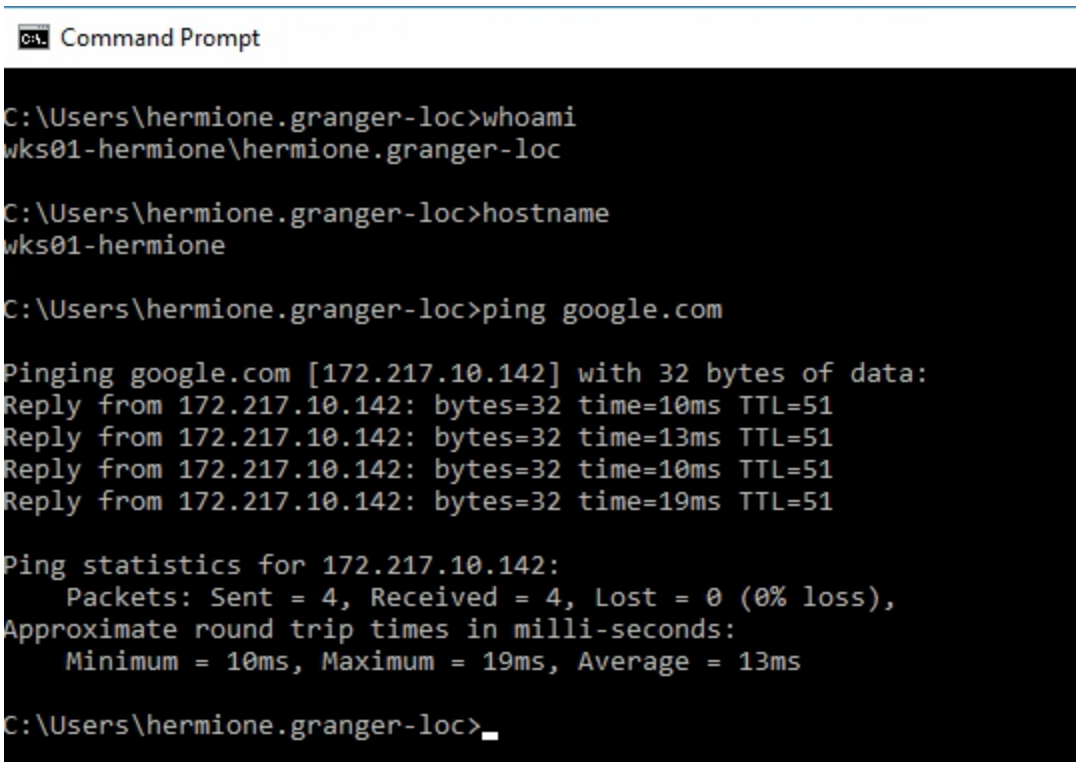
Lab02 - Server 2019, ADDS and DNS

💡 Any sizable environment needs a Domain Name Server (DNS) so that you don't need to manually associate IP addresses with hostnames. In Windows environments, you will often find that the DNS Server and a directory lookup service called active directory are combined on one platform. We will configure such a system on a Windows Server 2019 virtual machine that provides domain name and active directory services for the 10.0.5.0/24 network.

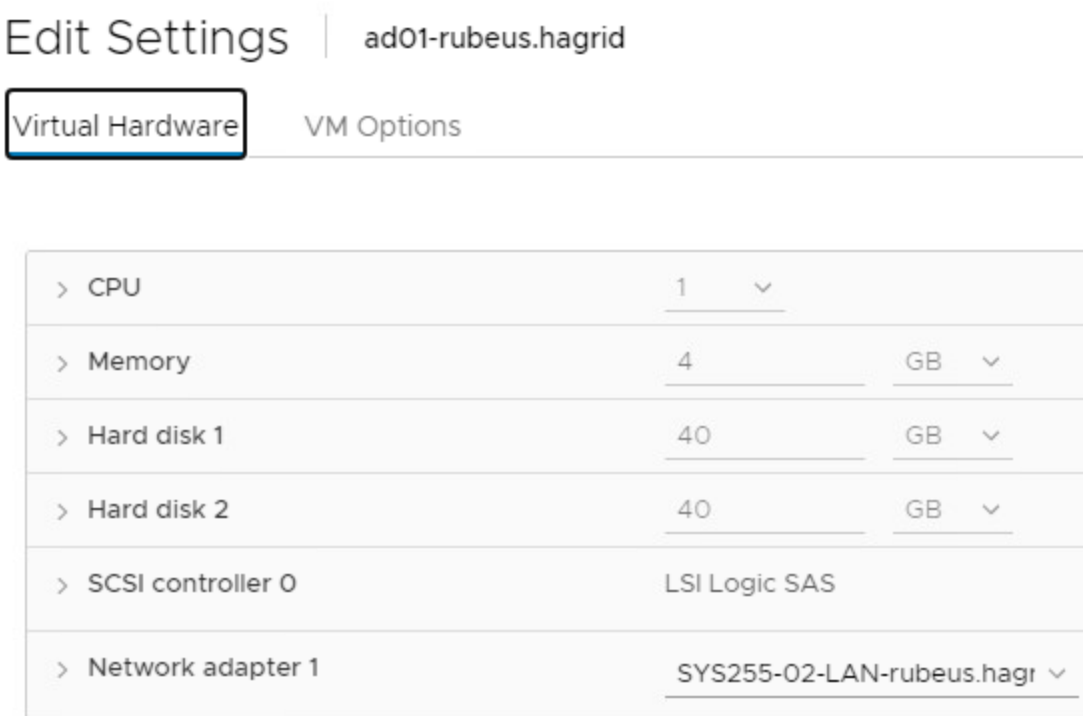
Prerequisites:

You should have completed lab01, and WKS01 should be able to ping champlain.edu via the default gateway(fw01) at 10.0.5.2. If not, then best focus on this before moving forward.



Server 2019

Find and edit the virtual machine properties for ad01 by adjusting the network adapter as so:



Server 2019 has already been installed for you. Start the VM and configure it as shown in the following instructions. Read -> Plan -> Do.

Use default settings with the following exceptions

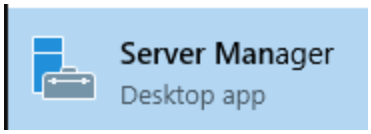
- Product Key -> Do this later
- Administrator Password

💣 *Make sure that the Administrator password you provide for ad01's local administrator is a strong password, and that you remember it, otherwise you will need to change it later or do a reinstallation.*

This local password will end up being the Domain Administrator's password!

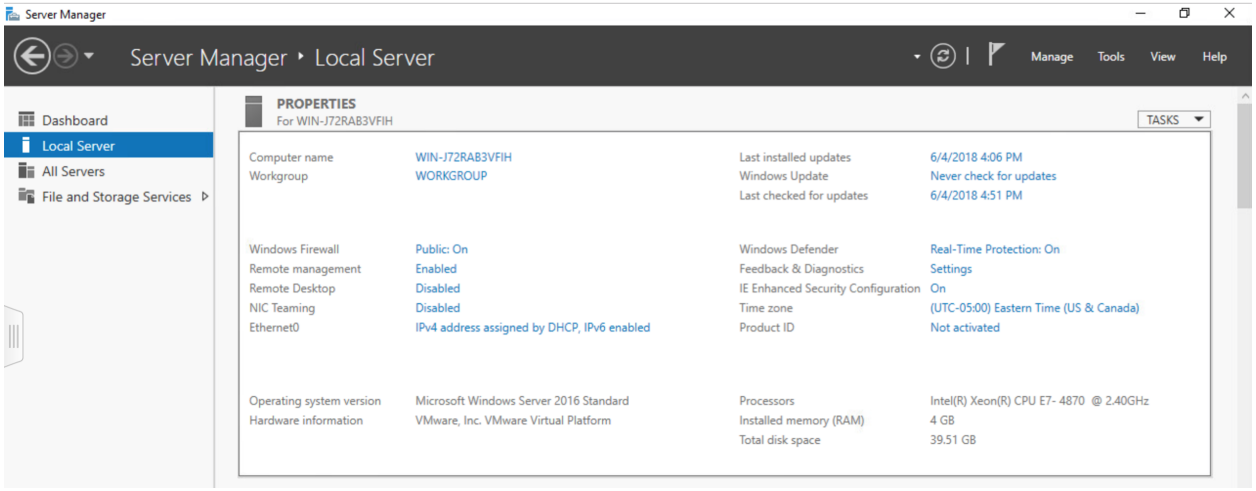
Host and Network Configuration

If it is not already running, find and invoke server manager from the start menu

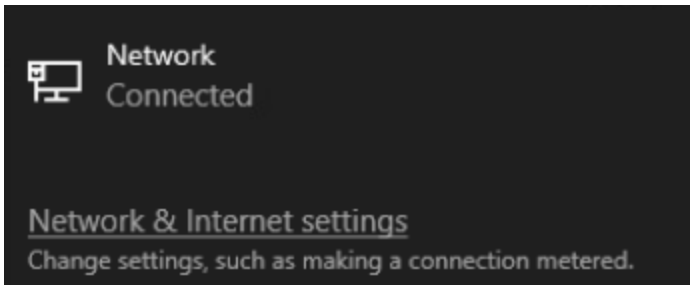


💡 Ignore prompts for installation of the server admin center, this is something that will be explored in subsequent courses.

The Local Server Manager is probably the easiest way to begin the configuration changes



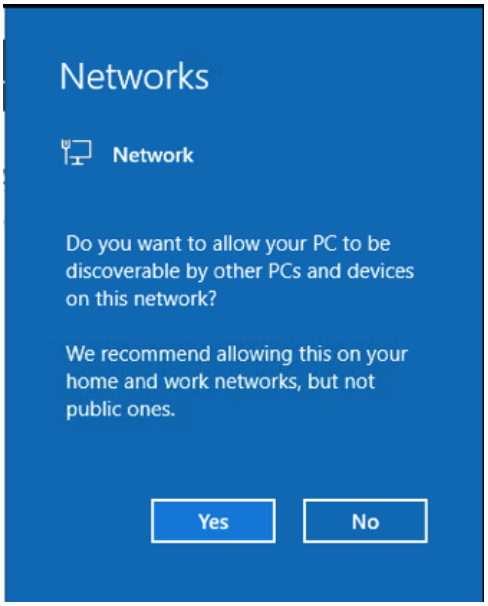
Another way to change Ethernet adapter options for IPv4 properties is via the network icon on the bottom-right in the task bar.



Set the following:

- IP Address: 10.0.5.5
- Netmask: 255.255.255.0
- Gateway 10.0.5.2 (Make sure fw01 is running).
- DNS 10.0.5.2

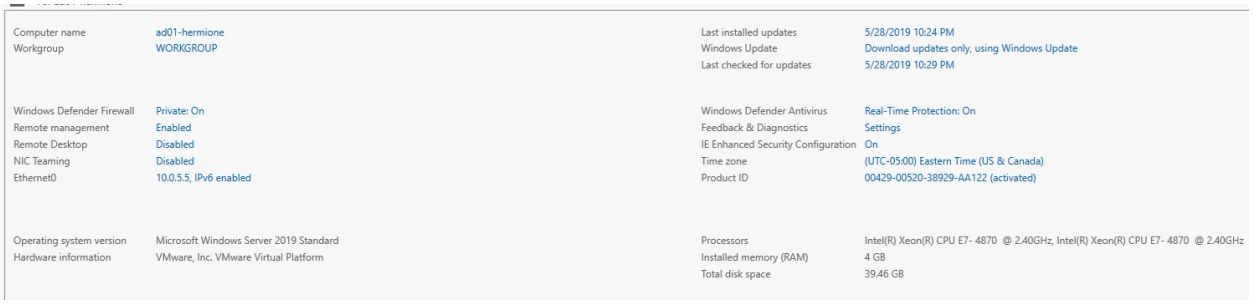
- Discoverable option. If this dialog shows up, select Yes for those systems on your LAN.



- Time should be set to UTC-5:00 Eastern Time (US & Canada)
- Computer name: ad01-yourname (make sure you get this right).

🕒 This reboot may take some time, this might be a good time to update your Tech Journal.

After reboot, your Local Server Settings Screen should look like this:



Check Networking

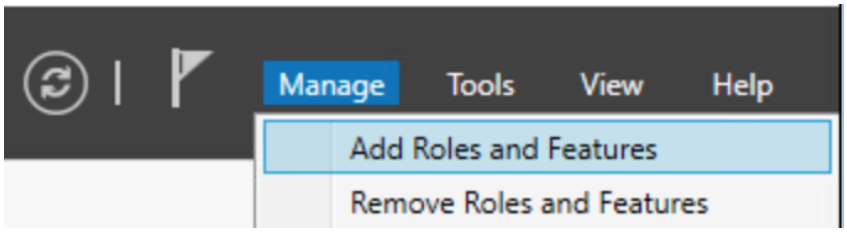
Using a command or powershell prompt, double check that your hostname has been set and that you have external connectivity as shown below.

Administrator: Windows PowerShell

```
PS C:\Users\Administrator> whoami
ad01-rubeus\administrator
PS C:\Users\Administrator> ping google.com

Pinging google.com [142.250.64.110] with 32 bytes of data:
Reply from 142.250.64.110: bytes=32 time=12ms TTL=115
Reply from 142.250.64.110: bytes=32 time=12ms TTL=115
Reply from 142.250.64.110: bytes=32 time=12ms TTL=115
Reply from 142.250.64.110: bytes=32 time=12ms TTL=115

Ping statistics for 142.250.64.110:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 12ms, Maximum = 12ms, Average = 12ms
PS C:\Users\Administrator>
```

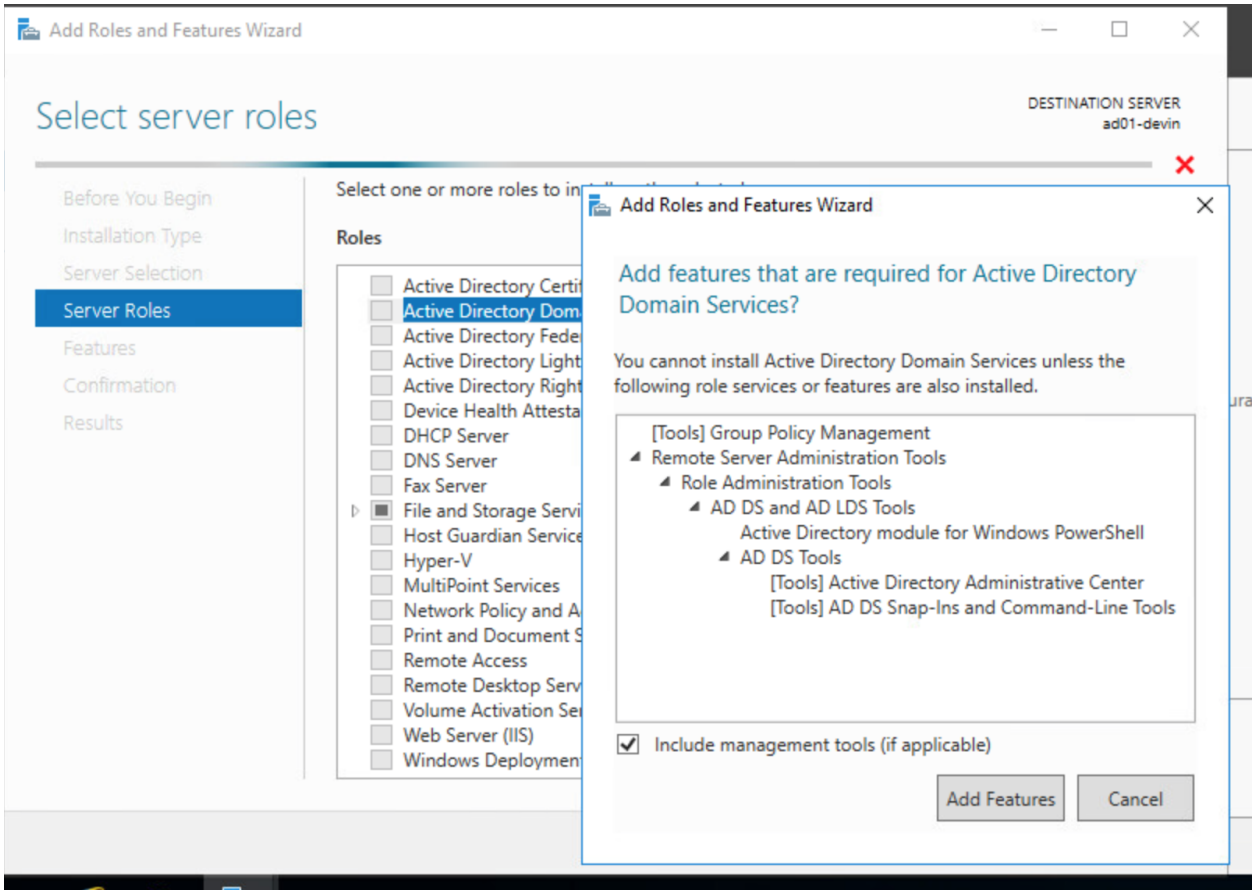
Installing the ADDS Role

Open Server Manager. From the Manage menu, Select Add Roles and Features

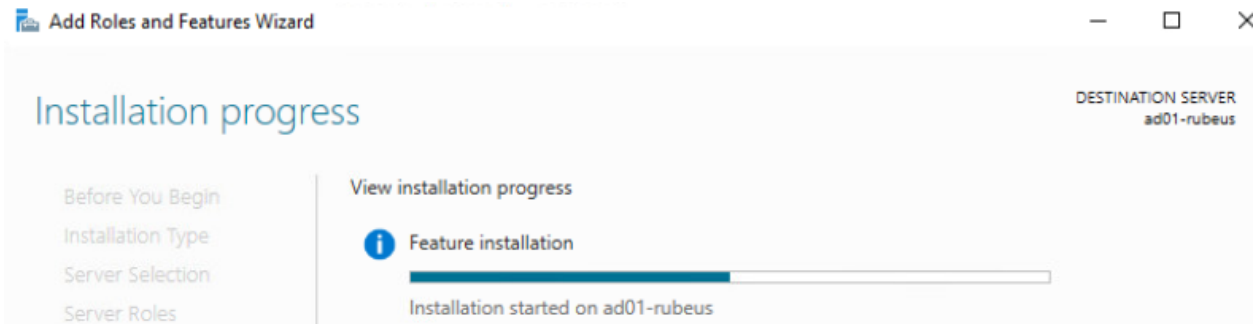


The following screenshots will show only those screens where non-default configuration is required.

Select Active Directory Domain Services->Add Features. Pick Active Directory Domain Services: ☑ Active Directory Domain Services



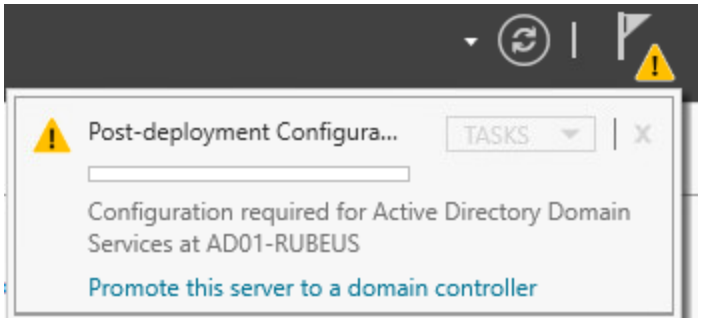
Choose the restart destination server option, and select yes on the confirmation dialog.



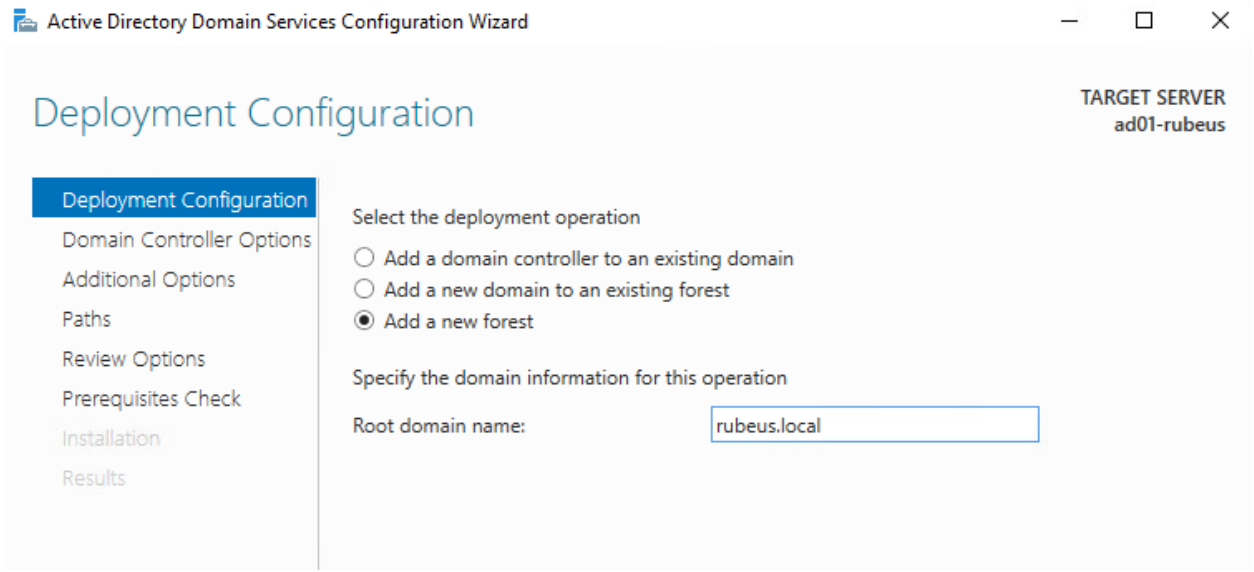
🕒 Again, this installation and promotion process can sometimes be lengthy. Find something else to do in the meantime, such as updating your tech journal. A systems administrator should always have something else to do when waiting for a process to complete.

Promotion

After installation, we need to configure our server to be the primary domain controller for our domain (yourname.local). Select the link to Promote this server to a domain controller. Make absolutely sure you have set the hostname before moving forward with promoting this system.



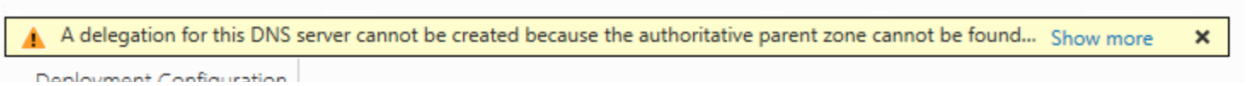
We are going to create a new forest. Name this forest yourname.local, where yourname is your first name.



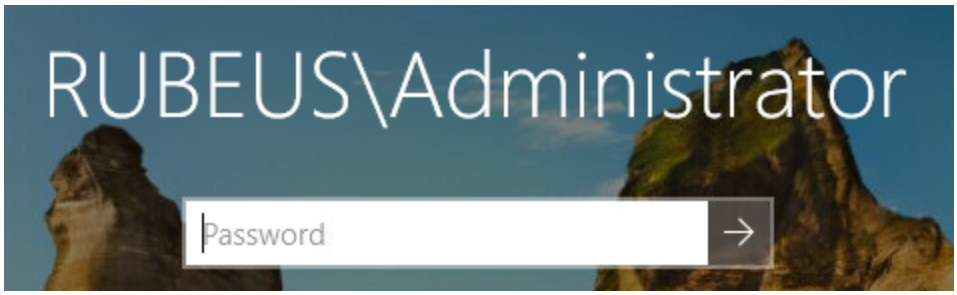
Enter a DSRM password. This password is used to recover the directory in case of error. You would use it in production if things went terribly wrong.

DNS Error

Because we gave our environment a .local top level domain(TLD), an error is indicated during installation. Valid top level domains are domains like .com, .gov, .edu, .net. Because this is an internal domain, we will leave it as is. The naming of local domains is the subject of many debates among systems administrators.



Installation will take a few minutes and a reboot. When you log back in, you will be logging in as the Domain Administrator (with credentials in Active Directory) as opposed to the Local Administrator (credentials stored locally within Windows OS credentials & not in AD domain credentials).

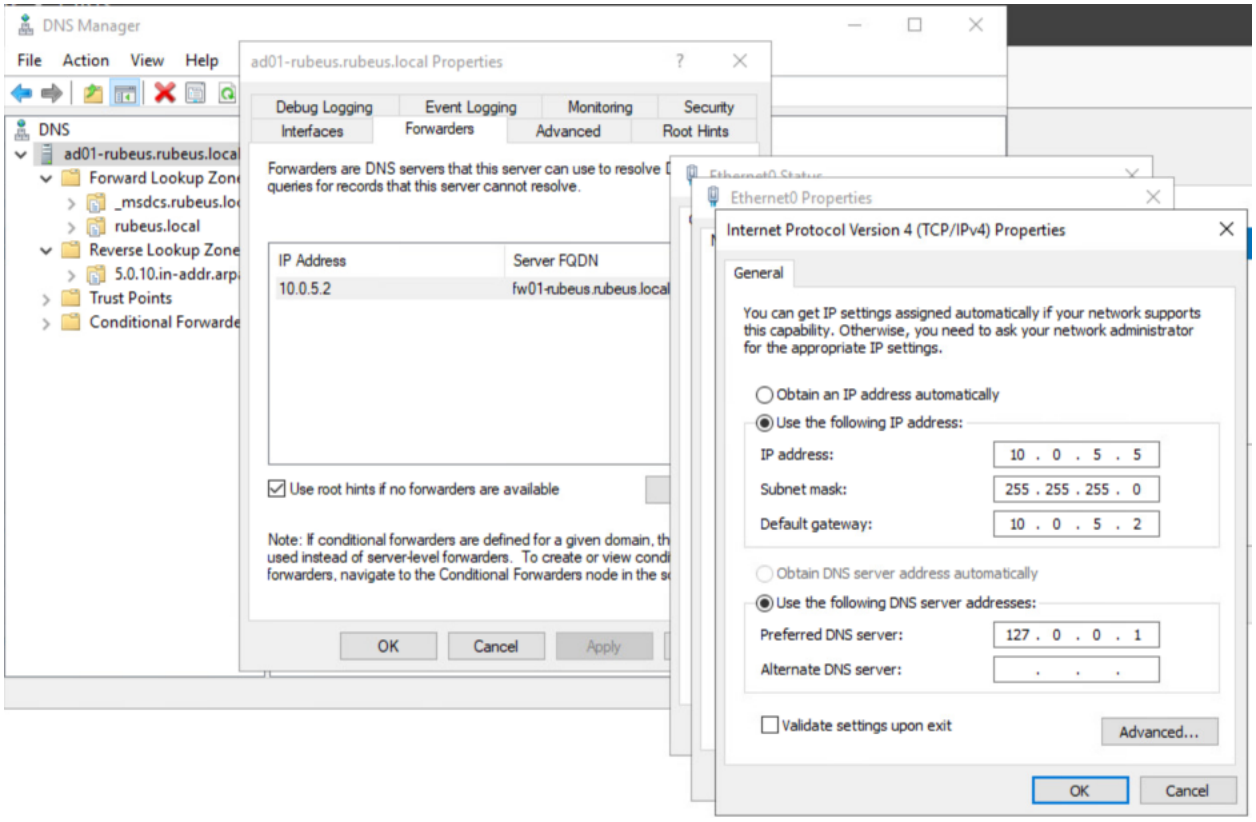


💡 Pro Tip: This frequently trips up newer admins, the difference between the 2 admin accounts since they both have “Administrator” as their account name.

Please note this difference: Domain Admins have power over items within an AD domain, whereas Local Admins have power over items within the singular installed OS and not within AD.

DNS

After installation and a lengthy reboot, you will find that your ad01 server's network configuration has changed somewhat. Your DNS server now points to 127.0.0.1 (which is the local loopback adapter for ad01, i.e. it’s pointing back to itself), and DNS queries not handled locally are forwarded to fw01 which will in turn forward to its DNS Server.



Adding a DNS Record

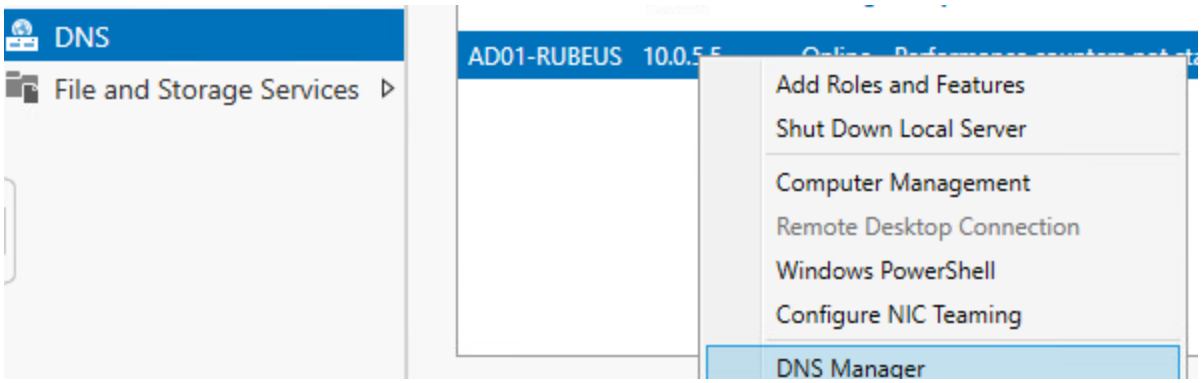
The following commands run from ad01 show that we cannot access fw01 by name and only by IP address. We are going to create a DNS record on our server such that anyone using ad01 as a DNS server (including itself) can resolve the domain name fw01.yourname.local to 10.0.5.2.

Administrator: Windows PowerShell

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> hostname
ad01-rubeus
PS C:\Users\Administrator> ping 10.0.5.2

Pinging 10.0.5.2 with 32 bytes of data:
Reply from 10.0.5.2: bytes=32 time<1ms TTL=64
Reply from 10.0.5.2: bytes=32 time<1ms TTL=64
Reply from 10.0.5.2: bytes=32 time<1ms TTL=64
Reply from 10.0.5.2: bytes=32 time<1ms TTL=64

Ping statistics for 10.0.5.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
PS C:\Users\Administrator> ping fw01-rubeus
Ping request could not find host fw01-rubeus. Please check the name and try again.
PS C:\Users\Administrator>
```

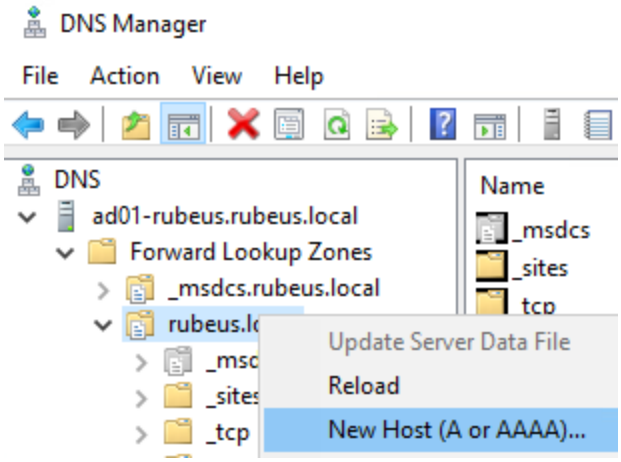
DNS Manager

Find and invoke DNS Manager from the Server Manager/DNS/AD01 context menu



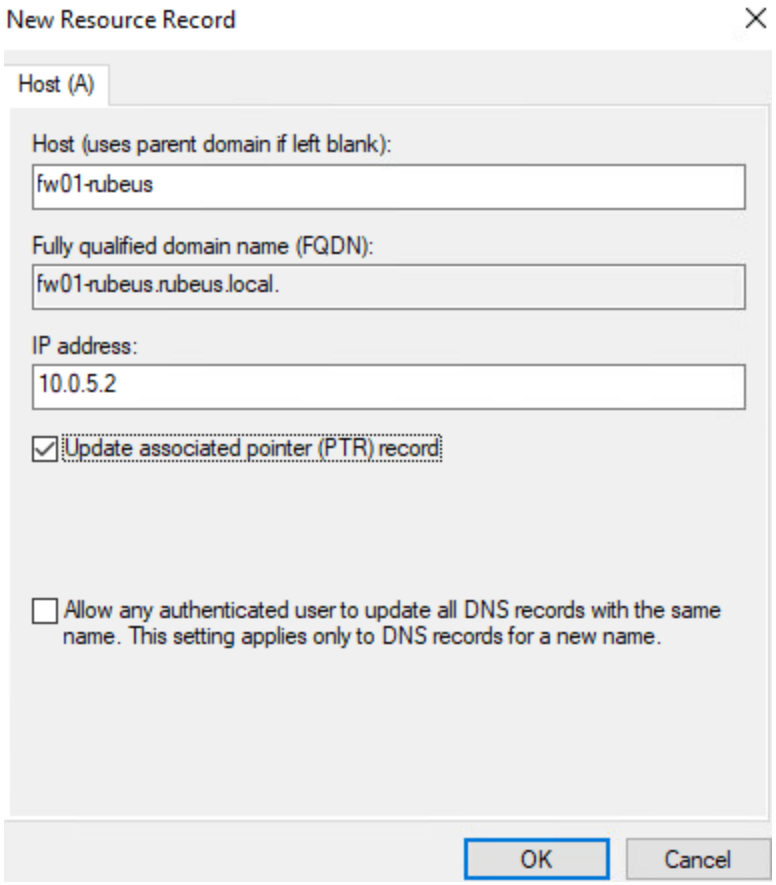
Forward Lookup Zone - yourname.local

Find and expand the forward lookup zone for your new domain



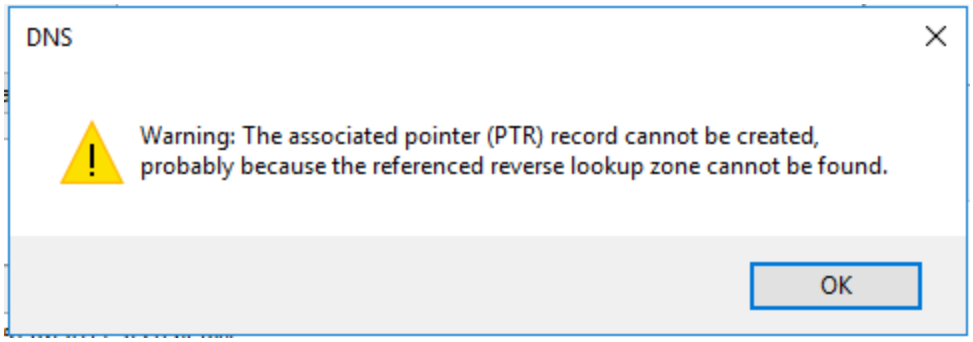
You should have an entry for ad01.yourname. This allows you to ping ad01 by hostname and/or domain name. We are going to add an entry for fw01

From the DNS Manager, select New Host (A or AAAA name):



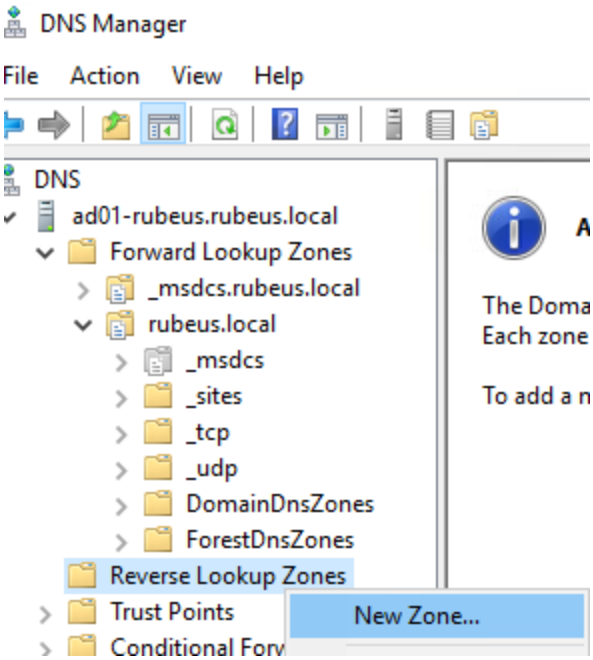
Add a reference to fw01, go ahead and check "Create associated (PTR) record"

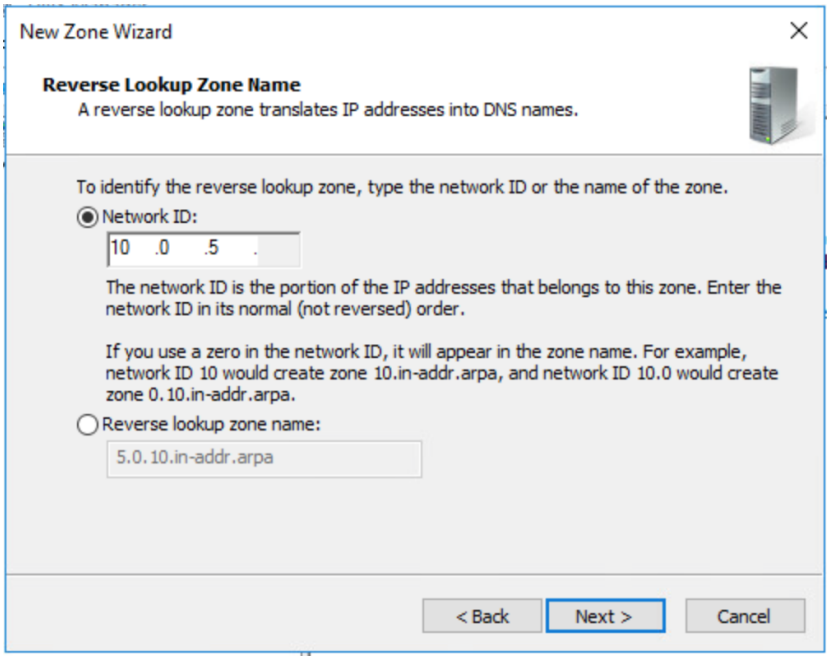
When your host is added, the capability to resolve a host by its hostname is enabled. The reverse is not true. We cannot get a hostname by IP address until we create a reverse lookup zone.



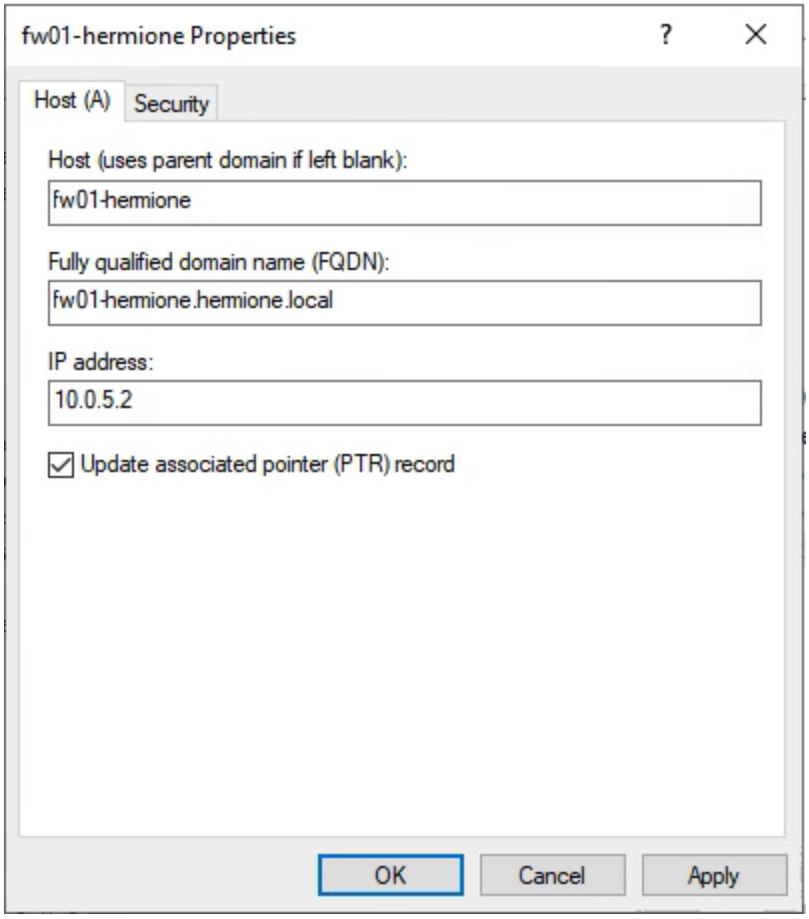
Reverse DNS

Add a reverse primary lookup for all IP addresses in the 10.0.5.0/24 Network by selecting the New Zone options from the right-click context menu as shown below. Use the defaults, and add a Network ID for 10.0.5.

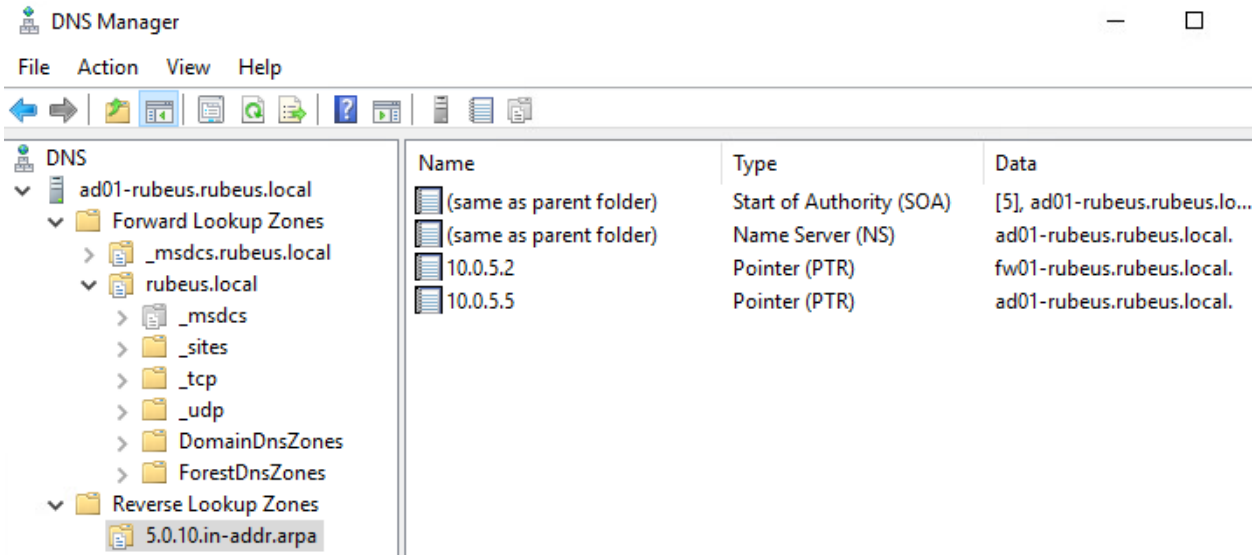




Create a new PTR record from the A record of fw01-yourname and ad01-yourname by unchecking, applying checking the update PTR record check box, and re-applying fw01's properties.



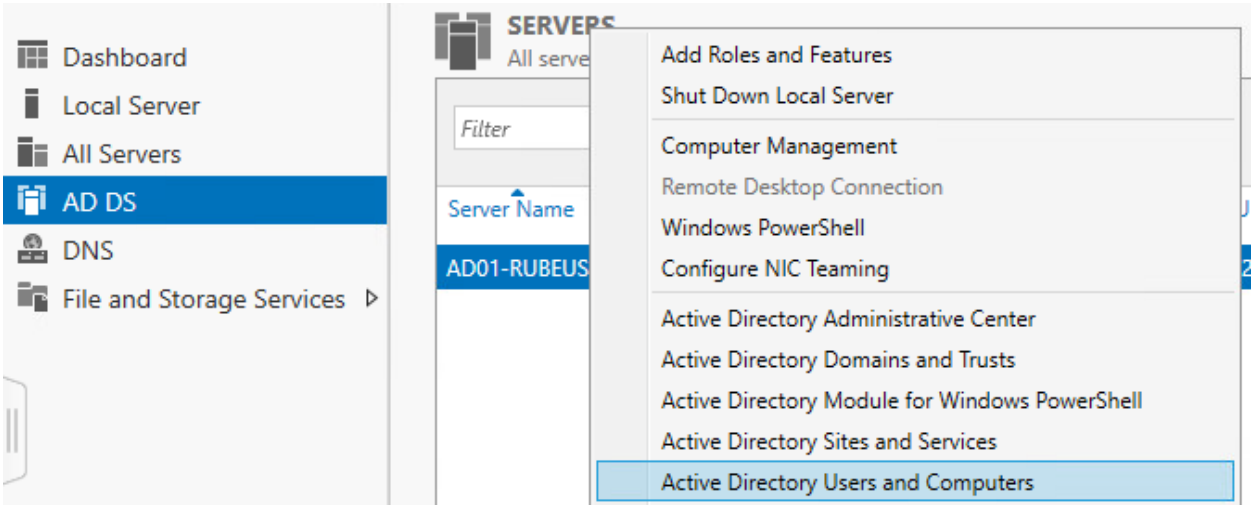
The reverse dns entry for fw01 and ad01 should now be in the 5.0.10 reverse lookup zone. You may need to refresh the view:



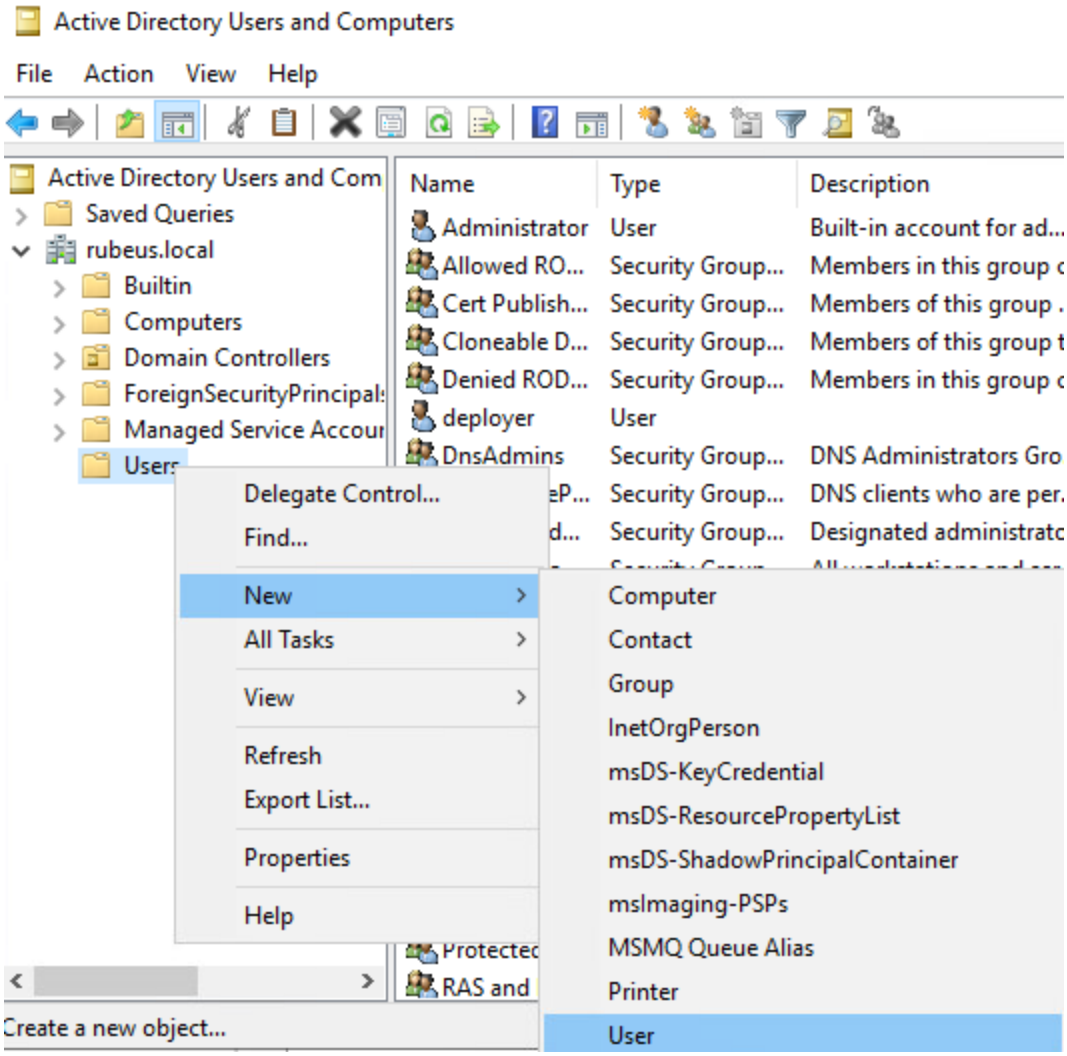
Create Named Domain Users on ad01

It is very easy to become confused between local accounts on either WKS1 and AD01 and domain accounts that are available on every system in the domain. We are going to create a named domain administrator account as well as a named non-privileged user account.

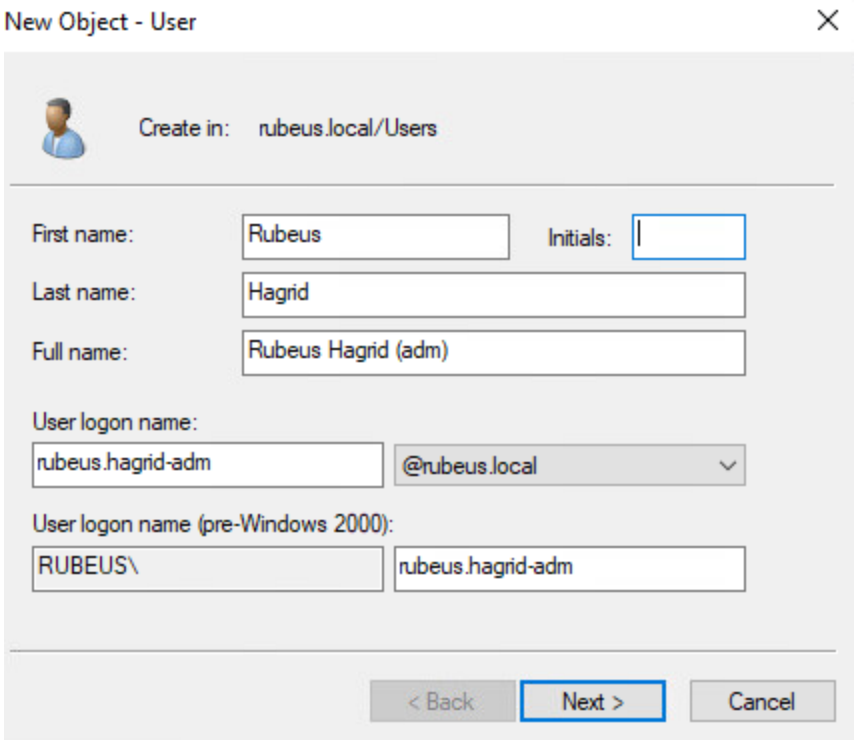
> 💡 Shared accounts like "Administrator" defeat the principle of accountability, and should be avoided after installation and configuration at all cost!



On AD01, find the Active Directory Users and Computers option.
Under the Domain's user folder, add a new User.

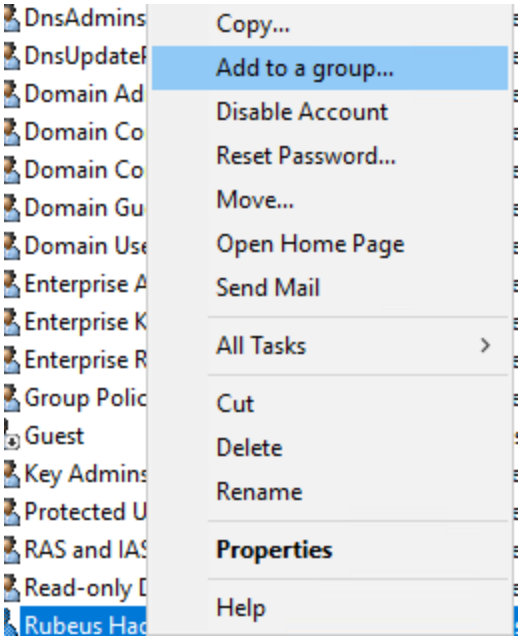


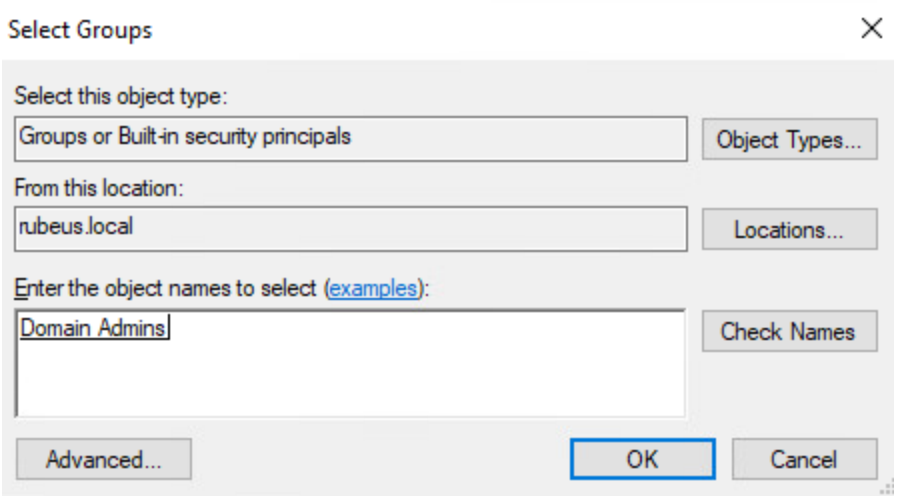
This user (first.lastname-adm) will be a Domain Administrator and will have a distinct suffix (ADM) to show this.



Uncheck user must change password at next login.

Add this user to the Domain Admins Group





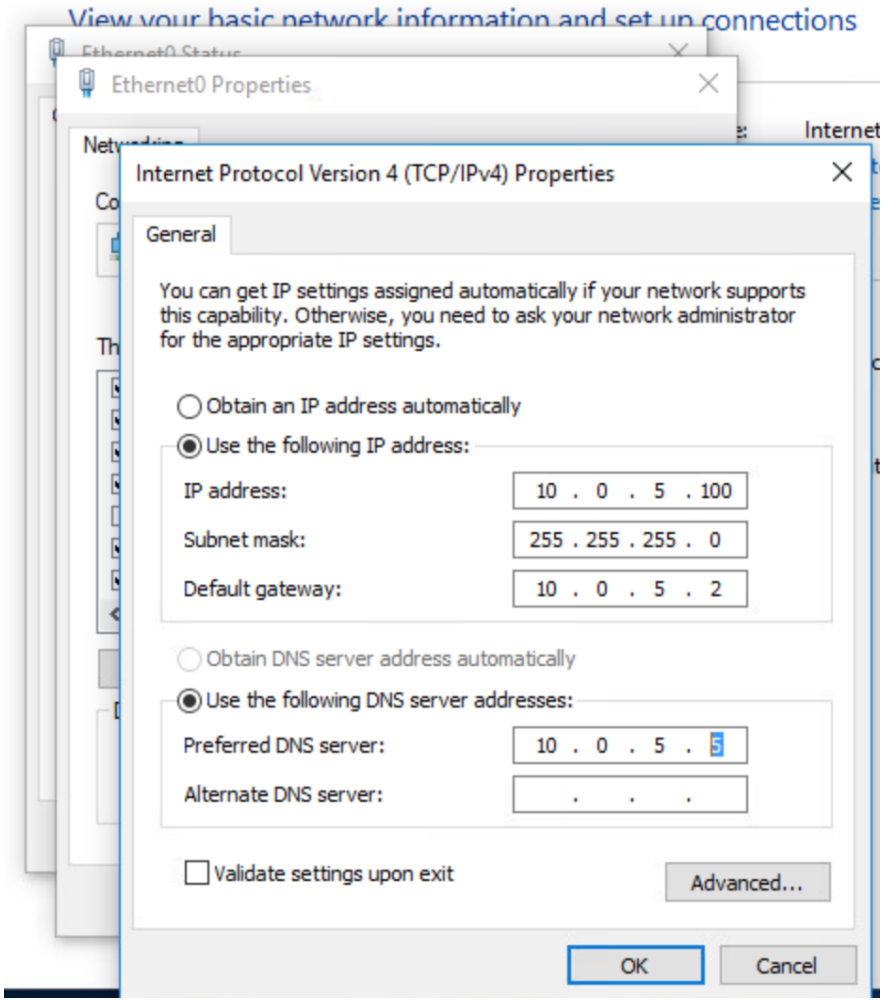
Create a non-privileged account (Skip the addition to Domain Admins) for user first.lastname

From this point forward you will login using your AD first.lastname or first.lastname-adm accounts depending on the privileges you need, and not the local accounts.

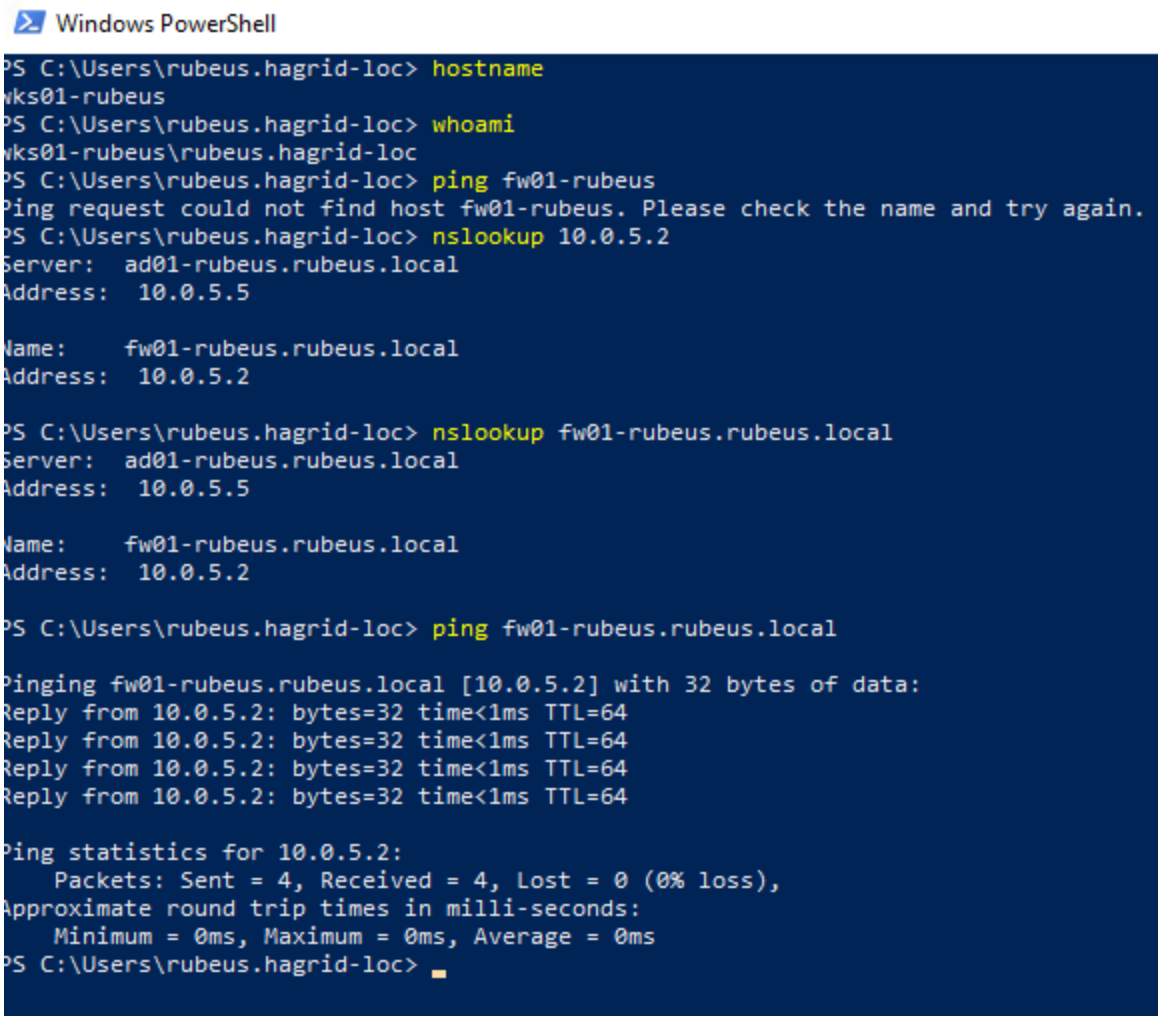
Preparing wks01 to join yourname.local

Set wks01's DNS to 10.0.5.5 (ad01's address), since our DNS has those 2 new A and PTR records created earlier.

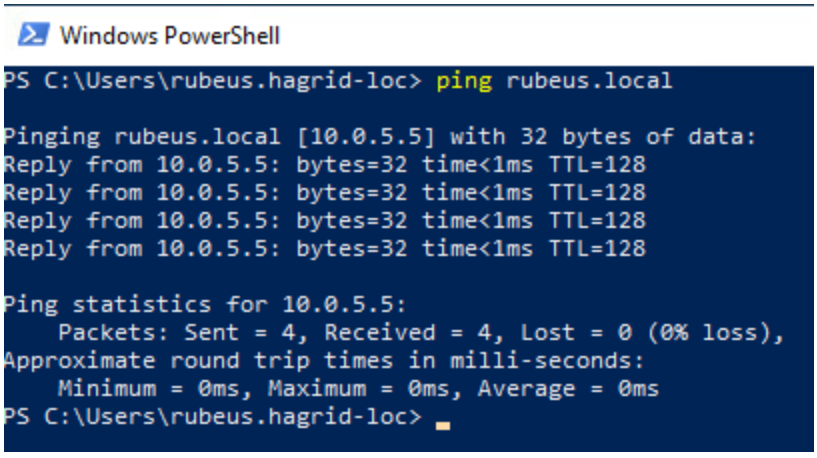
💣 **This is important**: Anytime you have a new system that needs to join the domain, it needs to refer to the domain's DNS server. This concept may trip you up in follow on assessments if you neglect this …



Now that you are using your new DNS server, we can attempt to ping by hostname. The following screen shows that you should be able to do a reverse lookup to fw01's PTR record using nslookup. You can also ping by fully qualified hostname. You cannot ping by the unqualified "fw01" hostname because we are not a domain joined system yet nor do we have a DNS suffix configured for yourname.local on wks01.

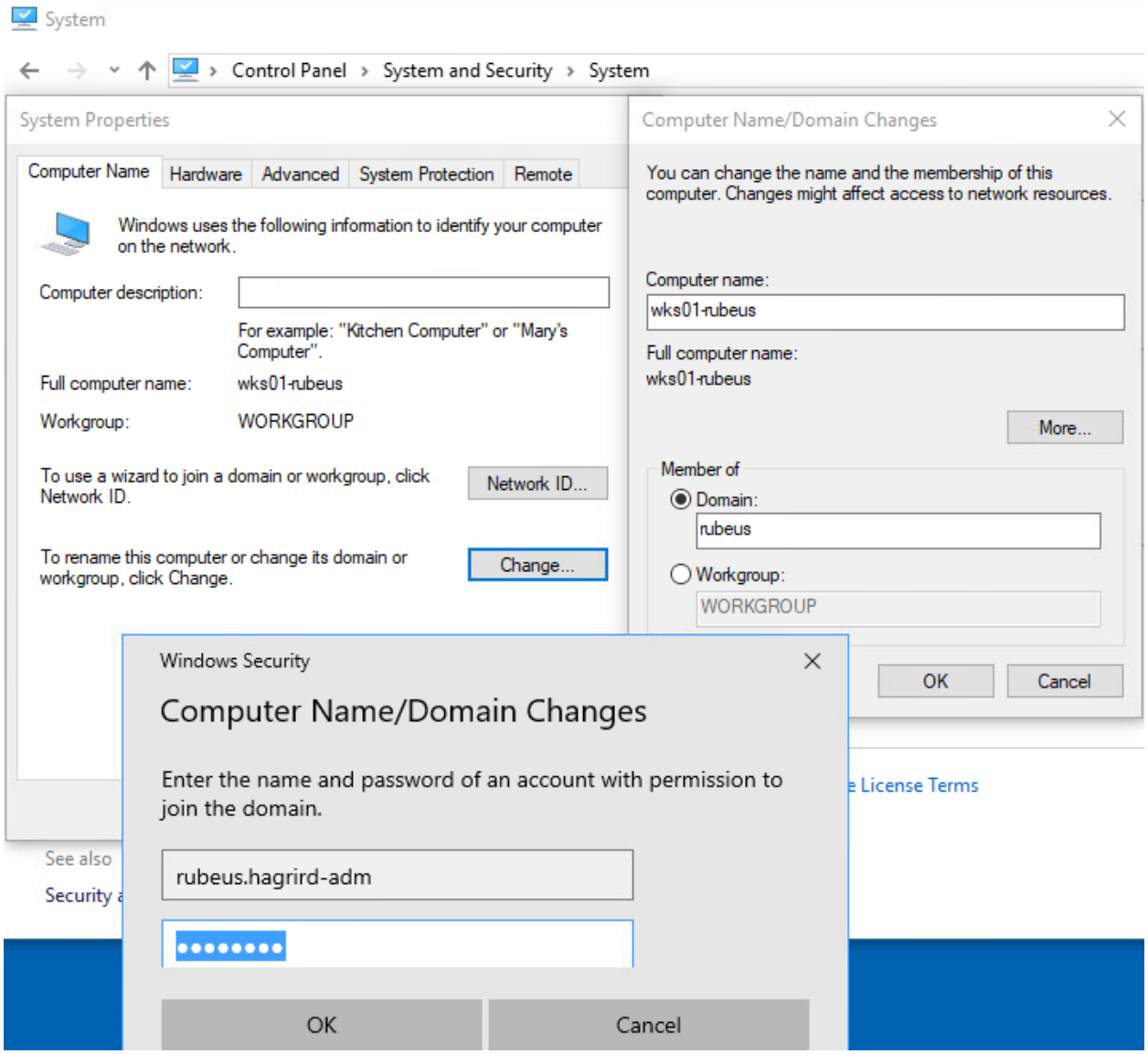


Let's ping the domain itself.

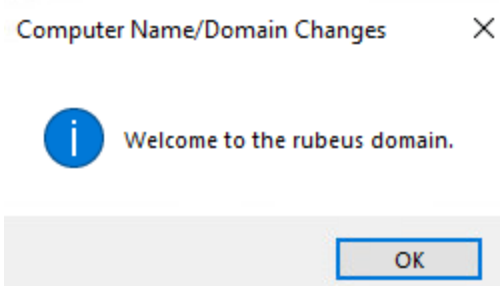


Joining WKS01 to your new domain

If you haven't changed the hostname from the random assigned hostname, do so now. Call it wks01-yourname.



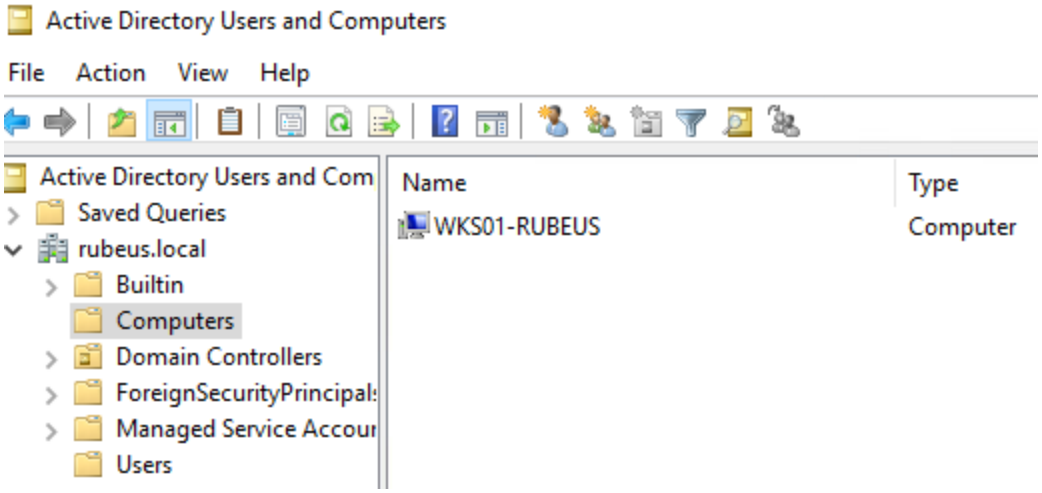
If everything went well, you will be prompted for an administrator password. Use the one you just created on AD01. You should have been successfully welcomed to the yourname domain.



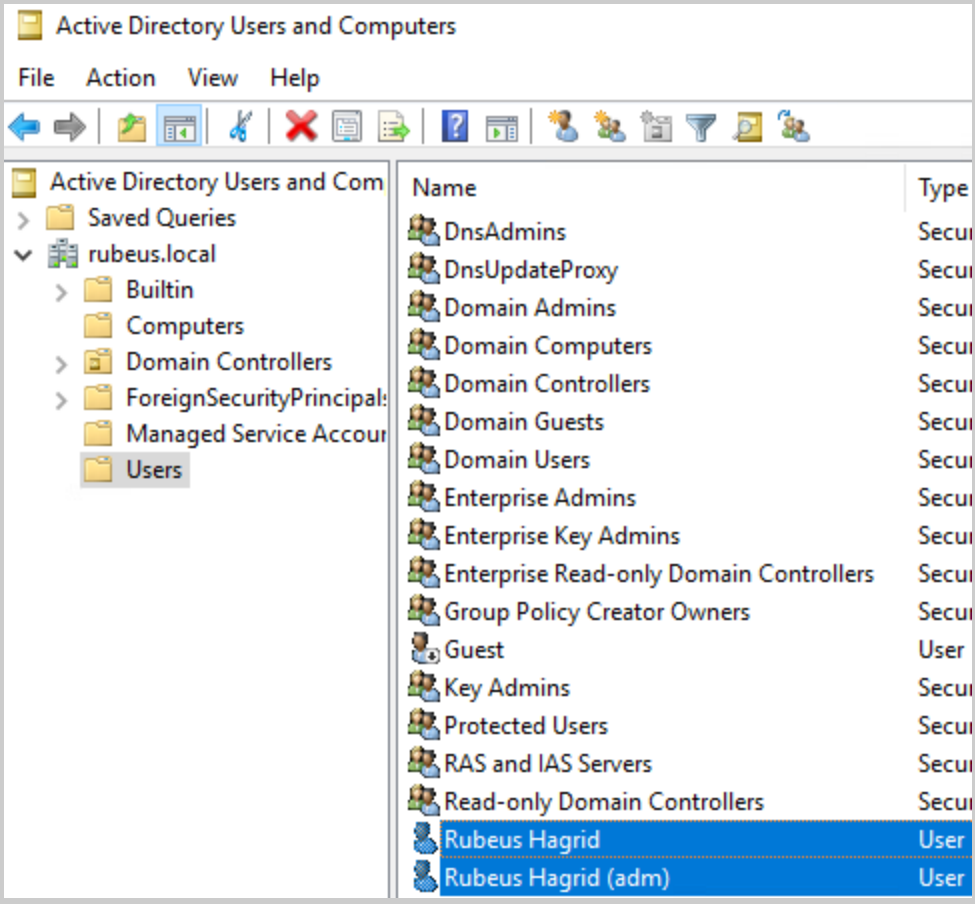
Restart wks01 now.

Deliverable 1: On AD01, find the Active Directory Users and Computers App, and provide a screenshot showing that WKS01 has been successfully added to the domain.

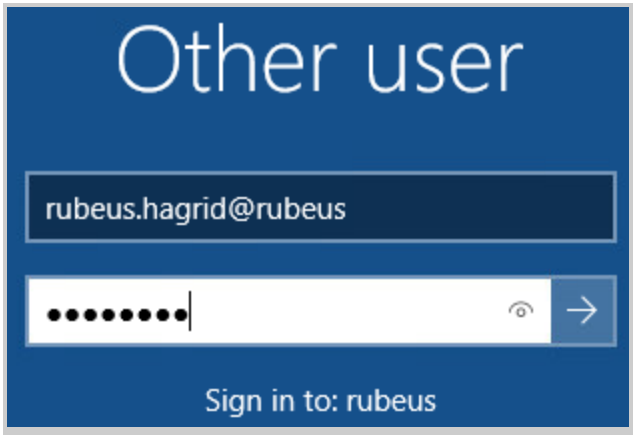
> 💡 Though you may be tempted, do not add entries to "Computers" manually. AD will add them automatically when a successful join has been made.



Deliverable 2. On AD01, select the two new users you have added and provide a screenshot.

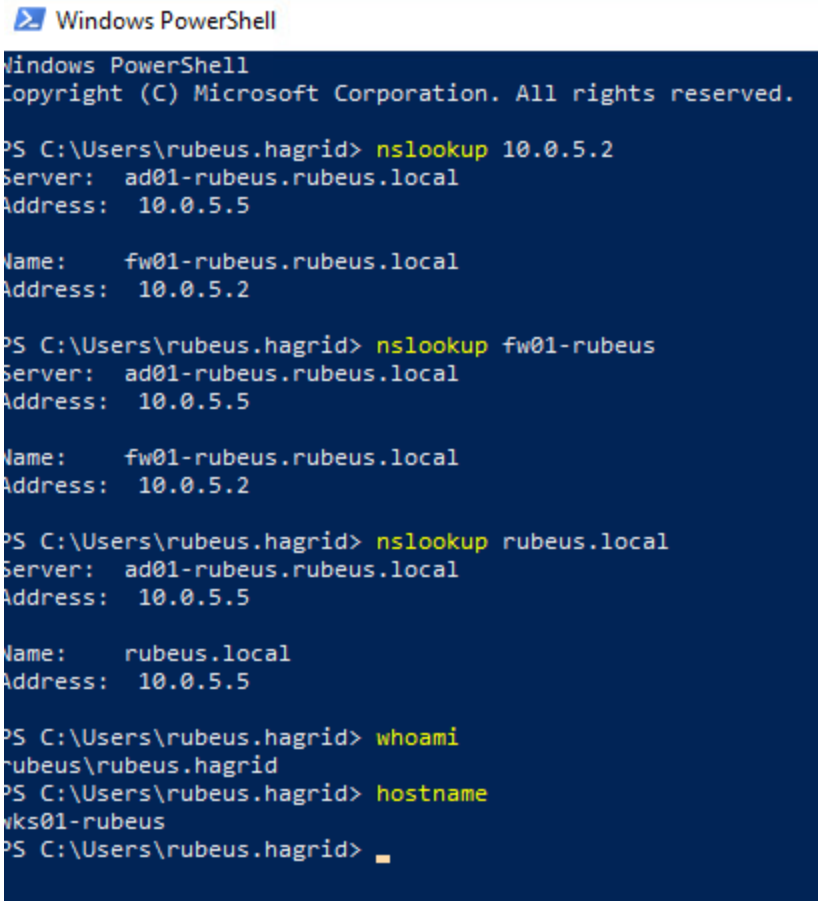


After the WKS01 has joined your Domain, we need to make sure we login to the system using our newly minted regular domain user credentials (and ***not*** the -adm account). Make sure you are signing into your Domain and not the local workstation.



Deliverable 3. From powershell or a command prompt on WKS01, provide the results of the following commands in one screenshot:

- nslookup 10.0.5.2 (this will perform a reverse dns query)
- nslookup fw01-yourname (this will query by host name)
- nslookup yourname.local (this will find the domain's DNS server)
- whoami (this will show that you are logged in as DOMAIN/User
- Hostname (this will show the name of your workstation)



Deliverable 4. Your deliverable meets the submission guidelines (1 point).

Deliverable 5. Tech Journal entry. Make your github public & include URL.