

made with mematic

ASSIGNMENT 6
Installing A Domain Controller

shelby armitage
W0491348

OSYS1200 – INTRO TO WINDOWS ADMINISTRATION

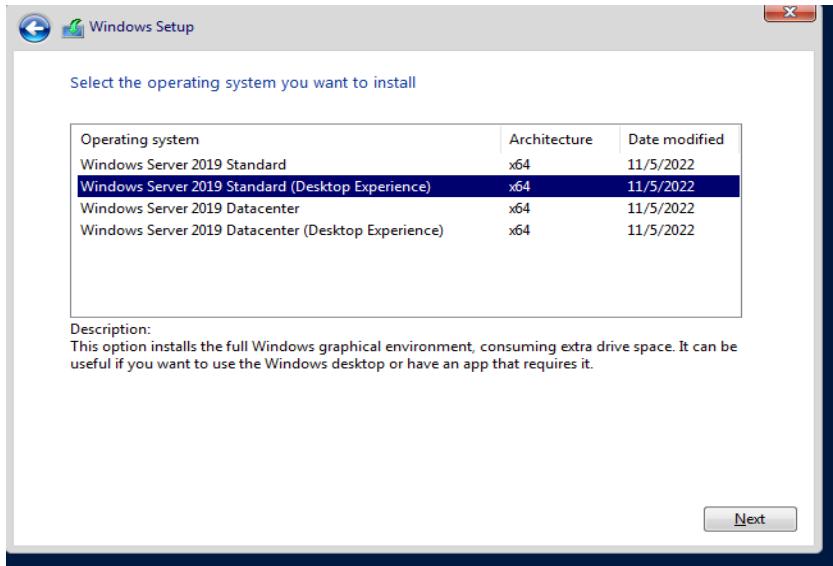
December 6th, 2023

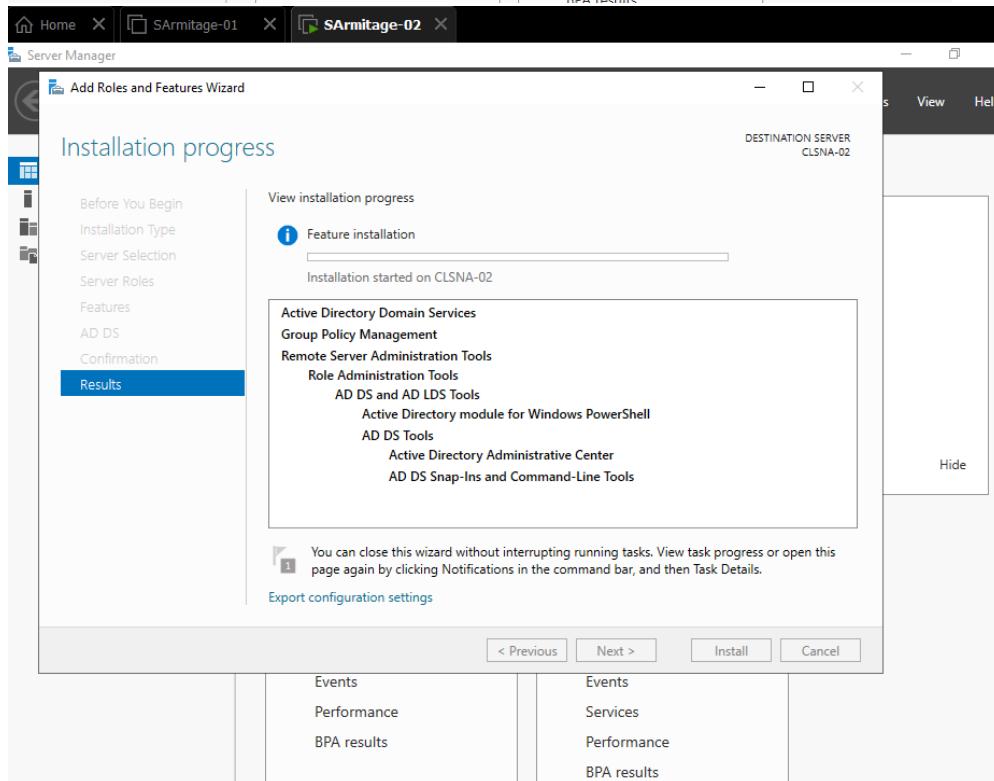
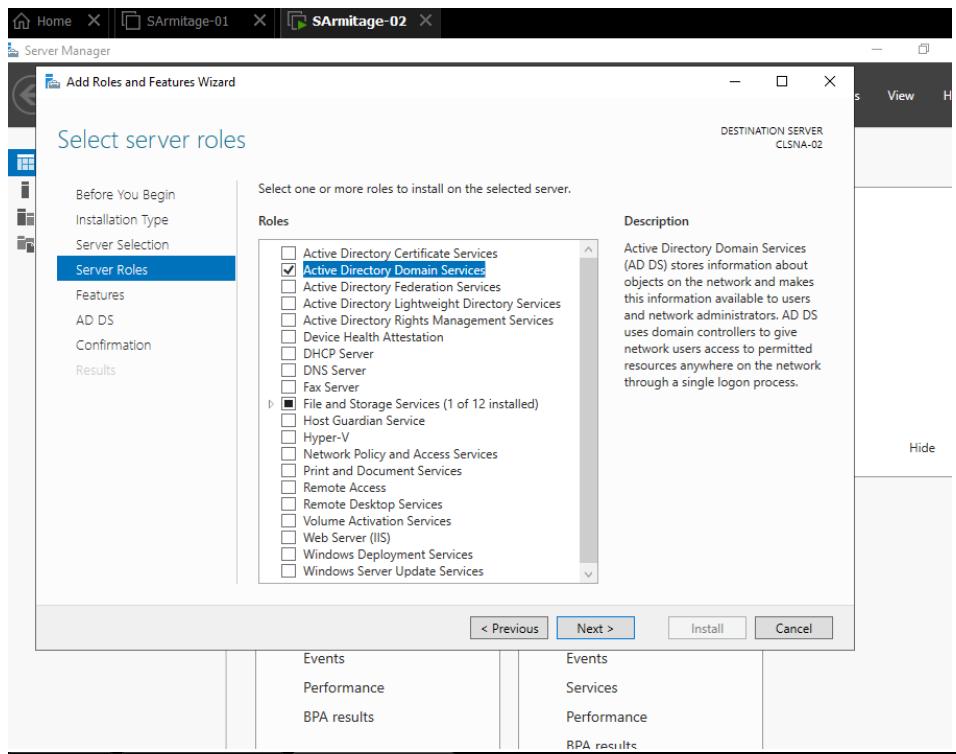
Table of Contents

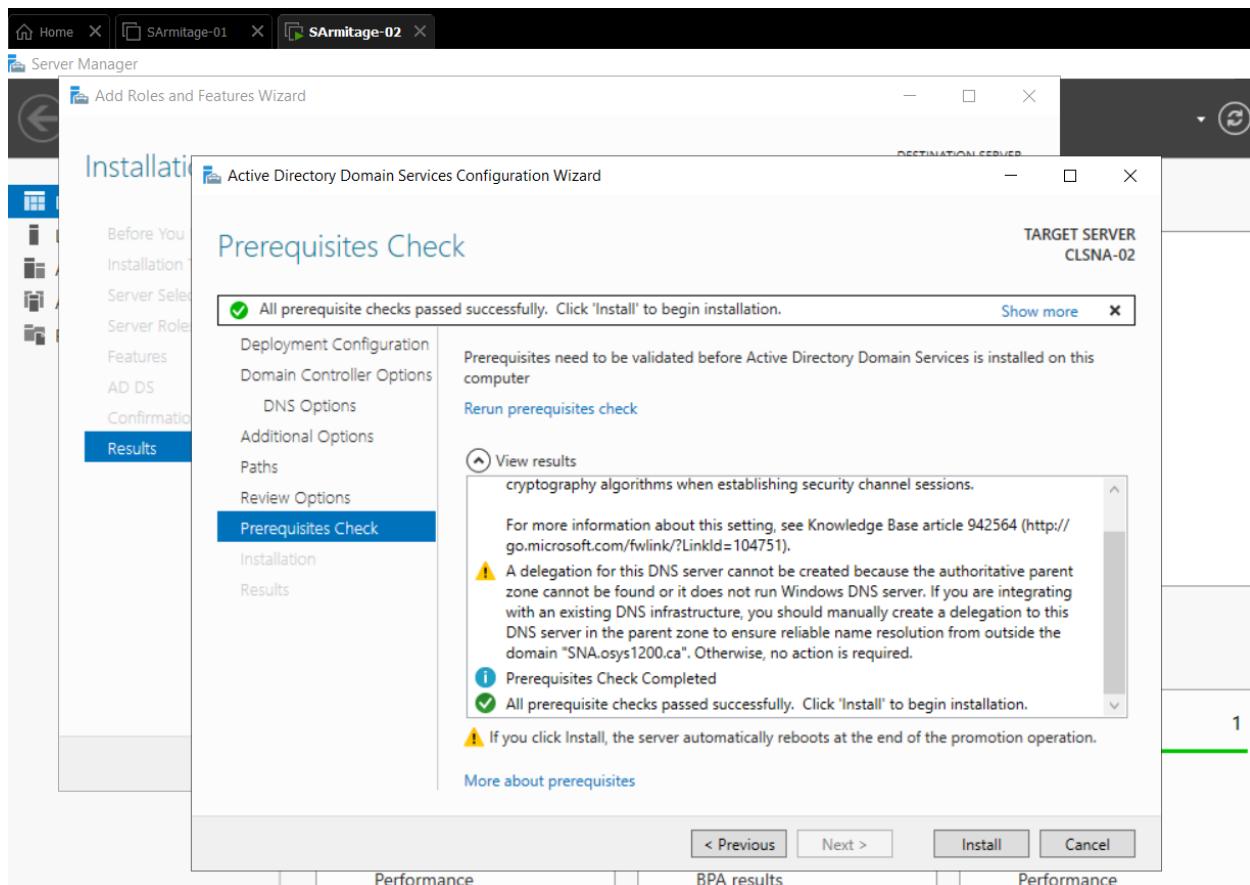
Part 1 – Installing A Domain Controller.....	1
Task 2 – Adding A Workstation As A Client And Working With Group Policy	5
Task 3 – Remote Control	17
Task 4 – Backup and Documentation	21
Conclusion.....	22

Part 1 – Installing A Domain Controller

Activity 10—1. I've taken screenshots as a step-by-step process in how I was able to install my server. I'll list them in order of operation accordingly and make any notes in troubleshooting processes I took.







This last picture is to show that all the steps I took above it worked and passed the prerequisite check to install the server on my new VM, listed as SArmitage-02 (CLSNA-02).

Administrator: Windows PowerShell ISE

```
PS C:\Users\Administrator> GC env:computername
CLSNA-02

PS C:\Users\Administrator> Get-ADDomain

AllowedDNSSuffixes      : {}
ChildDomains             : {}
ComputersContainer       : CN=Computers,DC=SNA,DC=osys1200,DC=ca
DeletedObjectsContainer  : CN=Deleted Objects,DC=SNA,DC=osys1200,DC=ca
DistinguishedName        : DC=SNA,DC=osys1200,DC=ca
DNSRoot                  : SNA.osys1200.ca
DomainControllersContainer: OU=Domain Controllers,DC=SNA,DC=osys1200,DC=ca
DomainMode                : Windows2016Domain
DomainSID                 : S-1-5-21-2577330542-3762217335-1836882770
ForeignSecurityPrincipalsContainer: CN=ForeignSecurityPrincipals,DC=SNA,DC=osys1200,DC=ca
Forest                   : SNA.osys1200.ca
InfrastructureMaster      : CLSNA-02.SNA.osys1200.ca
LastLogonReplicationInterval: {CN={31B2F340-0160-11D2-945F-00C04FB984F9},CN=Polices,CN=System,DC=SNA,DC=osys1200,DC=ca}
LinkedGroupPolicyObjects  : CN=LostAndFound,DC=SNA,DC=osys1200,DC=ca
LostAndFoundContainer     :
Managedby                :
Name                      : SNA
NetBIOSName               : SNA
ObjectClass                : domainDNS
ObjectGUID                 : fc997f03-b8da-422a-9eed-d0d2aa41e1ed
ParentDomain               : CLSNA-02.SNA.osys1200.ca
PDCEmulator                : True
PublicKeyRequiredPasswordRolling: CN=NTDS Quotas,DC=SNA,DC=osys1200,DC=ca
QuotasContainer            : {}
ReadOnlyReplicaDirectoryServers: {CLSNA-02.SNA.osys1200.ca}
ReplicaDirectoryServers    : CLSNA-02.SNA.osys1200.ca
RIDMaster                  : {DC=ForestDnsZones,DC=SNA,DC=osys1200,DC=ca, DC=DomainDnsZones,DC=SNA,DC=osys1200,DC=ca, CN=Configuration,DC=SNA,DC=osys1200,DC=ca}
SubordinateReferences      : CN=System,DC=SNA,DC=osys1200,DC=ca
SystemsContainer            : CN=Users,DC=SNA,DC=osys1200,DC=ca
UsersContainer              : 
```

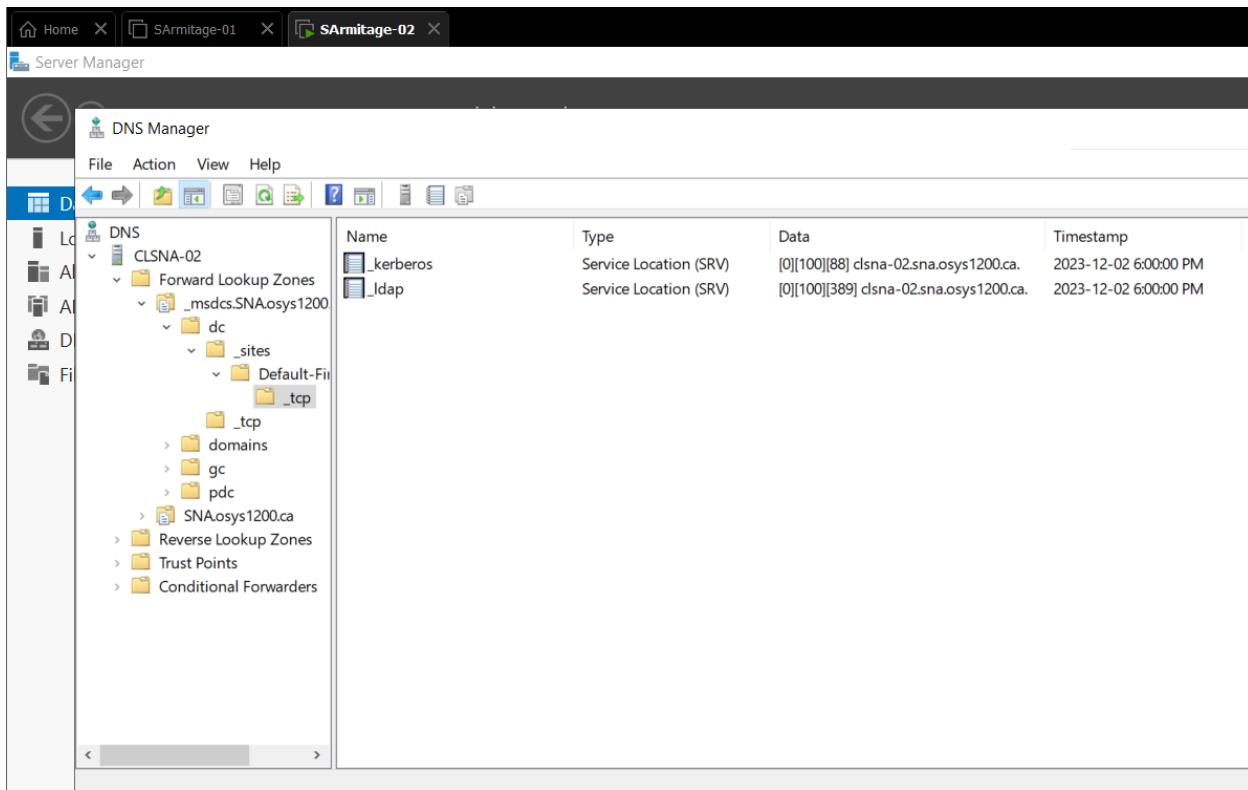
```
PS C:\Users\Administrator> Get-NetIPConfiguration

InterfaceAlias      : Ethernet0
InterfaceIndex       : 3
InterfaceDescription: Intel(R) 82574L Gigabit Network Connection
NetProfile.Name     : Network
IPv4Address         : 192.168.220.131
IPv6DefaultGateway  :
IPv4DefaultGateway  : 192.168.220.2
DNSServer           : ::1
                           127.0.0.1

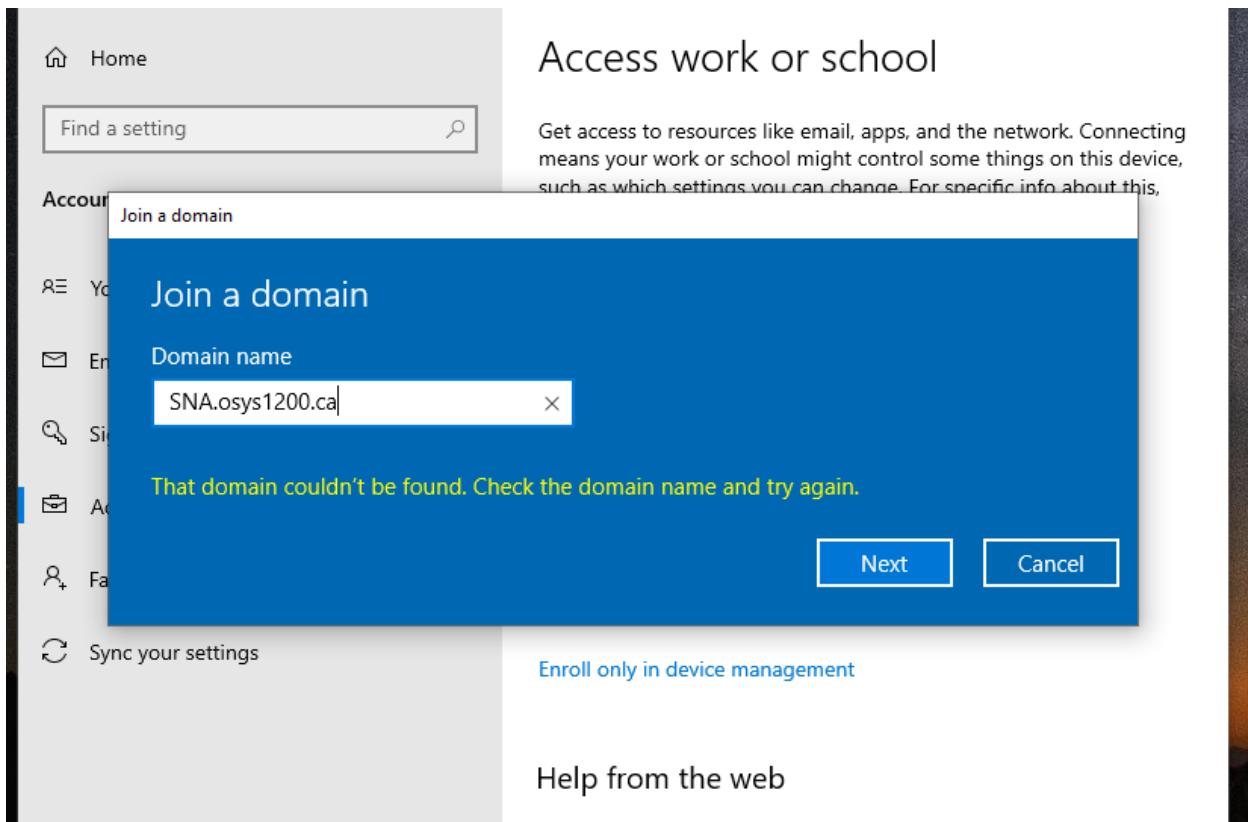
PS C:\Users\Administrator>
```

After task 42, I completed the following CMG Scripts in PowerShell.

Task 2 – Adding A Workstation As A Client And Working With Group Policy



Screenshot of activity 10-2 completed at step 6.



After getting the IP Domain error, I went into troubleshooting mode and tested my IP settings in various ways to try and gain access to it. I never want to see this error again. 😊

```
C:\Users\SArmittage>ipconfig/all
Windows IP Configuration

Host Name . . . . . : CLSNA01
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : localdomain

Ethernet adapter Ethernet0:

Connection-specific DNS Suffix . . . . . : localdomain
Description . . . . . : Intel(R) 82574L Gigabit Network Connection
Physical Address. . . . . : 00-0C-29-58-A1-51
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::8833:54f5:1cf5:e400%15(PREFERRED)
IPv4 Address. . . . . : 192.168.220.136(PREFERRED)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : December 3, 2023 1:26:50 PM
Lease Expires . . . . . : December 3, 2023 1:56:50 PM
Default Gateway . . . . . : 192.168.220.2
DHCP Server . . . . . : 192.168.220.254
DHCPv6 IAID . . . . . : 100666409
DHCPv6 Client DUID. . . . . : 00-01-00-01-2C-BF-07-1C-00-0C-29-58-A1-51
DNS Servers . . . . . : 192.168.220.2
Primary WINS Server . . . . . : 192.168.220.2
NetBIOS over Tcpip. . . . . : Enabled

Ethernet adapter Bluetooth Network Connection:

Media State . . . . . : Media disconnected
```

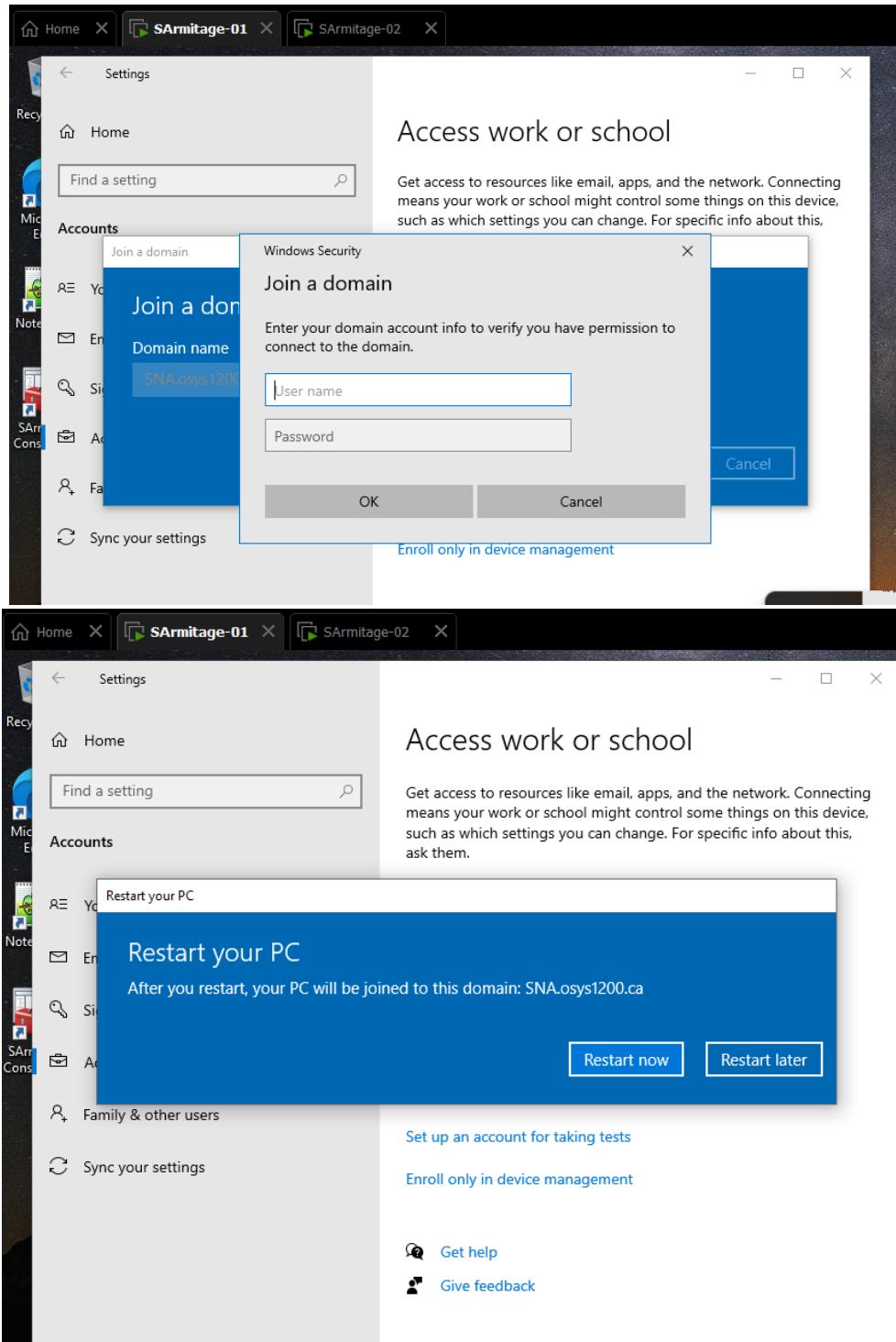
```
Windows IP Configuration

Host Name . . . . . : CLSNA-02
Primary Dns Suffix . . . . . : SNA.osys1200.ca
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : SNA.osys1200.ca

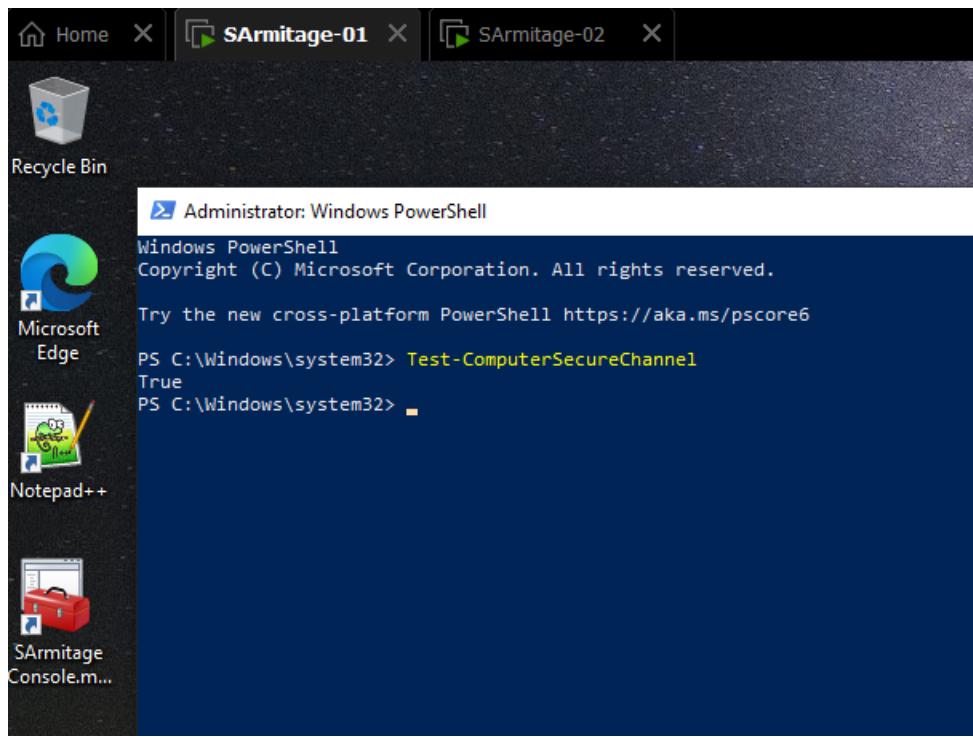
Ethernet adapter Ethernet0:

Connection-specific DNS Suffix . . . . . :
Description . . . . . : Intel(R) 82574L Gigabit Network Connection
Physical Address. . . . . : 00-0C-29-FD-5B-21
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::8311:eb54:684c:d315%3(PREFERRED)
Autoconfiguration IPv4 Address. . . . . : 169.254.242.219(PREFERRED)
Subnet Mask . . . . . : 255.255.0.0
IPv4 Address. . . . . : 192.168.220.136(Duplicate)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.220.2
DHCPv6 IAID . . . . . : 50334761
DHCPv6 Client DUID. . . . . : 00-01-00-01-2C-FD-57-BC-00-0C-29-FD-5B-21
DNS Servers . . . . . : ::1
192.168.220.2
127.0.0.1
NetBIOS over Tcpip. . . . . : Enabled
```

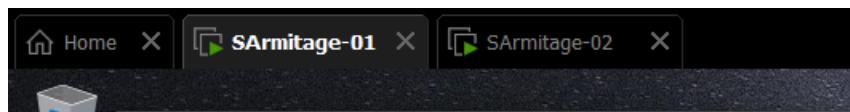
After realizing my original VM Workstation could not be manually changed, I had the server IP configured to exactly what my VM was set to, and manually configured the DNS on my workstation. Then voila!!!! I gained access!!!!



I had to make sure I properly documented this monumental success in case anything else were to go wrong, at least I made it in. 😊



Also a screenshot of the required prompt in step 10-3 to verify the trust relationship with my domain is working.



```
Administrator: Windows PowerShell
FrequencyCorrectRate: 4 (Local)
PollAdjustFactor: 5 (Local)
LargePhaseOffset: 50000000 (Local)
SpikeWatchPeriod: 900 (Local)
LocalClockDispersion: 10 (Local)
HoldPeriod: 5 (Local)
PhaseCorrectRate: 1 (Local)
UpdateInterval: 30000 (Local)

[TimeProviders]

NtpClient (Local)
DllName: C:\Windows\system32\w32time.dll (Local)
Enabled: 1 (Local)
InputProvider: 1 (Local)
CrossSiteSyncFlags: 2 (Local)
AllowNonstandardModeCombinations: 1 (Local)
ResolvePeerBackoffMinutes: 15 (Local)
ResolvePeerBackoffMaxTimes: 7 (Local)
CompatibilityFlags: 2147483648 (Local)
EventLogFlags: 1 (Local)
LargeSampleSkew: 3 (Local)
SpecialPollInterval: 3600 (Local)
Type: NT5DS (Local)

VMICTimeProvider (Local)
DllName: C:\Windows\System32\vmictimeprovider.dll (Local)
Enabled: 1 (Local)
InputProvider: 1 (Local)

NtpServer (Local)
DllName: C:\Windows\system32\w32time.dll (Local)
Enabled: 0 (Local)
InputProvider: 0 (Local)

PS C:\Windows\system32> w32tm /resync /rediscover
Sending resync command to local computer
The command completed successfully.
PS C:\Windows\system32>
```

Screenshot for 10-4 for new configuration settings in Windows Time Service.

The screenshot shows the Group Policy Management Editor interface. On the left, the navigation pane includes 'Local Server', 'All Servers', 'AD DS', 'DNS', and 'File and Storage'. The main pane displays the 'Ctrl+Alt+Del Options' section under 'User Configuration / Policies / Administrative Templates / System / Ctrl+Alt+Del Options'. A specific policy named 'Remove Task Manager' is selected. The right pane shows the configuration details:

Setting	State	Comment
Remove Change Password	Not configured	No
Remove Lock Computer	Not configured	No
Remove Task Manager	Enabled	No
Remove Logoff	Not configured	No

Description: This policy setting prevents users from starting Task Manager.

Task Manager (taskmgr.exe) lets users start and stop programs; monitor the performance of their computers; view and monitor all programs running on their computers, including system services; find the executable names of programs; and change the priority of the process in which programs run.

If you enable this policy setting, users will not be able to access Task Manager. If users try to start Task Manager, a message appears explaining that a policy prevents it.

Completed step 20 in Activity 10-5, showing I have enabled the setting to remove Task Manager.

The screenshot shows a Windows desktop environment. On the left, there are icons for 'Recycle Bin', 'Microsoft Edge', and 'Notepad++'. On the right, a 'Windows PowerShell' window is open, showing the following command and output:

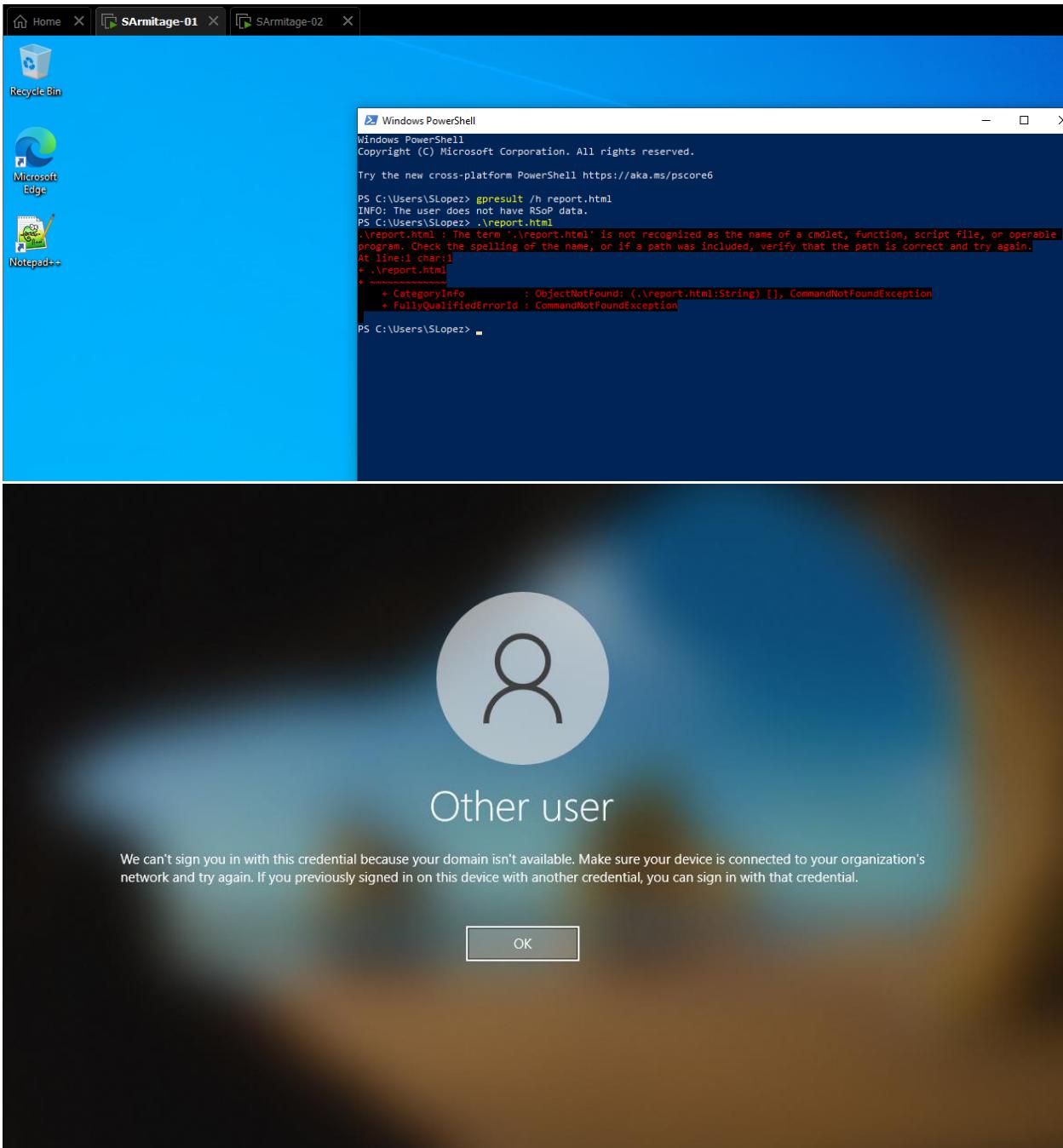
```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\SLopez> Get-WMIObject -class Win32_ComputerSystem | select username
username
-----
SNA\SLopez

PS C:\Users\SLopez>
```

And the results of the CMDLET required as SLopez.





Other user

CLSNA01/SArmitage

Password

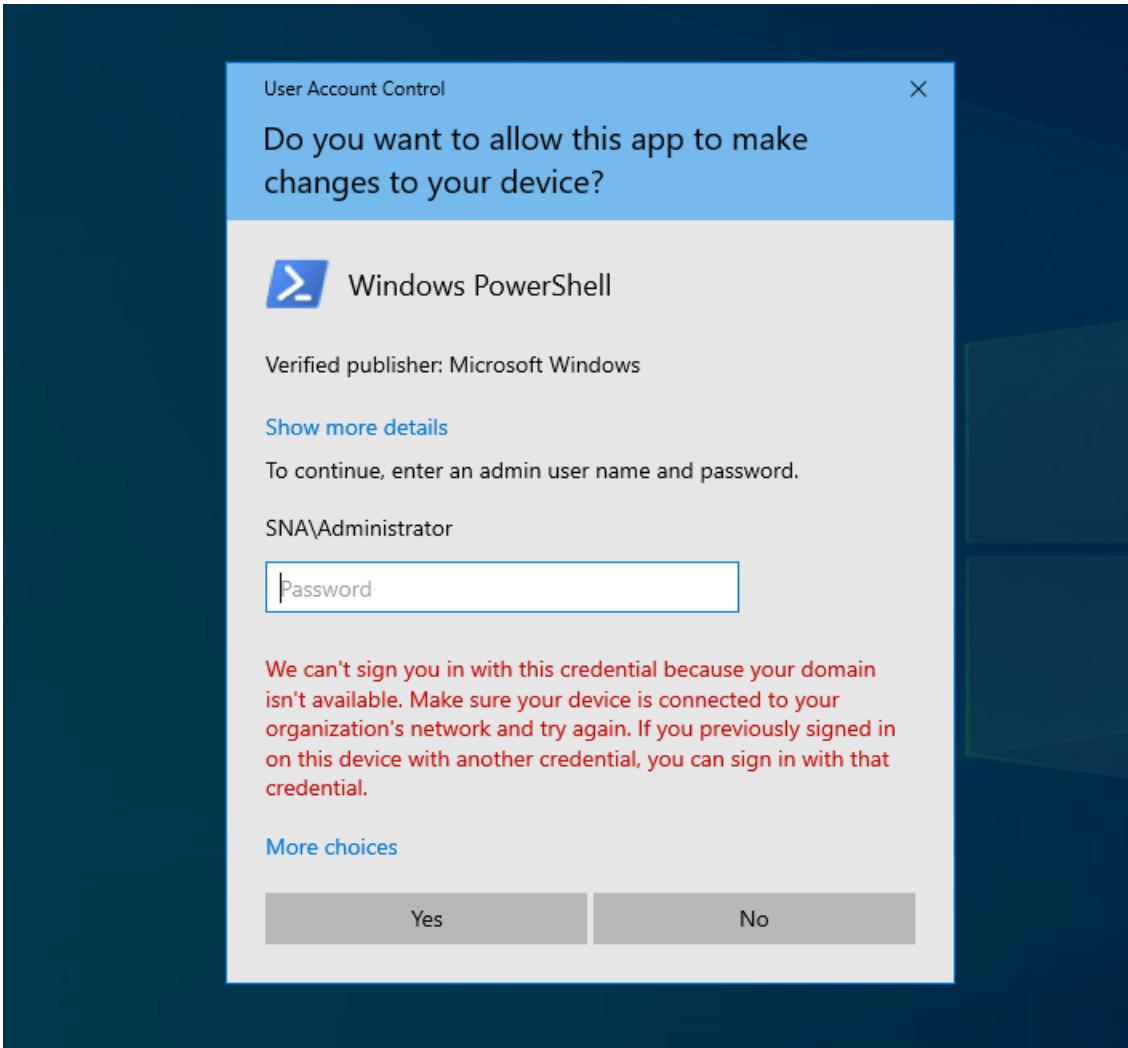


Sign in to: SNA

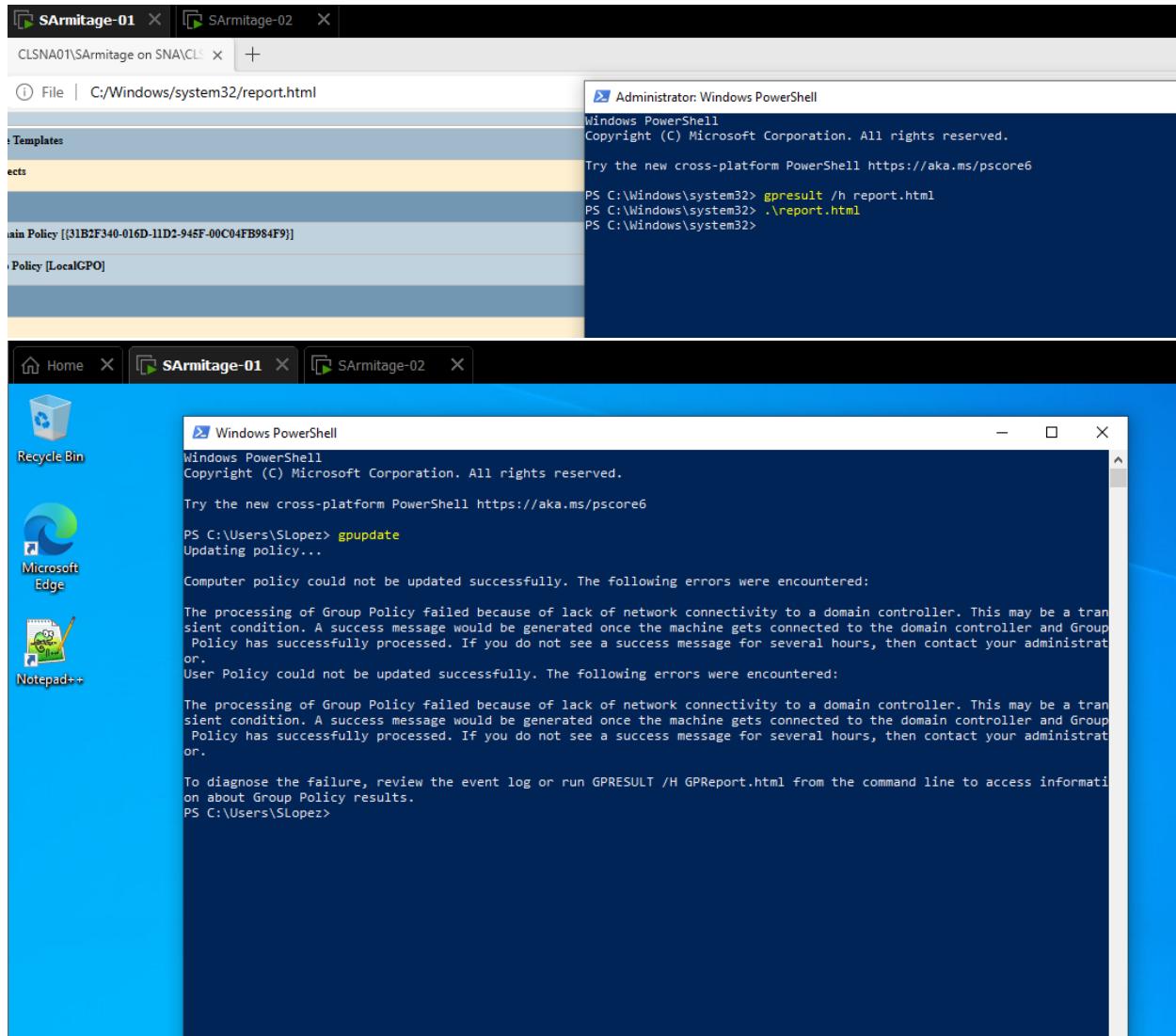
How do I sign in to another domain?

Type domain name\domain user name to
sign in to another domain.

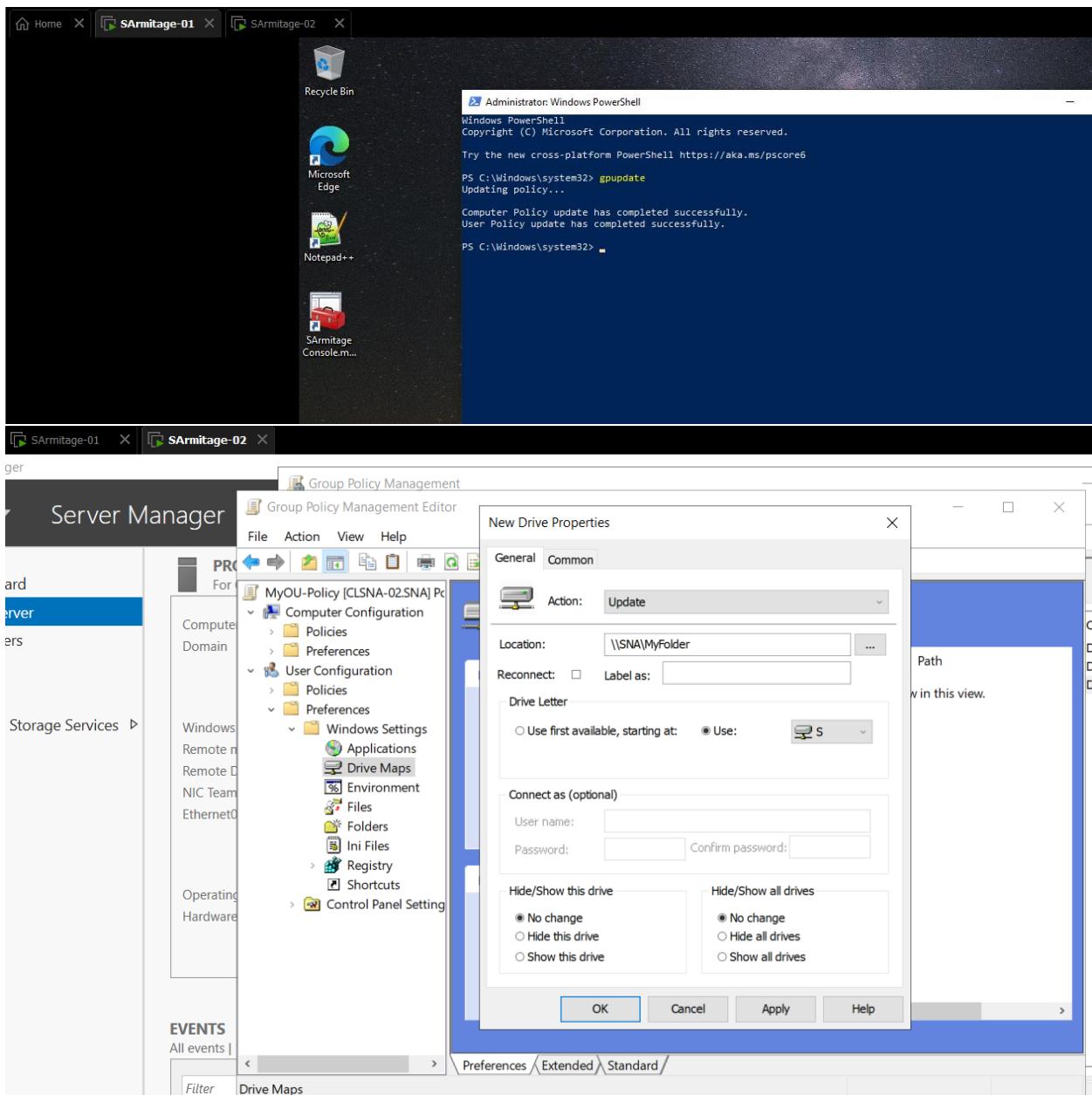
Type CLSNA01\local user name to sign in to
this PC only (not a domain).



The above screenshots are what I emailed you about, my VM was not able to allow me to perform the required tasks as SLopez as it wasn't allowing me to grant permission using my admin privileges. For the required script, I needed to be on my admin account to generate it. Below is a screenshot of me doing that in my admin account, and you will have the document separately in the drop box.

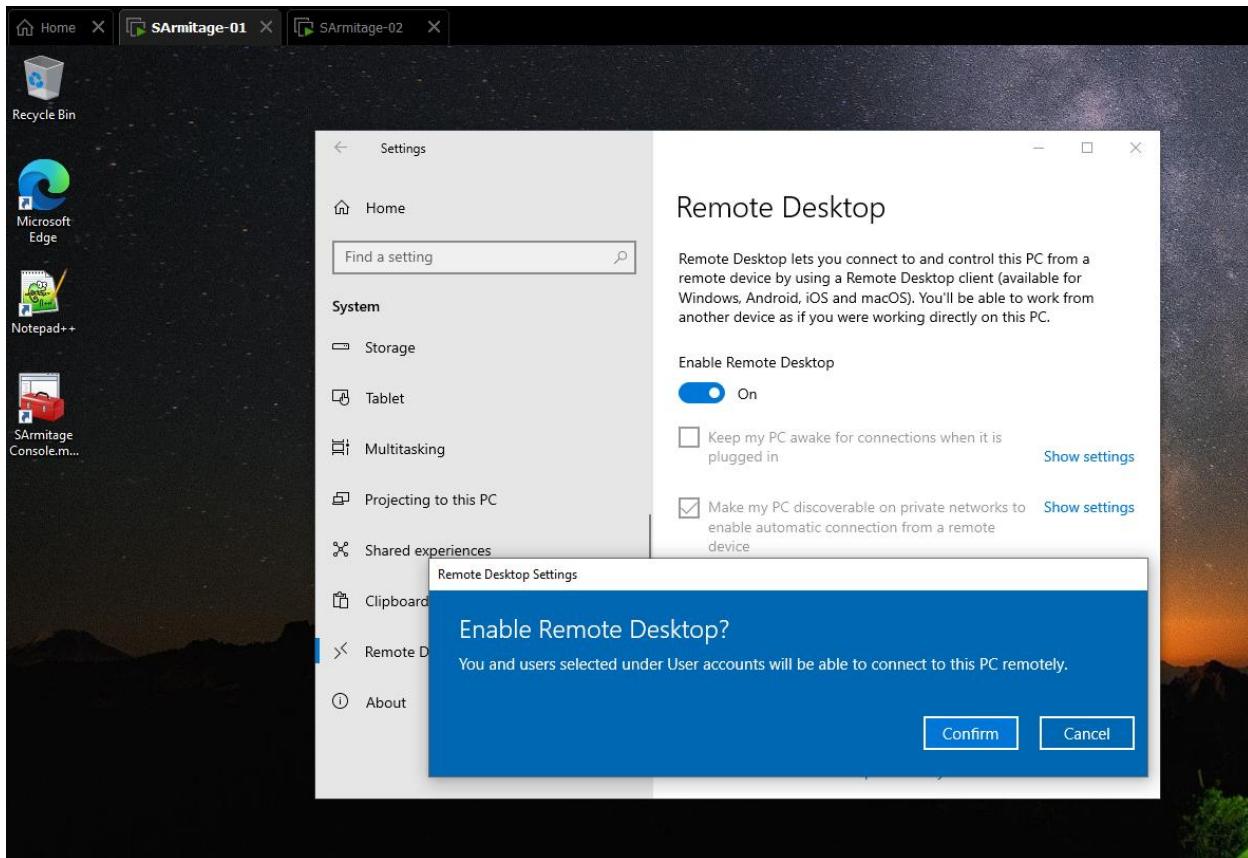


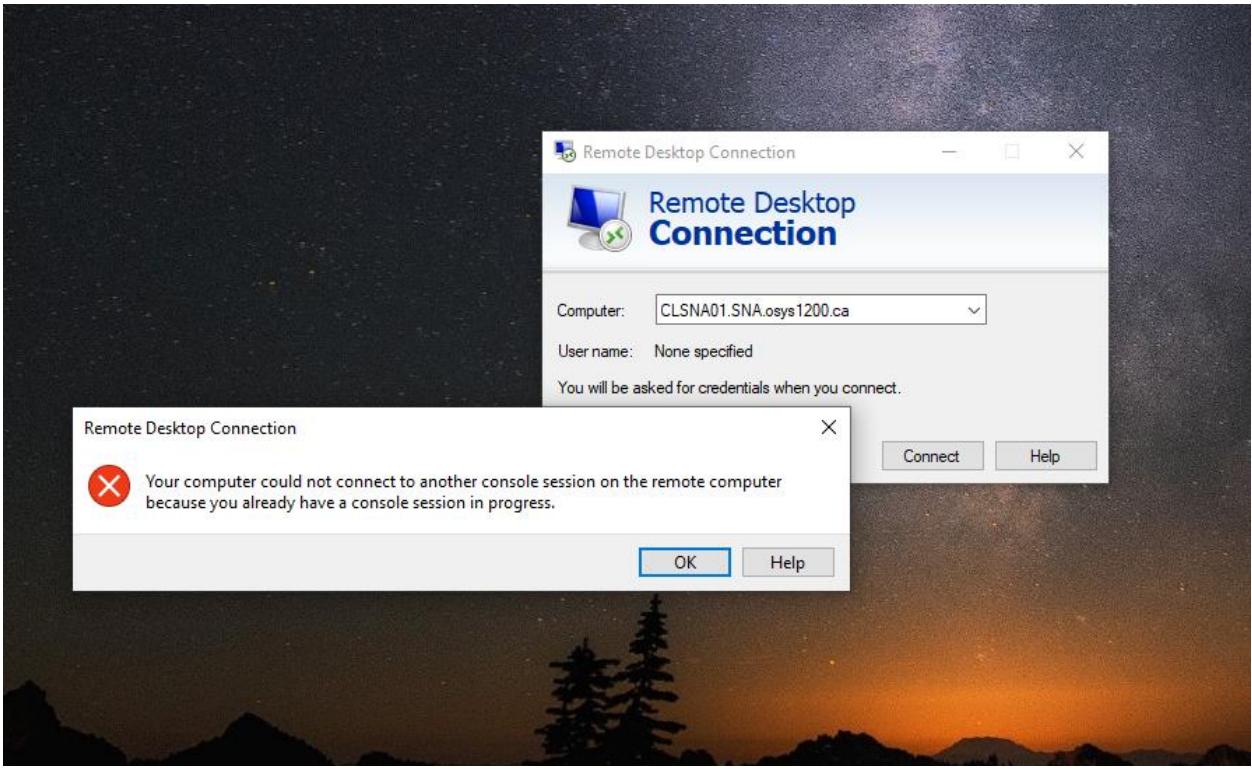
Again, I could not run these commands as SLopez due to the same issue above. I ran it using my admin account once again.



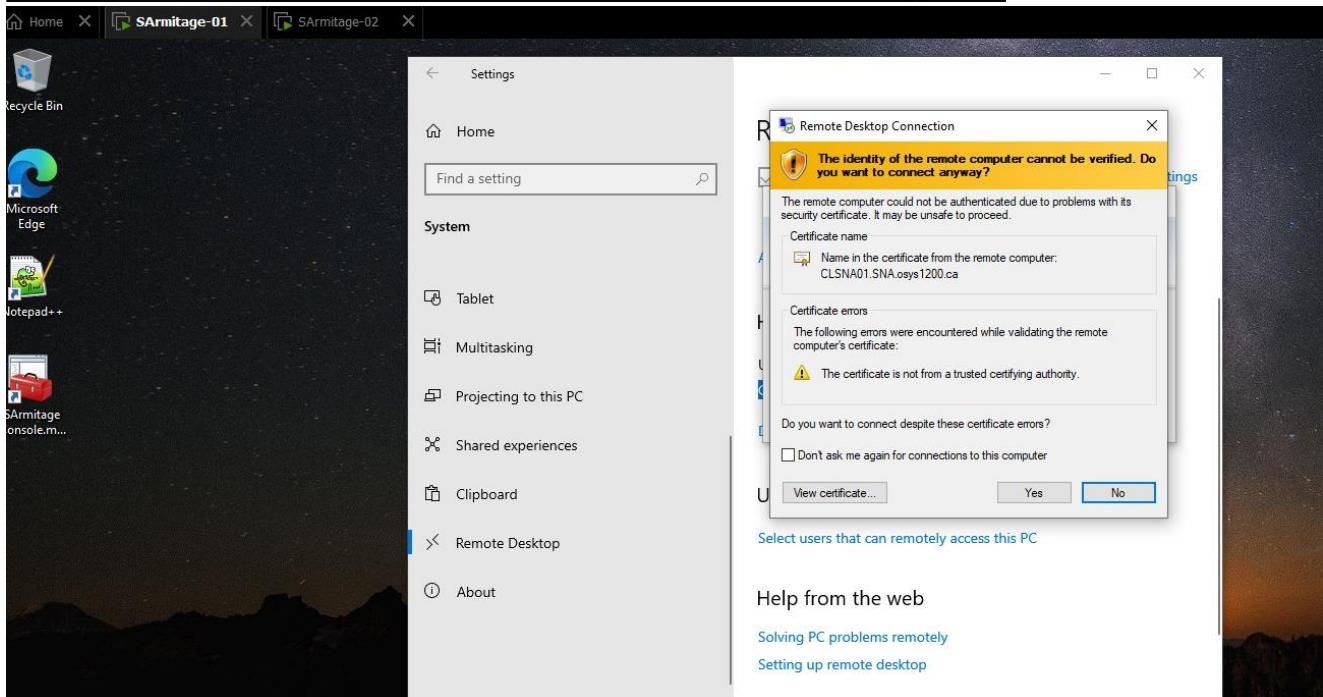
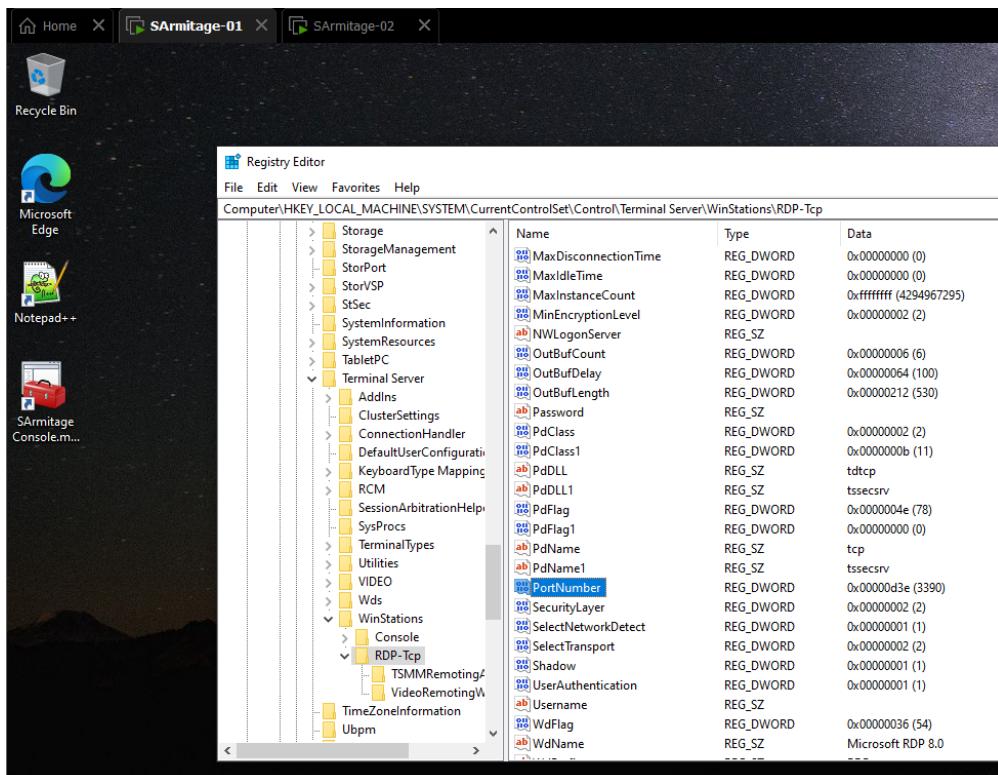
Screenshot of completed step 31 in 10-7 with correct drive letter S selected.

Task 3 – Remote Control

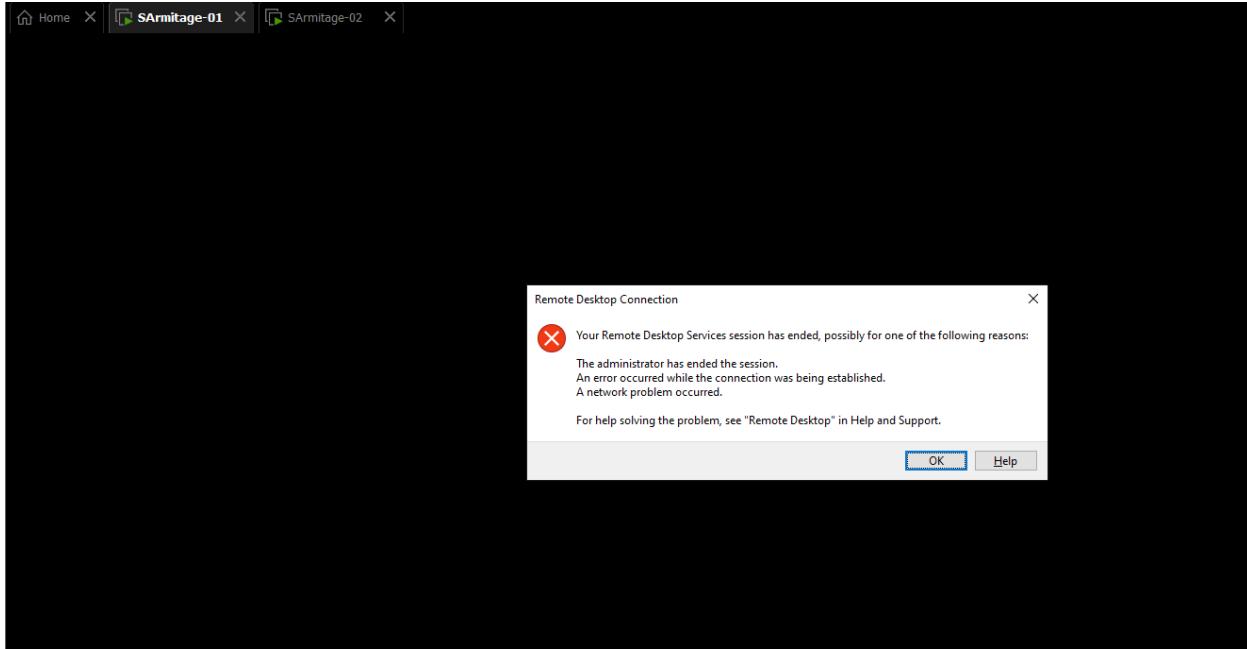




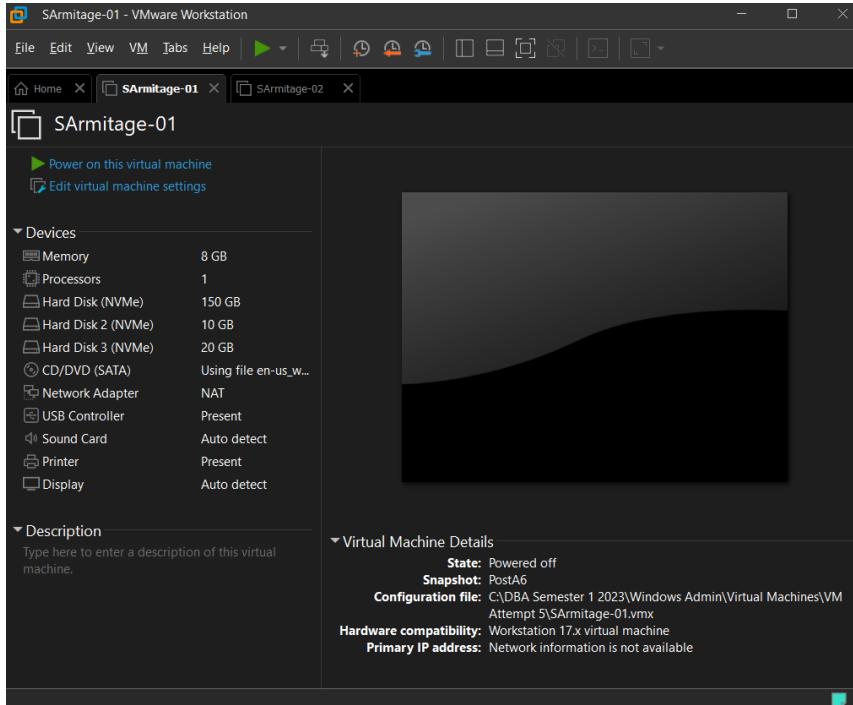
For this step my computer wasn't allowing me to remote control as it believed a session was already in progress, I assumed it was because I was currently running the VM. In the screenshot below you'll see I changed the port number to trick it. I was then able to gain access to remote control.



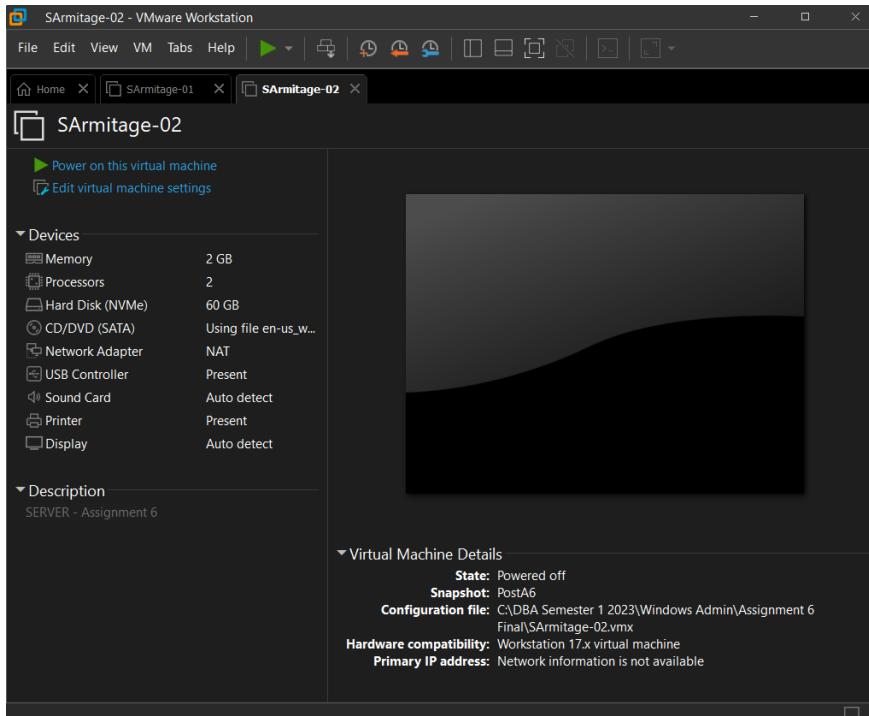
Unfortunately my machine kept timing out after about 5 minutes waiting for my screen to load, HOWEVER I did get a screenshot to prove I was able to get into the remote desktop using the troubleshooting I did!!

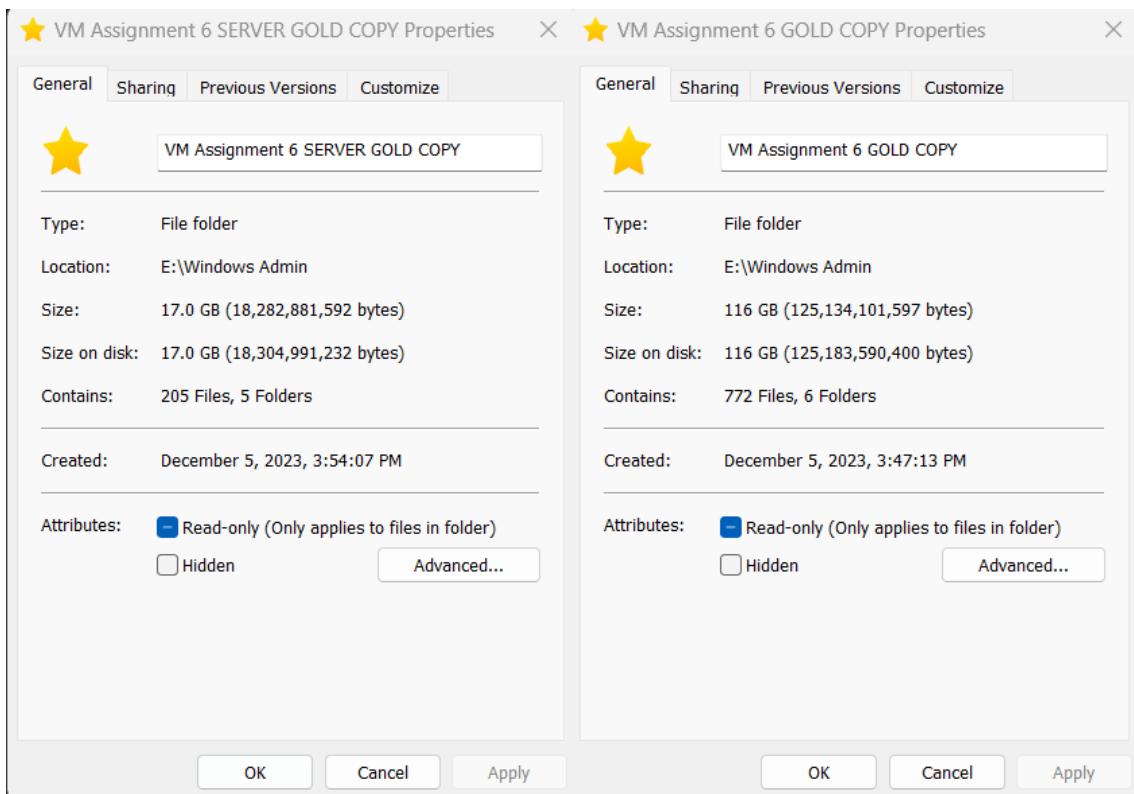


Task 4 – Backup and Documentation



Snapshot PostA6 in my original VM – and below the same snapshot in my new SERVER VM





Both screenshots of my gold copies – first being the SERVER and second being my WORKSTATION VM

Conclusion

This final assignment was absolutely more difficult than the others, however I am incredibly proud of myself and my ability to troubleshoot problems all on my own and only seeking help when I absolutely needed it.

Thank you for all the guidance and support you have provided during this first semester, I am looking forward to moving on to Linux with you in the new year!

Also, front page meme by :

https://www.reddit.com/r/pcmasterrace/comments/y7cyan/it_has_happened_to_me_and_im_still_in_awe_windows/