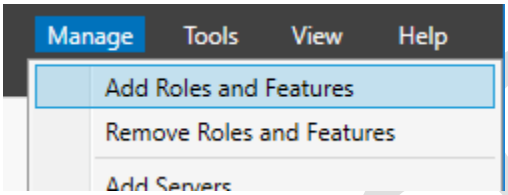
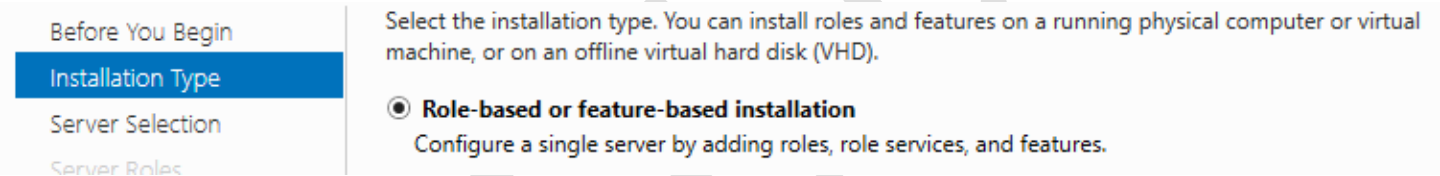
In this lecture we are going to create a Domain Controller by installing the Active Directory Domain Services (AD DS) role. Remember that any server running the AD DS role is considered a domain controller. We are going to add this role to our server and create a new domain called “itflee.com”. This is the name of my website and if you would like you can create any domain name you want. You won’t break any “real” websites since there are no internet DNS servers pointing to the domain that we are about to create. Finally, once we add the AD DS role we will promote the server as a Domain Controller.

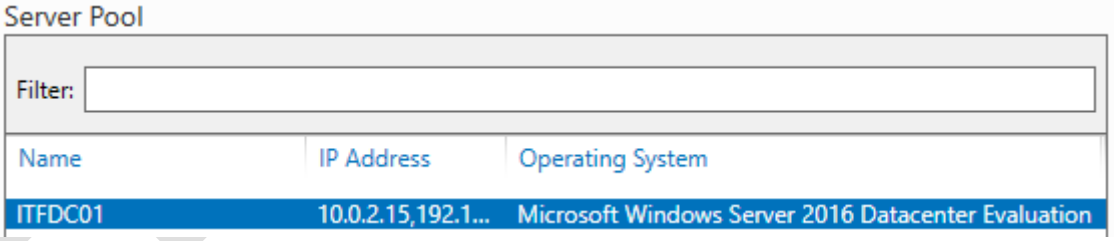
You should already know how to install a server role on the server you are currently logged in to but I am going to cover the steps again. Open Server Manager and select Manage > Add Roles and Features



On the Installation Type Screen leave the default option “Role-based or feature-based…” checkbox check and click next.

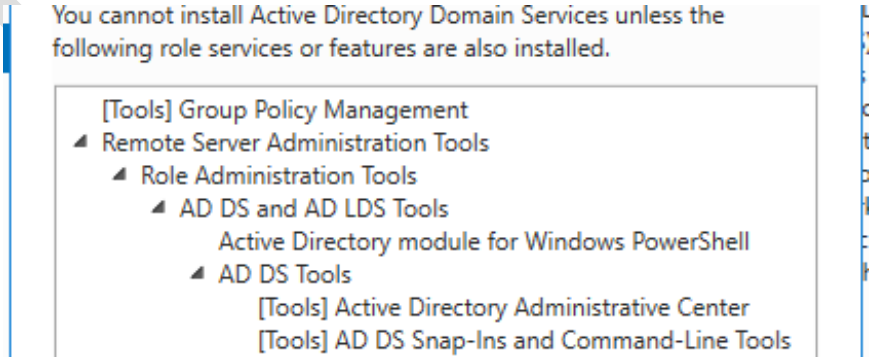


On the Server Selection screen choose the server we built earlier called “ITFDC01” and click next.

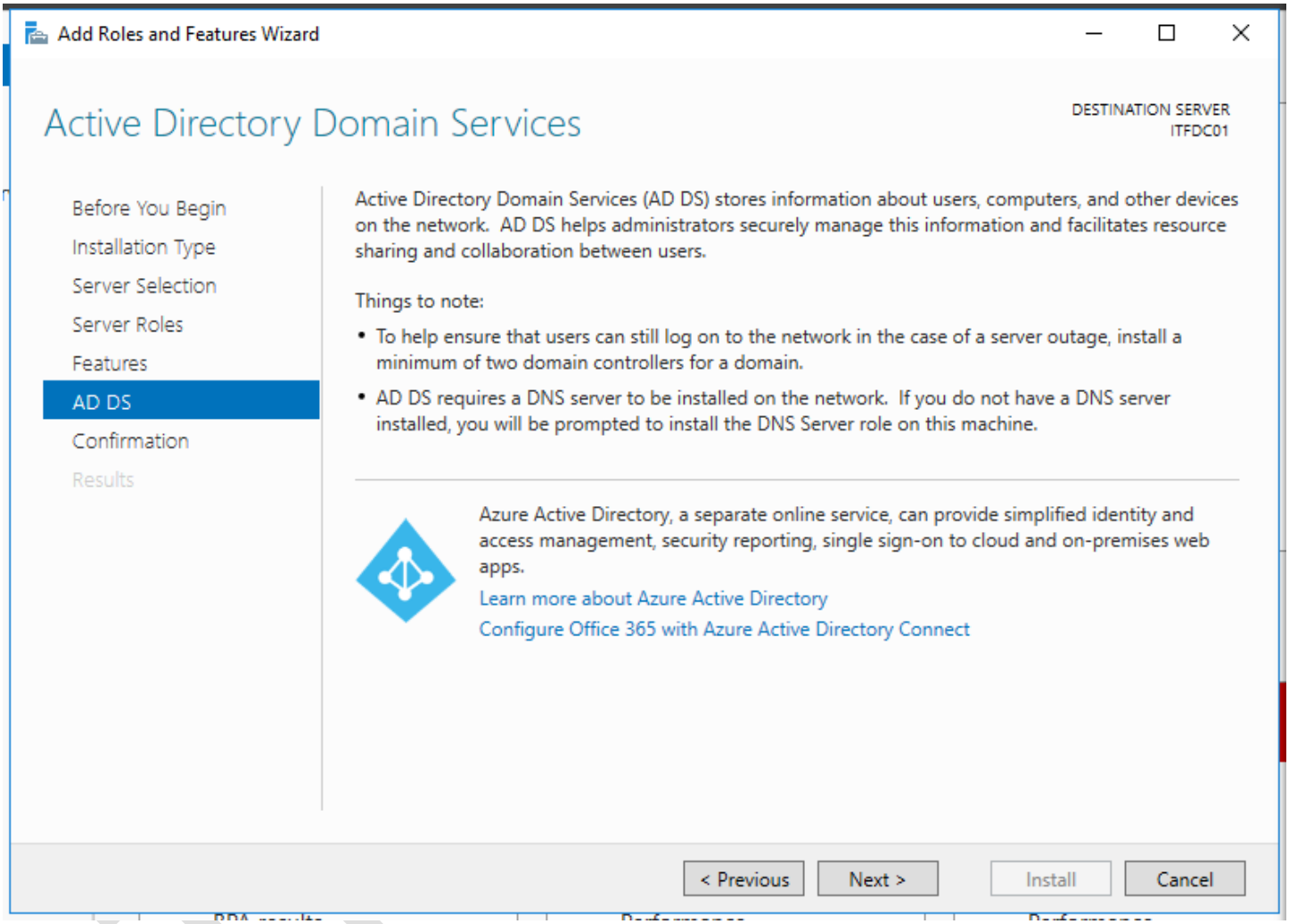


In the server roles list choose the “Active Directory Domain Services” role 

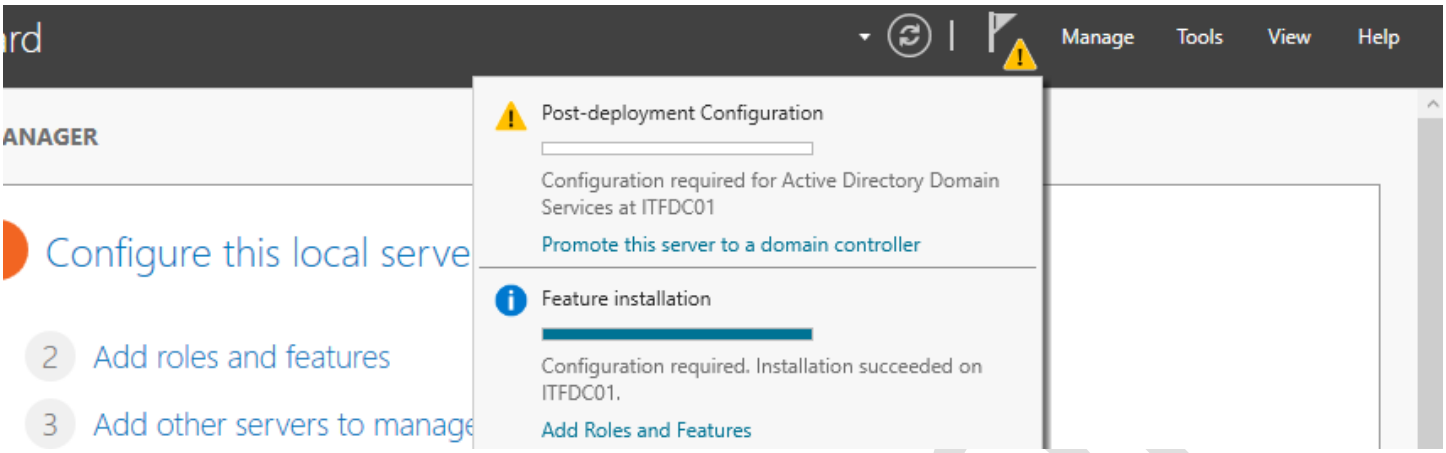
. You will see a popup window stating you cannot install AD DS unless certain role services or features are also installed:



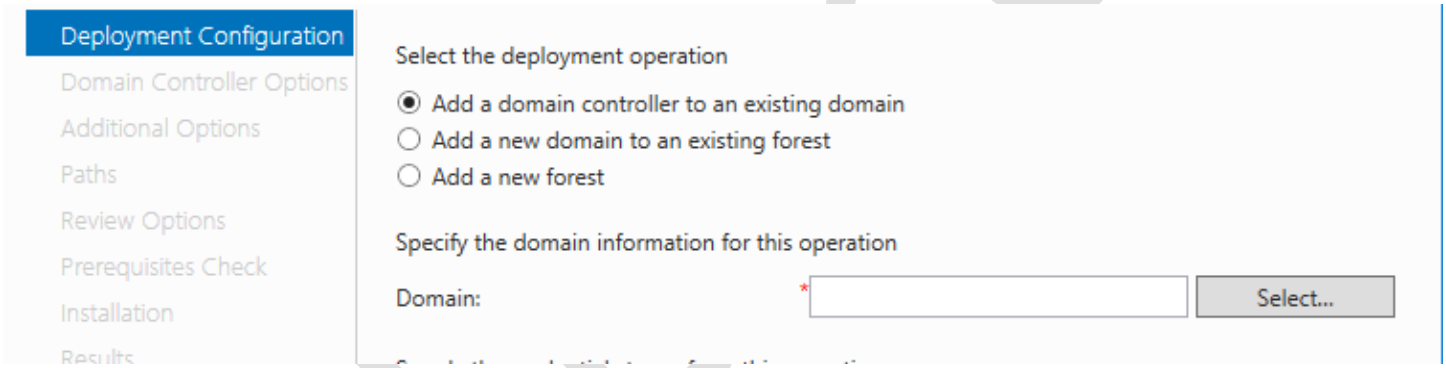
Click the Add Features button [Add Features] and then click Next to proceed to the Features screen. We do not need any additional features as all the required features were already added. Again click Next. Now you will be brought to the AD DS screen. It tells us that we will also need install the DNS role if we do not already have it set up.



Click Next and continue on to the Confirmation screen. Here we can see the roles and features we are about to install. Click Install and wait for the installation to finish. Once the installation is complete you will have post-deployment configuration steps to complete as well:

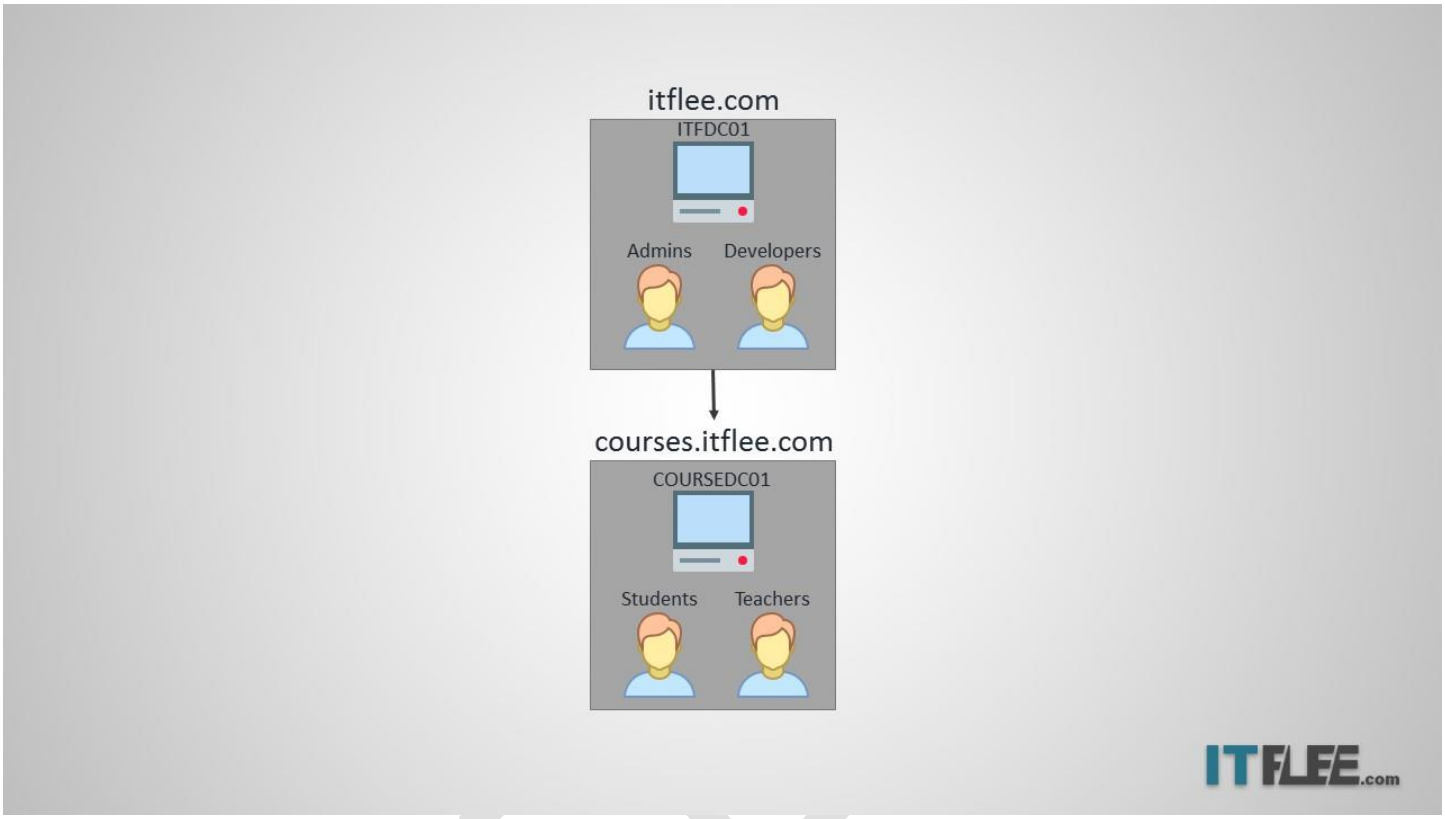


Click the notification flag next to manage and choose “Promote this server to a domain controller”. The AD DS configuration wizard will appear giving us three options:



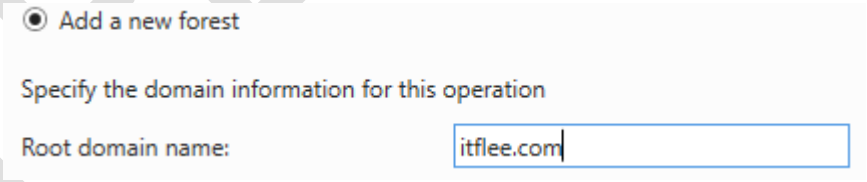
The first option, “Add a Domain Controller to an existing domain” is for adding additional domain controllers to a domain you have already created. This option is not suitable for us now because we have not created a domain yet.

The second option, “Add a new domain to an existing forest” is for adding child (also called sub) domains. Let me explain. We are going to create a domain called itflee.com. If that domain already existed we could create a sub (or child) domain called courses.itflee.com. In theory we could setup this sub domain called courses.itflee.com simply to separate our students and teachers from the administrators who reside in the domain itflee.com.



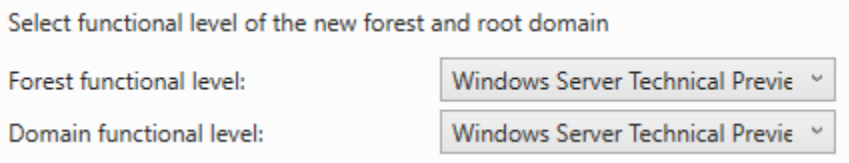
You could configure this sub domain so that Admins from the itflee.com domain can reach into the courses.itflee.com domain, but students and teachers could not reach back to the resources in the itflee.com. Again this is not an appropriate option for us because the itflee.com domain does not yet exsit.

The third option is to “Add a new forest”. This allows us to create and specify a new domain. Choose this option and specify a root domain name.

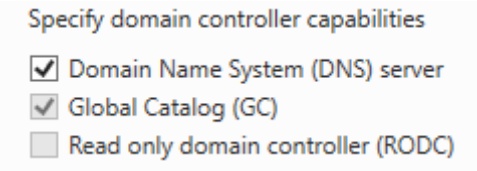


I am going to enter itflee.com and click next. It will take a second before the Domain Controller Options screen will appear to just be patient while it processes. The first two options Forest Functional Level and Domain Functional Level specify which operating system the DC will use. You need to specify the OS you are using (in this case it is Windows Server 2016).

There is a bug with the latest version of Server 2016 where the developers did not configure this screen to show the latest version as “Server 2016” but instead show it as the “Windows Server Technical Preview” so I have to choose this options.



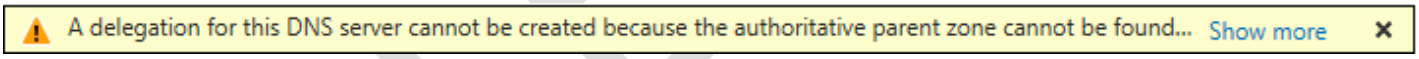
Make sure the Domain name System (DNS) server checkbox is checked. If you remember, when we installed the AD DS role it said that we had to install this in order for the DC to function properly. The Global Catalog option means that the server will list all active directory objects. This is a requirement for a primary domain controller or when we are creating a new domain forest.



If you choose the Read Only Domain Controller option, then the domain controller will not be able to make changes to the domain. We will want to make changes to our domain so do not check this checkbox. Type in a DSRM password and make sure that you either write it down or memorize it.

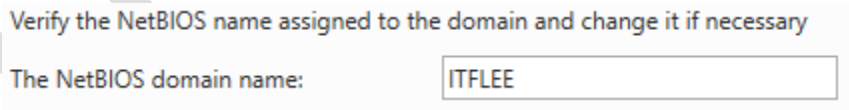
The DSRM (Directory Services Restore Mode) password allows an administrator to take an instance of AD offline for reasons like maintenance or troubleshooting. This is not a commonly used password but you will want to keep "just in case". Click next to proceed on to the DNS options.

On the DNS Options screen you will see a warning about the DNS delegation.

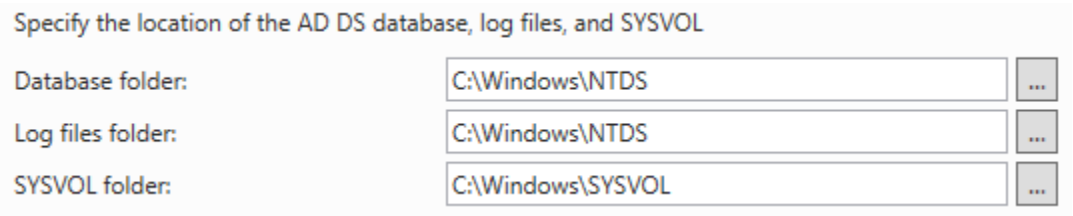


This warning means that people on the internet will not be able to resolve local DNS names on your local DNS server (names like itflee.com or ITFDC01 etc). This is fine because we don't want people on the internet to be able to access our server for security reasons. Click next and proceed on to the Additional Options.

The NetBIOS domain name is populated for us as ITFLEE. The NetBIOS name is an abbreviate of the Fully Qualified Domain Name (FQDN) which is itflee.com. I am going to leave this at the default of ITFLEE and click continue.



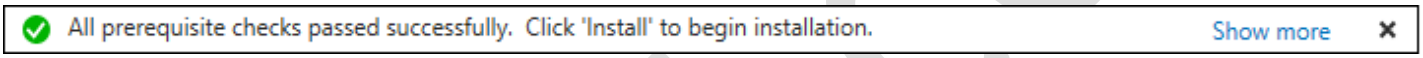
On the Paths screen we can see the default paths chosen for the folders that are required by AD DS. If you would like to choose an alternate drive you can do so by clicking the "…" button  and choosing the alternate path. I recommend that you leave them at the default setting and click next.



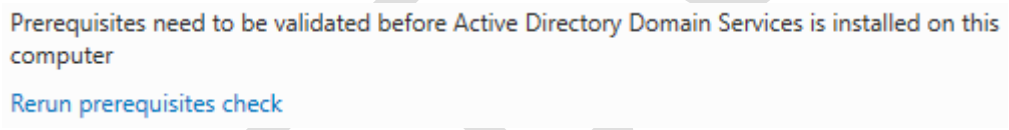
We are brought to the Review Options screen where we can see all of the options we have chosen so far. If you would like you can click the "View script" button 

and you will be presented with a powershell script that you can save in order to later execute and quickly complete the wizard with the same settings we just used. Close the powershell script and click next.

Now we are brought to the "Prequisites Check" window. The wizard is going to go verify that the server is ready to be promoted as a DC. This will take a few minutes before it is ready so just be patient wait for it to complete the checks. Once the checks complete at the top you will see that all prerequisite checks have passed:



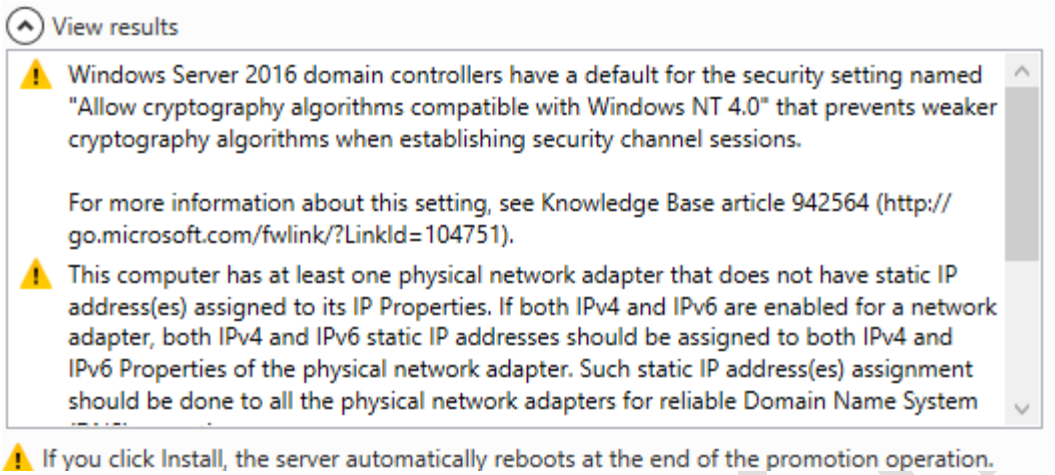
If you have errors, you can address the errors (Google is your friend) and click the rerun prerequisite checks text:



Under the view results window we can see there are various warnings. None of these are critical but it is worth reading through them. We can see that the first one is a security setting stating that anything with crypography not compatible with Windows NT 4.0 will be blocked. This is not an issue for us because we are not using old servers or old technology.

The second is in regards to our first networking adapter not having a static IP address. This is because the first adapter is connected to our NAT adapter and will not be used for our local domain. This can be ignored.

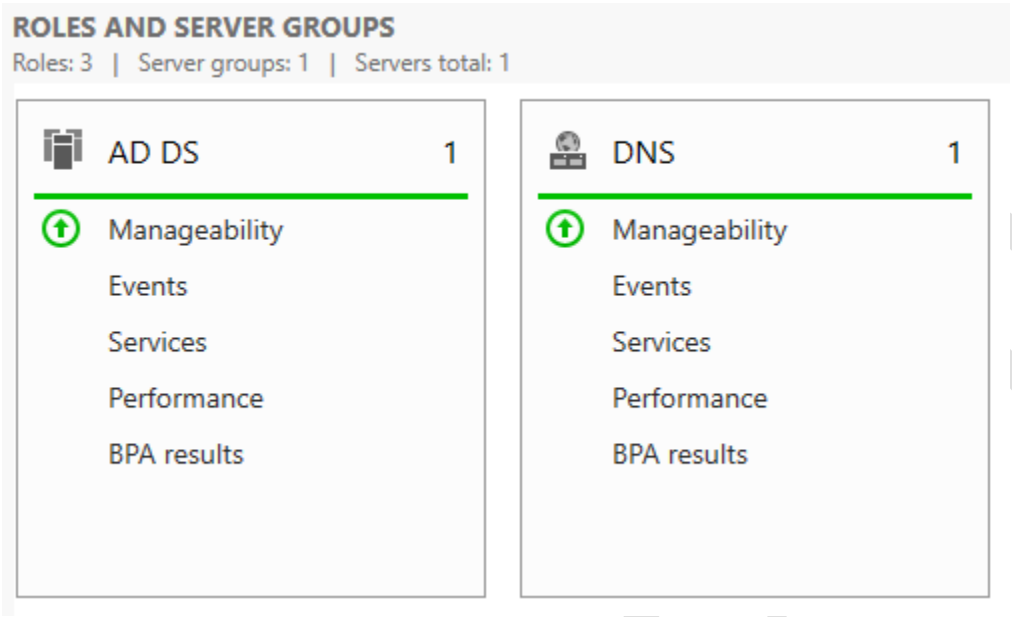
The third warning is about the DNS delegation. Again we do not care if people on the internet can resolve our DNS records within our network.



Click the install button and wait for the installation to complete and the server to reboot. This can take a good while depending on the speed of your server so you will need to be patient while it works. I am going to speed up this video so you don't need to sit and watch the entire installation.

Once the installation completes and the server reboots, press ctrl+alt+del to log in. The first thing you will notice is the NetBIOS name of our domain preceeds the user account we are logging into (in this case, "ITFLEE\Administrator"). This is in the format of [Domain Name]\[Domain Username].

If we had multiple domain names we could specify a different domain name by typing the name of the domain we want to use followed by a backslash and the name of the user account you want to log into. Type in the password you used to create the administrator account when you installed the server and log in. Under the server manager you will see the new server roles of AD DS and DNS.



We have successfully built a Domain Controller. Great job on that and I will see you in the next lecture!