

Adam Gatherer – EC1835226
Windows Server Administration
Skills Integration Project
09/12/20

Table of Contents

0 - Introduction & Preparation

1 – IP Addressing & DHCP

2 - Password Policy

3 - Windows Deployment Services

4 - Firefox as Default Browser

5 - Organisational Units

6 - Security Groups

7 - Hard Quotas for Storage

8 - Backup & Update Policy

9 - SSH Access for Operations Group

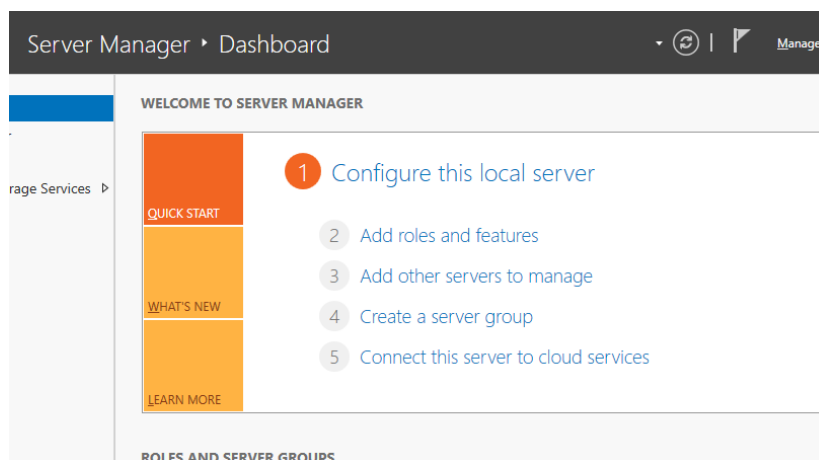
10 - Monitoring for Performance

Introduction

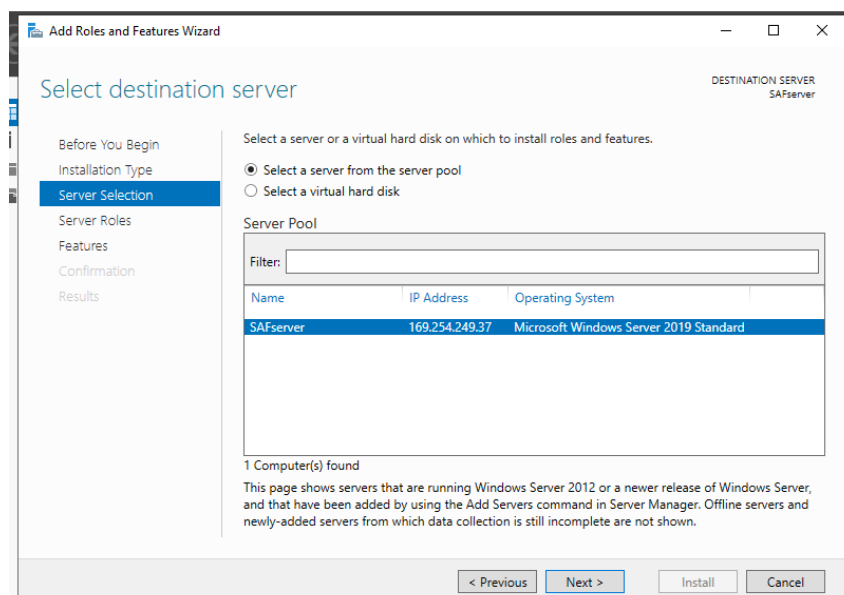
Following a merger Scot-Finance Ltd. and Ecosse-Assets Ltd. have become Scottish Assets and Finance Inc. (SAF). In this document I will be outlining the steps involved to merge the two computer systems by the means of prototyping the new system in a virtual environment. This will take the form of a Windows 2019 server and Windows 10 client virtual machines.

The server machine will be appropriately named “safserver” and the client computer will be “safclient”. Usernames will take the format of the first three letters of the user’s firstname, the first three letters of their surname and the last two digits of the employees birth year. For example “Adam Gatherer” becomes adagat92.

0.1 - Adding Roles & Features



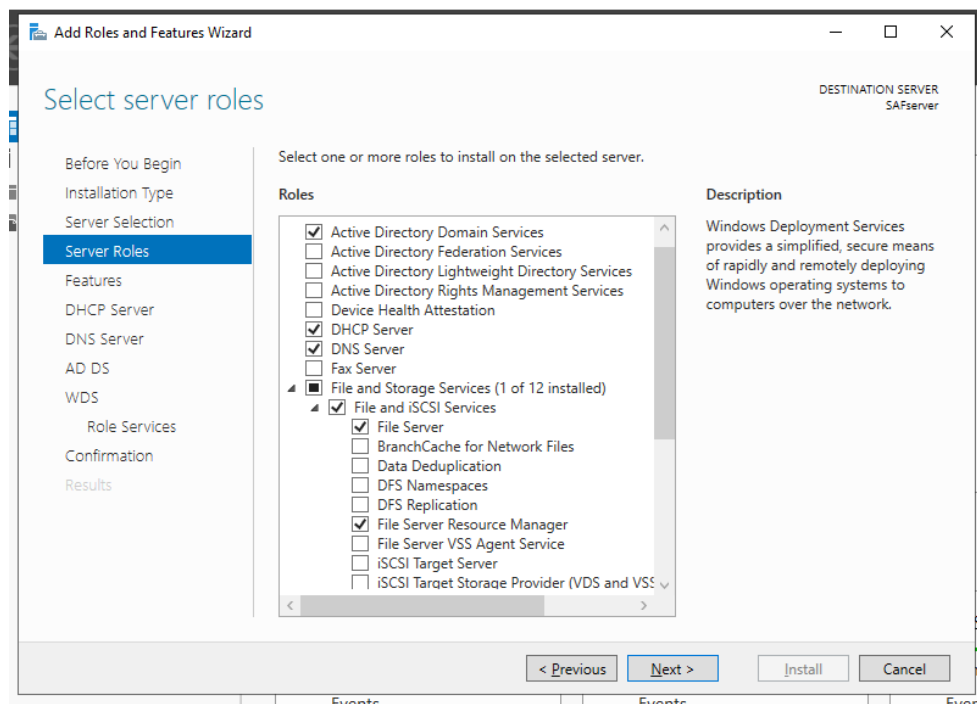
From the main dashboard, select “Add roles and features”



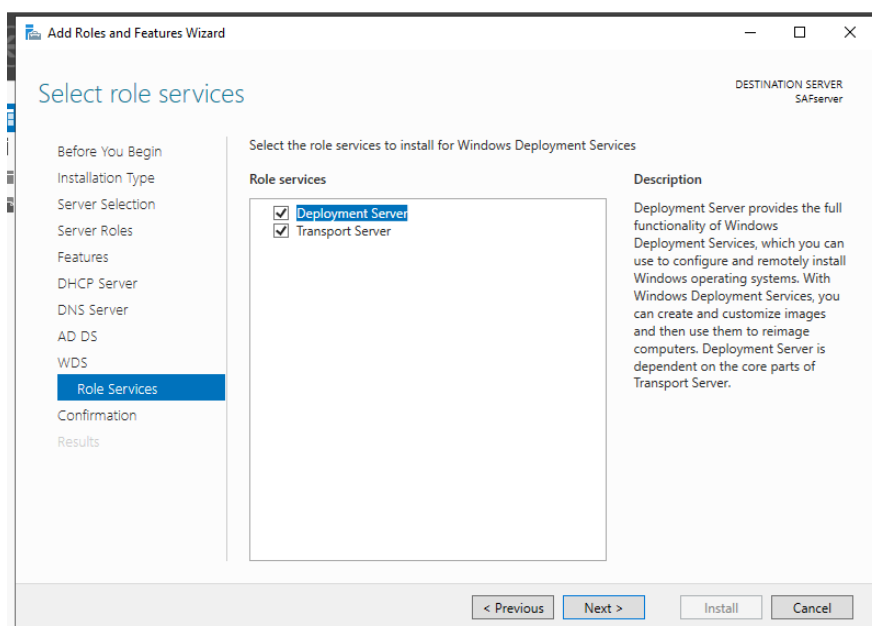
In the wizard, select “Role-based or feature-based installation”, then choose the server

For this server we will need the following services/features:

- Active Directory Domain Services
- DHCP Server
- DNS Server
- File Server
- File Server Resource Manager
- Windows Deployment Services
- Bitlocker
- Windows Server Backup

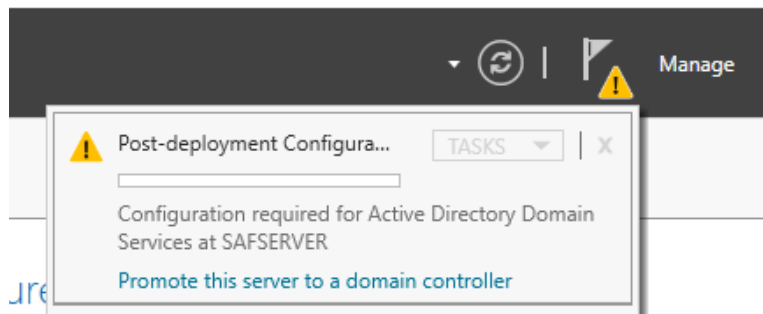


Add these features with the wizard and click next through all the windows

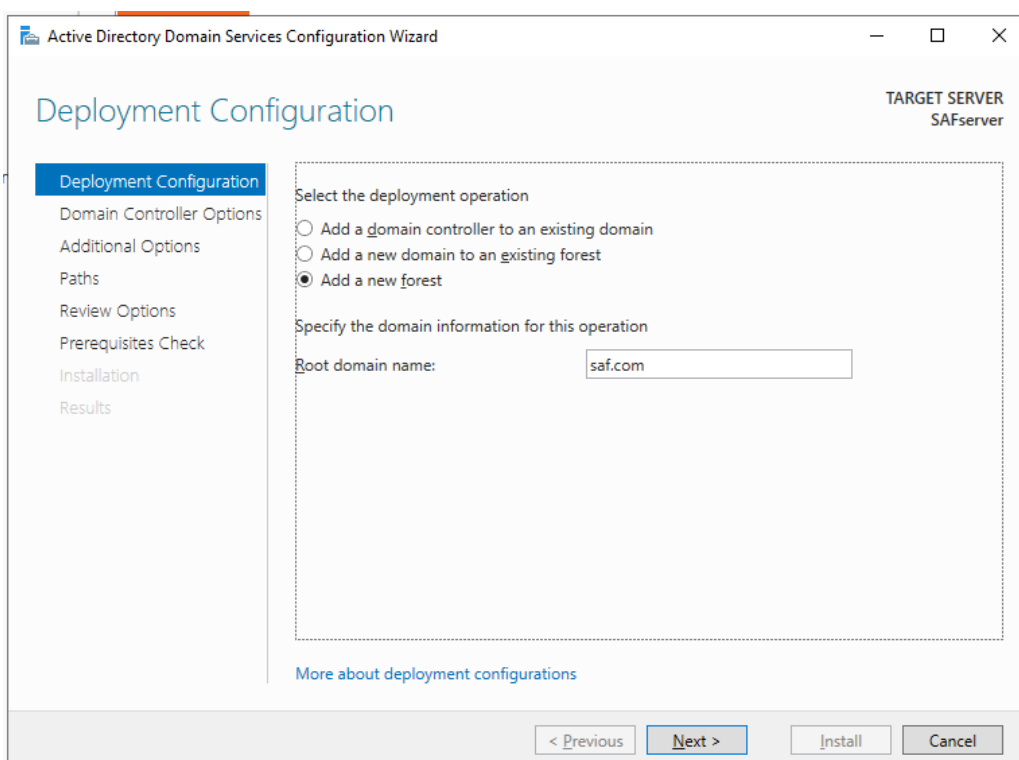


Be sure to install both Deployment Server and Transport Server under Windows Deployment Services. Once installed the server is ready to be worked on.

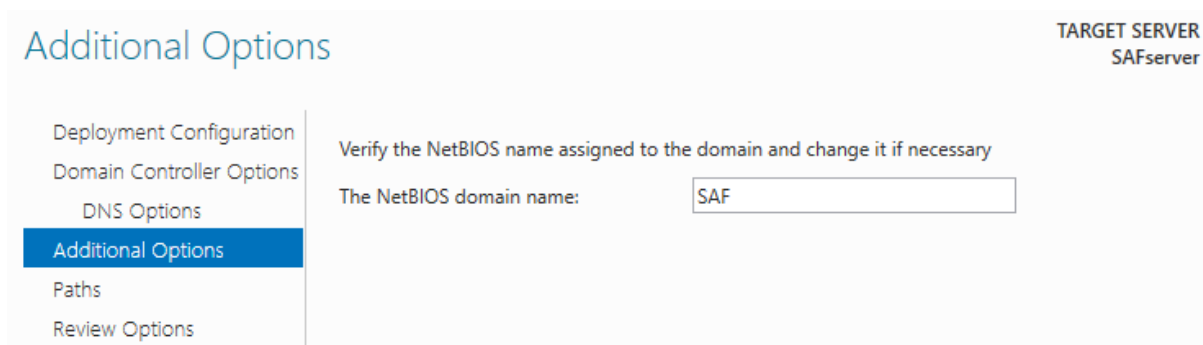
0.2 - Configuring the Active Directory



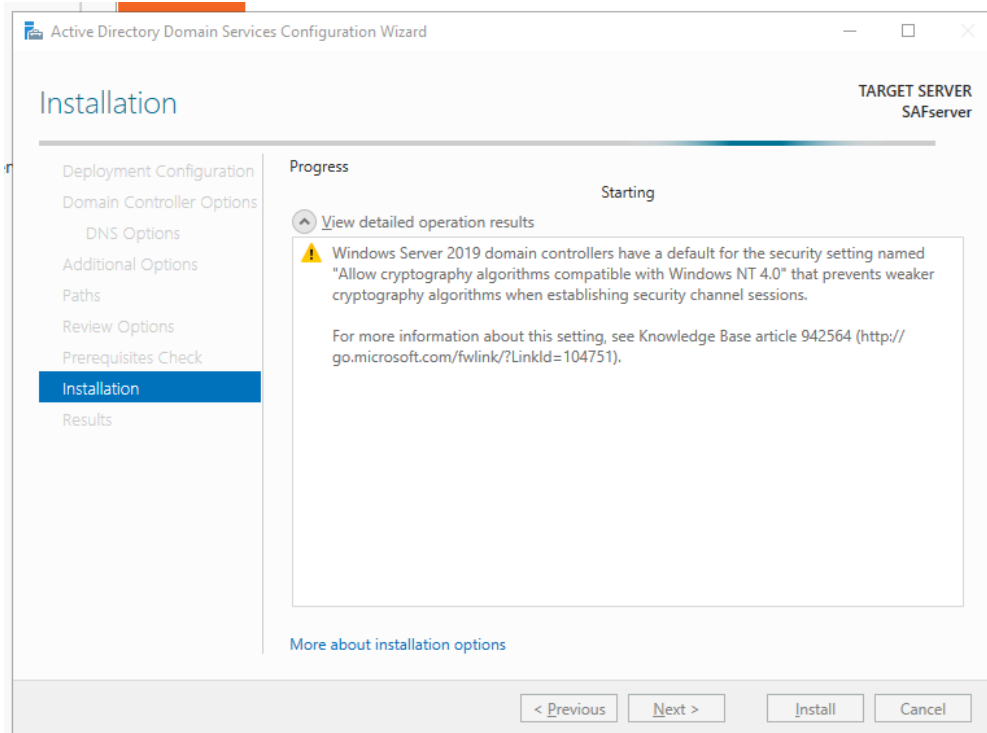
Click the flag at the top right side of the server manager window and click “Promote this server to a domain controller” to open the configuration window for ADDS.



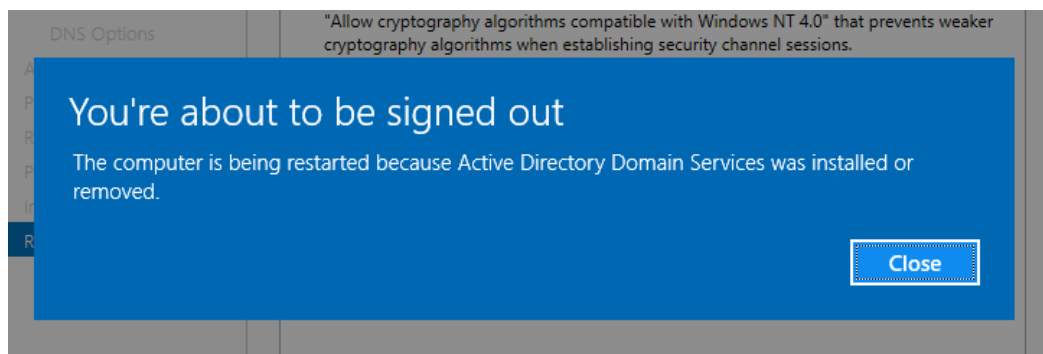
Selecting “Add a new forest”, enter saf.com as the root domain name and for the password we’ll use the same example password (saf!123)



Skip over creating a DNS delegation, leave the NetBIOS name as the default (SAF in this example), click Next and leave the paths as default.



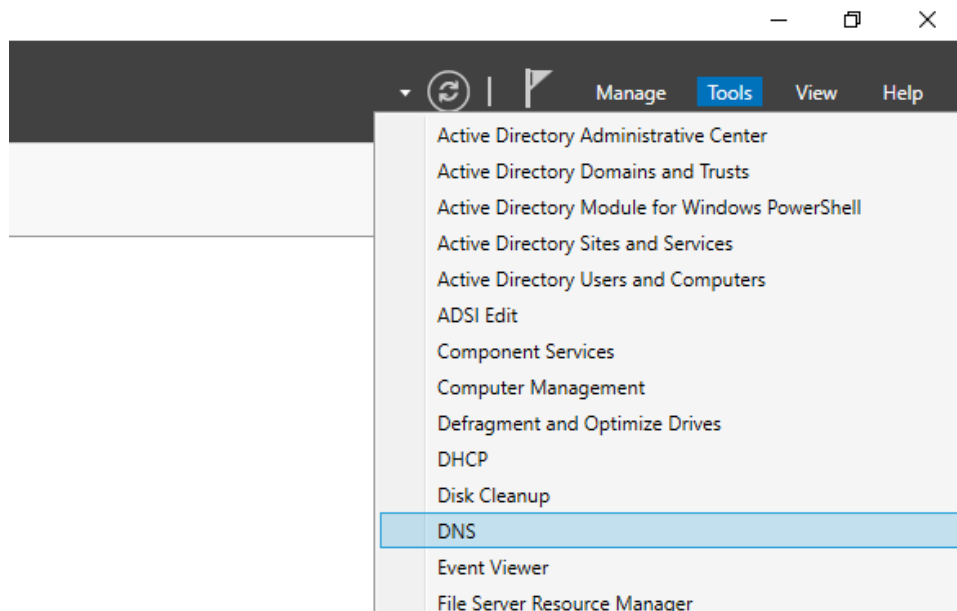
Review the options and observe the prerequisite checks. There will be a number of yellow triangle exclamation mark symbols but these are not important for our needs just now and can be ignored. Let the server install the ADDS by clicking Install. This will take a few minutes.



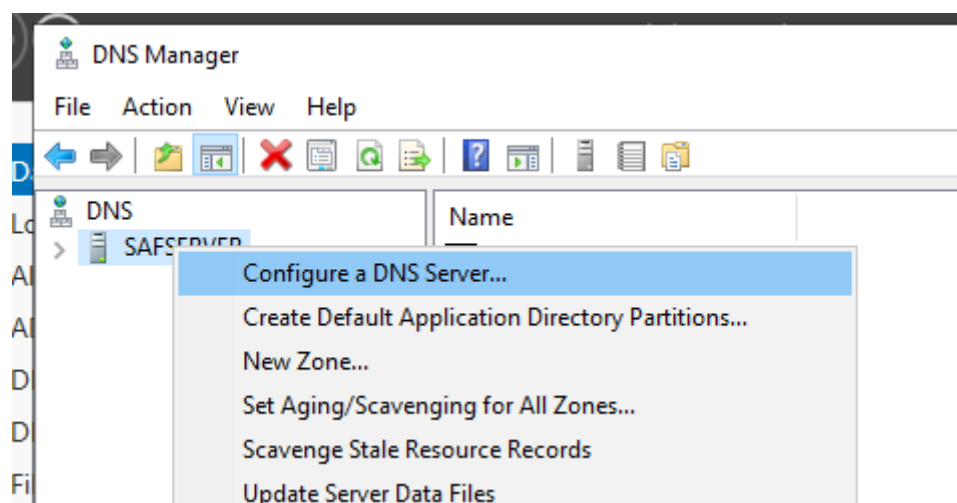
The server will now restart.

0.3 - Configuring the Server As A DNS Server

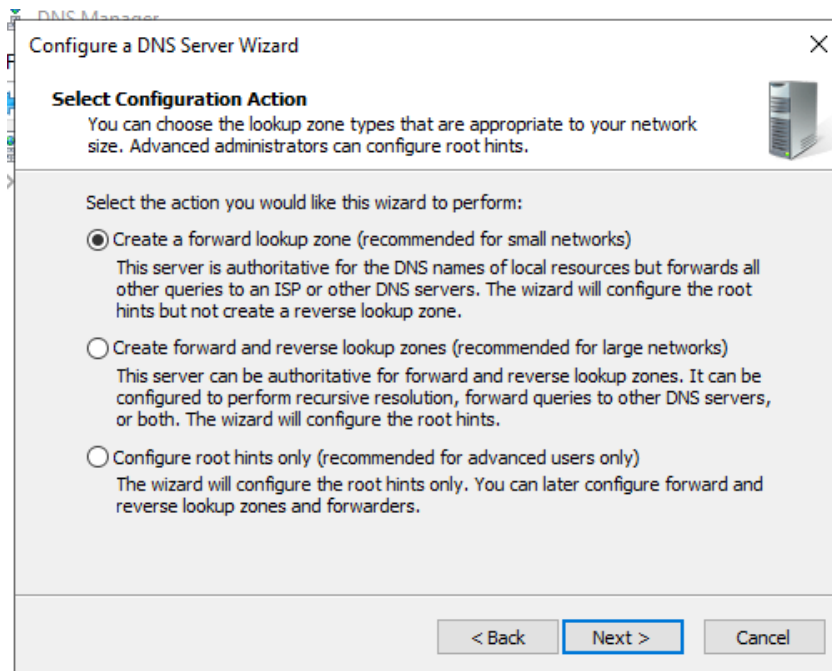
To make things easier for computers joining the domain we can set the server up as a DNS server. This means that computers will be able to connect to saf.com. It is also required for Windows Deployment Services, which we shall see later on.



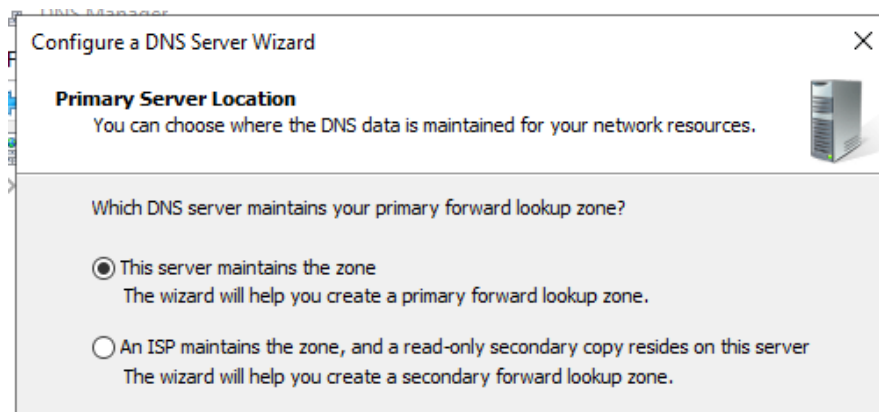
In the top right hand side of the Server Manager window is the Tools menu. We will be using this a lot. Click it and select "DNS" from the menu.



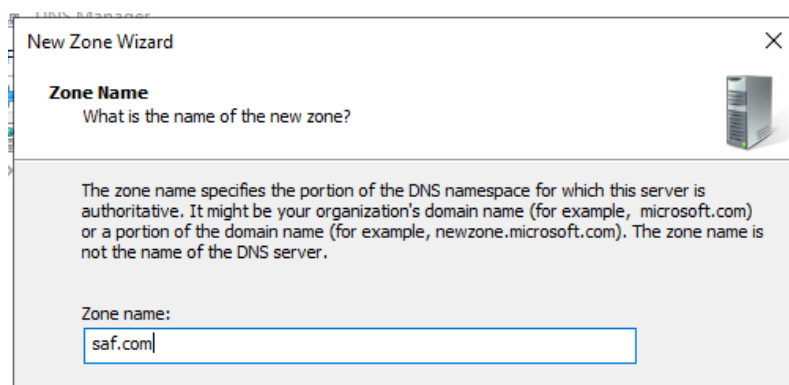
Right click the server from the list and select "Configure a DNS Server..."



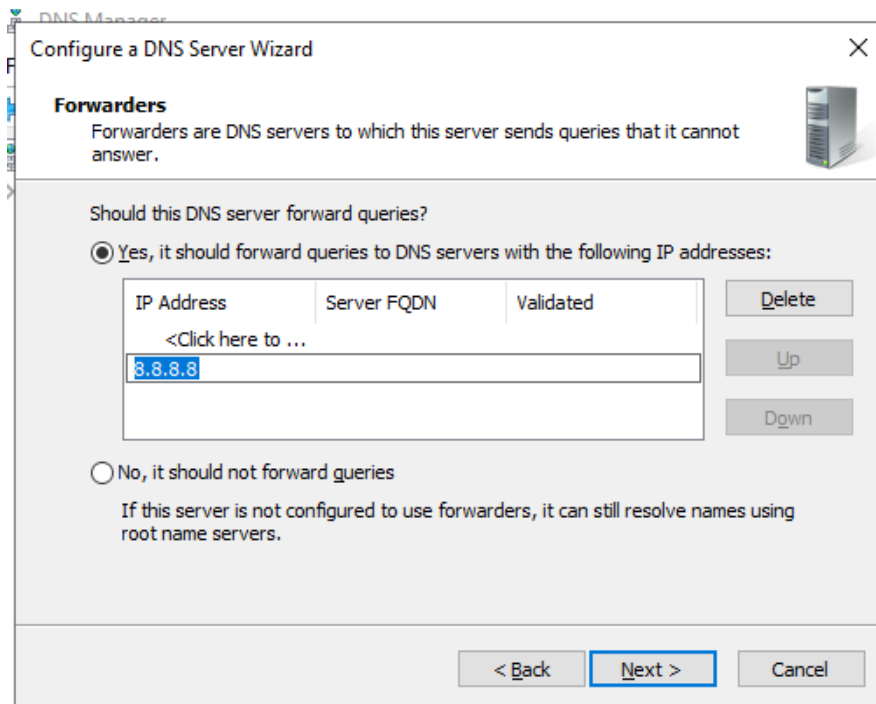
In the wizard, click Next then “Create a forward lookup zone” and Next again



Select the “This server maintains the zone” radio button and click Next



We'll name the zone saf.com, then click next again



Allow only secure dynamic updates via the radio button, click next and then we'll configure the DNS server to forward queries to an external DNS server (in this demonstration we are using Google's DNS server, 8.8.8.8). Check the summary and click Finish to finish setting up the DNS server.

1 - IP ADDRESSING & DHCP

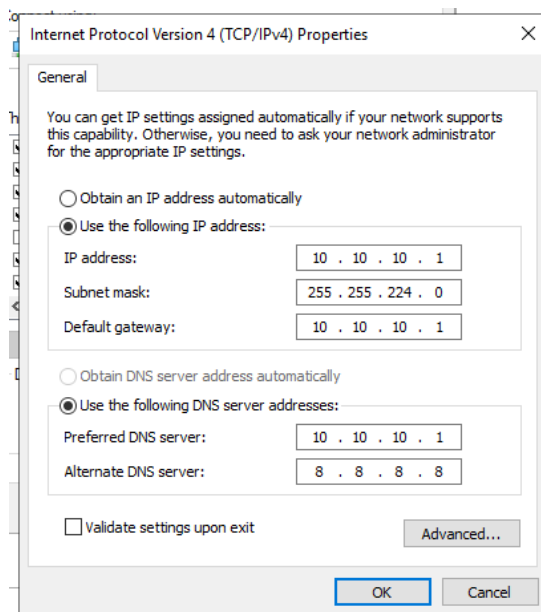
1.1 - The addressing Scheme

As there will be a need to support 4,000 devices and the DHCP scope is to start at 10.10.10.2 I will be using the 10.10.0.0/19 network. This will allow for 4,000 addresses starting from 10.10.10.2 to all be in the same network.

Subnet Mask	255.255.224.0
First Usable Address	10.10.0.1
Last Usable Address	10.10.31.254
Broadcast Address	10.10.31.255
DHCP Scope Start	10.10.10.2
DHCP Scope End	10.10.26.2

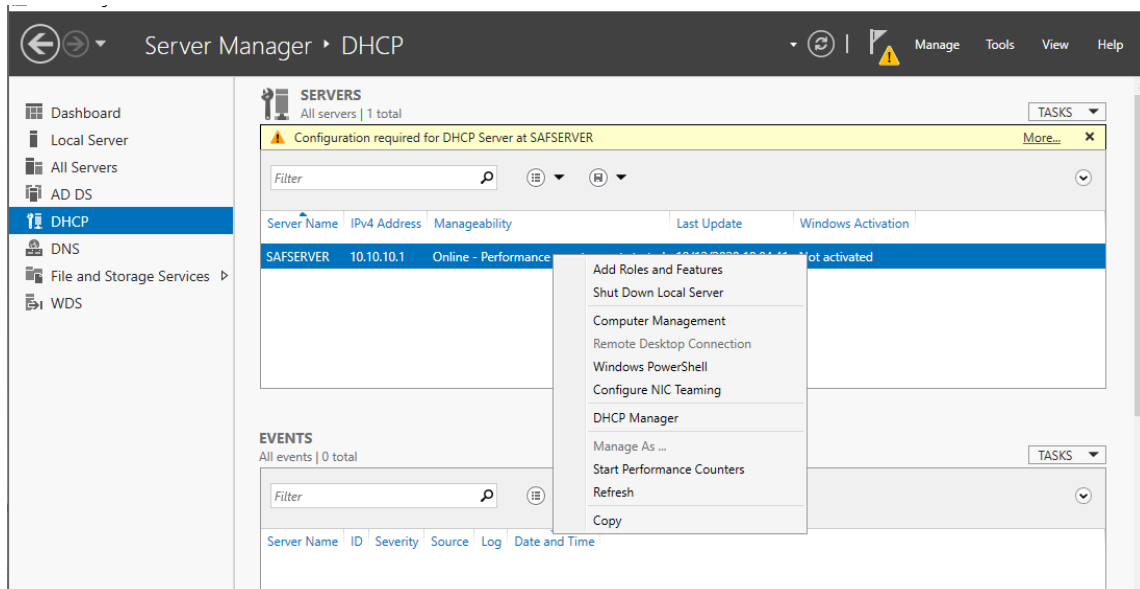
The DHCP scope will account for

First things first, we statically set the server's IP address to 10.10.10.1.

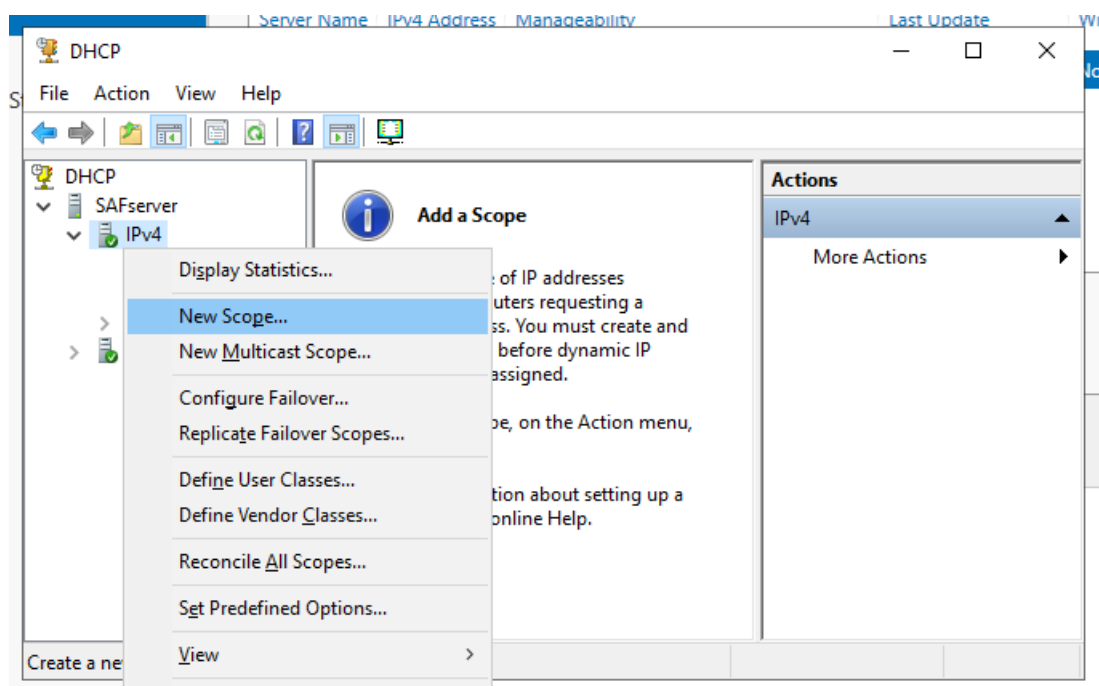


1.2 - Setting up DHCP

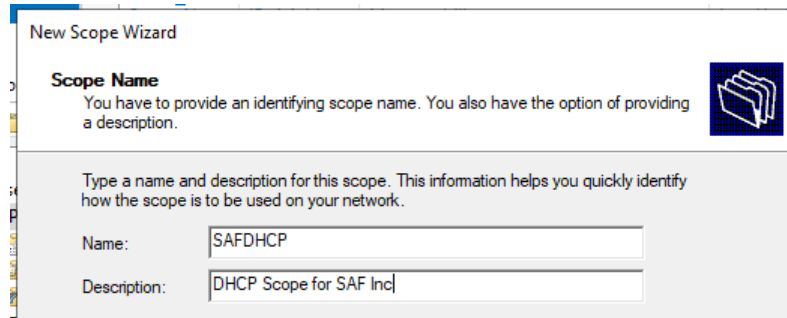
To start using DHCP on the network we can initialise a DHCP service on the Windows Server machine. The process to do this is outlined in the steps below.



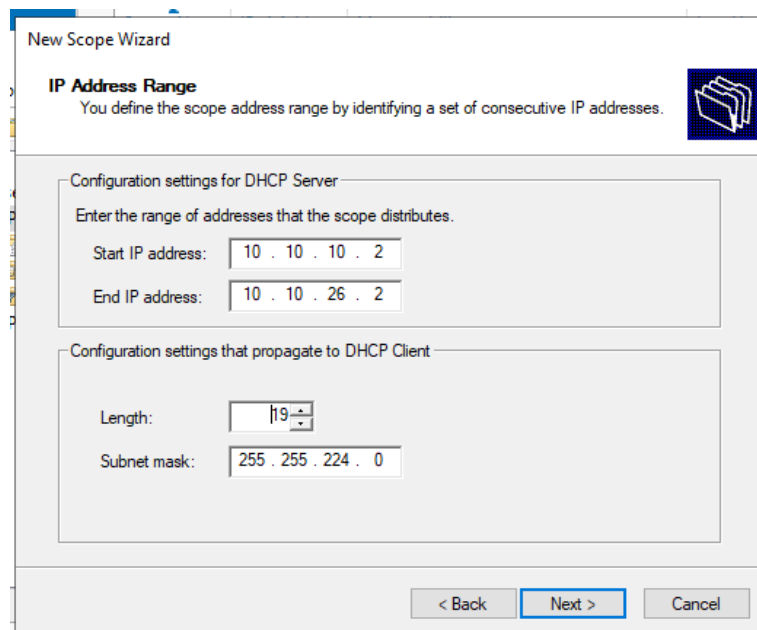
Click the DHCP service from the left hand pane of the Server Manager window then right click the server name from the list of servers and choose “DHCP Manager”



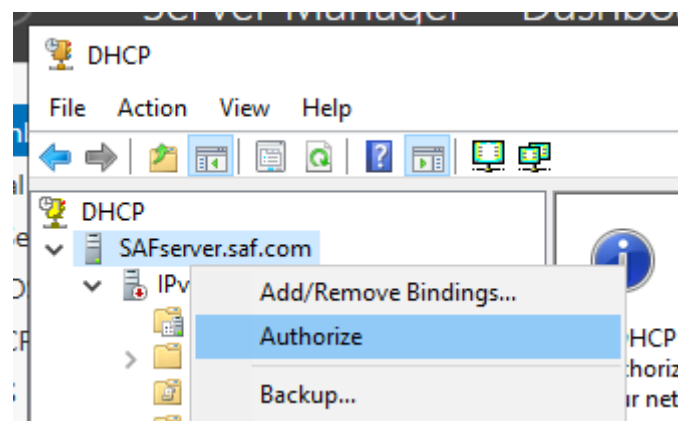
From the DHCP menu, expand the server and right click on IPv4 and select New Scope



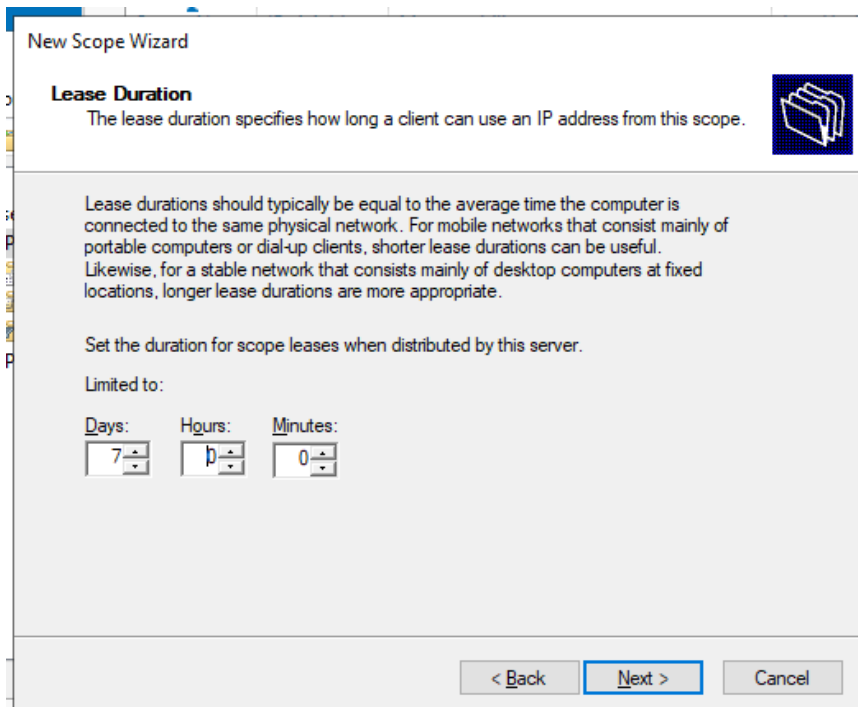
In the DHCP Scope wizard, give the new scope an appropriate name and a description that explains what the scope is for and click Next



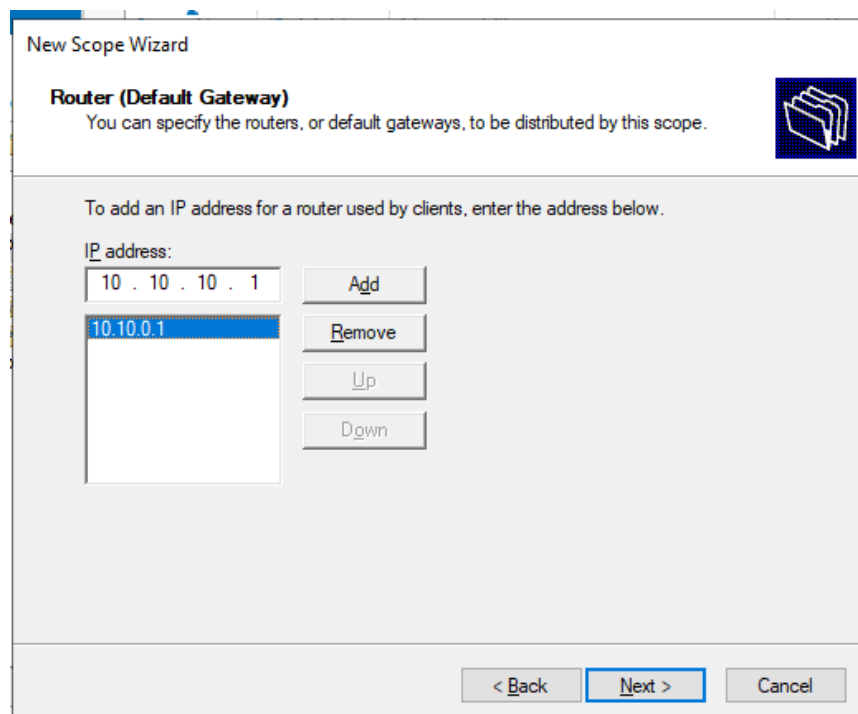
From here, enter the details for the DHCP Scope from the table at the start of this section. No exclusions will be needed for this situation.



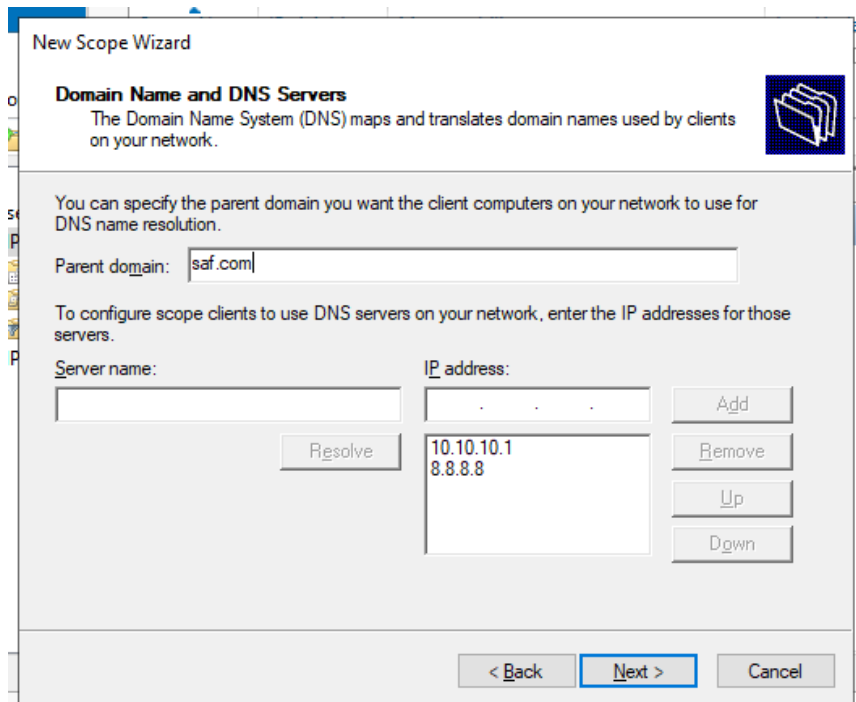
Lastly for DHCP we must right click on the server and select "Authorize" to start the DHCP service.



The lease will be set to 7 days, chosen to allow users to keep the same IP for the work week. From here click Next again and choose to configure the options now.



For this example we will tell devices via DHCP to use 10.10.0.1 as the default gateway. Click Next.



Set the parent domain name for the DNS server to be saf.com and check the IP address of the server is in the list of IP addresses. Click Next and then choose to activate the scope now.

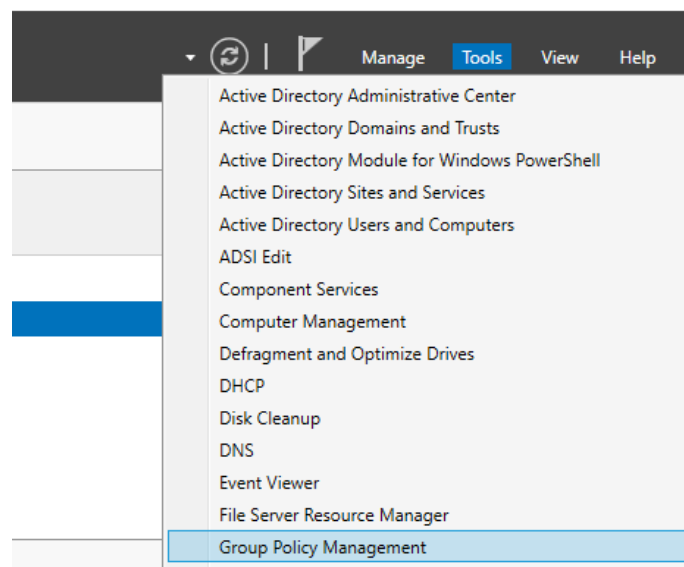
DHCP scope has now been configured so any device connecting to the 10.10.0.0/19 network will see the SAFserver as a source of DHCP information and obtain an address within the scope.

2 - PASSWORD POLICY

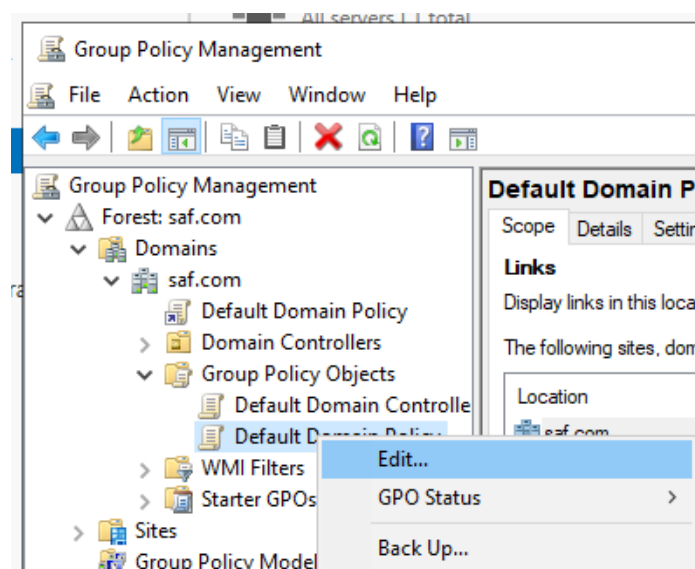
The password policy for the company should be strong but not so intense that users will forever be forgetting passwords and overloading the IT department with support tickets. Passwords therefore must be:

- 8 characters long
- use a mix of letters, numbers and symbols
- not contain any part of the user's username
- change every month
- not be the same as any password from the past two years

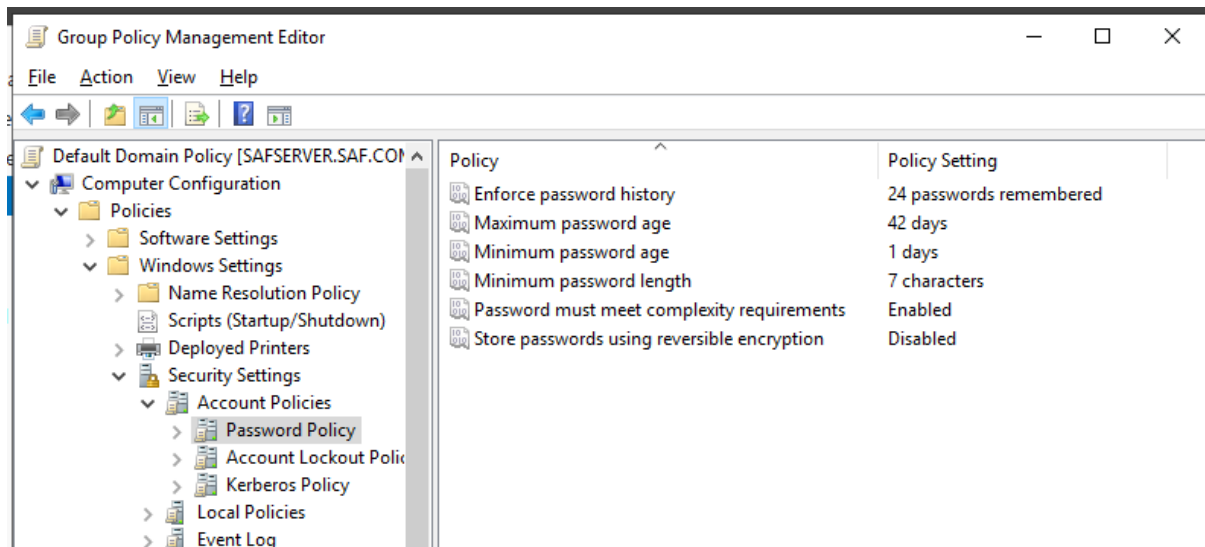
We can apply the password policy to the default domain policy. This can be configured via the steps below.



Select "Group Policy Management" from the Tools menu at the top right hand side of the Server Manager window.



From here expand the saf.com forest and domain and right click on "Default Domain Policy" under "Group Policy Objects". From this menu, select "edit"



Expand the sections to get to Computer Configuration, Policies, Windows Settings, Security Settings, Account Policies, Password Policy. This is where we can alter the policy settings by right clicking on them and selecting "Properties" to bring up the configuration window.

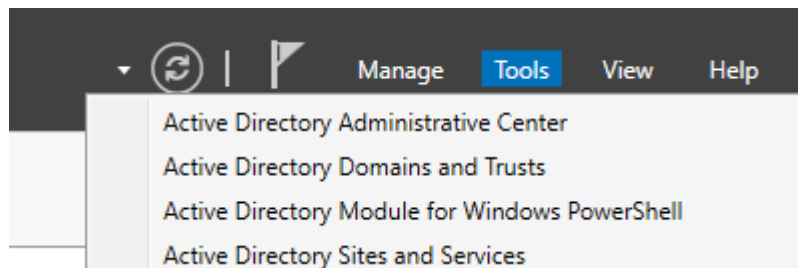
Policy	Policy Setting
Enforce password history	24 passwords remembered
Maximum password age	30 days
Minimum password age	1 days
Minimum password length	8 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

To meet our specified policy we set it to remember the last 24 passwords (password history), require a password change every 30 days (maximum age), use the mix of letters/numbers/symbols (complexity requirements) and have a minimum length of 8 characters. Leave minimum length and storing using reversible encryption as their default values.

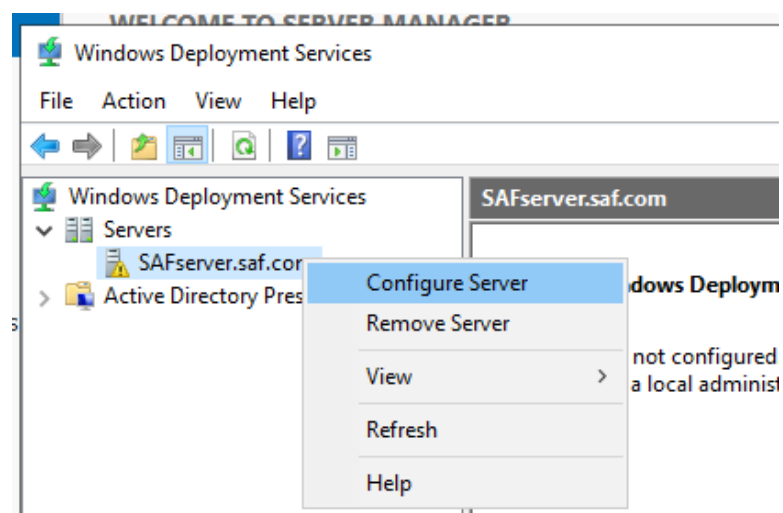
3 - WINDOWS DEPLOYMENT SERVICES

Rather than installing Windows manually onto every desktop computer in the company (some 4,000 odd) we can set up our Windows Server to deploy a Windows 10 image to computers booting into network boot mode. We can install Windows 10 to one desktop computer, configure it to be our ideal install and then upload an image to the Windows Deployment Services. This saves time not just for installation of the operating system, but also for installing applications and software after OS installation.

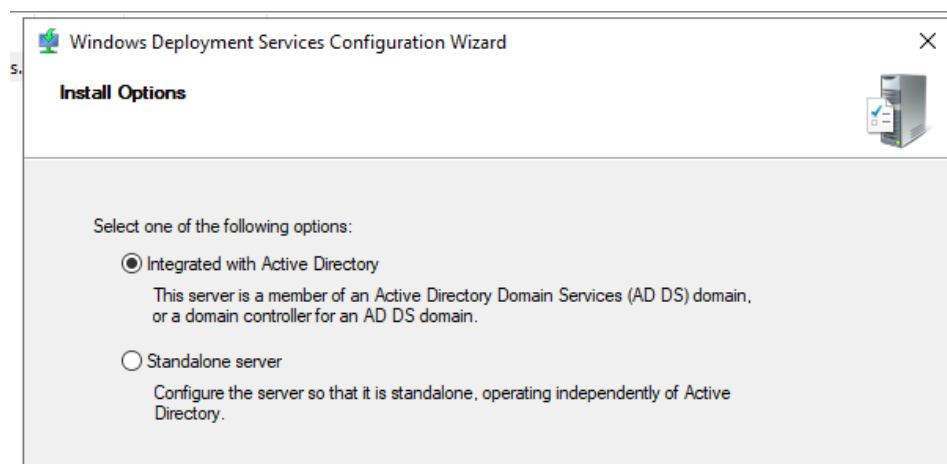
3.1 - Configuring the WDS Role



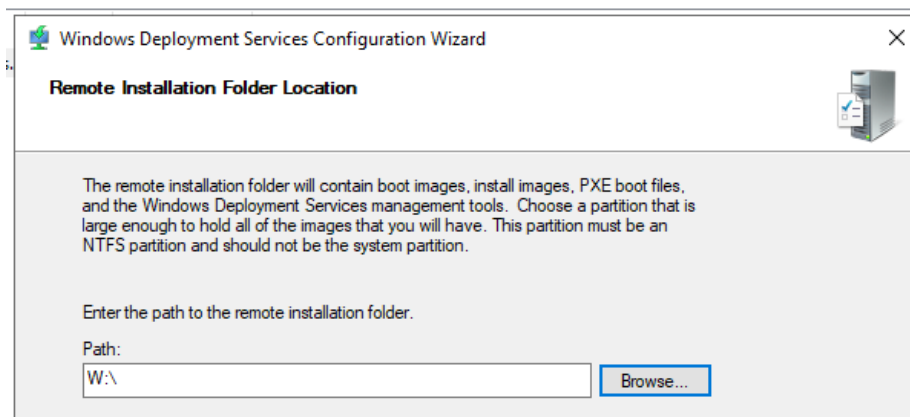
We start by clicking the “Tools” menu in the top right hand side of the Server Manager window. Scroll down to find “Windows Deployment Services” and click it to open the WDS window.



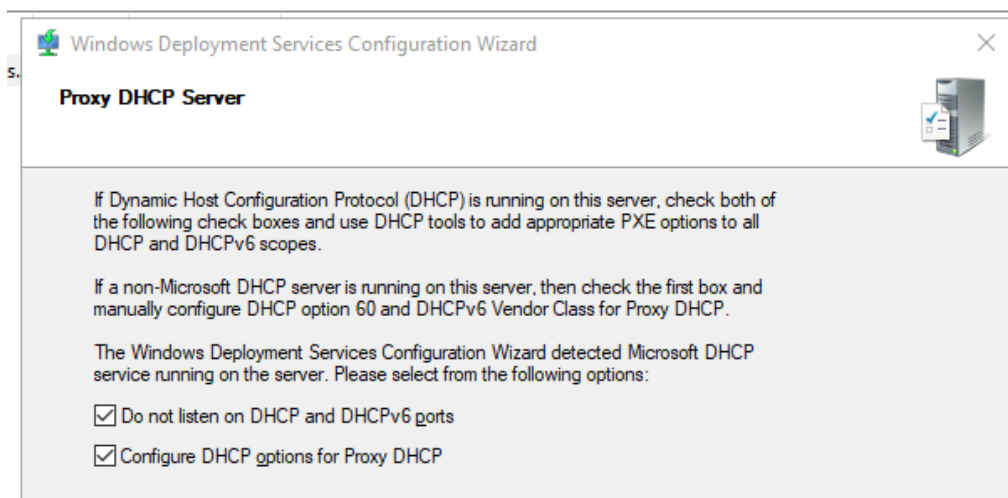
In this window, expand the server tree and right click on the SAFserver.saf.com server and click “Configure Server”



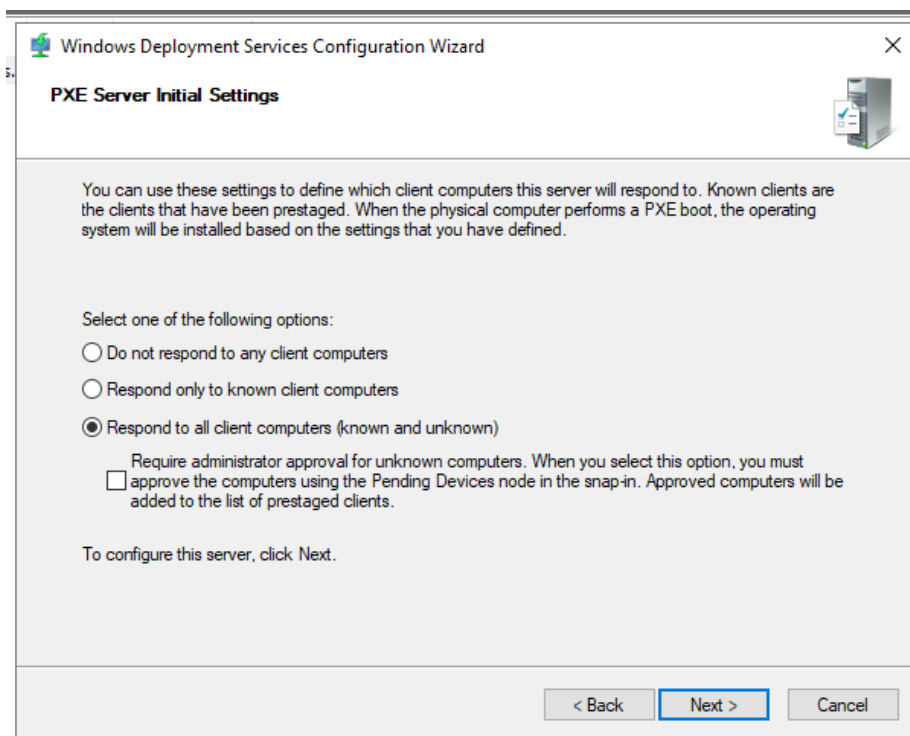
Choose to integrate the WDS server with the Active Directory and click next



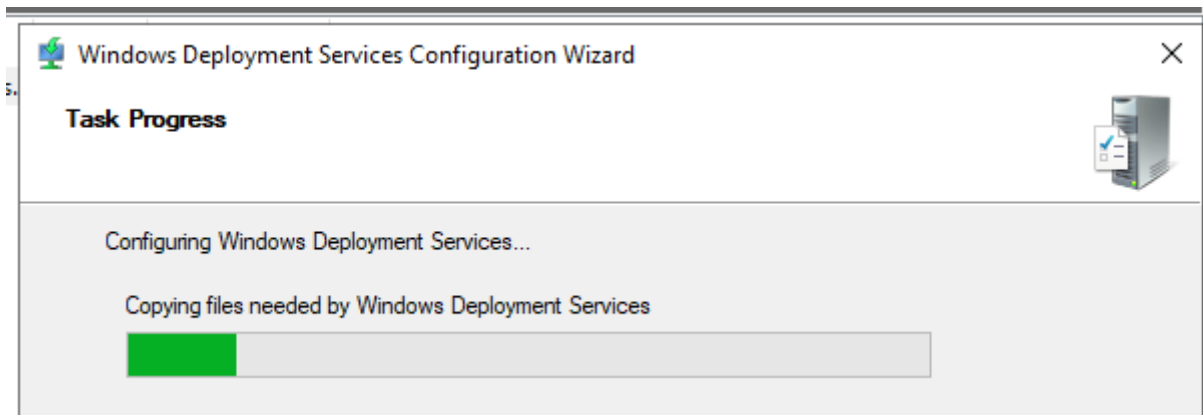
Set the path to the location where we will be putting our boot and install images. In this demonstration we are using an external disk, drive W:



We will want to check both boxes here and click next



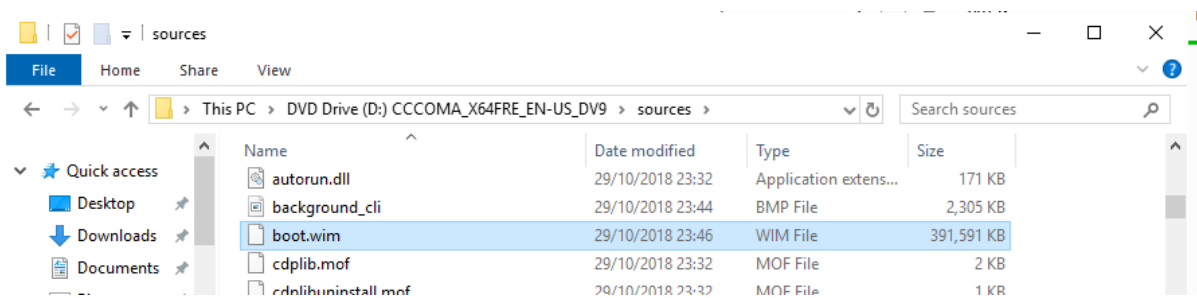
Click the radio button to respond to all client computers (this can be changed as per the needs of the server once live in the enterprise scenario) and click Next



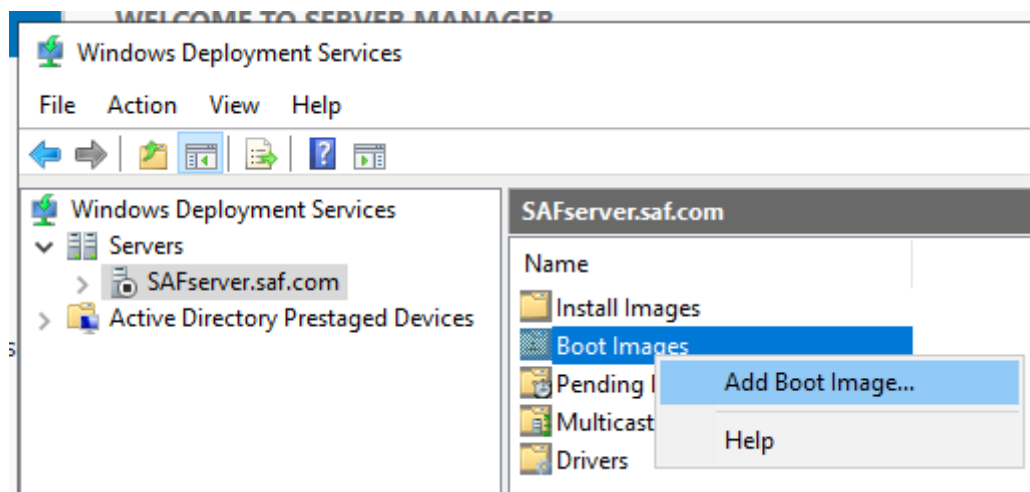
The WDS server is now being set up. Next we will need some images.

3.2 - Sourcing Boot & Install Images

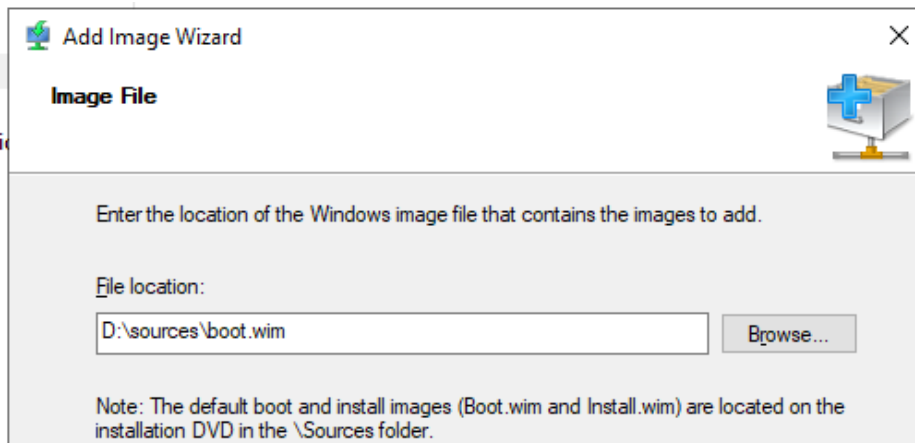
Now that WDS is active we need some images for it to send to client computers. These can be found in and extracted from the Windows 10 installation disc/image.



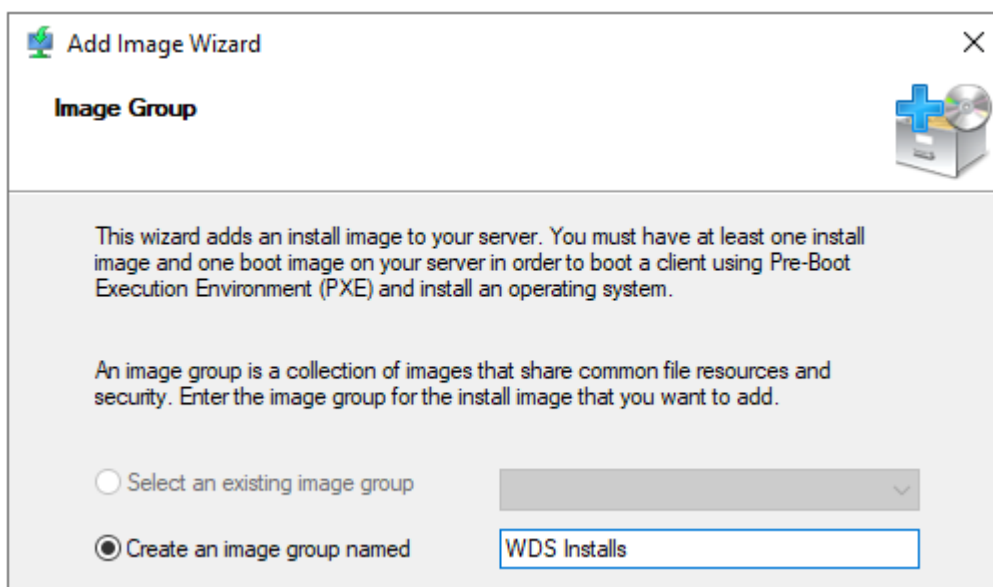
Firstly, we'll insert the Windows 10 installation disc image to our virtual server (this can be done with a physical disc as well!). Open the image in Explorer and find the boot.wim image in the sources folder. Also make sure that install.wim is there.



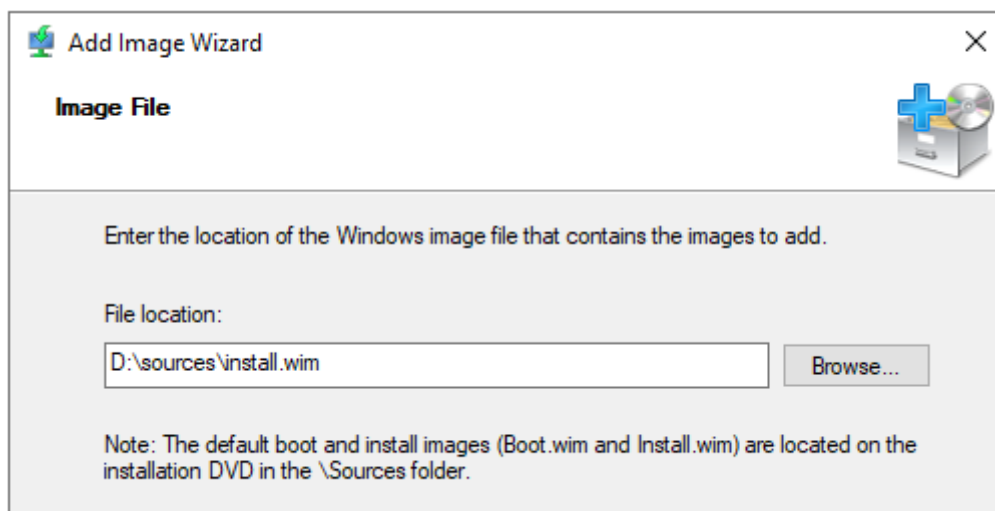
Back in the WDS window, right click boot images and select "Add Boot Image..."



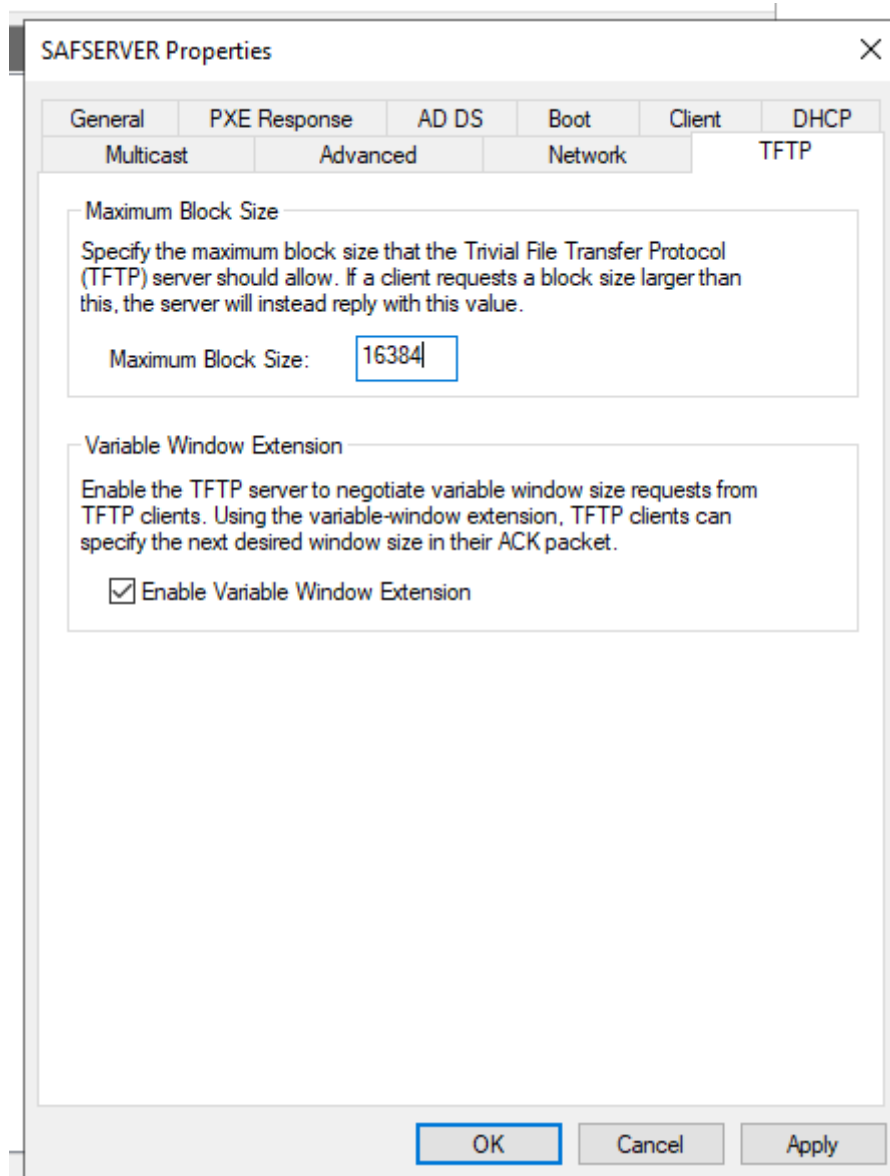
Use the boot.wim image we found in the previous step and click next. Then give it an appropriate name and description. Click next again and once more to add the boot image.



We now repeat this step but right clicking on Install Images and then selecting install.wim. We will also have to create an Image Group. Call this "WDS Installs"



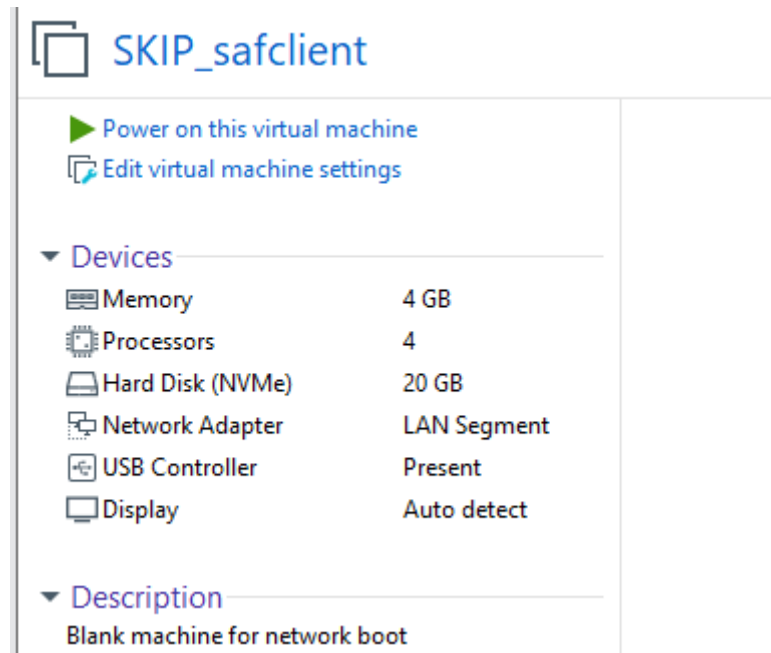
Click next after finding install.wim and then next again, checking all the boxes for the various versions of Windows we wish to install. Then Next once more to add the images.



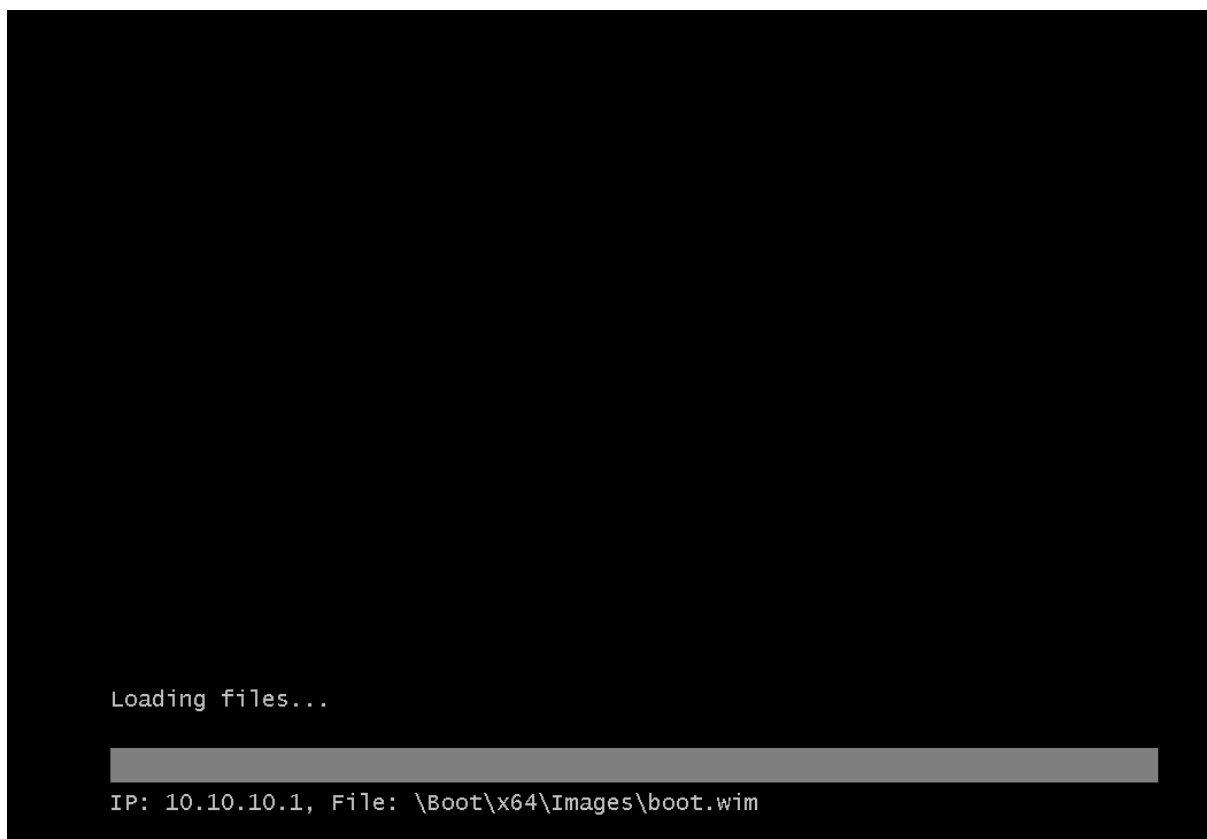
The last thing to do is to change the TFTP block size to 16384. This is done by right clicking on the server in the WDS window and selecting properties. From here we go to the TFTP tab and update the maximum block size.

3.3 - Installing Windows To A Client Via WDS

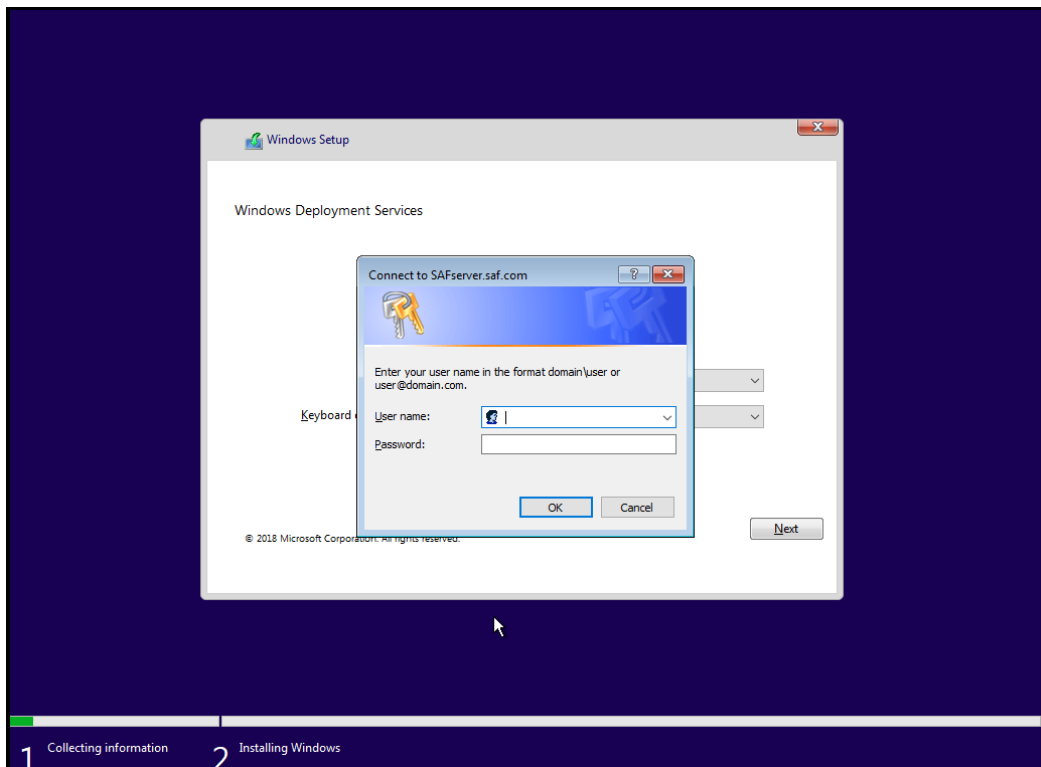
Now we can test out our WDS server with a demonstration install. Simply done, we put the client in the same network as the virtual server and boot it into network boot mode.



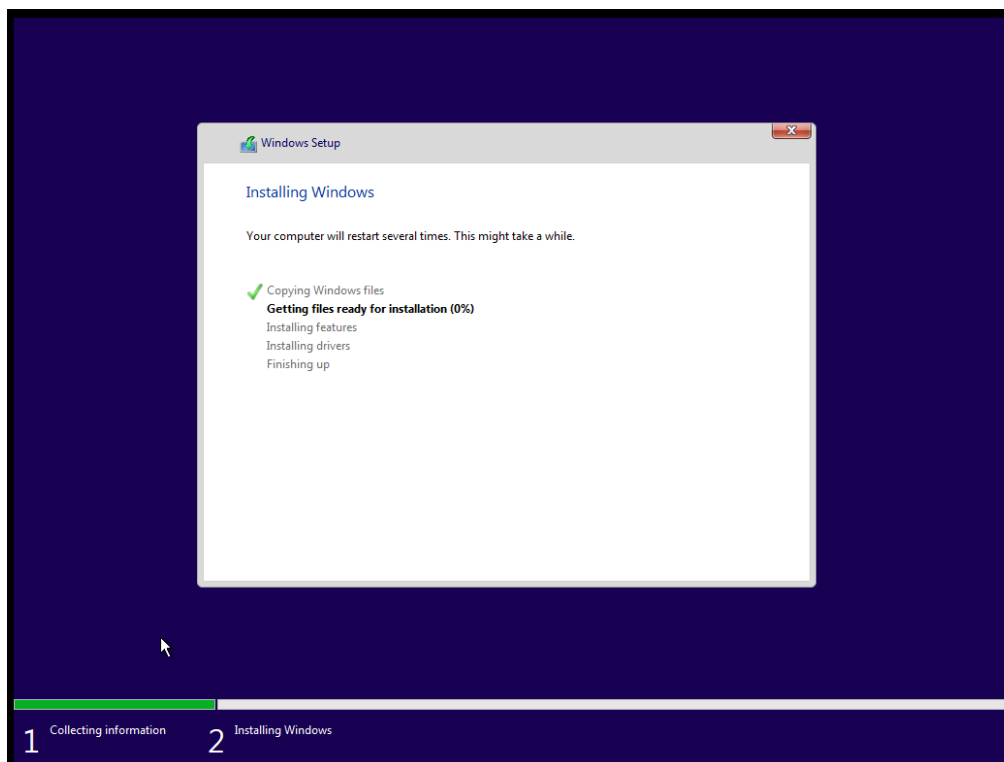
Here we have a blank VM ready for network booting. It's in the same LAN segment as our server and does not have any installation media. When it boots, it will receive an IP address from our DHCP server and then start installing Windows 10 from our images.



Pressing F12 as the client boots puts it into PXE network boot mode. Now we wait...



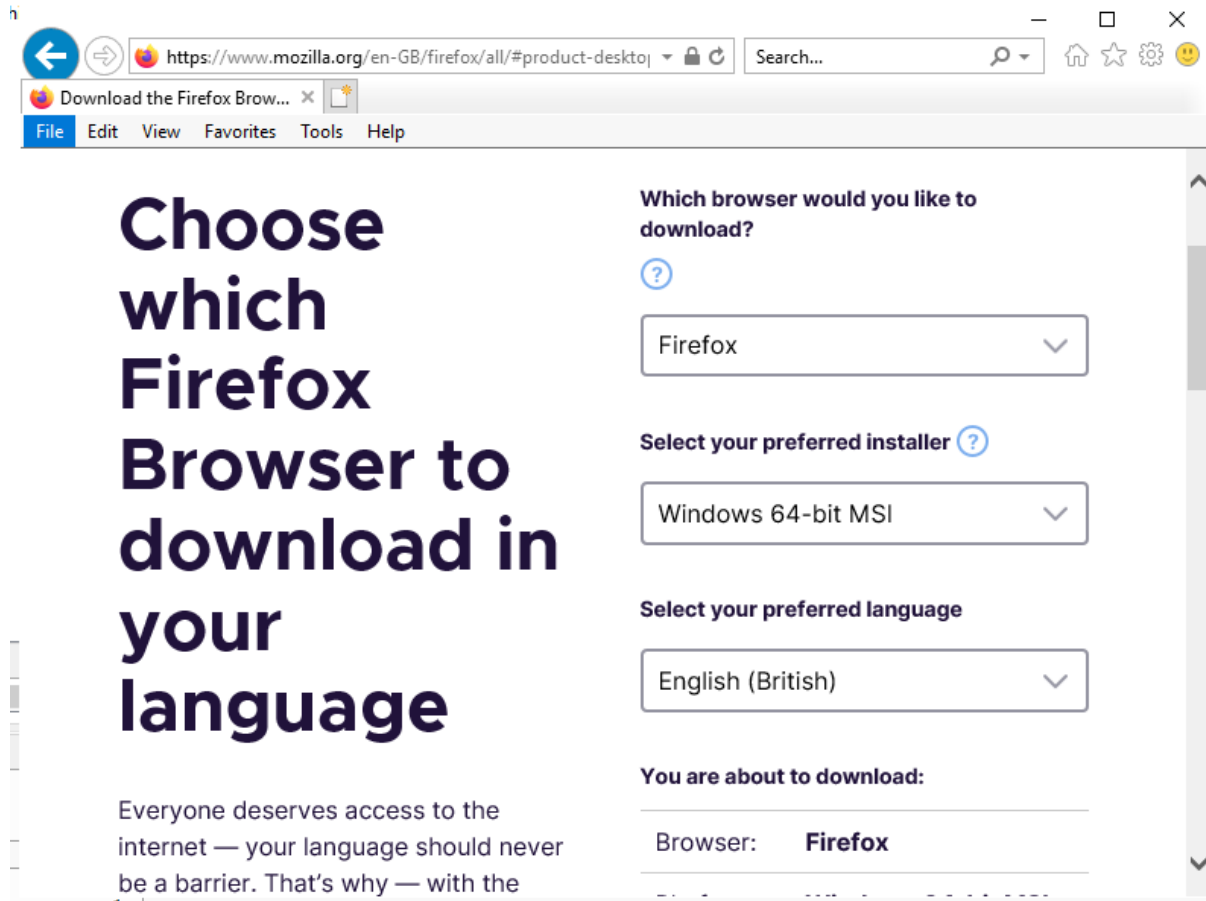
Simply enter the administrator username and password, select the version of windows and the empty hard drive to start the installation



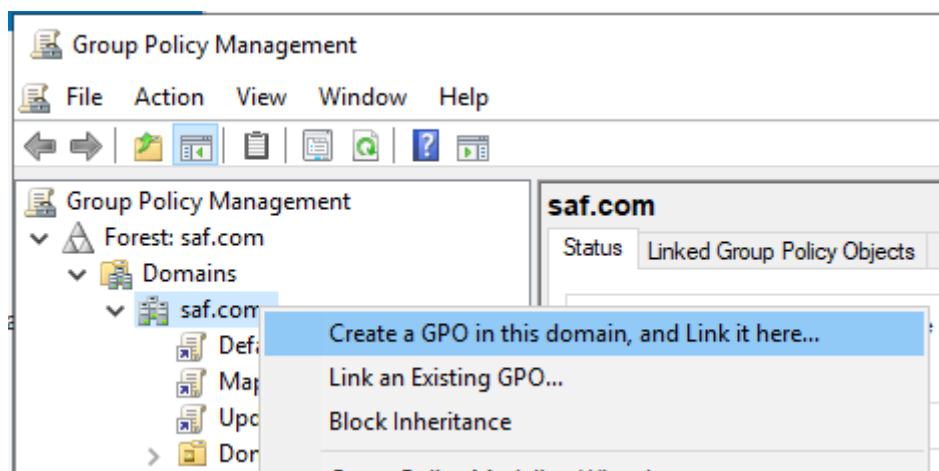
The rest of the installation mostly does itself.

4 - FIREFOX AS DEFAULT BROWSER

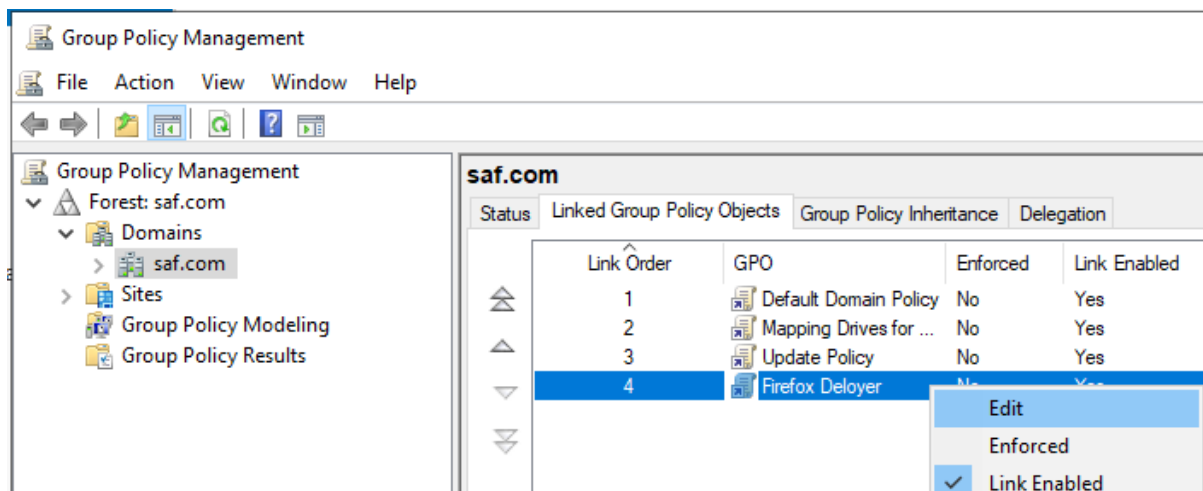
To conform to SAF's decision to move away from Internet Explorer we can deploy Firefox to all the computers in the domain. This is done via Group Policy Management.



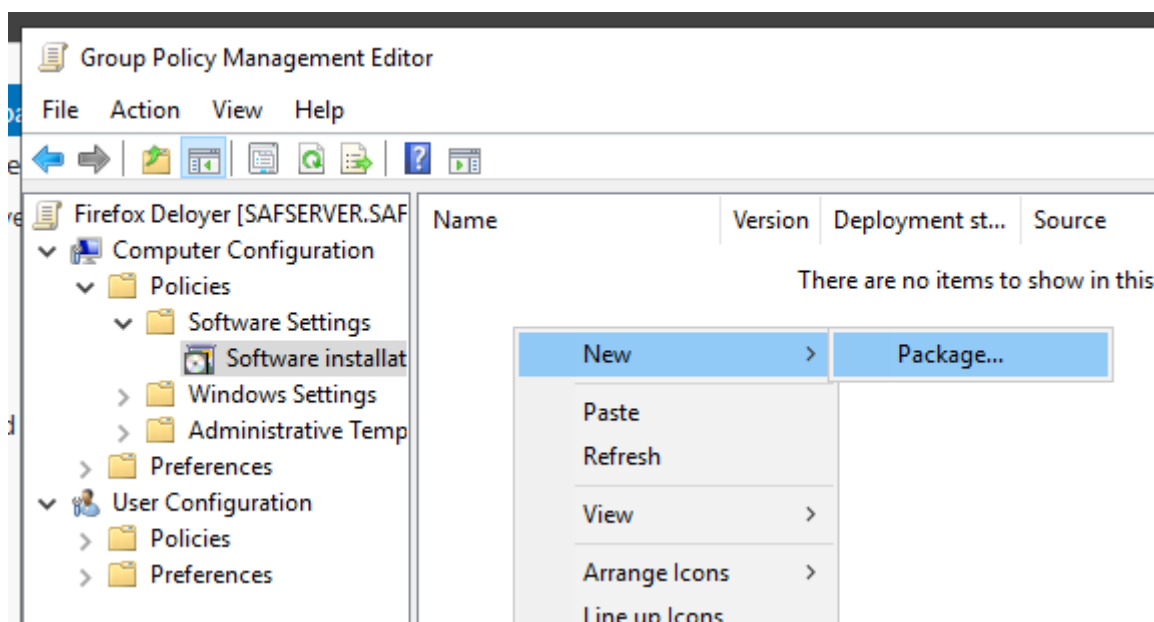
Firstly we download the latest Firefox msi installer from www.mozilla.org and save it to a shared folder on the C:\ drive so computers joining the domain can access it.



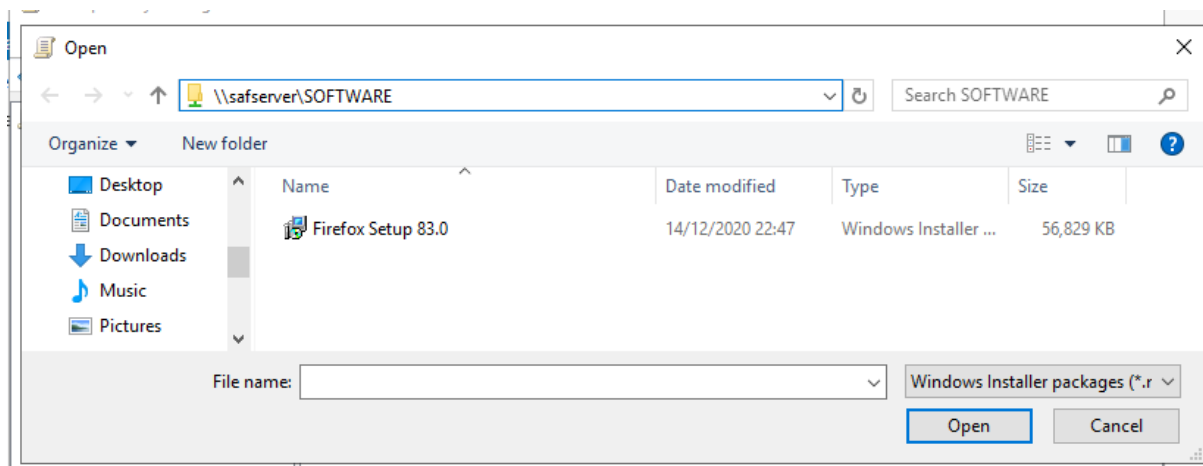
Select "Group Policy Management" from Tools in the main Server Management window. Right click on the saf.com domain and select "Create a GPO in this domain, and Link it here...". From here we give the policy an appropriate name and click OK.



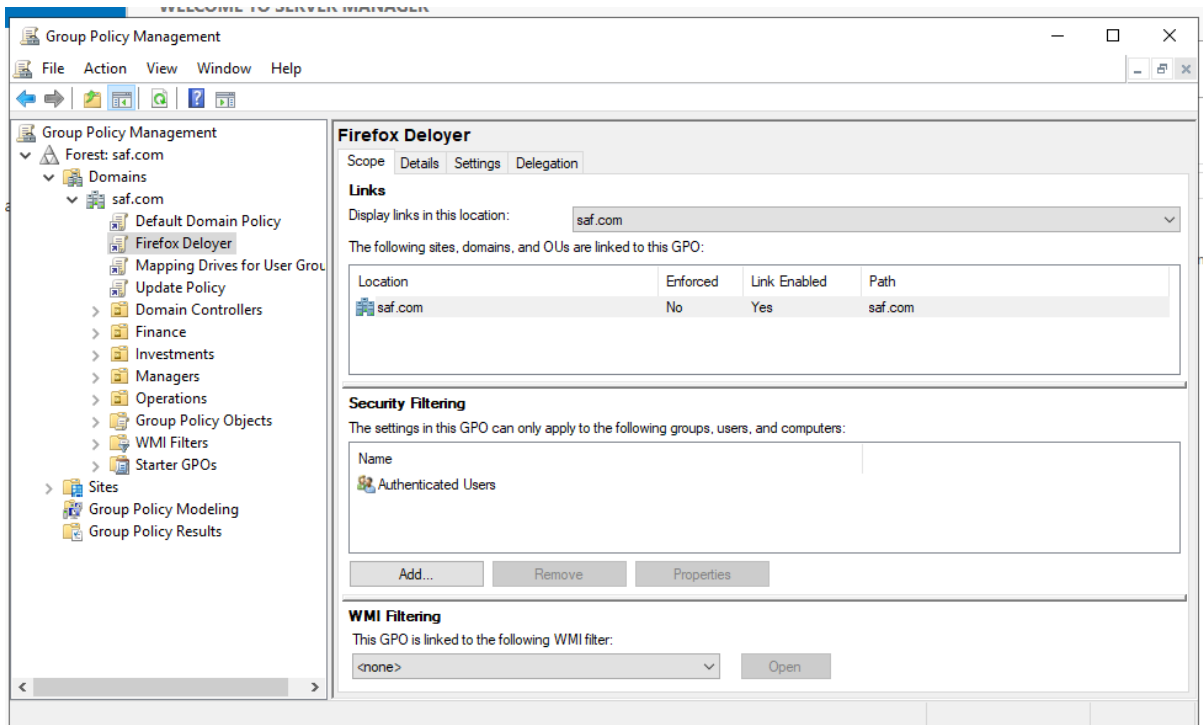
Right click the new GPO and click Edit



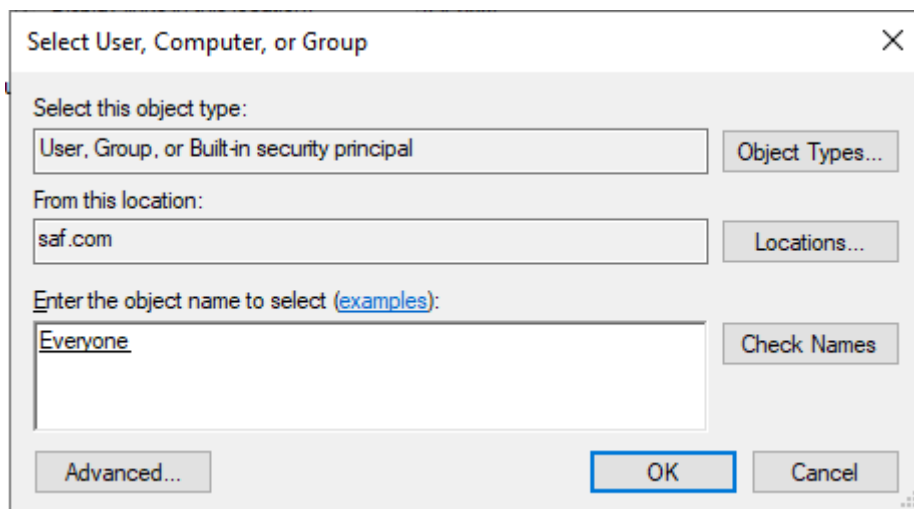
Navigate to Computer Configuration, Policies, Software Settings, Software Installation and right click the empty space in the panel. From the menu choose New, Package...



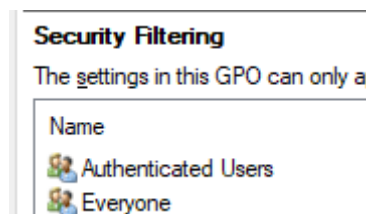
Navigate to the shared folder on the network and select the setup msi. Select it as "assigned"



Returning to the Group Policy Management, double click the “Firefox Deployer” GPO and click “Add...” at the bottom of the Security Filtering section



Type “Everyone” in and click OK to target every user in the domain with this policy.

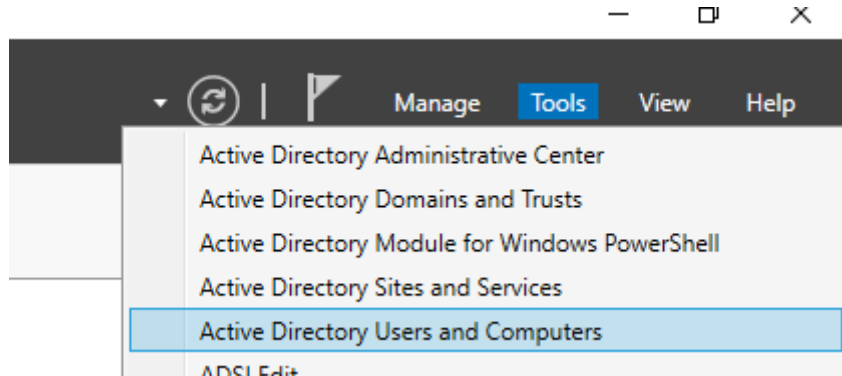


Now everyone will get Firefox!

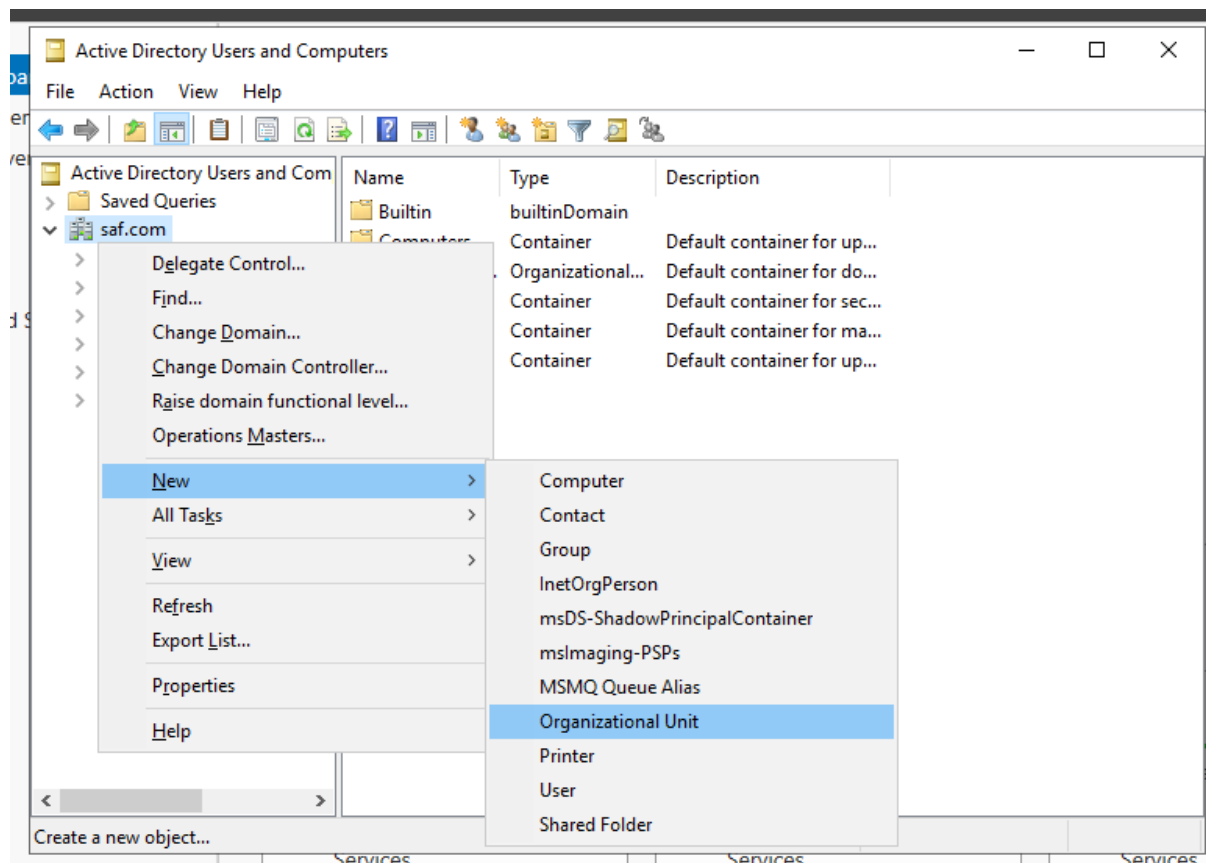
5 - ORGANISATIONAL UNITS

Organisational units help keep things... organised.

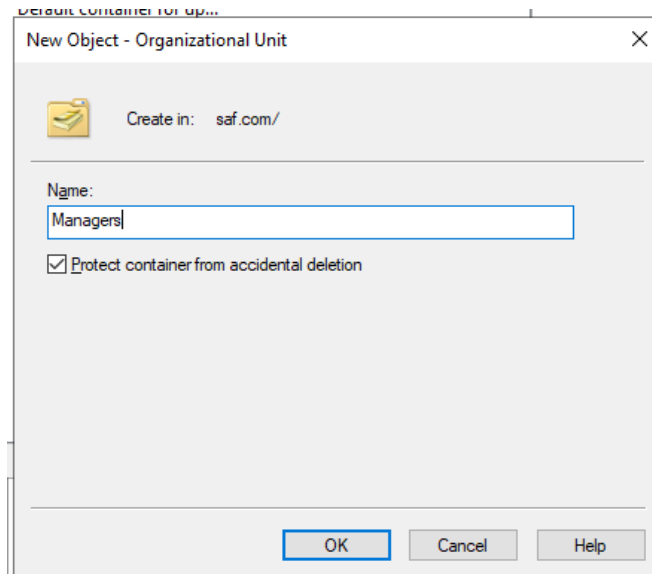
5.1 - Creating OUs



From the Tools menu at the top right hand side of the Server Manager window select “Active Directory Users and Computers”



Right click on the domain and select “New” then “Organisational Unit” (spelling corrected as Windows Server 2019 does not have an English UK language option. Typical.)



Type in the name of the Organisational Unit ("Managers" in this example) and click OK. Repeat thrice for "Investments", "Finance" and "Operations".

Name	Type	Description
Builtin	builtinDomain	
Computers	Container	Default container for up...
Domain Con...	Organizational...	Default container for do...
ForeignSecu...	Container	Default container for sec...
Managed Se...	Container	Default container for ma...
Users	Container	Default container for up...
Managers	Organizational...	
Investments	Organizational...	
Finance	Organizational...	
Operations	Organizational...	

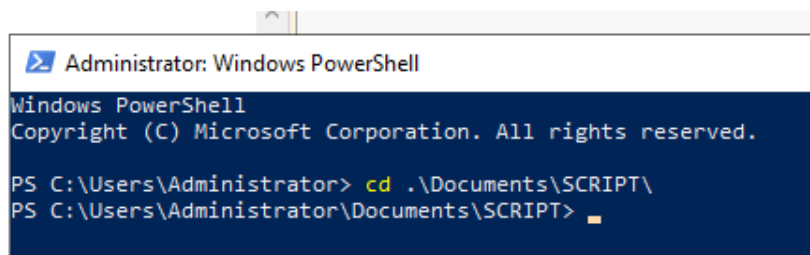
Four organisaitonal units.

5.2 - Creating Demo Users

For demonstration purposes we will create some dummy user accounts. Rather than going through the Active Directory Computers and Users wizard we can do this in the Powershell command line. To optimise/automate this we can use Powershell scripts.

```
# finance
for ($num = 1 ; $num -le 3 ; $num++)
{
$username = ("fUser"+$num)
$userpw = ("fUserPW="+$num)
$userdisp = ("fUser Number "+$num)
$usersam = ("fUserNo"+$num)
New-ADUser `
  -Name $username `
  -Path "OU=Finance,DC=saf,DC=com" `
  -SamAccountName $usersam `
  -DisplayName "User One" `
  -AccountPassword (ConvertTo-SecureString ($userpw) -AsPlainText -Force) `
  -ChangePasswordAtLogon $true `
  -Enabled $true
}
```

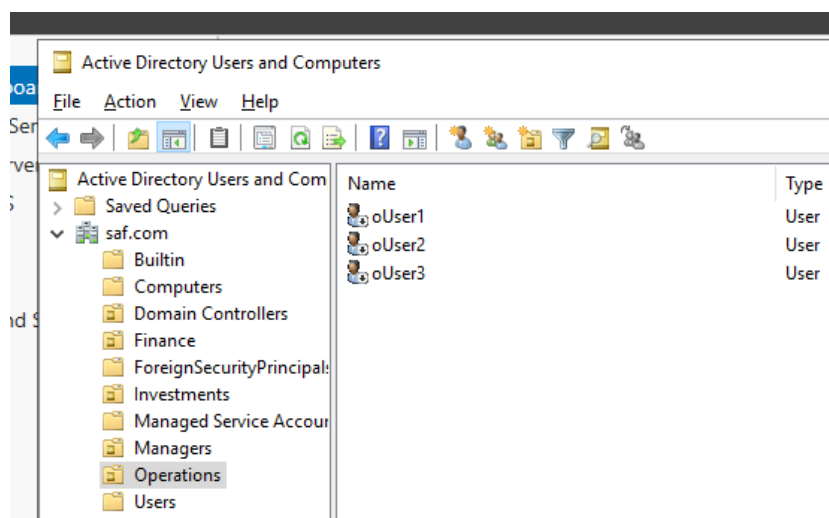
The above script will loop three times. With each loop, \$num increases in value by 1. This variable (\$num) is used in variables such as \$username, to alter them with each run of the loop. This means we will get fUser1, fUser2 and fUser3 as the usernames. The same selection of code is then repeated 4 times per loop (for Management, Investments, Finance and Operations) altering the variables (fUser, mUser, iUser etc.).



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

PS C:\Users\Administrator> cd .\Documents\SCRIPT\
PS C:\Users\Administrator\Documents\SCRIPT>
```

Using Powershell, we can navigate to the directory where the script is stored. From here we run the script by typing in its name.

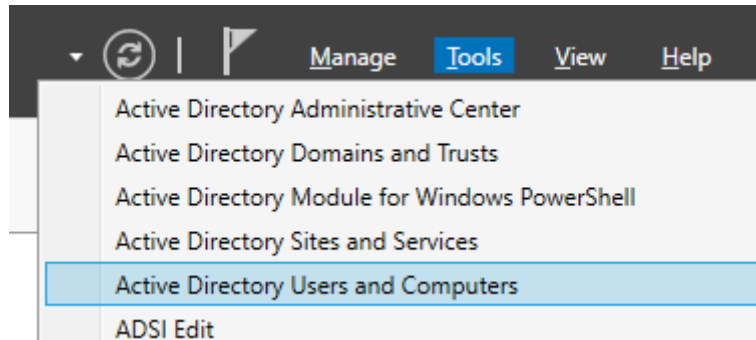


After it has run we now have three demo users in each OU!

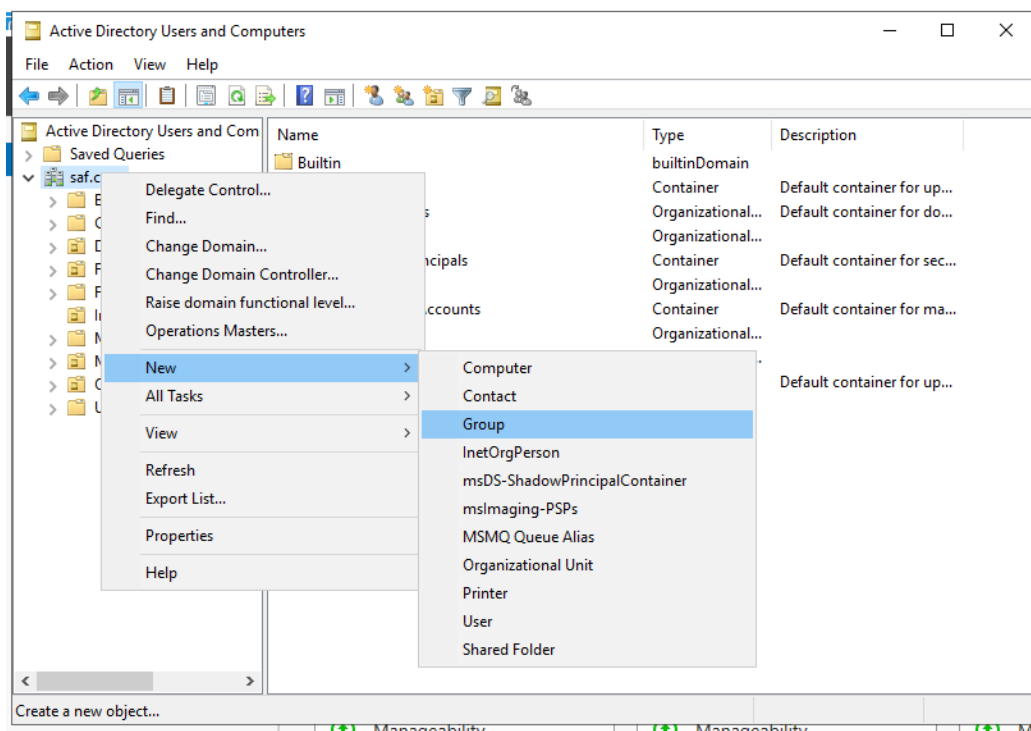
6 - SECURITY GROUPS

To manage shared drives and access permissions for individual groups of users we can use Security Groups. Changing group policy objects with these Security Groups allows us to control the shared drives.

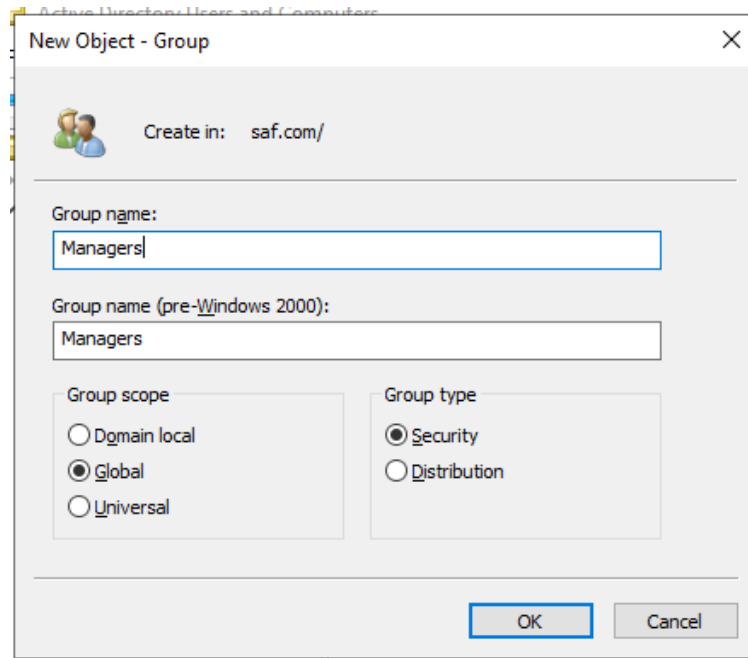
6.1 - Creating the Security Groups



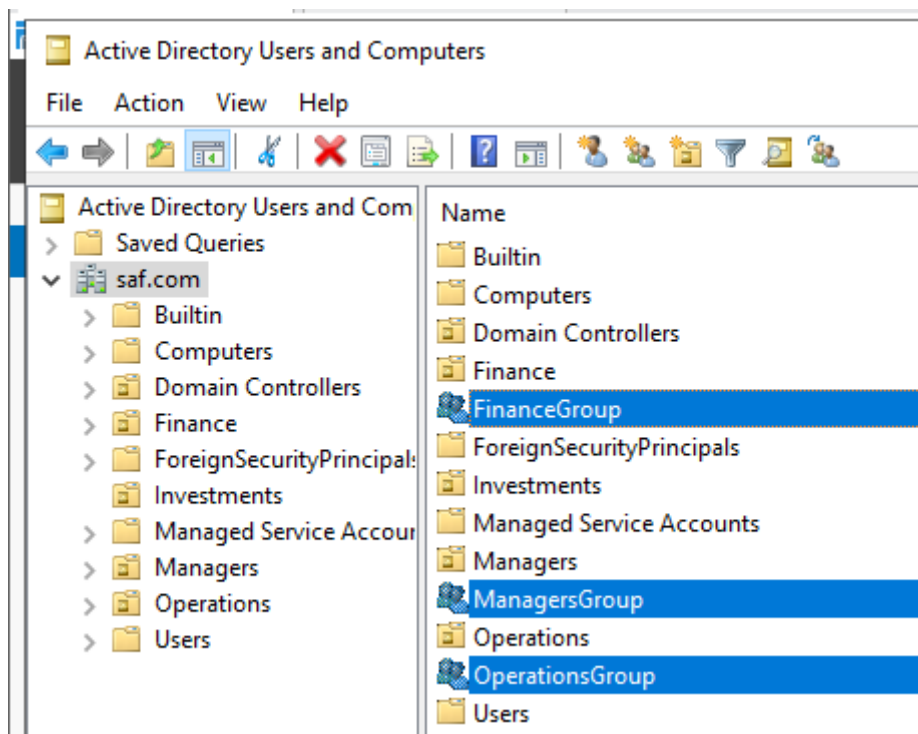
Select "Active Directory Users and Computers" from the Tools menu



From here, right click on the domain (saf.com) and select new group

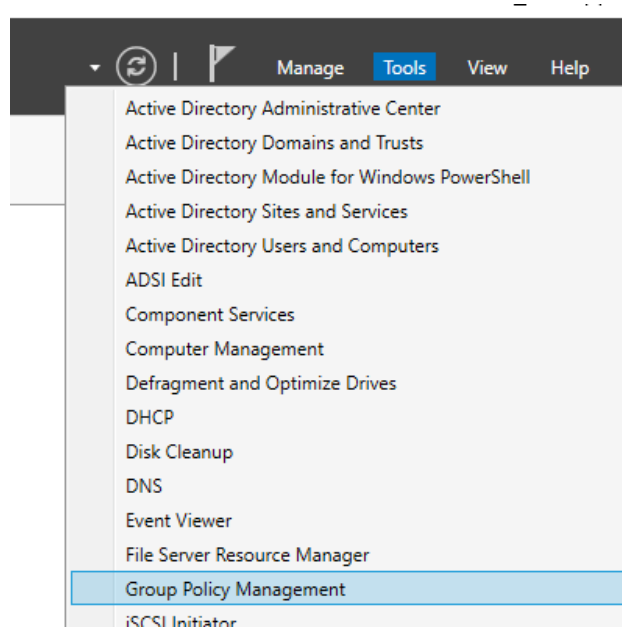


Type in the name and select the group type as “Security”, repeat for all required groups.

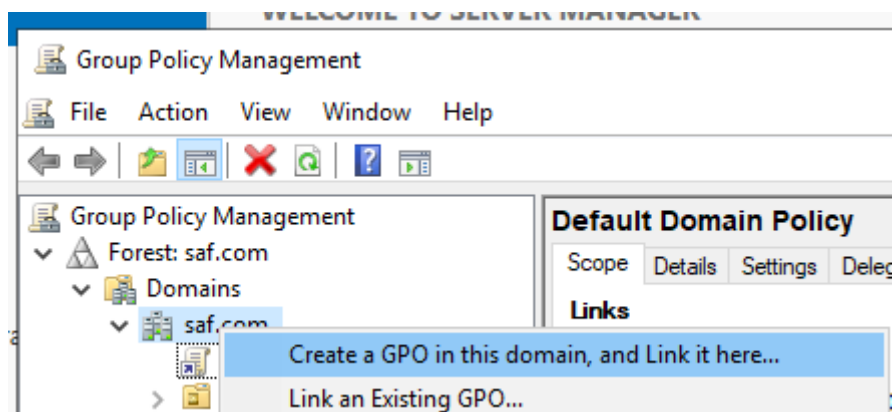


The three Security Groups in the domain

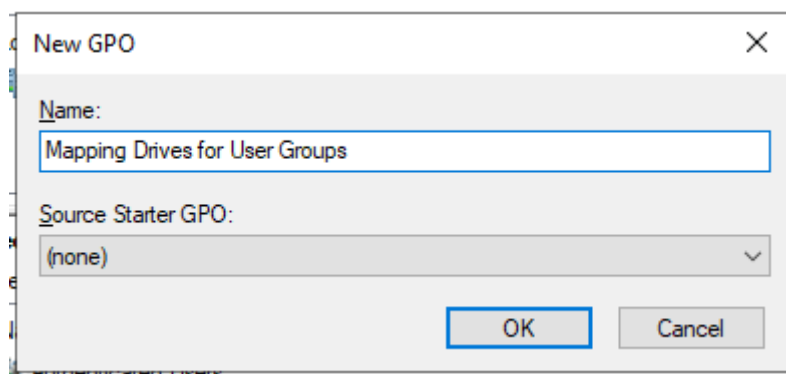
6.2 - Shared Drives



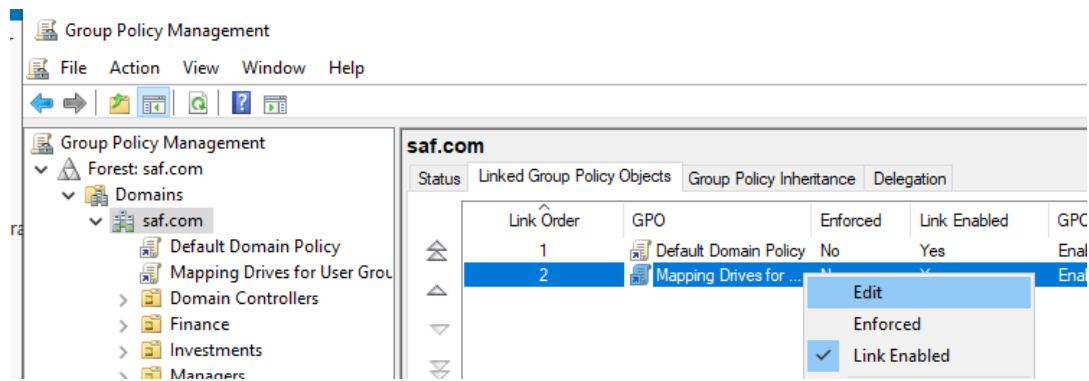
Select "Group Policy Management" from Tools



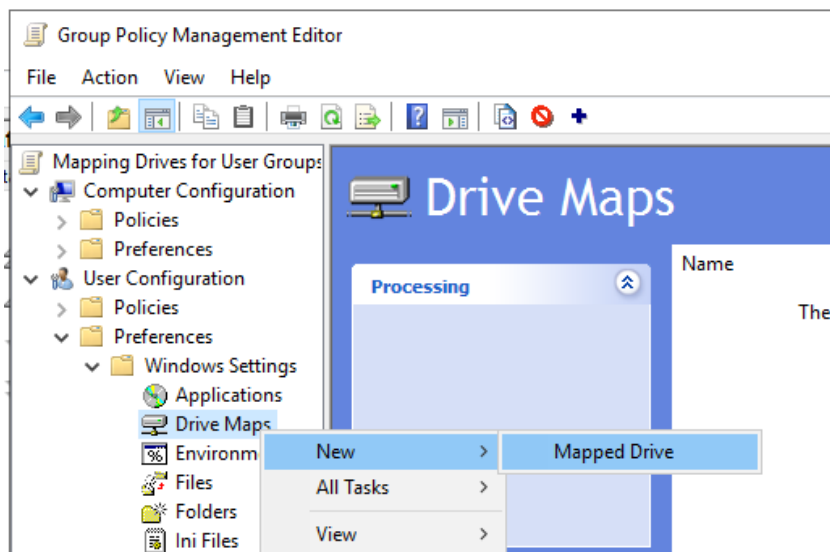
Right click the saf.com domain and select "Create a GPO in this domain, and Link it here..."



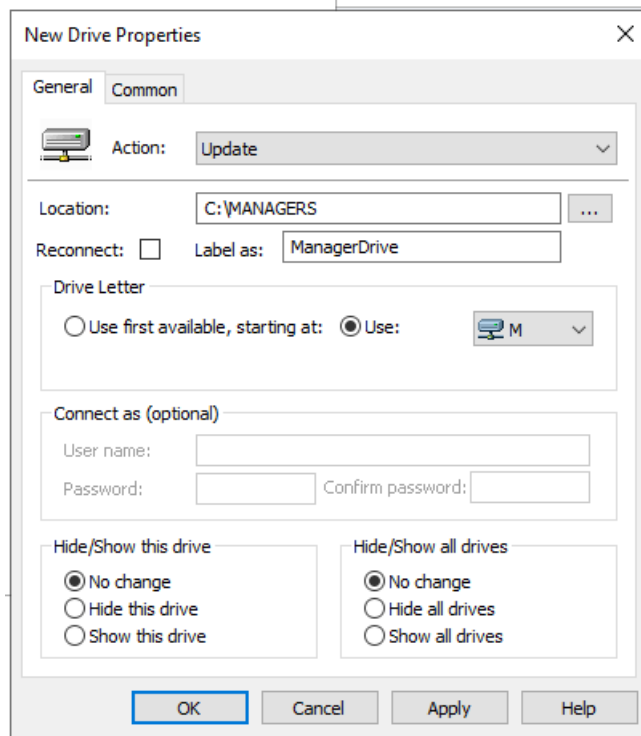
Give the GPO a name and click OK



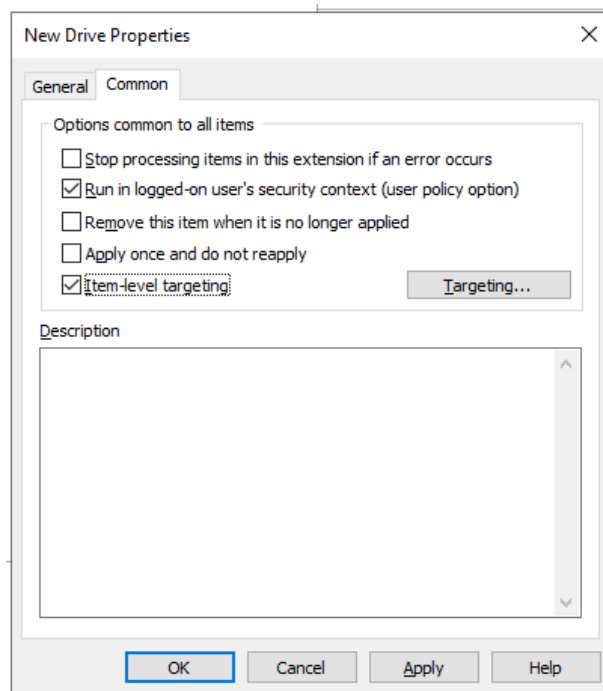
Right click on the newly created GPO and click edit



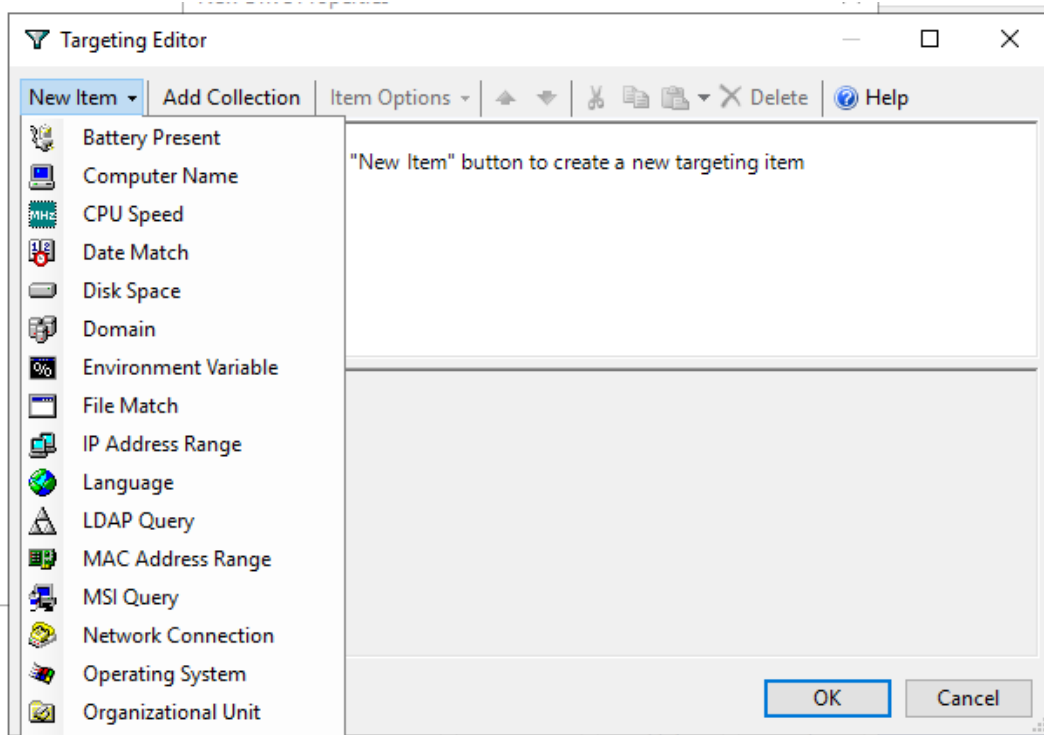
Expand the tree as shown above, right click on Drive Maps and select New Mapped Drive



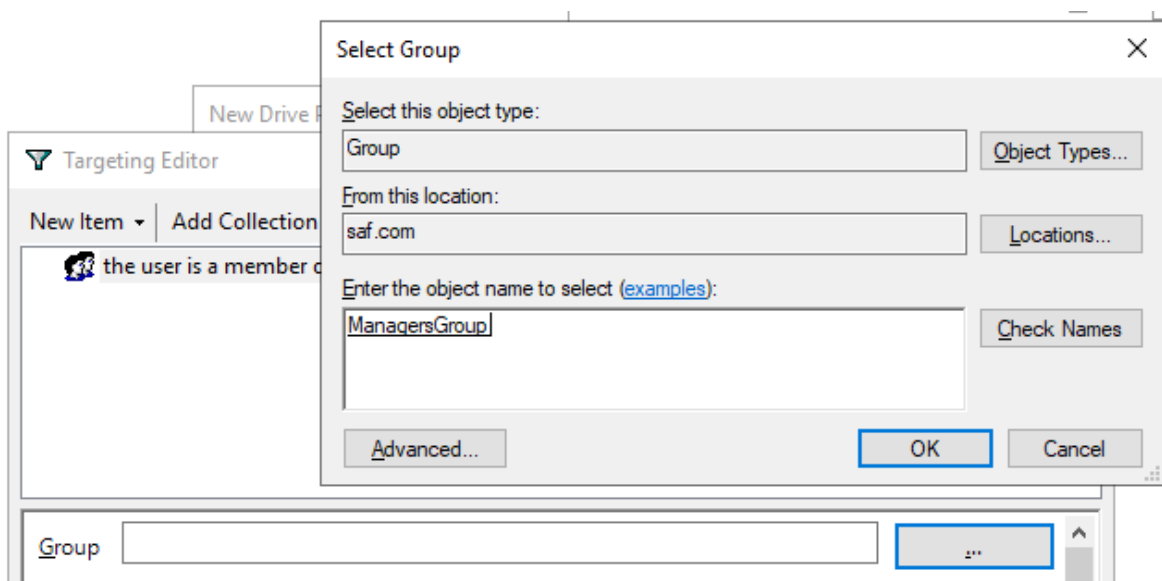
Select the location of the folder to set up as the new drive and give it an appropriate letter (M for managers in this case!)



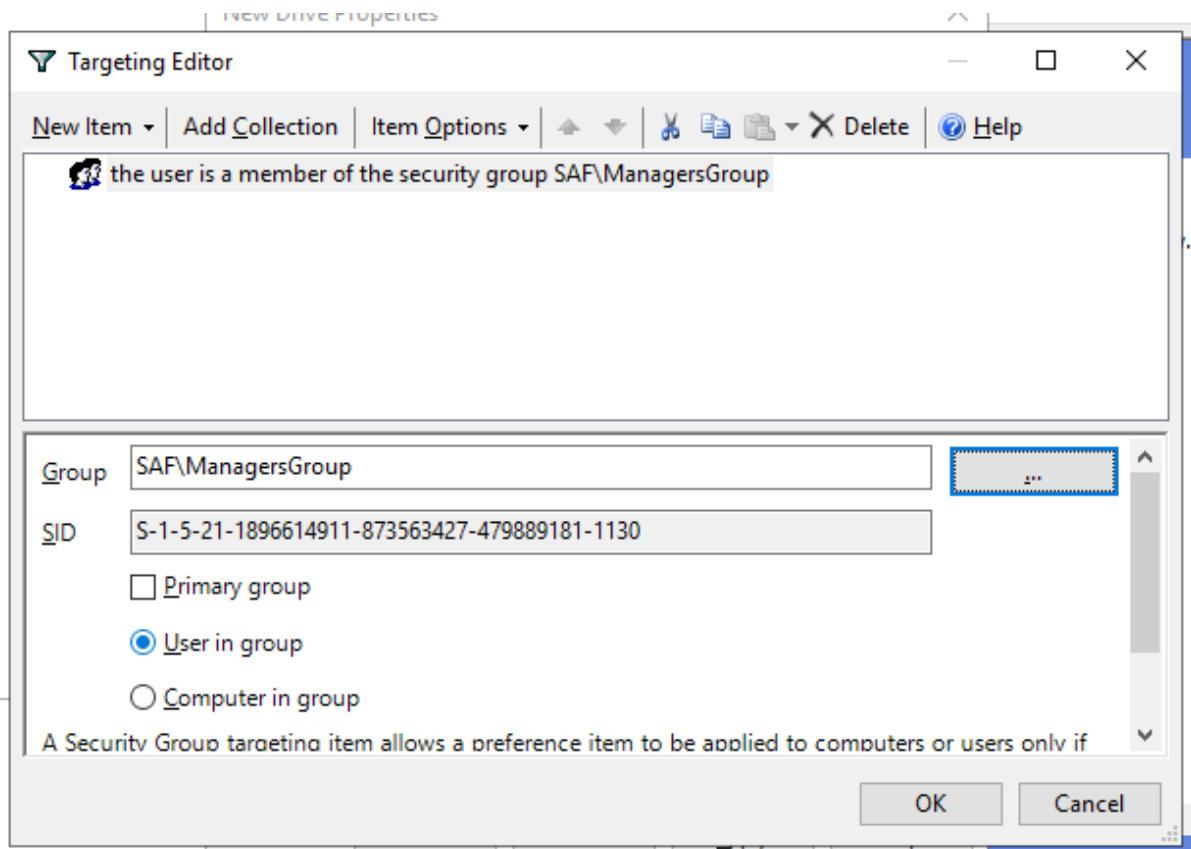
Click on the "Common" tab and select "Run in logged-on user's security context" and "Item-level targeting". Then click on the Targeting button.



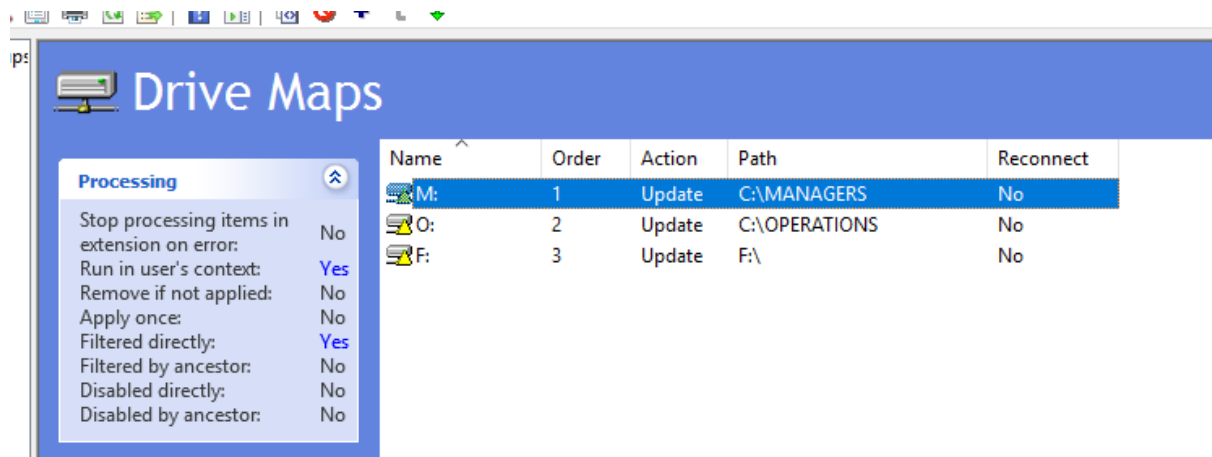
Click "New Item" then select "Security Group" A



Click the ellipses button to start looking for a group. Type in "managers" and click "Check Names" to select the ManagersGroup, then click OK.

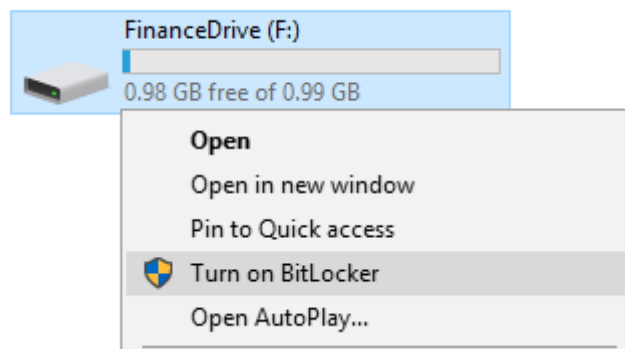


Check all the details are correct and click OK to set the mapped drive to be available for the ManagersGroup. Then click Apply on the New Drive Properties window.



Repeat the process for the FinanceGroup (using a different volume) and the OperationsGroup (but make the drive available to both OperationsGroup and ManagersGroup, select “OR” for the ManagersGroup by clicking on them and pressing F6). The finished Drive Maps window should look like above.

6.2 - BitLocker Encryption



Right click on the hard drive in This PC and select “Turn on BitLocker”

← BitLocker Drive Encryption (F:)

Choose how you want to unlock this drive

Use a password to unlock the drive

Passwords should contain uppercase and lowercase letters, numbers, spaces, and symbols.

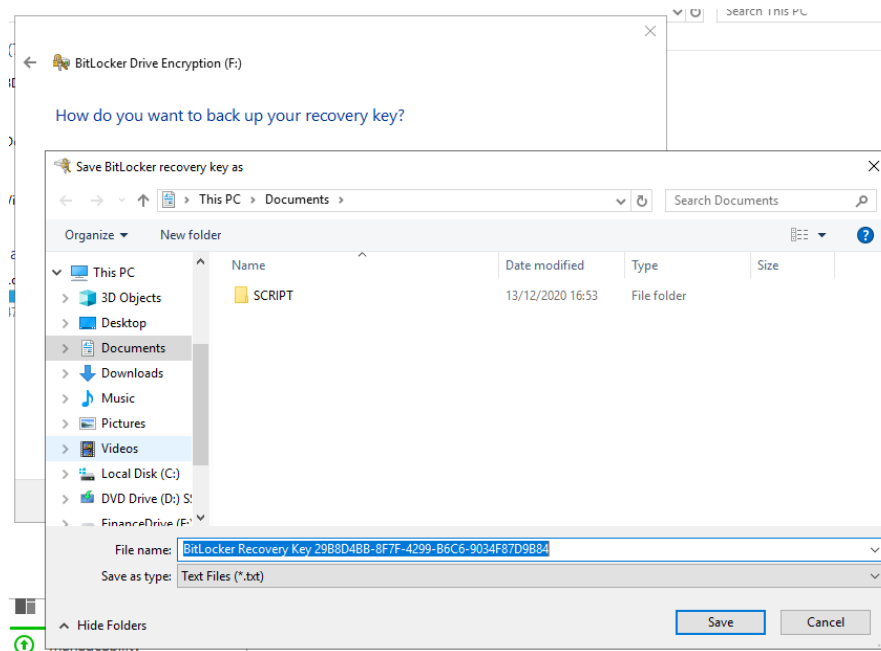
Enter your password

Reenter your password

Use my smart card to unlock the drive

You'll need to insert your smart card. The smart card PIN will be required when you unlock the drive.

Enter the password you will use for the drive (in this example we are using “saf!123qwe”).



Save the backup recovery key to a file that can use printer or saved elsewhere.

← BitLocker Drive Encryption (F:)

Choose how much of your drive to encrypt

If you're setting up BitLocker on a new drive or a new PC, you only need to encrypt the part of the drive that's currently being used. BitLocker encrypts new data automatically as you add it.

If you're enabling BitLocker on a PC or drive that's already in use, consider encrypting the entire drive. Encrypting the entire drive ensures that all data is protected—even data that you deleted but that might still contain retrievable info.

- Encrypt used disk space only (faster and best for new PCs and drives)
- Encrypt entire drive (slower but best for PCs and drives already in use)

For security we will encrypt the entire drive.

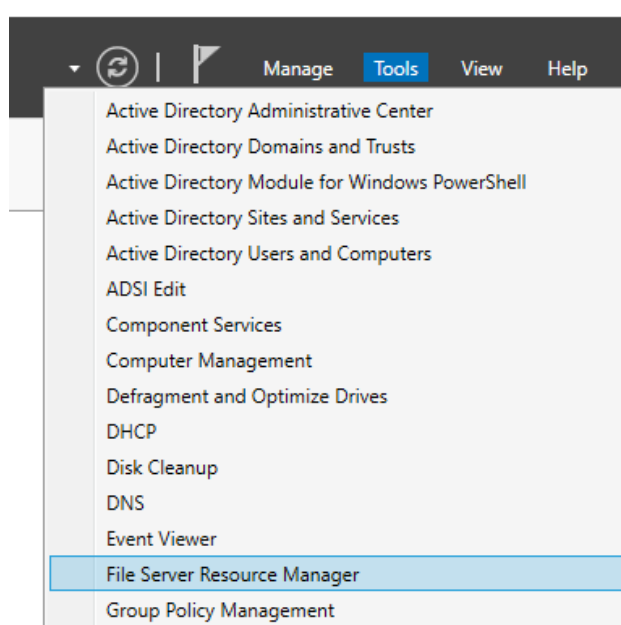


Select compatible mode just in case the drive is used in other devices and click next then OK to start encrypting the drive with BitLocker.

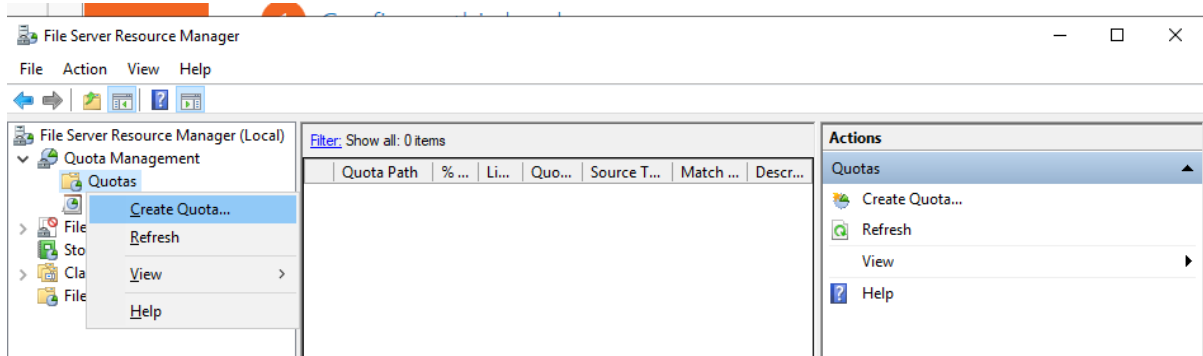
7 - HARD QUOTAS FOR STORAGE

We can prevent users filling up our available storage by implementing hard data quotas. For demonstration purposes in this document we will be setting up a 100Mb data limit.

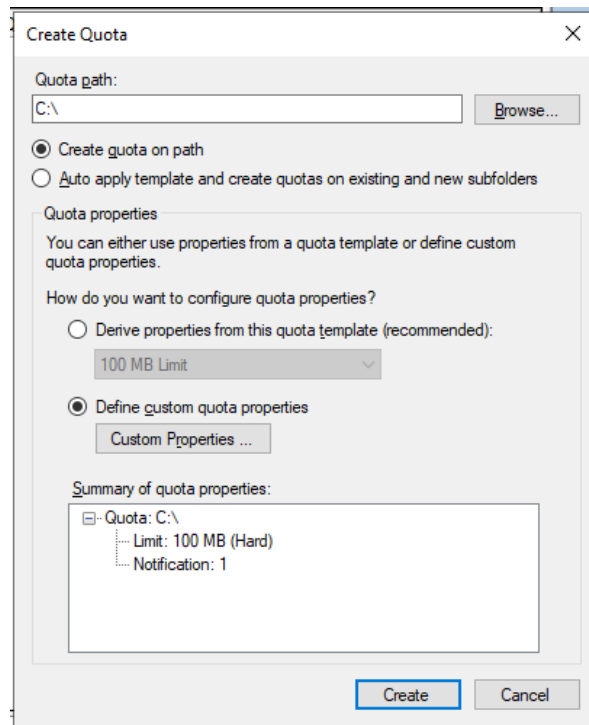
7.1 - Creating the Security Groups



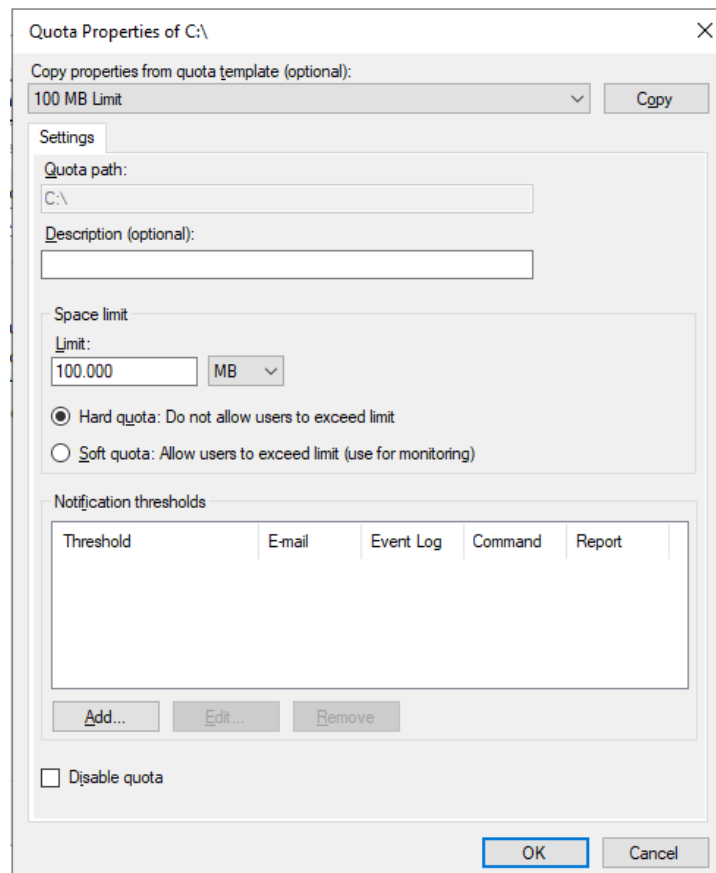
Begin by selecting "File Server Resource Manager" from the Tools menu in Server Manager



In the FSRM window, expand "Quota Management" and right click on Quotas. Select "Create Quota..." to open the Create Quota window.



Select the directory to apply the quota to. In our case it will be the entirety of the C: drive. Whilst there is the option to use the pre-existing 100Mb template we will define a custom quota to demonstrate that the values can be changed as our needs scale.



From here enter the quota limit, description, hard/soft setting and then click “Add...” to start adding the thresholds.

The screenshot shows the 'Add Threshold' dialog box with the following configuration:

- Generate notifications when usage reaches (%): 85
- Tab: Email Message
- Send e-mail to the following administrators:
 - [Admin Email]
 - Format: account@domain. Use semicolons to separate accounts.
- Send e-mail to the user who exceeded the threshold
- E-mail message:
 - Type the text to use for the Subject line and message.
 - To identify the quota, limit, usage, or other information about the current threshold, you can use Insert Variable to insert a variable in your text.
 - Subject: You have used too much data!
 - Message body: Listen here, [Source to Owner]. You're only allowed [Quota Limit MB] and you're at [Quota Used Percent]% of that. Stop it. [Quota Used MB] MB is a lot. If you go over I will fire you.
 - Select variable to insert: [Admin Email] (dropdown)
 - Insert Variable button
 - Inserts the e-mail addresses of the administrators who receive the e-mail.
- Additional E-mail Headers... button
- OK and Cancel buttons

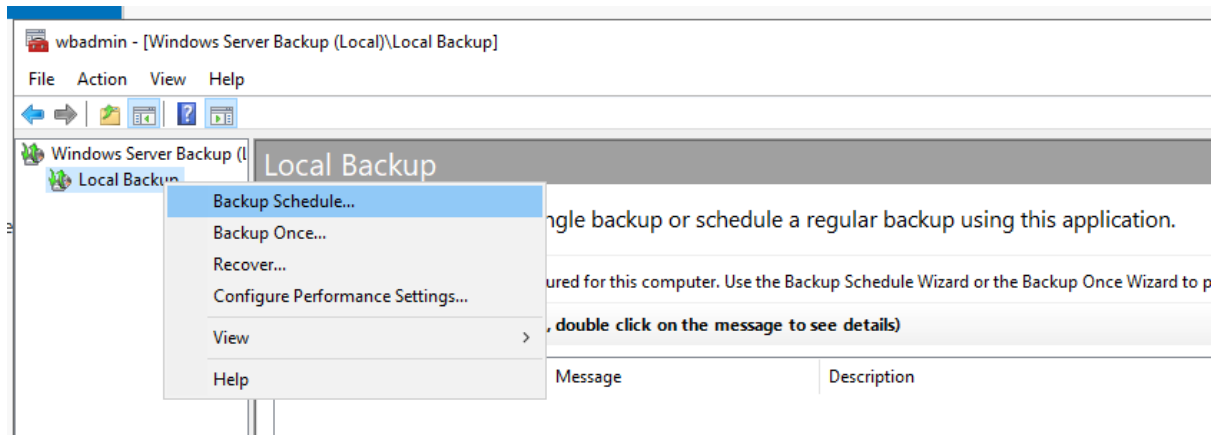
In this window we set the threshold level for a warning at 85%. We can send an email to the user who has transgressed the threshold to warn them about their usage. The other tabs along the top give other options, such as logging the event, running a command, filing a report etc.

After creating a second threshold for 100% usage we simply click "Create" at the bottom of the Create Quota window and the quota is now applied to the specified drive. We are also given the option to save the quota as a template for future usage.

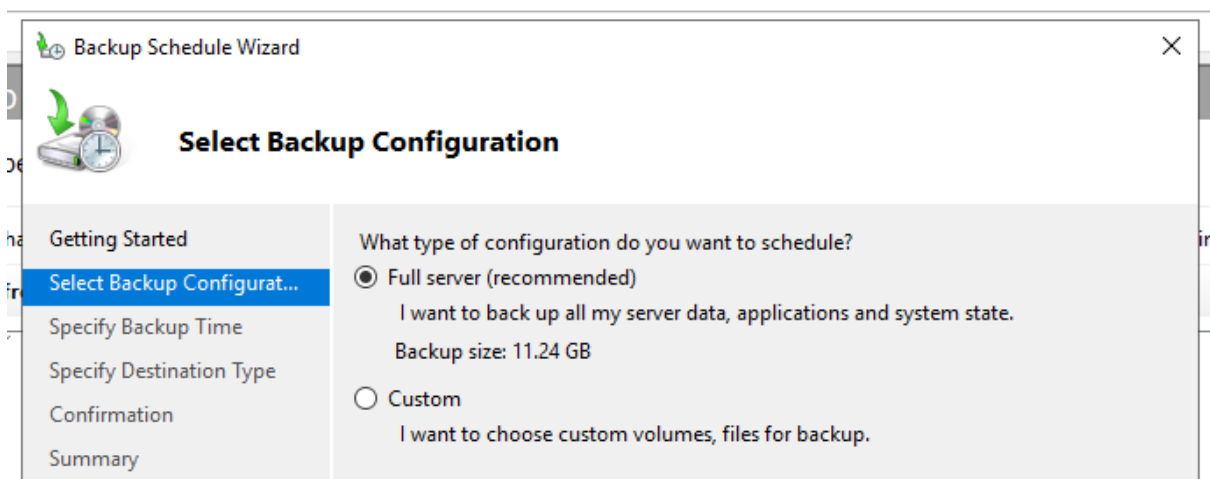
8 - BACKUP & UPDATE POLICY

We are able to schedule backups and updates to happen with the Windows Server Backup tool and Group Policy Objects. The details below will show the steps taken to schedule these at a time when the office will be empty.

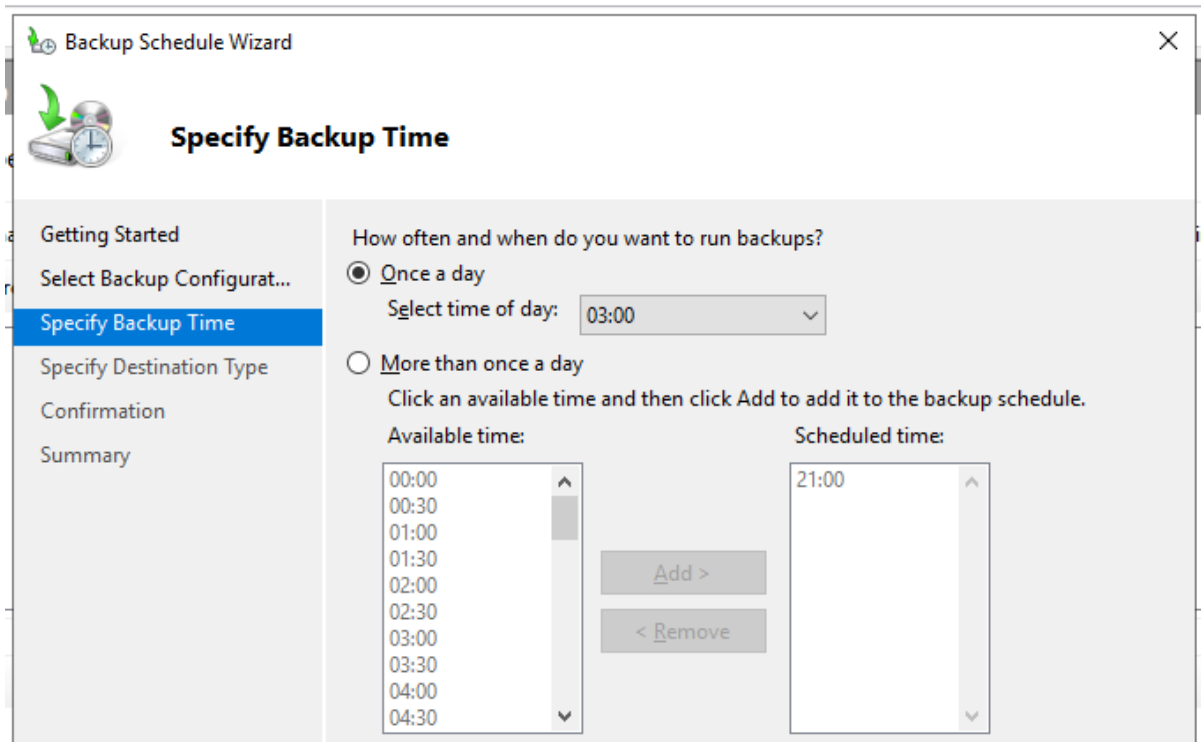
8.1 - Scheduling Backups



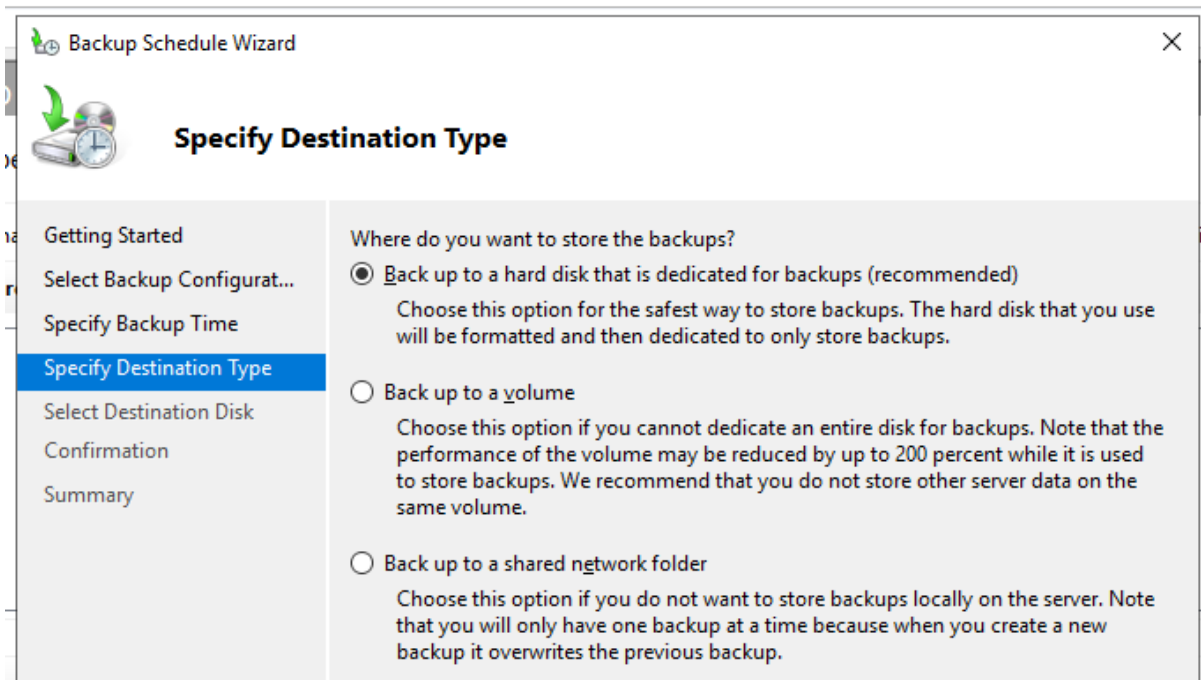
Start by selecting "Windows Server Backup" from the Tools menu in Server Manager. In this new window right click "Local Backup" and select "Backup Schedule..."



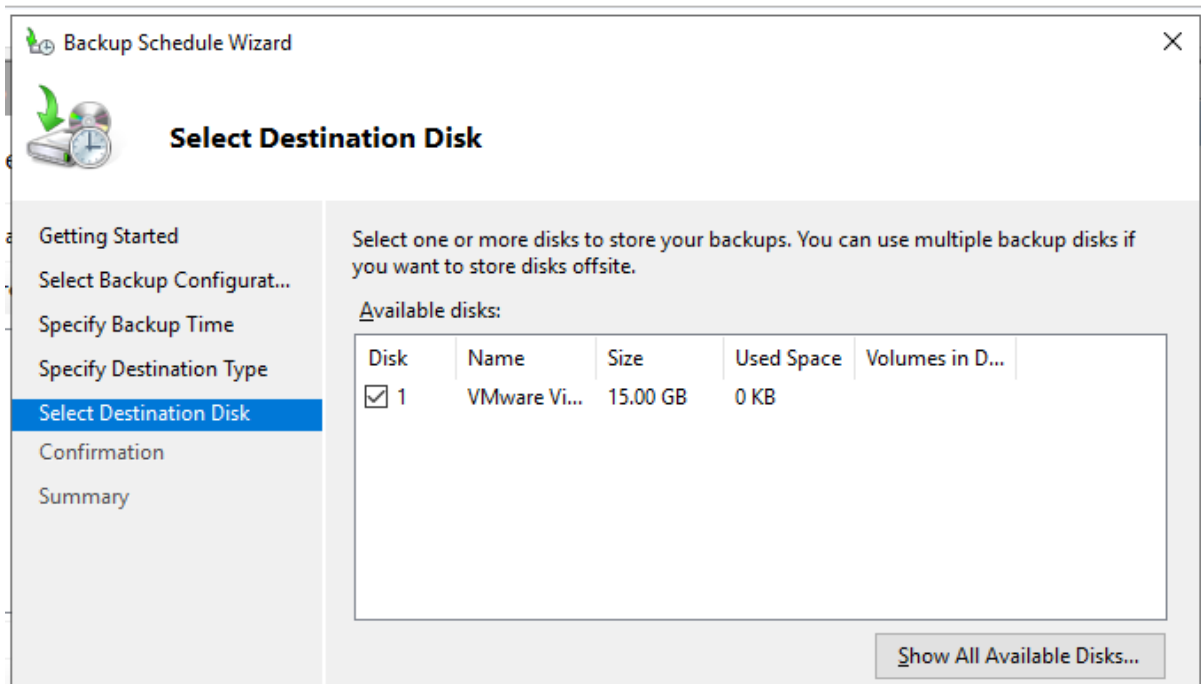
Click Next to start the wizard. For this demonstration we are choosing to do a full server backup, though smaller backups of individual volumes or files can be configured via the same method. Click Next at the bottom of the window to continue



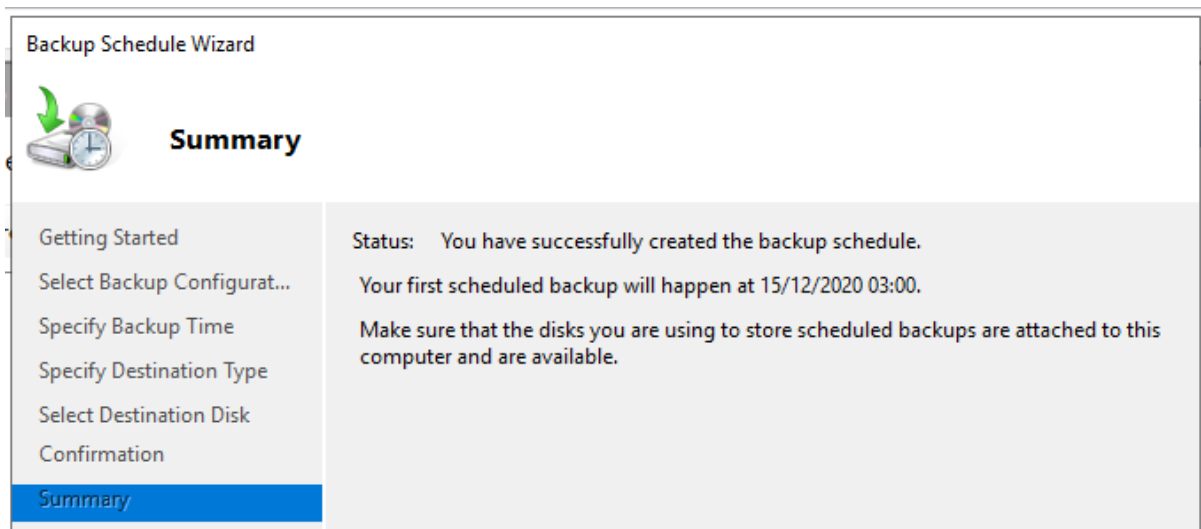
Here we can choose the time for the backup. As no users will be in the office at 3am and the on-call junior admin will be awake, this will be our chosen time.



Again for demonstration purposes we will be choosing to backup to a dedicated backup drive.

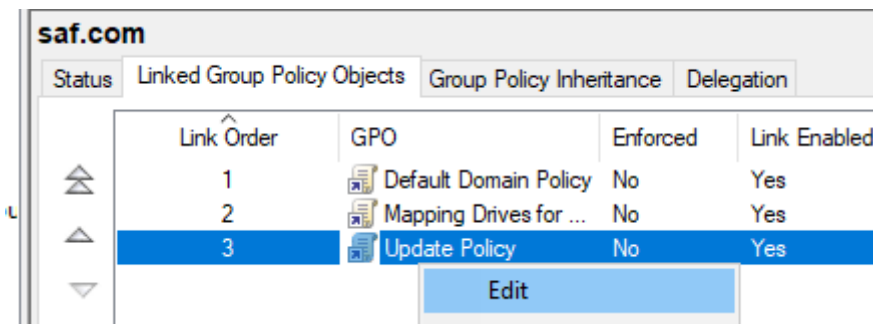


We select the disk we want and click next. A warning will pop up to remind us that the disk used will be formatted, all data on it erased and then used as a dedicated backup disk.

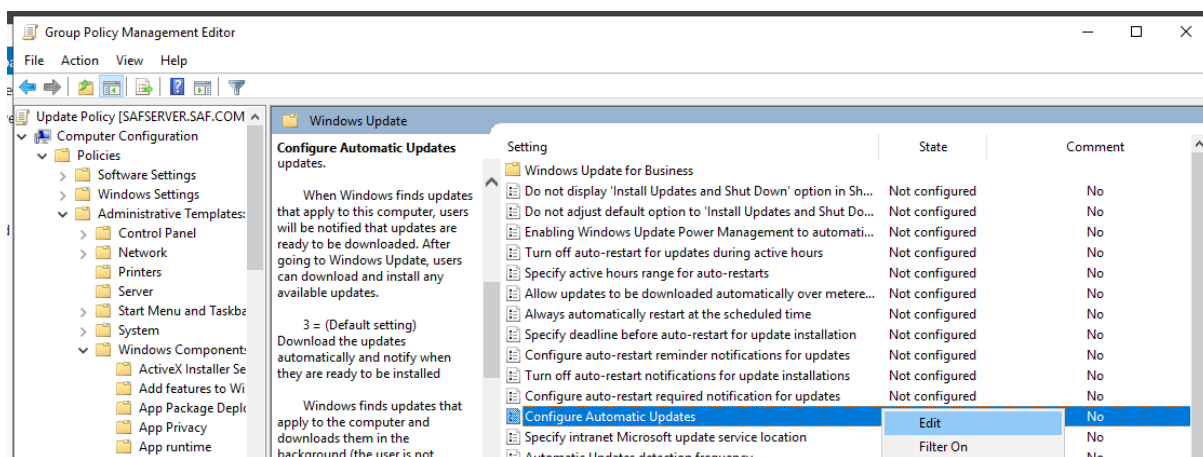


After checking the summary, click Next to schedule the backups. The screen above will confirm that we have backups scheduled and will show the upcoming back up.

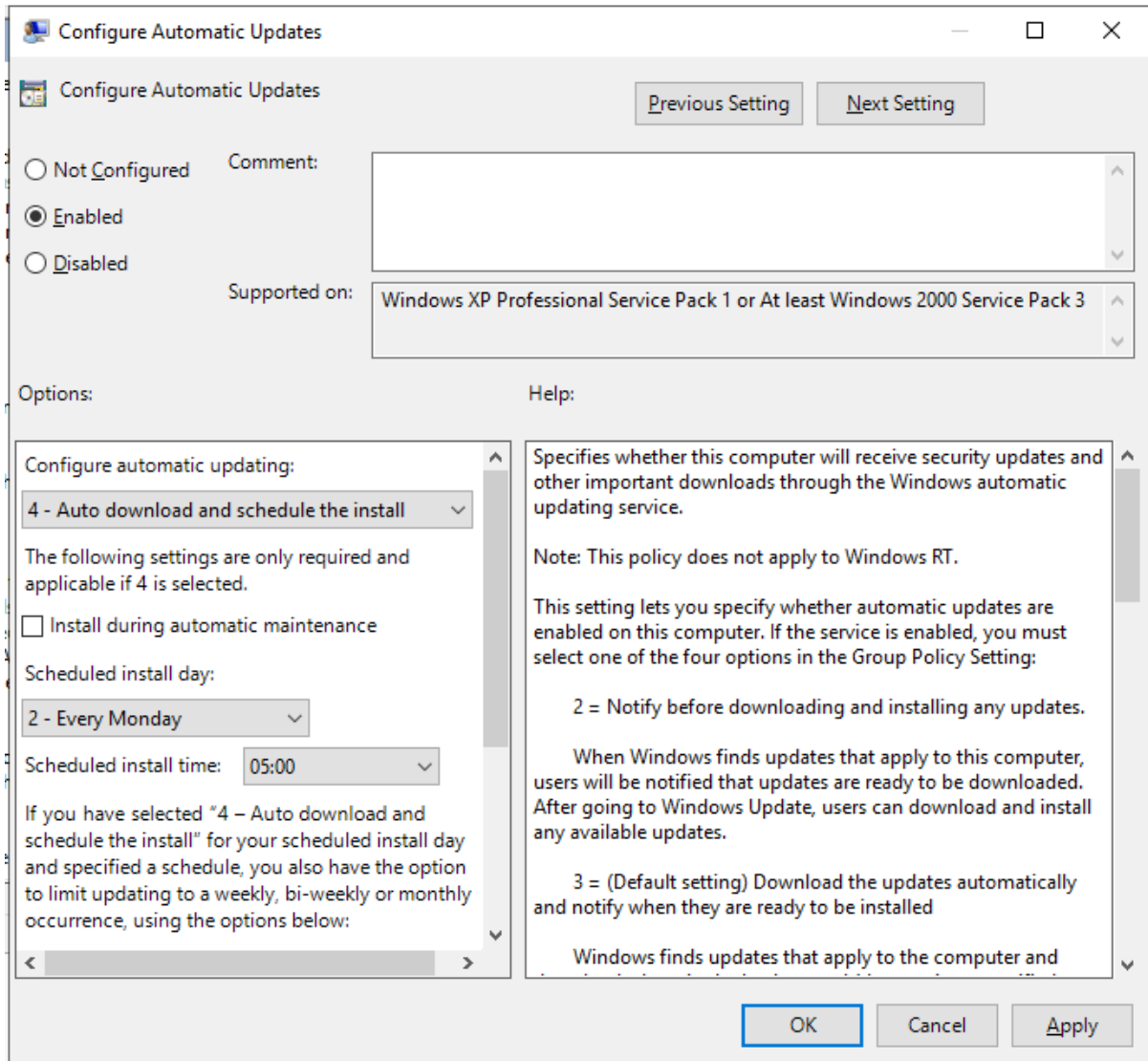
8.2 - Scheduling Updates



Open the Group Policy Manager via the Tools menu again. Right click on the domain, select “Create a GPO in this domain, and Link it here...” and name it. Then right click on the new GPO and select edit.

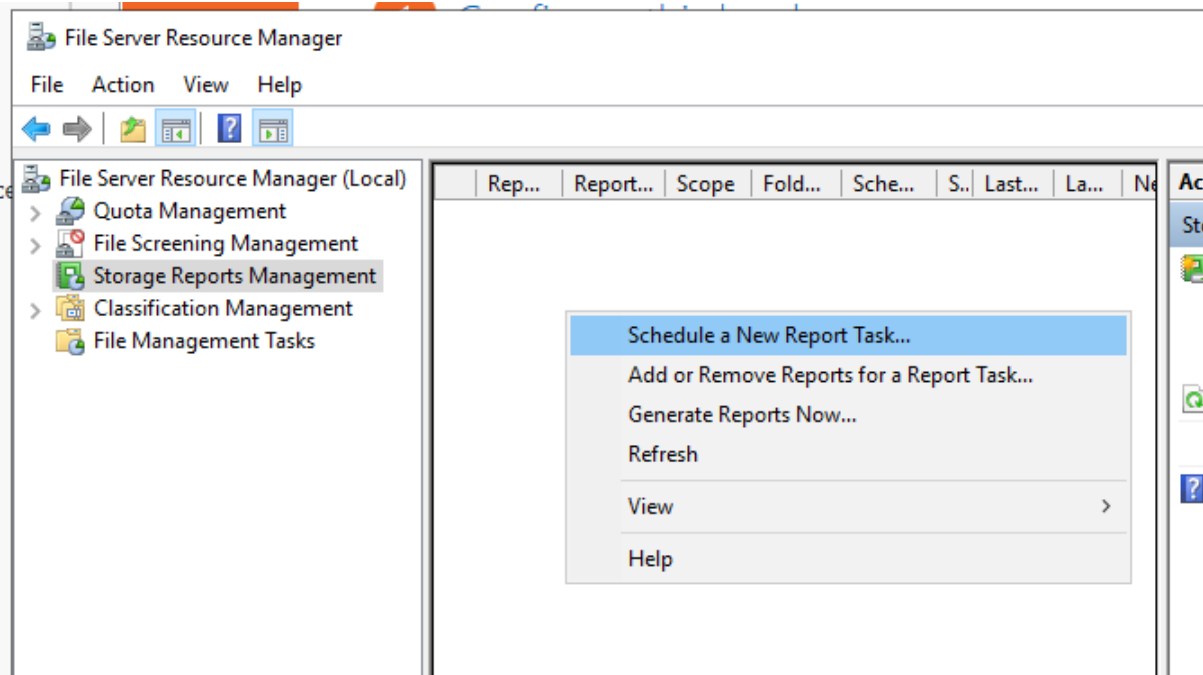


Expand the trees on the left to navigate to Computer Configuration, Policies, Administrative Templates, Windows Components, Windows Updates and left click on it to open the policies in the right hand pane. In here, we right click on “Configure Automatic Updates” and select Edit

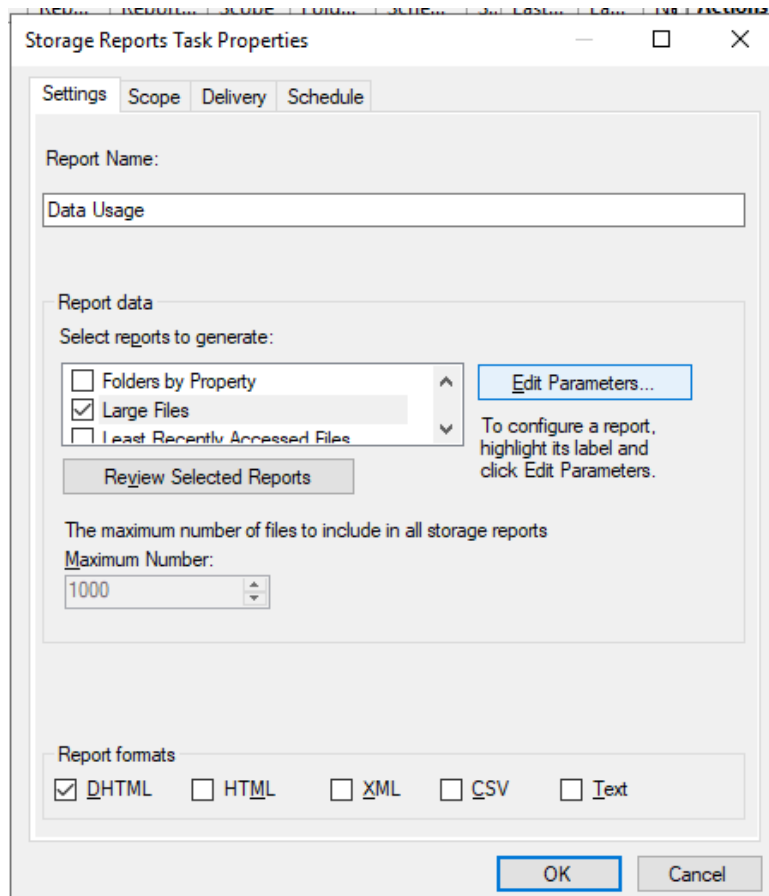


In this window, we first enable the policy by clicking the Enabled radio button, then select “4 - Auto download and schedule the install” from the drop down menu, then schedule it to happen every Monday at 0500 after the backup. To apply these changes we simply click “Apply” then “OK” to close the window.

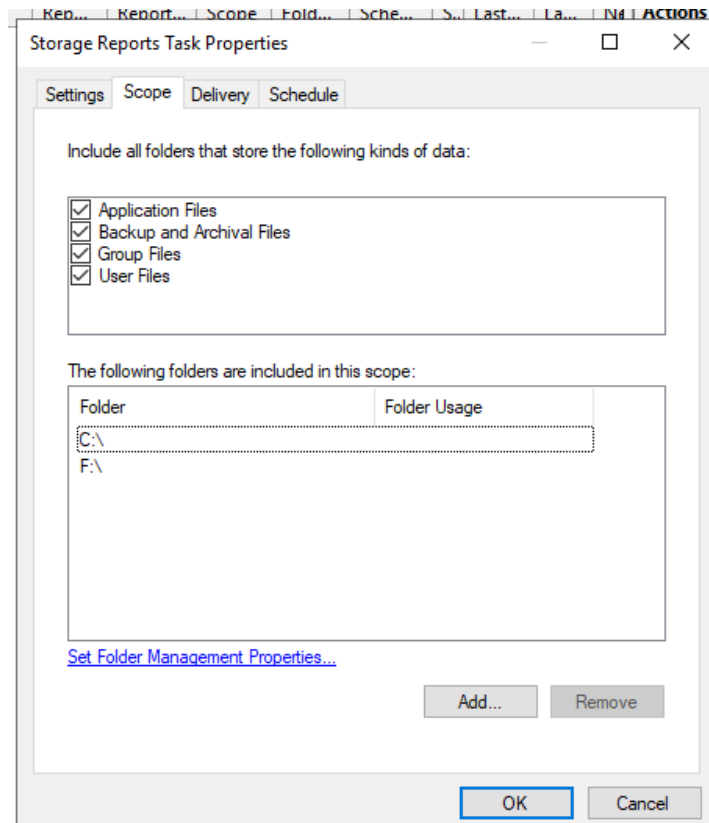
8.3 - Storage Reports



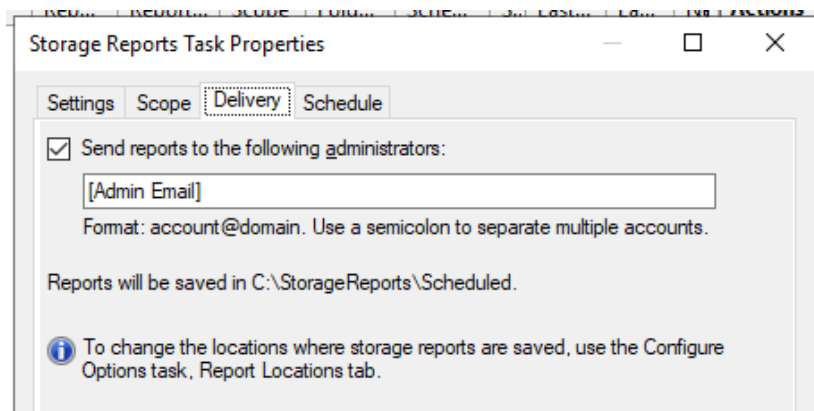
Open up File Server Resource Manager from the Tools menu again. Click “Storage Reports Manager” and then right click in the empty pane and select “Schedule a New Report Task...”



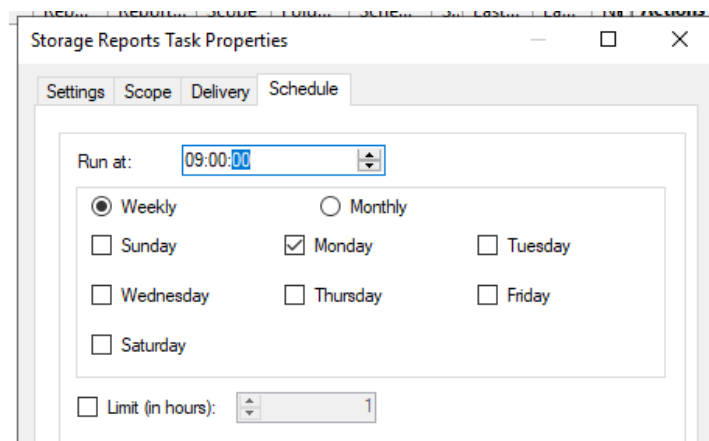
Set the report name, and select the specific reports to generate.



In the Scope tab we'll select all file types and add the two drives to the report. This is just for this demonstration. More articulated scopes can be determined as needed.



Likewise, the email address in the Delivery tab can be altered as needed.

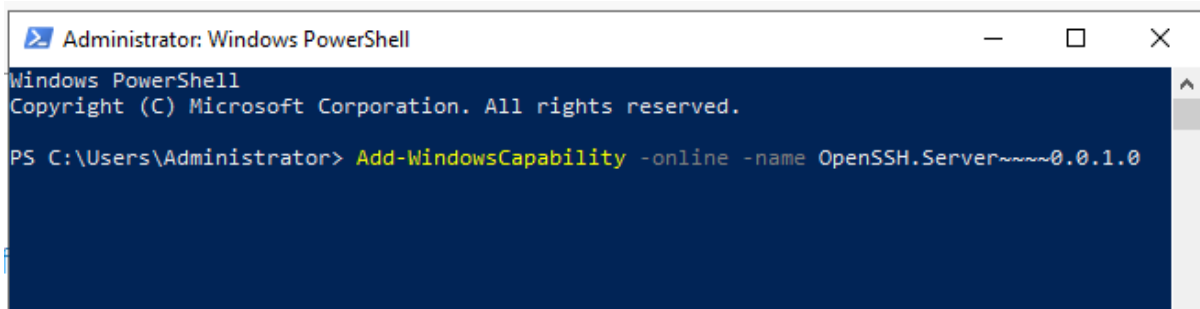


The Schedule tab allows us to have the report sent first thing on Monday morning! Click OK to save

9 - SSH ACCESS FOR OPERATIONS GROUP

The users in the Operations Group will want to be able to access the server remotely via the command line. This is simply done by enabling SSH and configuring it so it will only allow logins from the members of that group. The Managers also wish to have remote access, but they wish to use remote desktop. SSH will not suffice for their needs so we must set up RDP.

9.1 - Setting up SSH Access

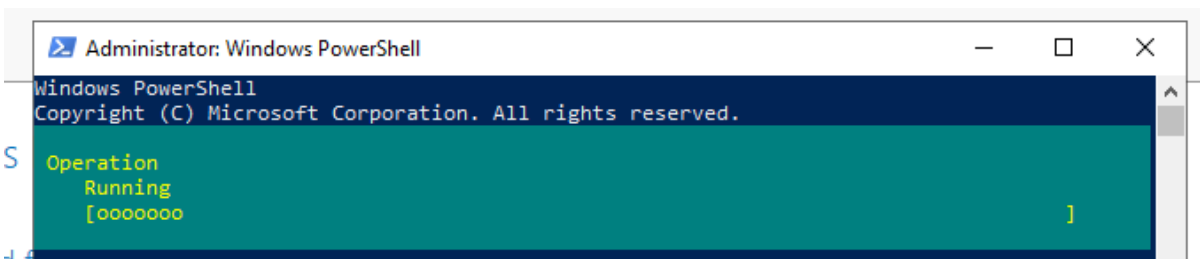


```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> Add-WindowsCapability -online -name OpenSSH.Server~~~~0.0.1.0
```

We begin by opening Powershell and entering the following command:

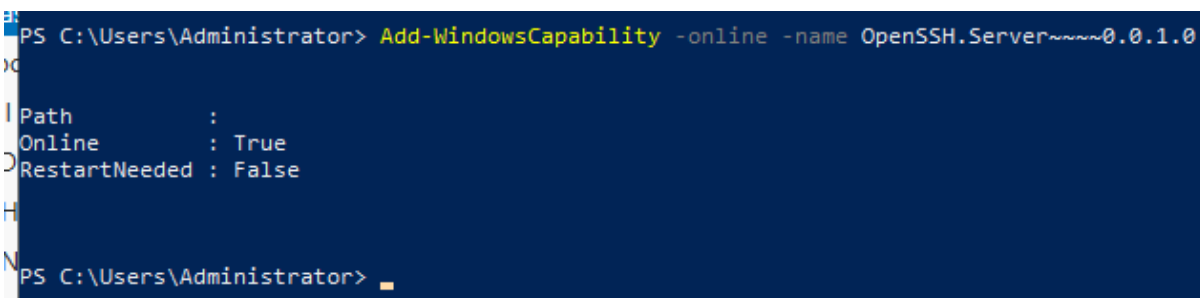
```
Add-WindowsCapability -online -name OpenSSH.Server~~~~0.0.1.0
```



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

S Operation
  Running
  [ooooooooo]
```

It takes a moment or two to run. We can just wait in this time.



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

PS C:\Users\Administrator> Add-WindowsCapability -online -name OpenSSH.Server~~~~0.0.1.0
Path :
Online : True
RestartNeeded : False

PS C:\Users\Administrator>
```

When it has finished installing we will see the above message letting us know SSH is now online and no restart is required at this time.

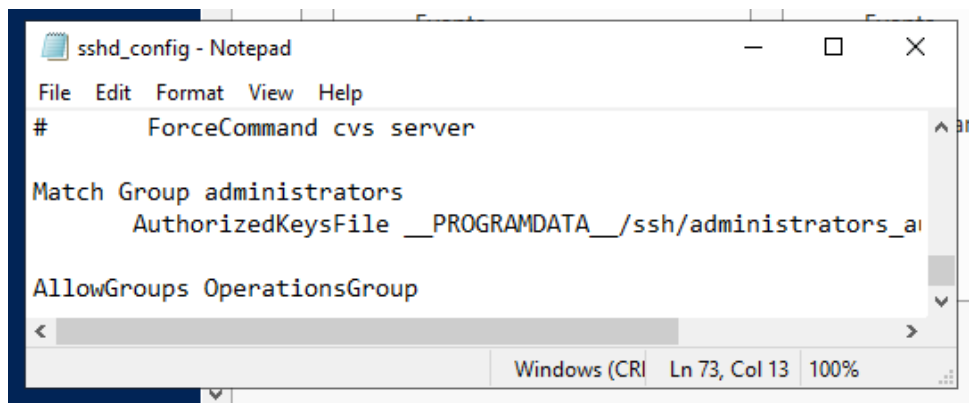
```
PS C:\Users\Administrator> Add-WindowsCapability -online -name OpenSSH.Client~~~~0.0.1.0

Path      :
Online    : True
RestartNeeded : False

PS C:\Users\Administrator> set-service -name ssh-agent -startuptype 'automatic'
PS C:\Users\Administrator> set-service -name sshd -startuptype 'automatic'
PS C:\Users\Administrator> start-service ssh-agent
PS C:\Users\Administrator> start-service sshd
PS C:\Users\Administrator>
```

Now we enter the following commands one at a time:

```
Add-WindowsCapability -online -name OpenSSH.Client~~~~0.0.1.0
set-service -name ssh-agent -startuptype 'automatic'
set-service -name sshd -startuptype 'automatic'
start-service ssh-agent
start-service sshd
```



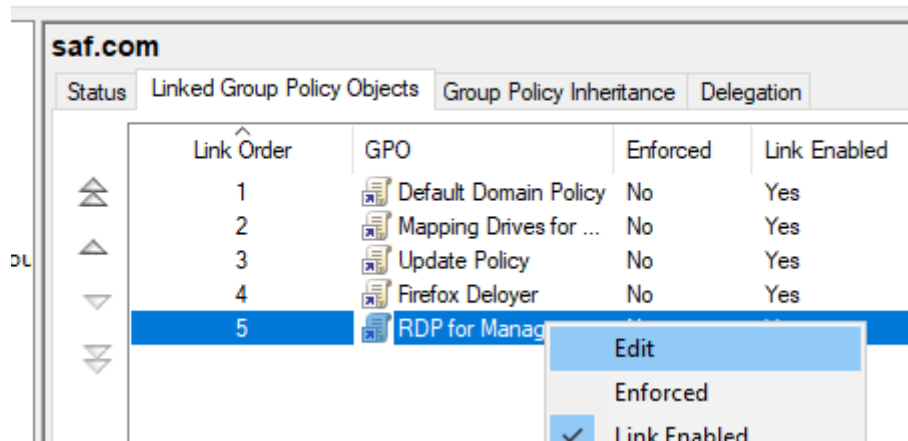
The next step is to edit the sshd_config file, located at C:\ProgramData\ssh. Open with a text editor and add the following line to the end: “AllowGroups OperationsGroup”. This can be any previously created group, but for the demonstration we will use OperationsGroup.

```
PS C:\Users\Administrator> Restart-Service sshd
PS C:\Users\Administrator> Restart-Service ssh-agent
PS C:\Users\Administrator>
```

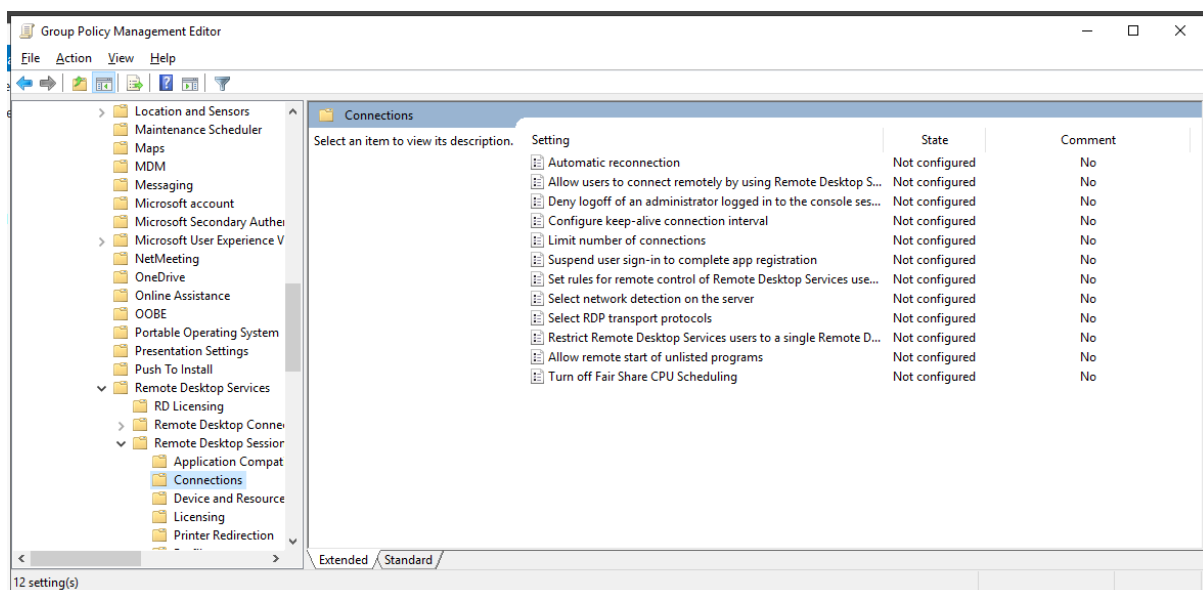
From here we run “start-service ssh-agent” and “start-service sshd” to restart ssh

9.2 - Setting up RDP Access

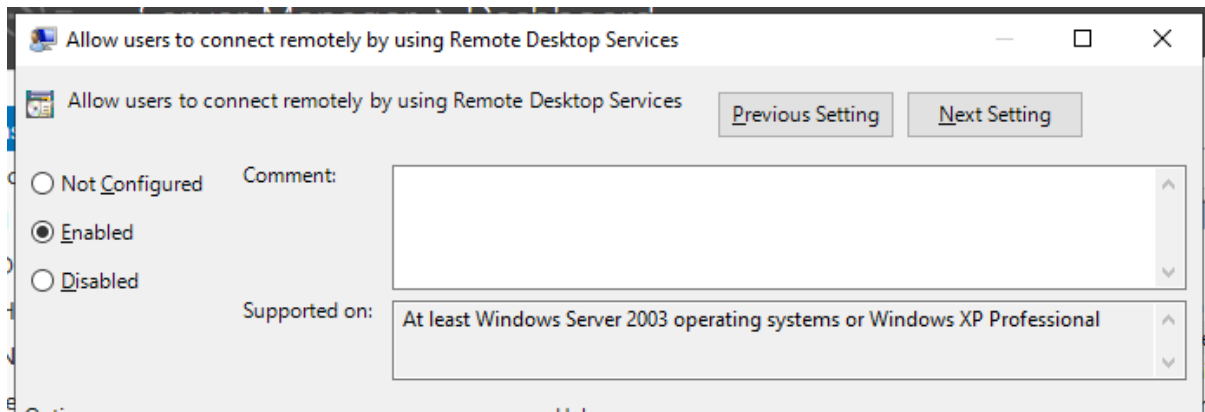
RDP can be enabled for groups via the use of a Group Policy Object. By now we should be fairly familiar with creating GPOs. This section will assume previous experience and summarise various aspects without showing all steps.



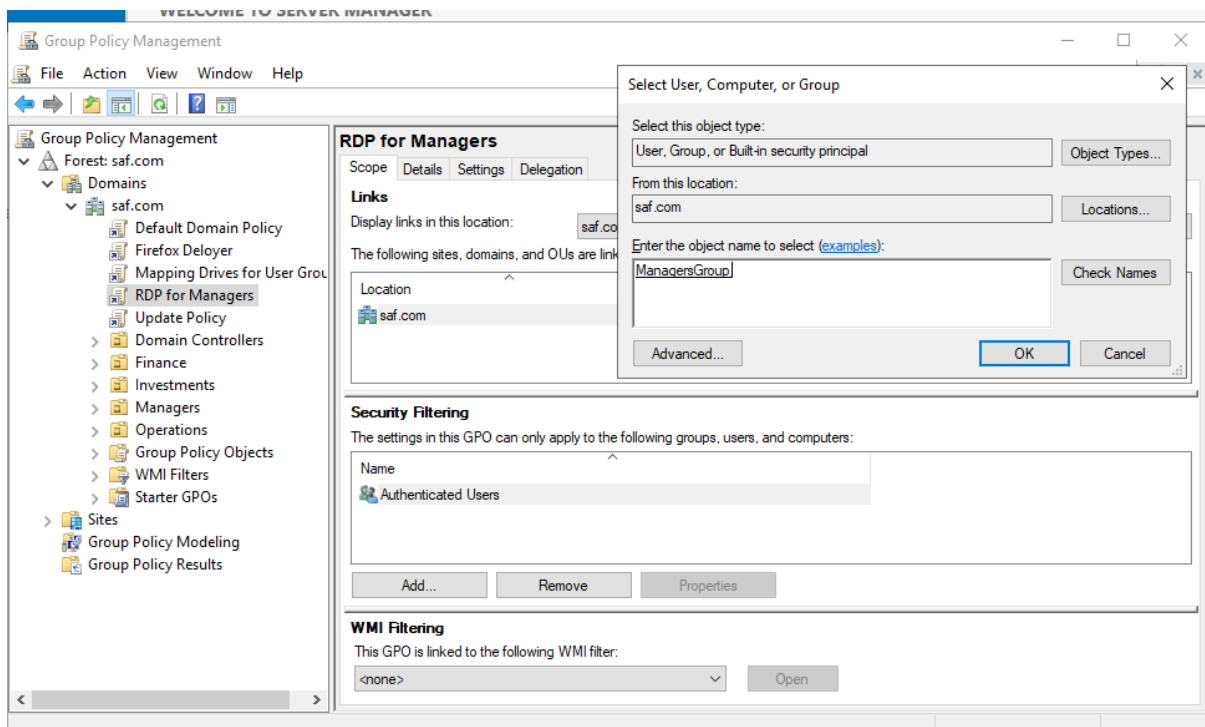
For RDP we once again go to Group Policy Management via the Tools menu. From here, right click on the domain and select "Create a GPO in this domain, and Link it here...", name the GPO, right click on it and select "Edit"



Expand the tree on the left hand panel to Computer Configuration, Administrative Templates, Windows Components, Remote Desktop Services, Remote Desktop Session Host, Connections and then right click on "Allow users to connect remotely using Remote Desktop Services".



In this window, simply click the “Enabled” radio button followed by “Apply” and OK

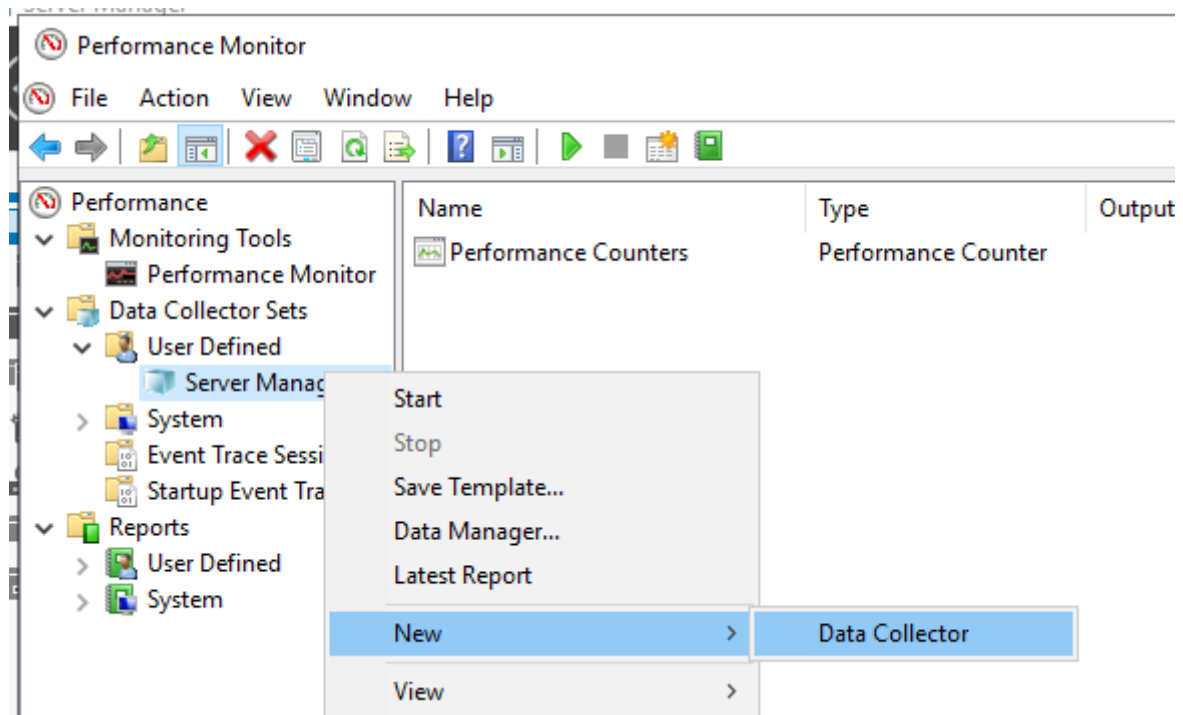


Returning to the Group Policy Management window, click on the “RDP for Managers” policy and click the “Add...” button in the Security Filtering section. Enter “ManagersGroup” and click “Check Names” to ensure it is spelled correctly. Then click “OK” to apply the policy to the group.

10 - MONITORING FOR PERFORMANCE

Monitoring performance is very important for running large scale servers such as SAFserver. Fortunately for us this is made easy through the use of a program in Windows Server 2019 called Performance Monitor. It can be configured to send out reports as shown below.

10.1 - Generating Performance Reports



Open Performance Monitor and expand the tree to find Server Manager under User Defined in Data Collector Sets. Right click on "Server Manager" and select New, Data Collector.

← Create new Data Collector

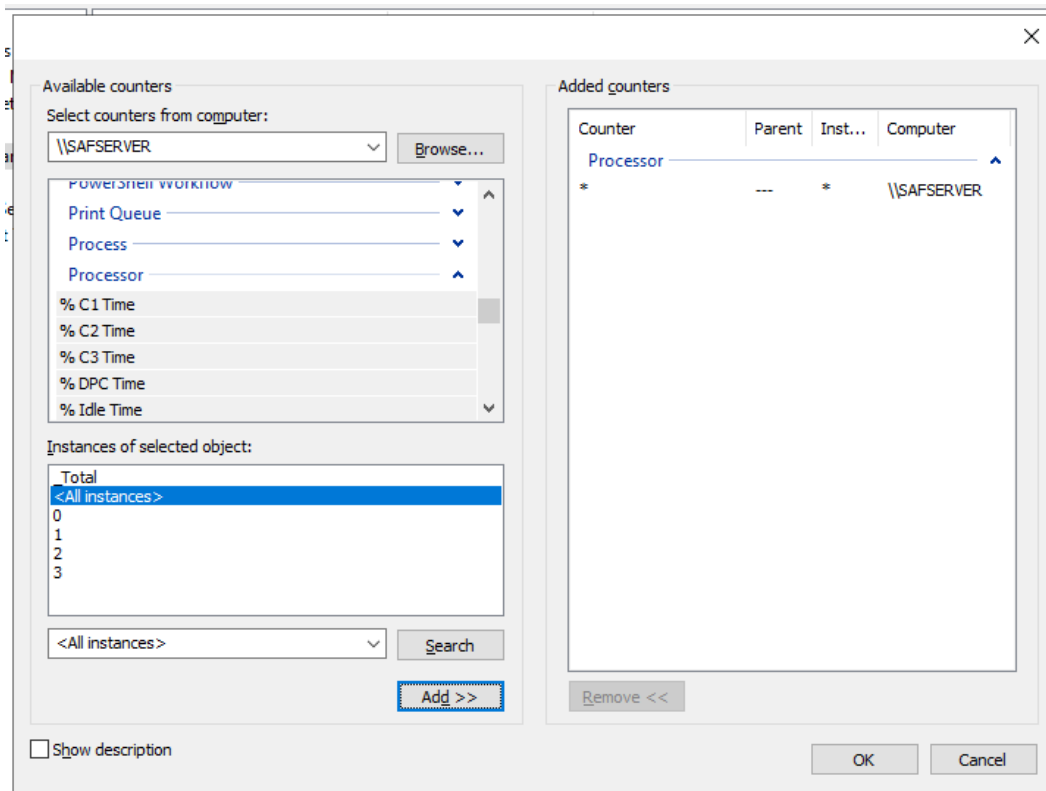
What type of data collector would you like to create?

Name:

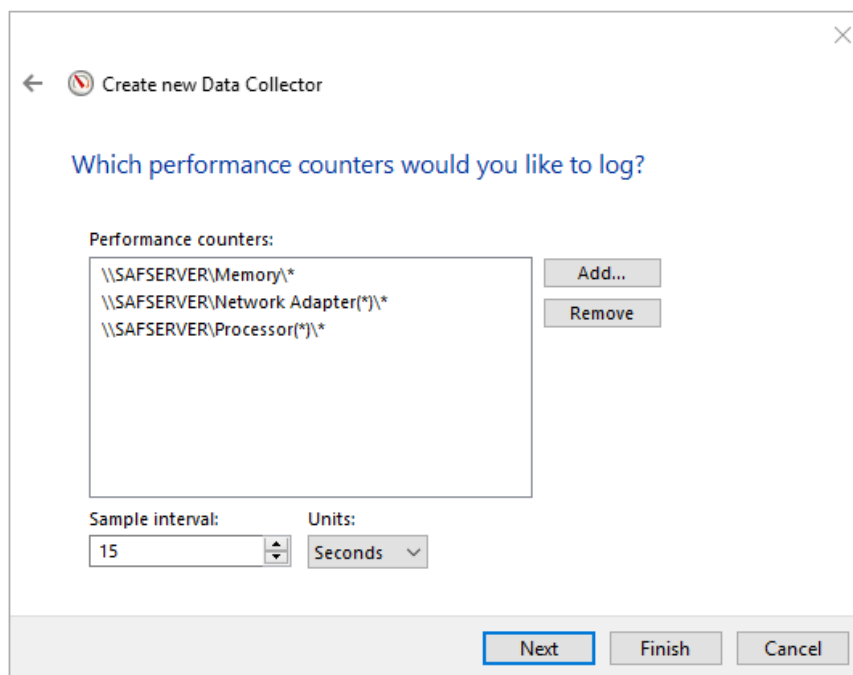
Monitor1

- Performance counter data collector
- Event trace data collector
- Configuration data collector
- Performance counter alert

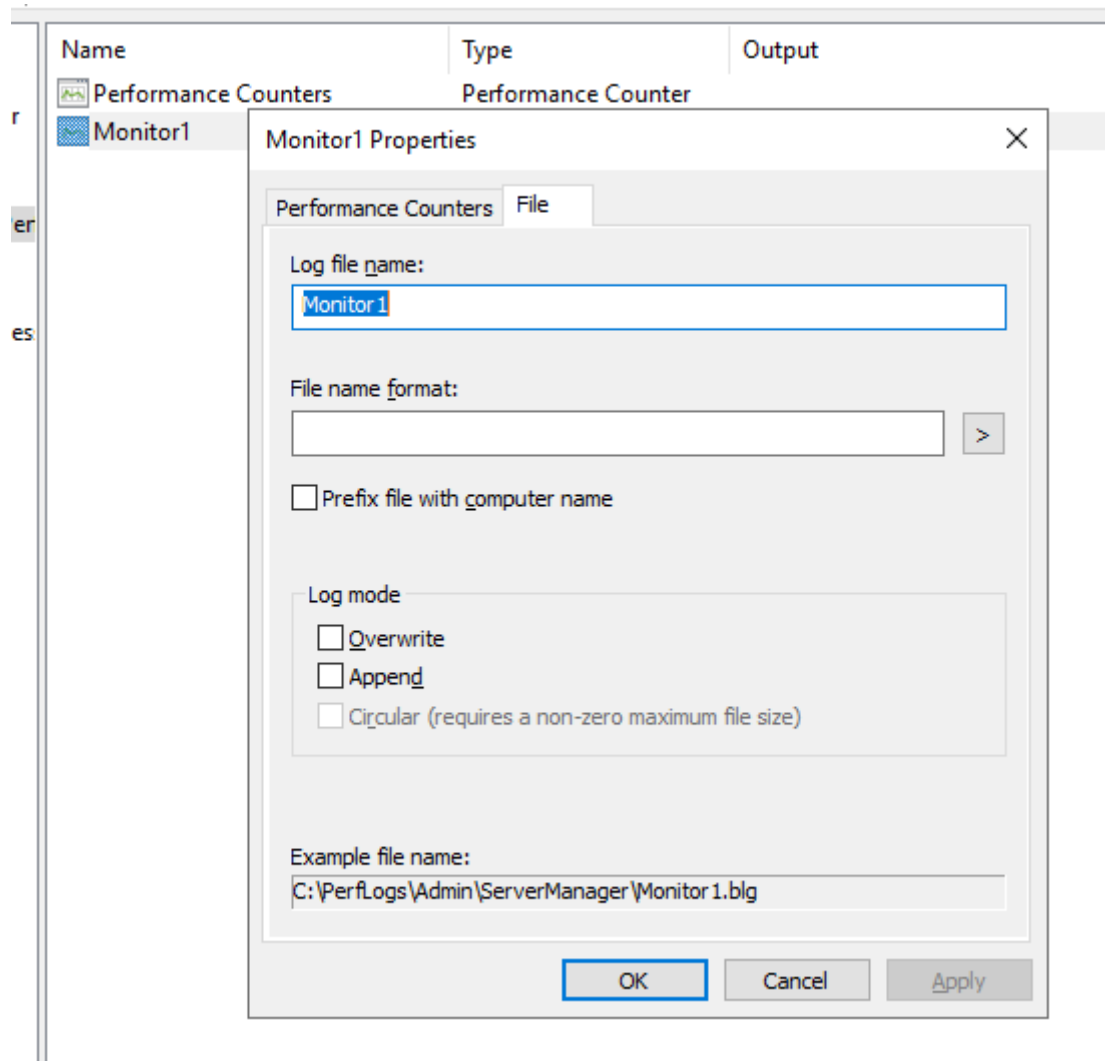
We give the collector a name and select the type with the radio buttons.



From the next window we click “Add” and this opens the available counters. Here we add the various counters for the things we wish to monitor. For demonstration purposes we will add all Processor, Network Adaptor and RAM data collectors available and click OK.



The Sample Interval can be set in this window. For demonstration purposes we will leave it at 15 seconds and click Finish to create the data collector.



Right click the new Data Collector and select properties. Open the File tab to have a look at the details for the log file that will be created by the collector. Changes can be made here should we need any. The collector is now collecting data.