

# NetWork Set

First Arabic Magazine For Networks

**KRA**  
Key Recovery Agent

كيف تحدد آخر نظام  
تشغيل خاص قامت  
سيسكو بإصداره .

**HONEY POT**

**WINDOWS INTUNE**

الاستضافة في  
Datacenters الـ  
و انواعها

**SHADOW COPY  
WINDOWS  
SERVER 2012**

**HOW TO USE  
HYPER-V  
2012 REPLICA**





مجلة NetworkSet مجلة الكترونية  
شهرية متخصصة تصدر عن موقع:  
[www.networkset.net](http://www.networkset.net)



جميع الآراء المنشورة تعبر عن وجهة نظر  
الكاتب ولا تعبر عن وجهة نظر المجلة

جميع المحتويات تخضع لحقوق الملكية  
الفكرية و لا يجوز الاقتباس أو النقل دون  
إذن من الكاتب

[www.networkset.net](http://www.networkset.net)

## أسرة المجلة :

المؤسس

م.أيمن النعيمي



رئيس التحرير

م. أسامة كامل



## المحررون

م.حسام الدين حشيش



م.خالد الدسوقي



م.محمد عماد الجفصي



م.ولاء عصام حسن



م.باسم حامد بكر



م.أحمد خير الدين



التصميم و الاخراج الفني

محمد زرقة



# NetWork Set

First Arabic Magazine For Networks

## CONTENTS

51 - 49

كيف تحدد آخر نظام تشغيل خاص قامت سيسكو بإصداره.

بقلم :م.أيمن النعيمي

57 - 53

Honey pot

بقلم :م. محمد عماد الجفصي

59 - 58

خمسة نصائح لمنع المستخدم من الاستخدام الخاطئ

بقلم :م. أيمن النعيمي

الكلمة الافتتاحية

04

الإيمان المطلق

بقلم : محمد زرقعة

مقال العدد المميز

28 - 07

KRA (Key Recovery Agent )

بقلم : م. باسم حامد بكر

مقالات العدد

34 - 31

Shadow Copy windows server

2012

بقلم :م. حسام الدين حشيش

38 - 35

Windows Intune

بقلم : م.خالد الدسوقي

41 - 40

الاستضافة في الـ Datacenters وأنواعها

بقلم : م. أحمد خير الدين

48 - 42

How to Use Hyper-V 2012

Replica

بقلم : م.ولاء عصام حسن



# الإيمان المطلق

بقلم محمد زرقة

في كل عام في وقت محدد من السنة اعتدنا على الطوفان الذي تسببه الأمطار الغزيرة في منطقة معينة في مدينتي فصادف أن كنت بالجوار في هذا العام و شاهدت المنازل و المحال التجارية و هي تفيض و أهلها يتساعدون على تفريغ محلاتهم و بيوتهم من فائض الماء ، و تذكرت أن صديقي منزله في هذه المنطقة و هو بالطابق الأرضي فأسرت الخطى إليه لعلني أمد له يد المساعدة و أساهم معهم في حل هذه المشكلة و لاحظت كم الجوار متضرر و الحدائق تنبع منها المياه من كل حدب و وصوب ، و عندما وصلت الى منزل صديقي لم أجد فيه آثار للمياه و لا الطوفان و كل شيء طبيعي فيه ... فاستغربت .. و عندما فتح لي الباب بادرت بالسؤال هل تضررت بالطوفان؟؟؟ فجاوبني بابتسامة واثقة ... كلا ... و لم أتأثر بالطوفان و قد قرأت دعاء حفظ المنزل من الحريق و الغريق صباحاً ... !! فقال لي : ألم يقل لنا رسول الله صلى الله عليه وسلم :من يقول هؤلاء الكلمات في الليل أو النهار لم يضره شيء فمن قالها لم يصبه في نفسه ولا في أهله و لا ماله شيء يكرهه و هي:

((اللهم أنت ربي لا اله إلا أنت عليك توكلت و أنت رب العرش العظيم ,ما شاء الله كان ,و ما لم يشأ لم يكن ,لا حول ولا قوة إلا بالله العلي العظيم أعلم أن الله على كل شيء قدير ,و أن الله قد أحاط بكل شيء علماً ,الهم أعوذ بك من شر نفسي ,ومن شر كل دابة أنت أخذ بناصيتها إن ربي على صراط مستقيم)).

ألا تؤمن بأن رسول الله أصدق الصادقين و ما ينطق عن الهوى؟؟؟ فقلت نعم ... فقال لي ...إذا آمن به و بيقين فلن يضرك الله شيئاً بإذن الله .

أخواني الأعزاء ... لا يخفى حالنا على أحد فبلدنا قد لاقى ما لاقى و كثر فيه القيل و القال و لم يبقى أحد إلا أفتى فيه و كثرت الحلول و لم تطبق ، و لم تبقى جهة دبلوماسية او شعبية الا و أرادت إيقاف أو الحد من الذي يجري في سورية ... ولكن كل هذه الجهود بأنت بالفشل ... و لم تفلح ... و كنا ولا زلنا نعول على فلان أو دولة أو مؤسسة علها تساهم في وقف العنف و الاقتتال ... و نسينا أن الله عز و جل هو المدبر و هو المبدئ و هو الذي بيده مفاتيح الحلول جميعاً ...

علينا أن نكون جميعاً كما حال صديقي ... مؤمنين بالله عز و جل و **بيقين** أن هذه الغمامة لن تنزاح عن بلدنا و هذه الفتن لن ترفع عنه إلا بحول الله وحده و أخص هنا ( اليقين المطلق ) و علينا أن نرجع جميعاً الى الله و نعلن التوبة الصادقة و أن نعمل بصدق لوقف هذا الحال و أن ندعو الله عز و جل بقلب طاهر صادق و أن نتخذ هذه القاعدة القرآنية: {وَمَنْ يَتَوَكَّلْ عَلَى اللَّهِ فَهُوَ حَسْبُهُ} و من كان الله حسبه فهو كافي و واقية فلا مطمع فيه لعدوه ، فلو توكل العبد على الله تعالى حق توكله و كادته السموات والأرض و من فيهن لجعل له مخرجاً من ذلك وكفاه ونصره.

و حسبنا الله نعم المولى و نعم الوكيل.



# NetWork Set



محدثى جديد لعالم الشبكات  
في سماء اللغة العربية

## المدونة



مدونة عربية متخصصة  
في مجال الشبكات

زيارة الصفحة [GO](#)

## المجلة



أول مجلة عربية متخصصة  
في مجال الشبكات

زيارة الصفحة [GO](#)

## الموسوعة



Wiki.NetworkSet

أول موسوعة عربية حرة  
و متخصصة في مجال الشبكات

زيارة الصفحة [GO](#)

## ترجم



أول مشروع عربي لترجمة  
المواد العلمية و التقنية

زيارة الصفحة [GO](#)

## القناة



قناة المدونة  
على موقع يو تيوب

زيارة الصفحة [GO](#)

## (س) و (ج)



قسم خاص  
بالأسئلة والاجوبة

زيارة الصفحة [GO](#)



# مقال العدد المميز

**NetWork Set** Magazine



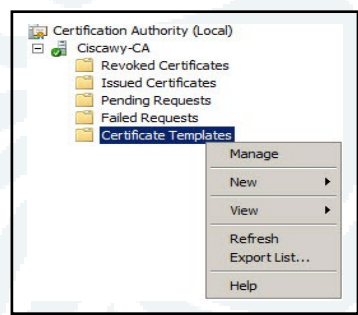


# KRA



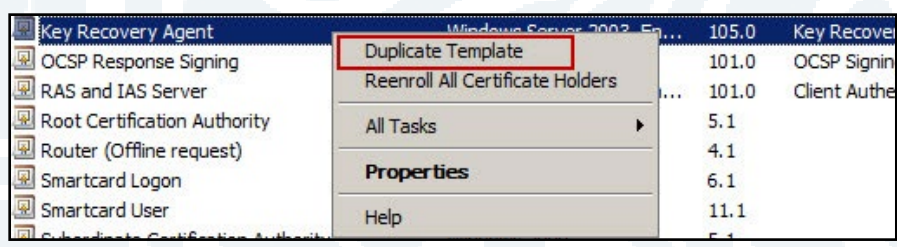
هل قابلك مشكله فقد الـ Certification الخاصة بك أو بأي مستخدم آخر ولم يعد بإمكانك أن تفتح الملفات الخاصة بك أو أن تفتح أي Office Files ؟ أو أنك قمت بتشفير بعض الملفات ولم تستطع أن تقوم بفتحها مرة أخرى باستخدام الـ Certification Authority المقدمة من ميكروسوفت ؟ بتوجب عليك أن تقوم بعمل **Key Recovery Agent ( KRA )** وهو عبارة عن مستخدم User له صلاحيات استرجاع الـ Certification الخاصة بالمستخدمين.

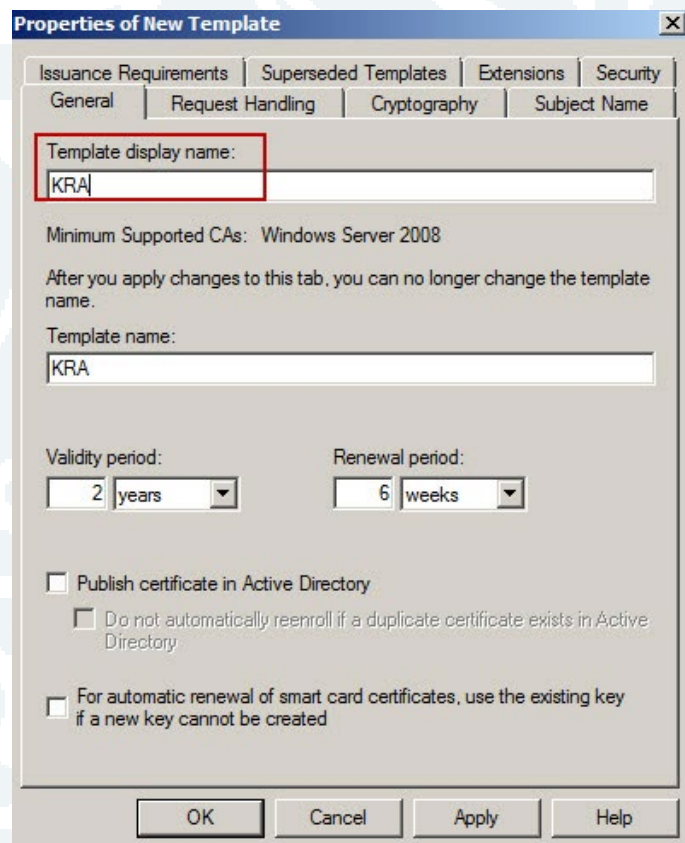
- يجب أن يتم إنشائه قبل أن يقوم أي مستخدم بطلب أي Cert. لمدة صلاحياتها سنتان.
- يجب أن نقوم بإنشاء User Account حتى يكون مسؤول عن هذه الخدمة ويكون لديه صلاحيات أنه يقوم بعمل Recover لأي Cert.
- لابد أن يكون هذا الـ User أيضاً Member of Domain Admin Group .
- نقوم بفتح الـ CA ونفتح الـ Cert Template .



Manage → R.click

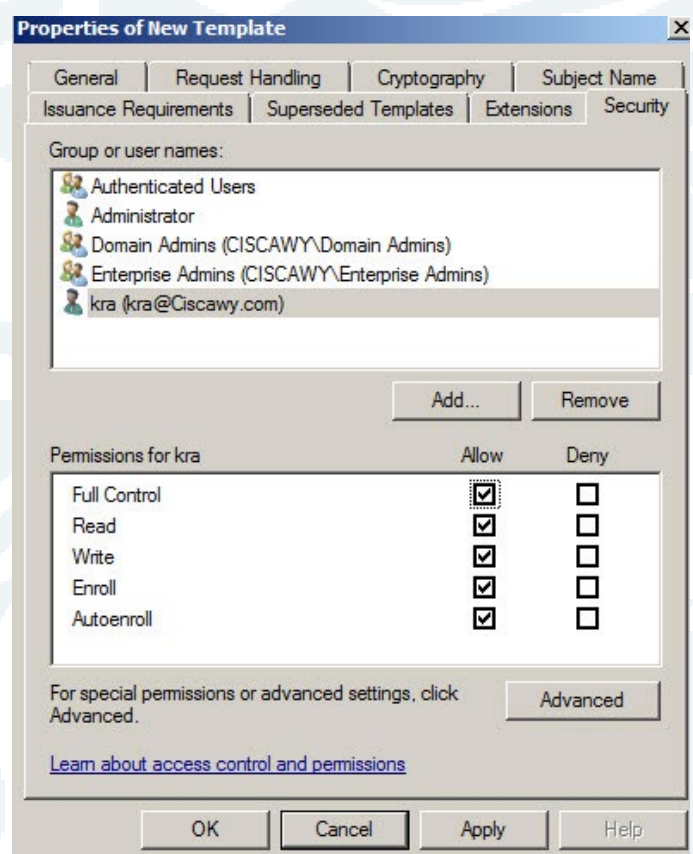
Duplicate ونختار الـ Template الخاصة بالـ KRA





### نختار الـ Security

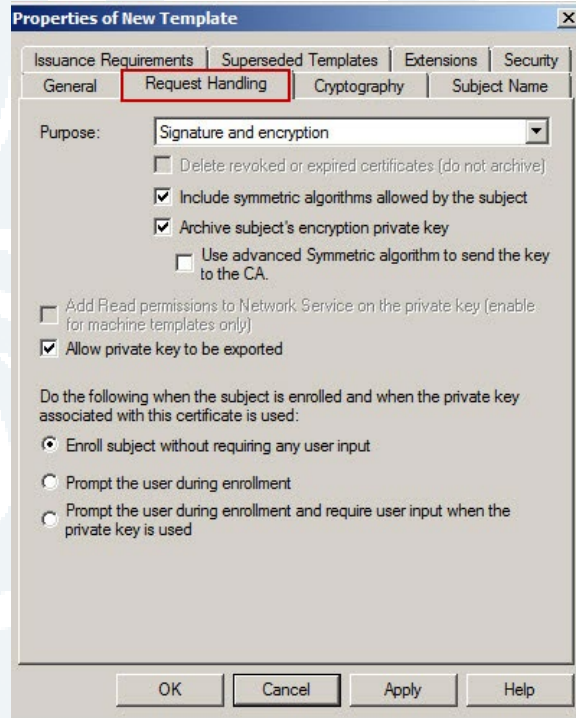
• يتم إضافة الـ User الذي تم إنشائه ونضيف له صلاحيات الـ Full Control





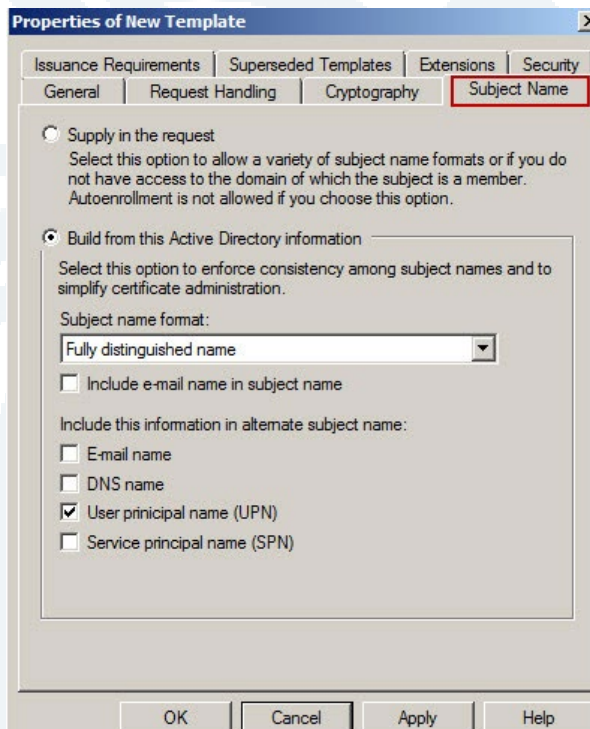
وأيضاً نقوم بإضافة Full Control للAuthenticated User  
OK → OK

نقوم أيضاً بعمل Duplicate لـ Template المسماه بالـ User  
نختار الـ Request Handling ونعدلها  
كما هو موضح أن الـ Private Key الخاص بأي Cert يقوم بحفظ الـ Private Key الخاص بها

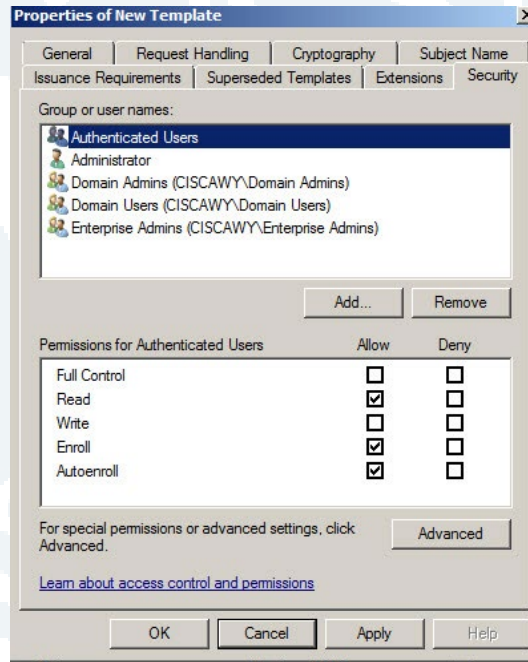


### Subject Name

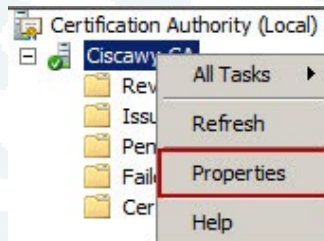
ونقوم بحذف الـ الخاصه بالـ E-mail والـ Include  
أي لا يشترط أن يكون الـ User المسؤول عنها سوا UPN فقط



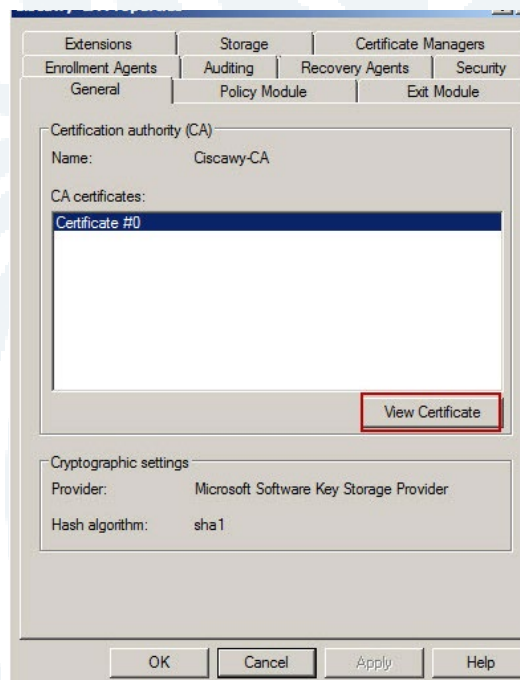
## نضيف للـ Authenticated صلاحيات Enroll & Autoenroll



- بعد ذلك نقوم بعمل Issued لهذين الـ Templates .
- نقوم بالدخول بحساب الـ KRA على الـ Server Machine .
- ونقوم بفتح الـ MMC لعمل Request للـ Cert الخاصة به حتى يتم التعامل مع بموثوقية من قبل الـ Server .
- نقوم بنسخ الـ Cert الخاصة بالـ Root لكي نقوم بتعريف الـ KRA من هو الـ Server Root
- R.click على اسم الـ Domain

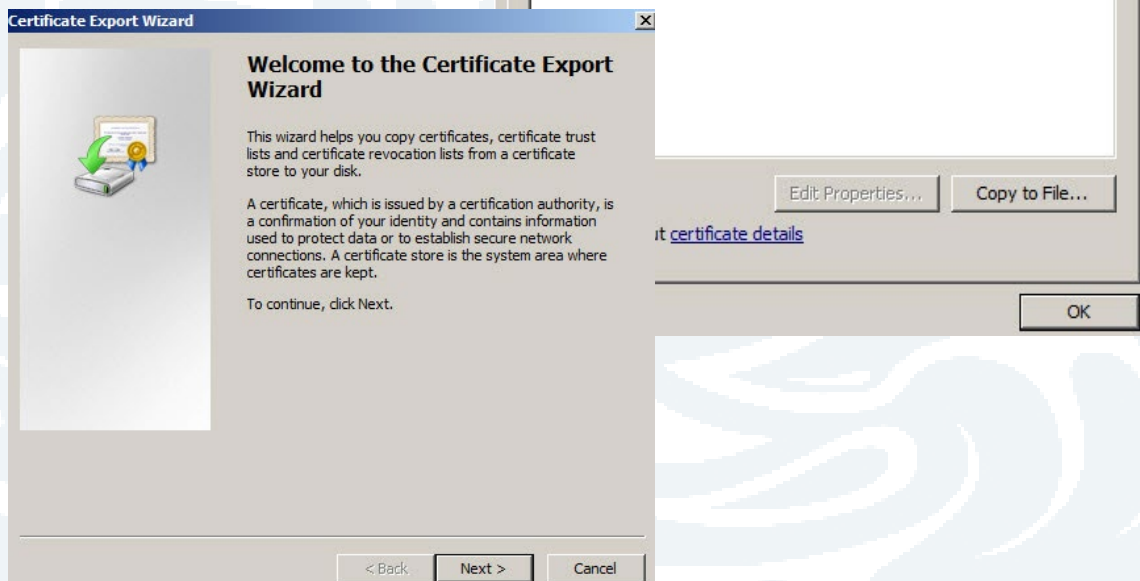
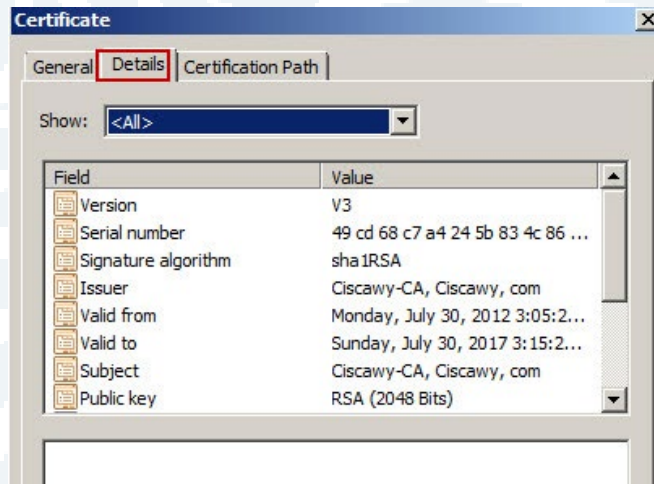


### نختار View Cert

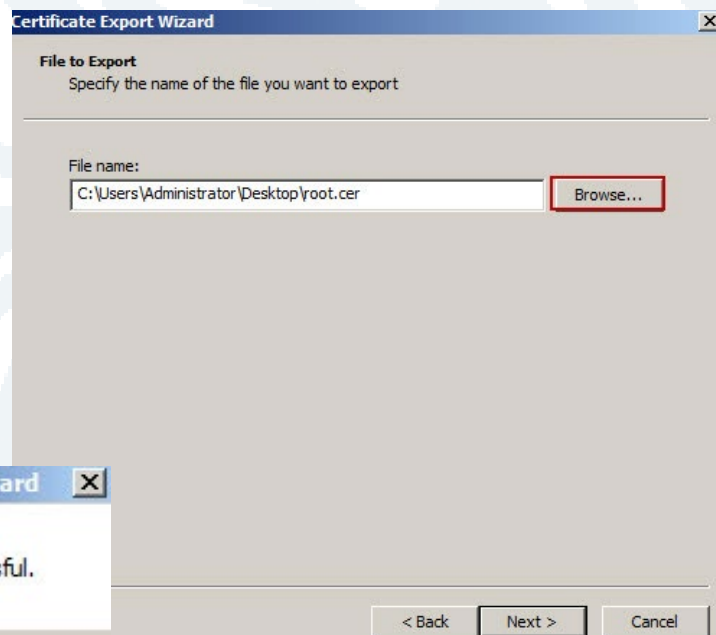




Details → Copy to File

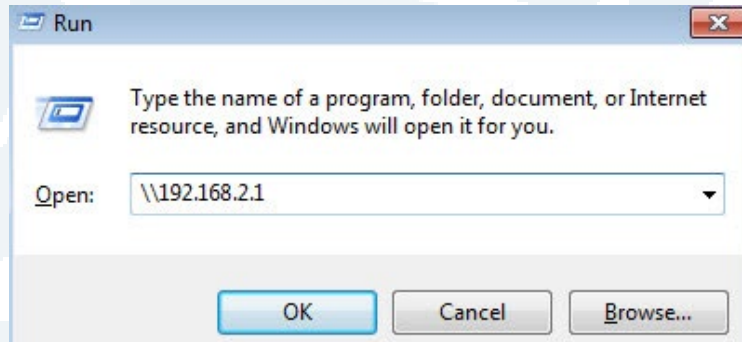


Next → Next  
نختار مكان الحفظ

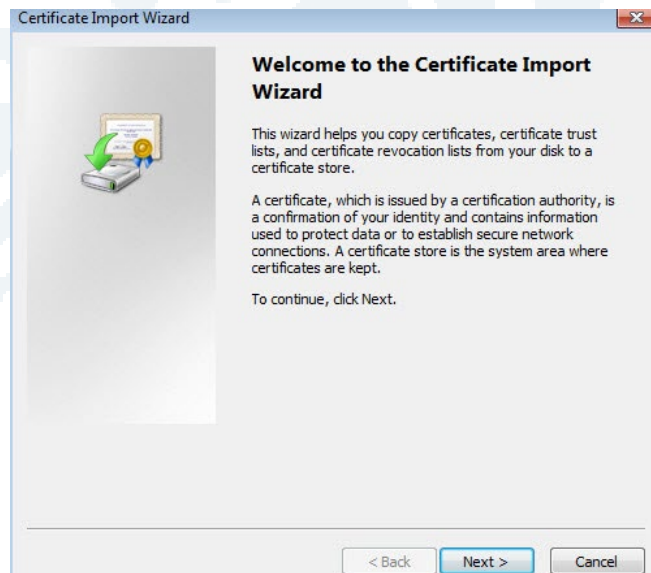
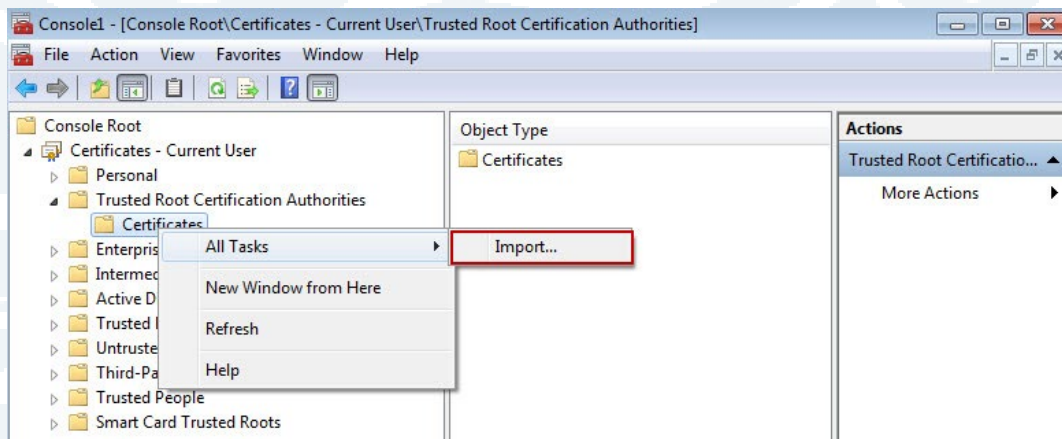


## ثم نقوم بوضعها في Shared Folder

- بعد ذلك نقوم بالدخول على حساب الـ Win-7 بالـ KRA User ونقوم بالدخول على الـ Shared Folder ونسج الـ Cert على سطح المكتب

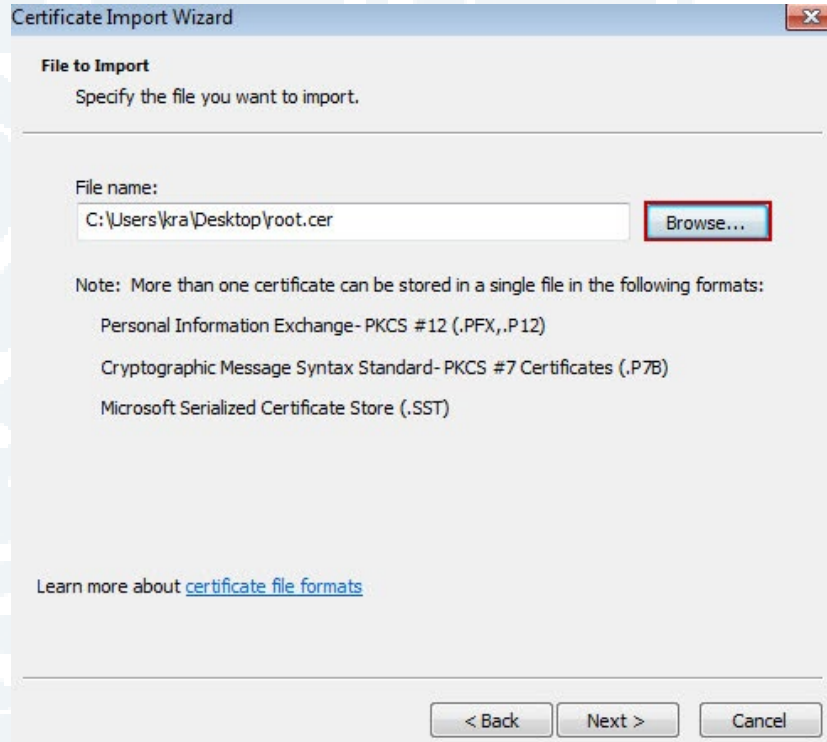


نقوم بفتح MMC → Run → Start  
 Add\Remove Snap-in → File  
 Trusted Root → All Tasks → Import





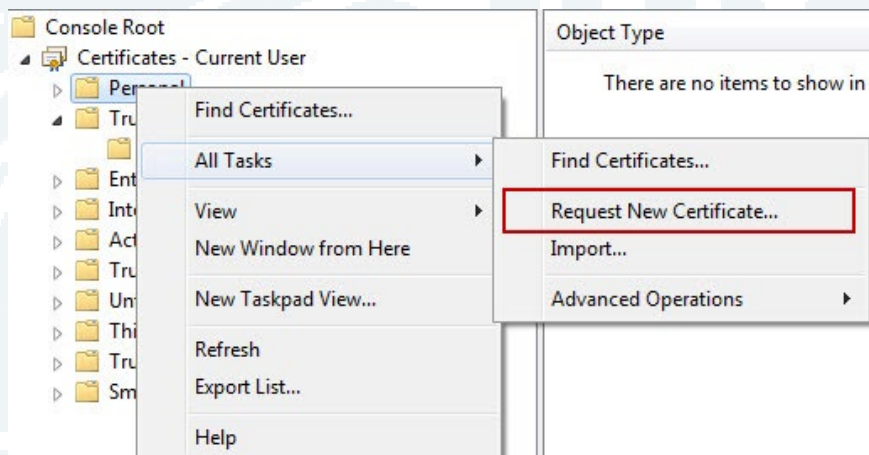
## نختار Cert

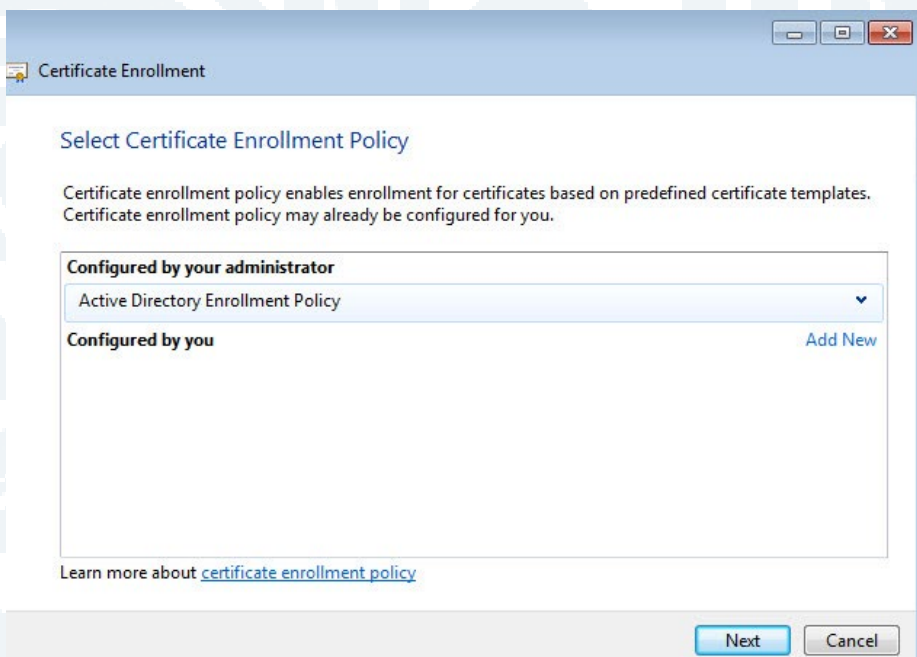
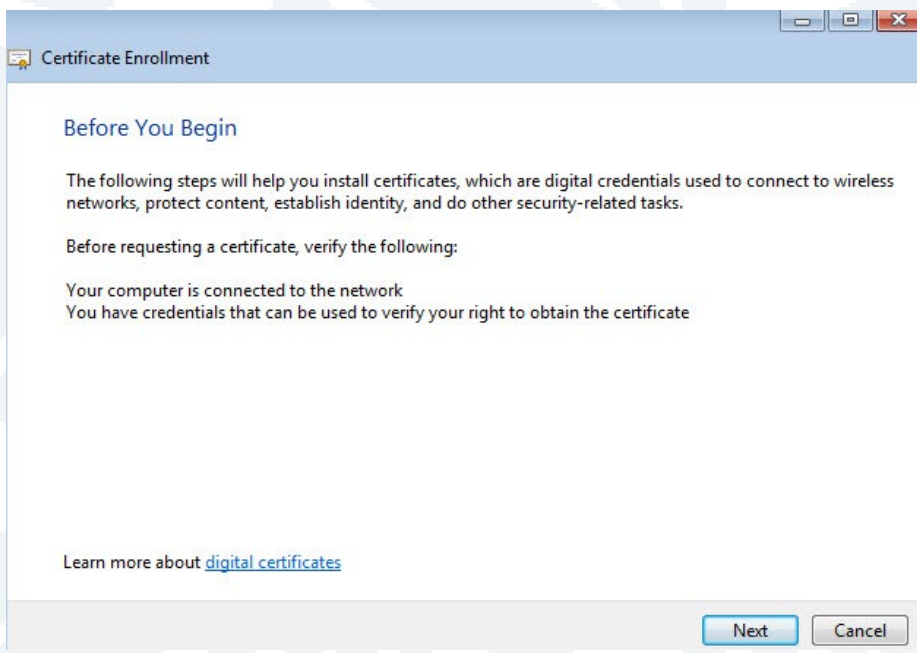


Next → Next

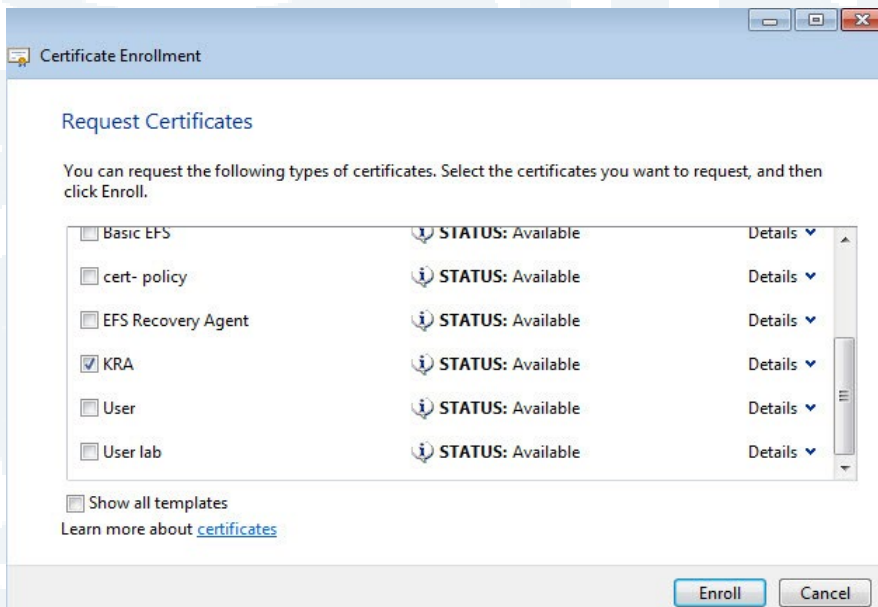


• على الـ Personal نقوم بعمل R.click ونختار Request New Cert





## نختار الـ KRA



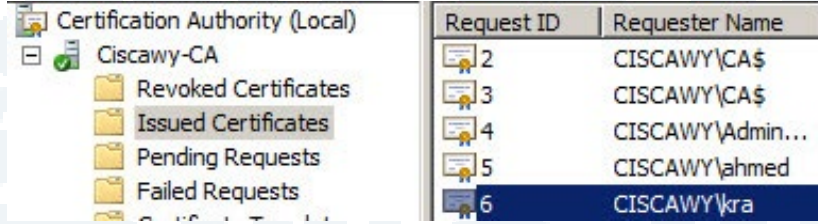


Next → Finish

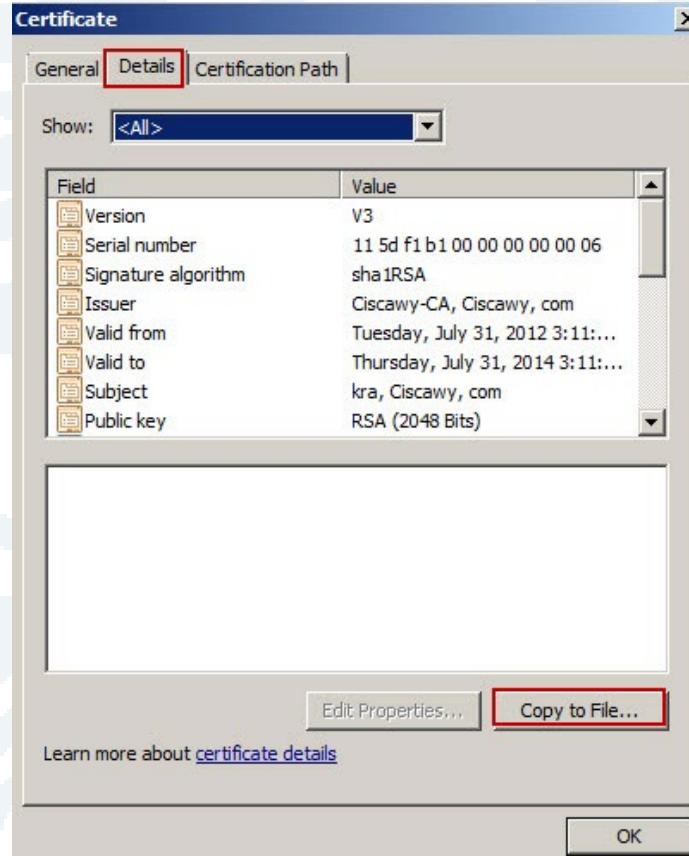
سنلاحظ أنه لم يتم إضافتها بعد

حيث أن هذه Cert هي الوحيدة التي يجب أن يقوم Administrator بعمل Issued من على الـ Root CA لها نظراً لأهميتها.

• نقوم بالدخول على الـ Server مرة أخرى.  
ونقوم بفتح الـ CA ونختار الـ Issued Cert ومنها الـ KRA

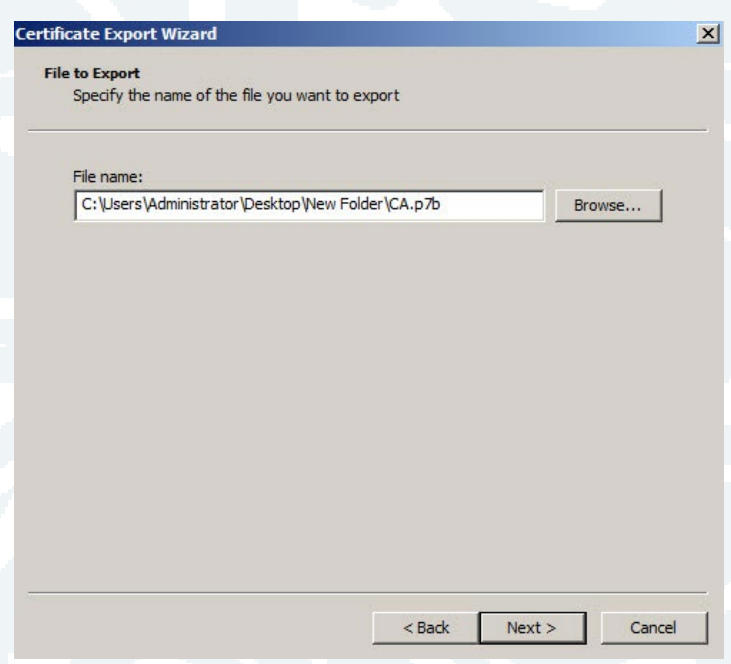
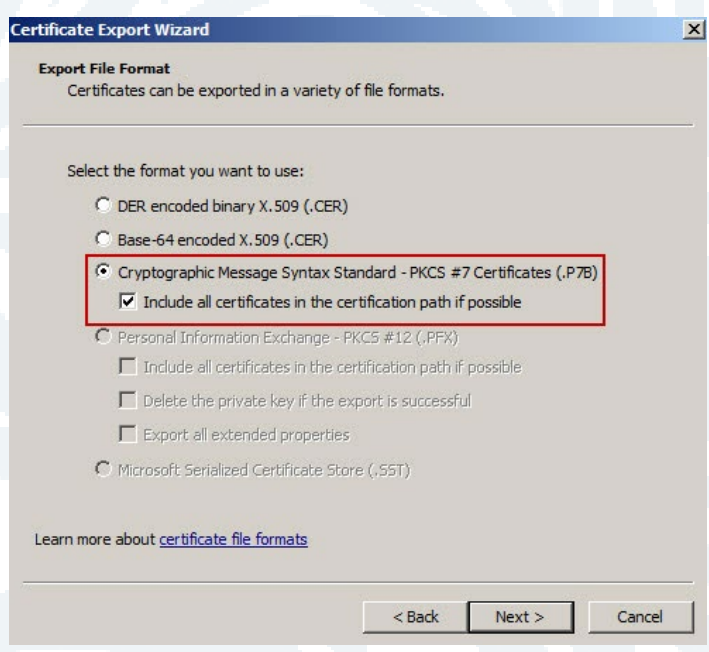


نقوم بالضغط D.Click عليها ونختار Details



ومنها Copy to File

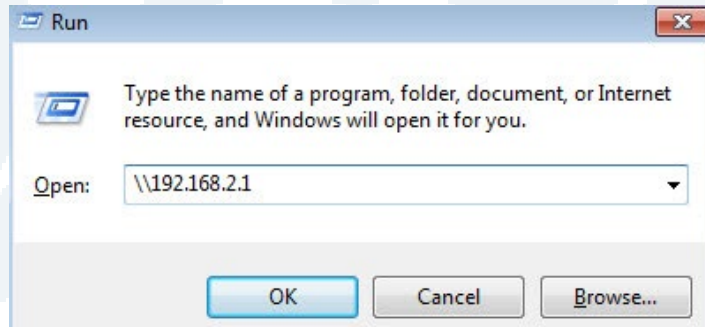
## ونختار الـ Cryptographic Message



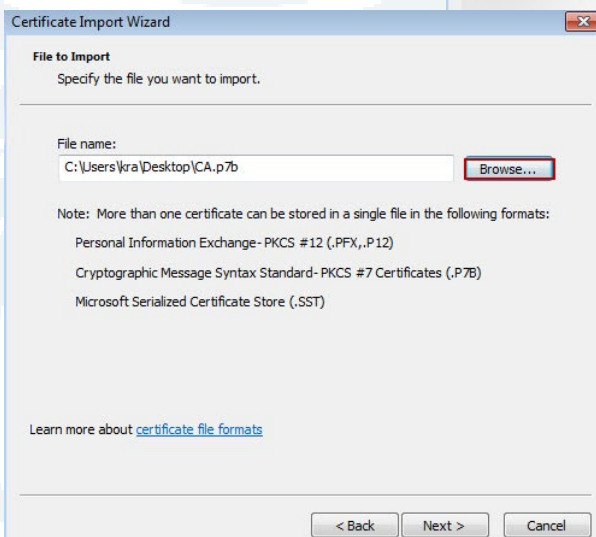
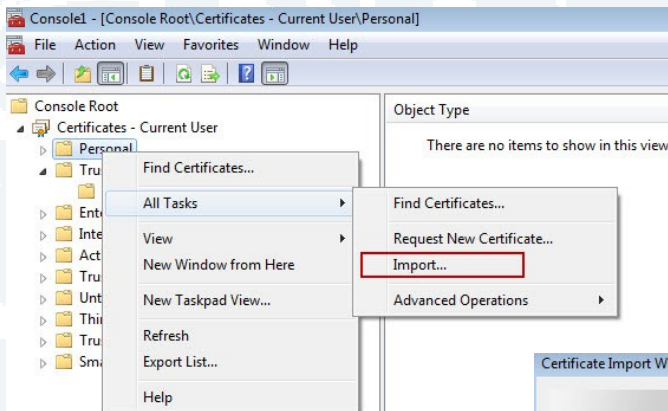


ثم نقوم بوضعها في Shared Folder أو نضعها في نفس الـ Shared السابق

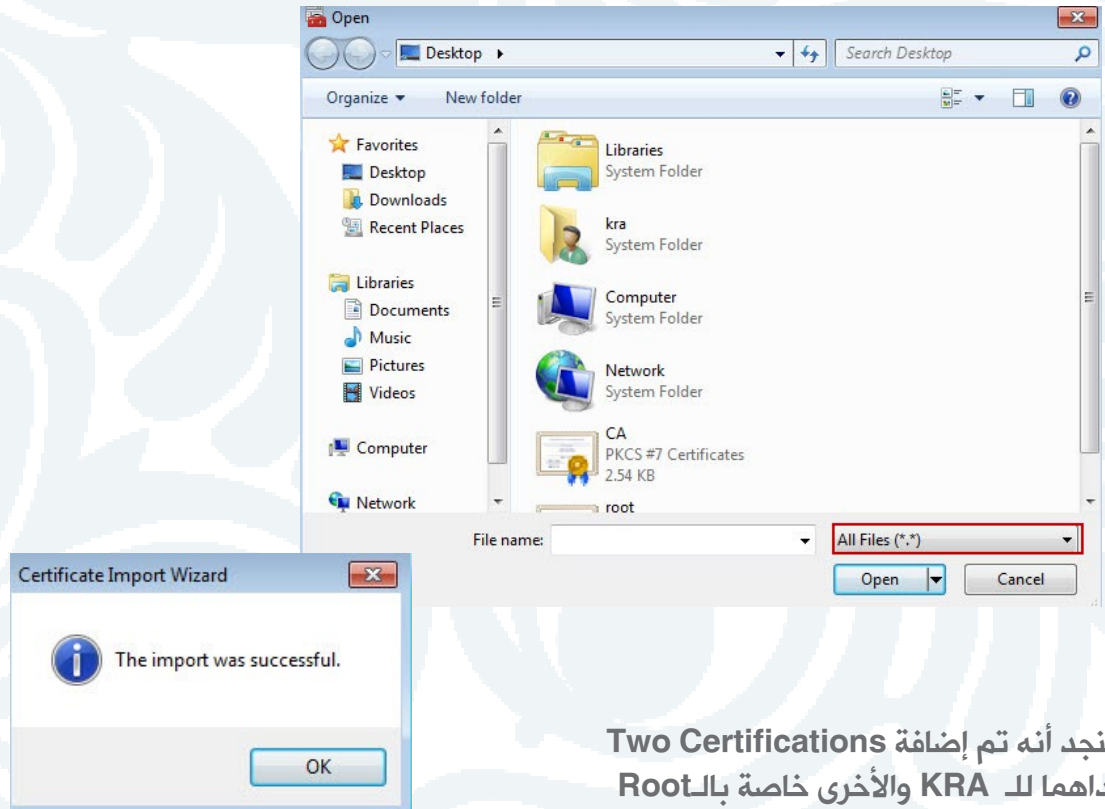
• بعد ذلك نقوم بالدخول على حساب الـ Win-7 ونقوم بالدخول على الـ Shared Folder ونسخ الـ Cert على سطح المكتب.



نقوم بفتح MMC Start → Run → MMC  
File → Add\Remove Snap-in  
R.click on Personal → All Tasks → Import

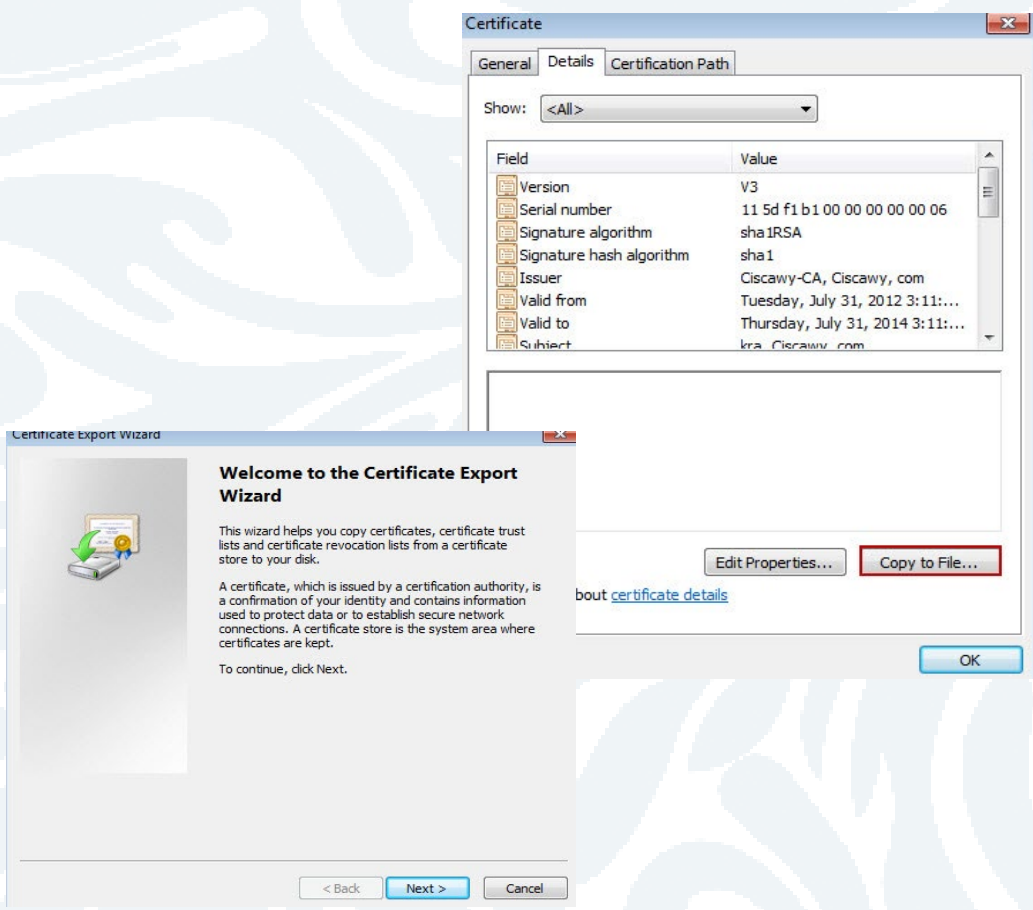


## نختار All Files حتى نستطيع أن نرى الامتداد الخاص بها



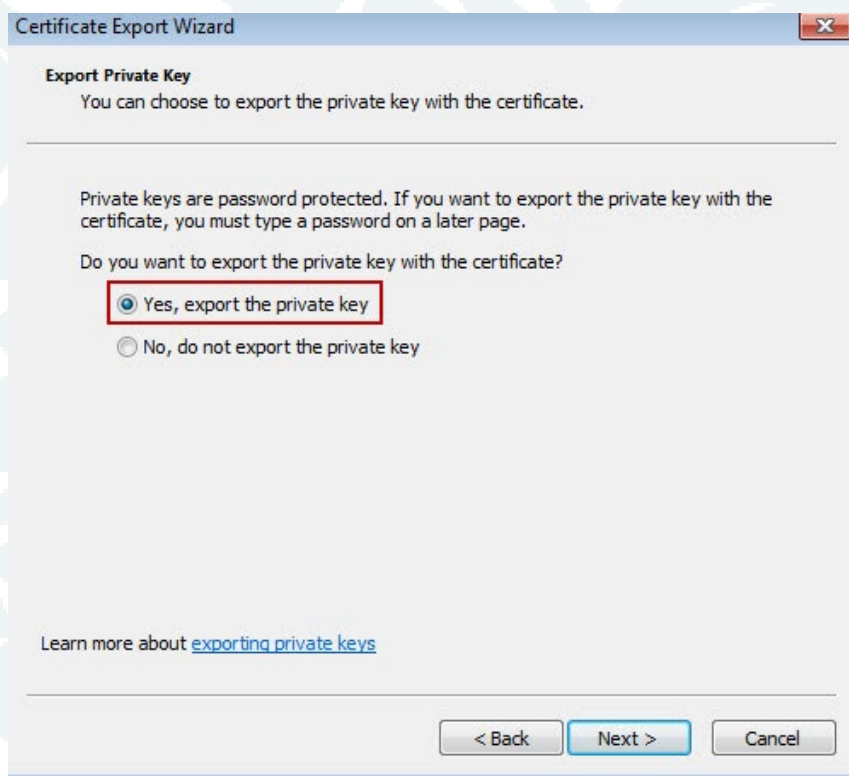
• سنجد أنه تم إضافة Two Certifications لإحداهما للـ KRA والأخرى خاصة بالـ Root

• نقوم بالضغط D.Click على الـ Cert الخاصة بالـ KRA  
Details → Copy to File



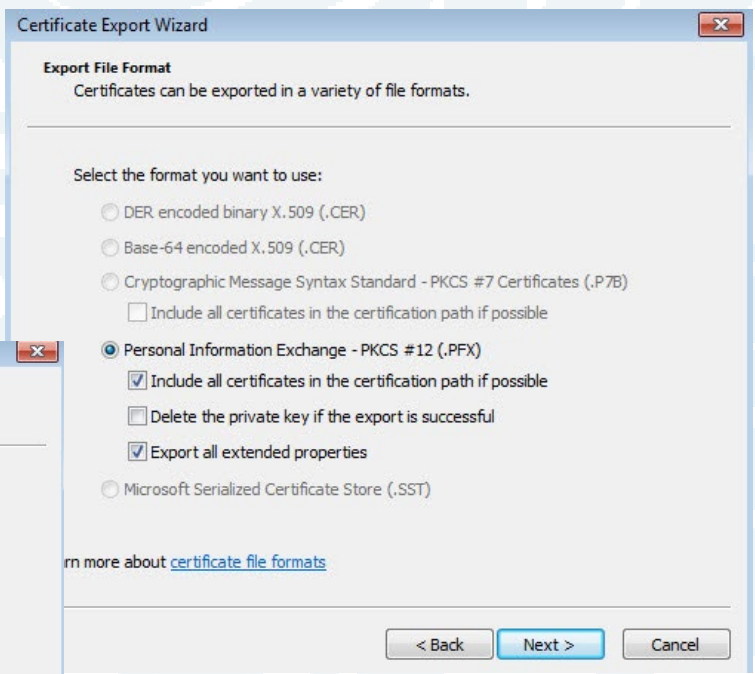
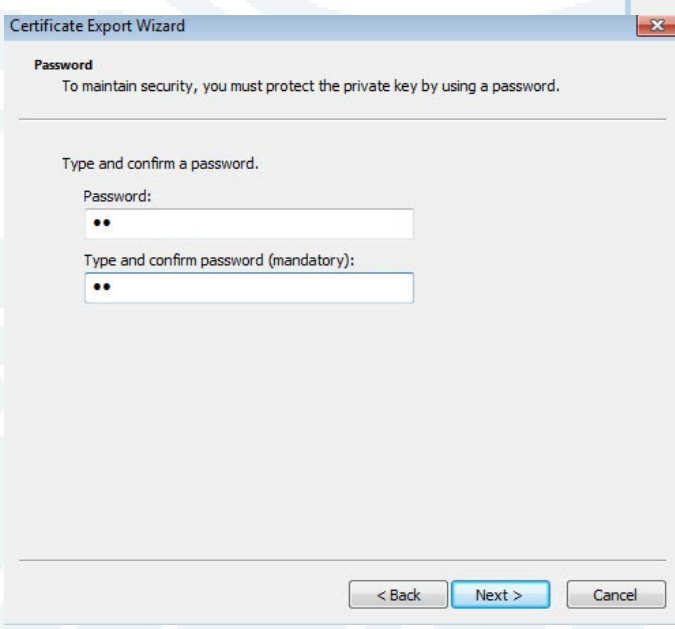


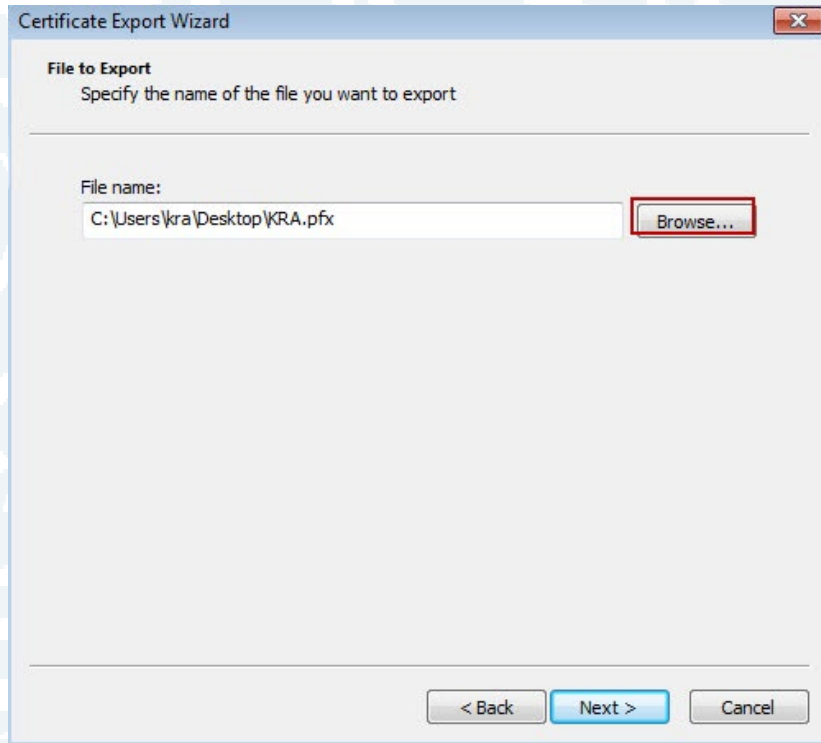
نختار أن يتم إضافة الـ Private Key معها حيث أنه عندما تقوم بعمل Import و Export لأي Cert يحدث تغيير في الـ Key الخاص بها



نقوم بالتعديل كما هو موضح

نضيف لها كلمة مرور



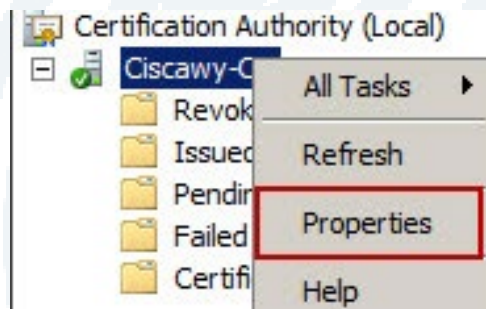


نقوم باختيار مكان للحفظ  
Next → Next

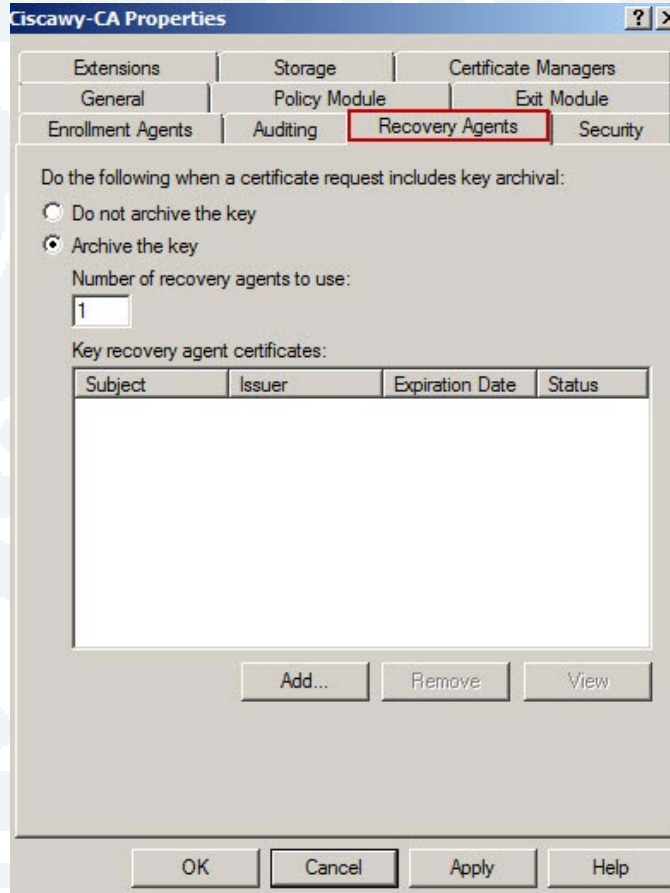


وبعد ذلك نقوم بحفظها في مكان هام جداً حتى لا نفقدتها.

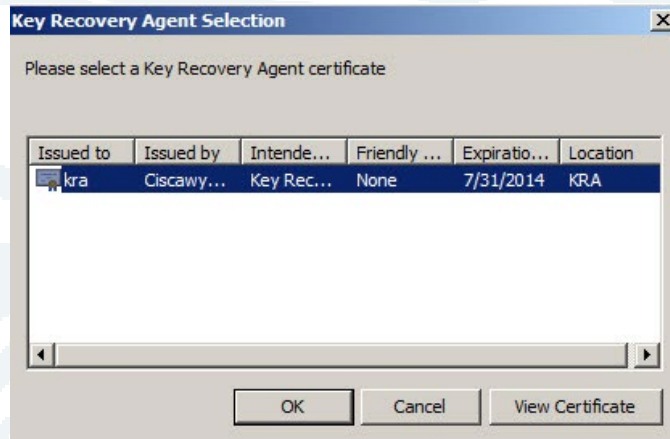
- وهي خطوة مهمة جداً KRA أن هناك Root CA نقوم بتعريف الـ R. Click on Domain → Properties



نختار الـ Recovery Agent ونختار Archive the Key



ونقوم بالضغط على **Add**  
 سنجد أنه موجود ونضغط على **OK**



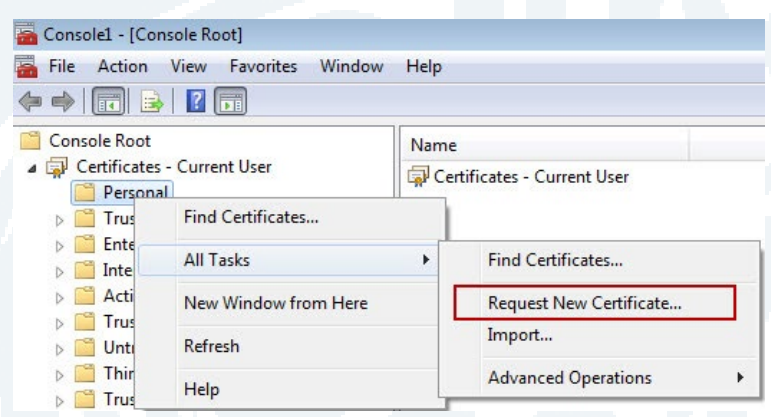
سيطلب أن يقوم بعمل إعادة تشغيل لـ **Service**



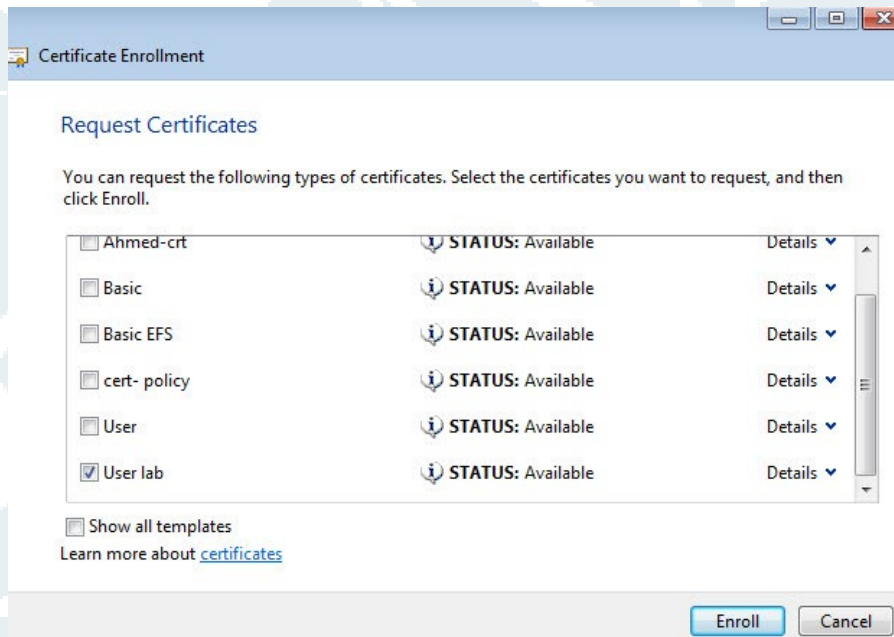


ستلاحظ أنها أصبحت Valid وإذا حدث أي Error نقوم بإعادة تشغيلها مرة أخرى

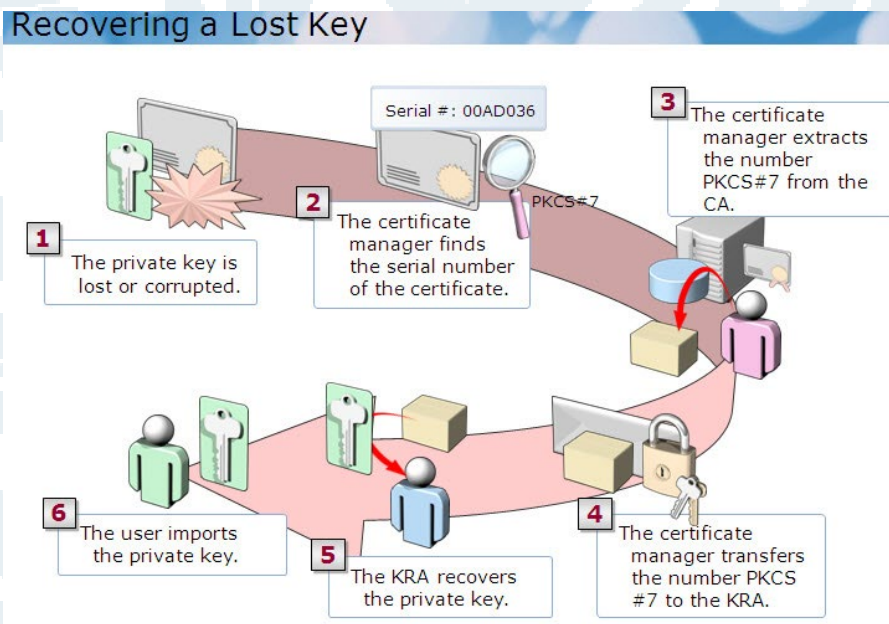
- على جهاز الـ Win-7 نقوم بالدخول بأي حساب مستخدم آخر  
 نقوم بفتح MMC Start → Run → MMC  
 File → Add\Remove Snap-in  
 R.click on Personal → All Tasks → Request New Cert



ونختار الـ Cert الخاصه بالـ User التي تم نسخها من قبل



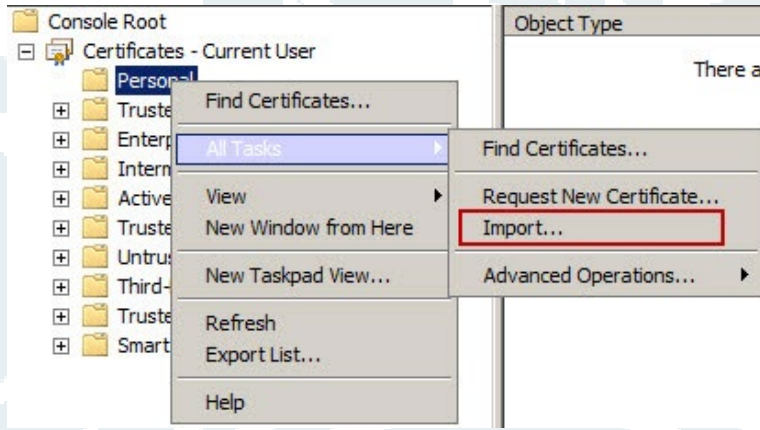
Enroll → Next → Finish



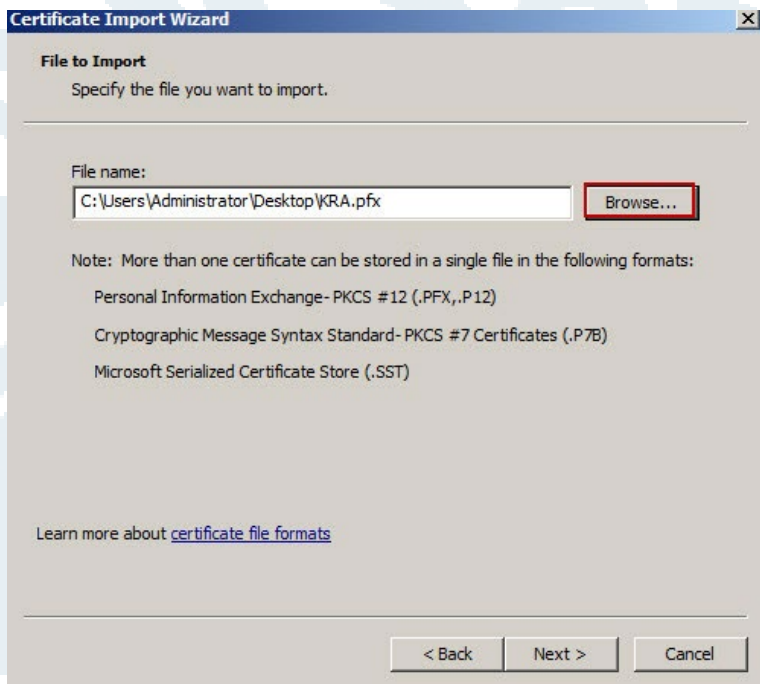
• ولكن ماذا يحدث إذا تم فقد هذه الـ Cert ???

نقوم بالدخول بحساب الـ KRA على الـ Machine الخاصة بالـ CA أي السيرفر الذي يلعب هذه الخدمة ولكن في هذه الحالة سنلاحظ أنه تم انشاء Profile جديد خاص به لذا يتوجب علينا أن نقوم بإضافة الـ KRA Cert الخاصة به مرة أخرى

نقوم بفتح الـ CA ونضغط على Personal ومنها  
All Tasks → Import

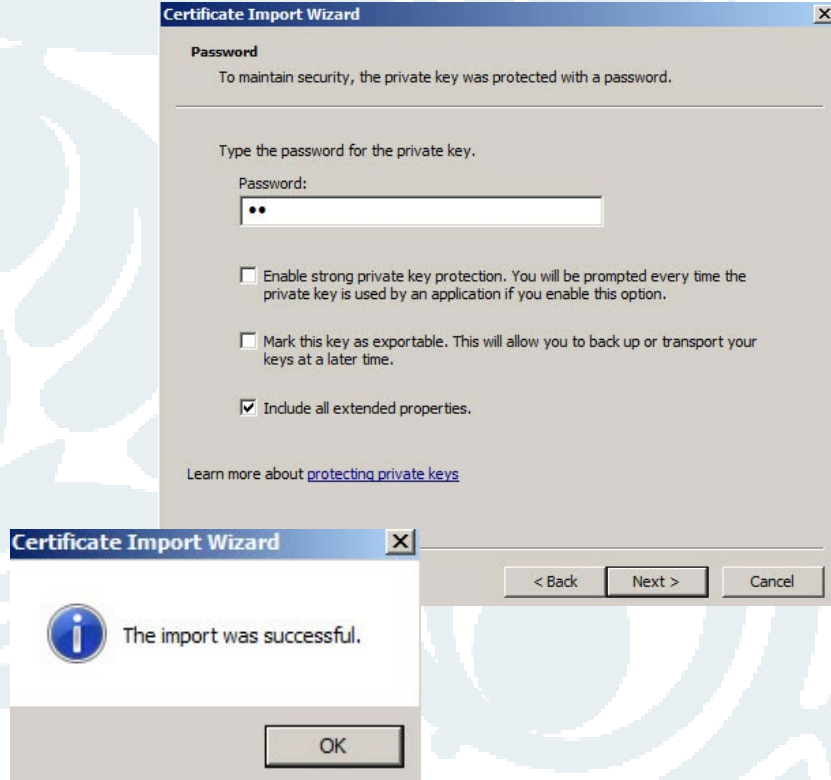


نقوم بإضافة الـ Cert التي تم نسخها من قبل في الإعدادات الأولية في بداية حديثنا

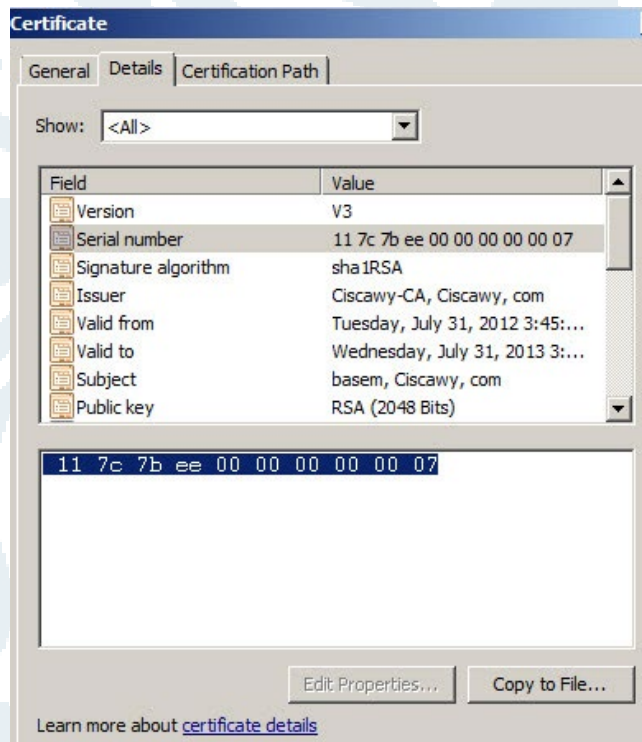
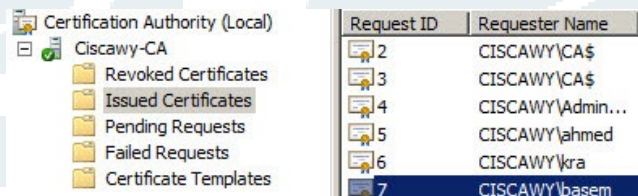




## يسال عن كلمة المرور التي تم وضعها لهذه الـ Cert



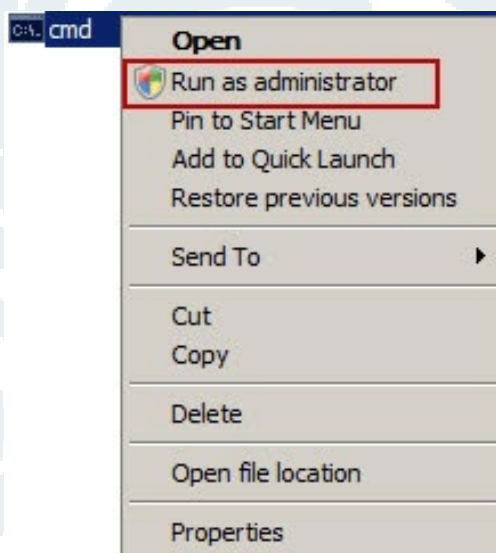
نقوم بالضغط D.click على الـ Cert التي تم فقدها من قبل الـ User وسنجدها في الـ Issued



نختار ومنها Serial Number وDetails

ونقوم بنسخه Ctrl+C حتى نستخدمه في عملية الـ Recovery لأننا حينما قمنا بعمل Import لهذه الـ Cert قمنا بنسخ الـ Private Key الخاص بها النقطة التي نوهت لأهميتها .

• نقوم بفتح الـ Run ونضغط عليها  
R.Click → Run as Administrator



نقوم بكتابة

Certutil -getkey "Serial Numer For Cert that Copied" file name

Certutil -getkey

بعد ذلك في " " يتم وضع الرقم الخاص بهذه الـ Cert  
ويتم وضع اسم لهذه الـ Cert

```
C:\Windows>certutil -getkey "11 7c 7b ee 00 00 00 00 00 07" basem
Querying CA.Ciscawy.com\Ciscawy CA.....
"CA.Ciscawy.com\Ciscawy-CA"
Serial Number: 117c7bee00000000000007
Subject: CN=basem, DC=Ciscawy, DC=com
UPN:basem@Ciscawy.com
NotBefore: 7/31/2012 3:45 PM
NotAfter: 7/31/2013 3:45 PM
Template: Userlab, User lab
Version: 3
Cert Hash(sha1): 45 9a 4c 80 06 91 b6 5d 92 62 66 b9 6c 76 f0 1d 64 50 0f bd

Recipient Info[0]:
MSG_KEY_TRANS_RECIPIENT(1)
CERT_ID_ISSUER_SERIAL_NUMBER(1)
Serial Number: 115df1b100000000000006
Issuer: CN=Ciscawy-CA, DC=Ciscawy, DC=com
Subject: CN=kra, DC=Ciscawy, DC=com
CertUtil: -GetKey command completed successfully.
```

ثم نقوم بكتابة هذا الأمر

```
C:\Windows>certutil -recoverkey basem basem.pfx
```

## Certutil –recoverkey

نضيف الاسم السابق

بعد ذلك نضيف الاسم pfx. الامتداد الخاص بالـ Cert  
سيطلب أن نقوم بإعطائه كلمة مرور جديدة

```
Enter new password:  
Confirm new password:  
CertUtil: -RecoverKey command completed successfully.
```

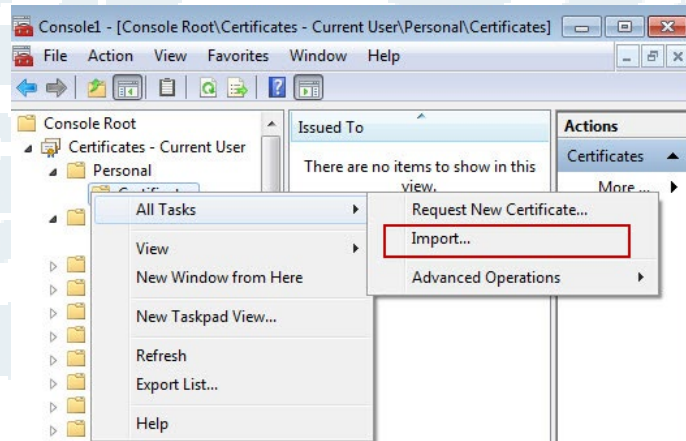
سيتم حفظها على الـ C:\  
نقوم بوضعها في Shared Folder

• بعد الانتهاء من هذه الخطوات  
نقوم بالدخول على حساب الـ Win-7 على حسابات الـ User الذي فقد الـ Cert الخاصة به  
نقوم بفتح مسار الـ Shared Folder ونقوم بنسخ الـ Cert على سطح المكتب

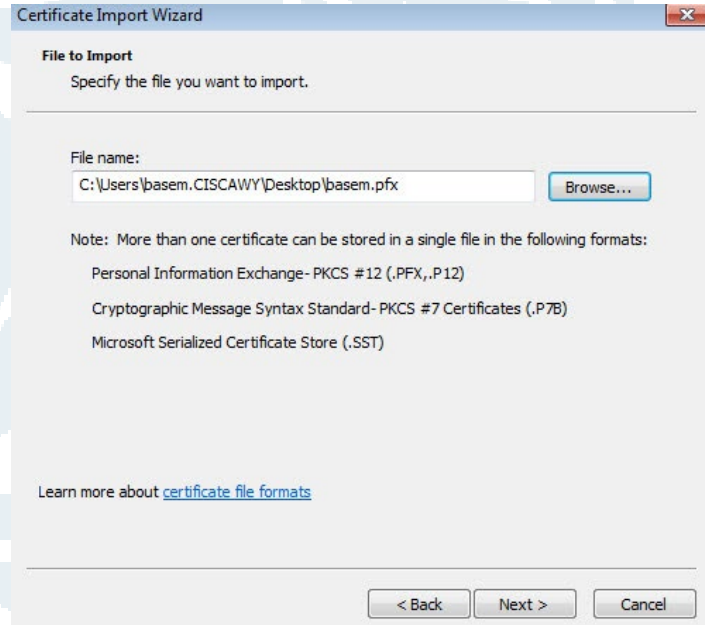
نقوم بفتح MMC

File → Add\Remove Snap-in

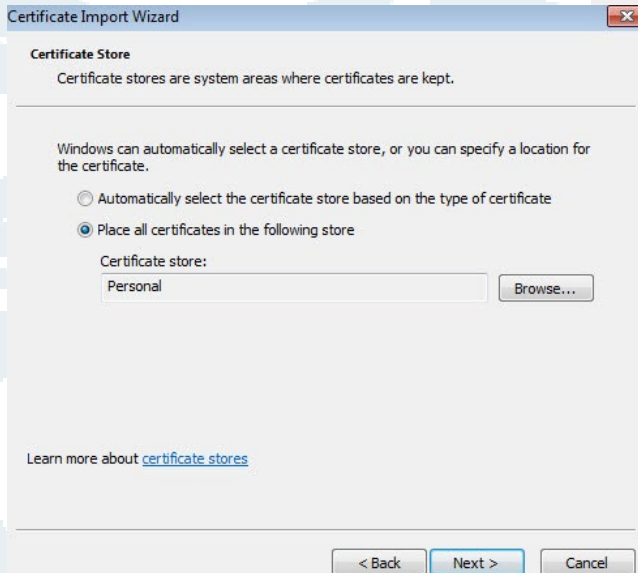
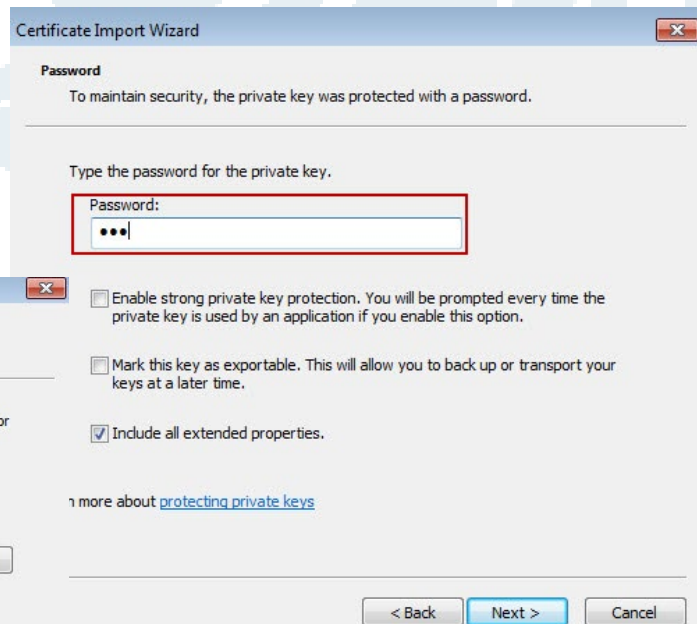
R.click on Personal → All Tasks → Import







## نقوم بوضع كلمة المرور الجديدة

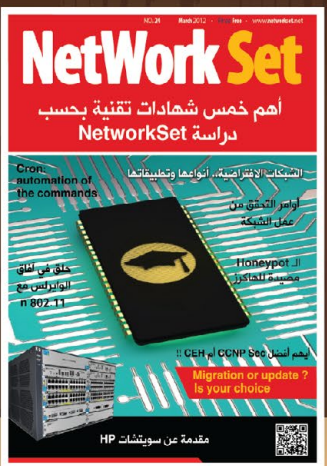
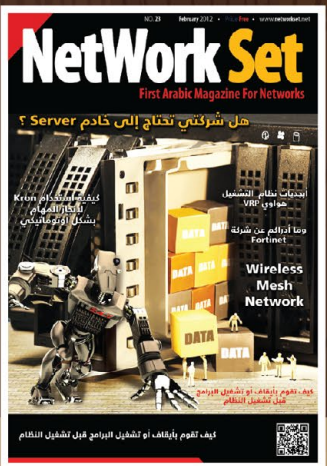
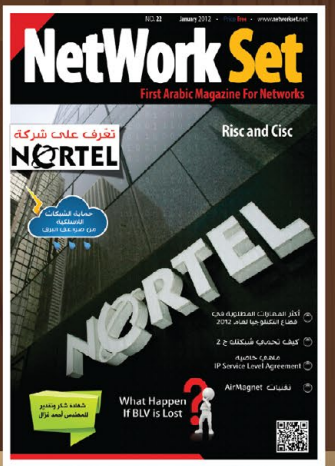
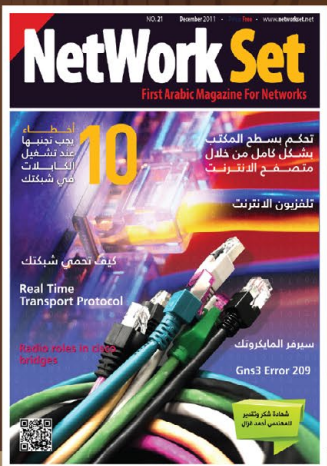
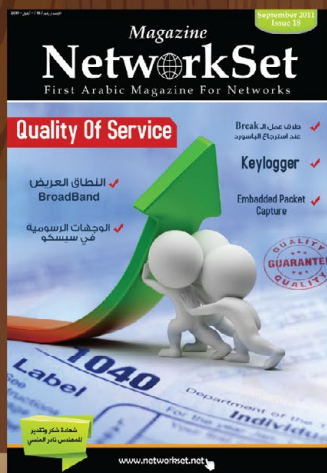


Next → Next → Finish

سنجد أنه تم إضافتها بنجاح للمستخدم ويمكنه استخدامها كما كان يفعل من قبل  
وسنلاحظ أنه نفس الـ SN الخاص بها

وبذلك نكون قد انتهينا من عملية الـ Recovery بنجاح

# Network Set Magazine Gallery





# مقالات العدد

**NetWork Set** Magazine



# Shadow Copy windows server 2012



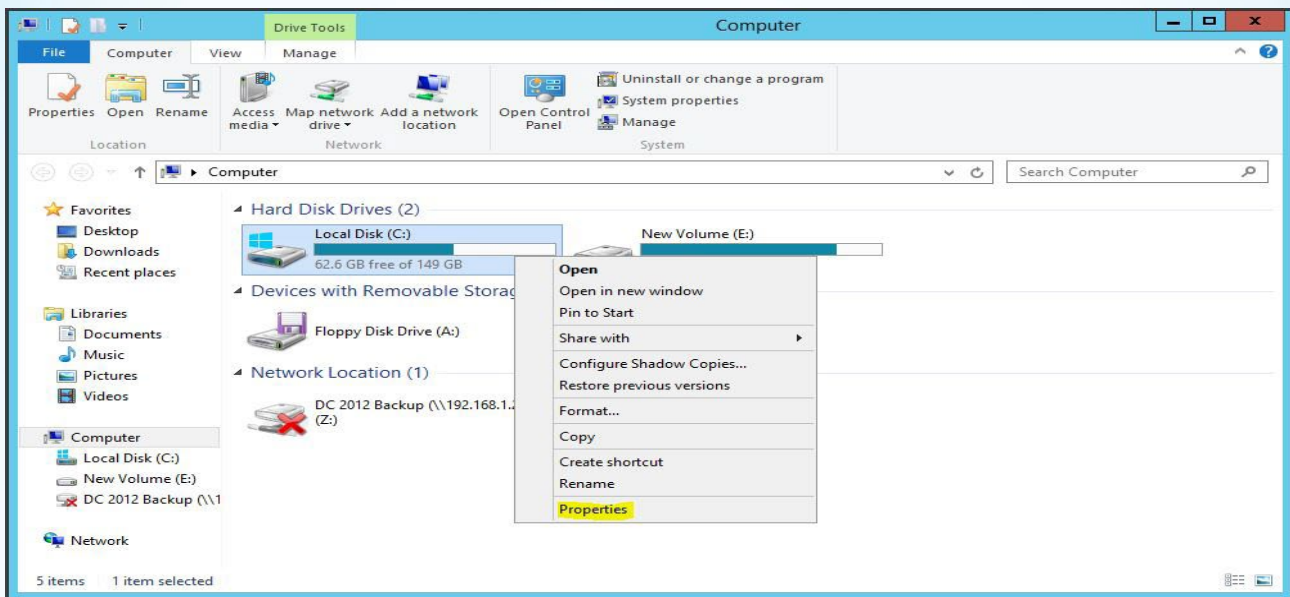
الخدمة التي أبقت مدراء الشبكات في مناصبهم وفي نفس الوقت الخدمة التي أقالت مدراء الشبكات من مناصبهم هذا ما شاهدته في السنوات السابقة من العمل في مجال الشبكات.

لقد تعمدت وضع العنوان مع الويندوز سيرفر لجلب اهتمام مدراء الشبكات Shadow Copy و previous versions server 2003، Xp ولكن بإمكاننا استعمالها بجميع إصدارات ويندوز من ما بعد الويندوز.

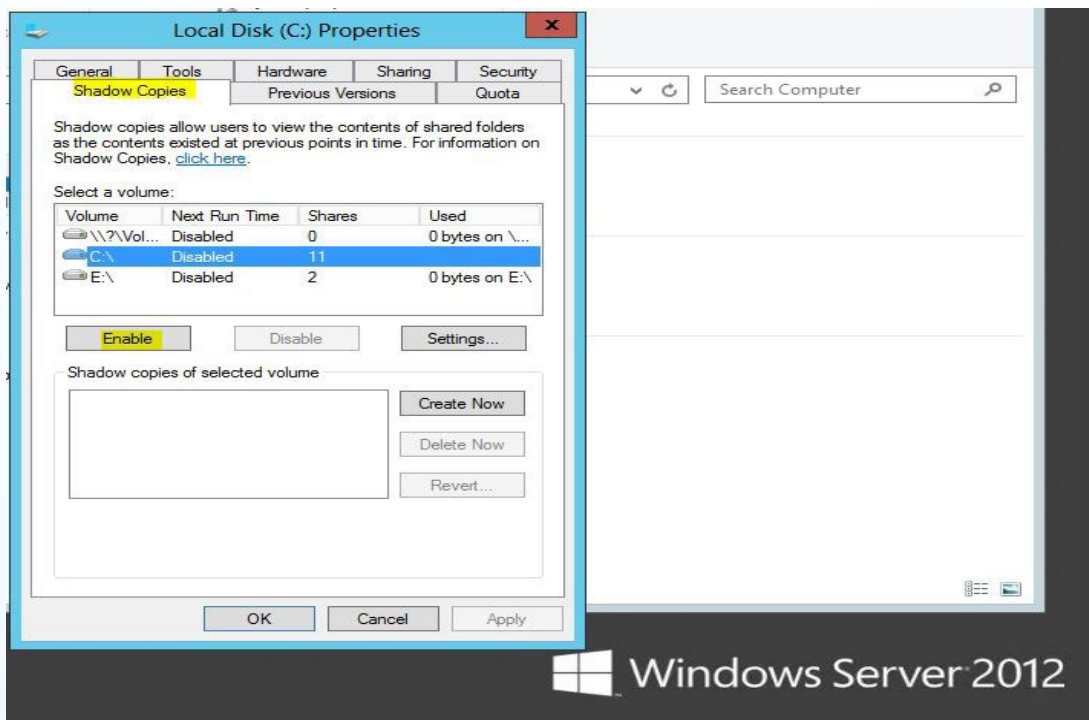
لنفترض التالي : جميعنا نملك ملفات على الشبكة خاصة بالموظفين، والسيناريو التالي أن الموظفين يعملون على ملف تم تعديله وبعد فترة يتم تعديله مرة أخرى ثم اكتشف أن التعديل الجديد خطأ ويريد العودة إلى التعديل الأول ومسح التعديلات الجديدة ولنفترض لم يكن لديك نسخة احتياطية بهذا الوقت من التعديل فما العمل ؟

والتي تعمل على إنشاء نسخ وهمية من ملفاتك ومجلداتك أو عدة نسخ منها بحيث يكون الحل : وهو تفعيل خاصية Previous versions .

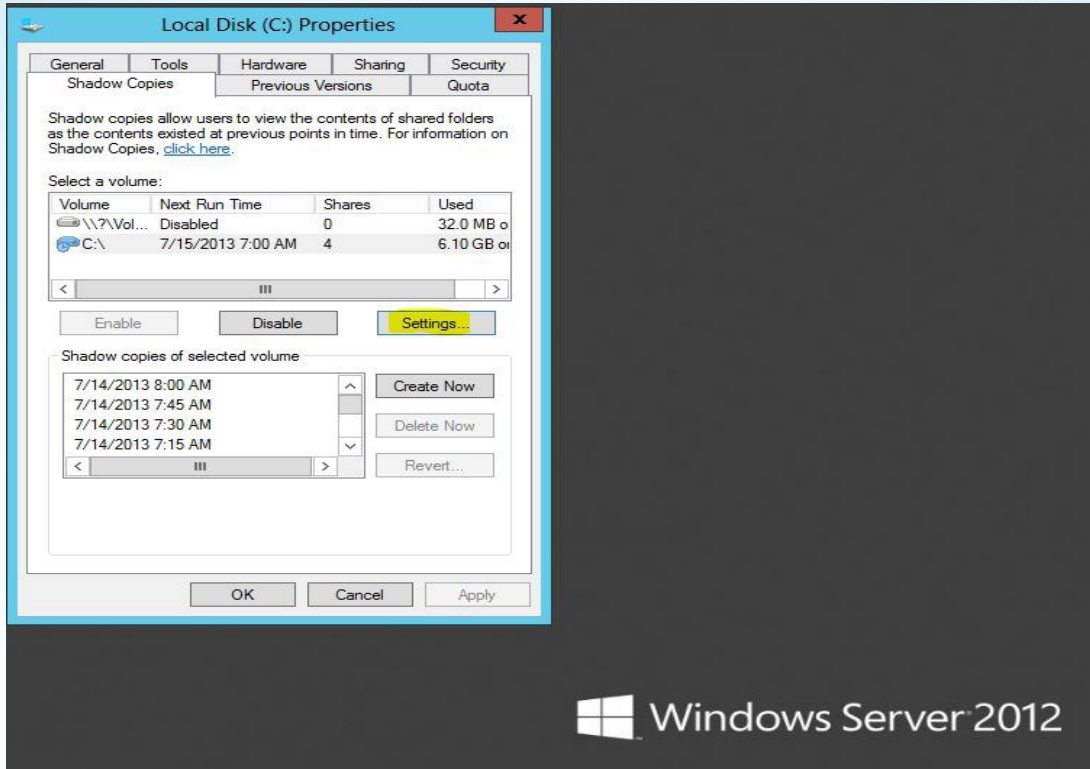
لديك عدة نسخ سابقة من هذا الملف وبإمكانك استرجاع الملف إلى أي حالة تريدها مع مراعاة حفظ الوقت التي تم التعديل به ليتم استرجاعها. يتم تفعيل هذه الخاصية على مستوى القرص كامل وبالحالة الافتراضية تكون الخاصية مفعلة بشكل أوتوماتيكي على القرص C لذلك سوف نقوم بتفعيلها على قرص آخر باستخدام الويندوز سيرفر 2012.



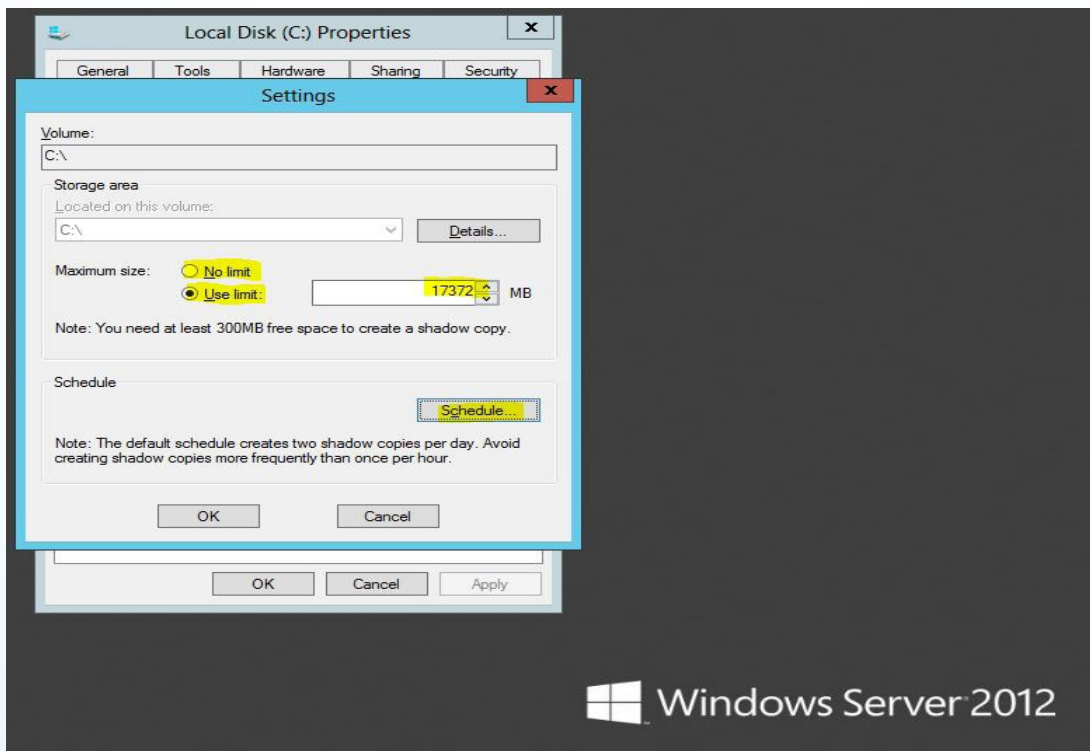
نلاحظ يجب علينا اختيار القرص الذي نريد تفعيل الخاصية به بالضغط على Enable.



من أجل إلغاء التفعيل بعد التفعيل نلاحظ تغير شكل القرص الذي حددناه وللتأكد من تفعيلها بظهور زر الـ Disable لتعديل بعض الإعدادات ثم نضغط على Settings

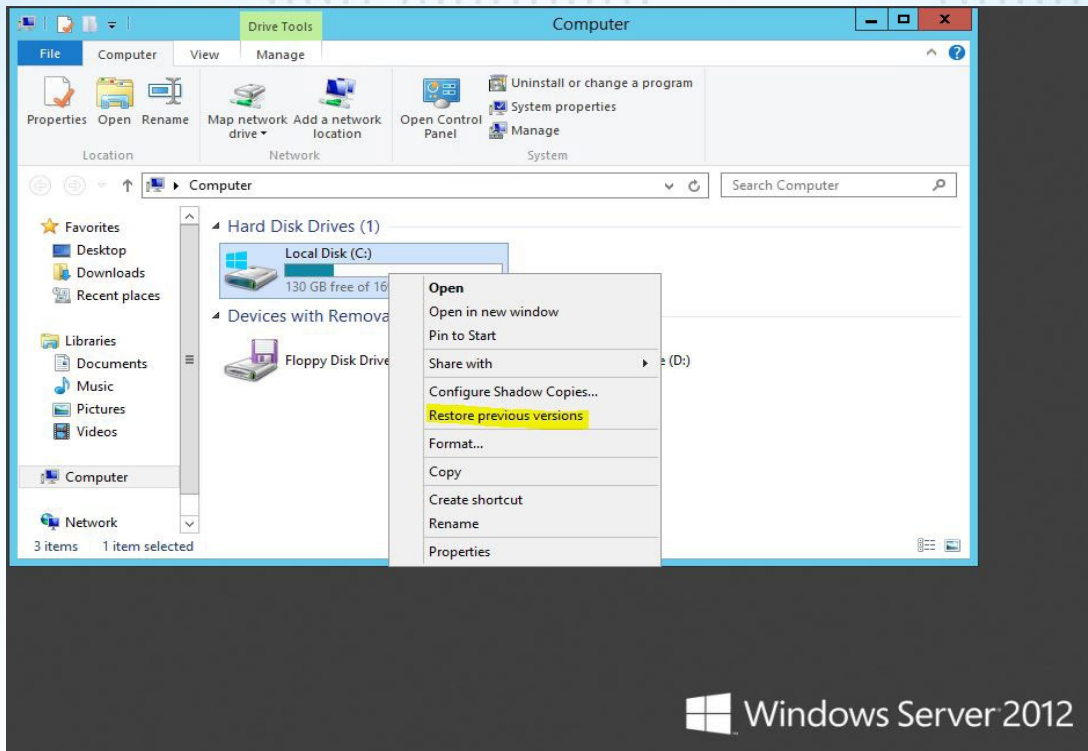


في صفحة الإعدادات التالية نلاحظ وجود مكان لوضع الحجم المراد تخزين نسخ وهمية من الملفات الموجودة بالقرص وهنا نستطيع التحكم بها على ما نملك من مساحات أو بإمكانك وضعها غير محدودة لاختيار أيام محددة لعمل هذه الخاصية ويمكننا أيضا بالضغط على زر **Schedule**.



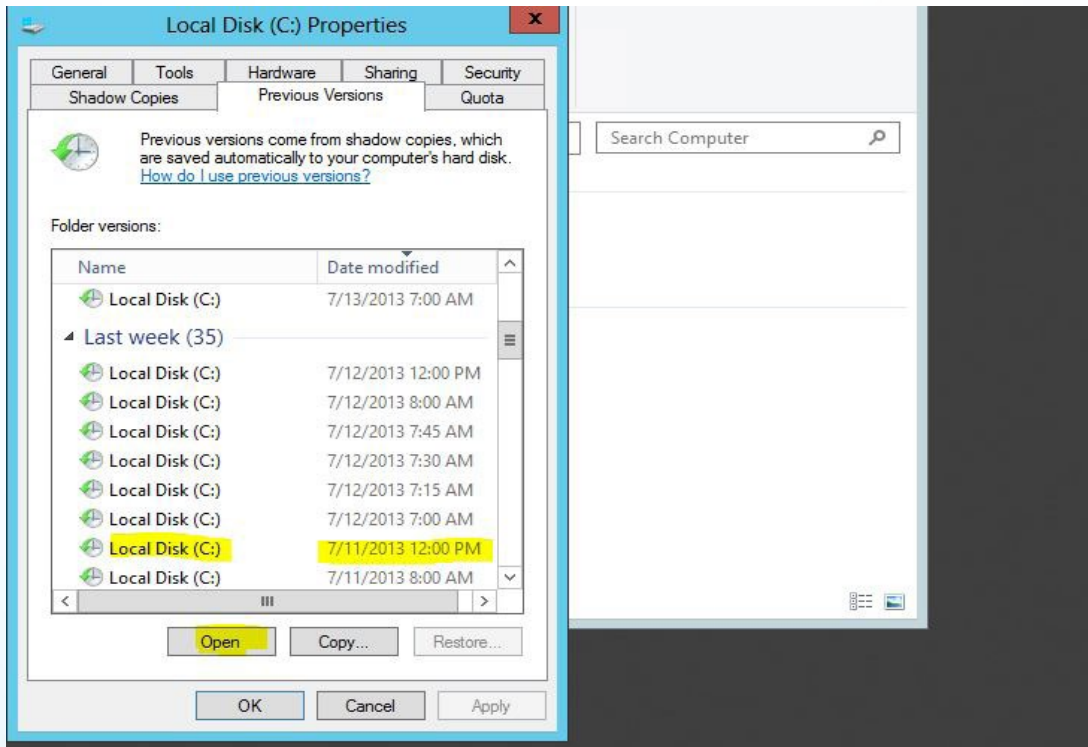
الآن انتهينا من تفعيل الخاصية ووضع الإعدادات اللازمة وكل شيء على مايرام ، وهنا الموظفون يستعملون ملفات الشبكة والأمور كلها بخير .  
فجأة حدث خطأ في ملف من الملفات في قسم المحاسبة مثلا أو غيره وطلب منك أن تعود بتاريخ 3 أيام سابقة ، فورا وبسرعة وبساطة نفعل التالي :





Windows Server 2012

في الصورة التالية نحدد التاريخ التي طلب منا أن نسترجع به الداتا ثم نضغط Open



بهذه الحالة تم الاسترجاع بنجاح وحل مشاكل كثيرة في هذا المجال ، وهنا اصبح احتمال ضياع شيء من الداتا أقل مما كان عليه .



# Windows Intune

سوف نتعرف معاً على منتج جديد من منتجات Microsoft Online في مجال إدارة الشبكات لكن هذا المنتج يختلف عن كل منتجات الإدارة عند مايكروسوفت لأنه يعمل من خلال تكنولوجيا الـ Cloud computing تحديداً بنظام الـ SaaS.

سوفت نقسم مقالنا الى عدة نقاط:

- أولاً : ما هو الـ Windows Intune.
- ثانياً: كيفية عملة وخدماته.
- ثالثاً: كيفيك الاشتراك فيه والعمل عليه.
- رابعاً: تقييمنا له.

## أولاً: ما هو الـ Windows Intune:

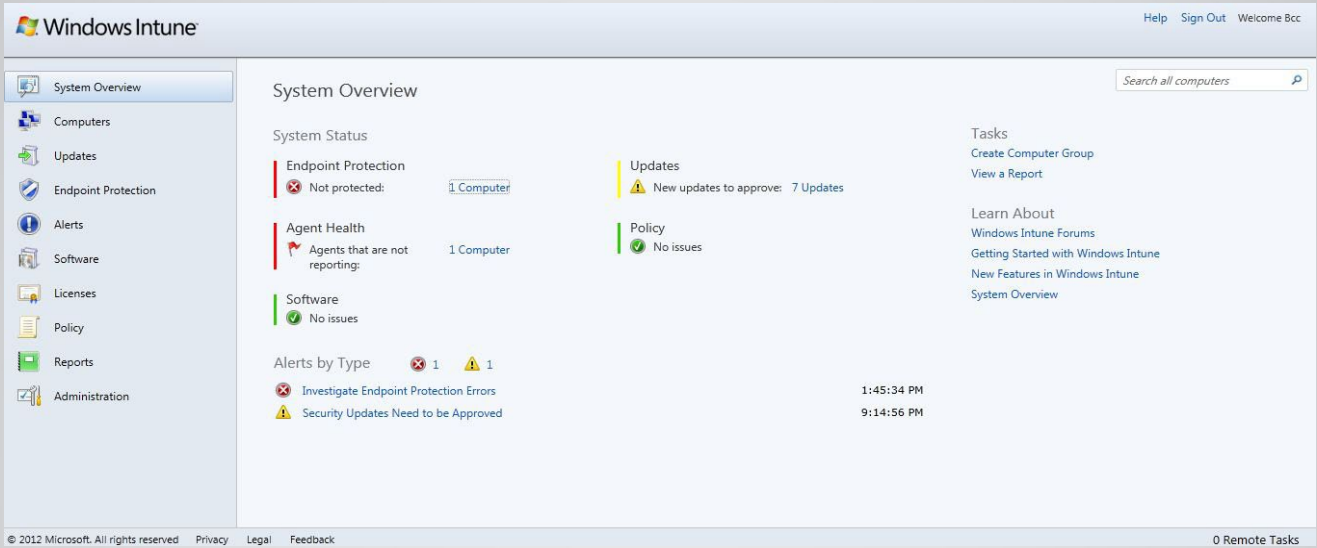
قد يعتقد البعض من الوهلة الأولى ومن خلال اسم المنتج أنه عبارة عن نظام تشغيل خاص بميكروسوفت أو ما شابه وذلك من اسمه. لكن هذا التطبيق يختلف عن هذا الاعتقاد تماماً جاءت كلمة Windows للاسم لسبب ان وظيفته هي إدارة أنظمة تشغيل windows فقط.

إذن ما هو هذا البرنامج : هو عبارة عن برنامج إدارة System Management لإدارة أنظمة تشغيل الويندوز من عدة نواح وهي التعرف على Hardware & Software الموجود على الاجهزة وعمل تحديث للويندوز ومراقبة السيكيورتي على الأجهزة عن طريق برامج malware وعمل تقارير عن حالة الأجهزة وغيرها.

لكن كل هذا بدون احتياجنا أن نقوم بتنزيل هذا التطبيق أو إعداده على سيرفرات داخل الداتا سنتر وإنما يعمل من خلال الداتا سنتر الخاصة بميكروسوفت وسوف نوضح كيف ذلك في الجزئية التالية.

## ثانياً: كيفية عمله وخدماته:

الخدمات التي يقدمها windows intune



يقوم هذا البرنامج بعدة أدوار مساعدة لكل مدير شبكة ومهندس نظم

1 - يقوم بعمل Inventory Hardware and Software لكل الاجهزة الموجودة في الشبكة ومتصلة بهذا البرنامج بغض النظر عن مكانها، المهم أن يكون بينها وبين التطبيق انترنت ويكون عليها الـ windows Intune Agent  
Same (SCCM)

2 - عمل Auto Deploy Software وهي عمل إعداد لبرنامج معين على الاجهزة الموجودة في الشبكة من خلال السيرفر بأسلوب الـ Push Software  
Same (SCCM)

3 - عمل Update Windows والبرامج الموجودة على الجهاز.  
Same (WSUS)

4 - الحماية عن طريق تنزيل برنامج Malware يعمل على اجهزة اليوزر ويتم ادارته وتحديثه عن طريق السيرفر  
Same (Forefront)

5 - عمل بوليسي على الأجهزة اليوزر

6 - الحصول على تقارير كاملة بعدد اجهزة اليوزر وموديلاتها بكم المعلومات عن الهاردوير الموجود فيها والبرامج التي تعمل عليها  
Same (SCCM)

7 - عمل Alert عن المشاكل الموجودة على الاجهزة وارسالها لمسئولي الشبكة  
Same (SCOM)



هذه الأدوار التي يقوم بها الـ Windows Intune لكن مع ملاحظة أن كل هذه يتم من خلال تطبيق واحد وتتم إدارته من صفحة الويب بدون ما الاحتياج أن يكون عندنا سيرفرات تقوم بكل هذه الأدوار من مراقبة وحماية وتحديث وغيرها وهذه مثال ناجح وتفاعلي لتطبيقات الـ Cloud SaaS.

البعض يمكن أن يقول أنه يمكنني أن أقوم بكل هذه الأدوات عن طريق برامج أخرى وتحديدًا برامج :

**System Center Configuration manager**  
**System Center operation Manager**  
**Forefront for malware**  
**WSUS**

هذا كلام صحيح بواسطة هذه البرامج يمكننا ان نقوم بنفس الأعمال التي تقوم بها خدمة الـ Windows Intune لكن مع ملاحظة الفرق الشاسع في التكاليف في Hardware and software التي تحتاجها السيرفرات للعمل وصيانتها وغيرها ولمن سبق لهم التعامل مع هذه البرامج سوف يفهم ما مقدار التعب والمجهود الذي سوف يقابله للقيام بنفس الخدمة التي يقدمها الـ windows intune.

ونقطة أخرى أن هذا النظام يدار بشكل تام من صفحة ويب بسيطة ويتم ربطه على أي جهاز له اتصال بالانترنت وليس شرطاً أن يكون بداخل الشبكة الخاصة بنا.

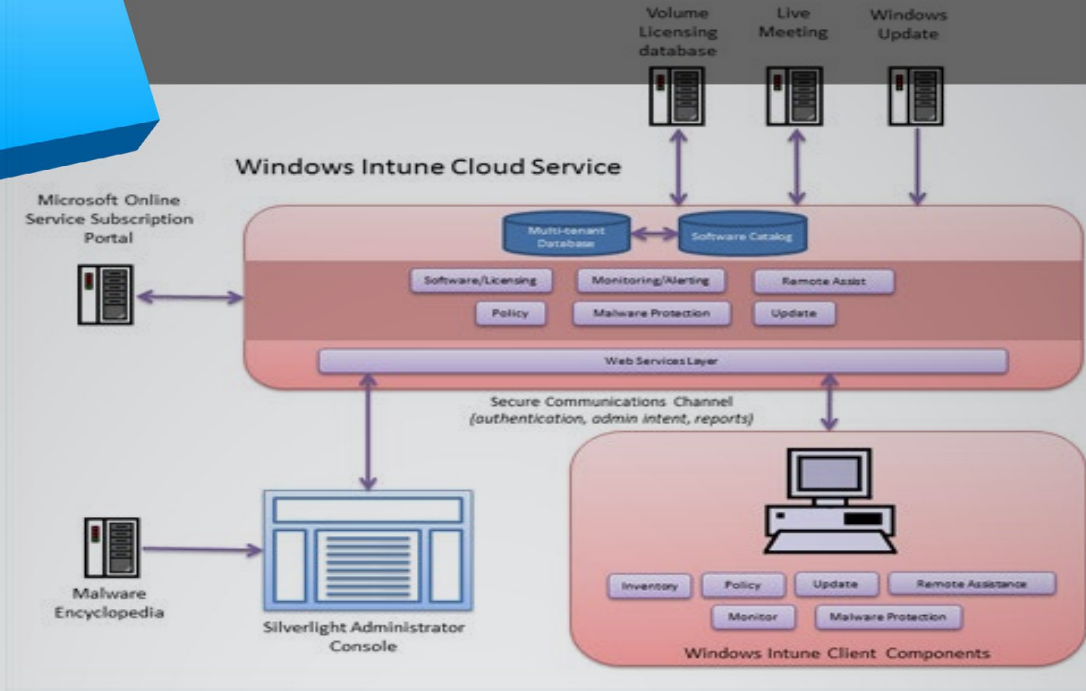
الصيانة والسيرفرات التحديث وغيرها تدار داخل الداتا سنتر الخاصة بميكروسوفت فلن نحتاج أي جهد في الصيانة أو النسخ الاحتياطي أو غيرها.

وهذا رابط لفيديو يعمل مقارنة بين استخدام windows intune وعدم استخدامه ويوضح فوائد هذا النظام:

<http://www.youtube.com/watch?v=bzzjrlGxYKM>

## فكرة عمل خدمة Windows Intune

فكرة العمل ببساطة لهذا التطبيق هي أهم مميزاتة وهي أن مايكروسوفت قامت ببناء كل هذه الخدمات على سيرفرات لديها وتتيح لك من خلال web interface أن تدير من خلاله الأجهزة التي لديك لن تحتاج سوى الاشتراك في هذه الخدمة وهذا سوف نوضحه لاحقاً بالإضافة أن القيام بأعداد الـ windows intune agent الذي سوف يربط بين أجهزة اليوزر داخل شركتك وبين حسابك في windows intune.



### ثالثاً: كيفية الاشتراك في ال Windows intune:

ميكروسوفت تتيح هذه الخدمة بمقابل مالي شهري على حسب عدد الأجهزة التي تديرها. لكن يمكنك أن تقوم بتجربة هذه الخدمة لمدة تجريبية 30 يوم ولكنها غير متاحة لمنطقتنا لذلك يجب عند القيام بالتسجيل في هذه الخدمة أن يكون الايميل الخاصة بك موضوع فيه أن منطقتك هي الولايات المتحدة وليس أي دولة عربية. البعض يمكن ان يعتبرها تحايل . هذا صحيح لكن هذا مقابل شيء أسوأ وهو سياسة التفریق العنصرية في توزيع الخدمات عند الشركات الكبرى

<http://www.microsoft.com/en-us/windows/windowsintune/pc-management.aspx>

بعد قيامك بالاشتراك في الخدمة سوف يكون لك حساب ويمكنك فتح حسابك من خلال صفحة الويب وتبدأ إدارة الحساب بتنزيل ال windows intune Agent على الأجهزة التي لديك.

### رابعاً: تقييمنا لهذه الخدمة:

الخدمة حتى الآن جيدة جداً وعملية وبسيطة ويجب أن يكون لديك داتا سنتر ضخمة وبها العشرات من البرامج والسيرفرات لإدارة ومراقبة وتحديث الأجهزة التي في الشبكة لديك. البعض يرى أن مشكلتها هي مقابلها المادي الشهري، لكن لو نظرت بنظرة أعم أنك لو حسبت تكلفة نفس هذه الخدمات على أرض الواقع سوف تجد أنك سوف تحتاج إلى مبالغ ضخمة hardware server and software والانترنت والصيانة الدورية والموظفين الذين سوف يديرونها.

لذلك برأيي أنه حل أمثل لمن يريد أن يدير الشبكة بأقل التكاليف وبشكل بسيط، وفي المستقبل القريب سوف تقل تكلفة هذه الخدمة نتيجة التنافس بين الشركات التي سوف تدخل هذا المجال .

هذه اول تطبيقات مشاريع Microsoft online ان شاء الله في المقابل سوف نتعرف على تطبيقات أخرى من تطبيقات Microsoft online مثل :

Office 365

Live meeting

Windows azure

# NetWork Set

First Arabic Magazine For Networks



ضع اعلانك معنا

وكن شريكنا في النجاح  
و مواكبة التطور مع أول  
مجلة عربية متخصصة

انتشار واسع - تغطية شاملة

حزم إعلانية مختلفة تناسب جميع الاحتياجات

بإمكانكم مراسلتنا على البريد الإلكتروني

[magazine@networkset.net](mailto:magazine@networkset.net)



# الاستضافة في الـ Datacenters وأنواعها



يكثُر الحديث هذه الأيام عن الـ cloud systems ، وعن ترشيده مصادر تكنولوجيا المعلومات والتوفير في استخدامها في الوقت التي أصبحت تكنولوجيا المعلومات هي أساس كل المجتمعات المتحضرة والبنية الأساسية التي تعتمد عليها.

في وقت مضى كان مزودوا خدمات الاستضافة هم ذاتهم مزودوا خدمات الانترنت، إلى الوقت الذي نشأت شركات ضخمة لتعمل في هذا المجال بشكل خاص و مستقل، فما هي الاستضافة وما هي أنواعها:  
لنبدأ بأخذ مثال بسيط عن برنامج محاسبة لشركة ما، حيث يخدم هذا البرنامج الموظفين الذين يعملون في قسم المحاسبة لإنجاز الأعمال المحاسبية للشركة.

من البديهي أن نقوم باستضافة هذا البرنامج على أحد سيرفرات الشركة الموجود في الـ Datacenter و تقديم كافة الخدمات لتجعله متصل بالشبكة بشكل دائم و مستقر، وهذه الخدمات على سبيل المثال (كهرباء، الوصل على الشبكة، إعطاء IP ، حمايته من الاختراق، تحديثات مستمرة . . .)، وهذا ما يدلنا على وجود فريق متخصص بتكنولوجيا المعلومات لإدارة جميع هذه الخدمات.



و لكن ما هو الحل المناسب في حال عدم وجود فريق متخصص في تكنولوجيا المعلومات؟ من المسؤول عن إدارة جميع هذه الخدمات و من الذي يضمن استمرار عمل هذا السيرفر بشكل مستمر و مستقر؟  
من هذه الحاجة وجدت خدمات الاستضافة الخارجية، و التي تمكنك من وضع هذا السيرفر في مكان خارج شركتك و القدرة على الوصول إليه وكأنه بالغرفة

المجاورة لك مع وجود فريق لإدارة جميع خدماته آنفة الذكر على مدار الساعة. بعد هذه المقدمة البسيطة يمكننا تعريف الاستضافة بأنها خدمة تقدمها شركات متخصصة لاستضافة موارد تكنولوجيا المعلومات على أنواعها ليتم الولوج إليها عن بعد.

## أنواعها:

### 1) Shared hosting:

في هذا النوع تتم الاستضافة عن طريق منح المستضيف جزءاً من سيرفر موجود مسبقاً في مركز البيانات ليتم رفع ما يشاء من معلومات عليه (موقع إلكتروني، برامج، ملفات . . .) حيث أن هذا السيرفر يكون مقسم بطريقة خاصة ليستضيف عدد معين من الحسابات عليه و الذين يتشاركون بموارد هذا السيرفر و بخط الانترنت الواصل إليه و الذي سوف يتم الولوج عن طريقه إلى السيرفر كل بحسب حسابه المنشأ له ليتم تحميل ما يرغب على القسم المخصص له.

ومما تجدر الإشارة إلى أن هناك العديد من الطرق للوصول إلى السيرفر عن بعد، إما عن طريق real IP من خلال شبكة الانترنت أو عن طريق DynDNS أو عن طريق الشبكة الداخلية في البلد (عن طريق مؤسسات الاتصالات) دون الحاجة إلى الولوج إلى الانترنت.

### 2) Dedicated hosting:

ويقصد في هذا النوع من الاستضافة، أنه في حال كان المستضيف يتطلب موارد كبيرة لتشغيل برامجه أو أن عدد كبير من المستخدمين سوف يقومون بالولوج إلى هذه البرامج على مستوى الثانية الواحدة.

هذا يعني أن هناك حمل كبير سوف يقع على السيرفر و على خط الانترنت الواصل بالسيرفر، و بالتالي يكون الخيار الأفضل في هذه الحالة الـ dedicated hosting لتوفير كل هذه الاحتياجات و هذا يعني تخصيص سيرفر كامل و خط انترنت لكل عميل يطلب هذا النوع من الاستضافة لتعمل برامجه بالشكل الأفضل مع امكانية زيادة سرعة خط الانترنت الواصل لهذا السيرفر.

في هذا النوع مركز البيانات هو من يقدم السيرفر للعميل و يكون بمثابة تأجير خلال فترة الاستضافة.

### 3) Co-location hosting :

من يحتاج هذا النوع هم العملاء الذين يمتلكون السيرفر و كل البرامج، ولكن يريدون وضعها في مكان آمن و مخدم على مدار الـ 24 ساعة بالطاقة الكهربائية و التبريد مع وجود فريق تقني مشرف على هذا السيرفر في حالات التوقف المفاجئ ليقوموا بإصلاحه مباشرة.

في هذه الحالة يكون الخيار الصحيح هو الـ Co-location hosting وهو استضافة سيرفر العميل في مركز البيانات كما هو دون أي تدخل.

في هذا النوع العميل هو من يقدم السيرفر لمركز البيانات لوضعه و امداده بكل وسائل الطاقة و الانترنت و الأمن والحماية.



# How to Use Hyper-V 2012 Replica

الكل يعلم أن Hyper-V التي تأتي مع Windows Server 2012 هي الإصدار الثالث من التقنيات الافتراضية المقدمة من ميكروسوفت MS Hyper-V 3.0 ولكن هناك سؤال دائماً ما يدور في عقولنا ألا وهو ماهي المميزات الجديدة التي تأتي مع المنتج؟ وهنا نحن نتحدث عن MS Hyper-V 3.0 حقيقة هناك الكثير من المميزات ولكن الميزة الأكثر حماساً هي Hyper-V replica. فهي ميزة مهمة جداً للتعافي من الكوارث DR وهي مناسبة للشركات الصغيرة إلى المتوسطة. في هذا المقال سوف اشرح مايمكن أن تتوقعه من هذه الميزة الجديدة.

وأحد من الأشياء التي قد لاحظتها من إعلان ميكروسوفت على هذه الميزة Hyper-V replica هناك الكثير من المفاهيم الخاطئة حول Hyper-V replica وماذا تفعل؟ وما إلى ذلك أريد أن ابدأ فيها في محاولة لتوضيح اللبس:

وأحد من المشاكل الكبيرة في server virtualization هو أن تتعطل، ممكن أن يؤدي الى نقص كبير في أداء مراكز البيانات Datacenter، فإن أعباء العمل التي كانت على ذلك السيرفر و توقفت عن العمل ستكون مصدر ازعاج ولكن على الأرجح لن تكون هناك كارثة كبرى.

الطريقة الوحيدة لمنع هذا النوع من المشاكل من الحدوث هو استخدام clustering للعمل مع بعضها البعض لتوفير الاستمرارية في العمل فإن فشل أحد السيرفرات أو أصيب في مشكلة تقنية ما يمكن لسيرفر آخر من ضمن cluster تجاوز الفشل وبهذه الطريقة يمكن أن نتجاوز الفشل. وبالنسبة لأحد السيرفرات Failover clustering هو أمر ضروري للحفاظ على أداء السيرفرات والاستمرار في تقديم الخدمات، قامت ميكروسوفت منذ الإصدار الأول لك Hyper-V من استخدام ميزة failover clustering مع ويندوز سيرفر 2008 Failover clustering مايزال متواجد على ويندوز سيرفر 2012 ولكن تطورت بشكل ملحوظ منذ أول تجسيد لها منذ عدة سنوات وقد أشرت أن failover clustering تعززت بشكل ملحوظ في Hyper-V 3.0 ولكن من الأمور الجميلة في Hyper-V 3.0 أنك لا تحتاج إلى استخدام تخزين مشترك وهذا الأمر يقلل كثيراً من التكلفة مما يضعه في متناول الشركات والمنظمات الأصغر حجماً.

وأيضاً أحد التحسينات الكبرى الأخرى التي قدمتها ميكروسوفت clustering أن تحتوي على 63 سيرفر ولم يعد شرطاً استخدام تخزين مشترك. ومن هنا نستطيع أن نفكر ب clustering موزعة جغرافياً وبعبارة أخرى cluster nodes من الممكن أن تتواجد في أماكن بعيدة عن المركز الرئيسي حتى لو تدمر المركز الرئيسي في أحد الكوارث الطبيعية، فمثلاً البيانات متواجد في مكان آمن ويمكن استرجاعها.

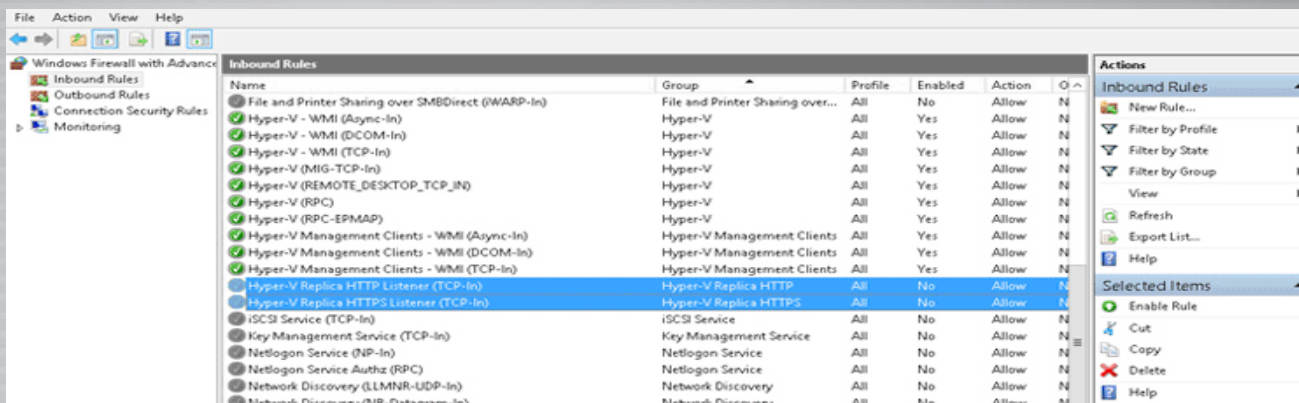
وكما ذكرت سابقاً أن أحد الأسباب لاستخدام Hyper-V replica هي في حالة فشل أحد الملقمات Servers عن العمل يمكن أن تبقى قيد التشغيل ولكن القيام بذلك يتطلب التدخل اليدوي فهي إلى الآن ليست تلقائية. إذن ماذا نحتاج لنبدأ :

ملاحظة : المسافة الجغرافية لاتهم





## قم بتفعيل الخدمات التالية من Windows Firewall

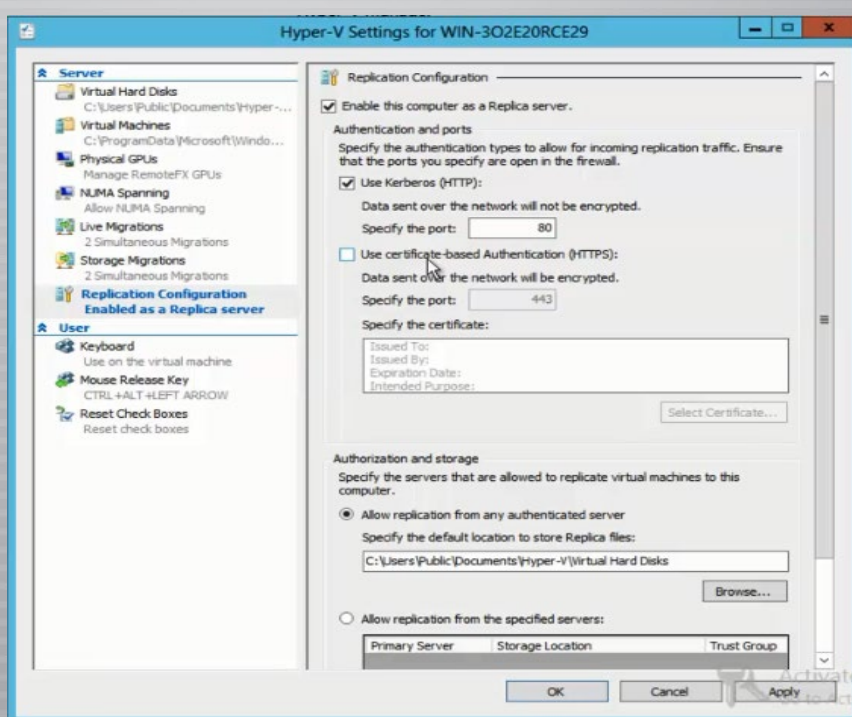


## طريقة إعداد Hyper-V Replication

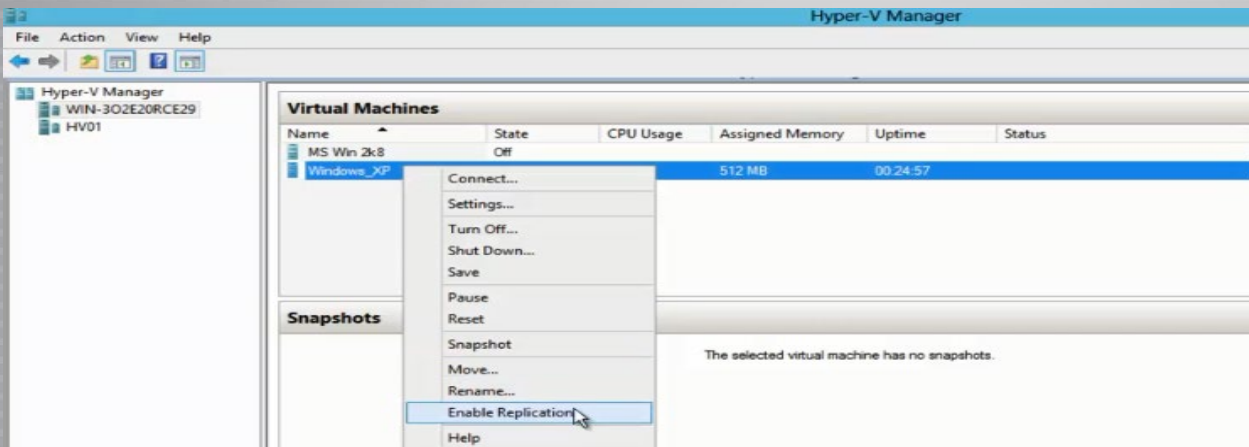
في عمل الـ replication، Hyper-V يكون أحد Hyper-V Host عبارة عن SOURCE والأخر عبارة عن Destination. بمعنى آخر أن الـ Destination Hyper-V Host ماهو إلا عبارة عن مستودع للـ VMs التي تريد تطبيق خاصية replication عليها نبدأ مع الخطوات التالية:

1 - أن نظرنا إلى الشكل، ما عليك القيام به لتمكين خاصية replication أولاً هو تحديد خانة الاختيار وبذلك سوف تسمح للـ Server بتلقي النسخ من المضيفين Hyper-V Hosts (يجب تحديد الخيار على كل Hyper-V Host)

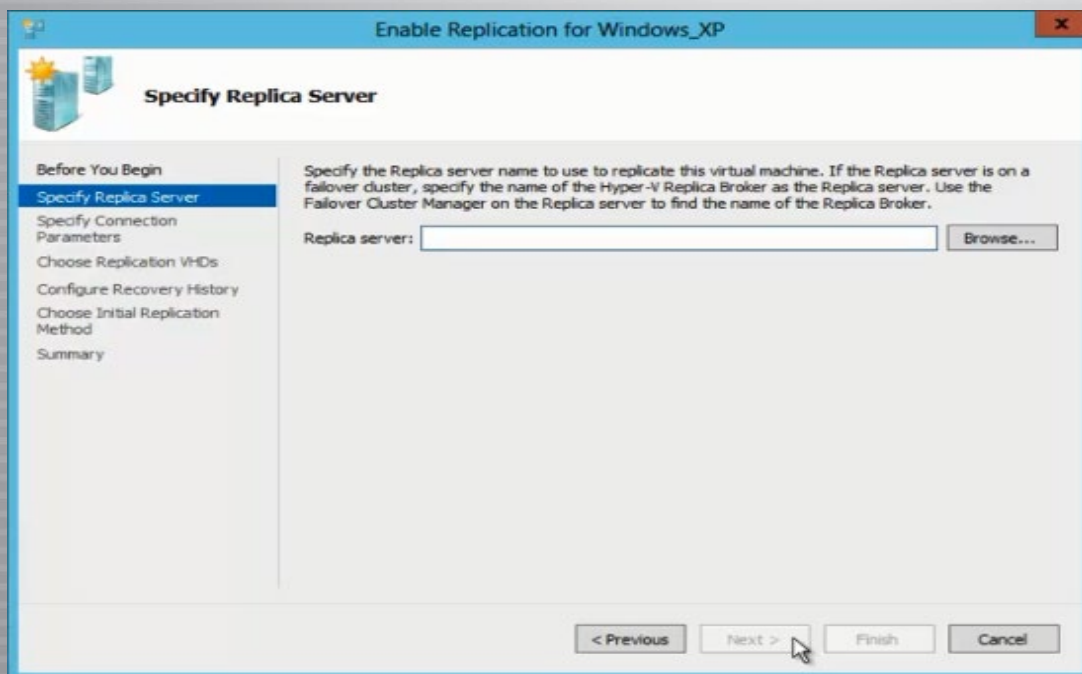
الخطوة التالية في هذه العملية تحديد بروتocol المصادقة، ميكروسوفت تمنحك خيارين مختلفين وهما الـ Kerberos عبر HTTP، أو يمكنك استخدام مصادقة مستندة إلى شهادة عبر HTTPS ويمكن استخدامهما معاً.



2 - الآن بعد أن قمنا وبتمكين خاصية الـ Replication وتحديد نوع المصادقية كما ذكرنا سابقاً قم بالنقر في الزر الأيمن على الـ VM التي تريد أن تقوم بعمل Replication لها كما هو مبين:



3 - بعد هذه النقطة سيقوم بتشغيل المعالج ويجب أن تختار التالي لتتخطى رسالة الترحيب.



وبعدها هناك العديد من الخيارات المهمة مثل تحديد اسم Destination Replication Server

Enable Replication for Windows\_XP

### Specify Replica Server

Before You Begin

Specify Replica Server

Specify Connection Parameters

Specify the Replica server name to use to replicate this virtual machine. If the Replica server is on a failover cluster, specify the name of the Hyper-V Replica Broker as the Replica server. Use the Failover Cluster Manager on the Replica server to find the name of the Replica Broker.

Replica server: HV01

Browse...

وتم قم بنقر التالي وسوف يطلب منك تحديد نوع المصادقة الذي تريد استخدامه في إطار عملية النسخ المتماثل. المصادقية التي تختارها يجب أن تطابق نوع المصادقية التي اخترتها في الأول على كل Hyper-V Hosts تحتوي هذه الشاشة أيضاً على خانة الاختيار التي يمكنك من استخدام ضغط البيانات أثناء إرسالها عبر الشبكة.

Enable Replication for Windows\_XP

### Specify Connection Parameters

Before You Begin

Specify Replica Server

Specify Connection Parameters

Choose Replication VHDs

Configure Recovery History

Choose Initial Replication Method

Summary

Replica server: HV01.hyperv.local

Replica server port: 80

Authentication Type

Use Kerberos authentication (HTTP)  
Data will not be encrypted while being transmitted over the network.

Use certificate-based authentication (HTTPS)  
Data will be encrypted while being transmitted over the network.

Issued To:  
Issued By:  
Expiration Date:  
Intended Purpose:

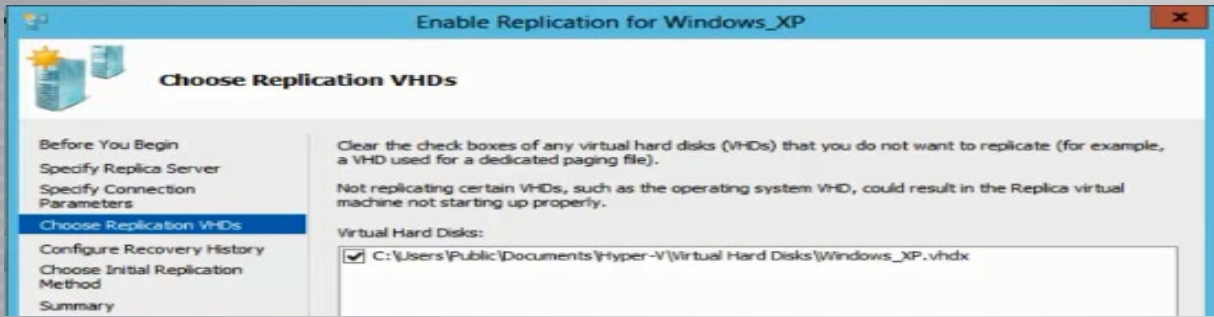
Select Certificate...

Compress the data that is transmitted over the network.

< Previous Next > Finish Cancel

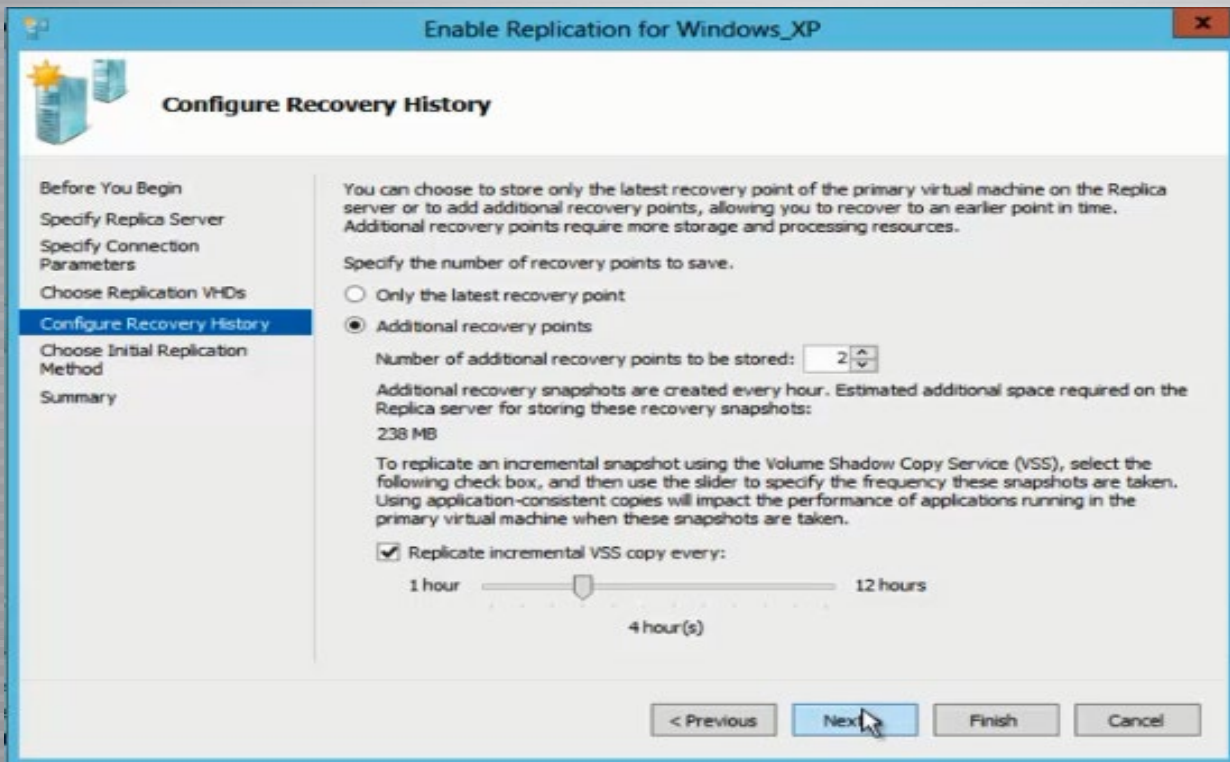


الشاشة التالية سوف يطالبك لتحديد الأقراص الذي تريد أن يعمل لها Replication. في معظم الحالات، وسوف تحتاج لتكرار كافة الأقراص الثابتة.

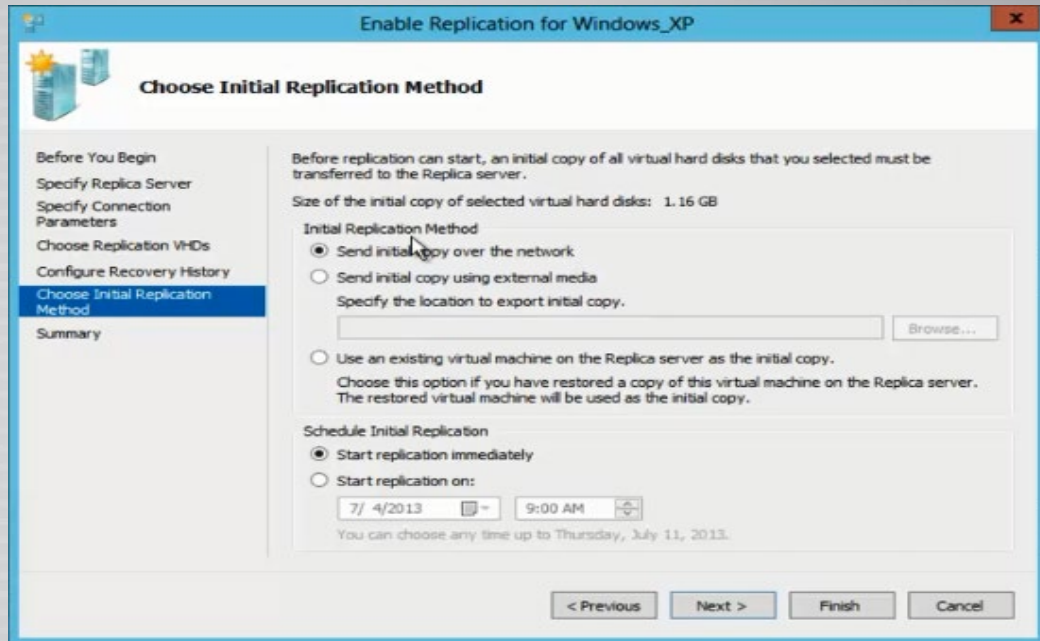


أنقر فوق التالي، وسوف يطلب منك تحديد عدد نقاط الاسترداد الذي تريد تخزينها على الجهاز. استخدام نقاط الاسترداد يمنحك القدرة على نسخة طبق الاصل العودة إلى نقطة سابقة في الوقت المناسب.

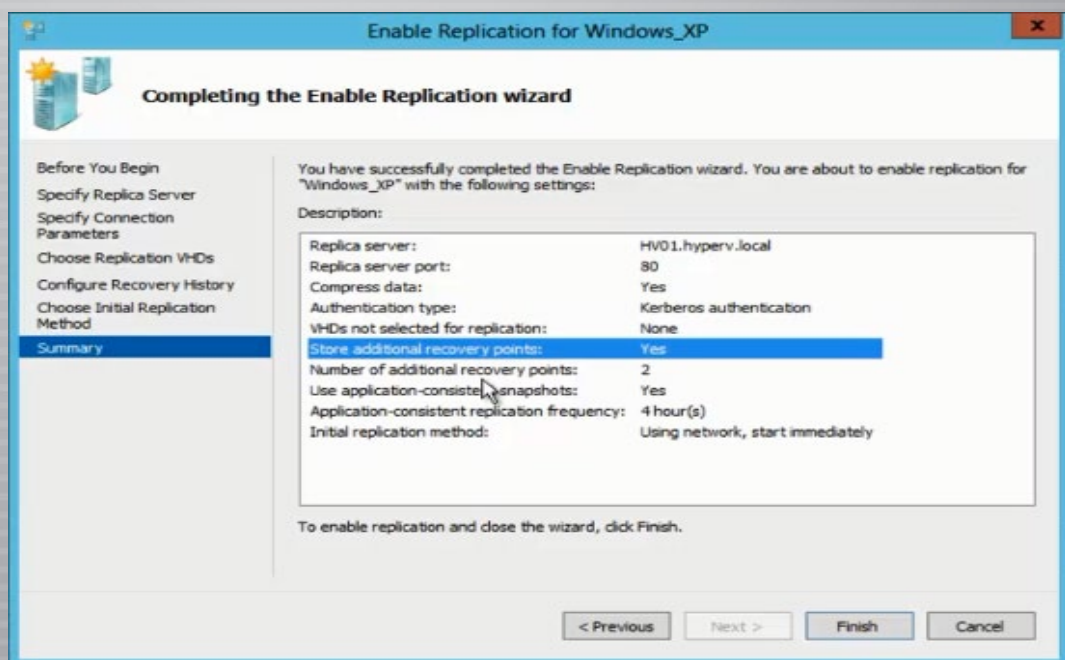
ملاحظة: كلما زاد عدد النقاط احتجت إلى مساحة أكبر.



وأخيراً، تتم مطالبتك لتحديد الطريقة التي ترغب بها في عملية النسخ المتماثل للبدء. في معظم الحالات سوف يحدث النسخ المتماثل عبر الشبكة والبدء فوراً.



أنقر فوق التالي، وسوف تشاهد شاشة تفصل خيارات التكوين التي قمت باختيارها وهي عبارة عن ملخص سريع لما قمت به:



وبعدھا ستلاحظ أن نسخة من تلك الـ VMs حصل لها نسخ من 01 Hyper-v host إلى Hyper-V .host02

Virtual Machines					
Name	State	CPU Usage	Assigned Memory	Uptime	Status
MS Win 2k8	Off				
Windows_XP	Running	1 %	512 MB	00:31:33	Sending Initial Replica (22%)

## Verifying Replication Health

The screenshot shows the Hyper-V Manager interface. The 'Virtual Machines' table lists 'Windows\_XP' as 'Running' with 46% CPU usage and 512 MB of memory. Below the table, the 'Snapshots' section is empty. The 'Replication' section for 'Windows\_XP' shows the following details:

- Replication Type: Primary
- Replication State: Replication enabled
- Replication Health: Normal (indicated by a green dot)
- Current Primary Server: hv01.hyperv.local
- Current Replica Server: WIN-302E20RCE29.hyperv.local
- Last synchronized at: 7/4/2013 7:57:57 AM

The 'Replication' tab is selected at the bottom, and the 'Replication Health' status is highlighted with a red circle labeled '2'. The 'Replication' tab itself is also highlighted with a red circle labeled '1'.

## Tips

### ماهي SAM database ؟

SAM database هي Security Accounts Manager database تستخدم من قبل ويندوز (وربما بعض انظمة التشغيل الاخرى) هي التي تدير حسابات المستخدمين وغيرها من الأمور. ومرتبطة في registry اثناء اقلع النظام . يتم تشفير المفتاح في اتجاة واحد one-way hash مما يجعل من الصعب كسرها. متواجدة في المسار التالي: c:\windows\system32\config\sam وتوجد العديد من الحيل لفتح قاعدة البيانات والحصول على معلوماتها منها LC5 يستخدم برنامج لكشف أسماء المستخدمين والباسورد او هناك العديد من البرامج المرفقة على اسطوانة hires boot cd



# كيف تحدد آخر نظام تشغيل خاص قامت سيسكو بإصداره.



عندما نرغب بتحديث نظام التشغيل الخاص بسيسكو فنحن دائماً نحاول إيجاد آخر نظام تشغيل قامت سيسكو بإصداره بحيث نكون على يقين تام بأن النظام الذي نرفعه هو الأفضل أداءً والأقل خطراً من ناحية الثغرات الأمنية، في السابق كنت أحاول تغيير الأرقام التي تكتب في نظام التشغيل والتي تعرف عادة رقم الإصدار والتي شرحت كل معانيها في تدوينة قديمة على المدونة على الرابط التالي، وكنت أرفع الرقم في كل مرة حتى أصل إلى أعلى رقم موجود على الإنترنت وأقوم بتحميلها ورفعها على الجهاز.

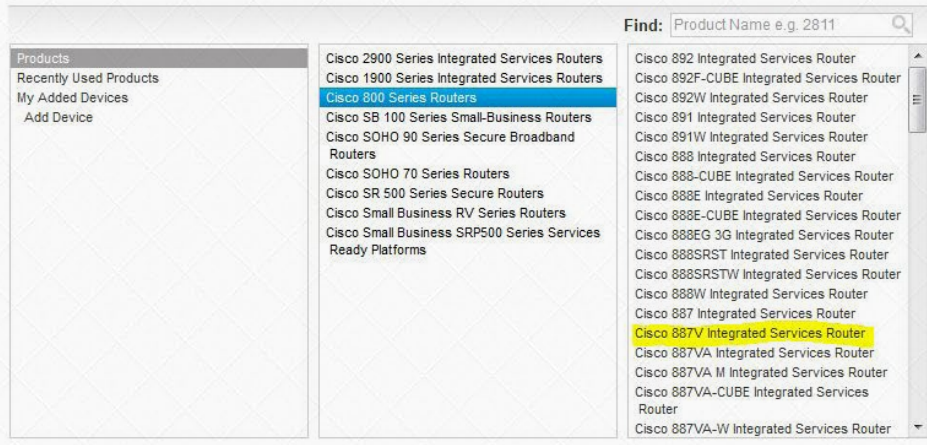
هذه الطريقة أنقرضت تماماً بعدما وجدت صفحة على موقع سيسكو توضح لي آخر التحديثات الخاصة بكل أنظمة التشغيل الخاصة بكل جهاز على حدى وأياً كان الجهاز راوتر، سويتش، فايبرول، أكسس بوينت.... إلخ.  
توجه أولاً إلى الرابط التالي لنرى الصورة التالية:

Downloads Home > Products



في الصفحة السابقة تستطيع أن ترى معي لائحة بكل شيء يخص أجهزة سيسكو اختار ماذا تريد بالضبط وتابع حتى تصل للشيء الذي تريده بالضبط، سوف أبحث عن روتر سيسكو 887 كما هو موضح بالصورة التالية.

Downloads Home > Products > Routers > Small Business Routers > Cisco 800 Series Routers



نضغط على اللينك لنرى صفحة جديدة تحوي عدة خيارات لن نتحدث عنهم الآن وسوف نتركها لموضوع آخر، سوف نختار أنظمة IOS كما هو موضح.

## Download Software


[Downloads Home](#) > [Products](#) > [Routers](#) > [Small Business Routers](#) > [Cisco 800 Series Routers](#) > [Cisco 887V](#)

### Select a Software Type:

- [IOS ROMMON Software](#)
- [IOS Software](#)
- [License Manager Software](#)
- [Very High Bitrate DSL \(VDSL\) Firmware](#)

في الخطوة القادمة سوف نرى كل الإصدارات الموجودة والخاصة بهذا الراوتر كما هو موضح بالصورة التالية:

#### Cisco 887V Integrated Services Router

Search...  [Release Notes for 15.3\(2\)T](#)



[Expand All](#) | [Collapse All](#)

▼ Latest Releases

- 15.3.2T(ED)**
- 15.2.4M3(ED)
- 15.2.3T3(ED)
- 15.1.4M6(MD)
- 15.1.3T4(ED)
- 15.0.1-XA2(ED)
- 15.0.1M10(MD)
- 12.4.24T8(ED)
- 12.4.22-YB8(ED)

▼ All Releases

- ▼ 15.3
  - ▶ 15.3T
- ▼ 15.2
  - ▶ 15.2T
  - ▶ 15.2M
- ▼ 15.1
  - ▶ 15.1T
  - ▶ 15.1M
- ▼ 15.0

File Information	Release Date	DRAM/Flash	
<b>UNIVERSAL</b>  c800-universalk9-mz.SPA.153-2.T.bin	29-MAR-2013	512 / 256	<a href="#">Download</a> <a href="#">Add to cart</a>
<b>UNIVERSAL - NO PAYLOAD ENCRYPTION</b>  c800-universalk9_npe-mz.SPA.153-2.T.bin	29-MAR-2013	512 / 256	<a href="#">Download</a> <a href="#">Add to cart</a>

بهذه الطريقة نكون قد وصلنا إلى الإصدار الأخير الذي قامت سيسكو بإطلاقه والذي سوف نبحت عنه، ولكي تعرف ماهي الإضافات التي تمت إضافتها أو التعديل عليها على كل نسخة موجودة، ضع الماوس على اسم النظام وسوف تخرج نافذة صغيرة فيها بعض المعلومات حول النظام وفي الأسفل سوف تجد رابط يطلعك على كل التحديثات كما هو موضح.



## Cisco 887V Integrated Services Router

Search...

Expand All | Collapse All

Latest Releases

- 15.3.2T(ED)
- 15.2.4M3(ED)
- 15.2.3T3(ED)
- 15.1.4M6(MD)
- 15.1.3T4(ED)
- 15.0.1-XA2(ED)
- 15.0.1M10(MD)
- 12.4.24T8(ED)
- 12.4.22-YB8(ED)

All Releases

- 15.3
  - 15.3T
- 15.2
  - 15.2T
  - 15.2M
- 15.1
  - 15.1T
  - 15.1M
- 15.0
  - 15.0XA
  - 15.0M

### Release 15.3.2T ED

File Information	Release Date
<b>UNIVERSAL</b>	29-MAR-2013
c800-universalk9-mz.SPA.153-2.T.bin	
<b>UNIVERSAL - NO PAYLOAD ENCRYPTION</b>	29-MAR-2013
c800-universalk9_npe-mz.SPA.153-2.T.bin	

#### Details

Description: **UNIVERSAL - NO PAYLOAD ENCRYPTION**

Release: **15.3.2T**

Release Date: **29/Mar/2013**

File Name: **c800-universalk9\_npe-mz.SPA.153-2.T.bin**

Min Memory: **DRAM 512 MB Flash 256 MB**

Size: **50.86 MB (53331476 bytes)**

MD5 Checksum: **11af563c151fc1a350b4151b1df6ae43**

[Release Notes for 15.3\(2\)T](#) | [Security Advisory](#) | [Field Notices](#)

**Tips**

## لاتربط حساباتك كلها معاً؟؟؟

نعلم كلنا ان العديد من الخدمات والمواقع توفر ميزة تسجيل الدخول بواسطة مواقع اجتماعية كبرى، Facebook، Twitter، Google، Yahoo، او غيرها، لكن ما لا نعيه اهتمام، انه لو تم اختراق حساب واحد من هذه الحسابات كفيس بوك مثلاً، فجميع الحسابات الأخرى ستفقد أيضاً، لأنها مرتبطة بحسابك الأول، فلهذا يفضل لك ان لا تربط جميع حساباتك معاً، والاكتفاء بالتسجيل بكل موقع بمفرده

المهندس : ولاء عصام حسن





# NetWork Set

First Arabic Magazine For Networks



**ضع اعلانك معنا**

وكن شريكنا في النجاح  
و مواكبة التطور مع أول  
مجلة عربية متخصصة

انتشار واسع - تغطية شاملة

**حزم إعلانية مختلفة تناسب جميع الاحتياجات**

بإمكانكم مراسلتنا على البريد الإلكتروني  
[magazine@networkset.net](mailto:magazine@networkset.net)

# Honey pot



يخوض العالم اليوم حرباً عالمية بكافة المقاييس ، نعم ولا داعي أن تستغربوا فالحرب اليوم هي ليست حرب سياسية ولا حرب عسكرية لا طائرات ولا دبابات إنها الحرب الالكترونية ،حرب الاختراقات والفايروسات حرب تدمير المفاعلات النووية والمنظومات الأمنية والعسكرية ، وكمثال على ذلك ما تتعرض له جمهورية إيران من محاولات حثيثة لاختراق أنظمتها النووية مثل فايروس Stuxnet الذي ضرب أنظمتها وأدى إلى توقف آلاف أجهزة الطرد المركزي وأيضاً الهجوم الذي شهده العالم منذ شهر Oplsrail ضد إسرائيل والذي نفذته مجموعة أنونيموس المشهورة حيث استهدفت فيه المواقع الحكومية وأدت إلى تعطلها وشلل كبير في شبكة الانترنت لديها ،كل تلك الهجمات والأخطار التي تشكل تحدٍ صارخ لمستقبل أمن واستقرار شبكات الدول مما دعا إلى تطوير أنظمة كثيرة تختص بالكشف عن الاختراقات IDS وأنظمة مختصة بعمليات الصد IPS حيث ينشغل التقنيون اليوم بالبحث عن أفضل الأنظمة التي تؤمن حماية عالية ضد الاختراقات والهجمات الالكترونية وهذا أشبه ما يكون بالمستحيل ، ستتحدث اليوم عن أحد التقنيات المستخدمة جنباً إلى جنب في أنظمة كشف الاختراقات وصدها حيث تساهم بشكل كبير في تخفيف الأضرار الناتجة عن تلك الهجمات ، إنها بيئة HoneyPot أو ما يسمى ببيئة وعاء العسل وسميت بذلك لأنها تعمل على جذب المخترقين إليها لتنفيذ هجماتهم ضمنها. وبمعنى آخر هي عبارة عن شبكة وهمية تضم تجهيزات وهمية وأنظمة تشغيل وهمية يركب عليها سكريبتات تحاكي الخدمات الحقيقية وقد تحدث المهندس خالد عوض ضمن العدد 24 عن ذلك النظام وشرحه شرحاً وافياً وما سأقوم به اليوم هو بناء تطبيق عملي يحاكي بيئة عمل وهمية يمكن أن نضيفها إلى شبكتنا للحد من الاختراقات وأدعوكم إلى الاطلاع على مقالة المهندس خالد قبل الخوض في عملية إعداد نظام HoneyPot

## الأدوات المستخدمة:

هناك عدد من الحلول التجارية التي تقدمها الشركات مثل

- PatriotBox : سهل الاستخدام وهو من نوع (low-interaction) مخصص لنظام Windows.
- Specter : من نوع (low-interaction) صمم ليعمل على أنظمة Windows أيضاً.



وهناك حلول مجانية مفتوحة المصدر مثل:

•Bubblemum Proxypot

•Bigeye

• Honeyd وهو الذي سنعتمده ضمن التطبيق العملي.

سنقوم بالتطبيق ضمن نظام تشغيل Linux توزيعة Ubuntu 12.04 .

أولاً سنقوم بإضافة الحزمة Honeyd يدوياً من خلال التعليمة :

```
sudo apt-get install honeyd
```

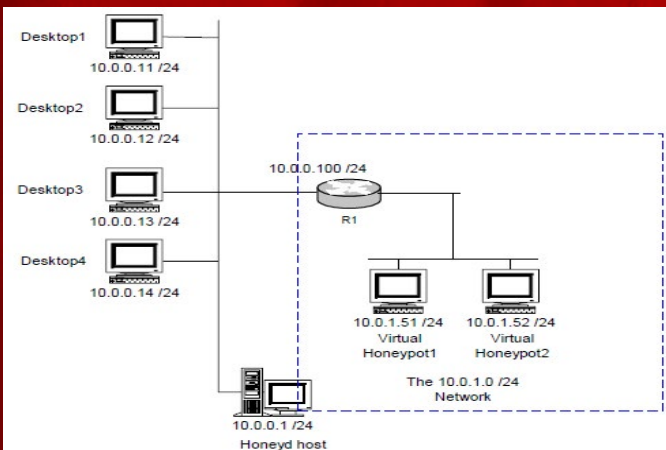
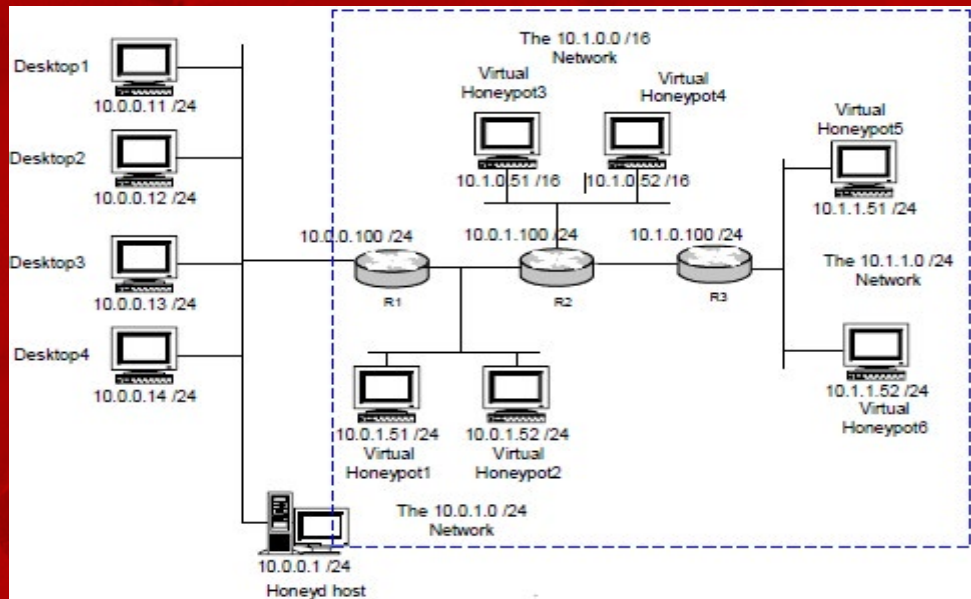
أو تلقائياً من خلال Synaptic Package والبحث عن الحزمة Honeyd .

**ثانياً:**

سنذهب إلى المسار /etc/honeyd/ سنجد هناك عدة ملفات أهمها هو الملف honeyd.conf والذي سنقوم بتوصيف الشبكة الوهمية داخله، والملف nmap.print المسؤول عن إعطاء وتعريف Fingerprint للتجهيزات التي ستوضع ضمن الشبكة بحيث يتم إيهام المخترق بأن الجهاز هو جهاز حقيقي ونظام التشغيل عليها هو نظام حقيقي وليس مزيف.

**ثالثاً:**

سنبدأ الآن ببناء الشبكة الوهمية ، حيث سنتعرف على التعليمات التي يجب وضعها ضمن الملف honeyd.conf لتعريف الشبكة ، حيث سنقوم ببناء الطبولوجيا التالية :



الشبكة السابقة عبارة عن 4 أجهزة Desktop 1,2,3,4 وهي أجهزة ضمن الشبكة الحقيقية أما الجهاز صاحب الـ IP 10.0.0.1/24 فهو الجهاز الذي سنستخدمه لبناء الشبكة الوهمية داخله كما ترون ضمن المخطط ، الشبكة المحاطة بمربع منقطع هي شبكة وهمية موجودة داخل الجهاز المضيف للنظام، سأقوم ببناء قسم قسم حتى لا تختلط علينا الأمور ونستطيع فهم التعليمات تماماً. سأقوم بداية بتنفيذ المخطط التالي:



نلاحظ أن الشبكة الوهمية بسيطة جداً، تحتوي على راوتر مدخل إلى الشبكة وحاسبين فقط والتعليمات التي تعرف هذه الشبكة هي:

```
route entry 10.0.0.100 network 10.0.0.0/16/
```

التعليمة السابقة تعرف الراوتر الذي يمثل مدخل الشبكة وما هو العنوان الذي سندخل عبره أي ال 10.0.0.100 كما هو موضح ضمن الشكل وهذا الموجه هو مدخل إلى الشبكة ذات العنوان 10.0.0.0/16

الآن سنقوم بتعريف نظام التشغيل الذي سيعمل على ذلك الراوتر وتحديد خصائص منافذه وما هي نسخة ال IOS التي ستعمل عليه وتعريفه بالملفات التي ستتولى عملية محاكاة الخدمات اي ملفات السكريبت.

```
create router
set router personality «Cisco IOS 11.3 - 12.0(11)»
set router default tcp action reset
set router default udp action reset
add router tcp port 23 «perl /usr/share/telnet/router-telnet.pl»
set router uid 32767 gid 32767
set router uptime 1327650
```

ومن ثم نقوم بإسناد هذا النظام الذي تم تعريفه إلى الراوتر من خلال التعليمة:

أي أسند النظام الذي عرفناه باسم router إلى الجهاز صاحب العنوان 10.0.0.100 بعد إتمام الضبط السابق لم يبق لإنهاء أمور الراوتر سوى :

```
route 10.0.0.100 link 10.0.1.0/24/
route 10.0.0.100 link 10.0.0.100/32/
```

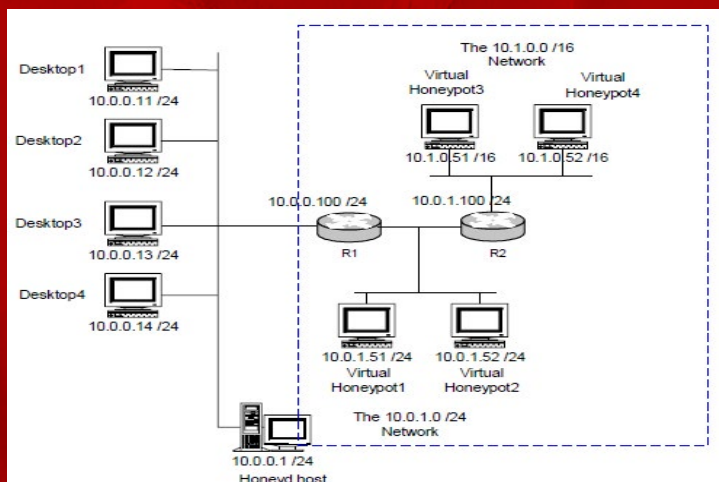
السطر الأول يدل أن الراوتر صاحب العنوان 10.0.0.100 يوصل إلى الشبكة 10.0.1.0/24 والسطر الثاني يعرف الطريق العكسي من أجل طريق عودة الطرود، بهذا نكون قد أنهينا تعريف الراوتر وسنقوم الآن بتعريف الأجهزة المتبقية. يتم تعريف نظام تشغيل حاسب كما تم تعريف نظام تشغيل الراوتر من خلال:

```
create windows
set windows personality «Microsoft Windows NT 4.0 SP5-SP6»
add windows tcp port 139 open
add windows tcp port 137 open
add windows udp port 137 open
add windows udp port 135 open
set windows default tcp action reset
set windows default udp action reset
```

ومن ثم إسناد هذا النظام مباشرة إلى الحواسيب كلاً حسب عنوانه :

```
bind 10.0.1.51 windows
bind 10.0.2.52 windows
```

الآن سنعمل على توسيع الشبكة قليلاً كما الشكل :



قمنا بإضافة الراوتر R2 ذو العنوان 10.0.1.100 إلى يوصل إلى الشبكة 16/10.1.0.0 تعليمات الضبط التي قمنا بها سابقاً تعاد هنا مع ملاحظة تغيير العناوين فقط :

```
route 10.0.1.100 link 10.1.0.016/
route 10.0.1.100 link 10.0.1.10032/
bind 10.1.0.51 windows
bind 10.1.0.52 windows
bind 10.0.1.100 router
```

بالنظر إلى شكل الشبكة التي قمنا بتحقيقها نرى أن الراوتر R1 لن يستطيع الوصول إلى الشبكة 10.1.0.0.16 لأنه غير موصولة معه مباشرة بل يجب إخباره بذلك ليعلم الطريق الذي سيسلكه للوصول لها من خلال الراوتر R2 ويتم ذلك بالتعليمة:

```
route 10.0.0.100 add net 10.1.0.010.0.1.100 16/ latency 100ms loss 20
```

التعليمة السابقة تشبه تعليمة تعريف بروتوكول التوجيه ويجدر الإشارة هنا إلى البارامترات المرفقة بالتعليمة وهي التأخير والضياع ويتم ضبط قيمها لتشعر المخترق بأن هناك ضياع وتأخير وكأنه ضمن شبكة حقيقية .

بقي الآن إضافة الراوتر الثالث كما الشكل الأساسي الذي تم طرحه بداية وتكون التعليمات الإضافية هي:

```
route 10.1.0.100 link 10.1.1.024/
route 10.1.0.100 link 10.1.0.10032/
bind 10.1.1.51 windows
bind 10.1.1.52 windows
bind 10.1.0.100 router
route 10.0.1.100 add net 10.1.1.010.1.0.100 24/ latency 50ms loss 1
bandwidth 1Mbps
```



```
Root@Mhdpc:~$/etc/init.d/honeyd start
```

## 2 - تشغيل الشبكة التي قمنا ببنائها ضمن بيئة Honeyd من خلال التعليمات:

```
Root@Mhdpc:~$ honeyd -f /etc/honeyd/ honeyd.conf -d
-p /etc/honeyd/nmap.prints
-x /etc/honeyd/xprobe2.conf >
-a </etc/honeyd/nmap.assoc >
-l </etc/honeyd/logs.log >
-i eth0 10.0.0.08/
```

طبعاً بعد تنفيذ التعليمات السابقة سيبدأ النظام بتسجيل وعرض كافة الطرود التي تمر عبر الشبكة الوهمية مع تفاصيلها من عنوان ومنفذ المصدر وعنوان ومنفذ الوجهة والوقت ونوع البروتوكول ، يمكن للتجريب استخدام أي حاسب من الحواسيب الحقيقية الموجودة ضمن الشبكة 1,2,3,4 Desktop للاختبار بحيث يمكن من خلال الحاسب 1 القيام ب telenet مع الراوترات الموجودة ضمن الشبكة الوهمية وسيتولى السكريبت الخاص بها عملية المحاكاة لإيهام المخترق بأنه يحاول الاتصال برأوتر حقيقي.

ملاحظة: عند تشغيل الشبكة ومحاولة الاتصال بأحد أجزاء الشبكة الوهمية لن يكون هناك استجابة لأن هناك طلبات arp ستوجه للحاسب المضيف لن يرد عليها على اعتبار العنوان المطلوب الوصول إليه لا يخصه لذلك يجب استخدام تعليمات تطلب من الحاسب المضيف بالرد على كافة طلبات arp لعنوان شبكة معين.

```
Root@mhdpc:~$/farpd -i eth0 10.0.0.08/ -d
```

### Tips

### الارقام السرية???

تعتبر الأرقام السرية الوسيلة الأكثر استخداماً في تشفير ما نملك من ملفات على الحاسوب والهاتف وعضويتنا على المواقع وايضا كل شيء شخصي لا نريد ان يصل اليه احد، لهذا فيجب علينا ان نضع كلمات قوية التشفير لكي لا يصل اليها احد، لكن المشكلة ان غالبية ان لم اقل كل مستخدمي الكلمات السرية يلجأون الى كلمات سهلة مثل ارقام الجوال او اسماء ابناء او اخوان او اصدقاء، او حتى عيد ميلادهم، وما يزيد الأمر بلة استعمال كلمة واحدة لا تتغير لكل المواقع والخدمات المستعملة، فهكذا انت فقط، تجعلك سمكة سهلة الإصطياد.  
يرجى استخدام كلمات مرور مختلفة ومعقدة





# خمس نصائح لمنع المستخدم من الاستخدام الخاطيء



في الحياة العملية لا يوجد أحد معصوم عن الخطأ وهذا طبعاً يينطبق في الحياة بشكل عام وطالما نحن هنا نتحدث عن الحياة العملية فسوف نأخذها من زاوية تقنية فقط، فالخطأ يمكن أن يقع فيه مدير الشبكات نفسه إلى أصغر موظف موجود في الشركة، في هذا المقال سوف أعطيكم خمس نصائح أو تدابير تقلل من نسبة الخطأ المتاحة التي من الممكن أن يقع فيها المستخدمين العاديين في أجهزتهم وفي أنظمتهم.

## 1 - جدولة المهام الأساسية.

لا يمكن أن تتخيل حجم الفائدة التي تمنحك أيها جدولة المهام في أجهزة المستخدمين والتي تقلل من نسبة حدوث مشاكل في أجهزتهم وإيكم قائمة أساسية من الأمور التي يجب جدولتها والتقييد بها.



- تحديثات برامج الأنتي فايروس.
- عمل فحص فيروسات
- تحديثات قاعدة بيانات برامج الـ Anti-Malware
- إلغاء تجزئة الأقراص
- تنظيف القرص
- النسخ الاحتياطي للبيانات

نقوم بعمل هذه المهام بشكل دوري لكي نتفادي جميع المخاطر التي تحيط بأجهزة المستخدمين.

## 2 - إبقاء الاذونات (permissions) على الحد الأدنى.

لكي نقوم بوضع أي مستخدم موجود لدينا في الدومين بصلاحيات أدمن على الجهاز الخاص به فيجب أن يتوفر سبب قوي لهذا الأمر، فهذا سوف يسبب لنا متاعب كثيرة في بعض الحالات وإذا لم نجعله محلي فمن الممكن أن نواجه تطبيقات معينة تحتاج منا حقوق المسؤول المحلي.





### 3 - إعادة تعيين كلمة المرور

من خلال حياتي العملية يوجد الكثير من المستخدمين من قام بتضييع كلمة المرور وهذا أدى إلى الاتصال بالمسؤول لكي يقوم بعمل reset ولكن المفاجأة أن المسؤول أو المدير قد قام بعمل ملف قد جمع فيه جميع الكلمات السر الخاصة بالمستخدمين في ملف وقام بتشفيره للأمان لترجيع كلمة المرور لمن فقدتها بشكل مباشر وسريع.

### 4 - لتسهيلات مقابل مستوى الأمان

المرونة وسهولة الاستخدام دائما يفضلها المستخدمين المتواجدين على أجهزة الكمبيوتر فعادة ماتؤدي برامج الأنتي فايروس والفايروس ومستوى الصلاحيات على الأجهزة إلى إبطاء الجهاز وتقليل فعالية أداء الأجهزة لكن هذا لا يجب أن يمنعنا أبداً من إزالتها أو التساهل فيها وصولاً عند رغبة المستخدمين فالنتائج السلبية نحن من سوف يتحملها مستقبلاً.



### 5 - أعطي المستخدمين كورسات تدريبية

لكي تتمكن من مخاطبة مستخدميك باللغة التي تعرفها لا بد لك من توفير بعض الكورسات والشروحات البسيطة والبدائية حول الكمبيوتر الذي يتعاملوا معه وكيف يستفيدوا منه بشكل أكبر، فأغلب المستخدمين يجهلوا المبادئ البسيطة للكمبيوتر فعلى سبيل المثال لا الحصر قد تخبر أحد المستخدمين أن يطفى الكمبيوتر فيقوم بضغط الزر الموجود على الجهاز أو يقوم بسحب القابس الموصول بالكهرباء لذلك يتوجب عليك تعليمهم على سبيل المثال ماهو المتصفح وماهي أدوات الأوفيس وكيف نتعامل مع الأوتلوك وكيف نستفيد منه بفعالية أكبر وماهي أهم الاختصارات الموجودة على لوحة التحكم.





# NetWork Set

First Arabic Magazine For Networks