A7010E Homework 2

Nico Ferrari (nicfer-0@student.ltu.se)

September 22, 2020

1. MiHis a Small and Medium-sized Enterprise (SME)that offers remote medical services such as online diagnosis, medical image analysis, and remote health monitoring. MiH has three sections, namely, management where level 2 of assurance is needed, a nursing section where level 3 of assurance is required, and physicians'section that needs level 4 of assurance. You have been appointed to decide a suitable authentication method(s)for each section, and you need to include the following points in your report to MiH:

---

according to NIST, Level 2 provides single factor remote network authentication.This level of authentication introduces the identity proofing requirements and a moderate risk is associated with wrong authentication. A person will be successfully authenticated after proving its entity through a secure authentication protocol, showing that the entity has *control* of an agreed credential.

Different methods have been adopted during the last decades, like biometrics data recorded during the "enrollment" phase of the employee. This results a really good alternative to passwords, in fact, users do not need to remember complex password which, usually, have to be changed frequently. Passwords, moreover, are often reused by the users in different contexts and , in order to easily remember them, are often common word which can be exploited with rainbow tables or/and some social engineering.

The problem of biometrics, as mentioned in the paper "*Recent Trends in User Authentication - A Survey*", is that once they are exploited, there is no way to recourse them.

Always according to NIST, level 2 of assurance allows also:

- Look-up Secret Tokens, storing a set of secrets and is used to look up the secret based on a prompt.
- Out of Band Tokens, received over a separate channel and presented to the authentication protocol.

I suppose that the management section needs to authenticate several times to the company platforms to, for example, read emails or other confidential data related to their business. In order to provide a level 2 of assurance, I would suggest biometric authentication using fingerprints or a Out of Band Token authentication protocol. I also assume that all the employees of the company have registered during enrollment a phone number or have a smartphone with phone number for work assigned from the company. In order to avoid problems related to stolen/compromised biometric data or lookup tokens , I propose an Out of Band authentication protocol, where a one-time PIN will be sent secretly by SMS to the phone number registred during enrollment when the employee wants to access the online platform. Then, the PIN code has to be entered in the platform in order to perform the authentication, as described in the following steps:

- Enrollment phase: the employee register a phone number. During this phase it is necessary to make sure that the number is correct and available. Moreover a email address or username is set.
- Employee start the login phase through the online platform: In this phase, the employee which wants to authenticate himself goes to the online platform and tries to login with his username or email. The central server will send a SMS to the registered number with a 6 digits long PIN code.
- Authentication phase: after sending the SMS, a popup window will appear asking for the PIN code.The employee enters the PIN code in the platform and, if accepted will be authenticated otherwise a new

PIN will be requested. The PIN code will be sent maximum 3 times, and after that the account will be blocked. To reactivate the account, the employee must contact the IT Department of the company and Identify himself in person.

The PIN Code and credential must be sent to the server using an encrypted channel and, moreover, a certificate from the server with his public key must be shared. To encrypt the message to the server, the server public key can be used. Level 3 of assurance is when substantial risk is associated with erroneous authentication. Since in Level 2 there is no verification of the identify, in level two more factors are involved in the authentication. Often, biometric data or passwords are associated with a second factor authentication, like a Out of Band Token, as show before. Since the protocol for LoA 2 is based on this last one, In order to not increase the complexity of the authentication protocols, i suggest to use this protocol together with another authentication factor. Biometrics authentication would increase the security without big overhead on user side. Nowdays, biometrics devices are included in a large variety of devices including smartphones. In this case, the smartphone is used already a s out of bound device, and using the biometrics device of it would mean having to authentication processes from the same device. A solution would be giving to the employees "personal" biometric devices to use instead. Using passwords as second factor is frequently used as well, but as mentioned in the beginning, passwords lead to many other different weaknesses.

In the company nurses are required to have LoA 3 and I assume that during enrollment, a working laptop or workstation is provided to them. I also assume that nurses are usually do not have experience and knowledge in Cybersecurity and need an easy way to securely authenticate themselves in order to access critical data. TO achieve the goal, I propose the following protocol:

- During enrollment, a laptop is assigned to the employee. The certificate of the server with its public key will be stored in the computer and also the public key (from a key pair generated ad the moment on the laptop) of the computer will be stored on the server thought a secure channel.
- An account will be created and secured by a PIN code and biometric key (in case there are problems with one of them) and the keys stored in the computer will be encrypted using the registred key.
- In order to login to the platform, the user must log in to his work-computer account using the PIN or biometric data and after that it will follow the same procedure explained for the managers but encrypting the received token with the user's private key and server's public key.

In this way, we can assure that the users access from the laptop assigned at work because the keys used are encrypted and are accessible only from the laptop. The access to the laptop will not be enough to authenticate the user into the platform, and a One-Time-Use pin code sent by SMS will be necessary to be authenticated.

Finally, LoA 4 is used when a high risk is associated with erroneous authentication. LoA4 provides the highest level of entity authentication assurance defined . In order to authenticate itself, a user must proof the possession of a key through a cryptographic protocol. This level requires a physical token and strong crytographic authentication of all parties and all sensitive data transfers between the parties.

For this purpose, cryptographic usb keys are being developed since only “hard” cryptographic tokens which cannot readily be copied are allowed. An example is the Yubico key with fingerprint sensor integrated. I would suggest to use this for the physicians' section instead of an account locked with pin code or biometric's. Moreover, public key of the server and the keypair for the user could be stored and encrypted in the USB using the internal crypto hardware. In this way even if the USB stick or the phone are stolen or compromized, it will be not possible to get authorization. Moreover, the authentication process is kept simple and relatively fast, removing the use of password and trying to overcome to the users' errors. The drawbacks are the costs, in fact these Cryptographic hard tokens are expensive and the company has to provide laptops for some of the employees. I assume that the nurses do not need high computational power or specific and expensive

resources in their workstations, so the cost of the hardware will not be expensive and the budget of the company can afford it.

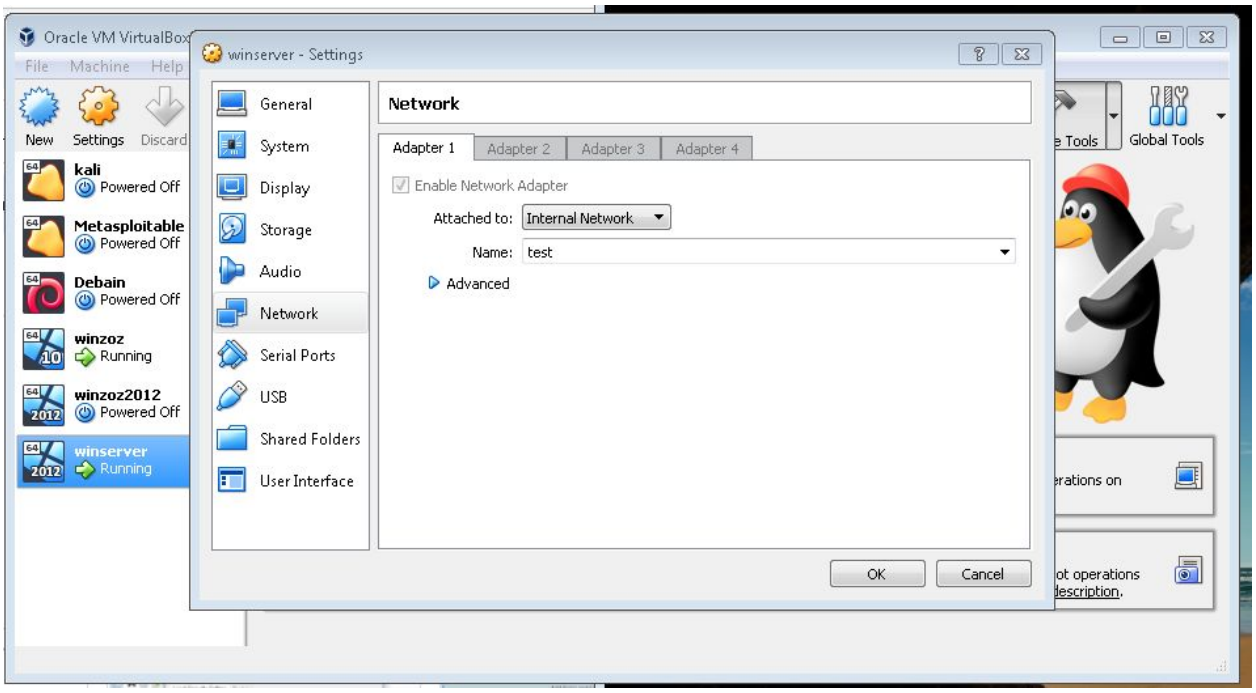
2. Have you done the lab assignment number (2)

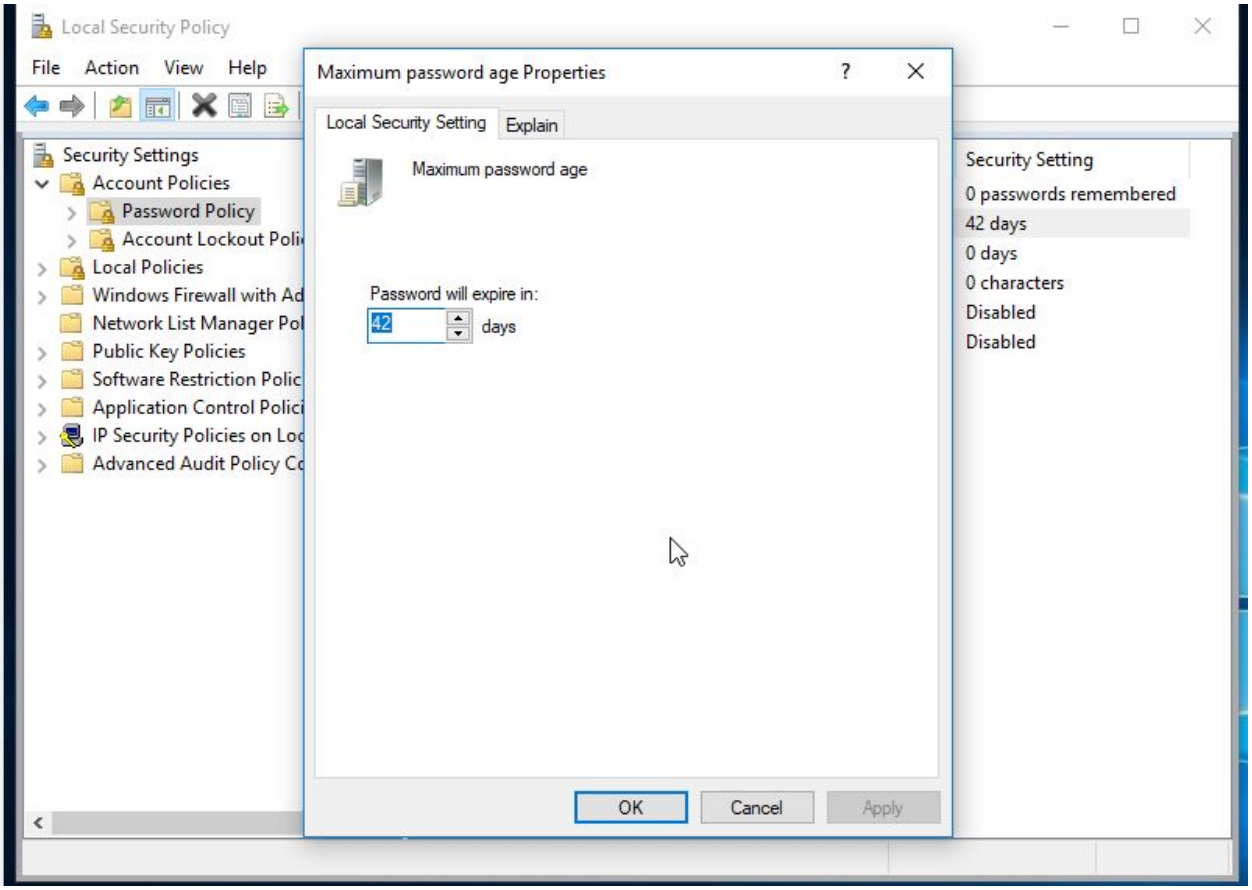
yea I have done it. Described in the other PDFs.

3. What is your own reflection on the entire week of the course?

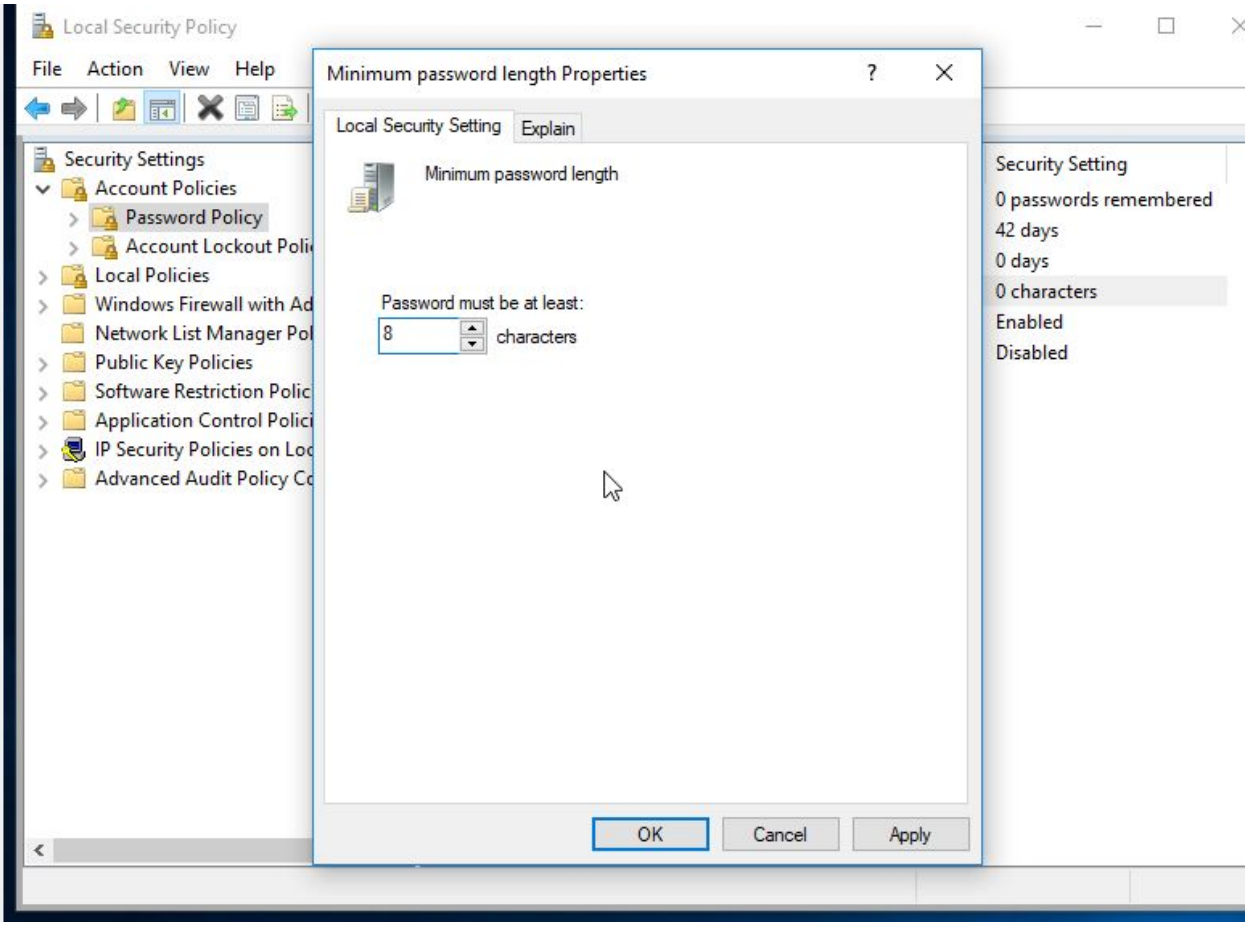
It is getting always more interesting. For this assignment many problems with VMs occurred and working with the othe VMs and this delayed all the assignment (but my fault because I started late). The Theoretical questions make me discover new interesting aspects and protocols of cryptography. So overall I think that the course is really interesting and well done and didn't expected such a well organized practical session to be honest.

After installing the two VMs, it is important to make sure that they are in the same network, in this case: test.



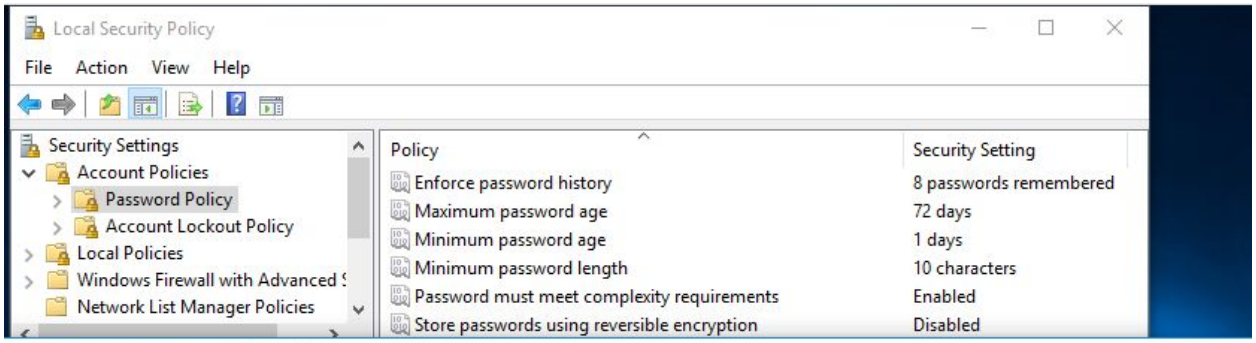


password policies changed using GUI:



Password policies changed using prompt:

```
C:\Windows\system32>wmic UserAccount set PasswordExpires=True
Updating property(s) of '\\DESKTOP-NCKOVP8\ROOT\CIMV2:Win32_UserAccount.Domain="DESKTOP-NCKOVP8",Name="Administrator"'
Property(s) update successful.
Updating property(s) of '\\DESKTOP-NCKOVP8\ROOT\CIMV2:Win32_UserAccount.Domain="DESKTOP-NCKOVP8",Name="DefaultAccount"'
Property(s) update successful.
Updating property(s) of '\\DESKTOP-NCKOVP8\ROOT\CIMV2:Win32_UserAccount.Domain="DESKTOP-NCKOVP8",Name="Guest"'
Property(s) update successful.
Updating property(s) of '\\DESKTOP-NCKOVP8\ROOT\CIMV2:Win32_UserAccount.Domain="DESKTOP-NCKOVP8",Name="ltu"'
Property(s) update successful.
```



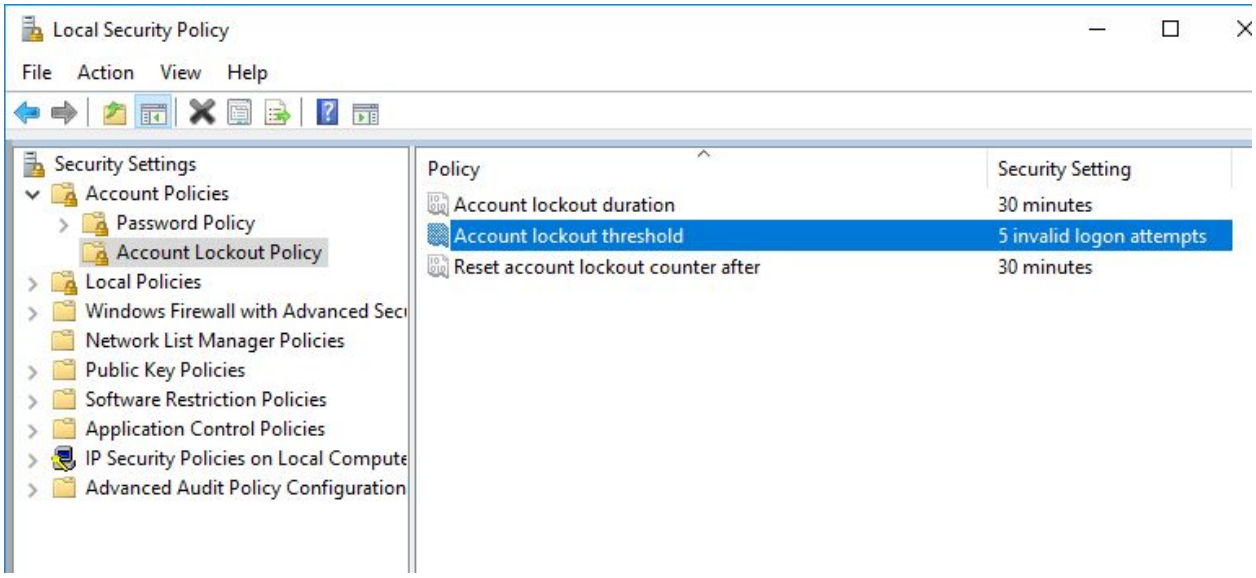
Administrator: Command Prompt

```
C:\Windows\system32>net accounts /minpwlen:10
The command completed successfully.


C:\Windows\system32>net accounts /maxpwage:72
The command completed successfully.


C:\Windows\system32>net accounts /minpwage:1
The command completed successfully.


C:\Windows\system32>net accounts /uniquepw:8
The command completed successfully.


C:\Windows\system32>net accounts
Force user logoff how long after time expires?:       Never
Minimum password age (days):                          1
Maximum password age (days):                          72
Minimum password length:                              10
Length of password history maintained:                8
Lockout threshold:                                    Never
Lockout duration (minutes):                           30
Lockout observation window (minutes):                 30
Computer role:                                        WORKSTATION
The command completed successfully.
```

It was not possible to change the same password policies for a specific account using the command nt user ltu. In the manual different policies where specified, i.e. */expires*

```
C:\Windows\system32>net user ltu /expires:jan,10
The command completed successfully.


C:\Windows\system32>net user ltu
User name                    ltu
Full Name
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              1/10/2021 12:00:00 AM
```

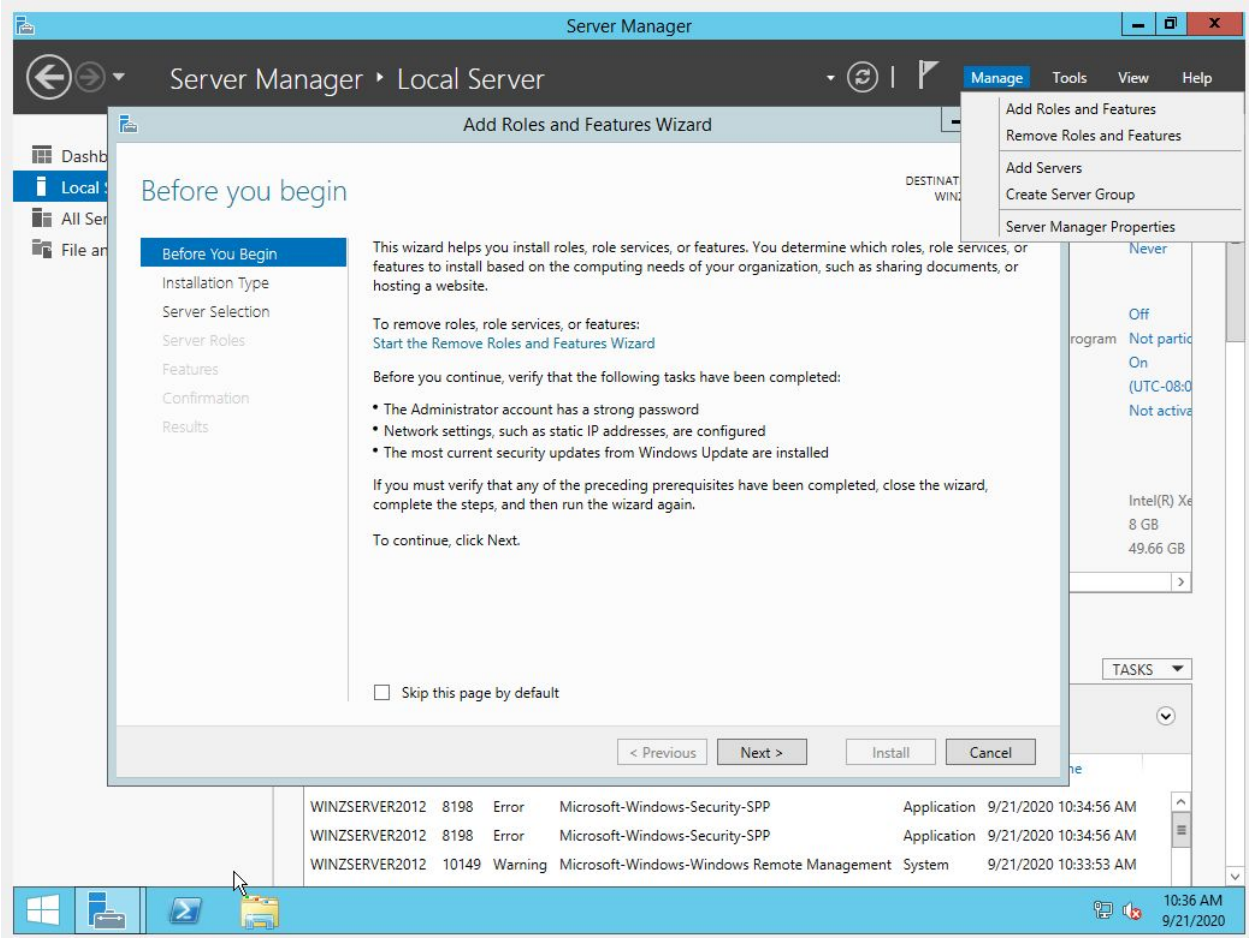
change Account Lockout Policy:



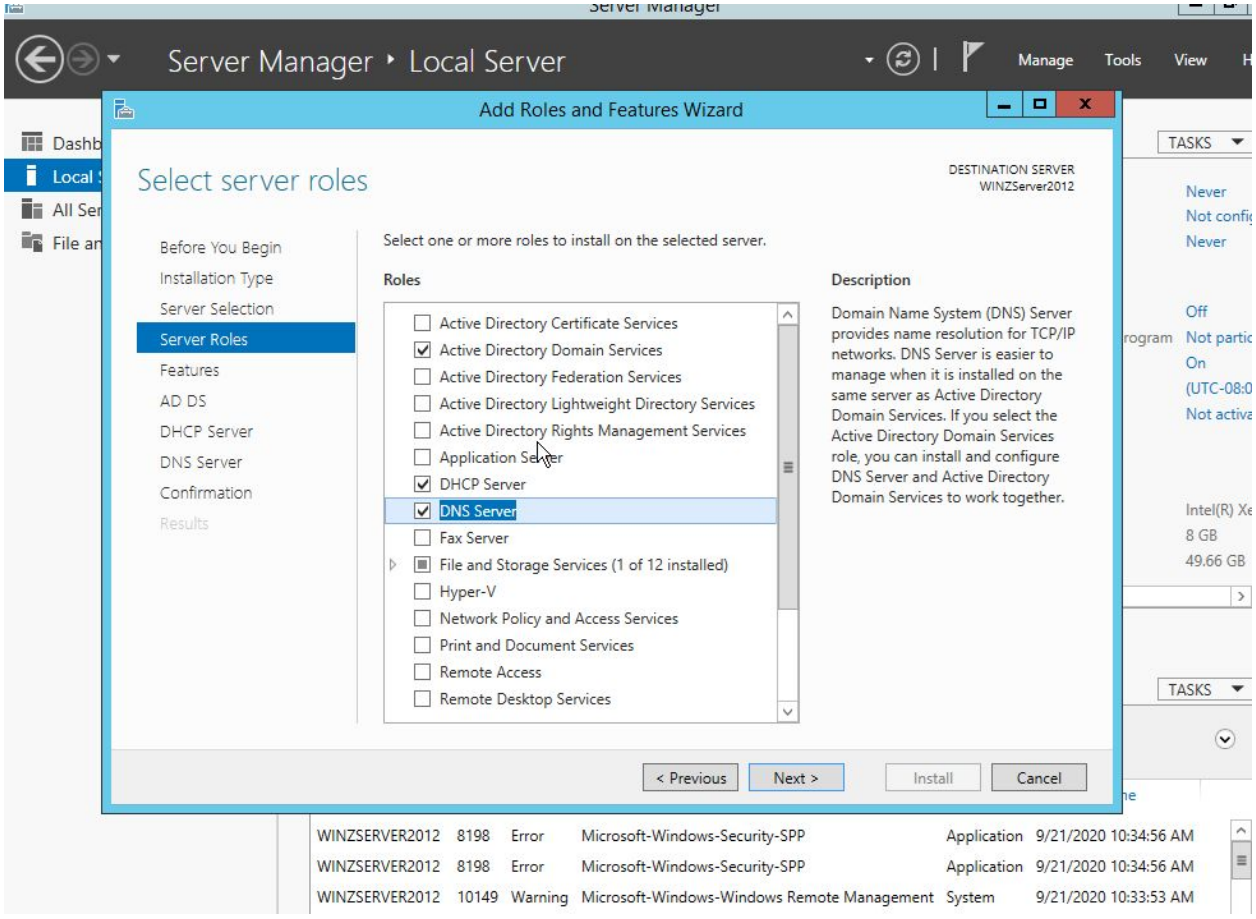
Part Four:

After installing Windows Server 2012, it is necessary to install the different services, in this case: active directory domain controller (AD CD), DHCP, DNS.

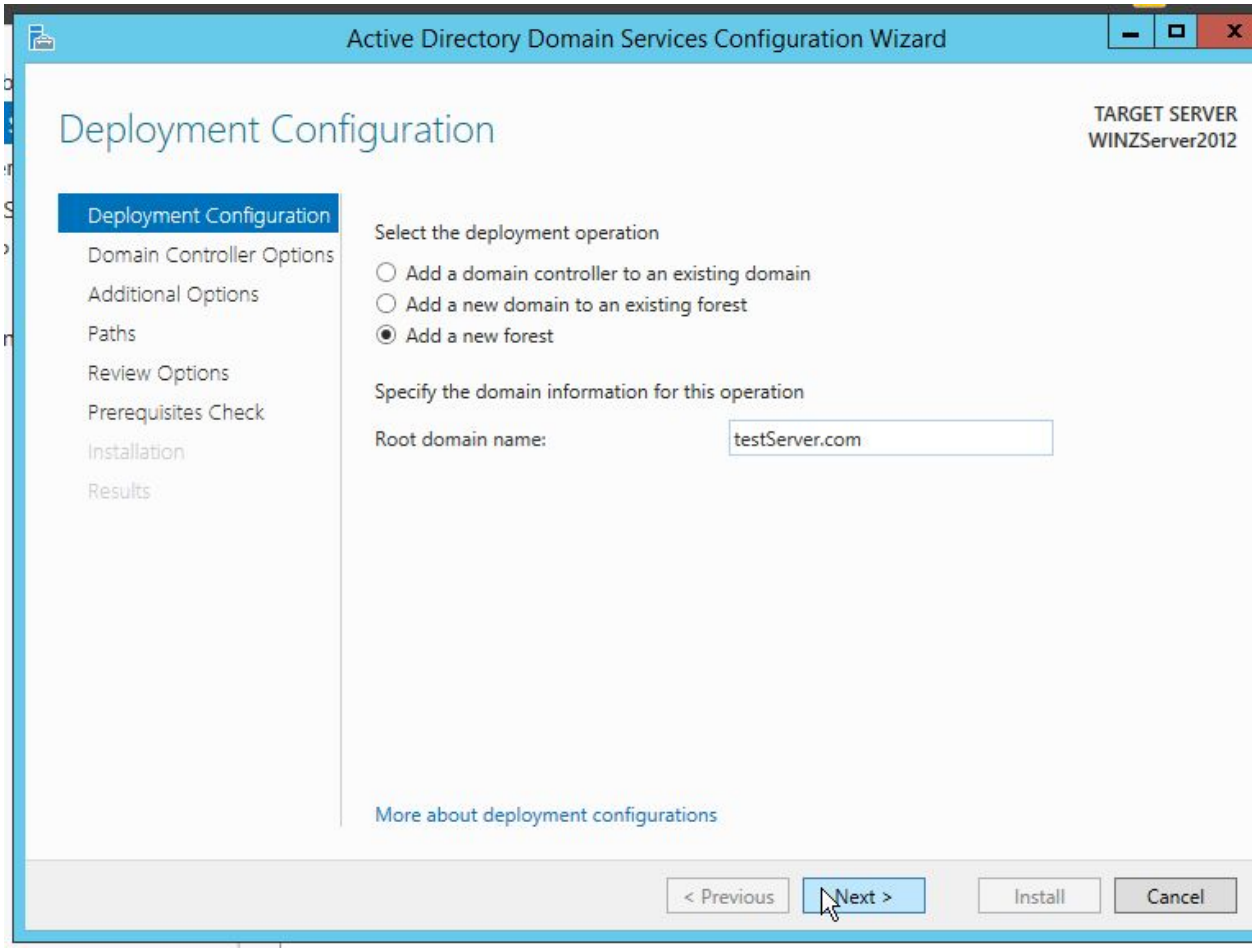
In order to do so, we navigate to ***Manage -> add roles and Features.***

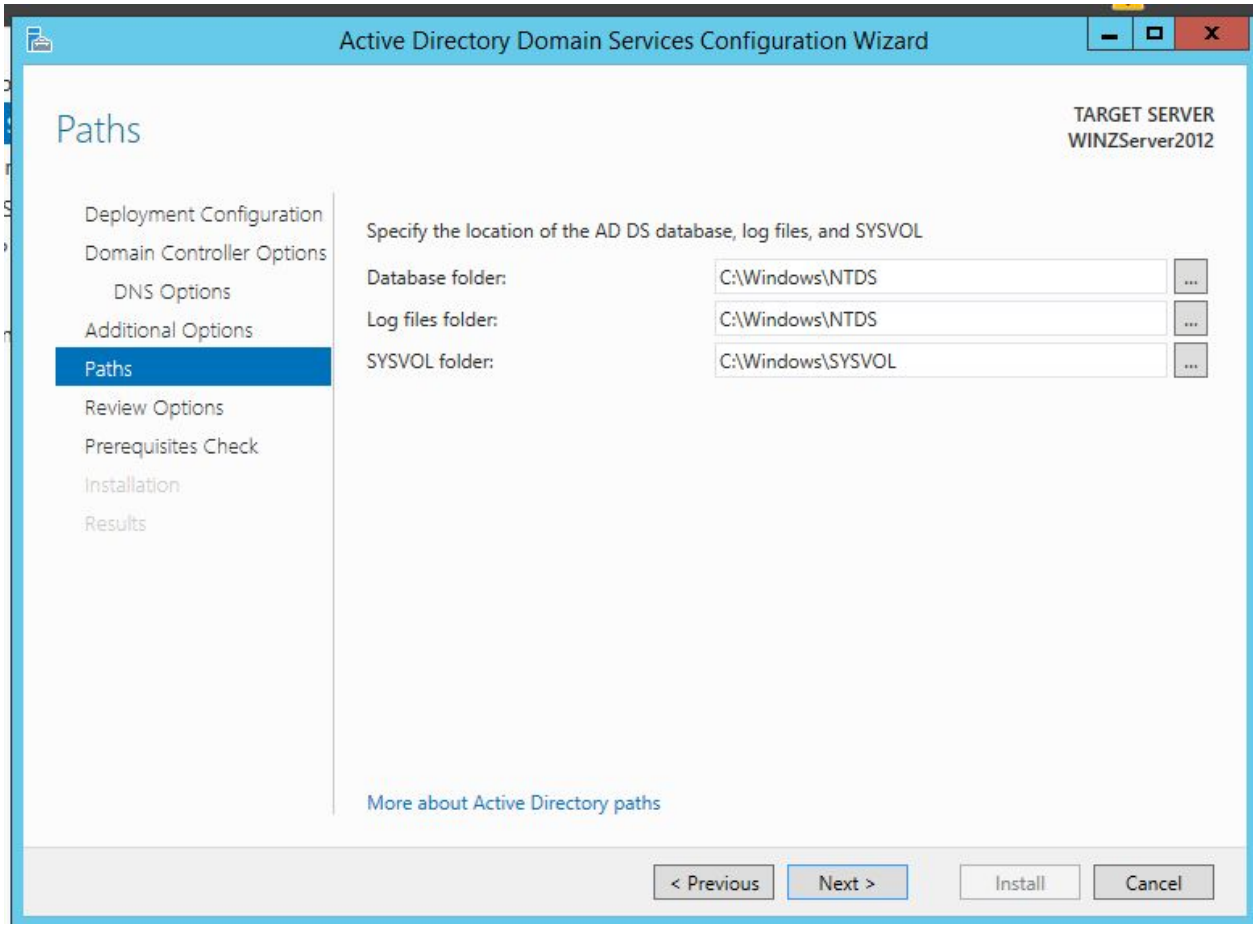


From there we can select the roles we want to add a select the ones shown in the next picture.



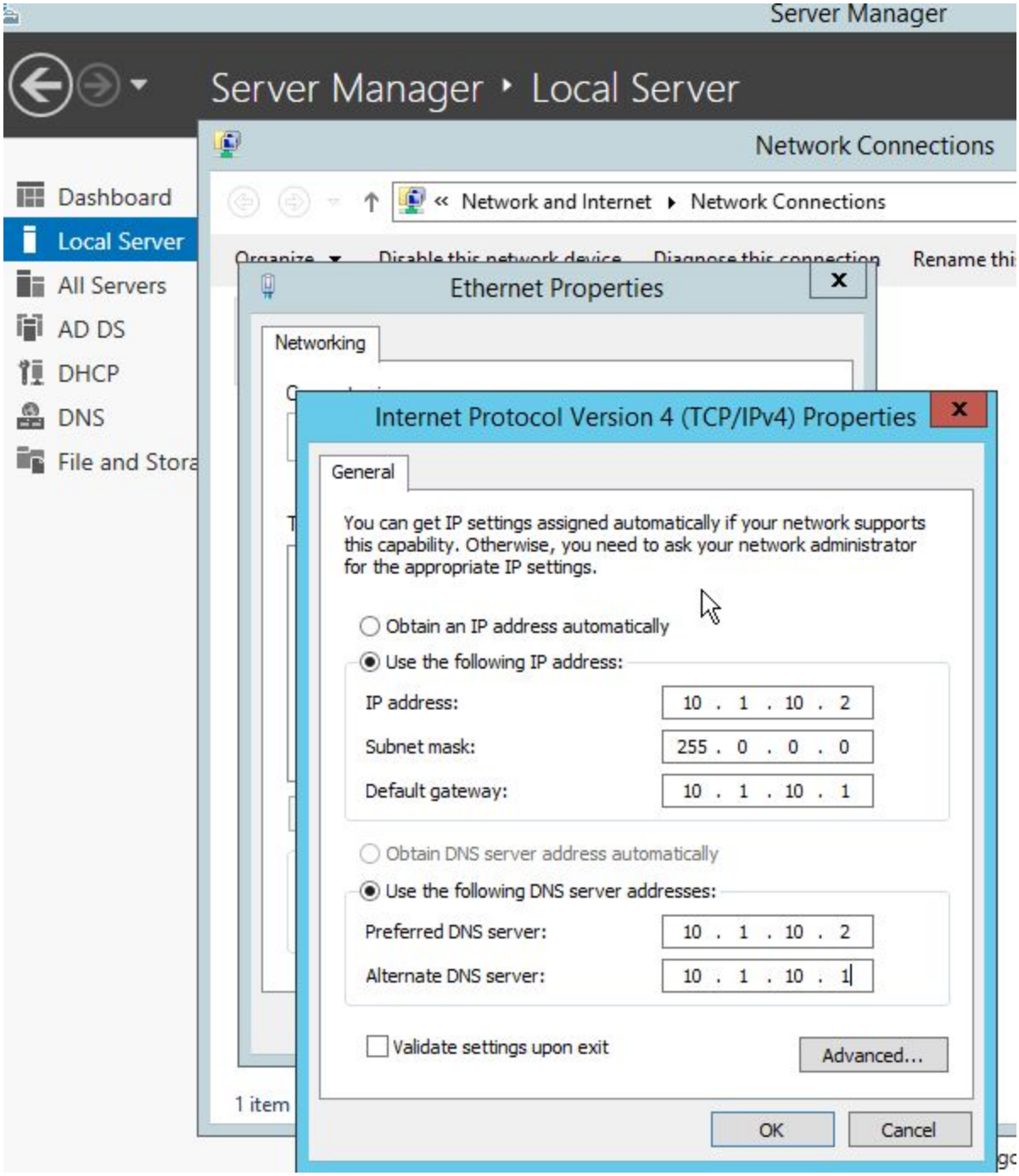
After being installed, it will be suggested to us that we have to promote the server (to remember more easily, I changed the name to WINSERVER) to an DC. Clicking there, will be necessary to add a new forest (there are no other domains) and setting a domain name.


Active Directory Domain Services Configuration Wizard
Deployment Configuration
TARGET SERVER
WINZServer2012
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
Root domain name:
testServer.com
More about deployment configurations
< Previous
Next >
Install
Cancel

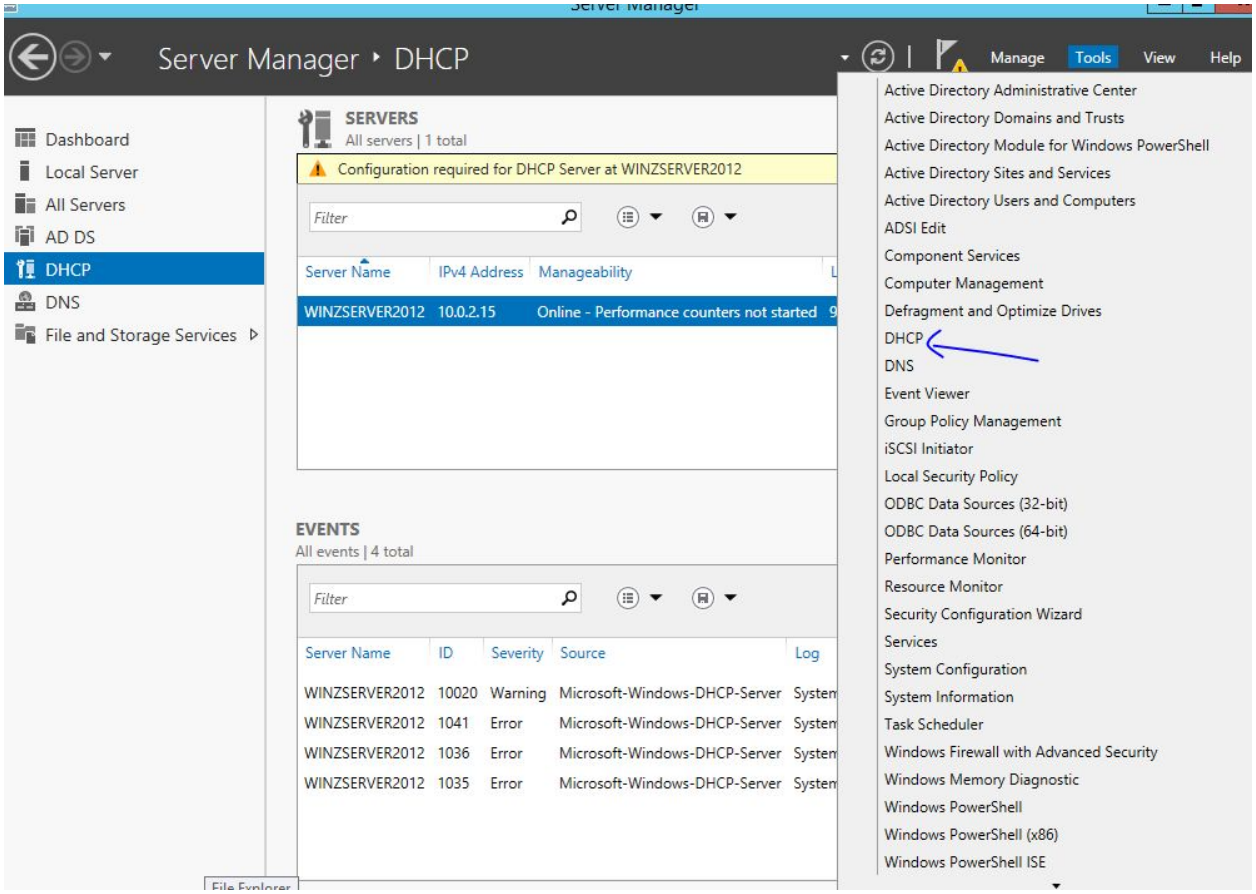


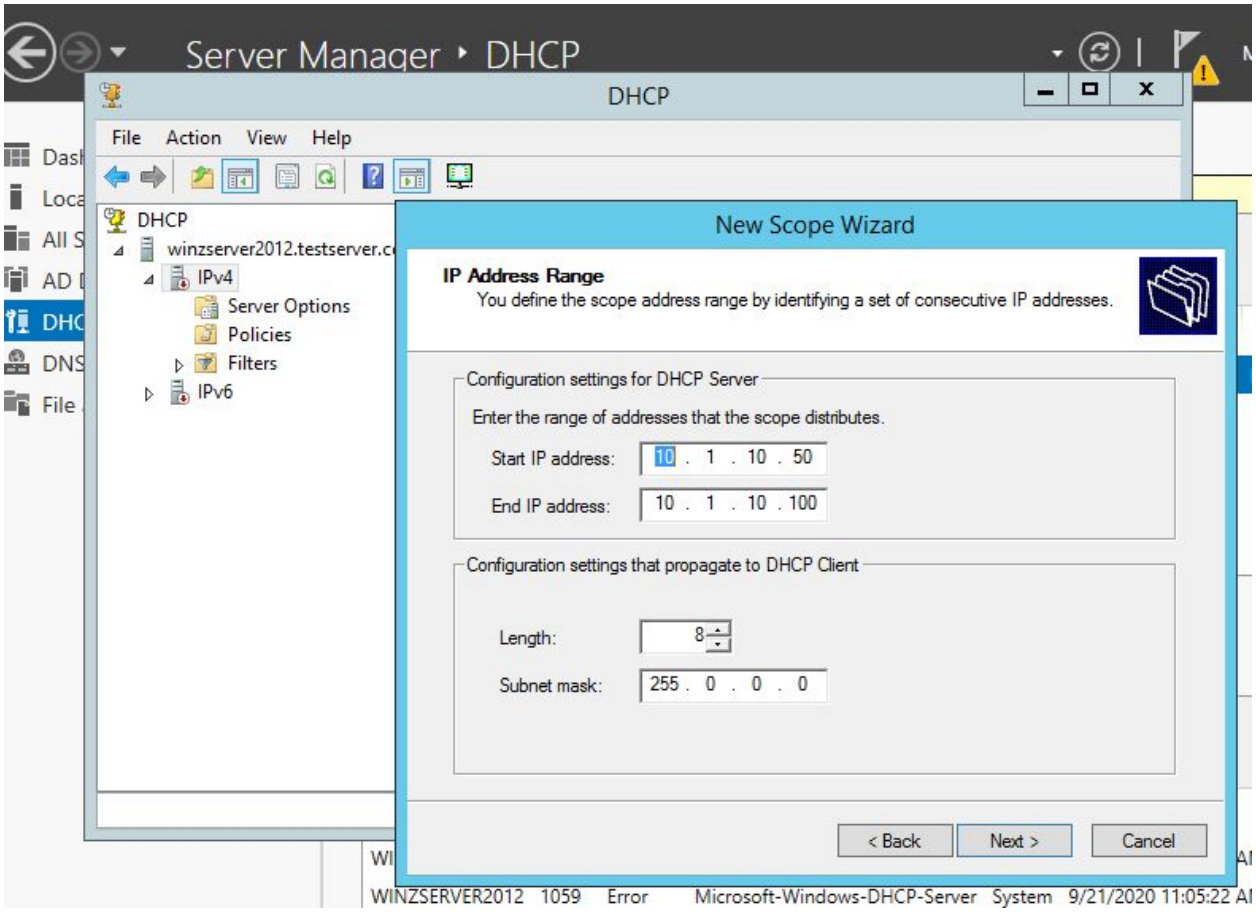
a local IP address for the server has to be set and the same for the DNS server. The first DNS server will link to the server, in order to resolve its IPs, and then a second one pointing to the

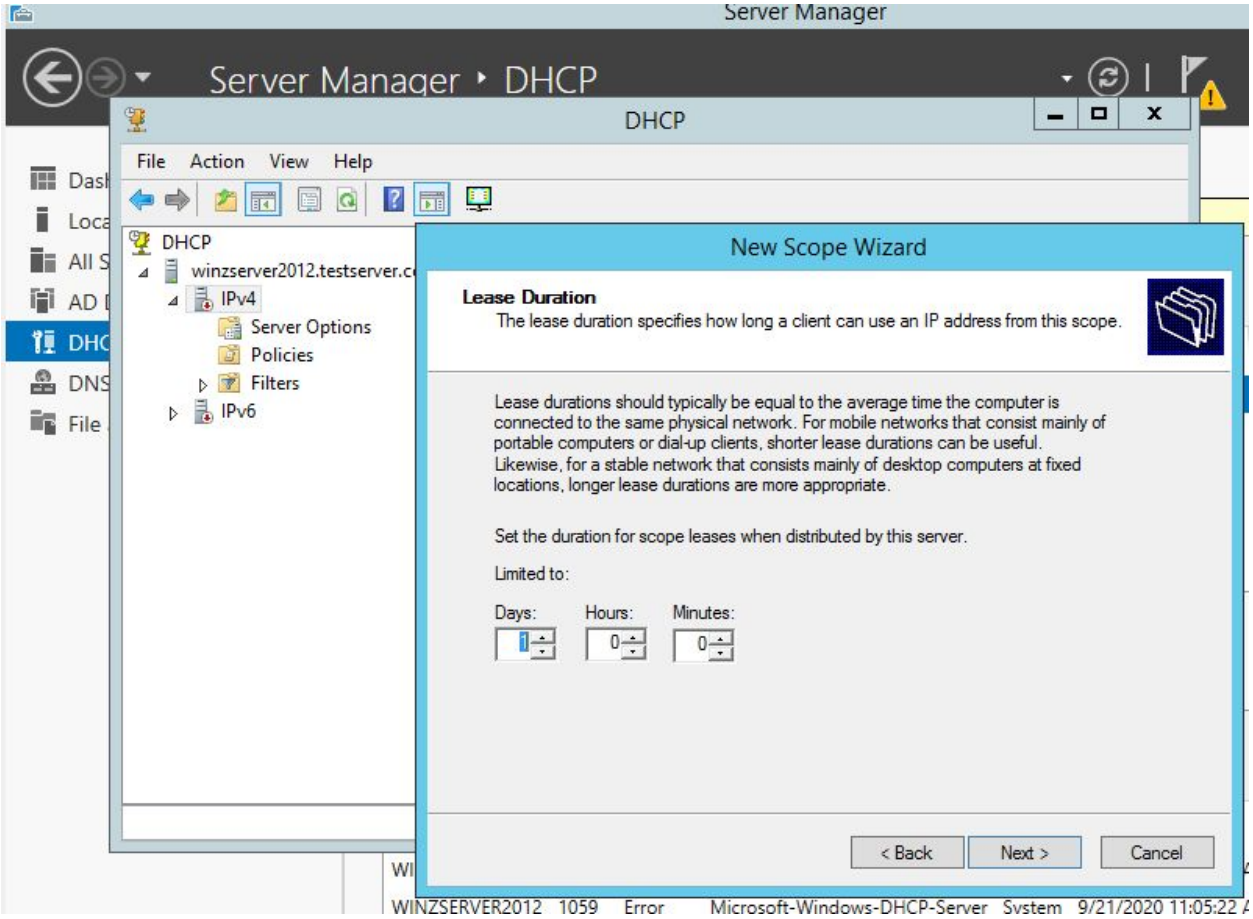
gateway.

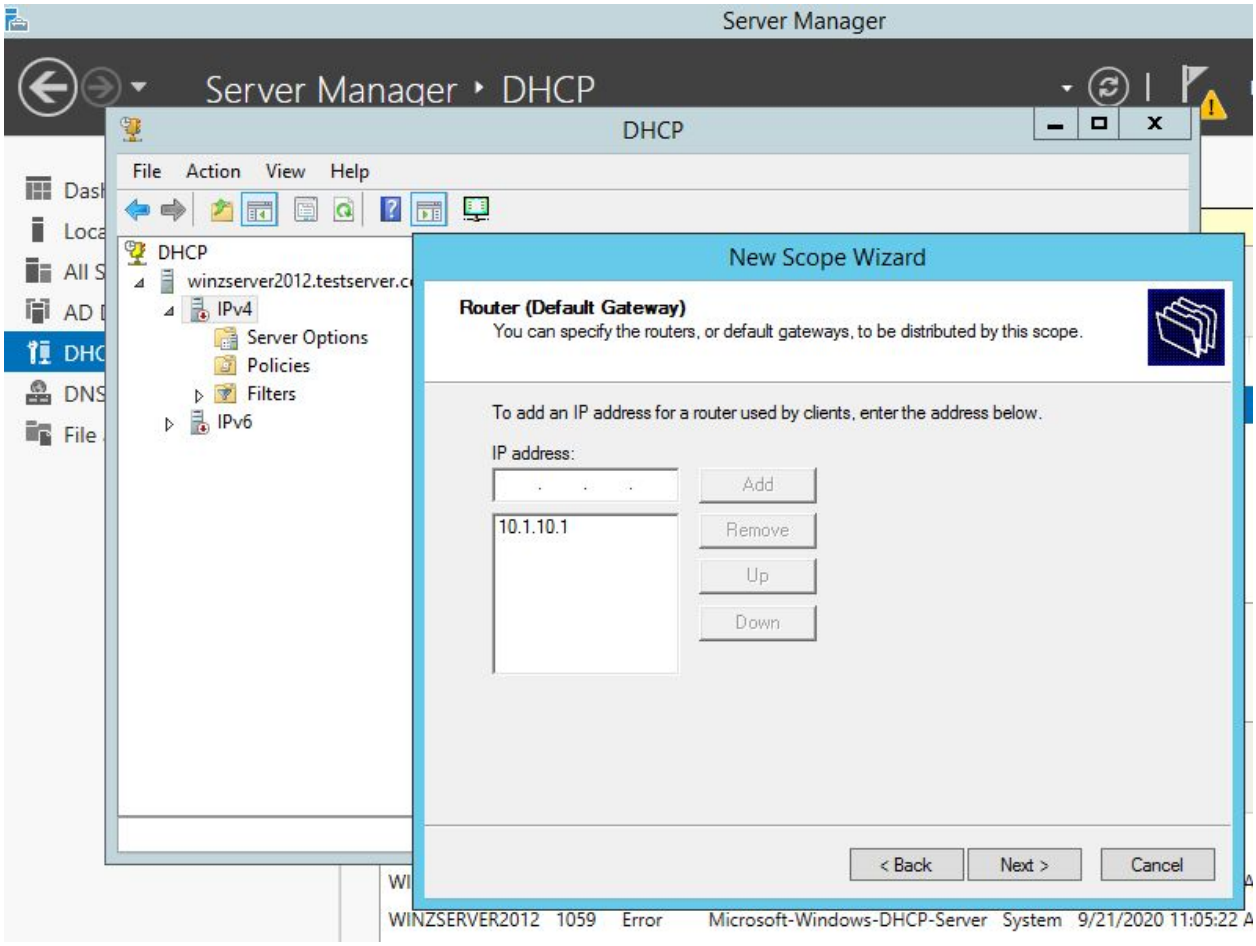


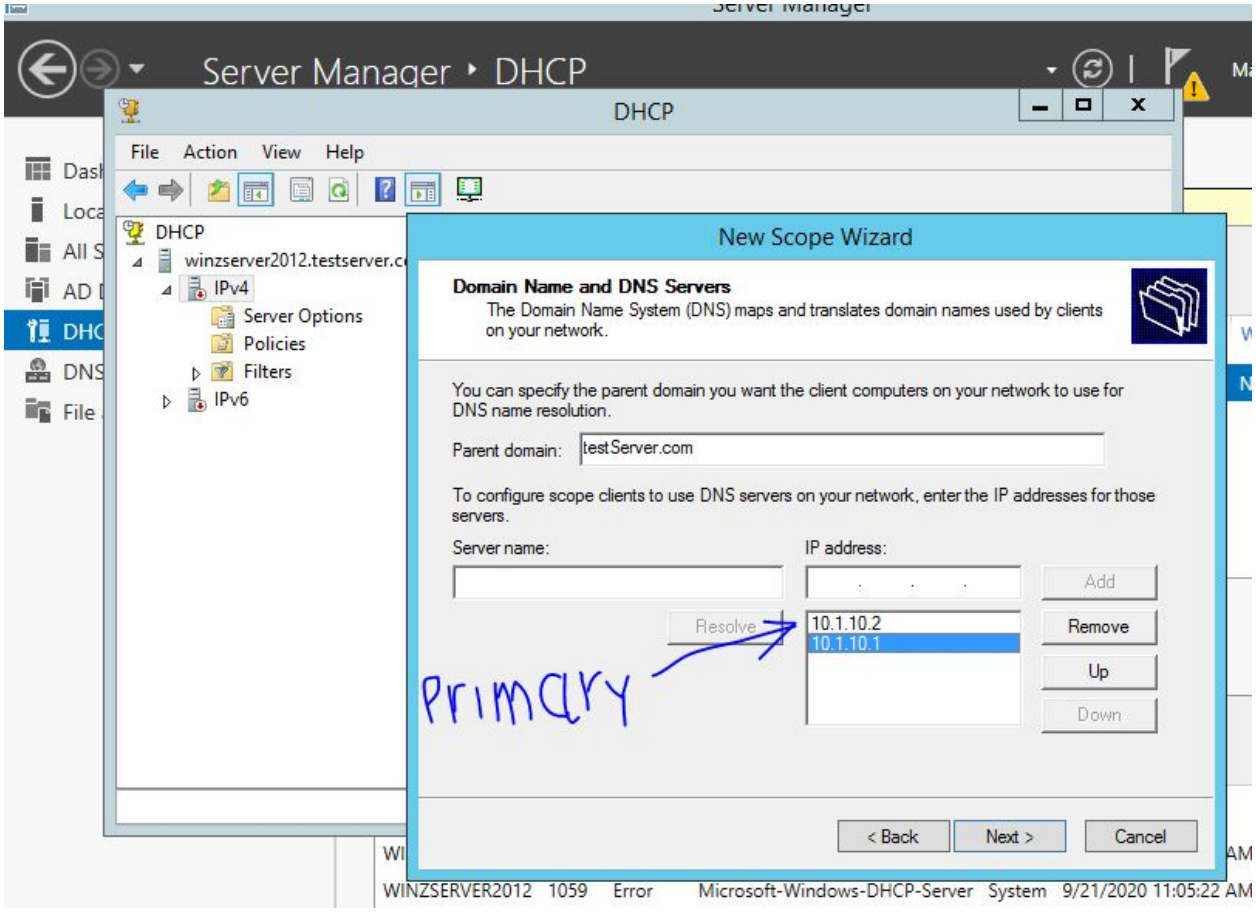
To configure the DHCP, we go to Tools and DHCP and then we can set a new scope in order to set the rules on how the IP addresses will be assigned.


Server Manager
Server Manager ▸ DHCP
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
AD DS
DHCP
DNS
File and Storage Services
SERVERS
All servers | 1 total
Configuration required for DHCP Server at WINZSERVER2012
Filter
Server Name
IPv4 Address
Manageability
WINZSERVER2012
10.0.2.15
Online - Performance counters not started
EVENTS
All events | 4 total
Filter
Server Name
ID
Severity
Source
Log
WINZSERVER2012 10020 Warning Microsoft-Windows-DHCP-Server
WINZSERVER2012 1041 Error Microsoft-Windows-DHCP-Server
WINZSERVER2012 1036 Error Microsoft-Windows-DHCP-Server
WINZSERVER2012 1035 Error Microsoft-Windows-DHCP-Server
Active Directory Administrative Center
Active Directory Domains and Trusts
Active Directory Module for Windows PowerShell
Active Directory Sites and Services
Active Directory Users and Computers
ADSI Edit
Component Services
Computer Management
Defragment and Optimize Drives
DHCP
DNS
Event Viewer
Group Policy Management
iSCSI Initiator
Local Security Policy
ODBC Data Sources (32-bit)
ODBC Data Sources (64-bit)
Performance Monitor
Resource Monitor
Security Configuration Wizard
Services
System Configuration
System Information
Task Scheduler
Windows Firewall with Advanced Security
Windows Memory Diagnostic
Windows PowerShell
Windows PowerShell (x86)
Windows PowerShell ISE

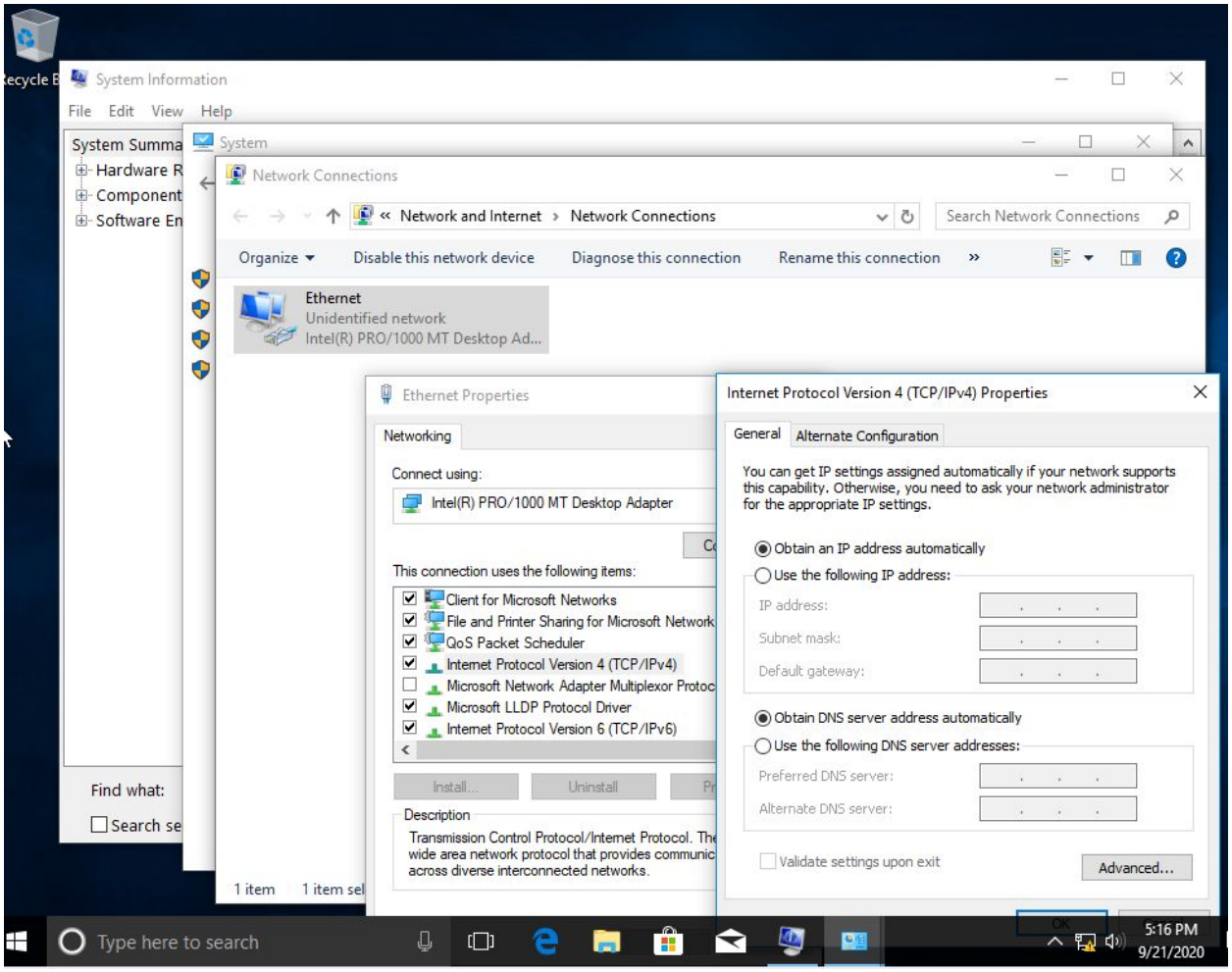

Server Manager ▸ DHCP
DHCP
File Action View Help
DHCP
winzserver2012.testserver.c
IPv4
Server Options
Policies
Filters
IPv6
New Scope Wizard
IP Address Range
You define the scope address range by identifying a set of consecutive IP addresses.
Configuration settings for DHCP Server
Enter the range of addresses that the scope distributes.
Start IP address: 10 . 1 . 10 . 50
End IP address: 10 . 1 . 10 . 100
Configuration settings that propagate to DHCP Client
Length: 8
Subnet mask: 255 . 0 . 0 . 0
< Back
Next >
Cancel
WINZSERVER2012 1059 Error Microsoft-Windows-DHCP-Server System 9/21/2020 11:05:22


Server Manager
Server Manager ▸ DHCP
DHCP
File Action View Help
DHCP
winzserver2012.testserver.c
IPv4
Server Options
Policies
Filters
IPv6
New Scope Wizard
Lease Duration
The lease duration specifies how long a client can use an IP address from this scope.
Lease durations should typically be equal to the average time the computer is connected to the same physical network. For mobile networks that consist mainly of portable computers or dial-up clients, shorter lease durations can be useful. Likewise, for a stable network that consists mainly of desktop computers at fixed locations, longer lease durations are more appropriate.
Set the duration for scope leases when distributed by this server.
Limited to:
Days:
Hours:
Minutes:
1
0
0
< Back
Next >
Cancel
WINZSERVER2012 1059 Error Microsoft-Windows-DHCP-Server System 9/21/2020 11:05:22

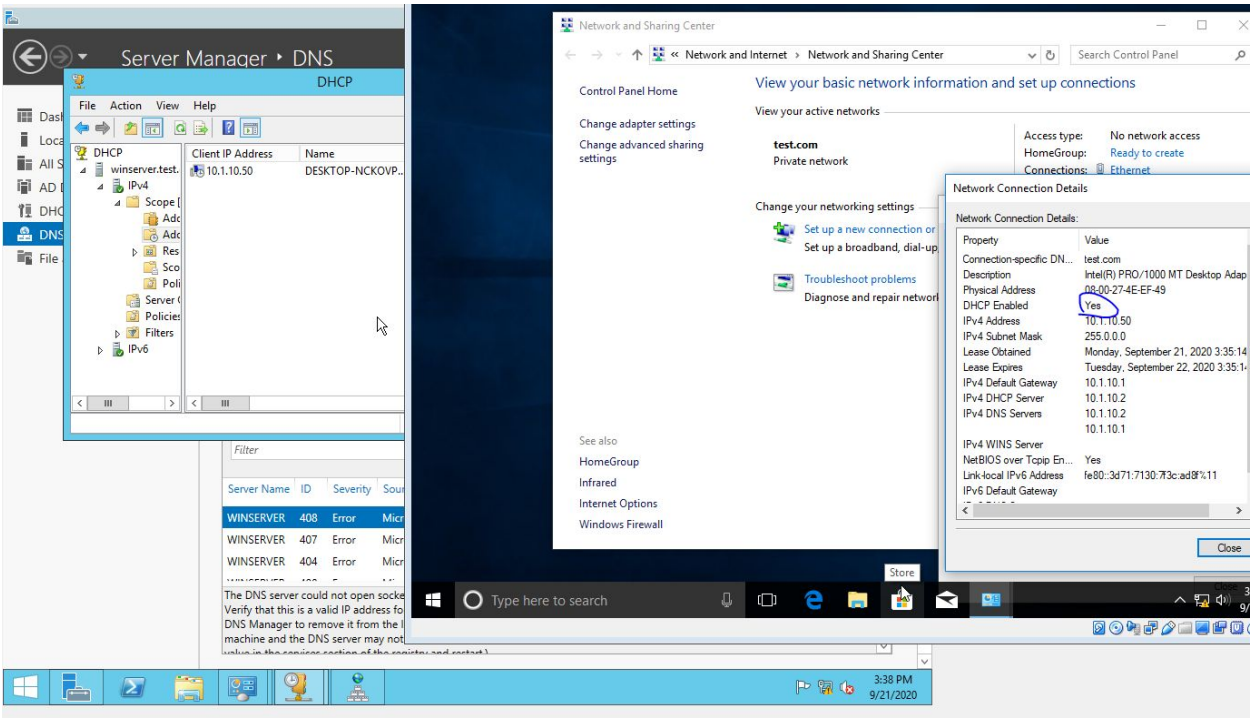

Server Manager
Server Manager ▸ DHCP
DHCP
File Action View Help
DHCP
winzserver2012.testserver.c
IPv4
Server Options
Policies
Filters
IPv6
New Scope Wizard
Router (Default Gateway)
You can specify the routers, or default gateways, to be distributed by this scope.
To add an IP address for a router used by clients, enter the address below.
IP address:
Add
10.1.10.1
Remove
Up
Down
< Back
Next >
Cancel
WINZSERVER2012 1059 Error Microsoft-Windows-DHCP-Server System 9/21/2020 11:05:22 A



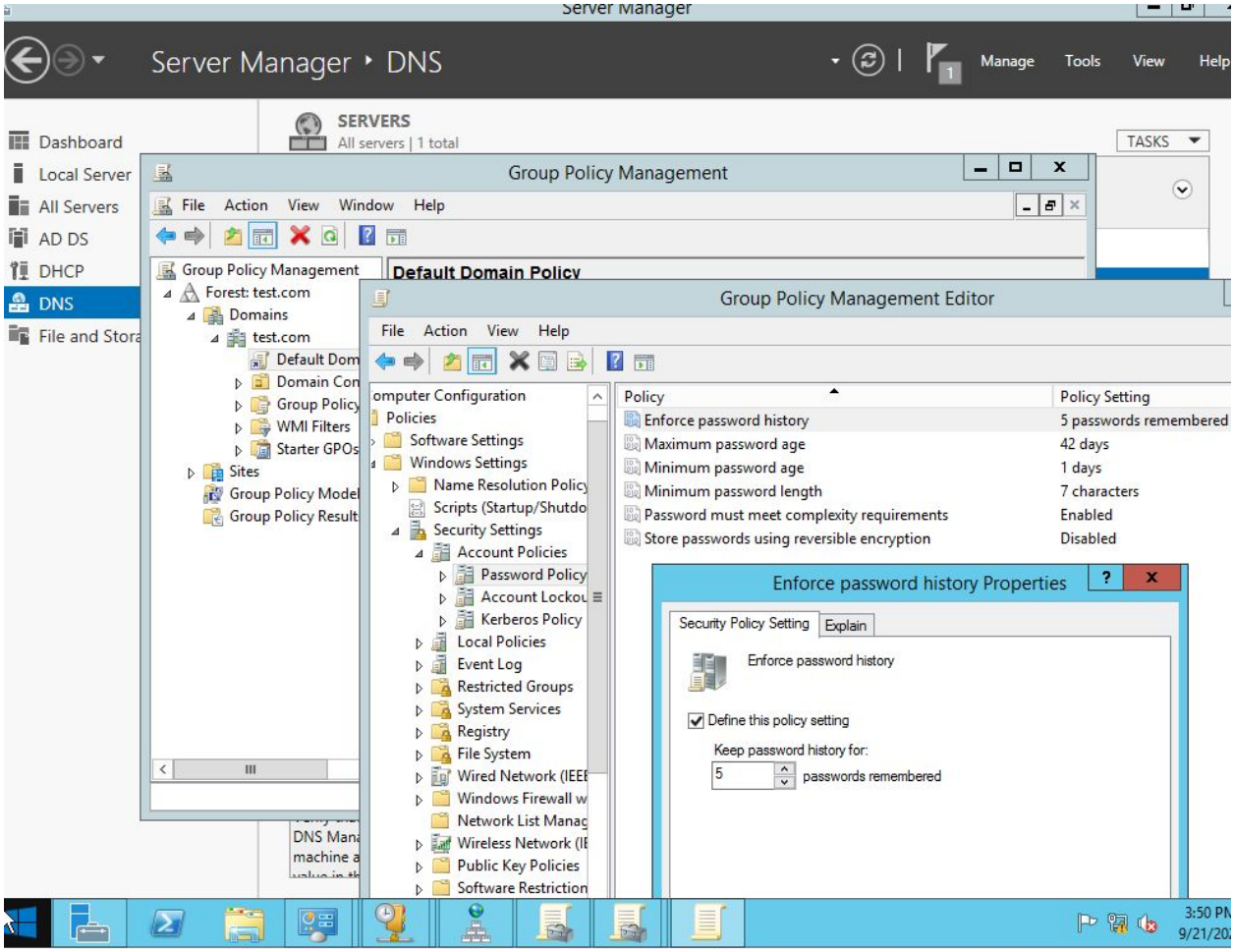
After Setting the DHCP server, we can turn on the windows 10 client machine and, as soon they are on the same network (set with virtual box, using the same internal network among the VMs), the client will get automatically the IP from the DHCP server (moreover, the properties). In order to obtain the address from the DHCP server, no others DHCP servers have to be in the network (No NAT network) and theNetwork connection in Panel ***Control/Network and Internet/Network Connections*** must be set with IPv4 as shown in the picture below:



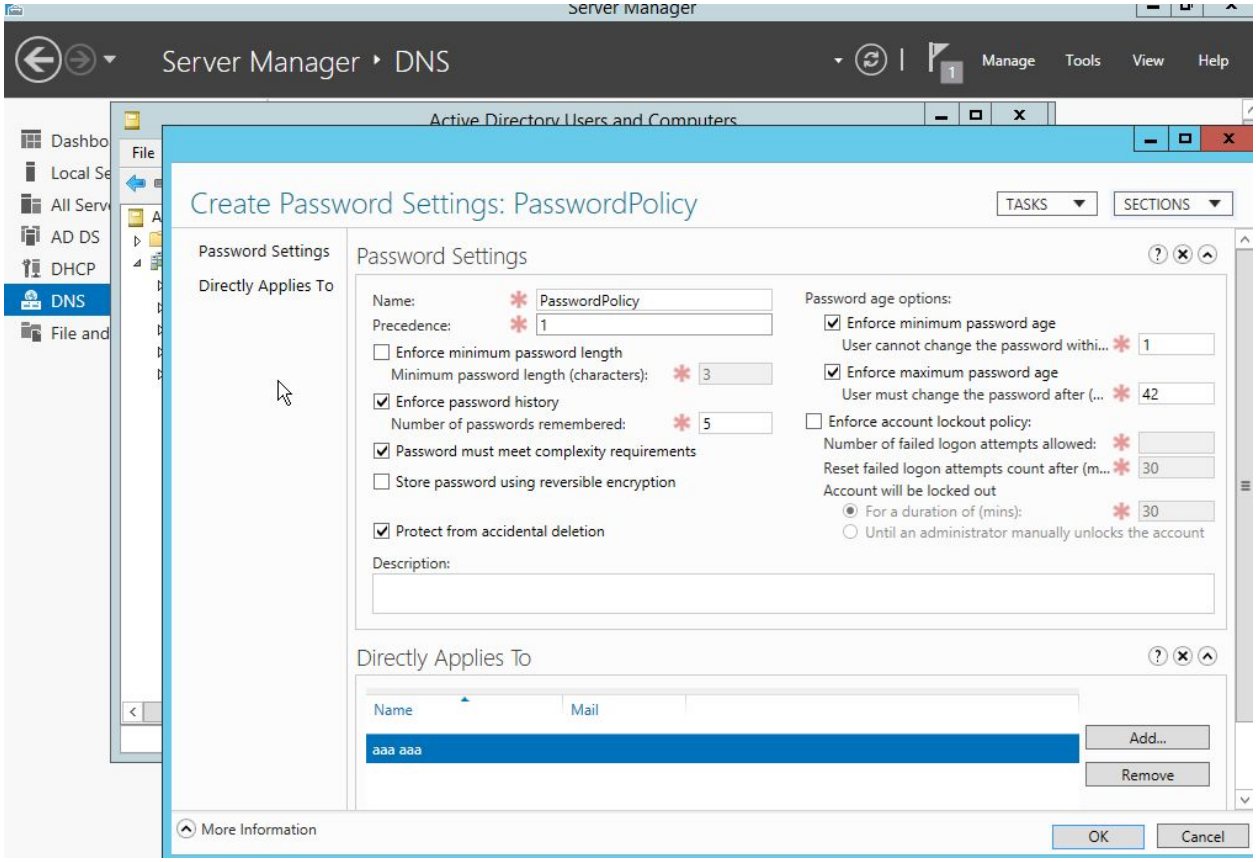
After receiving the address from the DHCP server, in the server we can see that in ***Tools/DHCP-><server>/address leases*** there is the client .



In the picture below, is shown how to access the password policies. The ***Group policy Management*** is in ***Tools .***



Another way to create and manage User and groups policies is to select **Active Directory Administrative Center** from the Tools menu. Then, in the server(local) section and System, the is another subsection called **Password Settings Container** and selecting **New** > **Password Settings** from the menu it will be possible to generate new password policies for a user or a group. In order to have the user(as the user *aaa aaa* shown below), it is necessary to add the a user a domain. In order to do so, in the Windows server we right click in ***tools->Active directory Users And Computers -> <domain> -> Users*** and then ***New->User*** and here we can create a new user (*aaa aaa*). Once the process is done, we can login in the windows client using the new credentials (and selecting the right domain if it is not already selected).
The user will be selected when the policy is created, under the section ***Directly applies to*** as shown below:


Server Manager
Server Manager ▸ DNS
Manage
Tools
View
Help
Dashbo
Local Se
All Serv
AD DS
DHCP
DNS
File and
Active Directory Users and Computers
File
Create Password Settings: PasswordPolicy
TASKS
SECTIONS
Password Settings
Directly Applies To
Password Settings
Name:
PasswordPolicy
Precedence:
1
Enforce minimum password length
Minimum password length (characters):
3
Enforce password history
Number of passwords remembered:
5
Password must meet complexity requirements
Store password using reversible encryption
Protect from accidental deletion
Description:
Password age options:
Enforce minimum password age
User cannot change the password withi...
1
Enforce maximum password age
User must change the password after (...
42
Enforce account lockout policy:
Number of failed logon attempts allowed:
Reset failed logon attempts count after (m...
30
Account will be locked out
For a duration of (mins):
30
Until an administrator manually unlocks the account
Directly Applies To
Name
Mail
aaa aaa
Add...
Remove
More Information
OK
Cancel