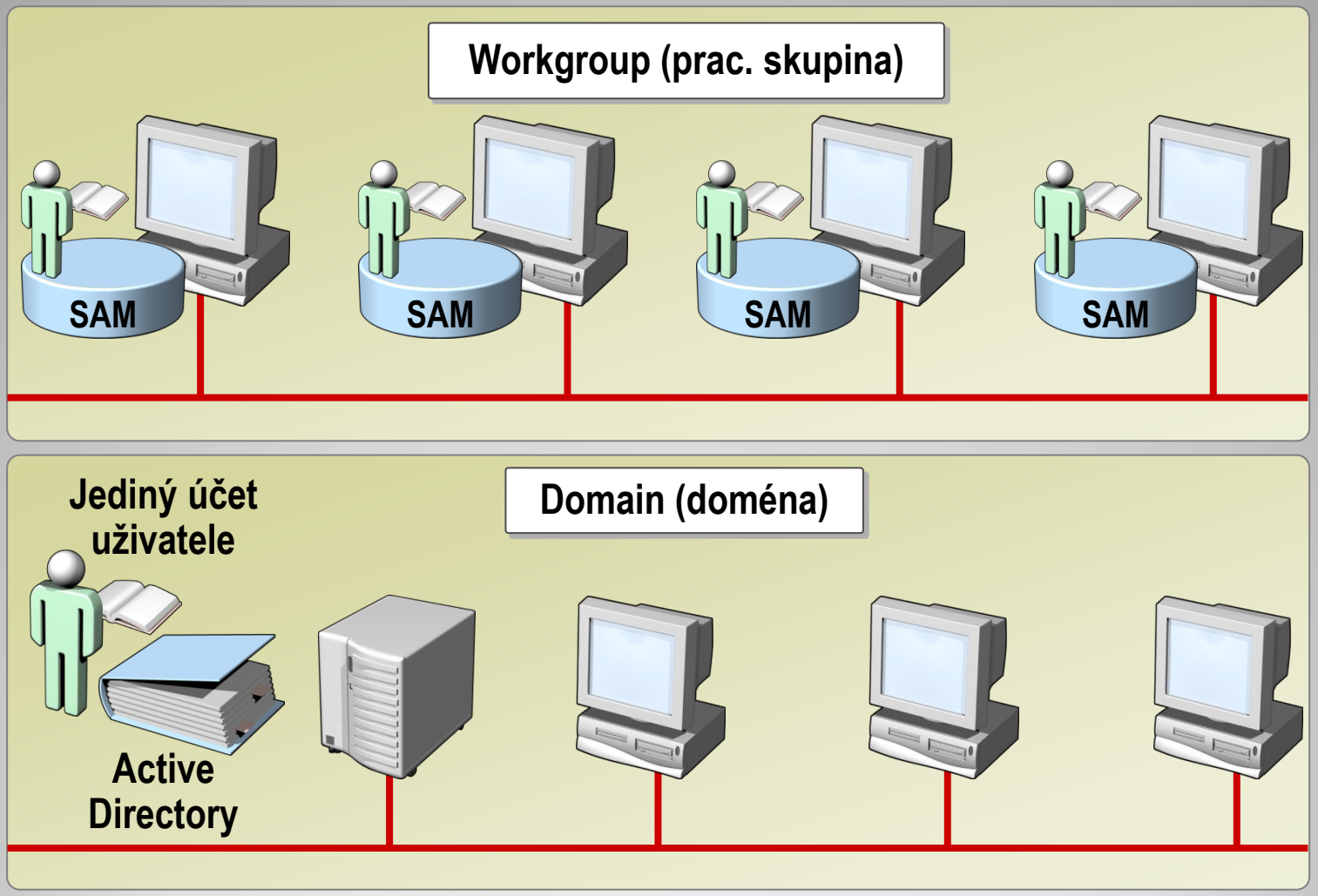
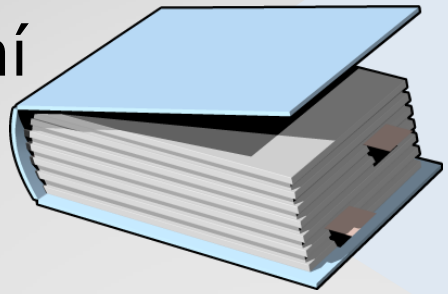
Active Directory
(Active Directory Directory Services)



Workgroup vs. Domain

K čemu adresářové služby?

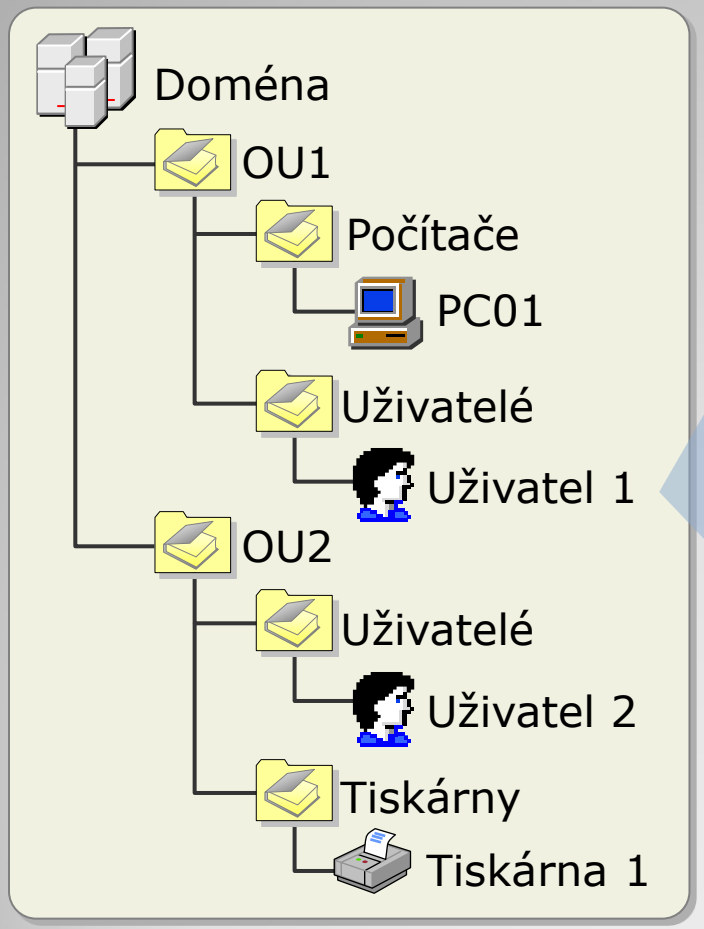
- Identifikace zdrojů
- Poskytuje možnosti pro:
  - Pojmenování
  - Popis
  - Umístění a vyhledávání
  - Přístup
  - Správu
  - Zabezpečení



Vlastnosti AD DS

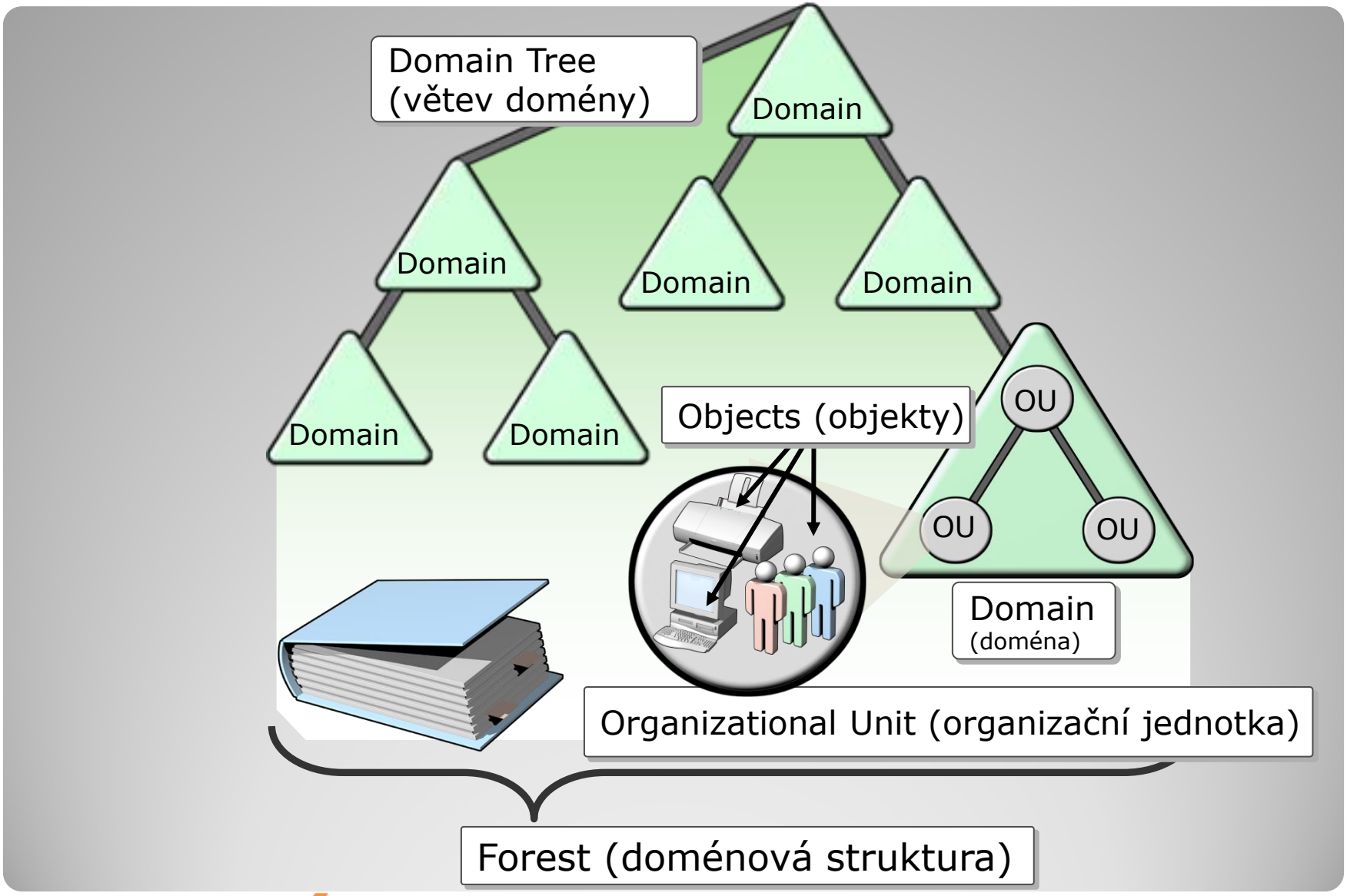
- **Integrace DNS**
- **Škálovatelnost**
- **Centralizace správy**
- **Delegování oprávnění**

Strukturované úložiště informací o lidech a zdrojích v rámci organizace

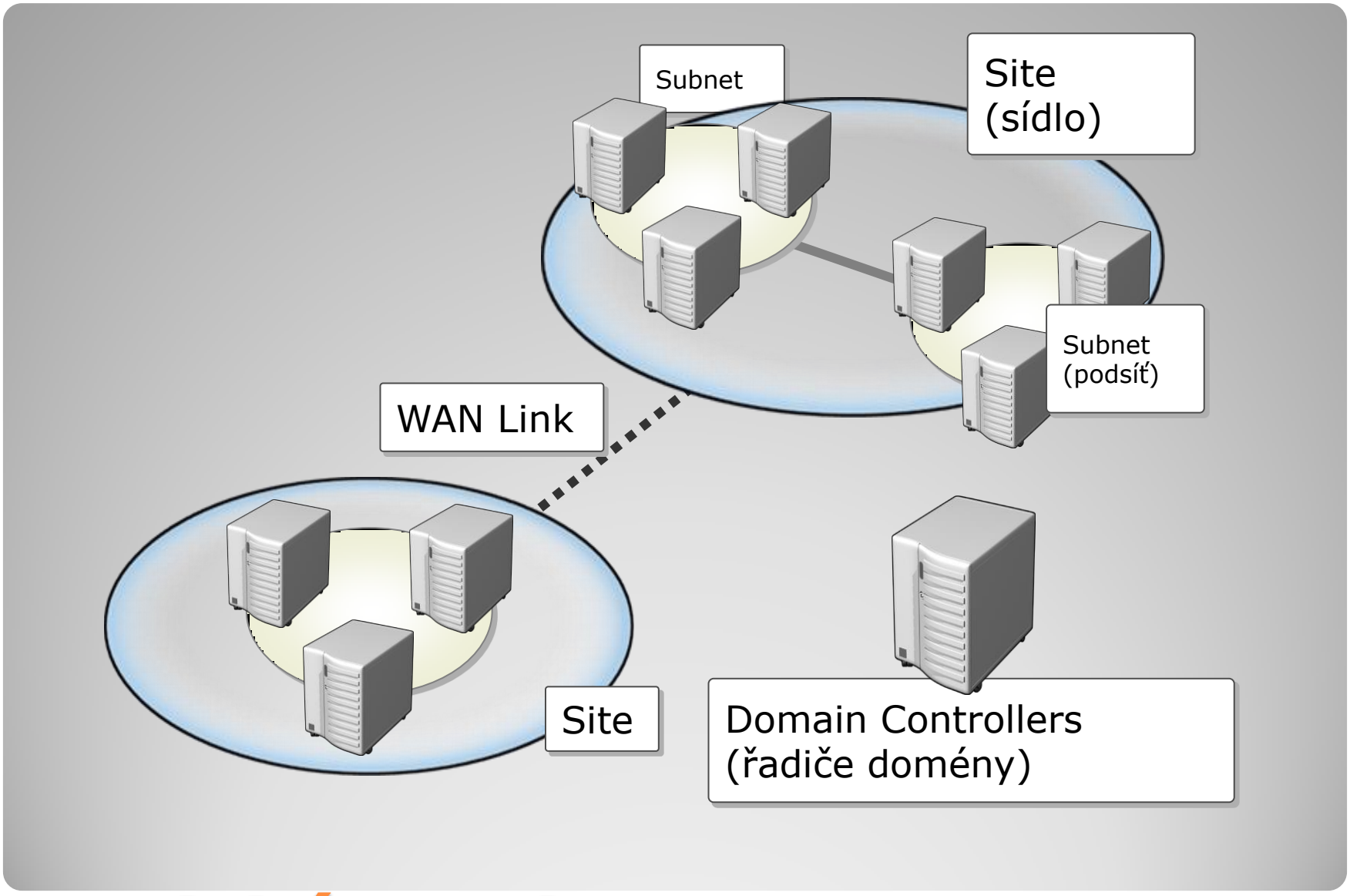


František Uživatel	
Atribut	**Hodnota**
Jméno	František
Příjmení	Uživatel
Budova	15
Patro	3
Os. číslo	567889

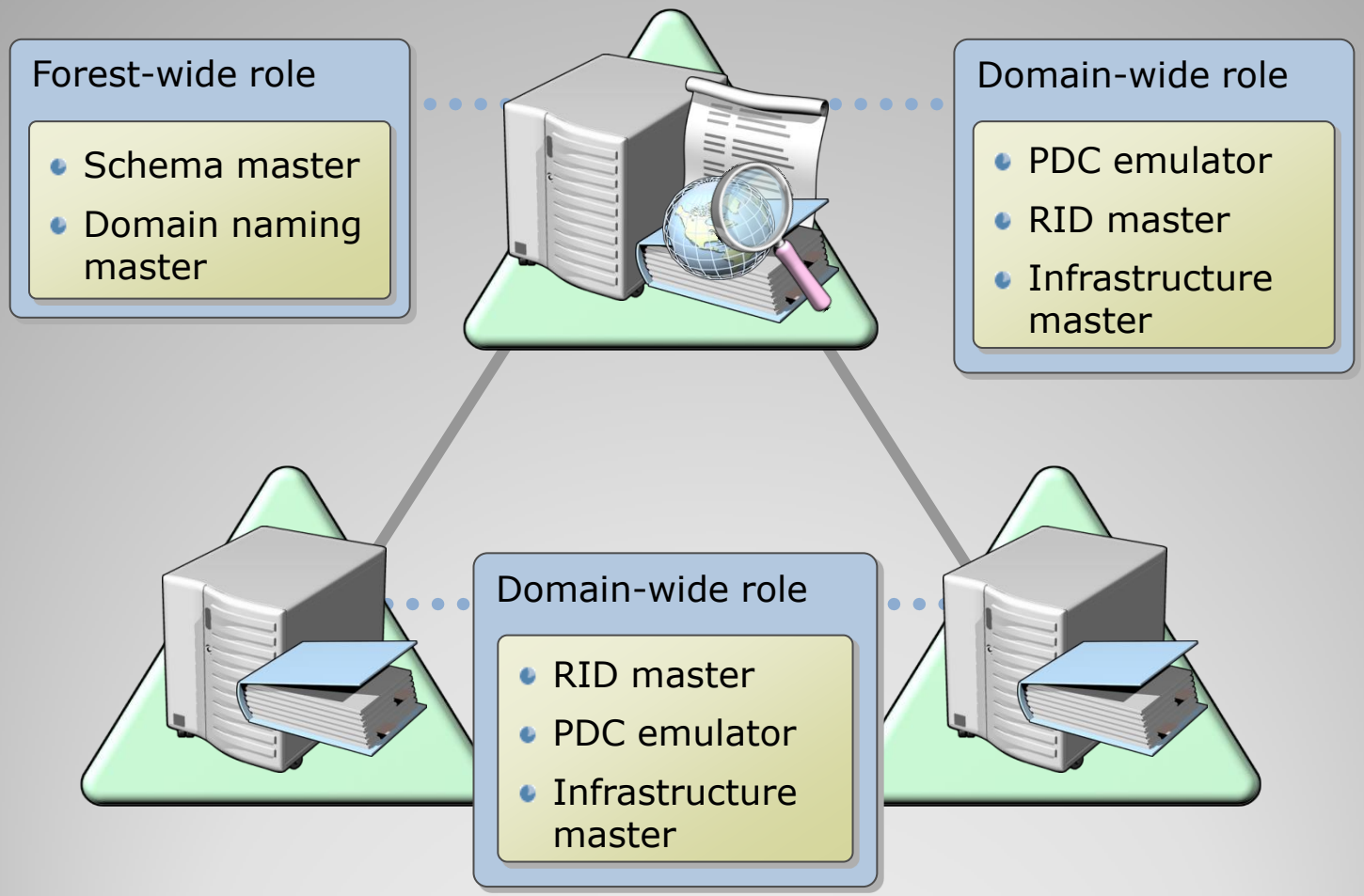
Adresářová služba - příklad



Logická struktura AD



Fyzická struktura AD



FSMO

(Flexible Single Master Operations Roles)

- **Hlavní server schémat (Schema Master)**: Jeden držitel role hlavního serveru v jedné doménové struktuře. Držitel role FSMO hlavního serveru schémat je řadič domény zodpovědný za aktualizace ve schématu adresářů.
- **Hlavní server názvů domén (Domain Naming Master)**: Jeden držitel role hlavního serveru v jedné doménové struktuře. Držitel role FSMO hlavního serveru názvů domén je řadič domény zodpovědný za provádění změn v oboru názvů adresáře založeném na doméně v celé doménové struktuře.
- **Hlavní server infrastruktury (Infrastructure Master)**: Jeden držitel role hlavního serveru v jedné doméně. Držitel role FSMO infrastruktury je řadič domény zodpovědný za aktualizaci identifikátoru SID a rozlišujícího názvu v odkazu na objekt mezi doménami.
- **Hlavní server relativních ID (RID Master)**: Jeden držitel role hlavního serveru v jedné doméně. Držitel role FSMO hlavního serveru relativních ID (RID) je jeden řadič domény zodpovědný za zpracování požadavků fondu RID ze všech řadičů domény v dané doméně.
- **Emulátor primárního řadiče domény (PDC Emulator)**: Jeden držitel role hlavního serveru v jedné doméně. Držitel role FSMO emulátoru primárního řadiče domény je řadič domény systému Windows, který se pracovním stanicím, členským serverům a řadičům domény, které používají starší verze systému Windows, inzeruje jako primární řadič domény. Jedná se také o hlavní prohledávač domény, který zároveň zpracovává neshody v heslech.

FSMO

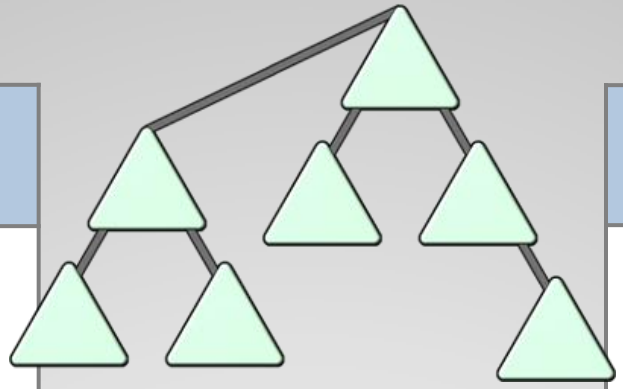
- **Schema Master**: The schema master domain controller controls all updates and modifications to the schema*. To update the schema of a forest, you must have access to the schema master. There can be **only one** schema master **in the whole forest**.
- **Domain naming master**: The domain naming master 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**.
- **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/Vista/7 or Microsoft Windows 200x 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.

FSMO (EN)

Schéma

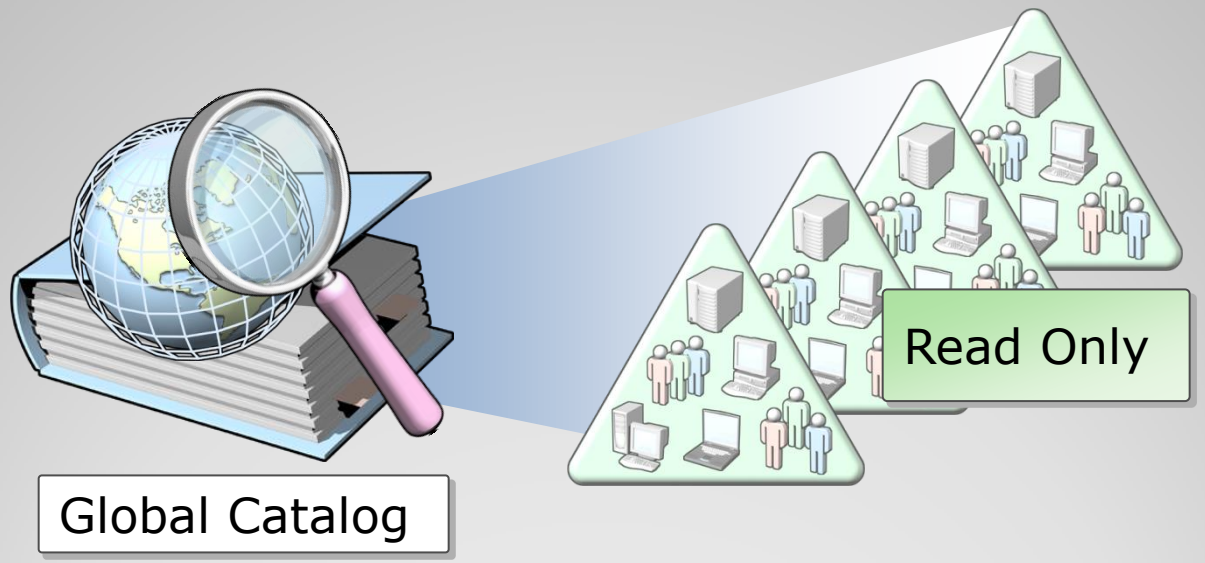
- Definice tříd a atributů objektů, platná pro celý forest. Je možné je dále rozšiřovat.
- Změny ve schématu je možné deaktivovat a modifikovat.

Třídy objektů	
	User
	Computer
	Printer



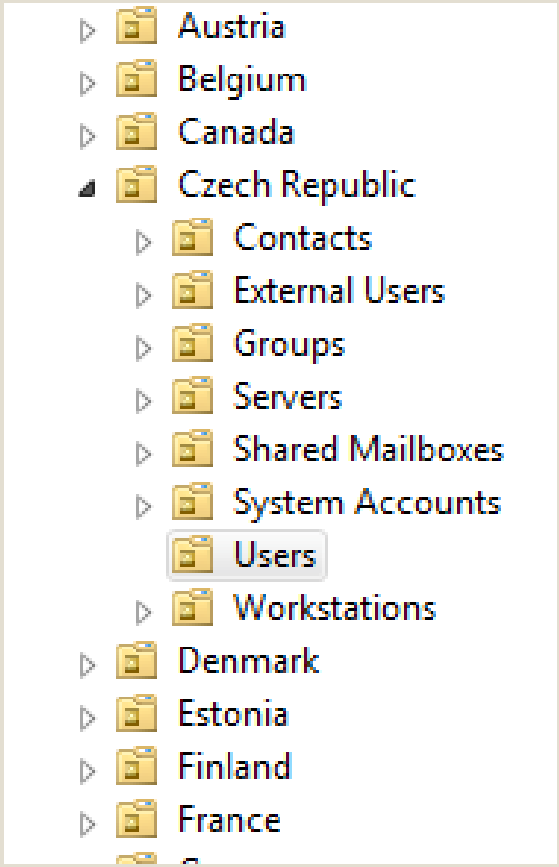
Atributy
accountExpires
department
distinguishedName
directReports
dNSHostName
operatingSystem
repsFrom
repsTo
firstName
lastName

- Obsahuje podmnožinu atributů pro všechny objekty v AD (pouze pro čtení)
- Umožňuje vyhledávat objekty v různých doménách
- Je další „rolí“ DC

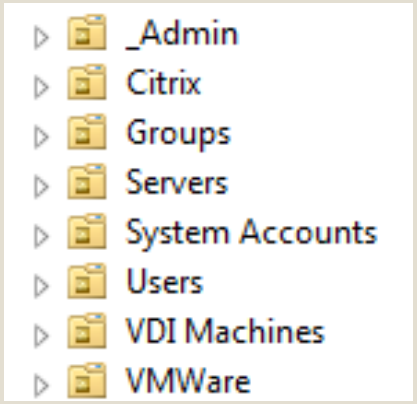


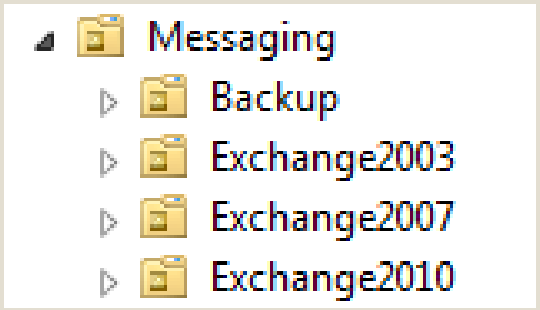
Global Catalog
(globální katalog)

Geopolitický model



Obchodní model





Umístění objektů ve struktuře organizačních jednotek

Jméno	Příklad
LDAP relative distinguished name	**OU=Ostrava**
LDAP distinguished name	**OU=Ostrava, DC=vsb, DC=com**
Canonical name	**vsb.com/Ostrava**
SID	**S-1-5-21-1417401333-308236325-725345543-108617**
GUID	**8402a48a-680c-41a7-c5ba-25175c5ece01**

Identifikace objektů

DCPROMO

- Standalone server (v prac. skupině)
- Member server (člen domény)
- Domain controller (řadič domény)

- DCPROMO se používá pro povýšení stand-alone/member serveru na domain controller (řadič domény), event. pro odebrání role AD DS.
- http://technet.microsoft.com/en-us/library/cc732887%28WS.10%29.aspx

One-way trust
: One domain allows access to users on another domain, but the other domain does not allow access to users on the first domain.

Two-way trust
: Two domains allow access to users on both domains.

Trusted domain
: The domain that is trusted; whose users have access to the trusting domain.

Transitive trust
: A trust that can extend beyond two domains to other trusted domains in the forest.

Intransitive trust
: A one way trust that does not extend beyond two domains.

Explicit trust
: A trust that an admin creates. It is not transitive and is one way only.

Trusts

Umožňují přístup uživatelů z jedné domény ke zdrojům v jiné doméně.

Cross-link trust

An explicit trust between domains in different trees or in the same tree when a descendant/ancestor (child/parent) relationship does not exist between the two domains.

Shortcut

Joins two domains in different trees, transitive, one- or two-way.

Forest trust

Applies to the entire forest. Transitive, one- or two-way.

Realm

Can be transitive or nontransitive (intransitive), one- or two-way.

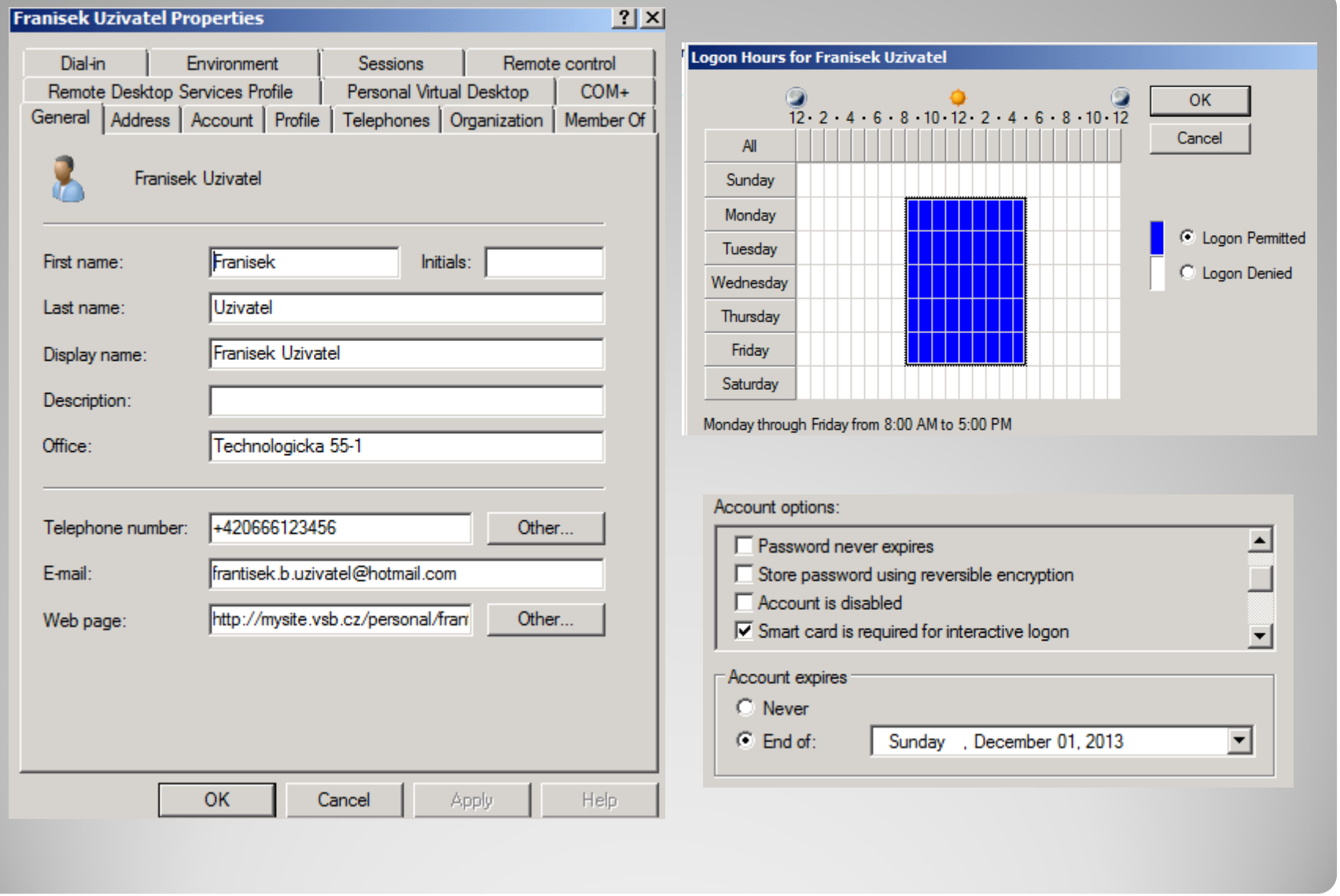
External

Connect to other forests or non-AD domains. Nontransitive, one- or two-way.

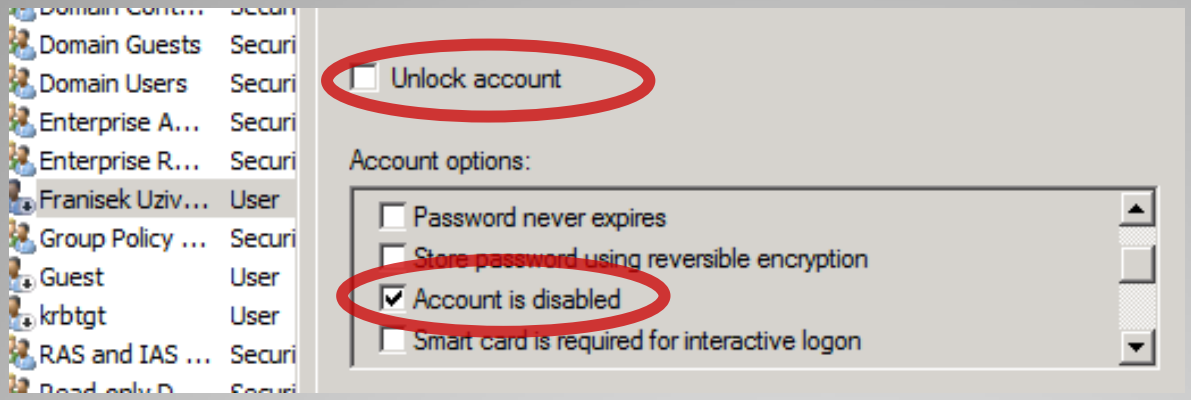
Trusts

Účty objektů

Uživatelé a počítače

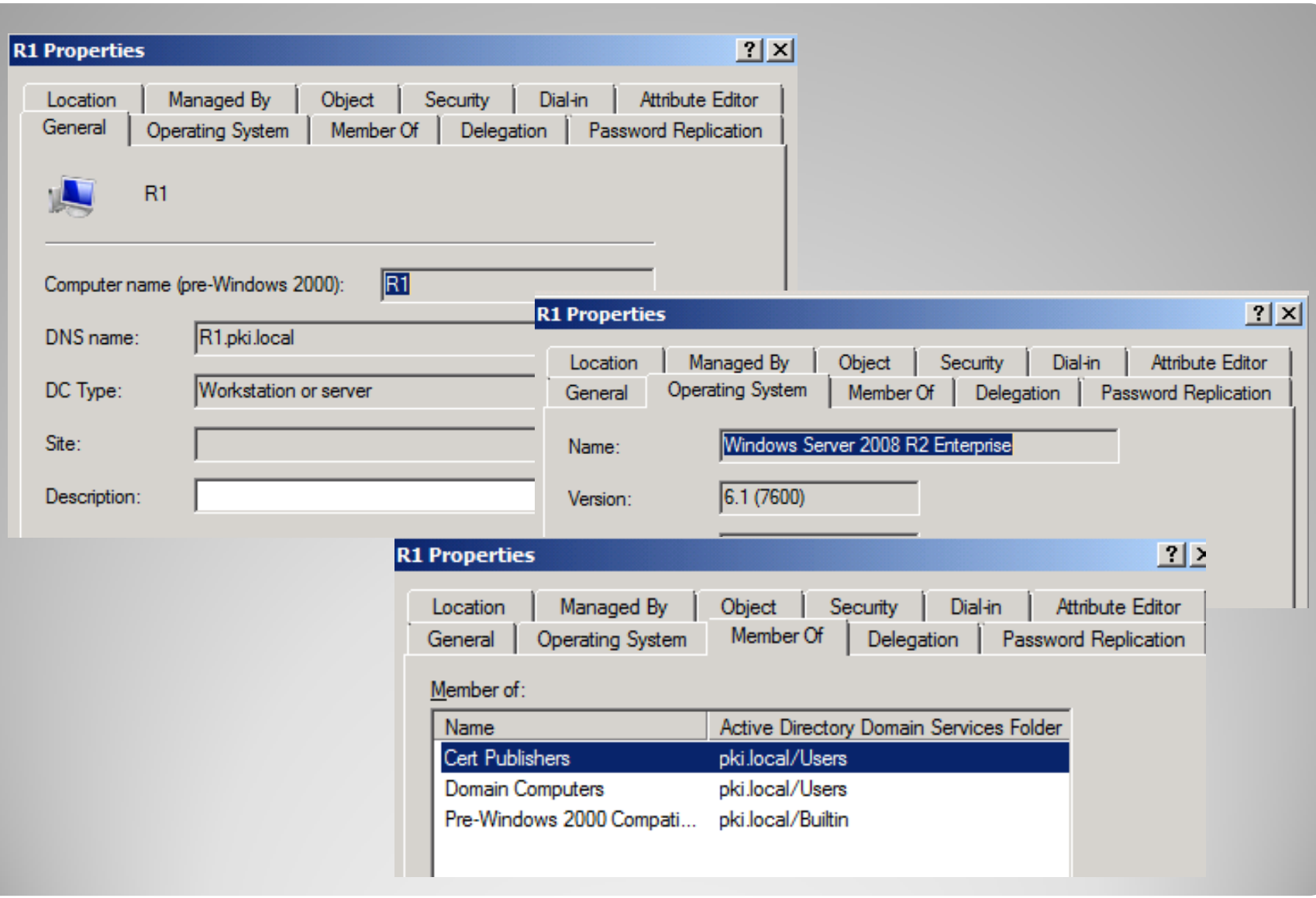


Vlastnosti uživatelského účtu



- Citlivost zamčení účtu:
  - Počet neúspěšných pokusů o přihlášení
  - Ochrana před odhadnutím hesla
  - Pozor např. na Win32/Conficker a další!
- Selhání přihlášení při:
  - Přihlášení k účtu
  - Odemčení spořiče obrazovky s heslem
  - Přístup k síťovým prostředkům

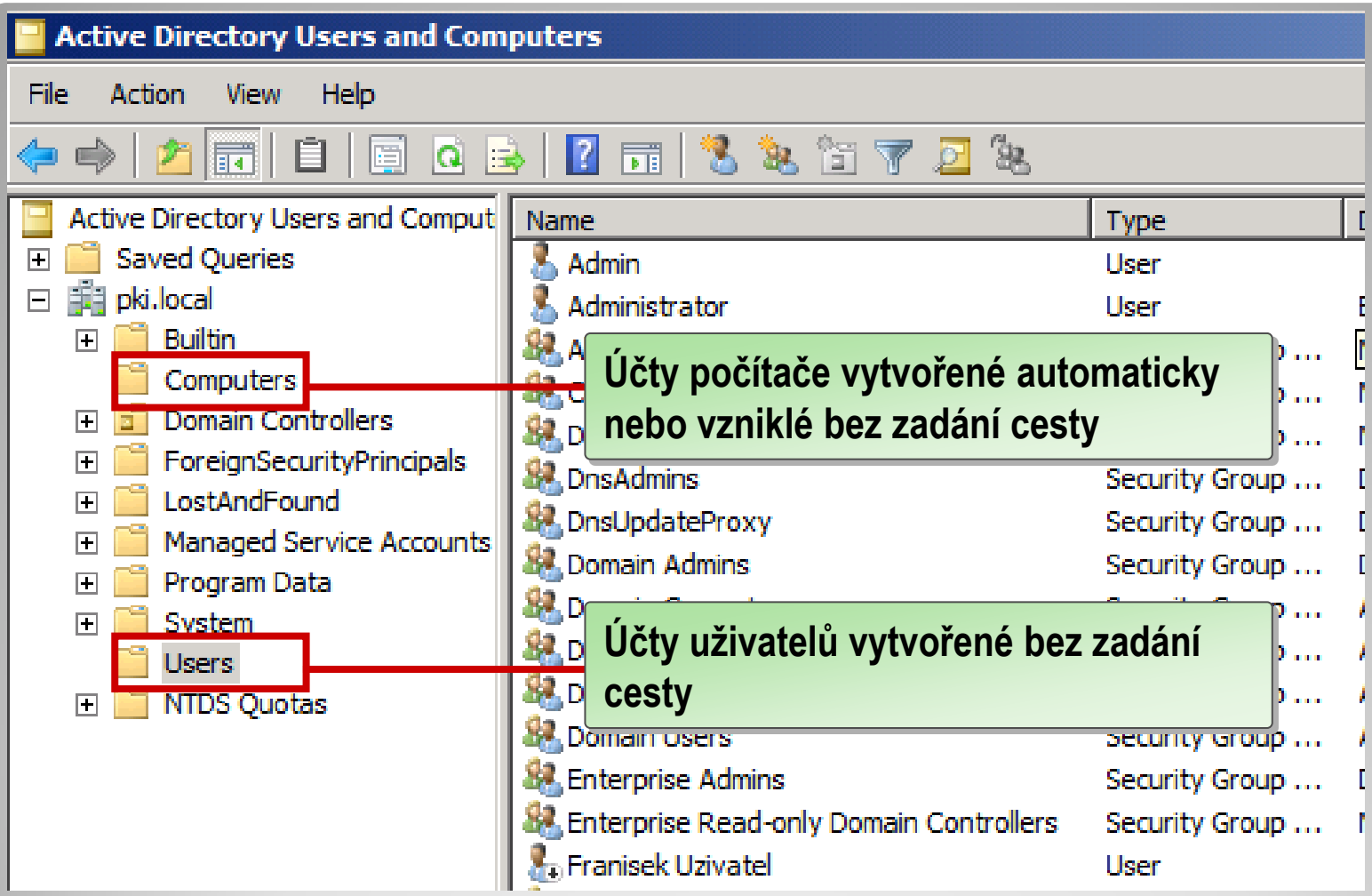
Zamčené a zakázané účty



Vlastnosti účtu počítače

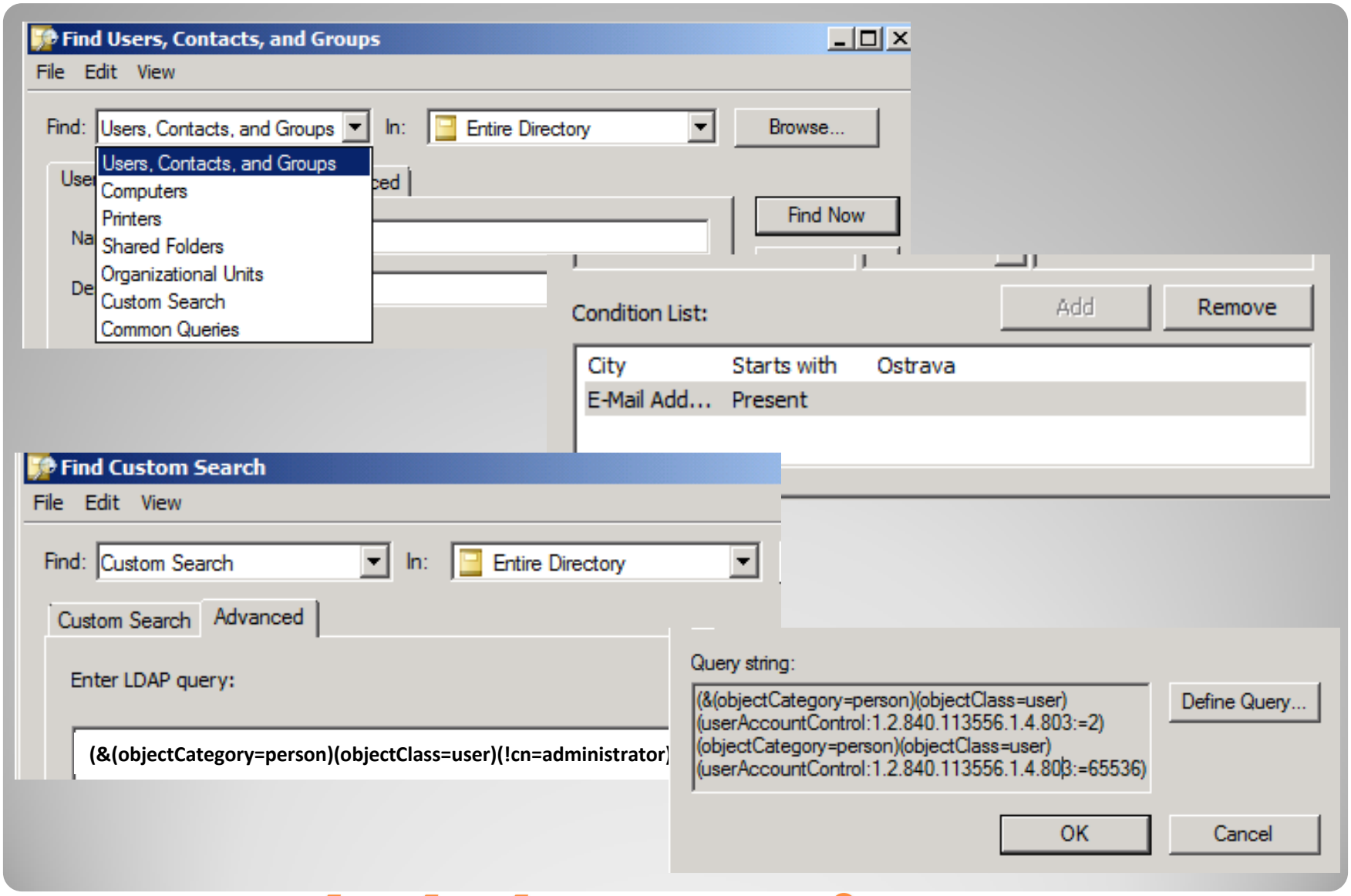
Proč mají počítače účty

- Identifikují počítače v doméně
- Umožňují ověřování a audit přístupů k síti a síťovým prostředkům
- Umožňují nastavit práva pro počítače (např. při instalaci softwaru)
- Využívají je počítače s OS Windows
  - Windows Server 2000 a novjší
  - Windows 2000/XP/Vista/7/8…
  - Windows NT
  - „Home" edice nelze připojit do domény
- Mohou je využívat i jiné OS (Red Hat Enerprise Linux, OS X …)



- Je možné definovat vlastní výchozí kontejnery
- Obvykle se objekty přesouvají do OU

Výchozí kontejnery pro účty



Vyhledávání objektů

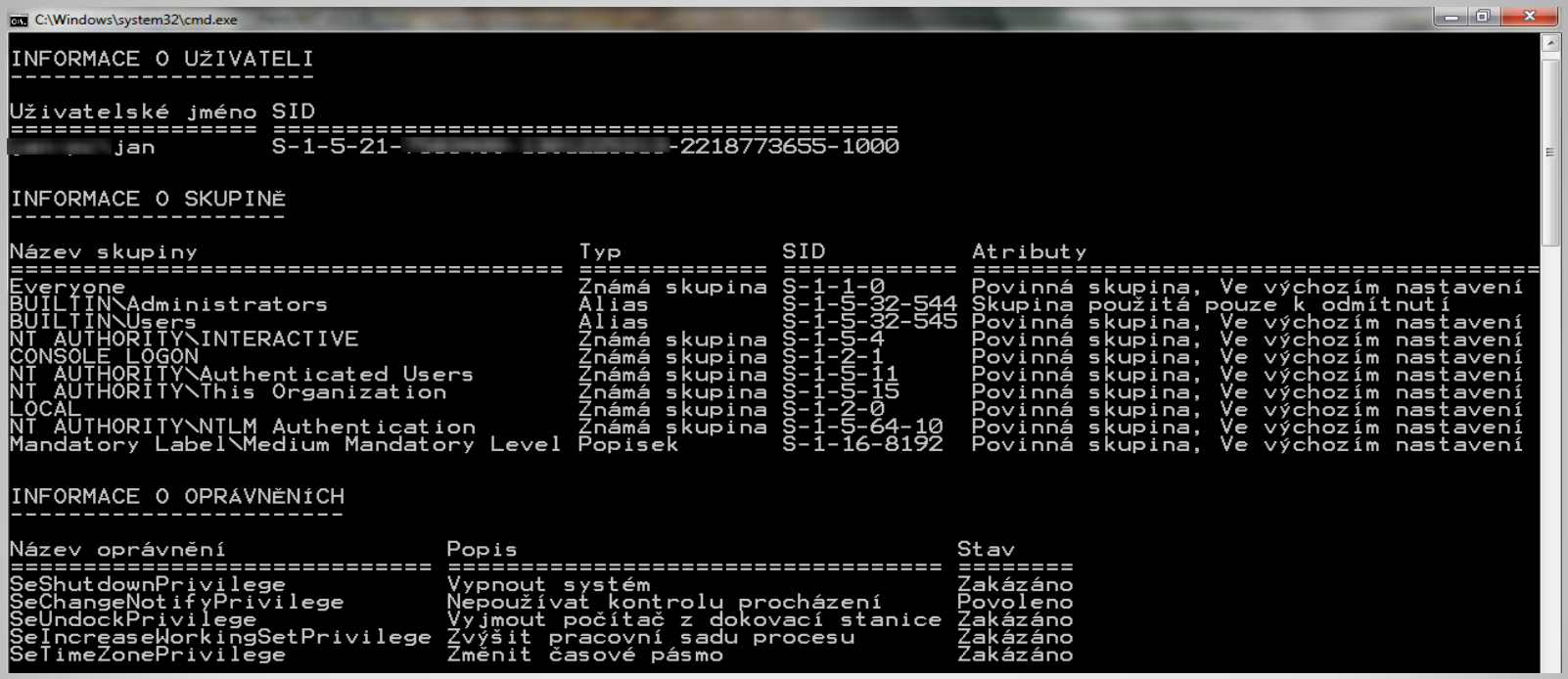
Modely zabezpečení

Účty skupin
Přístupová práva

Autentizační protokoly

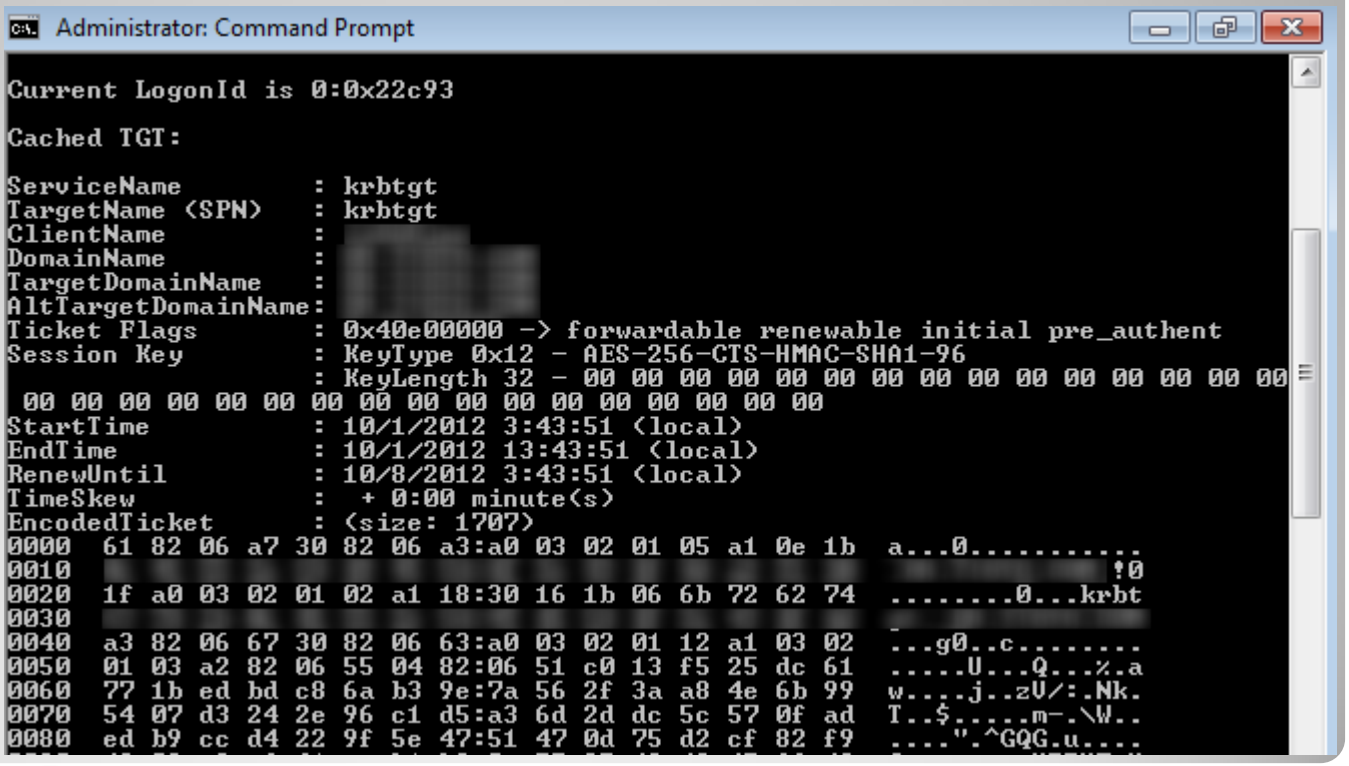
- **Kerberos V 5** Standard protokolu pro autentizaci uživatelů a systémů. Je primárním autentizačním mechanizmem pro Windows 2000 a vyšší.
- **NT LAN Manager (NTLM)** Primární autentizační protokol pro systémy Windows NT.
- **Secure Socket Layer/Transport Layer Security (SSL/TLS)** Primární mechanizmus pro autentizaci pro přístupy k zabezpečeným webovým serverům.

- Po ověření uživatele je vytvořena datová struktura „**access token**“ a „**session**“ uživatele.
- whoami /all



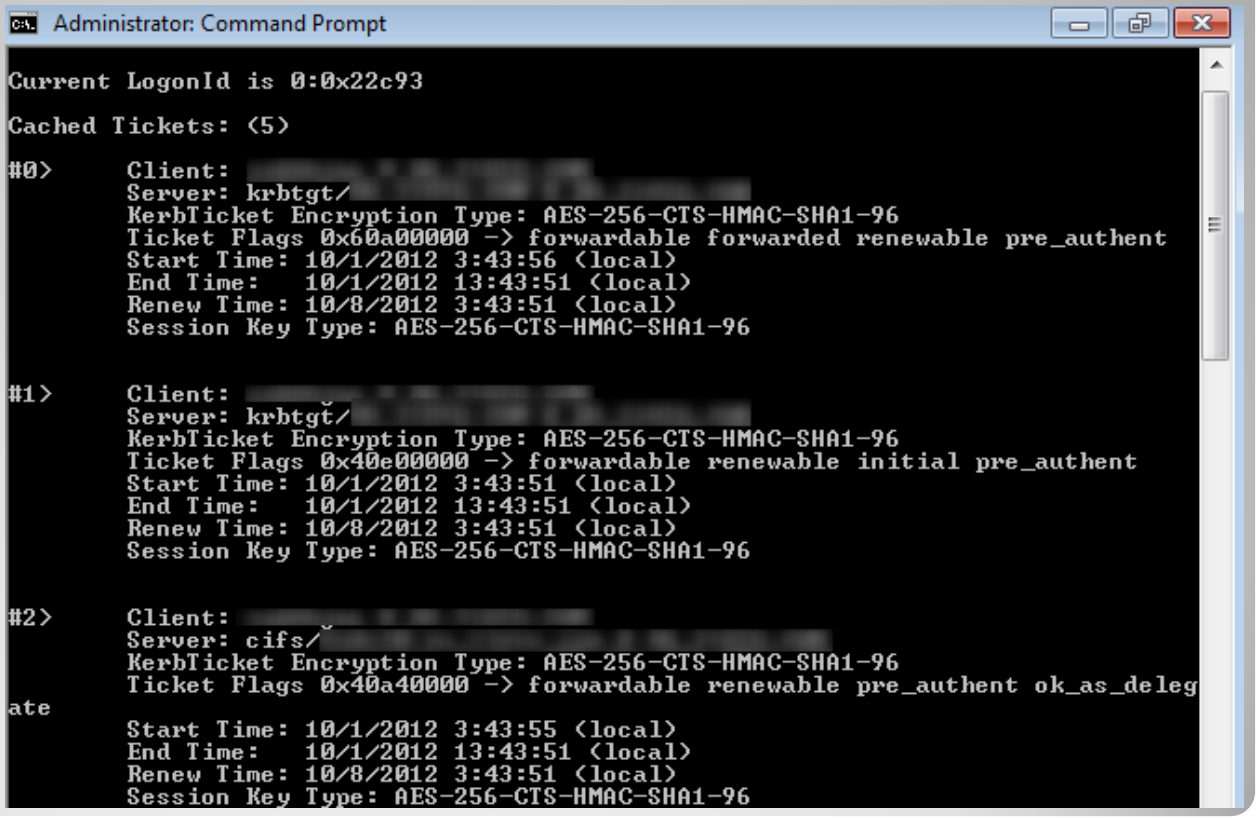
Ověření - Access token

- **TGT** – (Ticket Granting Ticket) slouží k vytváření dalších tiketů. „Přihlašovací tiket“, vystaven na základě (před)ověření heslem.



Ověření - TGT

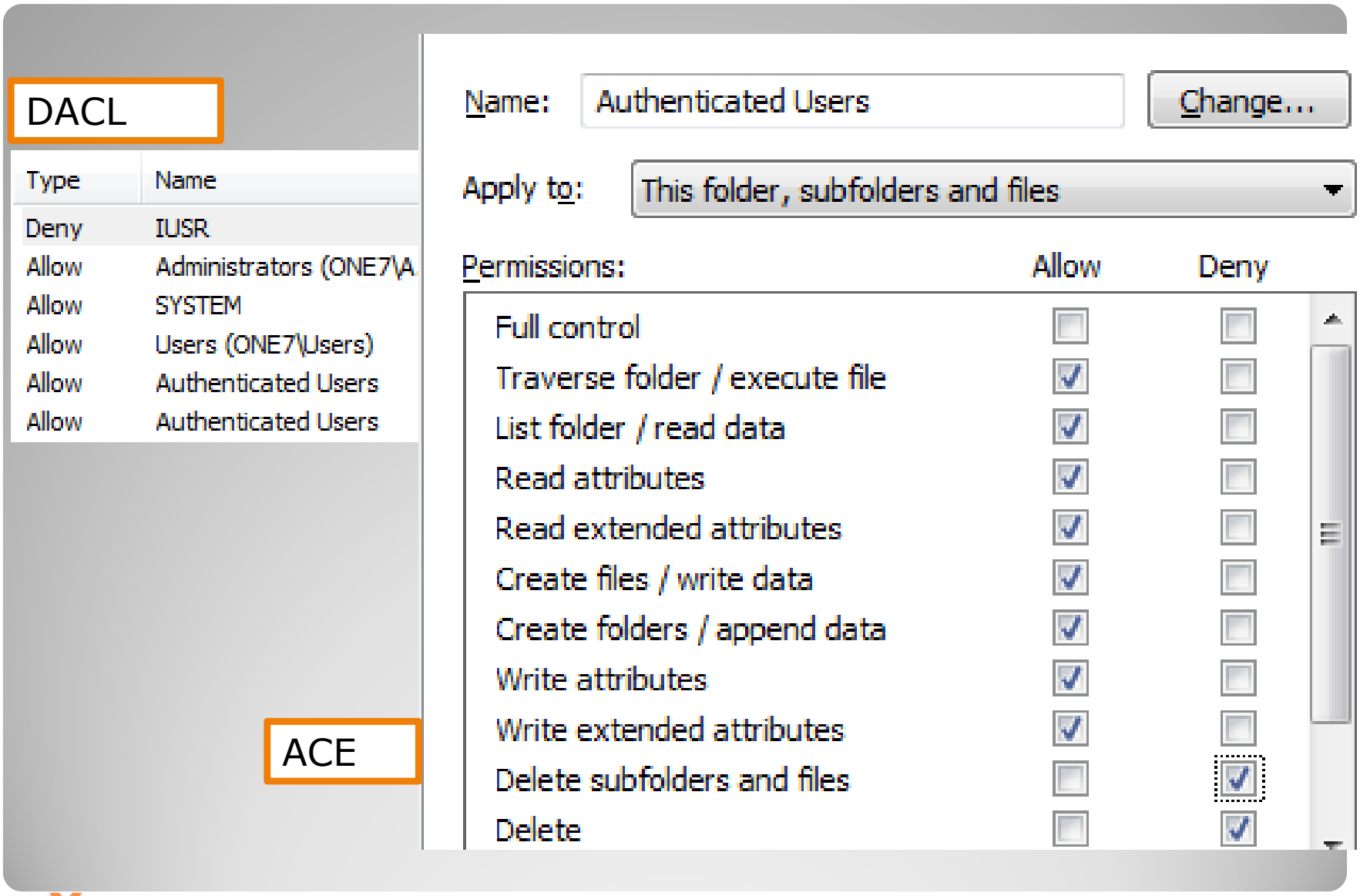
- **TGS** – (Ticket Granting Service) umožňuje přístup ke službám (sdílené soubory, pošta, SQL…).



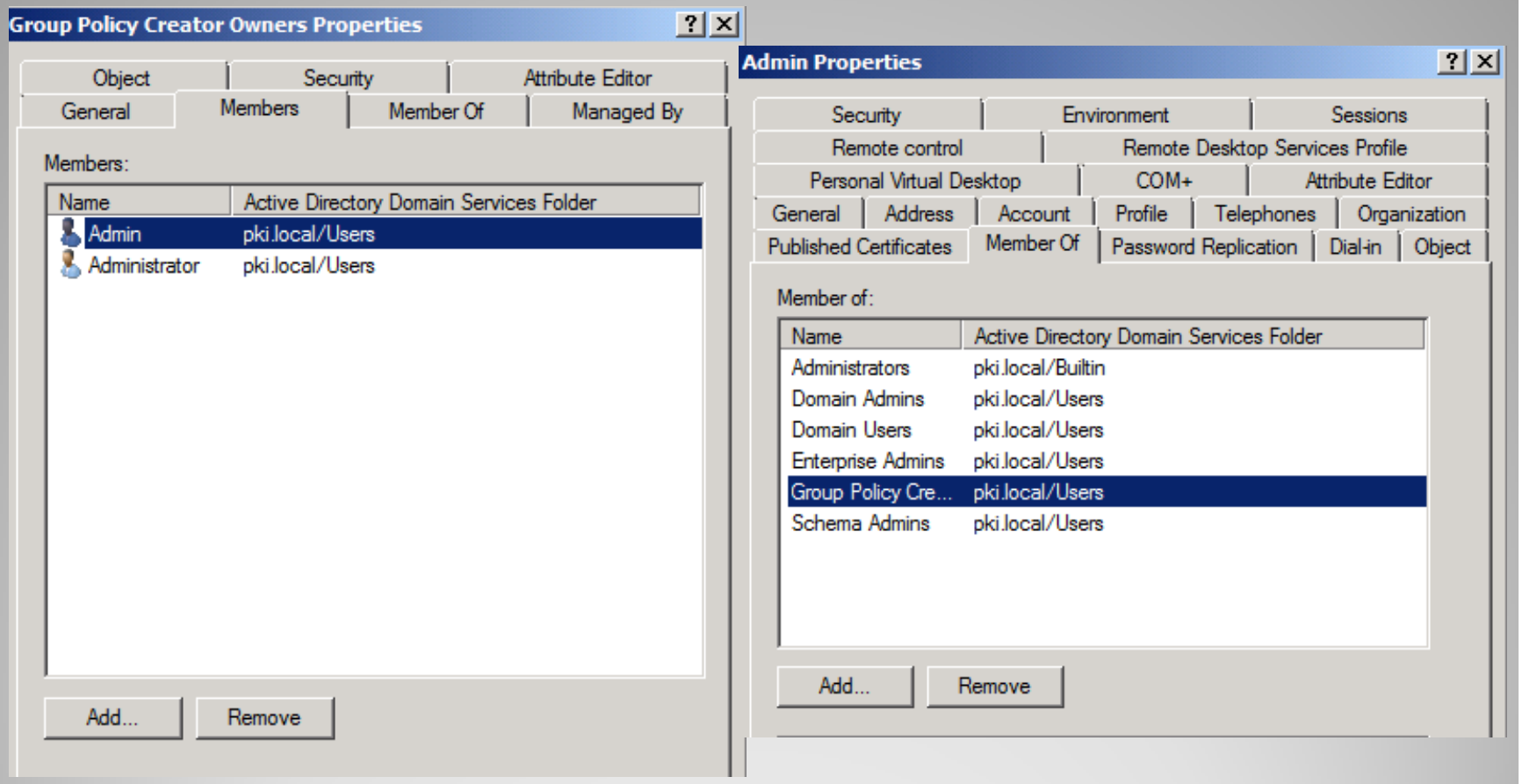
Ověření - TGS

Řízení přístupu

- Uživatelé, počítače, skupiny a další jsou definovány jako objekty.
- Řízení přístupu k objektům využívá popisovače zabezpečení – „**security descriptors**“:
  - Seznam uživatelů a skupin, kterým byl udělen přístup k objektu
  - Určení udělených oprávnění, dědění
  - Definování událostí, které by měly být předmětem auditu
  - Definování vlastníka objektu

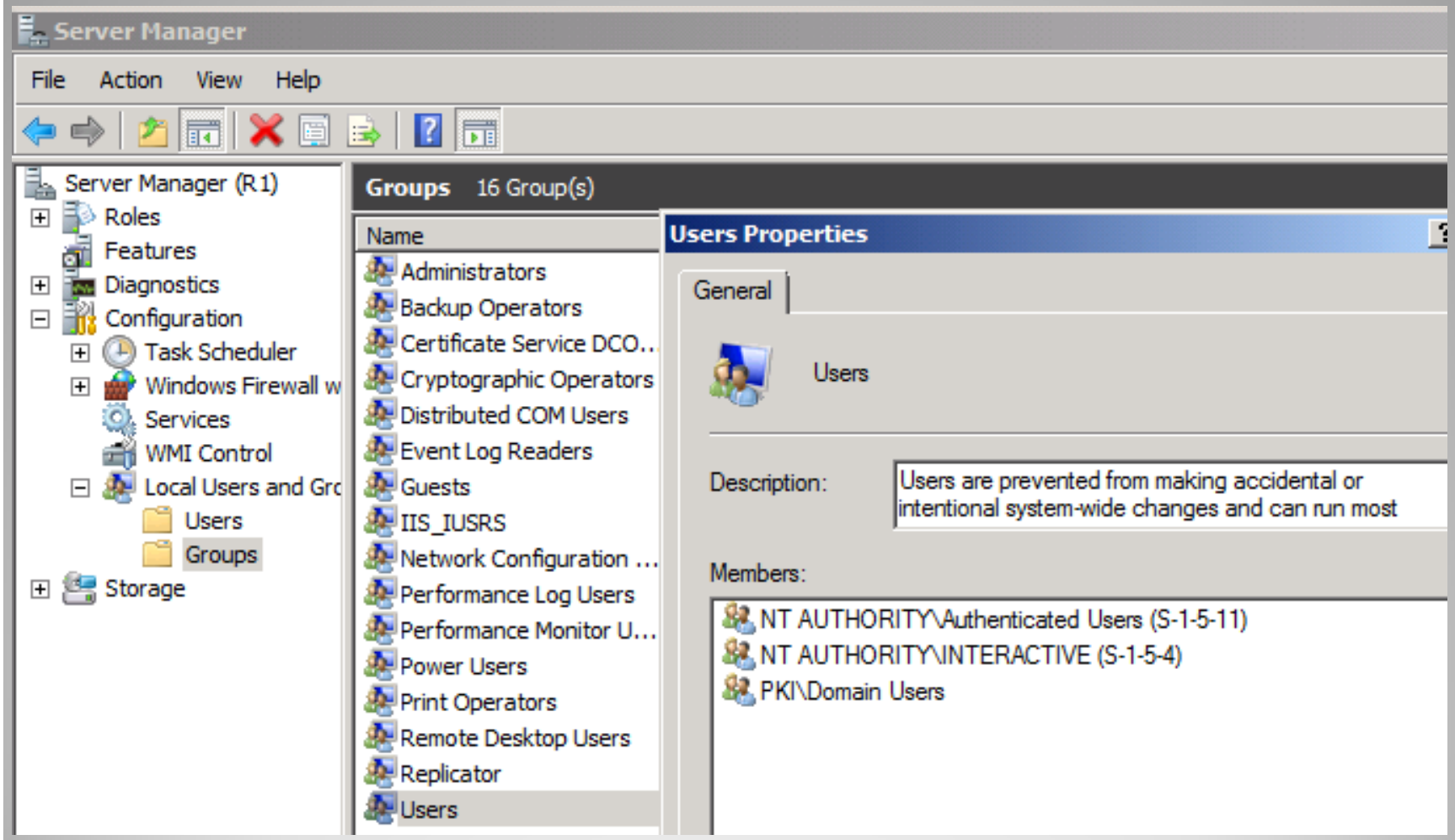


Řízení přístupu

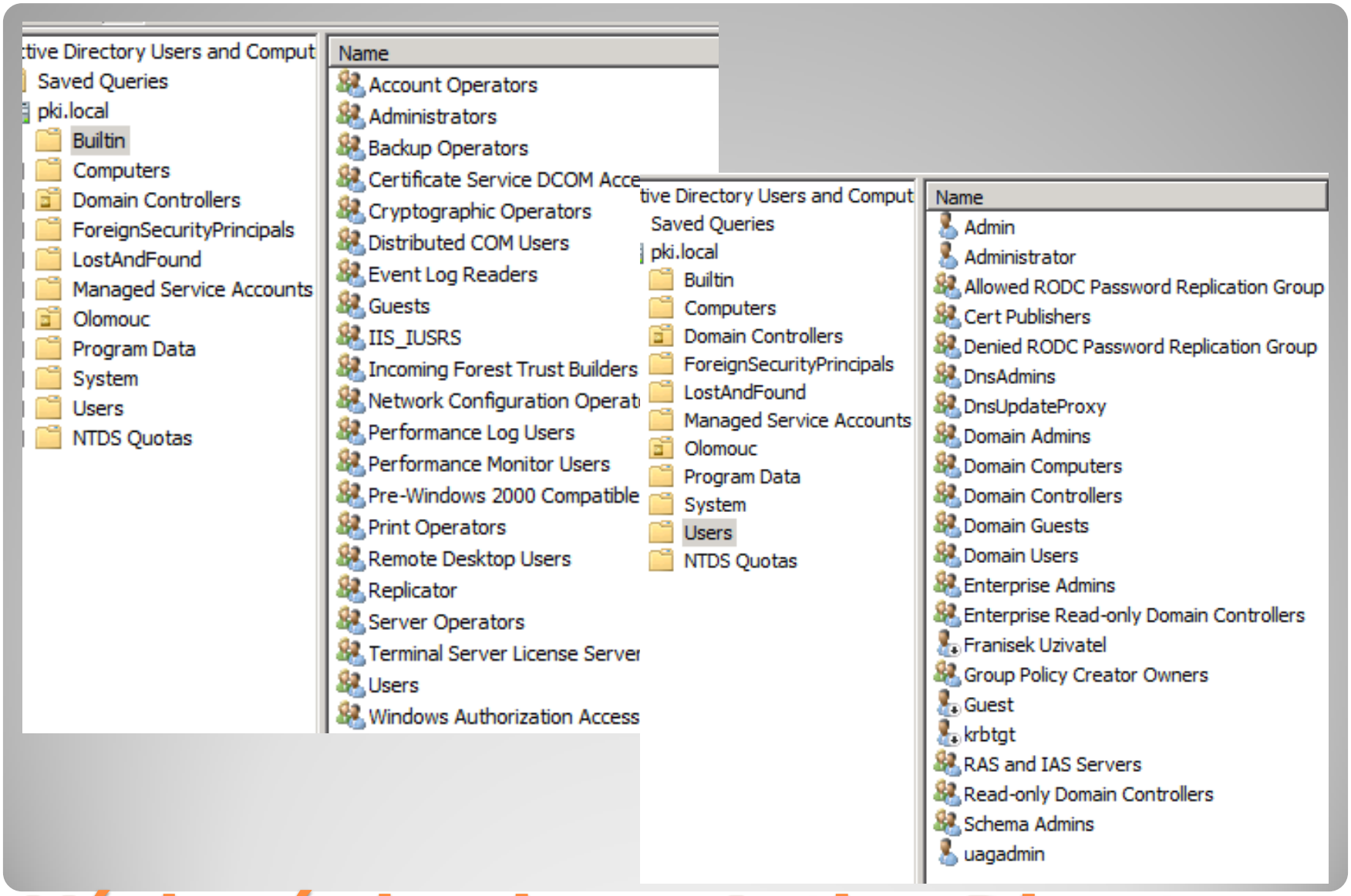


Změny je možné provádět např. i pomocí příkazu **DSMOD.EXE**
nebo **Add-ADGroupMember** / **Remove-ADGroupMember**

Modifikace členství ve skupině



Výchozí lokální skupiny



Výchozí skupiny v Active Directory

Skupiny - typy

Skupiny zjednodušují administraci a řízení přístupu

Typ skupiny	Popis
Security	• Používá se pro přidělení přístupových práv a oprávnění. • Může být využita jako emailová distribuční skupina
Distribution	• Může být použita pouze emalovou aplikací • Nelze ji použít pro řízení oprávnění
Local	• Skupiny jsou definovány na lokálním počítači. • Lze je používat pouze na daném počítači

Skupiny - rozsahy

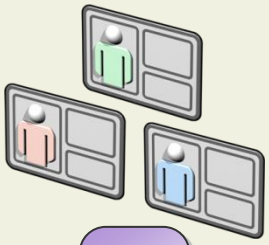
Rozsah skupin	Zjednodušený popis
Domain local	Oprávnění pro jednu doménu. Členy mohou být pouze účty (už. a pc) a skupiny ze stejné domény.
Global	Oprávnění pro objekty v libovolné doméně v rámci forestu. Členy mohou být pouze účty a skupiny ze stejné domény (ve které je definována skupina).
Universal	Oprávnění v různých doménách ve forestu. Replikují se na GC.

Typ skupiny	Může obsahovat		
	Domain local	Global groups	Universal
Domain local group	☺	☺	☺
Global group		☺	
Universal group		☺	☺

http://technet.microsoft.com/en-us/library/bb726978.aspx

Vnořování skupin (zjednodušený přehled)

Accounts



A

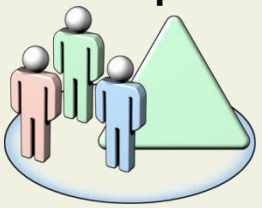
Global Groups

G

Universal Groups

U

Domain Local Groups

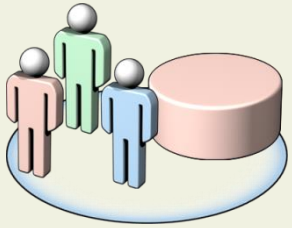


DL

Permissions

P

Local Groups



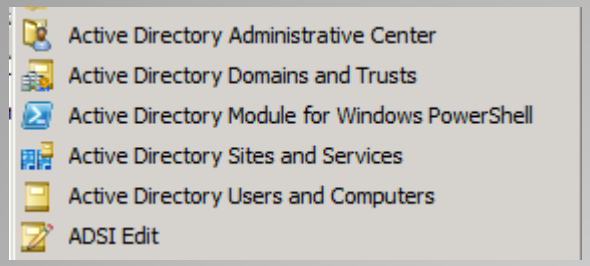
L

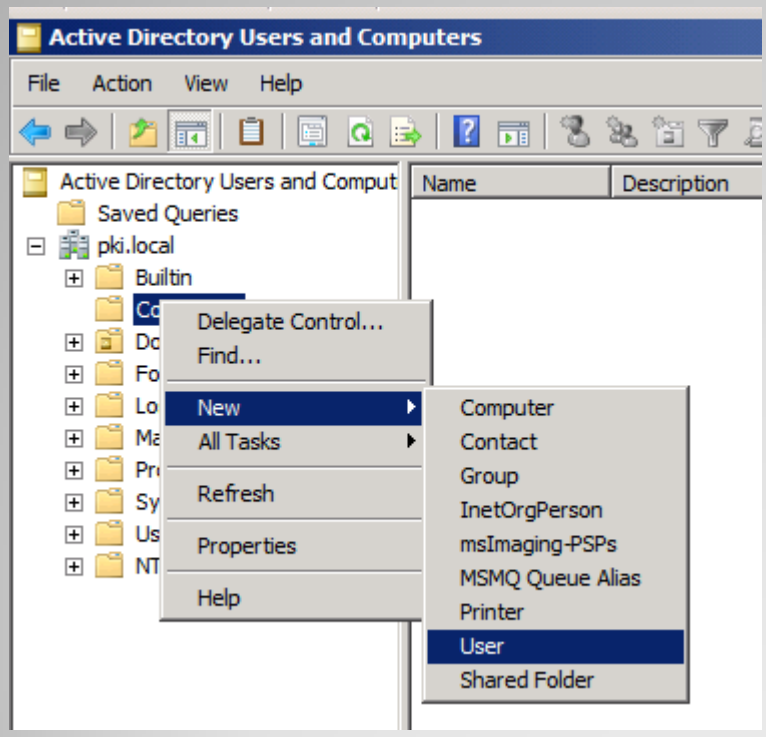
Group strategies:

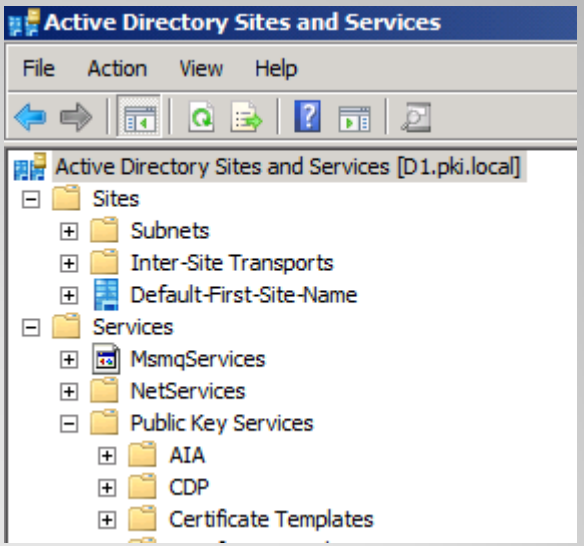
- A G P
- A G DL P
- A G U DL P
- A G G DL P
- A G L P

Strategie AGDLP (nově také IGDLA)

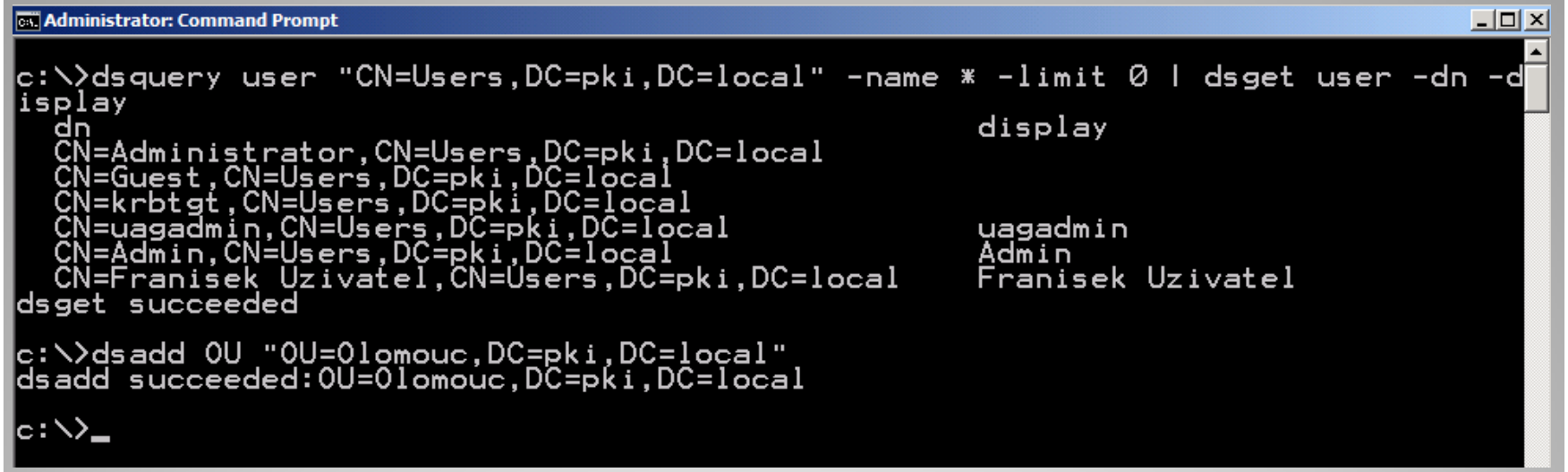
Nástroje pro správu

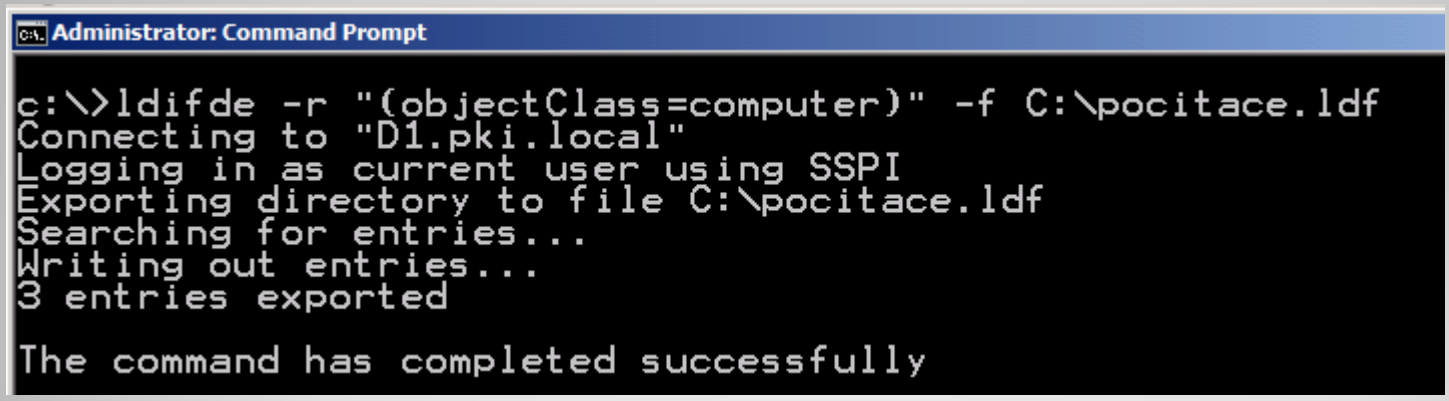




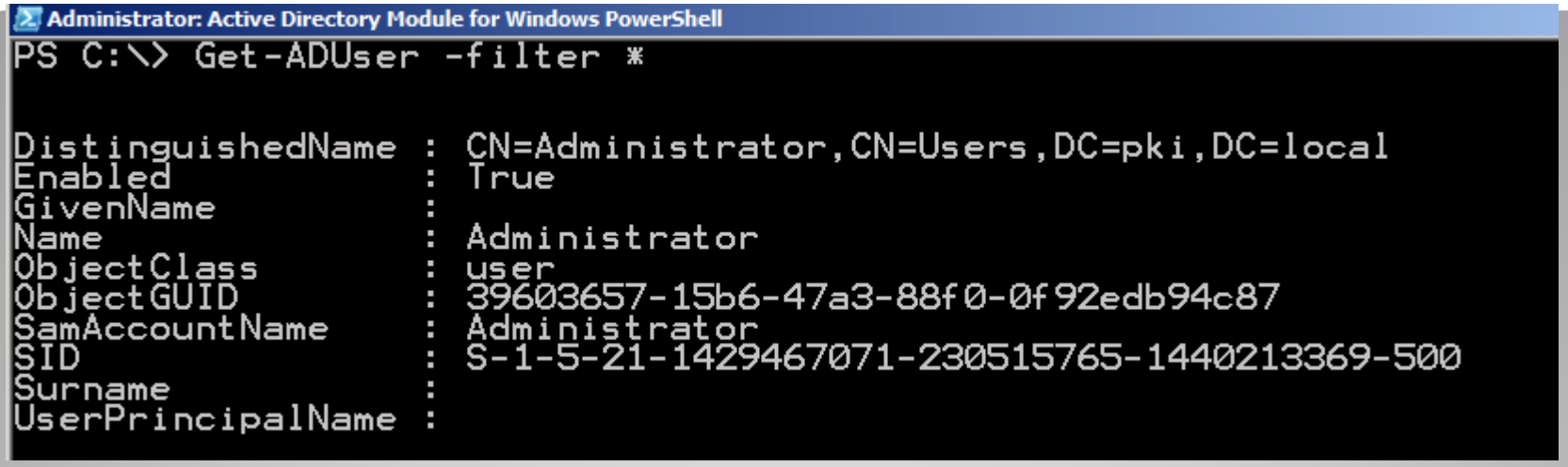


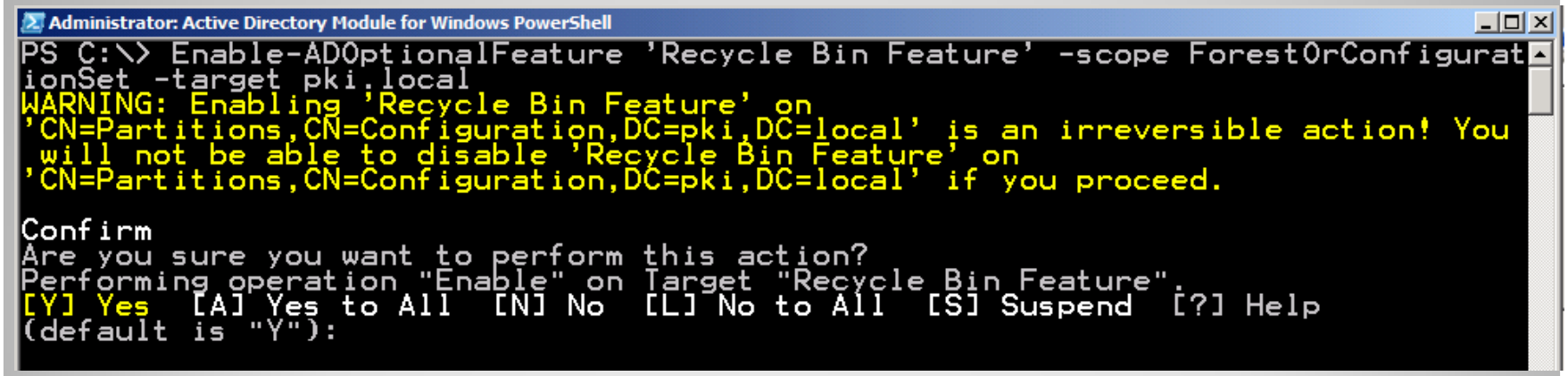
Nástroje pro správu AD - GUI





Nástroje pro správu AD – příkazová řádka; export/import





Nástroje pro správu AD - PowerShell

```
On Error Resume Next

Set objUser=GetObject("LDAP://CN=Frantisek Uzivatel, OU=Users, DC=vsb,
DC=cz")

Set colGroups = objUser.Groups

For Each objGroup in colGroups
    Wscript.Echo objGroup.CN
    GetNested(objGroup)
Next
Function GetNested(objGroup)
    On Error Resume Next
    colMembers = objGroup.GetEx("memberOf")
    For Each strMember in colMembers
        strPath = "LDAP://" & strMember
        Set objNestedGroup = _
        GetObject(strPath)
        WScript.Echo objNestedGroup.CN
        GetNested(objNestedGroup)
    Next
End Function
```

Nástroje pro správu AD – skripty a mnoho dalších

PowerShell

Ukázky a příklady pro práci s Active Directory

```
PS > Import-Module ActiveDirectory

PS > Get-Command *-AD*

CommandType     Name
-----------     ----------
...
Cmdlet          Add-ADGroupMember
Cmdlet          Add-ADPrincipalGroupMembership
...
```

```
PS > (get-adforest).domains | foreach {Get-
ADDomainController -discover -DomainName $_} |
foreach {Get-addomaincontroller -filter * -server $_} | ft
hostname
```

AD a PowerShell

```
PS > New-ADUser "Dexter Morgan" -SamAccountName
"Dexter"  -GivenName "Dexter" -Surname "Morgan”
-DisplayName "Morgan, Dexter" -Path
'CN=Users,DC=jan,DC=test' -OtherAttributes
@{title="Director";mail="dexter@miami.com"}
```

```
PS > Set-ADAccountPassword Dexter -Reset -
NewPassword (ConvertTo-SecureString -AsPlainText
"P@ssword" -Force)
```

```
PS > Set-ADUser Dexter -Enabled 1
```

AD a PowerShell – práce s uživateli

```
PS > Get-ADGroupMember  "CN=Group1, OU=Groups, DC=vsb,DC=cz" | Measure-Object
```

```
PS > $usr=”Bart Simpson”
PS > $dom1=”vsb.cz"
PS > $dom2=”vsb.local"

PS > (Get-ADUser -Identity $usr -Properties MemberOf -server $dom1 |Select-Object (MemberOf).MemberOf |Out-File ".\$usr MemberOf.txt”

PS > (Get-ADUser -Identity $usr -Properties MemberOf -server $dom2 |Select-Object (MemberOf).MemberOf |Out-file ".\$usr MemberOf.txt" -Append
```

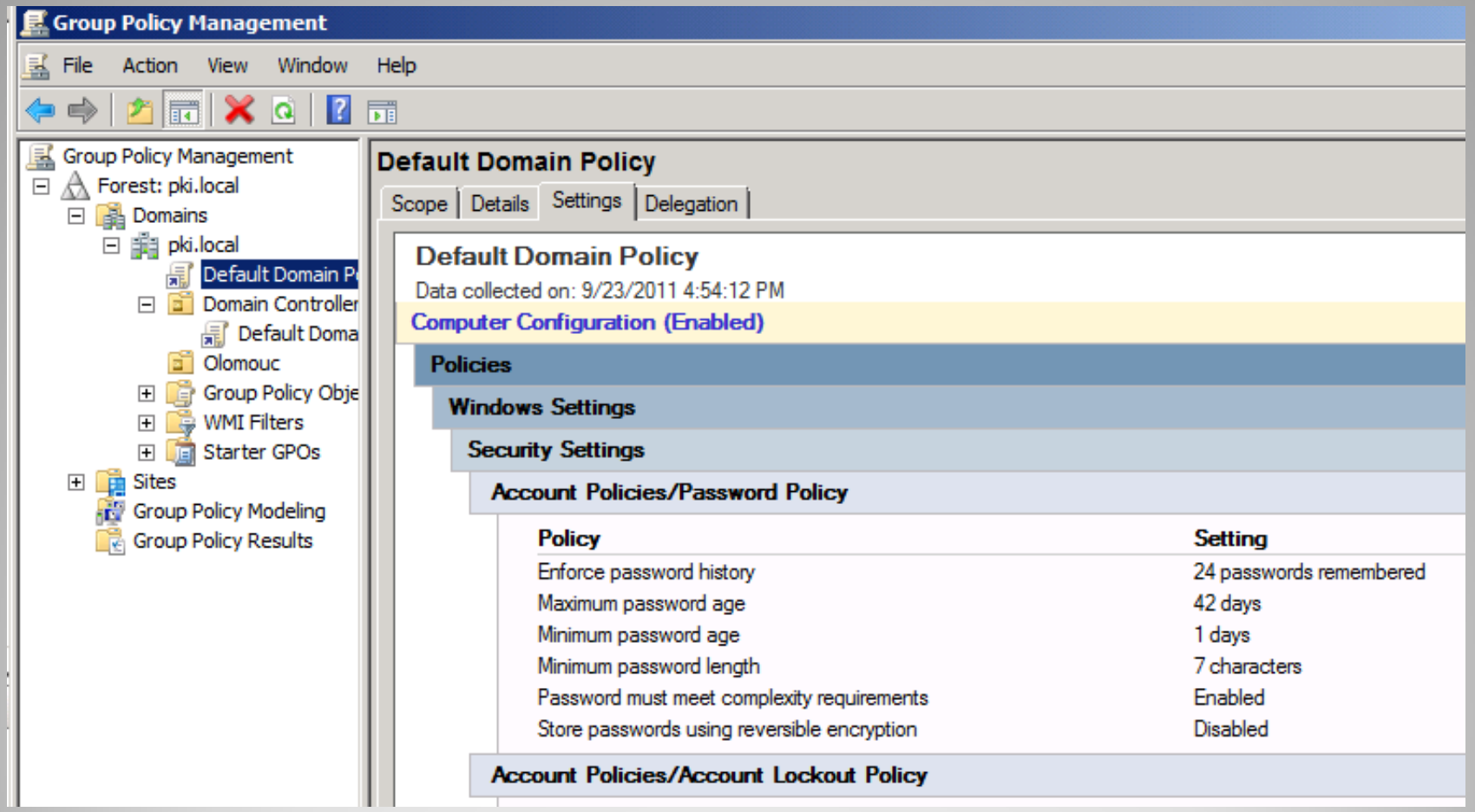
AD a PowerShell – práce se skupinami

```
PS > Get-ADComputer ”WSSQL1”

PS > Get-ADComputer -Filter 'Name -like "*"’
```

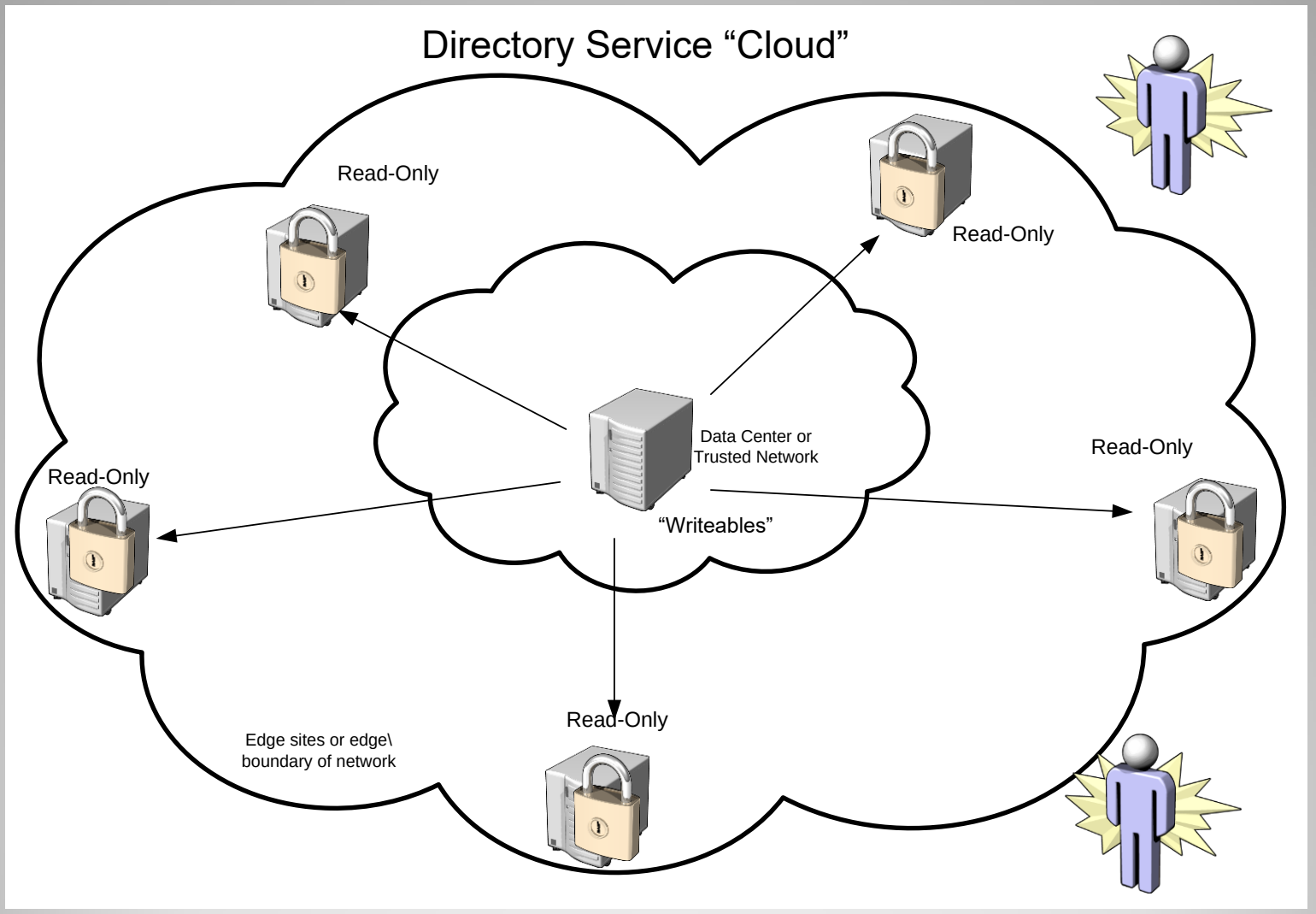
```
PS > $compy=Get-Content “.\compy.txt”

PS > $compy | Get-ADComputer | Select-Object DistinguishedName
```

AD a PowerShell – práce účty počítačů

Co se jinam nevešlo



Group policy (zásady skupin)



Read-Only Domain Controller

	Funkční úroveň domény	Funkční úroveň forestu
Windows 2000 mixed		
Windows 2000 native	Univerzální skupiny; vnořování skupin;SID history	
Windows Server 2003 interim		
Windows Server 2003	Přejmenování DC; selektivní ověřování	Forest trust; přejmenování domén,;schopnost nasadit RODC 2008; deaktivace tříd ve schématu
Windows Server 2008	Fine-grained password policy; lepší šifrování	
Windows Server 2008 R2	Vylepšení přihlašování v AD FS	Recycle Bin (koš v AD)

Funkční úrovně – vybrané schopnosti