

IT Unit 9.4

By Adam Chu



Contents

**No table of contents entries found.**

# How to install and Use Active Directory

## Related image

## New User:

At the top ribbon there is an icon shaped like a person with a plus which allows you create a new user with First Name and Second Name Burner Password and the setting that the password needs to be changed after first login.

## New Group:

You can create groups shown in the right image, similarly to when you make new users and you can edit the properties of that group shown in the left image.

## Access Times:

This includes Access Times (I showed this inside of the practical), where days and time slots are shown in blue and restrict access using that account. You can also access file permissions this includes Read, Write & Viewing. This at College means that each user can access their respective file storage for BTEC students H(): whereas the apprenticeship students can access a different partition on the server.

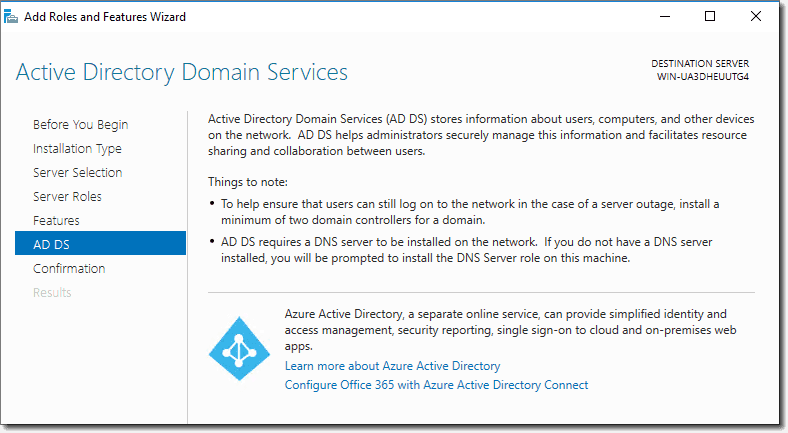
## Software:

Inside each user you can enable certain programs installed on the server, for instance allowing the IT and Media Students access Autodesk Mya and the Adobe Suite. You would want to restrict access to these programs as they are subscription based.

## Shared Resources:

In the list of devices you can select shared devices and inside that will be any network attached printers this then can have its properties altered like its name so it could be more descriptive i.e. B&W Laser Library Xerox Model No. instead of Xerox Model No. This is similar for all network attached devices like printers and scanners.

## Adding Devices to the Domain



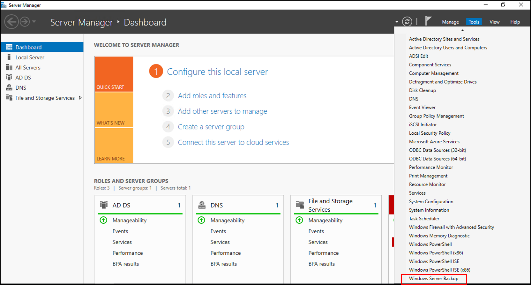
Using Active Directory Domain Services it allows the user to set up sub-nets as well as control the bought Ip Addressees and control which PC’s are attached to them. This is important if you want to segregate networks into smaller departmentalised networks as well as deciding which IP Addresses are given to each PC. It also allows you to use a DNS server to set up an intranet only website like for example ELIP is only accessible on the college intranet.

## Anti-virus

Inside Shared Computers and Applications you can have an install package save to a drive set-up to have do a mass install on all connected devices, this would include anti-virus programs as well as generic ones. You can also have the anti-virus set up to run in the background of the active directory to protect against attack.

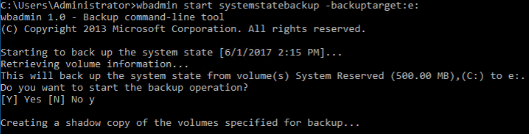
## Backups

Inside active directory you can create a backup by opening ‘Server Manager’, then selecting ‘Tools’ from the ribbon. There will be an icon that is called ‘Windows Server Backup’, Then create a local backup and choose where to save it (this will take a large amount of time as it is creating a full backup for the server). There will be a section called the action and will have options for the amount of backups you would like to generate in-case one is corrupted during the creation or saving processes. Then you have select which ‘Volumes’ will be backed up (usually all of them) and you need to select ‘Enable System Recovery’ so that if this back-up is required then it can rebuild all of the data prior to its creation.



Using a back-up on a windows server is quite simple you would go into CMD or Windows PowerShell and use this code which tells the system to run a system back up with administrator privileges and what the target is called and which area it was saved to. Then you will have to reset up parts of your active directory, and some data might have been lost since the back-up was created.

wbadmin start systemstatebackup -backuptarget:<targetDrive>:



# Report on the Security at the College

The college has a series of systems that protect data from theft or corruption to enter the server room that I have used active directory to add users. You will need a key-card to enter the building where the Server Room is (this has automatic locking doors), then you need a physical key to the actual server room which then allows access to the Rack-Mounted Server.

If you want to borrow or take a device outside of the college’s intranet whilst having a VPN to tunnel inside the network then that device need to have the use of BitLocker AES – 256 bit Encryption. This is where all volumes on a borrowed machine need to have an decryption key before the files are useable so even if the device or file is stolen they need the 256 bit long encryption key. Bit locker does full volume encryption meaning all partitions on a drive are protected and safe from theft.