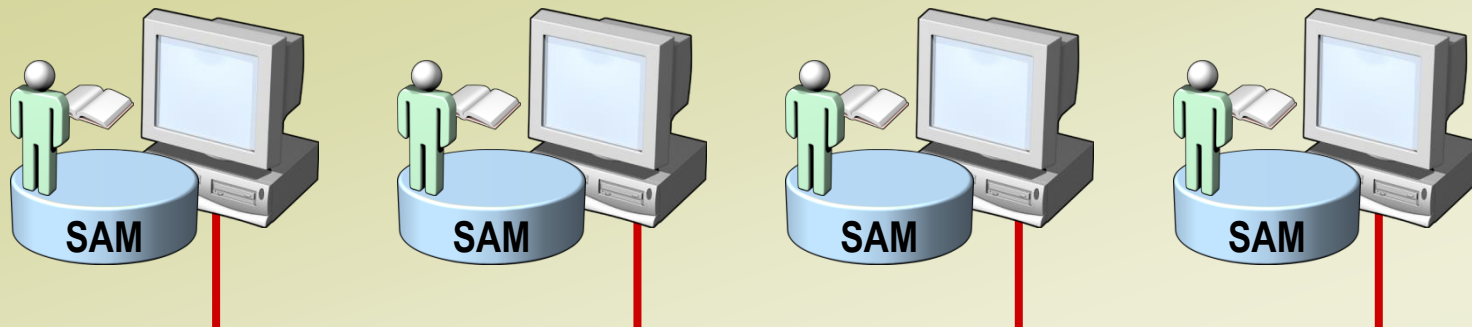


Active Directory

(Active Directory Directory Services)

Workgroup (prac. skupina)



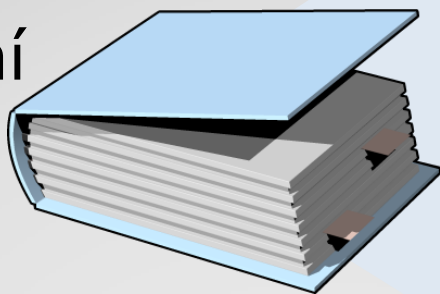
Jediný účet
uživatele

Domain (doména)



Workgroup vs. Domain

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



Vlastnosti AD DS

• Integrace DNS

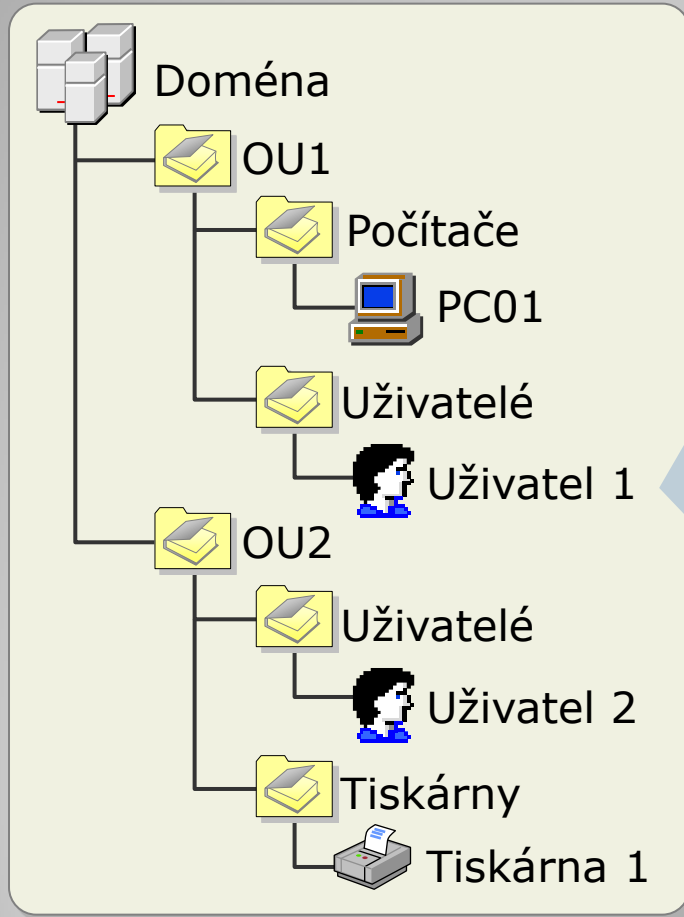
• Škálovatelnost

• Centralizace
správy

• Delegování
oprávnění

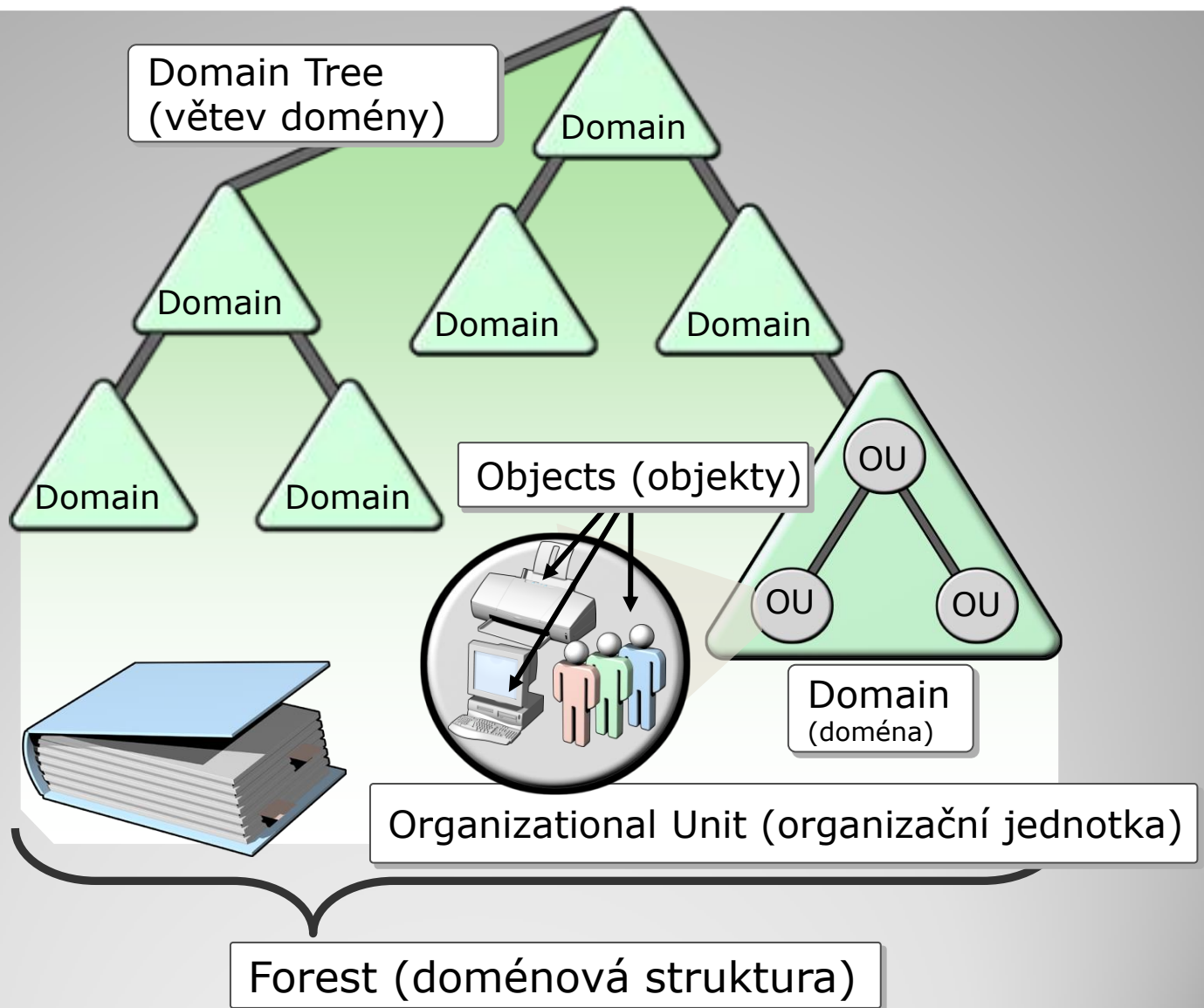
K čemu adresářové služby?

Strukturované úložiště informací o lidech a zdrojích v rámci organizace

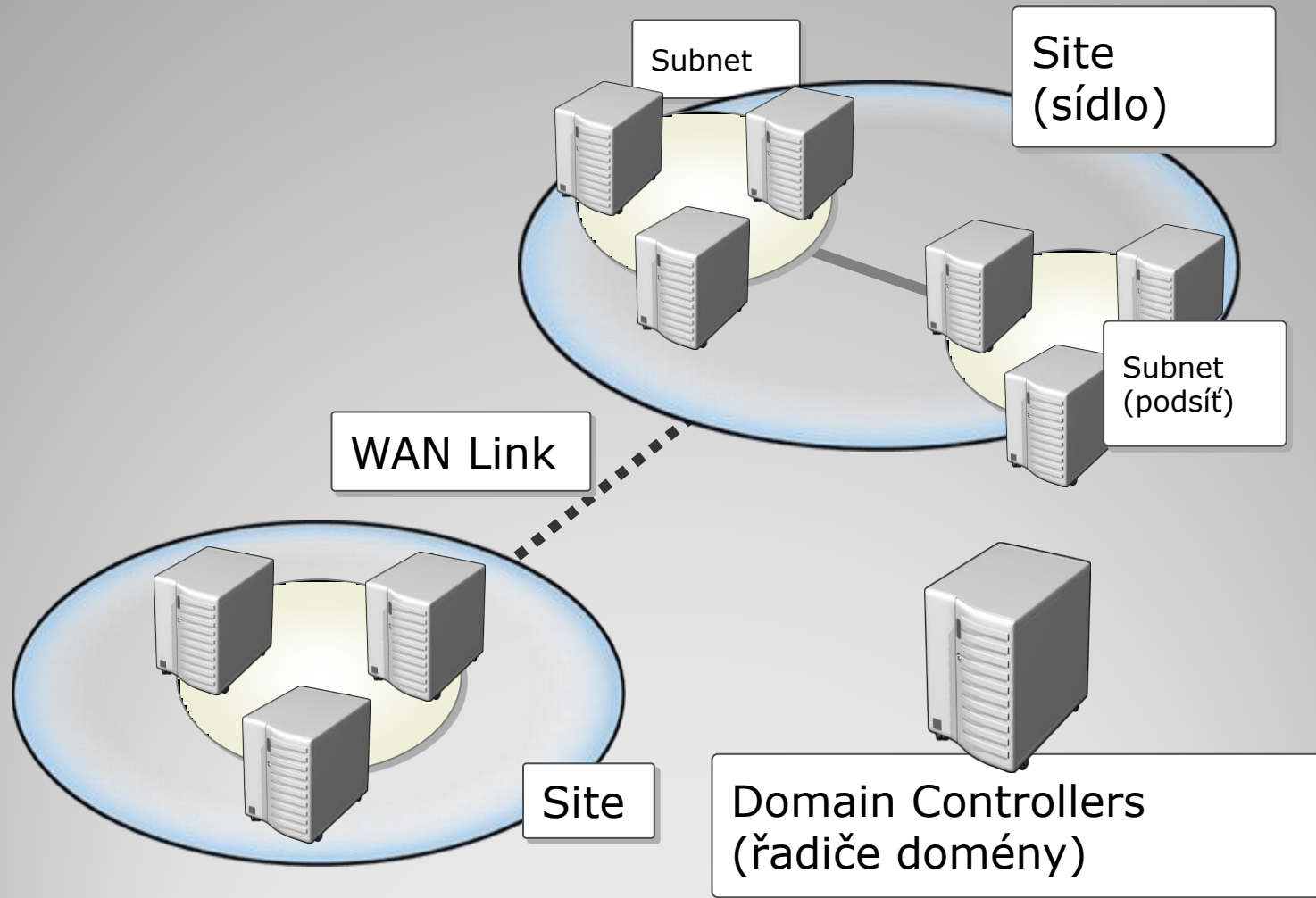


František Uživatel	
Atribut	Hodnota
Jméno	František
Příjmení	Uživatel
Budova	15
Patro	3
Os. číslo	567889

Adresářová služba - příklad



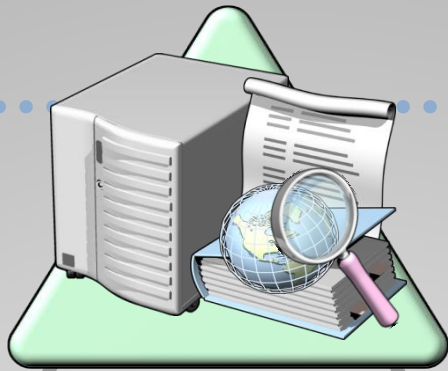
Logická struktura AD



Fyzická struktura AD

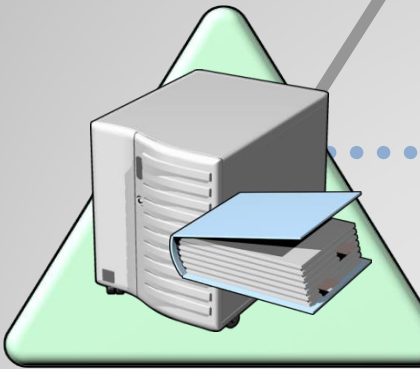
Forest-wide role

- Schema master
- Domain naming master



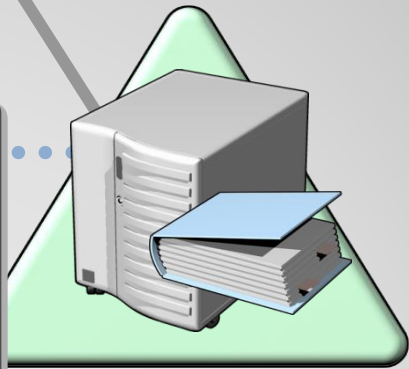
Domain-wide role

- PDC emulator
- RID master
- Infrastructure master



Domain-wide role

- RID master
- PDC emulator
- Infrastructure master



FSMO

(Flexible Single Master Operations Roles)

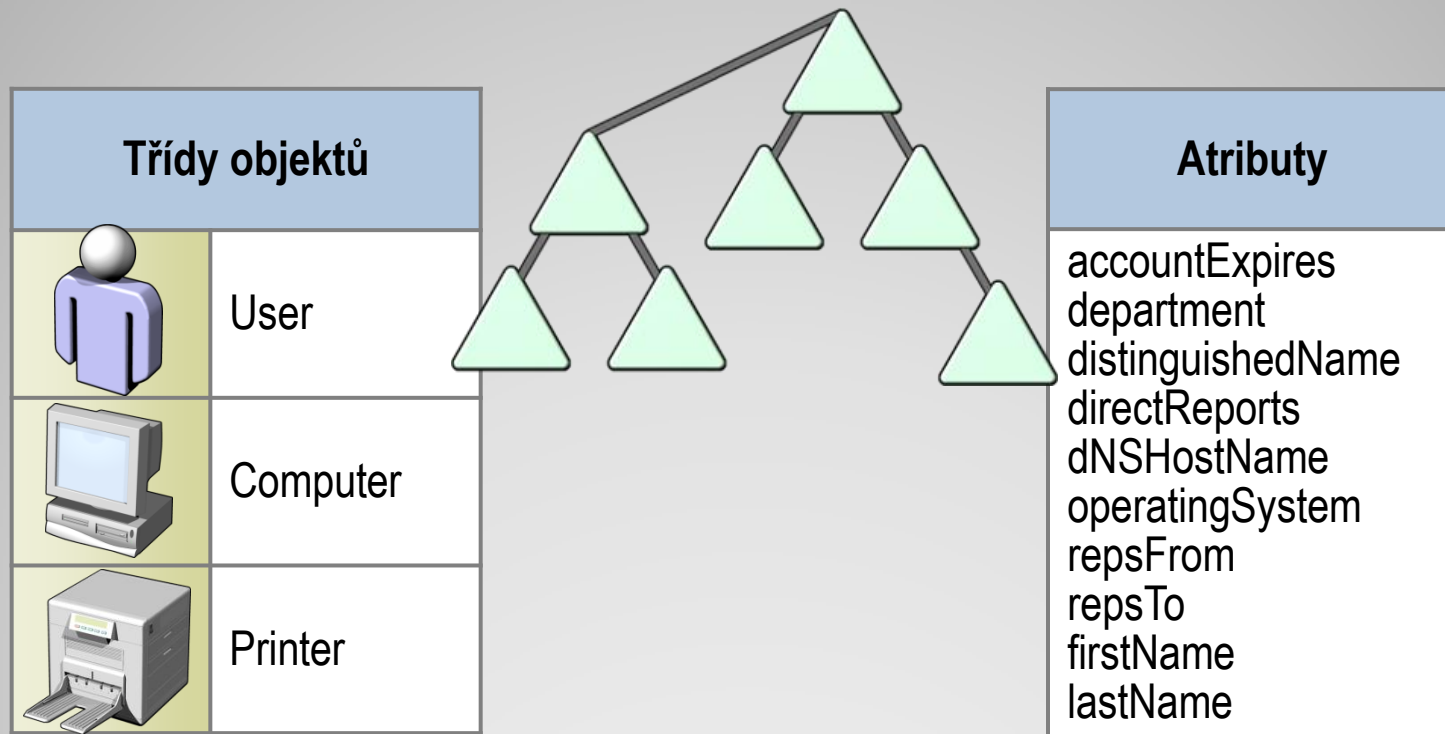
- **Hlavní server schémat (Schema Master)**: Jeden držitel role hlavního serveru v jedné doménové struktuře. Držitel role FSMO hlavního serveru schémat je řadič domény zodpovědný za aktualizace ve schématu adresářů.
- **Hlavní server názvů domén (Domain Naming Master)**: Jeden držitel role hlavního serveru 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.

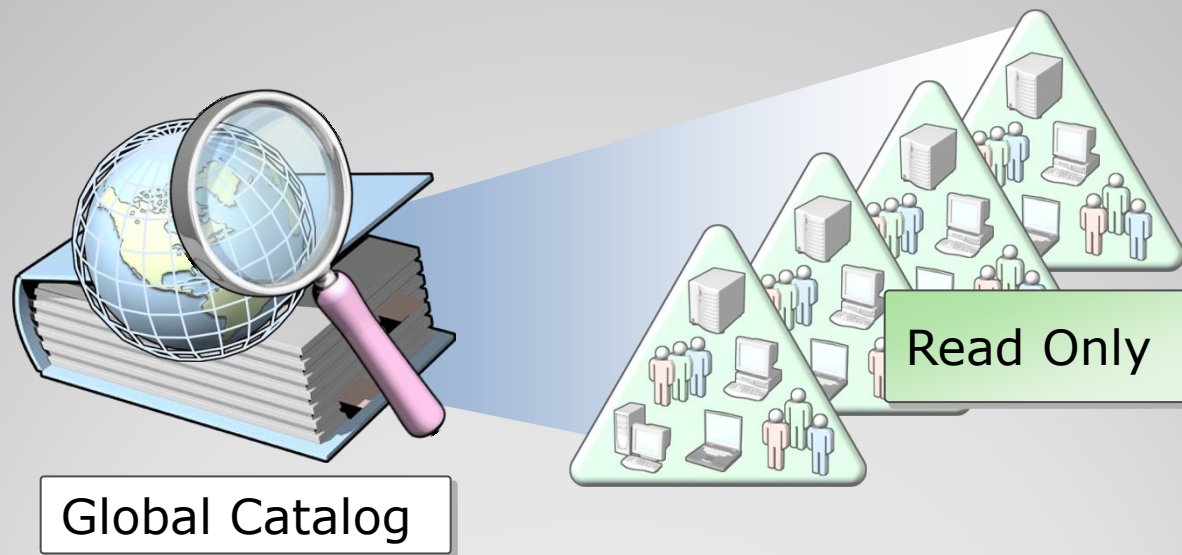
FSMO (EN)

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



















Schéma

- 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

- ▷  Austria
- ▷  Belgium
- ▷  Canada
- ▾  Czech Republic
 - ▷  Contacts
 - ▷  External Users
 - ▷  Groups
 - ▷  Servers
 - ▷  Shared Mailboxes
 - ▷  System Accounts
 -  Users
 - ▷  Workstations
- ▷  Denmark
- ▷  Estonia
- ▷  Finland
- ▷  France

Obchodní model

- ▷  _Admin
- ▷  Citrix
- ▷  Groups
- ▷  Servers
- ▷  System Accounts
- ▷  Users
- ▷  VDI Machines
- ▷  VMWare

- ▾  Messaging
 - ▷  Backup
 - ▷  Exchange2003
 - ▷  Exchange2007
 - ▷  Exchange2010

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

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

- DCPROMO se používá pro povýšení standalone/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>

DCPROMO

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

Franisek Uzivatel Properties [?] [X]

Dial-in | Environment | Sessions | Remote control
 Remote Desktop Services Profile | Personal Virtual Desktop | COM+
 General | Address | Account | Profile | Telephones | Organization | Member Of

 **Franisek Uzivatel**

First name: Initials:

Last name:

Display name:

Description:

Office:

Telephone number:

E-mail:

Web page:

Logon Hours for Franisek Uzivatel

12 • 2 • 4 • 6 • 8 • 10 • 12 • 2 • 4 • 6 • 8 • 10 • 12

All																								
Sunday																								
Monday																								
Tuesday																								
Wednesday																								
Thursday																								
Friday																								
Saturday																								

Logon Permitted
 Logon Denied

Monday through Friday from 8:00 AM to 5:00 PM

Account options:

Password never expires

Store password using reversible encryption

Account is disabled

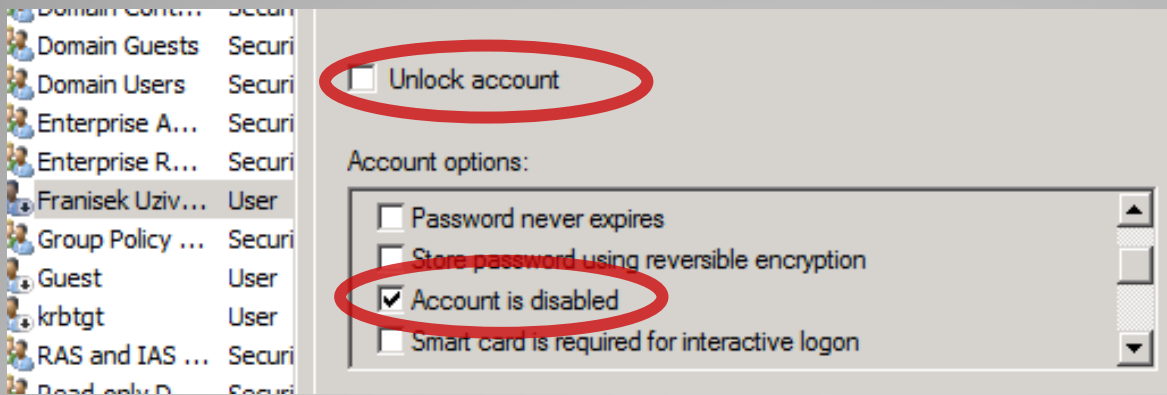
Smart card is required for interactive logon

Account expires:

Never

End of:

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

R1 Properties



Location | Managed By | Object | Security | Dial-in | Attribute Editor
General | Operating System | Member Of | Delegation | Password Replication



Computer name (pre-Windows 2000):

DNS name:

DC Type:

Site:

Description:

R1 Properties



Location | Managed By | Object | Security | Dial-in | Attribute Editor
General | Operating System | Member Of | Delegation | Password Replication

Name:

Version:

R1 Properties



Location | Managed By | Object | Security | Dial-in | Attribute Editor
General | Operating System | Member Of | Delegation | Password Replication

Member of:

Name	Active Directory Domain Services Folder
Cert Publishers	pki.local/Users
Domain Computers	pki.local/Users
Pre-Windows 2000 Compati...	pki.local/Builtin

Vlastnosti účtu počítače

- 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 Enterprise Linux, OS X ...)

Proč mají počítače účty

Active Directory Users and Computers

File Action View Help

Active Directory Users and Comput

- Active Directory Users and Comput
 - Saved Queries
 - pkilocal
 - Builtin
 - Computers**
 - Domain Controllers
 - ForeignSecurityPrincipals
 - LostAndFound
 - Managed Service Accounts
 - Program Data
 - System
 - Users**
 - NTDS Quotas

Name	Type
Admin	User
Administrator	User
A...	
D...	
DnsAdmins	Security Group ...
DnsUpdateProxy	Security Group ...
Domain Admins	Security Group ...
D...	
D...	
D...	
D...	
Domain Users	Security Group ...
Enterprise Admins	Security Group ...
Enterprise Read-only Domain Controllers	Security Group ...
Franisek Uzivatel	User

Účty počítače vytvořené automaticky nebo vzniklé bez zadání cesty

Účty uživatelů vytvořené bez zadání cesty

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

Výchozí kontejnery pro účty

Find Users, Contacts, and Groups

File Edit View

Find: Users, Contacts, and Groups In: Entire Directory Browse...

Users, Contacts, and Groups

Computers

Printers

Shared Folders

Organizational Units

Custom Search

Common Queries

Find Now

Condition List:

Add

Remove

City Starts with Ostrava

E-Mail Add... Present

Find Custom Search

File Edit View

Find: Custom Search In: Entire Directory

Custom Search Advanced

Enter LDAP query:

(&(objectCategory=person)(objectClass=user)(!cn=administrator)

Query string:

```
(&(objectCategory=person)(objectClass=user)
(userAccountControl:1.2.840.113556.1.4.803:=2)
(objectCategory=person)(objectClass=user)
(userAccountControl:1.2.840.113556.1.4.803:=65536)
```

Define Query...

OK

Cancel

Vyhledávání objektů



Modely zabezpečení

Účty skupin
Přístupová práva

- **Kerberos V 5** Standard protokolu pro autentizaci uživatelů a systémů. Je primárním autentizačním mechanismem 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 mechanismus pro autentizaci pro přístupy k zabezpečeným webovým serverům.

Autentizační protokoly

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

```

C:\Windows\system32\cmd.exe

INFORMACE O UŽIVATELI
-----
Uživatelské jméno SID
-----
jan S-1-5-21-...-2218773655-1000

INFORMACE O SKUPINĚ
-----
Název skupiny Typ SID Atributy
-----
Everyone Známá skupina S-1-1-0 Povinná skupina, Ve výchozím nastavení
BUILTIN\Administrators Skupina použitá pouze k odmítnutí
BUILTIN\Users Alias S-1-5-32-544 Povinná skupina, Ve výchozím nastavení
NT AUTHORITY\INTERACTIVE Povinná skupina, Ve výchozím nastavení
CONSOLE_LOGON Známá skupina S-1-5-4 Povinná skupina, Ve výchozím nastavení
NT AUTHORITY\Authenticated Users Povinná skupina, Ve výchozím nastavení
NT AUTHORITY\This Organization Povinná skupina, Ve výchozím nastavení
LOCAL Známá skupina S-1-2-0 Povinná skupina, Ve výchozím nastavení
NT AUTHORITY\NTLM Authentication Povinná skupina, Ve výchozím nastavení
Mandatory Label\Medium Mandatory Level Popisek S-1-5-64-10 Povinná skupina, Ve výchozím nastavení
S-1-16-8192 Povinná skupina, Ve výchozím nastavení

INFORMACE O OPRÁVNĚNÍCH
-----
Název oprávnění Popis Stav
-----
SeShutdownPrivilege Vypnout systém Zakázáno
SeChangeNotifyPrivilege Nepoužívat kontrolu procházení Povolené
SeUndockPrivilege Vymout počítač z dokovací stanice Zakázáno
SeIncreaseWorkingSetPrivilege Zvýšit pracovní sadu procesu Zakázáno
SeTimeZonePrivilege Změnit časové pásmo Zakázáno

```

Ověření - Access token

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

```
Administrator: Command Prompt

Current LogonId is 0:0x22c93

Cached TGT:

ServiceName      : krbtgt
TargetName (SPN) : krbtgt
ClientName       : 
DomainName       : 
TargetDomainName : 
AltTargetDomainName: 
Ticket Flags     : 0x40e00000 -> forwardable renewable initial pre_authent
Session Key      : KeyType 0x12 - AES-256-CTS-HMAC-SHA1-96
                  : KeyLength 32 - 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                  : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
StartTime       : 10/1/2012 3:43:51 (local)
EndTime         : 10/1/2012 13:43:51 (local)
RenewUntil      : 10/8/2012 3:43:51 (local)
TimeSkew        : + 0:00 minute(s)
EncodedTicket    : (size: 1707)
0000  61 82 06 a7 30 82 06 a3:a0 03 02 01 05 a1 0e 1b  a...0.....
0010  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ?0
0020  1f a0 03 02 01 02 a1 18:30 16 1b 06 6b 72 62 74  .....0...krbt
0030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0040  a3 82 06 67 30 82 06 63:a0 03 02 01 12 a1 03 02  ...g0...c.....
0050  01 03 a2 82 06 55 04 82:06 51 c0 13 f5 25 dc 61  ....U...Q...%.a
0060  77 1b ed bd c8 6a b3 9e:7a 56 2f 3a a8 4e 6b 99  w....j...zU/;.Nk.
0070  54 07 d3 24 2e 96 c1 d5:a3 6d 2d dc 5c 57 0f ad  T..$....m-.\W..
0080  ed b9 cc d4 22 9f 5e 47:51 47 0d 75 d2 cf 82 f9  ....^GQG.u....
```

Ověření - TGT

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

```
Administrator: Command Prompt
Current LogonId is 0:0x22c93
Cached Tickets: <5>
#0> Client: ██████████
Server: krbtgt/
Kerbticket Encryption Type: AES-256-CTS-HMAC-SHA1-96
Ticket Flags 0x60a00000 -> forwardable renewable pre_authent
Start Time: 10/1/2012 3:43:56 <local>
End Time: 10/1/2012 13:43:51 <local>
Renew Time: 10/8/2012 3:43:51 <local>
Session Key Type: AES-256-CTS-HMAC-SHA1-96
#1> Client: ██████████
Server: krbtgt/
Kerbticket Encryption Type: AES-256-CTS-HMAC-SHA1-96
Ticket Flags 0x40e00000 -> forwardable renewable initial pre_authent
Start Time: 10/1/2012 3:43:51 <local>
End Time: 10/1/2012 13:43:51 <local>
Renew Time: 10/8/2012 3:43:51 <local>
Session Key Type: AES-256-CTS-HMAC-SHA1-96
#2> Client: ██████████
Server: cifs/██████████
Kerbticket Encryption Type: AES-256-CTS-HMAC-SHA1-96
Ticket Flags 0x40a40000 -> forwardable renewable pre_authent ok_as_deleg
ate
Start Time: 10/1/2012 3:43:55 <local>
End Time: 10/1/2012 13:43:51 <local>
Renew Time: 10/8/2012 3:43:51 <local>
Session Key Type: AES-256-CTS-HMAC-SHA1-96
```

Ověření - TGS

- 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

DAACL

Type	Name
Deny	IUSR
Allow	Administrators (ONE7\A
Allow	SYSTEM
Allow	Users (ONE7\Users)
Allow	Authenticated Users
Allow	Authenticated Users

ACE

Name: Authenticated Users

Change...

Apply to: This folder, subfolders and files

Permissions:

Allow

Deny

Full control

Traverse folder / execute file

List folder / read data

Read attributes

Read extended attributes

Create files / write data

Create folders / append data

Write attributes

Write extended attributes

Delete subfolders and files

Delete

Řízení přístupu

Group Policy Creator Owners Properties

Object	Security	Attribute Editor
General	Members	Member Of Managed By

Members:

Name	Active Directory Domain Services Folder
Admin	pki.local/Users
Administrator	pki.local/Users

Add... Remove

Admin Properties

Security	Environment	Sessions			
Remote control	Remote Desktop Services Profile				
Personal Virtual Desktop	COM+	Attribute Editor			
General	Address	Account	Profile	Telephones	Organization
Published Certificates	Member Of	Password Replication	Dial-in	Object	

Member of:

Name	Active Directory Domain Services Folder
Administrators	pki.local/Builtin
Domain Admins	pki.local/Users
Domain Users	pki.local/Users
Enterprise Admins	pki.local/Users
Group Policy Cre...	pki.local/Users
Schema Admins	pki.local/Users

Add... Remove

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

Modifikace členství ve skupině

The screenshot shows the Windows Server Manager interface. On the left, the 'Server Manager (R1)' tree is expanded to 'Local Users and Groups' > 'Groups'. The main pane displays a list of 16 groups. The 'Users' group is selected, and the right-hand pane shows its 'Users Properties' dialog box. The 'General' tab is active, showing the group name 'Users' and its description: 'Users are prevented from making accidental or intentional system-wide changes and can run most'. The 'Members' list includes:

- NT AUTHORITY\Authenticated Users (S-1-5-11)
- NT AUTHORITY\INTERACTIVE (S-1-5-4)
- PKI\Domain Users

Výchozí lokální skupiny

The screenshot displays the Active Directory Users and Computers console. On the left, the tree view shows the hierarchy: Active Directory Users and Computers > pki.local > Built-in. The main pane shows a list of built-in groups. A secondary pane on the right shows a list of default groups.

Name
Account Operators
Administrators
Backup Operators
Certificate Service DCOM Access
Cryptographic Operators
Distributed COM Users
Event Log Readers
Guests
IIS_IUSRS
Incoming Forest Trust Builders
Network Configuration Operators
Performance Log Users
Performance Monitor Users
Pre-Windows 2000 Compatible
Print Operators
Remote Desktop Users
Replicator
Server Operators
Terminal Server License Server
Users
Windows Authorization Access

Name
Admin
Administrator
Allowed RODC Password Replication Group
Cert Publishers
Denied RODC Password Replication Group
DnsAdmins
DnsUpdateProxy
Domain Admins
Domain Computers
Domain Controllers
Domain Guests
Domain Users
Enterprise Admins
Enterprise Read-only Domain Controllers
Franisek Uzivatel
Group Policy Creator Owners
Guest
krbtgt
RAS and IAS Servers
Read-only Domain Controllers
Schema Admins
uagadmin

Výchozí skupiny v Active Directory

Skupiny zjednodušují administraci a řízení přístupu



Typ skupiny	Popis
Security	<ul style="list-style-type: none">• Používá se pro přidělení přístupových práv a oprávnění.• Může být využita jako emailová distribuční skupina
Distribution	<ul style="list-style-type: none">• Může být použita pouze emailovou aplikací• Nelze ji použít pro řízení oprávnění
Local	<ul style="list-style-type: none">• Skupiny jsou definovány na lokálním počítači.• Lze je používat pouze na daném počítači

Skupiny - typy

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.

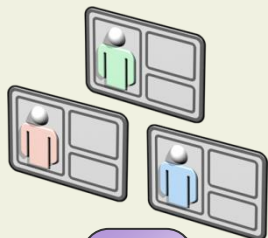
Skupiny - rozsahy

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



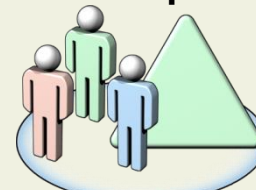
G

Universal Groups



U

Domain Local Groups



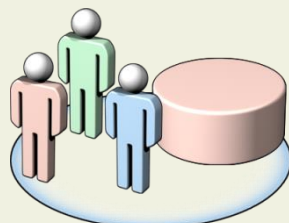
DL

Permissions



P

Local Groups



L

Group strategies:

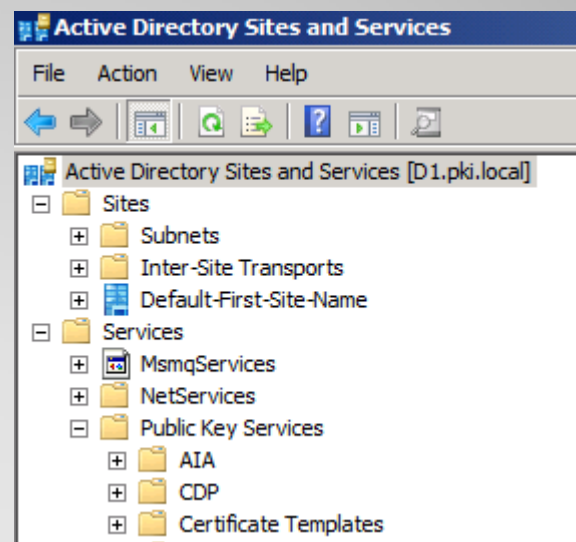
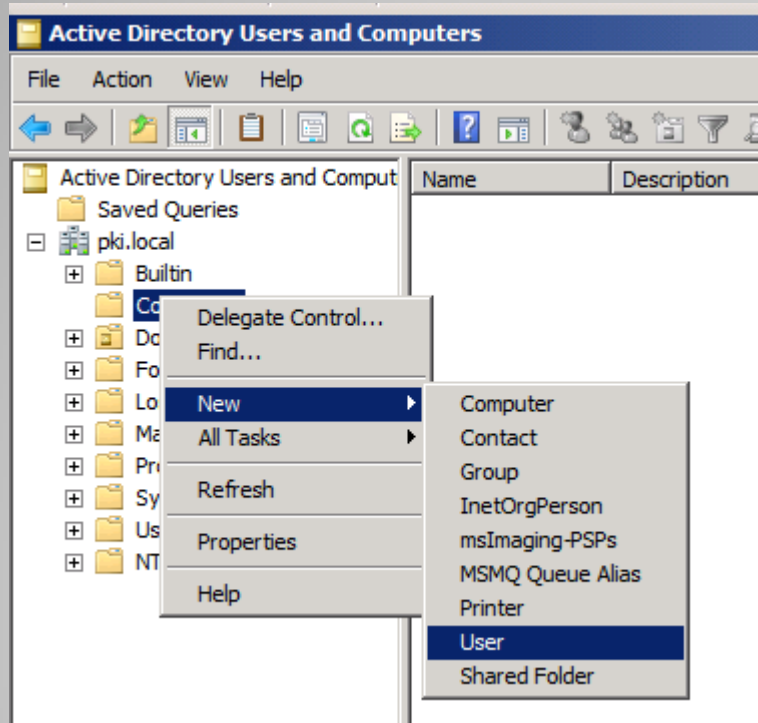
- AGP
- AGDL P
- AGUDLP
- AGGDL P
- AGLP

Strategie AGDLP (nově také IGDLA)



Nástroje pro správu

- Active Directory Administrative Center
- Active Directory Domains and Trusts
- Active Directory Module for Windows PowerShell
- Active Directory Sites and Services
- Active Directory Users and Computers
- ADSI Edit



Nástroje pro správu AD - GUI

Administrator: Command Prompt

```
c:\>dsquery user "CN=Users,DC=pki,DC=local" -name * -limit 0 | dsget user -dn -display
dn                                display
CN=Administrator,CN=Users,DC=pki,DC=local
CN=Guest,CN=Users,DC=pki,DC=local
CN=krbtgt,CN=Users,DC=pki,DC=local
CN=uagadmin,CN=Users,DC=pki,DC=local    uagadmin
CN=Admin,CN=Users,DC=pki,DC=local      Admin
CN=Franisek Uzivatel,CN=Users,DC=pki,DC=local    Franisek Uzivatel
dsget succeeded

c:\>dsadd OU "OU=Olomouc,DC=pki,DC=local"
dsadd succeeded:OU=Olomouc,DC=pki,DC=local

c:\>_
```

Administrator: Command Prompt

```
c:\>ldifde -r "(objectClass=computer)" -f C:\pocitace.ldf
Connecting to "D1.pki.local"
Logging in as current user using SSPI
Exporting directory to file C:\pocitace.ldf
Searching for entries...
Writing out entries...
3 entries exported

The command has completed successfully
```

**Nástroje pro správu AD –
příkazová řádka; export/import**

Administrator: Active Directory Module for Windows PowerShell

```
PS C:\> Get-ADUser -filter *
```

```
DistinguishedName : CN=Administrator,CN=Users,DC=pki,DC=local
Enabled           : True
GivenName        :
Name             : Administrator
ObjectClass      : user
ObjectGUID       : 39603657-15b6-47a3-88f0-0f92edb94c87
SamAccountName   : Administrator
SID              : S-1-5-21-1429467071-230515765-1440213369-500
Surname          :
UserPrincipalName :
```

Administrator: Active Directory Module for Windows PowerShell

```
PS C:\> Enable-ADOptionalFeature 'Recycle Bin Feature' -scope ForestOrConfigurationSet -target pki.local
```

```
WARNING: Enabling 'Recycle Bin Feature' on 'CN=Partitions,CN=Configuration,DC=pki,DC=local' is an irreversible action! You will not be able to disable 'Recycle Bin Feature' on 'CN=Partitions,CN=Configuration,DC=pki,DC=local' if you proceed.
```

Confirm

Are you sure you want to perform this action?

Performing operation "Enable" on Target "Recycle Bin Feature".

[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help

(default is "Y"):

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 Management

File Action View Window Help

Group Policy Management

- Forest: pki.local
 - Domains
 - pki.local
 - Default Domain Policy**
 - Domain Controller
 - Default Domain Policy
 - Olomouc
 - Group Policy Objects
 - WMI Filters
 - Starter GPOs
 - Sites
 - Group Policy Modeling
 - Group Policy Results

Default Domain Policy

Scope Details Settings Delegation

Default Domain Policy
Data collected on: 9/23/2011 4:54:12 PM

Computer Configuration (Enabled)

Policies

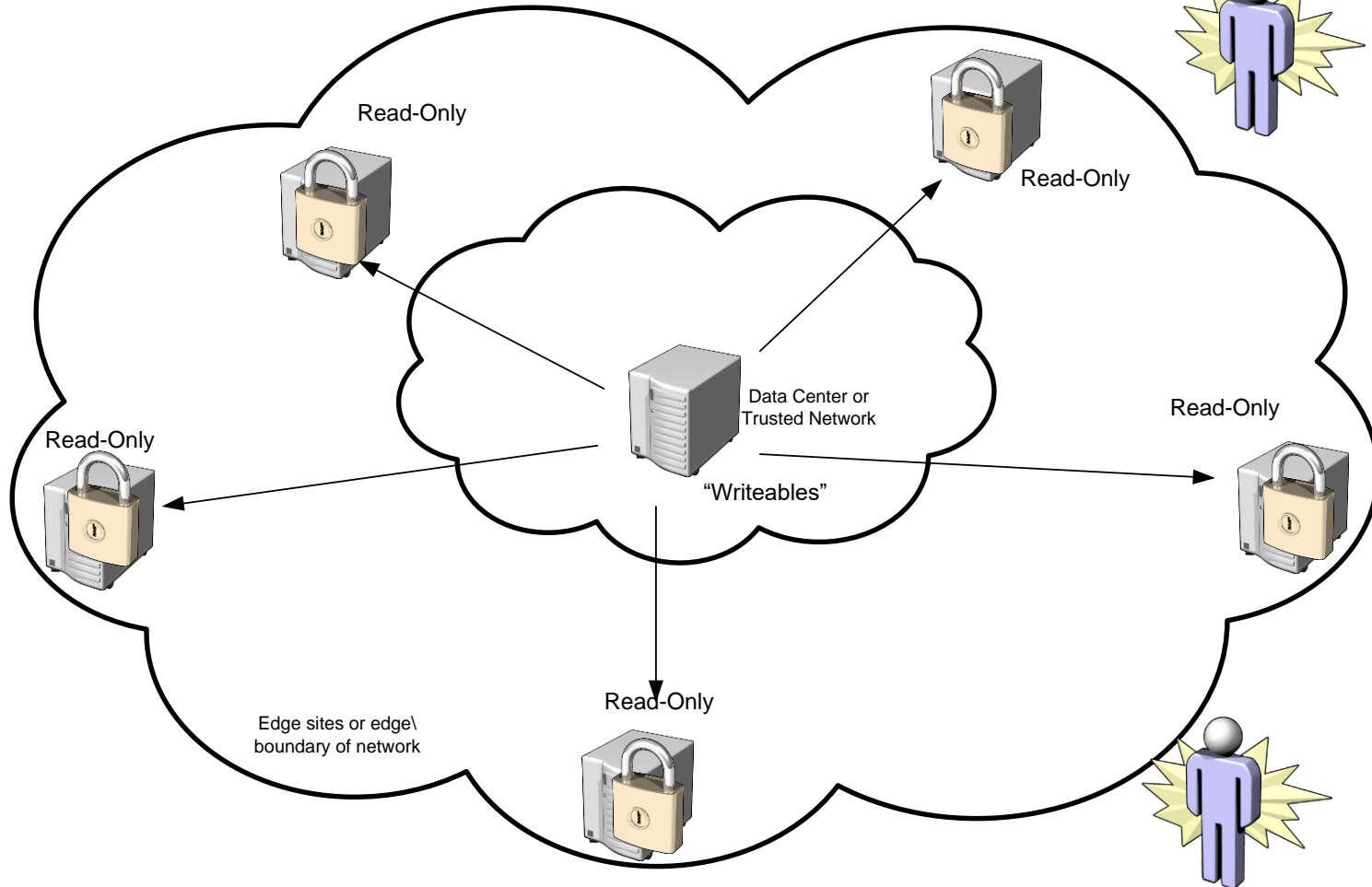
- Windows Settings
- Security Settings
 - Account Policies/Password Policy**

Policy	Setting
Enforce password history	24 passwords remembered
Maximum password age	42 days
Minimum password age	1 days
Minimum password length	7 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

- Account Policies/Account Lockout Policy**

Group policy (zásady skupin)

Directory Service "Cloud"



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