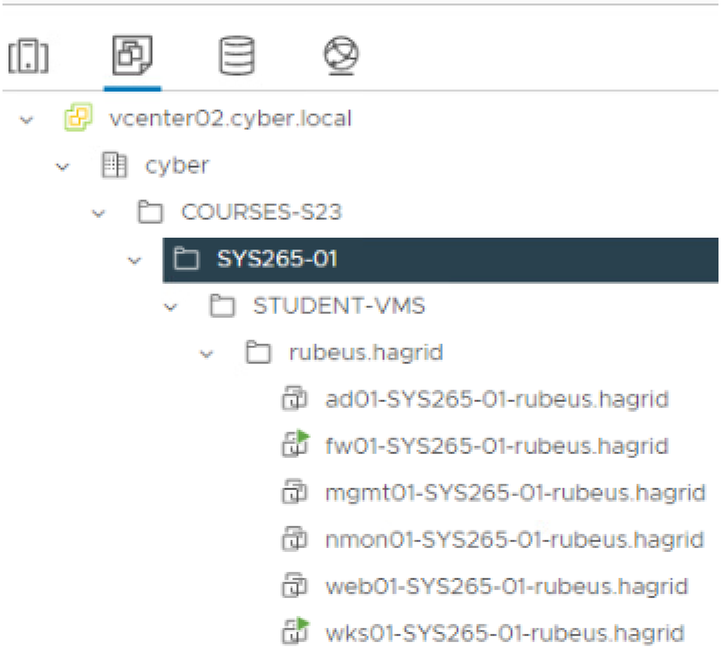
Lab00 - Routing and Windows

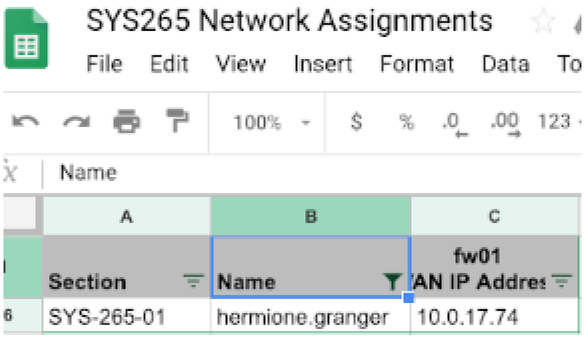
> 💡This lab will rely on some of the skills you have already learned in Systems Administration 1 and Network Protocols. You will build a simple network that will serve as the foundation for future labs. It is important that you make this a reliable build that you have total familiarity with because subsequent activities will use this architecture as a point of departure.

Our goal is to build a realistic server environment consisting of a routed network (LAN and WAN) as well as introduce Server 2019 Desktop and Core and the systems required to manage them.



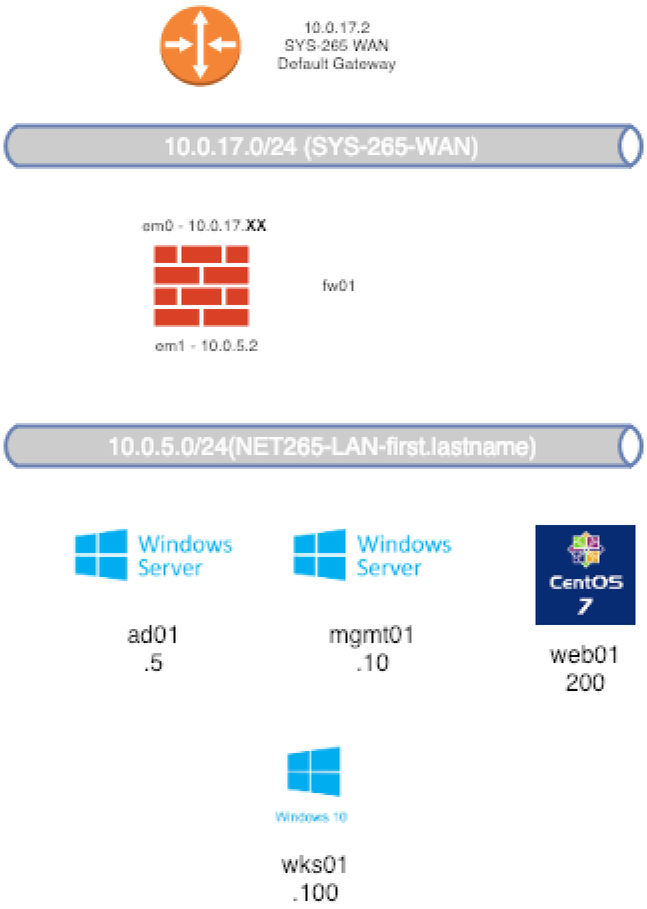
```
vcenter02.cyber.local
  cyber
    COURSES-S23
      SYS265-01
        STUDENT-VMS
          rubeus.hagrid
            ad01-SYS265-01-rubeus.hagrid
            fw01-SYS265-01-rubeus.hagrid
            mgmt01-SYS265-01-rubeus.hagrid
            nmon01-SYS265-01-rubeus.hagrid
            web01-SYS265-01-rubeus.hagrid
            wks01-SYS265-01-rubeus.hagrid
```

The figure below shows your lab architecture after Parts 1 and Parts 2 of the lab are complete. In part 1, you will establish routing and concentrate on the Windows portions of the Architecture.



Name

	A	B	C
	Section	Name	fw01 'AN IP Addres
6	SYS-265-01	hermione.granger	10.0.17.74

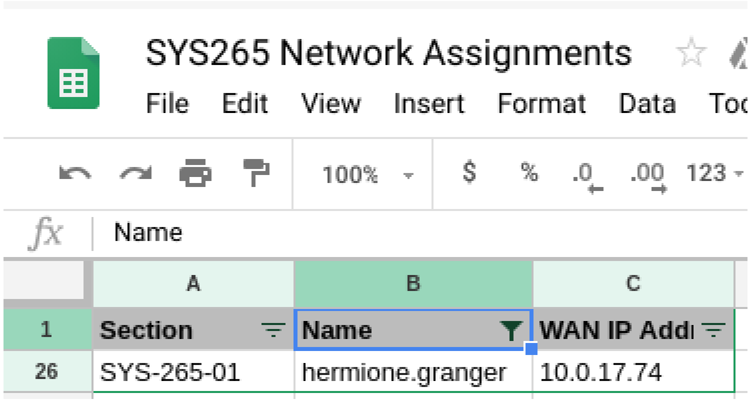


Requirements

FW01

Firewall is a pfSense router + firewall + gateway that you will need to configure in order to route traffic between your private network and your public network. As in SYS-255, FW has two network interfaces.

You will have your unique public IP address assigned via on the Canvas home page.



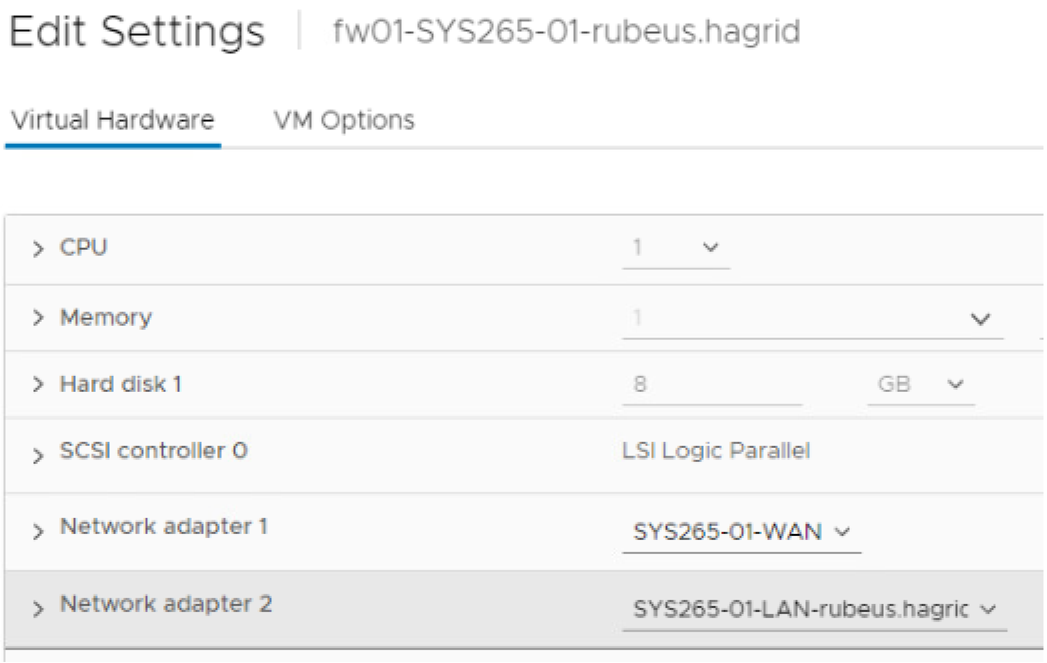
SYS265 Network Assignments

Name

	A	B	C
1	Section	Name	WAN IP Addı
26	SYS-265-01	hermione.granger	10.0.17.74

Virtual Networking

The following screenshot shows the appropriate virtual network configuration for fw01.



Edit Settings | fw01-SYS265-01-rubeus.hagrid

CPU	1
Memory	1
Hard disk 1	8 GB
SCSI controller 0	LSI Logic Parallel
Network adapter 1	SYS265-01-WAN
Network adapter 2	SYS265-01-LAN-rubeus.hagric

OS Configuration

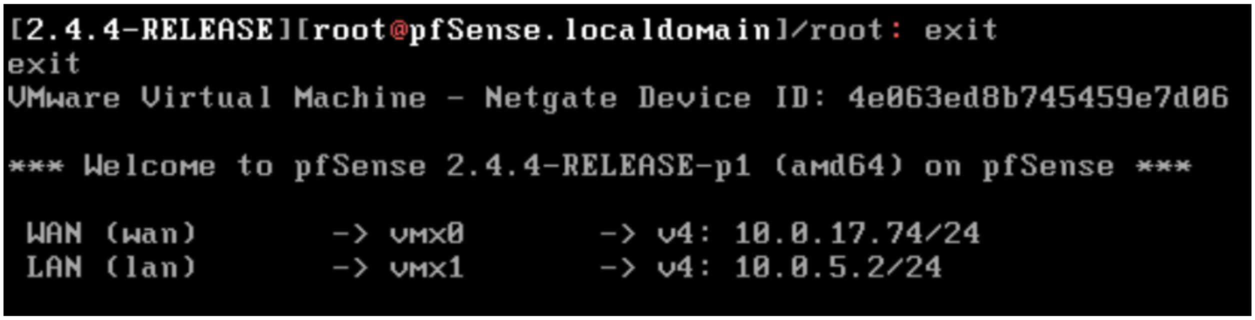
Configure pfSense similarly as you did during SYS255. If you run into trouble, here's the link to the SYS255 Lab that covers pfSense. A couple pointers:

- It will take a minute or so for a timeout to occur when configuring interfaces. It is waiting for a dhcp server that just does not exist.
- We are not using VLANs
- VMX0/em0 and VMX1/em1 are WAN and LAN respectively
- Your WAN interface will be set to your assigned IP, while the LAN IP will be set to 10.0.5.2/24
- Your WAN upstream gateway address is 10.0.17.2

- We are not using IPv6 on WAN nor LAN
- We are not using the firewall for DHCP on the LAN

When done, your console should look similar to this:

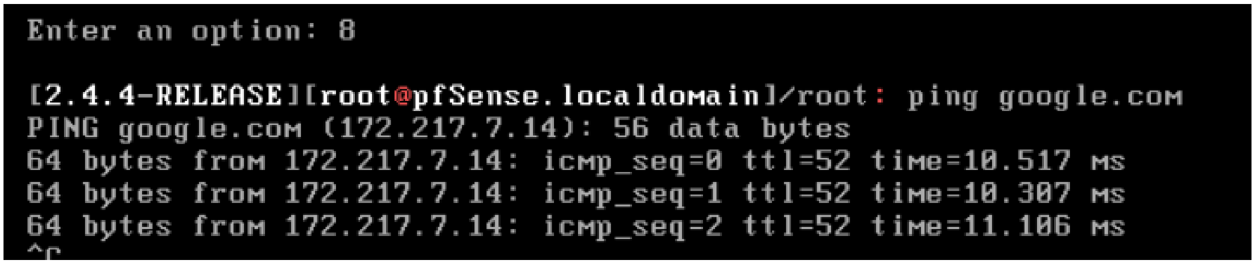
💣Do not use Hermione's WAN IP (.74), use your own!



```
[2.4.4-RELEASE][root@pfSense.localdomain]/root: exit
exit
VMware Virtual Machine - Netgate Device ID: 4e063ed8b745459e7d06

*** Welcome to pfSense 2.4.4-RELEASE-p1 (amd64) on pfSense ***

 WAN (wan)       -> vmx0       -> v4: 10.0.17.74/24
 LAN (lan)       -> vmx1       -> v4: 10.0.5.2/24
```

We will complete our configuration using the web interface from our Windows 10 system (wks01)

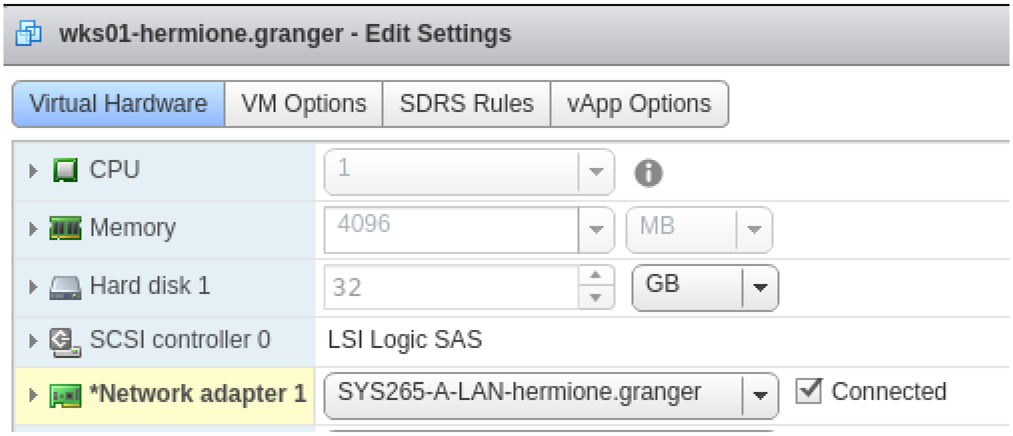
You should also be able to enter a shell (8) and ping google.com



```
 Enter an option: 8

 [2.4.4-RELEASE][root@pfSense.localdomain]/root: ping google.com
 PING google.com (172.217.7.14): 56 data bytes
 64 bytes from 172.217.7.14: icmp_seq=0 ttl=52 time=10.517 ms
 64 bytes from 172.217.7.14: icmp_seq=1 ttl=52 time=10.307 ms
 64 bytes from 172.217.7.14: icmp_seq=2 ttl=52 time=11.106 ms
 ^C
```

WKS-01

Virtual Networking:



wks01-hermione.granger - Edit Settings

CPU: 1
Memory: 4096 MB
Hard disk 1: 32 GB
SCSI controller 0: LSI Logic SAS
*Network adapter 1: SYS265-A-LAN-hermione.granger ☑ Connected

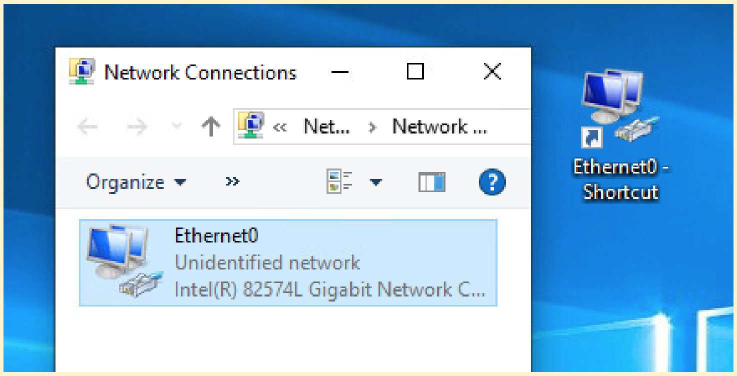
OS Configuration:

> 💡The Windows 10 desktop system (wks01) will display the *champuser* username, which is our deployer account. You will need to set up a new Local Named Administrator account, which you will use for the rest of the term.
>
> Here are specific instructions on how to add a new Local Named Administrator account.

Go through the normal configuration steps:

- During 1st boot, the setup asks to “Connect Now to Save Time Later” > Select **No**
- Username: yourname (you may need to add a new local administrative user)
- Adjust your privacy settings by turning everything off when prompted
- Give wks01 a static IP address of 10.0.5.100, netmask of 255.255.255.0 and a gateway and DNS of 10.0.5.2 (your fw01 LAN interface).
- Give your system a hostname of wks01-yourname.

💡 Pro Tip

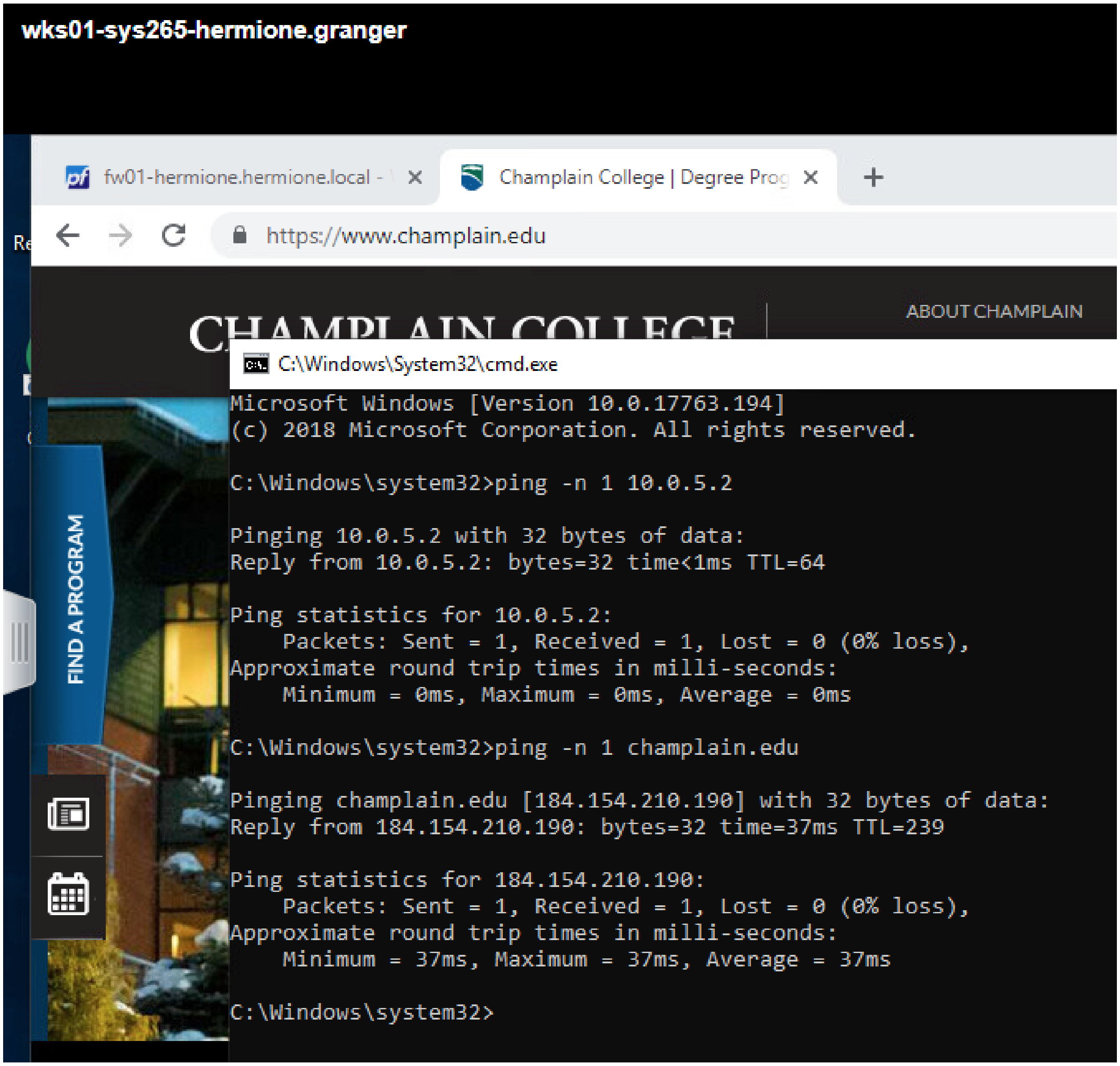


Navigate to https://10.0.5.2 and login using admin/pfsense

Follow the FW wizard and make the following changes:

- hostname:fw01-yourfirstname
- Domain: yourfirstname.local
- Primary DNS Server 8.8.8.8
- Uncheck block RFC1918 Private Networks (Step 4)
- If you change the password, take steps to remember it

Your Windows 10 system, WKS01, should be able to ping your LAN's default gateway 10.0.5.2 and resolve and ping google.com

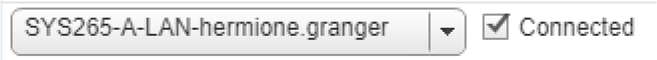


wks01-sys265-hermione.granger
fw01-hermione.hermione.local -
Champlain College | Degree Prog
https://www.champlain.edu
CHAMPLAIN COLLEGE
ABOUT CHAMPLAIN
FIND A PROGRAM
C:\Windows\System32\cmd.exe

```
Microsoft Windows [Version 10.0.17763.194]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>ping -n 1 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

Ping statistics for 10.0.5.2:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Windows\system32>ping -n 1 champlain.edu

Pinging champlain.edu [184.154.210.190] with 32 bytes of data:
Reply from 184.154.210.190: bytes=32 time=37ms TTL=239

Ping statistics for 184.154.210.190:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 37ms, Maximum = 37ms, Average = 37ms

C:\Windows\system32>
```

AD01 - Server Core

Make sure AD01 is on your SYS265-LAN network



SYS265-A-LAN-hermione.granger ☑ Connected

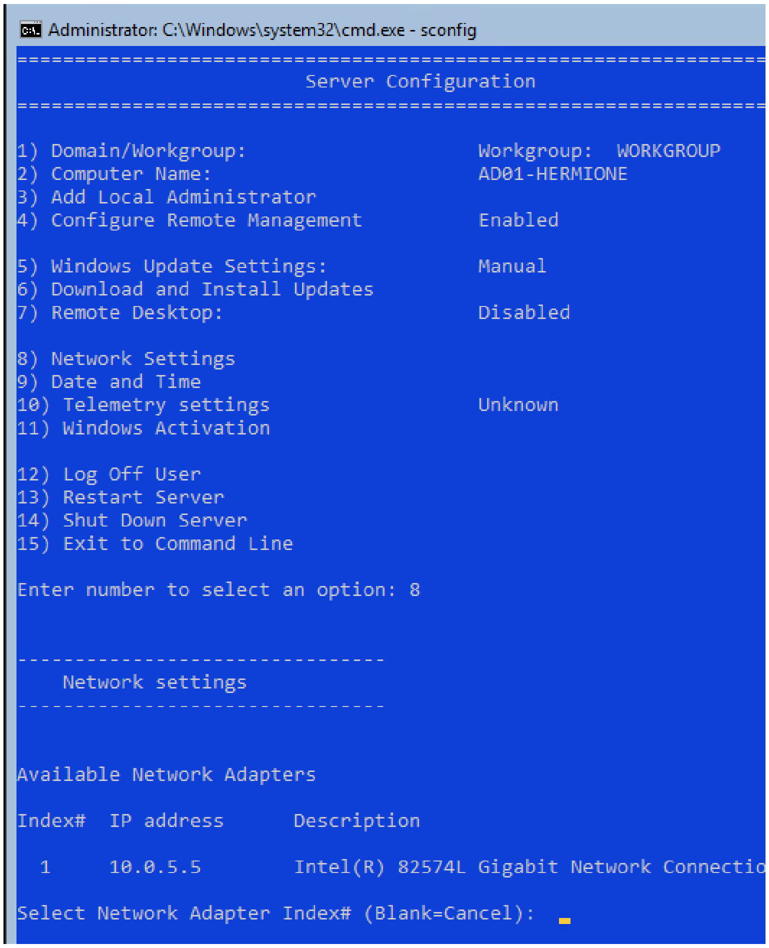
Change and record the new administrator password for the Server Core machine.
Using `sconfig`, configure the following:
Network Settings

- IP: 10.0.5.5
- Netmask: 255.255.255.0
- Gateway: 10.0.5.2
- Preferred DNS: 10.0.5.2

Computer Name: ad01-yourname
Manual Windows Update

💣This is important, renaming your server after AD installation is a recipe for disaster!

When rebooted, the sconfig screen should look similar to:



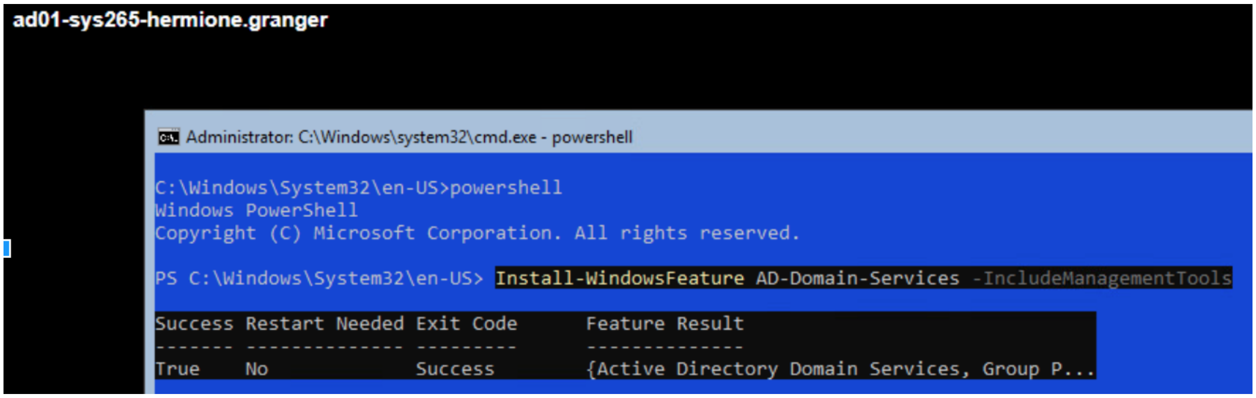
Administrator: C:\Windows\system32\cmd.exe - sconfig

```
===============================================================
                         Server Configuration
===============================================================

1) Domain/Workgroup:                        Workgroup:  WORKGROUP
2) Computer Name:                           AD01-HERMIONE
3) Add Local Administrator
4) Configure Remote Management              Enabled

5) Windows Update Settings:                 Manual
6) Download and Install Updates
7) Remote Desktop:                          Disabled

8) Network Settings
9) Date and Time
10) Telemetry settings                      Unknown
11) Windows Activation

12) Log Off User
13) Restart Server
14) Shut Down Server
15) Exit to Command Line

Enter number to select an option: 8


--------------------------------
    Network settings
--------------------------------


Available Network Adapters

Index#  IP address      Description

  1     10.0.5.5        Intel(R) 82574L Gigabit Network Connectio

Select Network Adapter Index# (Blank=Cancel):  _
```

Installing AD on Server Core.

In previous courses, you have relied on the GUI to install AD. This time, we will use powershell.

On AD01, invoke Powershell and use the CLI to install Active Directory and create a new Forest with a Domain Name of yourfirstname.local (not hermione.local…)

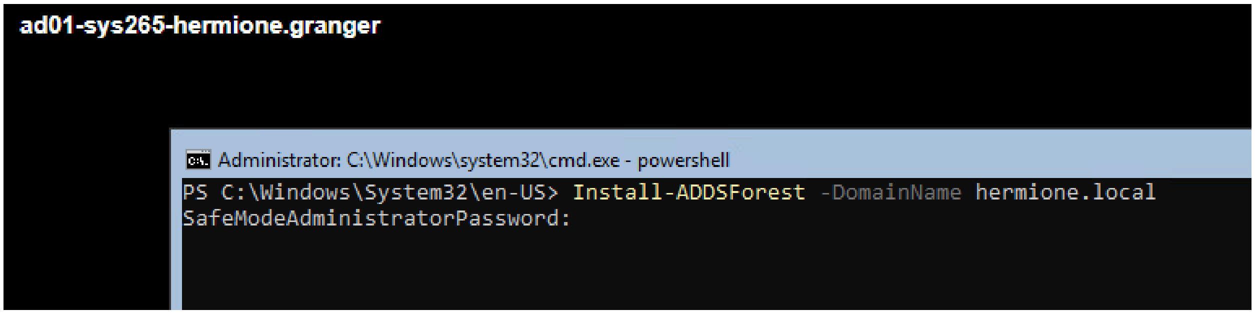


ad01-sys265-hermione.granger

Administrator: C:\Windows\system32\cmd.exe - powershell

```
C:\Windows\System32\en-US>powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Windows\System32\en-US> Install-WindowsFeature AD-Domain-Services -IncludeManagementTools

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             Success        {Active Directory Domain Services, Group P...
```

Install the Forest with the following command:



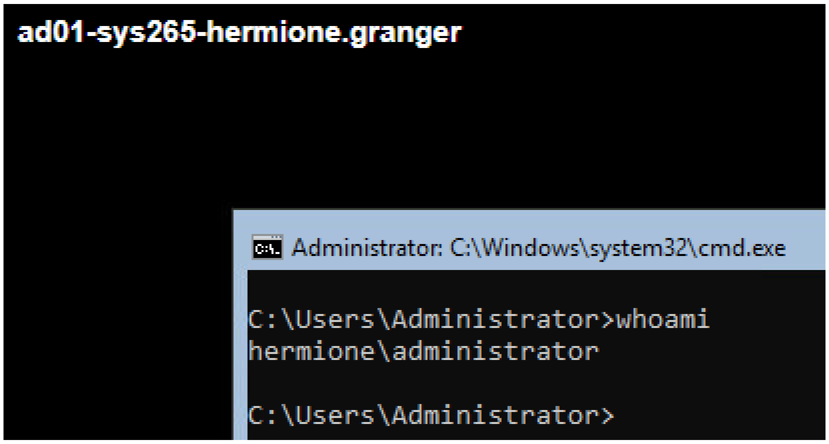
ad01-sys265-hermione.granger

Administrator: C:\Windows\system32\cmd.exe - powershell

```
PS C:\Windows\System32\en-US> Install-ADDSForest -DomainName hermione.local
SafeModeAdministratorPassword:
```

Read through the install prompts, and it will take some moments & of course an auto reboot.

When complete, you should be able to show that you are the Domain Admin account of yourname.local, and NOT the Local Admin Pre-AD account (this Local Admin account is suppressed on Domain Controllers, but not on Member Servers or Clients):



ad01-sys265-hermione.granger

Administrator: C:\Windows\system32\cmd.exe

```
C:\Users\Administrator>whoami
hermione\administrator

C:\Users\Administrator>
```

Configure MGMT01

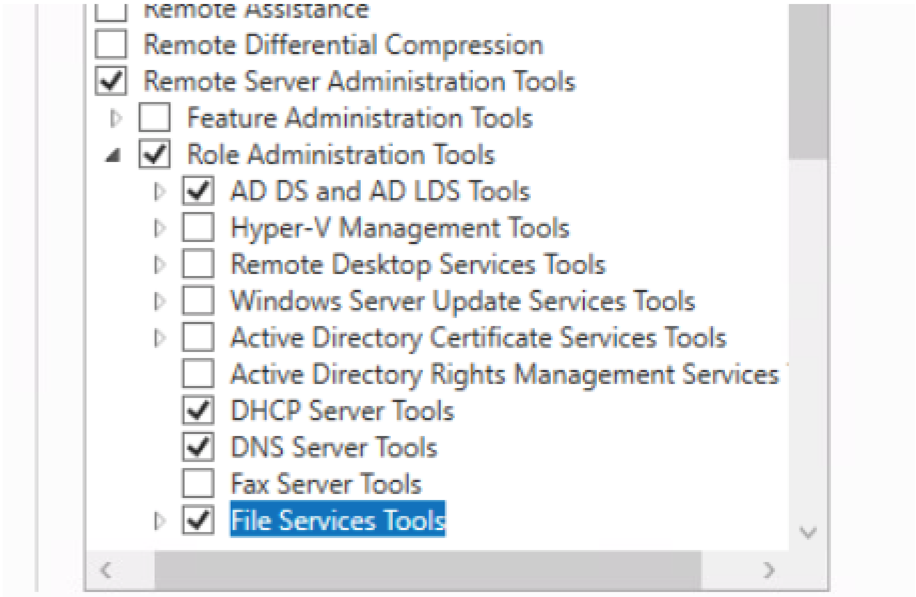
MGMT01 is a Server 2019 with GUI. Its job will be to remotely manage any server core systems. It should be configured with Network Adapter 1 on SYS265-LAN-your.name just like the other LAN based VMs.

> 💡If you are asked for an activation key, skip that option.

- Using sconfig from command prompt, make updates manual
- MGMT01 should have the IP address of 10.0.5.10
- gateway of 10.0.5.2
- DNS should be set to the IP of ad01(10.0.5.5)
- Hostname should be mgmt01-firstname
- Join it to yourname.local

After rebooting mgmt01, make sure you login to the domain and not the local host.

On MGMT01, figure out how to Install the following Features on mgmt01:



- □ Remote Assistance
- □ Remote Differential Compression
- ☑ Remote Server Administration Tools
  - □ Feature Administration Tools
  - ☑ Role Administration Tools
    - ☑ AD DS and AD LDS Tools
    - □ Hyper-V Management Tools
    - □ Remote Desktop Services Tools
    - □ Windows Server Update Services Tools
    - □ Active Directory Certificate Services Tools
    - □ Active Directory Rights Management Services
    - ☑ DHCP Server Tools
    - ☑ DNS Server Tools
    - □ Fax Server Tools
    - ☑ File Services Tools

Using Server Manager on mgmt01, add ad01 to the list of managed servers.

Domain Users

Using Active Directory Users and Computers, create the following named users
first.lastname (normal user)
first.lastname-adm (named domain admin)

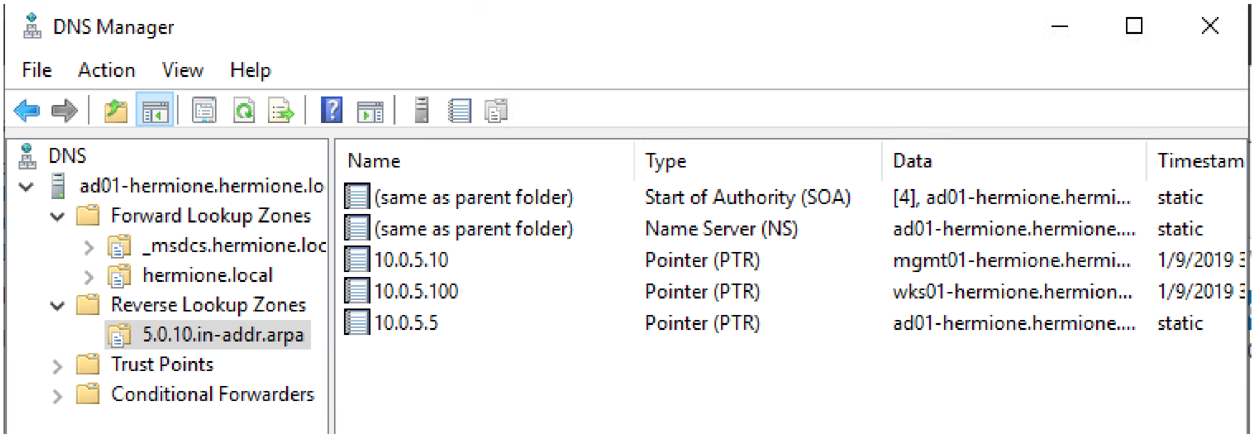
Add your -adm account to the Domain Admins group

DNS

Create a Reverse Lookup Zone for the 10.0.5 network

Create an A record and PTR record for fw01-yourname

Manually add the PTR records for ad01 and mgmt01. Your PTR records should look similar to this:



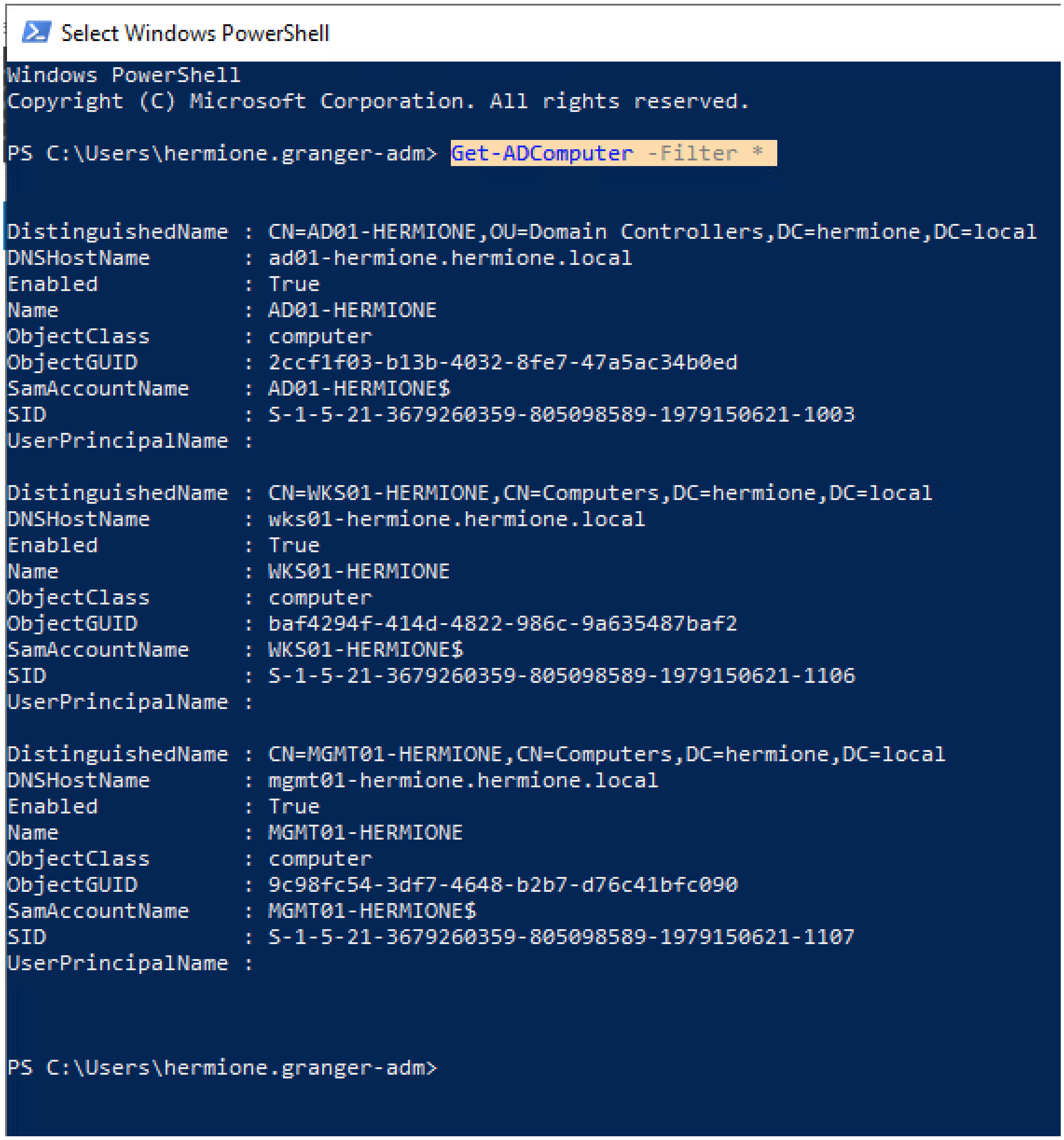
Name	Type	Data	Timestam
(same as parent folder)	Start of Authority (SOA)	[4], ad01-hermione.hermi...	static
(same as parent folder)	Name Server (NS)	ad01-hermione.hermione....	static
10.0.5.10	Pointer (PTR)	mgmt01-hermione.hermi...	1/9/2019 3
10.0.5.100	Pointer (PTR)	wks01-hermione.hermion...	1/9/2019 3
10.0.5.5	Pointer (PTR)	ad01-hermione.hermione....	static

On MGMT01, logout and then re-login as your -adm@yourdomain account.

Joining WKS01 to the domain

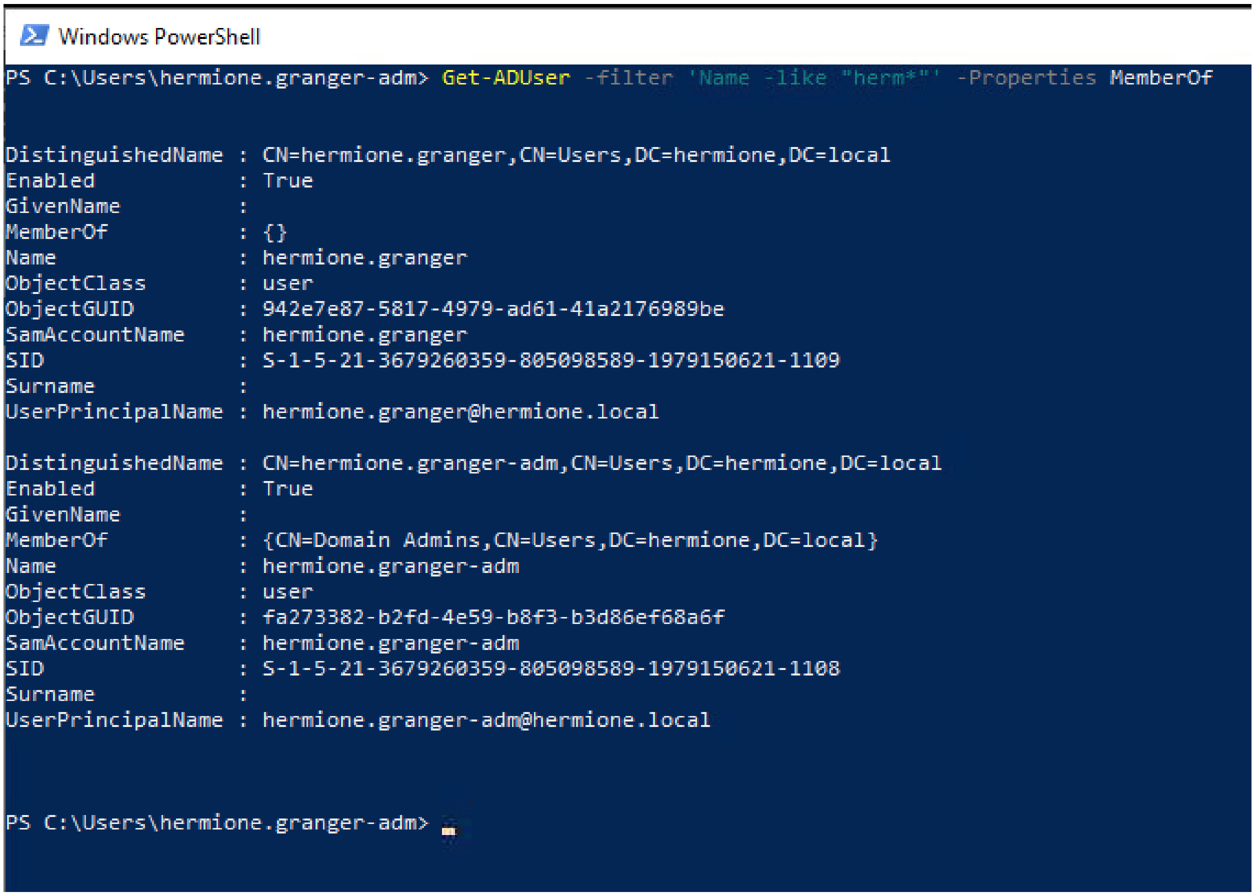
Go ahead and join wks01 to the domain as your Named Domain user. **What needs to be changed to facilitate these changes?**

Deliverable 1: Invoke powershell on mgmt01 and query the active directory for your three Windows computers:



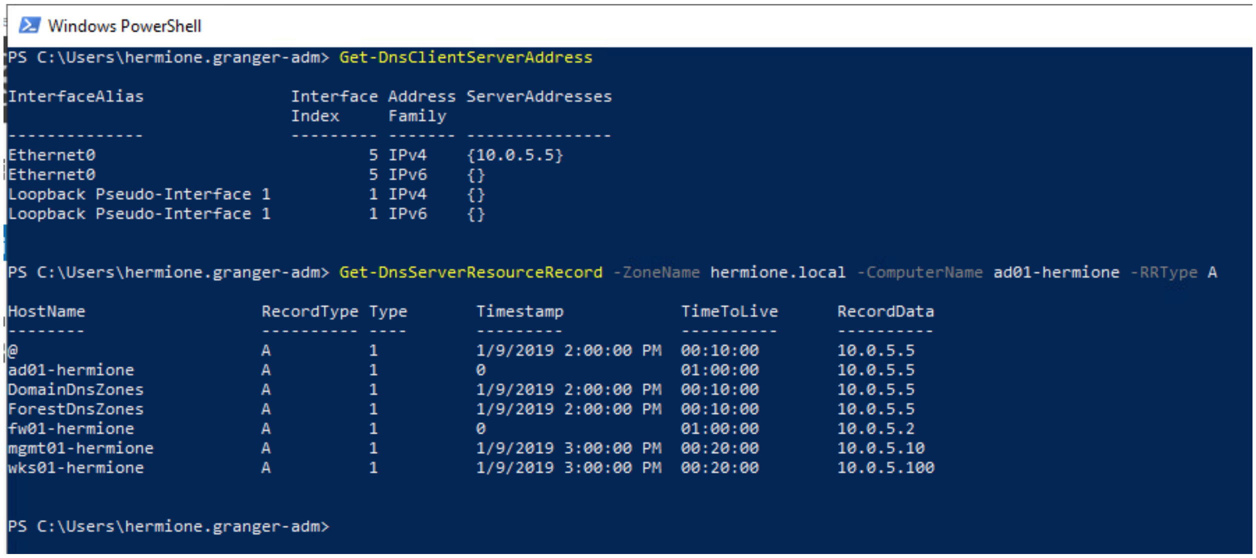
```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\hermione.granger-adm> Get-ADComputer -Filter *


DistinguishedName : CN=AD01-HERMIONE,OU=Domain Controllers,DC=hermione,DC=local
DNSHostName       : ad01-hermione.hermione.local
Enabled           : True
Name              : AD01-HERMIONE
ObjectClass       : computer
ObjectGUID        : 2ccf1f03-b13b-4032-8fe7-47a5ac34b0ed
SamAccountName    : AD01-HERMIONE$
SID               : S-1-5-21-3679260359-805098589-1979150621-1003
UserPrincipalName :

DistinguishedName : CN=WKS01-HERMIONE,CN=Computers,DC=hermione,DC=local
DNSHostName       : wks01-hermione.hermione.local
Enabled           : True
Name              : WKS01-HERMIONE
ObjectClass       : computer
ObjectGUID        : baf4294f-414d-4822-986c-9a635487baf2
SamAccountName    : WKS01-HERMIONE$
SID               : S-1-5-21-3679260359-805098589-1979150621-1106
UserPrincipalName :

DistinguishedName : CN=MGMT01-HERMIONE,CN=Computers,DC=hermione,DC=local
DNSHostName       : mgmt01-hermione.hermione.local
Enabled           : True
Name              : MGMT01-HERMIONE
ObjectClass       : computer
ObjectGUID        : 9c98fc54-3df7-4648-b2b7-d76c41bfc090
SamAccountName    : MGMT01-HERMIONE$
SID               : S-1-5-21-3679260359-805098589-1979150621-1107
UserPrincipalName :



PS C:\Users\hermione.granger-adm>
```

Deliverable 2: Enumerate your two named Domain Users (adjust filter for your name)



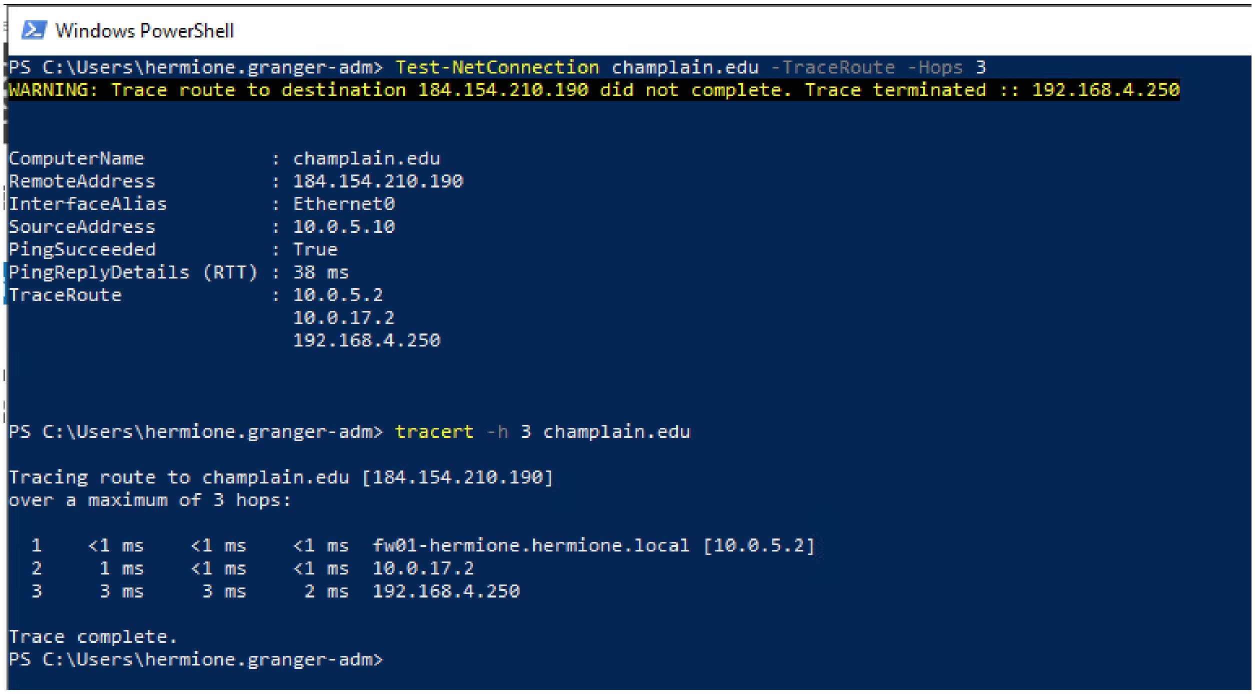
```
PS C:\Users\hermione.granger-adm> Get-ADUser -filter 'Name -like "herm*"' -Properties MemberOf


DistinguishedName : CN=hermione.granger,CN=Users,DC=hermione,DC=local
Enabled           : True
GivenName         :
MemberOf          : {}
Name              : hermione.granger
ObjectClass       : user
ObjectGUID        : 942e7e87-5817-4979-ad61-41a2176989be
SamAccountName    : hermione.granger
SID               : S-1-5-21-3679260359-805098589-1979150621-1109
Surname           :
UserPrincipalName : hermione.granger@hermione.local

DistinguishedName : CN=hermione.granger-adm,CN=Users,DC=hermione,DC=local
Enabled           : True
GivenName         :
MemberOf          : {CN=Domain Admins,CN=Users,DC=hermione,DC=local}
Name              : hermione.granger-adm
ObjectClass       : user
ObjectGUID        : fa273382-b2fd-4e59-b8f3-b3d86ef68a6f
SamAccountName    : hermione.granger-adm
SID               : S-1-5-21-3679260359-805098589-1979150621-1108
Surname           :
UserPrincipalName : hermione.granger-adm@hermione.local



PS C:\Users\hermione.granger-adm>
```

Deliverable 3: Print your DNS Server address and DNS A Records.



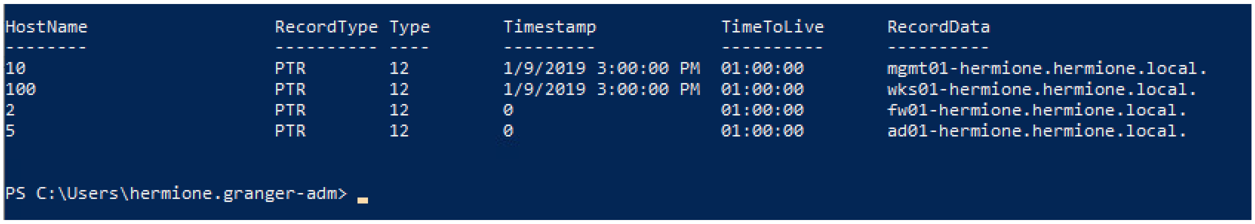
```
PS C:\Users\hermione.granger-adm> Get-DnsClientServerAddress

InterfaceAlias               Interface Address ServerAddresses
                             Index     Family
--------------               --------- ------- ---------------
Ethernet0                            5 IPv4    {10.0.5.5}
Ethernet0                            5 IPv6    {}
Loopback Pseudo-Interface 1          1 IPv4    {}
Loopback Pseudo-Interface 1          1 IPv6    {}


PS C:\Users\hermione.granger-adm> Get-DnsServerResourceRecord -ZoneName hermione.local -ComputerName ad01-hermione -RRType A

HostName                  RecordType Type       Timestamp            TimeToLive      RecordData
--------                  ---------- ----       ---------            ----------      ----------
@                         A          1          1/9/2019 2:00:00 PM  00:10:00        10.0.5.5
ad01-hermione             A          1          0                    01:00:00        10.0.5.5
DomainDnsZones            A          1          1/9/2019 2:00:00 PM  00:10:00        10.0.5.5
ForestDnsZones            A          1          1/9/2019 2:00:00 PM  00:10:00        10.0.5.5
fw01-hermione             A          1          0                    01:00:00        10.0.5.2
mgmt01-hermione           A          1          1/9/2019 3:00:00 PM  00:20:00        10.0.5.10
wks01-hermione            A          1          1/9/2019 3:00:00 PM  00:20:00        10.0.5.100


PS C:\Users\hermione.granger-adm>
```

Deliverable 4: Check the first 3 hops of your route. Your network route should go through fw01's LAN interface(10.0.5.2) to the WAN default gateway 10.0.17.2 and then out through the CYBER.LOCAL default gateway on the 192.168.4.0/24 Network. You can use the powershell or the traditional tracert method. Provide a screenshot.



```
PS C:\Users\hermione.granger-adm> Test-NetConnection champlain.edu -TraceRoute -Hops 3
WARNING: Trace route to destination 184.154.210.190 did not complete. Trace terminated :: 192.168.4.250


ComputerName           : champlain.edu
RemoteAddress          : 184.154.210.190
InterfaceAlias         : Ethernet0
SourceAddress          : 10.0.5.10
PingSucceeded          : True
PingReplyDetails (RTT) : 38 ms
TraceRoute             : 10.0.5.2
                         10.0.17.2
                         192.168.4.250



PS C:\Users\hermione.granger-adm> tracert -h 3 champlain.edu

Tracing route to champlain.edu [184.154.210.190]
over a maximum of 3 hops:

  1    <1 ms    <1 ms    <1 ms  fw01-hermione.hermione.local [10.0.5.2]
  2     1 ms    <1 ms    <1 ms  10.0.17.2
  3     3 ms     3 ms     2 ms  192.168.4.250

Trace complete.
PS C:\Users\hermione.granger-adm>
```

Deliverable 5: Deliverable 3 asked for A records. Figure out how to enumerate all the PTR records. Provide the command and output ptr records. Here's what the output should look like:



```
HostName                  RecordType Type       Timestamp            TimeToLive      RecordData
--------                  ---------- ----       ---------            ----------      ----------
10                        PTR        12         1/9/2019 3:00:00 PM  01:00:00        mgmt01-hermione.hermione.local.
100                       PTR        12         1/9/2019 3:00:00 PM  01:00:00        wks01-hermione.hermione.local.
2                         PTR        12         0                    01:00:00        fw01-hermione.hermione.local.
5                         PTR        12         0                    01:00:00        ad01-hermione.hermione.local.


PS C:\Users\hermione.granger-adm> _
```

Deliverable 6: Tech Journal - This is similar to last term. This week’s journal should include a course journal page for SYS265 that has an initial entry, and include your notes from your environment configuration (in far more detail than the example). Make sure you include a list of at least 3 terms or topics from the lecture or lab that you want to learn more about, and your research results. Be sure to add your instructor’s GitHub account as a collaborator if your wiki is not public.

Deliverable 7. Your deliverable meets the submission guidelines.