Az OS-sel szemben támasztott legfontosabb biztonsági követelmények felsorolás

1. Együttműködő
2. Költségkímélő
3. Megbízhatóság
4. Elérhetőség
5. Méretezhetőség
6. Kezelhetőség

2

Együttműködő követelmények

o Biztosítani a különböző rendszerek zökkenőmentes összekapcsolását.
o Kompatibilis sok más gyártó termékeivel, ipari szabvánnyal, valamint minden jelenleg is támogatott, a Windowstermékcsaládhoz tartozó kiszolgáló- és ügyféloldali operációs rendszerrel, a Microsoft Office-szal és a Microsoft többi vállalati alkalmazásával is.
o Együttműködik az XML-alapú alkalmazásokkal és szolgáltatásokkal a natív XML-támogatás és a hozzá kapcsolódó technológiák segítségével.

3

Költségkímélő követelmények

Költségkímélő legyen és garantálni kell a befektetések biztos megtérülését.

4

Megbízhatóság követelmények

o egy rendszer v. eszköz milyen valószínűséggel képes folyamatosan üzemelni egy adott időszakban, meghatározott körülmények között.
o Fürtözés (az Enterprise Edition és a Datacenter Edition támogatják a 8 csomópontos fürtözést).
o Beépített hálózati terheléselosztás (növeli a webalapú alkalmazások és szolgáltatások teljesítményét).
o Nyelvfüggetlen futtatórendszer.
o Elosztott hitelesítési rendszer támogatása (Kerberos).
o Nyilvános kulcsú infrastruktúra tovább fejlesztése.
o Jobb memóriakezelés - nagyobb sebesség, megbízhatóság és rugalmasság
o Szilárd rendszerarchitektúra

♣ Pl. nem válaszoló alkalmazások kezelése, korábbi illesztőprogramok visszaállíthatósága, ha egy frissített illesztőprogram nem működik megfelelően.
o Diagnosztikai eszközök a rendszer állapotának figyelése
o Indítás csökkentett módban
o Windows fájlvédelem
♣ Megakadályozza, hogy más programok módosítsák az o.r. számára szükséges fájlokat (pl. .sys, .dll, .ocx, .ttf, .fon .exe).
o Helyreállítási konzol: Parancssoros konzolon is megkísérelhetjük a rendszer helyreállítását. Szolgáltatások engedélyezhetők és tilthatók le, meghajtók formázhatók, helyi lemezen lévő adatok olvashatók és írhatók (NTFS fájlrendszerrel formázott meghajtók esetében is), stb. Szükséges a beépített rendszergazdai fiók jelszava.
o Kompatibilitási üzemmód: A korábbi Windows OS-ek működéséhez.
o Biztonságimásolat-készítő segédprogram
o Automatikus rendszer-helyreállítás (ASR)
♣ A teljes rendszert a biztonsági másolat készítésekor fennálló állapotba állíthatjuk vissza. Csak, ha a többi lehetőség nem segít, pl. csökkentett mód, legutolsó helyes konfiguráció használata.
o Megjegyzések:
♣ Rendszer-helyreállítási terv részeként.
♣ Az adatfájlokról külön kell rendszeres biztonsági másolat.
♣ Max. 2,1 GB FAT16 fájlrendszerű köteteket támogatja, nem támogatja a 64 kB-os szektor-csoportokat használó, 4 GB-os, FAT16 fájlrendszerű partíciókat, át kell alakítani azokat NTFS rendszerűvé az Automatikus rendszer-helyreállítás előtt.

5

Elérhetőség követelmények

Az alkalmazások, szolgáltatások és rendszerek rendelkezésre állásának mértéke.
o Elérhetőség szempontjából magas színvonalú az a rendszer, amelynek tervezett vagy váratlan üzemszünete csekély.
o Kiszolgálófürtök:
♣ Csak Enterprise Edition és Datacenter Edition rendszereken. Magas szintű elérhetőséget, skálázhatóságot és kezelhetőséget biztosítanak a fontos erőforrások és alkalmazások számára.
♣ A fürtben lévő kiszolgálók (csomópontok) folyamatosan kommunikálnak egymással. Ha egy csomópont nem érhető el hiba v. karbantartás miatt, akkor egy másik azonnal átveszi a feladatát. ◊ Folyamatos kapcsolat a kiszolgáló erőforrásaival.
o Hálózati terheléselosztás

♣ Két alapvető feladata a magas szintű elérhetőség biztosítása a webkiszolgáló-programok számára, ill. a kiszolgáló teljesítményének növelése. Két v. több számítógép erőforrásainak fürtbe foglalása esetén elosztja a bejövő hálózati forgalmat. Megnöveli az internetes kiszolgálóalkalmazások rendelkezésre állását és skálázhatóságát. Pl. a weben és FTP-n használt szolgáltatások, a tűzfal, a proxy, a VPN, stb.
♣ Előnyei:
• Az állomásokra jutó terhelés súlyozása beállítható.
• A fürt dinamikusan bővíthető.
• A teljes adatforgalom egyetlen kiszolgálóra (alapértelmezett állomás) továbbítható.
• A fürt összes számítógépe ugyanazzal a fürt IP-címkészlettel megcímezhető (de az eredeti dedikált IP-címeket is megőrzi).
• Az állomás meghibásodásakor v. kikapcsolásakor a program a terhelést automatikusan a többi, még működő számítógépre osztja el.
o Kevesebb kiszolgáló-újraindítás
♣ Számos tevékenység a kiszolgáló újraindítása nélkül hajtható végre.
♣ Pl.: Tárolókötet kiterjesztése
♣ Hálózati protokollok konfigurálása
♣ Beállítások újra konfigurálása PCI és egyéb Plug and Play hardverek esetén
o A kiszolgáló indítása tükrözött kötetről
♣ Megfelelő előkészítéssel el lehet indítani a kiszolgálót az adatok tükrözött köteten lévő másolatáról, egyenletesebb rendszer-elérhetőséget biztosítva a kiszolgáló helyreállítása és az ütemezett karbantartás során.
o Felhasználóállapot-áttelepítő eszköz (User State Migration Tool)
♣ A felhasználói beállítások, fájlok és dokumentumok rögzítése és helyreállítása. A felhasználóknak nem szükséges újra megadniuk egyes beállításokat, pl. a levelezőkiszolgálót, a proxykiszolgálót, az asztal színsémáját és tapétáját.
o Válságkezelési szolgáltatások
♣ Távoli felügyeleti és rendszer-helyreállítási műveletek végrehajtására, amikor a kiszolgáló nem érhető el a hálózaton keresztül v. más szokásos távoli felügyeleti eszközzel és módszerrel. Fizikai hozzáférésre csak akkor van szükség, ha hardvereszközöket kell beszerelni v. kicserélni. Nem grafikus felhasználói felületen (GUI), hanem szöveges módú terminálon kezelhetőek, más platformokkal (pl. UNIX) is együttműködnek.

6

Méretezhetőség követelmények

o Az eddigieknél nagyobb kötetméret, több fájl tárolható kötetenként.
o Elosztott fájlrendszer (Distributed File System, DFS), SAN-okról (storage

area network – tárolóhálózatok) történő rendszerindítás képessége.
o IIS 6.0-tól (a windows webszolgáltatása) a teljesítmény és megbízhatóság növelésével javítja a méretezhetőséget.
o Skálázhatóság: egy számítógép, szolgáltatás v. alkalmazás milyen mértékben képes megfelelni a teljesítménykövetelmények növekedésének. Kiszolgálófürtök esetén újabb rendszer(ek) meglévő fürthöz adásának lehetőségét jelenti.
o Fizikai cím kiterjesztése (PAE)
♣ A nagyobb fizikai memória csökkenti a lapozás mértékét, és így növeli a rendszer teljesítményét. Egyes szoftverek számára lehetővé teszi, hogy több fizikai memóriát képezzenek le az alkalmazás virtuális címtartományába.
o Jelentősen javítja az alábbi típusú alkalmazások teljesítményét:
♣ Adatbáziskezelők, pl. a Microsoft SQL/E 7.0 v. későbbi verziói.
♣ Tudományos és mérnöki alkalmazások, pl. áramlástani számítások.
♣ Statisztikai elemző alkalmazások, amelyek széles körű adatbányászatot végeznek.
o I2O-támogatás (Intelligent Input/Output)
♣ Bizonyos I/O műveletekhez egy másodlagos tehermentesítő processzort használ. Javítja a be- és kimeneti teljesítményt a nagy sávszélességet használó alkalmazásoknál, pl. a hálózati videoalkalmazásoknál, a csoportmunka-szoftvereknél és az ügyfél-kiszolgáló folyamatoknál.
o A szimmetrikus multiprocesszálás (SMP)
♣ Az OS bármely elérhető processzoron tud végrehajtási szálakat futtatni, így az alkalmazások több processzort is használhatnak. Több egyenrangú processzor osztozik a memórián és a perifériás készülékekhez illeszkedő síndrendszeren.
o Hálózati terheléselosztás
o Kiszolgálófürtök
o Enterprise Memory Architecture (nagyvállalati memóriaszerkezet)
(Enterprise Edition, Datacenter Edition, de a 64 bites verziókon nem használható)
♣ Lehetővé teszi olyan alkalmazások futtatását, amelyek nagy mennyiségű fizikai memóriát használnak. Kétfajta memóriabővítést támogat: az alkalmazásmemória növelését – más néven a 4 GB alapú memórianövelés (4- gigabyte tuning, 4GT) –, valamint a fizikaicím-kiterjesztést (PAE X86). Alapértelmezés szerint egyik sincs engedélyezve. Az alkalmazásmemória növelését és a PAE-t is kézzel kell engedélyezni a Boot.ini fájlban.

o Internet Information Services
♣ Biztonságos, elérhető és méretezhető webes kiszolgáló támogatását biztosítja;
♣ Ezen futtathatók a webhelyek és -alkalmazások.

♣ Webkiszolgáló szolgáltatásokat nyújt intraneten, interneten vagy extraneten.
♣ Dedikált alkalmazási üzemmódot biztosít, amely minden alkalmazáskódot elszigetelt környezetben futtat.

7

Kezelhetőség követelmény

o Jól felügyelhető
♣ Vállalati szintű felügyeleti szolgáltatások:
• Active Directory
• Csoportházirend
• Parancssori segédprogramok
• WMI
• Távtelepítő szolgáltatás (Remote Installation Services, RIS)
• Active Directory Management Tool (ADMT)
• Windows Installer
o IntelliMirror
♣ Üzleti szerep, csoporttagság és hely alapján lehet házirendbeállításokat megadni, melyek segítségével a Windows 2000 Professional és a Windows XP Professional rendszert futtató asztali sz.g.-k újrakonfigurálása (a felhasználók adatai, szoftverei és személyes beállításai) automatikusan megtörténik a felhasználó minden bejelentkezésekor, függetlenül a bejelentkezés helyétől.
♣ Változás- és konfigurációkezelési szolgáltatásokat tartalmaz.
♣ A rendszergazdák a távtelepítési szolgáltatással is elvégezhetik az operációs rendszer távtelepítését.
o Windows Management Instrumentation
♣ Méretezhető kezelési infrastruktúra, a web alapú vállalatirányításon (Web-based enterprise management – WBEM) alapul. Megfigyelhetők, nyomon követhetők és vezérelhetők a szoftveralkalmazásokkal, hardverösszetevőkkel és hálózatokkal kapcsolatos rendszeresemények. Egységes parancsfájlkezelő alkalmazásprogramozási felületet (API) is tartalmaz.
o Active Directory áttelepítési eszköz (Active Directory Migration Tool, ADMT) Windows NT 4.0
♣ tartományokból Active Directory tartományokba (amelyek tartományvezérlői Windows 2000 v. Windows Server 2003 rendszert futtatnak) telepíthetjük át a felhasználói fiókokat, csoportokat és számítógépfiókokat.
o Távtelepítési szolgáltatás (RIS)
♣ Az op. rendszerek lemezkép alapú telepítése a távtelepítési kiszolgálóról az ügyfélszámítógépre a hálózaton keresztül. Egyszerűsíti az op.

rendszerek és az alkalmazások kezelését, és javítja a hiba-helyreállítás hatékonyságát.
o Távoli asztal felügyeleti célokra (Korábbi nevén Terminálszolgáltatás távfelügyelet üzemmódban.) A számítógép a hálózat bármely számítógépéről felügyelhető.
o Távolról felügyelt kiszolgálók támogatása
♣ Monitorral, VGA videokártyával, billentyűzettel v. egérrel nem rendelkező számítógép telepítésére, kezelésére. Magában foglalja a válságkezelési szolgáltatásokat is, amikor az OS nem működik (pl. a számítógép újraindításakor, a távtelepítési szolgáltatás használata közben, v. ha a kiszolgáló nem elérhető a hálózaton).
o Felhasználóállapot-áttelepítő eszköz (User State Migration Tool) Mint az elérhetőségnél.
o Eredő házirend
♣ Használatával a Csoportházirendet használó számítógépeken és felhasználókon alkalmazott házirend-beállításokat szimulálhatjuk és tesztelhetjük. Lekérdezi a meglévő – és a tervezett – házirendeket, jelentést készít a lekérdezés eredményeiről. Az adatokat a WMI segítségével gyűjti össze.
o Engedélyezéskezelő
♣ Segítséget nyújt azon alkalmazásfejlesztőknek, akik engedélyezési szolgáltatásokat használnak az alkalmazásaikban, valamint azon rendszergazdáknak, akik csoportokat határoznak meg és rendszerbiztonsági tagokat rendelnek hozzá olyan szerepek és feladatok végrehajtásához, amelyek megfelelő felhasználói jogosultságokat és engedélyeket igényelnek.

8

Diagnosztikai eszközök felsorolás

1. Feladatkezelő
2. Rendszerinformációk
3. Rendszertulajdonságok
4. Szolgáltatások beépülő modulok
5. Eseménynapló
6. A teljesítmény figyelése
7. SNMP
8. Eszközkezelő
9. Rendszerleállási események követése
10. WMI

9

Feladatkezelő

A számítógépen futó programokra és folyamatokra vonatkozó információkat, valamint a folyamatok leggyakrabban használt teljesítmény jellemzőit jeleníti meg. Folyamatok fül: futó alkalmazások és folyamatok adatai, processzor és memóriakihasználtság. Leállítható és elindítható is. Teljesítmény fül: dinamikusan írja ki a CPU, memória kihasználtságot. Users fül: szghez hozzáférő felhasználók, munkamenetinek állapota található. Tartomány tagjaként a Users lap nem jelenik meg.

10

Rendszerinformációk

Összegyűjti és megjeleníti a rendszer konfigurációs adatait (helyi számítógép, v. amelyhez gépünk csatlakoztatva van). Administrative tools belül System Information. (vagy Msinfo32.exe). Keresni is van lehetőség, valamint szövegfájlba is ki lehet menteni. Ezutóbbit távoli asztal esetén csak admin joggal tehetjük meg. Nyomtatásra is van lehetőség.

11

Rendszertulajdonságok

Meg tudjuk változtatni helyi és távoli esetben is. Helyi esetben nem kell admin hitelesítés, távoli esetén kell. Administrative Tools ◊ Computer Management.

12

Szolgáltatások beépülő modulok

A számítógépen futó alkalmazásokat lehet kezelni, mind helyi mind távoli esetben. Szolgáltatások adatainak exportálása, hasznos lehet, ha vissza kell állítani alaphelyzetbe. Módosítás előtt végezzük el a teszteléseket és a biztonsági másolatokat. A szolgáltatások együttműködhet az Asztallal beállítás esetén minden információ, ami az asztalon van az megjelenik a felhasználó asztalán is, ezért érdemes az alapbeállítást meghagyni. Ellenőrizzük a függőségeket mielőtt elindítanánk vagy leállítanánk valamilyen szolgáltatást. Erről értesítsük az illetékes felhasználókat. Sok szolgáltatás alaphelyzetben le van tiltva (Letiltva, Kézi, Automatikus).
Administrative Tools ◊ Services
Beállítható, hogy a LogOn fülön, hogy milyen fiókkal lehessen belépni:

Local System account (helyi rendszerfiók), LocalService (helyi szolgáltatásfiók), NetworkService (hálózatszolgáltatás fiók). Meg is adható, hogy pontosan melyik felhasználói fiók tudjon belépni.
A szolgáltatások funkciói: indítás, leállítás, felfüggesztés, folytatás vagy újraindítás. Ezeket lehet grafikusan és parancssorból is beállítani. Vannak olyan szolgáltatások, amik nem állíthatóak le pl.: eseménynapló. Meghibásodott szolgáltatást helyreállítható. Lehet programot telepíteni, ahol az abszolút elérési utat kell megadni. Újra indítás esetén lehet értesítést küldeni a felhasználónak.
Szolgáltatás függőségek megtekintése esetén a prop◊dependencies fülön található. Itt látható, hogy melyikektől függ a mi szolgáltatásunk és hogy melyikek a mienktől.

13

Eseménynapló

Rögzített eseményeket figyelünk. Általában az alkalmazási, a biztonsági és a rendszernaplók kerülnek tárolásra. További naplók is megadhatók. Naplózási házirendben testreszabhatóak a beállítások, rendszergazdai jog kell hozzá, Administrative Tools ◊ Local Security◊Security ◊ Local Policies. Eseménynapló segítségével kiderül, hogy történt jogosulatlan tevékenység vagy rosszindulatú felhasználói belépés esetleg támadás általi behatolási kísérlet. Engedélyezzük a kritikus objektumok és műveletek esetében a naplózást és rendszeresen ellenőrizzük azt. Administrative Tools◊ Event Viewer. Action Refresh funkcióval frissíthető a nézet. Archivált fájl nem frissíthető. Mentés esetén, ha meghagyjuk az eredeti kiterjesztést akkor megtudjuk nézni az Eseménynaplóban, viszont, ha txt-ként akkor egy pontos vesszővel tagolt csv fájlt kapunk, amit bármilyen szövegszerkesztővel meg tudunk nyitni, rendszergazdai jog kell. Törlölni a Clear Log-gal lehet, rendszergazdai jog kell. Archivált eseménynapló megtekintéséhez csak abban az esetben kell rendszergazdai jog, ha távoli szg van szó.
Fájlra vagy mappára, Tulajdonságok (Properties), Biztonság (Security) fül, Speciális (Advanced) gomb, Naplózás (Auditing) fül.
A naplózás beállítása előtt engedélyezni kell az objektum-hozzáférések naplózását. ϖ Ha az eredeti objektum alatt lévő fájlokra és almappákra is szeretnénk tovább örökíteni ezeket a naplóbejegyzéseket, akkor be kell jelölni „A naplózási beállítások alkalmazása a fán lejjebb található objektumokra és/vagy tárolókra” jelölőnégyzetet. A fájlok és mappák naplózása csak NTFS meghajtókon állítható be.

14

A teljesítmény figyelése

A Rendszerfigyelő és a Teljesítménynaplók és riasztások szolgáltatás segítségével részletesen figyelhető az operációs rendszer erőforrás-felhasználása. A teljesítményfigyelő eszköz a naplófájlok mérete és az elfoglalt lemezterület miatt is hatással lehet a teljesítményre. Csökkentése érdekében növeljük meg a frissítési időközt. A naplófájlokat ne azon a lemezen tároljuk, amelyiket figyeljük. A gyakori naplózás növeli a lemezolvasási és -írási műveletek számát is. Távoli számítógép figyelése esetén ajánlott folyamatosan naplózni a távoli számítógépen, de a naplókat csak ritkán feltölteni, pl. naponta egyszer.
A kapacitástervezés érdekében figyeljük a változások tendenciáit, és szükség szerint adjunk hozzá új összetevőket v. frissítsük a meglévőket. A naplózott adatokat tároljuk adatbázisban, és figyeljük a változásokat, hogy követhessük az erőforrásigények változásait. A terhelés és erőforrás-igények változásának figyelése után megállapíthatjuk, hogy mely területek igényelnek további erőforrásokat.

15

SNMP

Az SNMP-kezelőrendszer lehetőséget biztosít az állapotadatok figyelésére és több állomás közötti átvitelére. Szolgáltatások kezelése: WINS szolgáltatás, DHCP, Internet Information Services, Microsoft LAN Manager alkalmazások.
Felhasználási területek:
7. Távoli eszközök konfigurálása. A kezelőrendszerről a konfigurációs információkat minden hálózatba kötött állomásnak el lehet küldeni.
8. Hálózati teljesítmény figyelése. Követhető a feldolgozási és hálózati átvitel, információ gyűjthető az adatátvitelek sikerességéről.
Hálózati hibák és nem megfelelő hozzáférések érzékelése. Beállíthatók hálózati eszközökre vonatkozó eseményindítóriasztások. Riasztás ◊ az eszköz egy eseményüzenetet küld a kezelőrendszernek.
A riasztások általános típusai: eszköz leállítása majd újraindítása, útválasztón érzékelt vonalhiba, nem megfelelő hozzáférés.
Hálózathasználat naplózása. Segítségével azonosítható a felhasználók és a csoportok hozzáférése, valamint a hálózati eszközök és szolgáltatások használatának típusai.
Rendszeresen figyelni és frissíteni kell az állomásnév-beállításokat (illetéktelen behatolások időben történő észlelése). Csak meghatározott (ne bármely) állomásokról érkeze csomagok fogadását engedélyezzük az állomásokon. Használjuk ki az SNMP biztonsági ellenőrző funkcióját: állítsunk be hitelesítést minden SNMP-ügynökön. Ellenőrizzük a

szolgáltatás-specifikus összetevők helyes működését.
Az SNMP-ügynökrendszert az illetéktelen kezelőrendszerektől érkező kérési üzenetek visszautasítására konfiguráljuk. (Belső támadások kockázatának csökkentése.) Az SNMP nem biztonságos protokoll! A biztonság érdekében az SNMP-kezelőrendszerek és az ügynökök között IPSec protokollt használjunk az SNMP üzenetek védelméhez megfelelő IP-szűrőlistában szűrőfeltételek létrehozásával. Próbáljuk az SNMP logikai csoportokat funkcionális szerveződés alapján rendezni.

16

Eszközkezelő

9. hardvereszközök illesztőprogramjainak frissítése
10. hardverbeállítások módosítása
11. hibák elhárítása

17

Rendszerleállási események követése

♣ Dokumentálható, hogy milyen okból indítják újra vagy állítják le a számítógépet.
♣ A rögzített adatok alapján átfogó kép állítható össze a szervezet rendszerkörnyezetéről.
♣ Alapértelmezés szerint be van kapcsolva, kivéve Windows XP Professional esetében, ahol nem volt használható.

18

WMI

A Windows operációs rendszerek beépített szolgáltatása. Lehetővé teszi a gépek távoli felügyeletét és menedzselését a hálózaton keresztül. Egy komplett hálózat minden programozható, aktív összetevője elérhető, lekérdezhető és módosítható. Pl. a számítógép minden hardver és szoftver összetevőjének paraméterei, tulajdonságai, egy hálózati útválasztó táblája, de még akár a légkondicionáló adatai is.
Korlátozott biztonsági funkciókkal rendelkezik, amelyek minden felhasználót azonosítanak, mielőtt engedélyeznék számára a csatlakozást a WMI szolgáltatásaihoz, akár a helyi számítógépen, akár valamely távoli számítógépen. A WMI nem bírálja felül és nem kerüli meg az operációs

rendszer biztonsági beállításait és korlátozásait. Alapértelmezés szerint a kezelt gépen a Rendszergazdák csoport minden tagja teljes körű hozzáféréssel rendelkezik a WMI szolgáltatásaihoz. Mindenki más csak írási, olvasási és végrehajtási engedélyekkel rendelkezik saját helyi számítógépén.
A rendszer csak a Windows Management szolgáltatáshoz csatlakozáskor ellenőrzi a biztonsági beállításokat és az engedélyeket, azok módosításai csak a legközelebbi WMI szolgáltatás indításakor lépnek életbe. Pl.: ha a r.g. visszavonja a felhasználó hozzáférési jogosultságát, az csak akkor lép életbe, amikor a felhasználó kilép a WMI szolgáltatásból és legközelebb megpróbál csatlakozni.