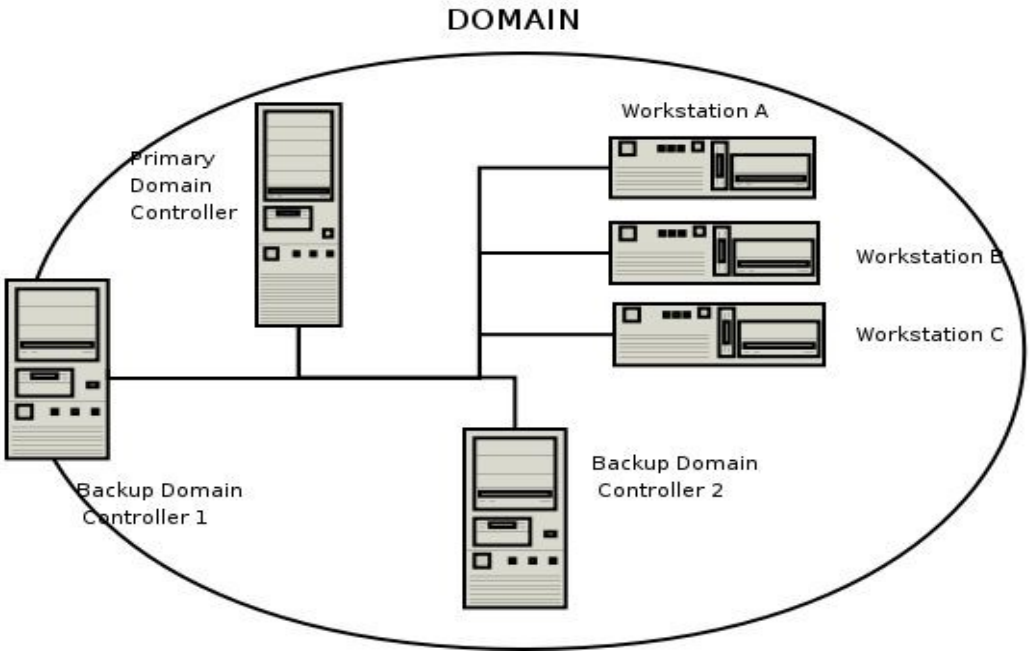
Windows'i võrgu domeenid



Windows'i võrgu domeen on loogiliselt ühte kuuluv Windows operatsioonisüsteemiga arvutite grupp, mis jagavad keskset andmebaasi. Jagatav andmebaas sisaldab domeeni kuuluvate kasutajate kontosid (igal kasutajal on unikaalne konto koos selle kontoga seotud õigustega) ja turvainformatsiooni domeenis olevate ressursside kohta. Domeeni keskne andmebaas asub arvutis, mida nimetatakse domeeni kontrolleriks (domain controller), tegemist on serveriga, mis haldab kõiki kasutaja ja domeeni vahelisi tegevusi, samuti võimaldab see domeenikeskset administreerimist ja turvahaldust. Ühte domeeni kuuluvad arvutid ei pruugi asuda füüsiliselt samas paigas – domeeni võivad kuuluda nii samas lokaalvõrgus olevad arvutid kui ka maailma eri paigus olevad arvutid kui leidub võimalus ühenduse saamiseks domeenikontrolleriga (tavaliselt kasutatakse sellisel juhul VPN'i).

Windows'i domeen erineb töögrupist selle poolest, et domeeni puhul on tegemist klient-server tüüpi mudeliga, töögrupp meenutab pigem aga klient-klient tüüpi mudelit. Töögruppi kuuluvad arvutid on iseseisvad – töögruppide liikmeid ei autendita. Samuti puuduvad töögrupis paljud domeenile omased turvakontrollid ja võimalused arvutite keskseks haldamiseks. Üldiselt loetakse, et üle 15 arvutiga töögruppi on ebamõistlikult rakse hallata ja sellisel juhul oleks juba parem kasutada domeeni.

Peamine andmevahetus nii töögruppides kui domeenis toimub SMB/SMB2 (Server Message Block) võrguprotokolli vahendusel. Tegemist on rakenduse taseme võrguprotokolliga, mida kasutatakse peamiselt sellistele ressurssidele nagu failid ja printerid jagatud juurdepääsu võimaldamiseks. Lühendi SMB puhul tuleb eristada protokolli ennast ja SMB teenuseid, mis töötavad selle protokolli põhiselt.

SAMBA

Samba on vabavaraline SMB/CIFS protokolli implementeering. Alates kolmandast versioonist on Samba võimeline pakkuma Windows'i faili- ja printerijagamisteenust ning seda saab liita Windows'i võrgudomeenile, kas domeenikontrollerina või domeeni liikmena. Samuti võib Samba olla osaks Active Directory domeenist. Samba töötab enamikul UNIX-laadsetel süsteemidel.
Domeenikontrollerina võimaldab Samba:

- Domeeni kasutajakontode tsentraalset haldamist – info kasutajate kohta võib olla samba enda kasutajate andmebaasis (PAM (Plugable Authentication Modules) abil on võimalik Samba ja Unixi/Linuxi kasutajate andmebaasi sünkroniseerituna hoida), LDAP serveris, Kerberos serveris, või mujal.
- Liikuvate kasutajaprofiilide haldus (Roaming User Profiles)
- UNIX/Linux masina kõvakettal olevaid katalooge välja jagada nagu tavalisi Windows'i jaoseid, koos sinna juurde kuuluva ligipääsukontrolliga.
- Lisada domeenis olevatele kasutajakontodele sisselogimise skripte, mille näol on tegemist tavaliste Windows'i käsureaskriptidega, mida hoitakse domeenikontrolleris ja käivitatakse masinas, millega kasutaja domeeni logib.
- Jagada domeenis printereid – seda võimalust kasutatakse tavaliselt koos CUPS (Common Unix Printing System) alamsüsteemiga.

Samba kasutajate andmebaas „smbpasswd“ asub vaikimisi koos Samba konfiguratsioonifailiga „smb.conf“ kaustas /etc/samba/
Peale konfiguratsioonifaili oma vajadustele vastavaks muutmist (täpsemaks infoks vaata näiteks: http://samba.netfirms.com/sambconf.htm) tuleb enne Windows'i masina domeeniliikmeks registreerimist luua masina konto (Samba machine account). Konto nimi peab vastama domeeni liikmeks registreeritava arvuti nimele ja lõppema märgiga $.
Windows XP operatsioonisüsteemiga arvuti liitmiseks domeeni tuleb:

1) valida My Computer, teha sellel hiirega paremklik ja kontekstimenüüst valida „properties“
2) valida sakk „Computer name“
3) Kontrollida üle, et arvutinimi vastab domeenikontrollerisse lisatud masina kontole.
4) Valiku „Member of:“ juures valida Domain ja sisestada domeeni nimi
5) Lõpuks küsitakse domeenikontrolleri administraatorkasutaja kasutajanime ja parooli

Active Directory

Installeerime Windows Server 2012 R2:

1) Seadistame operatsioonisüsteemi asukohamaaga seotud valikud
    1. Operatsioonisüsteemi keeleks Inglise keel
    2. Aja ja valuutaformaadiks: Eesti
    3. klaviatuuripaigutus: Eesti
    4. Vajutame „Next“
2) Vajutame „Install Now“, et alustada installeerimisprotseduuri
    1. Sisestame aktiveerimisvõtme
    2. Tühistame valiku „Automatically activate Windows when I'm online“
    3. Vajutame „Next“
3) Valime „Windows Server 2012 R2 (Server with a GUI)“
4) Nõustume litsentsitingimustega ja vajutame „Next“
5) Valime „Custon (advanced)“
6) Kuvataval ekraanil on võimalik valida operatsioonisüsteemi installeerimiseks partitsioon – või luua uus partitsioon, kui seda veel ei ole. Meie valime olemasoleva kettaseadme ja vajutame „Next“ (terve kettaseade formaaditakse kui üks partitsioon, millele installeeritakse operatsioonisüsteem).
7) Algab operatsioonisüsteemi installeerimine
8) Peale installeerimise lõppu tuleb määrata Administrator kasutaja salasõna.

Seadistame Windows 2012 Serveri ActiveDirectory domeeniserveriks

1) Peale installeerimise lõppu ja sisselogimist kuvatakse aken „Initial Configuration Tasks“
2) Valime “Configure Networking“
    1. Kontrollime üle võrguseaded.
    2. Seadistame liidese „Local Area Connection“. Paremklõps liidesel ja kontekstimenüüst

„Properties“. Eemaldame TCP/IPv6 protokolli. Valime TCP/IPv4 protokolli ja vajutame „properties“ nuppu. Määrame järgmised võrguseaded:

1. IP aadress: 192.168.0.1
2. Mask: 255.255.255.0
3. Gateway: 192.168.0.1
4. DNS server: 192.168.0.1

3) Valime „Provide Computer Name and domain“
    1. Seadistame arvuti nimeks „win2012server“
    2. Teeme masinale taaskäivituse
4) Installeerime serverile Active Directory domeeni teenuse – valime „Add roles and features“
    1. Valime „Role-based or feature-based installation“
    2. Valime masina, millele soovime uue rolli paigaldada.
    3. Valime Active Directory Domain Services.
    4. Peale installatsiooni lõppemist valime „Promote this server to domain controller“
5) Configureerime Active Directory domeeni
    1. Loome uue domeeni uues „metsas“ - valime „Create a new domain in a new forest“
    2. Anname uuele domeenile nime: osakond.firma.ee
    3. Valime Forest Functional leveliks: „Windows 2012“ ja Domain functional leveliks „Windows 2012“
    4. On soovitav, et peamine domeenikontroller käitub ka DNS serverina. Seega installeerime ka DNS serveri teenuse jättes valituks „DNS server“ ja vajutades „Next“
    5. Edasi võimaldatakse valida asukoht domeeniserveri andmebaasile, logidele ja süsteemijaosele. Jätame selle nagu on ning valime „Next“
    6. Sisestame domeeni Administrator kasutaja parooli
    7. Teeme masinale taaskäivituse

Domeeni kasutajate, seadmete ja jaoste haldamine

Domeeni objektide haldamiseks käivitame Active Directory Users and Computers konsooli. Start -> Administrative Tools -> Active Directory Users and Computers

Active Directory on hierarhiline ning koosneb objektidest (teatud objektid võivad paikneda teiste objektide sees). AD objektid võib jaotada kaheks:

- Ressurssidega seotud objektid Näiteks:
    - User– domeeniserveris olev kasutajakonto
    - Group – kasutajakontode grupp õiguste lihtsamaks haldamiseks
    - Computer – domeeniga liidetud tööjaam
    - Shared Folder – domeeni piires väljajagatud võrguketas või kataloog
    - Printer – domeeni piires väljajagatud võrguprinter
- AD hierarhiaga seotud objektid – nende objektide abil saab grupeerida teisi, loogiliselt ühte kuuluvadi objekte lihtsamaks haldamiseks.
    - Organizational Unit – organisatsiooniüksus on mõeldud teiste AD objektide koondamiseks loogilisteks rühmadeks. OU on ka väikseim AD jaotis, millega saab siduda eraldiseisva GroupPolicy.
    - Container Objects – põhimõtteliselt nagu OU-d aga on eelnevalt loodud (tagamaks tagurpidiühilduvust Windows NT-ga)
        - Builtin – vaikimisi olemasolevad AD kasutajagrupid
        - Computers – domeenis olevad tööjaamad
        - Domain Controllers – domeenikontrollerid
        - ForeignSecurityPrincipals – teiste domeenidega seotud turvaseaded
        - Users – Windows NT vaikimisi loodud kasutajakontod.

Loome domeeni kaks uut OU-d: „boss“ ja „alluvad“

OU loomiseks teeme paremklõpsu domeeninimel ja valime kontekstimenüüst: new -> Organizational Unit

Loome tehtud OU-de alla kaks uut kontot: „Mari Maasikas“ ja „Peeter Pirn“

Uue kasutajakonto loomiseks teeme paremklõpsu OU-l (või mõnel teisel konteineril) ja valime

kontekstimenüüst: new -> User

Installeerime domeeniserverile generic printeri ja jagame selle välja Peeter Pirnile, avaldame (publish) jagatud printeri AD-s

Start -> Control Panel -> Printers -> Add Printer -> Add a Local Printer -> Next

Valime: Generic -> Generic / Text Only - > Next

Jätame valituks „Share this printer ...“ ja vajutame „Next“ ja „Finish“

Teeme installeeritud printeril paremklõpsu ja valime kontekstimenüüst „Sharing“

Anname printerile nime, millega seda võrgus jagada näiteks „generic“

Märgime ära valiku „List in directory“ (avaldamiseks AD-s)

Saki „Security“ alt eemaldame „everyone“ ja lisame „Peeter Pirn“

Jagame domeeniserverist välja kataloogi c:\test kasutajale „Mari Maasikas“, avaldame jagatud kataloogi AD-s

Loome kataloogi c:\test

Teeme loodud kataloogil paremklõpsu ja valime „Share ...“

Valime „Advanced Sharing ...“ -> Share this folder

Vajutame Permissions, eemaldame „everyone“ ja lisame „Mari Maasikas“

Kataloogi avaldamiseks AD-s lisame AD-sse uue „shared folder“ objekti, mis viitab tehtud jaosele.

Group Policy AD domeenis

Group Policy haldamiseks käivitame Group Policy konsooli: Start->Administrative Tools->Group Policy Management

Loome uue Group Policy Object'i ja määrame selle kehtima Organization Unit'ile „Boss“

Paremklõps alajaotusel „Group Policy Objects“ kontekstimenüüst valik „new“

Anname GPO-le nime ja vajutame OK. Teeme uue GPO peal paremklõpsu ja valime „Edit“

Viime sisse soovitud muudatused.

Valime OU „boss“ teeme sellel paremklõpsu ja valime kontekstimenüüst „Link an Exsisting GPO“

Valime oma uue GPO ja tehes sellel hiirega paremklõpsu valime „Enforced“