Windows rendszeradminisztráció és Microsoft szerveralkalmazások támogatása

5. óra

Kocsis Gergely,
Supák Zoltán

2017.03.22.

Active Directory

Active Directory

Eredeti definíció: Active Directory Domain Services

Jelenlegi definíció: Hálózati erőforrások és azonosítók központosított elérésére és használatára szolgáló szolgáltatások (role-ok és feature-ök) gyűjteménye.

AD Role-ok

- AD Domain Services
  (felhasználók, számítógépek, policy-k)
- AD Certificate Services
  (szolgáltatás, kliens, szerver és felhasználó azonosítás)
- AD Federation Services
  (kiterjesztett erőforrás elérés)
- AD Rights Management Services
  (adatbiztonsági szolgáltatások)
- AD Lightweight Directory Services
  (tár és alkalmazás-specifikus adatok nem teljes AD igény esetén)

Active Directory

Történet:

Első bemutatás: 1999 Windows NT alapú felhasználó azonosítás kiváltására (NTDS).

Első megjelenés: Windows 2000 Server. Nem egyszerű felhasználói azonosítás, hanem valós címtárszolgáltatás

Windows Server 2008: Az AD innentől AD DS és megjelennek a további szolgáltatások

Feladatok:

Címtárszolgáltatás: LDAPv3 alapon
Authentikáció: Kerberos alapon
Névszolgáltatás: DNS alapon

Active Directory Domain Services

Felépítése:

Az AD (DS) objektumokból épül fel (erőforrás pl. nyomtató; szolgáltatás pl. e-mail; felhasználó pl. felhasználói fiók, csoport).

Egy objektum egy entitást ír le annak attribútumaival együtt.

Egyes objektumok más objektumokat tartalmazhatnak. Ezek a konténer objektumok.

Az objektumok azonosítására szolgál

- a distinguished name (megkülönböztetett név) – elérési út+név (változhat)
- objectGUID

Active Directory DS Séma

A séma tulajdonképpen **az AD tervrajza**. Definiálja,

- az adatok tárolására szolgáló objektumokat
- az objektumok szerkezetét előíró szabályokat
- az AD tartalmát és felépítését

A séma módosítása

Mivel a sémában leírtak az egész AD alapját képezik, a séma módosítása csak különleges körültekintés mellett ajánlott és komoly tervezést igényel.

Objektumot törölni nem lehet, csak deaktiválni.

Sémamódosítást csak a *Schema Administrator* végezhet

Active Directory DS Domain

A domain (tartomány) felhasználó, számítógép, csoport és egyéb objektumok logikai konténere

Replikáció: Az azonos tartományon belül dolgozó domain vezérlők (**D**omain **C**ontroller) bármelyikén végzett módosítás az összes többi vezérlőre *replikálódik*.

Adminisztráció: A domainen belül létrejön egy *Administrator* fiók, aki automatikusan tagja a szintén létrejövő *Domain Admins* csoportnak illetve a helyi *Administrators* csoportoknak

Autentikáció: A domain userek és gépek azonosításra kerülnek

Autorizáció: A domain szintjén egy magasabb szintű jogosultságkezelést valósíthatunk meg (a lokális mellett!)

Active Directory DS OU

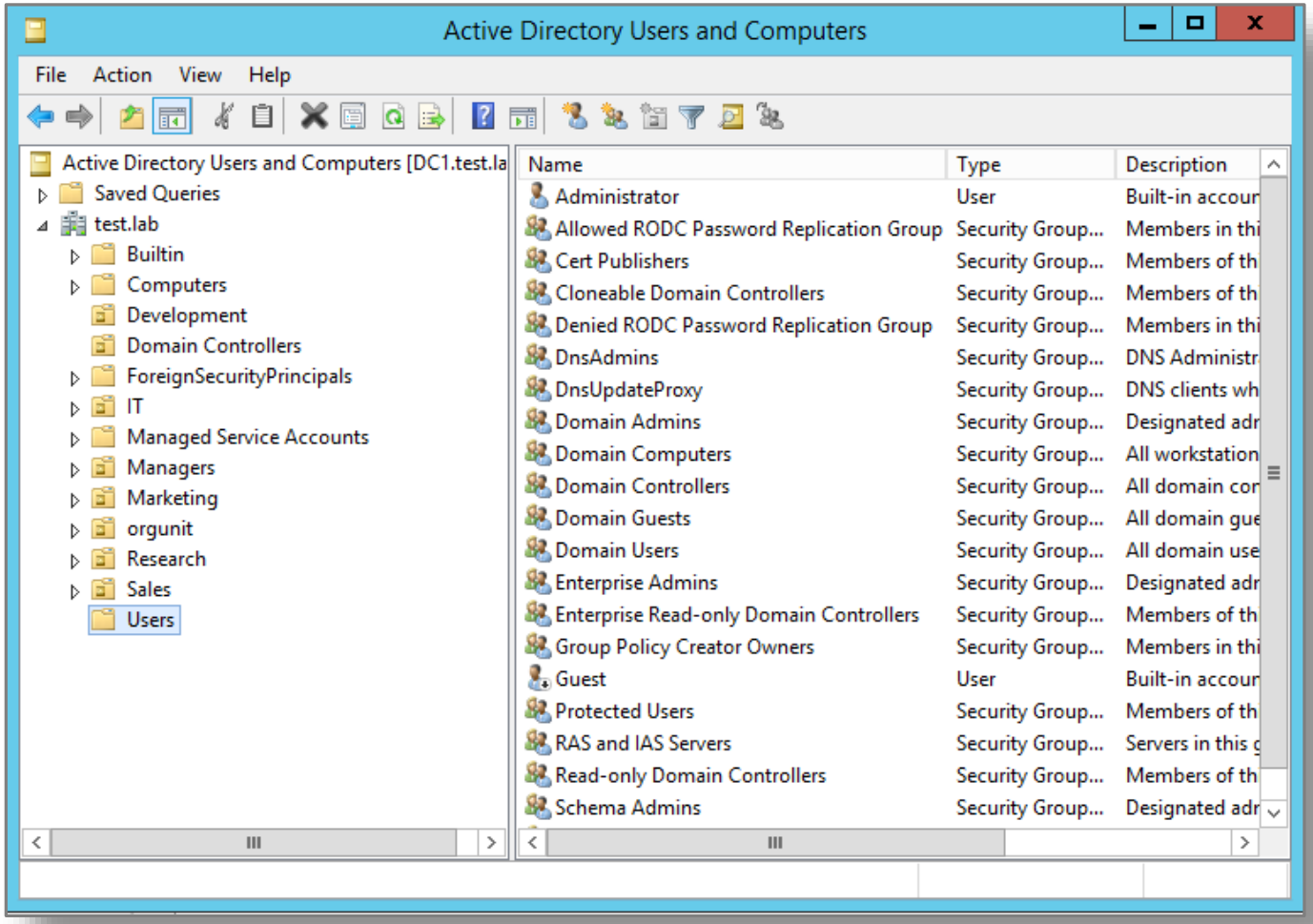
Az orgazinational unit (ou) egy limitált menedzsment lehetőségekkel felruházott konténer.

Mire jó?

- Az átlagos konténerekkel szemben egyszerűen létre lehet hozni.
- Objektumokat csoportosíthatunk és adhatunk rájuk közös szabályokat (GPO)
- Jogosultságokat adhatunk a csoportba foglalt objektumok felett
- Hierarchikusan szervezhetők pl. a vállalat felépítése alapján

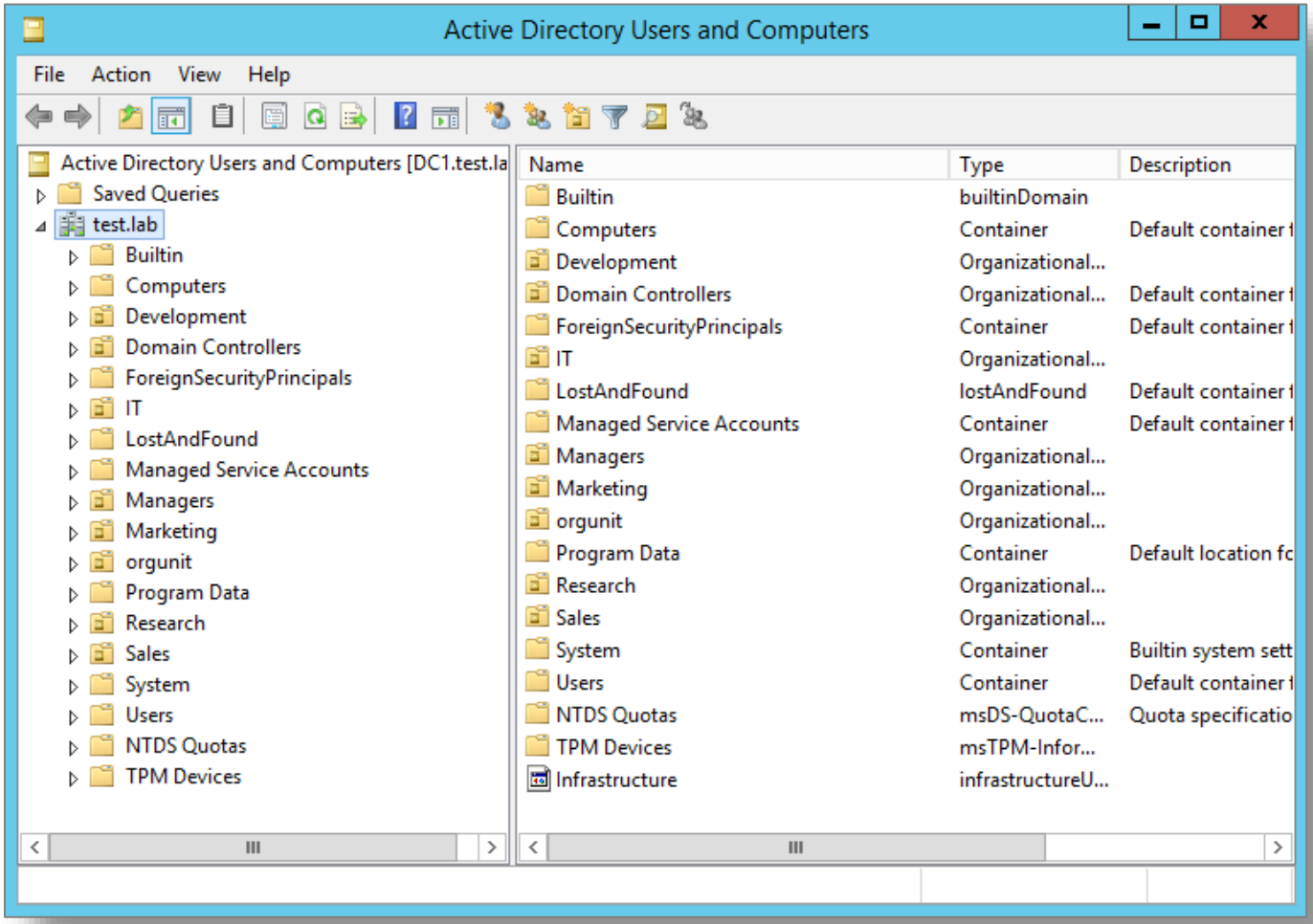
Active Directory DS OU

Előre definiált konténerek és ou-k



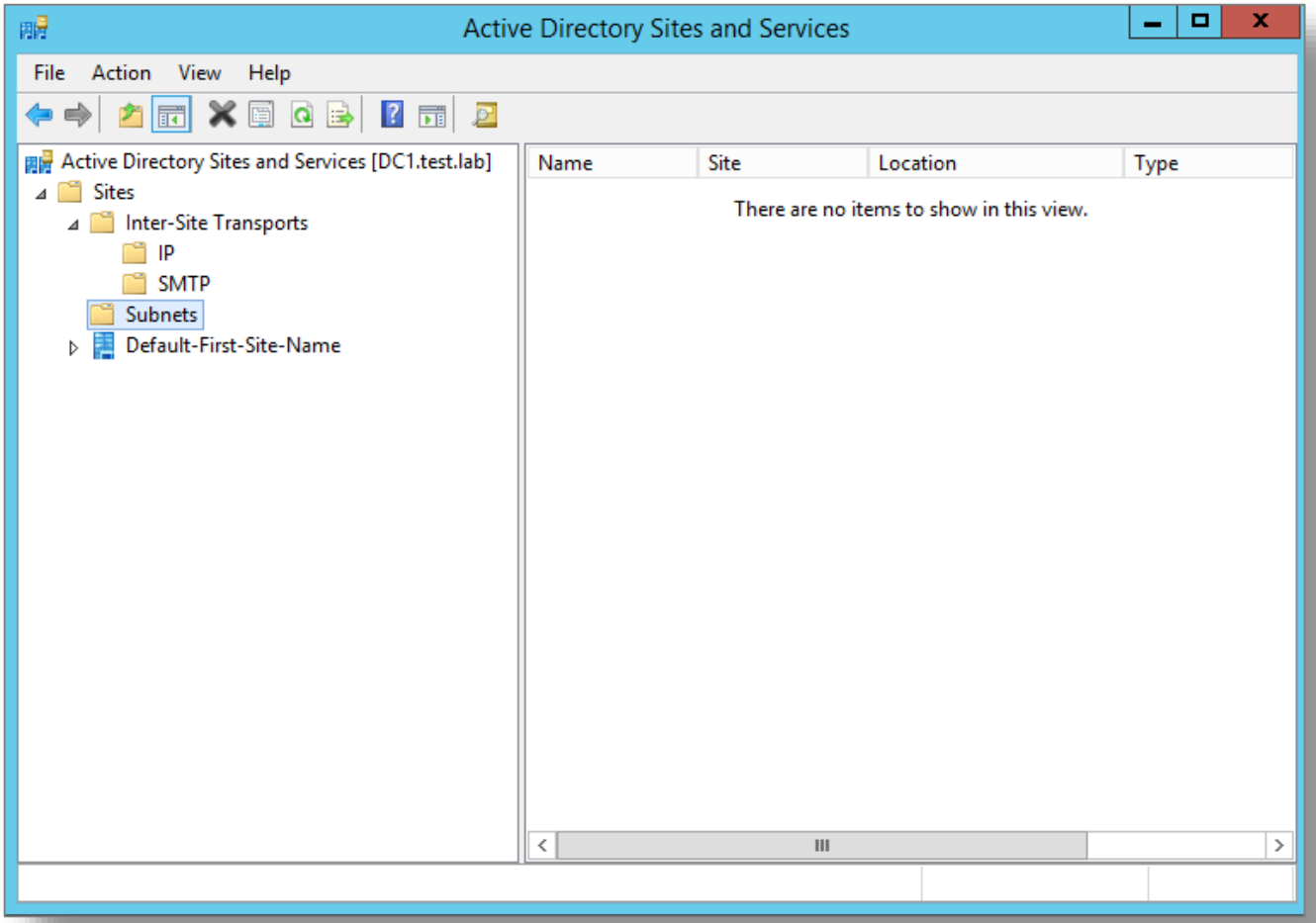
Active Directory DS OU

Előre definiált konténerek és ou-k (View->Advanced features után)



Active Directory DS Site

A site felhasználók, csoportok és számítógépek egy fizikai elhelyezkedés alapján kialakított csoportja. Adminisztrációs feladatok megkönnyítésére használható (pl. AD DS replikáció).



Active Directory DS partíció

A partíció az AD DS adatbázis egy szelete. Az adatbázis igazából egyetlen file (ntds.dit), ugyanakkor kezeléskor külön szektorokként dolgozunk rajta. Ezeket szokás *naming context*-nek is hívni.

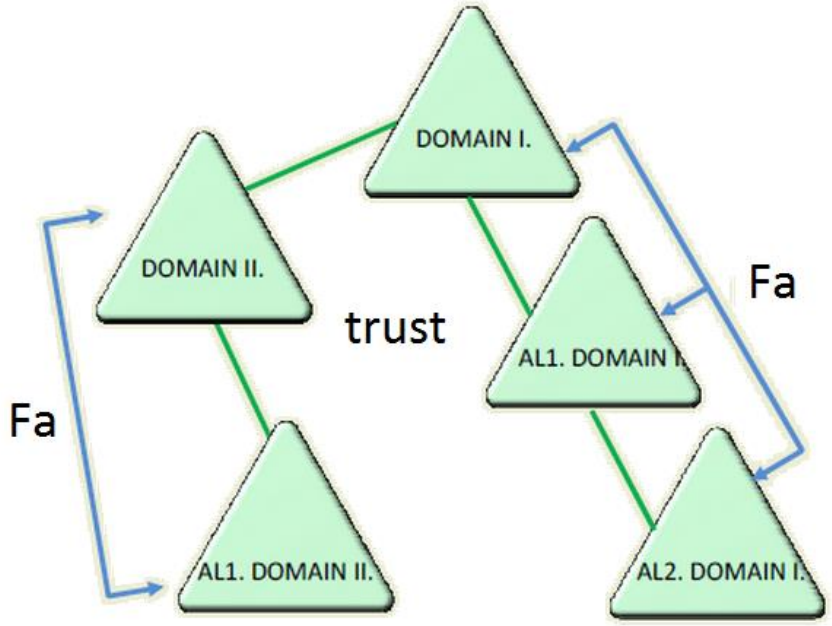
Partíciók:

- Sémapartíció (schema partition): meghatározza az objektumok létrehozásának és módosításának szabályait, az objektumok lehetséges attribútumait és beállításait.
- Konfigurációs partíció (configuration partition): az AD-ben ír le fizikai beállításokat
- Tartományi partíció (domain partition): minden információt tárol az adott tartományról.

Active Directory DS Tree és Forest

Fa (Tree): egy tartományhierarchiát alkotó domainek összessége, melyek konfigurációs és sémapartíciójukban megegyeznek. A tartományokat kétirányú bizalmi kapcsolat (trust) köti össze.

Forest (Erdő): Az AD hierarchia legmagasabb szintű egysége. Az erdőt egy vagy több, kétirányú és tranzitív bizalmi kapcsolat (trust) által összekötött fa (tree) alkotja.



Kép: *gamfinfo.hu*

FSMO szerepkörök

Multi master replikáció: A műveletek nagy részét bármelyik kiszolgálón el lehet végezni, mert a replikáció útján úgyis az összes egyenrangú kiszolgálóhoz eljut a változtatás.

FSMO szerepkörök: (Flexible Single Master Operations): néhány művelet csak bizonyos kitüntetett kiszolgálókon (pl. a schema masteren) végezhetők el.

FSMO szerepkörök

Szerep neve	Hatáskör	Leírás
Schema master	1/tree	A séma minden frissítését és módosítását ellenőrzi. Ha nem elérhető, nem lehet sémát bővíteni/frissíteni
Domain Naming Master	1/tree	Tartományok erdőhöz való hozzáadását/erdőből való eltávolítását ellenőrzi. Ha nem elérhető, a tartományfákkal kapcsolatos változtatások nem hajthatók végre.
PDC emulator	1/domain	Visszamenőleges kompatibilitást nyújt az NT 4-es kliensek számára a (Windows NT idejében csak a) PDC-n (Primary Domain Controller) végezhető műveletekhez, mint például jelszócsere.
RID master	1/domain	Feladata **R**elative **Id**entifier biztosítása újonnan létrehozott objektumok számára.
Infrastructure master	1/domain	A saját tartományába tartozó objektumok más tartományokba tartozó objektumokra való hivatkozásainak frissítéseit végzi.

Működési szintek

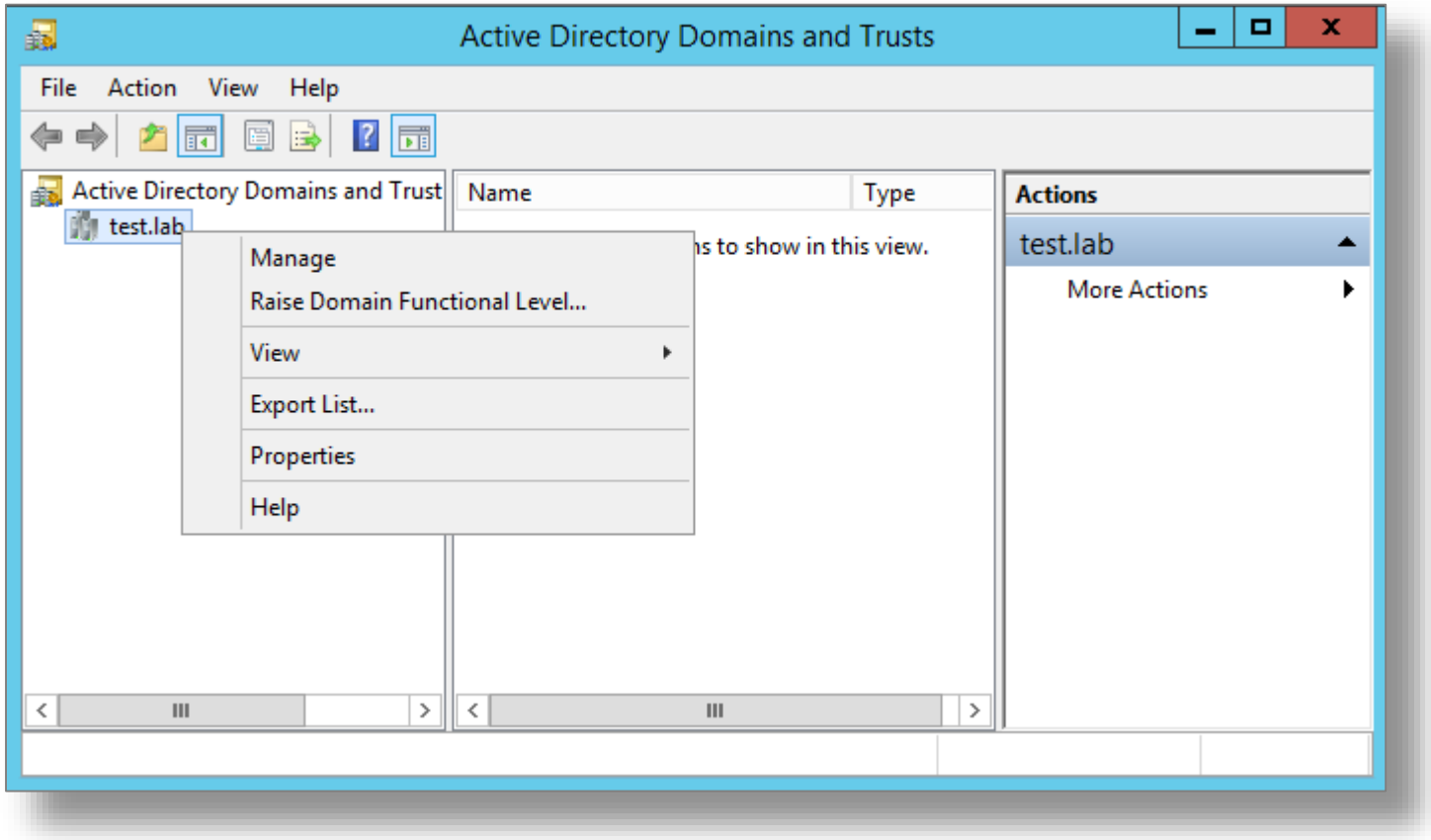
A Windows szerver funkciók kompatibilitási okokból történő szétválasztása domain és forest szinten.

Az újabb verziók általában nagyobb teljesítményt és új funkciókat hoznak. A tartományi működési szint akkor emelhető, ha minden tartományvezérlő rendelkezik a magasabb szint alkalmazásához szükséges szerver verzióval.

Alacsonyabb szintű szerver nem állítható magasabb szintű domain-be és alacsonyabb szintű domain nem vehető fel magasabb szintű erdőbe.

Működési szintek

AD Domains and Trusts



Gyakorlati feladat
Felkészülés a felmérőre