Injibara University

College of Engineering and Technology

Department of Information Technology

Network and System Administration (CoSc 4036)

Chapter Two: Account and Security Administration

Contents

- **Account and security Administration**
  - ✓ **User accounts**
  - ✓ **Workgroups**
  - ✓ **Domains**
  - ✓ **Domain controller**
  - ✓ **Active directory**
  - ✓ **Security**
- **Managing files and folder permission**

Workgroups

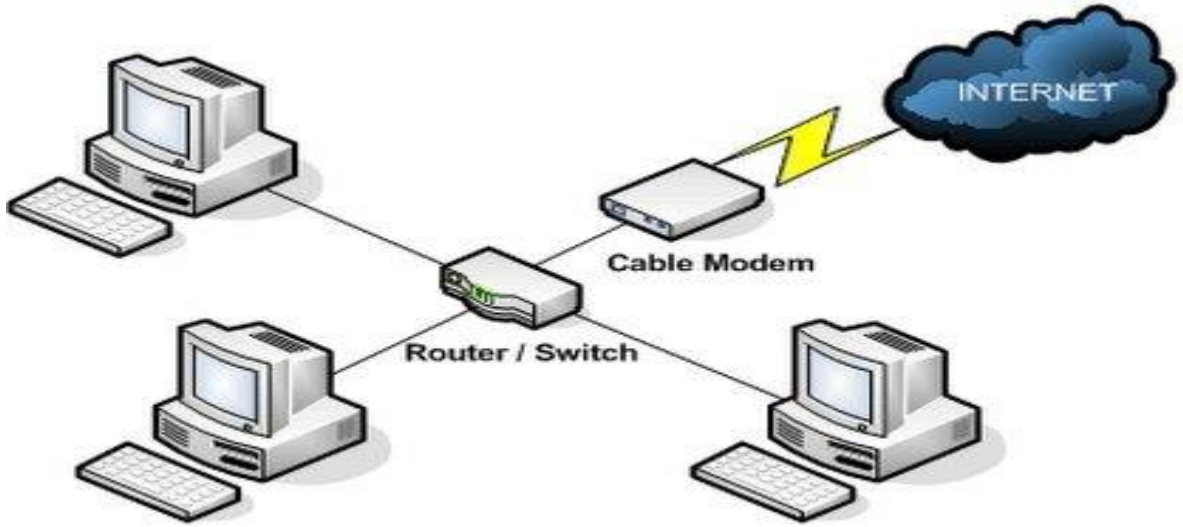
- In computer networking, a **workgroup** is a collection of computers on a local area network (LAN) that share common resources and responsibilities.
- Workgroups provide easy sharing of files, printers and other network resources.
- Workgroup is being a **peer-to-peer (P2P)** network design.
- Each workgroup computer may both **share and access** resources if configured to do so.
- **Workgroups** are designed for small LANs in homes, schools, and small businesses.
- Workgroup, for example, functions best with 15 or fewer computers.

Cont …

- As the number of computers in a workgroup grows, workgroup LANs eventually become too difficult to administer and should be **replaced** with alternative solutions like **domains** or other **client/server** approaches.
- A workgroup is a grouping of computers that are connected to each other over a network.
- This grouping is handled within the **Microsoft Windows operating system**, where the members of the workgroup assume **the same workgroup name** (though each computer in a workgroup must have a **unique computer name**).
- Computers in a workgroup communicate directly with each other and **do not require a server** to manage network resources.

Cont …

- Once a workgroup has been created, it is visible in **My Network** Places (available from the desktop in Windows).



- **Fig: Workgroup computers**

Adding a Computer to your Workgroup

- After the set up of your **network and workgroup**, you can **add computers** to the workgroup.
- The **procedure** varies slightly for different Microsoft Windows operating systems.
- Be sure to enter the **same workgroup names** on all computers you are adding to the workgroup.
- So that they appear together in **My Network** Places.
- Here are procedures for adding computers to a workgroup.

To specify a computer's Workgroup in Windows 10 operating system

- Click Start →This PC → Right click on This PC → Advanced System Settings → Computer Name → Change.
- Click Change, and then in the **Workgroup box**, enter the name of the workgroup you want to join.
- If you want to **rename your computer** so that it's easily recognizable among the other computer names in My Network Places, enter a new name in the **Computer name** box.
- However, be aware that some **internet connections** require a specific computer name.
- If your Internet service provider (ISP) has assigned you a computer name to use, **do not change it**.

Workgroup and Computer Naming Conventions

- When you create names for your workgroup or computer it's important to note some specific naming conventions.

Workgroup names

A workgroup name must:

✓ Be **the same** for all computers in the workgroup.

✓ Be different from any computer name in the workgroup.

✓ Usually be fewer than **16 characters**.

✓ Usually not contain any of the following characters: **; : " < > * + = \ | ?,**

Cont …

Computer names

A computer name must:

- ✓ Be unique in the workgroup (no other computer in the workgroup can have the same name).
- ✓ Be different from the workgroup name.
- ✓ Usually be less than 16 characters.
- ✓ Usually not contain any of these characters: ; : " < > * + = \ | ? ,
- ✓ Under some circumstances, be all uppercase.

Cont …

Limitations and considerations while renaming a computer name

- A computer can be renamed only by the **administrator** of the computer.
- If a computer is a member of an **Active Directory domain,** it should be removed from the domain before it is renamed.
- Although Windows prompts administrators to **restart** the computer after renaming, it should be restarted **manually** before making any further modifications.
- In most cases renaming a computer **does not affect the policies** that have been applied on it.

Cont …

- The **IP address** of the computer should also be modified accordingly.
- After you have established your workgroup and computer names, you can set up **file sharing** among the files, folders, and printers in your workgroup.
- To be able to access your workgroup and its shared resources, you must be **logged on** to the network.

Domain and workgroup

- **Domains**, and **workgroups** represent different methods for organizing computers in networks.
- The main difference among them is how the computers and other resources on the networks are managed.

In a workgroup

- All computers are peers; **no computer has control** over another computer.
- Each computer has **a set of user accounts**.
- To log on to any computer in the workgroup, you must have an account on that computer.
- There are typically no more than **twenty computers**.
- A workgroup is not protected by a password.
- All computers must be on the same **local network or subnet**.

Cont …

In a domain: one or more computers are **servers**.

- Network administrators use servers to control the **security and permissions** for all computers on the domain.
- This makes it easy to **make changes** because the changes are automatically made to all computers.
- Domain users must provide a **password** or other credentials each time they access the domain.
- If you have **a user account on the domain**, you can log on to any computer on the domain without needing an account on that computer.
- You probably can make only **limited changes** to a computer's settings because network administrators often want to ensure consistency among computers.
- There can be **thousands** of computers in a domain.
- The computers can be on **different local networks**.

Disadvantages of a domain

- One and only, but the major, disadvantage of having a domain oriented network environment is that it has a **single point of failure**.
- This means that if the **domain controller fails** because of any reason, the entire network goes down, and comes up only when the domain controller starts working properly again.

Considerations before Adding a Computer to Domain

- The client computer must have **a unique hostname** in the network assigned to it.
- The client computer must have **a static IP address** assigned to it.
- The client computer must be provided with **correct DNS address**.

How to add a client computer to the domain

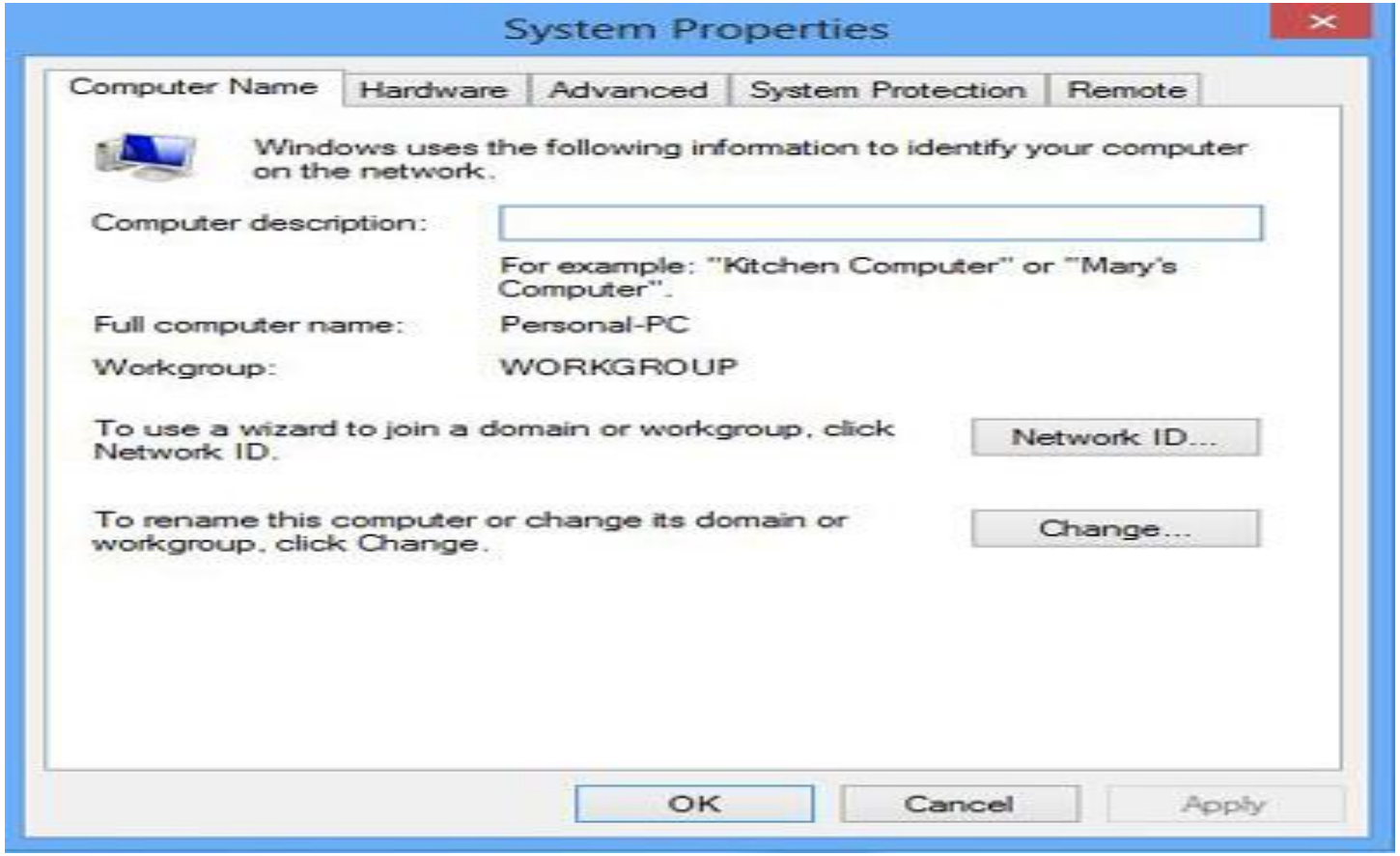
- To add a **Windows 8** computer to domain, steps below must be followed.
- Use the credentials of **local administrator account** to log on to Windows 8 computer, that is to be added to the domain.
- Click **Desktop** tile from the **Start** screen to go to the desktop.
- Once on the desktop screen, click **File Explorer** icon from the taskbar.
- On the **Libraries** window, right-click **Computer** icon from the left pane.
- From the context menu that appears, click **Properties**.
- On the **System** window, click **Change settings** option under **Computer name, domain, and work settings** section from the right pane.

Cont …


System
Control Panel
System and Security
System
Search Control Panel
Control Panel Home
Device Manager
Remote settings
System protection
Advanced system settings
Windows edition
Windows 8 Pro
© 2012 Microsoft Corporation. All rights reserved.
Get more features with a new edition of Windows
Windows 8
System
Rating:
4.7 Windows Experience Index
Processor: Intel(R) Core(TM) i7 CPU Q 720 @ 1.60GHz 1.60 GHz
Installed memory (RAM): 2.00 GB
System type: 64-bit Operating System, x64-based processor
Pen and Touch: No Pen or Touch Input is available for this Display
Computer name, domain, and workgroup settings
Computer name: Personal-PC
Change settings
Full computer name: Personal-PC
Computer description:
Workgroup: WORKGROUP
See also
Action Center
Windows Update
Performance Information and Tools
Windows activation
Windows is not activated. View details in Windows Activation
Product ID: 00178-10140-00000-AA486

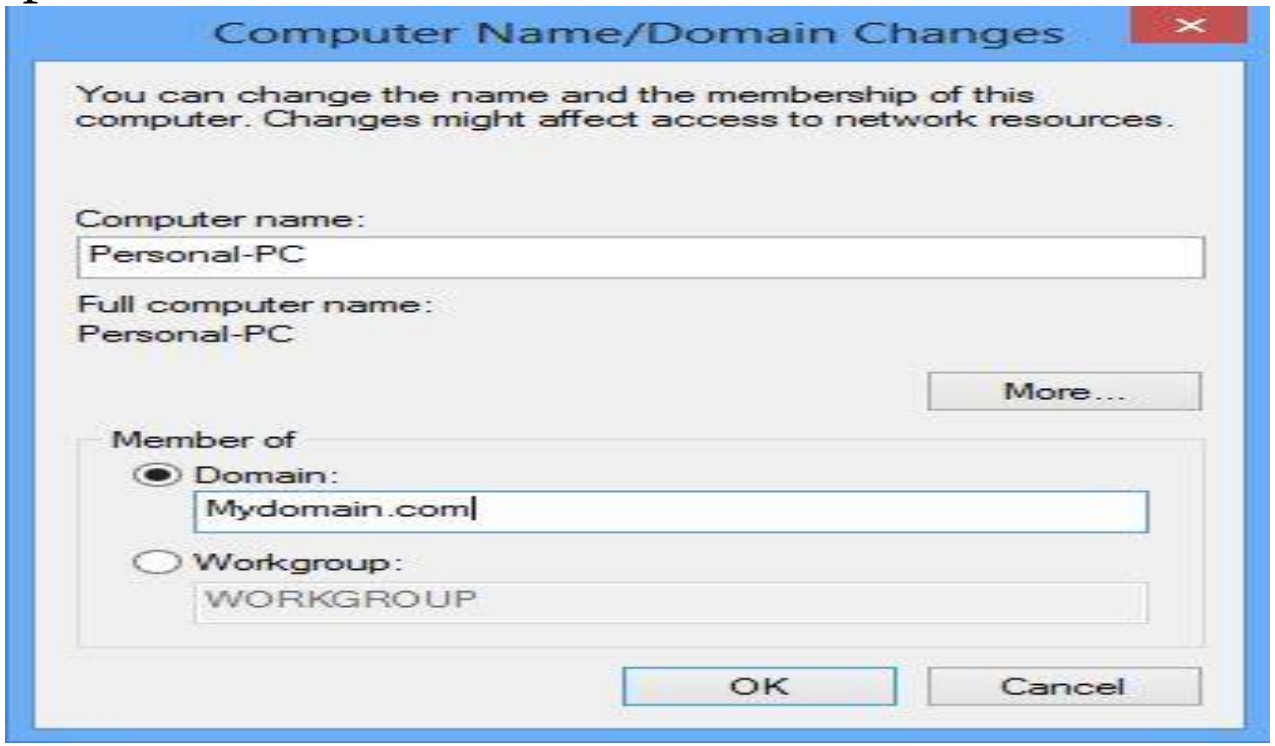
Cont …

- Click Change Settings
- On the **System Properties** box, ensure that **Computer Name** tab is selected.
- Once the tab is selected, click **Change** button.



Cont …

- Click **Change.**
- On the **Computer Name/Domain Changes** box, click to select **Domain** radio button under **Member of** section.
- In the enabled field, specify the fully qualified domain name (**FQDN**) of the domain to which the computer is to be added.



Cont …

- Specify Domain Name.
- On the **Windows Security** box, provide the name and password of the domain administrator or **domain user account** in the respective fields.

Cont …

- Specify Domain Admin Credentials
- Once done, click **OK** button.
- On the displayed welcome message box, click **OK**.
- Click **OK** on the next displayed box.
- Back on **System Properties** box, click **Close** when done.
- On **Microsoft Windows** box, click **Restart Now** button to restart the Windows 8 computer automatically in order to allow the changes to take effect.

Domain Controller

- **A domain controller** is a computer running Microsoft Windows Server 2008 that stores a **replica of the domain directory.**
- **A domain controller (DC)** is a **server** that handles **all the security requests** from other computers and servers within the **Windows Server domain**.
- Security requests include requests to **login to another server** and checking permissions for various functions that need to be performed (e.g., accessing a file, folder on a server or modifying a file within a folder).

Cont …

- The **domain controller** originated in **Windows NT** and managed the access to various resources **granted to users and other servers** through the use of a username and password.
- A **domain controller (DC)** is a server that responds to security authentication requests (logging in, checking permissions, etc.) within the Windows Server domain.
- A domain is a concept introduced in Windows NT whereby a user may be granted access to a number of **computer resources** with the use of a **single username and password combination.**

Cont …

- Having more than one domain controller in a domain provides **fault tolerance**.
- If one domain controller is offline, another domain controller can provide all of the required functions, such as recording changes to the **Active Directory service**.
- Domain controllers manage all aspects of users.
- Domain interaction, such as locating **Active Directory objects** and **validating user logon attempts**.
- In Windows NT, there was a **primary domain controller** and a **backup domain controller**.
- The **primary DC** focused on **domain services** only to avoid the possibility of a system **slow down or crash** due to over tasking from managing other functionality and security requests.

Cont …

- In the event of a primary DC going down, **a backup DC** could be promoted and become the primary DC to keep the rest of the server systems functioning correctly.
- Since Windows 2000, the need for **primary and backup DCs** was nearly eliminated because of the introduction of **Active Directory (AD) and multi-master replication**.
- **Primary Domain Controller,** a server in a Windows NT network that maintains a **read-write directory** of user accounts and security information.
- The PDC authenticates usernames and passwords when members log into the network.
- **Members** only have to log into **one domain** to access all resources in the network.
- In **a trusted relationship**, one domain may gain access to other domains.
- In this case, members who **log into the first domain** will have access to the resources in **the other domains**.

Cont …

- **Backup Domain Controller (BDC)** is a computer that has a copy of the user accounts database.
- Unlike the accounts database on the **Primary Domain Controller** (PDC), the BDC database is a **read-only copy.**
- When changes are made to the master accounts database on the PDC, the **PDC pushes** the updates down to the **BDCs**.
- Most domains will have at least **one BDC**, and often there are **several BDCs** in a domain.
- These additional domain controllers exist to provide **fault tolerance.**
- If the PDC fails, then it can be replaced by a BDC.
- In such circumstances, an **administrator promotes** a BDC to be the **new PDC**.
- BDCs can also authenticate user logon requests and take some of the authentication load from the PDC.

Trust relationship between two different domains

- **Trust:** A relationship between different **domains** or **forests** that allow **sharing of resources** between them.
- **Trust can be transitive or non-transitive**.
- **Transitive Trust:** Trust which can be extended to **other domains in the forests**.
- **Non- Transitive Trust:** Trust which cannot be extended to other domains in the forests, it is only between the **two domains of different forests**.

Types of Trusts

- There are several different types of trusts in Windows Server 2003/2008.
- These are listed below:
- **Shortcut trust:** A shortcut trust is used to improve user **logon times** between two domains which are logically distant from each other in the **Active Directory hierarchy**.
- This trust is created **manually** and **is transitive**.
- It can also be either **one-way or two-way**.
- **External trust:** An external trust is a trust created **manually** between domains in **two separate forests** or between a **Windows Server 2008 domain** and **a domain running Windows NT 4.0** or earlier. External trusts are **not transitive** and can be either one-way or two-way.

Types of Trusts

- **Realm trust:** a realm trust is a **trust** created **manually** between a Windows Server 2008 domain and domain running a **non-Microsoft** implementation, e.g. UNIX. This trust can be transitive, non-transitive, one-way or two-way.
- **Tree-root trust:** A tree-root trust is created **automatically** between a **new tree and its root** domain. This trust is **transitive and two-way** by default.
- **Parent-child trust:** a parent-child trust is created automatically between a child and its parent domain.
- This trust is transitive and **two-way by default**.
- **Forest trust:** A forest trust is created manually between **two Windows Server 2008** forests.
- The trust allows **all domains** in one forest to trust **all domains in another forest**, however a forest trust is **not transitive** across three or more forests.
- This trust can be either one-way or two way.

Cont …

- Configure the **scope of authentication** between two domains for manually creating forests.
- You can either allow **domain-wide authentication** where every computer in the domain is trusted, or you can use **selective authentication** where only a selected number of computers are trusted.
- If you apply **selective authentication** to a trust, then you will need to **manually configure** which users in the trusted domain can authenticate with specific computers in the trusting domain.
- Each user or group can be added to the relevant computers' **Access Control Lists**, which can be configured with the "**Allowed to Authenticate**" permission.

Direction of trust

- **One-way trust:** Network **A** trusts network **B**, and then network **B** can access network **A** only.
- **Two-way trust:** Network **A** trusts network **B**, and vice versa, then both networks A and B can access each other.

Active Directory

- An **active directory** is a **directory structure** used on Microsoft Windows based computers and servers to **store information and data** about networks and domains.
- An active directory (referred to as an **AD**) does a variety of functions including:
  - ✓ The ability to **provide information** on **objects** (users, applications, groups, devices).
  - ✓ Helps **organize these objects** for easy retrieval and access.
  - ✓ **Allows access** by end users and administrators.
  - ✓ Allows the administrator to **set security up** for the directory.
- An active directory can be defined as a **hierarchical structure** and this structure is usually broken up into **three main categories**.
- These are **the resources** which might include hardware such as printers, **services** for end users such as web email servers and **objects** which are the main functions of the domain and network.

Cont …

- It is interesting to note the **framework** for the objects.
- Remember that an **object** can be a **piece of hardware** such as a **printer, end user or security settings** set by the administrator.
- These objects can hold other objects within their file structure.
- All objects have an ID, usually an object name (folder name).
- In addition to these objects being able to hold other objects, every object has **its own attributes** which allows it to be characterized by the information which it contains.
- Most IT professionals call these setting or **characterizations schemas**.

Cont …

- Depending on the **type of schema created for a folder, it** will ultimately determine how these objects are used.
- For instance, some objects with certain schemas **cannot be deleted**, they can only be **deactivated**.
- Others types of schemas with certain attributes can be **deleted entirely**.
- For instance, a user **object can be deleted**, but the administrator object **cannot be deleted**.
- When understanding **AD**, it is important to know the **framework** that objects can be viewed at.
- In fact, an **active directory** can be viewed at either one of three levels.
- These levels are called **forests, trees or domains**.

Cont …

- The highest structure is called the **forest** because you can see all objects included within the active directory.
- Within the forest structure are **trees**, these structures usually hold **one or more domains**, going further down the structure of an active directory are **single domains**.

To put the forest, trees and domains into perspective, consider the following example.

- A large organization has many dozens of **users** and processes.
- The **forest** might be the **entire network of end users** and specific computers at a set location.
- Within this forest directory are **now trees** that hold information on specific objects such as **domain controllers, program data**, **system**, etc.
- Within these objects are even **more objects** which can then be controlled and categorized.

Cont …

- Some of the common tasks accomplished with **Active Directory Users and Computers** include:
  - ✓ **Adding new users to Active Directory.**
  - ✓ **Changing passwords.**
  - ✓ **Granting rights to file servers.**
  - ✓ **Allowing remote access to the network.**
  - ✓ **Setting login and logout scripts.**
  - ✓ **Restrict logon times.**
  - ✓ **Controlling when users can use the network.**
  - ✓ **Creating security groups - with either static or dynamic membership.**

Common Active Directory objects

- **Active directory objects** reside within each container.
- These objects represent **every resource** that has been added to your active directory.
- Objects appear on the **right pane** of the container.
- Microsoft has done a pretty good job of giving the objects **meaningful names**.
- You can usually quickly guess what an object does by its name.
- Example, the **DHCP Users object** is a group object containing members that have **read-only access to DHCP**.
- Microsoft has included **a description column** that tells you what each default object does.

Common Active Directory objects

- Each object is made up of a group of properties, which describe the object and what it can do.
- View the properties for an object by **right-clicking the object** and, from the resulting shortcut menu, selecting **Properties.**
- The kind of objects include:
  - ✓ **Computer objects**
  - ✓ **Group objects**
  - ✓ **User objects**
- Only the **default tabs** for each object will be discussed here.

Computer Objects

- The **computer object** describes **computers** that have rights on the network.
- It can describe **domain controllers, member servers, or workstations**.
- We can find domain controllers (DC) in the **Domain Controllers container**.
- Member servers and workstations will appear in the **Computers container**.
- When we right-click **a Computer object** and select **Properties**, we will see the screen shown in the following figure.

Cont …

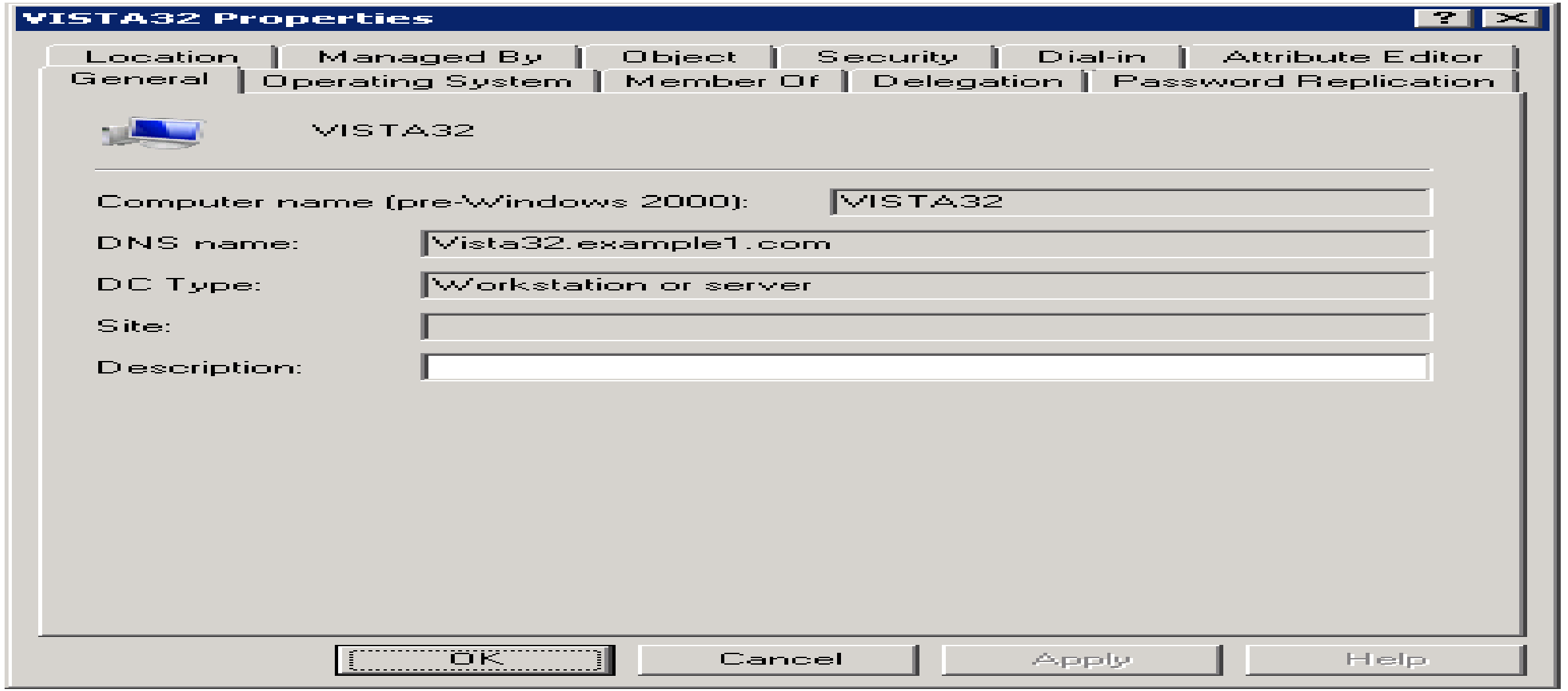


Figure: Properties of computer object in Active Directory Objects.

Tabs on the Computer Properties page

- **General**: this tab provides **basic information** about the object, including both its NetBIOS name, its DNS name, type, Active Directory site and description.
- **Operating System**: this tab will show you the **operating system running** on the computer and what service packs.
- **Member Of**: here, you can view the computer's **group memberships** and make any necessary adjustments.
- By default, all new computers are added to the group named **Domain Computers**.
- **Delegation**: In older versions of Windows Server, this information was located on the General tab.
- Select one of the '**trust**' options if you want the computer to be able to request services from another computer.
- **Password Replication**: The Password Replication tab holds a list of the **Read-Only Domain Controllers**.
- **Location**: Enter details describing the computer's **physical location**.

Cont …

- **Managed By**: provide information regarding the **staff person** responsible for the computer.
- You can quickly **assign someone** by selecting their information directly from Active Directory.
- **Object**: this tab displays information about the object including its name, when it was created, when it was last updated, and the **Update Sequence Numbers** for it.
- **Update Sequence Numbers** are critical components when it comes to handling Active Directory updates and keep things in check.
- On this tab, you can also indicate that the object should be protected from **accidental deletion**.

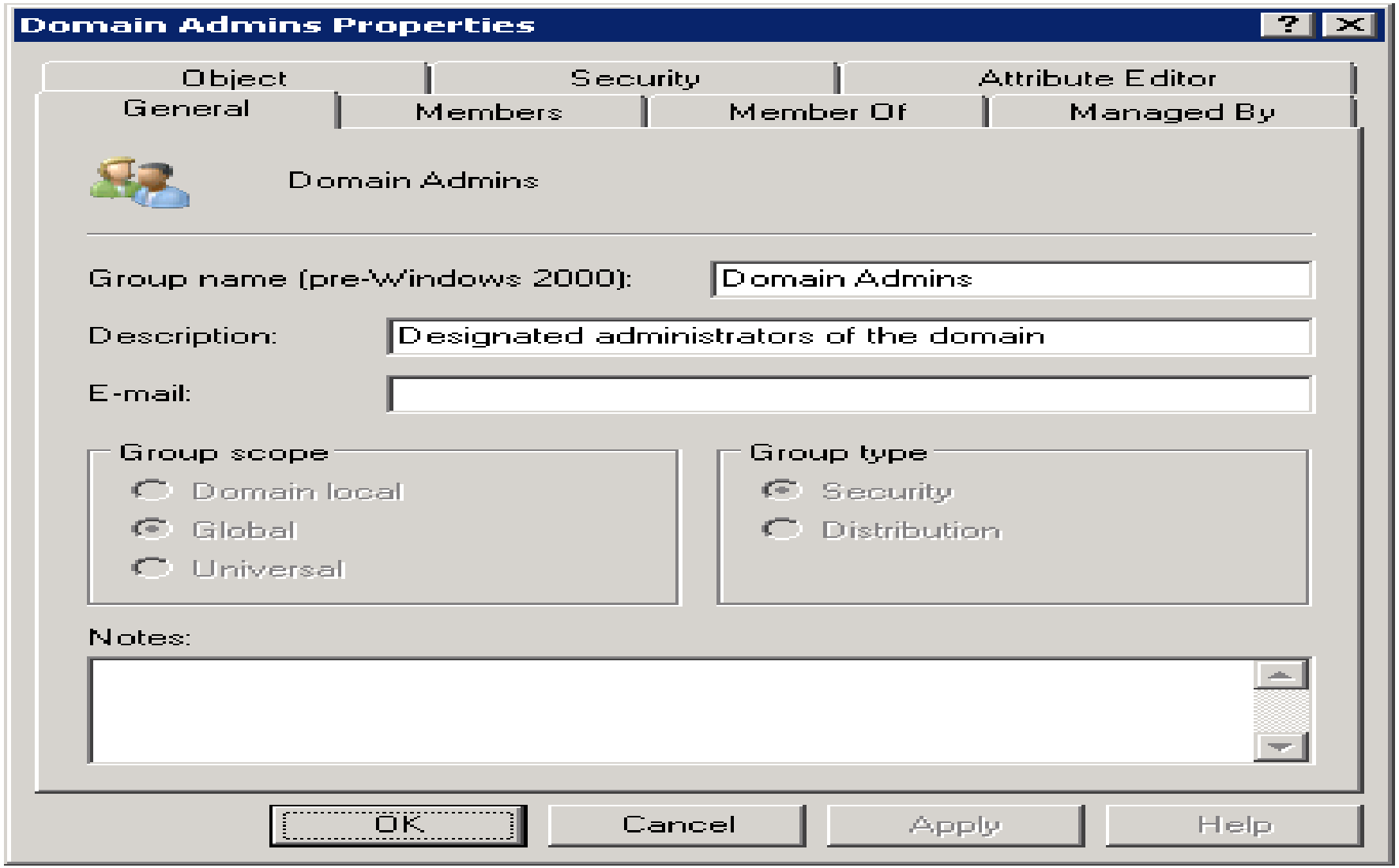
Cont …

- **Security**: this tab controls the **Active Directory rights** other objects have to this object.
- The **Group or user names box** lists the objects with rights; and the **Permissions box** describes the permissions the selected **user or group** has been granted or denied.
- **Dial-in**: decide whether or not users can remotely access the computer, whether by **dial-up or VPN**.
- **Attribute Editor (new tab in Windows Server 2008)**: allows you to directly **manipulate** all of the attributes associated with the selected object.

Group Objects

- There are a couple of kinds of group objects that can be created in Active Directory.
- The first kind, **the security distribution group**, provides a way to **manage access rights** for **multiple users** (or other objects) **all at once**.
- Rather than assign individual permissions to a file share, we can give rights to the **security group** and then **add and remove group members** as needed.
- **Security groups** can also be used as email distribution groups.
- The second kind of group, called a **distribution group**, is used solely as an **email distribution list**.

Cont …



- **Figure: Properties of group object in Active Directory Objects.**

Tabs on the Group object include:

- **General**: this tab displays information about the object.
  - ✓ You can view, but not change **Group Scope and Group Type** for Groups.
  - ✓ You can change all other fields on this page.
- **Member**: Here you can add and remove group members.
  - ✓ By clicking the Add button, you can add **individual objects** or select multiple objects.
- **Member Of**: This tab lists the **groups** that the object belongs to.
  - ✓ You can add or delete group membership here.
- **Managed By**: Here you can enter information about **who's in charge of the computer**.
  - ✓ You can quickly **assign someone** by selecting their information directly from Active Directory.

Cont …

- **Object**: this tab displays information about the object including its name, when it was created, when it was last updated, and the Update Sequence Numbers for it.

  ✓ On this tab, you can also indicate that the object should be protected from **accidental deletion**.

- **Security**: This tab controls the Active Directory rights **other objects have to this object**.

  ✓ The **Group or users box** lists the objects with rights and the **Permissions box** describes the permissions the selected object has.

- **Attribute Editor (new tab in Windows Server 2008):** allows you to directly **manipulate all of the attributes** associated with the selected object.

User Objects

- Users, after all, are the foundation of **your organization**.
- When we right-click a User object and select Properties, you'll see the screen shown in the following Figure.

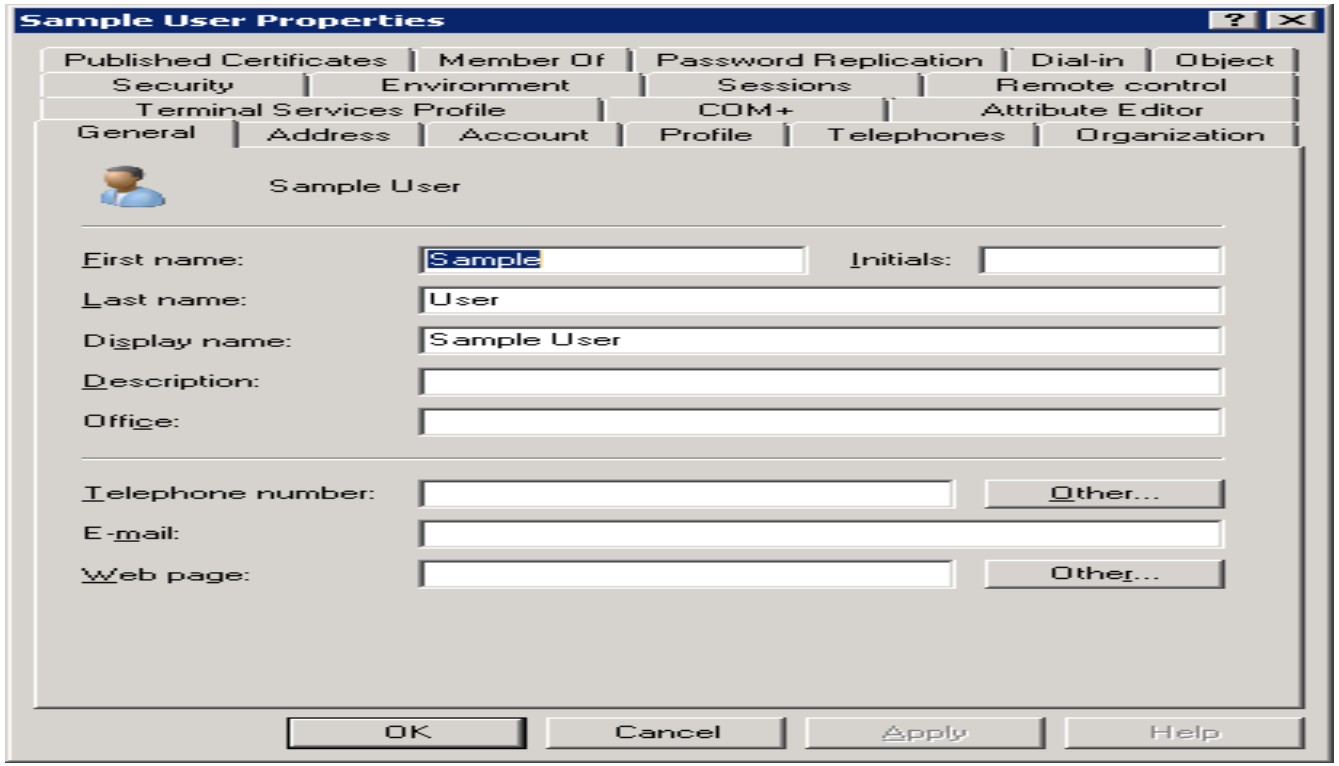


Figure: Properties of User Objects in the Active Directory Objects.

Tabs on User objects include:

- **General**: displays general descriptive information about the user, including name, email address and primary telephone number.
- **Address**: this tab displays **postal addresses** for the selected user.
- **Account**: the Account tab holds detailed account information for the user, including the **logon name** for the user and, via the **logon hours button** on this tab, account restrictions.
- The account options section gives you a way to force users to **change their password** at **next logon**, prevent them from changing passwords, require a Smart Card for logon, and enable **delegation** for the account.

Cont …

- We can use this page if the account **gets locked** out due to logon failures.
- Microsoft has made is easy **to unlock** accounts by adding an "**Unlock account**" option to this tab.
- **Profile**: the profile tab holds fields that specify the **paths** to any logon scripts the user needs to access.
- **Telephones**: this tab serves as a repository for any telephone numbers you have for the user such as **cell phones.**
- **Organization**: used to place information about the user's company, including job title, department, and company name.
  - ✓ We can also **link** the user to his or her **manager's Active Directory object**.
- **Terminal Services Profile**: this tab is similar to the Profile tab, but this only **controls profile information** for the terminal Services session, including **home folder location**.

Cont …

- **COM+**: You can assign the user to be part of a **COM+ partition** set here.
  - ✓ COM+ partition sets allow users in a domain to access COM+ applications throughout the domain.
- **Attribute Editor (new tab in Windows Server 2008)**: allows you to directly manipulate all of the attributes associated with the selected object.
- **Security**: this tab controls the Active Directory rights other objects have to this object.
  - ✓ The **Group or users box** lists the objects with rights and the **Permissions** box describes the permissions of the selected object.
- **Environment**: this tab controls the Terminal Services startup environment for the user.
- **Sessions**: the information on the Sessions tab helps you **control how the user interacts with Terminal Services**, including how long a session stays connected and what happens if a user disconnect from the server.

Cont …

- **Remote Control**: this tab indicates whether a user's Terminal Server session can be remotely controlled.
  - ✓ We can set options that allow you to establish **view-only sessions or that allow interaction**.
- **Published Certificates**: this tab allows you to **associate X.509 security certificates** with the user.
- **Member Of**: this tab lists the groups to which the user belongs; we can add or delete group membership here.
- **Password Replication (new tab in Windows Server 2008)**: the Password Replication tab holds a list of the **Read-Only Domain Controllers.**

Cont …

- **Dial-in**: On the Dial-in tab, we can decide whether or not users can **remotely access the network**, whether by dial-up or VPN.
- **Object**: this tab displays information about the object including its name, when it was created, when it was last updated, and the Update Sequence Numbers for it.
  - ✓ On this tab, you can also indicate that the object should be protected from **accidental deletion**.

Flexible Single Master Operations roles (FSMO)

- In fact, there are 5 Flexible Single Master Operation's roles (**FSMO**).
- These are also called **Operations Master roles** as well.
- The two terms are interchangeable.

The 5 roles and their function are:

- ***Domain Naming Master*** **-** there is only **one Domain Naming Master per forest.**

✓ The Domain Naming Master makes sure that when a new domain is added to a forest that it is **unique**.

✓ If the server holding this role is **offline**, it is impossible to make changes to the **AD namespace**, which includes things like **adding new child domains**.

Cont …

- ***Schema Master*** - There is only one **Schema Operations Master in a forest**.

✓ It is responsible for **updating** the Active Directory Schema.

✓ Tasks that require this, such as **preparing AD** for a new version of **Windows Server functioning as a DC.**

- **Infrastructure Master** - There is **one Infrastructure Master per domain**.

✓ If you only have **a single domain in your forest,** you don't really need to worry about it.

✓ If you have multiple forests, then you should make sure that **this role is not held by a server that is also a GC (Global Catalogue) holder unless every DC in the forest is a GC**.

✓ The infrastructure master is responsible for making sure that **cross-domain references** are handled properly.

✓ If a user in one domain is added to a group in another domain, the infrastructure master for the domains in question make sure that it is handled properly.

✓ This role **will not function correctly** if it is on a GC (global catalog).

Cont …

- **RID Master** - The Relative ID Master (RID Master) is responsible for issuing **RID pools to DCs**.

✓ There is one RID master per domain.

✓ Any object in an AD domain has a **unique Security Identifier (SID).**

✓ This is made up of a combination of the **domain identifier and a relative identifier**.

✓ Every object in a given domain has the **same domain identifier**, so the relative identifier is what makes objects unique.

- Each DC has a pool of relative IDs to use, so when DC creates a new object, it appends a RID that it hasn't used yet.
- Since DCs are issued **non-overlapping pools**, each RID should remain unique for the duration of the life of the domain.
- When a DC gets **to ~100 RIDs** left in its pool, it requests **a new pool from the RID master**.
- If the RID master is offline for an extended period of time, **object creation may fail.**

Cont …

- **PDC Emulator** - finally, we get to the most widely misunderstood role of them all, the PDC Emulator role.

✓ There is one **PDC Emulator per domain**.

✓ If there is a failed authentication attempt, it is forwarded to the PDC Emulator.

- The PDC Emulator is also the server that **controls time sync across the domain.**
- **All other DCs** sync their time from the **PDC Emulator.**
- **All clients** sync their time from the **DC** that they logged in to.
- It's usually trivial to **move these roles around**, so while some DCs do slightly more than others, if they go down for **short periods of time**, everything will usually function normally.
- If they're down for a long time, it's easy to transparently **transfer the roles.**

Current FSMO role holders

- Before transferring your FSMO roles to a new server you may want to know what current Domain Controller holds each FSMO role.
- There is a really easy way to do this from the command prompt.
- You can open **Active Directory Users** and Computers and **view the Operating Masters**
- The command prompt is the fastest easiest way.

Open Command Prompt

- Type **netdom query fsmo**

C:\>netdom query fsmo

- **Schema master ……..**
- **Domain naming master ……..**
- **PDC ……..**
- **RID pool manager ……..**
- **Infrastructure master ……...**

- The output above will give you a current list of all FSMO role holders.

Transfer FSMO Role Holders

- Microsoft recommends that you **transfer FSMO roles** in the following scenarios.
  - ✓ The current role holder is **operational** and can be accessed on the network by the **new FSMO owner**.
  - ✓ You are gracefully demoting a domain controller that currently owns FSMO roles that you want to assign to a specific domain controller in your Active Directory forest.
  - ✓ The domain controller that currently owns FSMO roles is being taken **offline** for **scheduled maintenance** and you need specific FSMO roles to be assigned to a "**live**" domain controller.
  - ✓ This may be required to **perform operations** that connect to the FSMO owner.
  - ✓ This would be especially **true** for the ***PDC Emulator*** role but **less true** for the RID master role, the Domain naming master role and the Schema master roles.

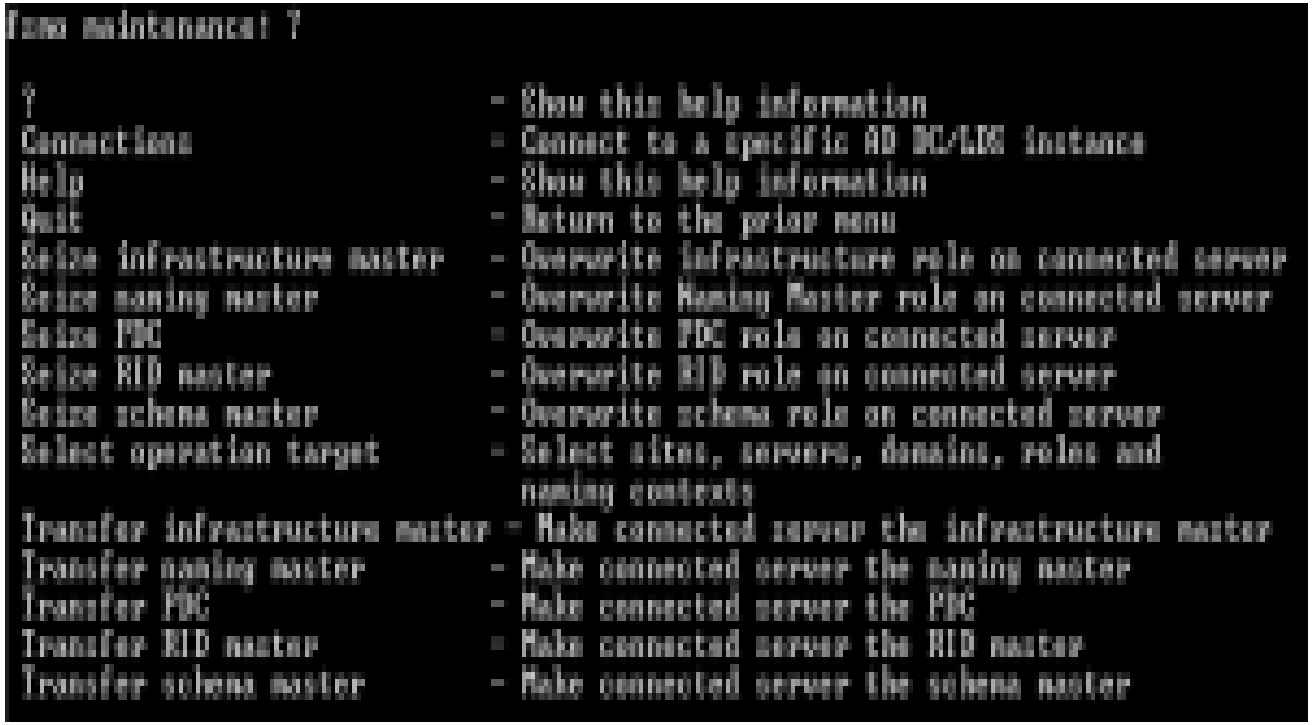
Cont …

- To migrate from one Domain Controller to another you will need to **transfer the FSMO roles** after running **DCPROMO** on the **new domain controller**.
- The easiest way to do so is by the command prompt.

Open Command Prompt

- ✓ Type **ntdsutil**, and then press ENTER
- ✓ Type **roles**, and then press ENTER.
- ✓ Type **connections**, and then press ENTER.
- ✓ Type **connect to server *servername***, and then press ENTER, where ***servername*** is the name of the domain controller you want to assign the FSMO role to.
- ✓ At the **Server Connections** prompt, type **q**, and then press ENTER.
- ✓ Type **transfer *role***, where ***role*** is the role you want to transfer.
- ✓ For a list of roles that you can transfer, type **?** at the **fsmo maintenance** prompt, and then press ENTER, or see image below.

Cont …



- At the **fsmo maintenance** prompt, type **q**, and then press ENTER to gain access to the **ntdsutil** prompt. Type **q**, and then press ENTER to **quit** the **ntdsutil utility**.

Cont …

Seise FSMO Role Holders

- Microsoft recommends that you seize FSMO roles in the following scenarios:

✓ The current role holder is experiencing **an operational error** that prevents an FSMO-dependent operation from completing successfully and **that role cannot be transferred**.

- A domain controller that owns an FSMO role is **force-demoted** by using the **dcpromo /forceremoval** command.
- The operating system on the computer that originally owned a specific role **no longer exists or has been reinstalled.**
- The **seise command** is great when your current role holder is **no longer** on the domain.
- **A domain controller whose FSMO roles have been seized should not be permitted** to communicate with the existing domain controllers in the forest.

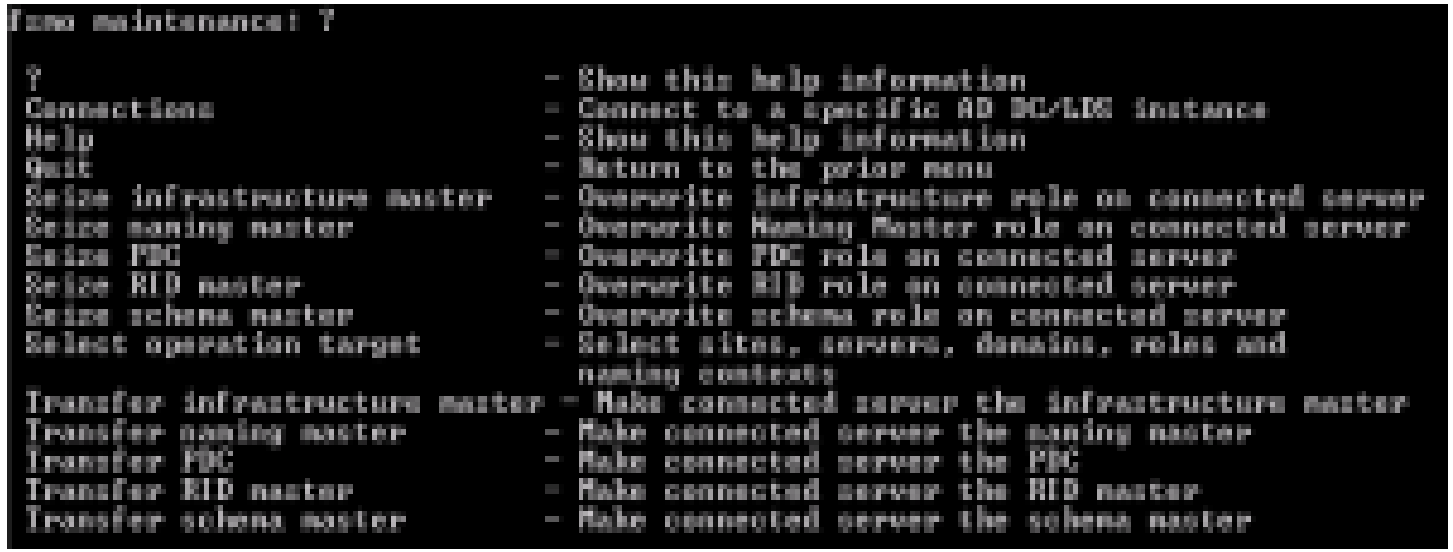
Cont …

- If you have to **seise** the FSMO roles from a domain controller either **format that servers hard drive** or **reinstall windows** to be sure that domain controller is never reintroduced to the forest.

Open Command Prompt

- Type **ntdsutil**, and then press ENTER
- Type **roles**, and then press ENTER.
- Type **connections**, and then press ENTER.
- Type **connect to server *servername***, and then press ENTER, where *servername* is the name of the domain controller you want to assign the FSMO role to.
- At the **Server Connections** prompt, type **q**, and then press ENTER.
- Type **seize *role***, where ***role*** is the role you want to transfer.
- For a list of roles that you can transfer, type **?** At the **fsmo maintenance** prompt, and then press ENTER, or see image below.

Cont …



- At the **fsmo maintenance** prompt, type **q**, and then press ENTER to gain access to the ntdsutil prompt.
- Type q and then press **ENTER** to quit the ntdsutil utility.

Change password policy settings

- If your computer is on a domain, only your network administrator can **change password** policy settings.
- Password policy setting can help protect your computer by customizing your password policy settings, including requiring users to change their password regularly, specifying a minimum length for passwords, and requiring passwords to meet certain complexity requirements.

Types of password policy

1. Enforce password history

- Prevents users from creating a new password that is the same as their current password or a recently used password.
- To specify how many passwords are remembered, provide a value.
- For example, a value of **1 means** that only the **last password** will be remembered, and a value of **5 means** that the previous **five passwords** will be remembered.
- So the recommended enforce password history must be greater than one (1).

Cont …

2. Maximum password

- Sets the maximum number of days that a password is valid.
- After this number of days, the user will have to change the password.
- Set a maximum password age of 70 days.
- Setting the number of days too high provides hackers with an extended window of opportunity to crack the password.
- Setting the number of days too low might be frustrating for users who have to change their passwords too frequently.

Cont …

3. Maximum password age

- Sets the minimum number of days that must pass before a password can be changed.
- Set the length between **8** and **12** characters (provided that they also meet complexity requirements).
- A longer password is more difficult to crack than a shorter password, assuming the password is not a word or common phrase.
- If you are not concerned about someone in your office or home using your computer, however, using no password gives you better protection against a hacker trying to break into your computer from the Internet or another network than an easily guessed password would.
- If you use no password, Windows automatically prevents anyone from logging on to your computer from the Internet or another network.

Cont …

4. Minimum password length

- Determines how short passwords can be.
- Although Windows 2000, Windows XP, and Windows Server 2003 support passwords **up to 28 characters**, the value of this setting can be only between 0 and 4 characters.
- If it is set to 0, users are allowed to have blank passwords, so you should not use a value of 0. It is recommended that you set this value to 8 characters.

5. Passwords must meet complexity requirements

- Determine whether password complexity is enforced.
- If this setting is enabled, user passwords meet the following requirements:
- The password is at least **six characters long**.

Cont …

- The password contains characters from at least three of the following five categories:
  - ✓ **English uppercase characters (A - Z)**
  - ✓ **English lowercase characters (a - z)**
  - ✓ **Base 10 digits (0 - 9)**
  - ✓ **Non-alphanumeric (For example: !, $, #, or %)**
  - ✓ **Unicode characters**
  - ✓ **The password does not contain three or more characters from the user's account name.**

Cont …

- If the account name is less than three characters long, this check is not performed because the rate at which passwords would be rejected is too high.
- When checking against the user's full name, several characters are treated as delimiters that separate the name into individual tokens: commas, periods, dashes/hyphens, underscores, spaces, pound-signs and tabs.
- For each token that is three or more characters long, that token is searched for in the password; if it is present the password change is rejected.
- For example, the name "Erin M. Hagens" would be split into three tokens: "Erin," "M," and "Hagens." Because the **second token** is only one character long, it would be ignored.
- Therefore, this user could not have a password that included either "erin" or "hagens" as a substring anywhere in the password. All of these checks are case insensitive.
- These complexity requirements are enforced upon password change or **creation of new passwords.**
- **It is recommended that you enable this setting**.

Managing files and folder permission

Standard Permission Types

- There are six standard permission types which apply to files and folders in Windows:
  - **Full Control**
  - **Modify**
  - **Read & Execute**
  - **List Folder Contents**
  - **Read**
  - **Write**

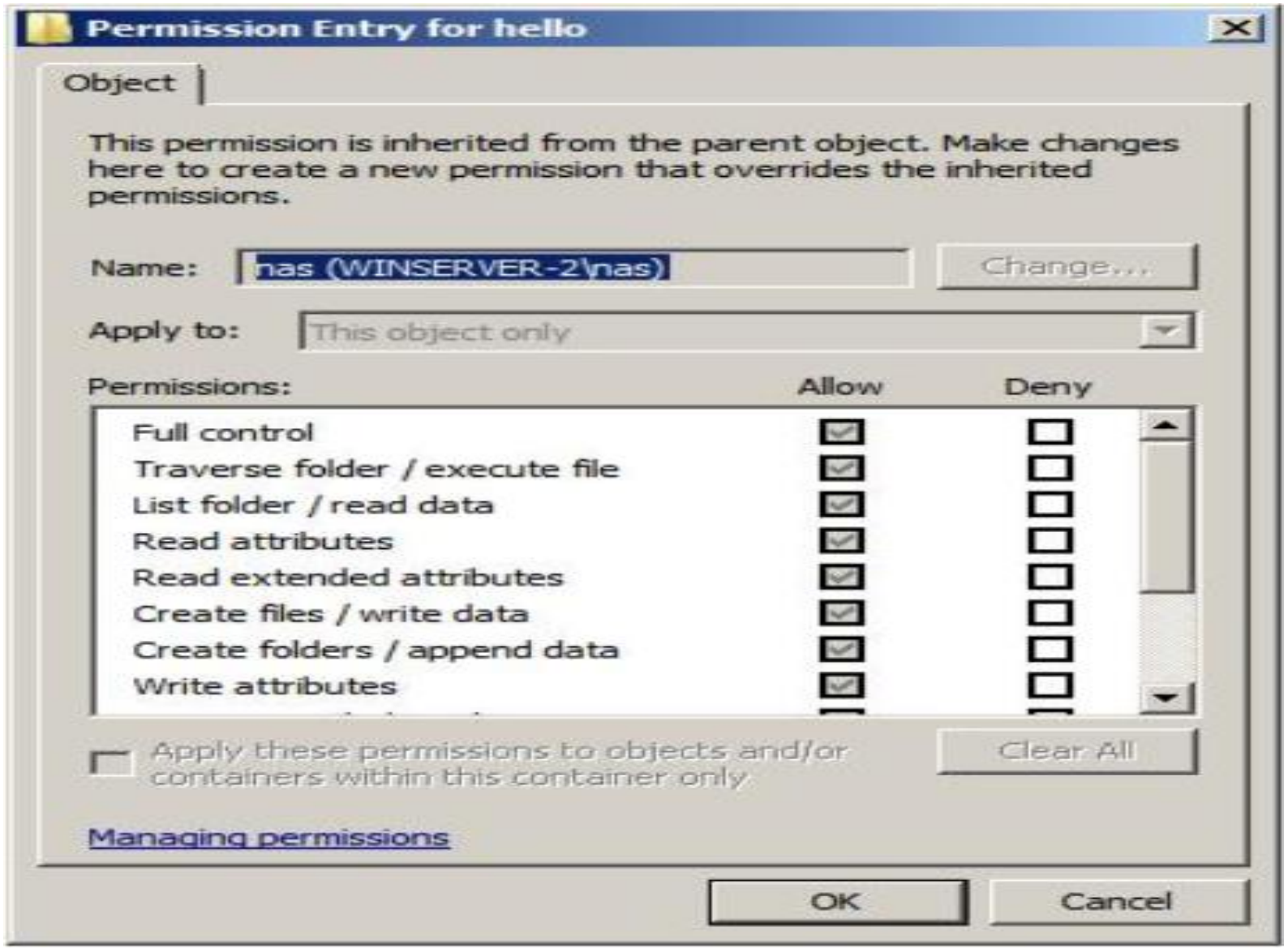
Basic File and Folder Permissions

Permission	Description
Full Control	Permission to read, write, change and delete files and sub-folders.
Modify	Permission to read and write to files in the folder, and to delete current folder.
List Folder Contents	Permission to obtain listing of files and folders and to execute files.
Read and Execute	Permission to list files and folders and to execute files.
Write	Permission to create new files and folders within selected folder.
Read	Permission to list files and folders.

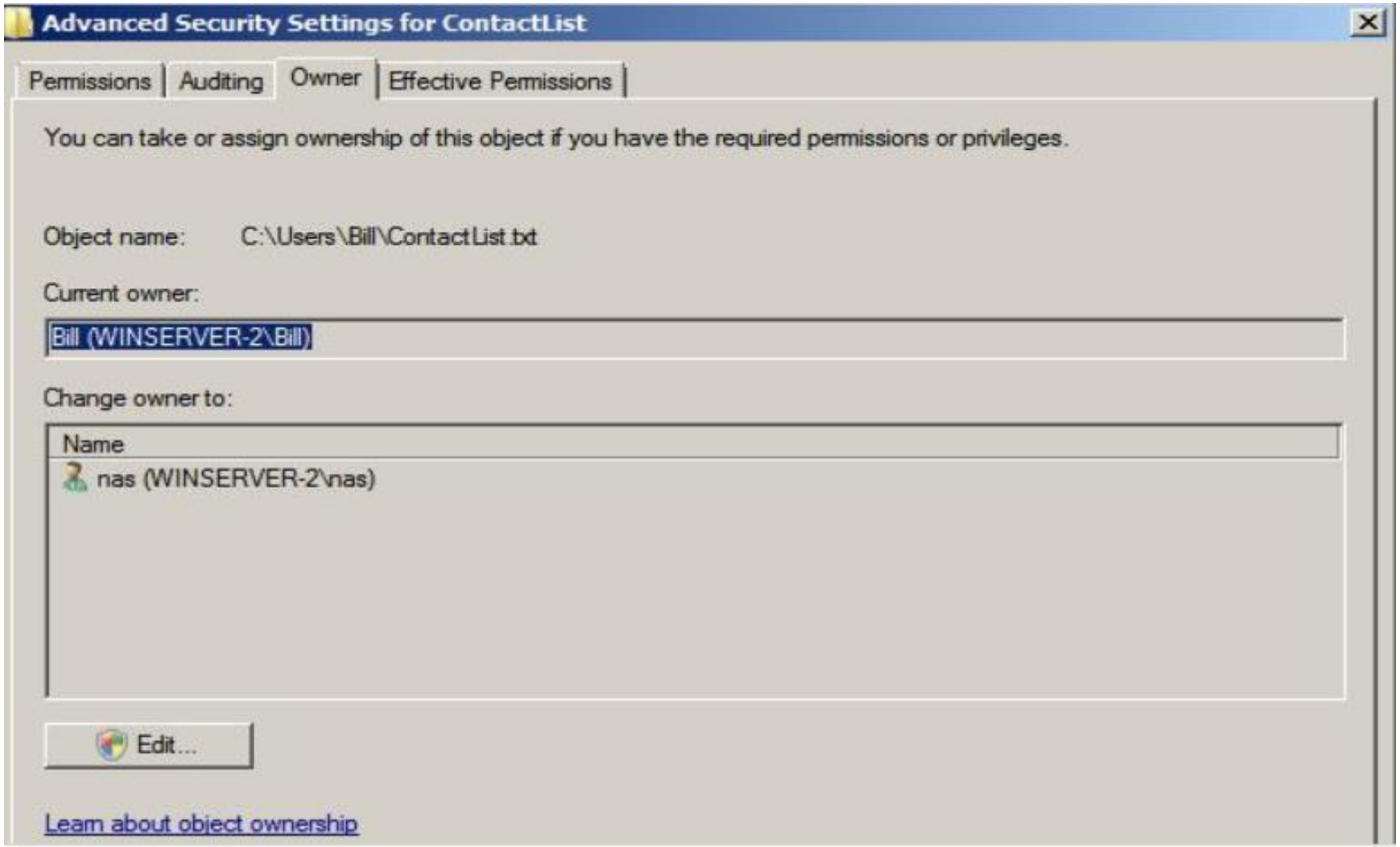
The following table outlines the basic file permissions:

Permission	Description
Full Control	Permission to read, write, change and delete the file.
Modify	Permission to read and write to and delete the file.
Read and Execute	Permission to view file contents and execute file.
Write	Permission to write to the file.
Read	Permission to view the files contents.

Special File and Folder Permissions

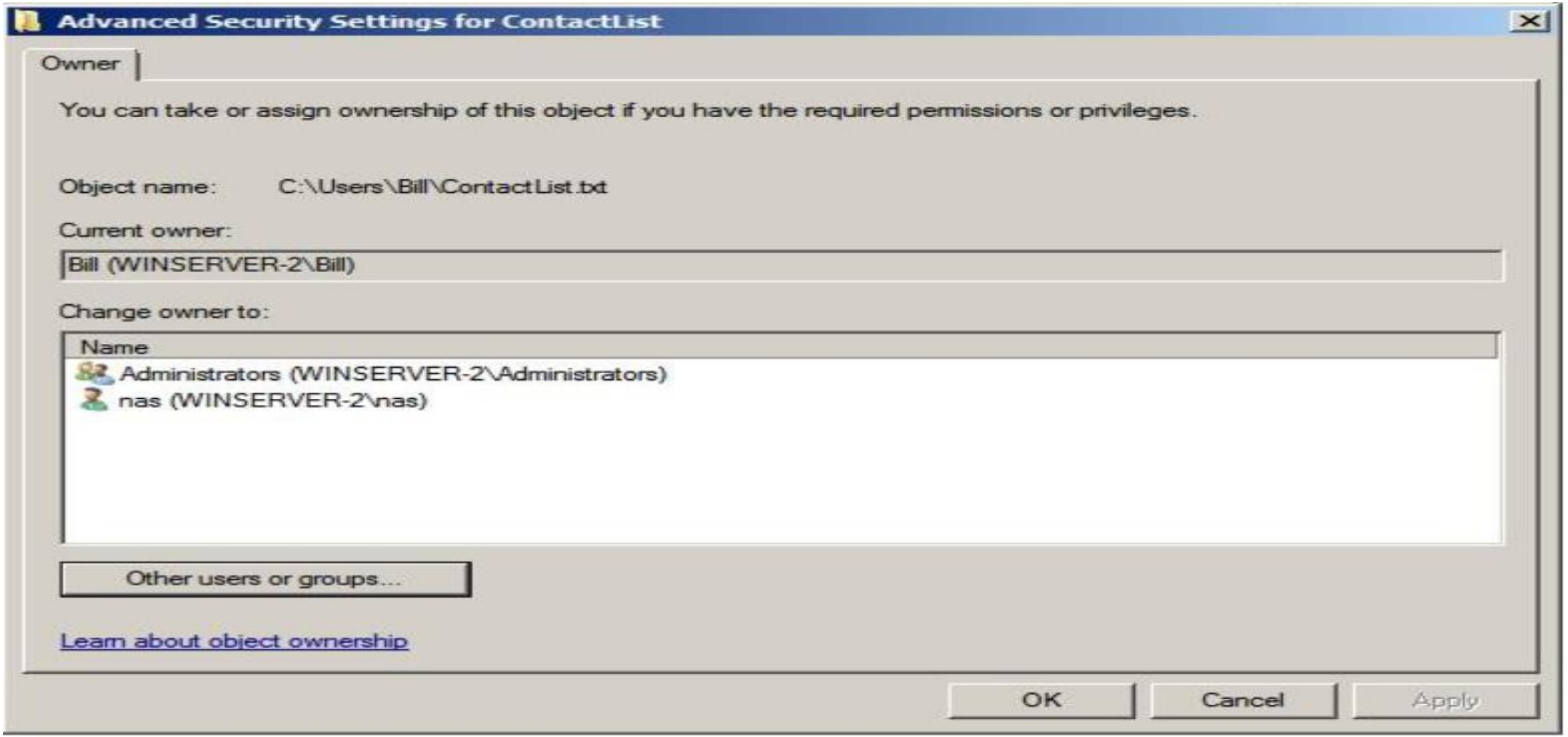


Cont …



Then, click edit

Cont …


Advanced Security Settings for ContactList
Owner
You can take or assign ownership of this object if you have the required permissions or privileges.
Object name: C:\Users\Bill\ContactList.txt
Current owner:
Bill (WINSERVER-2\Bill)
Change owner to:
Name
Administrators (WINSERVER-2\Administrators)
nas (WINSERVER-2\nas)
Other users or groups...
Learn about object ownership
OK
Cancel
Apply

Cont …

- To take ownership, select your user name from the list and click on ***Apply***.
- To transfer ownership to a different user, either select the name from the list, or search for the user by clicking on the ***Other users or groups***... button.
- Select the required user and click on ***Apply*** to commit the transfer.

Managing files and folder permission

Managing file ownership

How to give permission to file in Windows?

- ***Granting Access to a File or Folder***
  - ✓ **Access the Properties dialog box**
  - ✓ **Select the Security tab**
  - ✓ **Click Edit**
  - ✓ **Click Add**
  - ✓ **In the Enter the object names to select text box, type the name of the user or group that will have access to the folder (e.g., 2125.)**
  - ✓ **Click OK**
  - ✓ **Click OK on the Security window**

Cont …

What can you use to control file access?

- Operating systems control the file access by setting permissions for **files and directories**.
- Permissions can be set to grant or deny access to specific files and directories.
- When permission is granted, you can access and perform any function on the file or directory.

How do I manage file permissions?

- To change file and directory permissions, use the command ***chmod*** (change mode).
- The owner of a file can change the permissions for user (u), group (g), or others (o) by adding (+) or subtracting (-) the ***read***, ***write***, and ***execute*** permissions.

How do I give access to a file share?

- Open Windows Explorer and navigate to the shared folder.
- Right click and select Properties.
- Click on the Security tab and click Edit. Click Add and then type the username you wish to grant access.

Network Administration: User Access and Permissions

- In Windows, the concept of file or folder **ownership** is important.
- Every file or folder on a Windows server system has an owner.
- The *owner* is usually the user who creates the file or folder.
- However, ownership can be transferred from one user to another.

Windows Basic Permissions

Permission	Abbreviation	What the User Can Do
Read	R	The user can open and read the file.
Write	W	The user can open and write to the file.
Execute	X	The user can run the file.
Delete	D	The user can delete the file.
Change	P	The user can change the permissions for the file.
Take Ownership	O	The user can take ownership of the file.

Managing Disk Quotas

Enabling Disk Quotas

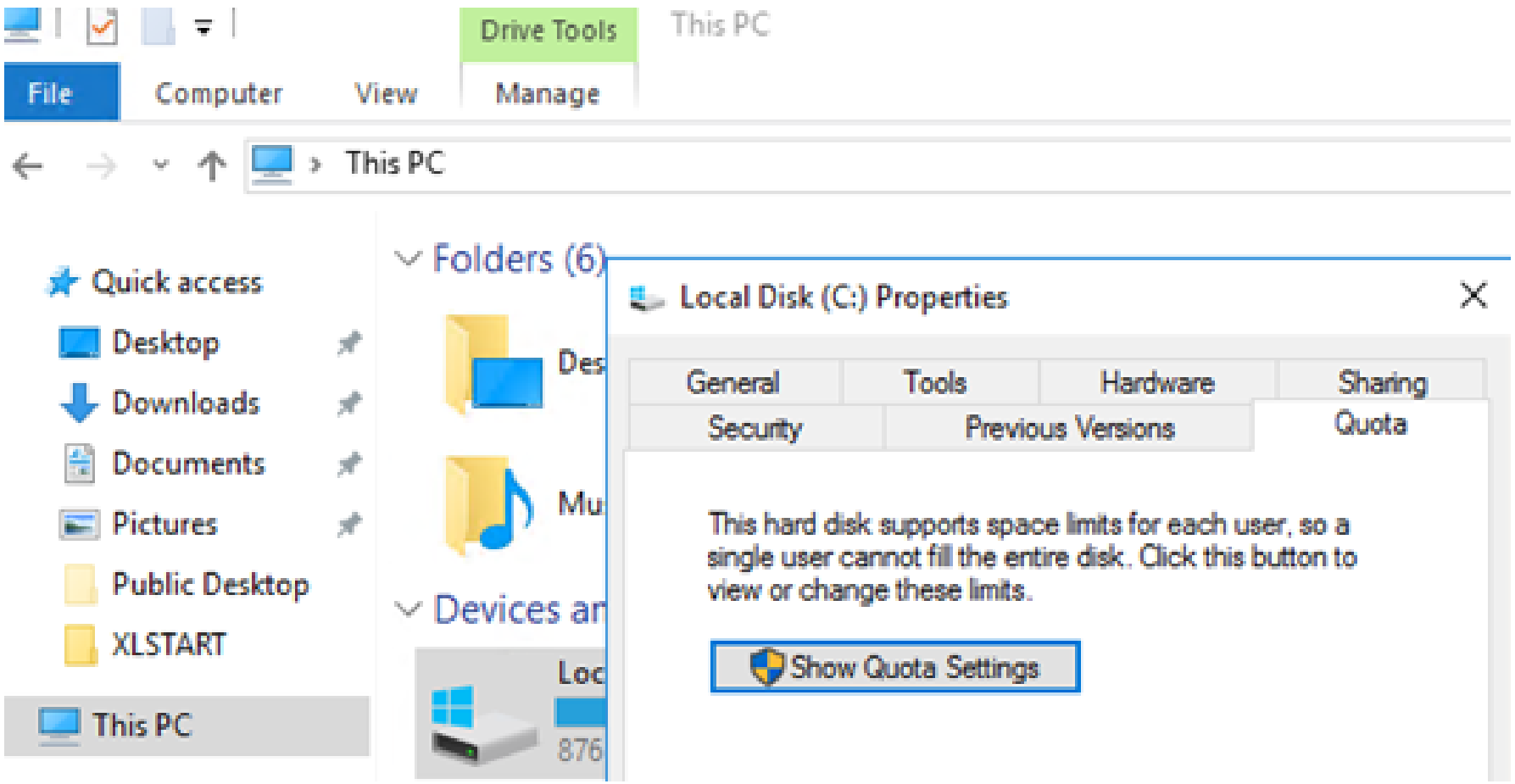
- ***Problem*:** You want to use disk quotas on an NTFS-formatted file system.
- ***Solution***

Using a graphical user interface

- Open Windows Explorer.
- Browse to the drive on which you want to enable quotas, right-click it, and select **Properties**.
- Click the **Quota** tab.
- Check the box beside **Enable quota management**. This turns on disk quota tracking.
- Check the box beside **Deny disk space to users exceeding quota limit** to turn on disk quota enforcement.
- Configure the default quota limit if you want to have one.
- Under the quota logging options, check the appropriate boxes if you want to have messages logged to the event log every time a user exceeds his quota warning or limit levels.
- Click **OK**.
- A dialog box will pop open that informs you the disk needs to be scanned to collect disk statistics. Click **OK**.

Enabling disk quotas in Windows

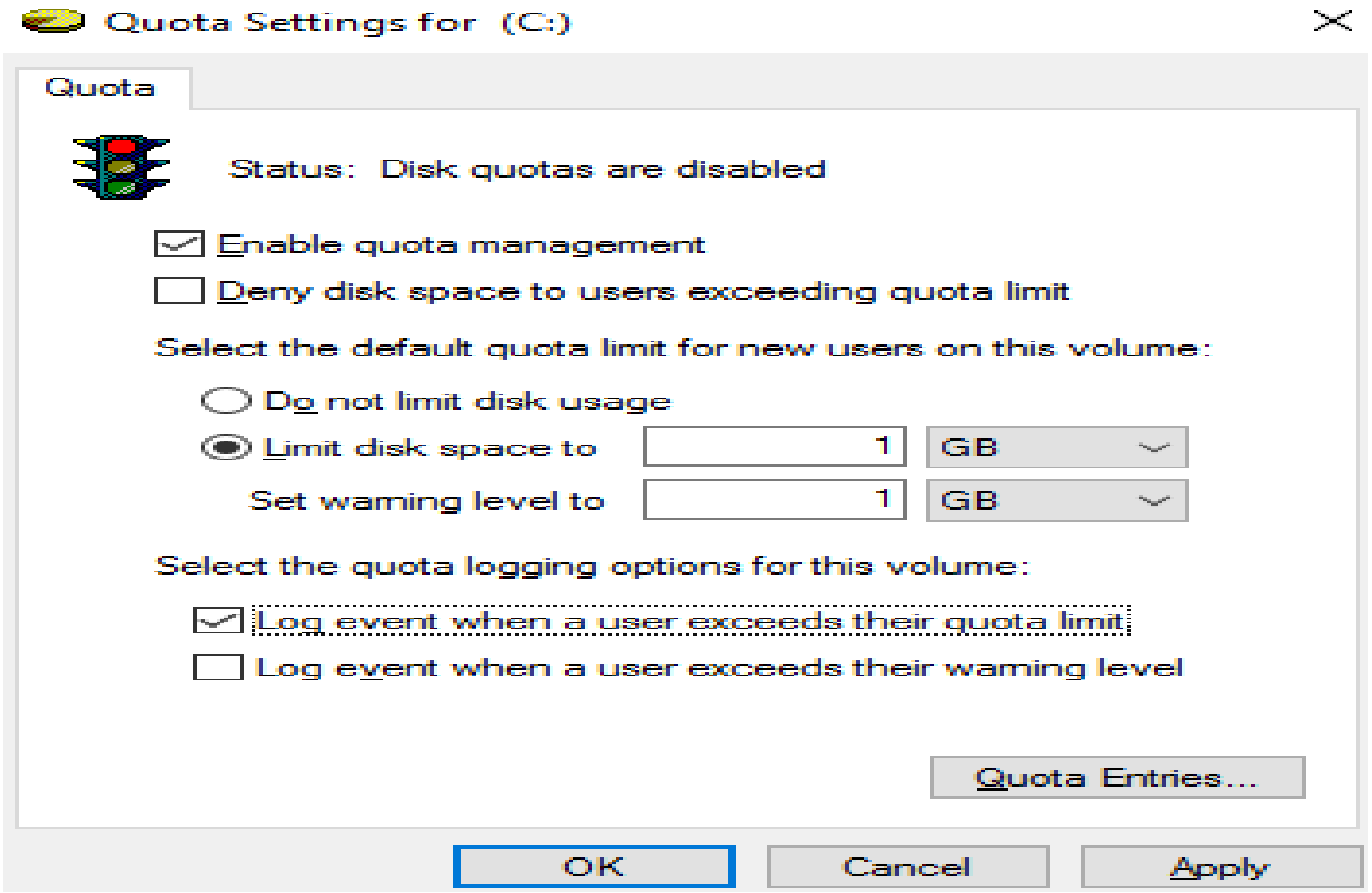
- Open the disk properties window, on which you want to enable quotas, go to the **Quota** tab. Then click **Show Quota Settings**:



Cont …

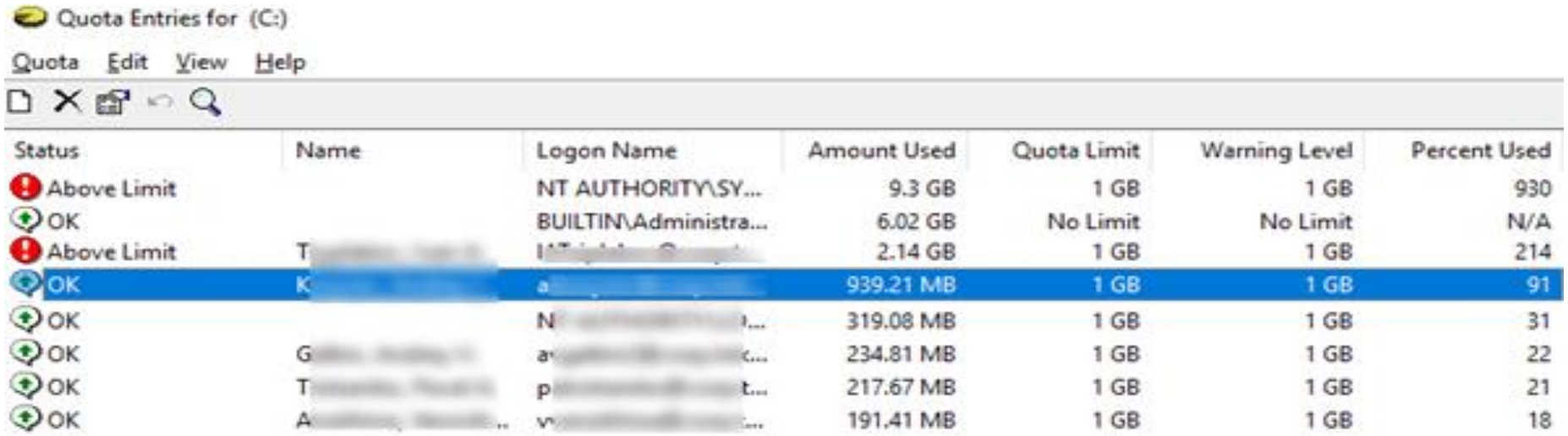
- To enable the quotas for this volume, check **Enable quota management**.
- The following options may be checked depending on the scenario of quota usage:
- **Deny disk space to users exceeding quota limit** – prevent users who have exceeded the quota limit from writing to disk;
- **Limit disk space to** — set a limit on the total size of files for one user;
- **Log event when a user exceeds their quota limit** – logs an event in the Event Viewer if a user exceeds the quota limit;
- **Log event when a user exceeds their warning level** – logs an event when the quota threshold is reached.
- It is not recommended to enable the option "**Deny disk space to users exceeding quota limit"** at once. It is preferable to estimate the current utilization of disk space by your users. In our example, we want to limit each user to 1 GB of disk space on the server.

Cont …


Quota Settings for (C:)
Quota
Status: Disk quotas are disabled
Enable quota management
Deny disk space to users exceeding quota limit
Select the default quota limit for new users on this volume:
Do not limit disk usage
Limit disk space to
1
GB
Set warning level to
1
GB
Select the quota logging options for this volume:
Log event when a user exceeds their quota limit
Log event when a user exceeds their warning level
Quota Entries...
OK
Cancel
Apply

Cont …

- Save the changes (Apply). In some time (depending on the disk size and the number of files), Windows will count the total usage of the disk space by every user.
- Click on the **Quota Entries** button.
- You will see a resulting table showing quotas and the current size of the space used by each user (whose files are found on file system).
- Here you can see at a glance which users have already exceeded their disk quotas.



Status	Name	Logon Name	Amount Used	Quota Limit	Warning Level	Percent Used
Above Limit		NT AUTHORITY\SY...	9.3 GB	1 GB	1 GB	930
OK		BUILTIN\Administra...	6.02 GB	No Limit	No Limit	N/A
Above Limit	T		2.14 GB	1 GB	1 GB	214
OK	K	a	939.21 MB	1 GB	1 GB	91
OK		N	319.08 MB	1 GB	1 GB	31
OK	G	a	234.81 MB	1 GB	1 GB	22
OK	T	p	217.67 MB	1 GB	1 GB	21
OK	A	v	191.41 MB	1 GB	1 GB	18

Thank you