The Windows Active Directory

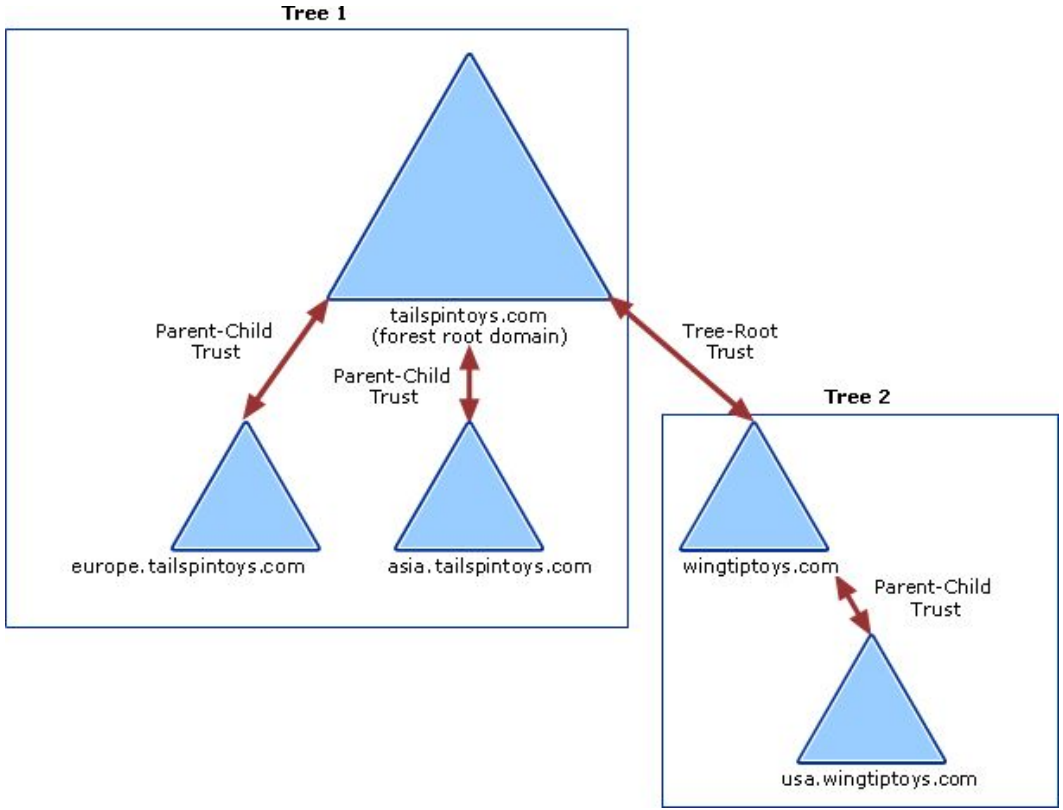
Module 2

What is Active Directory (Windows)

- The most common type of network for an office
- Structure of a computer network
- User accounts, computers, servers are registered in a central database (domain controller)
    - Security policies can apply to a whole domain, not just one computer
    - Anyone can logon to any machine and have the same Desktop and Documents

What is Active Directory (Windows)

- Forest
- Tree
- Domain


Tree 1
tailspintoys.com
(forest root domain)
Parent-Child
Trust
Parent-Child
Trust
Tree-Root
Trust
Tree 2
europe.tailspintoys.com
asia.tailspintoys.com
wingtiptoys.com
Parent-Child
Trust
usa.wingtiptoys.com

Parts of Active Directory

Domain Controller (DC)

- Usually a Windows Server
- The most important machine in a domain
  - Must be secured properly
- Responsible for authentication and security policies for a domain
  - Have to check with DC before logging into any computer
- Enables resource sharing for files or printers

Domain Controller (DC)

- Usually does internal DNS
- Usually does internal DHCP

DC -> Active Directory

Engine -> Car

User

- Someone who is using a computer within the domain
- Should have a locked down account
- Shouldn’t be able to (Principle of Least Privilege):
  - Install software
  - Change their computer’s configuration and registry keys
  - Change local policies
  - Access other user’s information

Administrator

- Like local administrator, but for all computers/servers
  - Can disable local administrator
- Should not be used for day-to-day operations
- Only to do things that users can't
  - Install software
  - Configure machines
  - Etc.
- Common Types
  - Install/Network Admins, Domain Admins, Enterprise Admins

Groups

- Groups of users
- Can assign privileges to a group
  - Access to certain file shares
- Add user to group to inherit privileges and policies

Organizational Units (OU)

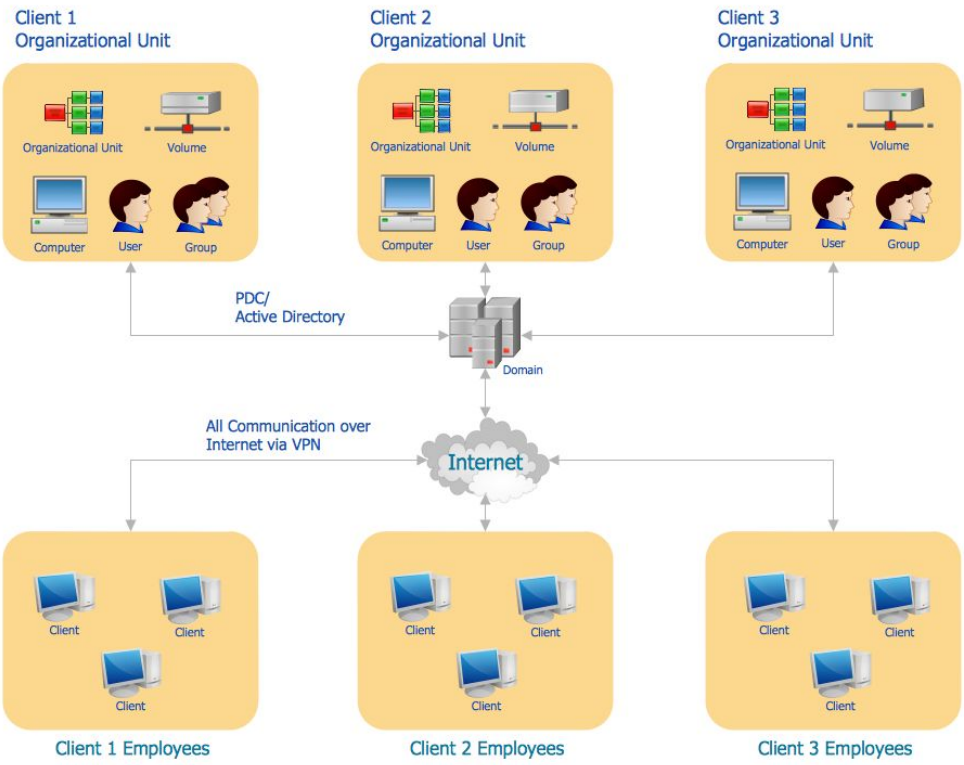
- Can hold users, groups and computers
- Can assign security policies to an OU
  - Password Complexity
  - Operating System Updates
  - Forcing you to use Edge (evil)

Difference Between OU and Group

Groups are for granting access to data and OUs are for organizing and controlling objects (users and computers) via delegation and group policy settings.

Volumes

- Remote files and servers
  - Good for sharing files between users

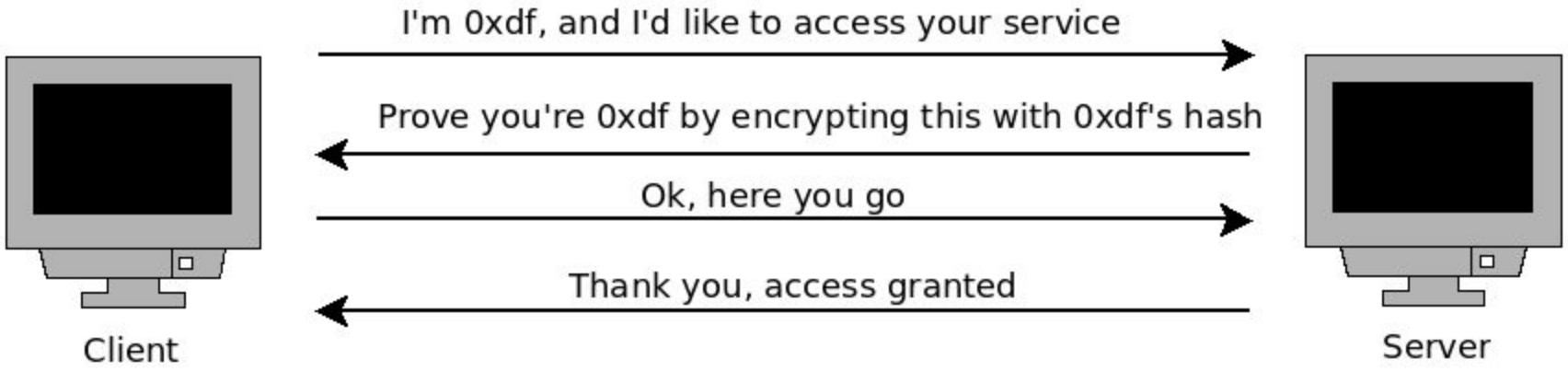

Client 1
Organizational Unit
Organizational Unit
Volume
Computer
User
Group
Client 2
Organizational Unit
Organizational Unit
Volume
Computer
User
Group
Client 3
Organizational Unit
Organizational Unit
Volume
Computer
User
Group
PDC/
Active Directory
Domain
All Communication over
Internet via VPN
Internet
Client
Client
Client
Client
Client
Client
Client
Client
Client
Client 1 Employees
Client 2 Employees
Client 3 Employees

Authentication

NTLM

- Version 1 and Version 2
- LM
  - LM and V1 are considered pretty insecure

NTLM Authentication Process



LM Hashes

- Breaks up password into 7 character-long chunks
  - Will pad with 0's
- Used 56-DES cipher to encrypts chunks, then jones them all together
- Can pass-the-hash

```
5f4dcc3b5aa765d61d8327deb882cf99:password
7c6a180b36896a0a8c02787eeafb0e4c:password1
f74a10e1d6b2f32a47b8bcb53dac5345:loveyou
bfd59291e825b5f2bbf1eb76569f8fe7:asd123
0f359740bd1cda994f8b55330c86d845:p@ssw0rd
```

NTLMv1 Hashes

- Can pass-the-hash
- Combination of LM:NT
- If NT hash of account is 31d6cfe0d16ae931b73c59d7e0c089c0, then account is disabled
- The below LM hashes indicate LM is not being used

```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:195db30d6dec38a8a7b71999073f807f:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
test:1003:aad3b435b51404eeaad3b435b51404ee:8c31690609c4d3c09fb76e466809962a:::
User:1000:aad3b435b51404eeaad3b435b51404ee:83414a69a47afeec7e3a37d05a81dc3b:::
```

LM Hash

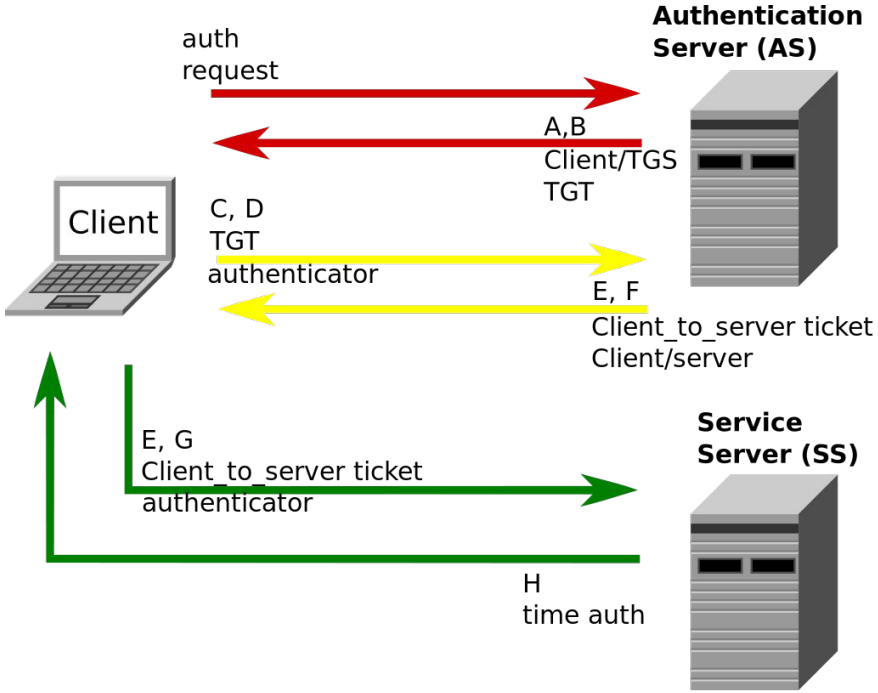
NT Hash

NTLMv2 Hashes

- More difficult to crack
- Cannot pass-the-hash
  - Time-based responses

```
[SMB] NTLMv2-SSP Hash     : Pentest::DESKTOP-UKIQM2O:1122334455667788:3BBCA6B
6BE9280264A663092956CA:0101000000000000FCAF2E089843D3015504B2CE682DAF69000000
2000A0053004D0042003100320001000A0053004D0042003100320004000A0053004D00420031
20003000A0053004D0042003100320005000A0053004D0042003100320008003000300000000
00001000000002000001972C411C02FD115AC2197983019AC23542BD0D64ADA42CF93C8B98C27
1C10A001000000000000000000000000000000000090024006300690066007300 2F00310039
2002E003100360038002E0031002E003100300033000000000000000000
```

Kerberos


Authentication Server (AS)
auth request
A,B
Client/TGS
TGT
Client
C, D
TGT
authenticator
E, F
Client_to_server ticket
Client/server
Service Server (SS)
E, G
Client_to_server ticket
authenticator
H
time auth

Common Active Directory Weaknesses

- Over-privileged accounts or groups
- Using NTLMv1 or LM
- Disabling SMB Signing
- Caching many logons
- Brute-force attacks from no lockout policy
- Abuse of local administrator
    - Should disable local administrator

Setting Up AD

Setting up a Domain Controller

- Windows 2019 or 2022
  - Can use previous server from last week

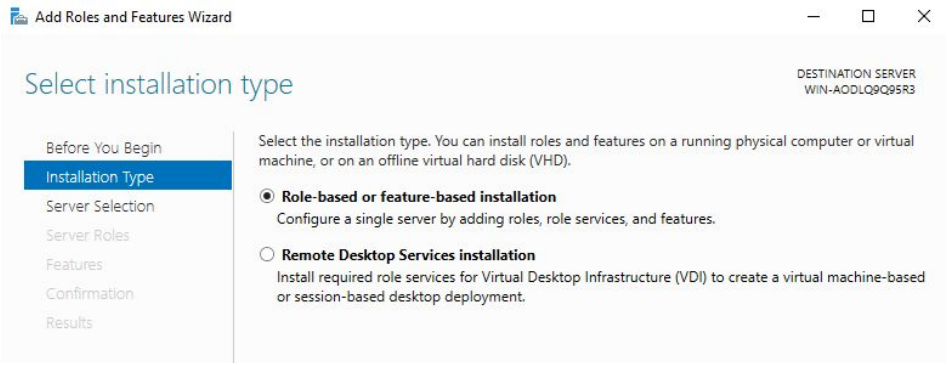
Setting up a Domain Controller

Go to the Server Manager Dashboard and Click on “Add roles of Features”. We will be adding the necessary features to turn this server into a DC.

You will get a popup called “Before you Begin”. This gives you a brief introduction to the Wizard (User Interface that will take you through the steps), and you can read this and click “Next”.

Setting up a Domain Controller

For the Installation Type, click Role-based installation. We are only configuring this server.

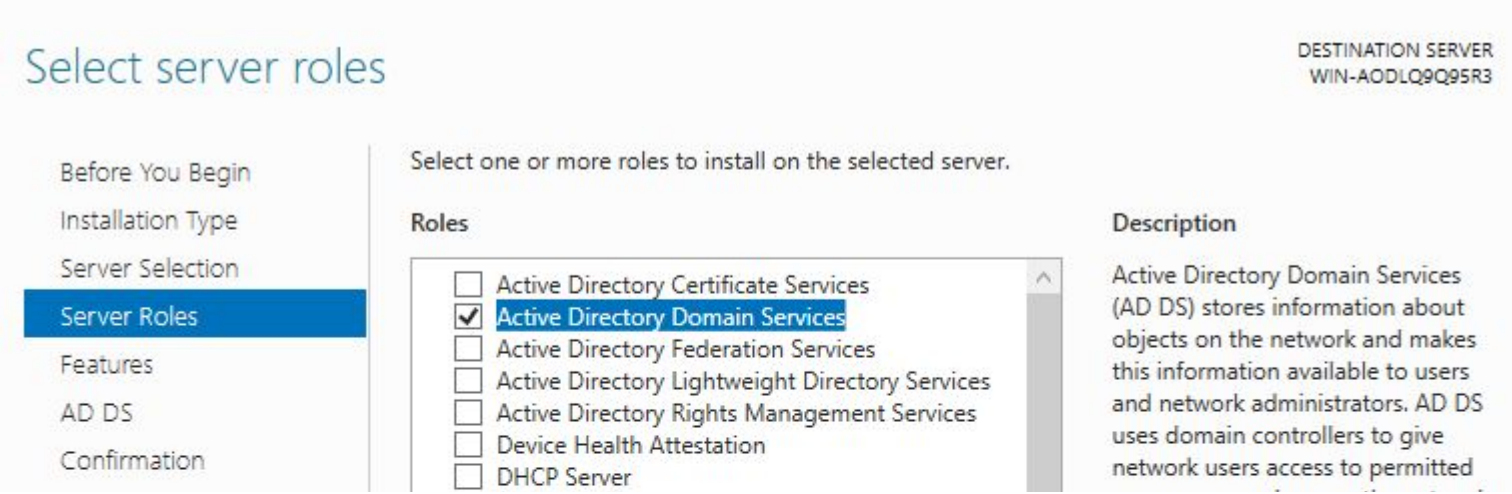


Setting up a Domain Controller

Next, you will choose which server to add DC features to. You should only have 1 server to choose from.

Setting up a Domain Controller

For the server roles, click “Active Directory Domain Services”. A popup will appear showing all the features that will be added to your server. Click Add Features, then hie “Next” in the Wizard.



Setting up a Domain Controller

In the “Select features” section, you will see several features already selected. These features are necessary for a DC and will already be selected. You do not have to add any additional features here, so just click “Next”.

Setting up a Domain Controller

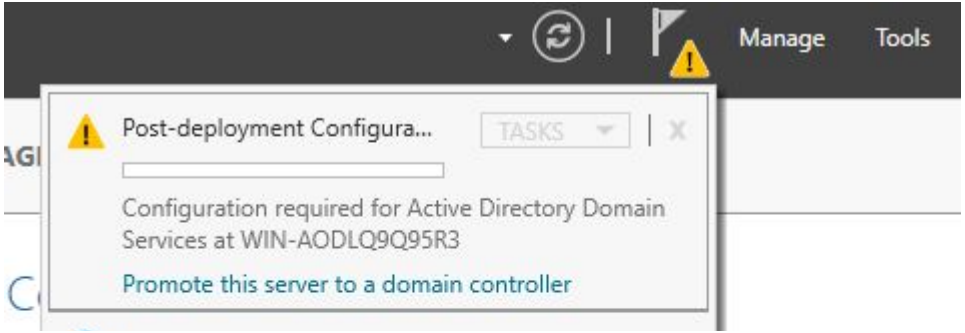
The Next “AD DS” gives you a little information about what Active Directory does. This information is located in the previous slides, but this is also worth a read. Click “Next” when you are ready.

Setting up a Domain Controller

Lastly, you will be at the Confirmation window. You will just need to click “Install” to add the necessary features for a DC. The process will take several minutes. Click “Close” when the installation is complete (the bar is full).

Setting up a Domain Controller

You will see a triangle notification at the top-right of Server Manager next to the flag. Click on it and click “Promote this server to a domain controller”. We will now be setting up the rest of the Domain.

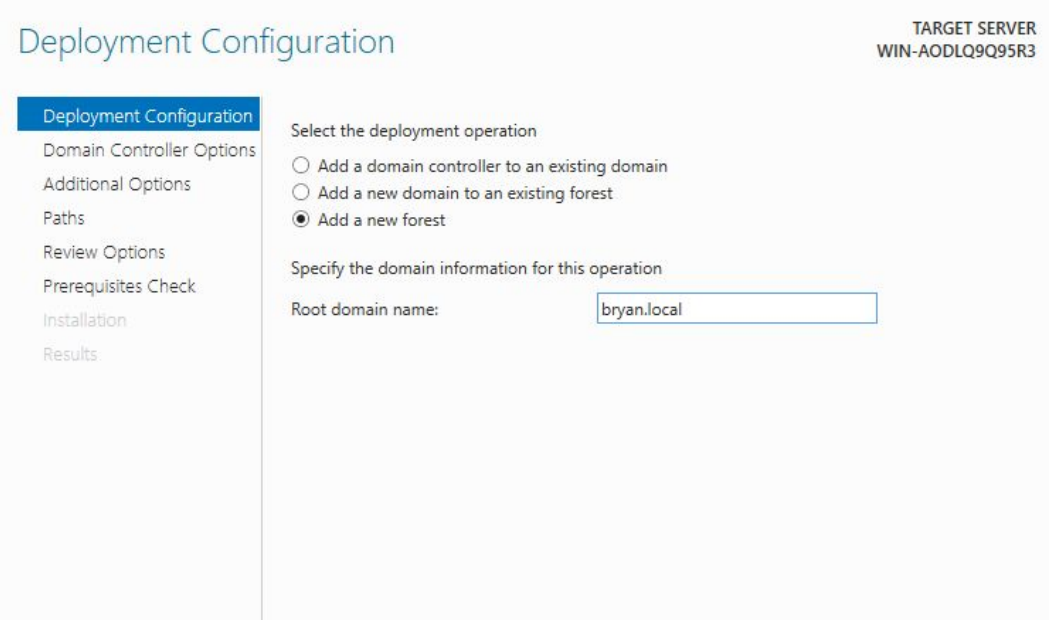


Setting up a Domain Controller (cont).

Click “Add a new forest”. Because we are starting our domain from scratch, we will not be able to join this DC to any existing domain as there are no other domains. You will have to create a domain name, which can be whatever you’d like. A good practice is to make the domain name not the same as an external domain. For example, don’t make it nscc.ca because that’s an external domain name already. .local is usually used

In my example,I call my domain bryan.local. An example image is on the next slide.

Setting up a Domain Controller (cont).



Setting up a Domain Controller (cont).

After you hit next, you will be prompted with the “Domain Controller Options” screen. The DNS server and GC boxes will already be ticked. These specify that you will also use this server to hold domain names of internal resources, such as a web server. It is recommended to use the DC as a DNS server as well. The global catalog allows users and applications to find objects in an Active Directory domain tree, given one or more attributes of the target object. This is pretty necessary for a DC to be able to do.

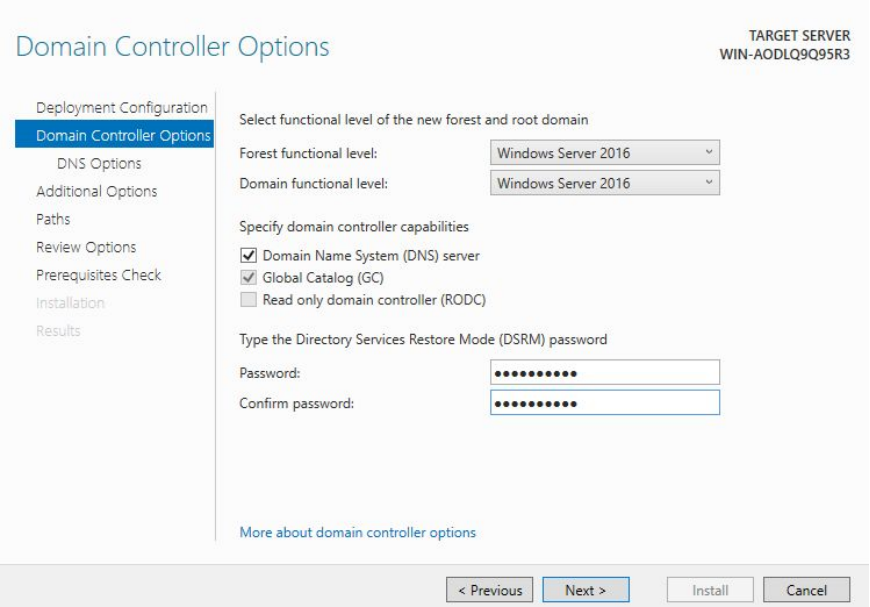
You are good to leave the default values here, but you will need to create a DSRM password.

Setting up a Domain Controller (cont).

A DSRM password provides the administrator with a back door to the database in case something were to go wrong in the future, but it does not provide access to the domain or to any services. Put any password you'd like here, but keep note of it just in case. After you confirm a DSRM password, click Next.

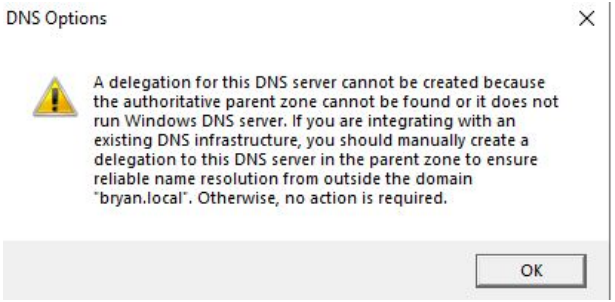
Image on next slide

Setting up a Domain Controller (cont).



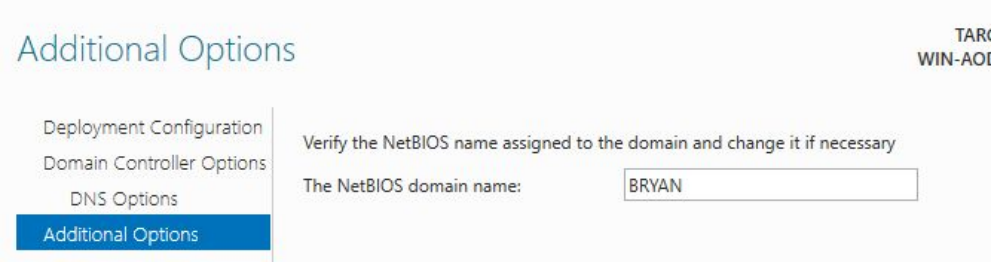
Setting up a Domain Controller (cont).

You will get a warning that a delegation for this DNS server cannot be created. You can click “Show More” to see the full warning. Because we have not set up another DNS server, and therefore won’t be integrating this DC into another DNS zone, we can ignore this error. Note the “Otherwise, no action is required”. We can hit OK and Next.



Setting up a Domain Controller (cont).

You will be asked to give the DC a NetBIOS name. By default, this will be your domain name without the suffix (.local if you used .local). This name is used by machines on a network to identify each other, and is used with older networking applications. Windows requires a NetBIOS name and limits it to 15 characters. The name can be whatever you'd like as long as it's not longer than 15 characters.

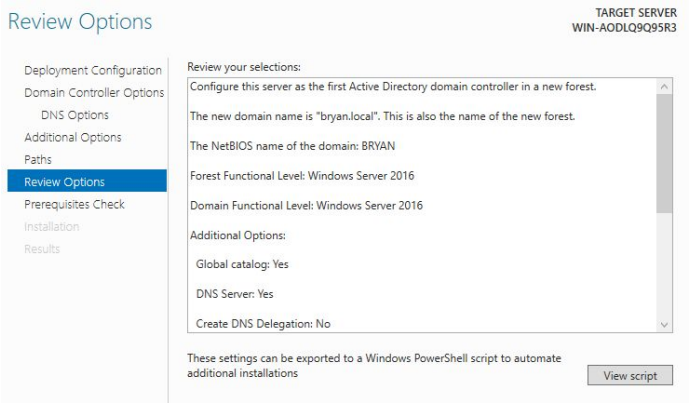


Setting up a Domain Controller (cont).

In the Paths windows, you will have the opportunity to decide where the DC's database and log files go to. These are files one would review for the monitoring of the DC's events and health. It is not recommended to change these paths, so you should just hit "Next".

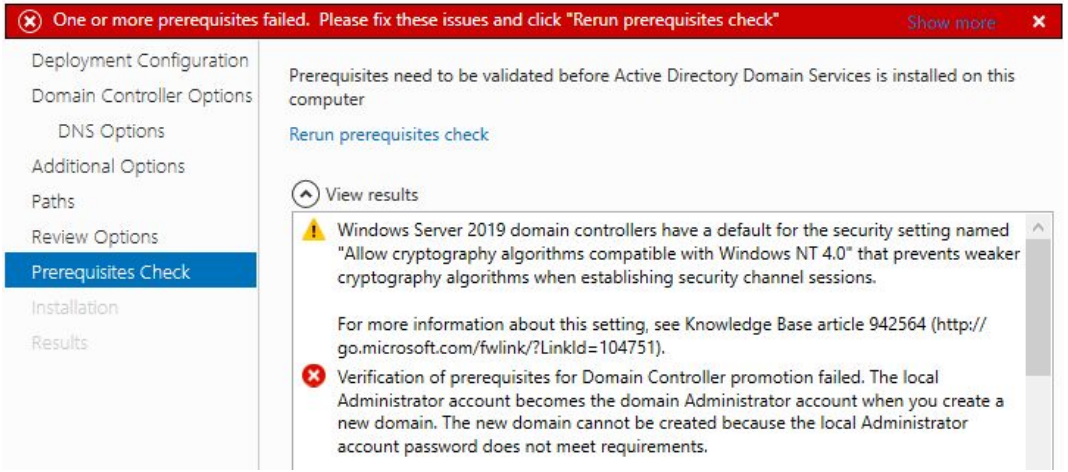
Setting up a Domain Controller (cont).

The Review Options section will give you a summary of your changes. You can export these instructions as a PowerShell script, which can be useful later on in life maybe. You can hit “Next” here.



Setting up a Domain Controller (cont).

The system will do a prerequisites check to make sure everything is OK. You may get the following error.



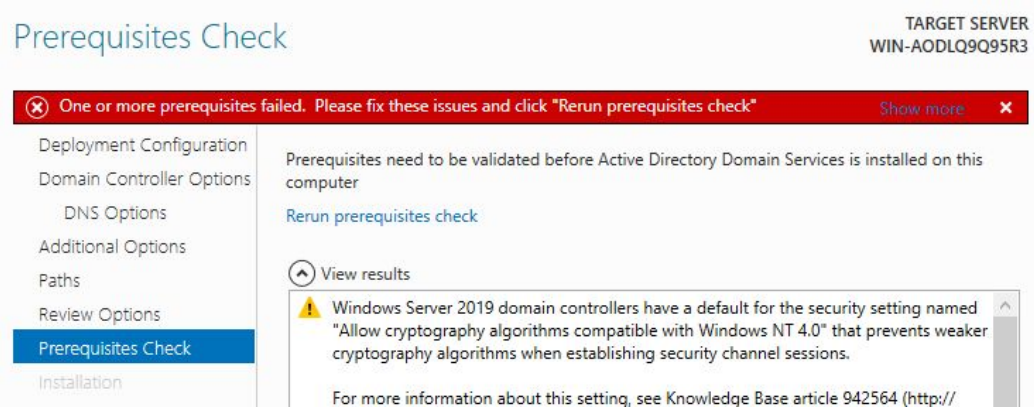
Setting up a Domain Controller (cont).

In this case, the default Administrator account (that comes on every Windows machine and is different from the administrator account you may have set up in the previous lab) has not been configured with a password. This is most likely due to using a custom local administrator account rather than the default. When a server becomes a DC, Active Directory promotes the default Administrator account to be the default Domain Administrator account, and if it doesn't have a password set it won't let you. You can use the following command to give the Administrator account a good password (upper-case, lower-case, number, symbol, at least 12 characters) using an elevated CMD prompt (run as administrator)

```
net user Administrator <password>
```

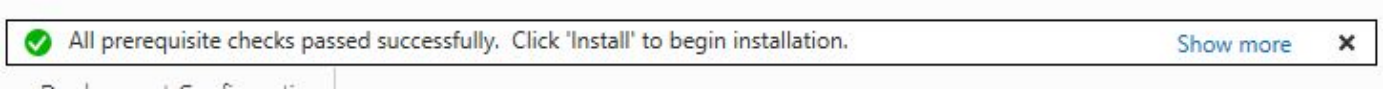
Setting up a Domain Controller (cont).

After you have changed the Administrator account, hit rerun prerequisites check.



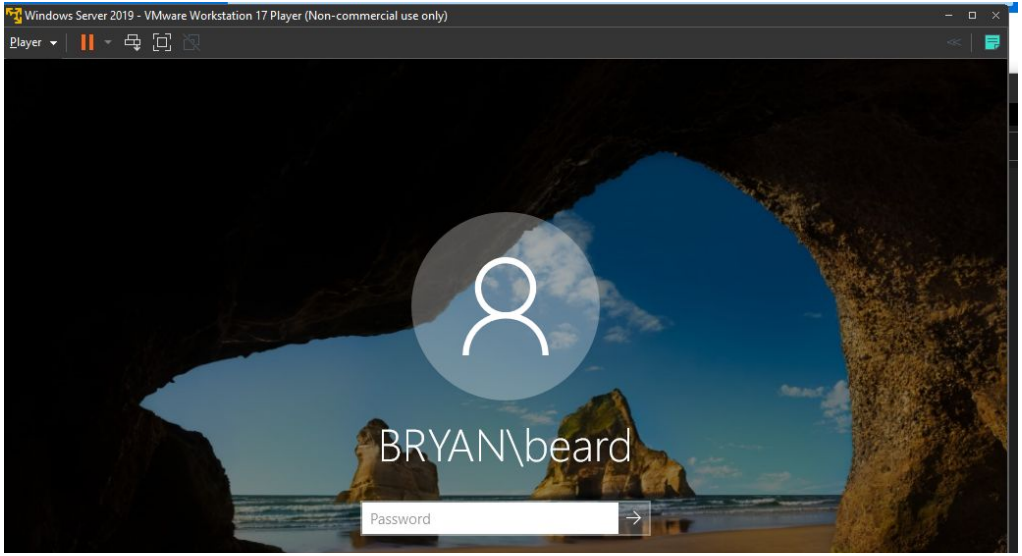
Setting up a Domain Controller (cont).

You should be good to go now, so just hit insall. If the DC does not reboot on its own, restart it for the changes to take effect.



Setting up a Domain Controller

When you DC boots up, you will be asked to login as your local administrator account in the format <domain>\<username>. This indicates you have successfully created a domain and DC.



Users and Groups

Setting up a Domain Controller - Creating Users

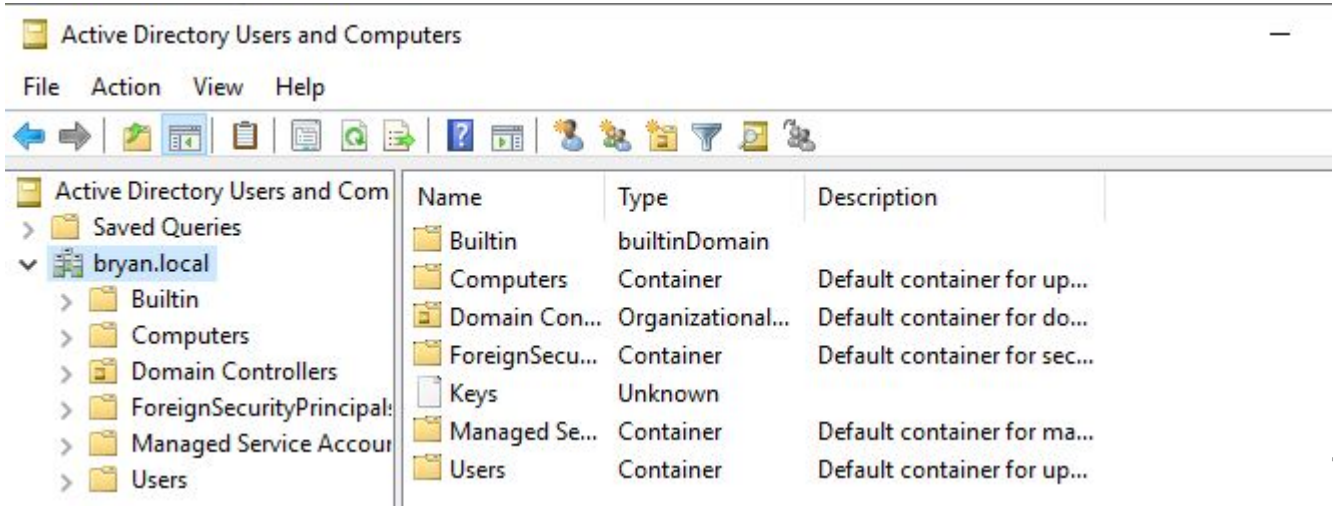
With the DC setup, now it's time to set up a Domain User and a Domain Admin (DA). The DA account will be used to configure the domain, and is a very high-privileged account. Be sure it has a strong password. We will be taking your local administrator account and adding it as a DA. In my case, this is my beard account.

The Domain User will act as a normal user account with no administrative privileges. It's important for Active Directory administrators to have a user account for day-to-day operations (Principle of Least Privilege).

Creating Users

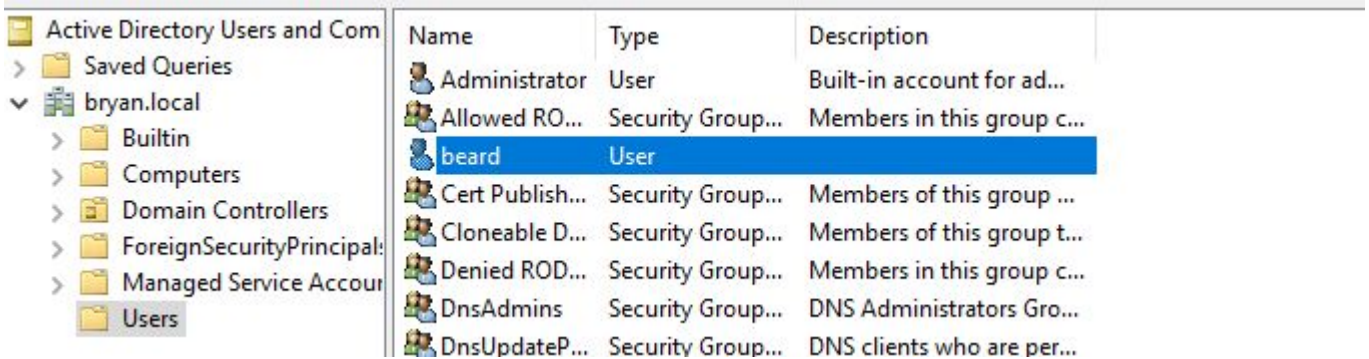
Go to Server Manager -> Tools -> Active Directory Users and Computers

This is how to manage users, groups and computers over Active Directory. Click on the drop-down menu for your domain on the left.



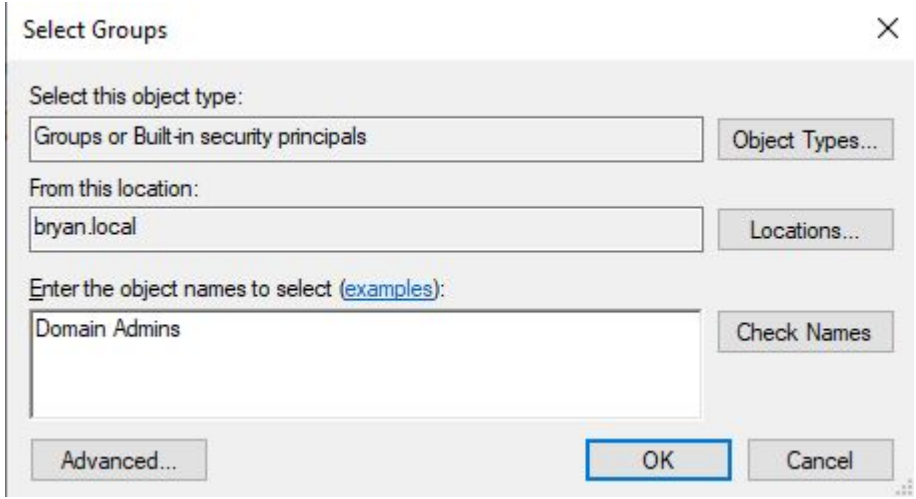
Setting up a Domain Controller - Creating Users

Find your user by clicking in the Users folder



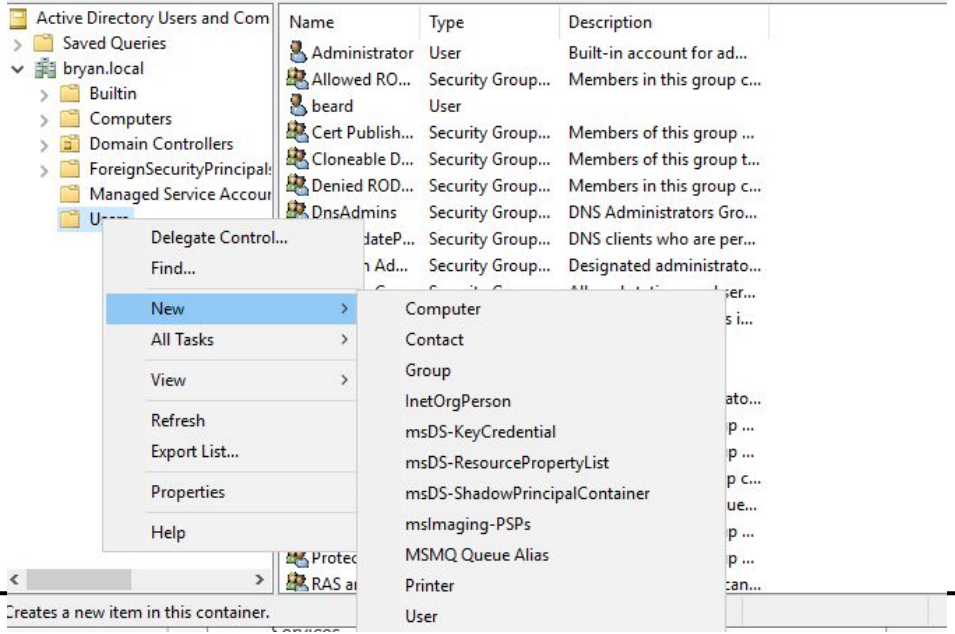
Setting up a Domain Controller - Creating Users

Right-Click your user and click “Add to Group” and type in “Domain Admins” under object names.



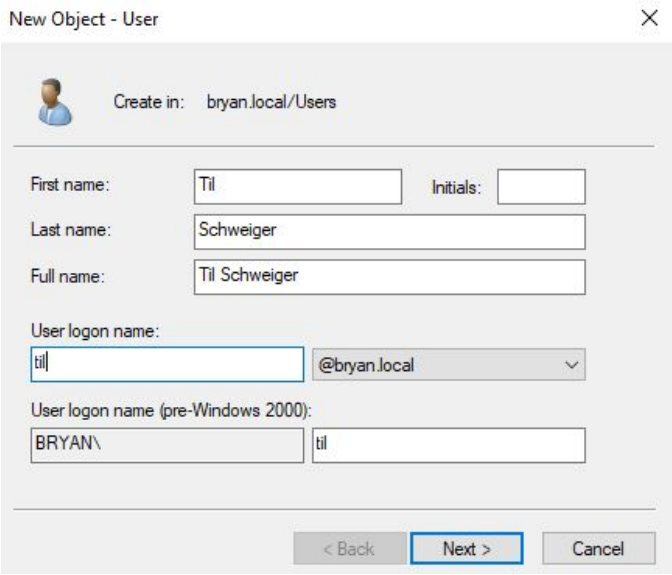
Creating Users

Now let’s create a regular ol’ Domain User. Right-click the user’s folder -> New -> User



Creating Users

Fill out the information with whatever you'd like. Be sure to give your new user a logon name.



Creating Users

Give your new user a password, but keep the box checked that they must change their password at next logon. Administrators shouldn’t know the logon password of any of their users.

Creating Users

By Default, all users will be part of the Domain Users group, so there is no need to add your new user to the Domain Users Group. This group, by default, gives them non-administrative permissions on the domain.

Strengthening Your DC

Setting up a Domain Controller - Strengthening DC

With your users all set up, we can get rid of the local administrator account. Having a local administrator account with the same credentials on each machine within a domain is a common practice. However, if one machine is compromised, it’s very easy for a hacker to compromise your DC with the local admin credentials (or NTLMv1 hash). Therefore, limiting the total amount of administrator accounts is advised.

Setting up a Domain Controller - Strengthening DC

You can disable the local administrator by opening an elevated CMD prompt and typing the following command.

```
net user administrator /active:no
```

Setting up a Domain Controller - Strengthening DC

You can verify the account is disabled by running the following command, and observing that the “Account active” value is no.

```
net user administrator
```

```
C:\Windows\system32>net user ADministrator
User name                    Administrator
Full Name
Comment                      Built-in account for administering the computer/domain
User's comment
Country/region code          000 (System Default)
Account active               No
Account expires              Never
```

Setting up a Domain Controller - Looking at Users

You can also use the “net user” command to look at domain users. Try running the following command to display users on the domain:

```
net user /domain
```

```
C:\Windows\system32>net user /domain

User accounts for \\WIN-AODLQ9Q95R3

-------------------------------------------------------------------------------
Administrator            beard                    Guest
krbtgt                   til
```

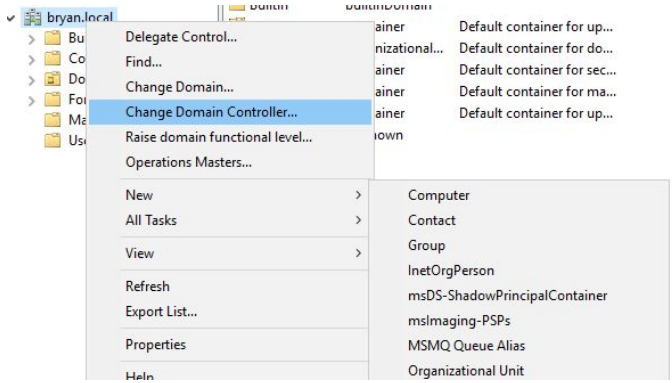
You can use “net user <username> /domain to view specifics about your domain user and admin, and see what Groups they belong to.

Setting up a Domain Controller - Looking at Groups

Similarly to the next slide, you can use “net group /domain” to display all groups on the domain, and “net group <group_name>/domain” to view specifics and members of that group. Try it for your Domain Admins and Domain Users groups.

Setting up a Domain Controller - Creating a New OU

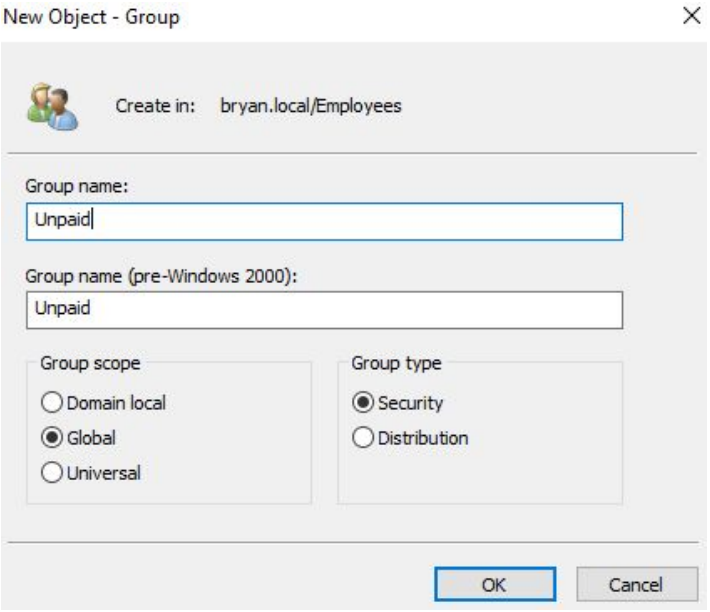
We can create our own OU (call it whatever you'd like) through the "Active Directory Users and Computers" section under Tools in the Server Manager (same place to create a user). Right click on your domain and click New -> Organizational Unit. Name it what you'd like.



Setting up a Domain Controller - Creating a New OU

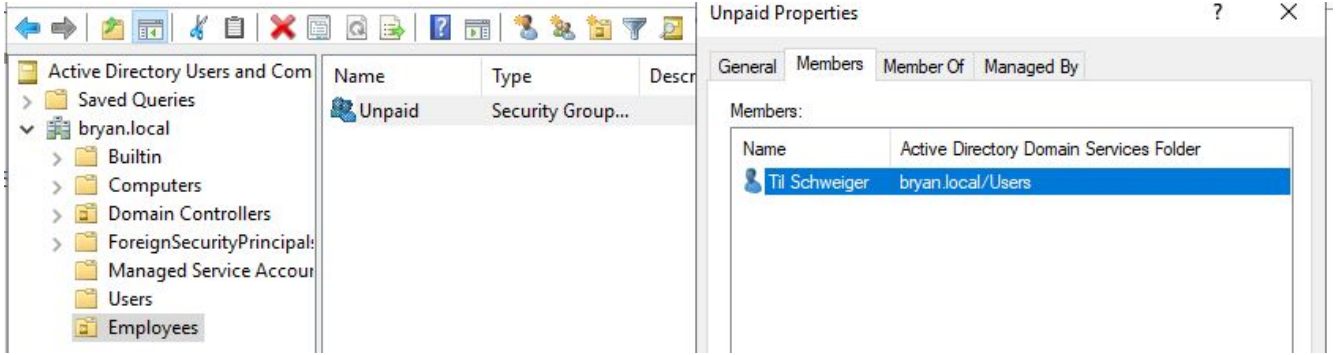
With selecting the new OU folder you've created("Employees in my example), create a group by right-clicking the OU folder and making a New group. Call this group whatever you'd like. For the Group Scope, select Global. Microsoft likes to be confusing with their group names, but think of Domain Local as resource groups, and Global as account groups. For example, as resource groups, Domain Local Groups should be used to grant access to IT resources in a domain, and as account groups, Global Groups should be used to collect all users in a domain in a group. As for group types, Security groups are for giving permissions on a network, and distribution groups are for sending people email notifications. Select Security group here.

Setting up a Domain Controller - Creating a New OU



Setting up a Domain Controller - Creating a New OU

Finally, make your new Domain User a member of the group you've just created. You can use the previous steps when you set up your Domain Admin to do so, but for your new group instead. After you have added your user to your group, you should be able to double-click the group and see they've been added.



Adding a Workstation

Setting up a Domain Controller - Add Computer

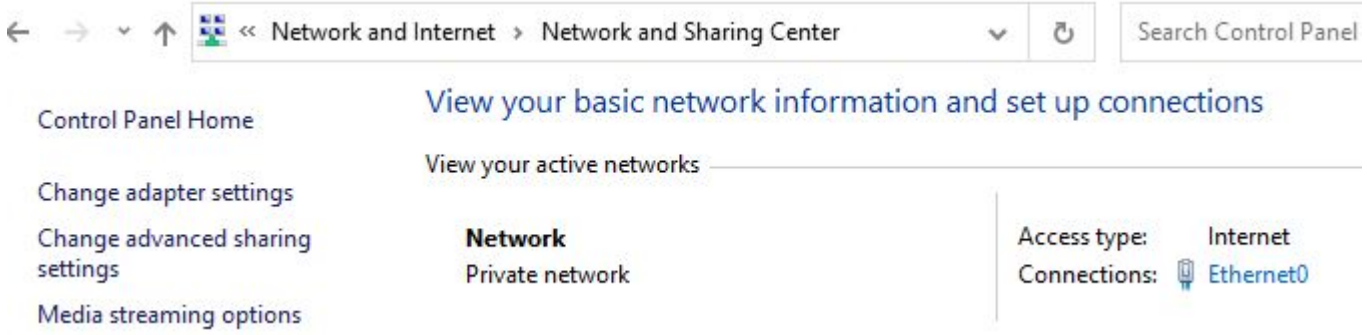
We can now add a workstation to talk to our DC and be part of the domain. First Create Windows 10 virtual machine or use your host machine if it’s Windows 10 Pro or Educational (will not work with Home edition) Be sure you can communicate with your DC (both systems should be using the NAT network adapter in your VMWare settings)

Setting up a Domain Controller - Add Computer

Next, we will have to add our DC as the PC's primary DNS server. When we add the PC to the domain, it will try to lookup where <domain>.local (whatever you called your domain) is. However, the only machine that knows where the domain is is your DC. Luckily, we configured it as a DNS server in the previous step. So when we configure the PC to use the DC as a DNS server,the DC will tell the PC what IP address the DC for your domain is.

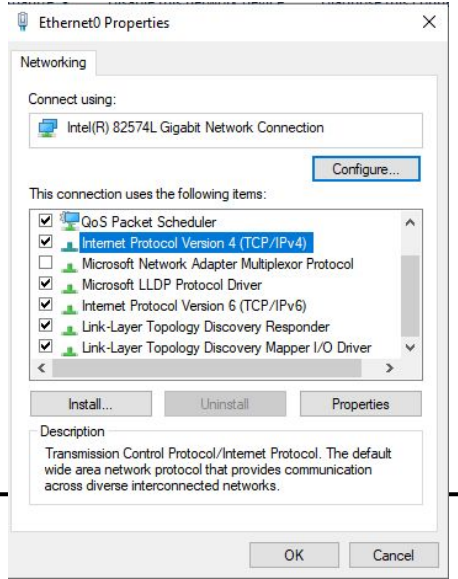
Setting up a Domain Controller - Add Computer

First go to Control Panel -> Network and Internet -> Network and Sharing Center and click on Change Adapter Settings on the left side.



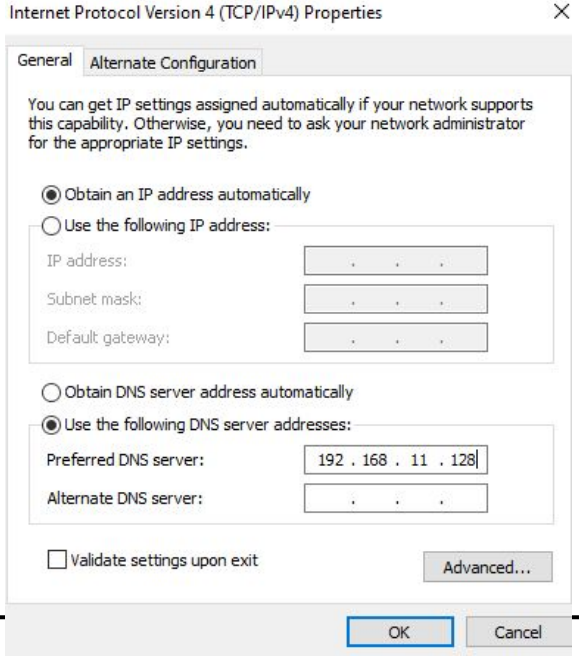
Setting up a Domain Controller - Add Computer

Right click what should be the only network adapter in there and click Properties. Scroll down and find Internet Protocol Version 4 (TCP/IPV4) and click on it,then click on Properties.



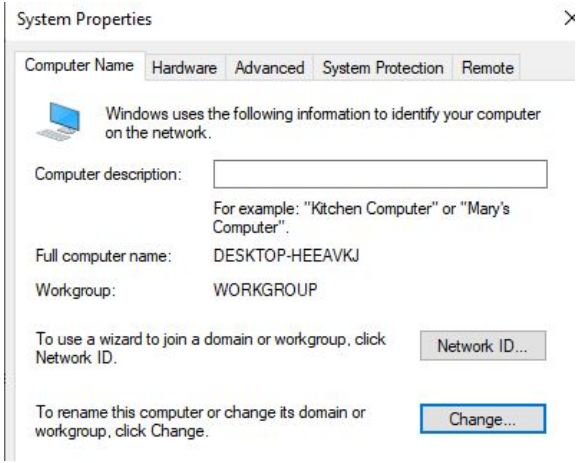
Setting up a Domain Controller - Add Computer

Add your DC's IP address as the preferred DNS server and click OK.



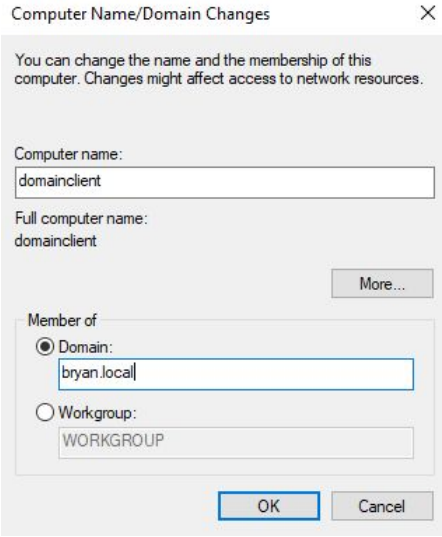
Setting up a Domain Controller - Add Computer

To add your PC to domain, got to Control Panel -> System and Security -> System and scroll down and hit “Rename this PC (advanced)” in Related Settings section. You will get a System Properties popup, click the Change button here.



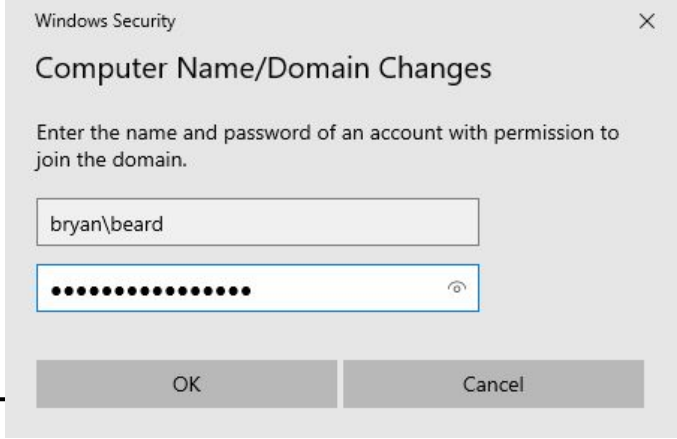
Setting up a Domain Controller - Add Computer

Change the name of the Computer to whatever you'd like, and click the Member of Domain bubble. Here you will type the domain name you set up for your DC.



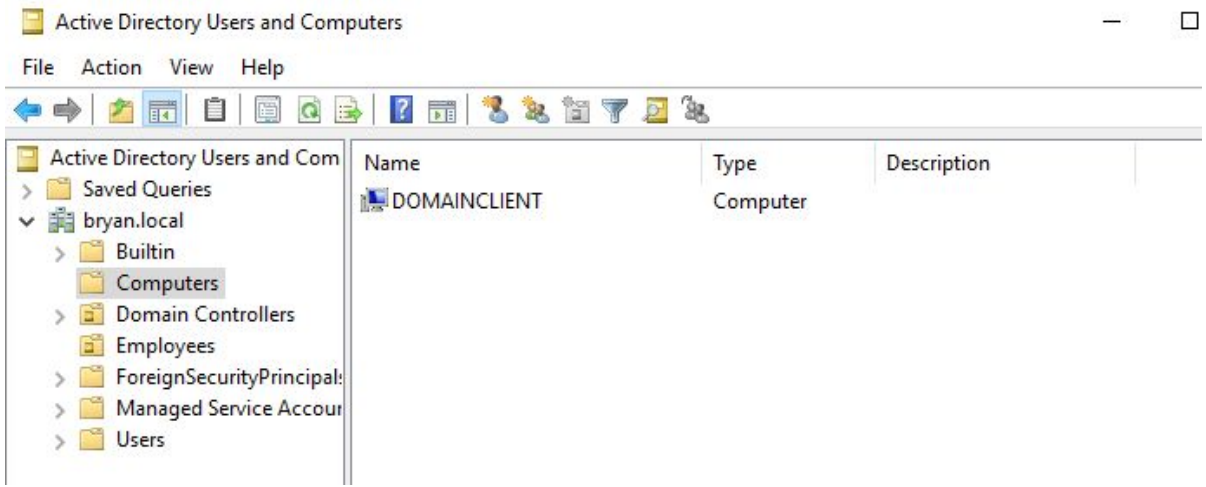
Setting up a Domain Controller - Add Computer

You will then be prompted to enter credentials. You will need to input your Domain Admin credentials here. Active Directory requires this so not anyone can add computers to a domain without the Domain Admin's permission. When your PC is added, you will get a cute welcome message. You will have to restart your PC.



Setting up a Domain Controller - Verify Computer Added

On your DC, go back to Server Manager -> Tools -> Active Directory Users and Computers, and click on the Computers folder under your domain. You should now see the name of the PC you just added.

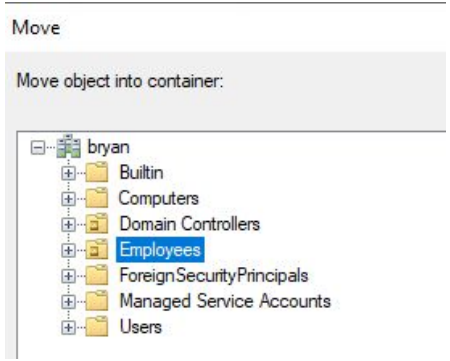


Setting up a Domain Controller - Verify Computer Added

Try logging onto your PC with the Domain User you set up previously. Try logging in as your Domain Admin.

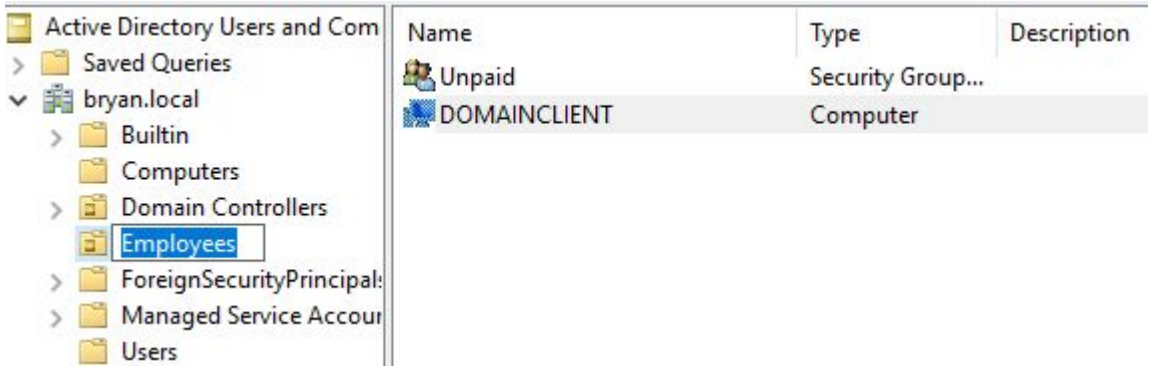
Setting up a Domain Controller - Verify Computer Added

Finally, let’s add this PC to the OU you set up previously. Right-click on the computer and click Move, then click on the OU you set up earlier.



Setting up a Domain Controller - Verify Computer Added

You should see your group you set up earlier and the PC in your OU now.



Strengthening Authentication

Strengthening Domain

By default, a domain allows NTLMv1 and even LM to be used for authentication. These are very weak, and we don't want any of our machines on our domain to use them. We could go to our DC and workstation and turn them off, but it's much simpler to create the policy on our DC and push it out to our workstation. For this we will use a Group Policy Object (GPO).

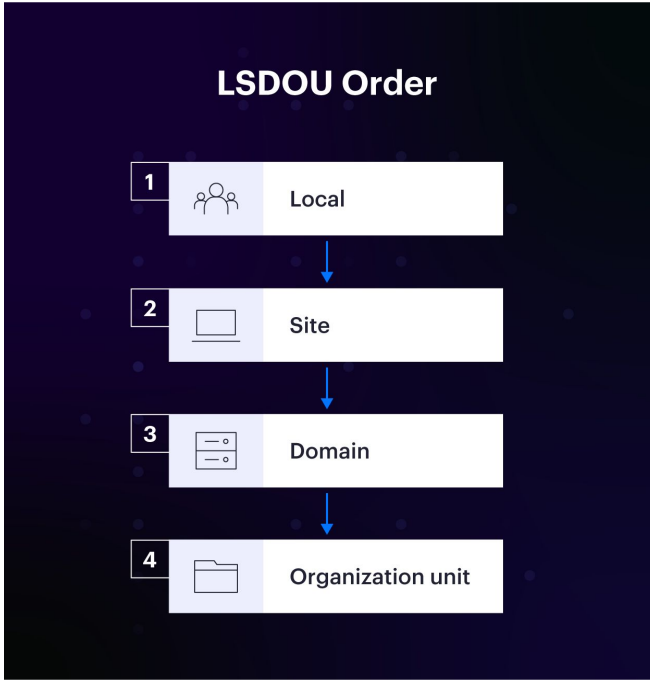
Strengthening Domain

GPOs are policies to configure settings for key areas, including registry keys and security options. They allow domain admins to manage the entire domain's systems just from Active Directory on the DC. This is very useful, especially when dealing with a domain with 100 machines on it.

You've already had experience with Local policies (gpedit in last week's lab).

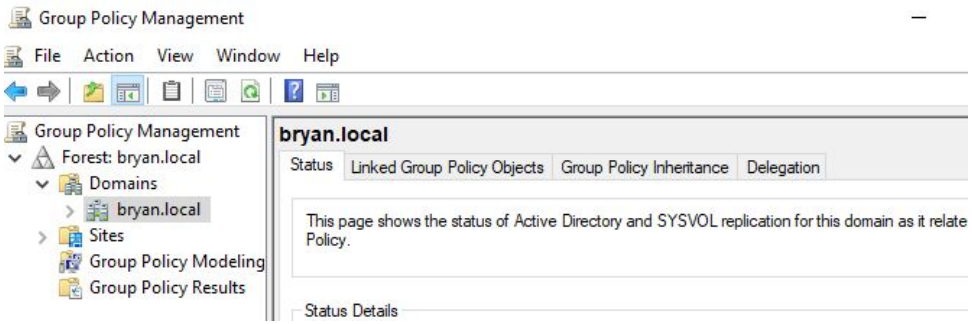
GPOs

Here is the order that policies
Are processed on a machine. Local
Policies are always processed first.
Therefore, any local policies can
Override Domain policies.



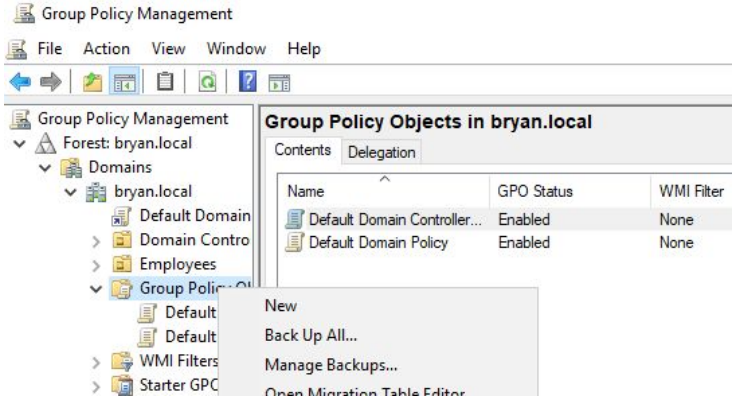
GPOs

GPOs are handled through GPMC, or Group Policy Management Console. You can access this through your Windows Search bar and typing “gpmc.msc”



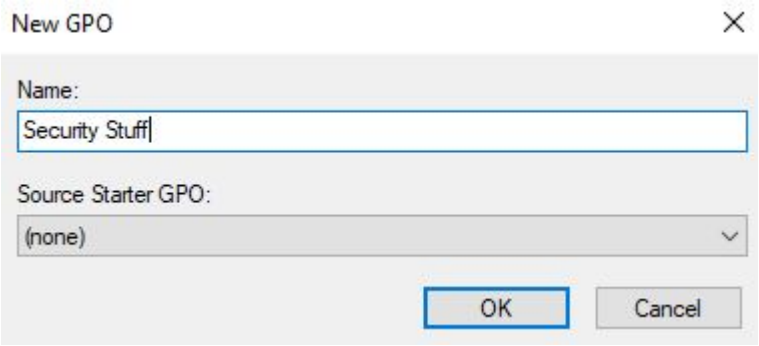
GPOs

Ideally, we would like to enable a GPO to disable NTLMv1 due to its weak security controls. Right-click on Group Policy Objects and Click new.



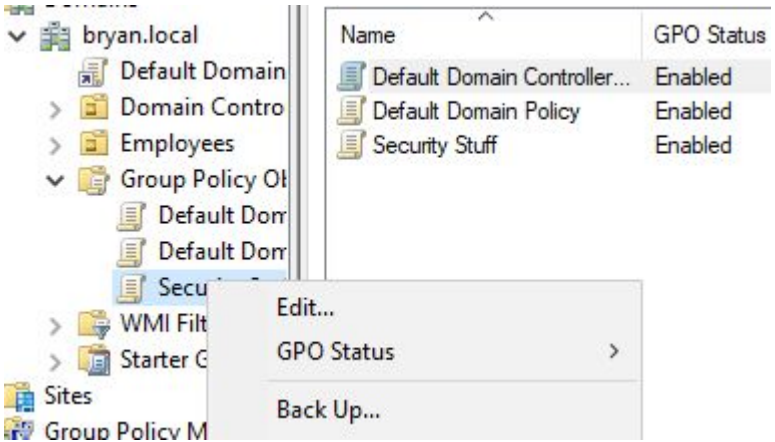
GPOs

We can call this GPO whatever we'd like. We will select our Source Starter GPO to be none because this is our first GPO. Ideally, you would use a starter GPO when you would like to start with a similar already-made GPO.



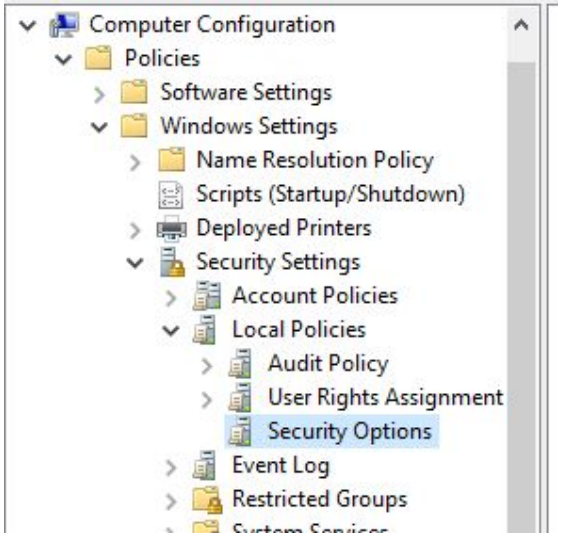
GPOs

Now right click your new GPO (mine is Security Stuff) and click edit.



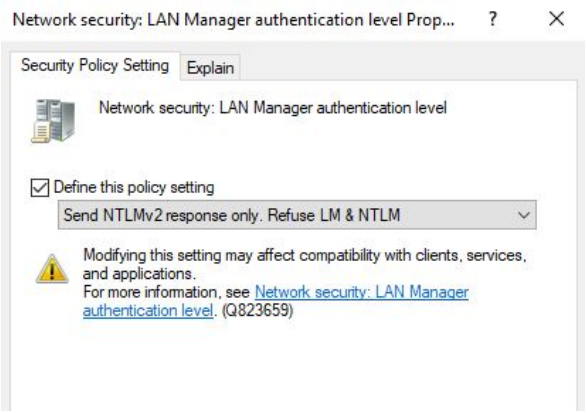
GPOs

Navigate to Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options



GPOs

You will see a lot of policies that are not defined. Find Network Security: LAN Manager authentication level and double-click it. You'll want to click the box to define this policy, and set the policy to "Send NTLMv2 response only. Refuse LM & NTLM".



GPOs

Additionally, we can enable SMB signing for the whole domain. This adds signatures to all SMB communication (Which NTLMv2 users) to ensure that the connections between clients and servers over SMB are legitimate. This is a good mitigation against the SMB relay attack, which is a common Active Directory adversary-in-the-middle attack.

GPOs

There are 4 policies we'd like to enable. For the server,

- Microsoft network server: Digitally sign communications (always)
- Microsoft network server: Digitally sign communications (if client agrees)

And for clients

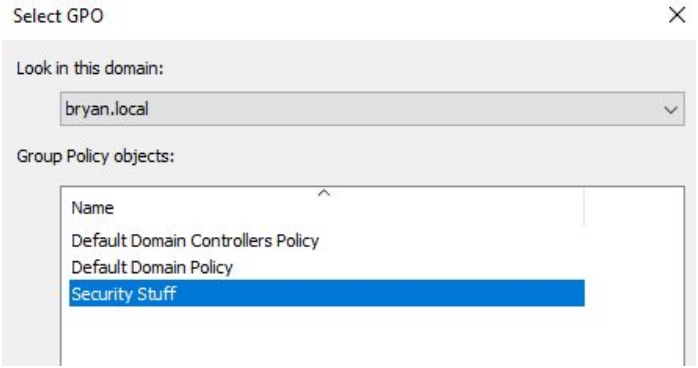
- Microsoft network client:Digitally sign communications (always)
- Microsoft network client:Digitally sign communications (if server agrees)

GPOs

The last policy we'd like to set is to limit the number of cached logons. Whenever someone on the domain logs into a machine, that machine caches an encrypted version of their credentials on the machine. This is just in case the DC is not available, the user can still login to the machine. If a hacker were to compromise a machine, they could get and crack credentials of all users in that machine's cache, which usually includes a Domain Admin's credentials. Setting the total cached logons to 0 is ideal from a security perspective, but may not be practical in the real world. We will be setting it to 0 in our lab, but in a real-world scenario you may want to limit this to 1. The policy to enable is "Interactive Logon: Number of previous logons to cache". Set the number of logons to 0.

GPOs

With all your policies defined, you can close the current Group Policy management Editor window to bring you back to the Group Policy Management windows. Right click your domain and click “Lick an Existing GPO”. Click on your new GPO and click OK to push it out to the domain.



GPOs

It can take 90 minutes for GPOs to take effect. However, for critical GPOs you can logon to your domain workstation as a Domain Admin, and run “gpupdate /force” from an elevated command prompt. (You can also use Win-RM to remotely run this command if you set it up earlier).

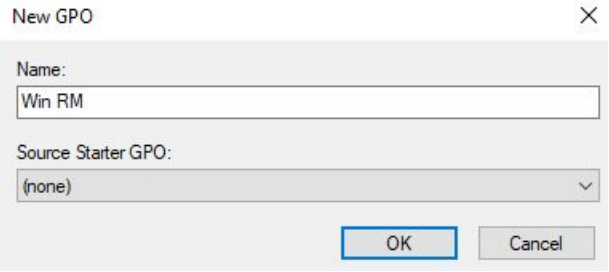
GPOs

On the workstation, you can run rsop.msc from the Windows search bar as a DOmain Admin and check on your policies. If you go to Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options you'll see all the policies you've set.

Win-RM

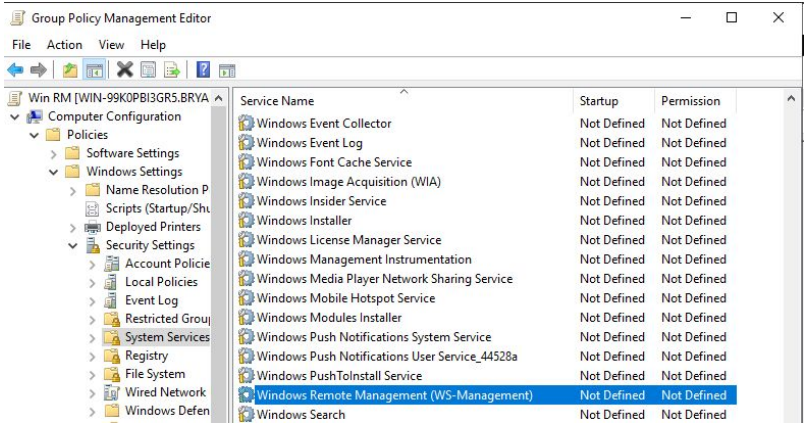
Win-RM

Win-RM is a wonderful tool for remotely running commands on other domain-joined machines without kicking users off like with RDP. Ideally, you can enable Win-RM via GPO. From the GroupoPolicy Management (gpmc.msc) you can right-click on your domain and click “Create a GPO in this domain, and Link it here”. By doing so, we create a GPO and automatically push it out.



Win-RM

Right-click your new GPO and click Edit. Go to Computer Configuration -> Policies -> Windows Settings -> Security Settings -> System Service and find Windows Remote Management (WS-Management)

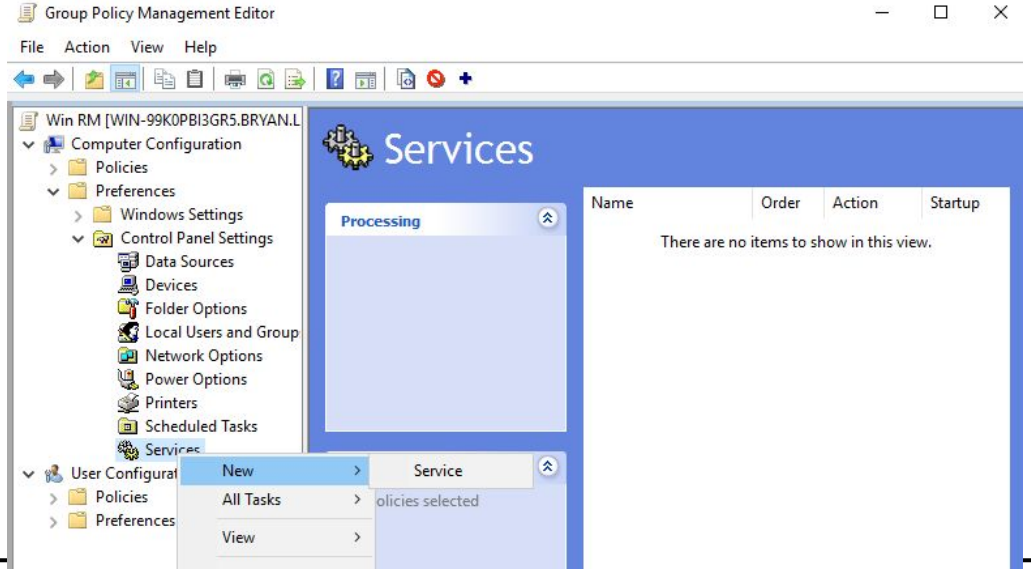


Win-RM

Double-click this policy and define it as Automatic. This way, the Win-RM service starts up automatically whenever any machine on the domain boots up.

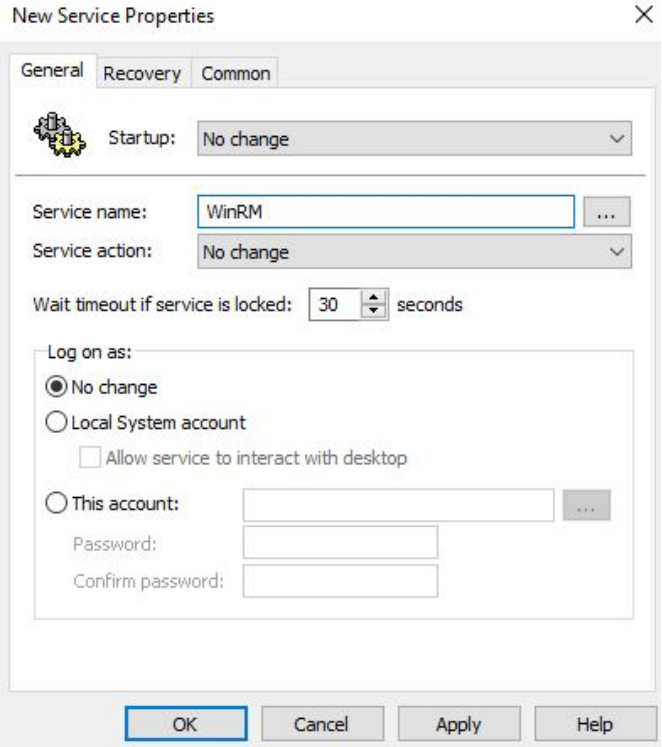
Win-RM

Then go to Computer Policies -> Preferences -> Control Panel Settings -> Services. Right-click services and select New -> Service.



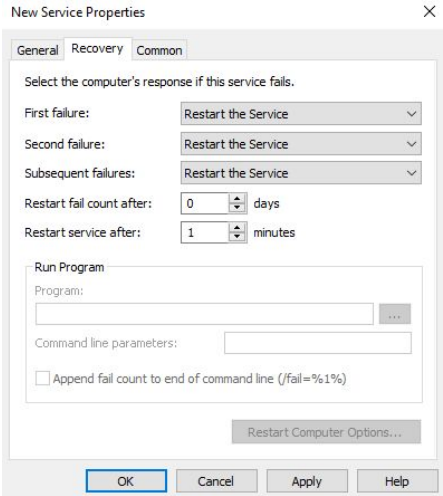
Win-RM

Call the service WinRM.



Win-RM

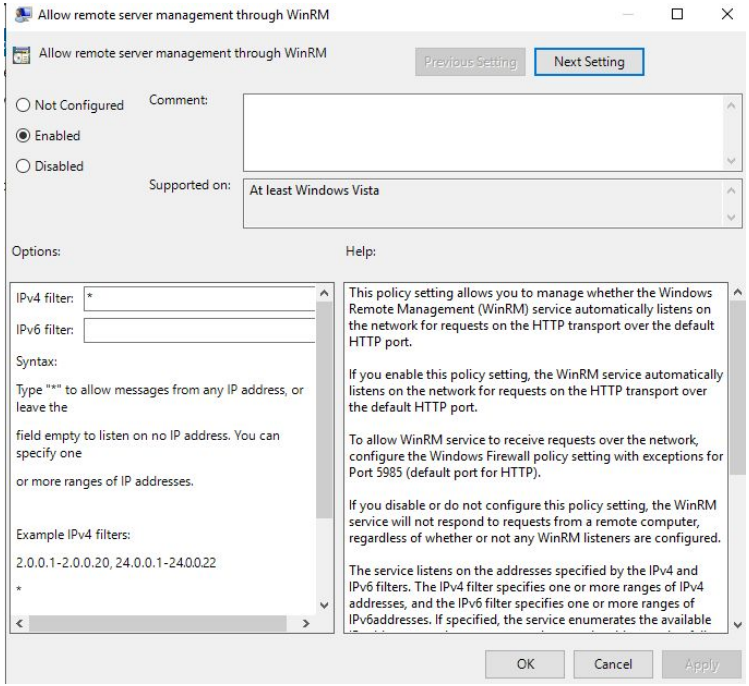
Then go to the Recovery tab and set all responses to Restart the Service. This tells the computers to restart WinRM in the case that it fails for whatever reason.



Win-RM

Computer Configuration -> Policies -> Administrative Templates -> Windows Components -> Windows Remote Management (WinRM) -> WinRM Service. Click Allow remote server management through WinRM and Enable it. For the IP filters, put a “*” under IPv4 filters.

Win-RM

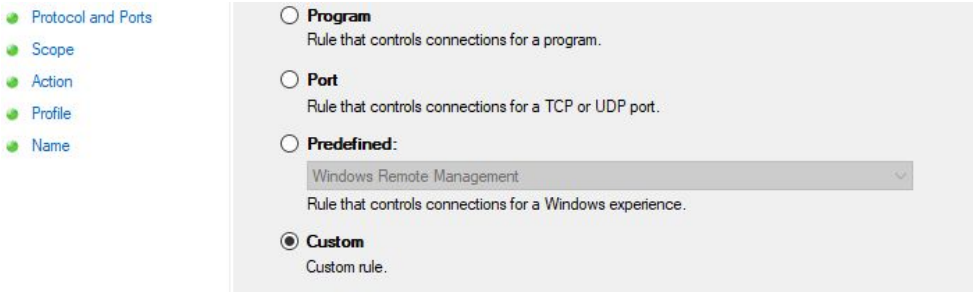

Allow remote server management through WinRM
Allow remote server management through WinRM
Previous Setting
Next Setting
Not Configured
Enabled
Disabled
Comment:
Supported on:
At least Windows Vista
Options:
Help:
IPv4 filter:
*
IPv6 filter:
Syntax:
Type "*" to allow messages from any IP address, or leave the
field empty to listen on no IP address. You can specify one
or more ranges of IP addresses.
Example IPv4 filters:
2.0.0.1-2.0.0.20, 24.0.0.1-24.0.0.22
*
This policy setting allows you to manage whether the Windows Remote Management (WinRM) service automatically listens on the network for requests on the HTTP transport over the default HTTP port.
If you enable this policy setting, the WinRM service automatically listens on the network for requests on the HTTP transport over the default HTTP port.
To allow WinRM service to receive requests over the network, configure the Windows Firewall policy setting with exceptions for Port 5985 (default port for HTTP).
If you disable or do not configure this policy setting, the WinRM service will not respond to requests from a remote computer, regardless of whether or not any WinRM listeners are configured.
The service listens on the addresses specified by the IPv4 and IPv6 filters. The IPv4 filter specifies one or more ranges of IPv4 addresses, and the IPv6 filter specifies one or more ranges of IPv6addresses. If specified, the service enumerates the available
OK
Cancel
Apply

Win-RM

Next, we will have to create firewall rules to allow incoming Win-RM traffic on computers. Go to Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Windows Firewall with Advanced Security -> Windows Firewall with Advanced Security. Right-click Inbound Rules and hit new.

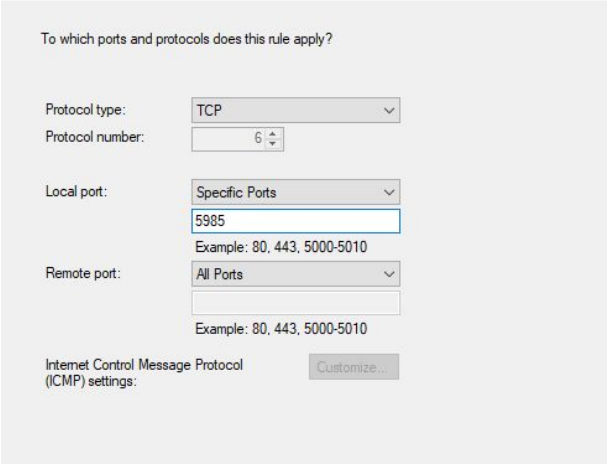
Win-RM

There are predefined rules for Win-RM, but they allow traffic from every machine on the network. We would like to create our own that only allows Win-RM connections from the DC. That way, if a hacker got onto your network, they wouldn't be able to run Win-RM attacks against your network unless they compromised the DC. Select Custom for the rule.



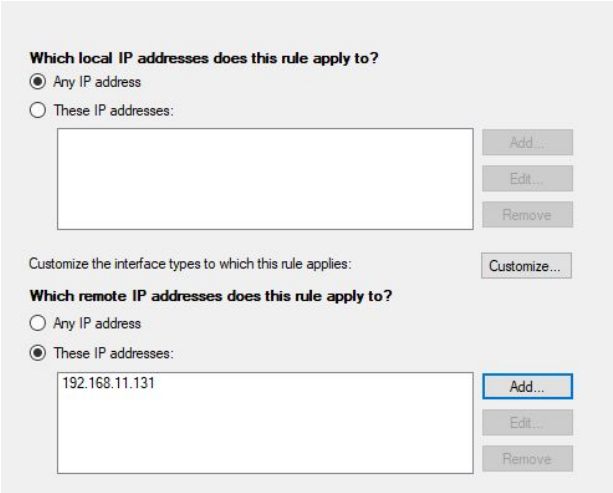
Win-RM

The Program section doesn't apply here as we are allowing remote connections and not a program to send traffic on its own. You can click Next to go to Protocol and Ports. Win-RM used TCP and will connect on the client's local port 5985.



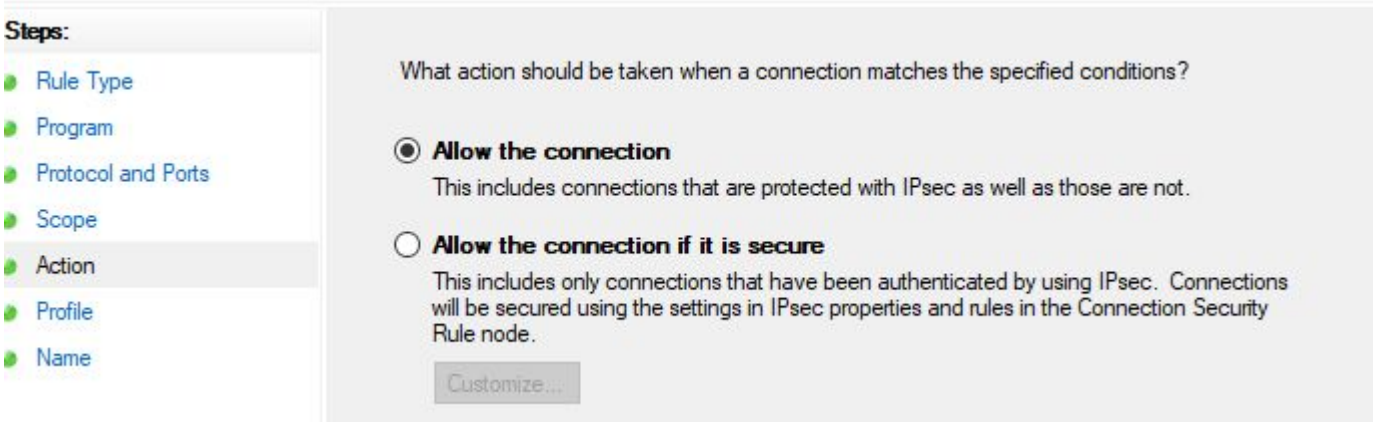
Win-RM

Set the remote IP addresses to your DC's IP address. This ensures that your workstation, and any other machine to join your domain, will only accept Win-RM connections from your DC.



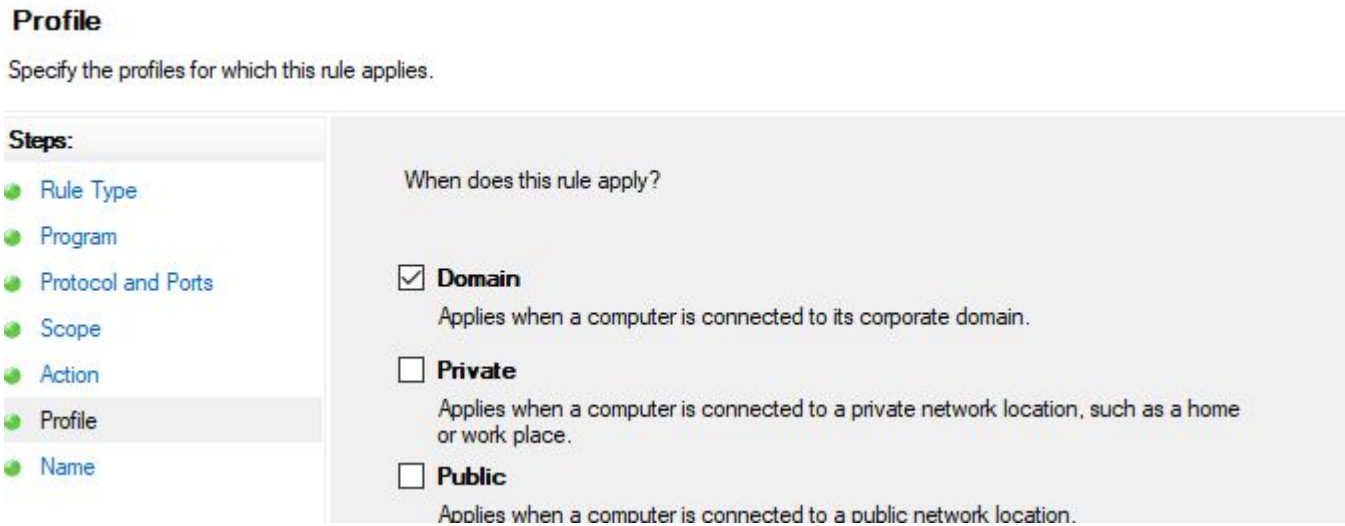
Win-RM

As for our action, we want to Allow the connection.



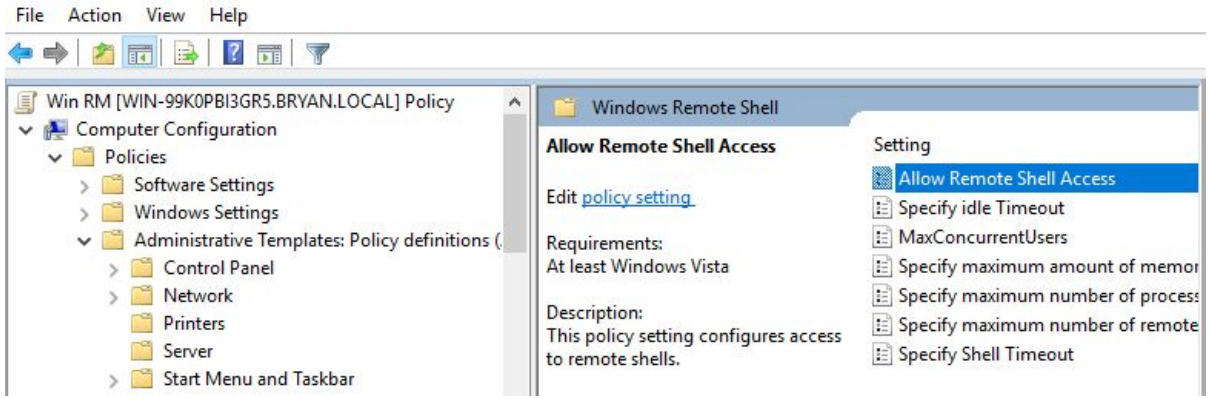
Win-RM

Lastly, we want to limit this rule to only when the workstation is on our Domain, It should not accept Win-RM commands when it is not on the domain. As for the name of the rule, call it whatever you'd like.



Win-RM

Go to Computer Configuration -> Policies -> Administrative Templates -> Windows Components -> Windows Remote Shell nand enable “Allow Remote Shell Access”



Win-RM

You can now close your GPMC and run gpupdate /force to your Workstation and DC to force this new GPO. You can logon to your Workstation and see that Win-RM is enabled by typing:

```
winrm e winrm/config/listener
```

This shows that the Workstation is listening for Win-RM connections. Notice the source is listed as GPO.

```
C:\Users\Administrator>winrm e winrm/config/listener
Listener [Source="GPO"]
    Address = *
    Transport = HTTP
    Port = 5985
    Hostname
    Enabled = true
    URLPrefix = wsman
    CertificateThumbprint
    ListeningOn = null
```

Win-RM

You can try using Nmap to scan port 5985 of your workstation from your DC. you should see the port open. However, if you scan it from you Kali machine, you should see the port as filtered. This will confirm that the firewall rule we made has worked, and your workstation is only allowing Win-RM traffic from your DC.

Win-RM

You can enter an interactive PowerShell session over Win-RM by running the following command from PowerShell from your DC while logged in as your Domain Admin

```
Enter-PSSession <Workstation_Name>
```

You can exit the interactive shell with `Exit-PSSession`.

Win-RM

You can also run a singular command Using Invoke-Command. For example,if I wanted to run the ipconfig command.

```
Invoke-Command -computername <Workstation_Name>
-ScriptBlock {ipconfig}
```