CNT 4603: System Administration
Spring 2011

User Account Management With Active Directory

Instructor : Dr. Mark Llewellyn
markl@cs.ucf.edu
HEC 236, 4078-823-2790
http://www.cs.ucf.edu/courses/cnt4603/spr2011

Department of Electrical Engineering and Computer Science
University of Central Florida

User Account Management With Active Directory

- Once Active Directory is installed and configured, you, as a system administrator, enable users to access network servers and resources through user accounts.

- Several accounts may have been created by default, depending on which version of Windows you are using and which Windows components you install, but two accounts are typically generated by default: Administrator and Guest. By default, the Guest account is disabled as a security measure, and must explicitly be enabled by the Administrator.

User Account Management With Active Directory

- User accounts can be set-up in two general environments:
  - Accounts that are set-up through a stand-alone server that does not have AD installed.
  - Accounts that are set-up in a domain when AD is installed.
- We are interested only in those user accounts established and maintained within the AD domain.
- When accounts are created in the domain through AD, then those accounts can be used to access any domain server or resource.

User Account Management With Active Directory

- When AD is installed and the server is a domain controller, you control user accounts from the Active Directory Users and Computers tool either from the Administrative Tools menu or as a MMC (Microsoft Management Console) snap-in.
- You create each new account by entering account information and password controls.

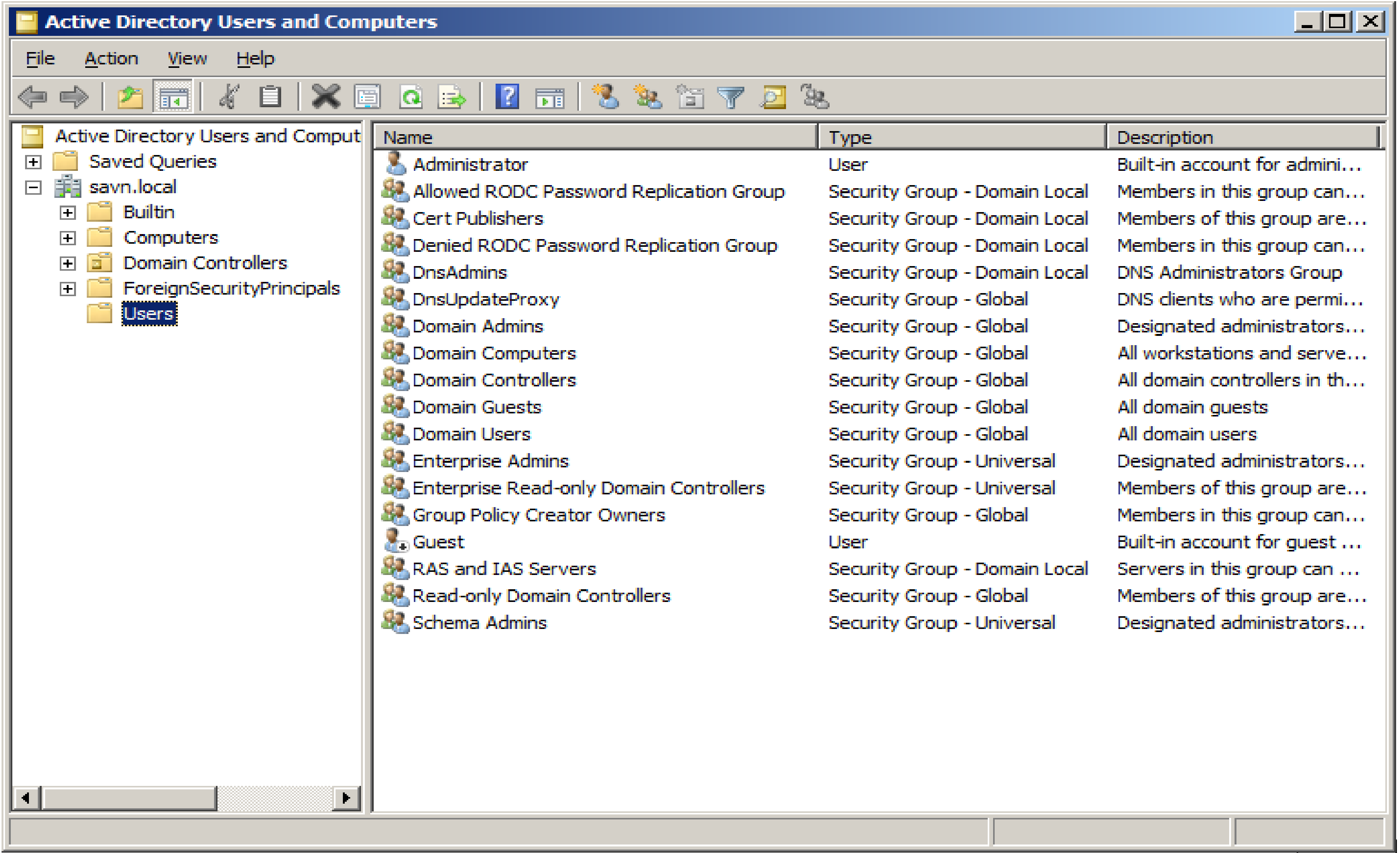
NOTE

If you are using AD and are working on a DC (domain controller), Windows Server 2008 will not allow you to install the Local Users and Groups snap-in, because you must use the AD Users and Computers snap-in instead since AD controls all user accounts in the domain, so there are no local users within the domain.

User Account Management With Active Directory

- As an exercise to see what user account management looks like in AD, start your DC for the `savn.local` network (`Server01`), and under Administrative Tools, select Active Directory Users and Computers. Click on Users in the left panel and you should see a listing similar to the one shown on the next page.
- Once you see this screen of user accounts, either double-click on the Administrator account or right-click on it and select Properties from the drop-down menu and you should see the window illustrating the account’s properties as shown on page 7.
- Next, we’ll look briefly at the options within the various tabs that define the user account properties.

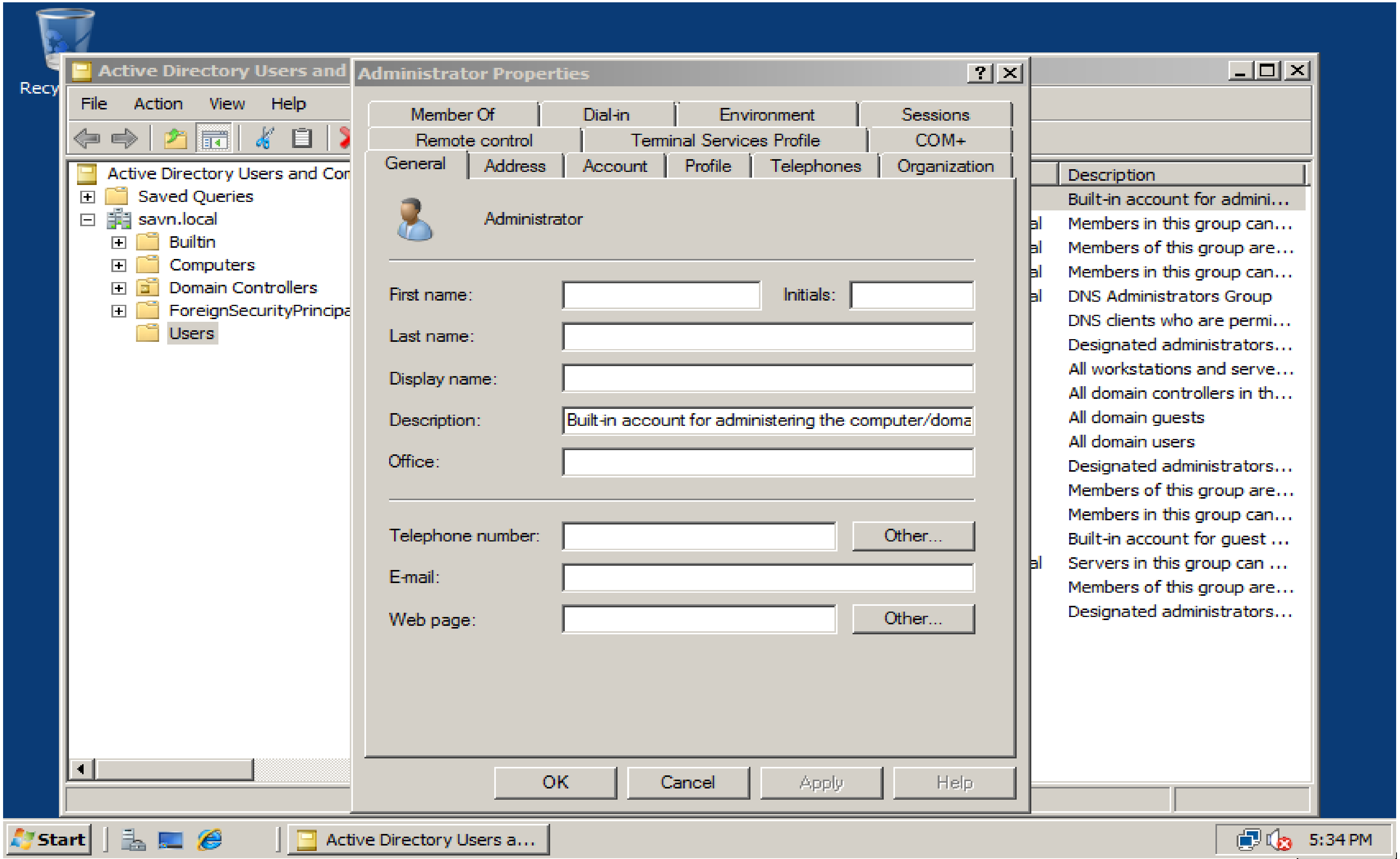
User Account Management With Active Directory



Active Directory Users and Computers
File
Action
View
Help
Active Directory Users and Comput
Saved Queries
savn.local
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Users

Name	Type	Description
Administrator	User	Built-in account for admini…
Allowed RODC Password Replication Group	Security Group - Domain Local	Members in this group can…
Cert Publishers	Security Group - Domain Local	Members of this group are…
Denied RODC Password Replication Group	Security Group - Domain Local	Members in this group can…
DnsAdmins	Security Group - Domain Local	DNS Administrators Group
DnsUpdateProxy	Security Group - Global	DNS clients who are permi…
Domain Admins	Security Group - Global	Designated administrators…
Domain Computers	Security Group - Global	All workstations and serve…
Domain Controllers	Security Group - Global	All domain controllers in th…
Domain Guests	Security Group - Global	All domain guests
Domain Users	Security Group - Global	All domain users
Enterprise Admins	Security Group - Universal	Designated administrators…
Enterprise Read-only Domain Controllers	Security Group - Universal	Members of this group are…
Group Policy Creator Owners	Security Group - Global	Members in this group can…
Guest	User	Built-in account for guest …
RAS and IAS Servers	Security Group - Domain Local	Servers in this group can …
Read-only Domain Controllers	Security Group - Global	Members of this group are…
Schema Admins	Security Group - Universal	Designated administrators…

User Account Management With Active Directory



Active Directory Users and Computers

- Saved Queries
- savn.local
  - Builtin
  - Computers
  - Domain Controllers
  - ForeignSecurityPrincipa
  - Users

Administrator Properties

Administrator

First name:

Initials:

Last name:

Display name:

Description: Built-in account for administering the computer/doma

Office:

Telephone number:

E-mail:

Web page:

Description
Built-in account for admini...
Members in this group can...
Members of this group are...
Members in this group can...
DNS Administrators Group
DNS clients who are permi...
Designated administrators...
All workstations and serve...
All domain controllers in th...
All domain guests
All domain users
Designated administrators...
Members of this group are...
Members in this group can...
Built-in account for guest ...
Servers in this group can ...
Members of this group are...
Designated administrators...

User Account Management With Active Directory

- Before we look at the various user account control options, from the Active Directory Users and Computers main Users window for the `savn.local` network (the screen shown on page 6), right click the Administrator user account and look at the drop-down list that appears.
- Notice in particular two entries: (1) Disable Account, which indicates that the account is currently enabled, and (2) Reset Password.
- Next right-click on the Guest user account and look at the drop-down list. Notice that the corresponding entry for the Guest account says "Enable Account" indicating that the account is currently disabled and cannot be used.

User Account Management With Active Directory

- There are 13 different tabs under the Account Properties that contain user account properties that can be manipulated by the system administrator. I'll give a brief summary of each of these areas, but you should examine each tab more carefully to get a feel for what each area is controlling.

General tab:

- Enables the system admin to enter or modify personal information about the account holder that include the first name, last name, and name as it is displayed on the console, description of the user of account, office location, telephone number, email address, and web page URL. There are also buttons to enter additional phone numbers and web page URLs for the account holder.

User Account Management With Active Directory

Address tab:

- Provides information about the account holder’s street address, post office box, city, state, or province, postal code, and country or region.

Account tab:

- Provides information about the logon name, domain name, and account options, such as requiring the user to change their password at next logon, and account expiration date, if one applies. A Logon Hours button on this tab enables you to set up and account so that the user only logs on to the domain at designated times, such as only from 8:00am to 7:00pm, Monday through Friday. Also, the Logon To button enables you to limit from which computer a user can log on to the server or domain.

User Account Management With Active Directory

Profile tab:

- Enables the system admin to associate a particular profile with a user or group of users, such as a common desktop (with deal more with user profiles a bit later). This tab is also used to associate a logon script and a home folder with an account. A logon script is a file of commands that are executed at logon. The home folder is disk space on a particular server assigned to the user to store their files.

Telephones tab:

- Enables the system admin to associate specific types of telephone contact numbers for an account holder, which include one or more number for home, work, mobile, fax, and IP phones.

User Account Management With Active Directory

Organization tab:

- Provides a place to enter the account holder's title, department, company name, and the name of the person who manages the account holder.

Remote Control tab:

- Enables the system admin to set up remote control parameters for a client that uses Terminal Services. The remote control capability enables you to view and manipulate the client session while it is active, in order to troubleshoot problems.

Terminal Services Profile tab:

- Enables the system admin to set up a user profile for a client that uses Terminal Services.

User Account Management With Active Directory

COM+ tab:

- Specifies the COM+ partition set of which the user is a member. COM+ is an older framework for running applications prior to the inception of the .NET framework.

Member Of tab:

- Enables the system admin to add the account to an existing group of users that have the same security and access requirements (we’ll look more closely at user groups later). This tab is also used to remove an account from a group.

Dial-in tab:

- Permits the system admin to control remote access from dial-in modems or from virtual private networks (VPNs).

User Account Management With Active Directory

Environment tab:

- Enables the system admin to configure the startup environment for clients that access one or more servers using Terminal Services (for running programs on the server).

Sessions tab:

- Enables the system admin to configure session parameters for clients using Terminal Services, such as a session time limit, a limit on how long a session can be idle, what to do when a connection is broken, and how to reconnect.

Disabling, Enabling, and Renaming Accounts

- When a user takes a leave of absence, you have the option to disable their account.
- Your organization may also have a policy of disabling accounts when someone leaves the organization.
- It might also be the case that when the person arrives who replaces the employee that left that the existing account should be renaming and enabled for the replacement employee. This is often easier than deleting the account and creating a new account.
- In the next project, you'll get some practice at disabling, renaming, and re-enabling an account.

Moving An Account

- When an employee moves from one department to another, you might need to move that person’s account from one container to another – between OUs (organizational units), for example.
- In the next project, you’ll get some practice at creating OUs within the `savn.local` domain and we’ll move some user accounts from one OU to another OU.

Resetting Passwords

- One of the most common requests encountered by system administrators is to reset a user’s password.

- Sometimes users change their passwords, or go several weeks without logging on – and forget their passwords. System administrators rarely have the option of looking up a password, but they can reset it for the user.

- For organizations that have accounts that handle sensitive information, particularly financial information, it is advisable to have specific guidelines that govern the circumstances under which an account password is reset. For example, an organization might require that the account holder physically visit the account manager, rather than placing a telephone call, in order to verify the authenticity of the request.

Resetting Passwords

- Accounts that handle financial information are typically audited by independent financial auditors. These auditors might require that you maintain records of each time a password is reset, so that they can examine them along with other financial information.

Deleting Accounts

- Good system administration practices as related to account management will delete accounts that are no longer in use.
- If this practice is not implemented, the number of dormant accounts can grow into an unmanageable mess and pose an unnecessary security risk for the organization.
- When an account is deleted, its globally unique identifier (GUID) is also deleted and will not be reused even if you create another account using the same name.

Security Group Management

- One of the best ways to manage accounts is by grouping accounts that have similar characteristics, such as those that are assigned to a single department (OU), in a specific project group, or that access the same directories and printers.
- The group management concept saves time by eliminating repetitive steps in managing user and resource access.
- Windows Server 2008 (as well as Server 2003, and Server 2000) expand on the concept of groups from the one originally used in Windows NT Server.

Security Group Management

- The two types of groups in Windows NT Server are local groups used to manage resources on a single workstation or on domain controllers in one domain and global groups used to manage resources across multiple domains.
- With the introduction of Active Directory, newer versions of Windows Server expand the use of groups through the concept of scope of influence (or scope), which is the reach of a group for gaining access to resources in AD.
- When AD is not implemented, the scope of a group is limited to the stand-alone server, and only local groups are created.
- In contrast, the implementation of AD increases the scope from a local server or domain to all domains in a forest.

Security Group Management

- The types of groups and their associated scopes in AD are as follows:
  - Local – Used on stand-alone servers that are not part of a domain. Scope of this type of group does not go beyond the local server on which it is defined.
  - Domain local – Used when there is a single domain or to manage resources in a particular domain so that global and universal groups can access those resources.
  - Global – Used to manage group accounts from the same domain so that those accounts can access resources in the same and other domains.
  - Universal – Used to provide access to resources in any domain within any forest.

Security Group Management

- All of these types of groups can be used for both security or distribution purposes.
- Security groups are used to enable access to resources on a stand-alone server or in AD.
- Distribution groups are used for e-mail or telephone lists, to provide quick, mass distribution of information.

Implementing Local Groups

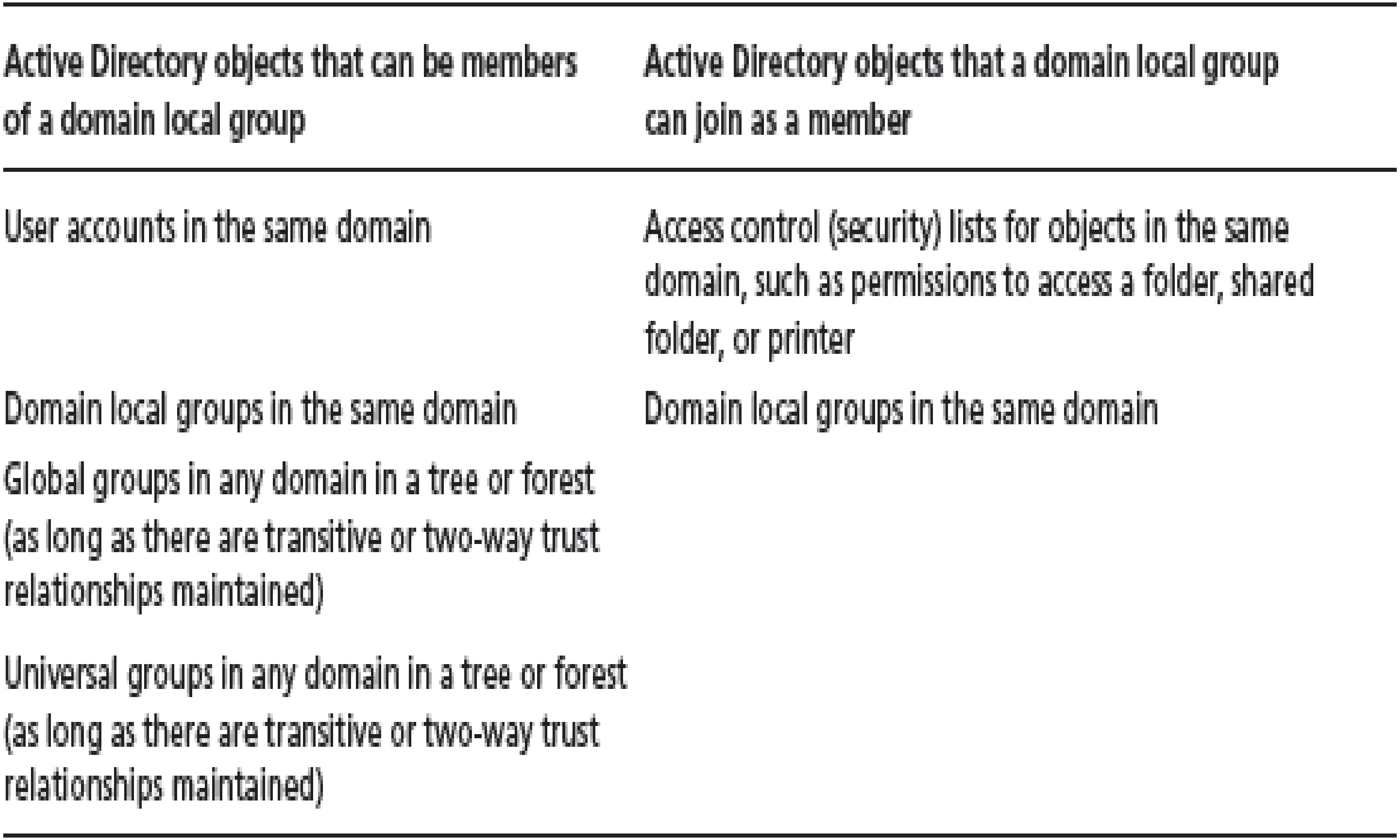
- A local security group is used to manage resources on a stand-alone computer that is not part of a domain and on member servers in a domain that is not a domain controller.

- For example, you might use a local group in a small office situation with only 5, 15, or 30 users. Consider an office with 18 user accounts, four of these are the founding partners of the firm, who manage employee hiring, payroll, schedules, etc.. Seven accounts are for consultants who specialize in one area and the remaining seven accounts are for other consultants who specialize in another area. In this situation the company may elect not to install AD and use three local groups each of which would be assigned different security access based on the resources of the server, which would include access to directories and printers.

Implementing Domain Local Groups

- A domain local group is used when AD is deployed. This type of group is typically used to manage resources in a domain and to give global groups from the same and other domains access to those resources.
- The table on the next page shows that a domain local group can contain user accounts, global groups, and universal groups.

Membership Capabilities of a Domain Local Group



Active Directory objects that can be members of a domain local group	Active Directory objects that a domain local group can join as a member
User accounts in the same domain	Access control (security) lists for objects in the same domain, such as permissions to access a folder, shared folder, or printer
Domain local groups in the same domain	Domain local groups in the same domain
Global groups in any domain in a tree or forest (as long as there are transitive or two-way trust relationships maintained)	
Universal groups in any domain in a tree or forest (as long as there are transitive or two-way trust relationships maintained)	

Implementing Domain Local Groups

- The scope of a domain local group is the domain in which the group exists, but you can convert a domain local group to a universal group as long as the domain local group does not contain any other domain local groups.
- Also, to convert any group, the domain must be in the Windows Server 2003 or Windows Server 2008 functional level. Prior to these, Windows Server did not provide the functionality to convert domain local groups to universal groups.
- Although a domain local group can contain any combination of accounts, global, and universal groups, the typical purpose of a domain local group is to provide access to resources, which means that you grant access to servers, directories, shared directories, and printers to a domain local group.

Implementing Domain Local Groups

- Under most circumstances, you should plan to put domain local groups in access control lists only, and the members of domain local groups should be mainly global groups.
- An access control list (ACL) is a list of security descriptors (privileges) that have been set up for a particular object, such as a shared directory or shared printer.
- Generally, a domain local group does not contain accounts, because account management is more efficient when you handle it through global groups.

Implementing Universal Groups

- In an Active Directory environment in which there are multiple hierarchies of domains, trees, and forests, universal security groups provide a means to span domains and trees.

- Universal group membership can include user accounts from any domain, global groups from any domain, and other universal groups from any domain.

- Universal groups are offered to provide an easy means to access any resource in a tree or among trees in a forest. If you carefully plan the use of universal groups, then you can manage security for single accounts with a minimum of effort.

- Planning is done in relation to the scope of access required for a group of accounts.

Planning Universal Groups - Guidelines

- Use global groups to hold accounts as members – and keep nesting of global groups to a minimum (or do not use nesting at all) to avoid confusion. Give accounts access to resources by making the global groups to which they belong members of domain local groups or universal groups, or both.

- Use domain local groups to provide access to resources in a specific domain. Avoid placing accounts in domain local groups – but do make domain local groups members of access control lists for specific resources in the domains, such as shared directories and printers.

- Use universal groups to provide extensive access to resources, particularly when AD contains trees and forests, or to simplify access when there are multiple domains.

Planning Universal Groups - Guidelines

- Make universal groups members of access control lists for objects in any domain, tree, or forest.
- Manage user account access by placing accounts in global groups and joining global groups to domain local or universal groups, depending on which is most appropriate to the scope required for access.

NOTE:

If you attempt to create a new universal group, but find the radio button in the Create New Object – (Group) dialog box is deactivated, this means that the domain is set up in Windows Server 2000 domain functional level and you must convert to the Windows Server 2003 or 2008 domain functional level in order to use universal groups.

Planning Universal Groups - Guidelines

- The example on the following page illustrates setting up access for the executive council in a college that has three domains.

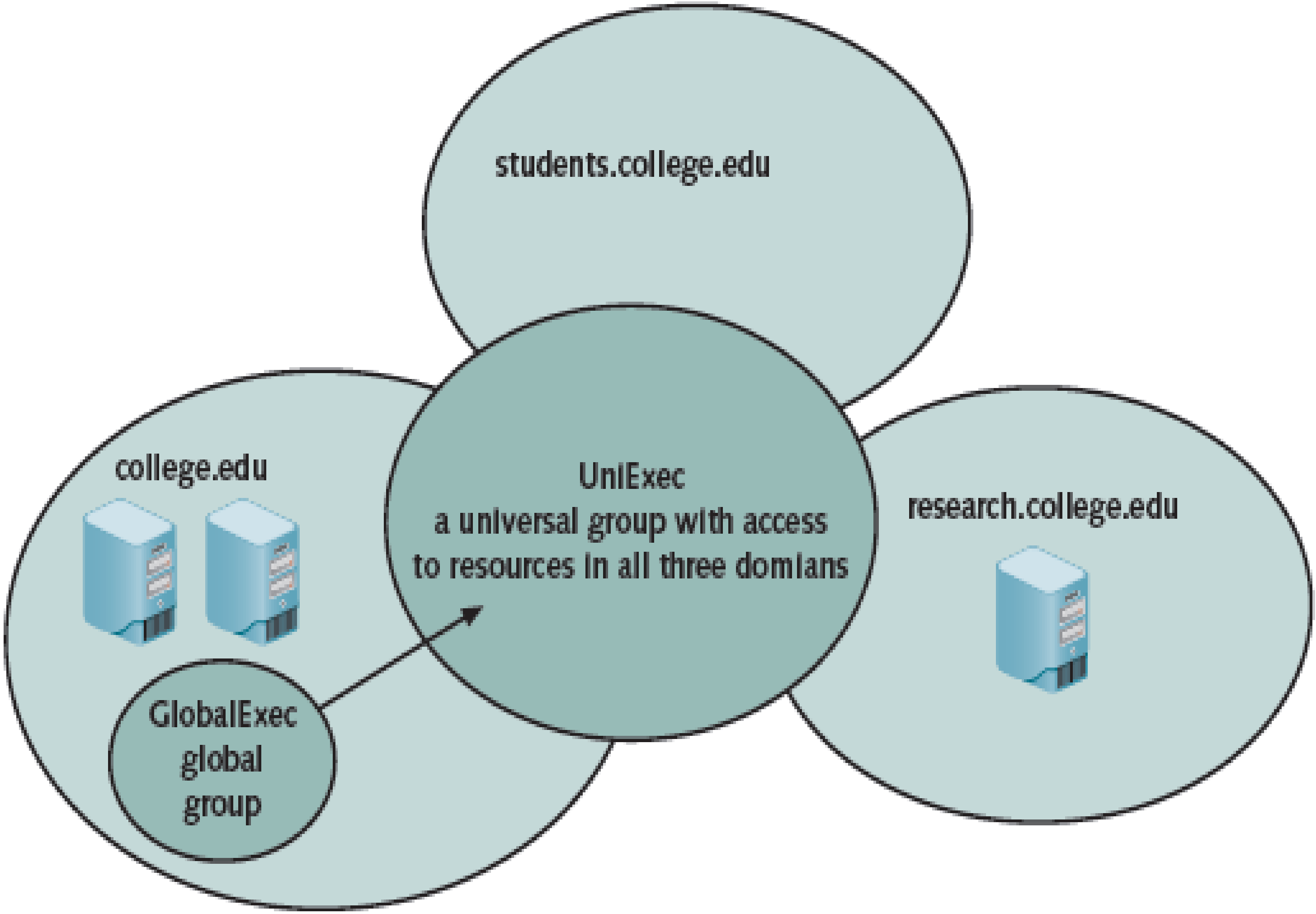
- Alternatives are:

  - Create one universal group that has access to all resources in the three domains.

  - Create one global group containing the president and vice presidents, and make that global group a member of the universal group.

- The second approach is the better of the two as this model has only two groups to manage. This is illustrated on the next page.

Planning Universal Groups - Guidelines



Properties of Groups

- All of the groups that you create in Windows Server 2008 have a set of properties that can be configured.
- You can configure the properties of a specific group by double-clicking that group in the Local Users and Groups tool for a stand-alone (non-domain) or member server, or in the Active Directory Users and Computers tool for domain controller servers in a domain.
- The properties that you can configure are listed and briefly explained on the next page. You will get some practice doing this in project six.

Properties of Groups

- Group properties are configured with four different tabs:
  - General: used to enter a description of the group, change the scope and type of the group, and provide email addresses for a distribution group.
  - Members: used to add members to a group, such as adding user accounts to a global group, and enables members to be removed.
  - Member Of: used to make the group a member of another group, or to remove the group’s membership.
  - Managed By: user to establish an account or group that will manage the group, if the manager is other than the server administrator. Also, sets the location, phone and fax numbers of the manager.

User Account Management With Active Directory

- When AD is installed and the server is a domain controller, you control user accounts from the Active Directory Users and Computers tool either from the Administrative Tools menu or as a MMC (Microsoft Management Console) snap-in.
- You create each new account by entering account information and password controls.

NOTE

If you are using AD and are working on a DC (domain controller), Windows Server 2008 will not allow you to install the Local Users and Groups snap-in, because you must use the AD Users and Computers snap-in instead since AD controls all user accounts in the domain, so there are no local users within the domain.

User Account Management With Active Directory

- In project six you will get some experience creating user accounts and establishing OUs within the `savn.local` domain.