NTDS Partitions:

- ✓ قاعدة بيانات ال **Active Directory** الموجودة في المسار التالي (**C:\Windows\NTDS**) والممثلة بالملف (**NTDS.dit**), يتم تقسيم قاعدة البيانات هذه داخليا الى **4Partition**:

1. **Domain partition**: و هو القسم الذي يخزن حسابات المستخدمين (**users Account**) و المجموعات (**groups**) و حسابات الأجهزة (**computer Account**،الأداة التي تمكننا من التعديل على هذا القسم ال (**Active Directory Users And computers**).
2. **Configuration partition**: هذا القسم يعبر عن المواقع الفيزيائية لل (**Active Directory**)، أيضا في هذا القسم يتم ضبط عملية ال **replication** بين أكثر من **Domain controller**, من خلال مفهوم الموقع الفيزيائي (**site**), حيث انه في حال كان كلا من أجهزة ال **domain controller** في نفس الموقع الفيزيائي (**site**)، وبالتالي سرعة النقل بينهما عالية فتتم عملية ال **replication** لمعلومة من **domain controller** الى أخر في نفس اللحظة، بينما لوكان كلا منهما في موقع فيزيائي مختلف (**site** مختلف)، سنقوم بجدولة عملية ال **replication** في وقت معين مختلف عن وقت العمل, كي لا يتم حجز عرض حزمة الاتصال من أجل عملية ال **replication**، والأداة التي تسمح بالتعديل على هذا القسم هي (**Active Directory site and services**)، حيث أنه بشكل افتراضي لو كان كلا من ال **domain controller** موجود في ذات الموقع الفيزيائي فإن عملية ال **replication** تحصل في الوقت الحالي , أما لو كانا في **2site** فتحصل عملية ال **replication** كل **180** دقيقة, ونستطيع تغيير الجدولة.

3. **Schema partition**: وهو يمثل الشكل العام لمكونات ال **Active Directory** مثل ال **users** و ال **groups**, حيث يقسم الى مجموعة من ال **class** وال **attributes**، مثل ال **user** يمثل ال **Class** والخصائص الخاصة بهذا ال **user** تمثل ال **attributes**، من غير المفضل أن تقوم بالتعديل على ال **Schema**، وفي حال أردت التعديل على ال **schema** هناك برامج مخصصة للتعدي عليها, حيث يتم فتح ال **Schema partition** بإستخدام الأداة **schmgmt.dll**، حيث أنها لاتظهر في قائمة **tools**، حيث يتم إضافتها بإستخدام الأمر (**Regsvr32.exe schmmgmt.dll**) في قائمة (**Run**), ومن ثم فتح الأداة (**mmc**) من قائمة **run** و إضافة ال **console** الخاص بال **schema** وذلك كما يلي , في نافذة **mmc** <<<< **file** <<<<< **add/remove snap-in** <<<< نقوم بإضافة الأداة (**Active Directory schema**), ومن ثم يمكننا حفظ هذا التخصيص على سطح المكتب.
4. **Application Partition** : الأداة المستخدمة لفتحه هي (**DNS**), وذلك من قائمة **Tools** في ال **Server manager**.

- **Operation Master Role** وهي الأدوار التي يمكن لل **domain Controller** أن يقوم بها:

1. **Domain Naming Master Role**: وهو جهاز واحد يقوم بهذا الدور على مستوى ال **forest** بشكل كامل، حيث أنه بشكل إفتراضي أول **Domain Controller** يتم إنشائه في ال **Forest**, وظيفة هذا الجهاز الذي يقوم بهذا الدور ،أن يقوم بتسجيل أسماء المجالات (**Domains**) التي يتم إنشائها على مستوى ال **forest** سواء (**Child Domain**، **Additional Domain**، .....).

2. **Schema Master Role**: أيضا جهاز واحد فقط على مستوى ال **Forest** يقوم بهذا الدور، حيث أن وظيفة الجهاز الذي يقوم بهذا الدور أن يتحكم بالشكل العام لل **Active Directory** وبالتالي الشكل العام لجميع ال **objects** وتحديد خصائصها على مستوى ال **forest** كاملة .

3. **Relative ID(RID)** : جهاز واحد فقط على مستوى ال **domain** يقوم بهذا الدور, ذكرنا سابقا أن لكل (**Object**) له رقم (**SID**) مختلف عن الأخر, فإن السيرفر الذي يقوم بهذا الدور هو المسؤول عن إعطاء كل **Object** ال (**SID**) مختلف .

4. **Primary Domain Controller** (**PDC**) : وهو جهاز واحد فقط على مستوى ال **Domain** يقوم بهذا الدور، وهو السيرفر المسؤول عن عملية تخزين المعلومات الأمنية **Security transaction**, على مستوى ال **domain** بشكل كامل، مثلا في حالة تغير ال **password** ل **user** معين, وكان لم يحصل **replication** لهذه ال **password** الى ال **Active Directory** الأخرى التابعة لنفس ال **domain** فإن ال **user** لايمكنه تسجيل الدخول, عندها سيقوم ال **Domain controller** الذي تم تسجيل الدخول عبر, بالتواصل مع ال **Domain Controller** الذي يقوم بدور ال **PDC** ليقوم بالتأكد منه أنه تم تغيير هذه ال **Password**.

5. **Infrastructure Role** :

- قبل أن نقوم بشرح ال **infrastructure Role** ، لدينا مفهوم ال **Global Catalog** وهو عبارة عن جهاز **Domain Controller** الذي يملك معلومات عن جميع الأغراض (**Objects**) على مستوى ال **Domain** وعلى مستوى ال **Forest** وبالتالي يسهل عملية البحث عن ال **Object**، حيث من الممكن أن يكون لدينا أكثر من **Domain Controller** يقوم بدور ال **Global catalog**، لكن على الأقل يجب أن يكون لدينا (**DC**) واحد يقوم بدور ال (**Global Catalog**).

- وبالتالي الجهاز الذي يقوم بدور ال (**infrastructure Role**), يقوم بالوظيفة ذاتها التي يقوم بها ال **Global Catalog** , وفي حال وجود كلا منهمها على نفس السيرفر يقوم ال(**Global Catalog**) بإيقاف وظيفة ال **Infrastructure Role**.
- وبالتالي من الممكن أن يكون لدينا أكثر من **Global Catalog**، لكن لا يمكن أن يكون لدينا سوى (**Infrastructure Role**) واحد على مستوى ال **Domain**.

إعداد Additional Domain Controller :

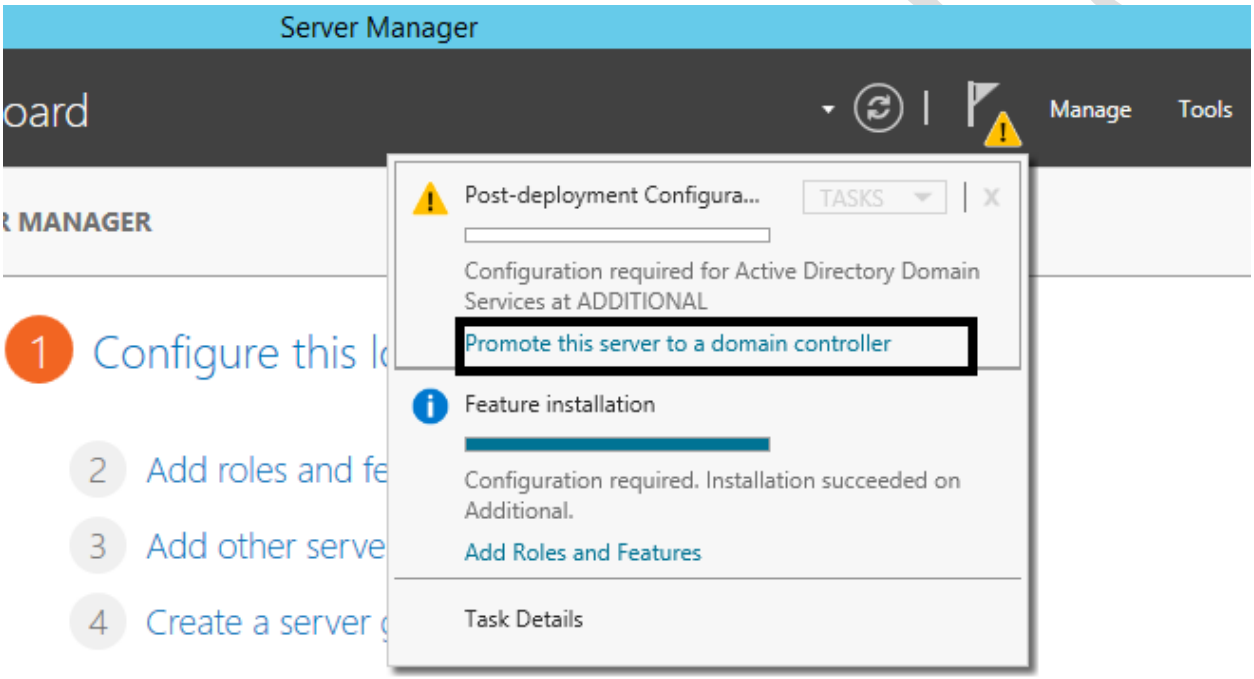
- ✓ في الإصدارات القديمة من **Windows server**، كان لدينا مفهوم ال **Primary Domain Controller** وال **Backup Domain Controller**، حيث كان ال **primary** يقوم بجميع الأدوار السابقة, وفي حال حصلت مشكلة يحل محله ال **Backup**, أما في الإصدارات الحديثة أصبح بإمكاننا توزيع الأدوار ما بين ال(**Primary Domain Controller**) و ال (**Additional Domain Controller**), الذي نقوم بإعداده كما يلي:

- نقوم بتجهيز مكنة وهمية جديدة, تملك أسم مختلف عن ال(**Primary**) ولنفرض له الإسم (**Additional**).
- يجب إعداد ال **ip** لل **Additional** من شبكة ال **primary** ذاتها .
- يجب أن نضع ال **DNS Server** لل **Additional** هو عنوان الجهاز ال **primary** الذي يقوم بدور مخدم ال **DNS Server** في الشبكة, وذلك لأن ال **Additional** سيقوم بالاتصال مع ال **primary** بإستخدام الإسم.
- قبل البدء بالإعداد نقوم بإختبار الاتصال مع جهاز ال **primary** كما يلي :

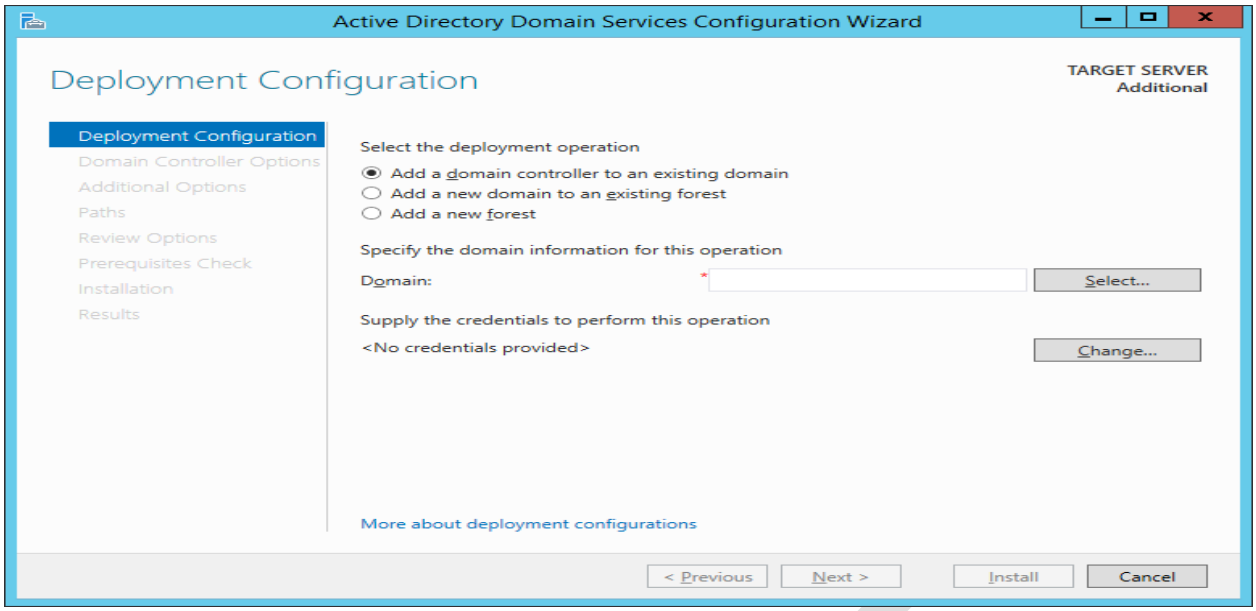
Ping info.local

Ping PDC.info.loca

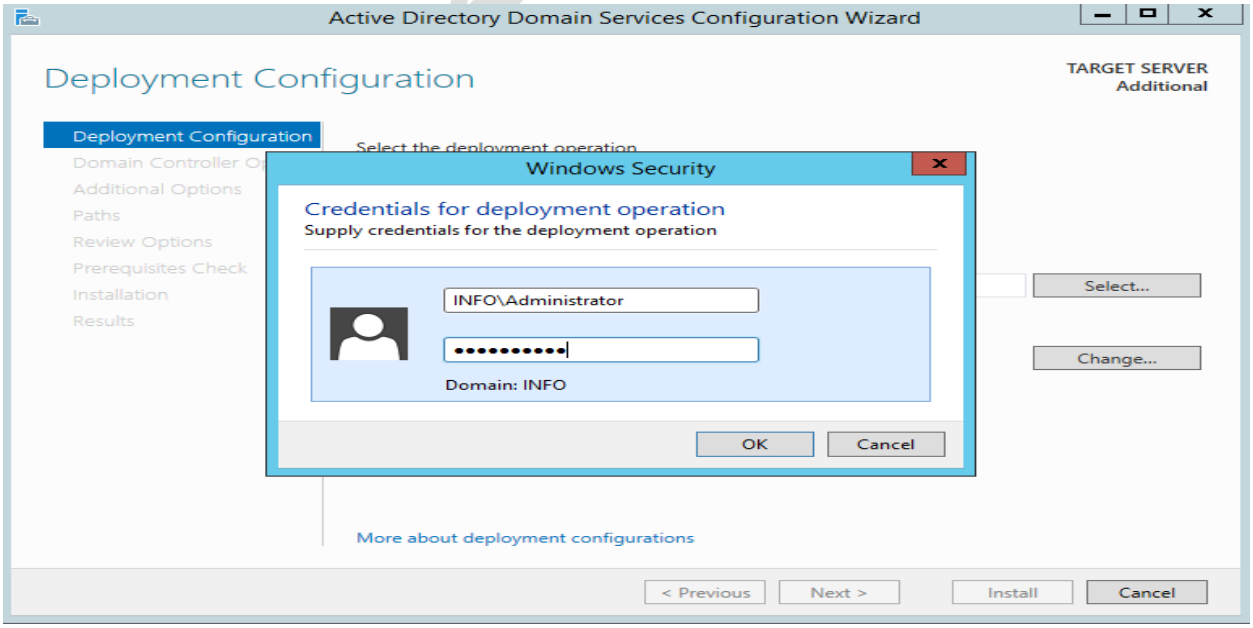
- نقوم بتبيت خدمة ال **Active Directory** ، وذلك من<<<<< **Add roles And** <<<<<<**Featuers** نضع ال **check** على**Active Directory Domain Services** <<<< **next** <<<< **Install**.
- بعد تثبيت خدمة ال **Active Directory** نقوم بترقية(**Promotion**) هذا الجهاز الى **Domain Additional controller** لل **domain** (**Info.local**)، كما يلي :
  - من ال **server manager** ننقر على إشارة العلم والتي عليها مثلث أصفر , ونقوم بتفعيل الخيار (**promot this server to domain controller**), كما يلي :

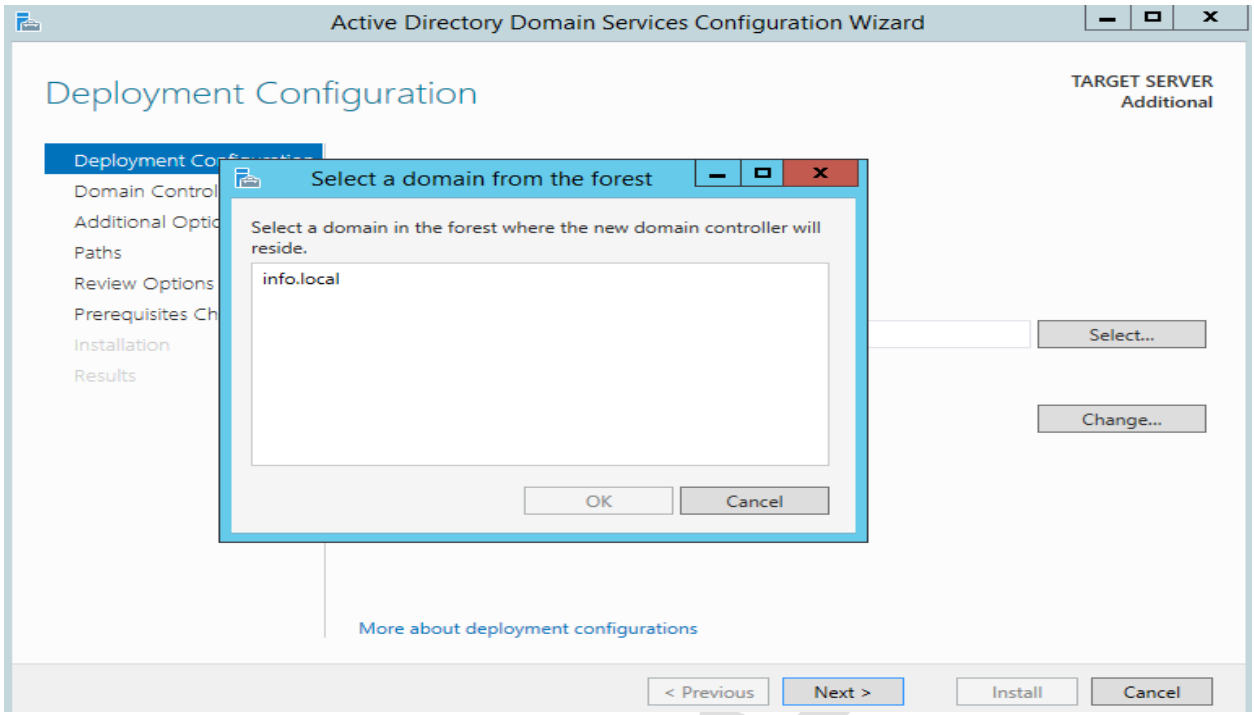


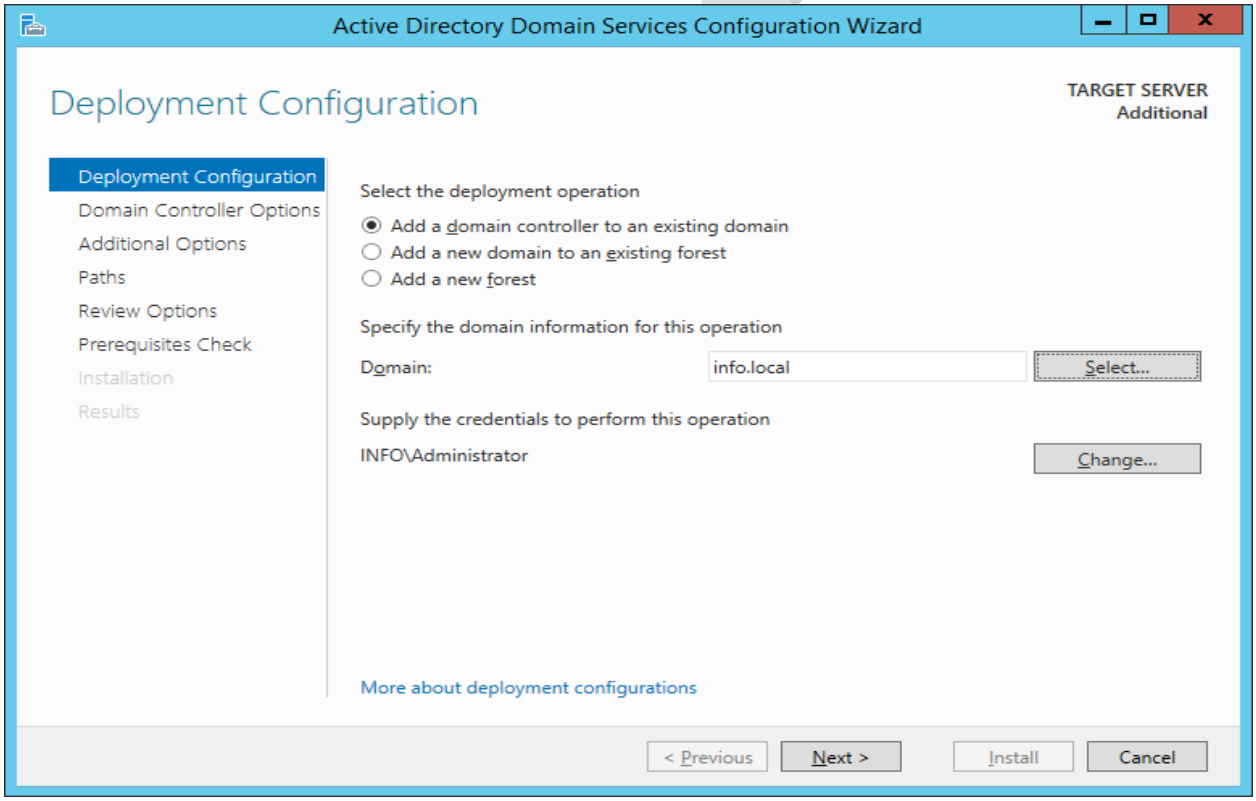
❖ تظهر النافذة التالية :



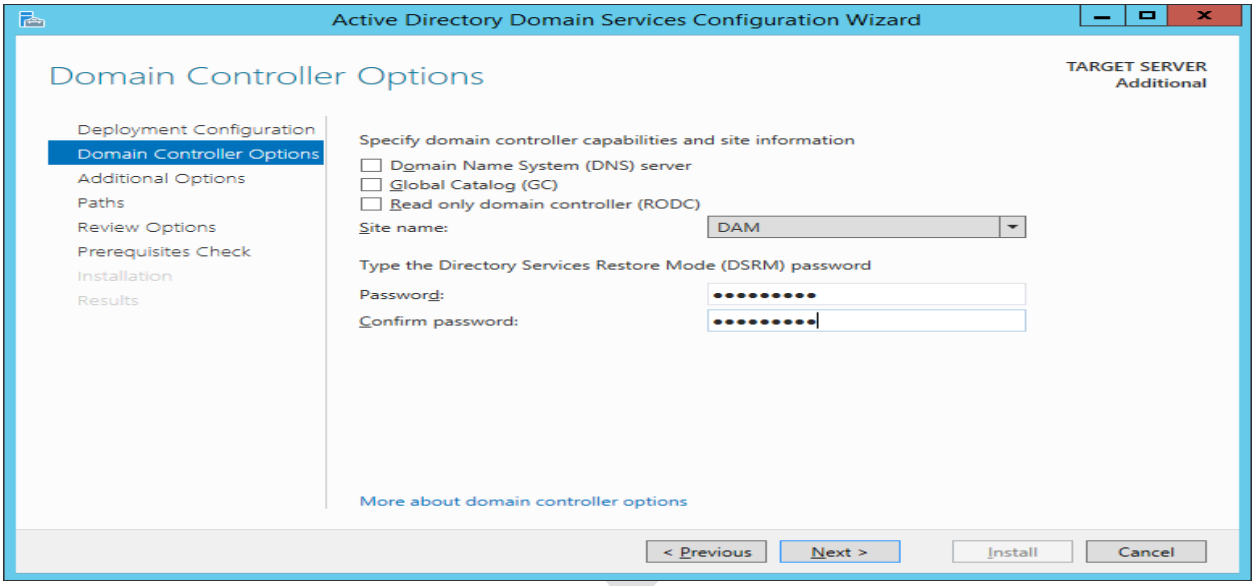
❖ نريد ترقية هذا السيرفر الى **Additional Domain Controller** ل **Domain** موجود وهو **info.local** لذلك يتم إختيار الخيار الأول (**Add a Domain controller to an existing domain**)، ثم ننقر على الزر **select** لإختيار ال **Domain** المراد إنشاء **additional** له، فتظهر نافذة تطلب حساب ال **Administrator** لهذا ال **domain** ، فيظهر ال **domain** ويتم إختياره، ثم **Next**:



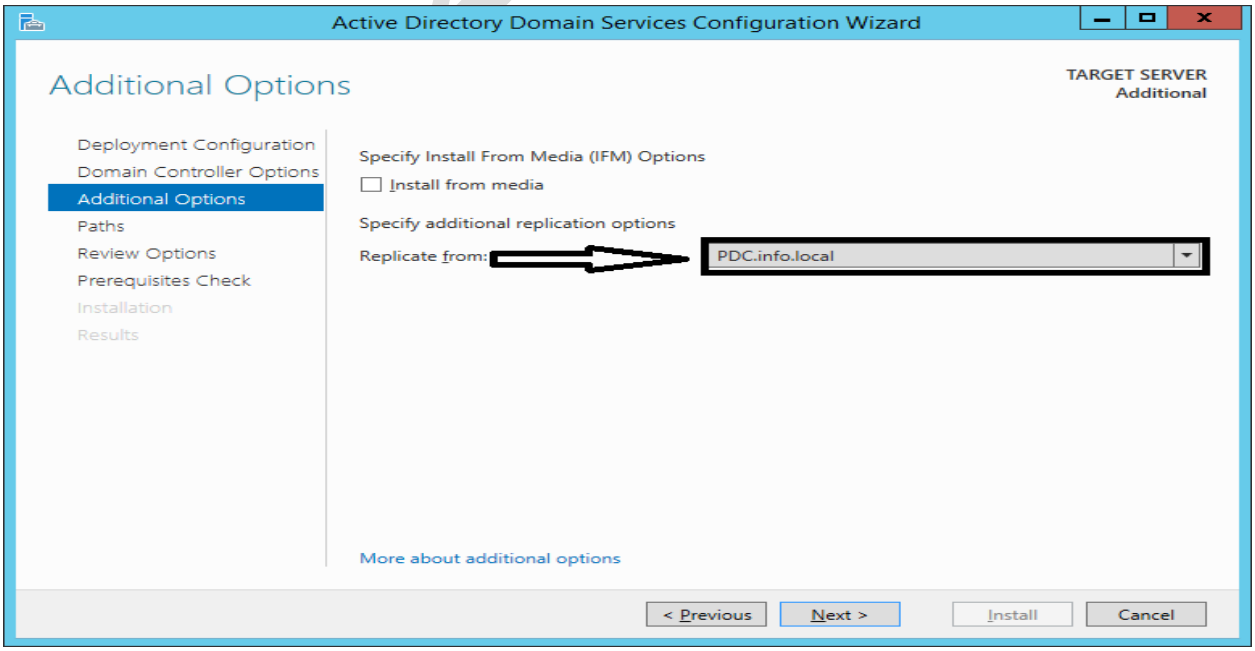

Active Directory Domain Services Configuration Wizard
Deployment Configuration
TARGET SERVER
Additional
Deployment Configuration
Domain Control
Additional Optic
Paths
Review Options
Prerequisites Ch
Installation
Results
Select a domain from the forest
Select a domain in the forest where the new domain controller will reside.
info.local
OK
Cancel
Select...
Change...
More about deployment configurations
< Previous
Next >
Install
Cancel


Active Directory Domain Services Configuration Wizard
Deployment Configuration
TARGET SERVER
Additional
Deployment Configuration
Domain Controller Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Select the deployment operation
Add a domain controller to an existing domain
Add a new domain to an existing forest
Add a new forest
Specify the domain information for this operation
Domain:
info.local
Select...
Supply the credentials to perform this operation
INFO\Administrator
Change...
More about deployment configurations
< Previous
Next >
Install
Cancel

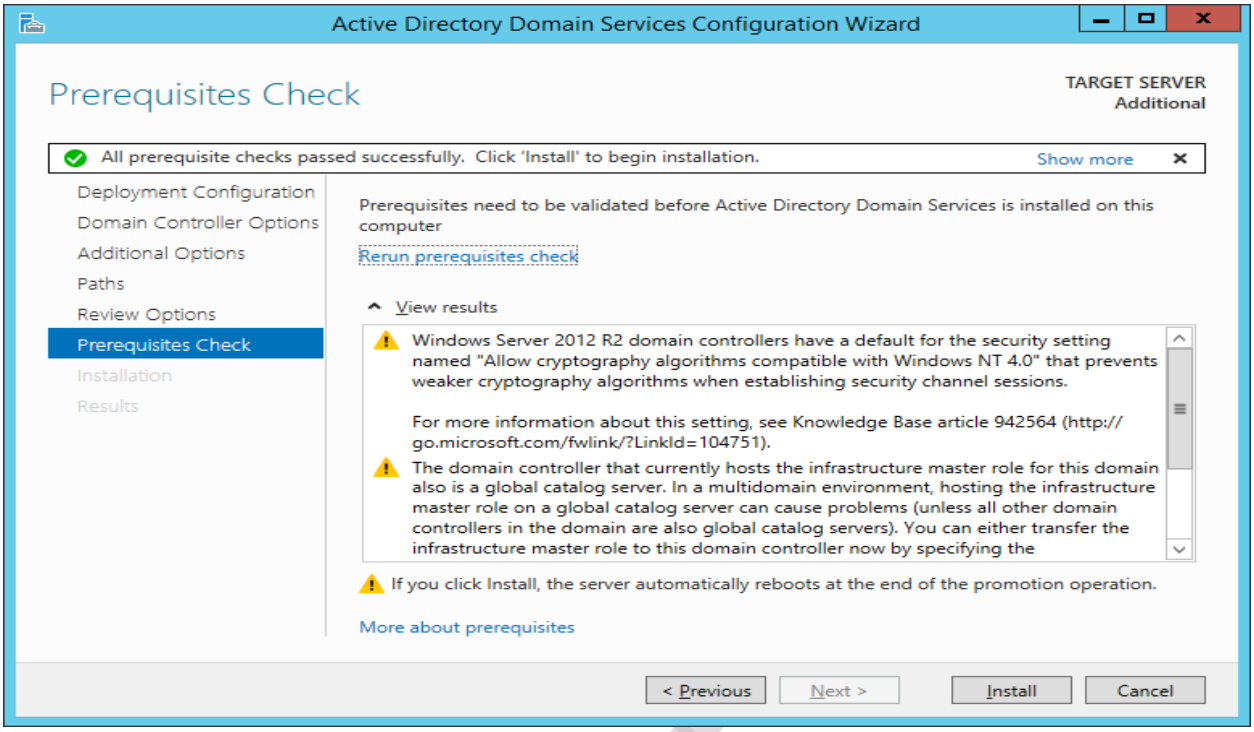
❖ ثم تظهر لدينا النافذة التالية ،حيث يتم الإختيار فيما لو نريد أن يقوم هذا ال **domain Controller** بالأدوار التالية (**DNS Server**، **global Catalog**) , فيما لو أردنا أن يكون للقراءة فقط (**Read onle Domain Controller**)، ثم نختار ال **Site** لهذا ال **Domain Controller**, وإسناء كلمة مرور من أجل ال **Restore Mode** ، ثم **Next** :



❖ في النافذة التالية، يتم تحديد ال **Domain Controller** التي ستتم عملية ال **Replication** منه:



❖ بعد إنهاء جميع الإعدادات نقوم بالتثبيت (**Install**):



❖ ملاحظة : بعد إنتهاء التثبيت، وإعادة الإقلاع , يصبح هذا ال **Domain Controller** نسخة عن ال **Primary Domain Controller**، وبالتالي عملية تسجيل الدخول على ال **Additional** تتم بإستخدام ال حساب ال **Administrator** لل **Primary**.