Doména, Active Directory (AD)

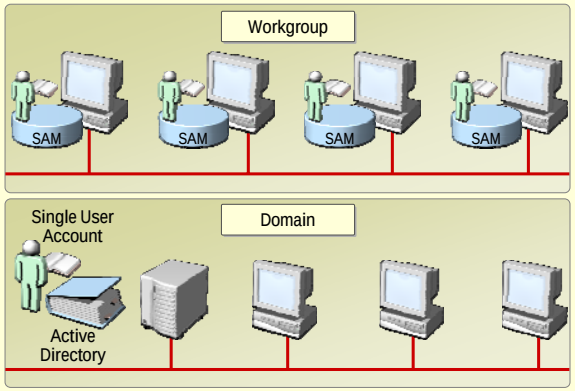
http://www.cs.vsb.cz/navrat

Jan Žák

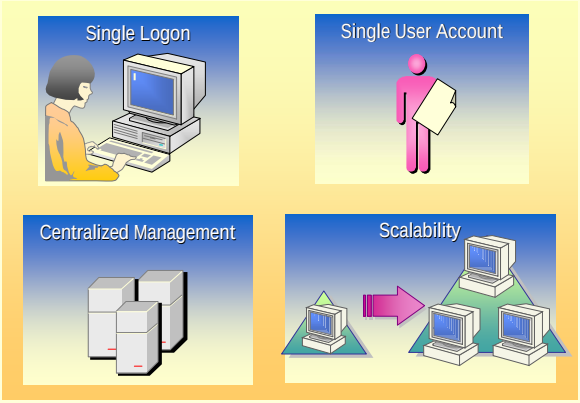
Agenda

- Domain, terms
- DCPROMO
- OU
- PC and User accounts
- Groups
- Functional levels
- FSMOs
- Administrative tools

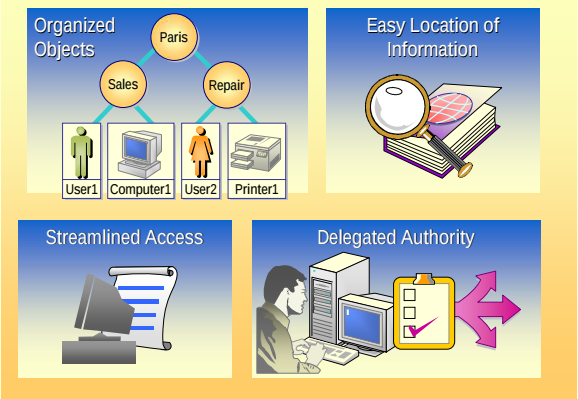
Deciding on a Workgroup or Domain Installation



Features of a Domain

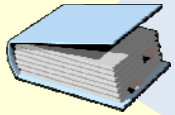


Benefits of a Domain



What Is a Directory Service?

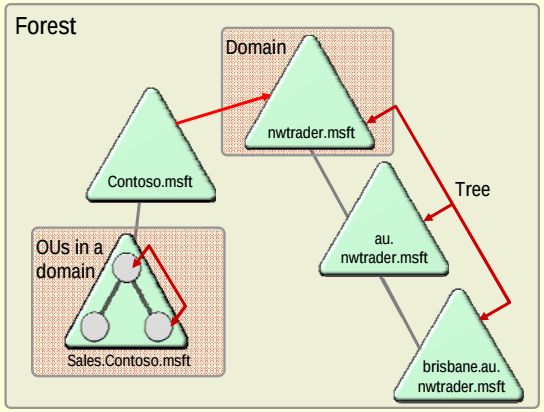
- Identifies resources
- Provides a consistent way to:
  - –Name
  - –Describe
  - –Locate
  - –Access
  - –Manage
  - –Secure



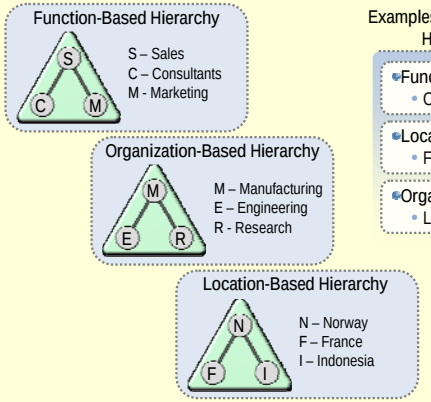
Active Directory Benefits

- DNS integration
- Scalability
- Centralized management
- Delegated administration

Active Directory Terms



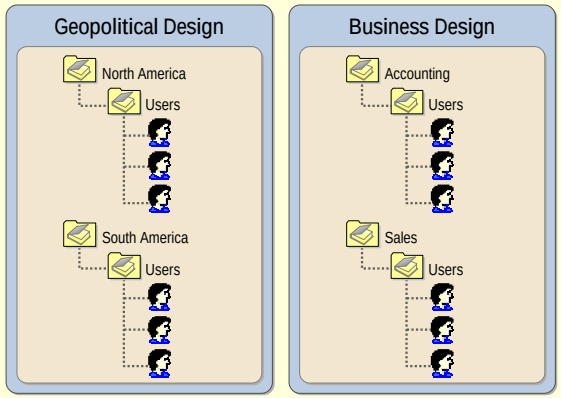
Organizational Unit Hierarchical Models



Examples of Hybrid-Based Hierarchies

- Function
  - Organization
- Location
  - Function
- Organization
  - Location

User Account Placement in a Hierarchy



Names Associated with Organizational Units

Name	Example
LDAP relative distinguished name	**OU=MyOrganizationalUnit**
LDAP distinguished name	**OU=MyOrganizationalUnit, DC=microsoft, DC=com**
Canonical name	**Microsoft.com/MyOrganizationalUnit**

DCPROMO

- DCPROMO is used to promote a stand-alone/member server to a domain controller and vice-versa
- see more: http://support.microsoft.com/kb/238369

FSMOs

- **Schema Master**: The schema master domain controller controls all updates and modifications to the schema*. To update the schema of a forest, you must have access to the schema master. There can be **only one** schema master **in the whole forest**. ZJ1
- **Domain naming master**: The domain naming master domain controller controls the addition or removal of domains in the forest. There can be **only one** domain naming master **in the whole forest.**
- **Infrastructure Master**: The infrastructure is responsible for updating references from objects in its domain to objects in other domains. At any one time, there can be **only one** domain controller acting as the infrastructure master **in each domain**.
- **Relative ID (RID) Master**: The RID* master is responsible for processing RID pool requests from all domain controllers in a particular domain. At any one time, there can be **only one** domain controller acting as the RID master **in the domain**. ZJ2
- **PDC Emulator**: The PDC emulator is a domain controller that advertises itself as the primary domain controller (PDC) to workstations, member servers, and domain controllers that are running earlier versions of Windows. For example, if the domain contains computers that are not running Microsoft Windows XP Professional or Microsoft Windows 2000 client software, or if it contains Microsoft Windows NT backup domain controllers, the PDC emulator master acts as a Windows NT PDC. It is also the Domain Master Browser, and it handles password discrepancies. At any one time, there can be **only one** domain controller acting as the PDC emulator master **in each domain** in the forest.

Snímek 12

ZJ1 Schema defines which objects can be created in domain (computer object, user object...) and also defines from which atributes objects can be created.

Zak Jan; 12.10.2006

ZJ2 In Windows 2000/2003, the relative identifier (RID) is the part of a security ID (SID) that uniquely identifies an account or group within a domain.

SID
S-1-5-12-7723811915-3361004348-033306820-515

Zak Jan; 12.10.2006

Accounts and groups

Names Associated with Domain User Accounts

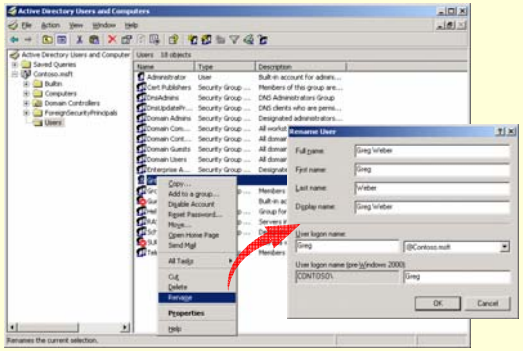
Name	Example
User logon name	**Tadams**
Pre-Windows 2000 logon name	**contoso\Tadams**
User principal logon name	**Tadams@contoso.msft**
LDAP distinguished name	**CN=terry adams,ou=sales,dc=contoso,dc=msft**
LDAP relative distinguished name	**CN=terry adams**

Properties Associated with User Accounts

The Properties dialog box for a user account contains:

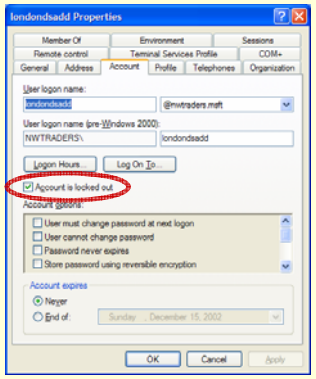
Renaming a User Account

The Rename User dialog box



What Are Locked-Out User Accounts?

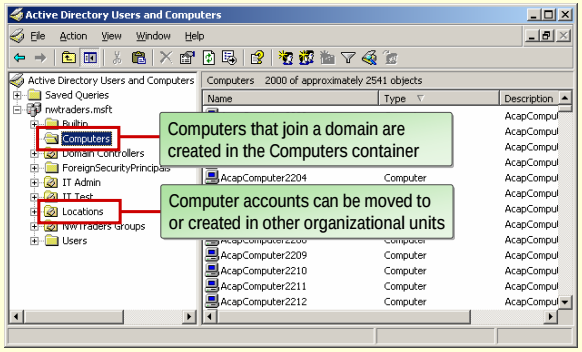
- Account lockout thresholds:
  - Define the number of failed logon attempts
  - Prevent hackers from guessing user passwords
- Logon failures can occur:
  - At the logon screen
  - At a screen saver protected by a password
  - When accessing network resources



What Is a Computer Account?

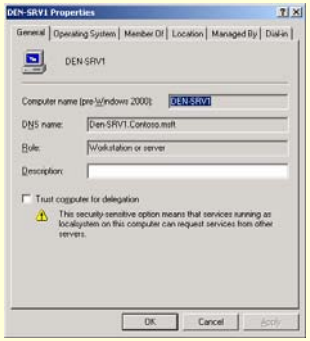
- Identifies a computer in a domain
- Provides a means for authenticating and auditing computer access to the network and to domain resources
- Is required for every computer running:
  - Windows Server 2003
  - Windows XP Professional
  - Windows 2000
  - Windows NT

Where Computer Accounts Are Created in a Domain



Properties Associated with Computer Accounts

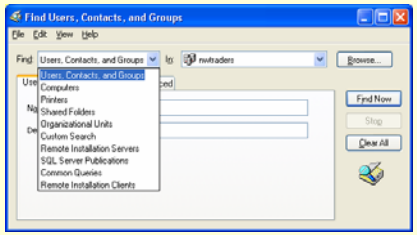
The Properties dialog box for a computer account contains:



Search Types

Basic query criteria include:

- Object type
- Location
- General values associated with the object, such as name and description



What Are Domain Functional Levels?

	Windows 2000 mixed (default)	Windows 2000 native	Windows Server 2003	Windows Server 2003 interim
Domain controllers supported	**Windows NT Server 4.0, Windows 2000, Windows Server 2003**	**Windows 2000, Windows Server 2003**	**Windows Server 2003**	**Windows NT Server 4.0, Windows Server 2003**
Group scopes supported	**Global, domain local**	**Global, domain local, universal**	**Global, domain local, universal**	**Global, domain local**

What Are Groups?

Groups simplify administration by enabling you to assign permissions for resources

Groups are characterized by scope and type

Group type	Description
Security	**Used to assign user rights and permissions** **Can be used as an e-mail distribution list**
Distribution	**Can be used only with e-mail applications** **Cannot be used to assign permissions**

What Are Global Groups?

	Global group rules
Membership can include	**Mixed functional level:** User and computer accounts from same domain **Native functional level:** User and computer accounts and global groups from same domain
Can be a member of	**Mixed functional level:** Domain local groups **Native functional level:** Universal and domain local groups in any trusting domain and global groups in the same domain
Scope	Visible in its own domain and all trusting domains
Permissions	All domains in the forest and trusting domains

What Are Universal Groups?

	Universal group rules
Membership can include	• **Mixed functional level:** Not applicable • **Native functional level:** User accounts, global groups, and universal groups from any domain in the forest
Can be a member of	• **Mixed functional level:** Not applicable • **Native functional level:** Domain local or universal groups in any domain
Scope	Visible in all domains in the forest and all trusting domains
Permissions	All domains in the forest and all trusting domains

What Are Domain Local Groups?

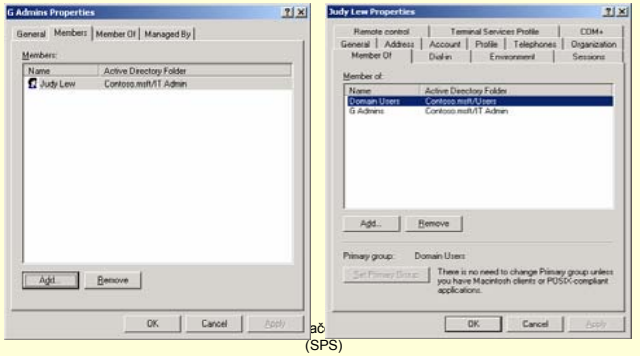
	Domain local group rules
Membership can include	• **Mixed functional level and Windows interim 2003:** User and computer accounts and global groups from any trusted domain • **Native functional level:** User and computer accounts, global and universal groups from any domain in the forest or trusted domains, plus domain local groups from the same domain
Can be a member of	• **Mixed functional level and Windows interim 2003: None** • **Native functional level:** Domain local groups in the same domain
Scope	Visible only in its own domain
Permissions	Domain to which the domain local group belongs

What Are Local Groups?

	Local group rules
Membership can include	Local user accounts, domain user and computer accounts, global and universal groups from the computer's domain and trusted domains
Can be a member of	Not applicable

Adding and Removing Members from a Group

Group membership can be modified by using Active Directory Users and Computers or the dsmod command

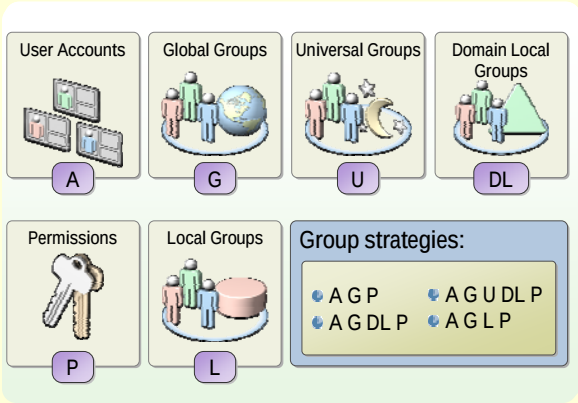


What Is Group Nesting?

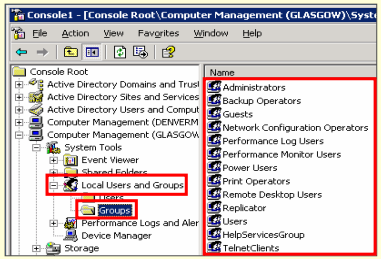
- *Group nesting* means adding a group as a member of another group

  - Nest groups to consolidate group management
  - Nesting options depend on the domain functional level

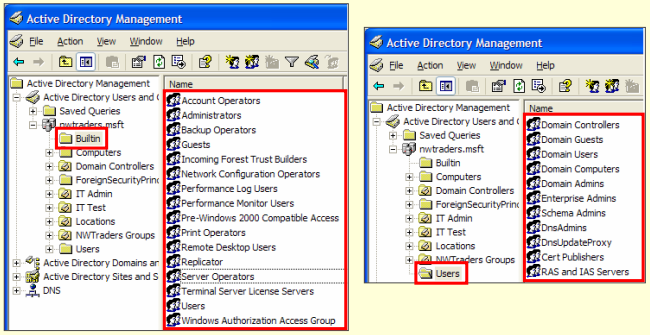
Group Strategies



Default Groups on Member Servers



Default Groups in Active Directory



What Are Administrative Tools?

- Commonly used administrative tools:
  - Active Directory Users and Computers
  - Active Directory Sites and Services
  - Active Directory Domains and Trusts
  - Computer Management
  - DNS
  - Remote Desktops
- Install to perform remote administration
- adminpak.msi (cd:\i386\adminpak.msi or from MS web)

Other admin tools

- Terminal services or remote desktop
- VNC, PC ANYWHERE etc
- Remote registry
- Telnet
- PATROL Central and other specific tools

... more info in next lessons ☺