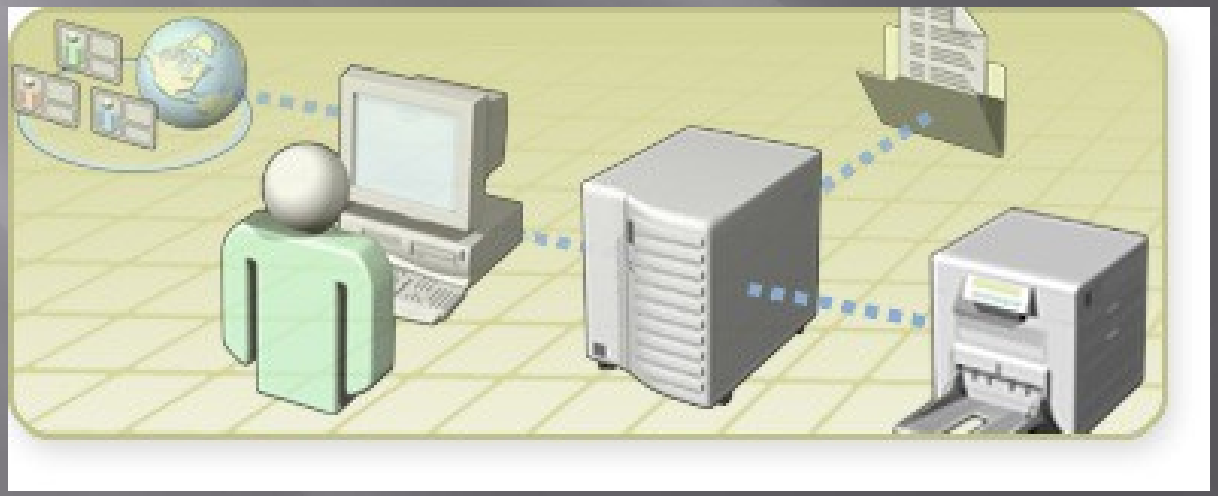
# UVOD V WINDOWS SERVER 2008 WEB, STANDARD, ENTERPRISE, CORE



# Kaj smo pogledali zadnjič?

- Namestitev Standard in CORE
- Upravljalec (Server Manager)
- Verzije in kaj katera verzija prinese
- Windows 2008 CORE – Namestitev
- Konfiguracija Windows 2008 CORE in nameščanje vlog
- Aplikacijski in spletni strežnik

# Kaj bomo pogledali danes?

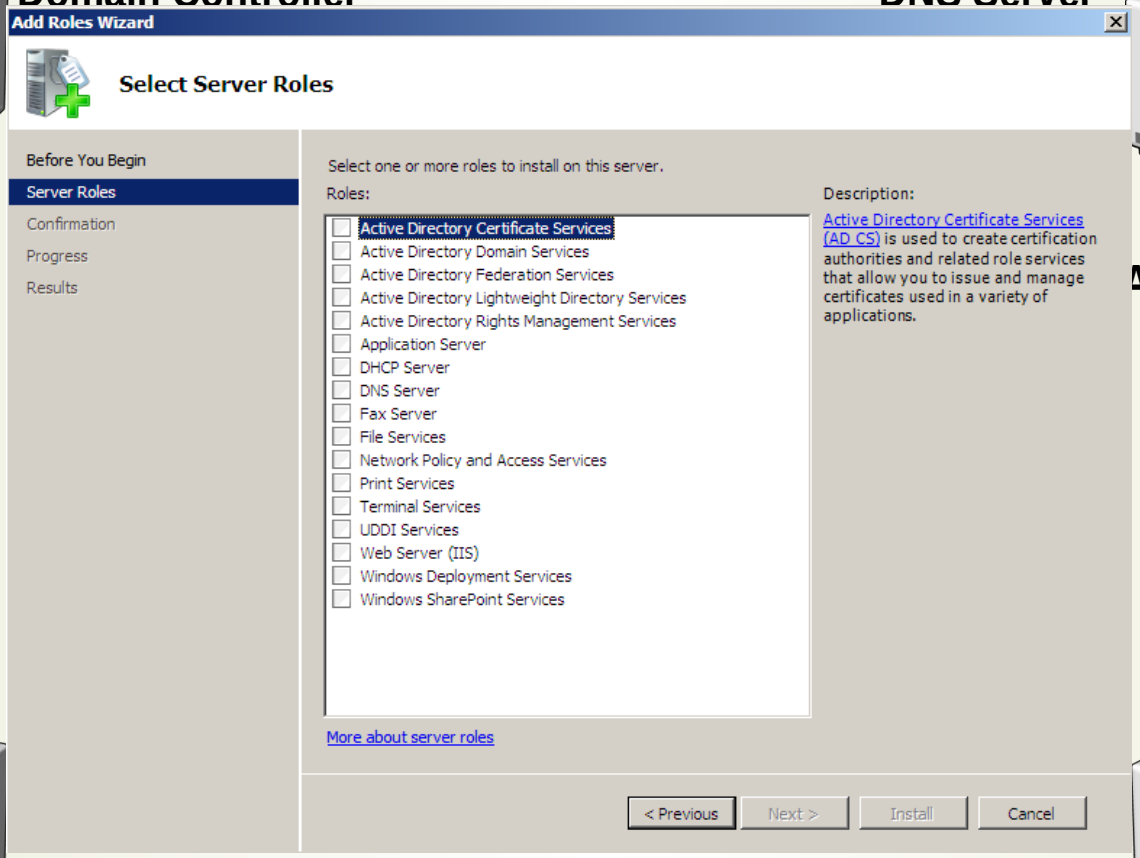
- Vloge in funkcionalnosti
- Modeli omreženja
- DNS
- Register
- Active Directory in novosti v Server 2008
- Upravljanje s skupinami in uporabniki
- Upravljanje tiskanja
- Upravljanje in konfiguracija medijev
- Varnost in nadzor strežnika

# Računalnikove vloge (Computer Roles)

Domain Controller

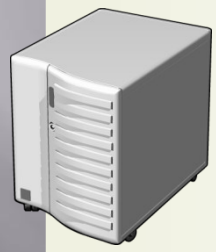
DNS Server

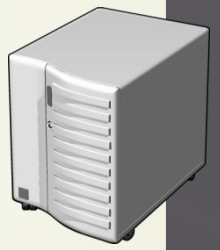


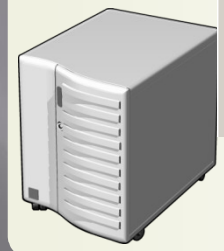


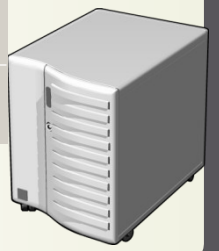

File Server

Application Server





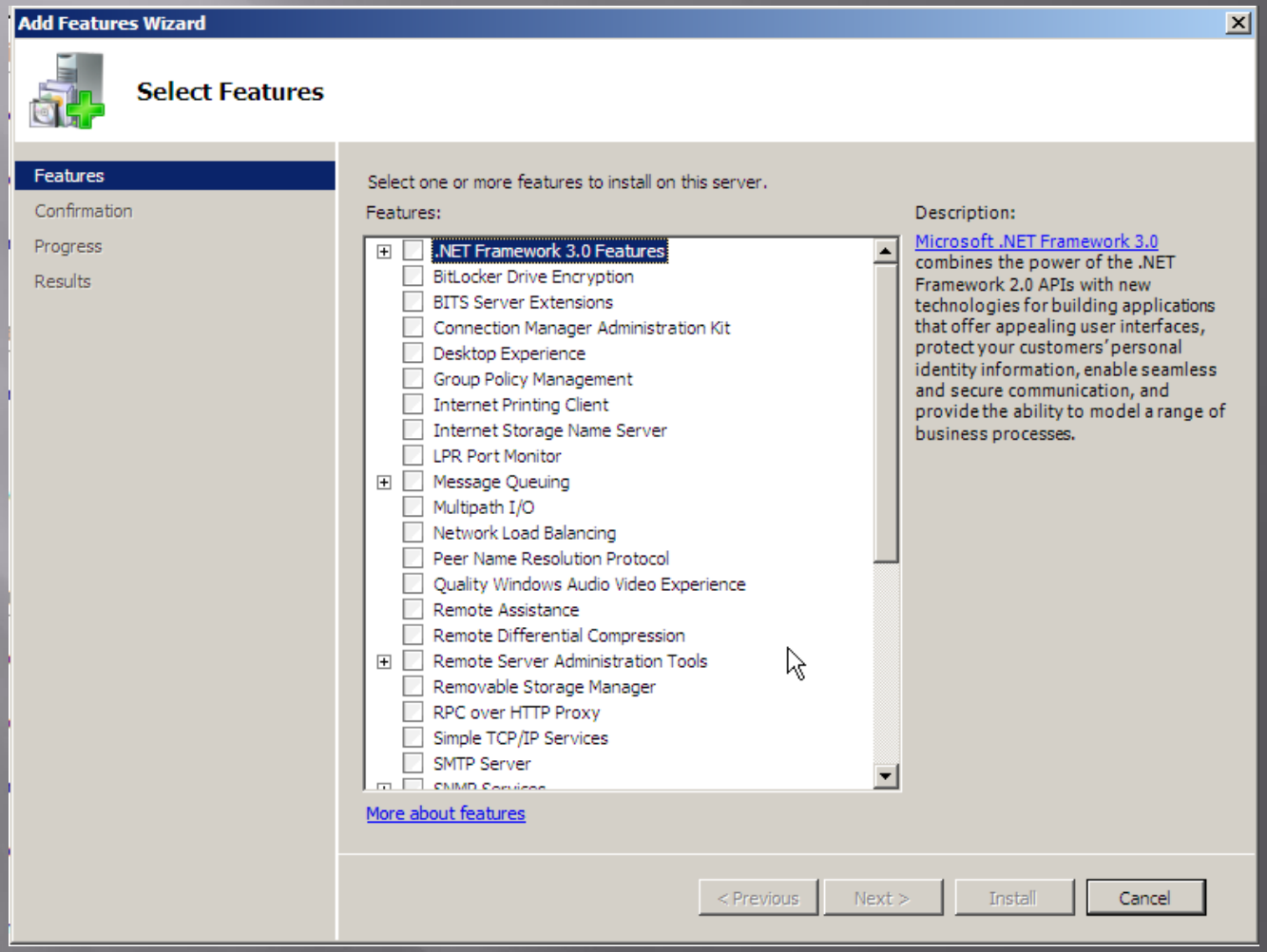




Print Server

Terminal Server

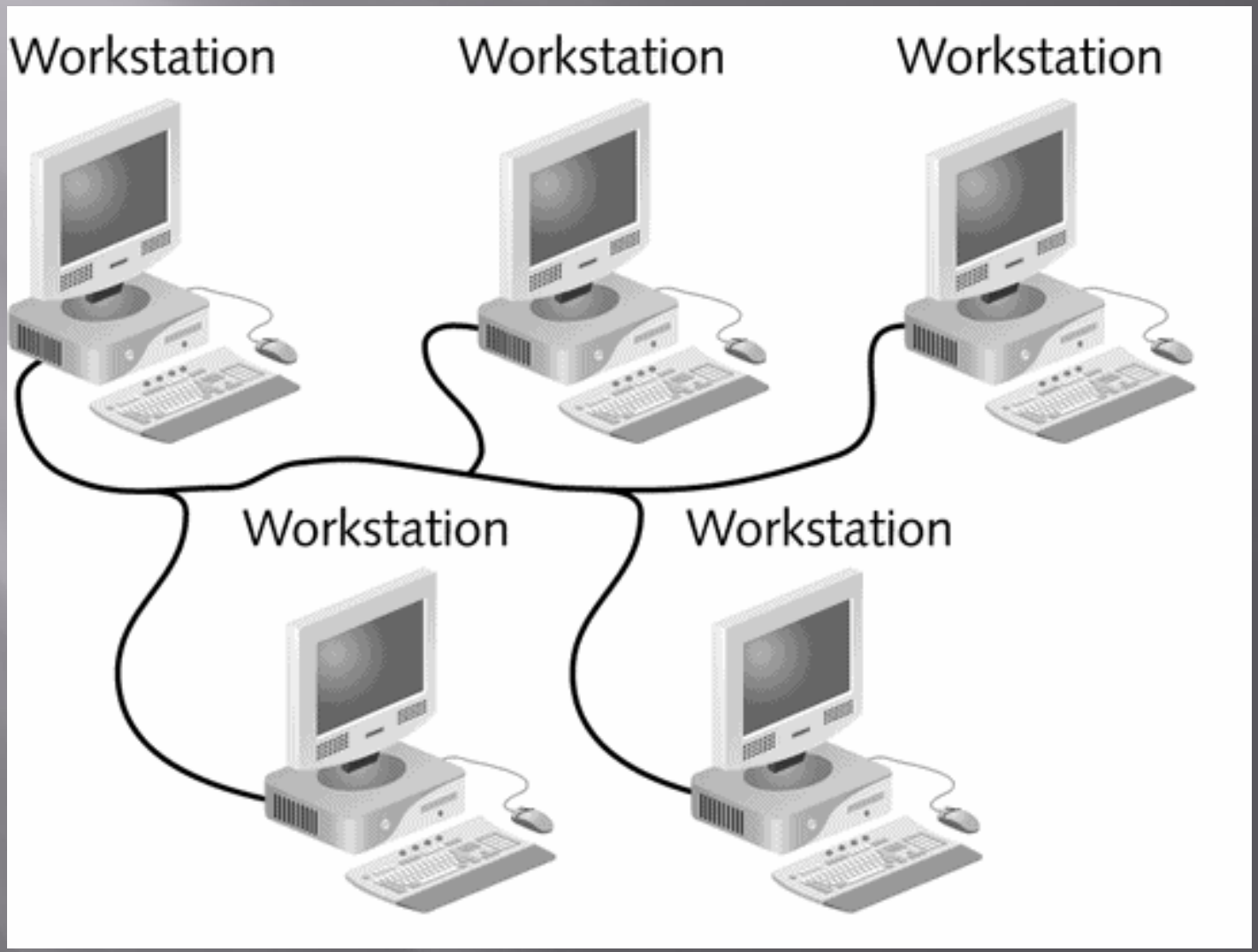
# Funkcionalnosti Windows 2008



# Načrtovanje modela omreženja z Windows Server 2008

- Omrežja so komunikacijski sistemi, ki povezujejo računalnike in njihova sredstva.
  - Fizična povezava je z ožičenjem ali z brezžičnimi napravami
  - Omrežja so lahko lokalna ali globalna
- Windows Server 2008 izvaja dva tipa omrežij.
  - Omreženje “Peer-to-peer” razprši administracijo med vsemi člani.
  - Omreženje, temelječe na strežniku, centralizira administracijo omrežja.

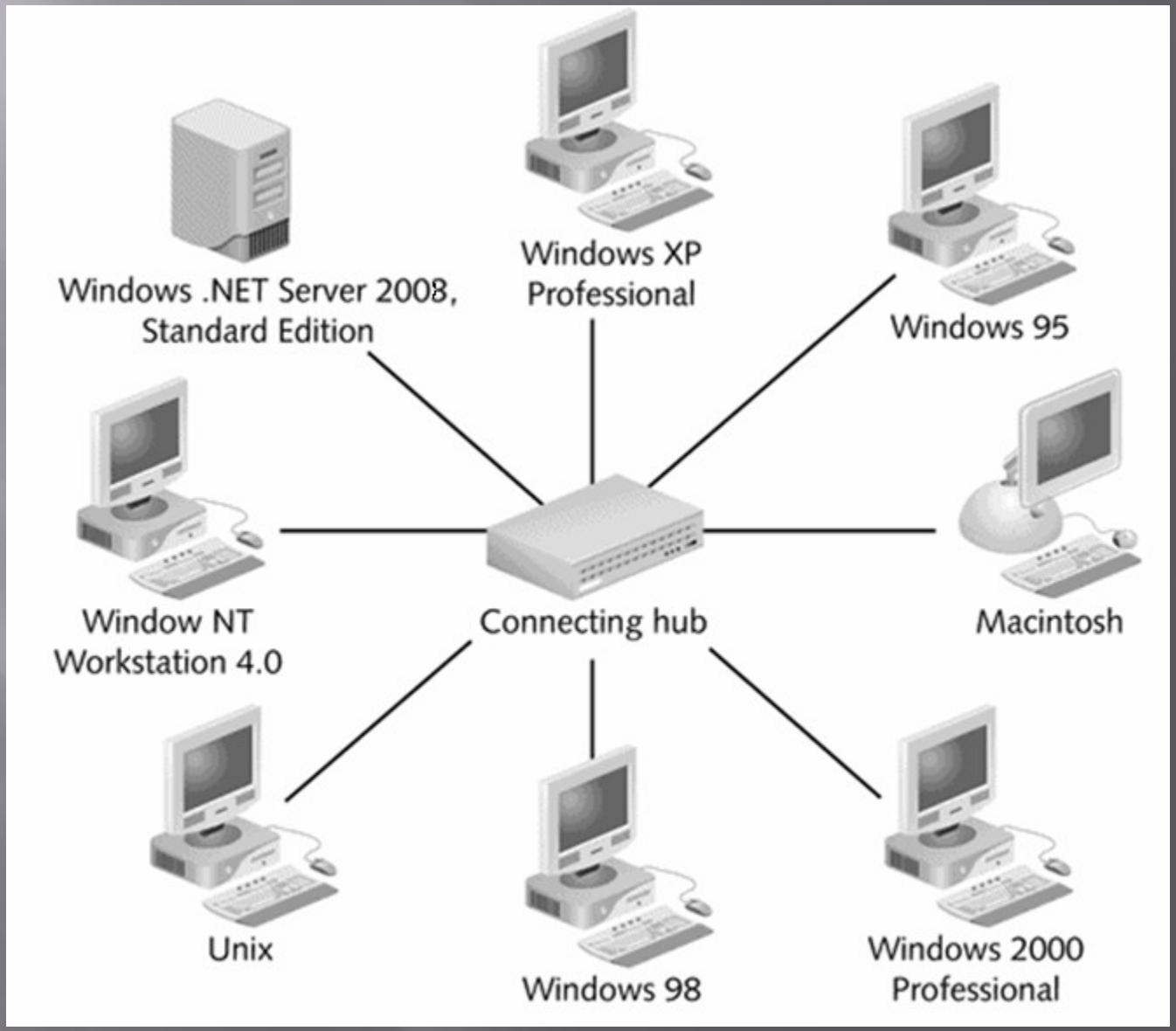
# Preprosto “peer to peer” omrežje brez strežnika



# Omrežja, osnovana na strežniku

- Uporabniki se za dostop do sredstev prijavijo (log in) le enkrat.
- Boljša varnost zaradi upravljanja s strežnikom
- Člani souporabljajo datoteke
- Souporaba tiskalnikov in drugih sredstev
- Zmožnost elektronske pošte preko strežnika elektronske pošte
- Hramba aplikacij na centralni lokaciji
- Rokovanje z varnostnimi kopijami (backups) planirano in izvajano s centralne lokacije
- Pri souporabi sredstev lahko opoštevamo delovne navade podskupin.
- Bolj učinkovito ažuriranje programske opreme

# Omrežja, osnovana na strežniku



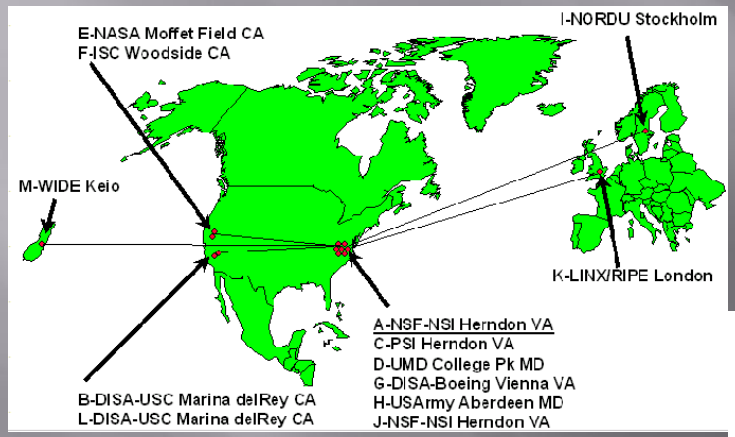
# Imena IP

- IP naslovi so morda lahko za računalnike, ljudje pa raje uporabljamo imena.
  - http://www.fri.uni-lj.si raje kot http://193.2.104.250
- To naredimo z:
  - Tabelami “Host lookup” na vsakem stroju

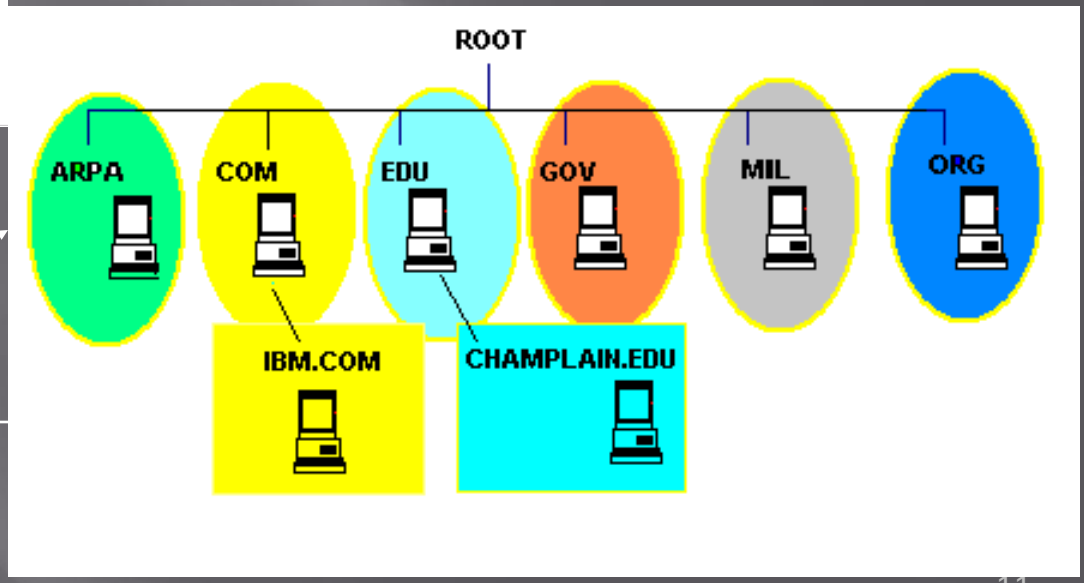
    - ali-
  - Strežnikom “Domain Name Server” (DNS)

# Hierarhija DNS

**DNS je organiziran v hierarhične domene**




Centralni DNS strežniki so locirani na vrhu DNS hierarhije. Vzdržujejo podatke o vsaki od con najvišjega nivoja.




- Domenski strežniki najvišjega nivoja so za arpa, com and edu itd.
- Posamezne organizacije vzdržujejo lokalne imenske strežnike

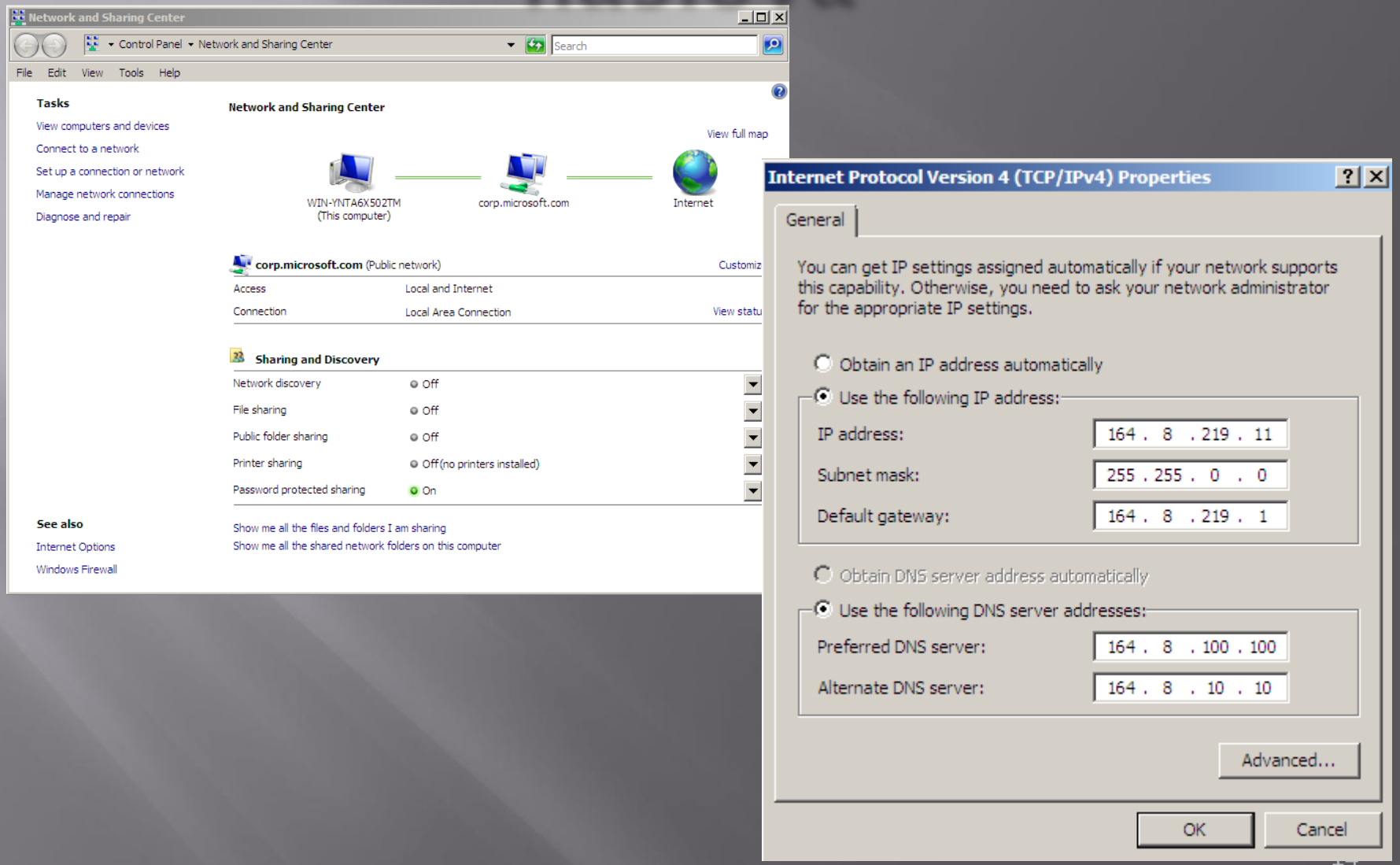
# Fizični naslovi in protokol za resolucijo naslova

- Vsak računalnik ima fizični naslov, ki je definiran z njegovo omrežno kartico “network interface card” (NIC).
- Fizičnemu naslovu pravimo  naslov “media access control” (MAC).
- TCP/IP temelji na naslovih IP in MAC.
- Naslove dobimo s pomočjo protokola “Address Resolution Protocol” (ARP).
  - ARP medpomnilnik (cache) vsebuje že ugotovljene in statične MAC naslove.
  - ARP pošlje paket, ki zahteva naslov MAC, če ta ni v medpomnilniku.

# Konfiguriranje TCP/IP

- Izbira o statičnega ali dinamičnega naslavljanja.
- Za usmerjevalnike, strežnike in za sledenje omrežnim problemom.
- Statično naslavljanje lahko izvedemo ročno, vendar pozor na napake!!.
- Windows Server 2008 podpira  avtomatično naslavljanje.
  - Automatic Private IP Addressing (APIPA)
  - Dinamično naslavljanje z uporabo strežnika DHCP

# Konfiguriranje statičnega IP naslova



# Windows Server 2008 Registry

- Kompleksna podatkovna baza, ki vsebuje vse podatke, ki jih o strežniku potrebuje operacijski sistem
- 5 osnovnih ključev
  - HKEY_LOCAL_MACHINE
    - Podatki o vseh aparaturnih komponentah
  - HKEY_CURRENT_USER
    - Podatki o namestitvi namizja za uporabnika, ki je trenutno logiran na konzoli strežnika
  - HKEY_USERS
    - Podatki o profilu vseh uporabnikov, logiranih na računalnik
  - HKEYS_CLASSES_ROOT
    - Podatki za asociacijo podaljškov datotek s programi
  - HKEY_CURRENT_CONFIG
    - Podatki o trenutnih profilih aparaturne opreme

# Vsebina registra (nadaljevanje)

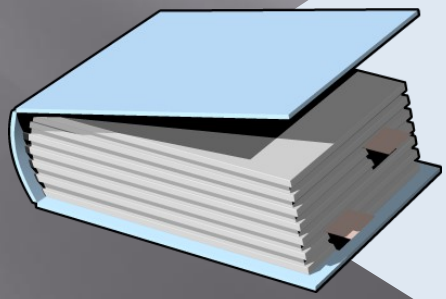
Bolj podrobno razdeljena na podključe in vhode

- Vhodi
  - Trije deli:
    - Ime
    - Tip podatka
    - Konfiguracijski parameter
  - Trije formati podatkov:
    - DWORD je šestnajstiški
    - String je tekstovni podatek
    - Binary sta dve šestnajstiški vrednosti

# UVOD V AKTIVNI IMENIK IN UPRAVLJANJE KONTOV

# Kaj je “Domain Service”?

- Identificira sredstva
- Nudi konsistenten način za:
  - poimenovanje
  - opisovanje
  - lociranje
  - dostop
  - upravljanje
  - varovanje



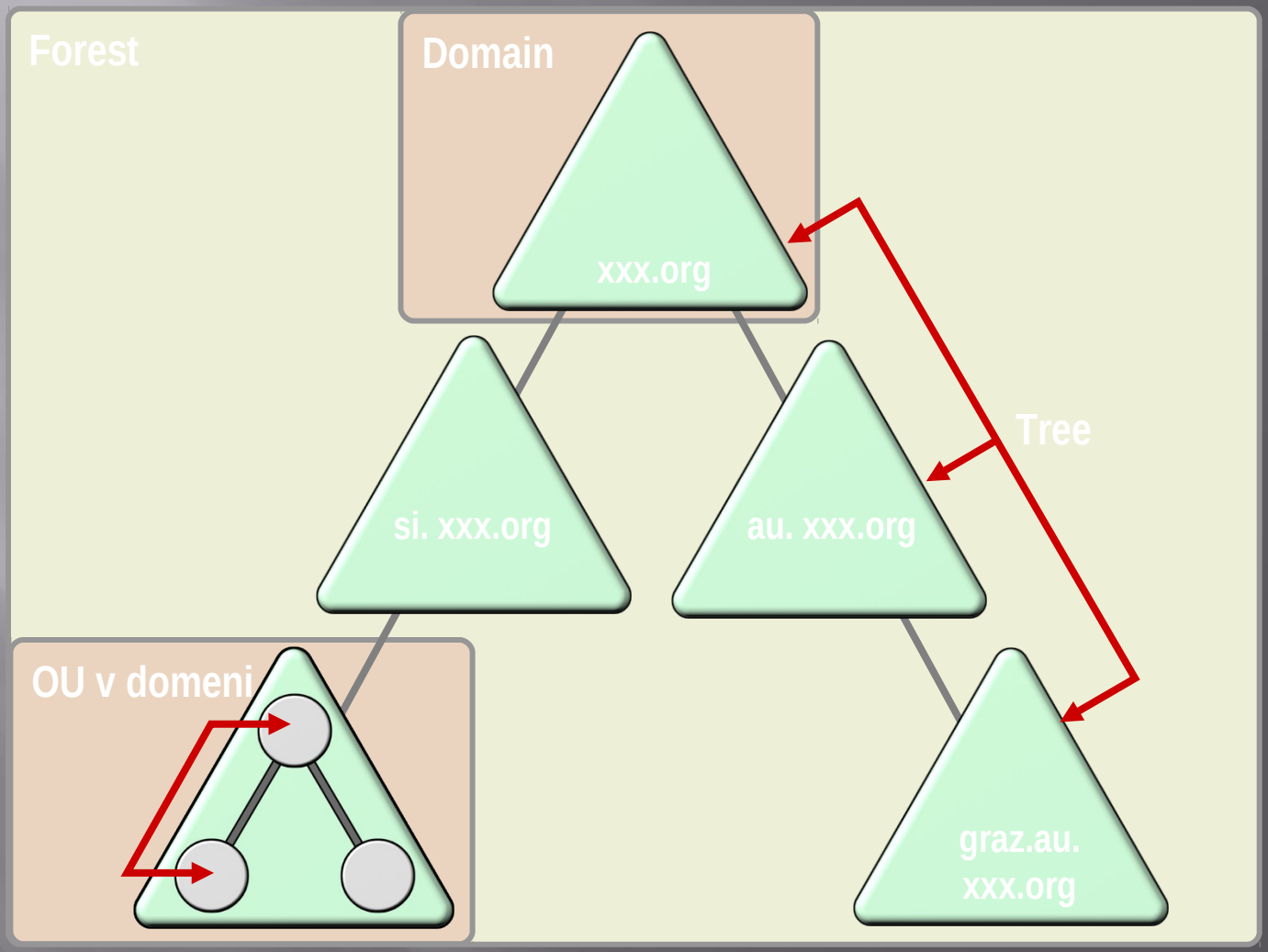
**Ugodnosti aktivnega imenika**

- **DNS integracija**
- **Skalabilnost**
- **Centralizirano upravljanje**
- **Delegirana administracija**

# Zakaj aktivni imenik?

- Servis, ki hrani podatke o vseh omrežnih sredstvih
- Centralizirano upravljanje omogoča hitro iskanje in dostop do sredstev

# Terminologija aktivnega imenika



# Aktivni imenik je porazdeljen

- *Porazdeljenost pomeni, da je podatkovna baza AD razdeljena na particije direktorija (**directory partitions**)*
  - Vsaka particija vsebuje
    - Shemo celotnega gozda
    - Konfiguracijo gozda (metadata)
    - Razdelke imenika po domenah (aktualni objekti)
  - Omogoča razdelitev in porazdelitev delov podatkovne baze AD zaradi bolj učinkovitega omrežja, predvsem za..
    - Hitrejše logiranje
    - Zmanjšanje prometa pri replikacijah
- Vsak DC ima podatkovno bazo **Ntds.dit**, ki pomni podatke AD (aktivnega imenika).

# Replikacije aktivnega imenika

- Kopije Multimaster
  - Vsaka sprememba na enem DC se skopira (replication) na druge DC
  - Če en DC izpade, ni vidne prekinitve omrežja
- Kopiranje lahko nastavimo na določene intervale namesto takojšnjega kopiranja, ko pride do spremembe
- Omrežni promet zaradi kopiranj lahko zmanjšamo s:
  - Kopiranjem posameznih lastnosti namesto celotnih kontov
  - Kopiranjem, osnovanim na hitrosti omrežnih povezav
    - Bolj pogosto kopiramo preko lokalne mreže (LAN), kot preko globalne (WAN)

# Replikacije aktivnega imenika

- ***Replikacija*** *je način, kako se spremembe v aktivnem imeniku posredujejo med vsemi domenskimi krmilniki (DC, domain controllers) v gozdu (forest).*

- AD replikacija je **multi-master** replikacija
  - Noben domenski krmilnik ni "glavni". Vsak DC je zapisljiv (writable) in lahko sprejme posodobitve podatkov.
  - Konflikti med posodobitvami se rešujejo po principu "zmaga zadnji pisalec"

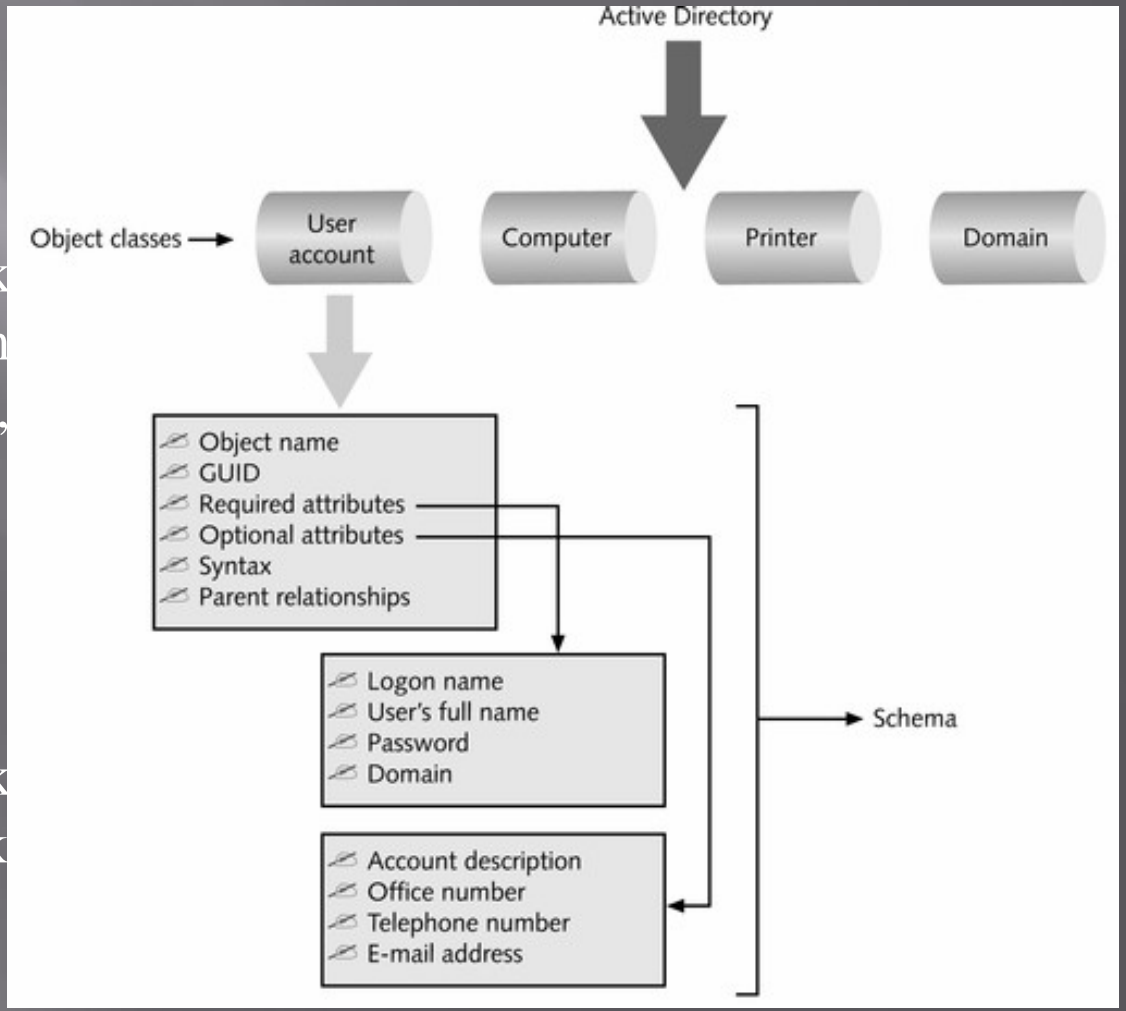
- **Latenca** – Zavedati se moramo, da je za to, da posodobitve dosežejo vse DC v gozdu, potreben čas. V danem trenutku se lahko zgodi, da aktivni imenik ni konsistenten.

# Shema (schema)

- *Shema je opis (ali slika ali diagram) struktur podatkovne baze.*

- Shema aktivnega imenik (Active Directory schem določa razrede objektov, kot so uporabniki, skupine, računalniki, domene itd.

- Shema aktivnega imenik je razširljiva. Stvari lahk dodajamo!



# Shema

- Definira razrede objektov in njihove atribute, ki jih lahko vsebuje aktivni imenik
- Vsak razred objektov vsebuje globalno edinstven identifikator (globally unique identifier, GUID)
  - Edinstveno število, pridruženo imenu objekta
- Razred objektov ima lahko zahtevane in dodatne atribute
- Vsakemu atributu je dodana številka verzije in datum tvorbe ali spremembe
  - Omogoča posodobitve za le dane vrednosti v vseh domenskih kontrolerjih (DC)
- Windows Server 2008 ima več privzetih razredov objektov

# Globalni katalog

- *Medtem ko vsak domenski krmilnik vsebuje polno repliko za svojo domeno, drži strežnik z globalnim katalogom (**global catalogue server**) omejeno množico atributov za vse objekte v celotnem gozdu.*
  - Na primer:
    - Atribute, ki so najbolj pogosto iskani
    - Ali potrebni za logiranje
- Tako zagotavlja hiter dostop do podatkov za avtentikacijo in druga povpraševanja in iskanja. Klijentu ni potrebno skakati od strežnika do strežnika preko več domen, da bi dobil iskan podatek iz imenika.

# Globalni katalog

- Pomni podatke vseh objektih v gozdu (forest)
  - Popolne kopije objektov v lastni domeni in delne kopije objektov iz drugih domen
- Overovlja uporabnike, ko se logirajo
- Nudi vpogled in dostop do vseh sredstev v vseh domenah
- Nudi kopiranje ključnih elementov aktivnega imenika
- Zaradi hitrejšega dostopa vzdržuje kopijo najbolj pogosto uporabljanih atributov objektov.

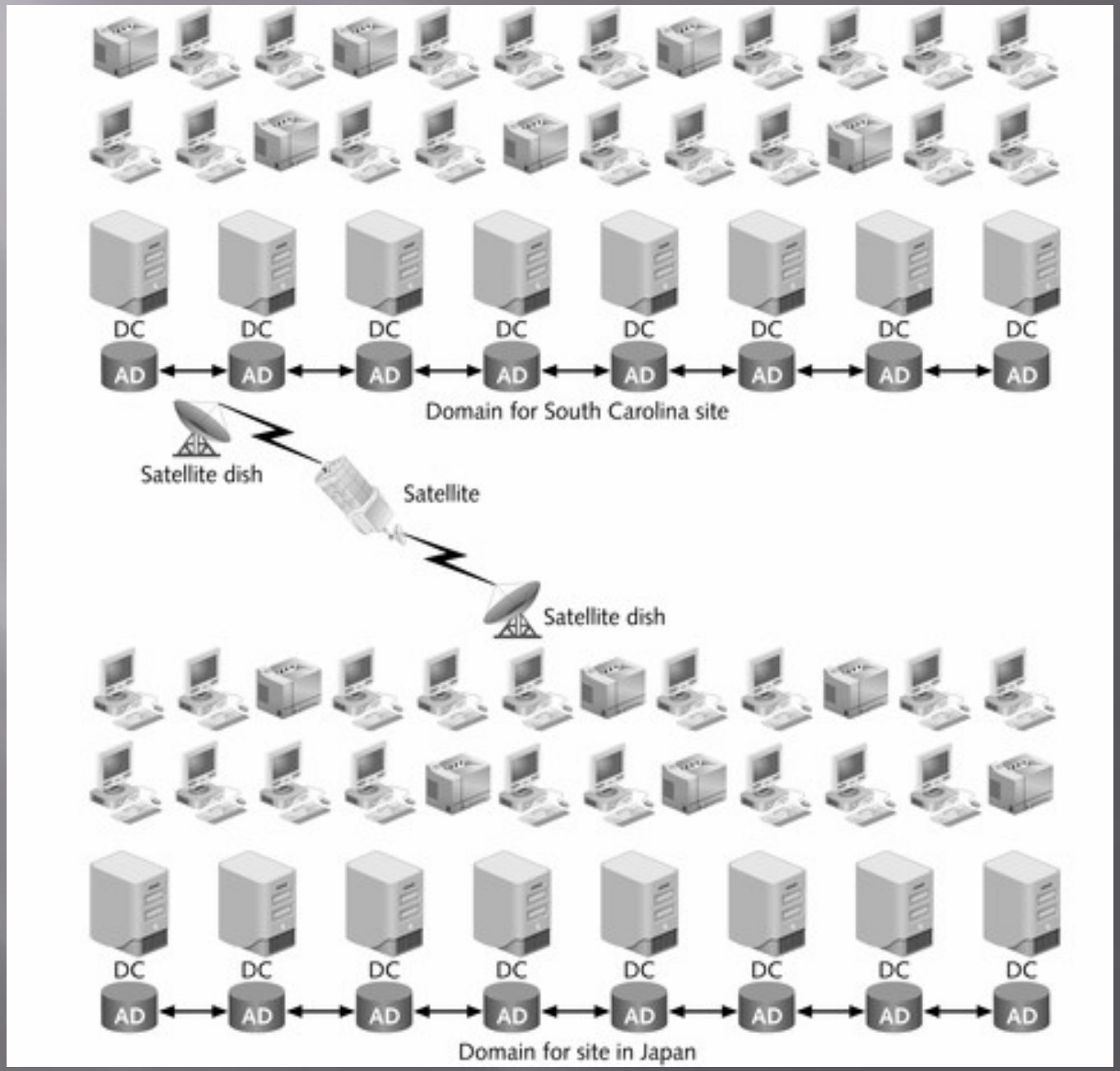
# Vsebovalniki v aktivnem imeniku

- Hierarhični elementi, urejeni v drevesno strukturo
- Vsebovalniki v aktivnem imeniku vključujejo:
  - Gozdove (Forests)
  - Drevesa (Trees)
  - Domene (Domains)
  - Organizacijske enote (Organizational units)
  - Položaje (Sites)

# Domena

- Primarni vsebovalnik skupine objektov
- Nudi particijo za pomnenje objektov, ki imajo skupno razmerje
  - Particije odražajo upravljalna in varnostna razmerja
- Vzpostavlja skupino podatkov, ki naj bi bila kopirana iz enega domenskega krmilnika (DC) na drugega
- Pospešuje upravljanje z množico objektov

# Uporaba več domen

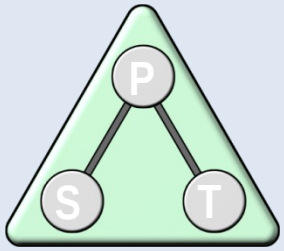


# Organizacijska enota

- Tvorba skupin objektov znotraj domene
- Omogoča delegiranje strežniških administrativnih vlog
  - Skupine objektov glede na upravljalske naloge
- Nudi možnost administracije objektov s skupinskimi politikami (Group Policies)
  - Skupine objektov s podobnim varnostnim dostopom
- Je lahko vgnezdena znotraj drugih organizacijskih enot
- Organizira objekte v domeni
- Omogoča delegiranje administrativnega nadzora
- Poenostavlja upravljanje sredstev, združenih v skupine

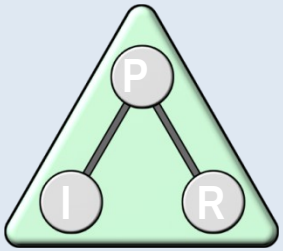
# Hierarhični modeli organizacijske enote

**Glede na funkcijo**



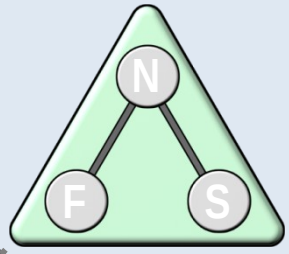

**P** – prodaja
**S** – Svetovanje
**T**- Trženje

**Glede na organiziranost**




**P** – Proizvodnja
**I** – Inženiring
**R** - Raziskave

**Glede na lokacijo**




**N** – Norveška
**F** – Francija
**S** – Slovenija

**Mešani primeri**

- **Funkcija**
  - Organiziranost
- **Lokacija**
  - Funkcija
- **Organiziranost**
  - Lokacija

# Navodila za vsebnike

- Aktivni imenik naj bo čimbolj preprost, njegovo strukturo planirajmo še pred njegovo izvedbo
- Implementirajmo čim manjše število domen
- Na večini majhnih omrežij uvedimo le eno domeno
- Ko neka organizacija načrtuje svojo reorganizacijo, uporabimo organizacijske enote, ki naj odražajo njeno strukturo
- Tvorimo le toliko organizacijskih enot, kolikor je nujno potrebnih

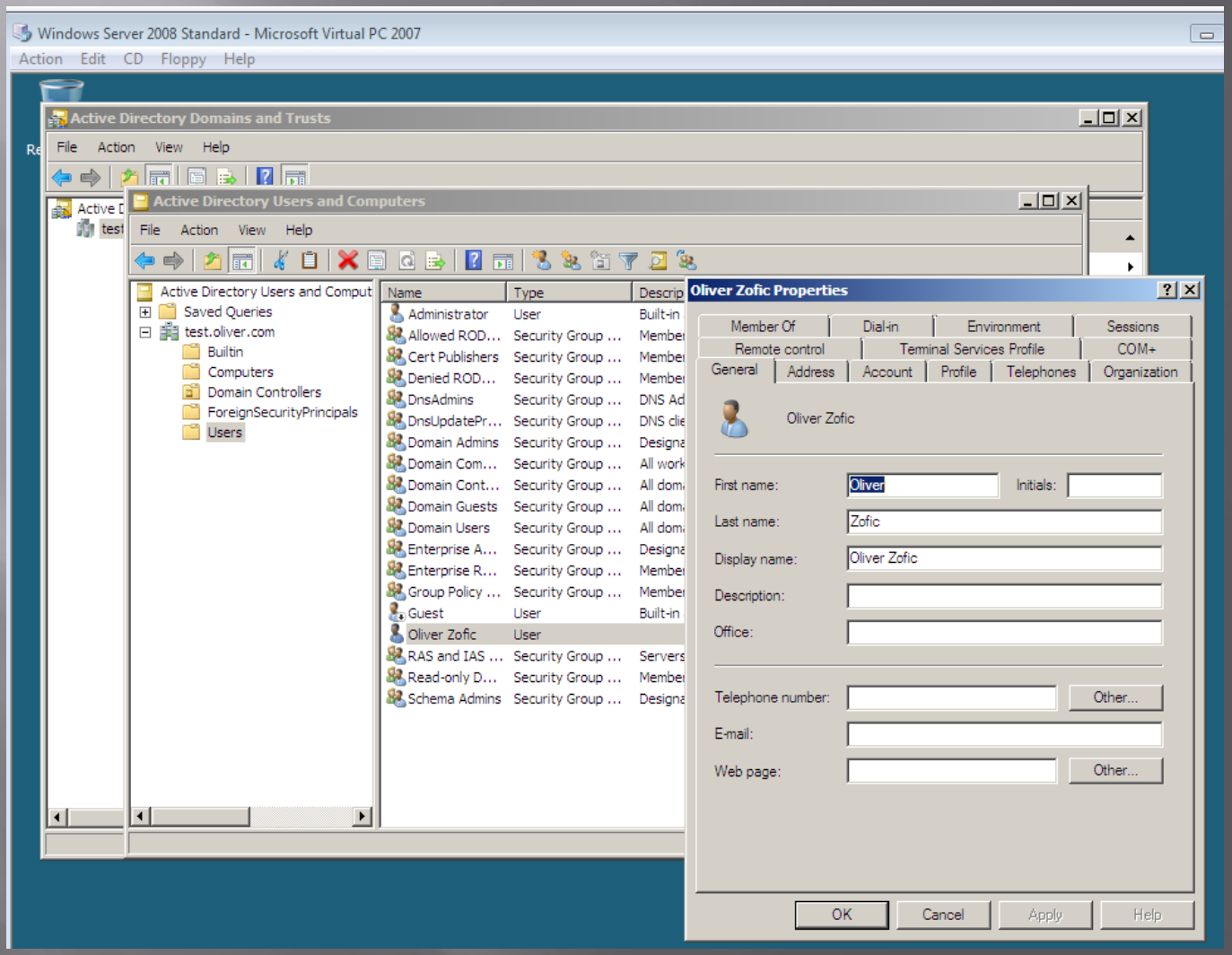
# Navodila za vsebnike (nadaljevanje)

- Ne tvori aktivnega imenika z več kot 10 nivoji organizacijskih enot (najbolj primerno 1 ali 2 nivoja)
- Uporabi domene kot razdelke v gozdih in tako označi povezane konte in sredstva, ki jih upravljamo s skupinskimi in varnostnimi politikami
- Uporabi več dreves in gozdov le, če je nujno potrebno
- Uporabljaj položaje (sites) tam, kjer imamo več podomrežij in geografskih lokacij. Tako izboljšamo performanse logiranja in replikacij.

# Novosti Windows Server 2008

- Novo poimenovanje
  - Prej AD Directory Service je sedaj AD Domain Service
  - Prej AD Aplication Mode je sedaj AD Lightweight Directory Services
  - Prej Certificate Services  so sedaj AD Certificate Services
  - Prej Windows Rights Management Services so sedaj Active Directory Rights Management Services
- AD Directory Service in Certificate Services sta lahko nameščena ločeno
- Authorization Manager, Active Directory Application Mode, Active Directory Federation Services so sedaj ločene komponente

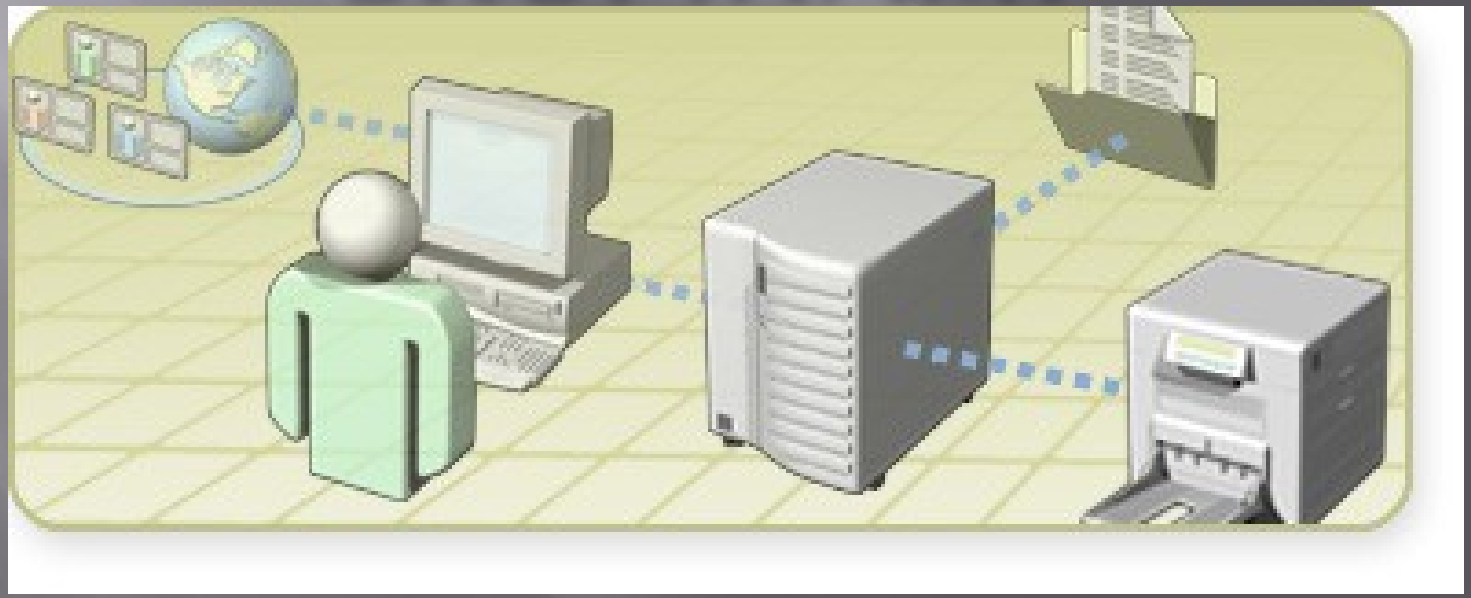
# Upravljanje z uporabniškimi konti



# Upravljanje z uporabniškimi konti

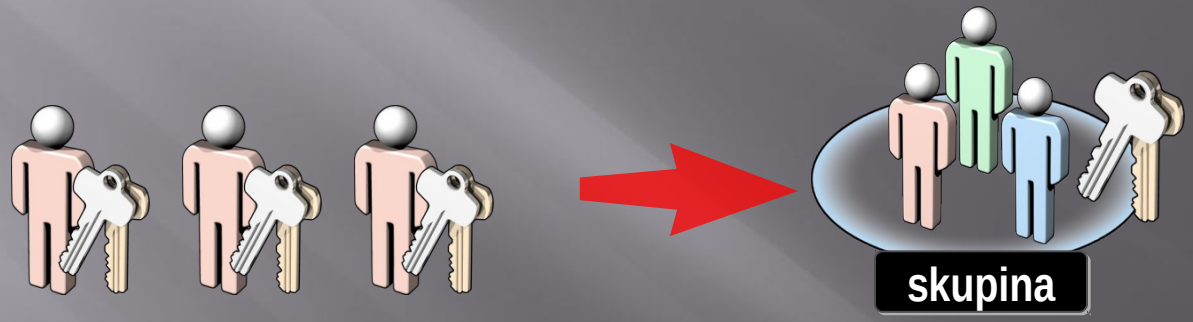
- Okolje za vzpostavitev in upravljanje kontov
  - S pomočjo samostojnega strežnika brez aktivnega imenika:
    - Uporabimo orodje “Local Users and Group”
  - V domeni z nameščenim aktivnim direktorijem:
    - Uporabimo orodje “Active Directory Users and Computers”
- Upravljalske naloge:
  - Tvorba konta
  - Blokiranje, omogočanje in preimenovanje konta
  - Premik konta
  - Resetiranje gesla
  - Brisanje konta

# UPRAVLJANJE S SKUPINAMI



# Kaj so skupine?

Skupine (groups) poenostavijo administracijo pri dodeljevanju dovoljenj za sredstva




| Tip skupine | Opis |
| --- | --- |
| Varnost | Uporaba za dodeljevanje pravic in dovoljenj uporabnikom<br>Lahko uporabljamo za distribucijski seznam e-pošte |
| Porazdeljenost | Lahko uporabimo le pri elektronski pošti<br>Ne moremo uporabljati za dodeljevanje dovoljenj |

# Skupine (groups)

- Vgrajene (built-in), Vnaprej določene (predefined) in posebne (special) skupine

**Vgrajene skupine:**

Account Operators
Administrators
Backup Operators
Guests
Print Operators
Replicator
Server Operators
Users

**Vnaprej določene:**

Cert Publishers
Domain Admins
Domain Computers
Domain Controllers
Domain Guests
Domain users
Enterprise Admins
Group Policy Admins
Schema Admins

**Posebne skupine:**

Everyone
Authenticated Users
Network Users
Interactive
Service
Self
Creator/Owner

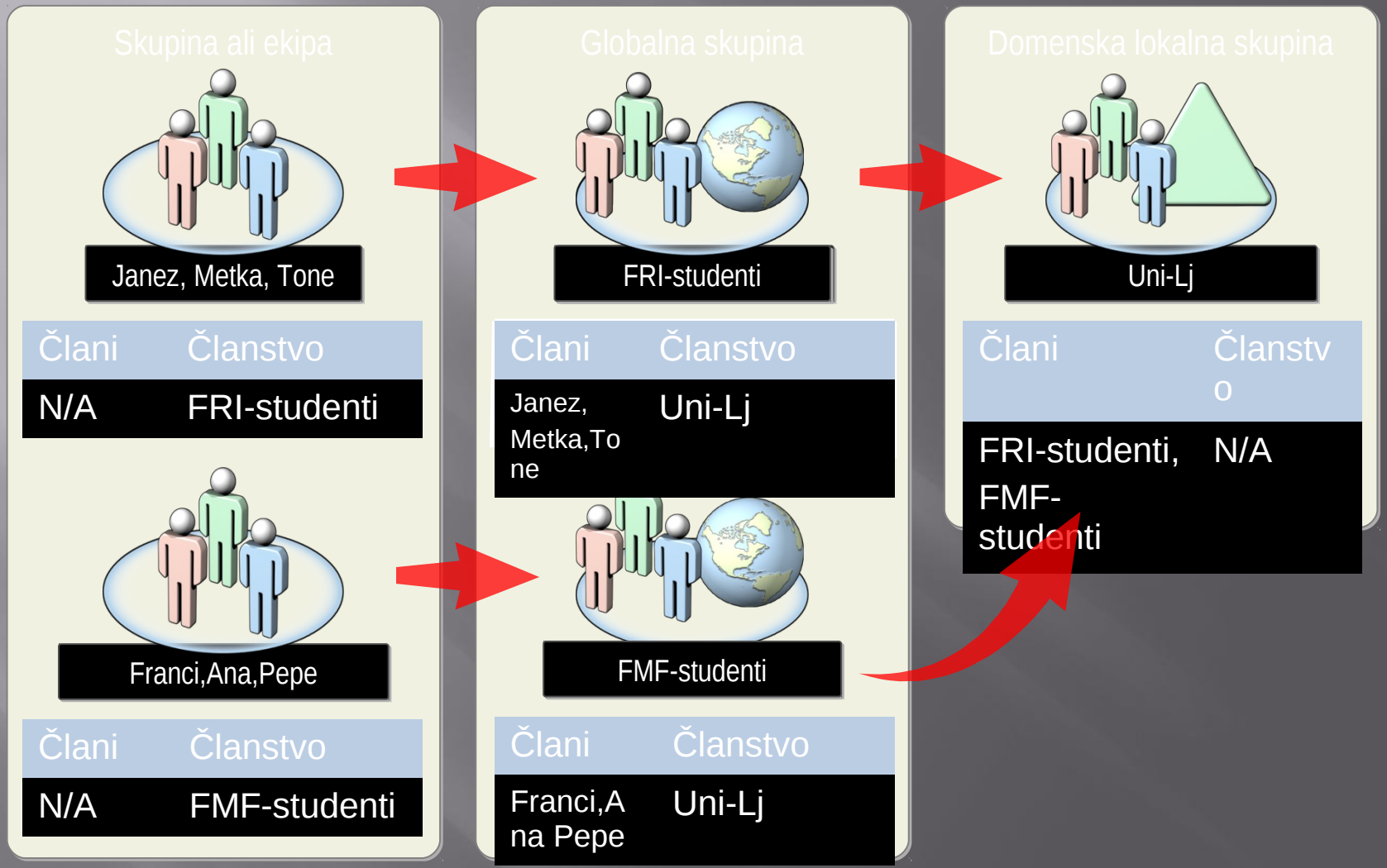
# Doseg skupine

- Doseg skupine (**scope of a group**) določa območje za dostop objektov aktivnega imenika.
  - V bistvu to pomeni:
    - Kje je skupina vidna
    - Katere uporabnike in skupine lahko ta skupina vključuje
  - Tipi skupin glede na delokrog:
    - **Lokalne (Local)** – le člani samostojnega strežnika
    - **Domenske lokalne (Domain local)** – Vidne v eni domeni, lahko vključujejo druge tipe skupin
    - **Globalne** – Vidne v gozdu. Vključujejo le uporabnike in skupine iste domene
    - **Univerzalne** – Vidne v gozdu, vsebujejo lahko kateregakoli uporabnika ali skupino

# Lastnosti skupin

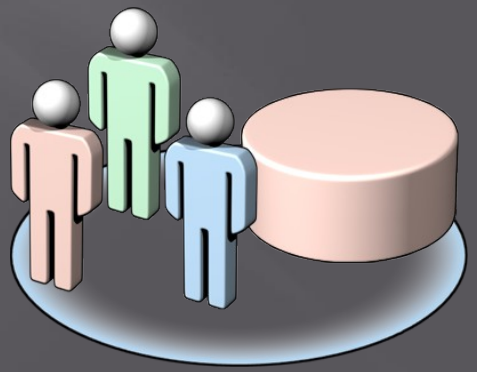
- Splošne
  - Spreminjanje opisa, delokroga in tipa skupine ter elektronskih naslovov za porazdeljeno skupino
- Člani
  - Dodajanje ali brisanje članov skupine
- Članstvo
  - Dodajanje ali brisanje članstva skupine v drugi skupini
- Upravnik (kdo jo upravlja)
  - Vzpostavitev konta ali skupine, ki upravlja s skupino

# Lastnosti "član" in "članstvo"

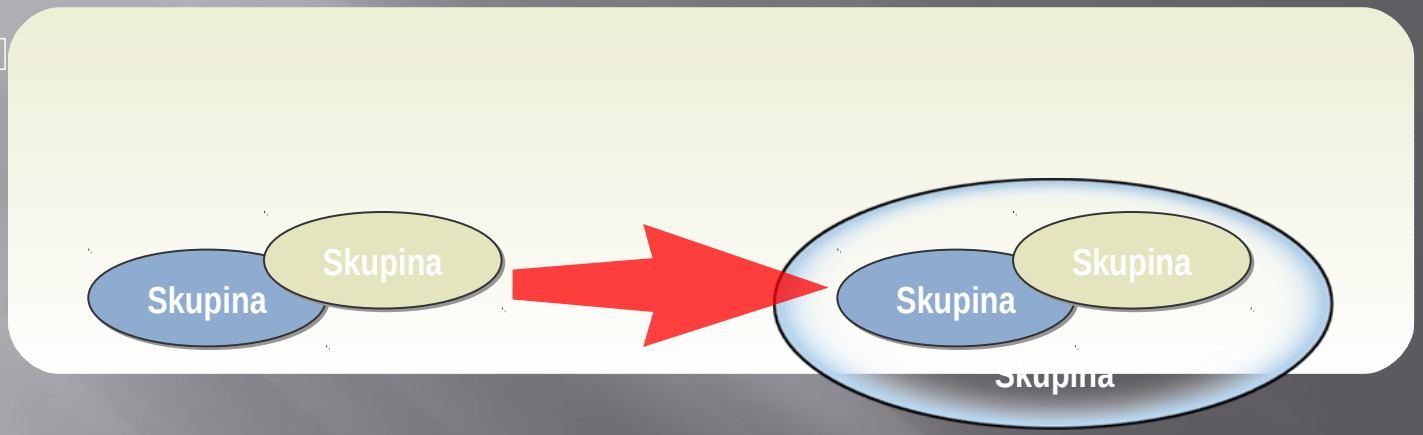


# Uvedba lokalnih skupin

- Uporabimo na samostojnih strežnikih, ki niso del domene
- Uporabimo tudi na članskih strežnikih v domeni
- Delokrog je omejen le na lokalni strežnik
- Skupine razdeljene na osnovi varnostnega dostopa do lokalnega strežnika
- Tvorba z orodjem za lokalne uporabnike in skupine



# Kaj je gnezdenje skupin?




- Z gnezdenjem skupin utrdimo upravljanje skupin
- Možnosti gnezdenja so odvisne od tega, ali je domenski funkcionalni nivo domene Windows Server 2003/2008 nastavljen na “Windows 2000 native” ali “Windows 2000 mixed”

# Navodila za imenovanje skupin

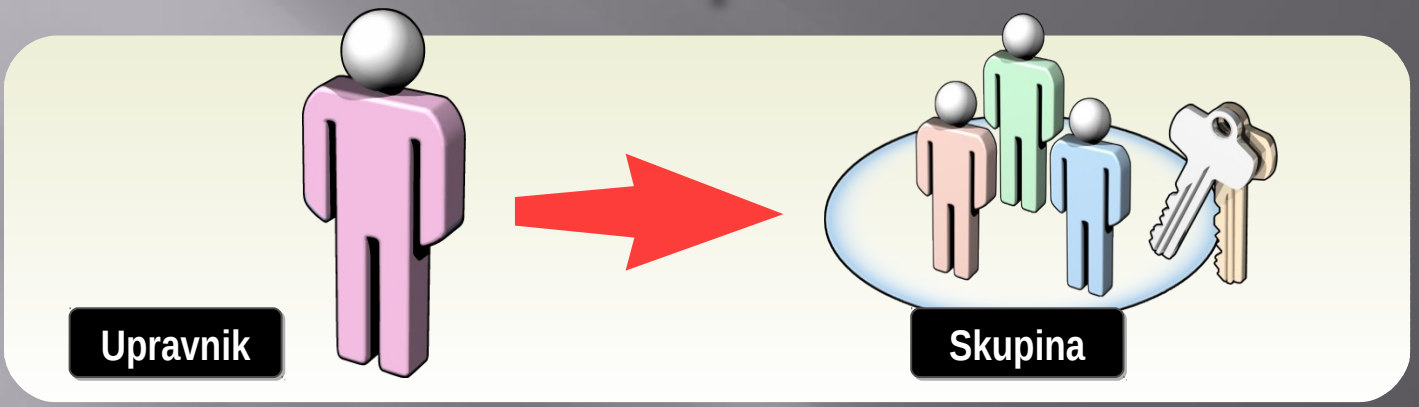
## Za varnostne skupine:

- V ime skupine vključi delokrog skupine
- Ime mora odražati pripadnost (ime oddelka ali ekipe)
- Na začetek imena skupine daj ime domene ali okrajšavo imena
- Uporabljaj opisnik za razpoznavo maksimalnih dovoljenj, ki jih lahko ima skupina, na primer UNILJ FRI OE ŠTUDENTI

## Za porazdeljene skupine:

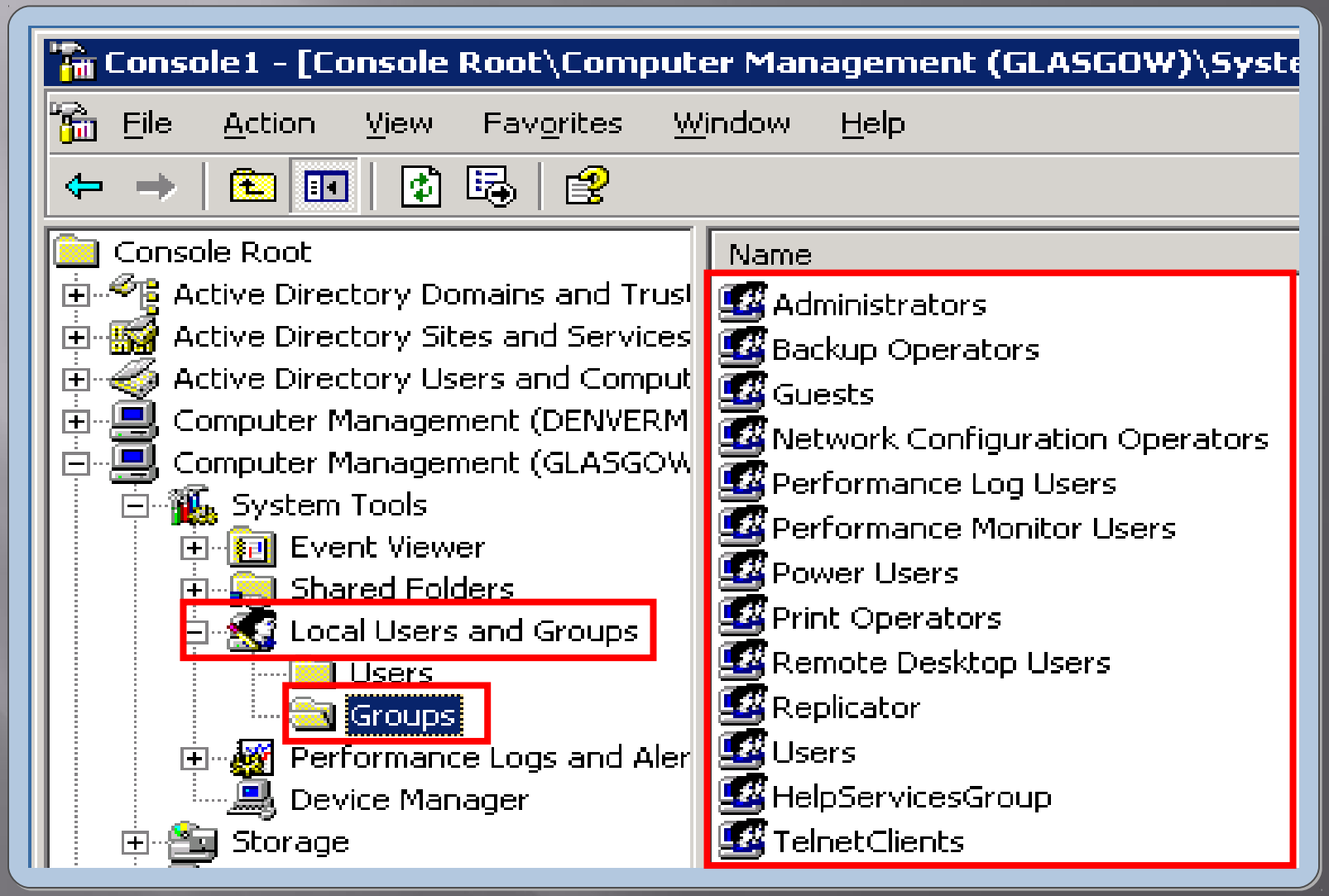
- Uporabljaj kratko ime (vzdevek, alias)
- Ne vključuj vzdevka uporabnikov kot dela prikazanega imena
- Ena porazdeljena skupina naj ima največ 5 solastnikov

# Zakaj dodelimo upravnika skupini?

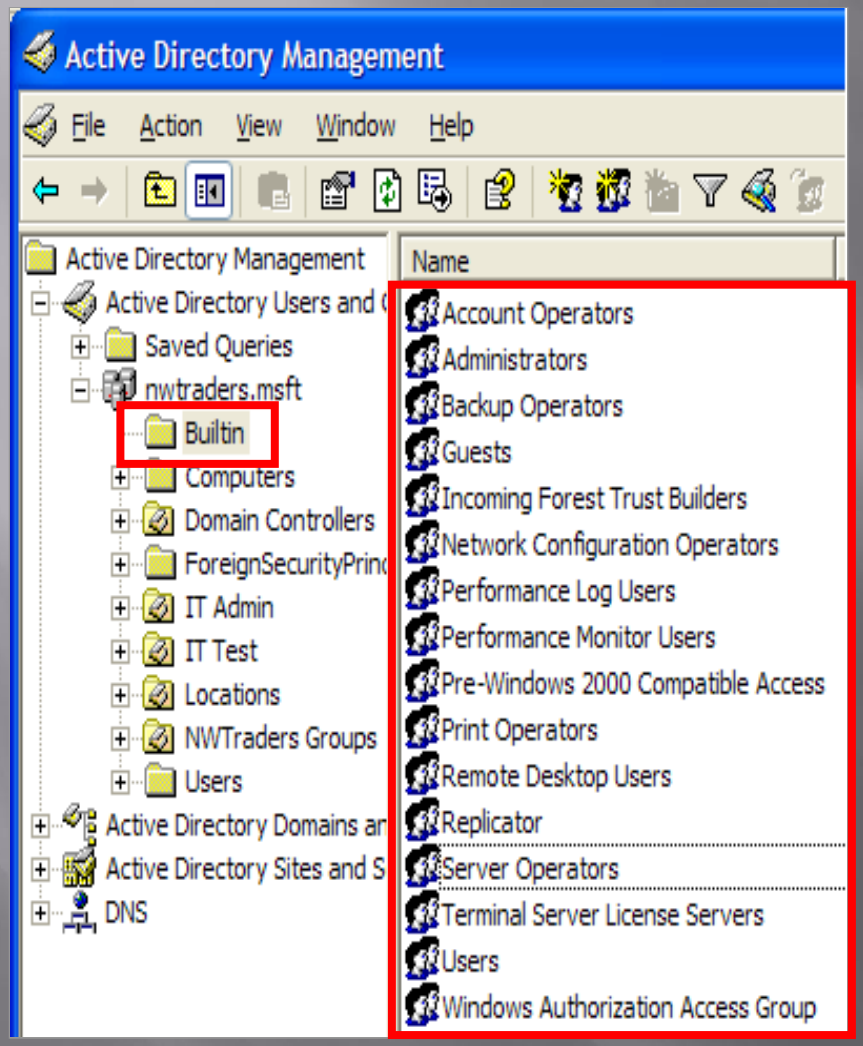


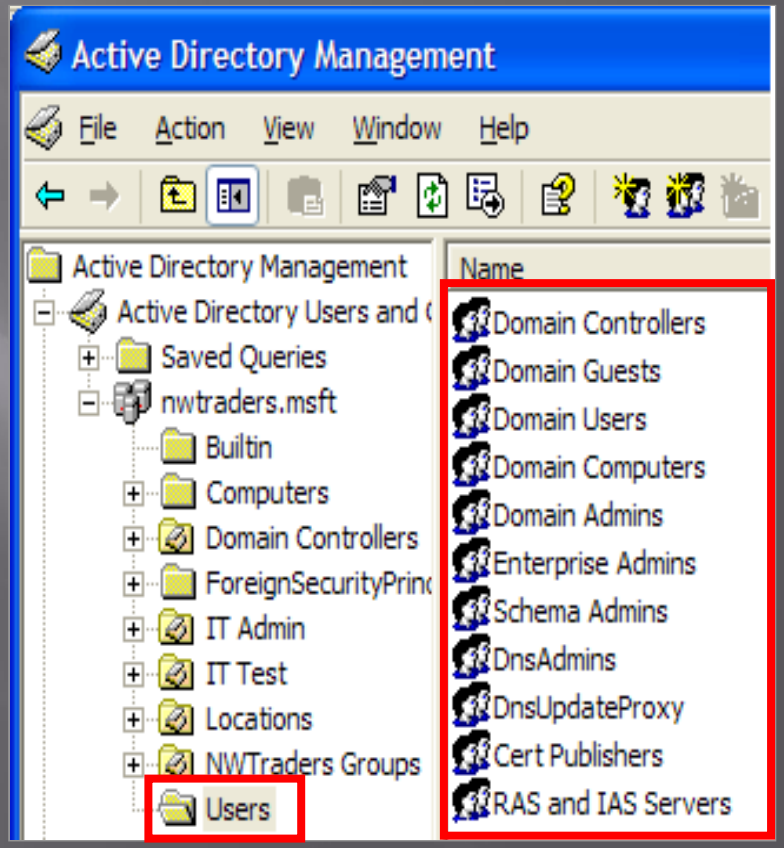

- Zato, da:
  - Vemo, kdo je odgovoren za skupine
  - Upravniku skupine delegiramo pooblastila za dodajanje uporabnikov ali brisanje uporabnikov s skupine
  - Porazdelimo administrativno odgovornost

# Privzete skupine za članske strežnike



# Privzete skupine v aktivnem imeniku



# Kdaj uporabimo privzete skupine

- Privzete skupine so:
  - tvorjene med namestitvijo operacijskega sistema ali pri dodajanju servisov, kot na primer aktivni imenik ali DHCP
  - avtomatično dodeljena množica pravic uporabnikov
- Uporabi privzete skupine za:
  - nadzor dostopa do souporabljanih sredstev
  - delegacijo določene administracije znotraj domene

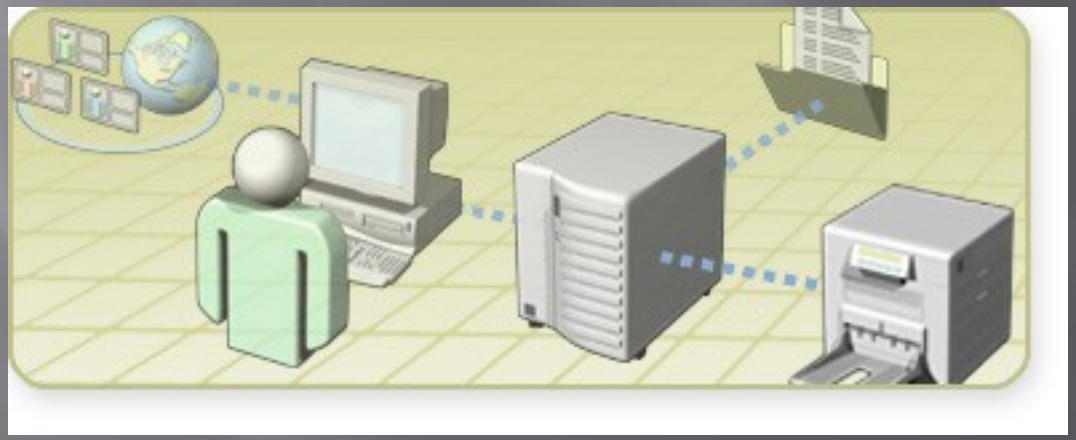
# Varnostni premisleki za privzete skupine

- Uporabnika damo v privzeto skupino le, če smo prepričani, da mu želimo dati uporabniške pravice in dovoljenja, ki so tej skupini dodeljene v aktivnem imeniku; sicer raje naredimo novo varnostno skupino
- Iz izkušenj sledi, da je najbolje, če uporabniki privzetih skupin uporabljajo “Run as”

# Dobre izkušnje za upravljanje skupin

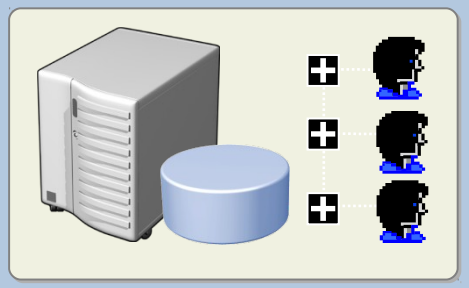
- Pri tvorbi skupin izhajamo iz administrativnih potreb
- Na računalniku, ki ni član domene, uporabljamo lokalne skupine
- Uporabniške konte dodajamo v skupino, ki je najbolj omejujoča
- Če je mogoče, namesto tvorbe novih skupin raje uporabljamo vgrajene skupine
- Za dodeljevanje večine uporabniških pravic in dovoljenj uporabljamo raje skupino “Authenticated Users” namesto skupine “Everyone”
- Omejujmo število uporabnikov v skupini “Administrators”
- Osebju, ki so člani skupin Administrators, Power Users, Print Operators in Backup Operators, moramo zaupati

# UPRAVLJANJE UPORABNIKOV IN RAČUNALNIŠKIH KONTOV

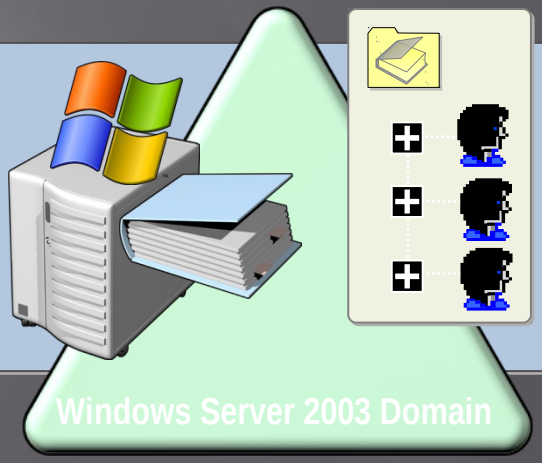


# Kaj je uporabniški konto?

- Lokalni konti uporabnikov (shranjeni v lokalnem računalniku)



- Domenski konti uporabnikov (shranjeni v aktivnem imeniku)




- Multimediji: Tipi uporabniških kontov

# Imena, združena z domenski uporabniškimi konti

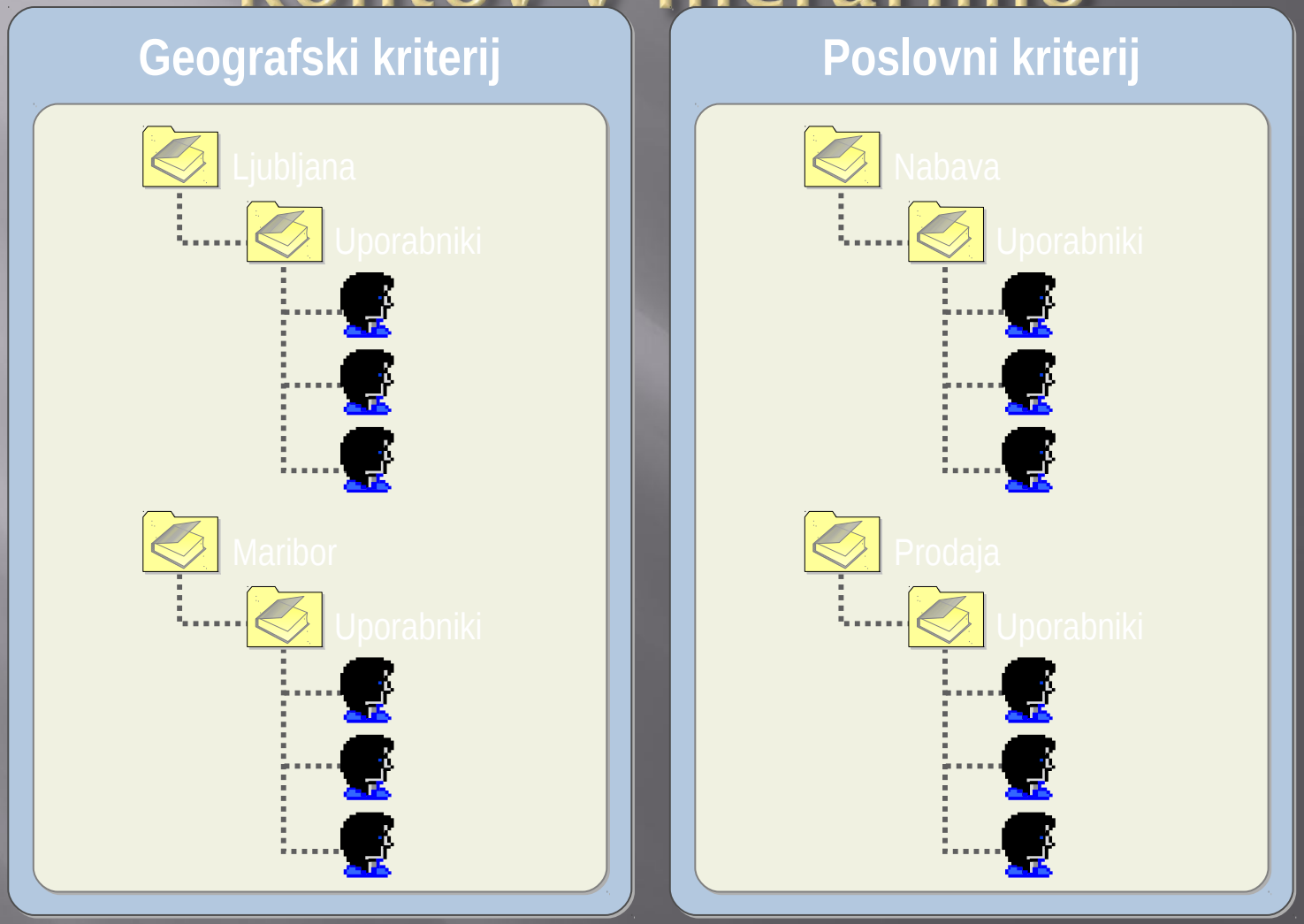
| Ime | Primer |
| --- | --- |
| User logon name | **sasadivjak** |
| Pre-Windows 2000 logon name | **XYZ\sasadivjak** |
| User principal logon name | **sasadivjak@XYZ.si** |
| LDAP relative distinguished name | **CN=sasadivjak,CN=users,dc=XYZ,dc=si** |

# Navodila za tvorbo poimenovanja uporabniških kontov

**Dogovor o poimenovanju uporabniških kontov mora rešiti:**

- **Problem imen delavcev z enakimi imeni**
- **Problem različnih tipov delavcev, kot so na primer začasni in pogodbeni delavci**

# Postavljanje uporabniških kontov v hierarhijo



# Možnosti gesel za uporabniške konte

| Možnosti kontov | Opis |
| --- | --- |
| Pri naslednjem logiranju mora uporabnik spremeniti geslo | Uporabniki morajo spremeniti svoja gesla naslednjič, ko vstopijo v omrežje |
| Uporabnik ne more spremeniti gesla | Uporabnik nima dovoljenja, da bi spreminjal svoje geslo |
| Geslo nikdar ne poteče | Uporabniškemu geslu nikdar ne poteče veljavnost. |
| Konto je blokiran | Uporabnik se z izbranim kontom ne more logirati |

# Napotki za tvorbo uporabniških kontov

## Napotki za tvorbo lokalnih uporabniških kontov

- Ne omogoči konta “Guest”
- Omeji število ljudi, ki se lahko logira lokalno

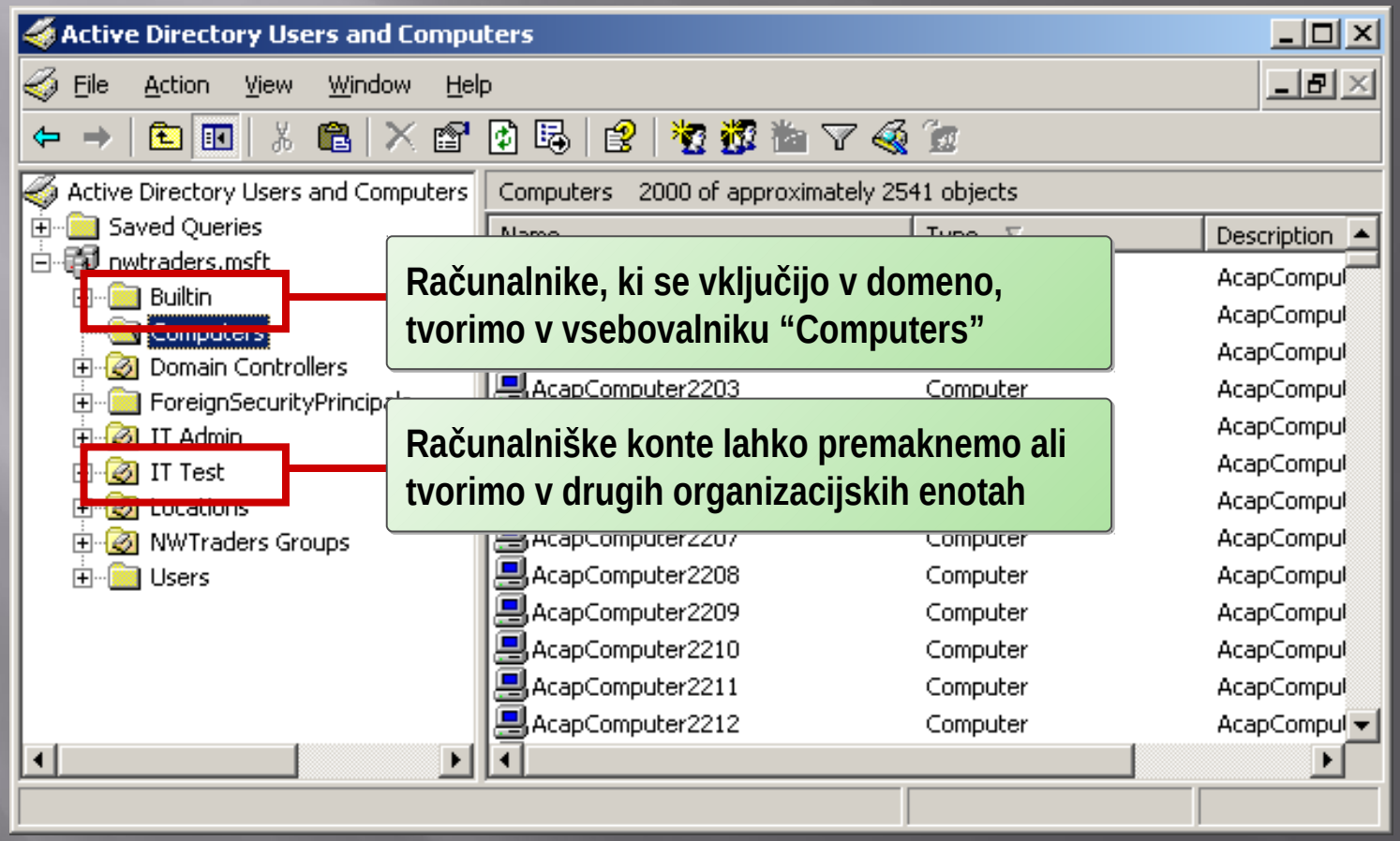
## Napotki za tvorbo domenskih uporabniških kontov

- Blokiraj konto, ki ne bo takoj uporabljan
- Zahtevaj, da uporabniki spremene svoja gesla pri prvem logiranju

# Zakaj naredimo računalniški konto?

- Varnost
  - Avtentikacija
  - IPSec (VPN Dostop)
  - Nadzor
- Upravljanje
  - Značilnosti aktivnega imenika:
    - Programsko razvijanje
    - Upravljanje z namizjem
  - “Hardware and software inventory through SMS”

# Kje v domeni tvorimo računalniške konte

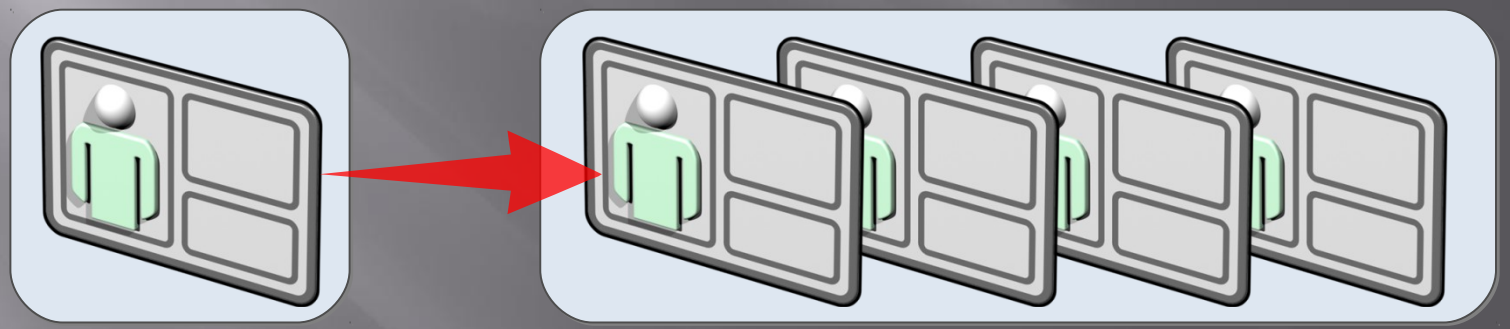


# Tvorba šablone za uporabniški konto (User Account Template)

- Kaj je “šablona za uporabniški konto  (User Account Template)?
- Katere lastnosti so v šabloni?
- Navodila za tvorbo šablon za uporabniške konte

# Kaj je šablona za uporabniški konto?

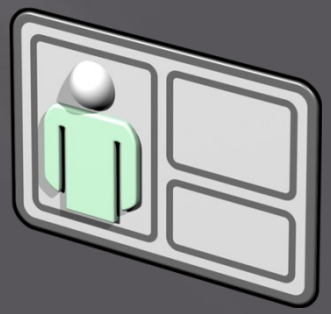
- Šablona za uporabniški konto je uporabniški konto, ki vsebuje lastnosti, ki naj bi jih imeli uporabniki s skupnimi zahtevami
- Šablone za uporabniški konto večajo učinkovitost tvorbe uporabniških kontov s standardiziranimi konfiguracijami



Šablona za uporabniški konto

# Katere lastnosti so v šabloni?

| Tab | Kopirane lastnosti |
|---|---|
| Address | **Vse lastnosti razen** naslova ulice |
| Account | **Vse lastnosti razen** vstopnega imena uporabnika |
| Profile | **Vse lastnosti razen** poti profila in domačega direktorija**, odražajo vstopno ime novega uporabnika** |
| Organization | **Vse lastnosti razen** naziva |
| Member Of | **Vse lastnosti** |

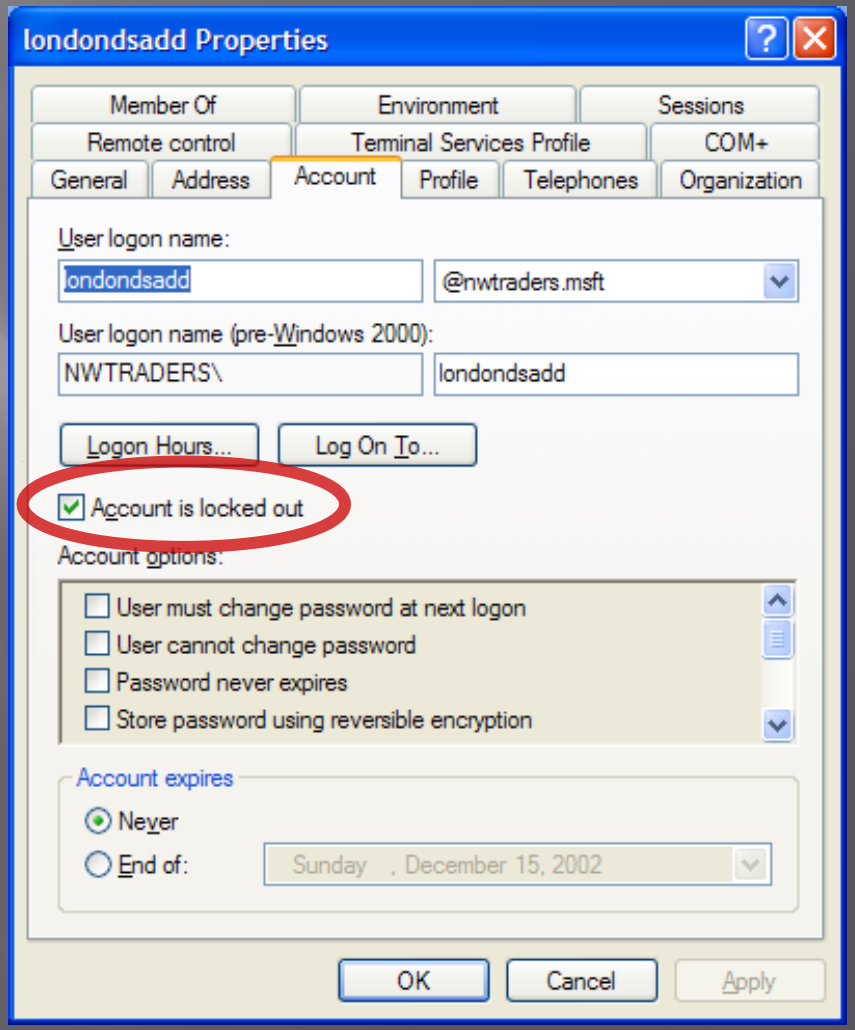


# Napotki za tvorbo šablon za uporabniške konte

- Za vsak oddelek naredimo ločeno klasifikacijo
- Za začasne zaposlence tvorimo posebno skupino
- Za začasno zaposlene in zaposlene za določen čas nastavimo datum prenehanja konta
- Blokiramo (disable) šablono za konte
- Identificiramo šablono za konte

# Kaj so zaklenjeni računalniški konti?

- Prag zaklepanja konta:
  - Določa število ponesrečenih poskusov vstopa
  - Hekerjem preprečuje ugibanje uporabniških gesel
- Konto lahko preseže prag s prevelikim številom ponesrečenih poskusov vstopa:
  - Pri vstopnem postopku
  - Pri ohranjevalniku zaslona, zaščitenem z geslom
  - Ko dostopamo do omrežnih sredstev

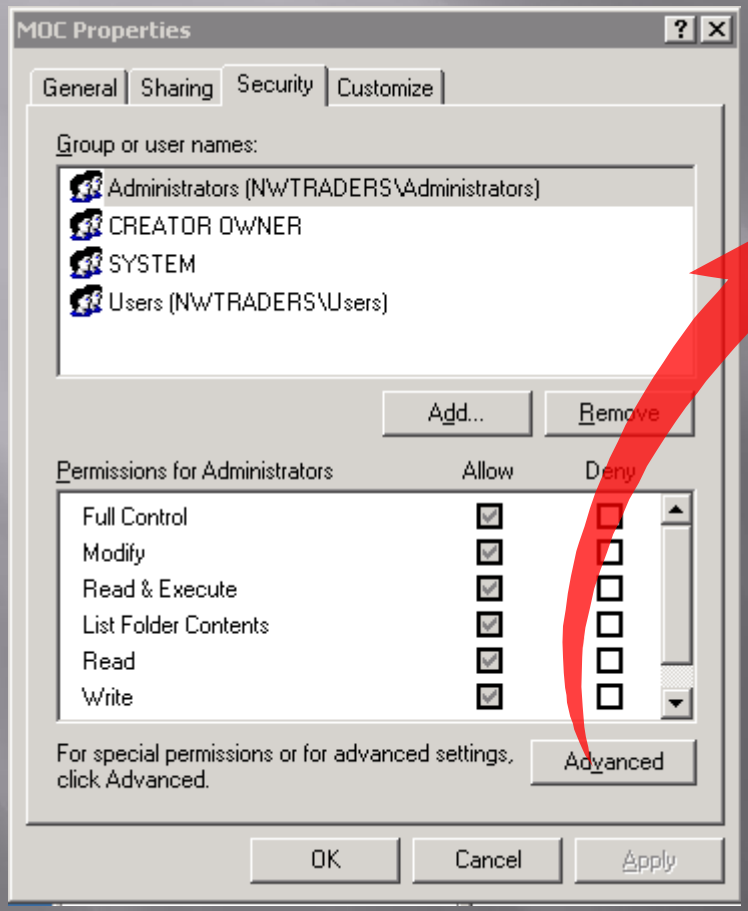


# Kaj so dovoljenja (permissions)?

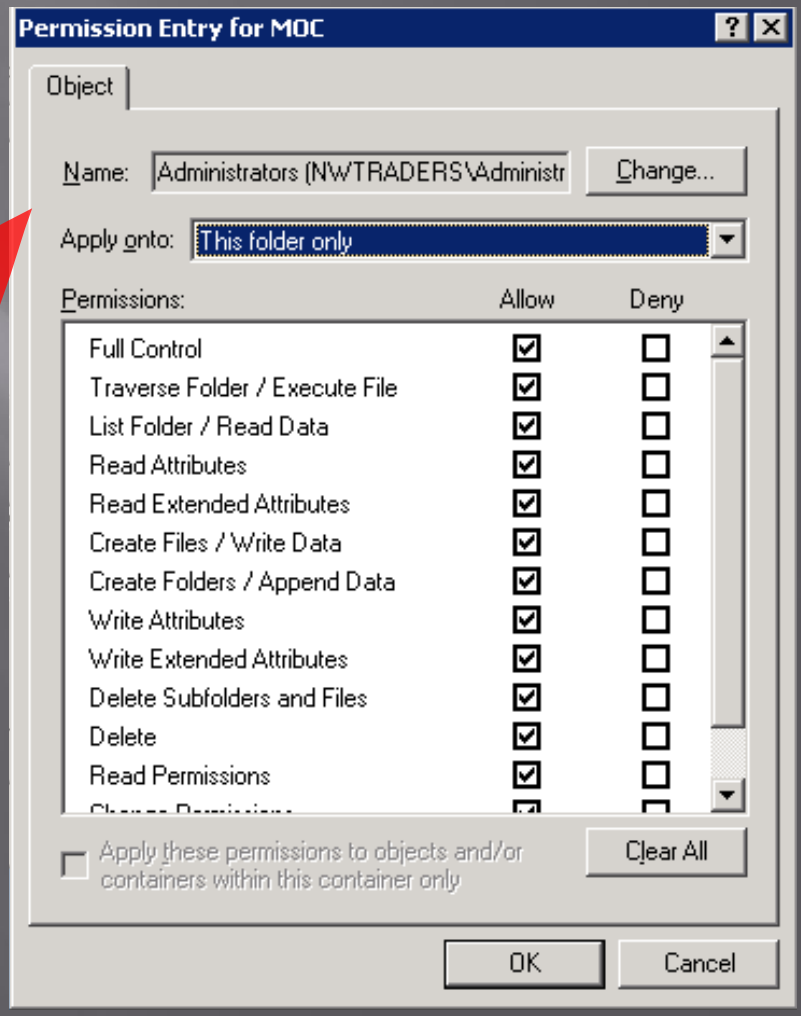
- Dovoljenja določajo tip dostopa, zagotovljen uporabniku, skupini, računalniku ali objektu
- Dovoljenja uvedemo za objekte, kot so datoteke, direktoriji, souporabljani direktoriji (shared folders) in tiskalniki
- Dovoljenja dodelimo uporabnikom in skupinam v aktivnem imeniku ali na lokalnem raču

# Kaj so standardna in posebna dovoljenja?

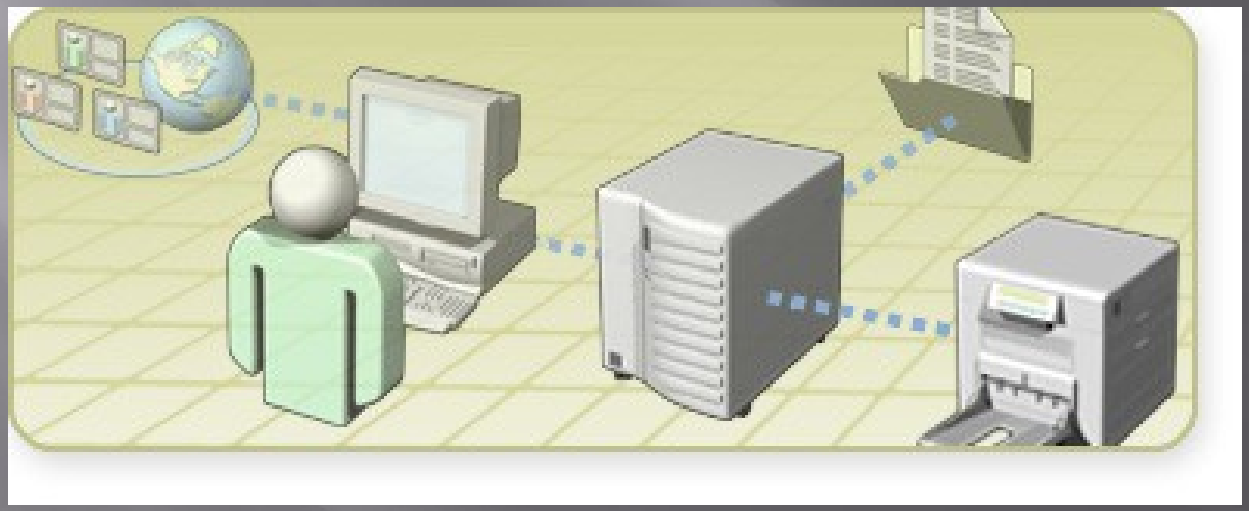
## Standardna dovoljenja




## Posebna dovoljenja



# UPRAVLJANJE TISKANJA NA WINDOWS 2008?

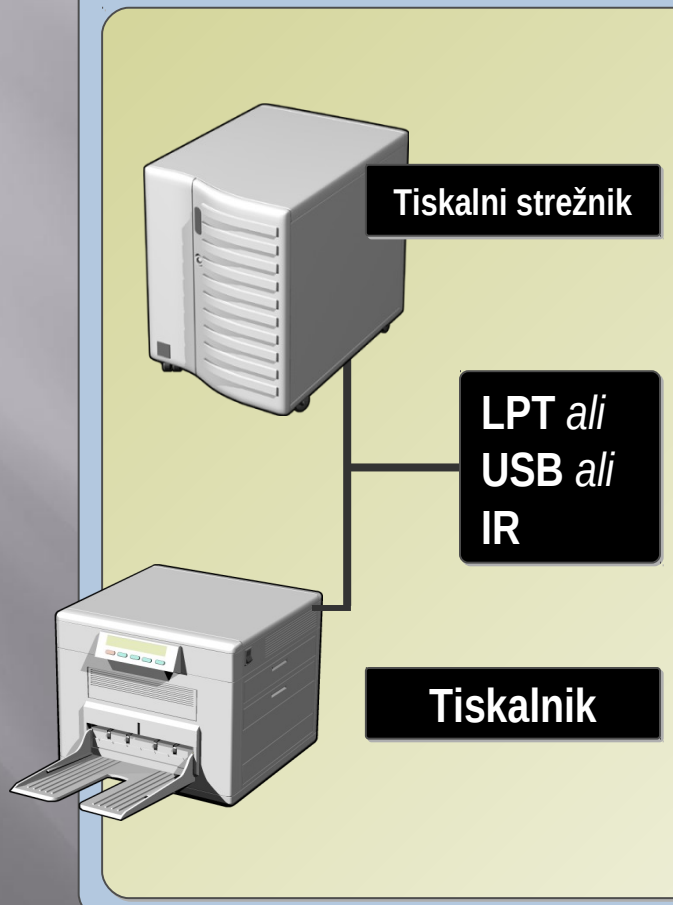


# Osnovni pojmi

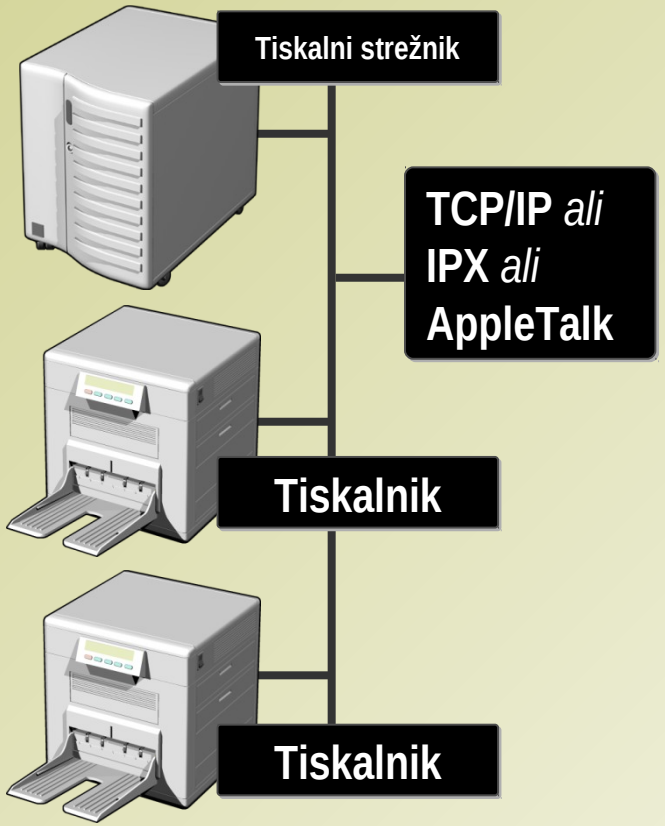
- Lokalni tiskalnik
  - Lokalno povezan na računalnik
- Omrežni tiskalnik (network print device)
  - Omrežni tiskalnik za souporabo (shared network printer)
  - Tiskanje preko interneta
- Tiskalni odjemalec (print client)
  - Računalnik ali aplikacija, ki sproži tiskanje (print job)
- Tiskalni strežnik (print server)
  - Računalnik oziroma strežna naprava, ki nudi souporabo tiskalnika

# Kaj je lokalni tiskalnik in kaj omrežni tiskalnik?

## Lokalni tiskalniki:



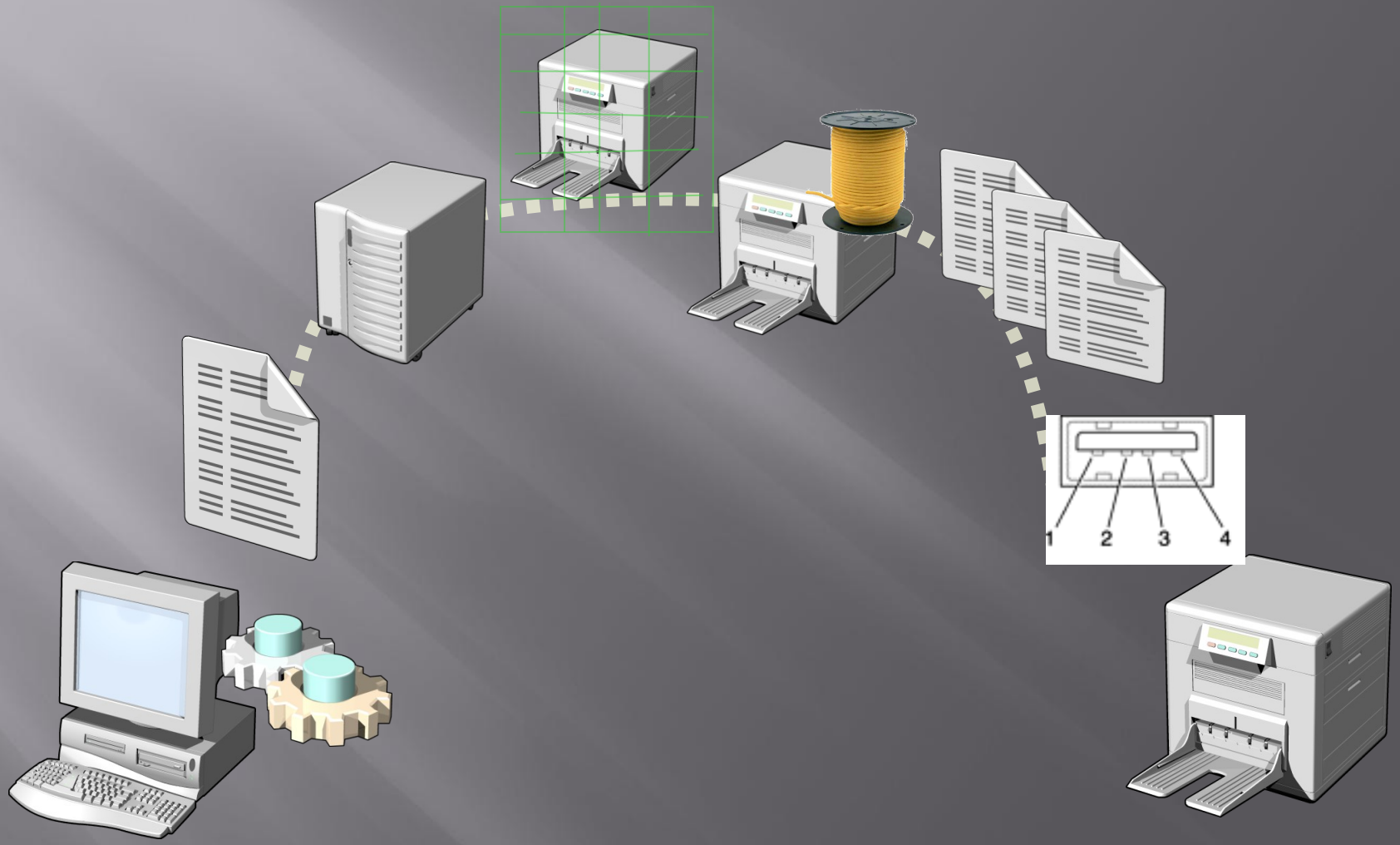

## Omrežni tiskalniki:



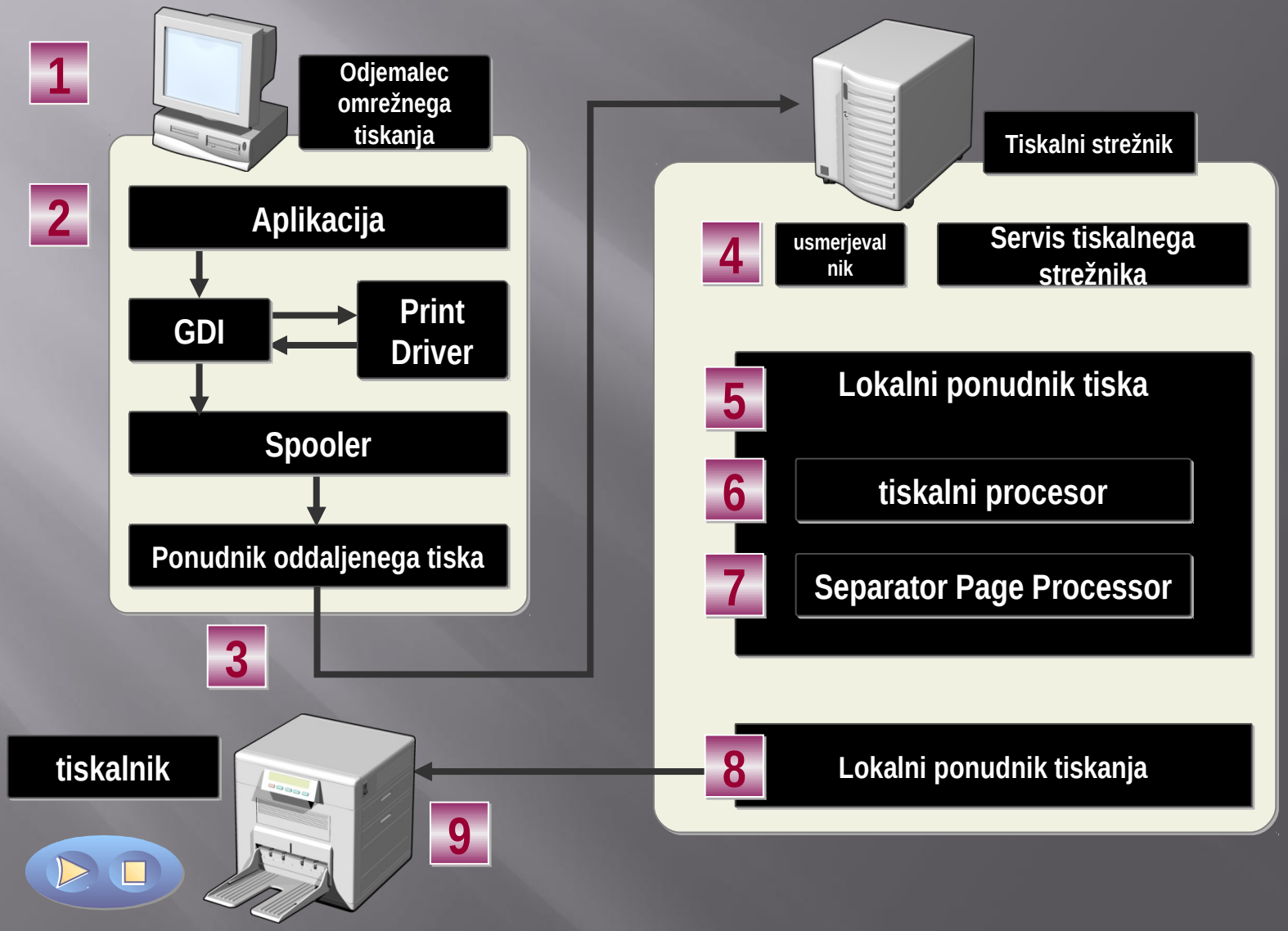
# Osnovni pojmi (nadaljevanje)

- Tiskanje v ozadju (spooling )
  - Datoteke za tiskanje pomni na posebnem delu diska, dokler niso izpisane
  - Razbremeni računalnik za obravnavo drugih zahtevkov
  - Vsebuje DLL, podatkovne datoteke in programe, ki jih uporablja tiskanje
- Gonilnik tiskalnika (printer driver)
  - Vsebuje konfiguracijske podatke in nudi navodila za oblikovanje
  - Je lociran na strežniku, lahko pa je tudi na odjemalcu

# Kako poteka tiskanje



# Kako poteka tiskanje v okolju Windows Server 2008



# Kako poteka tiskanje

- Programska aplikacija tvori datoteko za tiskanje (print file)
- Aplikacija komunicira z GDI (Graphics Device Interface)
- Tiskalno datoteko oblikuje s krmilnimi znaki (control codes)
  - Istočasno je taka datoteka zapisana v “spooler” odjemalca kot “spool file”
- “Remote print provider” s klicem oddaljene procedure (RPC) pokliče ciljni omrežni tiskalni strežnik
  - Ko je strežnik pripravljen, je datoteka posredovana tiskalnemu servisu na ciljnem strežniku

# Kako poteka tiskanje (nadaljevanje)

- Omrežni tiskalni strežnik uporablja 4 storitve za prevzem in obdelavo datoteke za tiskanje:
  - Usmerjevalnik (router)
  - Ponudnik tiska (print provider)
  - Izvajalec tiska (print processor)
  - Print monitor
- Ko oddaljeni ponudnik tiskanja pokliče strežnik, ta pokliče svoj usmerjevalnik v sklopu servisa “Print Spooler”
  - Usmerjevalnik usmeri tiskalno datoteko ponudniku tiskanja,ta pa jo shrani kot “spool file”

# Kako poteka tiskanje (nadaljevanje)

- Med pripravo datoteke “spool file” ponudnik tiskanja sodeluje z izvajalcem tiskanja (print processor) pri oblikovanju datoteke s pravilnimi tipi podatkov

- Ko je “spool file” izoblikovana, jo “print monitor” pošlje na tiskalnik

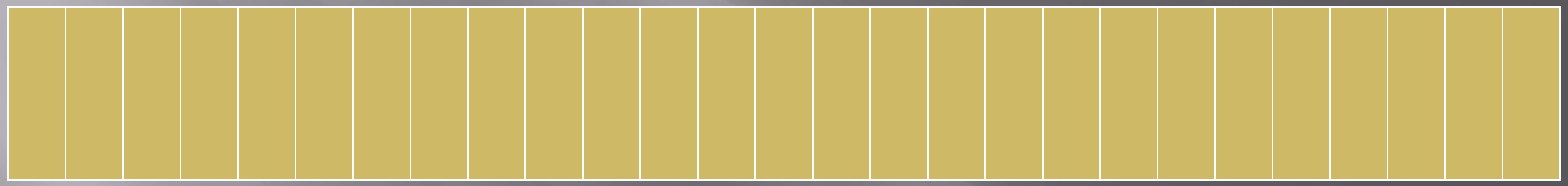
# Kaj je tiskalnik v ozadju (Print Spooler)?

- Izvršljiva datoteka, ki upravlja proces tiskanja, kar vsebuje:
  - Poišče lokacijo pravega gonilnika za tiskalnik
  - Naloži gonilnik
  - Kliče v visokonivojske funkcije tiskanja v ozadju
  - Planira naloge za tiskanje
- Prejme datoteke za tiskanje, jih shrani na trdi disk, nato jih pošlje tiskalniku, ko je ta pripravljen

# KONFIGURIRANJE IN UPRAVLJANJE PODATKOVNIH MEDIJEV?

# Pogled na trdi disk

**Veliko polje sektorjev po 512-bytov**

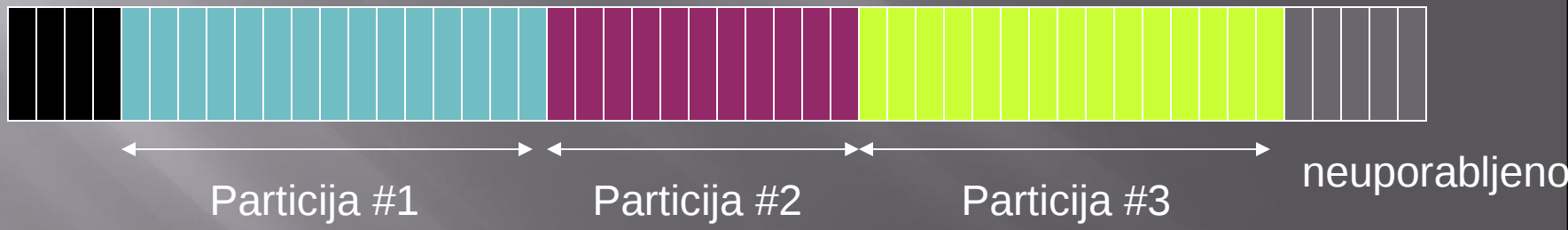


0 1 2 3 .....

**Kapaciteta diska (v bytih) = (število sektorjev) x (512 bytov/sektor)**

# Particije diska

- Celotno pomnilno področje diska je običajno razdeljeno regije, ki jim pravimo “particije diska”



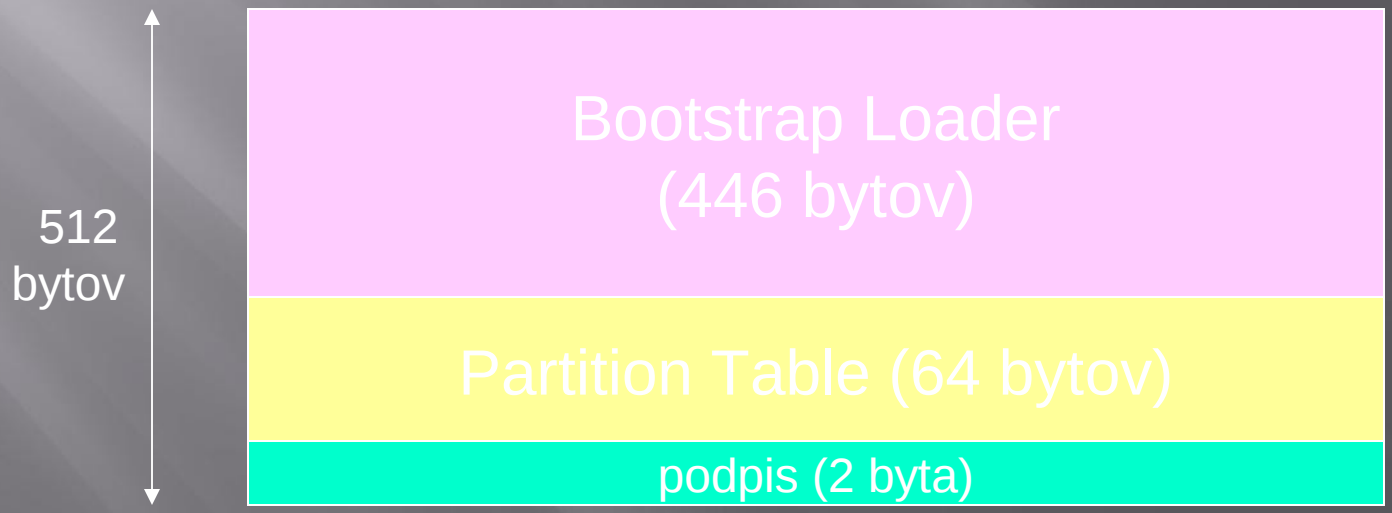
# Master Boot Record

- Majhno področje na začetku diska, namenjeno ‘upravljanju’ particij diska


- Sektor številka 0 je znan kot “Master Boot Record” (zelo pomembno!)

# Format MBR

- MBR je razdeljen na tri področja:
  - bootstrap loader program
  - Tabela particij
  - MBR podpis (i.e., 0x55, 0xAA)



# Pomnilne možnosti Windows Server 2008

- Osnovni (basic) disk
  - Uporablja tradicionalne particije diska
  - Vsebuje primarno particijo, razširjeno (extended) particijo in logične pogone
- Dinamični disk
  - Ne uporablja tradicionalnih particij
  - Nudi fleksibilnost v številu zvezkov (volumes) na disk

# Osnovni diski

- Particije
  - Rezervirajo skupino sledi in sektorjev na disku z namenom, da jih lahko uporabi določen datotečni sistem
- Formatiranje
  - Tvorba tabele s podatki o datotekah in direktorijih za dani datotečni sistem
- RAID
  - Skupina standardov za podaljševanje življenja diskov in preprečevanje izgube podatkov
  - Osnovni diski lahko uporabljajo RAID nivoje 0, 1 in 5

# Osnovni diski (nadaljevanje)

- Proge diskov (disk Striping)
  - Zmožnost razprostiranja podatkov preko več diskov ali zvezkov (volumes)
  - Zmanjšuje obrabo diskov
- Zrcaljenje diskov (disk mirroring)
  - Tvorba slike vseh podatkov z originalnega diska na rezervnem disku (backup disk)
  - Rezervni disk oživi le, če izpade originalni disk
- Diski, ki jih dodajamo na računalnik z “Windows Server 2008”, so avtomatsko konfigurirani kot osnovni (basic) diski
- Particije na osnovnih diskih so lahko primarne ali razširjene (extended)

# Primarne particije

- Osnovni diski morajo imeti najmanj eno primarno particijo, lahko pa imajo do 4 particije
  - Primarna particija je tista, s katere lahko zaženemo operacijski sistem
  - Lahko jo uporabimo tudi v druge namene, na primer za pomnenje datotek v drugačnem datotečnem formatu
- Natančno ena primarna particija mora biti označena kot aktivna
  - Aktivna particija je tista, na kateri išče računalnik aparaturno specifične datoteke za zagon operacijskega sistema
  - Tej particiji pravimo tudi "sistemska particija"

# Sistemske in zagonske particije in zvezki

- Sistemski zvezek oziroma particija vsebuje aparaturno odvisne datoteke (Ntldr, Boot.ini, Ntdetect.com), potrebne za nalaganje Windows.

- Zagonski (boot) zvezek oziroma particija vsebuje sistemske datoteke operacijskega sistema Windows, ki so locirane v direktorijih %Systemroot% in %Systemroot%\System32.

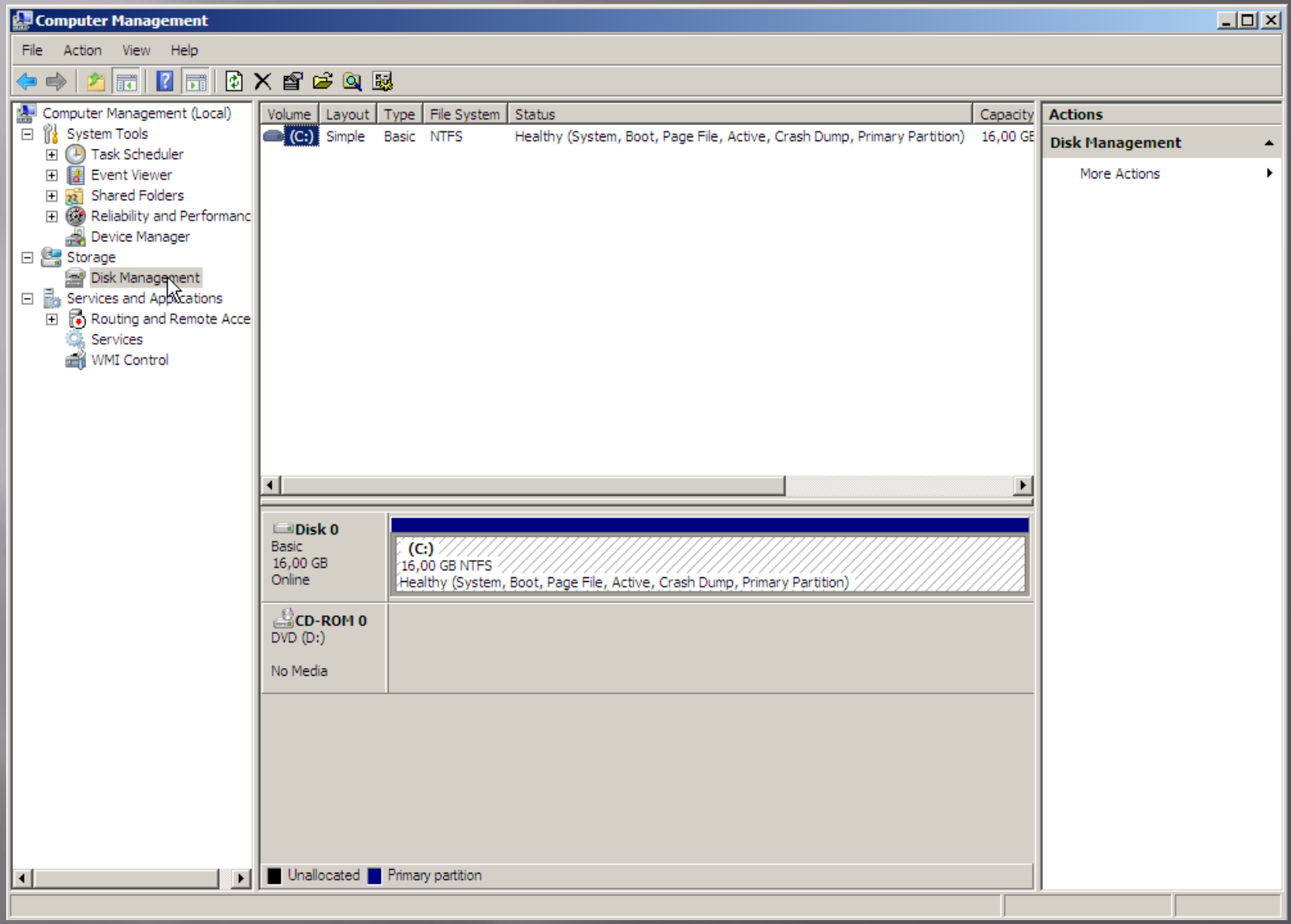
# Razširjene (extended) particije

- Naredimo jih s prostorom, ki še ni bil dodeljen participam
- Omogočajo, da osnovni disk prekorači omejitev na 4 particije
- Po tvorbi lahko tako particijo delimo dalje v logične pogone (logical drives)
  - Logične pogone nato formatiramo in jim dodelimo črkovne oznake
- Zagonsko particijo (boot partition) lahko namestimo na primarno ali na razširjeno particijo
  - Zagonska particija vsebuje datoteke operacijskega sistema in to v direktoriju \Windows

# Tvorba particij

- Ko tvorimo particijo, pustimo najmanj 1 MB prostora za pretvorbe iz osnovnega diska v dinamičnega
- Organiziraj pomnilne enote s particijami
  - Tako na primer imej operacijski sistem v ločeni particiji, podatke pa v drugi. Tako podatke zaščitiš
- Particijo lahko formatiramo med njeno tvorbo ali kasneje
  - Zvezek na dinamičnem disku, formatiran z orodjem “Disk Management” lahko formatiramo le za NTFS

# Preverjanje aktivne particije



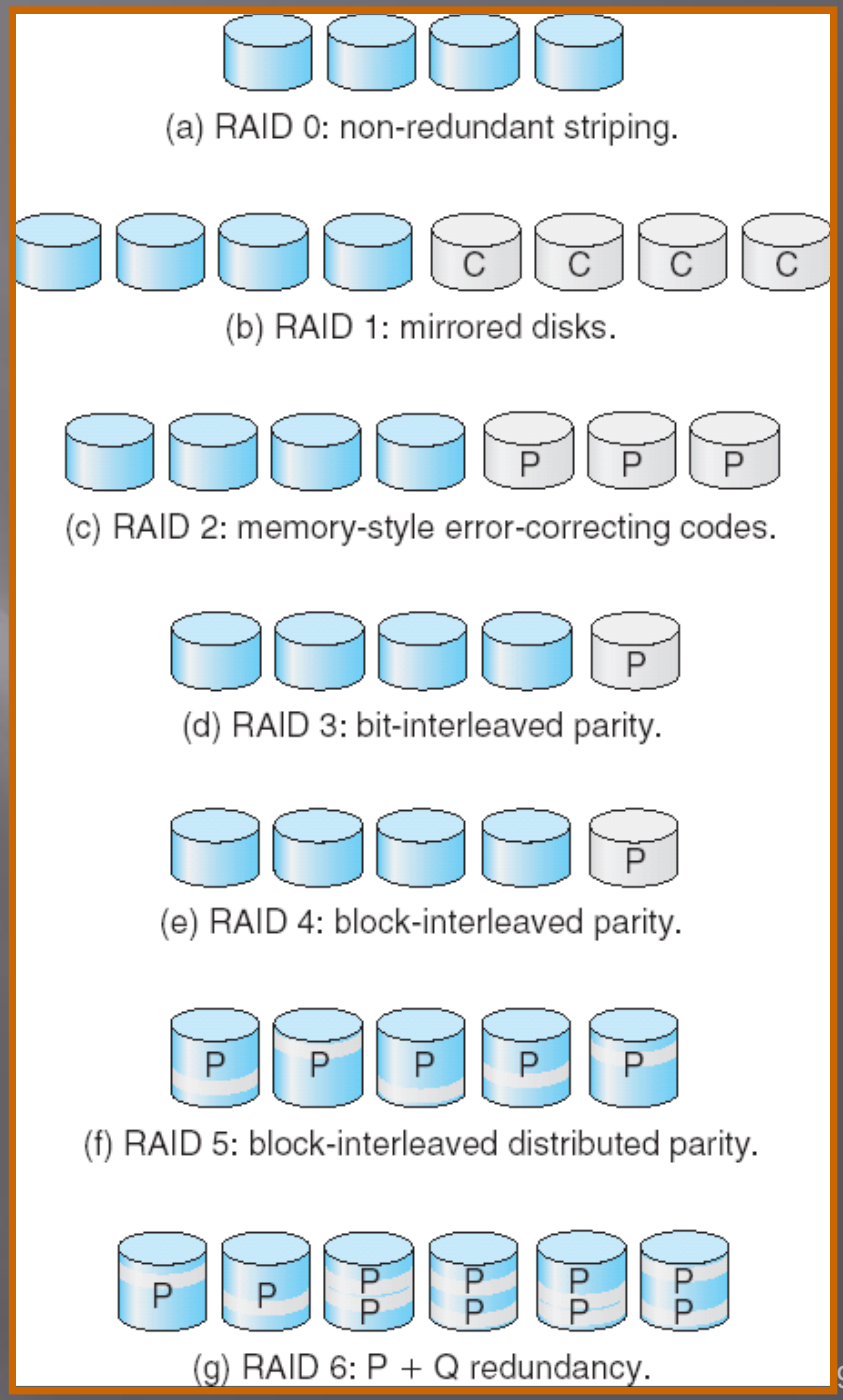
# Strpnost do napak (Fault Tolerance)

- Zmožnost, da se sistem mehko reši v primeru programskih ali aparaturnih napak oziroma izpadov
- Windows Server 2008 nudi toleranco do napak preko programskega RAID
- RAID ni nadomestilo za regularno tvorbo rezervnih kopij
- Podatke zapiše na več kot le en pogon
  - Ob izpadu enega pogona lahko dostopimo do podatkov na enem od preostalih pogonov

# RAID Strukture

- **RAID** – Več diskov povečuje zanesljivost s pomočjo redundance.
- RAID je organiziran v 6 različnih nivojih.
- "Disk striping" uporablja skupino diskov kot eno pomnilno enoto.
- RAID sheme za  večanje performance in zanesljivosti pomnilnega sistemas shranjevanjem redundančnih podatkov.
  - *Mirroring* or *shadowing* keeps duplicate of each disk.
  - *Block interleaved parity* uses much less redundancy.

# RAID nivoji


(a) RAID 0: non-redundant striping.
C
(b) RAID 1: mirrored disks.
P
(c) RAID 2: memory-style error-correcting codes.
(d) RAID 3: bit-interleaved parity.
(e) RAID 4: block-interleaved parity.
(f) RAID 5: block-interleaved distributed parity.
(g) RAID 6: P + Q redundancy.

# Zvezki RAID

- RAID nivo 0
  - Proge brez druge redundance
- RAID nivo 1
  - Zrcaljenje diska (disk mirroring) s podvajanjem podatkov na rezervnem disku na istem krmilniku oziroma adapterju
  - Dupleks diska (disk duplexing) s  podvajanjem diska na rezervnem disku na drugem krmilniku oziroma adapterju
  - Dostop za pisanje je počasnejši od dostopa za branje
  - Če uporabimo več kot tri zvezke, je ta nivo dražji od drugih RAID nivojev

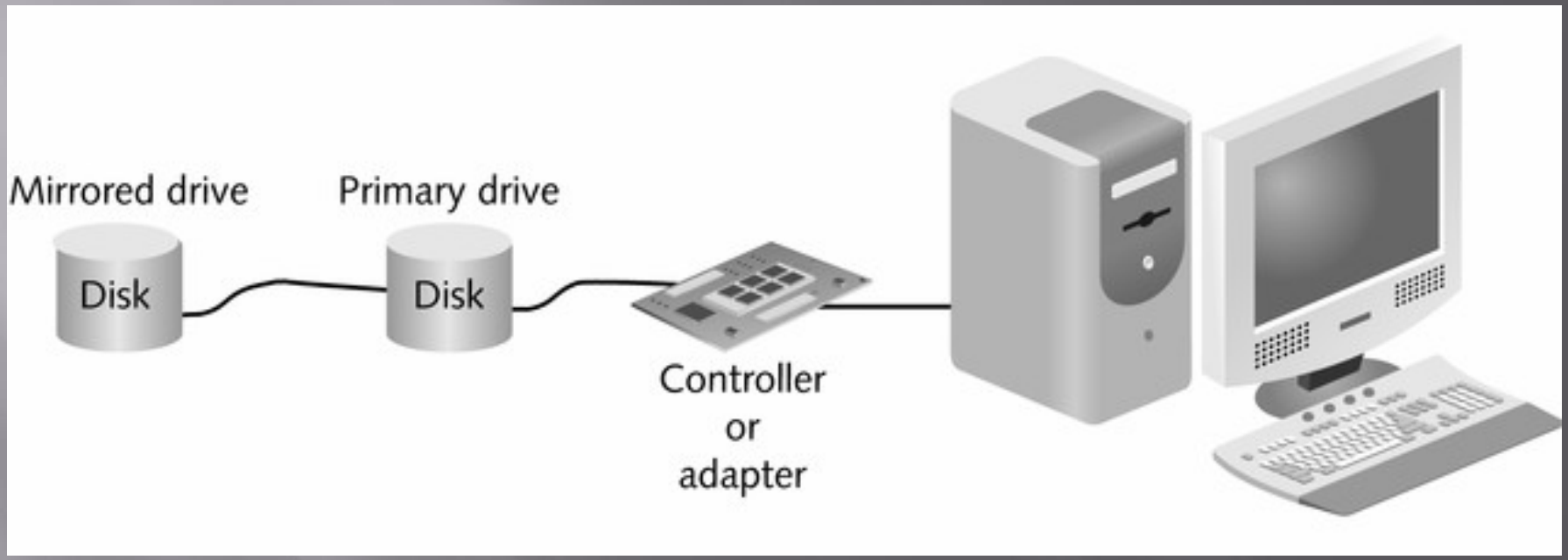
# Uporaba zvezka s progami (RAID nivo 0)

- Pri diskovnih pogonih zaradi enakomernega obremenjevanja
- Poveča performanso diska  v primerjavi z drugimi metodami konfiguriranja dinamičnih diskovnih zvezkov
- Uporabimo ga v primerih, ko imamo podatke pomnjene drugje in potrebujemo hiter dostop do sekundarnega pomnilnika

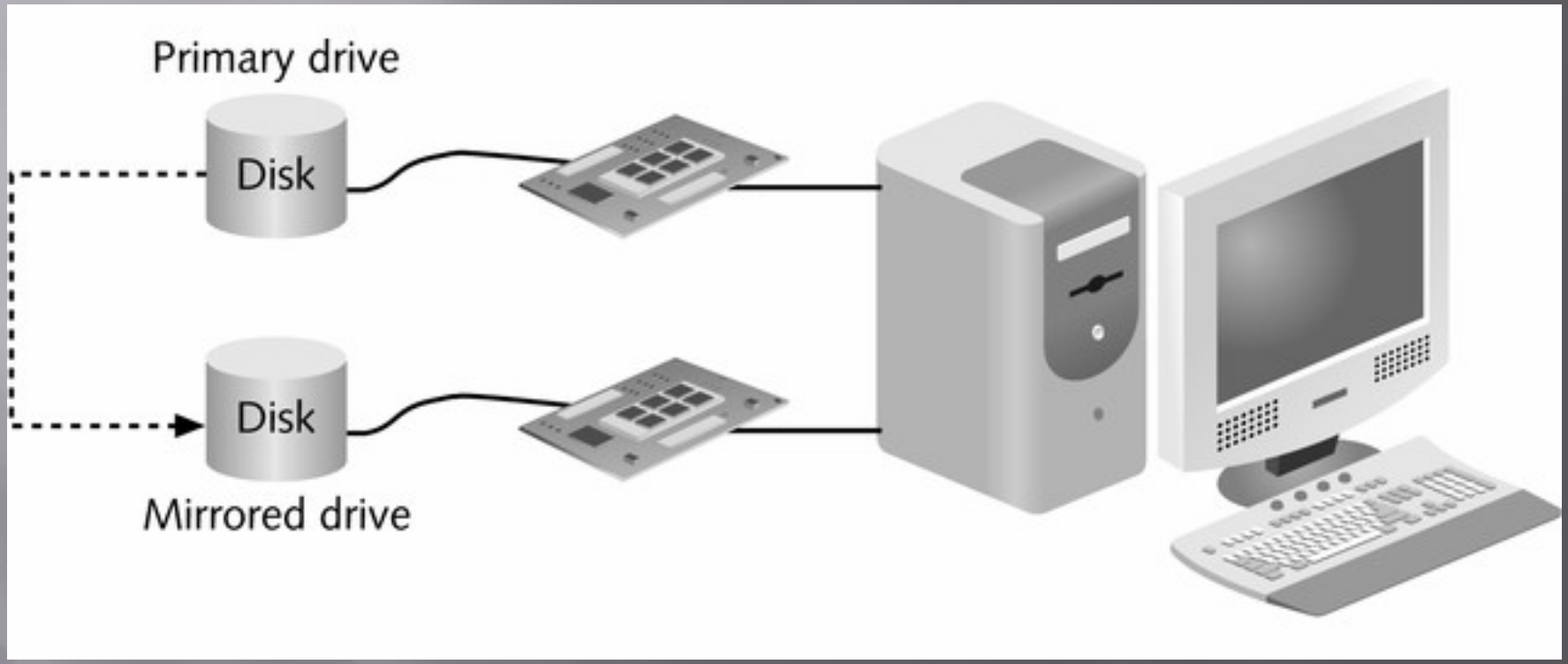
# Uporaba zrcalnega zvezka (RAID nivo 1)

- Kot zrcalne zvezke vzpostavimo le dinamične diske
- Ena od najbolj zanesljivih oblik tolerance do napak
- Čas za tvorbo in osveževanje podatkov je zaradi zrcalnega diska podvojen
- Hitrost branja diska je enaka kot pri enem disku
- Sistemske in zagonske datoteke imamo lahko na zrcalnem zvezku

# Zrcaljenje diska

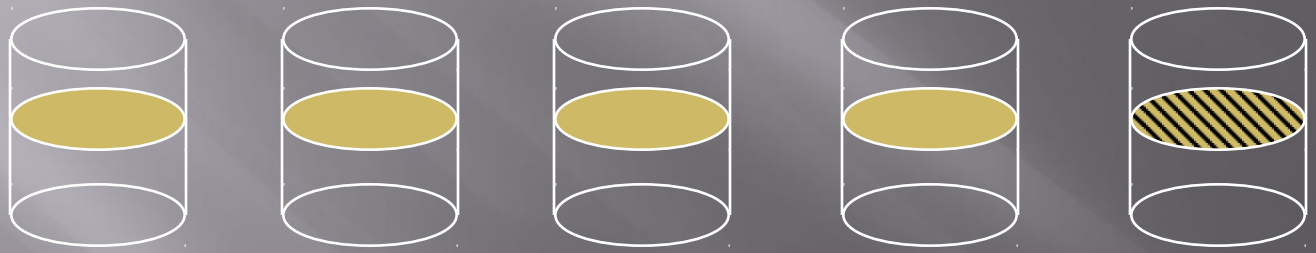


# Dupliciranje diska



# RAID

- Redundant Array of Inexpensive Disks



Striped Data

Parity Disk

(RAID nivoji 2 in 3)

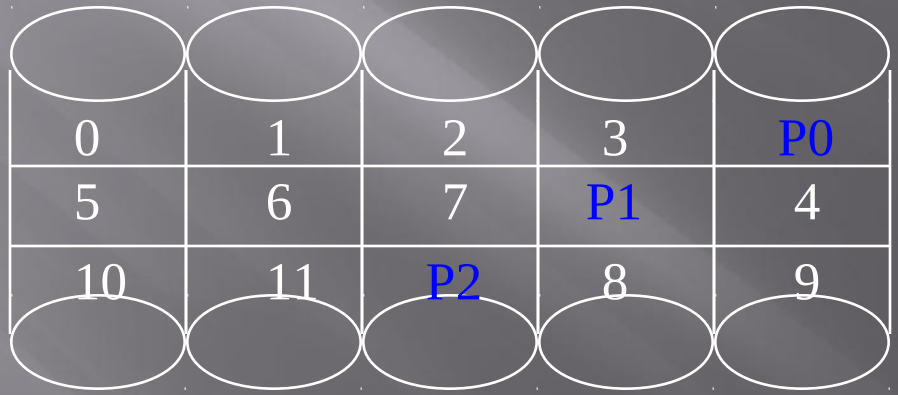
# RAID zvezki (nadaljevanje)

- RAID nivo 2
  - Polje diskov s progami in podatki za popravljanje napak (error-correction)
- RAID nivo 3
  - Kot nivo 2, toda podatki za popravljanje napak (error correction data) so napisani le na en disk
- RAID nivo 4
  - Kot nivo 2, z verificiranjem kontrolne vsote (checksum)
    - Kontrolna vsota (checksum) je vsota bitov v datoteki, kar omogoča verifikacijo, če datoteka ni bila spremenjena (corrupt)
- Server 2003 ne podpira RAID nivojev 2 do 4

# RAID zvezki (nadaljevanje)

- RAID nivo 5
  - Nudi proge (striping), popravljanje napak (error correction) in preverjanje kontrolne vsote (checksum) po vseh diskih
  - Uporablja več RAM kot drugi nivoji RAID
  - Zahteva polje najmanj 3 diskov
  - Ista garancija podatkov kot pri zrcaljenju, vendar počasnejše
  - Če izpade več kot en disk, so podatki zgubljeni

# RAID nivo 5




Številke blokov

Porazdelitev tako podatkov kot informacije o parnosti preko vseh diskov

# Primerjava RAID 0, 1 in5

- RAID 0 ne nudi tolerance do napak in ga v nekaterih primerih zato ne priporočamo
- Zagonske in sistemske datoteke lahko namestimo na RAID nivo 1, ne pa na RAID nivo 5
- RAID nivo 1 uporablja dva trda diska,  RAID nivo 5 uporablja tri do 32 diskov
- Implementacija RAID 1 je glede na pomnilno kapaciteto dražja od RAID 5
- RAID nivo 5 zahteva več spomina glede na RAID nivo 1

# Primerjava programskega RAID in aparaturnega RAID

- Aparaturni RAID je neodvisen od operacijskega sistema
- Aparaturni RAID je dražji od programskega, zato pa nudi naslednje prednosti:
  - Hitrejše branje in pisanje
  - Zmožnost dajanja zagonskih in sistemskih datotek na različne nivoje RAID
  - Zmožnost "vroče zamenjave" ("hot-swap") pokvarjenega diska brez izklapljanja strežnika
  - Več možnosti za reševanje okvarjenih podatkov in kombiniranje različnih nivojev RAID

# Množice zvezkov in prog (Volume and Stripe Sets)

- Volume set
  - Dve ali več particij združimo tako, da izgledajo kot en zvezek z enotno črkovno oznako
- Stripe set
  - Dva ali več kombiniranih diskov
  - Proge za Raid nivo 0 ali 5
- Kompatibilni z množicami, tvorjeni pod operacijskim sistemom NT
  - Če disk izpade, ne moremo tvoriti novih množic

# Dinamični diski

- Zmožnost vzpostavitve velikega števila zvezkov na enem disku
- Zmožnost širitve zvezkov na dodatne fizične diske
- Podpirajo nivoje RAID 0, 1 in 5
- Lahko jih formatiramo za datotečne sisteme FAT16, FAT32 in NTFS
- Po izpadu toka ali izklopu jih lahko reaktiviramo
- Nudijo boljše upravljanje diskov kot osnovni diski

# Konfiguracije dinamičnih diskov

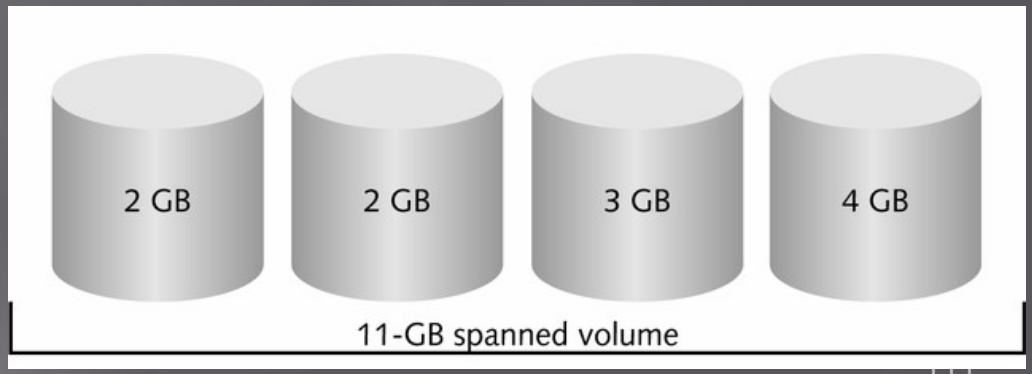
- Dinamične diske razpoznavata operacijska sistema Windows 2000 in Windows Server 2003
- Terminologija dinamičnih diskov uporablja zvezke (volumes) namesto particij oziroma množic (sets)
- Pet tipov zvezkov:
  - Preprosti zvezki (Simple volumes)
  - Speti zvezki (Spanned volumes)
  - Zvezek s progo (Striped volumes)
  - Zrcaljeni zvezki (Mirrored volumes)
  - Zvezki Raid-5

# Preprost zvezek (Simple Volume)

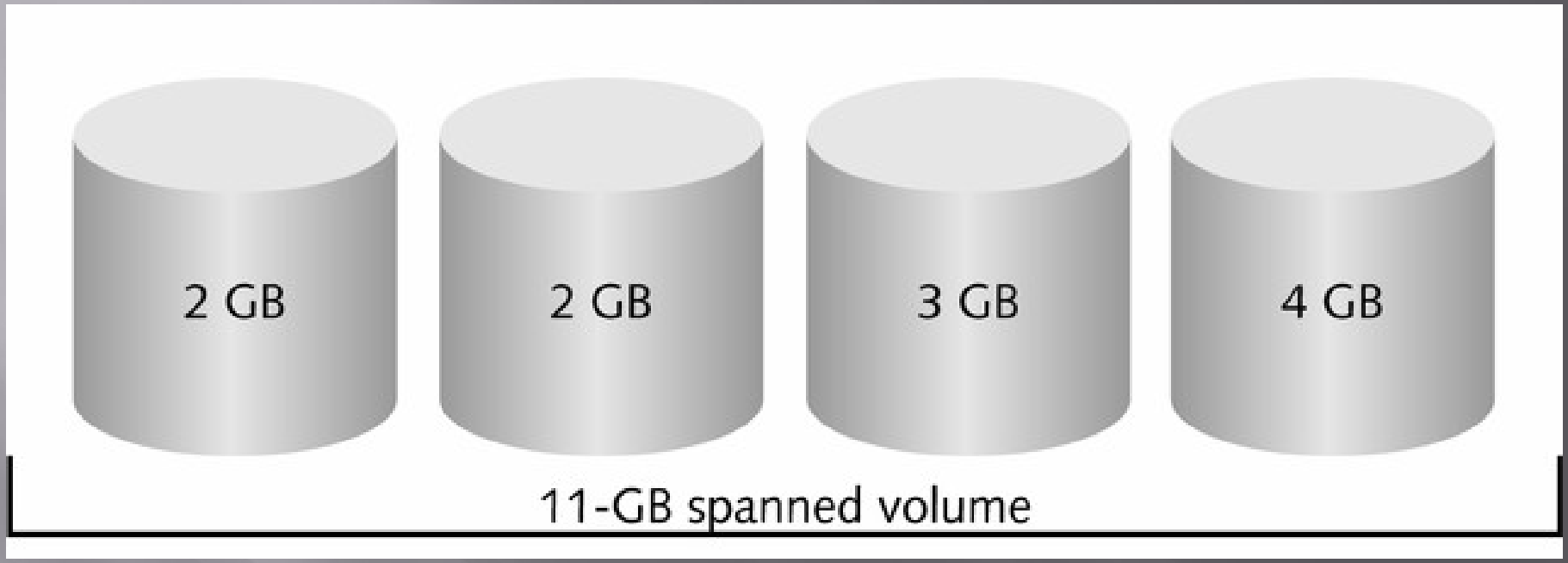
- Cel disk ali del diska, ki je vzpostavljen kot dinamični disk
- Možnost razširitve zvezka z nerazporejenim prostorom
- Lahko razširimo z do 32 sekcijami na istem disku
- Ne nudi tolerance napak

# Spet zvezek (Spanned Volume)

- 2 do 32 diskov, ki jih obravnavamo kot en zvezek
- Uporabno za kombiniranje več manjših delov prostora na disku ali za kombiniranje majhnih diskov
- Zvezke, formatirane za NTFS lahko razširjamo
- Če eden od diskov spetega zvezka izpade, je nedostopen celoten zvezek
- Če zbrišemo del spetega zvezka, je zbrisana celotna diskovna množica (disk set)

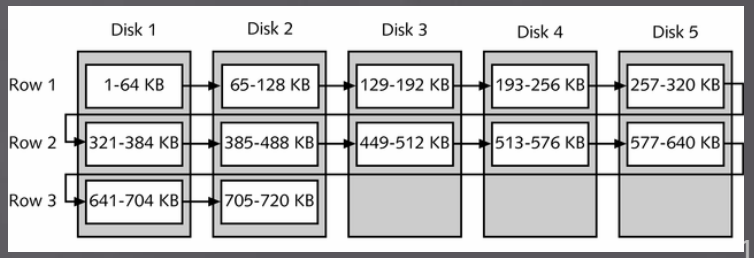


# Tvorba spetega zvezka iz štirih diskov

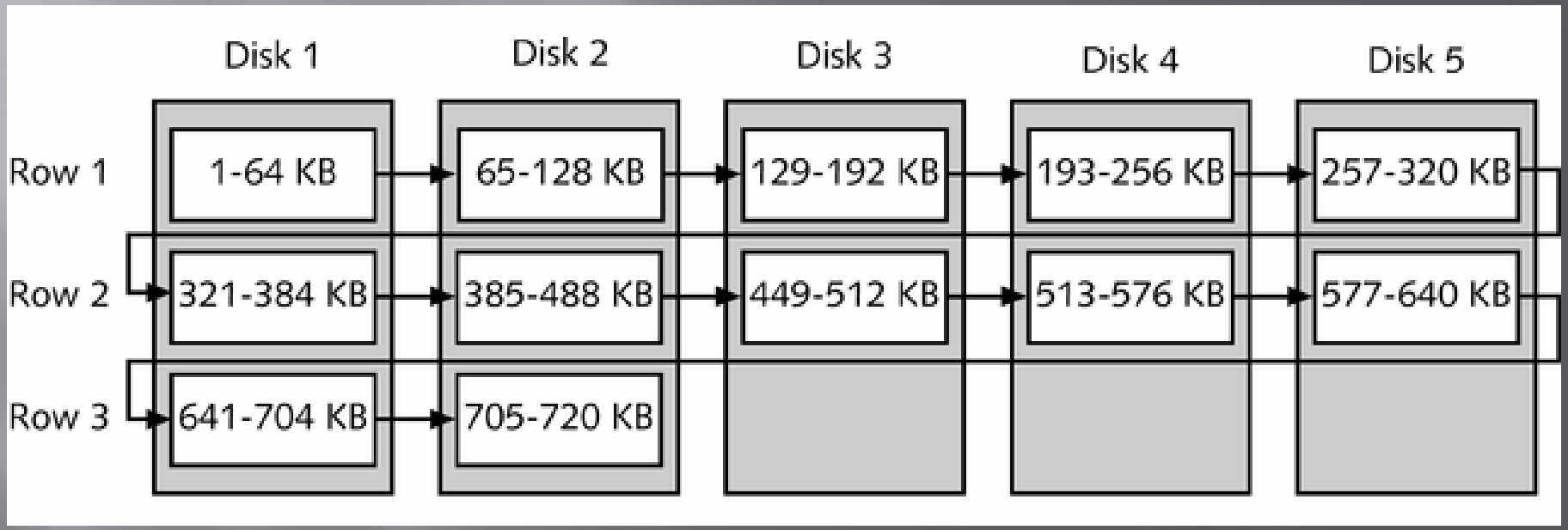


# Zvezek s progo (Striped Volume)

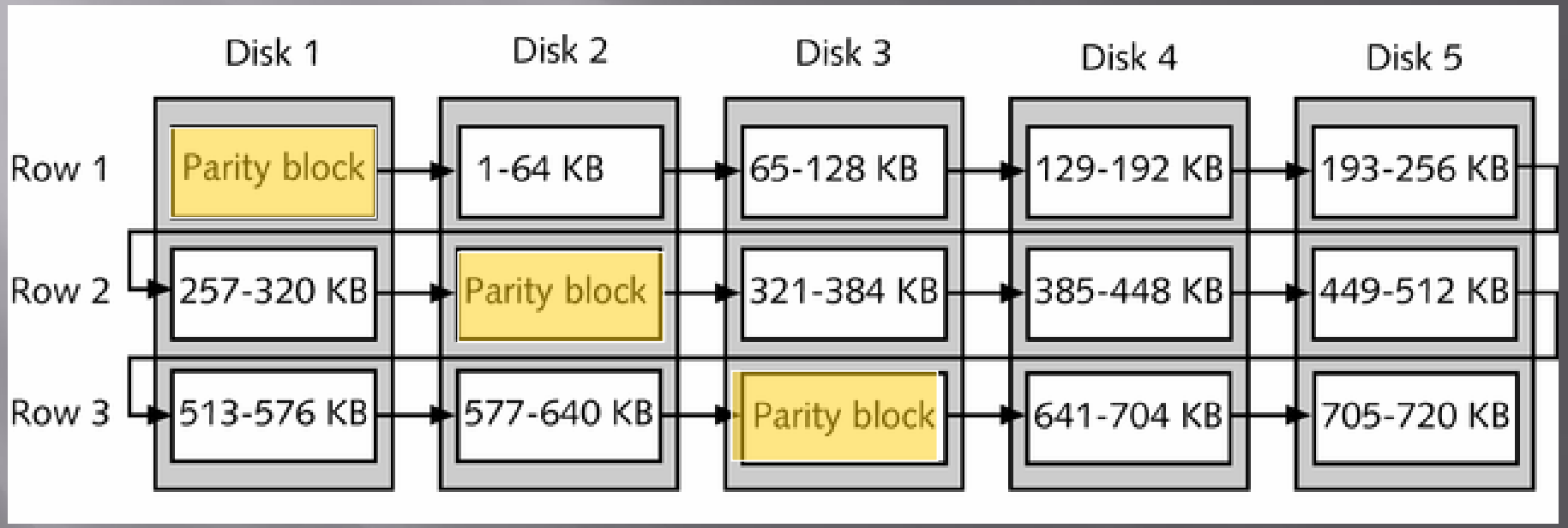
- Pravimo mu tudi RAID nivo 0
- Podaljša življenje trdih diskov z enakomernim razpostiranjem podatkov preko 2 do 32 pogonov
- Izboljša performance diska
- Enake količine podatkov v blokih velikosti 64 KB zapisujemo v vrstah na vsak disk
- Primerno za velike podatkovne baze in replikacijo podatkov
- Podatke izgubimo, če izpade eden ali več diskov



# Diski v zvezku s programi



# Diski v zvezku RAID5



# Uporaba zvezka RAID-5

- Uporablja parnostne bloke na vseh diskih. Podatki na teh so pomnjeni v vrstah blokov. Vsak blok ima 64 KB.
  - Parnost se obravnava z Boolovo logiko
  - Parnostni blik je vedno v vrstici *n* diska *n*, pri čemer je *n* številka diska
- Počasnejši od zvezka s progami
- Potrebuje več spomina kot  zrcaljenje ali preproste proge
- Velikost pomnilnega prostora je 1/*n,* pri čemer je *n* število fizičnih diskov v zvezku

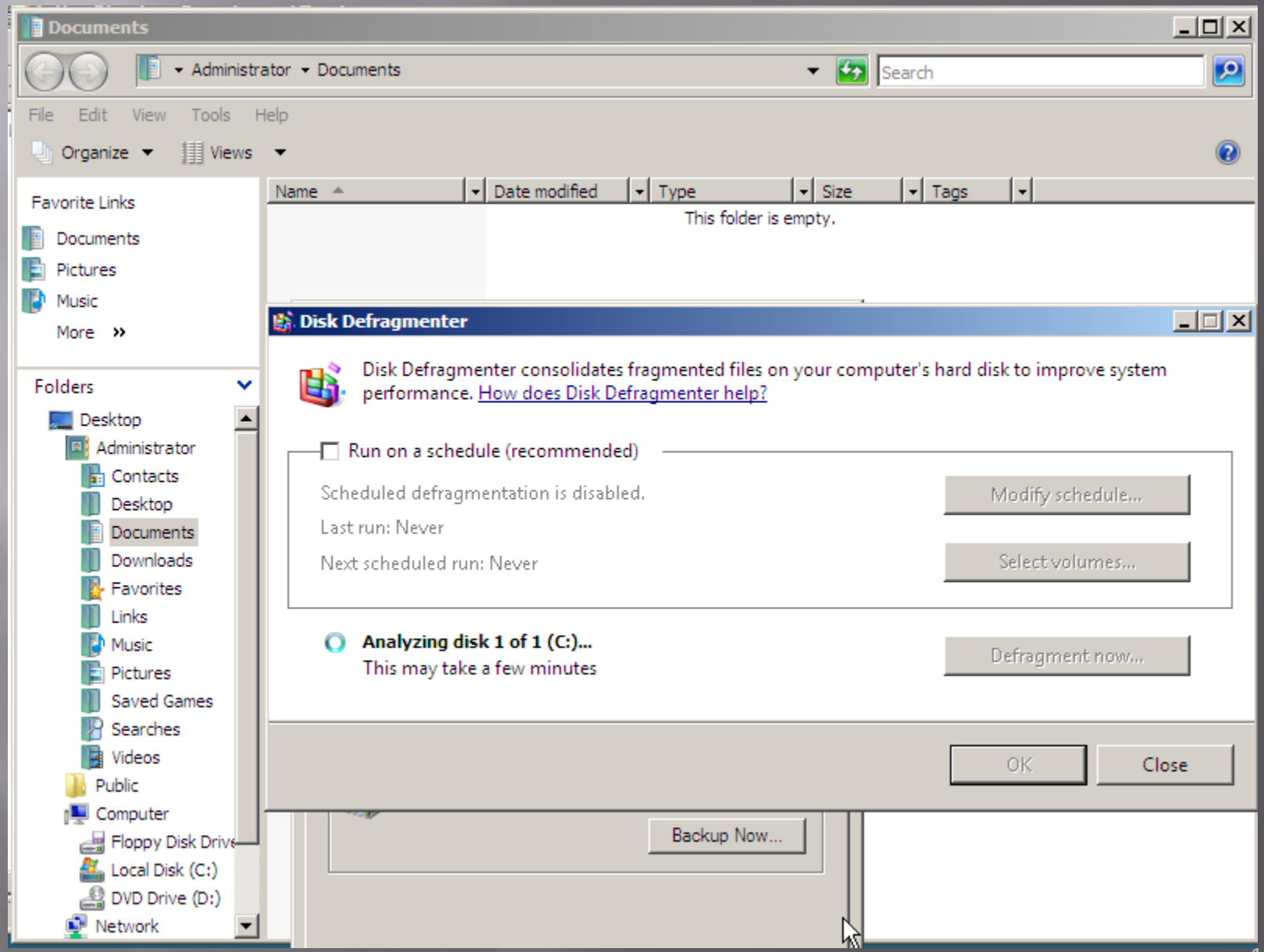
# Upravljanje diska

- Naloge
  - Vpogled v podatke o disku
  - Tvorba in brisanje particij in zvezkov
  - Pretvorba osnovnega diska v dinamični disk
  - Reševanje problemov z diskom
- Orodja
  - Disk Management
  - Disk Defragmenter
  - Check Disk
  - chkdsk

# Uporaba orodja Disk Defragmenter

- Diski postopoma postanejo fragmentirani
  - Datoteke se shranjujejo na prvo prosto področje na disku
  - Dostop do datoteke lahko zahteva branje z različnih lokacij na disku
- Disk Defragmenter
  - Analizira diske in tvori poročila
  - Locira fragmentirane direktorije in datoteke in jih prestavi na celovite lokacije na fizičnem disku
- Disk zelo zasedenega strežnika defragmentiraj enkrat na eden do dva tedna

# Uporaba orodja Disk Defragmenter



# Rezervne kopije diskov (disk backup)

- Kopiranje s traku na strežniku
  - Trakovi pomnijo več podatkov
  - Ne obremenjujemo dodatno omrežja
  - V primeru okvare traku lahko kopiramo z drugega traku
  - Assurance that the registry is backed up
- Kopiranje na omrežju
  - Lahko shranjujemo na en rezervni medij, kar poenostavlja administracijo
  - Ne moremo kopirati registra (registry )
  - Povečujemo promet na omrežju

# Možnosti tvorbe rezervnih kopij

- Normalni “backup”
  - Kopiranje celotnega sistema
  - Spreminja atribut “archive” vsake datoteke
- Inkrementalni “backup”
  - Kopiramo le nove oziroma spremenjene datoteke
  - Kopiramo le datoteke z atributom “archive”
  - Odstranjuje atribut “archive”
- Diferencialni “backup”
  - Podoben  inkrementalnemu, vendar ne odstrani atribut “archive”
  - Hitrejša obnova v primerjavi z inkrementalnim

# Možnosti tvorbe rezervnih kopij (nadaljevanje)

- “Copy backup”
  - Kopiramo le izbrane datoteke in direktorije
  - Atribut “archive” ostaja nespremenjen
  - Ne vpliva na regularne postopke tvorbe rezervnih kopij
- Dnevni “backup
  - Kopiramo le datoteke, ki so bile spremenjene na dan rezervnega kopiranja
  - Atribut archive¨” se ne spremeni
- Dodatna orodja v čarovniku “Backup or Restore”
  - Planirajmo avtomatsko izvajanje rezervnih kopiranj
  - Podatke restavriramo iz izmenljivih medijev

# DATOTEČNI SISTEMI, DATOTEKE, SOUPORABA DATOTEK

# Najprej nekaj o zaščiti objektov

- Vsak objekt ima seznam kontrole dostopov (access control list,  ACL) za upravljanje souporabe sredstev
- Dostop je nadzorovan z zaščitnimi tehnikami:
  - Atributi
  - Dovoljenja
  - Nadzor
  - Lastništvo

# Kaj je NTFS?

NTFS je datotečni sistem, ki nudi:

- Zanesljivost
- Zaščito na nivoju datotek in direktorijev
- Izboljšano upravljanje rasti pomnilnih medijev
- Večkratna uporabniška dovoljenja

# Dovoljenja za NTFS datoteke in direktorije

## Dovoljenja za datoteke

- Full Control
- Modify
- Read & Execute
- Write
- Read

## Dovoljenja za direktorije

- Full Control
- Modify
- Read & Execute
- Write
- Read
- List Folder Contents

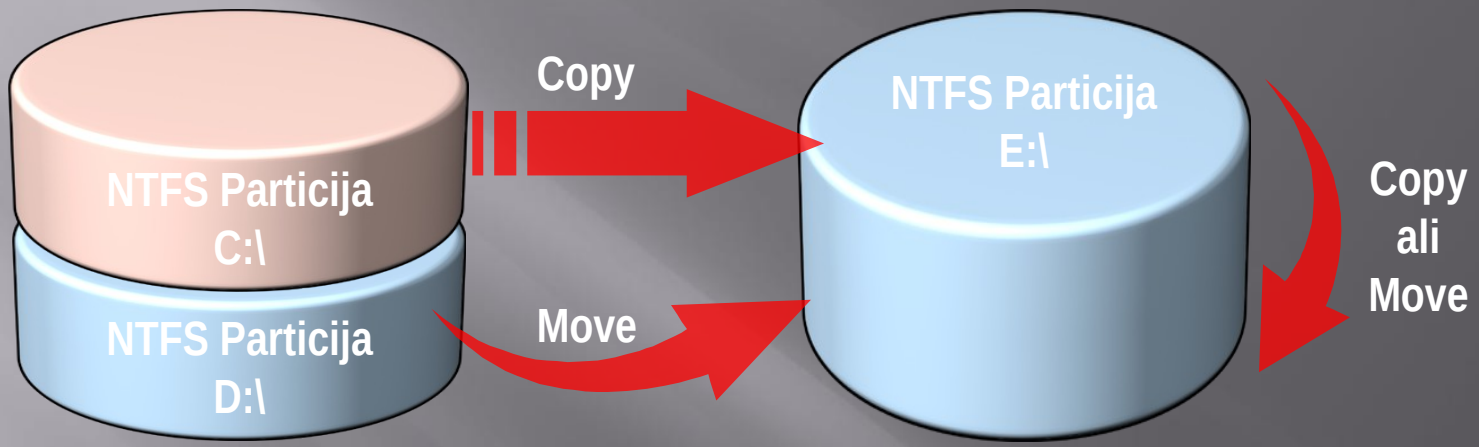
# Dobra praksa upravljanja dostopa do datotek in direktorijev s pomočjo dovoljenj NTFS

- Domenskim lokalnim skupinam damo dovoljenja, ki so obratna uporabniškim
- Sredstva združujemo v skupine zaradi lažje administracije
- Uporabnikom damo le tak nivo dostopa, kot ga potrebujejo
- Za aplikacijske (programske) direktorije damo dovoljenja  Read & Execute
- Za podatkovne direktorije damo dovoljenja Read & Execute and Write

# Kaj so veljavna dovoljenja nad NTFS datotekami in direktoriji?

- Dovoljenja so kumulativna
- Dovoljenja za datoteke so ločena od dovoljenj za direktorije
- Zapora (deny) prekrije vsa dovoljenja
- Prevzemanje lastništva

# Kaj se dogaja z NTFS dovoljenji pri kopiranju in premikanju datotek in direktorijev?



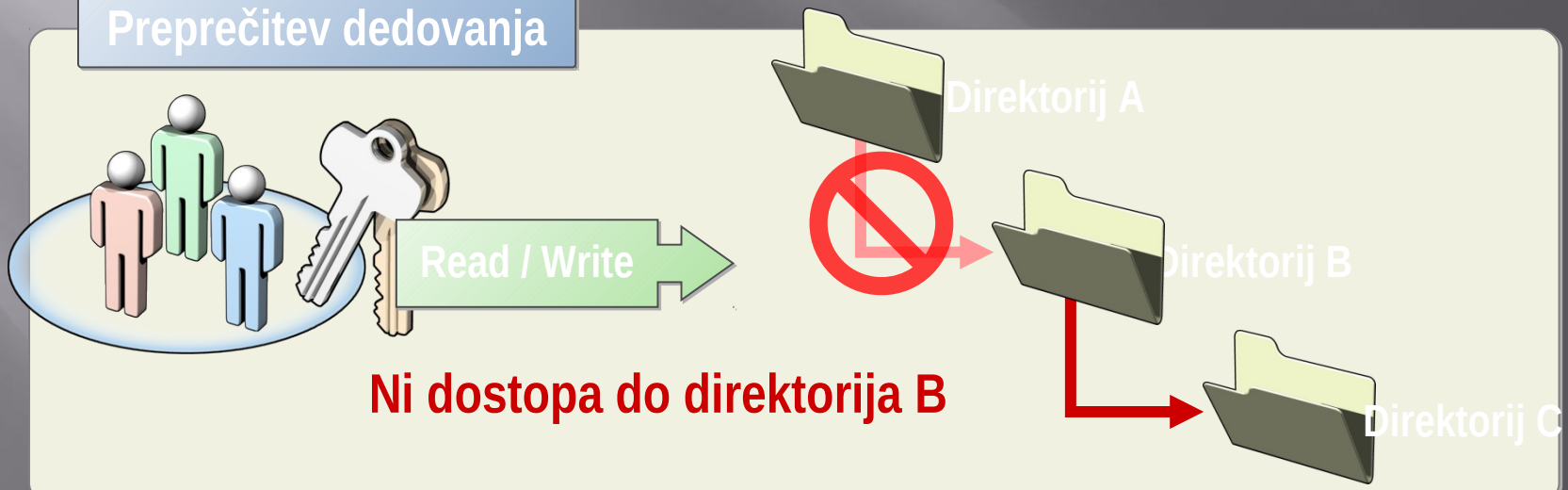

- Ko kopiramo datoteke in direktorije, le ti podedujejo dovoljenja ciljnega direktorija
- Ko premikamo datoteke in direktorije znotraj iste particije, zadržijo svoja dovoljenja
- Ko premikamo datoteke in direktorije v neko drugo particijo, podedujejo dovoljenja ciljnega direktorija

# Kaj je dedovanje NTFS dovoljenj?

## Dedovanje dovoljenj


**Dostop do direktorija B**

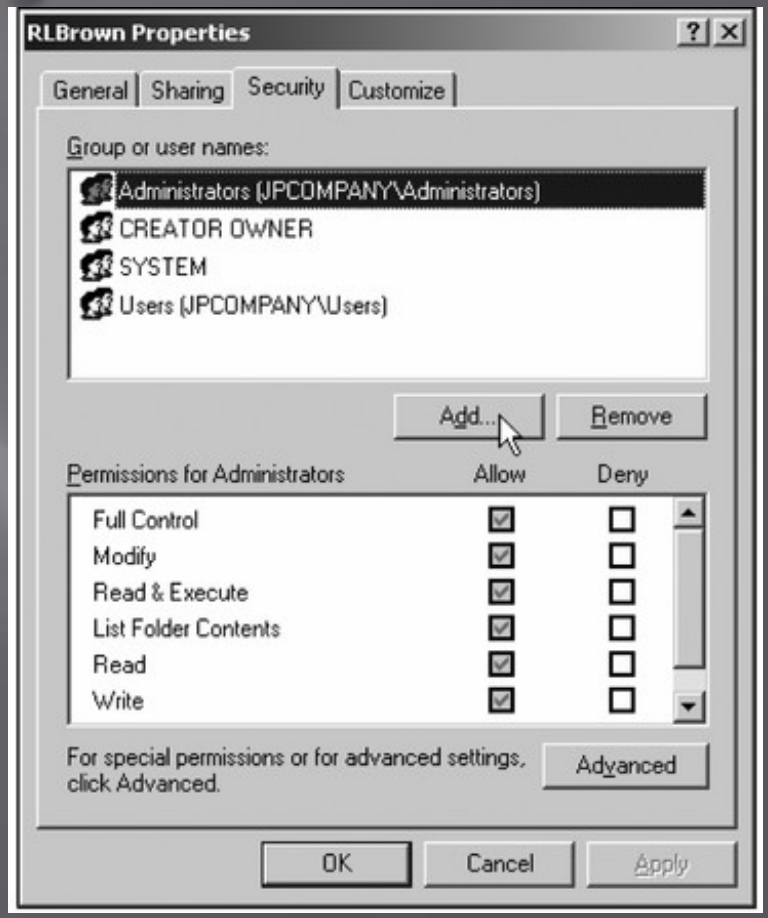
## Preprečitev dedovanja




**Ni dostopa do direktorija B**

# Dovoljenja datotek in direktorijev

- Dovoljenja za kontrolo dostopa do datoteke/direktorija s strani uporabnika ali skupine
- Odkljukamo dovoljenja ali zapreke
  - Če ne odkljukamo nič, uporabnik nima dostopa
  - Če odkljukamo zapreko, je dostop blokiran, ne glede na dovoljenja drugih
- Podedovana dovoljenja
  - Dovoljenja starševskega objekta veljajo za objekte-otroke
  - Glej sive kvadratke (ne moremo odkljukati)




*Dovoljenja za dostop do datoteke izberemo v zavihku "Security" lastnosti datotek oziroma direktorijev*

# Standardna dovoljenja za datoteke oziroma direktorije (pri sistemu NTFS)

| Permission | Description | Applies to |
|---|---|---|
| Full Control | Can read, add, delete, execute, and modify files plus change permissions and attributes, and take ownership | Folders and files |
| Modify | Can read, add, delete, execute, and modify files; cannot delete subfolders and their file contents, change permissions, or take ownership | Folders and file |
| Read & Execute | Implies the capabilities of both List Folder Contents and Read (traverse folders, view file contents, view attributes and permissions, and execute files) | Folders and files |
| List Folder Contents | Can list (traverse) files in the folder or switch to a subfolder, view folder attributes and permissions, and execute files, but cannot view file contents | Folders only |
| Read | Can view file contents, view folder attributes and permissions, but cannot traverse folders or execute files | Folders and files |
| Write | Can create files, write data to files, append data to files, create folders, delete files (but not subfolders and their files), and modify folder and file attributes | Folders and files |

# Posebna dovoljenja

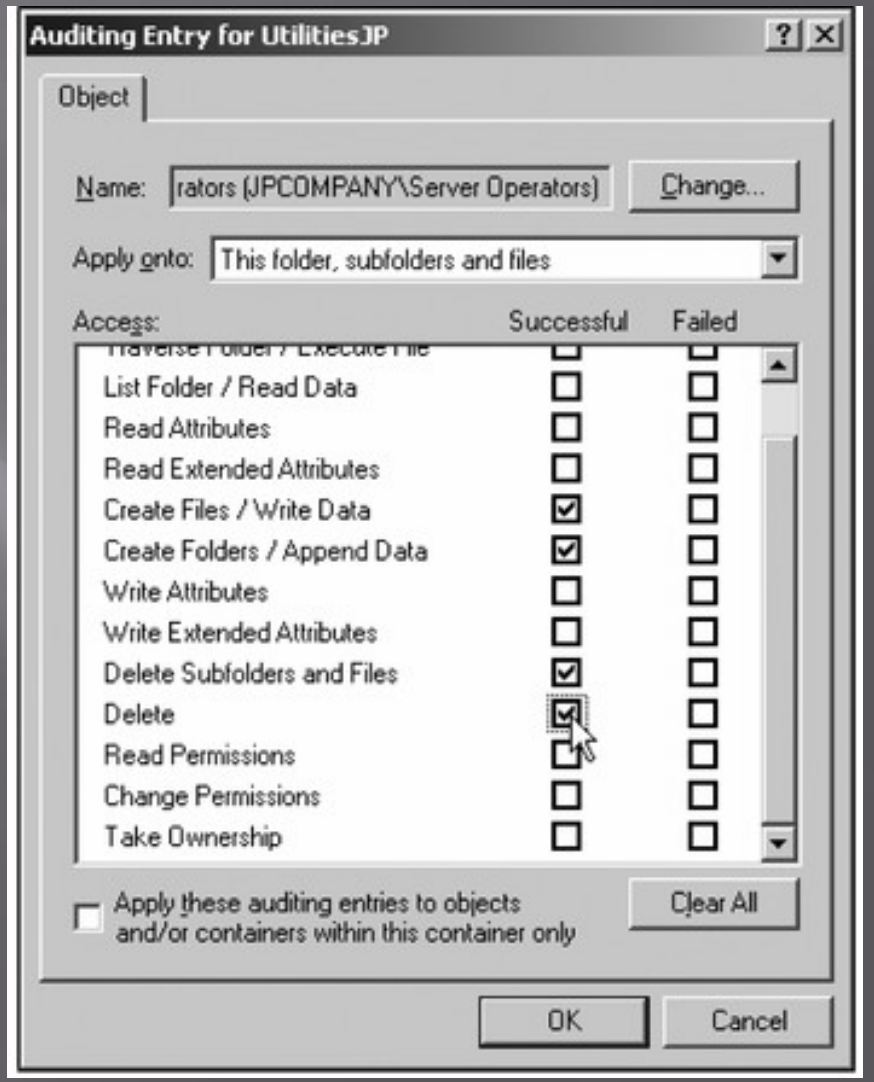
| Permission | Description | Applies to |
|---|---|---|
| Full Control | Can read, add, delete, execute, and modify files, plus change permissions and attributes, and take ownership | Folders and files |
| Traverse Folder / Execute File | Can list the contents of a folder and execute program files in that folder; keep in mind that all users are automatically granted this permission via the Everyone and Users groups, unless it is removed or denied by you | Folders and files |
| List Folder / Read Data | Can list the contents of folders and subfolders and read the contents of files | Folders and files |
| Read Attributes | Can view folder and file attributes (read-only and hidden) | |
| Read Extended Attributes | Enables the viewing of extended attributes (index, compress, encrypt) | |
| Create Files / Write Data | Can add new files to a folder and modify, append to, or write over file contents | |
| Create Folders / Append Data | Can add new folders and add new data at the end of files, but otherwise cannot delete, write over, or modify data | |
| Write Attributes | Can add or remove the read-only and hidden attributes | |
| Write Extended Attributes | Can add or remove the archive, index, compress, and encrypt attributes | |
| Delete Subfolders and Files | Can delete subfolders and files (the following Delete permission is not required) | |
| Delete | Can delete the specific subfolder or file to which this permission is attached | |
| Read Permissions | Can view the permissions (ACL information) associated with a folder or file (but does not imply you can change them) | |
| Change Permissions | Can change the permissions associated with a folder or file | |
| Take Ownership | Can take ownership of the folder or file (Read Permissions and Change Permissions automatically accompany this permission) | |

# Napotki za dovoljenja

- Direktorij \Windows  zaščitimo pred splošnimi uporabniki
- Direktorije s programskimi aplikacijami zaščitimo pred uporabniki, dovolimo pa jim izvajanje (Read & Execute, Write)
- Tvorimo javno uporabljane direktorije za splošen dostop, razen za administrativne naloge (Modify)
- Uporabniki naj imajo poln nadzor nad svojimi lastnimi direktoriji
- Iz zaupnih direktorijev odstranimo dostop za splošne skupine (Everyone in Users)
- Vedno se nagibajmo na stran prevelike zaščite

# Konfiguriranje sledenja nadzora (auditing) nad direktoriji in datotekami

- Z nadzorom sledimo aktivnosti nad direktorijem ali datoteko
- Direktoriji in datoteke Windows Server NTFS omogočajo nadzor nad katerokoli obliko posebnih dovoljenj
- Sledimo lahko vsaki obliki dostopa glede na uspeh ali neuspeh poskušanja
- Nastavimo politiko nadzora (auditing policy) na popoln nadzor objekta
  - Uporabimo orodje “Domain Security Policy”




*Nadzor direktorija*

# Upravljanje dostopa do souporabnih datotek s pomočjo "Offline Caching"

- Kaj so "offline" datoteke?
- Kako so sinhronizirane "offline" datoteke
- Možnosti predpomnenja (caching) "offline file"
- Kako uporabljamo "offline" predpomnenje

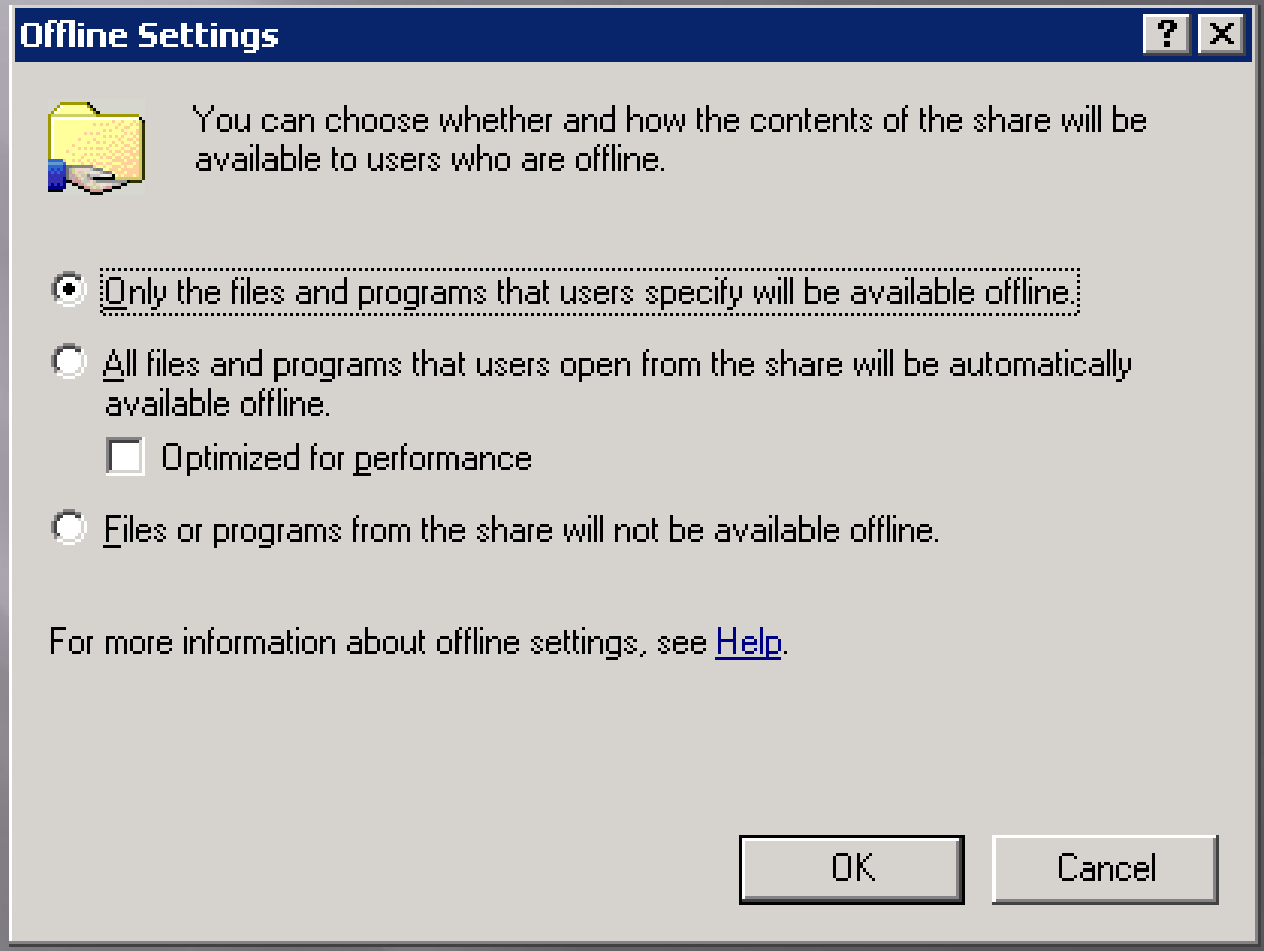
# Kaj so “offline” datoteke?

- “offline” datoteke predstavljajo zmožnost upravljanja z dokumenti, ki uporabnikom nudi konsistenten “online” in offline” dostop do datotek
- Prednosti uporabe “offline” datotek:
  - Podpora mobilnim uporabnikom
  - Avtomatska sinhronizacija
  - Prednosti performans
  - Prednosti tvorbe rezervnih kopij

# Kako so sinhronizirane “offline” datoteke

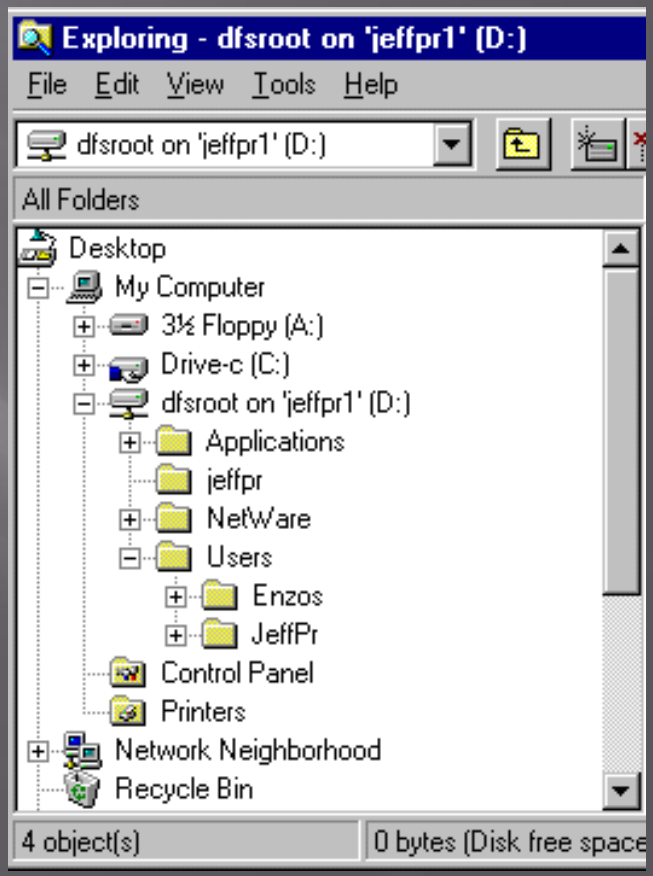
- Odklopljeni od omrežja
  - Windows Server 2003 sinhronizira omrežne datoteke z lokalno kopijo datotek
  - Uporabnik dela z lokalno kopijo datoteke
- Logirani na omrežje
  - Windows Server 2003 sinhronizira “offline” datoteke z omrežno verzijo datotek
- Če smo datoteko spreminjali na obeh lokacijah
  - Uporabnik odloči, katero verzijo bo uporabil. Lahko pa eno od datotek preimenuje in obdrži obe verziji

# Možnosti predpomnenja (Caching) "offline" datotek

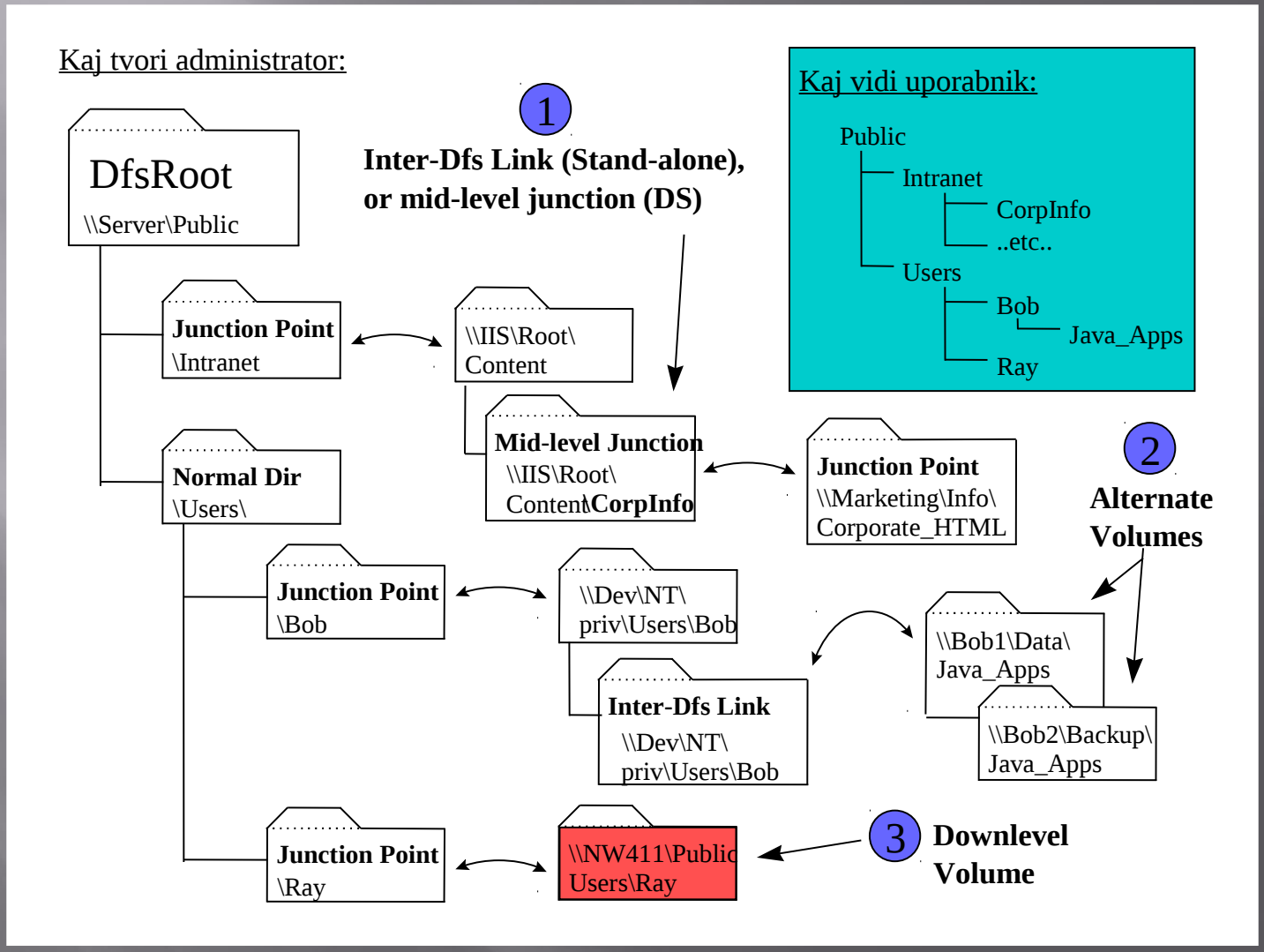


# Porazdeljen datotečni sistem (distributed file system)

- Souporabni direktoriji na omrežju lahko izgledajo kot hierarhija direktorijev
  - To poenostavlja dostop uporabnikov
- Pri replikaciji souporabnih direktorijev imamo možnost tolerance izpadov
  - Uporabljamo Microsoftov servis "File Replication"
- S porazdelitvijo dostopa do direktorijev med več strežniki dosežemo uravnovešenje bremena
- Izboljšan je dostop do internetnih in intranetnih lokacij
- Rezervno kopiranje iz ene množice glavnih direktorijev

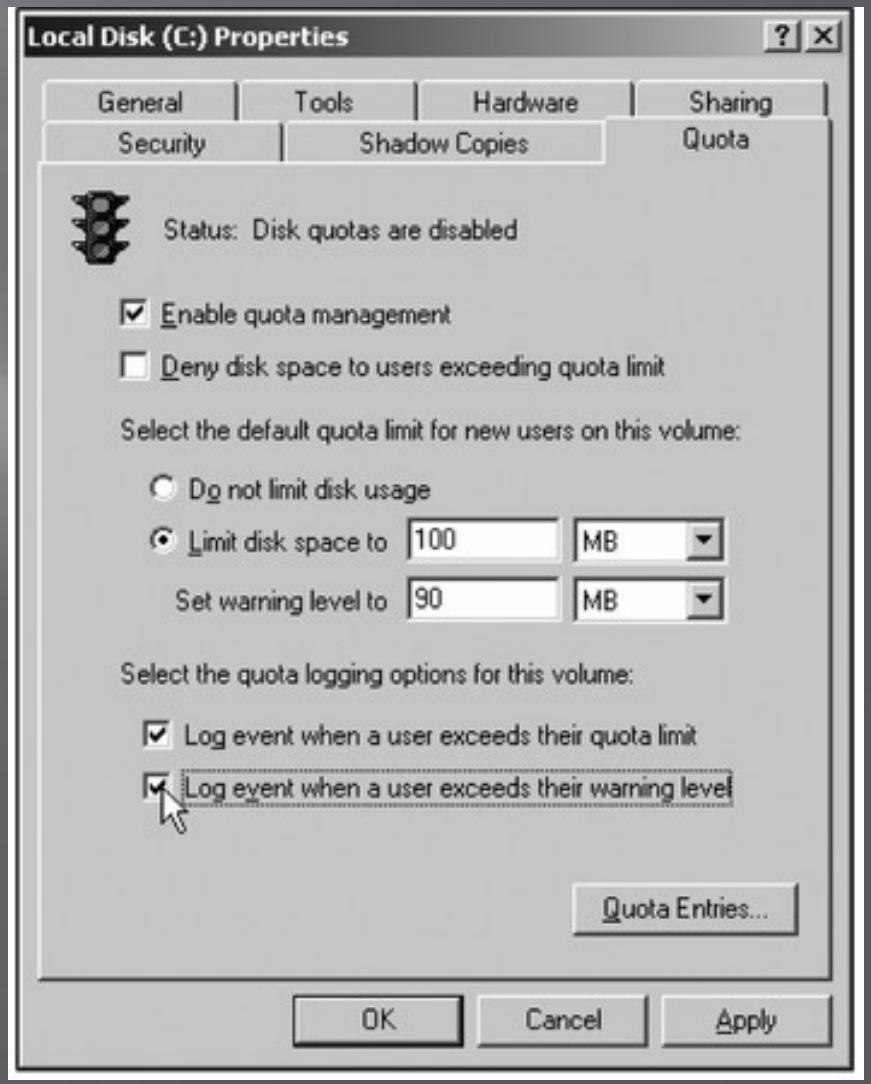


# Primer DFS (porazdeljenega datotečnega sistema)



# Konfiguriranje diskovnih kvot

- NTFS nudi možnost vzpostavljanja diskovnih kvot
- Onemogoča uporabnikom zapolnitev diskov
- Z opozorili o omejitvah kvot pomaga uporabnikom upravljanje z diski
- Sledi potrebe po diskovnih zmogljivostih glede na posamezne uporabnike. To omogoča planiranje vnaprej
- Nudi administratorju strežnika podatke, kdaj se uporabniki bližajo omejitvi kvot

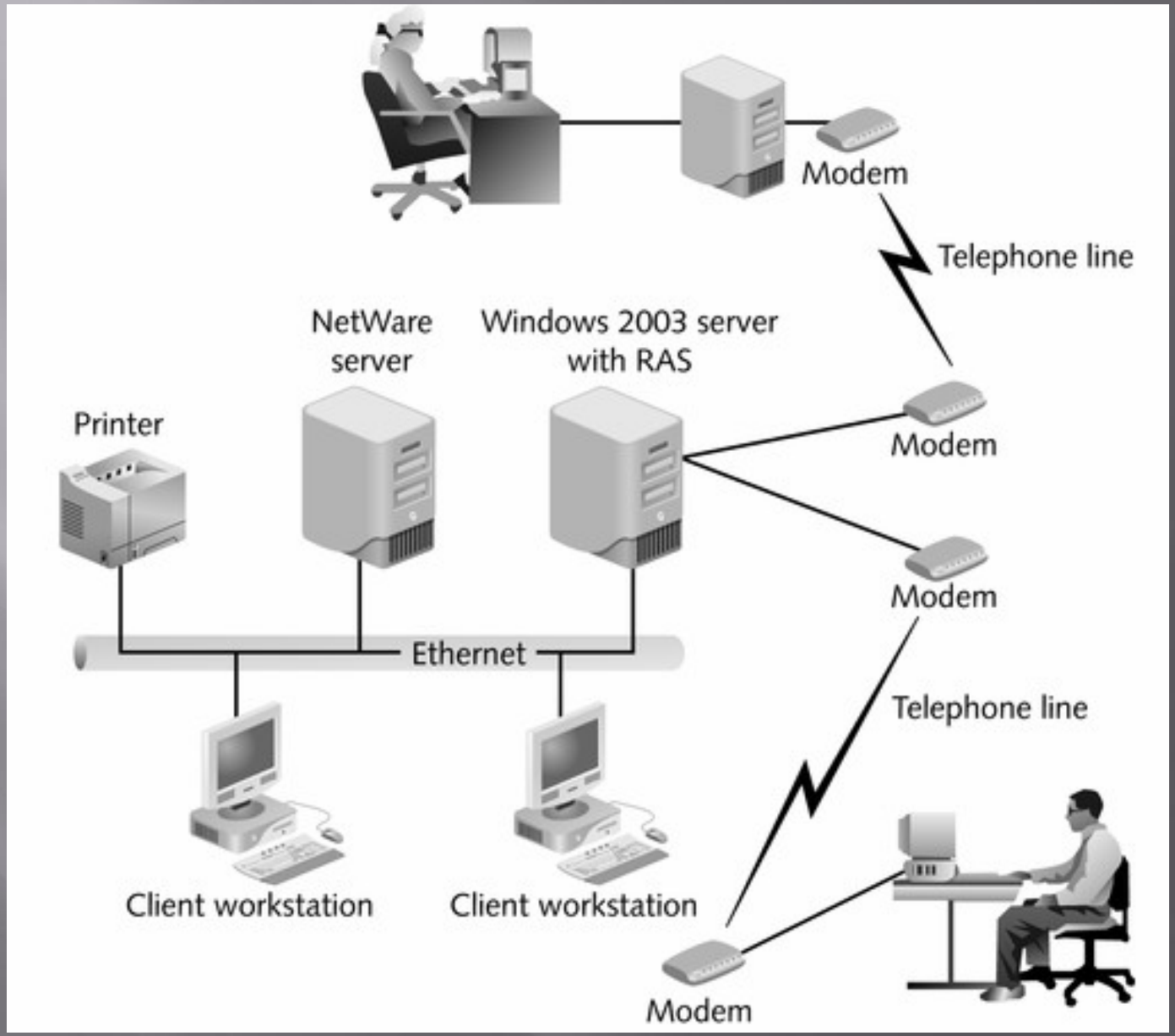


# KONFIGURIRANJE REMOTE ACCESS SERVICES

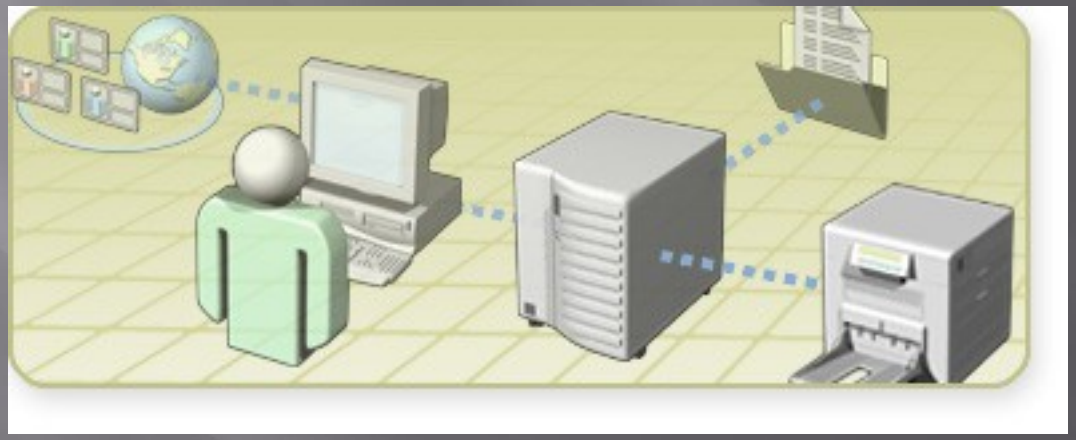
# Uvod v oddaljeni dostop

- Oddaljen dostop danes pogosto uporabljamo
  - Telekomunikacije in poslovna potovanja
- Windows Server 2003 omogoča strežniku, daq deluje tudi kot  strežnik za oddaljen dostop
  - Strežnik za oddaljen dostop (Remote Access Services (RAS) server) postane tako, da uporabi “Routing and Remote Access Services” (RRAS)
  - Istočasno lahko opravlja tudi normalne strežniške funkcije
- Uporabnik lahko dostopa do strežnika RAS preko telefona ali preko interneta ali intraneta

# Oddaljen dostop preko strežnika

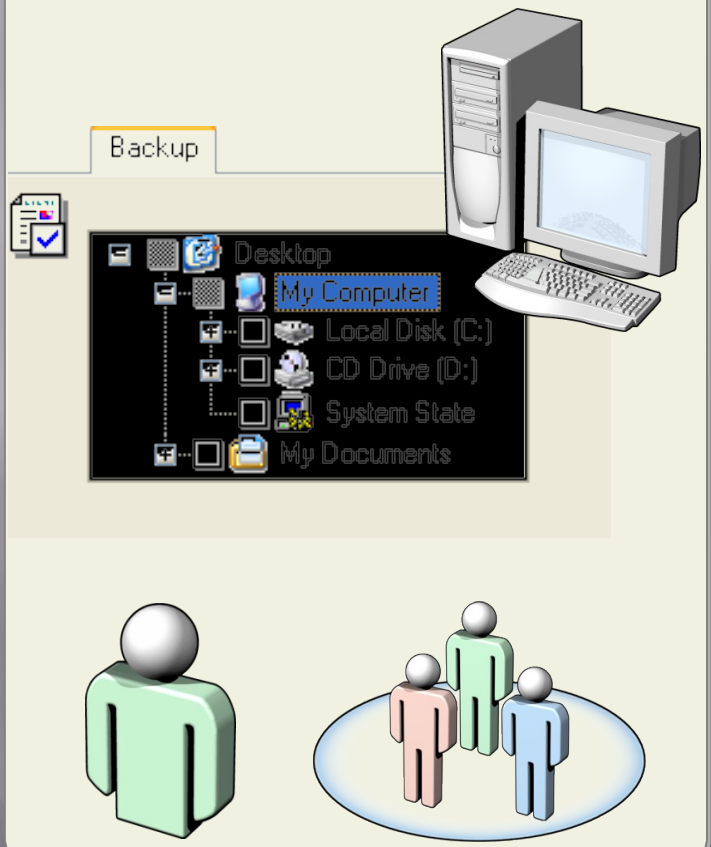


# VARNOST IN WINDOWS SERVER 2008

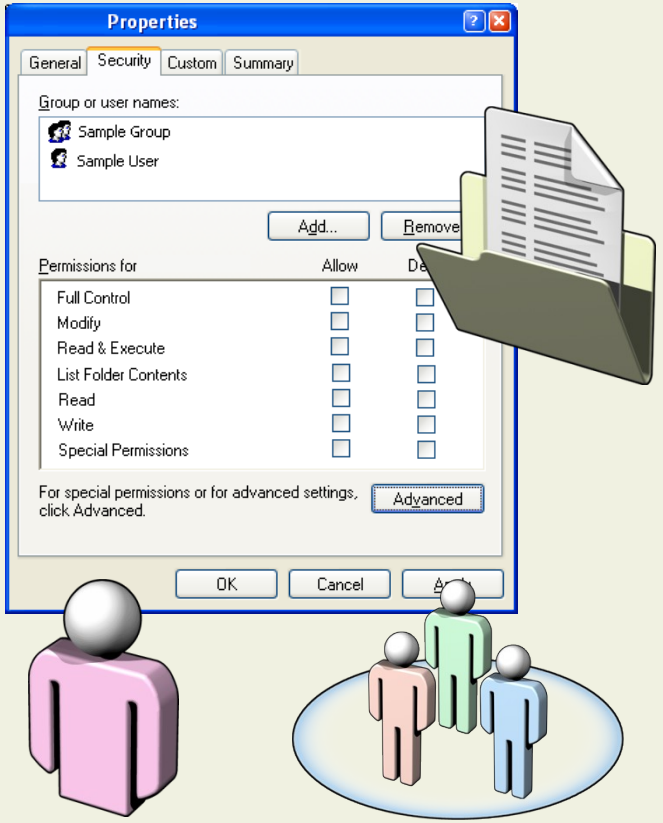


# Primerjava uporabniških pravic in dovoljenj

## Uporabniške pravice: Akcije na sistemu




## Dovoljenja: Akcije na objektu



# Kaj je nadzor (auditing)?

- Nadzor sledi aktivnostim uporabnika in operacijskega sistema in zapisuje izbrane dogodke v varnostne zapise (security logs)


- Omogoča nadzor za:
  - Tvorbo podatkovne baze
  - Odkrivanje groženj in napadov
  - Ugotavljanje škode
  - Preventivo nadaljnje škode
- Nadzor dostopa do objektov, upravljanja kontov, prijav in odjav uporabnikov

# Kaj je politika nadzora (Audit Policy)?

- Varnostna politika določa varnostne dogodke, o katerih bo poročano administratorju omrežja
- Varnostno politiko vzpostavimo za:
  - Sledenje uspešnim ali propadlim dogodkom
  - Minimiziranje nepooblaščene uporabe sredstev
  - Vzdrževanje zaposa o aktivnosti
- Varnostne dogodke beležimo v varnostne zapise (security logs)

# Tipi dogodkov za nadzorovanje

- Logiranje kontov
- Upravljanje kontov
- Dostop do servisov imenika
- Logiranje
- Dostop do objektov
- Sprememba politike
- Uporaba privilegijev
- Sledenje procesom
- Sistem

# Napotki za planiranje politike nadzora

- Določimo računalnike, na katerih bo vzpostavljen nadzor
- Določimo, katere dogodke bomo nadzorovali
- Določimo, ali bomo nadzorovali uspeh ali neuspeh dogodkov
- Določimo, če moramo slediti trend dogodkov
- Pogosto pregledujemo varnostne zapise

# Upravljanje z varnostnimi zapisi

- Kaj so “Log Files”?
- Pogosti varnostni dogodki
- Naloge, povezane z upravljanjem datotek z varnostnimi zapisi (Security Log Files)
- Kako upravljamo s podatki v datotekah z varnostnimi zapisi
- Kako gledamo na dogodke v varnostnih zapisih

# Kaj so “Log Files”?

**Orodje “Event Viewer” ima na voljo naslednje zapise:**

- Application
- Security
- System
- Directory service
- File Replication service

**Filtriranje datotek z varnostnim zapisom**
**Pogled na datoteke z varnostnim zapisom**

# Skupinska politika

- Vzpostavimo jo lahko za lokacijo, domeno, organizacijske enote ali lokalni računalnik
- Ne moremo je vzpostaviti za vsebovalnike, ki niso organizacijske enote (Cannot be set for non-OU folder containers)
- Nastavitve politike za skupine pomnimo v objektih "Group Policy objects" (GPO)
  - Vsak GPO ima edinstveno ime in GUID
- Imamo lokalne in ne-lokalne GPO
  - Če imamo več GPO, je njihov učinek inkrementalen
  - Vrstni red je: lokalno, privzeta domena, položaj (site), organizacijska enota (OU)
- Skupinsko politiko (Group Policy) lahko vzpostavimo tako, da vpliva na uporabniške konte, na računalnike ali na oboje
- Ko osvežimo skupinsko politiko, stare politike odstranimo ali osvežimo za vse klijente

# Varnostne šablone (Security Templates Snap-in)

- Uporabne, ko imamo večkratne skupinske politike (group policies) ali pa več organizacijskih enot (OU) souporablja isto skupinsko politiko
- Varnost nastavimo za naslednje
  - Konte in lokalne politike
  - Politike sledenja dogodkov (Event log tracking policies)
  - Omejitve skupin
  - Varnost dostopa do servisov
  - Varnost registra
  - Varnost datotečnega sistema

# Opcije varnosti gesla

- Uveljavljanje zgodovine gesla
  - Zahteva od uporabnikov, da izberejo nova gesla, ko spreminjajo gesla
- Največja starost gesla
  - Nastavi maksimalni čas do poteka gesla
  - Običajno 45 do 90 dni
- Najmanjša starost gesla
- Najmanjša dolžina gesla
  - Najmanj 7 znakov za “močno geslo”
- Geslo mora izpolnjevati zahtevo po kompleksnosti
  - Filtriranje zahtevkov za gesla
- Pomnenje gesel s pomočjo reverzibilnega kodiranja

# Opcije za zapiranje kontov

- Trajanje zapore konta
  - Lahko določimo v minutah, koliko časa je določen konto zaprt potem, ko je bilo izvedeno določeno število neuspelih poskusov logiranja
- Nivo zapore konta (account lockout threshold)
  - Določimo lahko omejitev za število neuspelih logiranj
- Reset števca zapore konta po
  - Določimo lahko število minut med dvema zaporednima neuspešnima poskusoma logiranja. S tem poreprečimo, da ne bi bil konto prehitro odklenjen

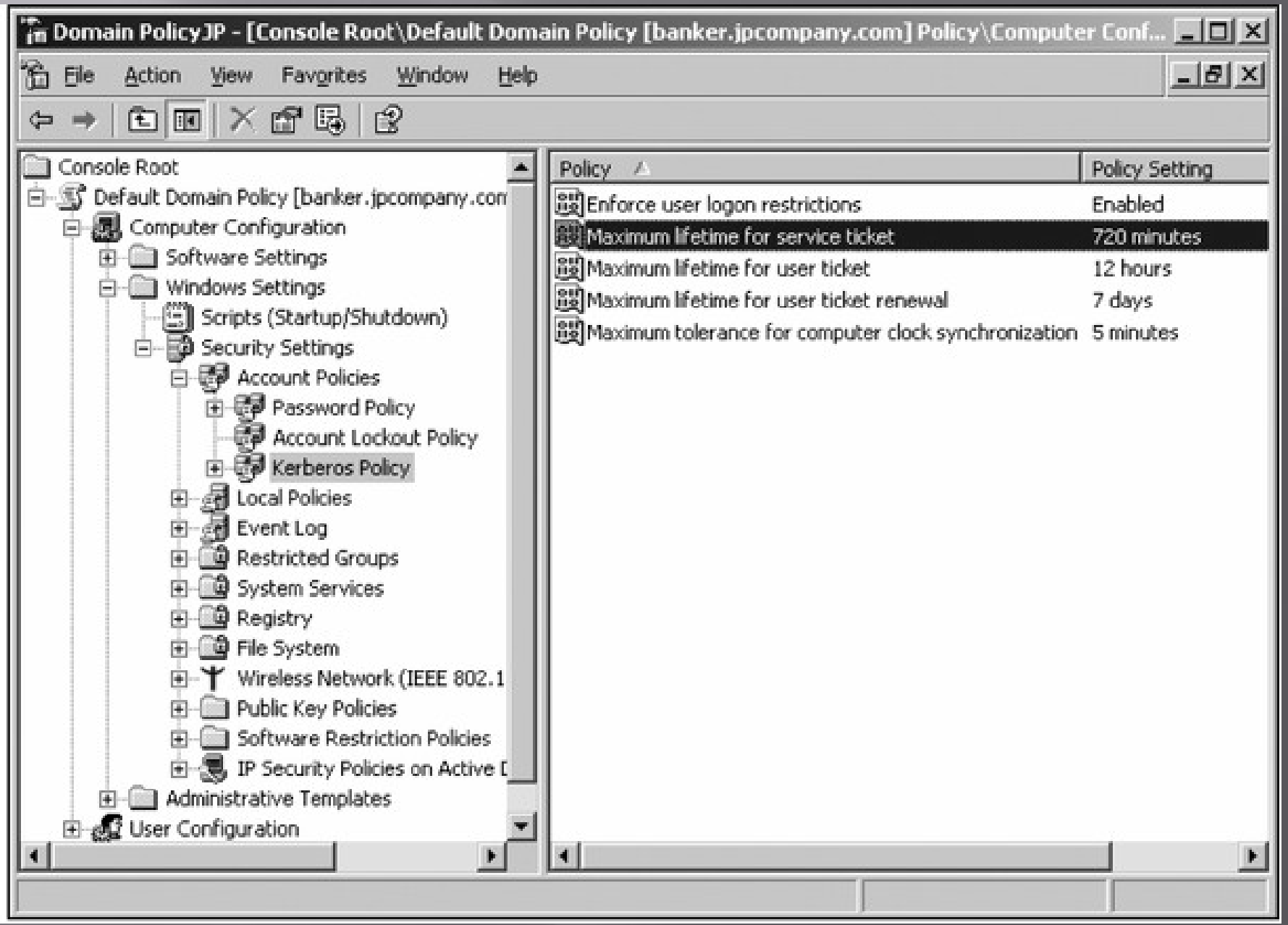
# Varnost Kerberos

- Vključuje uporabo listkov (tickets), ki si jih izmenjujeta klijent, ki zahteva dostop, in strežnik oziroma aktivni direktorij, ki zagotavlja dostop
- Distribucijski center ključev (DC ali strežnik) pomni konte uporabnikov in gesla
- Računalnik-klijent pošlje ime konta in geslo distribucijskemu centru ključev
- Distribucijski center pošlje začasno dovoljenje (temporary ticket), ki zagotavlja dostop do strežnika “ticket-granting server”
- “ticket-granting server” pošlje servisno dovoljenje “service ticket” za čas, dokler traja logiranje (logon session).

# Varnostne možnosti Kerberos

- Uveljavlja omejitve logiranja uporabnikov
  - Varnot Kerberos je privzeta
- Najdaljši čas veljavnosti servisnega dovoljenja
  - Maksimalni čas (v minutah), ko dovoljenje ( omogoča dostop do določenega servisa v eni seji
- Najdaljši čas veljavnosti uporabniškega dovoljenja
  - Maksimalni čas (v urah), ko lahko dovoljenje uporabljamo v enoviti seji za dostop do računalnika ali domene
- Najdaljši čas za za obnovitev uporabniškega dovoljenja
  - Maksimalno število dni, ko lahko obnovimo isto Kerberos dovoljenje vsakokrat, ko se logiramo
- Največja toleranca za sinhronizacijo računalniškega časa
  - Največ koliko minut čaka klijent na sinhronizacijo njegove ure

# Konfiguriranje politike Kerberos



# NADZOR STREŽNIKA IN OMREŽJA

# Uvod v nadzor strežnika

- Zakaj nadzorujemo
  - Preventiva problemov, preden sploh pride do njih
  - Diagnostika obstoječih problemov
- Vzpostavljanje testov (benchmarks) za primerjanje podatkov, ki smo jih dobili z nadzorom, s predvidenimi performansami
  - Disk, CPE, pomnilnik, odzivni časi omrežja
  - Počasna, tipična in zelo obremenjena uporaba strežnika in omrežnih sredstev

# Nadzor servisov strežnika

| Service | Description |
|---|---|
| Alerter | Sends notification of alerts or problems on the server to users designated by the network administrator |
| Computer Browser | Keeps a listing of computers and domain resources to be accessed |
| Event Log | Enables server events to be logged for later review or diagnosis in case problems occur |
| File Replication Service | Replicates the Active Directory elements on multiple DCs when Active Directory is installed |
| Intersite Messaging | Transfers messages between different Windows Server 2003 sites |
| IPSec Services | Enables IPSec security |
| Kerberos Key Distribution Center | Enables Kerberos authentication and the server as a center from which to issue Kerberos security keys and tickets |
| License Logging | Enables the monitoring of server and other licensing |

Primer servisov Windows Server 2003

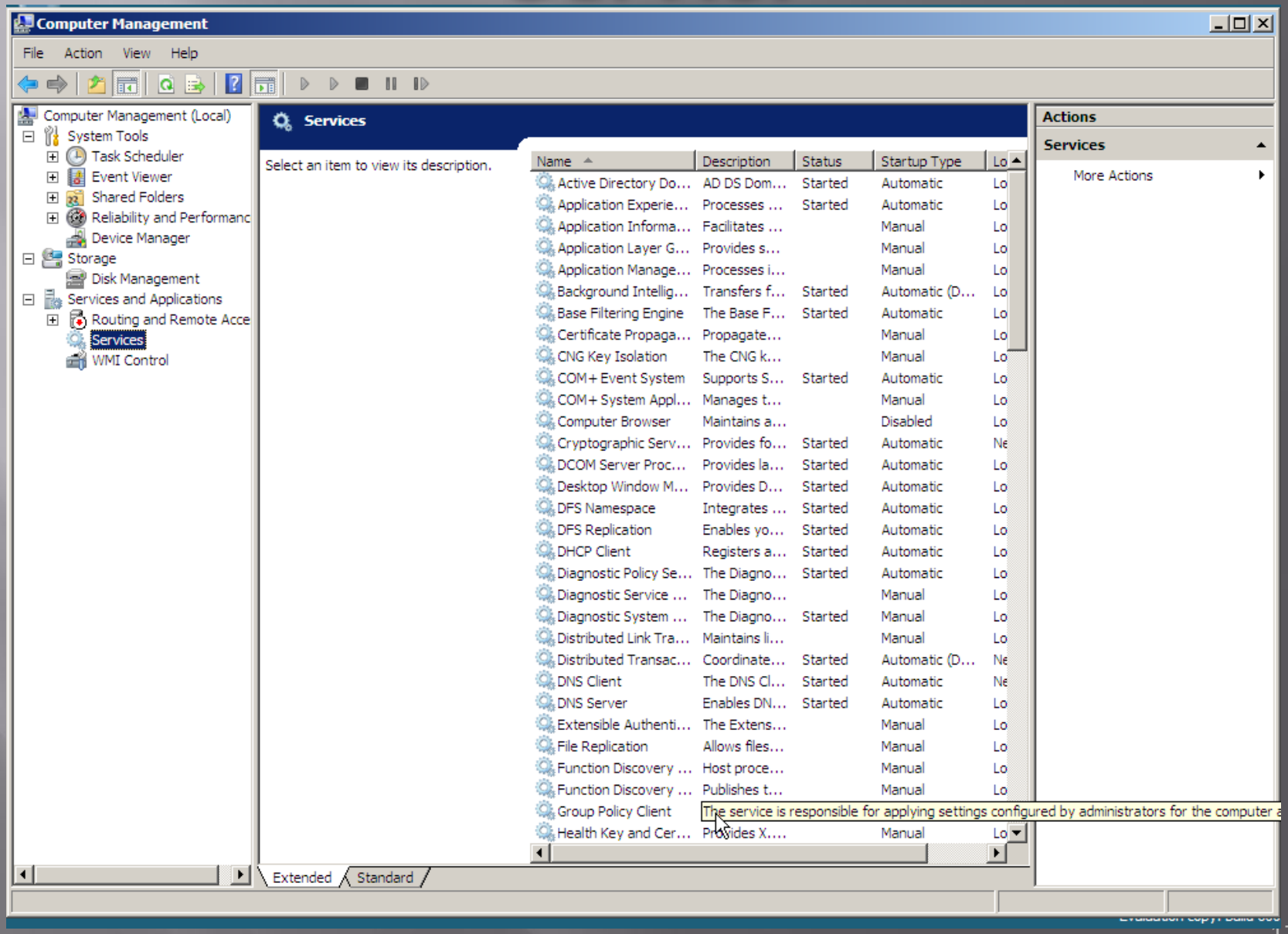
# Primer servisov v Windows 2008

| Service | Description |
|---|---|
| Logical Disk Manager | Monitors for disk problems, such as a disk that is nearly full |
| Messenger | Handles messages sent for administrative purposes |
| Net Logon | Maintains logon services such as verifying users who are logging onto the server or a domain |
| Plug and Play | Enables automatic detection and installation of new hardware devices or devices that have changed |
| Print Spooler | Enables print spooling |
| Protected Storage | Enables data and services to be stored and protected by using private key authentication |
| Remote Procedure Call (RPC) | Provides Remote Procedure Call Services |
| Remote Procedure Call (RPC) Locator | Used in communications with clients using remote procedure calls to locate available programs to run |
| Remote Registry | Enables the registry to be managed remotely |
| Removable Storage | Enables management of removable storage media, such as tapes, CD-RWs, and Zip and Jaz drives |
| Security Accounts Manager | Keeps information about user accounts and their related security setup |
| Server | A critical service that supports shared objects, log on services, print services, and remote procedure calls |
| System Event Notification | Enables the detection and reporting of important system events, such as a hardware or network problem |
| Task Scheduler | Used to start a program at a specified time and works with the software Task Scheduler |
| TCP/IP NetBIOS Helper | Activated when TCP/IP is installed and used to enable NetBIOS name resolution and NetBIOS network transport |
| Uninterruptible Power Supply | Used with a UPS to supply power to the server during power failures |
| Windows Time | Enables updating the clock |
| Workstation | Enables network communications and access by clients over the network |

# Dostop do servisov strežnika

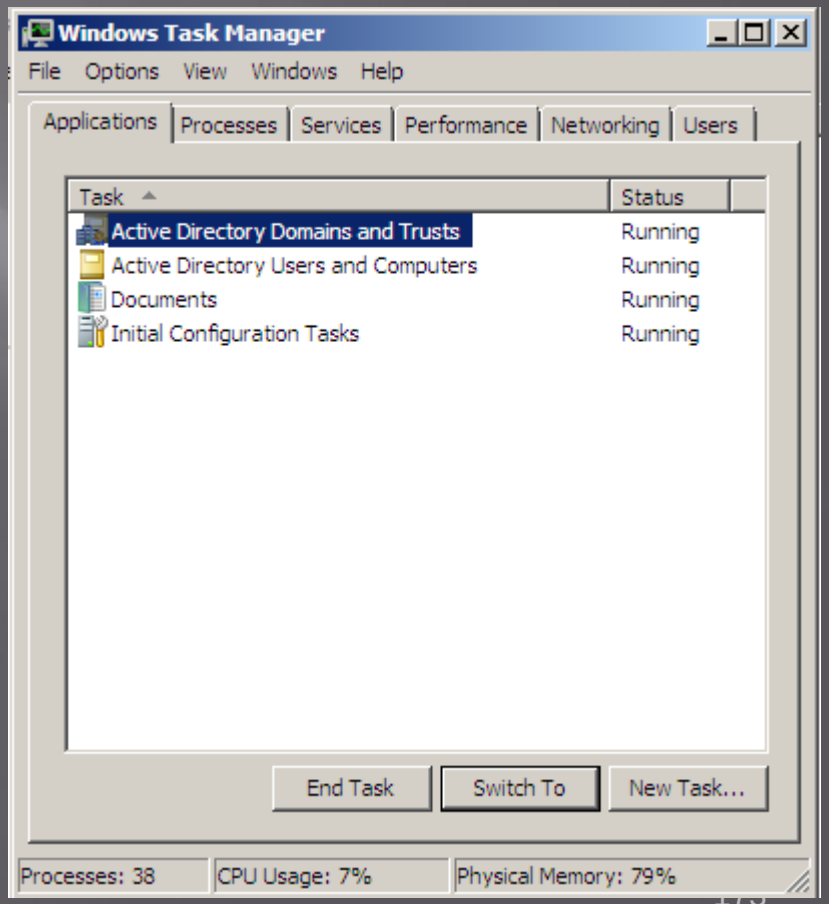
- Odpremo orodje “Computer Management”
- Okno s servisi ima 5 kolon
  - Name
  - Description
  - Status
    - Started, Paused, or blank
  - Startup Type
    - Automatic (most services), manual, or disabled
  - Log On As
    - Services usually log on to the Local System

# Servisi


Computer Management
File Action View Help
Computer Management (Local)
System Tools
Task Scheduler
Event Viewer
Shared Folders
Reliability and Performanc
Device Manager
Storage
Disk Management
Services and Applications
Routing and Remote Acce
Services
WMI Control
Services
Select an item to view its description.
Name Description Status Startup Type Lo
Active Directory Do... AD DS Dom... Started Automatic Lo
Application Experie... Processes ... Started Automatic Lo
Application Informa... Facilitates ... Manual Lo
Application Layer G... Provides s... Manual Lo
Application Manage... Processes i... Manual Lo
Background Intellig... Transfers f... Started Automatic (D... Lo
Base Filtering Engine The Base F... Started Automatic Lo
Certificate Propaga... Propagate... Manual Lo
CNG Key Isolation The CNG k... Manual Lo
COM+ Event System Supports S... Started Automatic Lo
COM+ System Appl... Manages t... Manual Lo
Computer Browser Maintains a... Disabled Lo
Cryptographic Serv... Provides fo... Started Automatic Ne
DCOM Server Proc... Provides la... Started Automatic Lo
Desktop Window M... Provides D... Started Automatic Lo
DFS Namespace Integrates ... Started Automatic Lo
DFS Replication Enables yo... Started Automatic Lo
DHCP Client Registers a... Started Automatic Lo
Diagnostic Policy Se... The Diagno... Started Automatic Lo
Diagnostic Service ... The Diagno... Manual Lo
Diagnostic System ... The Diagno... Started Manual Lo
Distributed Link Tra... Maintains li... Manual Lo
Distributed Transac... Coordinate... Started Automatic (D... Ne
DNS Client The DNS Cl... Started Automatic Ne
DNS Server Enables DN... Started Automatic Lo
Extensible Authenti... The Extens... Manual Lo
File Replication Allows files... Manual Lo
Function Discovery ... Host proce... Manual Lo
Function Discovery ... Publishes t... Manual Lo
Group Policy Client The service is responsible for applying settings configured by administrators for the computer
Health Key and Cer... Provides X... Manual Lo
Extended Standard
Actions
Services
More Actions

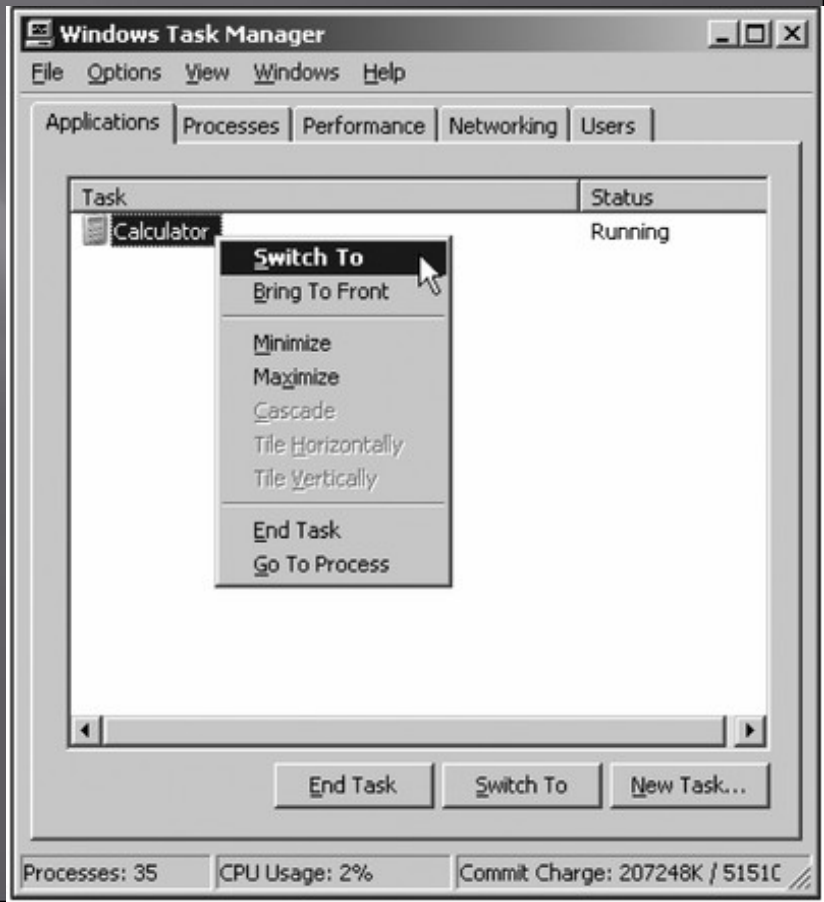
# Uporaba orodja "Task Manager"

- Z njim nadzorujemo in upravljamo sredstva strežnika
  - Aplikacije
  - Procesi
  - Servisi
  - Obnašanje v realnem času
  - Obnašanje omrežja
  - Uporabniki



# Nadzor aplikacij

- Zavihek “Applications” prikazuje vse aplikacije (tasks, naloge), ki smo jih pognali na konzoli strežnika
- Možnosti akcije:
  - Konec naloge, prehod na drugo nalogo, proženje nove naloge (End Task, Switch To, New Task)
- Statusna vrstica prikazuje podatke o procesih
- Desni klik na posamezno aplikacijo odpre naslednje možnosti:
  - Switch To, Bring To Front, Minimize, Maximize, End Task, Go to Process



# Nadzor procesov

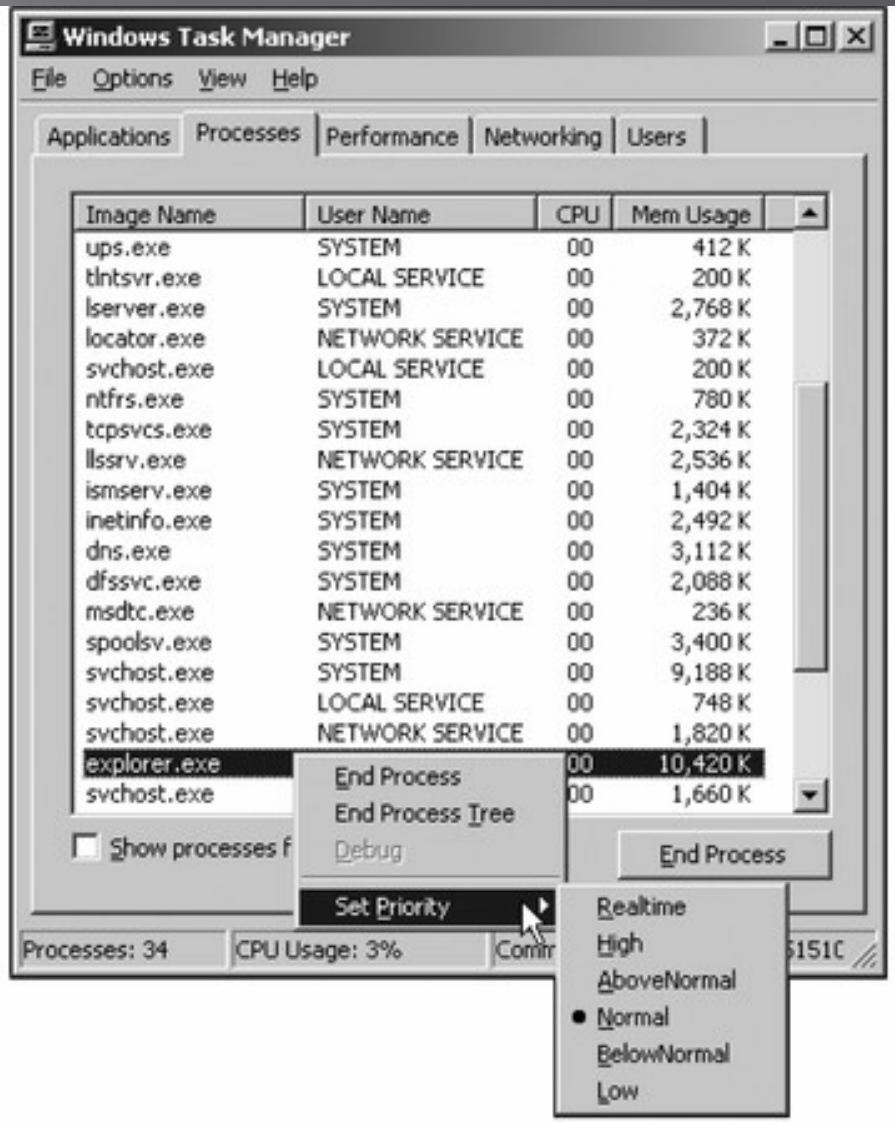
- Zavihek “Processes” prikazuje seznam vseh procesov, ki jih uporabljajo vse aplikacije
- Posamezen proces lahko ustavimo
- Posameznemu procesu lahko spremenimo prioriteto

- O procesu imamo na voljo nsalednje podatke:

| Process Information | Description |
|---|---|
| Image Name | The process name, such as winword.exe for Microsoft Word |
| User Name | The user account under which the process is running |
| CPU | The percentage of the CPU resources used by the process |
| Mem Usage | The amount of memory the process is using |

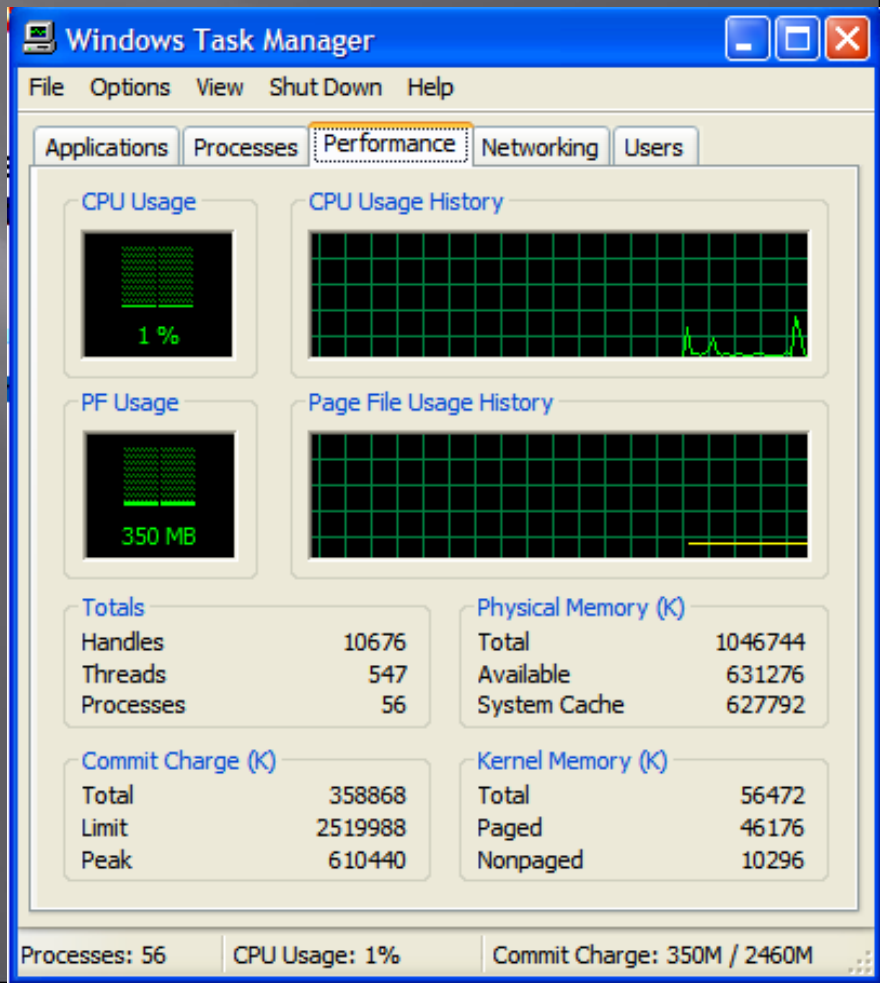
# Nastavljanje prioritet

- Osnovna prioriteta (base priority class) je interno nastavljena v aplikaciji
- Administrator strežnika lahko prioriteto spremeni v
  - Normalno (0)
  - nizko(-2)
  - Pod normalno (-1)
  - Nad normalno (+1)
  - visoko (+2)
  - Realni čas(+15)
  - To uporabljamo previdno, saj lahko proces prevlada na strežniku



# Nadzor performans realnega časa

- Zavihek “Performance” prikazuje podatke o zasedenosti CPE in pomnilnika
  - Uporaba CPE
  - Oporaba strani datotek (page file use)
  - Ročice (handles)
  - Niti

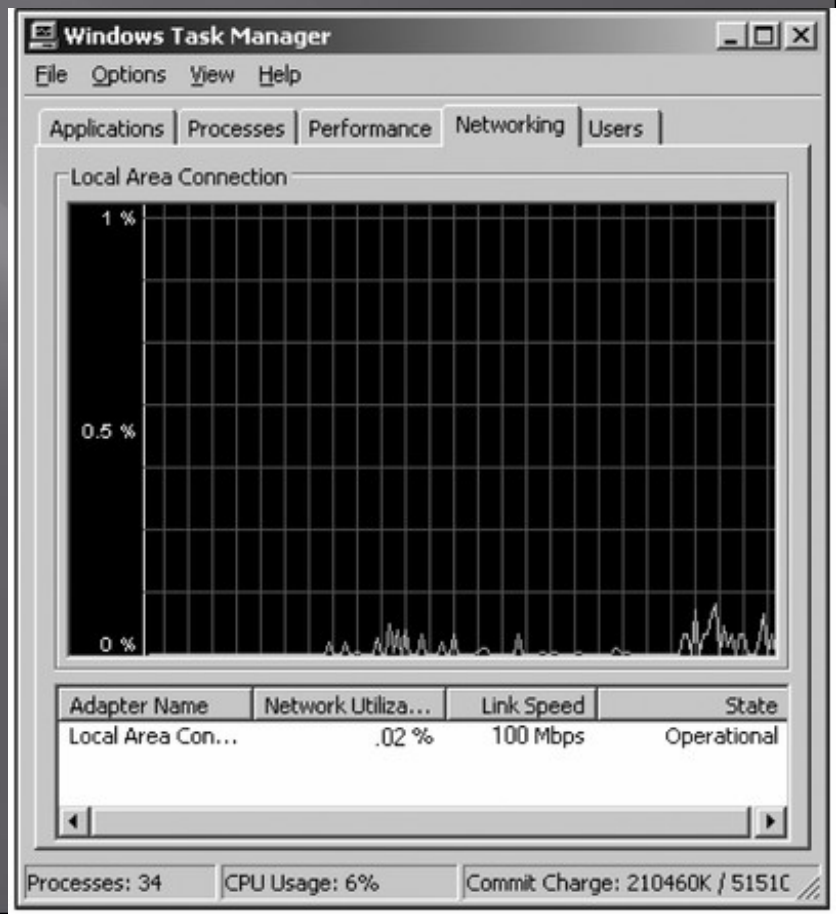


# Statistika o performansah

| Statistic | Description |
|---|---|
| Handles | The number of objects in use by all processes, such as open files |
| Threads | The number of code blocks in use, in which one program or process may be running one or more code blocks at a time |
| Processes | The number of processes that are active or sitting idle |
| Physical Memory Total | The amount of RAM installed in the computer |
| Physical Memory Available | The amount of RAM available to be used |
| System Cache | The amount of RAM used for file caching |
| Commit Charge Total | The size of virtual memory currently in use |
| Commit Charge Limit | The maximum virtual (disk) memory that can be allocated |
| Commit Charge Peak | The maximum virtual memory that has been used during the current Task Manager monitoring session |
| Kernel Memory Total | The amount of memory used by the operating system |
| Kernel Memory Paged | The amount of virtual memory used by the operating system |
| Kernel Memory Nonpaged | The amount of RAM memory used by the operating system |

# Nadzor omrežnih performans

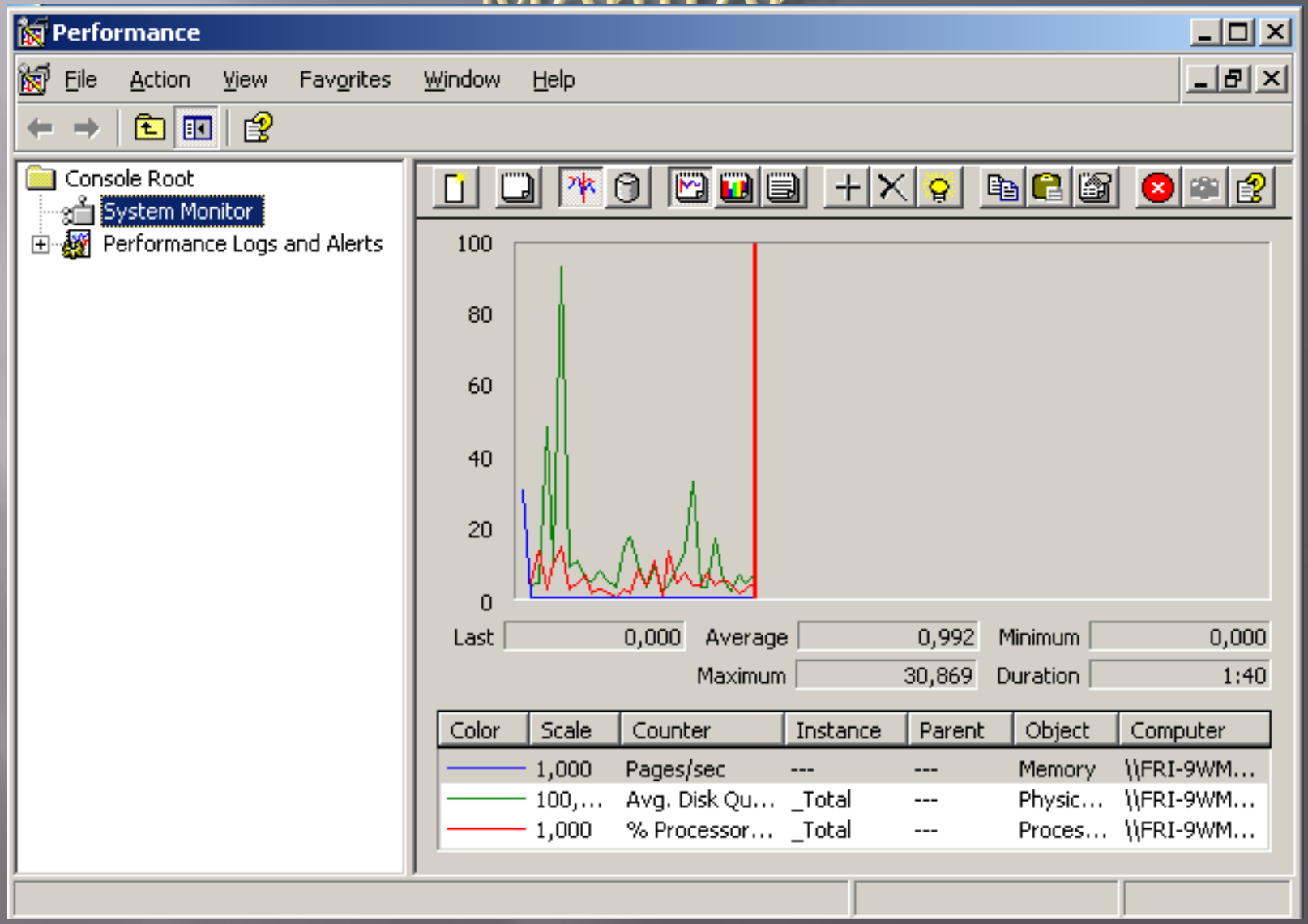
- Zavihek “Networking” omogoča nadzor omrežnih performans na vseh omrežnih karticah (NIC), nameščenih na strežniku
  - Prikazuje uporabo omrežja
  - Prikazuje omrežno performanso preko vsakega NIC adapterja
  - Tako lahko ugotovimo, če je s katerim od adapterjev problem
  - Lahko služitudi za opozarjanje o visoki obremenitvi omrežja(80% do 100%)



# Nadzor uporabnikov

- Zavihek “Users” podaja seznam uporabnikov, ki so v danem trenutku logirani
  - Uporabnika lahko odjavimo
    - Pred tem se zaprejo vse odprte datoteke
  - Uporabnika odvežemo, če se je povezava z njim “obesila”

# Uporaba orodja "System Monitor"

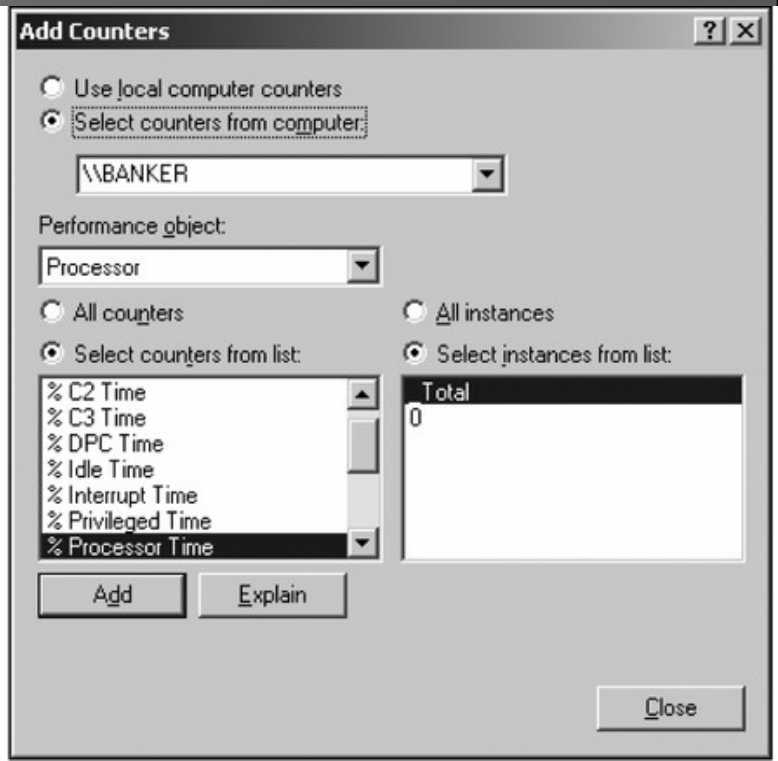


# Zajem sistemskih podatkov

- “System Monitor” uporabljamo za  nadzor komponent, kot je trdi disk, pomnilnik, procesorji, “disk caching”, sproženi procesi in “page files”
- Nadzorujemo objekte sistemskega monitorja
- Za vsak objekt imamo enega ali več števcev, ki jih lahko nadzorujemo
  - Števci imajo statusni podatek
- Če moramo nadzorovati več različnih elementov istega objektnega tipa, lahko instance asociiramo s števcem

# Primeri procesorskih števcev na sistemskem monitorju

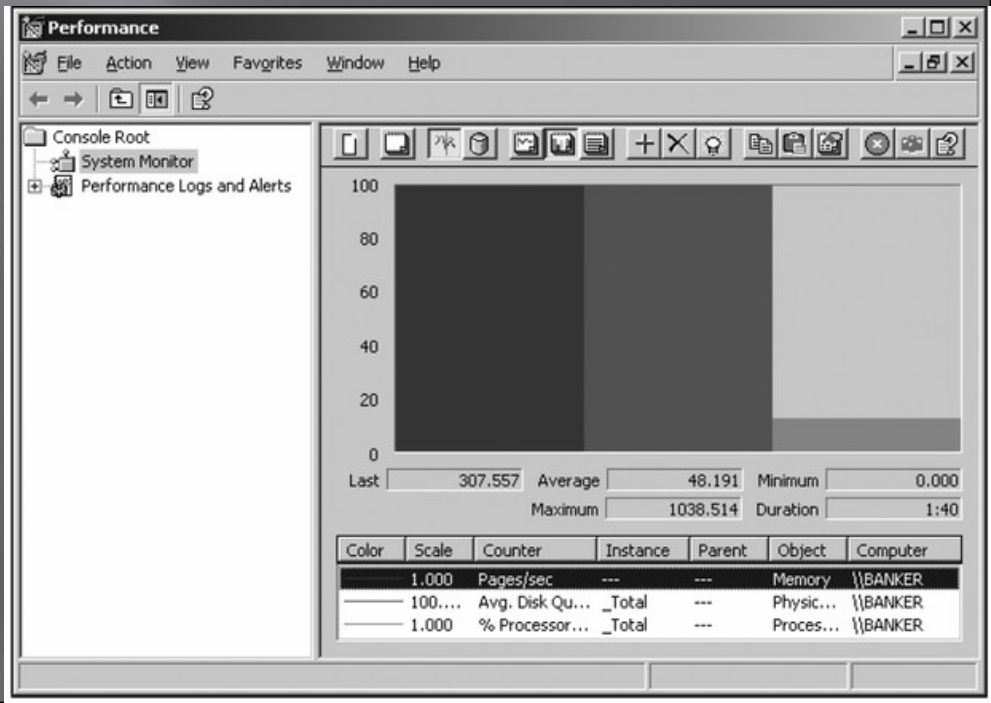
| Counter | Description |
|---|---|
| % DPC Time | Processor time used for deferred procedure calls, for example for hardware devices |
| % Interrupt Time | Time spent on hardware interrupts by the CPU |
| % Privileged Time | Time spent by the CPU for system activities in privileged mode, which is used for the operating system |
| % Processor Time | Time the CPU is busy on all non-idle activities |
| % User Time | Time spent by the CPU in user mode running software applications and system programs |
| Interrupts/sec | Number of device interrupts per second |




Pogovorno okno za dodajanje števcev

# Pogledi sistemskega monitorja

- Graph
  - Diagram poteka objekta
  - Črte v različnih barvah predstavljajo posamezne objekte
- Histogram
  - Palični diagrami (bar charts) kažejo posamezne objekte v različnih barvah
  - Na dnu zaslona so prikazani posamezni števci skupaj z legendo posameznih barv
- Report
  - Podatki na zaslonu so prikazani številčno in jih lahko izvozimo v poročilo



# Nadzor komponent sistema

- Pogosto nadzorujemo štiri objekte skupaj z njim dofeljenimi števci
  - Procesor
    - % Procesorskega časa kaže, ali je strežnik zelo obremenjen, sklepamo lahko, ali moramo zmanjšati obremenitev oziroma povečati zmožnosti
    - % prekinitvenega časa kaže, da imamo morda problem aparaturne narave
    - Interrupts/sec lahko opozarja, da je omrežni promet pretiran
    - Dolžina čakalne vrste (processor queue length) lahko nakazuje, da moramo obremenitev procesorja porazdeliti
  - Pomnilnik
  - Disk
  - Omrežni vmesnik

# Primeri objektov in števcev za nadzor sistema

| Object | Counters |
|---|---|
| Processor | % Processor Time—Percentage of time for threads to process<br>% Privileged Time—Time spent by the CPU for system activities in privileged mode<br>% User Time—Percentage of time spent processing user threads |
| Memory | Available Bytes—Physical memory currently available for use<br>Committed Bytes—Amount of virtual memory currently being used<br>Pages/Sec—Number of hard page faults per second |
| Physical Disk | % Disk Time—Amount of time the disk spends working<br>Avg. Disk Bytes/Transfer—Average number of bytes transferred between memory and disk during read and write operations<br>Disk Bytes/Sec—The speed at which bytes are transferred<br>Current Disk Queue Length—Number of requests waiting to be processed |
| Network Interface | Bytes Total/Sec—As measured across the NIC, number of bytes sent and received per second |

# Povzetek

- Za dobro razumevanje strežnikov na našem omrežju in tipične performanse omrežja uporabljamo nadzor sistema in omrežja
- Orodje “Computer Management” omogoča nadzor sistemskih servisov in ugotavljanje, ali je pri tem kaj problemov
  - Servis ponovno sprožimo
  - Preverimo odvisnosti
- Aplikacije, procese, performanse sistema in omrežja ter logirane uporabnike nadzorujemo z orodjem “Task Manager”
  - Problematično aplikacijo ali proces ustavimo
  - Odjavimo “obešene” povezave uporabnikov
- Vse tipe sistemskih im mrežnih aktivnosti nadzorujemo z orodjem “System Monitor”
  - Prikaz lahko prilagodimo, podatke lahko shranimo v datoteko

# Povzetek

- Zapis performans omogoča zajemanje in shranjevanje sistemskih podatkov v določenih trenutkih ali intervalih
- Podatke o performansah mreže zbiramo z orodjem “Network Monitor”, ki ga namestimo skupaj z gonilnikom “Network Monitor driver”
- Servis SNMP omogoča omrežnim agentom zbiranje mrežnih performančnih podatkov, kar lahko nato uporabljajo programi za upravljanje mreže
  - Upravlja in konfigurira določene omrežne naprave