Active Directory – Part 1

Executive Summary:
Modern problems require modern solution. Technology is developing so fast and the consequences from it also challenging the world to fight against it. With is perennial process the development has change its' pace and has provided a different, a better, world which human mankind cannot denied it. One of the examples from it is a computer technology, no one has any argument that technology has brought a devastating change in the world but arise in the computers was also difficult customizing them. One scenario can be if a company using thousands of computers, for an administrator it is the cumbersome activity to setup each computer manually going in that location and nearly impossible to sustain that setup, because problems appear while working and change is essential. Also, there are not only the computers to take care of. However, the development brought the solution for this as well which we say, 'directory service'. In this report, we have discussed about the directory service in the simple way, which can be beneficial for the students and someone who keens to know about the basics of 'directory Service'. I have tried to explain this service in the simple understandable way, including the diagram. I have also included the references to those who thoroughly want to understand about these services, can use as a resource. The information is collected using the web resources and I have interpreted it as I understand them in the simple language form.

Contents

INTRODUCTION TO ACTIVE DIRECTORY:

Firstly, we discuss about the organizations in the modern world. Well, being dominant by the computers and technology modern workplace cannot remain untouched with the network, inside that, computers, and users. Looking the size of an organization, locations for operation, and their objectives some has many and other may have less. In the physical word, organizations have rules and regulation for each staff, departments, regarding what resources they can use and what they cannot. Introducing, the technology there can arise problems regarding to maintain these rules, connecting users and computers because each user's profile from different departments and each computer should be manually configured. Further, once created they must be monitored and protected on daily basis what if problem arises in one part, physically an individual must be in that place and recover that problem. Well, small companies with less resources could maintain this but for big organizations it will be a nightmare doing so. However, one technology can discard the problems, and as a solution of this it was introduced which is known to be 'Active Directory'.

In the late 90's, Microsoft introduced 'Active Directory' in windows server 2000, followed the revised and more functional service in windows server 2003. After which, other competitors like Apple introduced their own Active Directory. With that competition, presently we can use the more advanced and developed Active Directory running on Lightweight Access Directory Protocol (LADP) which works simply accessing TCP/IP model. It can be clear that, why and who developed this project but what is Active Directory and how does it work.

What is Active Directory?

Active Directory is the database and a set of services that keep records about the computer network and provides environment on how users can access the network resources and,

maintain platform for managing and handling those services. The database contains all the information about the structure, which includes the users and computers with all the permissions assigned to them. It helps the administrators by simplifying the procedure to assign policy in a centralized manner and all users making simple environment for managing and using resources, like printers, handling shared files form central repository which increases flexibility and ease collaboration also helps in the backup of files providing security ensuring the continuity of the business.

Concept of Active Directory:

The hierarchical structure provides simple and securable environment for management of network resources and for administration works. The data is centralized but also the distributed among other servers for enhancing fault tolerance, high availability and for load balancing with the consistency which provide speed to the work. The flexible and scalable feature assures reliability and quality of services from the active directory. Below is the overview of working mechanism of active directory.

How does Active Directory Work?

Active Directory works in a hierarchical or tired structure. Main service in Active Directory is Active Directory Domain Service (AD DS), which is the feature of server and is install in the Domain Controller (server enabled Active Directory). A Domain controller controls the directory environment which has records of each object, their roles, and features inside that organization. Normally, there should be a backup domain controller in which the data stored, changed, or deleted on the main DC can replicated on the other DCs, which will maintain redundancy and fault tolerance for the data. DCs are protected by administrator credentials and accessing to a domain controller, one can access all the resources in an organization, so it is necessarily, important to have protection over DCs and administrative credentials. A Directory service can (2020) maintain more than one domain, other domains can be linked with one directory and can setup trust relation between them, which is maintained by Global Catalog Server which has records of all domains inside a forest. The full picture of domains, child domains and OU is called forest. OU are the container objects, which can represent certain departments inside domain. Parent domain is the main domain which represents the organization whereas child domain represents some branch of an organization which an organization could have to deal separately mainly because of the locations and working criteria. Such as a company with domain *knowledge.com* *can* have child class *english.knowledge.com* because it only works for English field, or it may have *australia.knowledge.com* because it is one branch woks in Australia which have two-way transitive trust. Main difference with separate domains is it should be oneway or two-way transitive trust between the domains. There is the inheritance to the Organizational units with the higher-level units by default while creating organizational units.

The figure shows logical structure with two trees one containing child domains.

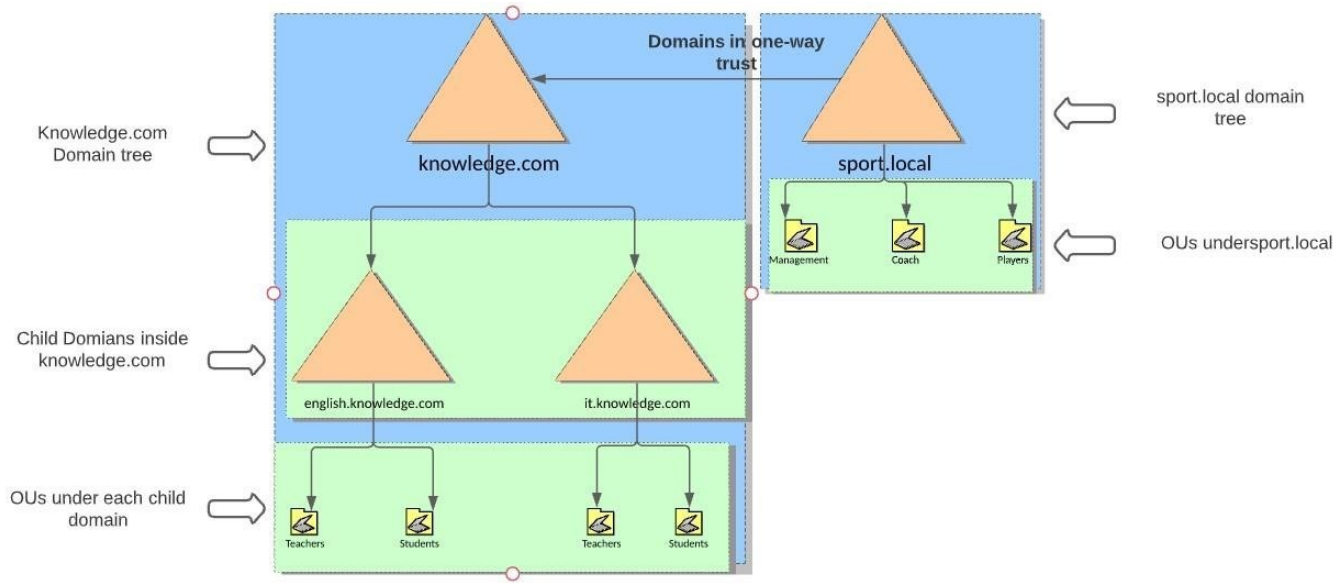


Fig: Forest of two trees in active Directory

Inside the organizational unit we setup objects (users, computers, printers, groups, servers), in which thereby are assigned policies. Figure below shows view of organizational unit teachers:

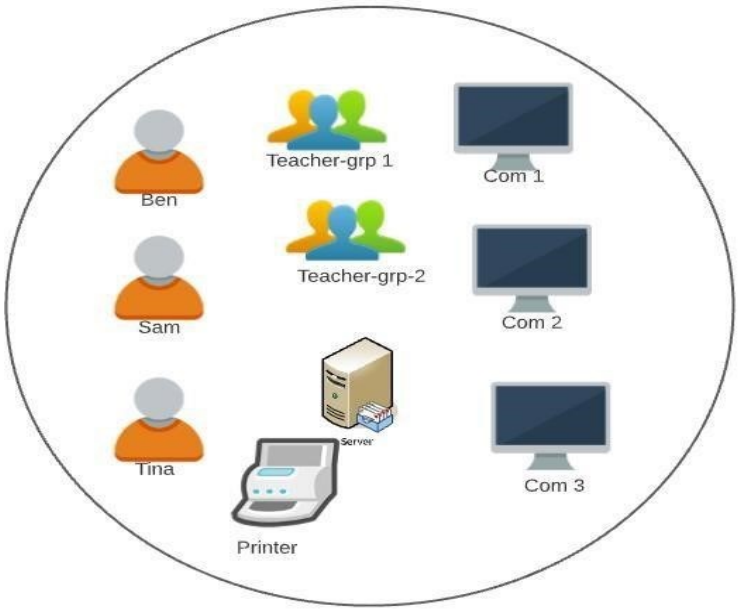


Fig: Teacher OU

Everything in a domain is made and controlled by using **Domain Controller**, which we have discussed above already, server manager after installing active directory, we can promote the server as domain controller by adding it in a domain, other OUs, users, computers are setup

using Active Directory Users and Computers console in server manager. The figure below gives how OUs and computers are managed using AD users and computers.

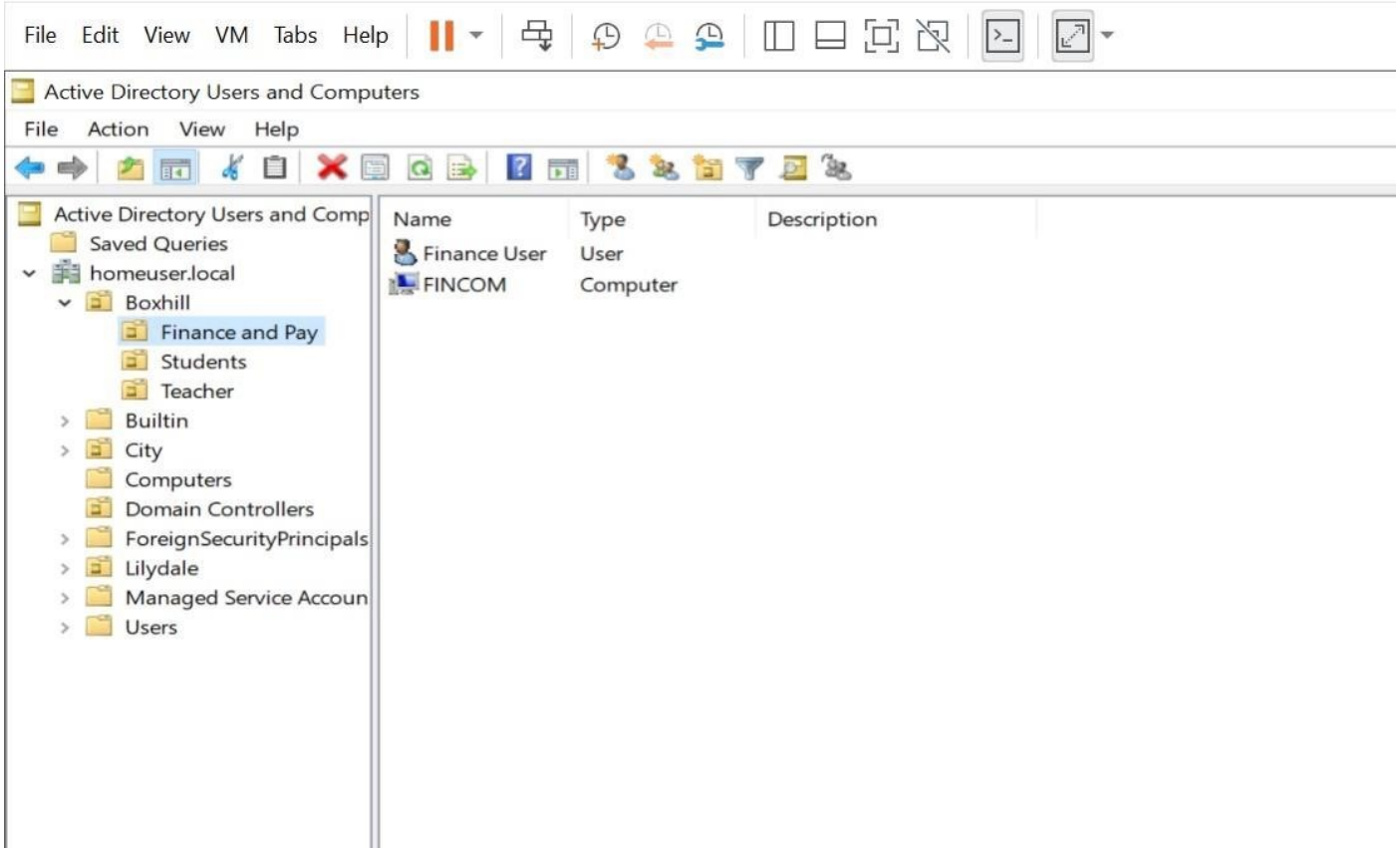


Fig: Active directory Users and Computers: Microsoft Active Directory:

Introduction to Different Directory Services:

Based on different types of operating systems and concerning to different working platform, different companies introduced different types of directory services. Some of the actively dominant services in the market at present time are Microsoft Active Directory, Apple Open Directory, Azure Active Directory and so on. The main difference is the software these companies release, however the working protocol for each service can be the same. LADP – Lightweight Access Directory Protocol is the advance protocol for active directory which is compatible with TCP/IP model. we have already discussed the general concept of directory service, which is the base idea and feature of all the directory services, but according to mechanism in different operating system for handling data and their unique solutions they can be vary in specific terms. In this section, we will try to explain different active directories on the basics of definition, structure, Authentication and Authorization.

Microsoft Active Directory:

Definition:

The directory service introduced by Microsoft in late 90's which work in the domain structure in windows networks for the ease of management and authorization. It uses lightweight Directory Access protocol (LDAP) which runs in TCP/IP networking protocol. The main reason for the development of this Directory service is to provide centralised environment to set-up and manage, applying policies to other windows machine inside the organization, giving full authorization to administrators using Domain controllers.

Structure:

It provides domain service for the hierarchical structure inside the networks, by not compromising the sectors and location of the organization. Any type of organization using network and network devices can be easily authenticate using this service, maintaining the co-relation among each sector. Main components inside this domain services are forest, trees, domain, sub-domains, domain controllers, organizational units, and objects.

Authentication:

Microsoft provides easy and secure environment to provide authentication as serving so long and used many protocols for authentication and currently it supports NTLMV2, Kerberos 5, which made harder for imposters to break into system using someone else's credentials.

Authorization:

So far in active directory Authorization handling is fully a part of administrators because only they are aware of the policy maintaining around the organization. AD security group membership – there are many built-in security groups such as Domain Admin and Guests also we can create our own security groups from which each groups can be assigned roles equally, Directly assigned permission –objects in the domain inherited it's parents object policies, which also can be prevent by blocking inheritance, and Group Policy – which is one of the strong tools in active directory from which control and customization of objects can be done, group policies defines what a user can and can't access as per the rule are three main features to control the users access.

Azure Active Directory:

Definition:

Azure Active Directory is another directory service introduced by Microsoft in 2008, which is a cloud service that provides administrators with the ability to manage end-user identities and access privileges. It is the part of the Microsoft Azure-which is a part of public cloud platform. It is in servers in Microsoft Datacentres. It is used by an organization in the subscription based and which organization need not has to configure. Azure AD is the different technology to Active Directory especially designed to provide the cloud infrastructures rather than on-prem environment.

Structure:

This active directory does not run-in domain structure so, there is no way to having Domains, forests and objects like in AD DS. It is based on the subscription based and main structure depends on tenant which is a dedicated instance for a specific company. When someone purchase subscription for the cloud services like Office 365. The tenant is provided dedicated directory which includes all the users and provides authentication and authorization.

Authentication:

Azure Ad uses protocols like SAML, OAuth and OpenID connect which are known to be modern authentication protocols. In addition, it provides services like self-service password reset, multifactor Authentication. Also, conditional access policies, including password less

authentication and more. As the use of the Azure Active Directory is moreover different these policies are also different.

Authorization:

Regarding Authorization, as well, AD DS and Azure DS are completely different. Three main components, Azure AD security groups – it is like AD security group membership structurally, specific groups members can access to the permissions assigned to the group. However, those groups can be compromised of Azure AD users account because of on-prem user accounts and on-prem application and resources, Microsoft 365 groups – Microsoft groups can include users form both inside and outside the organization who can be configured based on the attributes like department, location or title, Azure AD roles – it provides specific sets of rules to different types of administrators. There are dozens of built-in Azure AD roles also we can create the roles in a custom way, which shows there is a way difference in Azure AD and AD DS in terms of Authorization as well.

We can connect Azure AD form AD DS, doing so organization can feel the cloud benefits which is becoming essential in the modern progress.

.

Apple Open Directory:

Definition:

Apple Open Directory is the similar directory service regard to Microsoft directory service and was released shortly after Microsoft released Microsoft Active Directory, it is also a LADP directory service, which describes a shard LDAPv3 directory service which centralizes the users and computers of an organization. Apple is a different OS from Microsoft which then needs different software to handle mac computers for the organizations using Mac Computers.

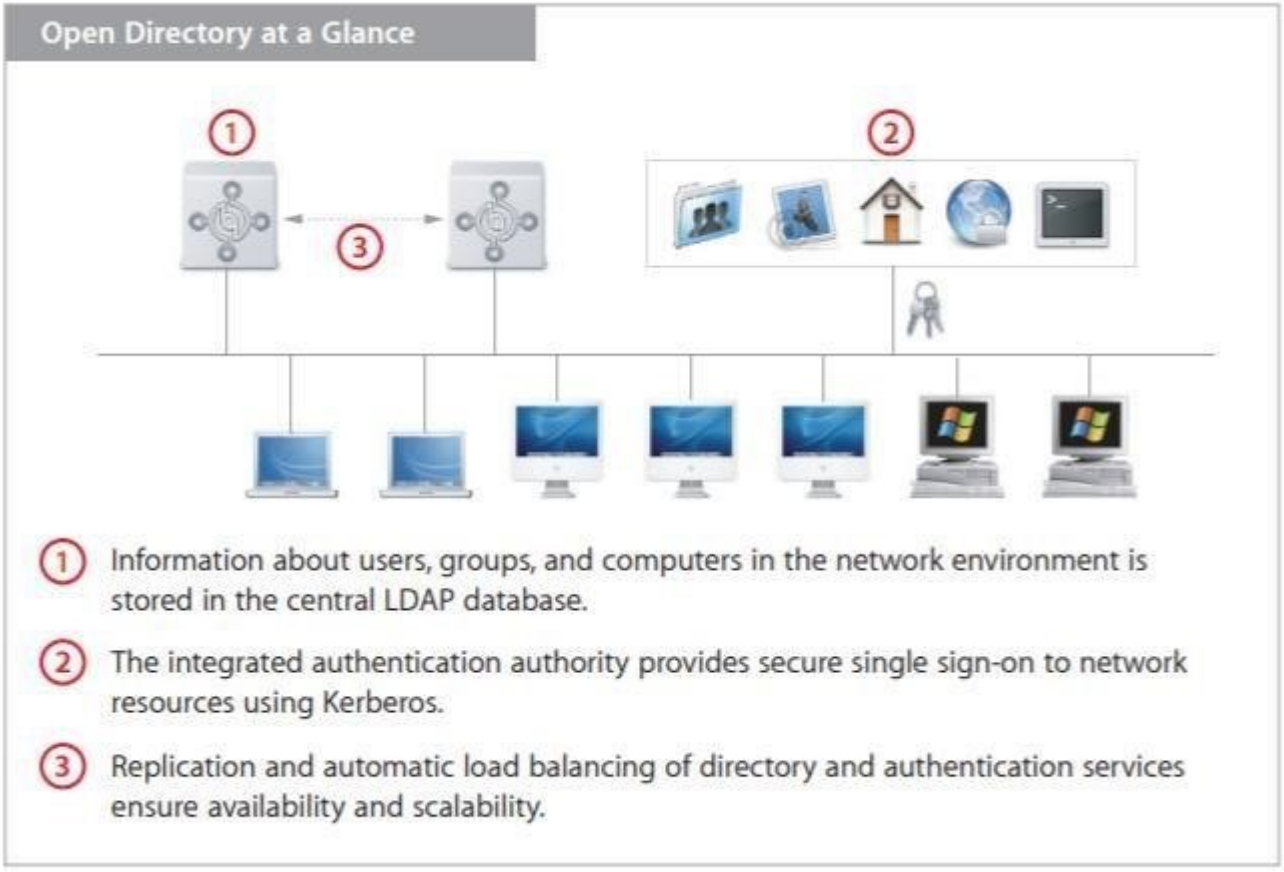


Fig 3: open directory at a glance.

Structure:

Apple Open directory also follows the same domain structure which is maintained in the mac server using the directory administrator account. We can add groups and users using this server, which like the Microsoft active directory provides central way of authenticating the users and macs.

Authentication:

Open directory uses MIT's Kerberos technology which allows single sign-on access which maximizes the security for the network and resources throughout the organization, maintaining easier accessing environment for the authorised users. In addition, it also supports legacy authentication method that uses SASL, in which users can setup only one password to access resources everywhere in network, which could be more economic and can reduces problems for resetting passwords and creating passwords for the administrators.

Authorization:

The directory administrator has privilege to set the rules, policies, firewalls so that the users are denied or access to the resources as per the configuration done by the administrators.

RESULTS AND CONCLUSION

In the conclusion, Directory Service can ease the process for maintaining, managing, and securing the environment and resources of an organization. It not only reduces the complexity

of the administrators sustain the rules and policies for computers and users, but also provides scalable and flexible working environment being under an umbrella for the staffs as well. Moreover, with the enhancement of the technology and way of accessing resources, different service providers have different types of directories set up which includes Microsoft Active Directory, Open Directory of apple, Azure Active Directory and so on. Each directory has their own importance and is used for the specific purpose. For example, Azure Active Directory is mainly used to browse the cloud infrastructures in the organization. Each directory has their own security principals, and they are working for achieving that success, which is, provide security, reliability, and quality of service, securing confidentiality, with the minimal risk, protecting the users' data. Flashback to the old days, there has been a lot of betterment in the technology, which is continuing, which is directly suggesting that there is a lot to come near in the future.

References

2020. 26 02. https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-compareazuread-to-ad.

Bryan Patton, CISSP. 2021. *Active Directory vs. Azure Active Directory: What You Need to Know.* 03 29. Accessed 06 19, 2021. https://www.quest.com/community/blogs/b/microsoft-platform-management/posts/.

2020. *Compare Active Directory to Azure Active Directory.* 02 26. https://docs.microsoft.com/enus/azure/activedirectory/fundamentals/active-directory-compare-azure-ad-to-ad.

n.d. *Open Directory.* Accessed 06 19, 2021. https://images.apple.com/server/docs/Open_Directory_TB_v10.4.pdf.

n.d. *what-is-active-directory.aspx.* Accessed 06 19, 2021. https://www.quest.com/solutions/active-directory/whatisactive-directory.aspx.

Part 2: Designing Active Directory

DESIGNING ACTIVE DIRECTORY

Background

Boxhill Institute is a large educational organization with three main branches located in Boxhill, Lilydale and City. Inside the organization, has many staffs, students, and administrators. To look after the management and users, it can be harder to apply policies in each level. Configuring and managing all the network resources inside the organization is a troublesome activity. So, to enhance the problem introducing the Active Directory Domain service can be helpful for the advancement of security, management, also for the centralization and decentralization of rights and providing policies for the users, computers, and other resources available in different level. Here, we have discussed how hoe the basic level of active Directory can be design looking the geographic locations of each branch staffs who are working in different

levels, also the students and computers in each branch. We will setup different policies so that each level resources can be used by specific departments who are assigned to it. We are using single level domain because it will keep the structure of Active Directory simple, straight forward, also reduce expenses and time to setup the domains, domain controllers, and so on.
Further, our branches are not located in single place, looking this situation we have different departments in each branch. For example, we have different faculties in Boxhill to Lilydale and city also the staffs working in each place. In addition, each place has finance and pay and some heads in each campus, furthermore each place has their own resources such as computers, servers, printers, and contacts. Looking this condition, we can create three Organizational units in our active directory based on the location and inside those organizational units we will put more organizational units based on the faculties and sectors of work. Here we will take example of common groups that are Teachers, Students and finance and Pay members, however the sectors are not limited to this, we can put sectors available in each organization according to our needs as organizational units for each location.

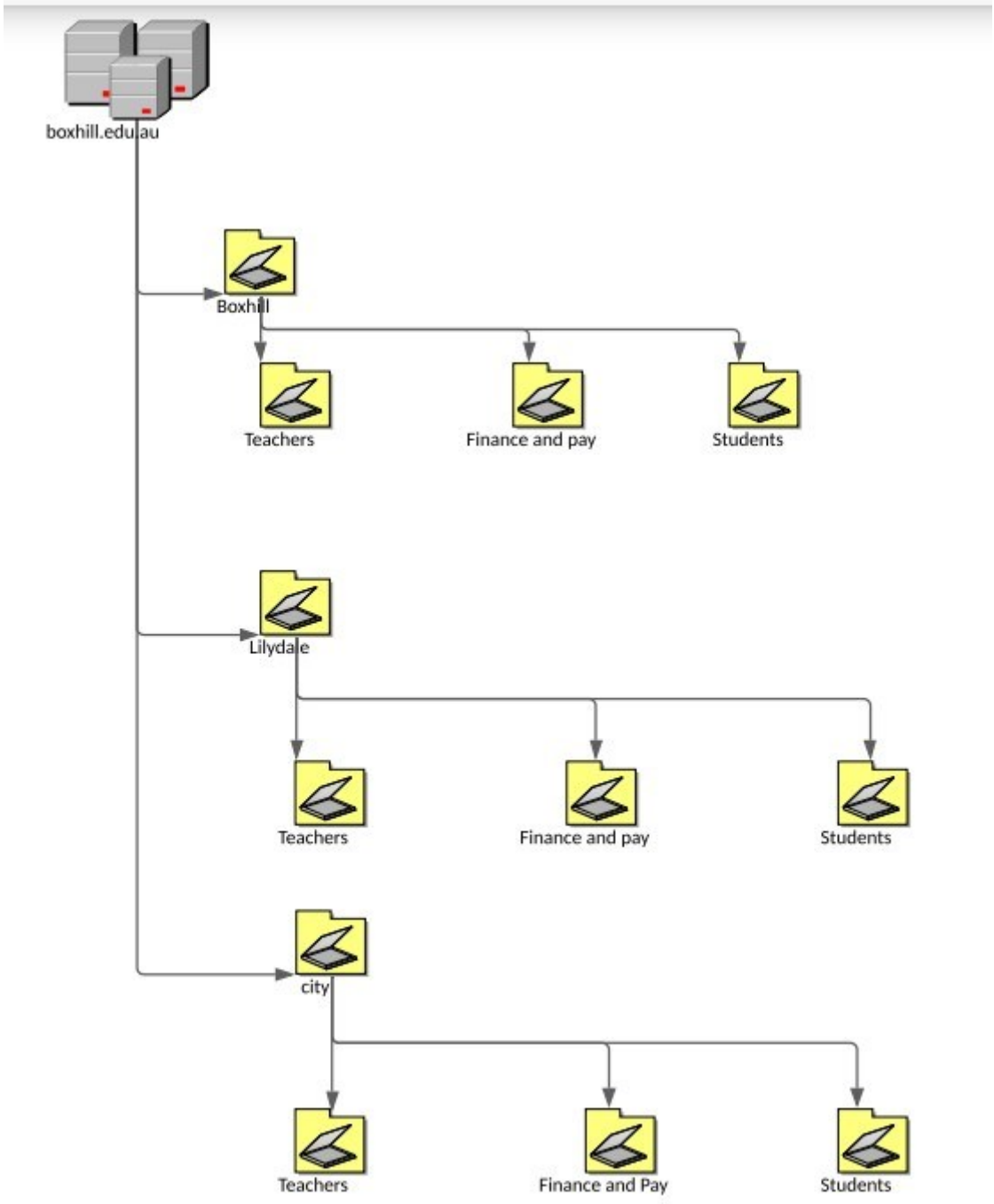


Fig 1.1 Arrange of Organizational Units according to location:

Above mentioned are the organizational units in which we can apply group policies. Now we can put users and computers inside these organizational units. For example, we can create users for teachers, finance and pay also, for the students. Keeping in mind that teachers can be from different faculties, and some may also have right to access resources from other faculties, for these we can create groups of those users in which we can assign policies which will be same for the finance and pay as well as students. Further we can have some computers accounts separated for finance and pay in which we can install software required for that sector. We can have delegation right to one staff from each sector, so that they can apply some policies required in their fields. Similarly for students we can put student accounts (as user) under student organizational unit where we can have policies assigned for students. Above that we can have computers and users related to organizational units related to locations for their heads in which they can run organization according to the need. By that it means not necessarily Boxhill should run with the same policy given to Lilydale. We can apply policies to organizational units (Boxhill, Lilydale and city) according to need.

Designing Leaf Objects

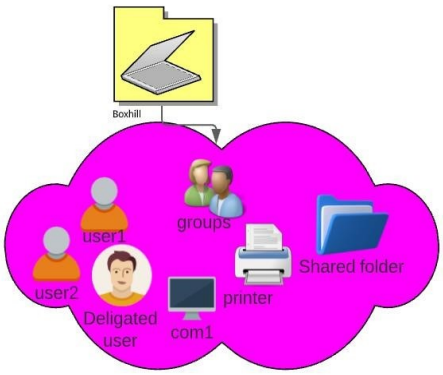


Fig 1.2: Resources managed in boxhill OU (leaf Objects)

Here boxhill OU is managed by some staffs who has user account under this OU. some computers are specified for their use. In this OU head of the organization are the members who can be given policies as the company's plan. The members can be staffs from different faculties, which can be similar in city and lilydale OU.

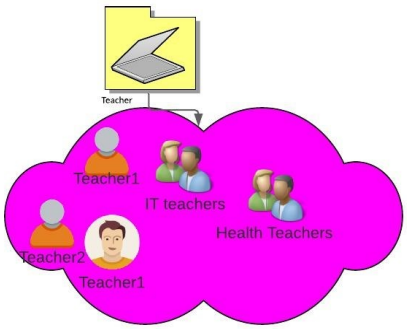
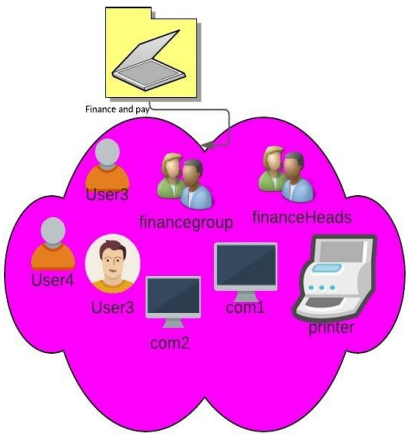


Fig 1.3: Teacher OU

Here, Inside Teacher OU teachers has accounts and group based on the faculties. Here teachers from different locations under same faculties are under one group so that giving policy will be user there are some delegated teachers as well who the head from the specific faculties can be. Here policies can be applied for a specific teacher and also for group of teachers.



Here, finance has different users, computer, and groups. Here computer accounts are created so that we can have required applications installed in each computer through active directory. We have delegated users and a group for finance heads from each location, which will work as a centralization of policies for overall organization. Printers for each user or PC can be found from the attributes set for each account and printer.

Fig 1.4: Resources in finance and pay OU

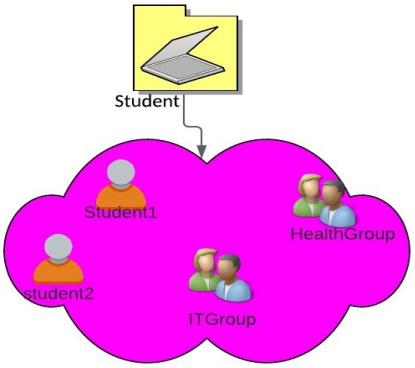


Fig 1.5: Student OU

Here, students are monitored by the accounts given to each student. Further, we can make a group of students as per their enrolment in different subjects, if we have different policies for students from some faculties.

GROUP POLICIES

Overall, we have created users account and computer accounts in our active directory, which can simply tell us about the structure of our organization. We added users to the group based on their sectors. Those users are the domain users, they are not the domain admins. It is the role of system administrator to set up the domain structure, who will decide what permissions to give to those users, what they can access within a domain, analysing the security and work policy. But permissions are not assigned directly in the active directory. It is done in Group Policy Management Console. In GPO policies are created and are linked to the appropriate group, members, and computers. Here we will apply basic group policies to our work members,

for example, assigning specific applications to computers in finance and pay, mandatory wallpapers to the teachers, secure environment to HR group and restriction on some sites, restriction on desktop change for students.
While creating the group Policies and linking to the OUs and objects can lead to wrong way if one is not fully aware about the settings. For example, if we configure the policy to the computer only, we will apply that policy to the computer only, but the policy was meant to whole OU. Here, user will not be impact by this policy if he/she log in with different computers. So, one should carefully aware whom to apply the policy. If a staff login remotely to the domain, he/she should not be accessed to that what he/she is not supposed to. For this we can apply policy to that user account.

Deploy Software to OUs via GPO

Finance and Payroll require access to special software that needs to be updated automatically via a GPO.

We will deploy a software to the finance and payroll OU which will be updated automatically via a GPO, for this we can use the OU called finance and pay from our active directory which contains computers and users from finance and payroll department. To deploy a software in our active directory we need a .msi package file of that software. For security options we can create a group softwareDeployment where we put all users form finance and pay, for which we can read/write control to this group while sharing the package.

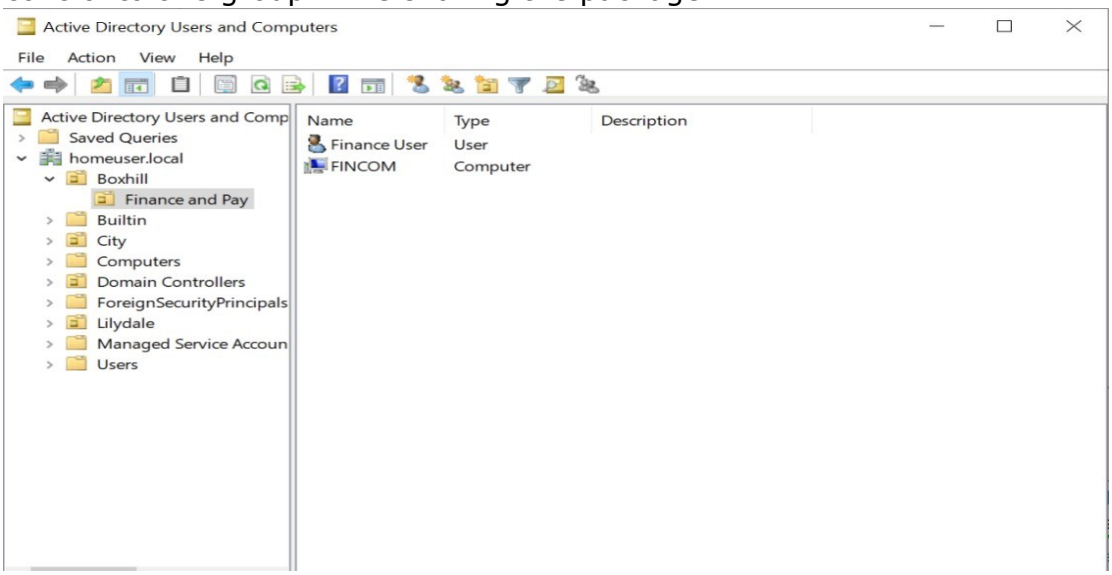


Fig:1.7 Active directory users and computer under Finance and pay OU.

Now we will add our package to our share folder and give full access to share folder from where the users and computers get path to install that package. After the folder is shared, in GPO we can create a policy under the organizational unit called Finance and pay name the GPO and edit that GPO in group policy management editor. Here we can deploy the software under computer configuration or in the user configuration or in both. If we configure under computer only and user logs in through another computer in that domain, it will not work. So, if we really want to make attach the user to that software we can deploy under user. From either option as required we can select **policies > software settings > software installation** , here right click in the right side and click new followed package it will open the file explorer. In the path type the shared file path, which will open the file to open.

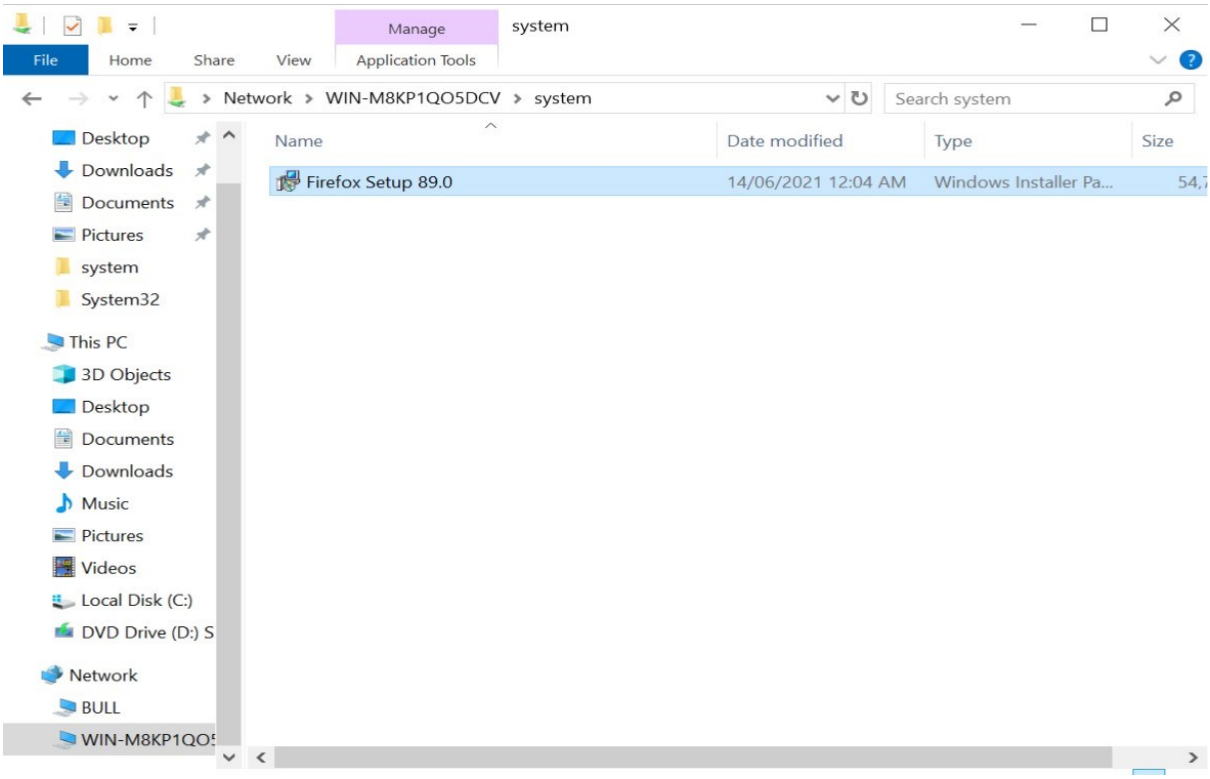


Fig 1.7 software deployment to GPO.

After adding the package click the package for edit the default options, we can add other package in upgrades tabs adding different GPO if we need to update it from Active Directory.

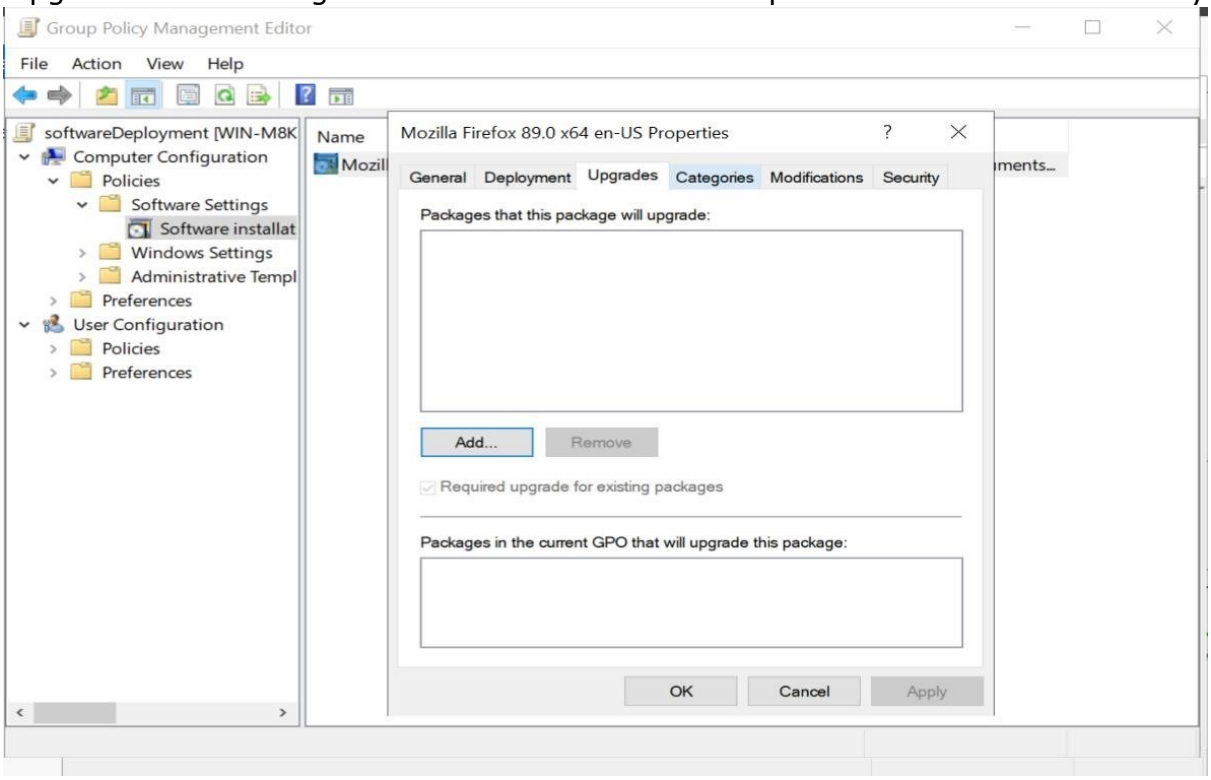


Fig1.8: Deploying software for OU.

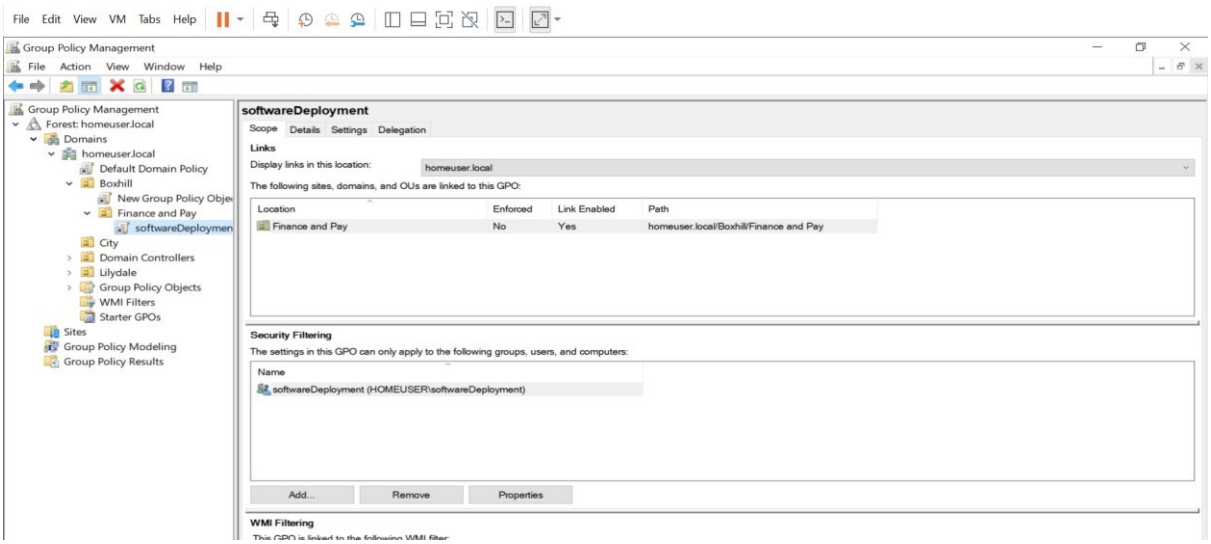


Fig 1.9: Verifying software deployment in GPO.

Deploy mandatory corporate wallpaper

To maintain mandatory corporate wallpaper in staff's computer, from domain controller let's pick a mandatory wallpaper and put it into shared folder giving access to everyone. We can assign this policy in OUs like (boxhill, Lilydale and City) so it will be applied to all the computers. If we do not want any departments to have this wallpaper setup we can simply disable the inheritance in that OU. In OU Boxhill right click create GPO in this domain and link here. It can be set either in computer or in users, here we will set it to user's fort that we have to go **user configuration > Policies > Administrative Templates > Desktop > Desktop** Wallpaper. Here we will enable this feature and in the path to the wallpaper put the shared path of the wallpaper in the network. Apply the changes and we made everyone inside Boxhill to have mandatory wallpaper.

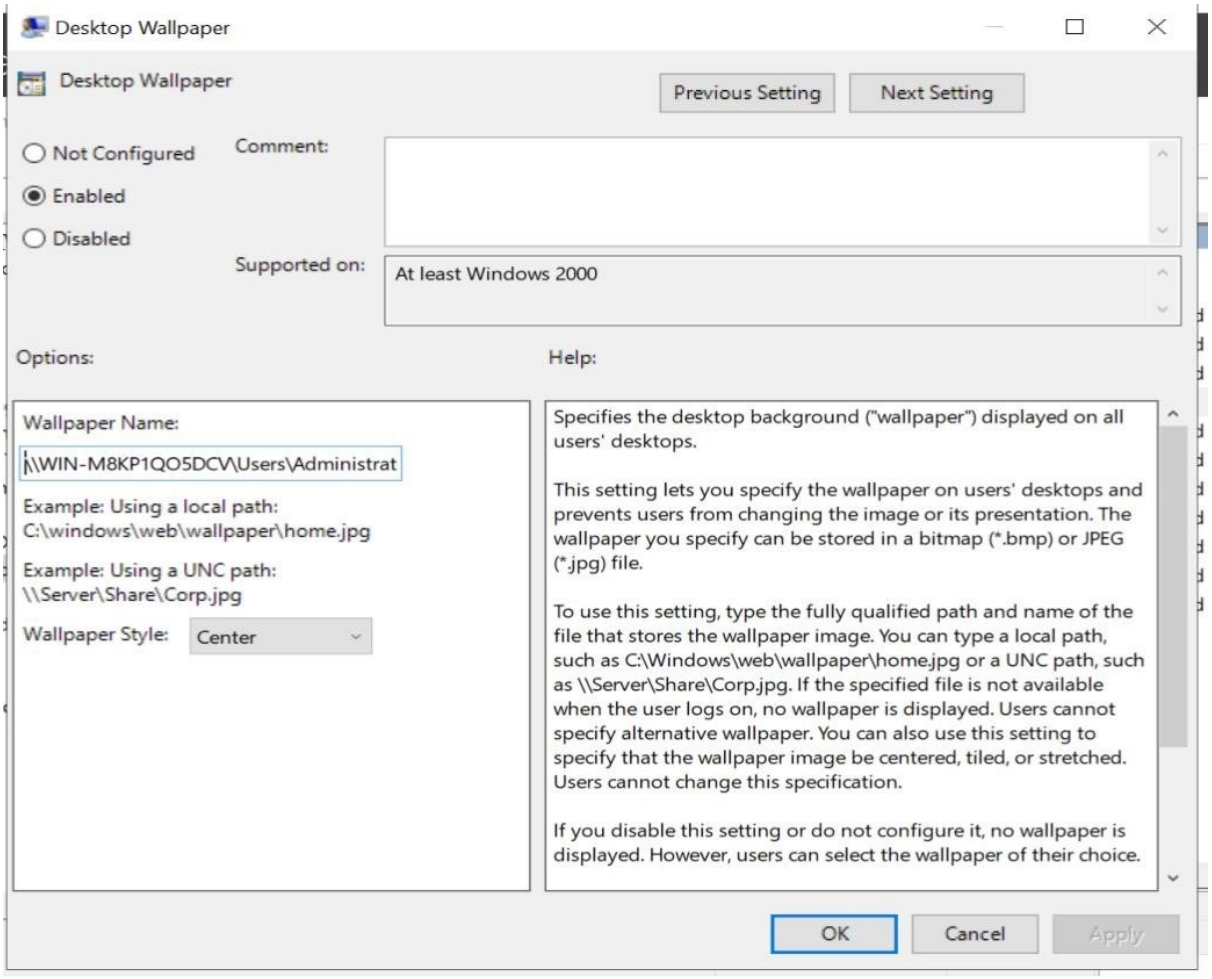


Fig 1.10 Change wallpaper in all staff's computer.

Restrict access to websites

To allow the default setting for internet in staffs computer we will not configure any properties for internet. But Students should be restricted to use some sites for that we will create and link a Group Policy under students OU.

For this create a gpo named (for eg: restrictWebsite). Enter Group Policy editor console by selecting the gpo , right click and clicking edit. Now from here, **user configuration > Policies > administrative Templates > Windows Component > Internet Explorer > Internet Control Panel > security Page > Site to Zone assignment** List. Enable this feature and enter zone assignments by clicking show button. Here enter the Url to restrict in value and value 4, which will restrict the user to enter that site.

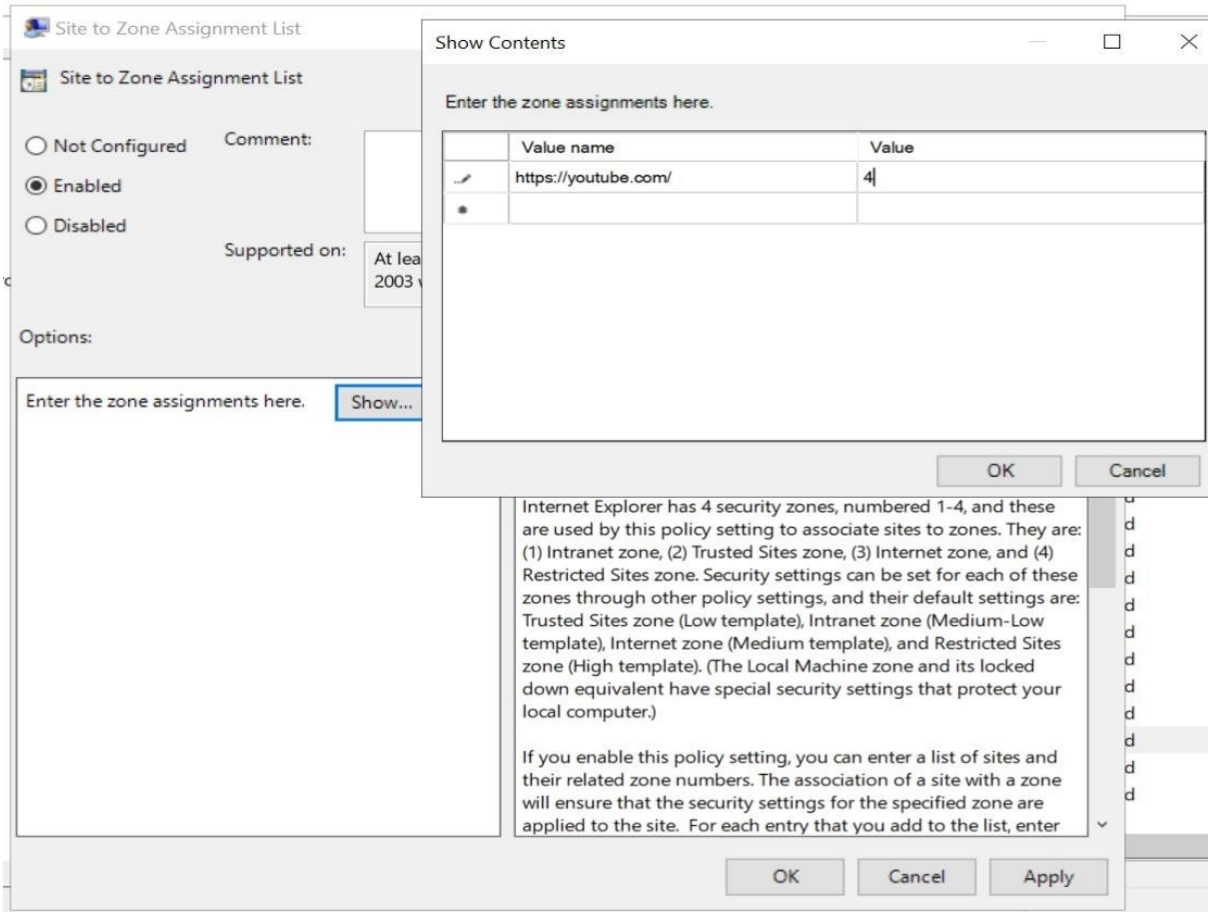


Fig 1.11 Restricting website to access for an OU.

Restrict desktop changes

To restrict to change the desktop changes and display characteristics for students we can create a GPO for ex: restrictDisplayChange and in group Policy Editor click **computer configuration > Policies > Administrative Templates > Desktop > Desktop > prohibit changes**. Enable this feature.

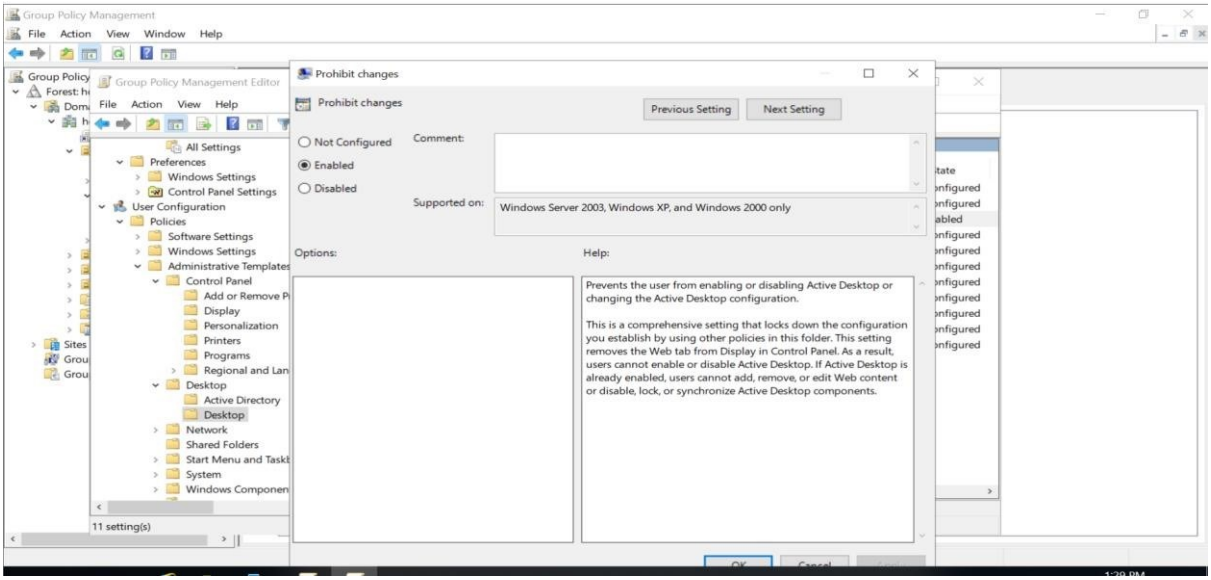


Fig 1.12 Prohibit access to desktop changes.

To restrict the display settings, click control panel in administrative templates and click display enable 'Disable the Display Control Panel'. It will restrict the users to access the display settings. For the mandatory wallpaper we have already setup in boxhill OU which will be inherited to student OU as well.

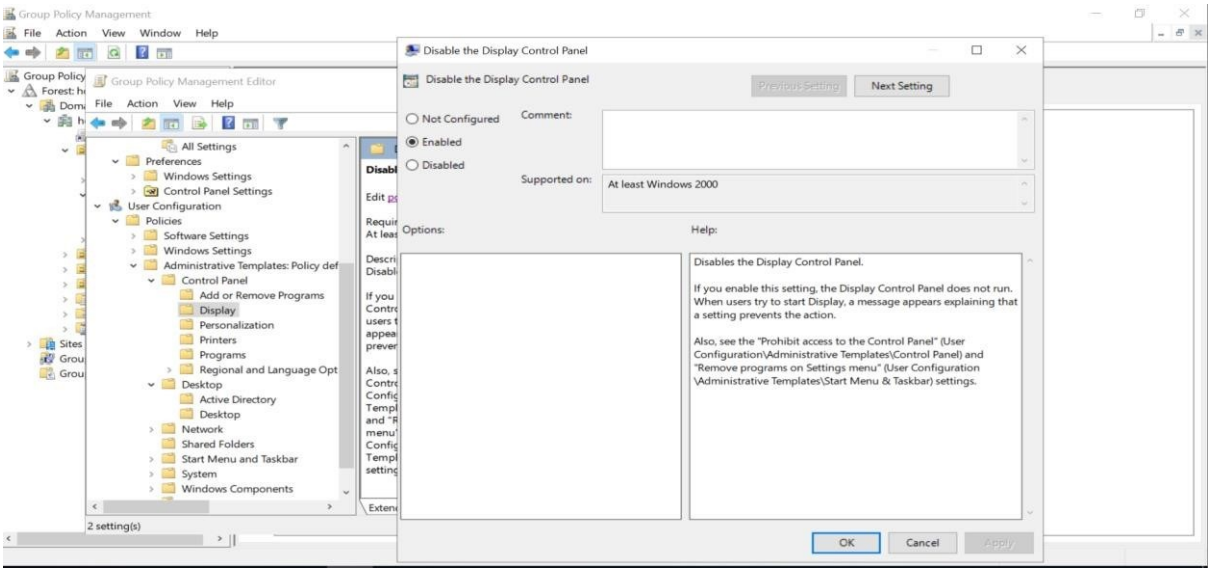


Fig 1.13 Restrict display settings:

Provide secure Environment and delegate a member for an OU.

Also providing secure environment for the HR we can delegated a member to look after the policies related to the HR. For the network security we can enable firewalls on the computers used in the HR department.

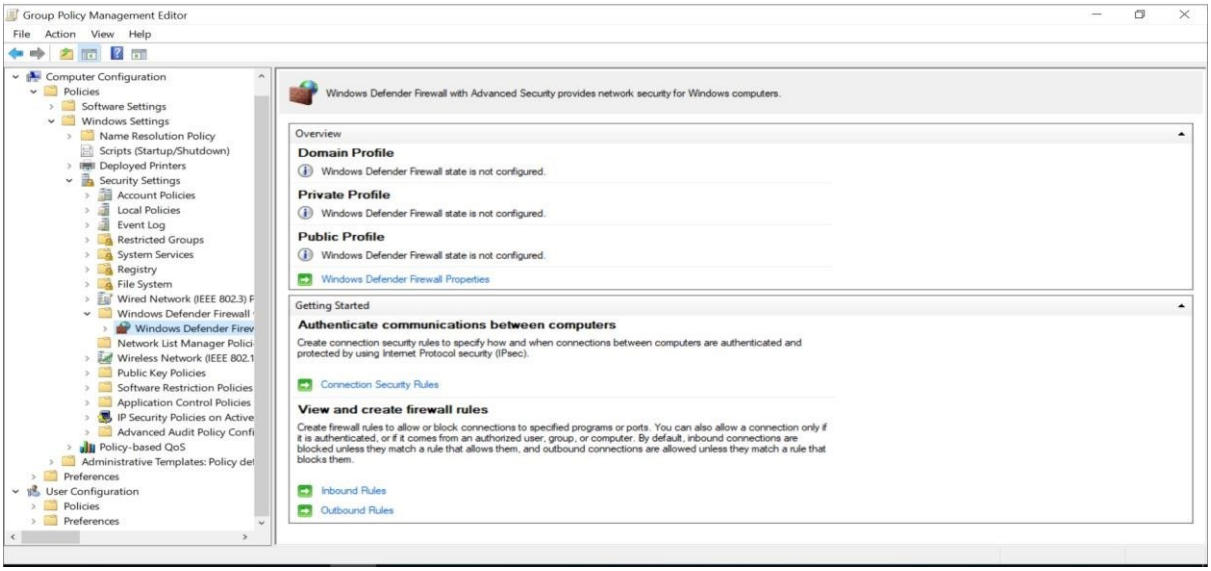


Fig 1.14: Firewall setting template in GPO.

In summary, single domain structure for boxhill organization was adjustable in simpler view as it is easy to set up, need less resources which can be cheap way of domain setup. We can have one single domain controller and one backup domain controller for the purpose of redundancy and fault-tolerance.

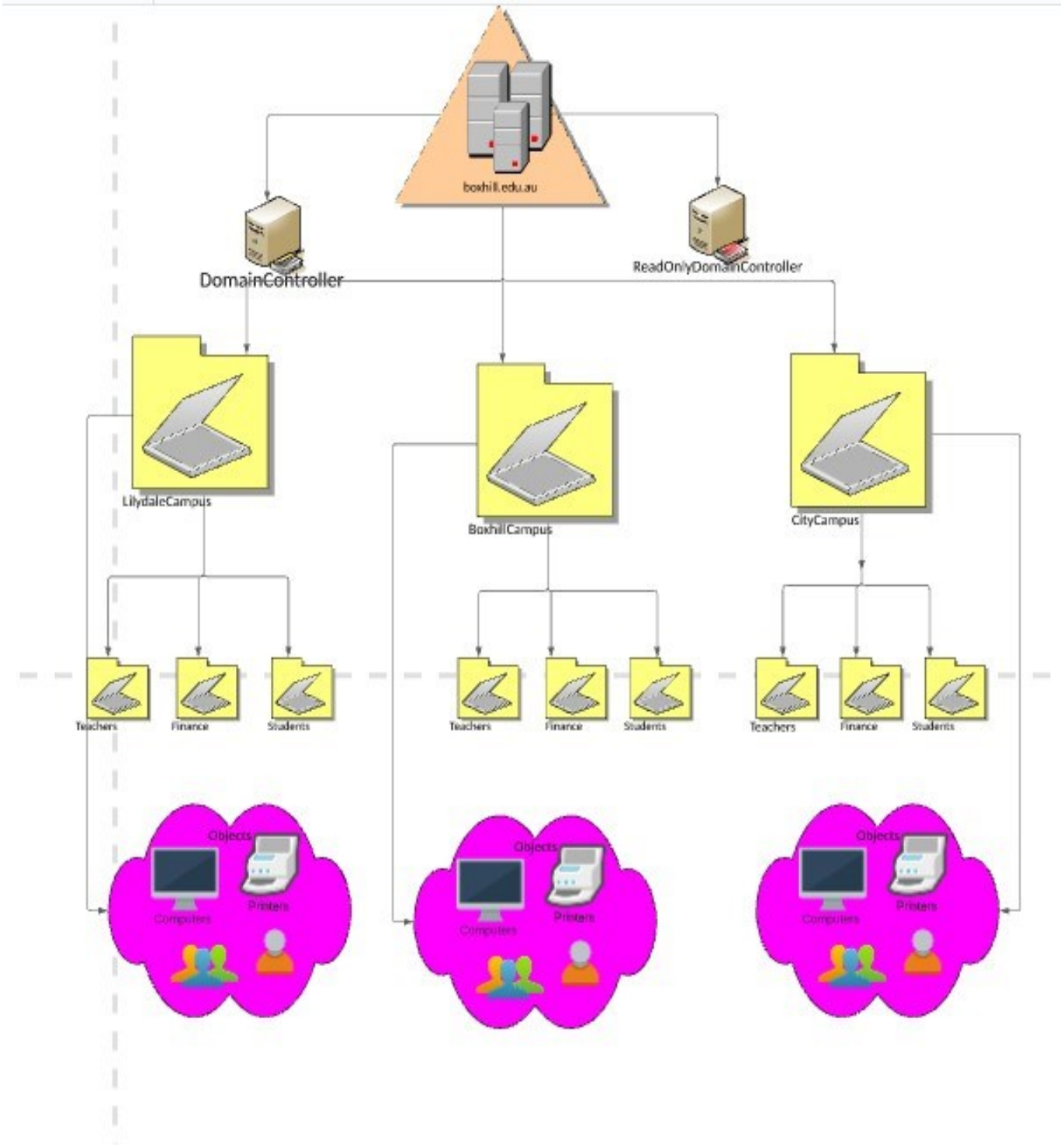


Fig 1.15: Design of Active Directory