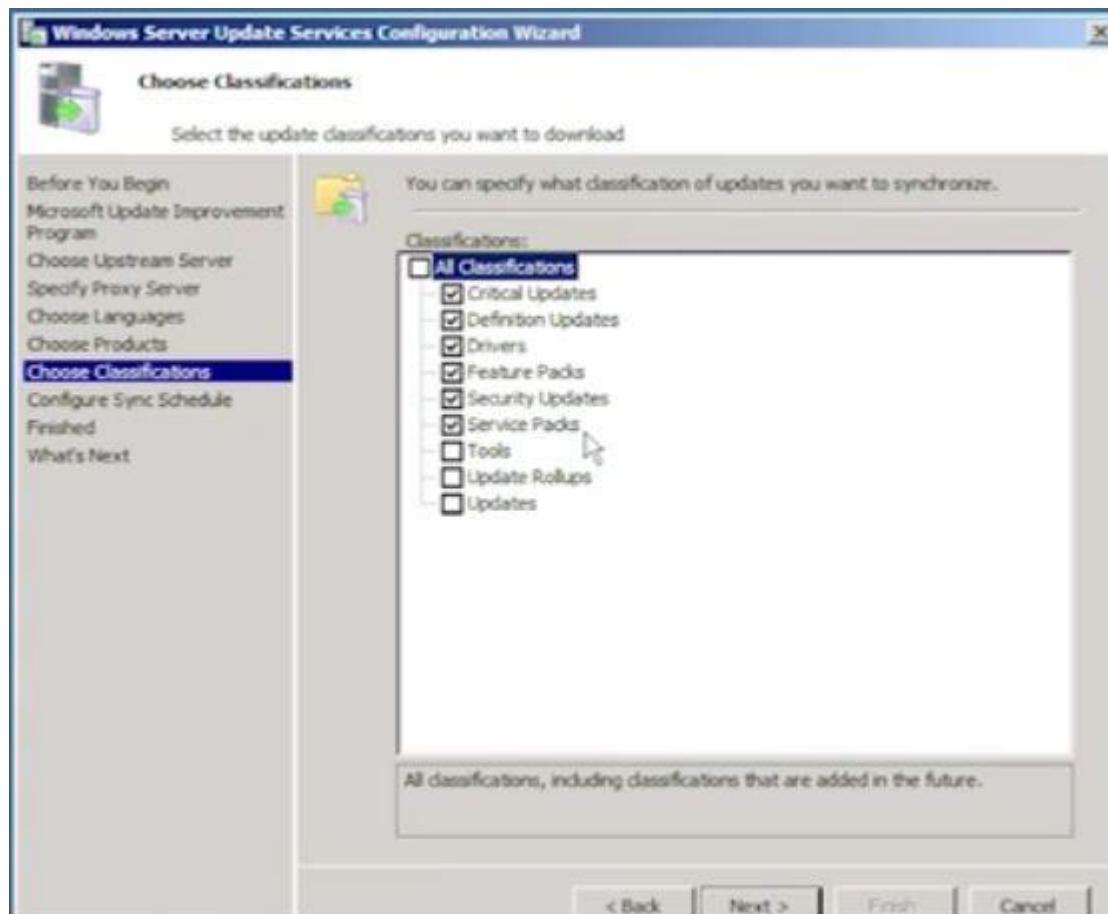


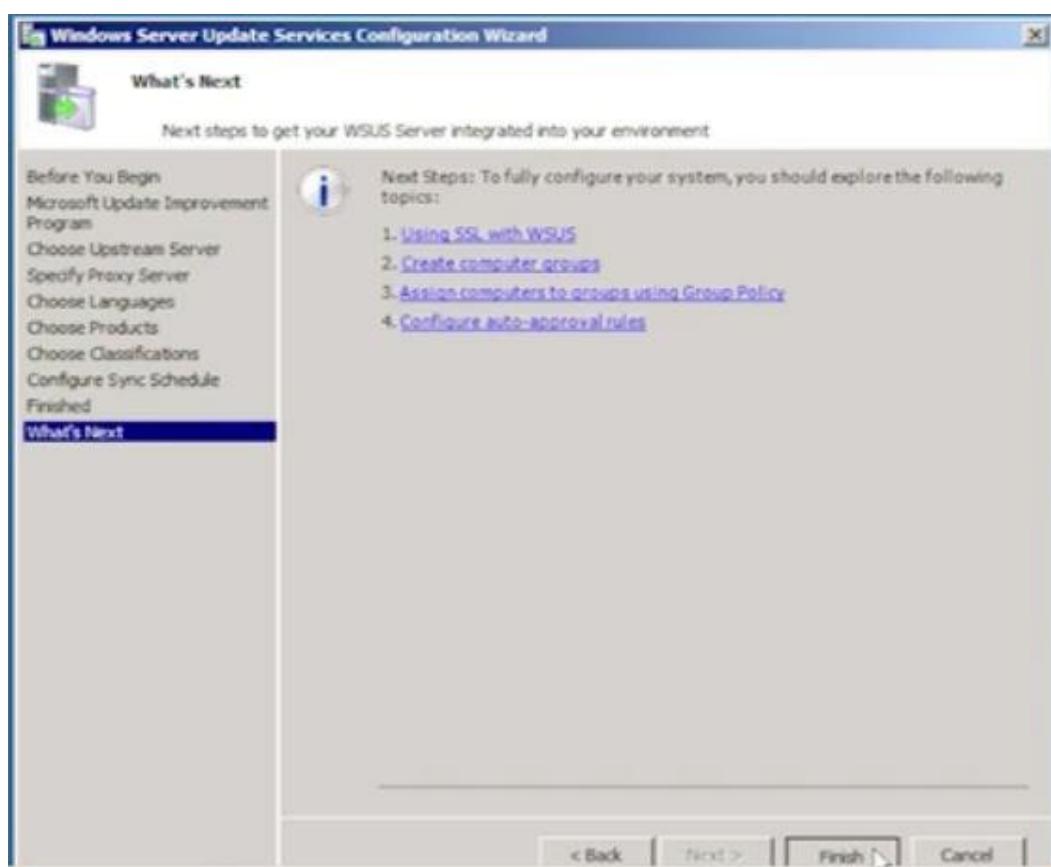
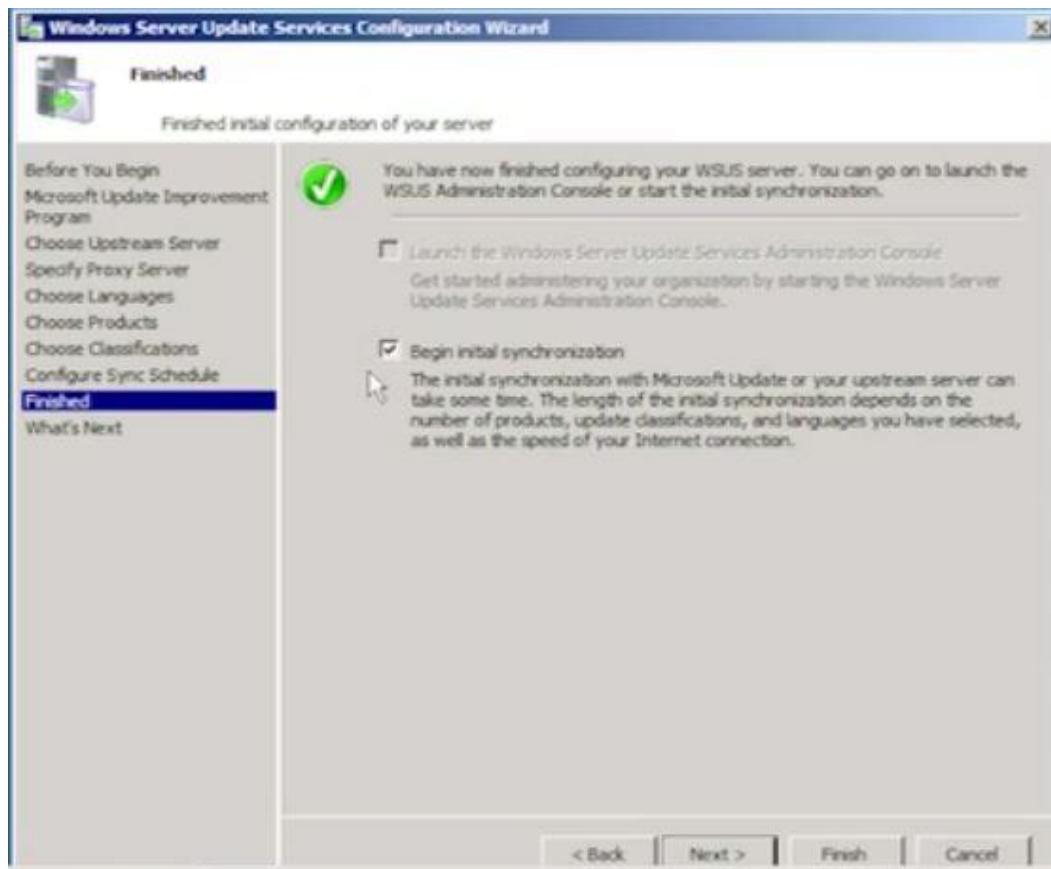












قبل البدء بالتنصيب لا بد من اتصال بالانترنت لتنزيل الخدمة على السرفر ولعمل التحديثات الازمة كما لا يمكن ان يعمل هذا المخدم الا بوجود اتصال بالانترنت لتحميل ومزامنة التحديثات منه



Exchange

لتنشئ بيئة Exchange الـ **Mailbox** في المجلد **Users** الـ **AD** .

من بعد ذلك نقوم بانشاء الـ **Mailbox** في المجلد **Users** الـ **AD** ...
بعد ذلك نقوم بعمل السياسات التي تحدد ضوابط ارسال واستقبال البريد الالكتروني بين المستخدمين.

التحضير والتصيب والاعداد:

```
Administrator: Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>cd C:\Program Files (x86)\Exchange

C:\Program Files (x86)\Exchange>
```

```
Administrator: Command Prompt - setup /prepareAD /organizationname:
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>cd C:\Program Files (x86)\Exchange

C:\Program Files (x86)\Exchange>setup /prepareAD /organizationname: hsbclo

Welcome to Microsoft Exchange Server 2010 Unattended Setup

Setup will continue momentarily, unless you press any key and cancel the
installation. By continuing the installation process, you agree to the license
terms of Microsoft Exchange Server 2010.
If you don't accept these license terms, please cancel the installation. To
review the license terms, please go to
http://go.microsoft.com/fwlink/?LinkId=150127&clcid=0x409

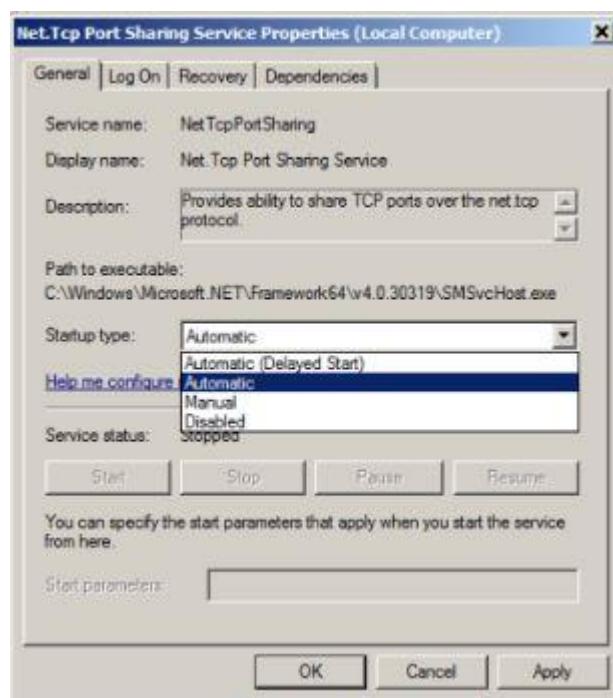
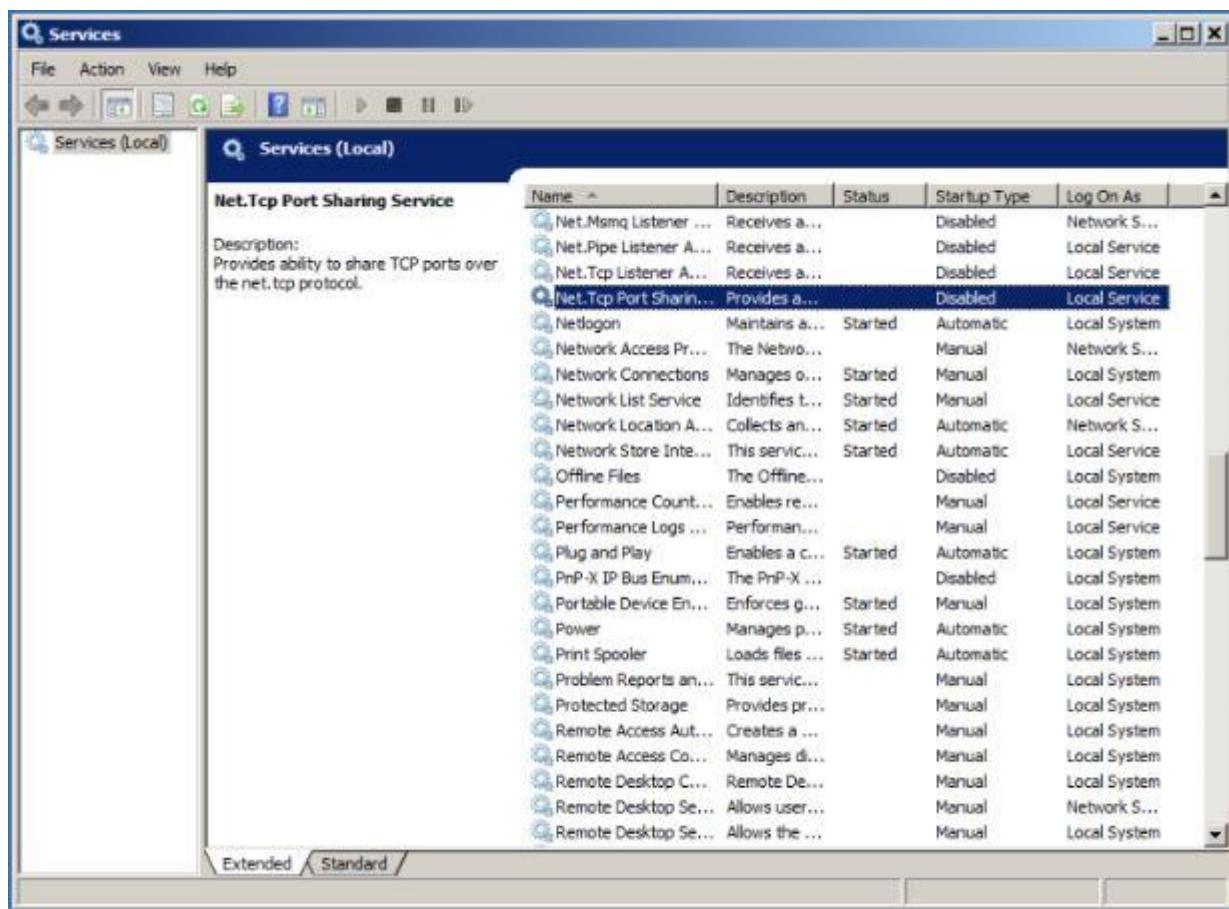
Press any key to cancel setup....
```

```
Welcome to Microsoft Exchange Server 2010 Unattended Setup

Setup will continue momentarily, unless you press any key and cancel the
installation. By continuing the installation process, you agree to the license
terms of Microsoft Exchange Server 2010.
If you don't accept these license terms, please cancel the installation. To
review the license terms, please go to
http://go.microsoft.com/fwlink/?LinkId=150127&clcid=0x409

Press any key to cancel setup.....
No key presses were detected. Setup will continue.

Preparing Exchange Setup
Copying Setup Files
COMPLETED
```



```
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> Import-Module ServerManager
PS C:\Users\Administrator> 
```

```
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> Import-Module ServerManager
PS C:\Users\Administrator> Add-WindowsFeature NET-Framework,RSAT-ADDS,Web-Server,Web-Basic-Auth,Web-Windows-Auth,Web-Met
abase,Web-Net-Ext,Web-Legacy-Mgmt-Console,WAS-Process-Model,RSAT-Web-Server,Web-ISAPI-Ext,Web-Digest-Auth,Web-Dyn-Compress
ion,.NET-HTTP-Activation,Web-Asp-Net,Web-Client-Auth,Web-Dir-Browsing,Web-Http-Errors,Web-Http-Logging,Web-Http-Redirect,
Web-Http-Tracing,Web-ISAPI-Filter,Web-Request-Monitor,Web-Static-Content,Web-WMI,RPC-Over-HTTP-Proxy -Restart
```



Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

Start Installation... ✓

[oooooooooooooooooooooo] 1

Web-Http-Tracing, Web-ISAPI-Filter, Web-Request-Monitor, Web-Static-Content, Web-WMI, RPC-Over-HTTP-Proxy -Restart

sr	4/9/2010 3:36 AM	File folder	
sr-cyril-cs	4/9/2010 3:36 AM	File folder	
sv	4/9/2010 3:36 AM	File folder	
th	4/9/2010 3:36 AM	File folder	
tr	4/9/2010 3:36 AM	File folder	
uk	4/9/2010 3:36 AM	File folder	
updates	4/9/2010 3:36 AM	File folder	
ur	4/9/2010 3:36 AM	File folder	
vi	4/9/2010 3:36 AM	File folder	
zh-hans	4/9/2010 3:36 AM	File folder	
zh-hant	4/9/2010 3:36 AM	File folder	
zh-hk	4/9/2010 3:36 AM	File folder	
autorun	8/22/2010 3:58 AM	Setup Information	1 KB
bores.dll	8/22/2010 3:58 AM	Application extension	82 KB
exchangeserver	8/22/2010 3:58 AM	Windows Installer P...	26,752 KB
lsetupui	8/22/2010 3:58 AM	Application	207 KB
microsoft.exchange.setup.acquirelanguagep...	8/22/2010 3:58 AM	Application extension	43 KB
microsoft.exchange.setup.signverfwrapper.dll	8/22/2010 3:58 AM	Application extension	64 KB
setup	8/22/2010 3:58 AM	MS-DOS Application	435 KB
setup	8/22/2010 3:58 AM	Application	582 KB

Plan

Read about Microsoft Exchange Server 2010 Service Pack 1

Read about deploying languages

Use the Exchange Server 2010 Deployment Assistant

Install

Step 1: Install .NET Framework 3.5 SP1 - Installed

Step 2: Install Windows PowerShell v2 - Installed

Step 3: Choose Exchange language option

Step 4: Install Microsoft Exchange

Step 5: Get critical updates for Microsoft Exchange

Enhance

Install Microsoft Forefront Protection 2010 for Exchange Server

Close



Use the Exchange Server 2010 Deployment Assistant



Install only languages included with Setup

Plan

Read about Microsoft Exchange Server 2010 Service Pack 1
Read about deploying languages
Use the Exchange Server 2010 Deployment Assistant

Install

Step 1: Install .NET Framework 3.5 SP1 - Installed
Step 2: Install Windows PowerShell v2 - Installed
Step 3: Choose Exchange language option
 Install all languages from the language bundle
 [Install only languages from the DVD](#)
Step 4: Install Microsoft Exchange
Step 5: Get critical updates for Microsoft Exchange

Enhance

Install Microsoft Forefront Protection 2010 for Exchange Server

[Close](#)



Install Exchange Server. This will copy the needed binaries and prepare the server to be configured.

Plan

Read about Microsoft Exchange Server 2010 Service Pack 1
Read about deploying languages
Use the Exchange Server 2010 Deployment Assistant

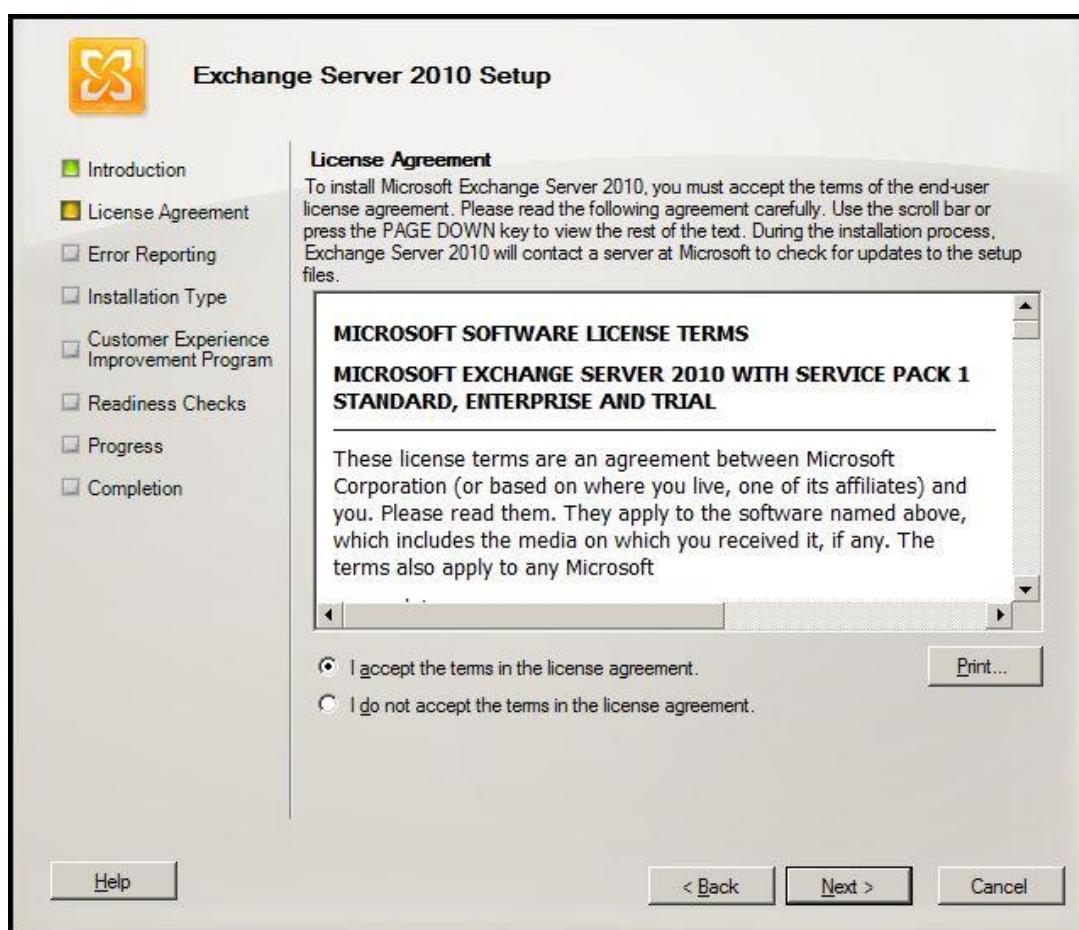
Install

Step 1: Install .NET Framework 3.5 SP1 - Installed
Step 2: Install Windows PowerShell v2 - Installed
Step 3: Choose Exchange language option
[Step 4: Install Microsoft Exchange](#)
Step 5: Get critical updates for Microsoft Exchange

Enhance

Install Microsoft Forefront Protection 2010 for Exchange Server

[Close](#)





Exchange Server 2010 Setup

 **Error Reporting**

We invite you to enable Exchange Error Reporting to improve the quality, reliability, and performance of Microsoft software and services.

If you enable the Exchange Error Reporting feature, Microsoft Exchange will automatically send error reports to Microsoft without bothering you. If an error occurs, the server uses HTTPS to send information to Microsoft over an encrypted channel. This information is stored in facilities with controlled access and is used only to improve Microsoft products. Exchange Error Reporting does not intentionally collect any personal information such as e-mail addresses. However individual error reports may inadvertently contain personal information. While such information could potentially be used to determine the identity of Microsoft Exchange Server users, if present, it will not be used.

When the Exchange Error Reporting feature is enabled and the issue has a known solution, the server will receive feedback from Microsoft. This feedback will contain a link to a Web page that may help resolve the problem.

Yes (Recommended) No

[Read more about Exchange Error Reporting](#)

Help **< Back** **Next >** **Cancel**

Exchange Server 2010 Setup

 **Error Reporting**

Introduction
License Agreement
Error Reporting
Installation Type
Customer Experience Improvement Program
Readiness Checks
Progress
Completion

Installation Type
Select the Exchange Server installation type:

Typical Exchange Server Installation
The following will be installed on this computer:


- Hub Transport
- Client Access
- Mailbox
- Exchange Management Tools

Custom Exchange Server Installation
Use this option to select which of the following roles you want to install on this computer:


- Hub Transport
- Client Access
- Mailbox
- Unified Messaging
- Edge Transport
- Exchange Management Tools

Specify the path for the Exchange Server program files:
 Browse...

Automatically install Windows Server roles and features required for Exchange Server

Help **< Back** **Next >** **Cancel**

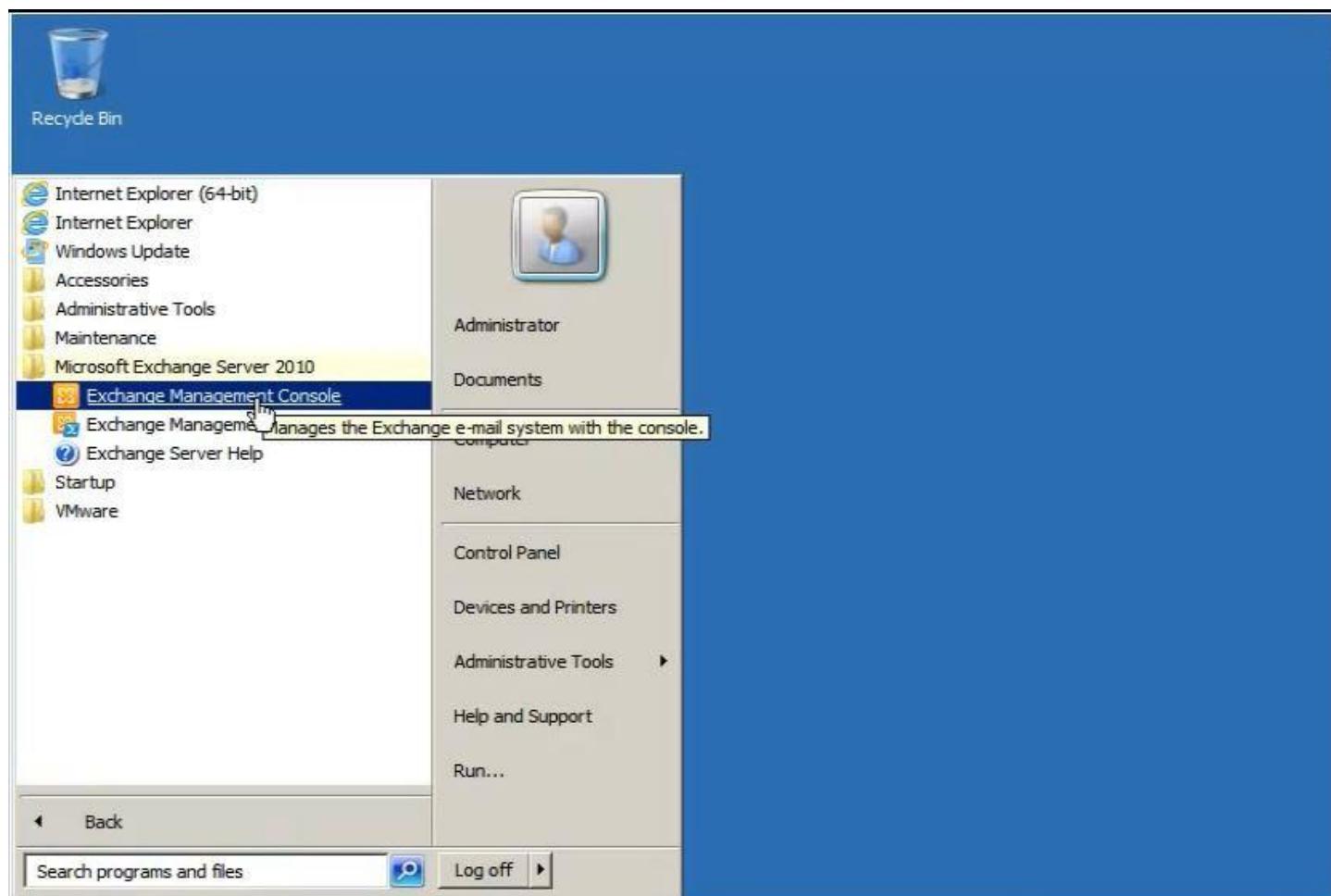


Exchange Server 2010 Setup

The window shows the Exchange Server 2010 Setup interface. On the left, a navigation pane lists several steps: Introduction, License Agreement, Error Reporting, Installation Type, Client Settings, Configure Client, Access server external domain (which is selected), Customer Experience Improvement Program, Readiness Checks, Progress, and Completion. The main panel is titled "Configure Client Access server external domain". It contains a descriptive text about configuring Client Access servers for Internet-facing services, a checked checkbox for "The Client Access server role will be Internet-facing", and a text input field for entering the domain name. At the bottom are standard setup buttons: Help, Back, Next, and Cancel.

Exchange Server 2010 Setup

The window shows the Exchange Server 2010 Setup interface. On the left, a navigation pane lists the same steps as the previous window. The main panel is titled "Customer Experience Improvement Program". It asks if the user wants to join the program, stating that it collects information about computer hardware and usage. It includes links to "Read more about the program online" and "Read the CEIP Privacy Statement". Two radio buttons are present: "Join the Customer Experience Improvement Program" (unchecked) and "I don't want to join the program at this time" (checked). A note at the bottom explains that joining the program includes the server in the program, which can be excluded later. At the bottom are standard setup buttons: Help, Back, Next, and Cancel.



Exchange Management Console

File Action View Help

Microsoft Exchange Microsoft Exchange On-Premises (v)

Organizational Health Customer Feedback

Exchange 2010 Organizational Health

Organization Summary

Database Summary

Total databases:	Unavailable	Manage databases
Total database copies:	Unavailable	
Total unhealthy database copies:	Unavailable	

License Summary for Exchange 2010

Users

Total users requiring CALs:	Unavailable
Standard CALs required:	Unavailable
Enterprise CALs required:	Unavailable

[View legal information regarding the Client Access License \(CAL\)](#)

Servers Summary

Recipients Summary

Data is loading...

The data marked with a yellow exclamation mark may be inaccurate due to errors that happened while the data was being collected.

Actions

Microsoft Exchange...

- Properties
- View
- Refresh
- Help

Initializing: In progress...

Exchange Management Console

File Action View Help

Microsoft Exchange Microsoft Exchange On-Premises (v)

Organization Configuration Server Configuration Recipient Configuration

- Mailbox
- Distribution Group
- Mail Contact
- Disconnected Mailbox
- Move Request
- Toolbox

Mailbox - Entire Forest 2 objects

Create Filter

Display Name	Alias	Organizational Unit
Administrator	Administrator	testad10.local/Users
Discovery Search Mailbox	DiscoverySearchMailbox{...}	testad10.local/Users

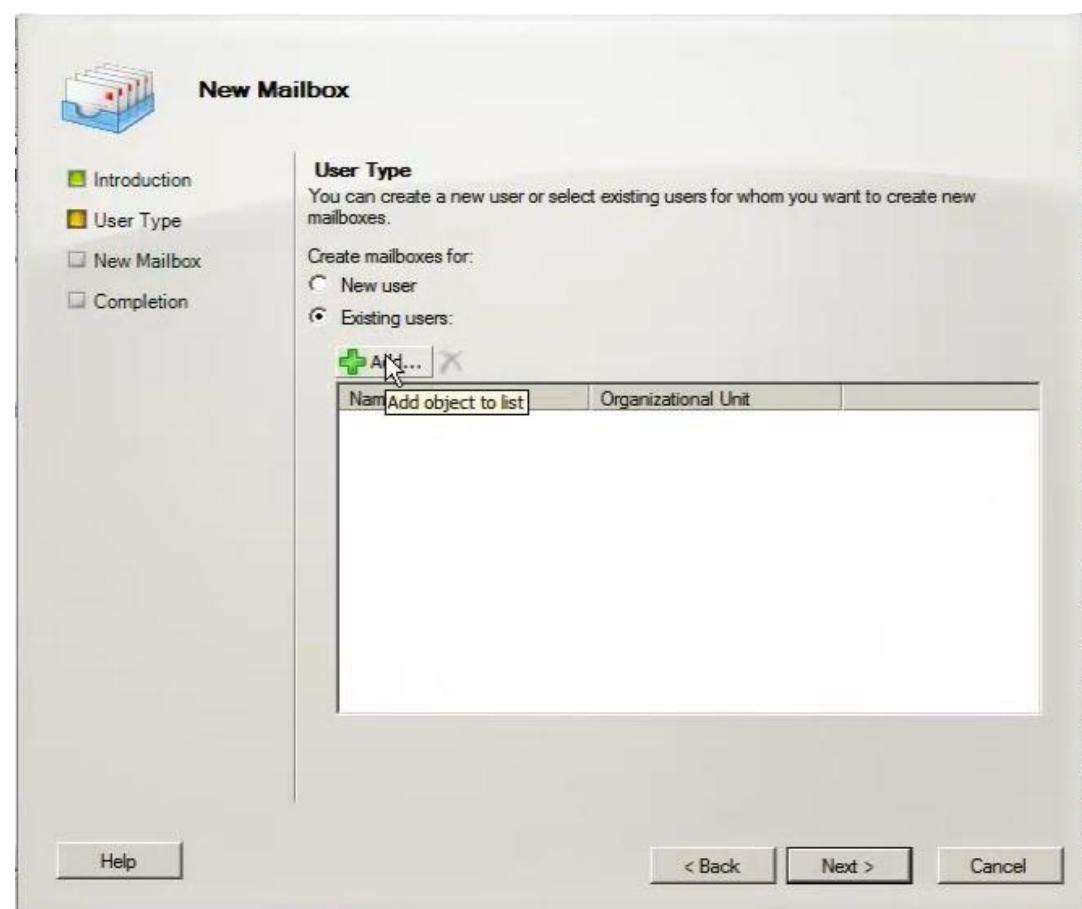
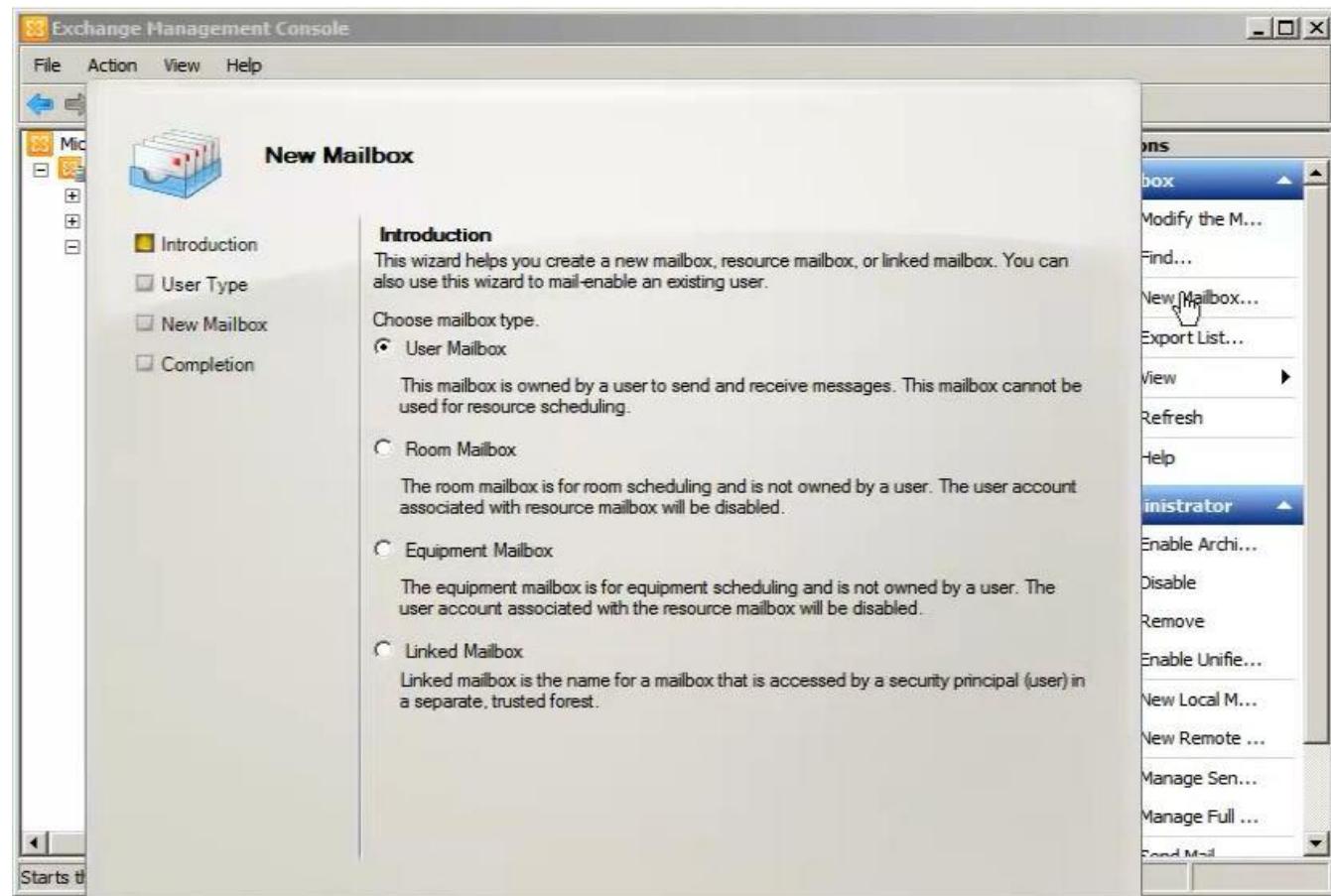
Actions

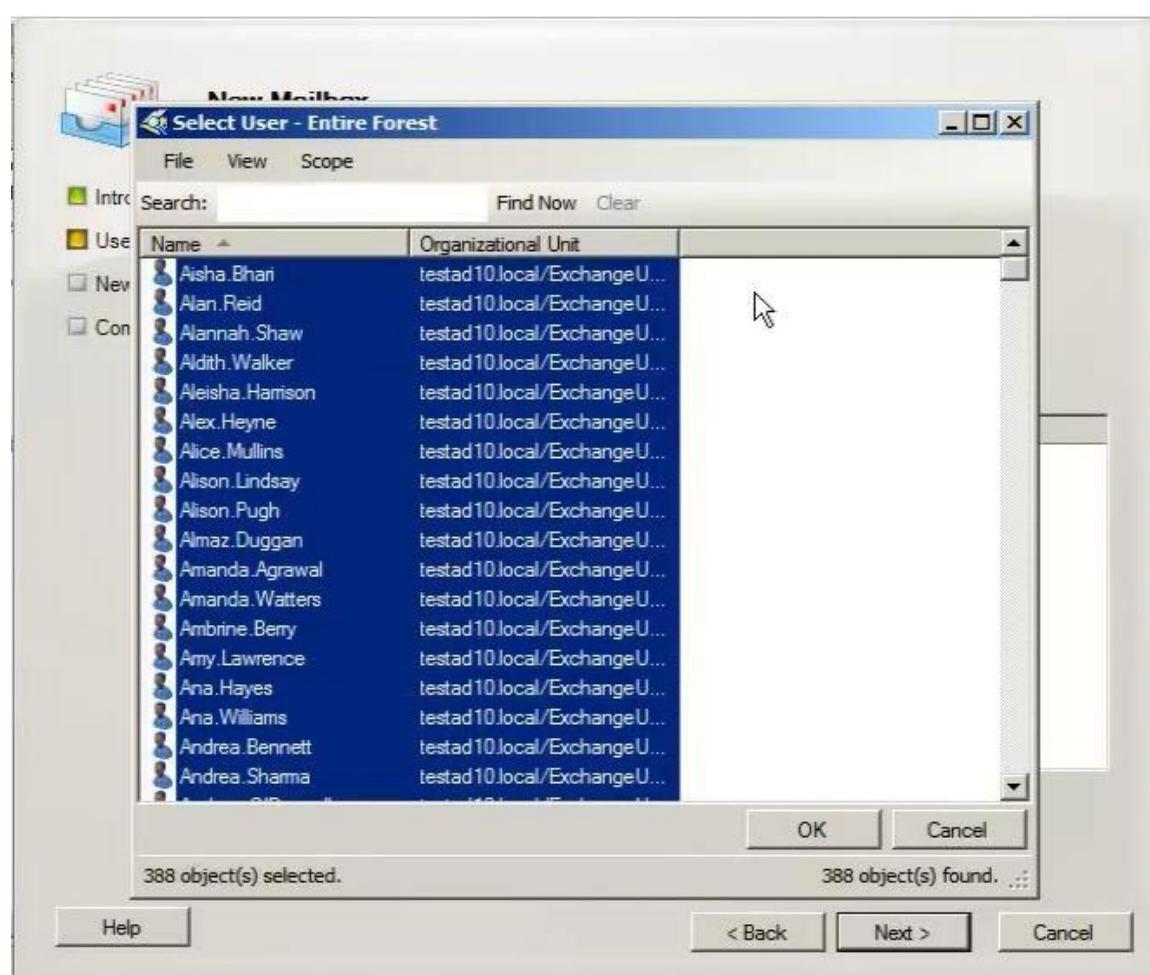
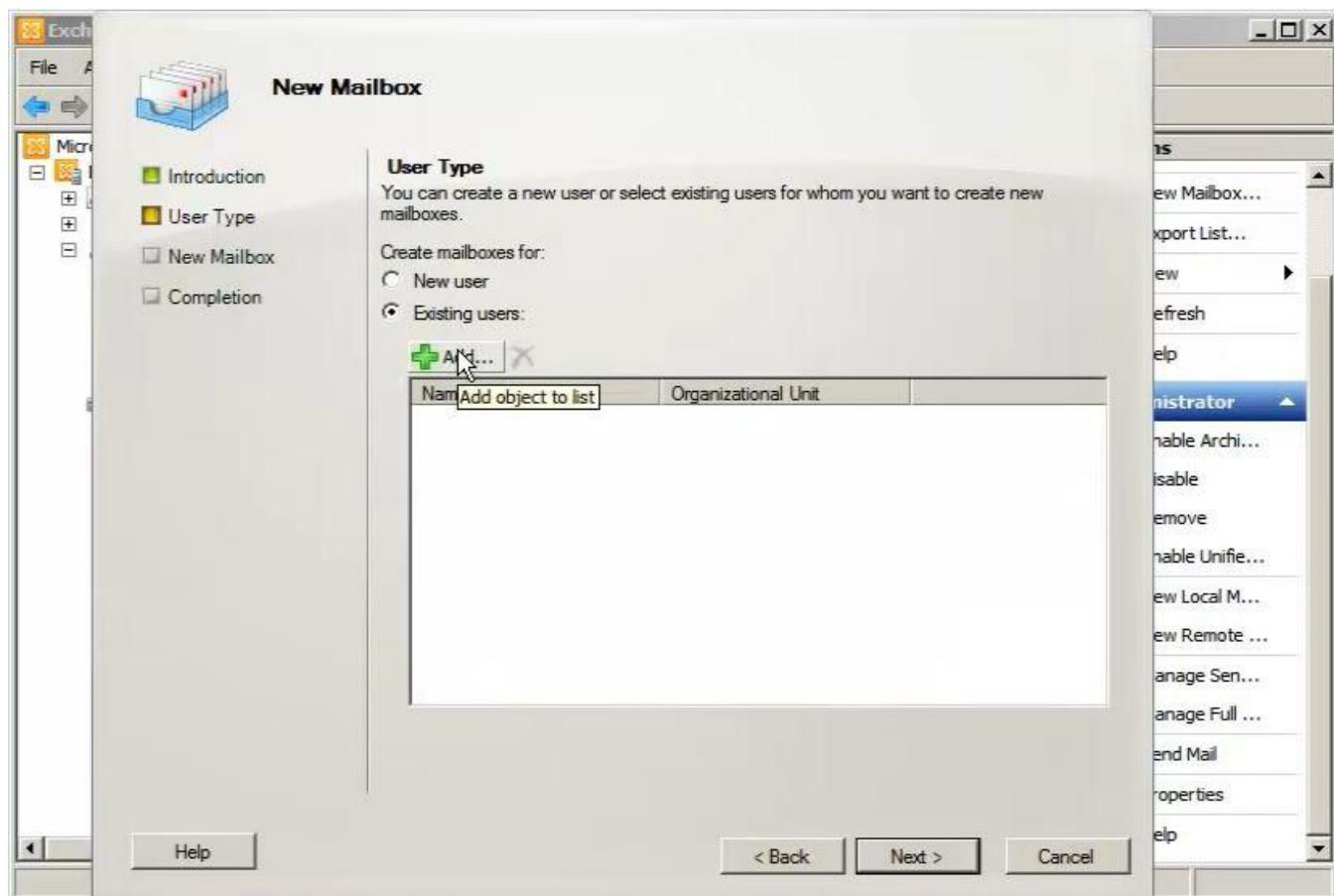
Mailbox

- Modify the M...
- Find...
- New Mailbox...
- Export List...
- View
- Refresh
- Help

Administrator

- Enable Archi...
- Disable
- Remove
- Enable Unifie...
- New Local M...
- New Remote ...
- Manage Sen...
- Manage Full ...
- Send Mail







New Mailbox

User Type
You can create a new user or select existing users for whom you want to create new mailboxes.

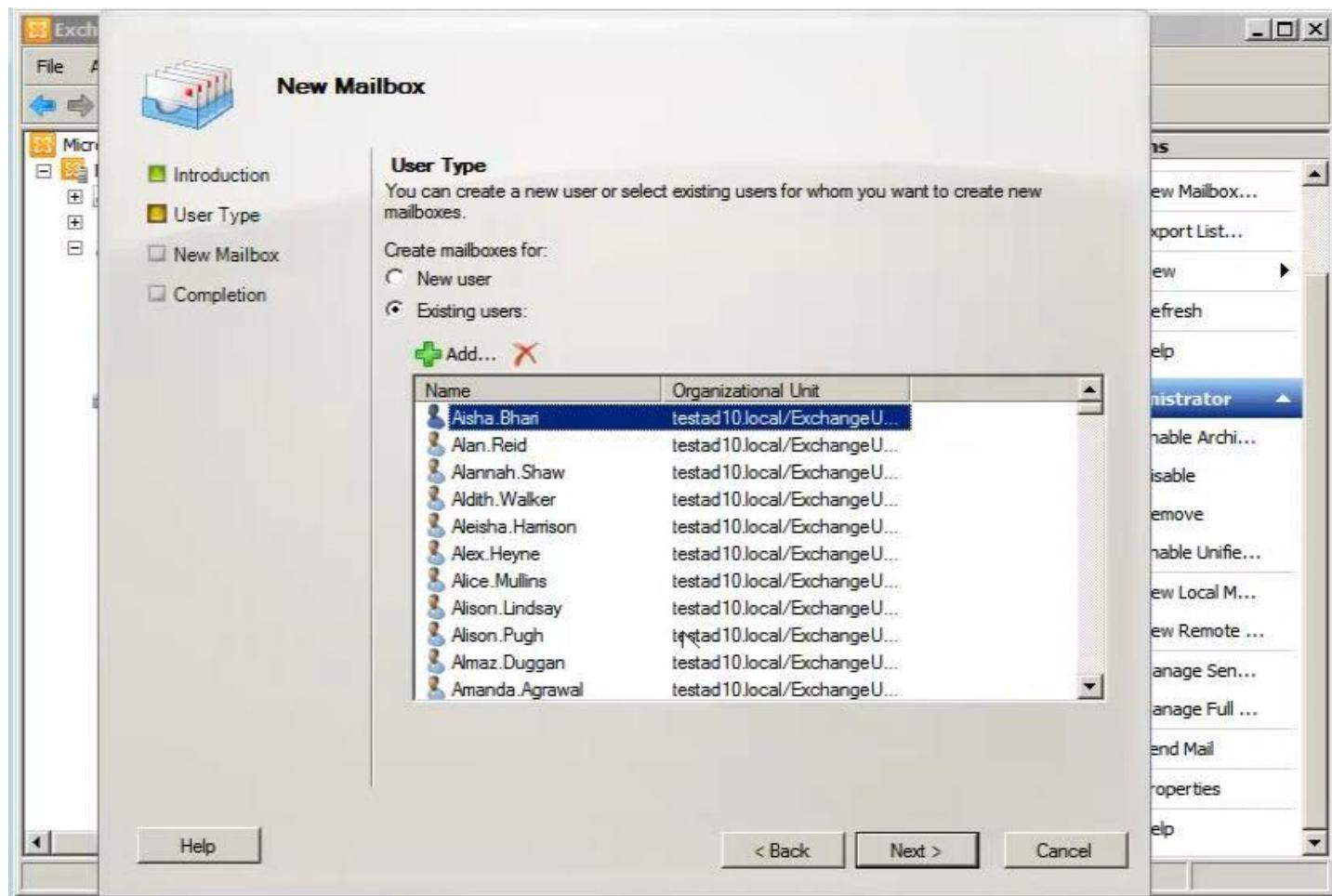
Create mailboxes for:

New user
 Existing users:

Add... **X**

Name	Organizational Unit
Aisha.Bhari	testad10.local/ExchangeU...
Alan.Reid	testad10.local/ExchangeU...
Alannah.Shaw	testad10.local/ExchangeU...
Aldith.Walker	testad10.local/ExchangeU...
Aleisha.Harrison	testad10.local/ExchangeU...
Alex.Heyne	testad10.local/ExchangeU...
Alice.Mullins	testad10.local/ExchangeU...
Alison.Lindsay	testad10.local/ExchangeU...
Alison.Pugh	testad10.local/ExchangeU...
Almaz.Duggan	testad10.local/ExchangeU...
Amanda.Agrawal	testad10.local/ExchangeU...

Help **< Back** **Next >** **Cancel**



New Mailbox

Mailbox Settings
Enter the alias for the mailbox user, and then select the mailbox location and policy settings.

Alias:

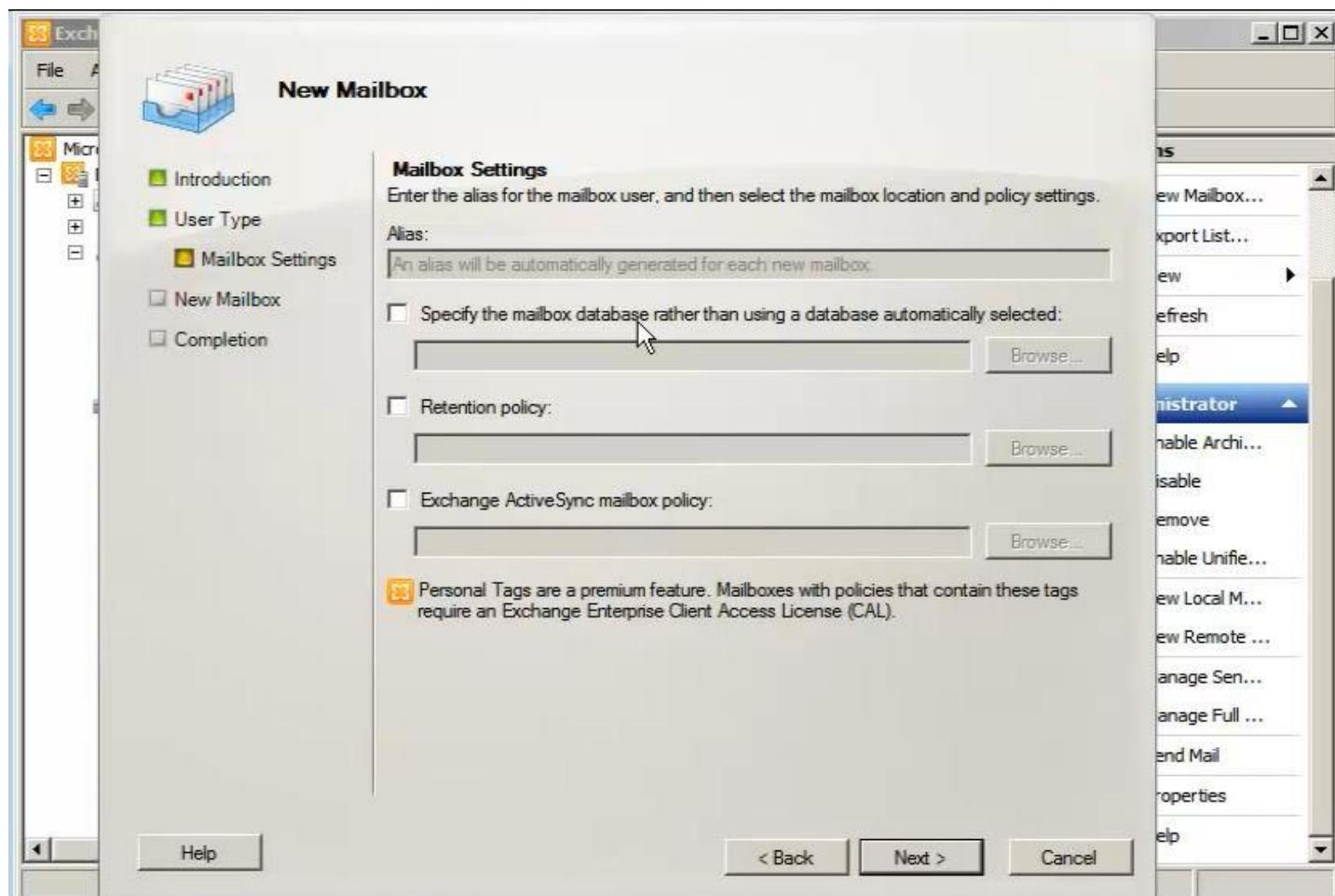
Specify the mailbox database rather than using a database automatically selected: **Browse...**

Retention policy: **Browse...**

Exchange ActiveSync mailbox policy: **Browse...**

Personal Tags are a premium feature. Mailboxes with policies that contain these tags require an Exchange Enterprise Client Access License (CAL).

Help **< Back** **Next >** **Cancel**





New Mailbox

New Mailbox
Elapsed time: 00:00:00
Configuration Summary:

Denise.Ahadi	Pending
Denise.Darrell	Pending
Diana.Samuda	Pending
Diana.Williams	Pending
Diane.Hall	Pending
Diane.Jones	Pending
Donna.A'Bear	Pending
Doreen.Brown	Pending
Dukh.Morgan	Pending
Elaine.West	Pending
Elise.Daeth	Pending
Elizabeth.Holloway	Pending
Ella.Amaral	Pending

To copy the contents of this page, press CTRL+C.

< Back **New** Cancel

File A Micro New Mailbox... Export List... ew Refresh elp Administrator... able Arch... isable remove able Unifie... ew Local M... ew Remote ... anage Sen... anage Full ... end Mail properties elp Help

New Mailbox

Completion
The wizard completed successfully. Click Finish to close this wizard.
Elapsed time: 00:00:35
Summary: 388 item(s). 388 succeeded, 0 failed.

Aisha.Bhari	Completed
Alan.Reid	Completed
Alannah.Shaw	Completed
Aldith.Walker	Completed

Exchange Management Shell command completed:
'TESTAD10.local/ExchangeUsers/Aisha.Bhari' | Enable-Mailbox
Elapsed Time: 00:00:07

Exchange Management Shell command completed:
'TESTAD10.local/ExchangeUsers/Alan.Reid' | Enable-Mailbox
Elapsed Time: 00:00:00

Exchange Management Shell command completed:
'TESTAD10.local/ExchangeUsers/Alannah.Shaw' | Enable-Mailbox
Elapsed Time: 00:00:00

Exchange Management Shell command completed:
'TESTAD10.local/ExchangeUsers/Aldith.Walker' | Enable-Mailbox
Elapsed Time: 00:00:00

To copy the contents of this page, press CTRL+C.

< Back **Finish** Cancel

File A Micro New Mailbox... Export List... ew Refresh elp Administrator... able Arch... isable remove able Unifie... ew Local M... ew Remote ... anage Sen... anage Full ... end Mail properties elp Help



Mailbox - Entire Forest 390 objects

Display Name	Alias	Organizational Unit
Administrator	Administrator	testad10.local/User
Aisha Bhari	Aisha.Bhari	testad10.local/Exch
Alan Reid	Alan.Reid	testad10.local/Exch
Alannah Shaw	Alannah.Shaw	testad10.local/Exch
Aldith Walker	Aldith.Walker	testad10.local/Exch
Aleisha Harrison	Aleisha.Harrison	testad10.local/Exch
Alex Heyne	Alex.Heyne	testad10.local/Exch
Alice Mullins	Alice.Mullins	testad10.local/Exch
Alison Lindsay	Alison.Lindsay	testad10.local/Exch
Alison Pugh	Alison.Pugh	testad10.local/Exch
Almaz Duggan	Almaz.Duggan	testad10.local/Exch
Amanda Agrawal	Amanda.Agrawal	testad10.local/Exch
Amanda Watters	Amanda.Watters	testad10.local/Exch
Ambrine Berry	Ambrine.Berry	testad10.local/Exch
Amy Lawrence	Amy.Lawrence	testad10.local/Exch
Ana Hayes	Ana.Hayes	testad10.local/Exch
Ana Williams	Ana.Williams	testad10.local/Exch
Andrea Bennett	Andrea.Bennett	testad10.local/Exch
Andrea Sharma	Andrea.Sharma	testad10.local/Exch
Andrew O'Donnell	Andrew.O'Donnell	testad10.local/Exch
Andrew O'Grady	Andrew.O'Grady	testad10.local/Exch

Actions

- New Mailbox...
- Export List...
- View
- Refresh
- Help
- Alex Heyne
- Enable Archi...
- Disable
- Remove
- Enable Unifie...
- New Local M...
- New Remote ...
- Manage Sen...
- Manage Full ...
- Send Mail
- Properties
- Help

وبهذا تكون الحسابات جاهزة للاستخدام ويتم تسجيل الدخول اما عن طريق الـ .Exchange Mobile Client أو عن طريق الـ Outlook او برنامج الـ OWA Outlook Web Application



SharePoint

نقوم أولاً بإضافة ثلاثة مستخدمين إلى Active directory وهم:

SQLADMIN و SPFARM و SPADMIN

SQL Installation

لتنصيب SQL نحتاج أولاً حزمة SQL Server لأنها تحتاج قاعدة بيانات أولية.

ثم أولاً نقوم بفتح ملف تنصيب SQL Server

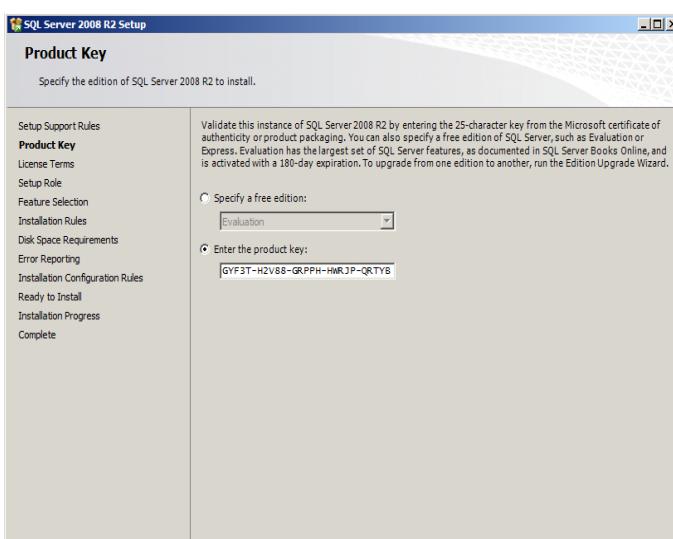
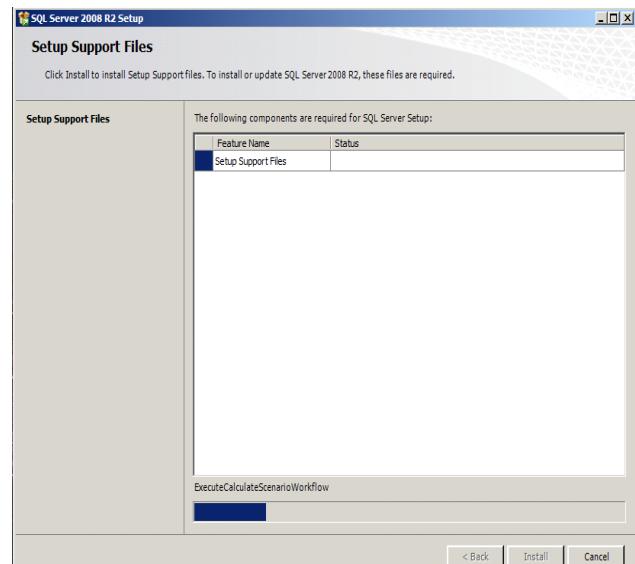
نضغط على New installation:

يقوم البرنامج بالتحضير للتنصيب



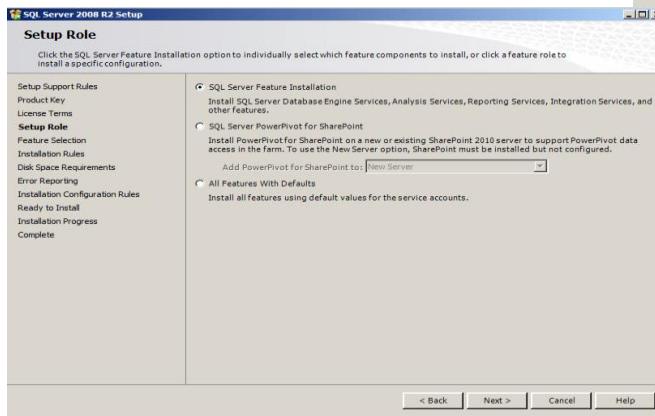
يطلب منا
مفتاح المنتج

نقوم بوضع مفتاح النسخة:



ومن ثم الموافقة على شروط البرنامج

نقوم

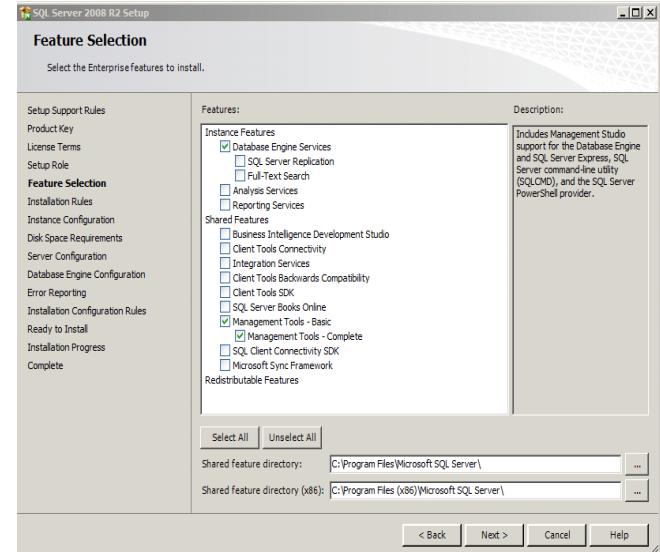


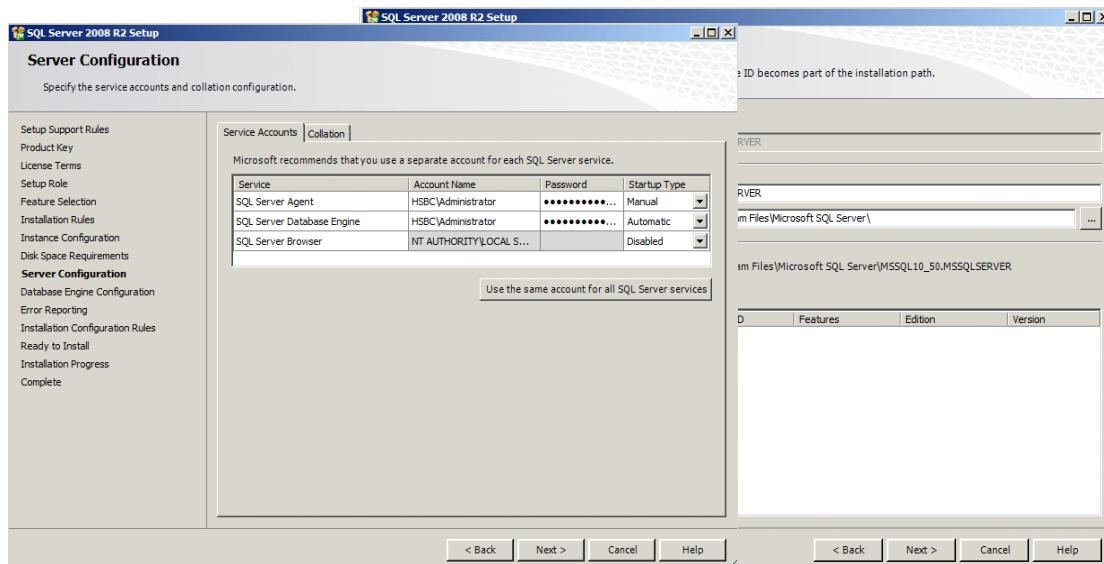
باختيار وهي SQL Server Feature installation النسخة التي تحتوي قاعدة بيانات مستقلة:

بعدها يطلب منا اختيار الميزات التي نريد تضمينها في البرنامج، فنختار:

Database Engine Services-
-Management Tools

من ثم نقوم باختيار مكان التنصيب وندع ال ID Instance كما هو:

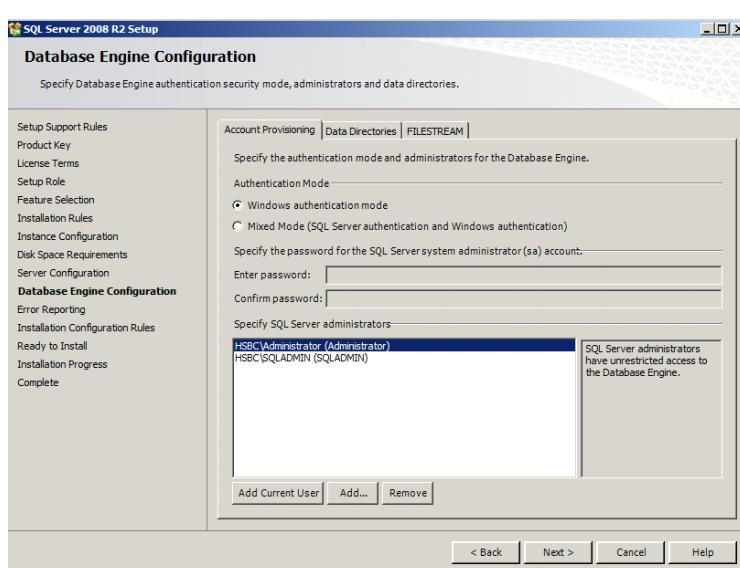




ال

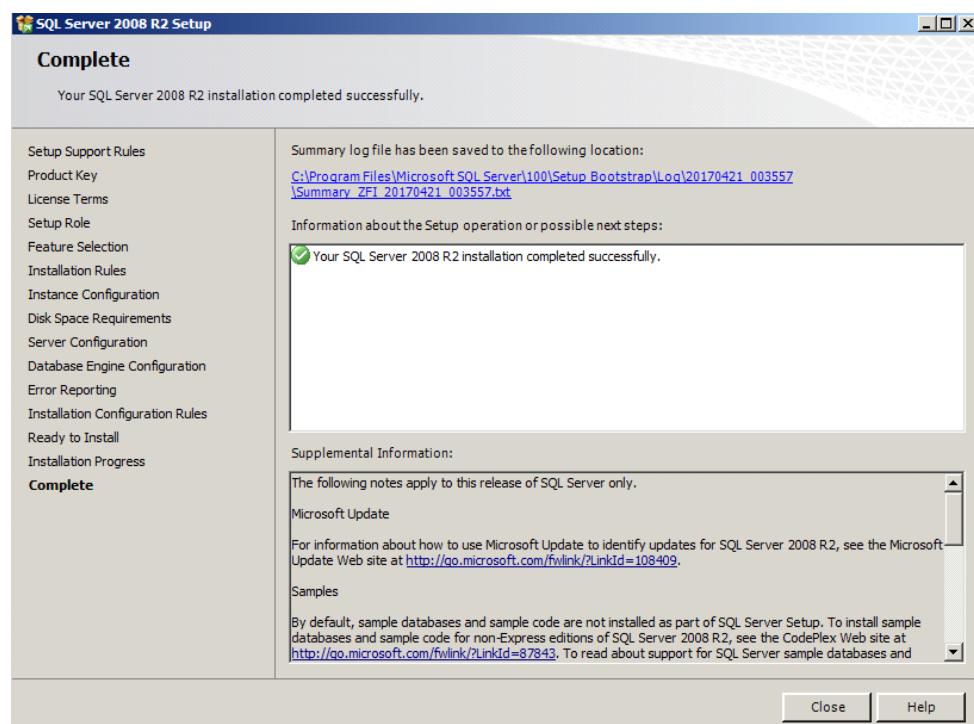
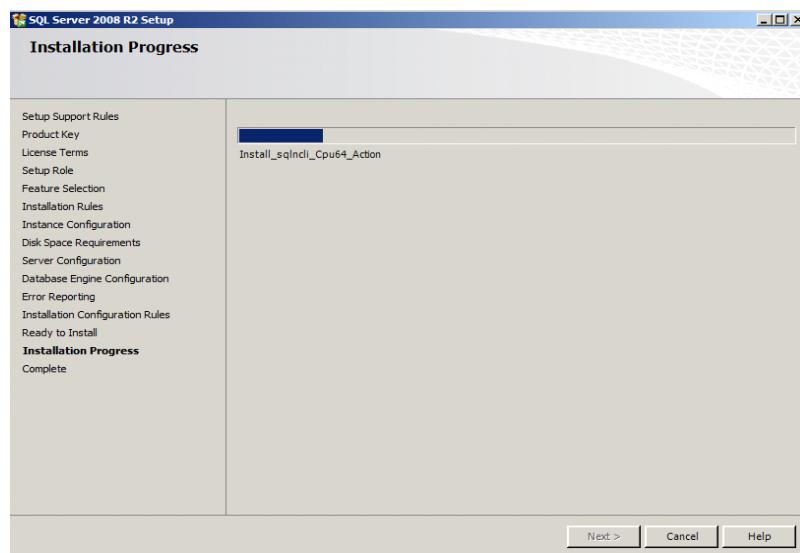
نقوم بتحديد المستخدمين الذين سيستخدمون

SharePoint، نحدد المستخدمين الذين أضفناهم إلى ال Active directory سنقوم بتحديد جميعها لل SharePoint ومن ثم نضيف المستخدمين من إعدادات ال Administrator



نحدد المسؤولين عن قاعدة بيانات المخدم:

نضغط على Next ليقوم البرنامج بالتنزيل:





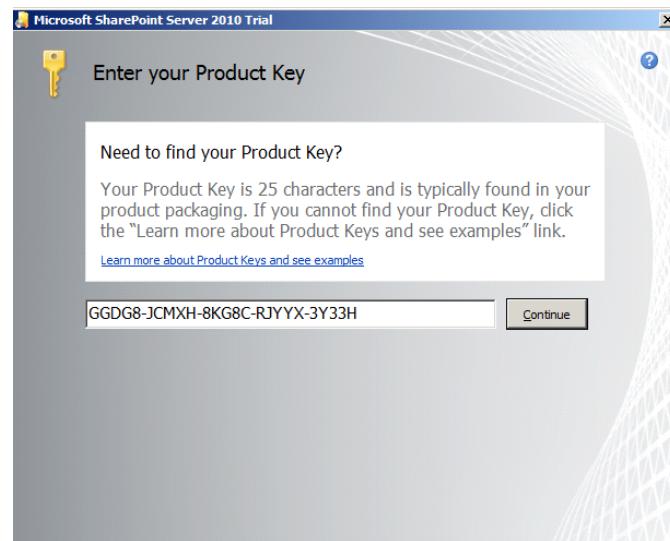
تنصيب الـ SharePoint

البرنامج،



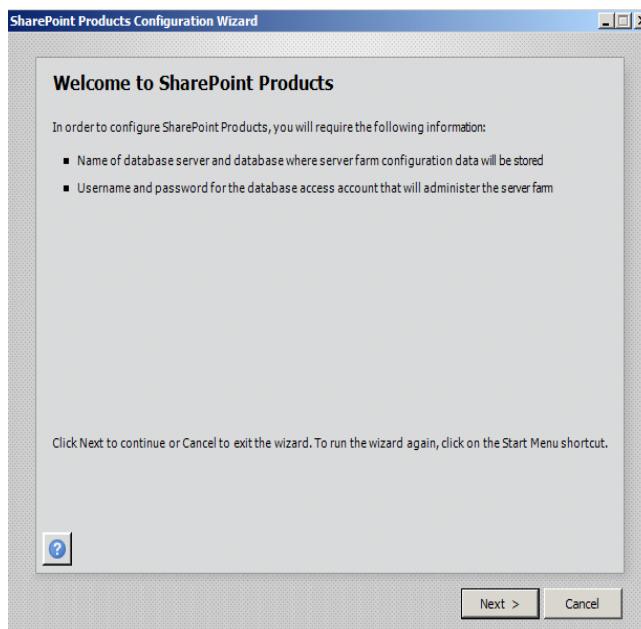
أولاً نفتح ملف تنصيب الـ SharepointServer.exe:

بعد التأكد من تنزيل البرامج التي يعتمد عليها
نقوم بالضغط على "Install SharePoint" ثم نضع مفتاح المنتج:
"Server".



Configuration Wizard الى الـ Next

نضغط





Specify Configuration Database Settings

All servers in a server farm must share a configuration database. Type the database server and database name. If the database does not exist, it will be created. To reuse an existing database, the database must be empty. For additional information regarding database server security configuration and network access please see [help](#).

Database server:	ZFI
Database name:	SharePoint_Config

Specify Database Access Account

Select an existing Windows account that this machine will always use to connect to the configuration database. If your configuration database is hosted on another server, you must specify a domain account.

Type the username in the form DOMAIN\User_Name and password for the account.

Username:	SPFARM
Password:	*****

< Back | Next > | Cancel | ?

نقوم بتحديد اسم مخدم قاعدة البيانات التي يعتمد عليها واسم قاعدة البيانات، واسم مستخدم وكلمة سر لقاعدة البيانات، نقوم باختيار SPFARM لأنها سيكون مسؤولة عن ال Farm الحالية:

Specify Farm Security Settings

Please enter a new passphrase for the SharePoint Products farm. This passphrase is used to secure farm configuration data and is required for each server that joins the farm. The passphrase can be changed after the farm is configured.

Passphrase:	*****
Confirm passphrase:	*****

< Back | Next > | Cancel | ?

نضع كلمة سر ل Farm الحالية:

نحدد ال Port الذي سيعمل عليه ال SharePoint:

Configure SharePoint Central Administration Web Application

A SharePoint Central Administration Web Application allows you to manage configuration settings for a server farm. The first server added to a server farm must host this web application. To specify a port number for the web application hosted on this machine, check the box below and type a number between 1 and 65535. If you do not specify a port number, a random one will be chosen.

Specify port number: 9090

Configure Security Settings

Kerberos is the recommended security configuration to use with Integrated Windows authentication. Kerberos requires special configuration by the domain administrator. NTLM authentication will work with any application pool account and the default domain configuration. [Show me more information](#).

Choose an authentication provider for this Web Application.

NTLM
 Negotiate (Kerberos)

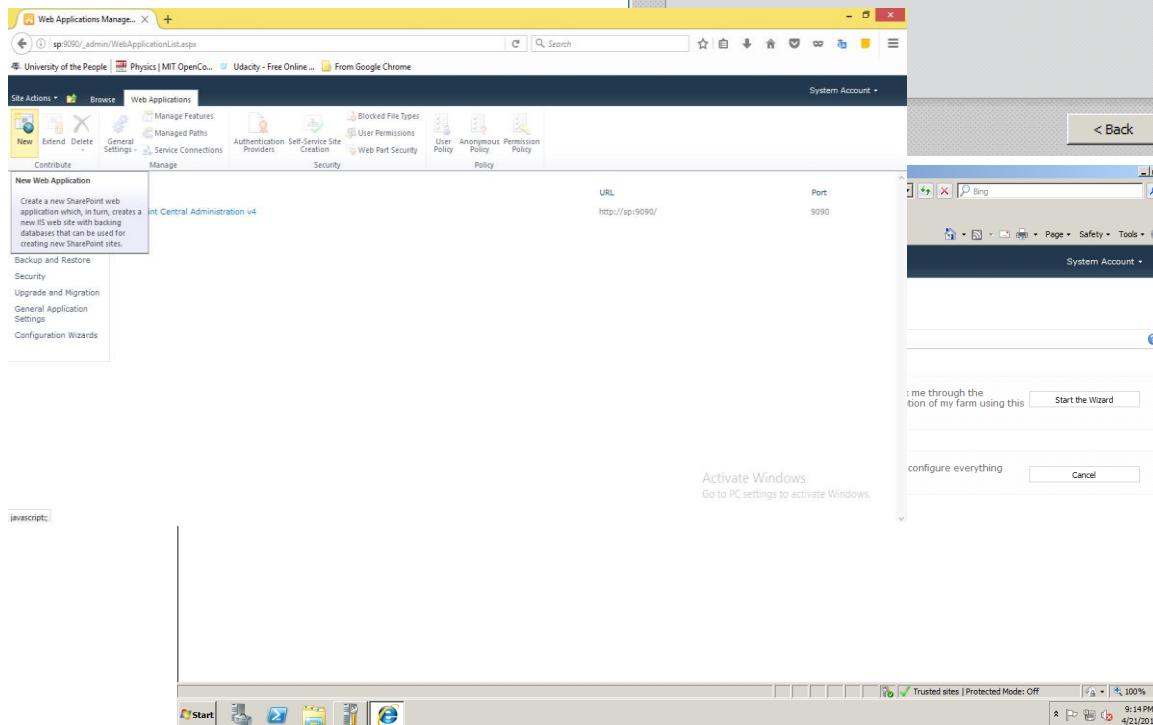
< Back | Next > | Cancel | ?

من ثم يعرض لنا معلومات المخدم:

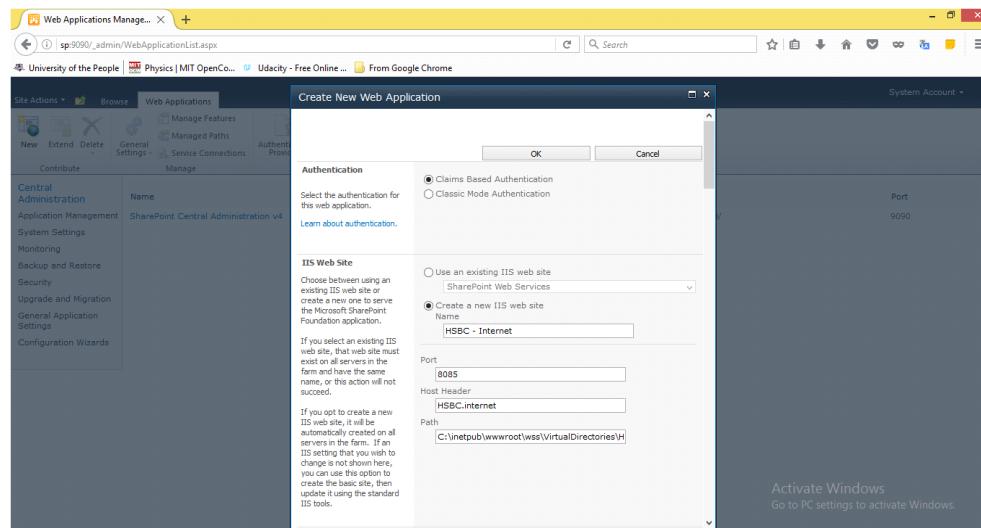


فتح متصفح الإنترن特 ، ونضع الرابط HYPERLINK "http://zfi:9090/"
 ونقوم بتنزيل Start the Wizard أولاً بالضغط على: Wizard

من ثم ننشئ تطبيق بالدخول إلى
 New: ومن ثم نضغط

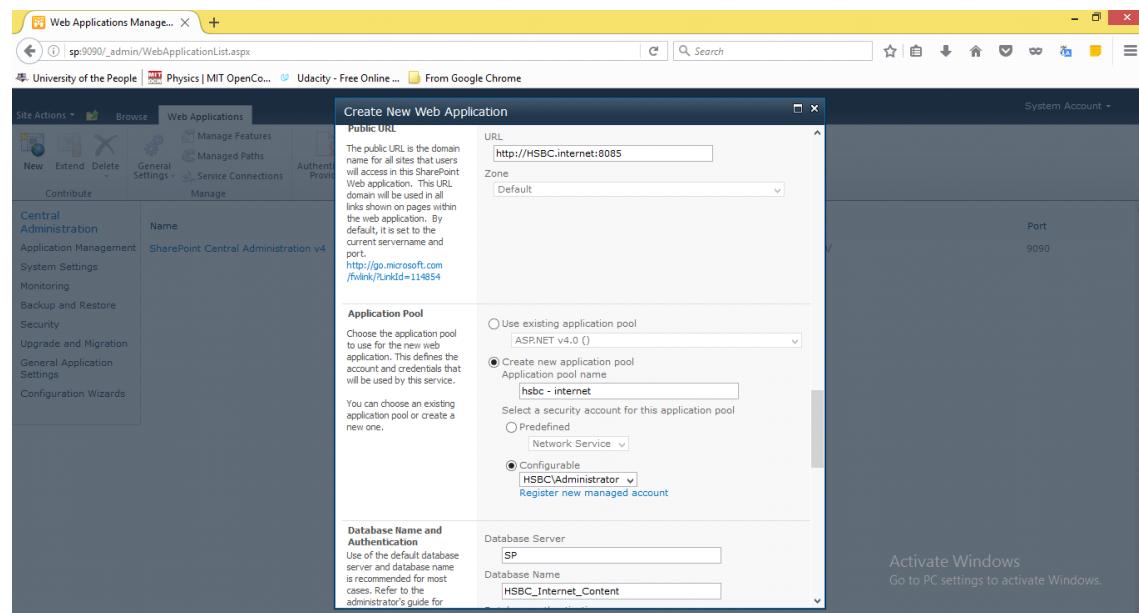


من ثم نختار الخيارات التي نريد أن يحويها التطبيق من عنونه و المندى الذي يستخدمه



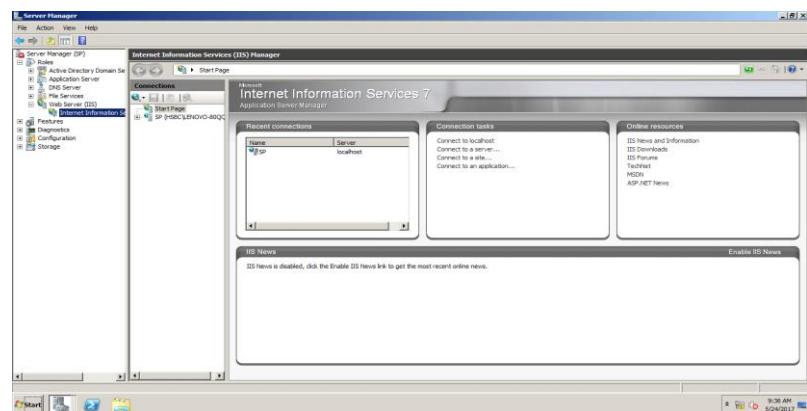


ونختار إعدادات قاعدة البيانات والمستخدم المسؤول عن التطبيق:



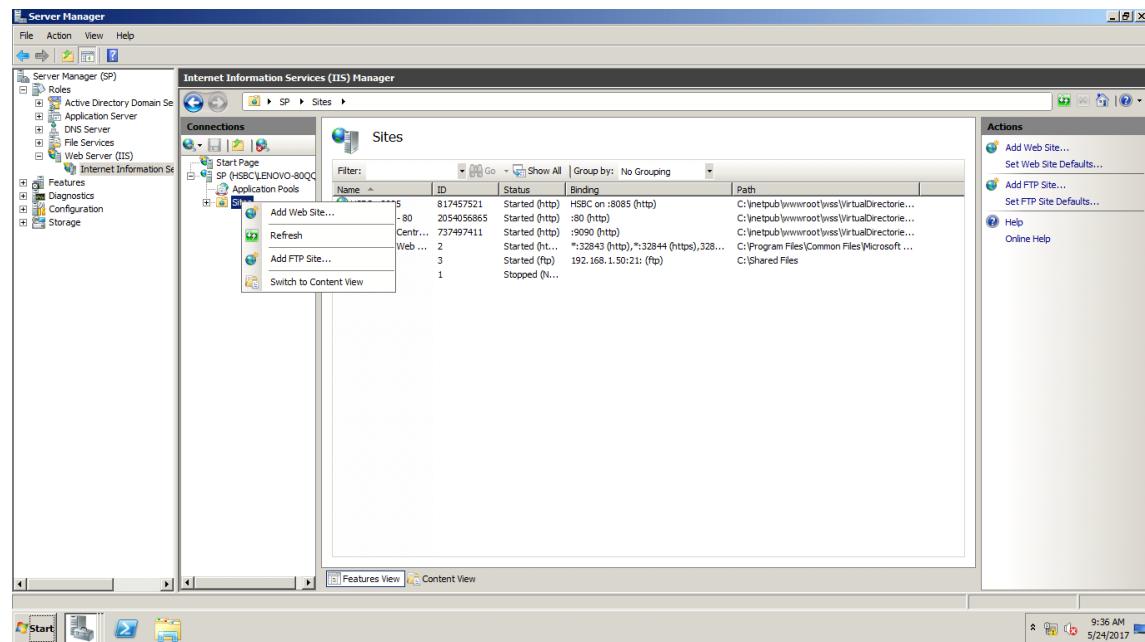
FTP

نفتح مخدم الويب بعد تنصيب خدمة الـ FTP مع مخدم الويب سابقاً(يقوم مخدم الويب بالتنصيب تلقائياً مع تنصيبنا للـ SharePoint):

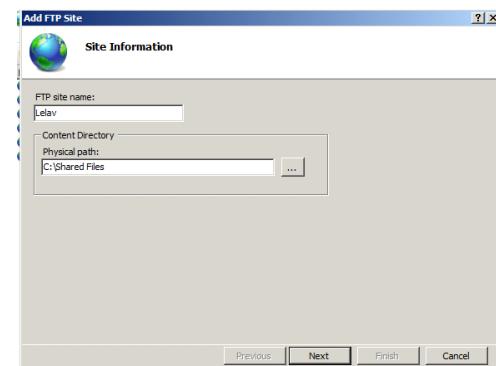




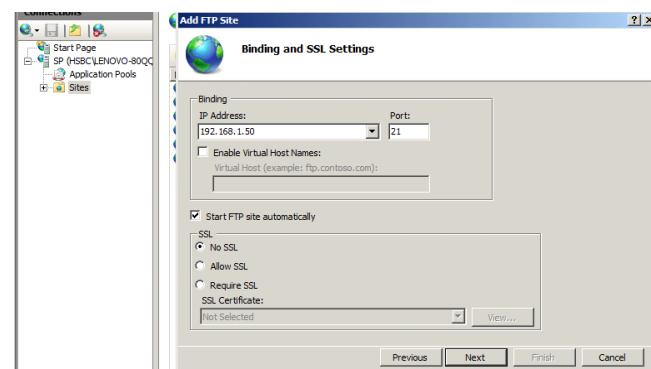
نقوم بالضغط زر يميني على ال Sites ومن ثم نضغط:



نقوم بتنمية موقع ال FTP ونحدد المسار الذي نريد مشاركته:

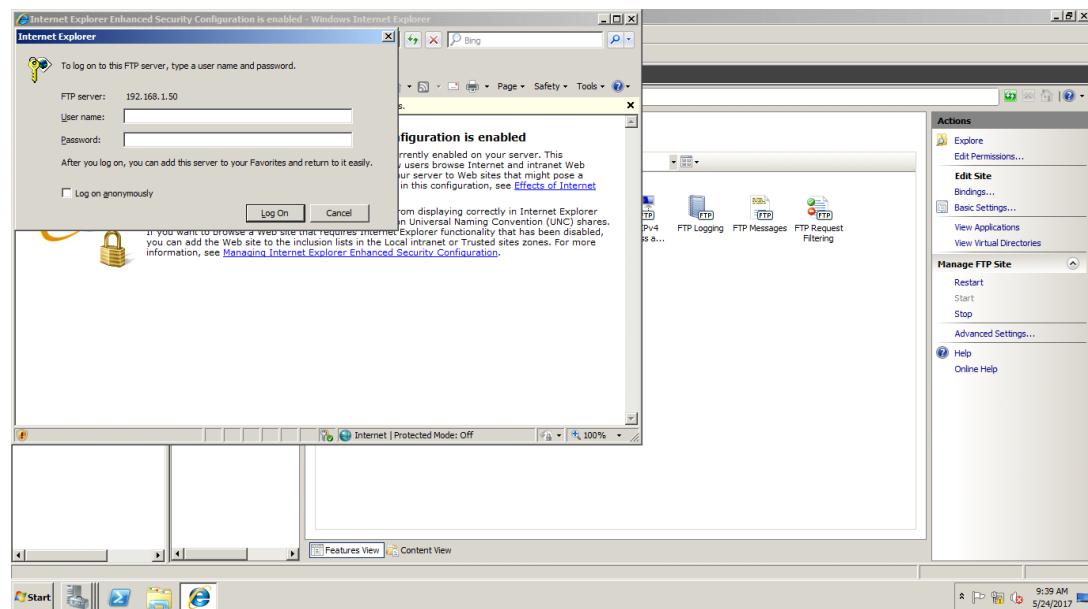


نقوم بتحديد عنوان ال IP لـ FTP Site ونختار اذا كان محمي بـ SSL أو لا:

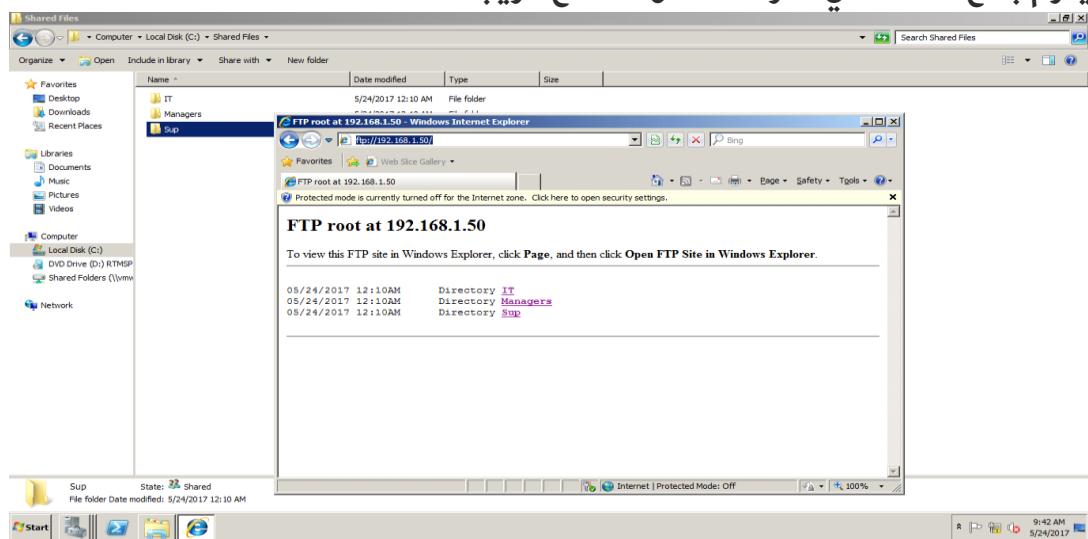




"ftp HYPERLINK "ftp://192.168.1.50/":// HYPERLINK "ftp://192.168.1.50/" HYPERLINK "ftp://192.168.1.50/" HYPERLINK "أي عنوان الموقع الذي حددناه سابقاً: ftp://192.168.1.50/"192.168.1.50"

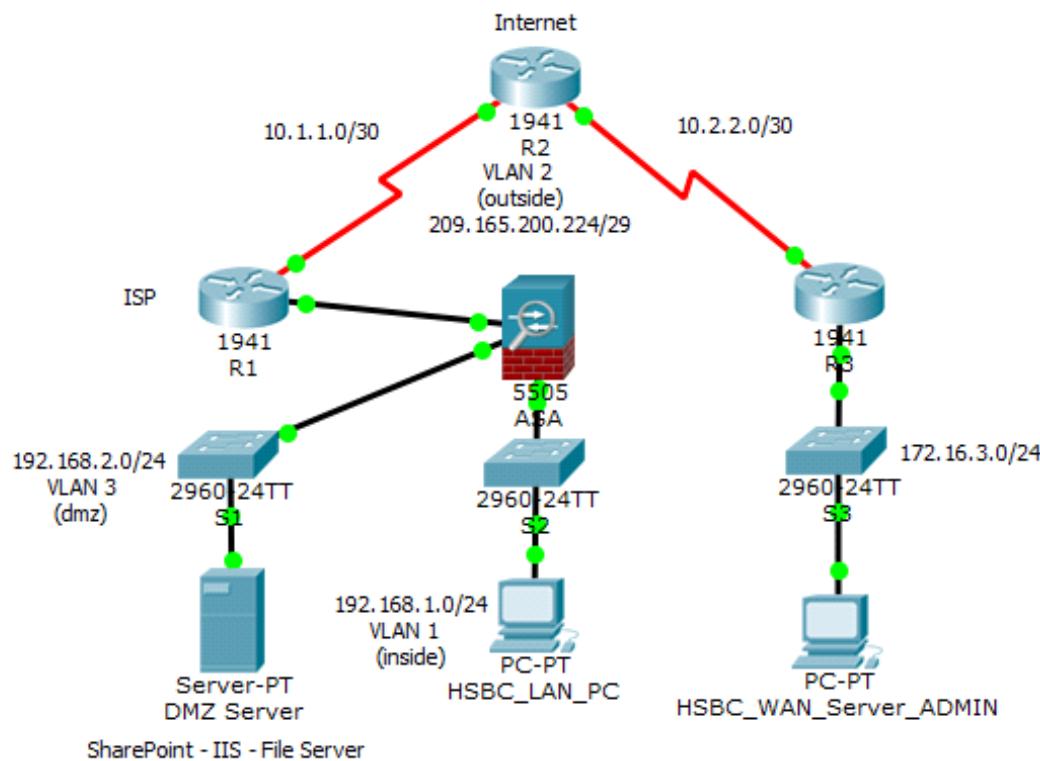


يقوم بفتح الملف الذي شاركناه داخل متصفح الويب:





DMZ



نقوم بتفعيل خدمة الـ

ASA على DMZ

على برنامج الـ Firewall

Cisco Packet Tracer

وذلك بـ

تعريف Interfaces Vlans

مختلفة سويات الحماية:

```
ciscoasa#conf t
```

```
ciscoasa(config)#hostname hsbc
```

```
hsbc(config)#domain-name hcbs.com
```

```
hsbc(config)#enable password 123
```

```
hsbc(config)#clock set 12:04:00 7 may 2017
```

```
hsbc(config)#interface vlan 1
```

```
hsbc(config-if)#nameif inside
```

```
hsbc(config-if)#security-level 100
```

```
hsbc(config-if)#ip address 192.168.1.1 255.255.255.0
```

```
hsbc(config-if)#ex
```

```
hsbc(config)#interface vlan 2
```

```
hsbc(config-if)#nameif outside
```

```
hsbc(config-if)#security-level 0
```

```
hsbc(config-if)#ip address 209.165.200.226 255.255.255.0
```



```
hsbc(config-if)#ex
```

من ثم نقوم بالتوجيه بين الـ Vlans للشبكتين الداخلية والخارجية:

```
hsbc(config-if)#route outside 0.0.0.0 0.0.0.0 209.165.200.225
```

```
hsbc(config)#show route
```

```
hsbc(config)#object network inside-net
```

```
hsbc(config-network-object)#subnet 192.168.1.0 255.255.255.0
```

```
hsbc(config-network-object)#nat (inside,outside) dynamic interface
```

```
hsbc(config-network-object)#end
```

وبعدها نقوم بتحديد الـ Vlan الثالثة المخصصة لـ DMZ ونقوم بتوجيهها:

```
hsbc(config)#interface vlan 3
```

```
hsbc(config-if)#no forward interface vlan 1
```

```
hsbc(config-if)#nameif dmz
```

INFO: Security level for "dmz" set to 0 by default.

```
hsbc(config-if)#security-level 70
```

```
hsbc(config-if)#ip address 192.168.2.1 255.255.255.0
```

```
hsbc(config-if)#ex
```

```
hsbc(config-if)#switchport access vlan 3
```

```
hsbc(config)#object network dmz-server
```

```
hsbc(config-network-object)#host 192.168.2.3
```

```
hsbc(config-network-object)#nat (dmz,outside) static 209.165.200.227
```

```
hsbc(config-network-object)#ex
```

وبعدها نقوم بوضع ACL ليتم تمرير فقط البروتوكولين HTTP و ICMP إلى الشبكة الخارجية:

```
hsbc(config)#access-list OUTSIDE-DMZ permit icmp any host 192.168.2.3
```

```
hsbc(config)#access-list OUTSIDE-DMZ permit tcp any host 192.168.2.3 eq 80
```

```
hsbc(config)#access-group OUTSIDE-DMZ in interface outside
```

Resources

- technet.microsoft.com
- Lynda.com
- Edx.org
- Active Directory for Dummies 2nd Edition
- Active Directory Design Guide by Microsoft
- Active Directory Fundamentals by Microsoft TechNet
- A Guide to Microsoft Active Directory (AD) Design by John Dias
- MCSA Guide to Installing and configuring Microsoft Windows Server 2012/R2 (Exam 70-410) By Greg Tomsho
- Installing and Configuring Windows Server 2012 R2 Exam Reference 70-410 by Craig Zacker
- Windows Server 2012 Administration Instant Reference by Matthew Hester and Chris



1	فكرة المشروع:
1	أهداف المشروع:
2	القسم النظري THEORETICAL DIVISION
3	NETWORK DESIGN
3.....	تقسيم طبقات الشبكة:
3.....	MSTP (MULTIPLE SPANNING TREE PROTOCOL)
3.....	تقسيم الـ VLANs على الفرع الرئيسي INSTANCES
4.....	GLBP (GATEWAY LOAD BALANCING PROTOCOL)
5.....	BPU FILTER
5.....	ROOT GUARD
6.....	LOOP GUARD
6.....	PORT FAST
6.....	OSPF (OPEN SHORTEST PATH FIRST)
7.....	SSH (SECURE SHELL)
7.....	BANNER
7.....	TRUNK
8.....	VLAN (VIRTUAL LAN)
9.....	INTER VLAN ROUTING
9.....	VTP
10.....	Vtp mode
10.....	VTP PRUNING
11.....	ETHER CHANNEL
12.....	IP HELPER
12.....	DHCP SNOOPING
13.....	NTP: (NETWORK TIME PROTOCOL)
13.....	SYSLOG
14.....	IP SLA (IP SERVICES LEVEL AGREEMENT)
14.....	RSPAN
15	NETWORK SECURITY
15.....	الشبكة الافتراضية VPN
15.....	PORT SECURITY
15.....	ACCESS CONTROL LIST
15.....	IPSEC
16.....	ENCAPSULATING SECURITY PAYLOAD (ESP)
16.....	LEASED LINE
16.....	TMG
17.....	AAA
18.....	MANAGEMENT SECURITY
18.....	NAT
19	NETWORK ADMINISTRATION
19.....	DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP)
19.....	DHCP Failover

19.....	DHCP Policies
19.....	Enabling Audit Logging
19.....	DOMAIN NAME SYSTEM (DNS)
20.....	Conditional Forwarder
20.....	Secure Dynamic Updates
20.....	Resource Records Aging & Scavenging
20.....	Active Directory Integrated Zone
20.....	DNS Socket Pool
21.....	DNS Cache Locking
21.....	DNSSEC
21	ACTIVE DIRECTORY DOMAIN SERVICES
21.....	Logical Active Directory
22.....	Physical Active Directory
22.....	Recycle Bin
22.....	Password Policies
22.....	Account Lock out Policy
22.....	Fine-Grained Password Policy
23.....	Group Policy Object (GPO)
23.....	Redircmp & Rediusr
23.....	RAID TECHNOLOGY
23.....	EXCHANGE
24.....	NAP (NETWORK ACCESS MANAGEMENT)
24.....	WSUS
24.....	MANAGE DISK QUOTE
24.....	RSAT (MICROSOFT REMOTE SERVER ADMINISTRATION TOOLS)
24.....	RDS (REMOTE DESKTOP CONNECTION)
24.....	SHAREPOINT
24.....	SQL SERVER
25.....	WEB SERVER
25.....	FILE SERVER
25.....	DMZ
25.....	BACKUP SERVER
26.....	VSS (VOLUME SHADOW COPY SERVICE)
27.....	WINDOWS DEPLOYMENT SERVICES
28.....	ADCS (ACTIVE DIRECTORY CERTIFICATE SERVICES)
29.....	DYNAMIC ACCESS CONTROL
30	القسم العملي PRACTICAL DIVISION
31	NETWORK DESIGN
31.....	TRUNK PROTOCOL
31.....	VLAN
32.....	INTER VLAN ROUTING
32.....	VLAN TRUNKING PROTOCOL (VTP)
34.....	ETHERCHANNEL

34.....	IP-HELPER
35.....	DHCP SNOOPING
35.....	NETWORK TIME PROTOCOL (NTP)
35.....	SYS LOG
35.....	STANDARD SERVICES AGREEMENT
36.....	RSPAN
36.....	OSPF
37.....	<i>damas-des2</i>
38.....	<i>damas-des1</i>
38.....	<i>damas-edge2</i>
38.....	<i>damas-edge1</i>
39.....	<i>ISP2</i>
39.....	<i>ISP1</i>
40.....	<i>western-union</i>
40.....	<i>homs-edge1</i>
41.....	<i>homs-edge2</i>
41.....	<i>homs-des1</i>
42.....	<i>homs-des2</i>
43.....	SSH
43.....	<i>configuration-damascus</i>
43.....	<i>damas-des1</i>
43.....	<i>damas-des2</i>
44.....	<i>Daccsw-vlans</i>
44.....	<i>Daccsw2-serv</i>
45.....	<i>Daccsw-serv</i>
46.....	<i>damas-edge1</i>
46.....	<i>damas-edge2</i>
47.....	<i>ssh configuration-homs</i>
47.....	<i>homs-des1</i>
47.....	<i>homs-des2</i>
48.....	<i>accsw-serv</i>
48.....	<i>accsw-vlans</i>
49.....	<i>homs-edge1</i>
49.....	<i>homs-edge2</i>
50.....	BANNER
50.....	MULTIPLE SPANNING TREE PROTOCOL (MST)
51.....	BPDU FILTER
51.....	ROOT GUARD
51.....	LOOP GUARD
52.....	GLBP (GATEWAY LOAD BALANCING PROTOCOL)
53	NETWORK SECURITY
53.....	AND IPSEC VPN
54.....	PORT SECURITY

56	CONTROL ACCESS LIST
57	AAA
64	اعدادات سيرفر ال TMG
91	NAT
92	MANAGEMENT SECURITY
93	NETWORK ADMINISTRATION
93	تثبيت ملفات ال BINARIES الخاصة بـ DHCP, DNS, ADDS
95	DHCP
95	DHCP Scopes
96	DHCP Policies
97	DHCP Failover
98	DNS
98	DNS Zone Creation
99	Adding resource records
99	Aging and Scavenging
100	DNS Cache Locking
101	Secure Dynamic Updates
102	Socket Pool
102	Conditional Forwarder
103	DNSSEC
104	ADDS
104	Domain Creation
104	Main Damascus DC (MDADD)
109	Promoting SDADD to a Domain Controller
110	Promoting HADD to a Read-Only Domain Controller
110	Replication Policy
111	OU Design and Creation
112	Users Addition
113	LogOn Hours
114	Trust Relationship
115	AGDLA
115	Global Groups
117	Domain Local Groups
117	Groups Creation
117	Group Members Addition
117	PSO
117	Employees PSO
118	Management and IT PSO
118	Default Domain PSO
118	GPO
118	Normal Employees
119	Management
120	IT Staff

120.....	<i>Redircmp & Redirusr</i>
121.....	<i>Recycle Bin</i>
121.....	BACKUP SERVER
122.....	تنصيب خدمة النسخ الاحتياطي
122.....	إعداد جدولة النسخ الاحتياطي
124.....	استعادة البيانات
126.....	VSS (VOLUME SHADOW COPY SERVICE)
127.....	WDS
130.....	DAC
131.....	<i>Create claim</i>
132.....	<i>create central access role</i>
133.....	<i>إنشاء central access policy</i>
134.....	ADCSs ACTIVE DIRECTORY CERTIFICATE SERVICES
134.....	CERTIFICATE AUTHORITY
136.....	CONFIGURATION
147.....	RAID REDUNDANT ARRAY OF INDEPENDENT DISKS
147.....	RAID 10
147.....	FILE AND STORAGE
152.....	انشاء المجال الاول للاول قرصين
156.....	انشاء الاقراص الـ Mirror من المجالين السابقين
157.....	الخطوة الأخيرة وهي انشاء الـ Strip volume
161.....	NAP NETWORK ACCESS PROTECTION
177.....	WSUS WINDOWS SOFTWARE UPDATE SERVER
202.....	SHAREPOINT
202.....	<i>SQL Installation</i>
206.....	<i>SharePoint</i> تنصيب الـ
209.....	FTP
212.....	DMZ
214	RESOURCES