**MCSE 1 Lecture 7**

**Local and Domain User Accounts**

**Peer-to-Peer (ptp) Networks vs Client-Server Networks**

**Peer-to-Peer (ptp) or Workgroup Model**

A typical peer-to-peer network consists of a number of workstations. The network may even contain some servers that perform services like DNS, DHCP, WINS, etc. An example of a ptp network is the computer set up you probably have at home. Most people have a router which allows them to connect more than 1 computer to the internet modem supplied by the ISP, (Shaw, MTS, etc.)

The computers in your home form a ptp network. They are all on the same network address and can therefore share resources (files and printers).

There is no centralized control of accounts or resources. All computers are considered equals; thus the name “peer” is used in describing this type of network.

Workgroup or ptp networks do not scale well. Microsoft recommends that the workgroup model should not exceed 10 hosts. This means ptp networks are small. Each user needs an account on each computer that he has to log in at. If you have 10 computers with 10 users and no one is assigned to any particular computer, you would have to have 100 accounts in the network; 10 on each computer.

If a user changes his password on one computer, he must change his password on the other 9 computers. This is a lot of administrative overhead which is prone to error.

**Advantages of a peer-to-peer network over a client-server network**

**Cost** – no need to purchase a server operating system and CALs.

**Administrator’s level of knowledge**– the administrator does not have to know as much about networking as he would if it was a client-server network.

**Client-Server or Domain Model**

A client-server network consists of workstations (clients) which are controlled by servers. There is at least 1 domain controller that allows users to log into the domain. An administrator can control thousands of client machines from 1 server. When networks get large, (more than 10 workstations), a client-server network should be employed.

In a client-server or domain network, each user has 1 account located on a server called a **domain controller**. Users can log into their domain accounts and then be granted access to resources on any computer in the network without requiring an account on each computer they access.

The administration of many client computers and many user accounts is centralized to save manpower and reduce errors. For instance, in a ptp network of 8 computers, if you want to install the Office Suite you would have to go to each of the 8 computers with the installation DVD and sit there while the program installs 8 times.

With a domain network, you can install the software on a server and then automatically have the Office Suite install on the clients when they are turned on. You can have 100’s of workstations installed with the Office Suite without having to do anything more than place the software on a server and create a group policy to install the software to selected computers or selected users.

**Advantages of a client-server network over a peer-to-peer network**

**Administration** - Makes it possible to take care of many clients, from 1 centralized location, with a minimal amount of administrative overhead.

**Scalability** - Whether you have 10 or 100 workstations to administer, the amount of work is almost the same.

**User Accounts**

**Local user account**

This type of account only has significance on the computer the account was created on. The authentication credentials reside in the **Security Account Manager (SAM)** database. This is the type of account used in a ptp network.

**Domain user account**

This account allows the user to gain access to resources anywhere in the domain. The user only requires 1 account no matter which computer in the domain she logs in at. The authentication credentials reside on a special type of server called a **Domain Controller**. The database on the domain controller which contains the credentials is called **Active Directory**.

**Built-in user accounts**

Built-in accounts exist in both a ptp network and a domain network. They are accounts that are preconfigured with the permissions and rights that allow the owner of the account to perform special tasks. These accounts are created when the operating system is installed. Two important built-in accounts are **Administrator** and **Guest**.

**Local User Account Types**

There used to be 3 levels of local user accounts; Limited, Standard and Administrator. With XP the limited account had the least amount of rights. The administrator account had full rights to do anything on the local computer. The standard account fell somewhere between the limited account and administrator account.

With Windows 7 and later operating systems there are still 3 types of local user accounts but that is just for backward compatibility. The standard account no longer has any more rights than the limited account.

**Limited user Account**

member of the **Users** group

can change his own password

full control over his own data

can only run programs that do not change the operating systems settings

**Standard user Account**

member of the **Power user** group

Same rights as the limited account.

**Administrator Account**

member of the **Administrators** group

can do anything

You can change a user account from one level to another by making it a member of a different group. In figure 1, if we add Mary White to the **power user** group, she would have a **standard** account.

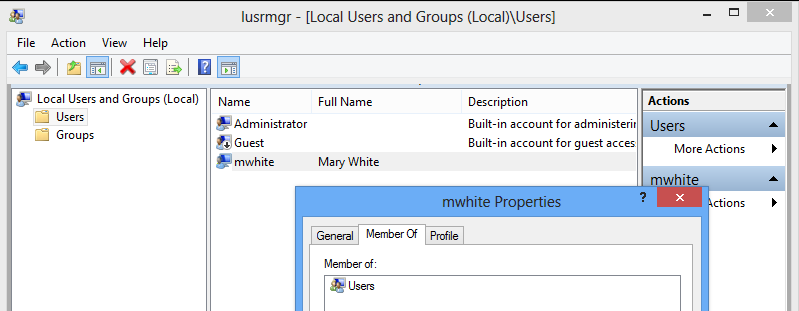
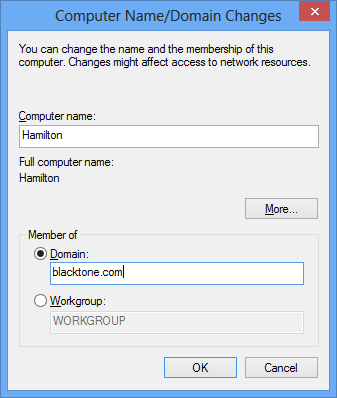


Fig. 1 mwhite is a member of the **Users** group making her a limited user

You can see in figure 1, the default user account when creating a new user is to make a **Limited** account.

****You can also create a **Microsoft account**. Most people already have a Microsoft account such as your email on hotmail.com or Live.com. You can log into your computer with your Microsoft email address and password. This gives you access to “cloud” technology. You can store files on the Microsoft servers, have access to Microsoft applications, and upload your pictures and music to the cloud. You can then access your personal information from any computer, tablet, or phone.

**Joining a Domain**

When a computer joins a domain an account is created for the computer in the **Computers** container in Active Directory. By having an account assigned to the computer, it can be controlled by domain group policies.

Anyone who has an account in Active Directory can join up to 10 computers to the domain. The administrator can raise or lower this number or remove the privilege all together. Usually, the administrator removes this right since it could constitute a threat to the network.

Someone might join a computer to the network Fig. 2 Joining the domain

that was infected with a virus which would then

infect the network. To join a computer to a domain click on **Start,** right-click on **Computer**, click on **Properties**, and click on the **Computer Name** tab. Then click on the **Change** button. Figure 2 should be visible.

When a computer joins a domain, a computer account is created for the computer in the **Computers** container in Active Directory Users and Computers. In figure 3, you can see there is an account for Halifax and Ottawa after they joined the domain.

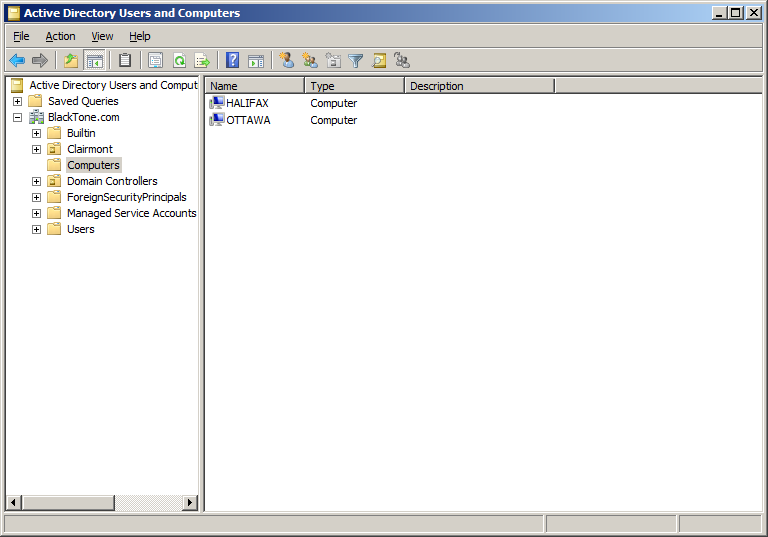


Fig. 3 Ottawa and Halifax have joined the domain and accounts

have been created for them in Active Directory.

If the computer has not joined a domain, the user will not be able to log into the network even if the user has a valid domain user account.

**Logging into the server**

Only the administrator or a member of the administrators group can log in on a domain controller. This is a security issue. You don’t want just any user being able log into a domain controller.

Figure 4 shows what happens when a user who is not an administrator tries to log into a domain controller.

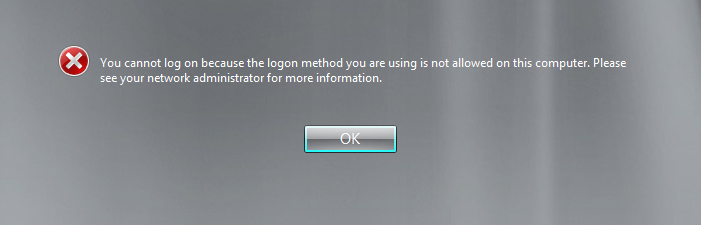


Fig. 4 The results of a non-administrator trying to log onto a domain controller

Member servers have local accounts like workstations. Domain Controllers do not have local accounts. Users must have an administrator domain account to log directly on a domain controller.