

# Users & Groups

- ▶ Create user objects to represent the employees, customers, or students in your environment.

- ▶ group :-

is just a collection of things. Groups are used most frequently in a security context you set up a group of users and apply certain permissions or rights to that group. Using a group is much easier when applying security than using individual users because you have to apply the security only once instead of once per user.

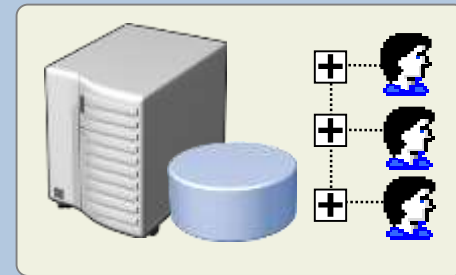
# Guidelines for Creating a User Account Naming Convention

A convention for naming user accounts should accommodate:

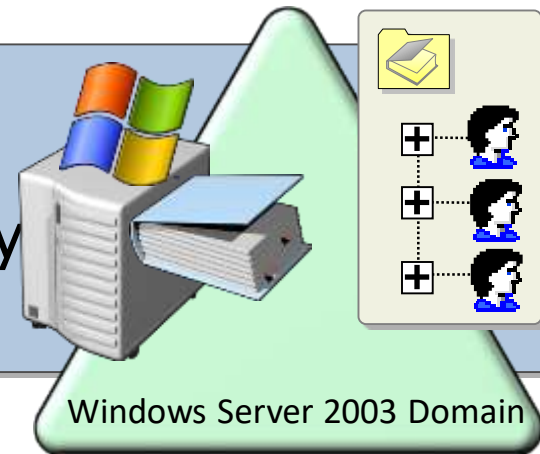
- Employees with duplicate names
- Different types of employees, such as temporary or contract employees

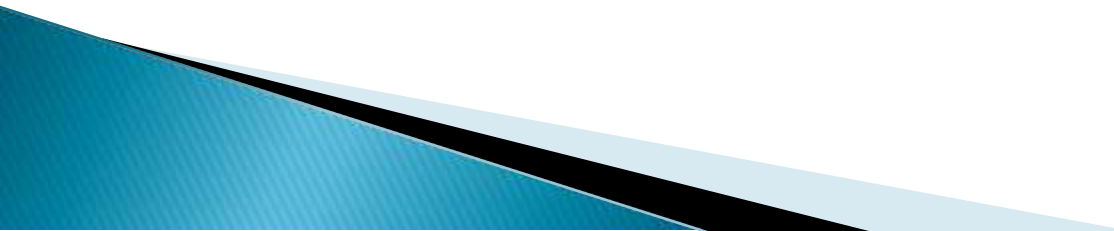
# What Is a User Account ?

- Local user accounts  
(stored on local computer)



- Domain user accounts  
(stored in Active Directory)



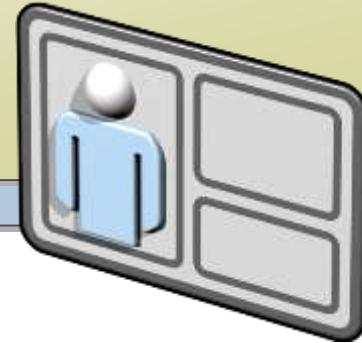
- ▶ Two different types of user accounts can be created:
    1. local user accounts
    2. domain user accounts.
  
  - ▶ **Local user accounts** :- are used to control access to the computer on which you are working. They are created on Windows Server 2003 by using the Local Users and Groups
  - ▶ **Domain accounts**:- are created in Active Directory and are considerably different from local user accounts. Rather than storing information on the local machine, account information is stored in the directory and replicated to other DCs.
- 

# ACCOUNT NAMING

- ▶ Account names can be between 1 and 20 characters (letters and/or numbers).
- ▶ Account names are not case sensitive.
- ▶ The following characters cannot be used in the account name:
  - " / \ [ ] : ; | , + = \* ? < > @

# How to Create User Accounts

- Create a domain user account
- Create a local user account



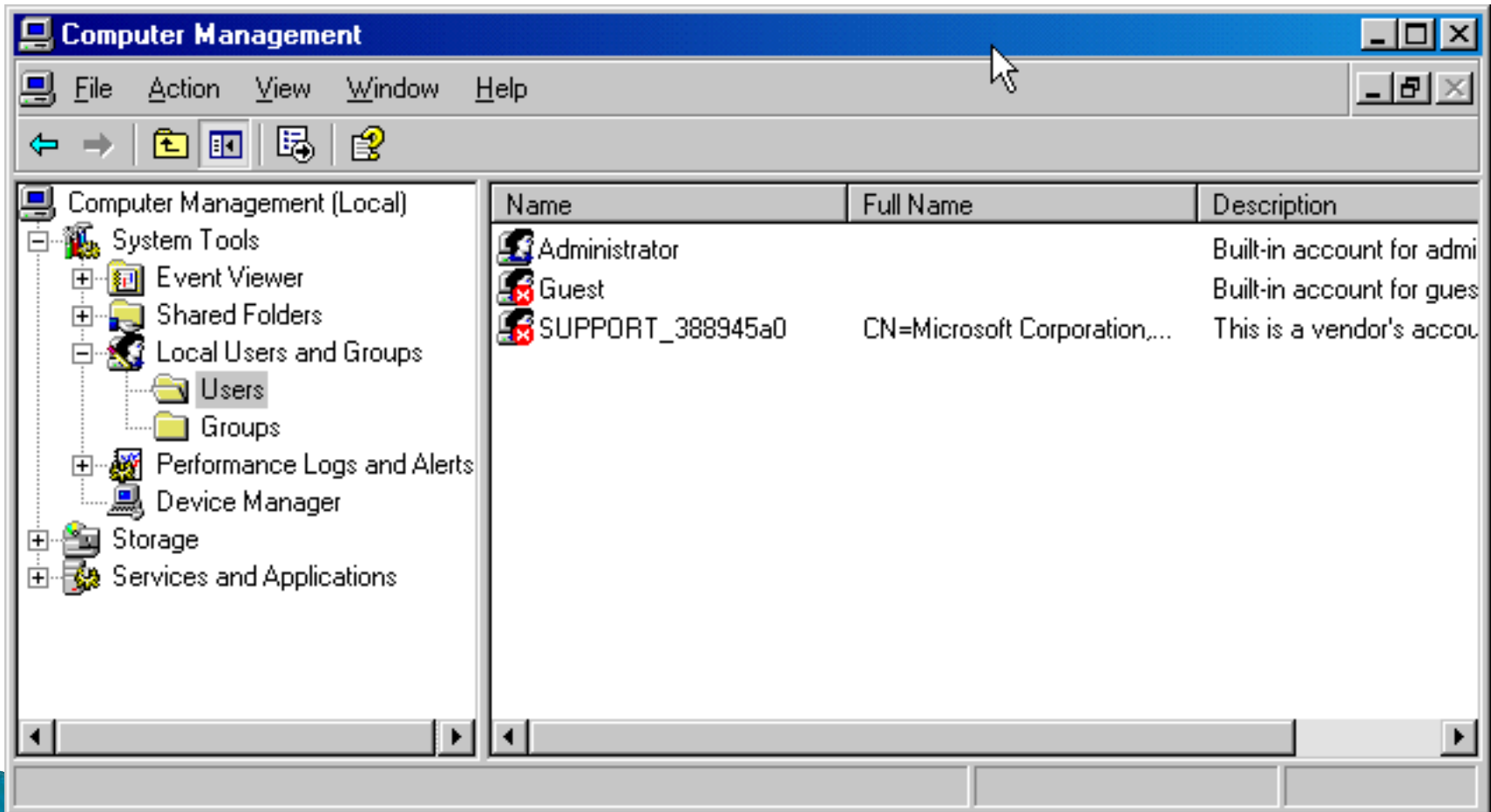
# WORKING WITH DOMAIN USER ACCOUNTS

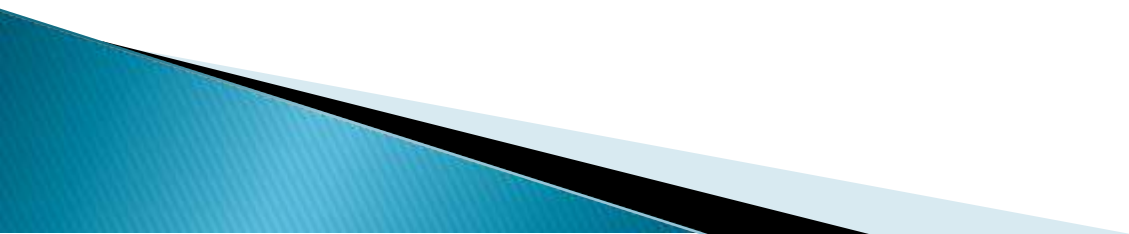
The screenshot shows the Active Directory Users and Computers console for the contoso290.com domain. The left pane shows the tree structure with 'Users' selected. The right pane displays a list of 21 objects in a table format.

Name	Type	Description
Administrator	User	Built-in account for administering the computer/d...
Cert Publishers	Security Group - ...	Members of this group are permitted to publish ce...
DnsAdmins	Security Group - ...	DNS Administrators Group
DnsUpdateProxy	Security Group - ...	DNS clients who are permitted to perform dynami...
Domain Admins	Security Group - ...	Designated administrators of the domain
Domain Computers	Security Group - ...	All workstations and servers joined to the domain
Domain Controllers	Security Group - ...	All domain controllers in the domain
Domain Guests	Security Group - ...	All domain guests
Domain Users	Security Group - ...	All domain users
Enterprise Admins	Security Group - ...	Designated administrators of the enterprise
Group Policy Creator Owners	Security Group - ...	Members in this group can modify group policy for...
Guest	User	Built-in account for guest access to the computer...
HelpServicesGroup	Security Group - ...	Group for the Help and Support Center
IIS_WPG	Security Group - ...	IIS Worker Process Group
IUSR_SERVER01	User	Built-in account for anonymous access to Internet..
IWAM_SERVER01	User	Built-in account for Internet Information Services t...
krbtgt	User	Key Distribution Center Service Account
RAS and IAS Servers	Security Group - ...	Servers in this group can access remote access ...
Schema Admins	Security Group - ...	Designated administrators of the schema
SUPPORT_388945a0	User	This is a vendor's account for the Help and Supp...
TelnetClients	Security Group - ...	Members of this group have access to Telnet Ser...



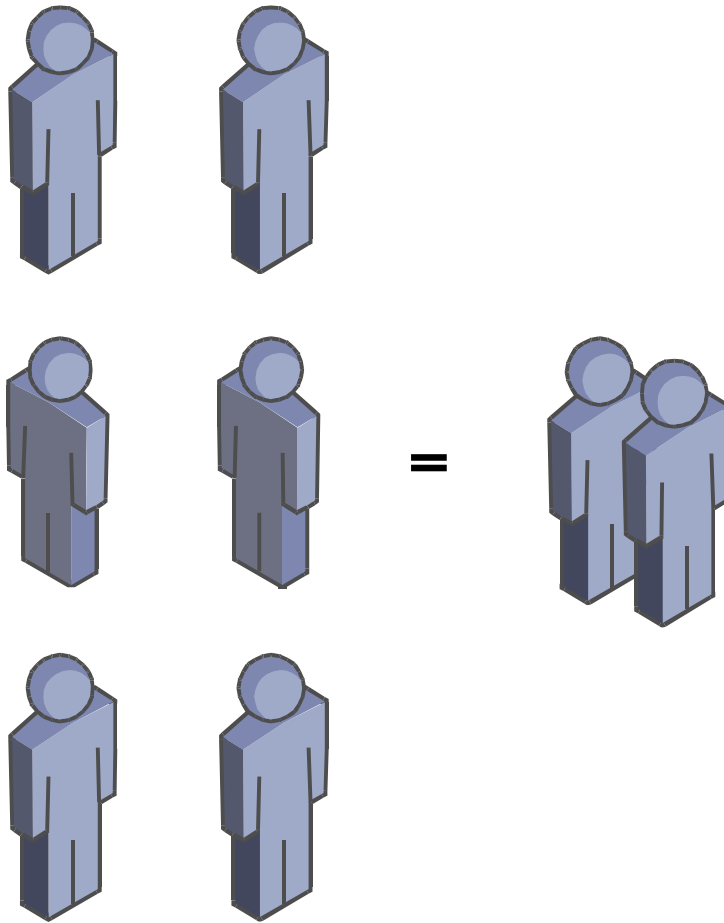
# WORKING WITH LOCAL USER ACCOUNTS

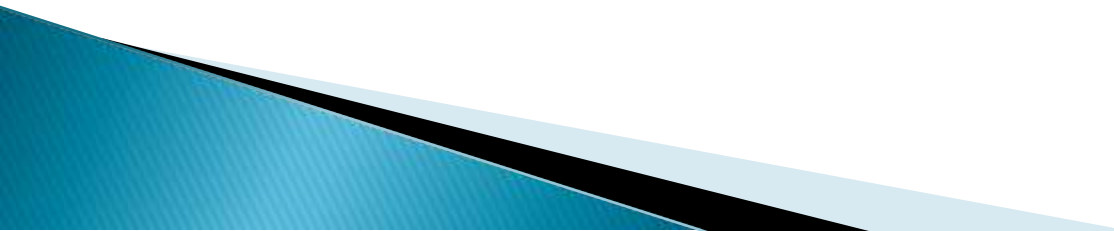






# UNDERSTANDING GROUPS



- ▶ Using groups, you can perform a variety of tasks that will affect the accounts and groups that are members. These include:
  - ▶ Assigning rights to a group account to authorize them to perform a certain task
  - ▶ Assigning permissions on shared resources to a group, so that all members can access the resource in the same manner
  - ▶ Distributing bulk e-mail to all members of the group
- 

# Group Types

- ▶ There are two different types, which are used for two different purposes:

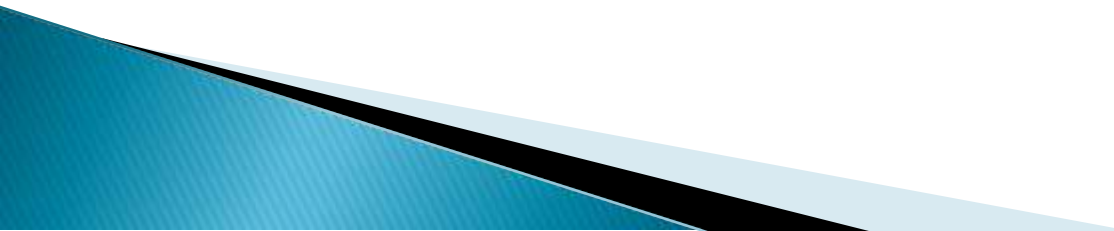
1. Security groups
2. Distribution groups

- ▶ **Security Groups**:-A security group is a collection of users who have specific rights and permissions to resources.

*Rights* are assigned to users and groups, to control the actions a user or member of a group can take. rights are also sometimes called *privileges*.

*Permissions* are used to control access to resources.

When permissions are assigned to a group, it determines what the members of the group can do with a particular resource.

- ▶ **Distribution groups**:- are used for sharing information. This type of group has nothing to do with security. It is used for distributing e-mail messages to groups of users.
  - ▶ Distribution groups allow applications such as Microsoft Exchange to send e-mails to collections of users.
  
  - ▶ Active Directory provides three different scopes for groups:
    1. Universal
    2. Global
    3. Domain Local
- 

- **Global Groups** :-

Global security groups are most often used to organize users who share similar network access requirements. A global group has the following characteristics:

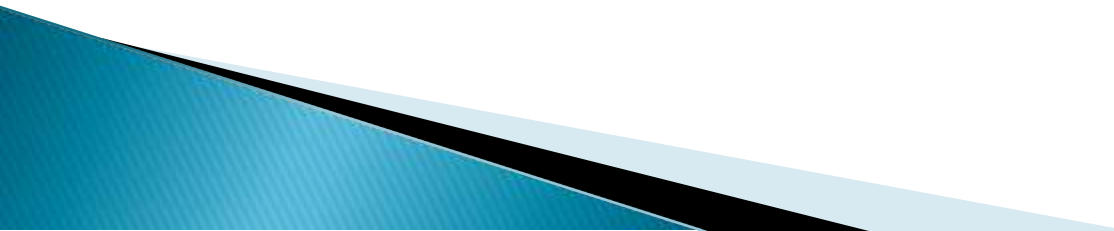
- **Limited membership** You can add members only from the domain in which you create the global group.
- **Access to resources in any domain** You can use a global group to assign permissions to gain access to resources that are located in any domain in the tree or forest.





▶ **Domain Local Groups** :-

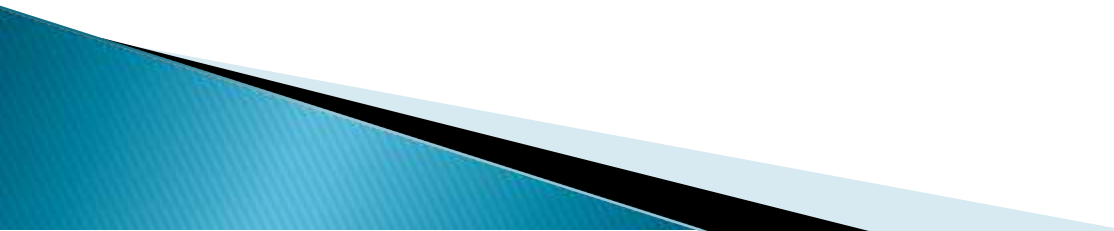
Domain local security groups are most often used to assign permissions to resources. A domain local group has the following characteristics:

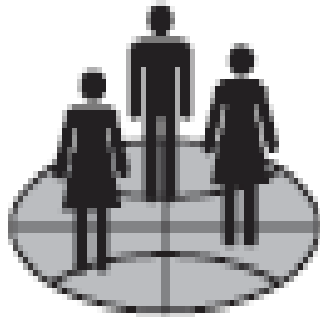
- ▶ **Open membership** You can add members from any domain.
  - ▶ **Access to resources in one domain** You can use a domain local group to assign permissions to gain access to resources that are located only in the same domain where you create the domain local group.
- 

▶ **Universal Groups**

Universal security groups are most often used to assign permissions to related resources in multiple domains. A universal security group has the following characteristics:

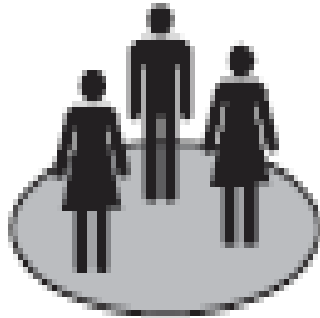
- ▶ **Open membership** You can add members from any domain in the forest.
- ▶ **Access to resources in any domain** You can use a universal group to assign permissions to gain access to resources that are located in any domain in the forest.





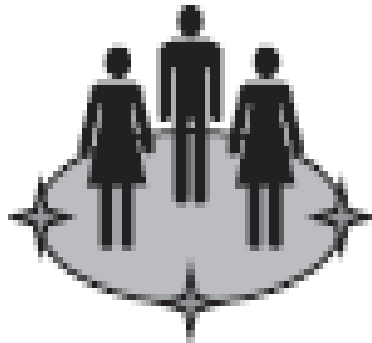
### Global group

Members can come only from local domain.  
Members can access resources in any domain.



### Domain local group

Members can come from any domain.  
Members access resources only in local domain.



### Universal group

Members can come from any domain.  
Members can access resources in any domain.