

- Create User Accounts for Each Person Who Regularly Uses the Network
- Create Multiple User Accounts for New Users in a Single Batch Operation
- Group User Accounts to Manage User Access to Shared Resources
- Nest Groups Within Other Groups to Reduce Administration

Users



- In AD DS, all users who require access to network resources must be configured with a user account.
- With this user account, users can authenticate to the AD DS domain and access network resources.
- In Windows Server 2012, a *user account* is an object that contains all of the information that defines a user. A user account includes the user name, user password, and group memberships.
- A user account also contains many other settings that you can configure based upon your organizational requirements.

Users

- With a user account, you can:
 - Allow or deny users permission to sign in to a computer based on their user account identity.
 - Grant users access to processes and services for a specific security context.
 - Manage users' access to resources such as AD DS objects and their properties, shared folders, files, directories, and printer queues.
- A user account enables a user to sign in to computers and domains with an identity that the domain can authenticate. When you create a user account, you must provide a user logon name, which must be unique in the domain and forest in which the user account is created.
- **To maximize security, you should avoid multiple users sharing a single account, and instead ensure that each user who signs in to the network has a unique user account and password.**

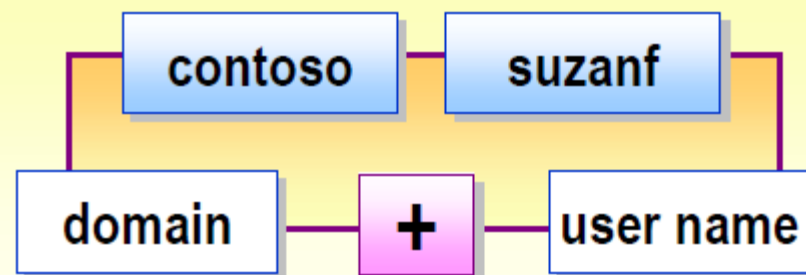
■ User Principal Name

- The suffix defaults to the name of the root domain, but it can be changed and others added



■ User Logon Name (Pre-Windows 2000)

- A user selects the domain when logging on



■ User Logon Name Uniqueness Rules

- Full name must be unique within the container
- User principal name is unique within the forest
- User logon name (pre-Windows 2000) is unique within the domain

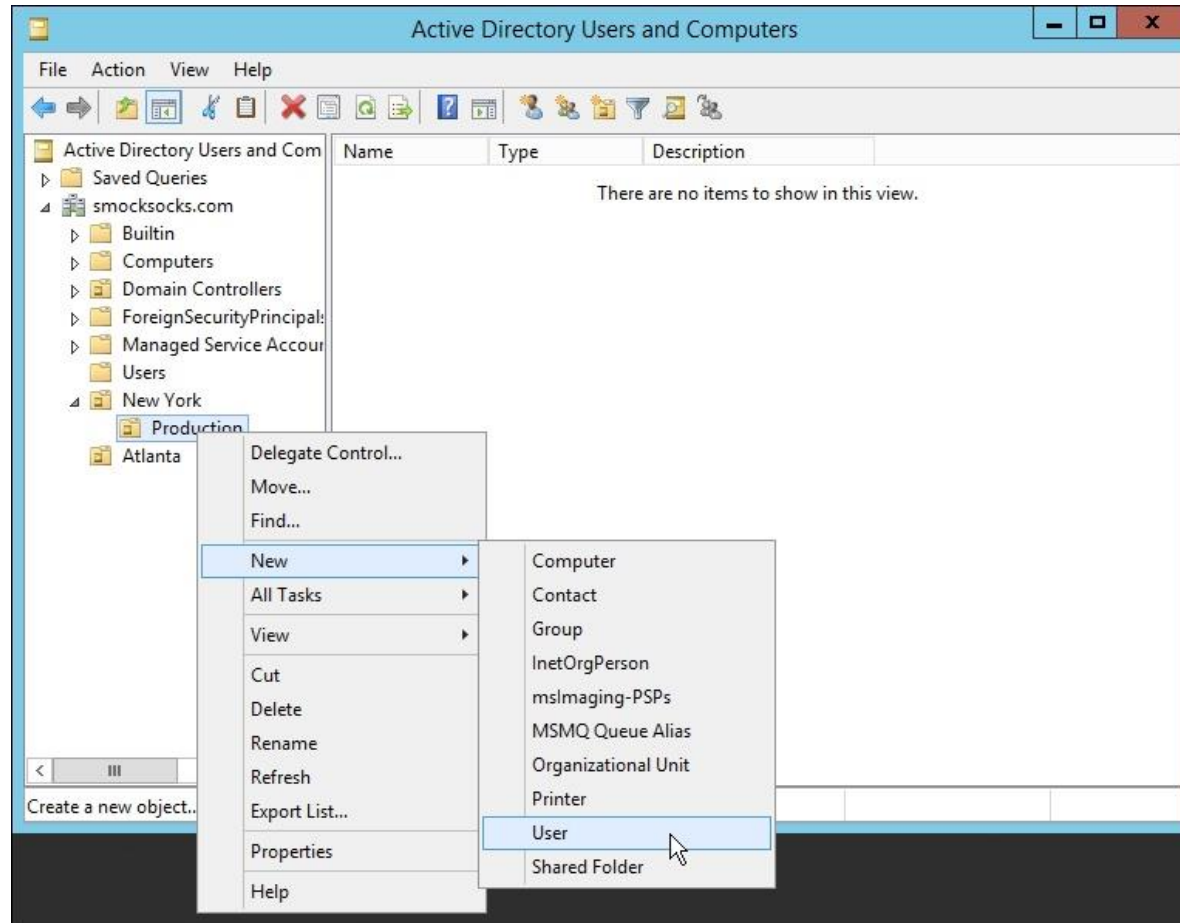
User Logon Name Uniqueness Rules

- User logon names for domain user accounts must follow *uniqueness rules* in Active Directory. When creating user logon names, consider the following uniqueness rules:
 - The full name must be unique within the container in which you create the user account. The full name is used as the relative distinguished name.
 - The user principal name must be unique within the forest.

Creating User Accounts

- **A user account includes the user name and password**, which serve as the user's sign-in credentials. A user object also includes several other attributes that describe and manage the user.
- You can use Active Directory Users and Computers, Active Directory Administrative Center, Windows PowerShell, or the **dsadd** command-line tool to create a user object. When you create user accounts, consider the following elements:
 - The Full Name. The Full Name is used to create several attributes of a user object, most notably, the common name and display name attributes. The common name of a user is the name displayed in the details pane of the snap-in, and it must be unique within the container or OU. If you create a user object for a person with the same name as an existing user in the same OU or container, you need to give the new user object a unique Full Name.
 - The User Principal Name (UPN) Logon. User UPN Logons follow the format *user logon name@(UPN suffix)*.

Creating User Accounts



Creating User Accounts

The screenshot shows the 'Jack Frost Properties' dialog box with the 'Account' tab selected. The 'User logon name' is 'frost' and the domain is '@GLOBOMANTICS.local'. The 'User logon name (pre-Windows 2000)' is 'GLOBOMANTICS\'. The 'Logon Hours...' and 'Log On To...' buttons are visible. The 'Unlock account' checkbox is unchecked. The 'Account options' section has four checkboxes: 'User must change password at next logon' (checked), 'User cannot change password' (unchecked), 'Password never expires' (unchecked), and 'Store password using reversible encryption' (unchecked). The 'Account expires' section has two radio buttons: 'Never' (selected) and 'End of:' (unchecked). The 'End of:' date is 'Sunday, February 23, 2014'. The 'OK', 'Cancel', 'Apply', and 'Help' buttons are at the bottom.

Jack Frost Properties

Member Of Environment Sessions Remote control
Remote Desktop Services Profile COM+ UNIX Attributes
General Address Account Profile Telephones Organization

User logon name:
frost @GLOBOMANTICS.local

User logon name (pre-Windows 2000):
GLOBOMANTICS\ frost

Logon Hours... Log On To...

☐ Unlock account

Account options:

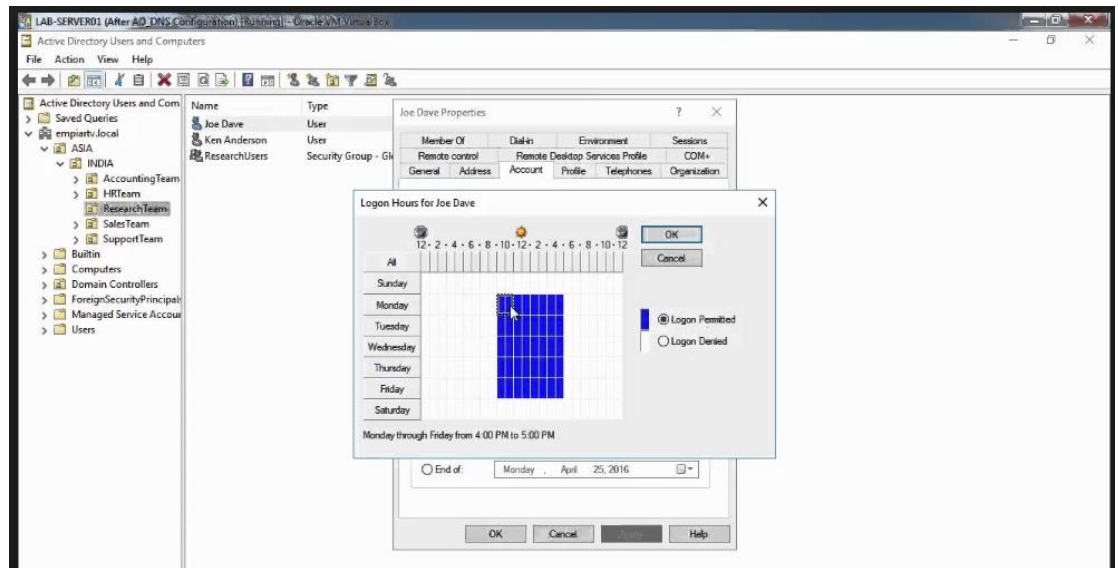
- ☒ User must change password at next logon
- ☐ User cannot change password
- ☐ Password never expires
- ☐ Store password using reversible encryption

Account expires:
☒ Never
☐ End of: Sunday, February 23, 2014

OK Cancel Apply Help

Logon Hours

- This property defines when the account can be used to access domain computers. You can use the weekly calendar style view to define Logon permitted hours and Logon denied hours.



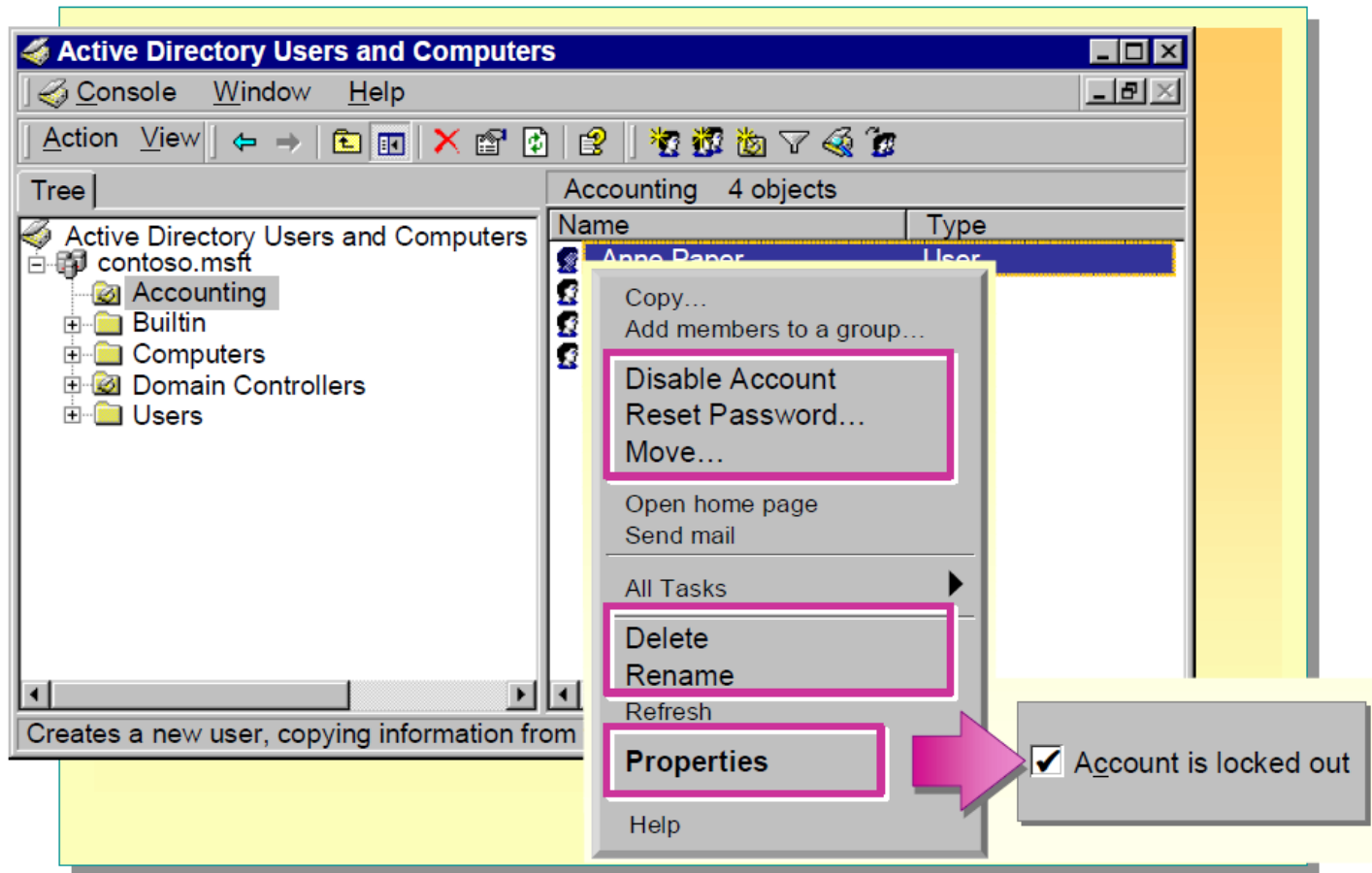
Logon Hours



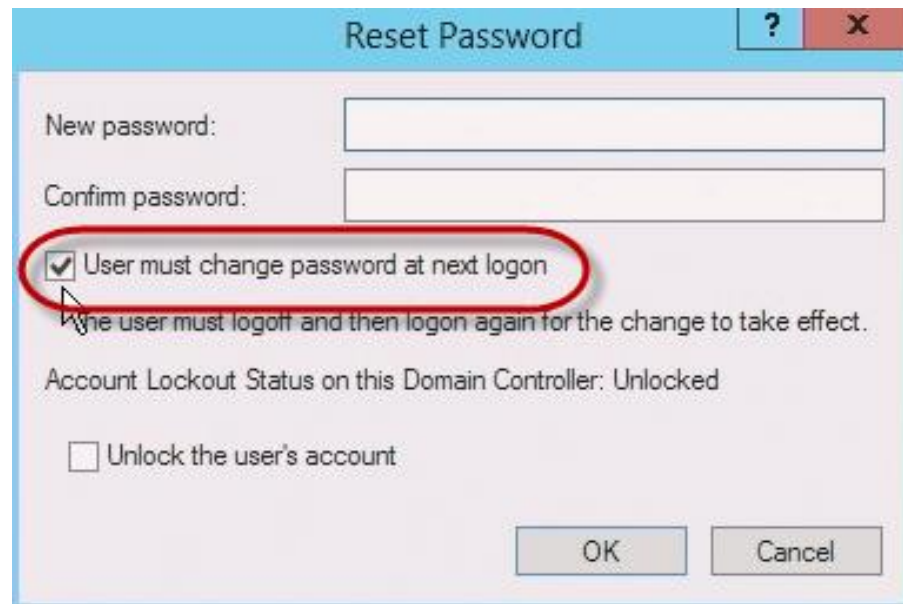
Properties

- **Log on to.** Use this property to define which computers a user can use to log on to the domain. Specify the computer's name and add it to a list of allowed computers.
- **Account expires.** This value is useful when you want to create temporary user accounts. For example, you might want to create user accounts for interns who will be at your company for just one year. You can set the account expiration date in advance. The account cannot be used after the expiration date until it is reconfigured by an administrator manually.
- **User must change password at next log on.** This property enables you to force users to reset their own password the next time they log on. This is typically something you might enable after you reset a user's password.
- **Password never expires.** This is a property that you normally use with service accounts; that is, those accounts that are not used by regular users but by services. By setting this value, you must remember to update the password manually on a periodic basis. However, you are not forced to do this at a predetermined interval. Consequently, the account can never be locked out due to password expiration—a feature that is particularly important for service accounts.
- **User cannot change password.** This option is generally used for service accounts.

Performing Common Administrative Tasks



Reset Password



A screenshot of a Windows 'Reset Password' dialog box. The dialog has a title bar with a question mark and a close button. It contains two text input fields for 'New password:' and 'Confirm password:'. Below these is a checkbox labeled 'User must change password at next logon', which is checked and circled in red. A mouse cursor is pointing at the checkbox. Below the checkbox is a note: 'The user must logoff and then logon again for the change to take effect.' Below that is the text 'Account Lockout Status on this Domain Controller: Unlocked'. At the bottom is an unchecked checkbox labeled 'Unlock the user's account'. At the bottom right are 'OK' and 'Cancel' buttons.

Reset Password

New password:

Confirm password:

☒ User must change password at next logon

The user must logoff and then logon again for the change to take effect.

Account Lockout Status on this Domain Controller: Unlocked

☐ Unlock the user's account

OK Cancel

Unlock User Account

Simran Mago Properties

Member Of Password Replication Dial-in Environment
Sessions Remote control Remote Desktop Services Profile COM+
General Address **Account** Profile Telephones Organization

User logon name:
smago @test.com

User logon name (pre-Windows 2000):
TEST\ smago

Logon Hours... Log On To...

☒ Unlock account. This account is currently locked out on this Active Directory Domain Controller.

Account options:

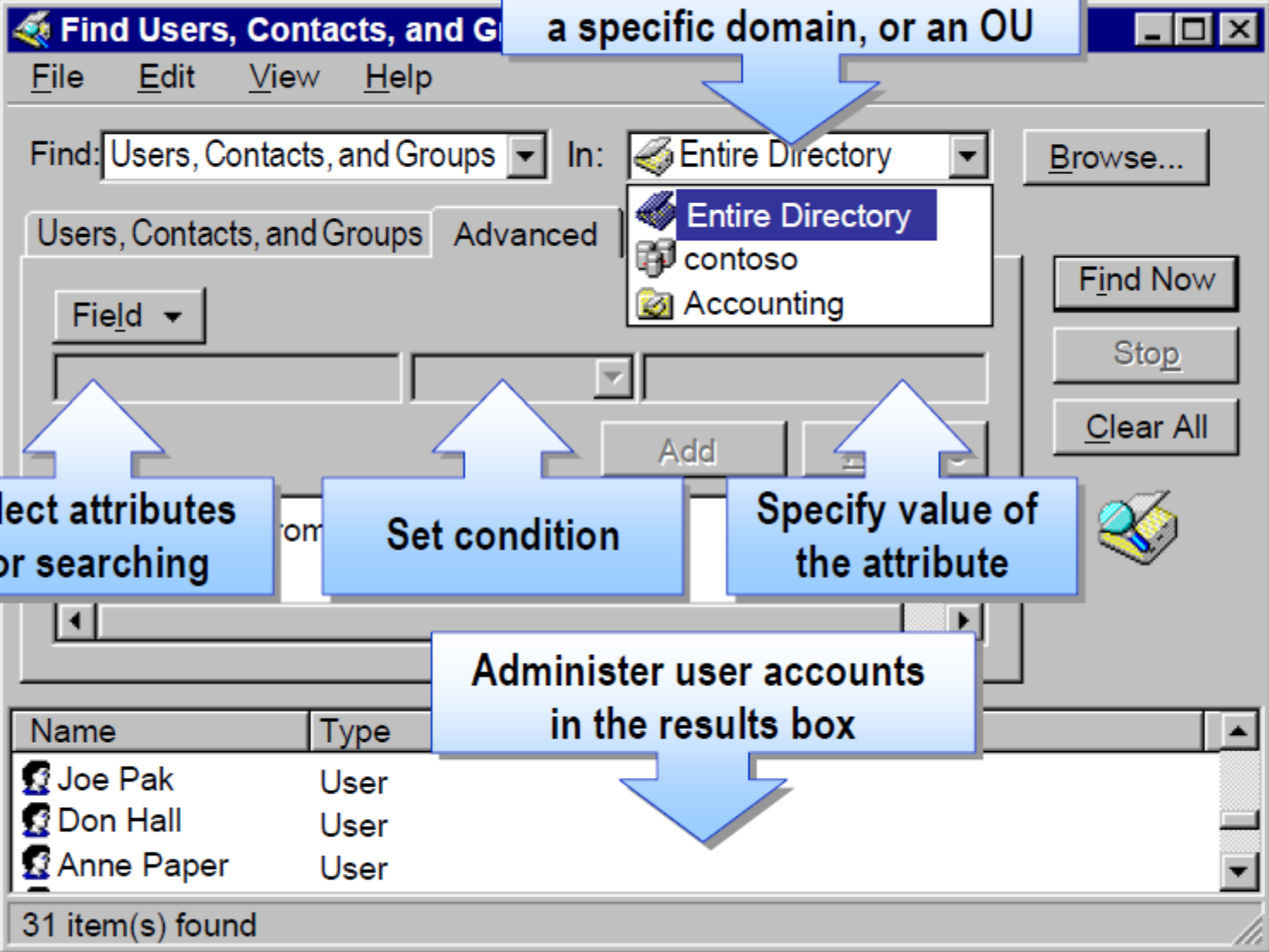
- ☐ User must change password at next logon
- ☐ User cannot change password
- ☐ Password never expires
- ☐ Store password using reversible encryption

Account expires

☒ Never

☐ End of: Saturday , August 23, 2014

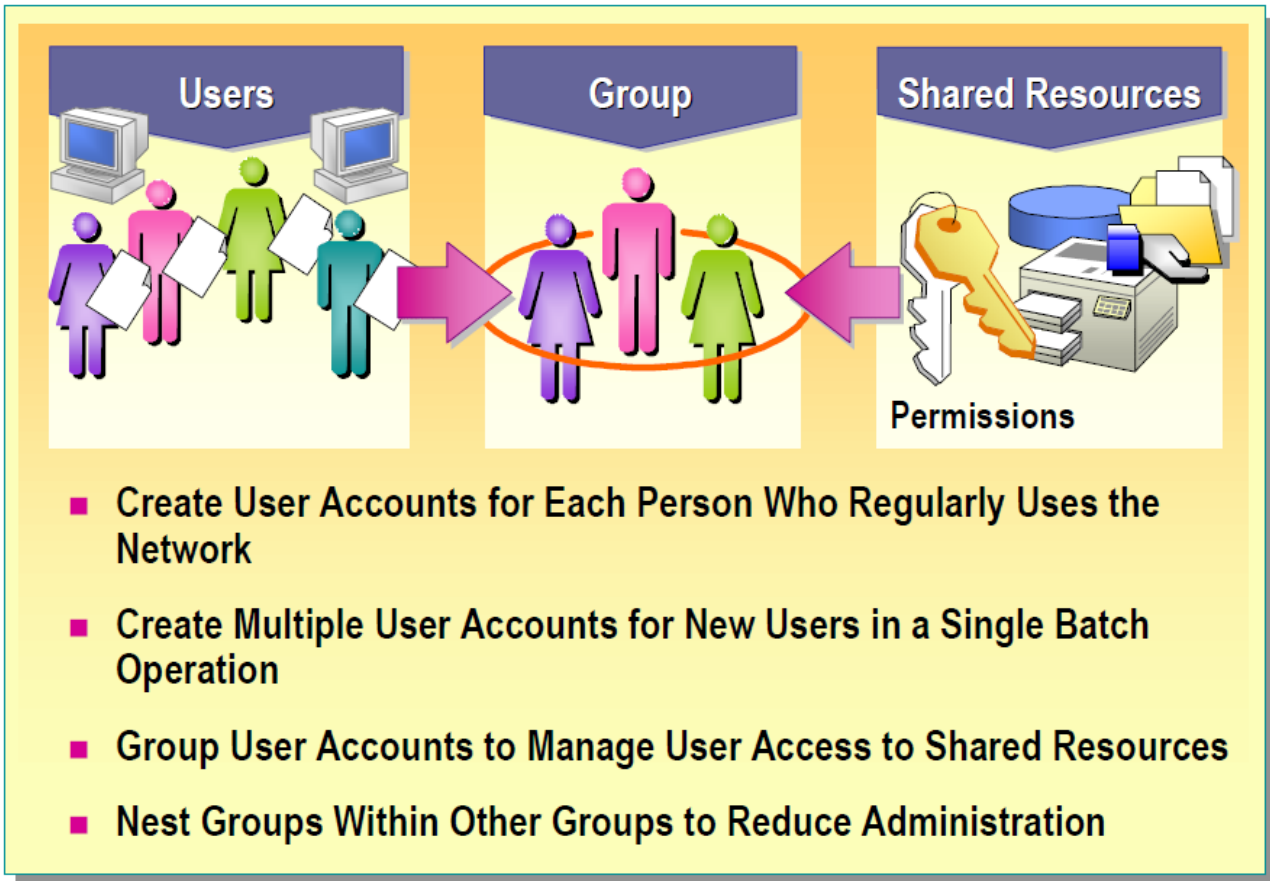
OK Cancel Apply Help



GROUPS

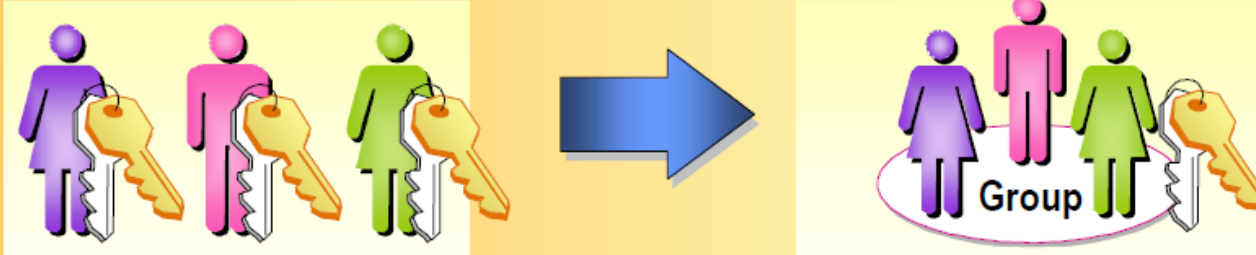
Grouping user accounts to efficiently manage access to domain resources, such as network shared folders, files, directories, and printers.

By using groups, an administrator needs to assign permissions for shared resources only once rather than multiple times. You can also make computers and other groups members of a group.

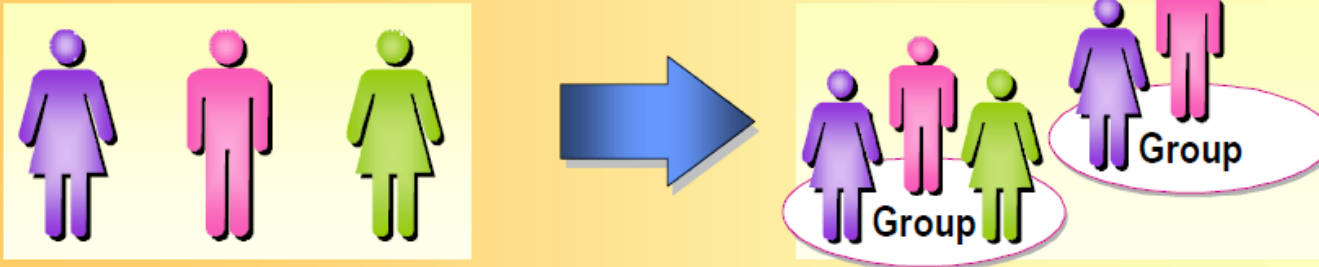


GROUPS

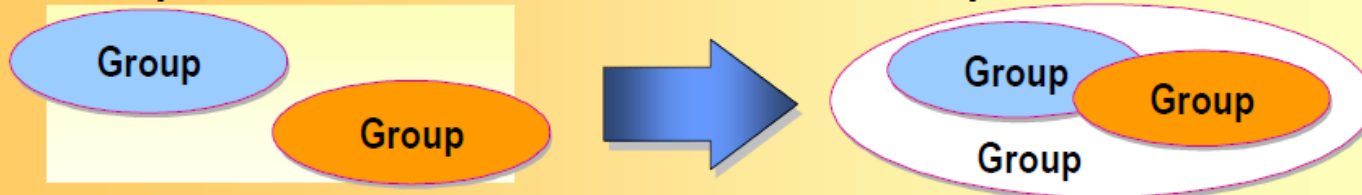
- Groups Simplify Assigning Permission to Resources



- Users Can Be Members of Multiple Groups



- Groups Can Be Nested Inside Other Groups



Distribution x Security Groups

- **Distribution groups**, which are not security-enabled, are **used mainly by email applications**.
- Sending an email message to a distribution group sends the message to all group members.
- **Security groups** are security-enabled, and are **used to assign permissions to various resources**.
- **You can therefore use these groups in permission entries in access control lists (ACLs) to control security for resource access.**
- Because they also include the account group type, you also can use security groups as a means of distribution for email applications. If you want to use a group to manage security, it must be a security group.



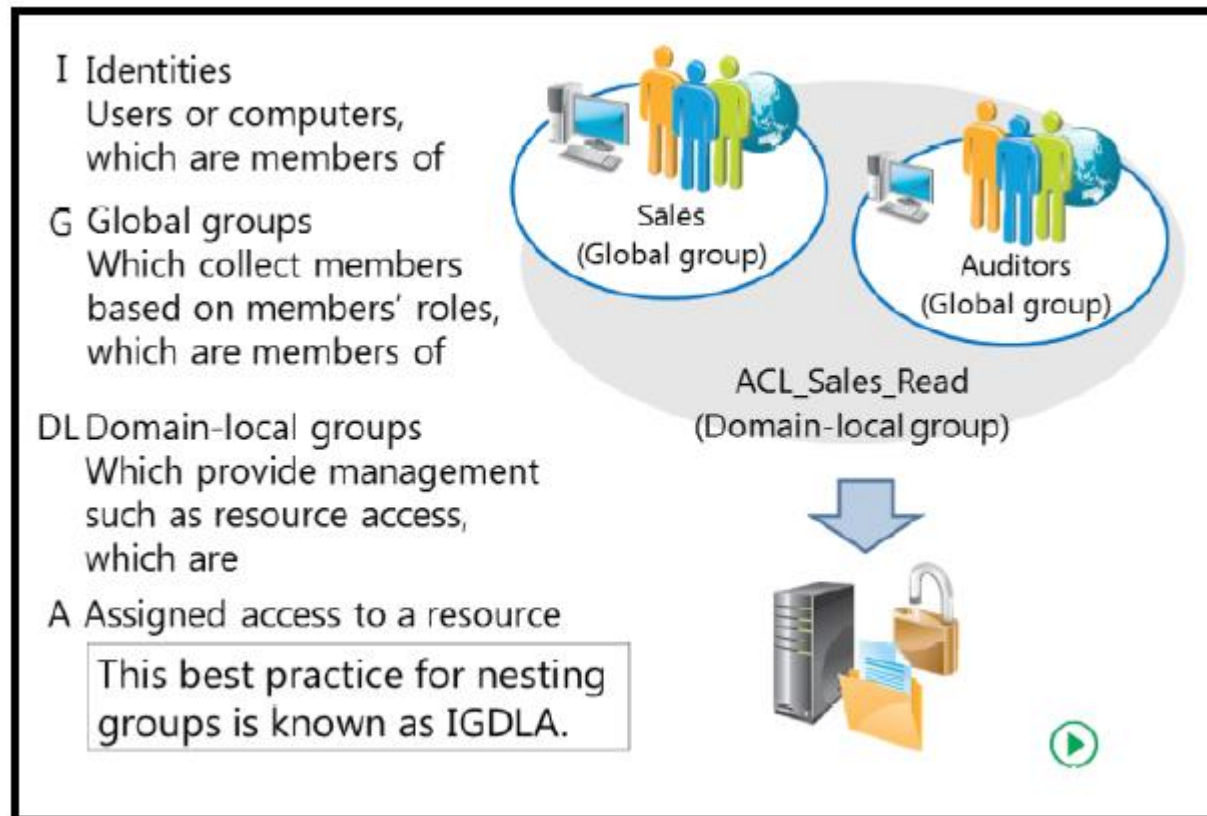
Domain Local Group

- **You use this type of group primarily to manage access to resources or to assign management responsibilities (rights). Domain local groups exist on domain controllers** in an AD DS forest, and consequently, the group's scope is localized to the domain in which they reside. The important characteristics of domain-local groups are:
- **You can assign abilities and permissions** on domain-local resources only, which means **on all computers in the local domain**.
- Members can be from anywhere in the AD DS forest, and can include:
 - Any security principals from the domain: users, computers, global groups, or domain local groups.
 - Users, computers, and global groups from any domain in the forest.
 - Users, computers, and global groups from any trusted domain.
 - Universal groups defined in any domain in the forest.

Global Group

- **You use this type of group primarily to consolidate users who have similar characteristics.** For example, global groups are often used to consolidate users who are part of a department or geographic location. The important characteristics of global groups are:
- **You can assign abilities and permissions anywhere in the forest.**
- Members can be from the local domain only, and can include:
 - Users, computers, and global groups from the local domain.

Implementing Group Management



Implementing Group Management

- These parts of IGDLA are related in the following way:
 - **Identities** (user and computer accounts) are **members of global groups**, which represent **business roles**.
 - **Global groups** (which are also known as role groups) are members of domain-local groups, **which represent management rules**—for example, determining who has Read permission to a specific collection of folders.
 - **Domain-local groups** (which are also known as rule groups) are **granted access to resources**. In the case of a shared folder, access is granted by adding the domain-local group to the folder's ACL, with a permission that provides the appropriate level of access.

Default Groups that Provide Administrative Privileges

- Carefully manage the default groups that provide administrative privileges, because these groups:
 - Typically have broader privileges than are necessary for most delegated environments
 - Often apply protection to their members

Group	Location
Enterprise Admins	Users container of the forest root domain
Schema Admins	Users container of the forest root domain
Administrators	Built-in container of each domain
Domain Admins	Users container of each domain
Server Operators	Built-in container of each domain
Account Operators	Built-in container of each domain
Backup Operators	Built-in container of each domain
Print Operators	Built-in container of each domain
Cert Publishers	Users container of each domain

Default Groups that Provide Administrative Privileges

- **Enterprise Admins** (in the Users container of the forest root domain). This group is a member of the Administrators group in every domain in the forest, which gives it complete access to the configuration of all domain controllers. It also owns the Configuration partition of the directory and has full control of the domain naming context in all forest domains.
- **Schema Admins** (Users container of the forest root domain). This group owns and has full control of the Active Directory schema.
- **Administrators** (Built-in container of each domain). Members of this group have complete control over all domain controllers and data in the domain naming context. They can change the membership of all other administrative groups in the domain, and the Administrators group in the forest root domain can change the membership of Enterprise Admins, Schema Admins, and Domain Admins. The Administrators group in the forest root domain is generally considered the most powerful service administration group in the forest.

Default Groups that Provide Administrative Privileges

- **Domain Admins** (Users container of each domain). This group is added to the Administrators group of its domain. It therefore inherits all of the capabilities of the Administrators group. It is also, by default, added to the local Administrators group of each domain member computer, thus giving Domain Admins ownership of all domain computers.
- **Server Operators** (Built-in container of each domain). Members of this group can perform maintenance tasks on domain controllers. They have the right to sign in locally, start and stop services, perform backup and restore operations, format disks, create or delete shares, and shut down domain controllers. By default, this group has no members.
- **Account Operators** (Built-in container of each domain). Members of this group can create, modify, and delete accounts for users, groups, and computers located in any OU in the domain (except the Domain Controllers OU), and in the Users and Computers containers. Account Operator group members cannot modify accounts that are members of the Administrators or Domain Admins groups, nor can they modify those groups. Account Operator group members also can sign in locally to domain controllers. By default, this group has no members.

Default Groups that Provide Administrative Privileges

- **Backup Operators** (Built-in container of each domain). Members of this group can perform backup and restore operations on domain controllers, and sign in locally and shut down domain controllers. By default, this group has no members.
- **Print Operators** (Built-in container of each domain). Members of this group can maintain print queues on domain controllers. They also can sign in locally and shut down domain controllers.
- **Cert Publishers** (Users container of each domain). Members of this group are permitted to publish certificates to the directory.

Computers



- Before you create a computer object in the Directory Service, you must have a place to put it.
- When you create a domain, the Computers container is created by default (common name (the **cn** attribute)=Computers). This container is not an OU; instead, it is an object of the container class.
- There are subtle but important differences between a container and an OU. You cannot create an OU within a container, so **you cannot subdivide the Computers container. You also cannot link a GPO to a container.** Therefore, **we recommend that you create custom OUs to host computer objects, instead of using the Computers container.**

OUs for Computers

- Most organizations **create at least two OUs for computer objects—one for servers, and another to host computer accounts for client computers**, such as desktops, laptops, and other user devices.
- **These two OUs are in addition to the Domain Controllers OU** that is created by default during the AD DS installation.
- Computer objects can be created in in any OU in your domain. There is no technical difference between a computer object in a client OU, a computer object in a server OU, a computer object in a domain controllers OU, or even a computer object in an OU intended for users. Computer objects are computer objects. **However, separate OUs typically are created to provide unique scopes of management, so that you can delegate management of client objects to one team and management of server objects to another.**

Secure channel

- Every member computer in an AD DS domain maintains a computer account with a user name (sAMAccountName) and password, just like a user account does. **The computer stores its password in the form of a local security authority (LSA) secret, and changes its password with the domain approximately every 30 days.** The NetLogon service uses the credentials to log on to the domain, which establishes the secure channel with a domain controller.
- **To reset the secure channel by using Active Directory Users and Computers, follow this procedure:**
 1. Right-click a computer, and then click **Reset Account**.
 2. Click **Yes** to confirm your choice.
 3. Rejoin the computer to the domain, and then restart the computer.

Introduction to Active Directory

- [70-410 Objective 5.3 - Creating and Managing Groups and OUs on Windows Server 2012 R2.mp4](#)
- [https://www.youtube.com/watch?v=GD-jxhocJZU](#)



Atividade

Nome:

Turma:

Data: / /