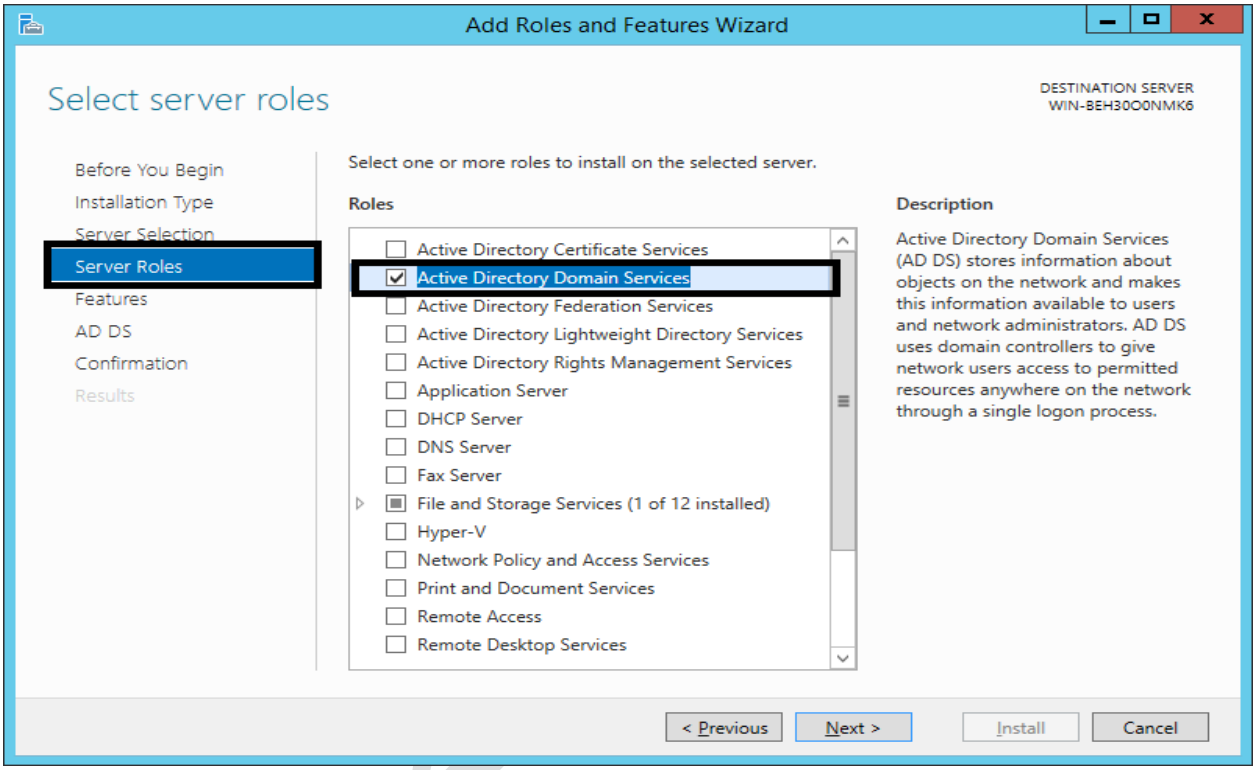
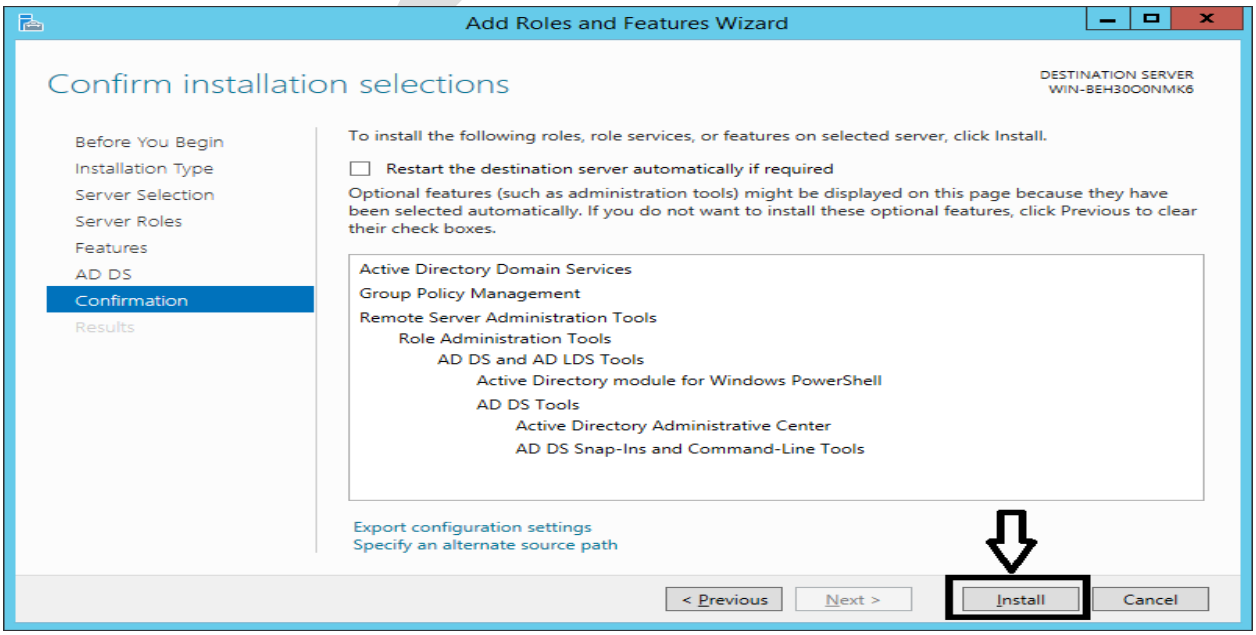
تنصيب خدمة ال Active Directory

- **مميزات ال Active Directory :**
  - **تخزن جميع المستخدمين ضمن ال Domain.**
  - **تستخدم لإدارة الشبكة بشكل مركزي.**
  - **عند تسجيل الدخول على بيئة ال Active Directory, فإنها تقوم بإرسال جميع السماحيات التي يمكننك القيام بها, أي أنه بعد تسجيل الدخول لا يتم أي طلب ل (إسم مستخدم وكلمة مرور) لإعطاء أي سماحية كما هو الحال في شبكة ال workgroup.**

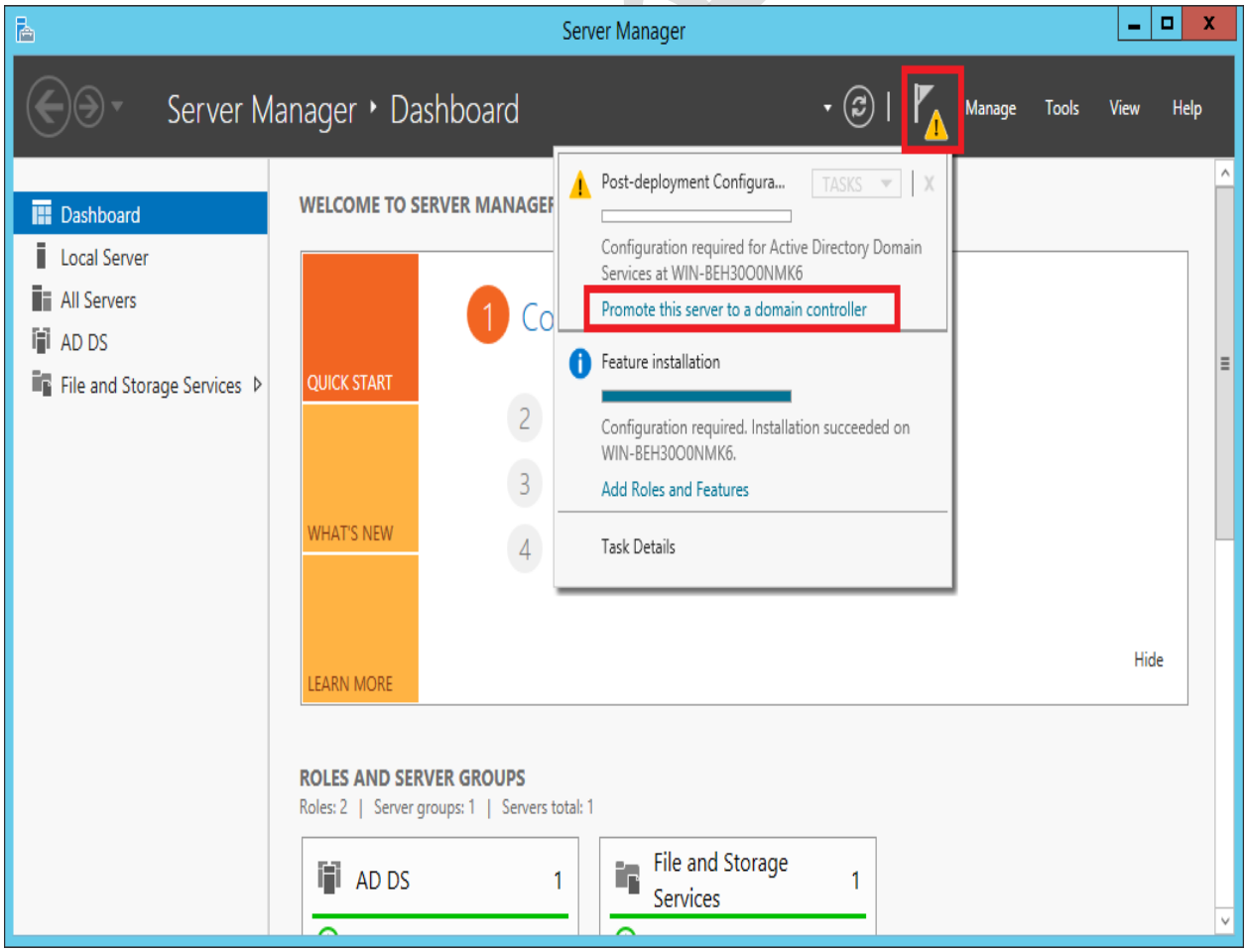
- **قبل البدء بتثبيت ال Active Directory يجب التأكد من وجود بعض المتطلبات :**
  - **التأكد أن الحاسب له (Static IP) , ويجب أن يتم إعداد ال DNS Server له بعنوان الحاسب ذاته أو عنوان ال Loopback (127.0.0.1), لكي لا يتم تغيره كلما تم تغيير عنوان السيرفر , وذلك لأن تثبيت ال Active Directory يتطلب تثبيت خدمة ال DNS معها , وبالتالي سيصبح السيرفر ذاته مخدم DNS أيضا وذلك من أجل ربط أسماء الأجهزة في ال Domain مع عناوينها وبالتالي سهولة في التعامل مع الأجهزة.**
  - **من المفضل أن يكون النظام محدث من خلال (Windows Update).**
  - **يجب أن يكون لحساب ال Administrator كلمة مرور معقدة.**

- **بعد ذلك نبدأ بتنصيب ال Active Directory:**
  - **ندخل الى ال Server manager.**
  - **ننتقل الى Add roles and features لتثبيت ال Active Directory.**



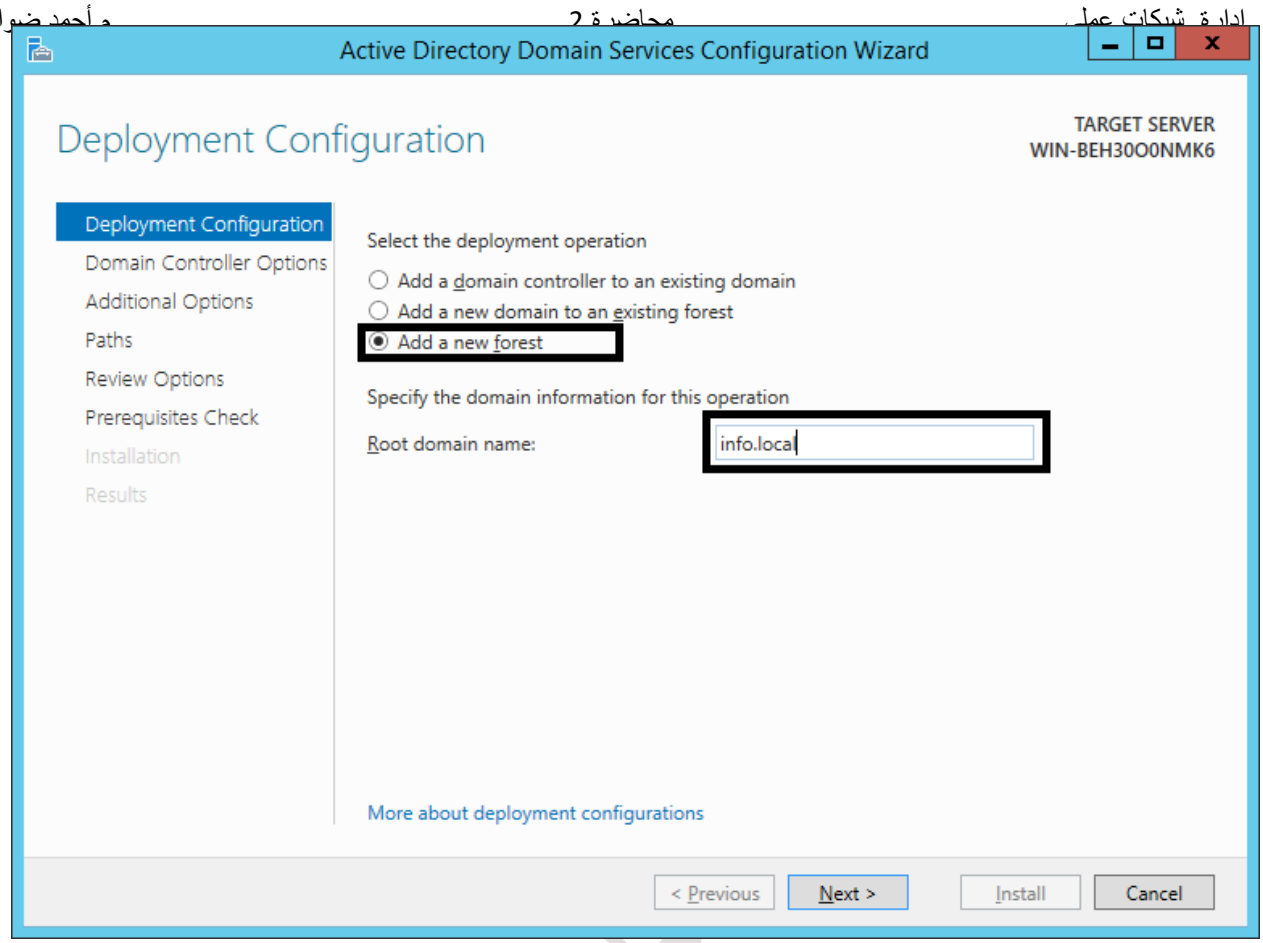


- مفهوم ال **Active Directory** : الخدمة التي يتم عن طريقها تحويل الأجهزة الى **Domain**.
- مفهوم ال **Domain** هو مفهوم منطقي وهمي, حيث أن جميع الموارد ستكون أعضاء من هذا ال **Domain**.
- مفهوم ال **Domain controller** :هو مفهوم فيزيائي, وهو الجهاز المسؤول عن إدارة أجهزة ال **Domain**.
- في الإصدارت السابقة من **Windows server** مثل (**2003–2008**) فإنه بعد تثبيت خدمة ال **Active Directory** يجب ترقية الجهاز الى (**Domain controller**) بإستخدام الأمر من قائمة (**Run**) وهو (**dcpromo**), أما في **windows 2012** لا يوجد الأمر **DCpromo** لترقية السيرفر الى **Domain Controller** وتتم عملية الترقية من واجهة ال **Server manager**, كما يلي :



- سيظهر لدينا **Wizard** لعملية الترقية, من النافذة التالية التي سنحدد بها ما هو نوع ال **Domain Comtroller** الذي سيتم إنشائه, حاليا سيتم إختيار الخيار الثالث (**Add a new forest**) لأنه أول **Domain controller** يتم إنشائه في ال **Domain** أو ال **Forest** بشكل كامل,وبالتالي يكون هو ال **Primary Domain controller** وثم نحدد إسم لهذا ال **Domain** مثلا (**info.local**), ويكون لديه القدرة على التحكم بجميع المجالات الأبناء تحته.
- لنفرض مثلا أن هذا ال **Domain** خاص بشركة كبيرة تحتوي على عدد من الأقسام و عدد كبير من الموظفين, وبالتالي لا يكفي **Domain controller** واحد لإدارة هذا هذه الشركة , لأنه سيشكل حمولة كبيرة بالإدارة على **domain controller** واحد, وبالتالي يمكننا أن نقوم بإنشاء (**Child domain controller**) على مستوى كل قسم, ولنفرض لدينا قسم خاص للموظفين(**emp**) وقسم خاص للطلاب(**student**), وبالتالي يمكننا إنشاء **Child Domain controller** لإدارة الموظفين بإسم مجال (**emp.info.local**) و **Child Domain controller** لإدارة الطلاب بإسم مجال (**Student.info.local**), وكل مجال ابن يمكنه التحكم فقط بالموارد التابعة له فقط, أيضا يمكننا إنشاء مجالات أبناء للمجالات الأبناء لدينا.
- وبالتالي يظهر لدينا مفهوم الأشجار (**tree**): وهو عبارة عن ال **parent domain controller** مع واحد فقط من الأبناء له, وبالتالي يشكل فرع شجرة.
- ومفهوم ال **forest** :هو عبارة عن **parant domain controller** مع جميع الأبناء له , يشكل ما يسمى غابة (**Forest**).

- يجب إنشاء **domain controller** إضافي (**Additional**) له ذات إسم ال **Domain** الأساسي (**info.local**), وذلك في حال حصلت مشكلة ما في ال **primary Domain controller** , فإن هناك **domain controller** أخر (**Additional**) يكون عبارة عن نسخة من ال **Primary Domain controller** , يحل محله, وبالتالي نحافظ على عمل الشبكة مستمر, حيث يكون بينها علاقة (**replication**) أي أن الِ **Additional Domain controller**يحصل على قاعدة بياناته من ال **Primary Domain controller** , وأي تعديل يحصل على ال **primary Domain controller** ينتقل ال **Additional** وبالعكس أيضا أي تعديل على **Additional** ينتقل الى ال **Primary**.
- لنفرض مثلا أن شركة ما قامت بشراء شركة أخرى , وكلا من الشركتين تحتوي على **Domain** مختلف عن الأخر, الأولى لنفرض أن ال **Domain** الخاص بها (**info.local**) والشركة الأخرى ال **Domain** الخاص بها هو (**techno.local**), هل من المعقول أن نقوم بهد البنية التحتية لإحدى الشركتين وإعادة بنائها بما يتوافق مع ال **domain** بالشركة الأخرى, لا يمكن فعل ذلك , وبالتالي أقوم بترك كلا من الشركتين كما هي, و نقوم بإنشاء بينها علاقة تدعى علاقة **trust** , تسمح بوصول الأجهزة في ال **Domain** الأول الى الأجهزة في ال **Domin** الأخر.
- يجب الملاحظة أنه في حال كان سيتم وصل هذا ال **Domain** ال شبكة الانترنت, فإن إسم ال **domain** هذا يجب أن يتم شرائه.
- الخيار الأول في النافذة التالية (**Add a domain controller to an existing domain**) وهو يستخدم في حال إنشاء (**additional domain controller**) .
- الخيار الثاني (**Add a new domain to an existing forest**), وهو يستخدم في حال إنشاء **chiled domain controller**.
- الخيار الثالث (**add a new forest**) : وهو يستخدم لإنشاء **primary domain controller** , المتحكم المجال الأساسي في ال **Domain** بكامله.

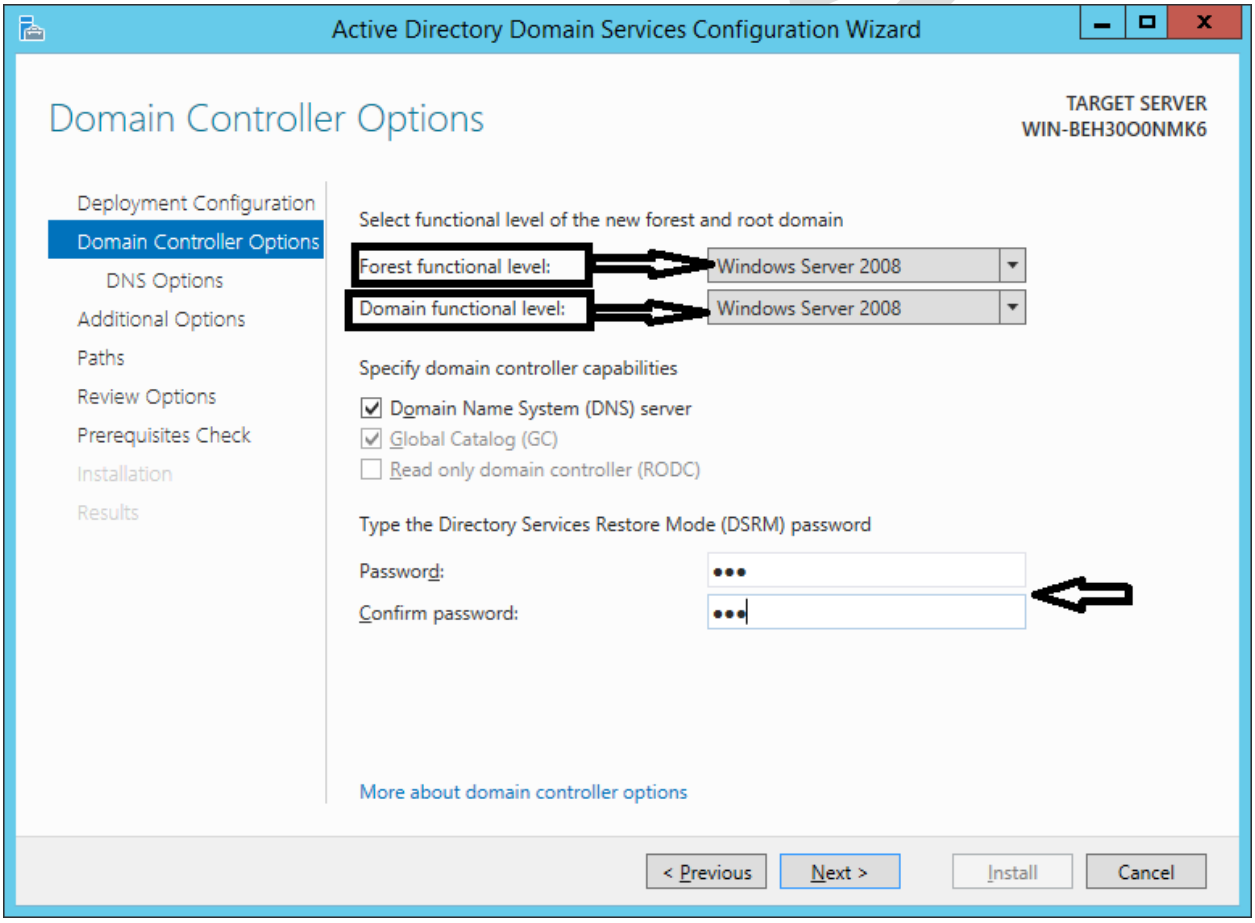


- في النافذة التالي نقوم بتحديد كلا مما يلي :

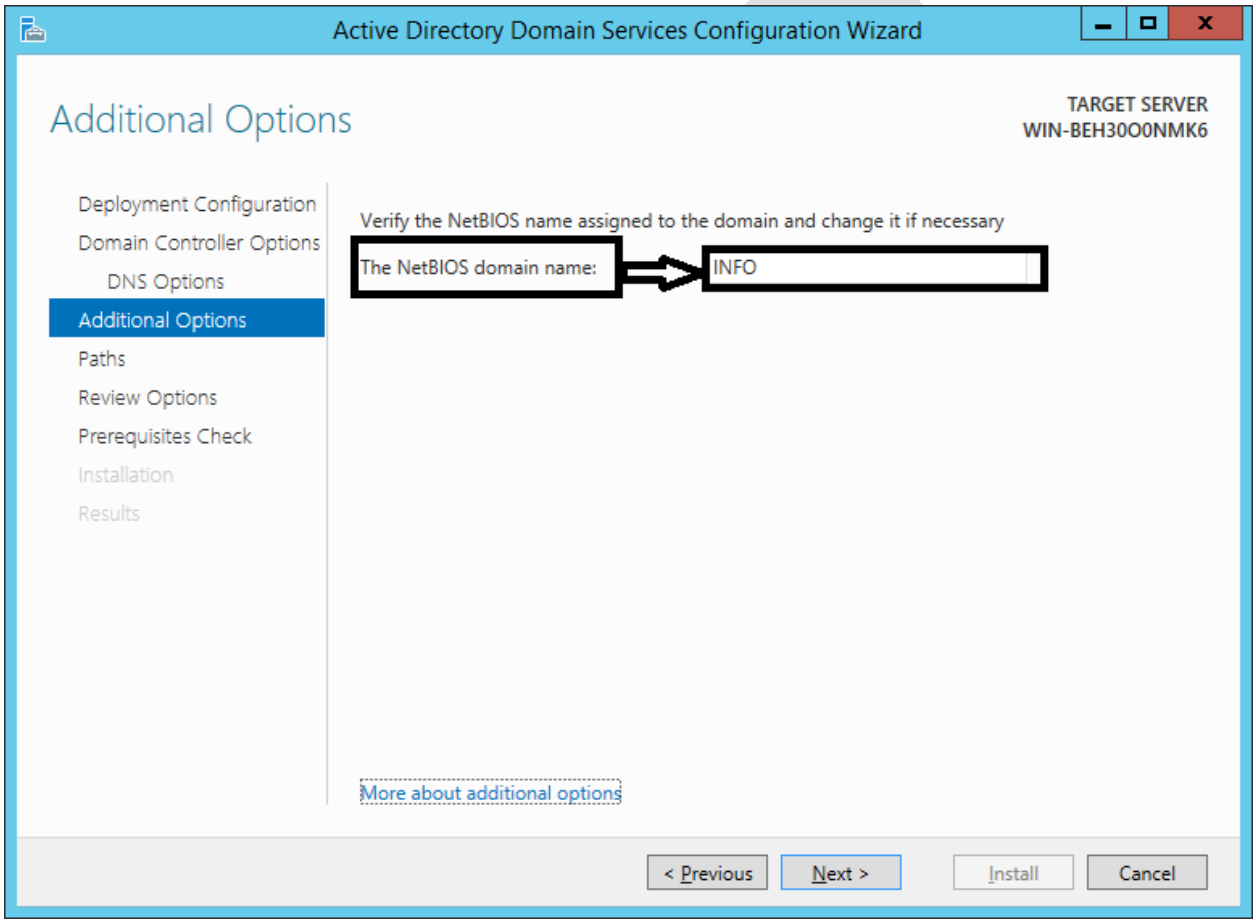
- **Forest functional level**: الخيار الذي يتم إختياره يحدد أقل إصدار من ال **Windows server** الذي يمكن إستخدامه على مستوى ال **Forest**.
- **Domain functional level**: الخيار الذي يتم إختياره يحدد أقل إصدار من ال **Windows server** الذي يمكن إستخدامه على مستوى ال **Domain**.
- ثم نحدد فيما إذا أردنا تنصيب خدمة ال **DNS** مباشرة على هذا ال **Domain controller**, بوضع ال **Check** أو إزالته عن الخيار **Domain Name System (DNS) server**, ونقوم بتنصيبه وذلك من أجل السماح بالدخول الى الأجهزة بإستخدام الإسم بدلا من العناوين.
- ثم نحدد فيما إذا كنا نريد أن يكون ال **Domain controller** الذي يتم إنشائه (**Global gatalog**), وهذا يعني أن يكون ال **Domain controller** الذي يتم إنشائه يمتلك معلومات

حول جميع الأغراض على مستوى ال **Forest** أو ال **Domain** بالكامل من أجل أن يعمل كمحرك بحث عن الموارد لجميع المستخدمين, وعلى الأقل يجب أن يكون لدينا **global gatalog** واحد وبما أن ال **Domain controller** الذي يتم إنشائه حاليا هو أول **Domain controller** فحكما يجب أن يكون **Global Gatalog**.

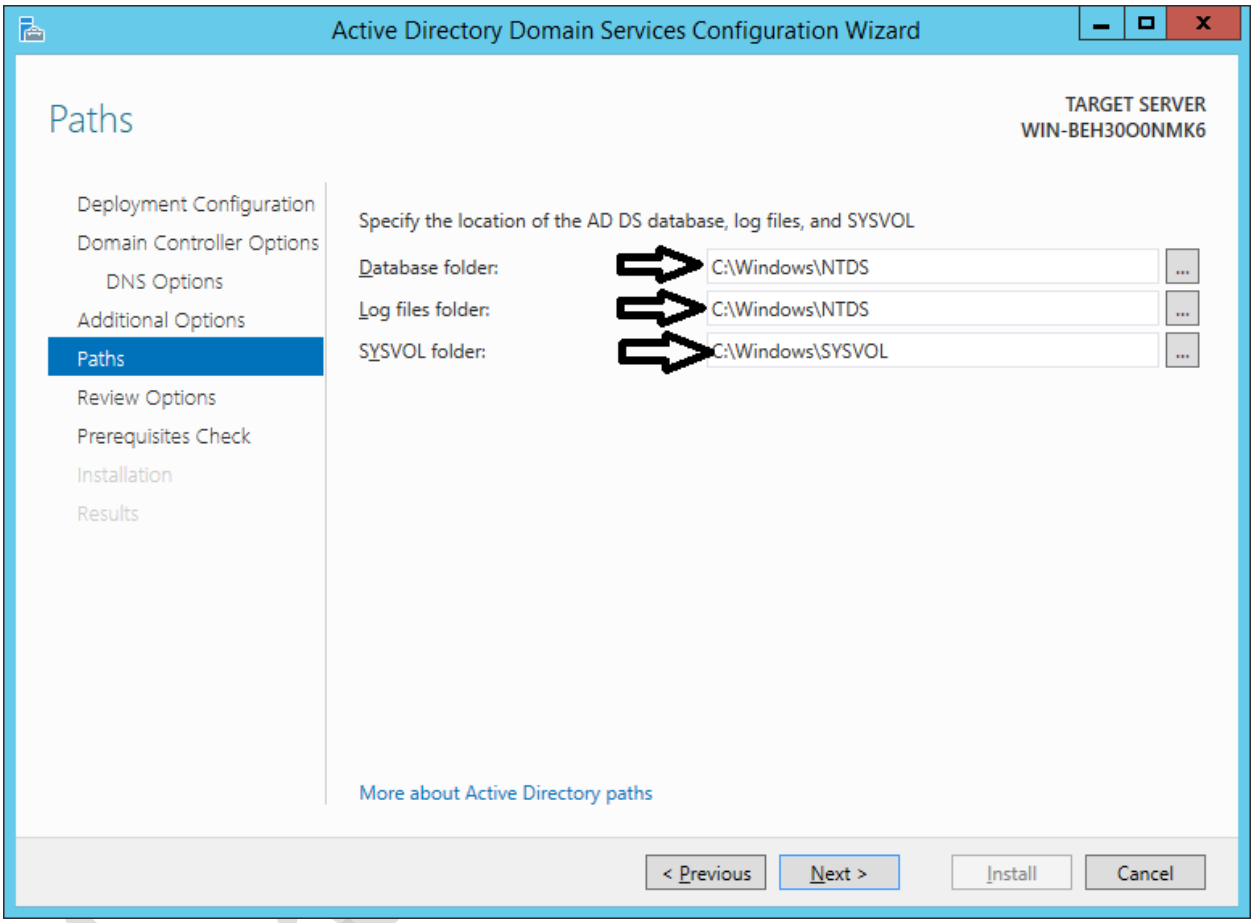
- ثم نحدد فيما لو أردنا أن يكون ال **Domain Controller** قابل للقراءة فقط بإستخدام الخيار (**Read only domain controller(RODC)**), أي لا يمكن التعديل عليه وإضافة أية أغراض أو حذفها , وذلك لا يمكن أن يتم إختياره في ال **Primary Domain controller**.
- وأخيرا يتم وضع كلمة مرور من أجل ال **Restor Mode** والذي نتمكن من خلاله إستعادة ال **Active directory** في حال حصل لها أية مشكلة.

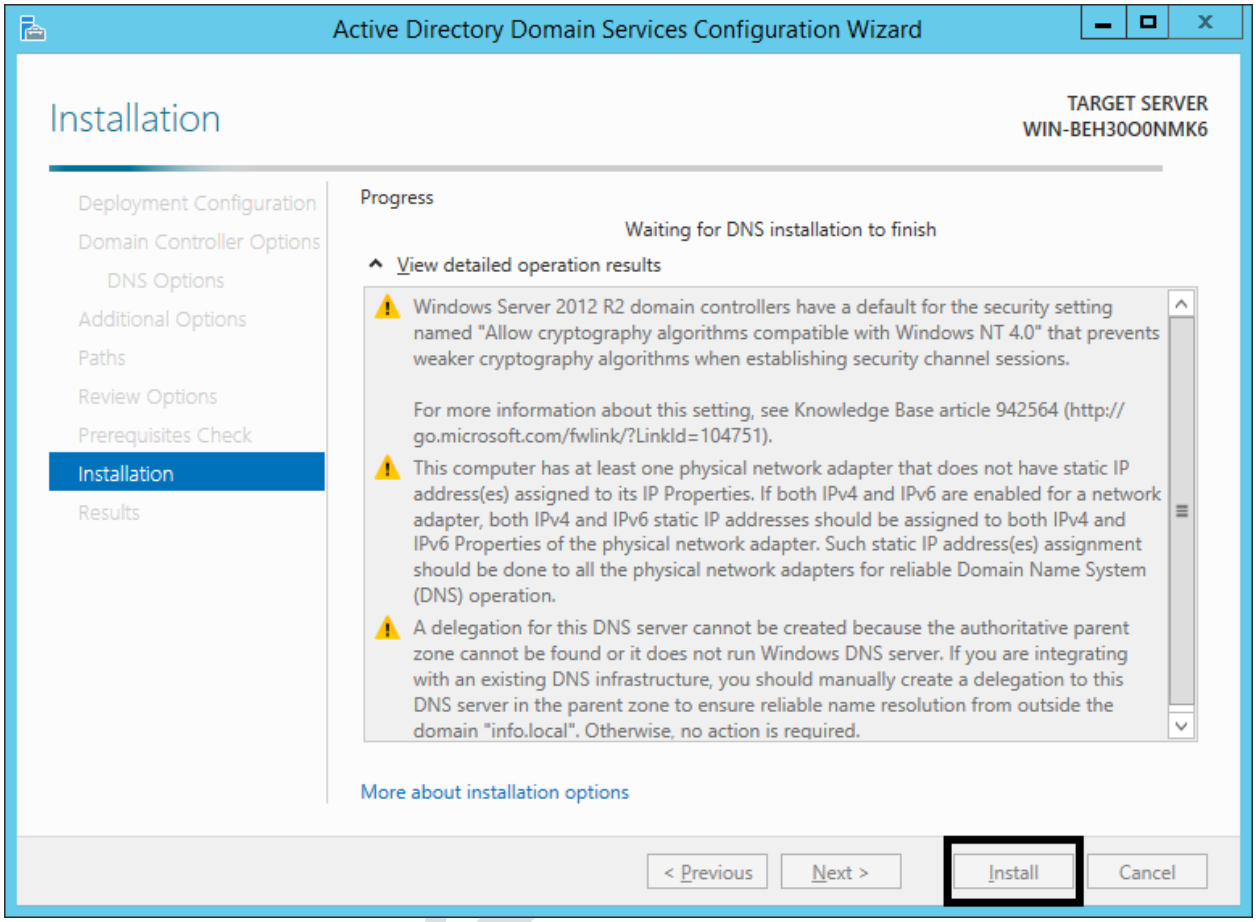
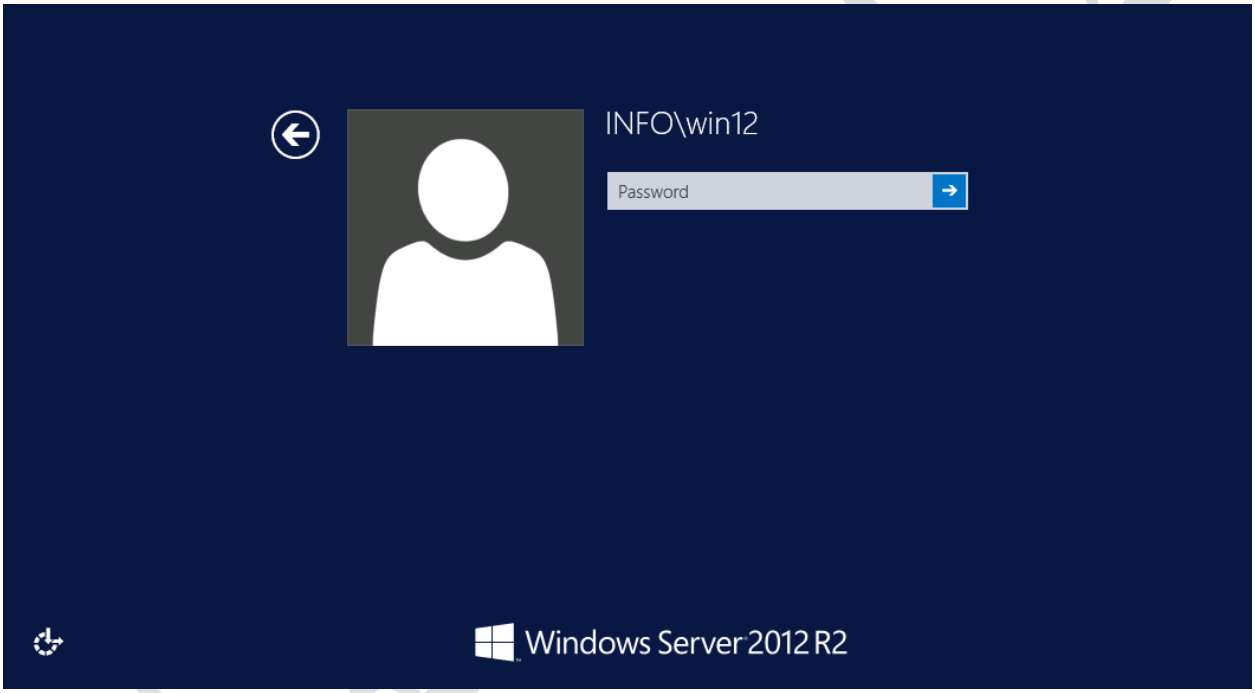


- في النافذة التالي يتم تحديد ال **Netbios Name** لل **Domain** بالكامل , وهو بشكل عام إسم الجهاز دون إسم ال **Domain**, حيث برتوكول ال **NetBios** يعمل بألية ال **broadcast** عند الاتصال مع جهاز أخر بإسم ال **NetBios** له, وذلك مما يزيد من حمولة البيانات على الشبكة , وأيضا لا يمكن التعامل مع الأجهزة بأسماء ال **Netbios** لها عند ربط ال **Domain** على شبكة الانترنت لأنه من الممكن أن يحصل تضارب بالأسماء من **Domain** لأخر, لذلك ظهر ال **FQDN (fully qualified domain name)** , والذي هو عبارة عن ال **Hostname** مضاف اليه **domain name** , وبذلك لن يحصل تضارب بين أسماء الأجهزة على مستوى العالم.



- في النافذة التالية يتم تحديد موقع تخزين قاعدة بيانات ال **Active Dire** و وسجل الأحداث (**log files**) وهو مجلد (**NTDS**) و أيضا موقع تخزين ال **polices** التي سيتم تطبيقها على المستخدمين وهو مجلد (**SYSVOL**) :




Active Directory Domain Services Configuration Wizard
Installation
TARGET SERVER
WIN-BEH30O0NMK6
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Progress
Waiting for DNS installation to finish
View detailed operation results
Windows Server 2012 R2 domain controllers have a default for the security setting named "Allow cryptography algorithms compatible with Windows NT 4.0" that prevents weaker cryptography algorithms when establishing security channel sessions.
For more information about this setting, see Knowledge Base article 942564 (http://go.microsoft.com/fwlink/?LinkId=104751).
This computer has at least one physical network adapter that does not have static IP address(es) assigned to its IP Properties. If both IPv4 and IPv6 are enabled for a network adapter, both IPv4 and IPv6 static IP addresses should be assigned to both IPv4 and IPv6 Properties of the physical network adapter. Such static IP address(es) assignment should be done to all the physical network adapters for reliable Domain Name System (DNS) operation.
A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found or it does not run Windows DNS server. If you are integrating with an existing DNS infrastructure, you should manually create a delegation to this DNS server in the parent zone to ensure reliable name resolution from outside the domain "info.local". Otherwise, no action is required.
More about installation options
< Previous
Next >
Install
Cancel

- **عندما يكون النظام في شبكة ال Workgroup فإن جميع المستخدمين المحليين يتم تخزينهم في ملف ال (SAM) الموجود في (C://windows/system32/config/SAM), وبعد الانتهاء من ترقية الجهاز الى Domain controller, فإن جميع الحسابات يتم إقتطاعها من ال SAM file ووضعها في قاعدة البيانات الخاصة بال Active Directory (NTDS), وبالتالي تصبح عملية تسجيل الدخول بالشكل التالي (Netnios domain name / username) , كما يلي :**