2011. ősz – 2**. ZH** Név:_____ NEPTUN kód:_____

ZH feladatok *Hálózati operációs rendszerek_3* tárgyból

Minden kérdésnél 1 pont szerezhető, összetett kérdéseknél részpont is kapható. Az elégséges osztályzathoz legalább a pontok 50%-át, azaz 5 pontot kell megszerezni.

1. Milyen típusú fiókokat különböztetünk meg biztonsági szempontból?(0,3) Közülük jellemezze az egyiket.(0,7)

Administrator *(Rendszergazda)* fióktípus: Az Administrators *(Rendszergazdák)* csoport tagjai, magas jogosultsággal használhatják a gépet. Alapértelmezés szerint a telepítés során megadott fiók is ebbe a csoportba kerül, és csak e csoport tagjaként hozhatunk létre, változtathatunk és törölhetünk további felhasználói fiókokat. A teljesség igénye nélkül, nézzük meg, hogy melyek a legfontosabb további műveletek, amelyre csak egy admin fiók birtokában leszünk képesek:

- bármely felhasználó jelszavának megváltoztatása;
- alkalmazásokat telepíteni és eltávolítani;
- a hardver eszközök eszközmeghajtóit telepíteni vagy eltávolítani;
- mappákat megosztani;
- engedélyeket és jogosultságokat beállítani más felhasználóknak vagy önmaguknak);
- a kötetek összes állományát elérni, más felhasználók fájljait is beleértve;
- fájlok és mappák tulajdonjogát átvenni;
- a *Program Files* és a *Windows* mappákba írni;
- lementett rendszerfájlokat visszaállítani;
- a rendszeridőt és a naptárt beállítani;
- a Windows Tűzfalat konfigurálni;
- beállítani a biztonsági frissítéseket, illetve manuálisan biztonsági frissítéseket telepíteni.

2. **Standard *(Általános jogú)* fióktípus**: A Users *(Felhasználók)* csoport tagjai a korábbi operációs rendszereknél csak egy alapszintű jogosultságcsokorral voltak kénytelenek beérni. A Windows Vista esetében jelentős haladás történt: itt már egy standard felhasználó gyakorlatilag mindenre képes, ami a számítógép napi használatához szükséges – de ha mélyebb, a rendszer biztonságát, működését alapjaiban megváltoztató műveletet szeretnénk elvégezni, akkor rendszergazda segítségére (vagy jogosultságra) lesz szükségünk. Lássunk néhány konkrét lehetőséget – főképp a viszonyítás kedvéért – amelyekre a Vistán egy standard felhasználó képes:

- saját jelszó megváltoztatása;
- a telepített programok használata;
- hardvereszközök eszközmeghajtóinak telepítése, (ha külön kapunk rá engedélyt);
- a jogosultságok megtekintése;

Osztályzat: 5-6,2 pont- *elégséges(2)*; 6,3-7,5 pont- *közepes(3)*; 7,6-8,8 pont- *jó(4)*; 8,9-10 pont- *jeles(5)*

- fájlok létrehozása, változtatása és törlése a saját Dokumentumok mappában, illetve a saját, megosztott mappákban;
- a személyesen lementett fájlok visszaállítása;
- a rendszeridő és naptár megtekintése, az időzóna megváltoztatása;
- az energiaellátási opciók beállítása;
- belépés csökkentett módban-

3. **Guest *(Vendég)* fióktípus**: A Guests *(Vendégek)* csoportba tartozó fiókok megszemélyesítői nagyon minimális jogosultságokkal rendelkeznek, mélyen a standard felhasználók jogosultsági szintje alatt. Ideiglenes jelleggel és/vagy nagyon korlátozott hozzáférés céljából használjuk.
Jó példa erre, hogy az azonos nevű Guest *(Vendég)* fiók tulajdonosa még a saját jelszavát sem hozhatja létre, a Users *(Felhasználók)* csoportnak sem tagja, és alapesetben ez a fiók le is van tiltva.

2. Sorolja fel a félév során megismert hitelesítési protokollokat(0,4), és írja le a Kerberos V5 hitelesítési folyamat lépéseit.(0,6)

LAN Manager(LANMAN); NTLMv1 (NT LAN Manager v1); NTLMv2 (NT LAN Manager v2); Kerberos V5
A Kerberos V5 hitelesítési folyamata egyszerűsítve a következőképpen működik:

1. Az ügyfélgépen belépni szándékozó felhasználó – jelszó és/vagy intelligens kártya használatával – hitelesíti magát a szintén a tartományvezérlőkön futó összetevő, a hitelesítésszolgáltató *(Authentication Service – AS)* felé.
2. Az AS leellenőrzi a felhasználót az AD segítségével, majd felveszi a kapcsolatot a KDC-vel az új kulcs legyártása érdekében.
3. A KDC egy egyedi *(session)* kulcsot biztosít az ügyfélnek. Az AS ezt egy speciális jeggyel *(Ticket Granting Ticket – TGT)* együtt küldi el a felhasználónak. A TGT azért is fontos (az ügyfél el is tárolja), mert a további jegyeket is ezzel lehet majd kérni, immár anélkül, hogy a jelszóra/felhasználónévre szükség lenne. Ez a kedvezmény persze nem tart örökké, alapbeállítás szerint mindösszesen csak 10 óráig.
4. Az ügyfél a nála lévő TGT felhasználásával jegyet kér és kap a harmadik fontos kiszolgálóoldali komponenstől, a Ticket Granting Service-től (TGS).
5. Végül az ügyfél ezt a jegyet mutatja be a kért hálózati szolgáltatásnak (azaz az NTLM-mel ellentétben nem utazik minden alkalommal a jelszó kivonat a hálózaton!), pl. jelen esetben a tartományi belépést kontrolláló tartományvezérlőnek, és kap engedélyt a tartományi belépésre. Ha ezek után az adott 10 órán belül valamilyen más szolgáltatás esetén újra igazolnia kell magát, akkor a letárolt TGT-vel megint kér egy szolgáltatásjegyet, és aztán csendben ezt bemutatja a kérő felé.

Osztályzat: 5-6,2 pont- *elégséges(2)*; 6,3-7,5 pont- *közepes(3)*; 7,6-8,8 pont- *jó(4)*; 8,9-10 pont- *jeles(5)*

2011. ősz – 2**. ZH** Név:_____ NEPTUN kód:_____

3. Mi az az UAC(angolul, magyarul)?(0,5) Mire, mikor használjuk?(0,5)

User Account Control - *Felhasználói fiókok felügyelete;*

4. Írja le a DHCP címkérés folyamatát!(0,8)Minden lépésnél írja oda hogy mi a célcím! (0,2)

A címkérés teljes folyamata négy lépésből áll, vagyis négy hálózati csomagra van szükség:

- **DHCP Discover** *(felderítés)* – ezt a csomagot az ügyfél küldi ki (broadcast), vagyis tulajdonképpen belekiabál az ismeretlenbe: Hahó, valaki! Címet kérek! Ha esetleg senki nem válaszol, akkor jöhet APIPA.
- **DHCP Offer** *(ajánlat)* – ezt a csomagot a DHCP Discover üzenetre válaszul a kiszolgáló küldi vissza, még mindig broadcast címzéssel, vagyis az ügyfélnek az üzenetekben szereplő azonosítószámok segítségével el kell döntenie, hogy a válasz valóban az ő kérésére érkezett-e. A csomag tartalmazza a felajánlott IP-címet és a hozzá tartozó egyéb paramétereket, vagyis szabad fordításban ezt jelenti: Ez jó lesz?
- **DHCP Request** *(kérés)* – ezután az ügyfél még mindig broadcast üzenetet küld, ami azt jelenti: Rendben, jöhet. Talán fölöslegesnek tűnhet ez a plusz kör a folyamatban, hiszen az ügyfél akár mindenféle visszabeszélés nélkül beállíthatná a kapott paramétereket. A pontos egyeztetésre tulajdonképpen csak akkor van szükség, ha több DHCP-kiszolgáló is üzemel a hálózatban.
- **DHCP Ack** *(visszaigazolás)* – az utolsó üzenet a visszaigazolás, az ügyfél az ebben szereplő IP-címet és opciókat fogja beállítani. Szintén ebben az üzenetben szerepel, hogy mikor fog lejárni a címbérlet, vagyis az üzenet tartalma ennyi: OK, nyolc napig a tiéd ez a cím.

5. Ismertesse a zóna fogalmát.

Zónának nevezzük a DNS-adatbázisokban a DNS-fa egy összefüggő részét, amelyet a DNS-kiszolgáló önálló egységként kezel. Minden zóna tartalmazza a hozzá tartozó nevekhez kapcsolódó valamennyi erőforrásrekordot.

6. Mire használjuk a WINS kiszolgálót?

A WINS-kiszolgáló a hálózaton használt számítógépekhez és csoportokhoz tartozó NetBIOS-nevek és IP-címek összerendeléseinek regisztrálásához és lekérdezéséhez biztosít dinamikusan felépíthető, elosztott adatbázist.

Osztályzat: 5-6,2 pont- *elégséges(2)*; 6,3-7,5 pont- *közepes(3)*; 7,6-8,8 pont- *jó(4)*; 8,9-10 pont- *jeles(5)*

2011. ősz – 2**. ZH** Név:_____ NEPTUN kód:_____

7. Soroljon fel legalább 5 féle rekordot, amelyet egy zóna tartalmazhat.(5x0,2)

- **SOA-rekord** – (Start of Authority) A SOA-rekord minden szabványos zóna esetén a zóna első rekordja. Felelős a zóna inicializásáért és a többi kiszolgáló számára jelzi a zóna hitelességét. A SOA-rekord határozza meg a zónaátvitel időzítését, a másodlagos kiszolgálók pedig az itt tárolt (és a zóna minden módosításakor növekvő) sorszám alapján dönthetik el, hogy szükséges-e a zóna letöltése. Ugyancsak a SOA-rekordban tárolt érték szabja meg, hogy az ügyfelek mennyi ideig tárolhatják saját gyorsítótáraikban a letöltött rekordokat.
- **A-rekord**: az A-rekordok egy számítógép nevének és IP-címének összerendelését határozzák meg, a lekérdezések többségére a megfelelő Arekord a válasz.
- **NS-rekord**: az NS-rekordok a zóna további mérvadó névkiszolgálóinak kijelölésére szolgálnak. A DNS-kiszolgáló alapértelmezés szerint csak a zóna NS erőforrásrekordjaiban szereplő kiszolgálókra engedélyezi a zónaletöltést.
- **CNAME-rekord**: Egy másodnevet, vagyis aliast rendel a megadott A-rekordhoz, (illetve esetleg másik CNAME-rekordhoz). Általában CNAME használatával születnek a külvilágnak szóló *www, ftp, mail, proxy* stb. gépnevek, így a valódi gépnév (ami az A-rekordban szerepel) követheti a szervezeten belül kialakított elnevezési szokásokat, illetve a terhelés megosztása miatt több gép is elérhetővé tehető egyetlen név használatával.
- **MX-rekord**: Az MX-erőforrásrekordot az elektronikus levelezésre szolgáló alkalmazások használják az üzenetek címzésében szereplő tartomány levelező kiszolgálójának azonosítására. A rekord annak a számítógépnek (vagy számítógépeknek) a nevét tartalmazza, amely az adott tartományba érkező levelek fogadásáért felelős. A számítógép nevén kívül a rekord tartalmaz egy számot is, ami az adott kiszolgáló prioritását jelzi (az alacsonyabb érték magasabb prioritást jelent).
- **PTR-rekord**: a PTR (pointer, *mutató)* erőforrásrekordok a névkeresési műveletek támogatására szolgálnak, egy IP-cím és egy hostnév összerendelését határozzák meg.
- **WINS-rekord**: A WINS-erőforrásrekordban egy WINS-kiszolgálót adhatunk meg, ide továbbítódnak majd a DNS-adatok alapján meg nem válaszolható IP-cím lekérdezések.
- **WINS-R-rekord**: ugyancsak egy WINS-kiszolgáló címét adhatjuk meg ebben a rekordban, ide a sikertelen fordított lekérdezések (ilyenkor név alapján keresünk IP-címet) fognak továbbítódni.
- **SRV-rekord**: az SRV-rekordok az Active Directoryhoz kapcsolódó szolgáltatások megtalálását teszik lehetővé.

Osztályzat: 5-6,2 pont- *elégséges(2)*; 6,3-7,5 pont- *közepes(3)*; 7,6-8,8 pont- *jó(4)*; 8,9-10 pont- *jeles(5)*

2011. ősz – 2**. ZH** Név:_____ NEPTUN kód:_____

8. Milyen új funkciókat nyújt a DNS kiszolgálói szerepkör (WS2008R2) a korábbiakhoz képest? (5x0,2)
   - Zóna betöltése a háttérben
   - IPv6-címek támogatása
   - Írásvédett tartományvezérlő támogatása
   - GlobalNames zóna
   - Globális lekérdezési tiltólista

9. Mi az a RAID technológia és mire szolgál?

A **RAID** (**Redundant Array of Inexpensive Disks** vagy **Redundant Array of Independent Disks**) napjaink egyik fontos technológiája. A RAID technológia alapja az adatok elosztása vagy replikálása több fizikailag független merevlemezen, egy logikai lemezt hozva létre. Minden RAID szint alapjában véve vagy az adatbiztonság növelését vagy az adatátviteli sebesség növelését szolgálja.

10. Milyen RAID szinteket támogat a WS2005R2? (0,3) Írja le az egyik ilyen szint működési logikáját.(0,7)

RAID 0, 1, 5

RAID 0 (összefűzés)

A RAID 0 az egyes lemezek egyszerű összefűzését jelenti, viszont semmilyen redundanciát nem ad, így nem biztosít hibatűrést, azaz egyetlen meghajtó meghibásodása az egész tömb hibáját okozza. Mind az írási, mind az olvasási műveletek párhuzamosítva történnek, ideális esetben a sebesség az egyes lemezek sebességének összege lesz, így a módszer a RAID szintek közül a legjobb teljesítményt nyújtja (a többi módszernél a redundancia kezelése lassítja a rendszert). A megoldás lehetővé teszi különböző kapacitású lemezek összekapcsolását is, viszont a nagyobb kapacitású lemezeken is csak a tömb legkisebb kapacitású lemezének méretét lehet használni.

A RAID 0 főleg olyan helyeken alkalmazható, ahol nem szempont az adatbiztonság vagy kevés merevlemez csatolható fel az operációs rendszer korlátozása miatt. (Például a régebbi Microsoft Windows rendszerek esetében összesen 26 meghajtó betűjelet tesznek elérhetővé, ezzel 24 eszközre korlátozva a partíciók számát. Az újabb rendszerek, mint a Windows 2000 Professional és az ezt követő Windowsok, valamint a Unix rendszerek lehetőséget adnak a partíciók könyvtárként való felcsatolására.) A másik pozitív tulajdonsága viszont továbbra is csábító lehet olyan, kifejezetten csak játékra épített rendszereknél, ahol ezzel tetemes teljesítménynövekedést érhetünk el. Ilyen célú alkalmazásra mégsem túl ajánlott, mivel az egyszer már összekapcsolt diszkek különálló alkalmazása csak újraszervezés után, a teljes adattartalom eltávolításával és újraformázással lehetséges.

Osztályzat: 5-6,2 pont- *elégséges(2)*; 6,3-7,5 pont- *közepes(3)*; 7,6-8,8 pont- *jó(4)*; 8,9-10 pont- *jeles(5)*

2011. ősz – 2**. ZH** Név:_____ NEPTUN kód:_____

RAID 1 (tükrözés)

A RAID 1 eljárás alapja az adatok tükrözése (disk mirroring), azaz az információk egyidejű tárolása a tömb minden elemén. A kapott logikai lemez a tömb legkisebb elemével lesz egyenlő méretű. Az adatok olvasása párhuzamosan történik a diszkekről, felgyorsítván az olvasás sebességét; az írás normál sebességgel, párhuzamosan történik a meghajtókon. Az eljárás igen jó hibavédelmet biztosít, bármely meghajtó meghibásodása esetén folytatódhat a működés. A RAID 1 önmagában nem használja a csíkokra bontás módszerét.

RAID 5

A RAID 5 a paritás információt nem egy kitüntetett meghajtón, hanem „körbeforgó paritás” (rotating parity) használatával, egyenletesen az összes meghajtón elosztva tárolja, kiküszöbölvén a paritás-meghajtó jelentette szűk keresztmetszetet. Minimális meghajtószám: 3. Mind az írási, mind az olvasási műveletek párhuzamosan végezhetőek. Egy meghajtó meghibásodása esetén az adatok sértetlenül visszaolvashatóak, a hibás meghajtó adatait a vezérlő a többi meghajtóról ki tudja számolni. A csíkméret változtatható; kis méretű csíkok esetén a RAID 3-hoz hasonló működést, míg nagy méretű csíkok alkalmazása esetén a RAID 4-hez hasonló működést kapunk. A hibás meghajtót ajánlott azonnal cserélni, mert két meghajtó meghibásodása esetén az adatok elvesznek!

A tárolható adatmennyiség "a legkisebb kapacitású meghajtón tárolható adatmennyiség" * ("meghajtók száma" - 1) lesz. (Pl. 4 db egyenként 1 TB -os HDD RAID 5-be fűzésének eredményeként egy 3 TB kapacitású logikai meghajtót látunk.)

Az írási sebességnél fontos figyelembe venni a paritás adatok előállítására szükséges számítási kapacitás igényt! Szoftveres megoldásnál ez jelentős processzorterhelést, illetve az írási sebesség csökkenését eredményezheti, ezért ajánlott a hardveres megoldás, ahol a célhardver látja el ezeket a feladatokat.

Osztályzat: 5-6,2 pont- *elégséges(2)*; 6,3-7,5 pont- *közepes(3)*; 7,6-8,8 pont- *jó(4)*; 8,9-10 pont- *jeles(5)*