Šola prihodnosti Maribor

Vzpostavitev Aktivnega imenika na šoli

Marko Zaletel
MSP, MCTS
Šola prihodosti Maribor
marko.zaletel@sola-prihodnosti.si

Potek delavnice

- Enodnevna
- Krajši odmori
- Postavitev produkcijskega okolja Šolski center Velenje – spremljanje vzpostavitve na projektorju
- Udeleženci hkrati postavljajo lastna okolja na svoji opremi
- Vprašanja postavljajte sproti ☺

Agenda

- Namestitev Windows Server 2008 R2 s SP1
- Nekaj o šolskih omrežjih
- Nekaj teorije na temo AD
- Zbiranje informacij, potrebnih za vzpostavitev AD
- Namestitev vloge AD DS in DNS
- Konfiguracija lokalnega NTP strežnika
- Organizacijske enote, uporabniki, skupine
- Pridružitev računalnikov v domeno
- Skupinske politike (Group Policy – GP)
- Deljenje virov (omrežni pogoni, tiskalniki)

Šola prihodnosti Maribor

Namestitev Windows Server 2008 R2 s SP1

Namestitev strežnika

- Windows Server 2008 R2 s SP1

Minimalne zahteve:

Component	Requirement
Processor	Minimum: 1.4 GHz (x64 processor) Note: An Intel Itanium 2 processor is required for Windows Server 2008 R2 for Itanium-Based Systems
Memory	Minimum: 512 MB RAM Maximum: 8 GB (Foundation) or 32 GB (Standard) or 2 TB (Enterprise, Datacenter, and Itanium-Based Systems)
Disk Space Requirements	Minimum: 32 GB or greater Note: Computers with more than 16 GB of RAM will require more disk space for paging, hibernation, and dump files
Display	Super VGA (800 × 600) or higher resolution monitor
Other	DVD Drive, Keyboard and Microsoft Mouse (or compatible pointing device), Internet access (fees may apply)

Pregled Windows Server

- Ime računalnika
- Konfiguracija TCP/IP
  - Konfiguracija IPv4
  - WAN: DHCP (ne v produkciji)
  - LAN: 172.0.0.1/24
- „Disable“ IE ESC (ne v produkciji)
- (Namestitev AV)
- (Windows Update)
- Server Manager
- Roles
- Features
  - Omogočimo Telnet client (in Windows Backup)
- Windows PowerShell in cmd.exe

Šola prihodnosti Maribor

Šolsko omrežje

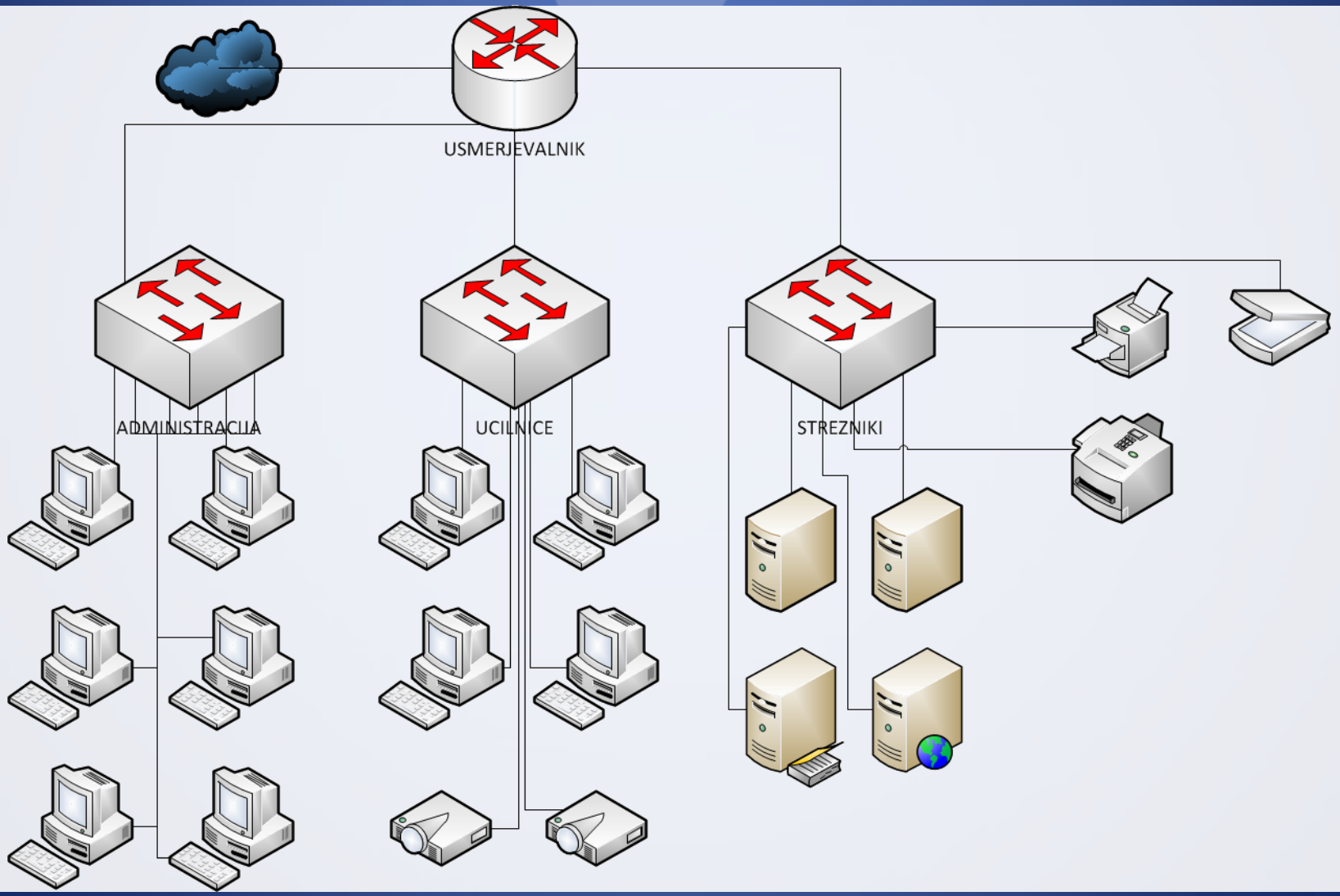
Šolsko omrežje

- Povezavo praviloma zagotavlja ARNES
- ARNES priporočila
  - Hitrost:
    - Videokonference (10/10Mbps+)
    - Lastni javni strežnik (x/10Mbps+)
    - Manjše organizacije (x/5Mbps+)
    - Večje organizacije (x/10Mbps+)
    - Optika 100Mbps+ (1Gbps optimalno)
    - Razmerje hitrost-kvaliteta/cena
  - Priporoča delitev omrežja na Omrežje za učence in Omrežje za zaposlene
  - Javni IP naslovi
  - Onemogočen DHCP?

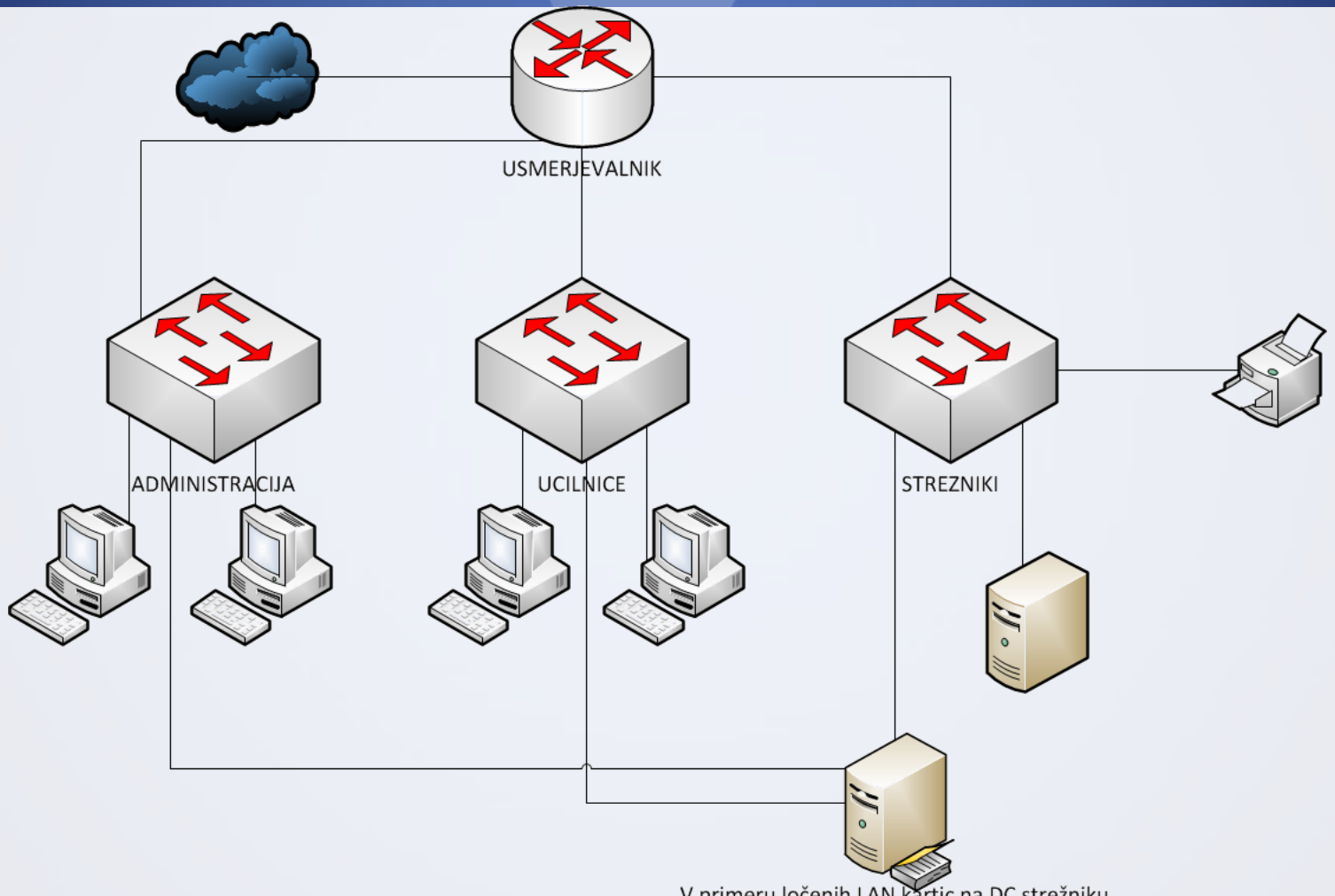
Šolsko omrežje II

- Lokalno omrežje Ethernet 100Mbps (1Gbps)
- Omrežje razdeljeno na:
  - Administrativni segment
  - Pedagoški segment
  - Strežniški segment
  - (management, eduroam, multimedija, itd.)
- Javni IP naslovi na odjemalcih
- (IPv6)
- Omogočen DHCP
- Pravilno nastavljeni filtri
- 802.1x, NAP

Šolsko omrežje III



Šolsko omrežje IV



Omrežna oprema

- Večje organizacije lastni usmerjevalnik?
  - Strežnik z OS Vyatta (http://www.vyatta.com/)
- Kupujte opremo skladno s priporočili ARNES:
  - http://aai.arnes.si/eduroam/Tehnicna_dolocila_dostopovne_tocke_20110606.odt
  - http://aai.arnes.si/eduroam/Tehnicna_dolocila_stikala_20060927.doc
- Za lokalno omrežje razmislite o nakupu cenejših stikal (HP, Dell, Cisco)
  - Dell PowerConnect 62xx
  - HP Procurve
  - Cisco SB 300
  - **Pred nakupom preverite tehnične lastnosti in dobro premislite kaj potrebujete!**

Šola prihodnosti Maribor

Nekaj teorije AD

Uporabniška identiteta

- Predstavlja organizacijo *(ime.priimek@domena.tld)*
- Uporabniška imena oblikovana po enotni šabloni *(ime.priimek@domena.tld, imepXXXX@domena.tld, itn.)*
- Transparentnost uporabniških računov (en uporabniški račun za vse sisteme)
- Močno geslo
- Opcijsko: enako uporabniško ime in elektronski naslov
- Opcijsko: podpora za Single Sign-On (SSO)

Realnost

- V realni situaciji bi za takšno implementacijo potrebovali bistveno več strežnikov (delavnica obravna organizacije, ki imajo vsaj nekaj 10 računalnikov in uporabnikov)
- Vsak IS je potrebno skrbno načrtovati, zagotoviti redundanco in „load balancing“ ključnih storitev

Namestitev strežnika

- Windows Server 2008 R2

Minimalne zahteve:

Component	Requirement
Processor	Minimum: 1.4 GHz (x64 processor) Note: An Intel Itanium 2 processor is required for Windows Server 2008 R2 for Itanium-Based Systems
Memory	Minimum: 512 MB RAM Maximum: 8 GB (Foundation) or 32 GB (Standard) or 2 TB (Enterprise, Datacenter, and Itanium-Based Systems)
Disk Space Requirements	Minimum: 32 GB or greater Note: Computers with more than 16 GB of RAM will require more disk space for paging, hibernation, and dump files
Display	Super VGA (800 × 600) or higher resolution monitor
Other	DVD Drive, Keyboard and Microsoft Mouse (or compatible pointing device), Internet access (fees may apply)

Aktivni imenik

- Microsoftova izvedba protokola LDAP, ki skrbi za poizvedovanje in urejanje podatkov v imeniških storitvah, preko TCP/IP protokola
- Skupek logično in hierarhično urejenih objektov z atributi
- Objekti so lahko uporabniki, računalniki, tiskalniki, Organizacijske enote, skupine uporabnikov, prostori, itn.
- Skrbi za centralno avtentikacijo in avtorizacijo uporabnikov v organizaciji
- Je predpogoj za delovanje večine ključnih storitev v organizaciji (WDS, NPS, WSUS...)

Nekaj pojmov

- Domain Controller (DC) - strežnik, na katerem se hrani baza Aktivnega imenika
- AD Forest – „collection of Trees“
- Tree – „collection of one or more domains“
- AD Sites – geografska lokacija IS. AD Sites se deli na podomrežja (subnets). Na podlagi AD Sites se lahko nastavlja GP
- Group Policy (GP) – skupek pravil, ki urejajo okolje uporabnika in računalnika (nastavitve, omejitve)
- Organanizacijska enota (OU) – zagotavlja logično in hierarhično razporeditev AD objektov znotraj AD. Na nivoju OU se lahko nastavlja GP, delegacija upravljanja, itn. OU naj bi ponazarjal realno organizacijsko strukturo organizacije.

AD Sistemske zahteve

- NTFS datotečni sistem z dovolj prostora
- Uporabniško ime in geslo administratorja
- Mrežni vmesnik
- Ročno nastavljen TCP/IP
- Mrežna povezljivost
- Delujoč DNS strežnik (lahko se namesti tudi med namestitvijo AD DS)
- Ime domene

Delovanje AD

- Za normalno delovanje AD sta ključna DNS strežnik in sinhronizacija časa
- Vse poizvedbe po Aktivnem imeniku (priključitev računalnika v domeno, prijava uporabnika, dostop do skupnih rab) se vršijo preko FQDN odjemalcev in strežnikov.
- Primer: Če DNS zapisi niso pravilni, se lahko določen računalnik preslika v napačen IP naslov.

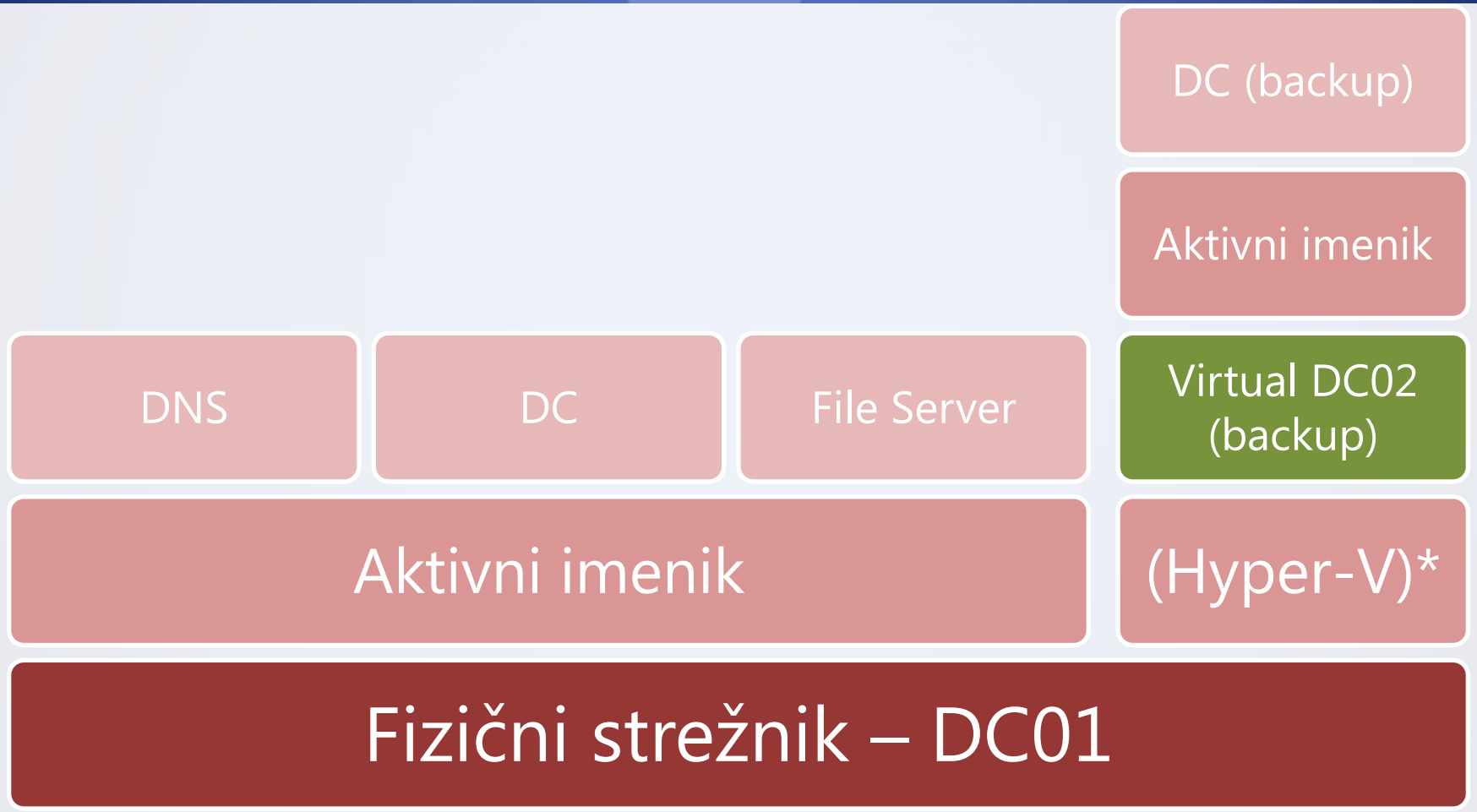
Šola prihodnosti Maribor

Zbiranje informacij, potrebnih za vzpostavitev AD

Pomembne informacije

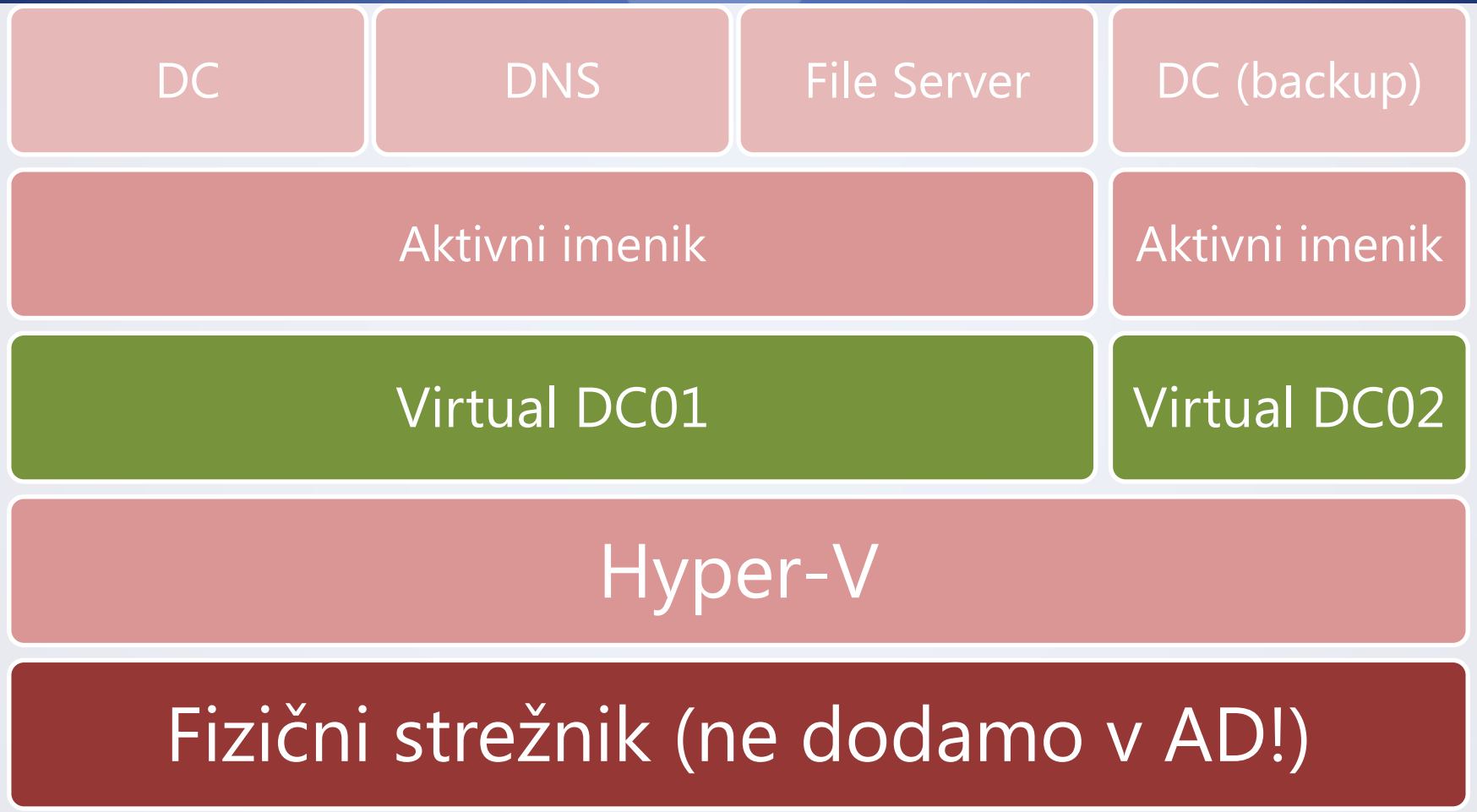
- Velikost organizacije
  - Osnovne šole:
    - Domenske storitve se uporabljajo delno (eno uporabniško ime za vse računalnike) – dovolj en strežnik in en DC/DNS/File server
    - Domenske storitve uporabljajo tudi zaposleni – če je možno glede na finance dva strežnika DC/DNS/File server
  - Srednje šole, šolski centri, (večje OŠ):
    - Domenske storitve se uporabljajo delno (eno uporabniško ime za vse računalnike) – dovolj en strežnik in en DC/DNS/File server
    - Domenske storitve uporabljajo tudi zaposleni – če je možno glede na finance dva strežnika DC/DNS/File server
    - Polna uporaba domenskih storitev – obvezno dva strežnika DC/DNS/File server
    - Oddaljene lokacije s slabimi povezavami - lastne DC/DNS/File server – pomembna segmentacija omrežja zaradi AD Sites!
- Shema omrežja
  - Segmentacija – CIDR, VLSM
  - Ugotoviti, na katerih segmentih se bodo uporabljale domenske storitve
    - V primeru enega segmenta strežnik(i) v istem segmentu
    - V primeru več segmentov ločen segment za strežnik(e)
- Požarni zid
  - Seznam omrežnih vrat: http://technet.microsoft.com/en-us/library/dd772723(WS.10).aspx
  - ali dovoliti ves promet med uporabniški segmenti in DC strežniki ter obratno
- Redundanca in „load-balancing“ / finance
  - Če je le možno zagotoviti podvojene storitve DC/DNS/File server

Določimo arhitekturo AD – majhna organizacija



* Ni uradno podprto

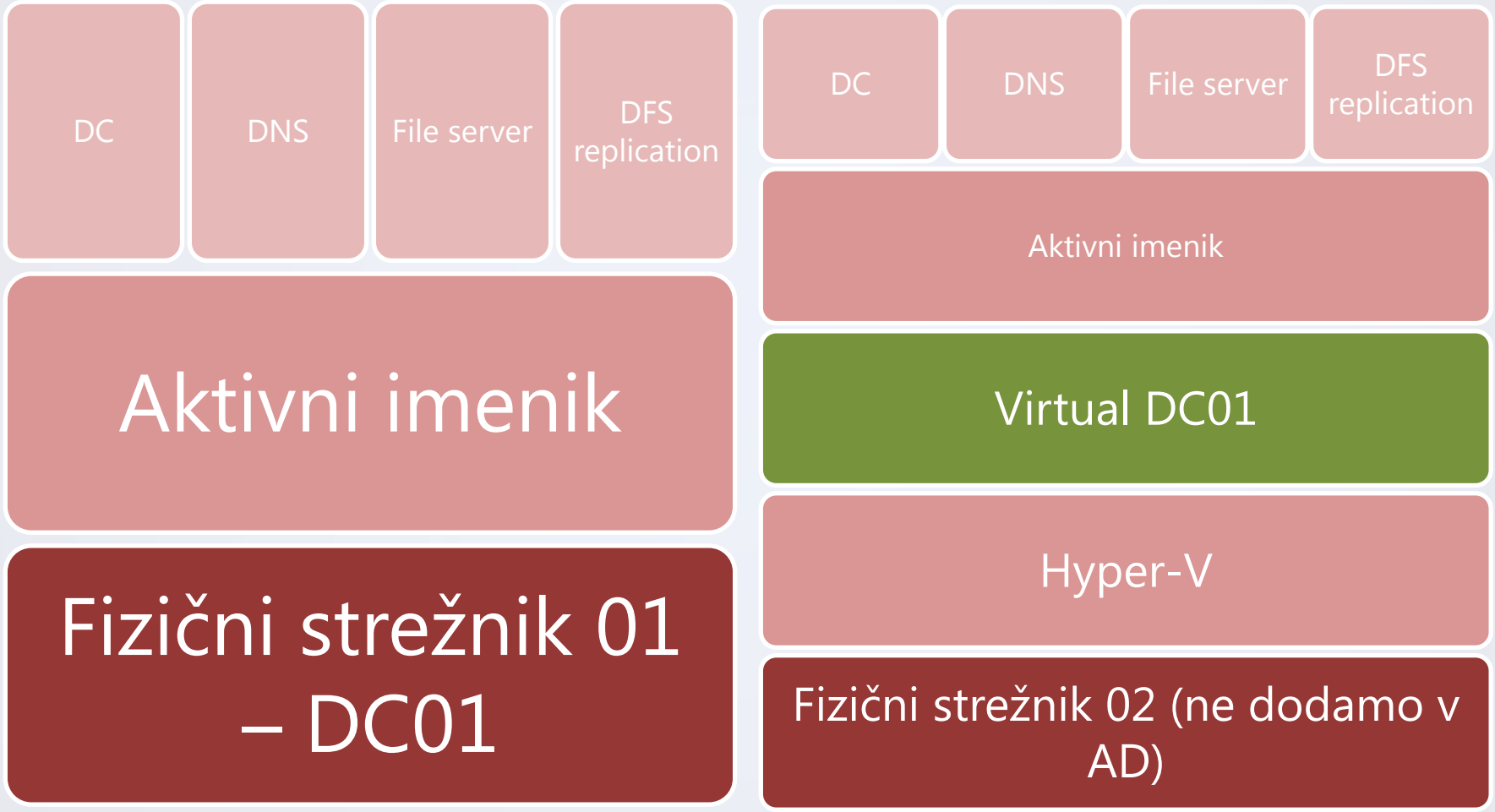
Določimo arhitekturo AD – majhna organizacija II



V primeru zmogljivega fizičnega strežnika in virtualizacije DC

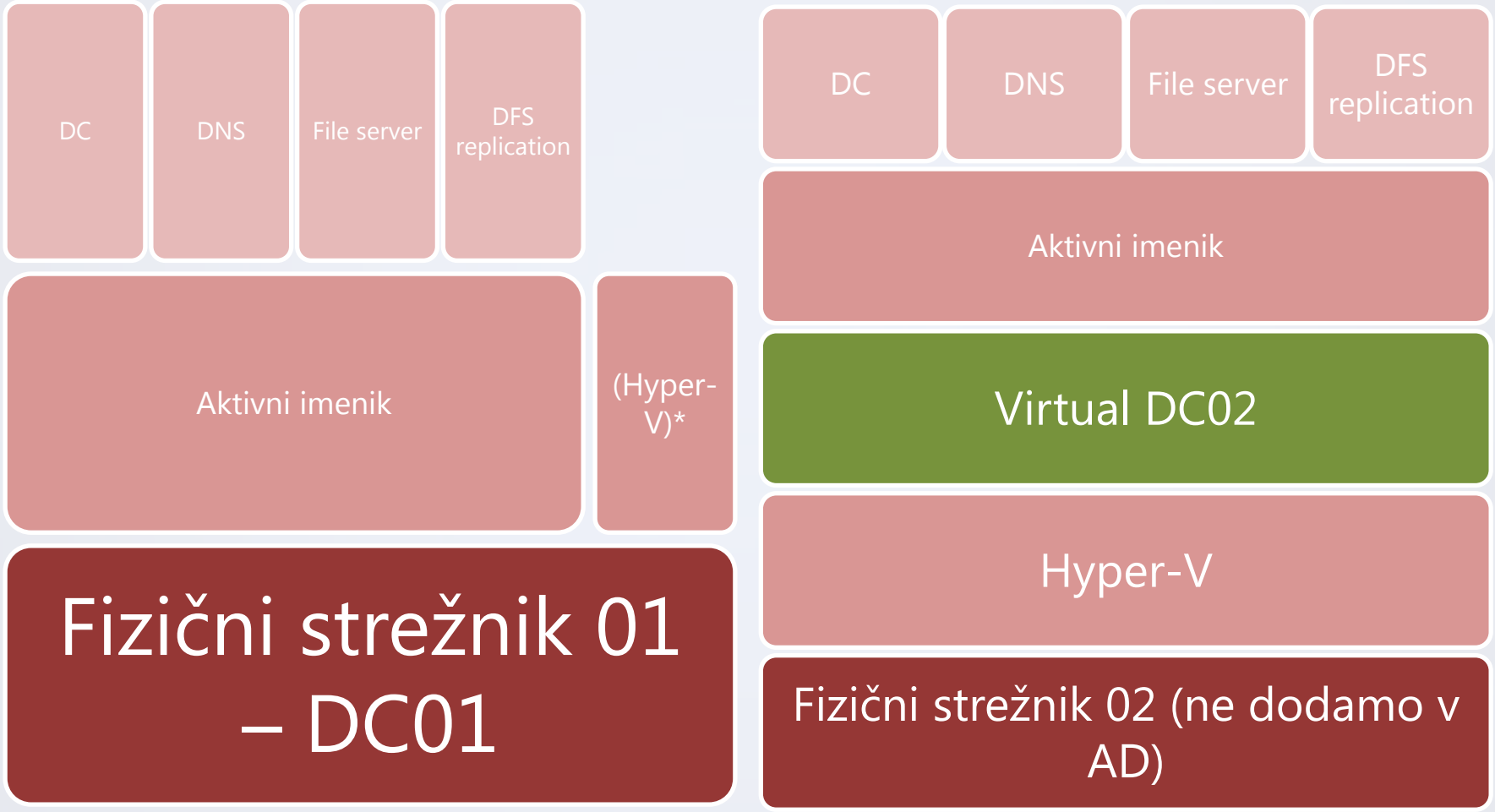
Določimo arhitekturo AD – večja organizacija

Določimo arhitekturo AD – večja organizacija II



http://blogs.dirteam.com/blogs/paulbergson/archive/2010/07/09/changing-the-weight-a

Določimo arhitekturo AD – večja organizacija – „hibrid“

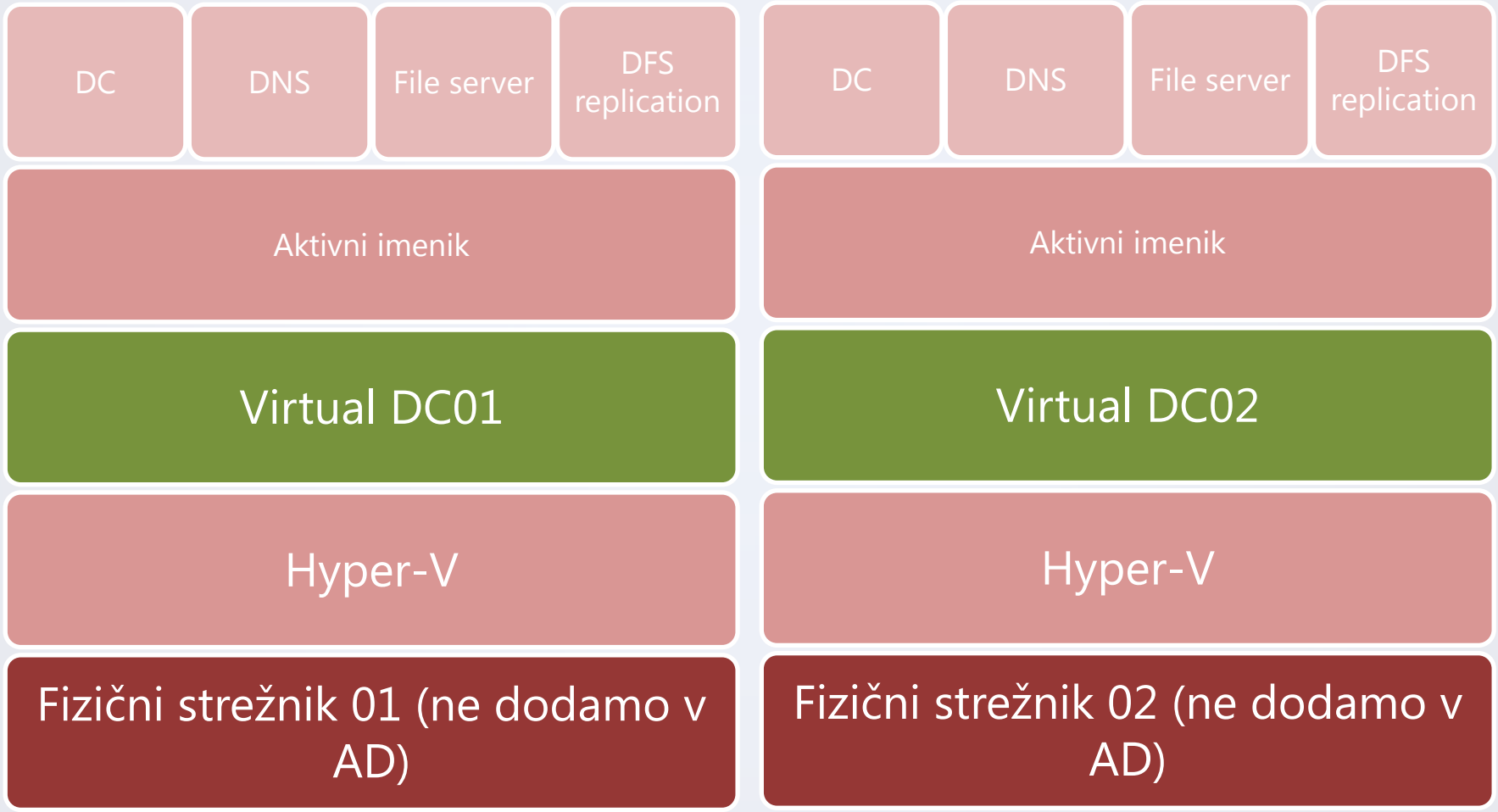


- * Ni uradno podprto
- DC „priority“

Določimo arhitekturo AD – večja organizacija – „hibrid“ II

* Ni uradno podprto

Določimo arhitekturo AD – večja organizacija – idealno



Kdaj virtualizirati/kdaj ne?

- Virtualiziramo, če je le mogoče!
- Virtualiziramo na ustrezni strojni opremi
  - Hitri diski 10000rpm+
  - RAID1/RAID10 polja
  - Dovolj RAM-a in procesorske moči
  - x64 arhitektura
- Izogibamo se uporabi dinamičnih virtualnih diskov v produkciji
- (Uporabljamo dinamične virtualne diske na manj zahtevnih virtualnih strežnikih)
- Za bolj obremenjene virtualne strežnike (npr. DC, File Server) uporabljamo statične virtualne diske na hitrih (RAID10) diskovnih poljih, ali virtualnemu strežniku dodelimo direktno fizični disk
- Ločene omrežne kartice za bolj obremenjene virtualne strežnike in ločena za upravljanje fizičnega strežnika

http://virtualisationandmanagement.wordpress.com/2011/03/

Pomembne informacije II

- Določiti AD domeno
  - Naj bo lokalna in ne internetna
  - domena.local
  - Uporabniška imena še vseeno lahko uporabljajo internetne domene (ime.priimek@domena.tld)
- Določiti pravila poimenovanj strežnikov, računalnikov, odjemalcev, tiskalnikov, itd.
  - Strežniki: [ORG prefix]-[vloga][zap. št]
    - SCS-DCSRV01, SCS-DCSRV02, SCS-WEBSRV01, itd.
  - Odjemalci: [prefix]-[št. stavbe]-[št. prostor]-[št. Odjemalca v prostoru]
    - PC-00-08-01, PC-01-12-21, itd.
  - Tiskalniki: [prefix]-[št. stavbe]-[št. prostor]-[št. Odjemalca v prostoru]
    - HPOJ-00-08-01, XRX-01-21-01, HPLJ-00-08-02, itd.
  - Maks. dolžina 15 znakov (NetBIOS)
  - Določiti in preveriti mejne vrednosti
    - Če imamo do 9 lokacij, potem je lahko št.stavbe enomestna
    - Če imamo do 100 prostorov, potem je št.prostora vedno trimestna
    - Določimo maks. število naprav, ki jih je lahko v enem prostoru na celi šoli – št.odjemalcev v VSEH prostorih tako zavzema toliko mestno število, z vodilnimi ničlami (če imamo v rač. učilnici 20 računalnikov, potem bo tudi v zbornici z enim računalnikom št.odjemalcev predstavljajo dvomestno število, z vodilnimi ničlami)
  - **OD PRAVIL POIMENOVANJ NIKOLI NE ODSTOPAMO!**

Pomembne informacije III

- Definiramo politiko gesel, oblike uporabniških imen
  - Zaposleni: ime.priimek@scs.si, dijaki: ime.priimek@dijak.scs.si
  - ali VSI ime.priimek@scs.si
  - **Od oblike uporabniških imen ne odstopamo!**
- Določiti organizacijsko strukturo AD (organizacije) in jo spoštovati
- Definirati AD skupine in jih uporabljati pri dodeljevanju privilegijev
- Pripraviti postopke za množični uvoz uporabnikov, ročno dodajanje in urejanje uporabnikov, ponastavljanje gesel
- Licence

Šola prihodnosti Maribor

Namestitev vloge AD DS in DNS

Storitve Aktivnega imenika

- FSMO vloge
  - Schema Master
  - Domain naming master
  - Infrastructure Master
  - Relative ID (RID) Master
  - PDC Emulator

  http://www.petri.co.il/understanding_fsmo_roles_in_ad.htm
- Global catalog

  http://technet.microsoft.com/en-us/library/cc728188(WS.10).aspx
- Group Policy
- DFS
- AD Certificate Services
- AD Federation Services

AD Sistemske zahteve

- NTFS datotečni sistem z dovolj prostora
- Uporabniško ime in geslo administratorja
- Mrežni vmesnik
- Ročno nastavljen TCP/IP
- Mrežna povezljivost
- Delujoč DNS strežnik (lahko se namesti tudi med namestitvijo AD DS)
- Ime domene

Namestitev AD

- Namestitev vloge AD DS
- Zagon čarovnika *dcpromo.exe*
  - Nova domena v novem gozdu
  - Ime domene: *domena.local*
  - AD „recovery“ geslo!
- Ponovni zagon – prva domenska prijava
  - Uporabnik: *domena\administrator*
- Preverimo lastnike GC in FSMO vlog
- Sprehod po orodjih AD

Nekaj pojmov

- Domain Controller (DC) - strežnik, na katerem se hrani baza Aktivnega imenika
- AD Forest – „collection of Trees“
- Tree – „collection of one or more domains“
- AD Sites – geografska lokacija IS. AD Sites se deli na podomrežja (subnets). Na podlagi AD Sites se lahko nastavlja GP
- Group Policy (GP) – skupek pravil, ki urejajo okolje uporabnika in računalnika (nastavitve, omejitve)
- Organanizacijska enota (OU) – zagotavlja logično in hierarhično razporeditev AD objektov znotraj AD. Na nivoju OU se lahko nastavlja GP, delegacija upravljanja, itn. OU naj bi ponazarjal realno organizacijsko strukturo organizacije.

Šola prihodnosti Maribor

Konfiguracija lokalnega NTP strežnika

Konfiguracija NTP strežnika

- Opisano v:

http://support.microsoft.com/kb/816042

- Orodje za konfiguracijo:

http://go.microsoft.com/?linkid=9729248

Šola prihodnosti Maribor

Ureditev Aktivnega imenika

Izdelava organizacijske strukture organizacije v AD

- AD uredimo logično in hierarhično
- Strukturo urejamo s pomočjo objektov Organizacijska enota (OU)
- OU-ji so zelo pomembni, ker se na njih vežejo Group Policy objekti (GPO), ki določajo nastavitve in omejitve uporabnikov in računalnikov
- „Recept“:
  - ORG[NN]
    - Computers
      - Servers
      - Computers
    - Users
      - [oddelki]
    - Groups
      - Users
      - Computers

Korenska mapa AD

- Vse nastavitve in profile AD je pametno hraniti na drugem disku, nekako hierarhično urejeno
- Na D: particiji uredimo strukturo map za nastavitve in profile AD
  - D:\AD
    - HomeDirs
    - Scripts
    - Shares
    - Settings
    - Programs

Šola prihodnosti Maribor

Uporabniški računi, skupine

Transparentnost uporabniških računov

- V aktivnem imeniku smo nastavili domeno domena.local, organizacija pa si lasti javno internetno domeno domena.si. Ker želimo, da bodo uporabniška imena enaka elektronskim naslovom uporabnikov, moramo nastaviti UPN Suffix-e.
- Nastavimo v Active Directory Domains and Trusts

Izdelava testnih uporabnikov in skupin

- Za vsak oddelek izdelamo najmanj enega testnega uporabnika po modelu:
  - Display name: Test [Oddelek]
  - Uporabnik: test.[oddelek] (brez šumnikov)
  - Geslo: password@1
- Za vsak oddelek izdelamo tudi skupino uporabnikov po modelu:
  - Group name: [Oddelek]
  - Group scope: Global
  - Group type: Security

Vrste profilov

- Lokalni – profil hranjen na lokalnem rač.
- „Mandatory“ – profil hranjen na lokalnem rač., ob odjavi se spremembe profila zbrišejo
- (Domenski) – prijava se vrši na strežniku, profil hranjen na lokalnem rač. (razen v primeru folder redirection)
- Roaming (domenski) – prijava se vrši na strežniku, profil hranjen na strežniku
- Začasni – če se domenski ali roaming ne uspe naložiti, se ustvari začasni profil. Ob odjavi uporabnik zgubi podatke

Folder redirection

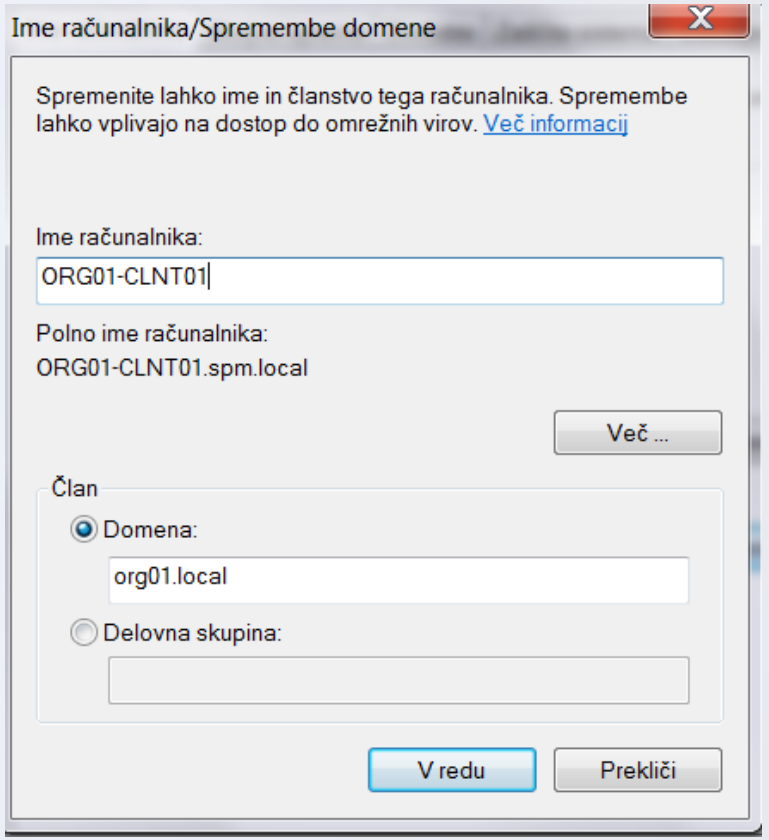
- S Folder redirection pravili dosežemo, da je uporabnikov profil hranjen na mreži
- Gre za kombinacijo Skupnih rab, NTFS in „Share“ privilegijev ter GP politike
- Urejamo znotraj Group Policy Management Console
- Nastaviti tudi v lastnostih uporabnika (*Profile -> Home Folder ->Connect*)
- Uporabnikom vseh oddelkov nastavimo Folder redirection in preko testnega računa preverimo delovanje

Šola prihodnosti Maribor

Pridružitev računalnikov v domeno

Pridružitev odjemalca v domeno organizacije

- Da uporabnik lahko koristi prednosti AD, mora biti njegov računalnik pridružen domeni.
- To storimo preko menija *Nadzorna plošča\Sistem in varnost\Sistem*, preko povezave *Spremeni nastavitve*, v kategoriji *Nastavitve računalnika, domene in delavne skupine*.
- Vpišemo FQDN domene
- Za pridružitev v domeno potrebujemo podatke uporabnika, ki ima dodeljene privilegije za priključitev računalnika v domeno.



- Pridružen računalnik dodamo v pravo OU

Šola prihodnosti Maribor

Skupinske politike (Group Policy – GP)

Group Policy (GP)

- S skupinsko politiko (GP) določamo omejitve in nastavitve računalnikov in uporabniških profilov
- GP objekte (GPO) po navadi vežemo na OU. GPO se uveljavlja na vseh objektih AD, ki so znotraj tega OU. GPO se podeduje tudi na vse podrejene OU-je in njegove AD objekte
- GPO lahko vežemo na računalnik ali na uporabika. Če vežemo na računalnik, se GPO uveljavi ob zagonu računalnika, če vežemo na uporabnika, se uveljavi ob prijavi uporabnika.
- Možno je filtriranje uveljavitev GPO preko privilegijev in WMI filtrov.
- GPO ločujemo na politike in na preference. Politike uporabniki ne morejo zaobiti, preference pa seveda lahko. Tako se prvi po navadi uporabljajo za omejitve, druge pa za nastavitve.
- Politika se ne nujno uveljavi ob prvem zagonu računalnika oz. prvi prijavi uporabnika

Šola prihodnosti Maribor

Deljenje virov (omrežni pogoni, tiskalniki)

Skupne rabe datotek

- Uporabljamo jih vsi
  - Doma za deljenje datotek med računalniki
  - V večjih sistemih za delovanje AD, Folder redirection, omrežni pogoni delavnih skupin orgnaizacije, itn.
- Nastavimo na nivoju mape ali diska, preko menija *Lastnosti -> Skupna raba*
- Oblika omrežne poti: *[ime rač.]**[ime sk. rabe]*
- Znak $ na koncu imena skrije skupno rabo

NTFS in Share privilegiji

- Za dokumente, do katerih bodo uporabniki dostopali preko mreže, moramo poleg NTFS privilegijev, nastaviti tudi „Share“ privilegije
- Naj velja pravilo, da na vsaki točki, kjer želimo spreminjati privilegije, prekinemo podedovanje NTFS privilegijev iz nadrejenega elementa
- Pazimo, da uporabniku ne damo preveč privilegijev (brisanje korenske mape določene skupne rabe, pravica spreminjanja privilegijev)

Print Server

- Namestimo kot vlogo Windows Server
- Tiskalnike vežemo na GPO in preko Print Server Manager-ja nastavimo ali se naj določen tiskalnik namesti le računalnikom, na katerih se GPO tiskalnika uveljavi ali uporabnikom, pri katerih se GPO tiskalnika uveljavi, ali pa naj se tisklanik namesti v obeh primerih.
- Z GP preferencami lahko nameščanje tiskalnikov avtomatiziramo tudi preko GP.
- Če tiskalnik ni mrežni, mora biti seveda računalnik, na katerega je priklopljen tiskalnik, med tiskanjem vključen.

AD Troubleshooting

- dcdiag – testiranje delovanja storitev AD
- Konzola „Uveljavljene varnostne politike“ znotraj MMC
- Repladmin – testiranje dleovanja replikacije (v primeru večih DC-jev)
- Eventvwr – pregled dnevnikov odjemalca (in strežnika)
- GP Modeling in GP Results znotraj GP Management Console
- Nslookup – preverimo ali se DNS strežnik domene odziva in preverimo ali vrača prave IP naslove za AD domeno in DC strežnike
- Ping – preverimo ali so DC strežniki dosegljivi (če niso, je lahko problem v kakšnem požarnem zidu)

Šola prihodnosti Maribor

Vprašanja?

Šola prihodnosti Maribor

Hvala za pozornost!

marko.zaletel@sola-prihodnosti.si