openSUSE

11.1

www.novell.com

2009. június 10.

Kézikönyv

Kézikönyv

Tartalomjegyzék

Az útmutatóról

Ez a kézikönyv az openSUSE általános tudnivalóit tartalmazza. Elsősorban rendszergazdáknak, illetve az alapszintű rendszergazdai ismeretekkel rendelkező otthoni felhasználóknak szól. A kézikönyv különböző részeiben a napi élethez szükséges sokféle alkalmazást ismerhet meg és részletes leírást talál a speciális telepítési és beállítási példahelyzetekről.

Speciális üzembe helyezési példahelyzetek
: Tanulja meg, hogyan telepíthető az openSUSE egy távoli helyszínről, illetve ismerkedjen meg az összetett lemezes telepítési példahelyzetekkel.

Szoftverkezelés és -frissítés
: Ismerkedjen meg azzal, hogyan telepíthetők és távolíthatók el a szoftverek a YaST és a parancssor használatával, hogyan kell használni a 1-Click-Install funkciót, illetve hogyan tarthatja naprakész állapotban a rendszert.

Adminisztráció
: Ebben a részben szó lesz az openSUSE frissítéséről és beállításáról, arról, hogyan adminisztrálható a rendszer szöveges módban, és megismerhet néhány, a Linux-adminisztrátorok számára készült fontos segédeszközt.

Rendszer
: Bemutatjuk a Linux-rendszer összetevőit és részletesen ismertetjük az ezek között fennálló interakciót.

Szolgáltatások
: Megtanulhatja, hogyan kell beállítani az openSUSE különféle hálózati és fájlszolgáltatásait.

Mobilitás
: Ismerkedjen meg az openSUSE mobil számítástechnikai megoldásaival, a különféle vezeték nélküli és energiagazdálkodási eszközökkel, illetve a tábla PC-k használatával.

Biztonság
: Ebben a részben az openSUSE biztonsági funkcióiról szólunk és megtudhatja, hogyan telepíthetők és állíthatók be a rendszert védő szolgáltatások.

A kézikönyv számos fejezete tartalmaz hivatkozásokat további dokumentációs erőforrásokra. Ezek között a rendszeren található kiegészítő dokumentációk ugyanúgy megtalálhatók, mint az internetről letölthető anyagok.

A termékhez rendelkezésre álló dokumentációs anyagok áttekintéséhez, illetve ezek legfrissebb bővítéseinek/kiegészítéseinek eléréséhez látogasson el a `http://www.novell.com/documentation/opensuse111` weboldalra, vagy tájékozódjon a következő fejezetből.

1 A rendelkezésre álló dokumentáció

A könyvek HTML- és PDF-változatban is hozzáférhetők, különféle nyelveken. A jelen termékhez az alábbi kézikönyvek állnak rendelkezésre a felhasználók és rendszergazdák számára:

Start-Up (↑*Start-Up*)
: Átvezet a rendszer telepítésének és alapszintű beállításának folyamatán. Azok számára, akiknek mindez még újdonság, a kézikönyv bemutatja a legfontosabb Linux-fogalmakat is, mint például a fájlrendszer, a felhasználók fogalma, valamint a hozzáférési jogosultságok, és áttekinti az openSUSE kifejezetten a mobil számítástechnikát támogató funkcióit is. Segítséget és tanácsokat ad a hibák elhárításához.

KDE Quick Start (↑*KDE Quick Start*)
: Egy rövid bevezetést ad a KDE-asztal kezeléséről és néhány kulcsfontosságú alkalmazás futtatásáról.

KDE User Guide (↑*KDE User Guide*)
: Az openSUSE rendszerben található KDE asztali környezetet mutatja be. Átvezet az asztali környezet beállításán és használatán, valamint segít a legfontosabb feladatok elvégzésében. Elsősorban azon végfelhasználóknak szól, akik a KDE asztali környezetet hatékonyan szeretnék használni, alapértelmezett asztali környezetként.

GNOME Quick Start (↑*GNOME Quick Start*)
: Egy rövid bevezetést ad a GNOME-asztal kezeléséről és néhány kulcsfontosságú alkalmazás futtatásáról.

GNOME User Guide (↑*GNOME User Guide*)
: Az openSUSE rendszerben található GNOME asztali környezetet mutatja be. Átvezet az asztali környezet beállításán és használatán, valamint segít a legfontosabb

feladatok elvégzésében. Elsősorban azon végfelhasználóknak szól, akik a GNOME asztali környezetet hatékonyan szeretnék használni, alapértelmezett asztali környezetként.

Application Guide (↑*Application Guide*)
: Az openSUSE asztali alkalmazásainak használatát és beállítását mutatja be. Ez a kézikönyv a böngészőket és a levelezőprogramokat mutatja be az irodai alkalmazásokkal és a csoportos munkát segítő eszközökkel együtt. Szól a grafikus és multimédiás alkalmazásokról is.

Kézikönyv (1. oldal)
: Általános ismertetőt nyújt az openSUSE rendszerről és bemutat speciális rendszerfelügyeleti feladatokat is. Elsősorban rendszergazdáknak szántuk, illetve az alapszintű rendszergazdai ismeretekkel rendelkező otthoni felhasználók számára. Részletes információt biztosít a speciális rendszertelepítési helyzetekről, a rendszer felügyeletéről, a rendszer legfontosabb elemeinek együttműködéséről, valamint az openSUSE által kínált különféle hálózati és fájlszolgáltatások üzembe helyezéséről.

Novell AppArmor Administration Guide (↑*Novell AppArmor Administration Guide*)
: Részletesen leírja a Novell AppArmor használatát az Ön környezetében. Az AppArmor egy biztonsági alkalmazás, amellyel programonként adható meg, hogy az adott program mely fájlokat jogosult elolvasni, írni és végrehajtani.

Lessons For Lizards
: Egy közösségi könyv az openSUSE disztribúcióhoz. A nyílt forráskódú közösség által írt kézikönyv adott állapotát tükröző pillanatképet együtt adjuk ki a Novell/SUSE kézikönyvekkel. Az egyes témák szakácskönyvszerűen vannak megírva, és a hagyományos kézikönyveknél részletesebb és egzotikusabb témákkal is foglalkoznak. További információkért lásd: `http://developer.novell.com/wiki/index.php/Lessons_for_Lizards`.

A legtöbb openSUSE kézikönyv HTML-változata megtalálható a telepített rendszer `/usr/share/doc/manual` könyvtárában, illetve a KDE vagy GNOME asztali környezet súgóközpontjában. A dokumentáció legfrissebb módosításai a `http://www.novell.com/documentation/` címen találhatók: innen tölthetők le a termékhez tartozó kézikönyvek PDF- és HTML-verziói.

Azzal kapcsolatban, hogy hol találhatók meg a könyvek a telepítési adathordozón, forduljon a termék kiadási megjegyzéseihez. A Kiadási megjegyzések a telepített rendszeren

az /usr/share/doc/release-notes/ könyvtárban, illetve a KDE vagy GNOME asztali környezet súgóközpontjában találhatók meg.

2 Visszajelzés

Számos csatorna áll rendelkezésre a visszajelzéshez:

- Egy adott komponens hibáinak bejelentéséhez, illetve továbbfejlesztések kéréséhez kérjük, használja a https://bugzilla.novell.com/ címen található rendszert. Ha még soha nem használta a Bugzillát korábban, akkor hasznos lehet elolvasni a *Hibajelentések benyújtása (Submitting Bug Reports)* című cikket a http://hu.opensuse.org/Hibabejelentés címen. A hibák bejelentésével kapcsolatos gyakori kérdésekre a http://en.opensuse.org/Bug_Reporting_FAQ címen találhat válaszokat.

- Szeretnénk, ha közölné velünk a jelen kézikönyvvel és a termék egyéb dokumentációival kapcsolatos megjegyzéseit és javaslatait. Kérjük használja az online dokumentáció egyes oldalainak alján található Felhasználói megjegyzések funkciót, és oda írja be az észrevételeit.

3 Jelölések a dokumentációban

Ebben a kézikönyvben a következő tipográfiai jelöléseket használjuk:

- /etc/passwd: fájlnevek és könyvtárnevek
- *Helyőrző*: helyettesítse be a *helyőrző* mezőt az aktuális értékkel
- Elérési út: a környezettől függően változó elérési út
- ls, --help: parancsok, beállítások és paraméterek
- felhasználó: felhasználók vagy csoportok
- Alt, Alt + F1: az a billentyű, vagy billentyűkombináció, melyet meg kell nyomni. A billentyűk nagybetűvel vannak feltüntetve úgy, ahogy a klaviatúrán vannak

- *Fájl*, *Fájl* > *Mentés másként*: menüelemek, gombok
- *Táncoló pingvinek* (*Pingvinek* fejezet, ↑ egy másik kézikönyv): Ez egy utalás egy másik kézikönyvben lévő fejezetre.

4 Hogyan készült ez a könyv?

Ez a könyv a Novdoc (a DocBook egy részhalmaza, lásd: `http://www.docbook.org`) használatával készült. Az XML-forrásfájlokat `xmllint`-tel ellenőriztük, az `xsltproc` programmal dolgoztuk fel és Norman Walsh stíluslapjainak egy módosított változatával alakítottuk XSL-FO formátumra. A végső PDF formázása a RenderX XEP programjával történt.

5 Forráskód

Az openSUSE forráskódja nyilvánosan elérhető. A forráskód letöltéséhez kövesse a `http://www.novell.com/products/suselinux/source_code.html` részben leírt utasításokat. Ha kéri, el tudjuk küldeni a forráskódot DVD-n is. Az elkészítésért, feldolgozásért és postázásért azonban felszámítunk egy 15 dolláros vagy 15 eurós összeget. Ha DVD-n kéri a forráskódot, küldjün egy e-mailt a sourcedvd@suse.de [`mailto:sourcedvd@suse.de`] címre, vagy küldjön egy levelet postán az alábbi címre:

SUSE Linux Products GmbH Product Management openSUSE Maxfeldstr. 5 D-90409 Nürnberg, Germany

6 Köszönetek

A Linux-fejlesztők rengeteg önkéntes munkát fektetnek bele az egész világon, hogy segítsék a Linux fejlődését. Köszönjük fáradozásaikat – nélkülük ez a disztribúció nem létezhetne. Hálásak vagyunk még Frank Zappának és Pawarnak is. Külön köszönet jár természetesen Linus Torvaldsnak.

Jó szórakozást kívánunk!

A SUSE csapat

I. rész - Speciális üzembe helyezési példahelyzetek

1 Távoli telepítés

Az openSUSE® többféle módon is telepíthető. Csakúgy, mint az adathordozókról végzett szokásos telepítés esetében (1. fejezet - *Installation with YaST* (↑*Start-Up*)), számos hálózati alapú megközelítés közül lehet választani, sőt, akár teljesen automatizált módon is telepíthető az openSUSE.

Mindegyik módszert két rövid ellenőrzőlistával vezetjük be: az egyik a módszer előfeltételeit sorolja fel, a másik pedig röviden áttekinti az eljárást. Ezután részletesebben is végigvesszük az adott telepítési helyzetben használt technikákat.

MEGJEGYZÉS

A következő szakaszokban azt a rendszert, amelyikre az új openSUSE kerül, *célrendszer* vagy *telepítési cél* néven fogjuk emlegetni. A *telepítési forrás* kifejezés az összes telepítési adatforrás együttesét jelöli. Ide tartoznak a fizikai adathordozók (CD és DVD), illetve a telepítési adatokat szétosztani képes kiszolgálók a hálózatban.

1.1 A távoli telepítés telepítési helyzetei

Ebben a szakaszban átvesszük a távoli telepítések leggyakoribb telepítési helyzeteit. Minden egyes helyzetnél tekintse meg az előfeltételek listáját és kövesse a helyzethez felvázolt eljárást. Ha egy adott lépéshez részletesebb utasításra van szüksége, kövesse a megadott hivatkozásokat.

FONTOS

Az X Window rendszer beállítását egyik távoli telepítési eljárásban sem részletezzük. A telepítés befejeztével jelentkezzen be a célrendszerre `root` felhasználóként, írja be a `telinit 3` parancsot és a SaX programmal állítsa be a grafikus hardvert (ennek leírása: 2.2. - Setting Up Graphics Card and Monitor (2. fejezet - *Setting Up Hardware Components with YaST*, ↑*Start-Up*)).

1.1.1 Egyszerű távoli telepítés VNC-n keresztül – statikus hálózati beállítások

Ehhez a fajta telepítéshez továbbra is szükséges kismértékben fizikailag hozzáférni a célrendszerhez, a rendszer elindításához. Magát a telepítést aztán teljes mértékben lehet egy távoli munkaállomásról vezérelni, VNC-n keresztül kapcsolódva a telepítőprogramhoz. A felhasználó közreműködésére szükség van, mint a kézi telepítésnél (1. fejezet - *Installation with YaST* (↑*Start-Up*)).

E telepítési típus esetén a következő követelményeket kell teljesíteni:

- Távoli telepítési forrás: NFS, HTTP, FTP vagy SMB, működő hálózati kapcsolattal.
- Célrendszer működő hálózati kapcsolattal.
- Vezérlőrendszer működő hálózati kapcsolattal, valamint VNC-megjelenítő szoftver vagy Javát futtatni képes böngésző (Firefox, Konqueror, Internet Explorer vagy Opera).
- Fizikai adathordozó (CD vagy DVD) a célrendszer elindításához.
- Érvényes statikus IP-címek, már hozzárendelve a telepítési forráshoz és a vezérlőrendszerhez.
- Érvényes statikus IP-cím a célrendszerhez rendeléshez.

E telepítési típus végrehajtása:

1. Állítsa be a telepítési forrást (1.2. - A telepítési forrásokat tároló kiszolgáló beállítása (12. oldal)). Válasszon ki egy NFS, HTTP vagy FTP hálózati kiszolgálót.

SMB telepítési forrás esetén itt talál útmutatást: 1.2.5. - SMB telepítési forrás kezelése (20. oldal).

2 Indítsa el a célrendszert az openSUSE telepítőcsomag első CD-jéről vagy DVD-jéről.

3 Amikor megjelenik a rendszerindítási képernyő a célrendszeren, használja a rendszerindítási parancssort a megfelelő VNC-beállítások, illetve a telepítési forrás címének megadásához. Ennek részletes leírása: 1.4. - A célrendszer elindítása telepítéshez (33. oldal).

   A célrendszer egy szöveges környezetben indul el, megadva azt a hálózati címet és kijelzőszámot, amely alatt a grafikus telepítési környezet megcímezhető a VNC-megjelenítő alkalmazással vagy böngészővel. A VNC-s telepítések OpenSLP-n keresztül hirdetik meg magukat és ha a tűzfalbeállítások megengedik, Konqueror alatt a `service:/` vagy `slp:/` módban meg is találhatók.

4 A vezérlő munkaállomáson nyisson meg egy VNC-megjelenítő alkalmazást vagy webböngészőt és csatlakozzon a célrendszerhez (1.5.1. - Telepítés VNC-vel (36. oldal)).

5 Hajtsa végre a telepítést a leírt módon (1. fejezet - *Installation with YaST* (↑*Start-Up*)). Csatlakozzon újra a célrendszerhez, miután az újraindult a telepítés utolsó fázisának végrehajtásához.

6 Fejezze be a telepítést.

1.1.2 Egyszerű távoli telepítés VNC-n keresztül – dinamikus hálózati beállítások

Ehhez a fajta telepítéshez továbbra is szükséges kismértékben fizikailag hozzáférni a célrendszerhez, a rendszer elindításához. A hálózati beállítás DHCP segítségével történik. A telepítés vezérlése teljes egészében egy távoli munkaállomásról történik, VNC-vel csatlakozva a telepítőhöz, de a felhasználó közreműködésére továbbra is szükség van a tényleges beállításokhoz.

E telepítési típus esetén a következő követelményeket kell teljesíteni:

- Távoli telepítési forrás: NFS, HTTP, FTP vagy SMB, működő hálózati kapcsolattal.
- Célrendszer működő hálózati kapcsolattal.
- Vezérlőrendszer működő hálózati kapcsolattal, valamint VNC-megjelenítő szoftver vagy Javát futtatni képes böngésző (Firefox, Konqueror, Internet Explorer vagy Opera).
- Fizikai adathordozó (CD, DVD vagy egyedi rendszerindító lemez) a célrendszer elindításához).
- Futó, IP-címeket osztó DHCP-kiszolgáló.

E telepítési típus végrehajtása:

1. Állítsa be a telepítési forrást (1.2. - A telepítési forrásokat tároló kiszolgáló beállítása (12. oldal)). Válasszon ki egy NFS, HTTP vagy FTP hálózati kiszolgálót. SMB telepítési forrás esetén itt talál útmutatást: 1.2.5. - SMB telepítési forrás kezelése (20. oldal).

2. Indítsa el a célrendszert az openSUSE telepítőcsomag első CD-jéről vagy DVD-jéről.

3. Amikor megjelenik a rendszerindítási képernyő a célrendszeren, használja a rendszerindítási parancssort a megfelelő VNC-beállítások, illetve a telepítési forrás címének megadásához. Ennek részletes leírása: 1.4. - A célrendszer elindítása telepítéshez (33. oldal).

   A célrendszer egy szöveges környezetben indul el, megadva azt a hálózati címet és kijelzőszámot, amely alatt a grafikus telepítési környezet megcímezhető a VNC-megjelenítő alkalmazással vagy böngészővel. A VNC-s telepítések OpenSLP-n keresztül hirdetik meg magukat és ha a tűzfalbeállítások megengdik, Konqueror alatt a `service:/` vagy `slp:/` módban meg is találhatók.

4. A vezérlő munkaállomáson nyisson meg egy VNC-megjelenítő alkalmazást vagy webböngészőt és csatlakozzon a célrendszerhez (1.5.1. - Telepítés VNC-vel (36. oldal)).

5. Hajtsa végre a telepítést a leírt módon (1. fejezet - *Installation with YaST* (↑*Start-Up*)). Csatlakozzon újra a célrendszerhez, miután az újraindult a telepítés utolsó fázisának végrehajtásához.

6 Fejezze be a telepítést.

1.1.3 Távoli telepítés VNC-n keresztül – PXE-s rendszerindítás és Wake-on-LAN

Ennél a telepítési típusnál egyáltalán nem kell hozzáférni a számítógéphez fizikailag. A célgép elindítása és újraindítása is távolról történik. A felhasználó közreműködésére csak a tényleges telepítéshez van szükség. Ez a megközelítés használható többtelephelyes környezetekben is.

E telepítési típus esetén a következő követelményeket kell teljesíteni:

- Távoli telepítési forrás: NFS, HTTP, FTP vagy SMB, működő hálózati kapcsolattal.
- TFTP-kiszolgáló.
- A hálózatban működő DHCP-kiszolgáló.
- PXE-rendszerindításra, hálózati csatlakozásra és Wake on LAN funkcióra képes célrendszer, áram alá helyezve és a hálózatra csatlakoztatva.
- Vezérlőrendszer működő hálózati kapcsolattal, valamint VNC-megjelenítő szoftver vagy Javát futtatni képes böngésző (Firefox, Konqueror, Internet Explorer vagy Opera).

E telepítési típus végrehajtása:

1 Állítsa be a telepítési forrást (1.2. - A telepítési forrásokat tároló kiszolgáló beállítása (12. oldal)). Válasszon egy NFS, HTTP vagy FTP hálózati kiszolgálót, vagy állítson be egy SMB telepítési forrást a leírás szerint (1.2.5. - SMB telepítési forrás kezelése (20. oldal)).

2 Állítson be egy TFTP-kiszolgálót, amelyik a rendszerindításhoz szükséges rendszerképet tartalmazza (ezt fogja letölteni a célrendszer). Ennek leírása: 1.3.2. - TFTP-kiszolgáló beállítása (25. oldal).

3 Állítson be egy DHCP-kiszolgálót, amely ad IP-címet minden gépnek és amely képes tudatni a TFTP-kiszolgáló helyét a célrendszerrel. Ennek leírása: 1.3.1. - DHCP-kiszolgáló (22. oldal).

4 Készítse fel a célrendszert PXE-rendszerindításra. Ennek részletes leírása: 1.3.5. - A célrendszer felkészítése PXE rendszerindításra (32. oldal).

5 Kezdeményezze a célrendszeren a rendszerindítási folyamatot Wake on LAN funkció használatával. Ennek leírása: 1.3.7. - Wake on LAN (32. oldal).

6 A vezérlő munkaállomáson nyisson meg egy VNC-megjelenítő alkalmazást vagy webböngészőt és csatlakozzon a célrendszerhez (1.5.1. - Telepítés VNC-vel (36. oldal)).

7 Hajtsa végre a telepítést a leírt módon (1. fejezet - *Installation with YaST* (↑*Start-Up*)). Csatlakozzon újra a célrendszerhez, miután az újraindult a telepítés utolsó fázisának végrehajtásához.

8 Fejezze be a telepítést.

1.1.4 Egyszerű távoli telepítés SSH-n keresztül – statikus hálózati beállítások

Ehhez a fajta telepítéshez továbbra is szükséges kismértékben fizikailag hozzáférni a célrendszerhez, a telepítés elindításához, valamint a telepítési cél IP-címének megállapításához. Magát a telepítést aztán teljes mértékben lehet egy távoli munkaállomásról vezérelni, SSH-n keresztül kapcsolódva a telepítőprogramhoz. A felhasználó közreműködésére szükség van, mint a szokásos telepítésnél (1. fejezet - *Installation with YaST* (↑*Start-Up*)).

E telepítési típus esetén a következő követelményeket kell teljesíteni:

- Távoli telepítési forrás: NFS, HTTP, FTP vagy SMB, működő hálózati kapcsolattal.
- Célrendszer működő hálózati kapcsolattal.
- Vezérlőrendszer működő hálózati kapcsolattal és működő SSH-kliensszoftverrel.
- Fizikai adathordozó (CD, DVD vagy egyedi rendszerindító lemez) a célrendszer elindításához.
- Érvényes statikus IP-címek, már hozzárendelve a telepítési forráshoz és a vezérlőrendszerhez.

- Érvényes statikus IP-cím a célrendszerhez rendeléshez.

E telepítési típus végrehajtása:

1. Állítsa be a telepítési forrást (1.2. - A telepítési forrásokat tároló kiszolgáló beállítása (12. oldal)). Válasszon ki egy NFS, HTTP vagy FTP hálózati kiszolgálót. SMB telepítési forrás esetén itt talál útmutatást: 1.2.5. - SMB telepítési forrás kezelése (20. oldal).

2. Indítsa el a célrendszert az openSUSE telepítőcsomag első CD-jéről vagy DVD-jéről.

3. Amikor megjelenik a rendszerindítási képernyő a célrendszeren, használja a rendszerindítási parancssort a hálózati kapcsolat megfelelő paramétereinek, a telepítési forrás címének, illetve az SSH használatának a megadásához. Ennek részletes leírása: 1.4.2. - Egyéni rendszerindítási paraméterek használata (33. oldal).

   A célrendszer egy szöveges környezetben indul el, megadva a hálózati címet, amely alatt a grafikus telepítési környezet elérhető bármely SSH klienssel.

4. A vezérlő munkaállomáson nyisson meg egy terminálablakot és csatlakozzon a célrendszerhez („Csatlakozás a telepítőprogramhoz” szakasz (39. oldal)).

5. Hajtsa végre a telepítést a leírt módon (1. fejezet - *Installation with YaST* (↑*Start-Up*)). Csatlakozzon újra a célrendszerhez, miután az újraindult a telepítés utolsó fázisának végrehajtásához.

6. Fejezze be a telepítést.

1.1.5 Egyszerű távoli telepítés SSH-n keresztül – dinamikus hálózati beállítások

Ehhez a fajta telepítéshez továbbra is szükséges kismértékben fizikailag hozzáférni a célrendszerhez, a telepítés elindításához, valamint a telepítési cél IP-címének megállapításához. A telepítés vezérlése teljes egészében egy távoli munkaállomásról történik,

VNC-vel csatlakozva a telepítőhöz, de a felhasználó közreműködésére továbbra is szükség van a tényleges beállításokhoz.

E telepítési típus esetén a következő követelményeket kell teljesíteni:

- Távoli telepítési forrás: NFS, HTTP, FTP vagy SMB, működő hálózati kapcsolattal.
- Célrendszer működő hálózati kapcsolattal.
- Vezérlőrendszer működő hálózati kapcsolattal és működő SSH-kliensszoftverrel.
- Fizikai adathordozó (CD vagy DVD) a célrendszer elindításához.
- Futó, IP-címeket osztó DHCP-kiszolgáló.

E telepítési típus végrehajtása:

1. Állítsa be a telepítési forrást (1.2. - A telepítési forrásokat tároló kiszolgáló beállítása (12. oldal)). Válasszon ki egy NFS, HTTP vagy FTP hálózati kiszolgálót. SMB telepítési forrás esetén itt talál útmutatást: 1.2.5. - SMB telepítési forrás kezelése (20. oldal).

2. Indítsa el a célrendszert az openSUSE telepítőcsomag első CD-jéről vagy DVD-jéről.

3. Amikor megjelenik a rendszerindítási képernyő a célrendszeren, használja a rendszerindítási parancssort a hálózati kapcsolat megfelelő paramétereinek, a telepítési forrás helyének, illetve az SSH használatának a megadásához. A paraméterek használatával kapcsolatos részletes útmutatás: 1.4.2. - Egyéni rendszerindítási paraméterek használata (33. oldal)

   A célrendszer egy szöveges környezetben indul el, megadva a hálózati címet, amely alatt a grafikus telepítési környezet elérhető bármely SSH klienssel.

4. A vezérlő munkaállomáson nyisson meg egy terminálablakot és csatlakozzon a célrendszerhez („Csatlakozás a telepítőprogramhoz” szakasz (39. oldal)).

5. Hajtsa végre a telepítést a leírt módon (1. fejezet - *Installation with YaST* (↑*Start-Up*)). Csatlakozzon újra a célrendszerhez, miután az újraindult a telepítés utolsó fázisának végrehajtásához.

6. Fejezze be a telepítést.

1.1.6 Távoli telepítés SSH-n keresztül – PXE-s rendszerindítás és Wake-on-LAN

Ennél a telepítési típusnál egyáltalán nem kell hozzáférni a számítógéphez fizikailag. A célgép elindítása és újraindítása is távolról történik.

E telepítési típus esetén a következő követelményeket kell teljesíteni:

- Távoli telepítési forrás: NFS, HTTP, FTP vagy SMB, működő hálózati kapcsolattal.
- TFTP-kiszolgáló.
- Működő DHCP-kiszolgáló a hálózatban, amelyik statikus IP-címet ad a telepítendő gépnek.
- PXE-rendszerindításra, hálózati csatlakozásra és Wake on LAN funkcióra képes célrendszer, áram alá helyezve és a hálózatra csatlakoztatva.
- Vezérlőrendszer működő hálózati kapcsolattal és SSH-kliensszoftverrel.

E telepítési típus végrehajtása:

1. Állítsa be a telepítési forrást (1.2. - A telepítési forrásokat tároló kiszolgáló beállítása (12. oldal)). Válasszon ki egy NFS, HTTP vagy FTP hálózati kiszolgálót. SMB telepítési forrás beállításával kapcsolatban itt talál útmutatást: 1.2.5. - SMB telepítési forrás kezelése (20. oldal).
2. Állítson be egy TFTP-kiszolgálót, amelyik a rendszerindításhoz szükséges rendszerképet tartalmazza (ezt fogja letölteni a célrendszer). Ennek leírása: 1.3.2. - TFTP-kiszolgáló beállítása (25. oldal).
3. Állítson be egy DHCP-kiszolgálót, amely ad IP-címet minden gépnek és amely képes tudatni a TFTP-kiszolgáló helyét a célrendszerrel. Ennek leírása: 1.3.1. - DHCP-kiszolgáló (22. oldal).
4. Készítse fel a célrendszert PXE-rendszerindításra. Ennek részletes leírása: 1.3.5. - A célrendszer felkészítése PXE rendszerindításra (32. oldal).
5. Kezdeményezze a célrendszeren a rendszerindítási folyamatot Wake on LAN funkció használatával. Ennek leírása: 1.3.7. - Wake on LAN (32. oldal).

6 A vezérlő munkaállomáson indítson el egy SSH-klienst és csatlakozzon a célrendszerhez (1.5.2. - Telepítés SSH-n keresztül (38. oldal)).

7 Hajtsa végre a telepítést a leírt módon (1. fejezet - *Installation with YaST* (↑*Start-Up*)). Csatlakozzon újra a célrendszerhez, miután az újraindult a telepítés utolsó fázisának végrehajtásához.

8 Fejezze be a telepítést.

1.2 A telepítési forrásokat tároló kiszolgáló beállítása

Az openSUSE hálózati telepítési forrásaként használt gépen futó operációs rendszertől függően többféle lehetőség is rendelkezésre áll a kiszolgáló beállításához. SUSE Linux 9.3 és frissebb rendszereken egy telepítési kiszolgáló beállításának legegyszerűbb módja a YaST használata.

TIPP

Akár Microsoft Windows gép is használható a linuxos üzembe helyezés telepítési kiszolgálójaként. Részletek: 1.2.5. - SMB telepítési forrás kezelése (20. oldal).

1.2.1 Telepítési kiszolgáló beállítása a YaST segítségével

A YaST egy grafikus eszközt kínál a hálózati telepítési források létrehozásához. HTTP, FTP és NFS hálózati telepítési kiszolgálók használatát támogatja.

1 Jelentkezzen be `root` felhasználóként a telepítési kiszolgálóként használni kívánt gépre.

2 Telepítse a `yast2-instserver` csomagot.

3 Indítsa el a *YaST* > *Vegyes* > *Telepítési kiszolgáló* modulját.

4 Válassza ki a kiszolgáló típusát (HTTP, FTP vagy NFS). A kiválasztott szolgáltatás automatikusan elindul minden egyes alkalommal a rendszer indulásakor. Ha a kiválasztott típusú szolgáltatás már fut a rendszeren és kézzel akarja beállítani a kiszolgálót, tiltsa le a szolgáltatás automatikus konfigurációját a *Semmilyen hálózati szolgáltatást ne állítson be* pont megjelölésével. Mindkét esetben adja meg a könyvtárat, amelyből a kiszolgálón a telepítési adatok elérhetők.

5 Állítsa be a kívánt kiszolgálótípust. Ez a lépés a kiszolgáló szolgáltatásainak automatikus beállításához kapcsolódik. Ha az automatikus beállítás ki van kapcsolva, akkor ez a lépés kimarad.

Adjon meg egy másodlagos nevet azon FTP vagy HTTP-kiszolgáló gyökérkönyvtárához, amelyiken a telepítési adatok találhatók. A telepítési forrás később az `ftp://`*`kiszolgáló-IP`*`/`*`Másodlagos_név`*`/`*`Név* (FTP) vagy `http://`*`kiszolgáló-IP`*`/`*`Másodlagos_név`*`/`*`Név* (HTTP) cím alatt lesz elérhető. A *`Név`* helyére a telepítési forrás nevét kell beírni; ezt a következő lépésben állítjuk be. Ha az előző lépésben NFS-t választott, akkor adja meg a dzsókerneveket és az exportálási paramétereket. Az NFS-kiszolgáló az `nfs://`*`kiszolgáló-IP`*`/`*`Név* cím alatt lesz majd elérhető. Az NFS-sel és az exportokkal kapcsolatos részletek: 27. fejezet - *Fájlrendszer megosztása NFS-sel* (435. oldal).

TIPP: Tűzfalbeállítások

Győződjön meg róla, hogy a kiszolgálórendszer tűzfalbeállításai átengedik a HTTP, NFS és FTP portok forgalmát. Ha nem tennék, akkor indítsa el a YaST tűzfal modulját és nyissa ki a megfelelő portokat.

6 Állítsa be a telepítési forrást. Még mielőtt a telepítési adathordozót átmásolná a helyére, adja meg a telepítési forrás nevét (ideális esetben ez a termék és a verziószám egy könnyen megjegyezhető rövidítése). A YaST engedi ISO-rendszerképek használatát a telepítő CD-k konkrét példányai helyett. Ha ezt a megoldást kívánja alkalmazni, jelölje meg a megfelelő négyzetet és adja meg azt a könyvtárelérési utat, ahol az ISO-fájlok helyileg találhatók. Attól függően, hogy milyen terméket oszt szét ezzel a telepítési kiszolgálóval, szükség lehet további kiegészítő vagy szervizcsomag CD-kre. Ezeket extra telepítési forrásokként fel kell venni. A telepítési kiszolgáló OpenSLP-n keresztüli meghirdetéséhez a hálózaton jelölje meg a megfelelő pontot.

TIPP

Ha a hálózati beállítások lehetővé teszik, érdemes megfontolni a telepítési forrás OpenSLP-n keresztüli meghirdetését. Ebben az esetben nem kell majd megadni minden egyes gépen külön a hálózati telepítés elérési útját. A célrendszereket egyszerűen csak el kell indítani az SLP rendszerindítási paraméterrel és minden további konfiguráció nélkül meg fogják találni a hálózati telepítési forrást. A beállítás részletei: 1.4. - A célrendszer elindítása telepítéshez (33. oldal).

7 Töltse fel a telepítési adatokat. A telepítési kiszolgáló beállításának leghosszabb lépése a tényleges telepítő CD-k felmásolása. Helyezze be az adathordozókat a YaST által kért sorrendben és várja meg, hogy a másolás befejeződjön. Az összes forrás teljes átmásolása után lépjen vissza a meglévő információs források összegző képernyőjére és zárja be a konfigurációs ablakot a *Befejezés* gombra kattintva.

A telepítési kiszolgáló ezzel be van állítva és készen áll kiszolgálni a szükséges adatokat. Automatikusan el lesz indítva a rendszer minden egyes indításakor. További beavatkozásra nincs szükség. A szolgáltatást csak akkor kell kézzel beállítani és elindítani, ha az első lépésként a YaST-ban letiltotta a kiválasztott hálózati szolgáltatás automatikus beállítását.

Egy telepítési forrás lekapcsolásához válassza ki az eltávolítani kívánt telepítési forrást, majd nyomja meg a *Törlés* gombot. A telepítési adatok törlődnek a rendszerről. A hálózati szolgáltatás deaktiválásához használja a megfelelő YaST-modult.

Ha a telepítési kiszolgáló egynél több termék számára biztosít telepítési adatokat, akkor indítsa el a YaST telepítési kiszolgáló modulját és a meglévő telepítési források ablakában nyomja meg a *Hozzáadás* gombot az új telepítési forrás beállításához.

1.2.2 NFS telepítési forrás beállítása kézzel

Az NFS telepítési forrás beállítása lényegében két lépésben történik. Az első lépésben hozza létre a telepítési adatokat tartalmazó könyvtárstruktúrát és másolja át a telepítési adathordozó tartalmát ebbe a struktúrába. Második lépésként exportálja a telepítési·adatokat tartalmazó könyvtárat a hálózaton.

A telepítési·adatokat tartalmazó könyvtár létrehozása:

1. Jelentkezzen be `root` felhasználóként.

2. Hozzon létre egy könyvtárat, amely majd a telepítési adatokat tárolni fogja és váltson át ebbe a könyvtárba. Például:

   ```
   mkdir install/product/productversion
   cd install/product/productversion
   ```

   A *`product`* helyére a termék nevének a rövidítését írja, a *`productversion`* pedig egy olyan karaktersorozat legyen, amelyik a termék nevét és verzióját tartalmazza.

3. A telepítőcsomag minden egyes CD-jéhez hajtsa végre a következő parancsokat:

   3a Másolja a telepítő CD teljes tartalmát a telepítési kiszolgáló könyvtárába:

   ```
   cp -a /media/path_to_your_CD-ROM_drive .
   ```

   A *`path_to_your_CD-ROM_drive`* helyére a CD vagy DVD-meghajtó tényleges elérési útját kell írni. A használt meghajtó típusától függően ez lehet `cdrom`, `cdrecorder`, `dvd` vagy `dvdrecorder`.

   3b Nevezze át a könyvtárat a CD számára:

   ```
   mv path_to_your_CD-ROM_drive CDx
   ```

   Az *`x`* helyére a CD száma kerüljön.

openSUSE rendszeren a telepítési források NFS-exportálása YaST-tal is elvégezhető: A következő műveleteket hajtsa végre:

1. Jelentkezzen be `root` felhasználóként.

2. Indítsa el a *YaST* > *Hálózati szolgáltatások* > *NFS-kiszolgáló* modult.

3. Válassza ki a *Start* és *Tűzfalport megnyitása* modult, majd kattintson a *Tovább* gombra.

4. Válassza ki a *Könyvtár hozzáadása* pontot és keresse ki a telepítési forrásokat tartalmazó könyvtárat, a jelen esetben a *`productversion`*-t.

5 Válassza ki a *Gép hozzáadása* pontot és adja meg azon gépek neveit, amelyekre exportálni kívánja a telepítési·adatokat. Gépnevek helyett dzsókerneveket, hálózati címtartományokat, vagy akár csak a hálózat tartománynevét is megadhatja. Adja meg a kívánt exportálási beállításokat, vagy hagyja meg az alapértelmezett értékeket (a legtöbb esetben teljesen megfelelők). További információ az NFS-megosztások szintaxisáról az `exports` kézikönyvoldalon olvasható.

6 Kattintson a *Befejezés* gombra. Az openSUSE telepítési forrásokat tároló NFS-kiszolgáló automatikusan elindul és beépül a rendszerindítási folyamatba.

Ha inkább kézzel kívánja exportálni a telepítési forrásokat NFS-en keresztül, nem a YaST NFS-kiszolgáló moduljával:

1 Jelentkezzen be `root` felhasználóként.

2 Nyissa meg az `/etc/exports` fájlt és írja be az alábbi sort:

```
/productversion *(ro,root_squash,sync)
```

Ez a */productversion* könyvtárat exportálja minden olyan gépre, amelyik része a hálózatnak vagy csatlakozni tud a kiszolgálóhoz. A kiszolgáló elérésének korlátozásához használjon hálózati maszkokat vagy tartományneveket az általános `*` dzsókernév helyett. További részletek az `export` kézikönyvoldalon olvashatók. Mentse el a konfigurációs fájlt és lépjen ki a szerkesztőből.

3 Ahhoz, hogy az NFS szolgáltatás bekerüljön a rendszerindításkor elindított kiszolgálók listájába, adja ki a következő parancsokat:

```
insserv /etc/init.d/nfsserver
insserv /etc/init.d/portmap
```

4 Indítsa el az NFS-kiszolgálót az `rcnfsserver start` paranccsal. Ha módosítania kell később az NFS-kiszolgáló beállításain, írja át a konfigurációs fájlt, majd indítsa újra az NFS démont az `rcnfsserver restart` paranccsal.

Az NFS-kiszolgálót OpenSLP-n keresztül meghirdetve a hálózat összes kliense egyszerűen megtudhatja a címét.

1 Jelentkezzen be `root` felhasználóként.

2 Lépjen be az `/etc/slp.reg.d/` könyvtárba.

3 Hozzon létre egy `install.suse.nfs.reg` nevű konfigurációs fájlt, benne az alábbi sorokkal:

```
# Register the NFS Installation Server
service:install.suse:nfs://$HOSTNAME/path_to_instsource/CD1,en,65535
description=NFS Installation Source
```

A *`path_to_instsource`* helyére a telepítési forrás tényleges helyét írja a kiszolgálón.

4 Mentse el a konfigurációs fájlt és indítsa el az OpenSLP démont (`rcslpd start`).

További információ az OpenSLP-ről a csomag dokumentációjában, az `/usr/share/doc/packages/openslp/` fájlban található, illetve az 21. fejezet - *SLP-szolgáltatások a hálózatban* (337. oldal) részben. További információ az NFS-ről: 27. fejezet - *Fájlrendszer megosztása NFS-sel* (435. oldal)

1.2.3 FTP telepítési forrás beállítása kézzel

Az FTP telepítési forrás létrehozása nagyon hasonlít az NFS telepítési forráséhoz. Az FTP telepítési források szintén meghirdethetők a hálózaton OpenSLP-vel.

1 Hozzon létre egy könyvtárat a telepítési forrásokhoz a leírt módon (1.2.2. - NFS telepítési forrás beállítása kézzel (14. oldal)).

2 Állítsa be az FTP-kiszolgálót, hogy kiszolgálja a telepítés könyvtár tartalmát:

2a Jelentkezzen be `root` felhasználóként és telepítse a `vsftpd` csomagot a YaST csomagkezelőjével.

2b Lépjen be az FTP-kiszolgáló gyökérkönyvtárába:

```
cd /srv/ftp
```

2c Hozzon létre egy alkönyvtárat az FTP gyökérkönyvtárában a telepítési források számára:

```
mkdir instsource
```

Az *instsource* helyére a termék neve kerüljön.

2d Csatolja fel a telepítési adattár tartalmát az FTP-kiszolgáló chroot-környezetébe:

```
mount --bind path_to_instsource /srv/ftp/instsource
```

A *path_to_instsource* és *instsource* helyére a telepített rendszernek megfelelő paraméterek kerüljenek. A módosítás állandósításához vegye fel az `/etc/fstab` fájlba.

2e Indítsa el a vsftpd-t a `vsftpd` paranccsal.

3 Hirdesse meg a telepítési forrást OpenSLP-n keresztül, ha ezt támogatják a hálózati beállítások:

3a Hozzon létre egy `install.suse.ftp.reg` nevű konfigurációs fájlt az `/etc/slp.reg.d/` könyvtárban, az alábbi sorokkal:

```
# Register the FTP Installation Server
service:install.suse:ftp://$HOSTNAME/srv/ftp/instsource/CD1,en,65535
description=FTP Installation Source
```

Az *instsource* helyére a kiszolgálón lévő telepítési forrás könyvtár tényleges neve kerüljön. A `service:` sort egy hosszú, folytonos sorként kell beírni.

3b Mentse el a konfigurációs fájlt és indítsa el az OpenSLP démont (`rcslpd start`).

TIPP: FTP-kiszolgáló beállítása YaST segítségével

Ha jobban kedveli a YaST használatát az FTP telepítési kiszolgáló kézzel való beállításánál, akkor a 29. fejezet - *FTP-kiszolgáló beállítása a YaST segítségével* (495. oldal) részben olvashat további részleteket a YaST FTP-kiszolgáló moduljának használatáról.

1.2.4 HTTP telepítési forrás beállítása kézzel

A HTTP telepítési forrás létrehozása nagyon hasonlít az NFS telepítési forráséhoz. A HTTP telepítési források szintén meghirdethetők a hálózaton OpenSLP-vel.

1 Hozzon létre egy könyvtárat a telepítési forrásokhoz a leírt módon (1.2.2. - NFS telepítési forrás beállítása kézzel (14. oldal)).

2 Állítsa be a HTTP-kiszolgálót, hogy kiszolgálja a telepítés könyvtár tartalmát:

2a Telepítse az Apache webkiszolgálót a 28.1.2. - Telepítés (452. oldal) leírtak szerint.

2b Lépjen be a HTTP-kiszolgáló gyökérkönyvtárába (`/srv/www/htdocs`) és hozzon létre egy alkönyvtárat a telepítési forrásoknak:

```
mkdir instsource
```

Az *instsource* helyére a termék neve kerüljön.

2c Hozzon létre egy szimbolikus láncot a telepítési források helyétől a webkiszolgáló gyökérkönyvtárába (`/srv/www/htdocs`):

```
ln -s /path_instsource /srv/www/htdocs/instsource
```

2d Módosítsa a HTTP-kiszolgáló konfigurációs fájlját (`/etc/apache2/default-server.conf`), hogy kövesse a szimbolikus láncokat. Cserélje le az alábbi sort:

```
Options None
```

módja

```
Options Indexes FollowSymLinks
```

2e Töltse újra a HTTP-kiszolgáló konfigurációját a `rcapache2 reload` paranccsal.

3 Hirdesse meg a telepítési forrást OpenSLP-n keresztül, ha ezt támogatják a hálózati beállítások:

3a Hozzon létre egy `install.suse.ftp.reg` nevű konfigurációs fájlt az `/etc/slp.reg.d/` könyvtárban, az alábbi sorokkal:

```
# Register the HTTP Installation Server
service:install.suse:http://$HOSTNAME/srv/www/htdocs/instsource/CD1/,en,65535
description=HTTP Installation Source
```

Az *`instsource`* helyére a kiszolgálón lévő telepítési forrás tényleges elérési útja kerüljön. A `service:` sort egy hosszú, folytonos sorként kell beírni.

3b Mentse el a konfigurációs fájlt és indítsa el az OpenSLP démont az `rcslpd start` paranccsal.

1.2.5 SMB telepítési forrás kezelése

SMB használatával a telepítési források akár egy Microsoft Windows kiszolgálóról is importálhatók és a linuxos üzembe helyezés úgy is elindítható, hogy nincs is a környéken linuxos gép.

Az openSUSE telepítési forrásokat tartalmazó exportált windowsos megosztás beállítása:

1. Jelentkezzen be a windowsos gépre.
2. Indítsa el az Intézőt és hozzon létre egy új mappát, amely a teljes telepítési fát tárolni fogja és nevezze el például `INSTALL`-nak.
3. Exportálja a megosztást a Windows-dokumentációban leírtak szerint.
4. Lépjen bele a megosztásba és hozzon létre egy *`termék`* nevű almappát. A *`termék`* helyére persze a termék valódi nevét írja.
5. Lépjen bele az `INSTALL/`*`termék`* mappába és másolja át az egyes CD-ket vagy DVD-ket egy-egy külön, például `CD1` és `CD2` nevű mappába.

SMB-n csatolt megosztás telepítési forrásként történő használata:

1. Indítsa el a telepítési célt.
2. Válassza ki a *Telepítés* menüpontot.
3. Nyomja meg az F4 gombot a telepítési források megadásához.
4. Válassza ki az SMB lehetőséget és adja meg a windowsos gép nevét vagy IP-címét, a megosztás nevét (`INSTALL/termék/CD1`, a fenti példában), az eléréséhez szükséges felhasználónevet és jelszót.

   Az Enter leütése után elindul a YaST és elvégezheti a telepítést.

1.2.6 A telepítési adathordozó ISO rendszerképeinek használata a kiszolgálón

A fizikai adathordozók a kiszolgáló könyvtárába való kézzel átmásolása helyett fel is csatolhatja a telepítési adathordozó ISO rendszerképeit a telepítési kiszolgálóra és használhatja azokat telepítési forrásként. HTTP, NFS vagy FTP-kiszolgáló beállítása ISO rendszerképek használatára az adathordozó másolatai helyett:

1. Töltse le az ISO-rendszerképeket és mentse el a telepítési kiszolgálóként használt gépre.
2. Jelentkezzen be `root` felhasználóként.
3. Válasszon ki vagy hozzon létre egy megfelelő helyet a telepítési adatokhoz, a 1.2.2. - NFS telepítési forrás beállítása kézzel (14. oldal), 1.2.3. - FTP telepítési forrás beállítása kézzel (17. oldal) vagy 1.2.4. - HTTP telepítési forrás beállítása kézzel (19. oldal) részekben leírt módon.
4. Hozzon létre alkönyvtárakat az egyes CD-khez vagy DVD-khez.
5. Az egyes ISO rendszerképek felcsatolásához és a végső helyre kicsomagolásukhoz adja ki a következő parancsot:

   ```
   mount -o loop path_to_iso path_to_instsource/product/mediumx
   ```

A *path_to_iso* helyére az ISO rendszerkép helyi példányának elérési útja kerüljön, a *path_to_instsource* helyére a kiszolgáló forráskönyvtára, a *product* helyére a termék neve és a *mediumx* helyére a használt adathordozó típusa (CD vagy DVD) és száma.

6 Ismételje meg az előző lépést a termék összes szükséges ISO rendszerképének felcsatolásához.

7 Indítsa el a telepítési kiszolgálót a szokásos módon (1.2.2. - NFS telepítési forrás beállítása kézzel (14. oldal), 1.2.3. - FTP telepítési forrás beállítása kézzel (17. oldal) vagy 1.2.4. - HTTP telepítési forrás beállítása kézzel (19. oldal)).

Az ISO-képfájlok automatikus felcsatolásához rendszerindításkor, vegye fel a megfelelő csatolási bejegyzéseket az `/etc/fstab` fájlba. A korábbi példának megfelelő bejegyzés így nézne ki:

```
path_to_iso path_to_instsource/product
    medium auto loop
```

1.3 A célrendszer felkészítése indításra

Ebben a szakaszban az összetettebb rendszerindítási helyzetek konfigurációs feladatait tekintjük át. Azonnal használható beállítási példákat mutatunk DHCP, PXE rendszerindítás, TFTP és Wake on LAN használatával.

1.3.1 DHCP-kiszolgáló

A DHCP-kiszolgálót kétféleképpen lehet beállítani. openSUSE rendszereken a YaST grafikus felületet biztosít a folyamathoz. A felhasználók kézzel is módosíthatják a konfigurációs fájlokat. További információ a DHCP-kiszolgálókról: 23. fejezet - *DHCP* (369. oldal).

DHCP-kiszolgáló beállítása a YaST segítségével

Ahhoz, hogy elküldje a TFTP-kiszolgáló helyét is a hálózati klienseknek és megadja a telepítési célok által használandó rendszerképfájlt, két deklarációra lesz szükség a DHCP-kiszolgáló konfigurációjában.

1. Jelentkezzen be `root` felhasználóként a DHCP-kiszolgálót futtató gépre.
2. Indítsa el a *YaST* > *Hálózati szolgáltatások* > *DHCP-kiszolgáló* modulját.
3. Végezze el a beállítási varázslót a DHCP-kiszolgáló alapszintű beállításainak megadásához.
4. Válassza ki a *Szakértői beállítások* pontot, majd nyomja meg az *Igen* gombot, amikor a program figyelmezteti arra, hogy kilép az indító párbeszédablakból.
5. A *Beállított deklarációk* ablakban válassza ki az alhálózatot, amelyben az új rendszer lesz, majd kattintson a *Szerkesztés* gombra.
6. Az *Alhálózat beállítása* ablakban a *Hozzáadás* gombbal vegyen fel egy új paramétert az alhálózat beállításai közé.
7. Válassza ki a `filename` paramétert és értéknek adja meg, hogy `pxelinux.0`.
8. Vegyen fel még egy (`next-server`) paramétert, amelynek értéke legyen a TFTP-kiszolgáló címe.
9. Nyomja meg az *OK* és a *Befejezés* gombot a DHCP-kiszolgáló beállításainak befejezéséhez.

Ahhoz, hogy a DHCP statikus IP-címet adjon egy adott gépnek, lépjen be a DHCP-kiszolgáló konfigurációs moduljának *Szakértői beállítások* részébe (4. Lépés (23. oldal)) és vegyen fel egy új deklarációt a géptípushoz. Vegye fel a `hardware` és `fixed-address` paramétereket ebbe a gépdeklarációba és adja meg a megfelelő értékeket.

DHCP-kiszolgáló beállítása kézzel

A DHCP-kiszolgálónak összesen annyit kell csinálnia (azon túl, hogy automatikusan címet oszt a hálózati klienseknek), hogy meghirdeti a TFTP-kiszolgáló IP-címét és a fájl nevét, amelyet a célgép telepítési rutinjainak le kell tölteniük.

1. Jelentkezzen be `root` felhasználóként a DHCP-kiszolgálót futtató gépre.

2. Adja hozzá a következő sorokat a DHCP-kiszolgáló konfigurációs fájljához (`/etc/dhcpd.conf`):

   ```
   group {
     # PXE related stuff
     #
     # "next server" defines the tftp server that will be used
     next server ip_tftp_server:
     #
     # "filename" specifies the pxelinux image on the tftp server
     # the server runs in chroot under /srv/tftpboot
     filename  "pxelinux.0";
   }
   ```

   Az *`ip_of_the_tftp_server`* helyére a TFTP-kiszolgáló tényleges IP-címe kerüljön. További információ a `dhcpd.conf` paramétereiről a `dhcpd.conf` kézikönyvoldalaiban található.

3. Indítsa újra a DHCP-kiszolgálót (`rcdhcpd restart`).

Ha SSH-t akar majd használni a PXE és Wake on LAN telepítés távoli vezérléséhez, akkor kifejezetten adja meg azt az IP-címet, amelyet a DHCP a telepítési célnak adjon. Ehhez a fenti DHCP konfigurációt az alábbiakhoz hasonlóan kell módosítani:

```
group {
  # PXE related stuff
  #
  # "next server" defines the tftp server that will be used
  next server ip_tftp_server:
  #
  # "filename" specifies the pxelinux image on the tftp server
  # the server runs in chroot under /srv/tftpboot
  filename "pxelinux.0";
  host test { hardware ethernet mac_address;
              fixed-address some_ip_address; }
      }
```

A host utasítás adja meg a telepítési cél gépnevét. A gépnév és az IP-cím egy adott géphez kötéséhez ismernie kell (és meg kell adnia) a rendszer hardver- (MAC-) címét. A példában használt változókat cserélje le a környezetnek megfelelő tényleges értékekre.

A DHCP-kiszolgáló újraindítása után statikus IP-t ad a meghatározott gépnek, így lehet SSH-n keresztül csatlakozni hozzá.

1.3.2 TFTP-kiszolgáló beállítása

A TFTP-kiszolgáló beállítható a YaST-tal, illetve beállítható kézzel bármely Linux operációs rendszeren, amelyik támogatja az xinetd-t és a tftp-t. A TFTP-kiszolgáló fogja elküldeni a rendszerindításhoz szükséges rendszerképet a célrendszerre annak indulása után, miután kapott egy kérést.

TFTP-kiszolgáló beállítása a YaST segítségével

1. Jelentkezzen be `root` felhasználóként.
2. Telepítse a `yast2-tftp-server` csomagot.
3. Indítsa el a *YaST* > *Hálózati szolgáltatások* > *TFTP-kiszolgáló* modult és telepítse a szükséges csomagot.
4. Kattintson az *Engedélyezés* pontra, hogy a kiszolgáló biztosan el legyen indítva és bekerüljön a rendszerindítási rutinok közé. További tevékenységre nincs szükség ehhez. Az xinetd rendszerindításkor elindítja a tftpd-t is.
5. Kattintson a *Tűzfalport megnyitása* gombra a gépen futó tűzfal megfelelő portjának kinyitásához. Ha nem fut tűzfal a kiszolgálón, akkor ez a lehetőség nem áll rendelkezésre.
6. Kattintson a *Tallózás* gombra a rendszerkép könyvtárának kikereséséhez. Az alapértelmezett könyvtár `/tftpboot` létrejön és ezt választja ki a program automatikusan.
7. Kattintson a *Befejezés* gombra a beállítások elmentéséhez és a kiszolgáló elindításához.

TFTP-kiszolgáló beállítása kézzel

1. Jelentkezzen be `root` felhasználóként és telepítse a `tftp` és `xinetd` csomagokat.

2. Ha nem léteznének még, akkor hozza létre az `/srv/tftpboot` és `/srv/tftpboot/pxelinux.cfg` könyvtárakat.

3. Vegye fel a rendszerképhez szükséges fájlokat a leírás szerint (1.3.3. - PXE rendszerindítás használata (26. oldal)).

4. Módosítsa az xinetd konfigurációját (`/etc/xinetd.d/`) ahhoz, hogy a TFTP-kiszolgáló el legyen indítva rendszerindításkor:

   4a Ha még nem létezne, hozzzon létre egy `tftp` nevű fájlt a könyvtár alatt a `touch tftp` paranccsal. Ezután futtassa le a `chmod 755 tftp` parancsot.

   4b Nyissa meg a `tftp` fájlt és írja be a következő sorokat:

```
service tftp
{
        socket_type             = dgram
        protocol                = udp
        wait                    = yes
        user                    = root
        server                  = /usr/sbin/in.tftpd
        server_args             = -s /srv/tftpboot
        disable                 = no
}
```

   4c Mentse el a fájlt és indítsa újra az xinetd-t az `rcxinetd restart` paranccsal

1.3.3 PXE rendszerindítás használata

Műszaki háttérinformáció és a PXE teljes specifikációja megtalálható a Preboot Execution Environment (Rendszerindítás előtti végrehajtási környezet, PXE) specifikációjában (http://www.pix.net/software/pxeboot/archive/pxespec.pdf).

1 Váltson át a telepítési adattár könyvtárába és másolja át a `linux`, `initrd`, `message` és `memtest` fájlokat az `/srv/tftpboot` könyvtárba:

```
cp -a boot/loader/linux boot/loader/initrd
      boot/loader/message boot/loader/memtest /srv/tftpboot
```

2 Telepítse a `syslinux` csomagot közvetlenül a telepítő CD-kről vagy DVD-kről a YaST segítségével.

3 Másolja át az `/usr/share/syslinux/pxelinux.0` fájlt az`/srv/tftpboot` könyvtárba:

```
cp -a /usr/share/syslinux/pxelinux.0 /srv/tftpboot
```

4 Váltson át a telepítési adattár könyvtárába és másolja át az `isolinux.cfg` fájlt az `/srv/tftpboot/pxelinux.cfg/default` fájlba:

```
cp -a boot/loader/isolinux.cfg /srv/tftpboot/pxelinux.cfg/default
```

5 Módosítsa az `/srv/tftpboot/pxelinux.cfg/default` fájlt és törölje a `gfxboot`, `readinfo` és `framebuffer` kezdetű sorokat.

6 Szúrja be a következő bejegyzéseket az alapértelmezett `failsafe` és `apic` címkék hozzáfűzési soraiba:

`insmod=`*`kernelmodul`*
: Ezzel a bejegyzéssel lehet beírni a PXE-kliens hálózati telepítésének támogatásához szükséges hálózati kernelmodult. A *`kernelmodul`* helyére a hálózati eszközhöz tartozó modul nevét kell írni.

`netdevice=`*`interface`*
: Ez a bejegyzés adja meg a kliensen a hálózati telepítéshez használni kívánt hálózati csatolót. Csak akkor kell megadni, ha a kliensben egynél több hálózati kártya van. Egyetlen hálózati kártya esetén ez a bejegyzés kihagyható.

`install=nfs://`*`ip_instserver`*`/`*`path_instsource`*`/CD1`
: Ez a bejegyzés adja meg az NFS-kiszolgálót és a telepítési forrást a kliens telepítéséhez. Az *`ip_instserver`* helyére a telepítési kiszolgáló tényleges IP-címét kell írni. A *`path_instsource`* helyére pedig a telepítési források

tényleges elérési útját. A HTTP, FTP vagy SMB forrásokat hasonló módon kell megcímezni, csak a protokollelőtag változik (`http`, `ftp` vagy `smb`).

FONTOS

Ha át kell adni más rendszerindítási paramétereket is a telepítési rutinoknak, például az SSH vagy VNC rendszerindítási paramétereket, akkor fűzze őket az `install` bejegyzés végére. A paraméterek áttekintés és néhány példa: 1.4. - A célrendszer elindítása telepítéshez (33. oldal).

Egy példa az `/srv/tftpboot/pxelinux.cfg/default` fájlra. Adja meg a protokollelőtagot a hálózati beállításoknak megfelelő telepítési forrás szerint és adja meg a telepítőhöz csatlakozás módszerét (az `install` bejegyzés `vnc` és `vncpassword`, illetve `usessh` és `sshpassword` paraméterei). A `\` jellel elválasztott sorokat egy hosszú sorként kell beírni, a `\` jel nélkül.

```
default linux

# default
label linux
  kernel linux
     append initrd=initrd ramdisk_size=65536 \
     install=nfs://ip_instserver/path_instsource/product/CD1

# failsafe
label failsafe
  kernel linux
  append initrd=initrd ramdisk_size=65536 ide=nodma apm=off acpi=off \
  install=nfs://ip_instserver/path_instsource/product/CD1

# apic
label apic
  kernel linux
  append initrd=initrd ramdisk_size=65536 apic \
  install=nfs://ip_instserver/path_instsource/product/CD1

# manual
label manual
  kernel linux
  append initrd=initrd ramdisk_size=65536 manual=1

# rescue
label rescue
  kernel linux
  append initrd=initrd ramdisk_size=65536 rescue=1
```

```
#  memory test
label memtest
  kernel memtest

# hard disk
label harddisk
  localboot 0

implicit     0
display      message
prompt       1
timeout      100
```

Az *ip_instserver* és *path_instsource* helyére az adott rendszerben használt értékeket kell írni.

Az alábbi szakasz röviden összefoglalja a beállításban használt PXELINUX paramétereket. A rendelkezésre álló paraméterekről további információ a `syslinux` csomag dokumentációjában, az `/usr/share/doc/packages/syslinux/` fájlban olvasható.

1.3.4 PXELINUX beállítási paraméterek

Az itt felsorolt paraméterek a PXELINUX konfigurációs fájlban használhatóknak csupán egy részét képezik.

`DEFAULT` *kernel paraméterek...*
: Az alapértelmezett kernel parancssort adja meg. Ha a PXELINUX automatikusan indul, akkor úgy viselkedik, mintha az alapértelmezés utáni bejegyzéseket a rendszerindítási parancssorban írták volna be, azzal a különbséggel, hogy az automatikus rendszerindítást jelző auto paramétert mindig hozzáadja.

  Ha nem található konfigurációs fájl, vagy a konfigurációs fájlban nincs default bejegyzés, akkor az alapértelmezés a kernel neve „linux” paraméterek nélkül

`APPEND` *paraméterek...*
: Egy vagy több paraméter hozzáadása a kernel paranccsorához. Ezek mind az automatikus, mind a kézi rendszerindításoknál hozzáadódnak. A paraméterek a kernel paranccsorának a legelejére íródnak be, általában lehetővé téve, hogy a közvetlenül beírt kernelparaméterek felülbírálhassák őket.

LABEL *címke* KERNEL *rendszerkép* APPEND *paraméterek...*

Azt jelenti, hogy ha indítandó kernelként a *címke* lett beírva, akkor ehelyett a PXELINUX a *rendszerkép*-et indítsa el a megadott APPEND paraméterekkel, nem pedig a fájl globális szakaszában (az első LABEL parancs előtt) megadottakkal. A *rendszerkép* alapértelmezése ugyanaz, mint a *címkéé*, és ha nincs megadva APPEND bejegyzés, akkor az alapértelmezés a globális bejegyzés használata (ha van ilyen). Maximum 128 LABEL bejegyzés adható meg.

Ne feledje, hogy a GRUB a következő szintaxist használja:

```
title mytitle
  kernel my_kernel my_kernel_options
  initrd myinitrd
```

A PXELINUX viszont a következőt:

```
label mylabel
  kernel mykernel
  append myoptions
```

A címkék úgy csonkolódnak, mintha fájlnevek lennének és csonkolás után is egyedieknek kell maradniuk. Például a „v2.1.30” és „v2.1.31” címkéket a PXELINUX nem tudja megkülönböztetni, mert ugyanarra a DOS-fájlnévre csonkolódnak.

A kernelnek nem kell Linux-kernelnek lennie; lehet boot szektor vagy egy COMBOOT fájl is.

APPEND –

Semmit nem fűz hozzá. Az egyetlen kötőjel argumentummal kiadott APPEND bejegyzés egy LABEL szakaszban a globális APPEND bejegyzés felülírására használható.

LOCALBOOT *típus*

PXELINUX alatt a LOCALBOOT 0 megadása egy KERNEL bejegyzés helyett az adott címke meghívását jelenti. A kernel helyett a helyi lemez lesz elindítva.

Paraméter	Leírás
0	Normál rendszerindítás végrehajtása

Paraméter	Leírás
4	Helyi rendszerindítás végrehajtása úgy, hogy az Universal Network Driver Interface (UNDI) illesztőprogram rezidens marad a memóriában
5	Helyi rendszerindítás végrehajtása úgy, hogy a teljes PXE csomag, beleértve az UNDI illesztőprogramot is, rezidens marad a memóriában

Az egyéb értékek nincsenek megadva. Ha nem tudja, hogy mit jelent az UNDI vagy PXE csomag, adjon meg `0`-t.

`TIMEOUT` *időkorlát*

Azt adja meg, hogy a rendszerindítási parancssor meddig várjon az automatikus indítás előtt, tizedmásodpercben. Az időkorlát abban a pillanatban felülíródik, ha a felhasználó bármit megnyom a billentyűzeten, hiszen a rendszer azt feltételezi, hogy a felhasználó egy parancsot kezdett beírni. A 0 időkorlát megadása teljesen törli az időkorlátot (ez az alapértelmezés is). A maximális lehetséges időkorlátérték 35996 (egy kicsivel kevesebb, mint egy óra).

`PROMPT` *flag_val*

Ha a `flag_val` 0, akkor a rendszerindítási parancssor csak akkor jelenik meg, ha lenyomják a Shift vagy Alt billentyűt, vagy ha a Caps Lock vagy Scroll Lock be van állítva (ez az alapértelmezés). Ha a `flag_val` értéke 1, akkor mindig megjeleníti a rendszerindítási parancssort.

```
F2  filename
F1  filename
..etc...
F9  filename
F10 filename
```

A megadott fájlt megjeleníti a képernyőn, ha egy funkcióbillentyűt megnyomnak a rendszerindítási parancssorban. Ez használható például rendszerindítás előtti online súgó készítéséhez (feltehetőleg a kernel parancssori paramétereihez). A korábbi kiadásokkal való visszamenőleges kompatibilitás érdekében az F10 F0-ként is megadható. Ne feledje, hogy jelenleg nincs mód a fájlnevek az F11 és F12 billentyűkhöz rendelésére.

1.3.5 A célrendszer felkészítése PXE rendszerindításra

A rendszer BIOS-át fel kell készíteni PXE rendszerindításra: szerepeltesse a PXE menüpontot a BIOS rendszerindítási sorrendjében.

FIGYELEM: BIOS rendszerindítási sorrend

Ne tegye a BIOS-ban a PXE menüpontot a merevlemezes rendszerindítási menüpont elé. Ebben az esetben a rendszer minden egyes indításnál megpróbálná magát újratelepíteni.

1.3.6 A célrendszer felkészítése Wake on LAN használatára

A Wake on LAN (WOL) használatához a BIOS megfelelő beállítását engedélyezni kell még a telepítés előtt. Ezenfelül írja le a célrendszer MAC-címét is. Erre az adatra szükség lesz a Wake on LAN funkció indításához.

1.3.7 Wake on LAN

A WOL (wake on LAN) annak a lehetősége, hogy egy készenléti állapotban levő számítógépet elindítsunk a hálózaton keresztül egy speciális, a gép MAC-címét tartalmazó csomag segítségével. Mivel a világon elvileg minden gépnek egyedi MAC-azonosítója van, nem kell aggódni amiatt, hogy véletlenül a rossz gépet indítja el.

FONTOS: Wake on LAN más hálózati szegmensen

Ha a vezérlő gép nem ugyanazon a hálózati szegmensen található, mint a felébresztendő telepítési cél, akkor vagy multicastként kell beállítani a WOL-kéréseket, vagy távolról kell vezérelni egy gépet ugyanazon a hálózati szegmensen, hogy küldje el a kéréseket.

1.4 A célrendszer elindítása telepítéshez

Alapvetően kétféle módon lehet testreszabni a telepítés rendszerindítási folyamatát a korábban (1.3.7. - Wake on LAN (32. oldal) és 1.3.3. - PXE rendszerindítás használata (26. oldal)) már említetteken kívül. Ahhoz, hogy a telepítőkernel által az adott hardveren igényelt paramétereket megadja, használhatja az alapértelmezett rendszerindítási paramétereket és funkcióbillentyűket, vagy használhatja a telepítéskor megjelenő rendszerindítási képernyő rendszerindítási parancssorát.

1.4.1 Az alapértelmezett rendszerindítási paraméterek használata

A rendszerindítási paraméterek részletes leírása: 1. fejezet - *Installation with YaST* (↑*Start-Up*). Általában a *Telepítés* kiválasztására elindul a telepítési rendszerindítási folyamat.

Amennyiben problémákat tapasztalna, úgy használja a *Telepítés – ACPI támogatás nélkül* vagy *Telepítés – Biztonságos beállításokkal* menüpontot. További információ a telepítési folyamattal kapcsolatos hibák kereséséről: 13.2. - Installation Problems (13. fejezet - *Common Problems and Their Solutions*, ↑*Start-Up*).

A képernyő alján látható menüsor egyes telepítések esetén extra funkciók használatát is lehetővé teszi. Az F-billentyűk használatával további paraméterek adhatók át a telepítési rutinoknak anélkül, hogy pontosan ismernie kellene a paraméterek részletes szintaxisát (lásd: 1.4.2. - Egyéni rendszerindítási paraméterek használata (33. oldal)). A rendelkezésre álló funkcióbillentyűk részletes leírása: 1.5. - The Boot Screen (1. fejezet - *Installation with YaST*, ↑*Start-Up*).

1.4.2 Egyéni rendszerindítási paraméterek használata

A megfelelő rendszerindítási paraméterek használata segít a telepítési folyamat végrehajtásában. Számos paraméter később is beállítható, a linuxrc rutinjaival, de a rendszer-

indítási paraméterek használata egyszerűbb. Egyes automatizált telepítéseknél a rendszerindítási paraméterek megadhatók az `initrd` vagy az `info` fájl segítségével.

A következő táblázat felsorolja a fejezetben említett különféle telepítési helyzeteket, a rendszer indításához szükséges paraméterekkel együtt, és az ezeknek megfelelő rendszerindítási paramétereket. Egyszerűen csak be kell írni őket abban a sorrendben, ahogy megjelennek a táblázatban, hogy megkapja a telepítési rutinoknak átadható rendszerindítási paramétersorozatot. Például (az egész egy sorba írandó):

```
install=... netdevice=... hostip=...netmask=... vnc=... vncpassword=...
```

A *`(...)`* értékeket cserélje le az adott rendszernek megfelelő értékekre.

1.1. táblázat *A fejezetben taglalt telepítési (rendszerindítási) helyzetek*

Telepítési helyzet	A rendszer indításához szükséges paraméterek	Rendszerindítási opciók
1. fejezet - *Installation with YaST* (↑*Start-Up*)	Nincs: a rendszer automatikusan indul	Nincs szükség
1.1.1. - Egyszerű távoli telepítés VNC-n keresztül – statikus hálózati beállítások (4. oldal)	• A telepítési kiszolgáló helye • Hálózati eszköz • IP cím • Alhálózati maszk • Átjáró • VNC engedélyezése • VNC-jelszó	• `install=(nfs,http, ftp,smb):///path_to _instmedia` • `netdevice=some _netdevice` (csak akkor szükséges, ha több hálózati eszköz is van) • `hostip=some_ip` • `netmask=some _netmask` • `gateway=ip_gateway` • `vnc=1` • `vncpassword=some _password`

Telepítési helyzet	A rendszer indításához szükséges paraméterek	Rendszerindítási opciók
1.1.2. - Egyszerű távoli telepítés VNC-n keresztül – dinamikus hálózati beállítások (5. oldal)	• A telepítési kiszolgáló helye • VNC engedélyezése • VNC-jelszó	• `install=(nfs,http,ftp,smb):///path_to_instmedia` • `vnc=1` • `vncpassword=some_password`
1.1.3. - Távoli telepítés VNC-n keresztül – PXE-s rendszerindítás és Wake-on-LAN (7. oldal)	• A telepítési kiszolgáló helye • A TFTP-kiszolgáló helye • VNC engedélyezése • VNC-jelszó	Nem alkalmazható; a folyamatot a PXE és a DHCP vezérli
1.1.4. - Egyszerű távoli telepítés SSH-n keresztül – statikus hálózati beállítások (8. oldal)	• A telepítési kiszolgáló helye • Hálózati eszköz • IP cím • Alhálózati maszk • Átjáró • SSH engedélyezése • SSH-jelszó	• `install=(nfs,http,ftp,smb):///path_to_instmedia` • `netdevice=some_netdevice` (csak akkor szükséges, ha több hálózati eszköz is van) • `hostip=some_ip` • `netmask=some_netmask` • `gateway=ip_gateway` • `usessh=1` • `sshpassword=some_password`

Telepítési helyzet	A rendszer indításához szükséges paraméterek	Rendszerindítási opciók
1.1.5. - Egyszerű távoli telepítés SSH-n keresztül – dinamikus hálózati beállítások (9. oldal)	• A telepítési kiszolgáló helye • SSH engedélyezése • SSH-jelszó	• `install=(nfs,http,ftp,smb):///path_to_instmedia` • `usessh=1` • `sshpassword=some_password`
1.1.6. - Távoli telepítés SSH-n keresztül – PXE-s rendszerindítás és Wake-on-LAN (11. oldal)	• A telepítési kiszolgáló helye • A TFTP-kiszolgáló helye • SSH engedélyezése • SSH-jelszó	Nem alkalmazható; a folyamatot a PXE és a DHCP vezérli

TIPP: További információ a linuxrc rendszerindítási paramétereiről

További információ a Linux-rendszerek indításához használt linuxrc rendszerindítási paramétereiről az `/usr/share/doc/packages/linuxrc/linuxrc.html` fájlban található.

1.5 A telepítési folyamat figyelése

Számos módon figyelhető távolról a telepítési folyamat. A megfelelő rendszerindítási paraméterek megadása esetén akár VNC, akár SSH használható a telepítés vezérlésére és a rendszer beállítására egy távoli munkaállomásról.

1.5.1 Telepítés VNC-vel

Bármilyen VNC-megjelenítő szoftver használható az openSUSE telepítésének távoli vezérléséhez, szinte minden operációs rendszeren. A jelen szakaszban azt mutatjuk

meg, hogyan történik a telepítése egy VNC-megjelenítő alkalmazás vagy egy webböngésző segítségével.

Felkészülés a VNC-s telepítésre

Ahhoz, hogy a telepítési célt felkészítse a VNC-s telepítésre, mindössze meg kell adni a megfelelő rendszerindítási paramétereket a telepítés utáni induláskor (1.4.2. - Egyéni rendszerindítási paraméterek használata (33. oldal)). A célrendszer szöveges környezetben indul el és várja, hogy a VNC-kliens csatlakozzon a telepítőprogramhoz.

A telepítőprogram meghirdeti a csatlakozáshoz szükséges IP-címet és képernyőszámot. Ha fizikailag is hozzáfér a célrendszerhez, akkor ezeket az adatokat rögtön azután megtekintheti, hogy a rendszer telepítése elindult. Írja be ezeket az adatokat a VNC-kliensszoftverbe, és adja meg a VNC-jelszót.

Mivel a telepítési cél OpenSLP-n hirdeti meg magát, a telepítési cél címadatai egy SLP-böngészővel is lekérdezhetők anélkül, hogy ténylegesen oda kellene menni a telepített géphez – feltéve, hogy a hálózat és a gépek mind támogatják az OpenSLP-t:

1. Indítsa el a KDE fájl- és webböngésző programját, a Konquerort.

2. A címsorba írja be, hogy `service://yast.installation.suse`. A célrendszer ikonként jelenik meg a Konqueror képernyőjén. Erre az ikonra kattintva elindul a KDE VNC-megjelenítője, amellyel elvégezhető a telepítés. Alternatív megoldásként futtathat másik VNC-megjelenítő szoftvert is a megadott IP-címmel. Adja hozzá az IP-cím végéhez, hogy `:1`. Ez annak a képernyőnek a száma, amelyen a telepítés zajlik.

Csatlakozás a telepítőprogramhoz

Alapvetően két módja van a VNC-kiszolgálókhoz (a jelen esetben a telepítési célhoz) csatlakozásnak. Elindíthat egy független VNC-megjelenítő alkalmazást bármely operációs rendszeren, vagy csatlakozhat egy Javát futtatni képes webböngészővel.

A VNC használata esetén a Linux-rendszer telepítése bármely más operációs rendszer alól (legyen az akár másfajta Linux, Windows vagy Mac OS) is vezérelhető.

Linuxos gépen győződjön meg róla, hogy a `tightvnc` csomag telepítve van. Windowsos gépen telepítse az alkalmazás windowsos változatát, amely a TightVNC weboldaláról (`http://www.tightvnc.com/download.html`) tölthető le.

Csatlakozás a célgépen futó telepítőprogramhoz:

1. Indítsa el a VNC-megjelenítőt.
2. Írja be a telepítési cél (az SLP-böngészőből vagy magából a telepítőprogramból kiolvasott) IP-címét és képernyőszámát:

   ip_address:*display_number*

   Megjelenik egy ablak az asztalon, benne a szokásos helyi telepítés YaST-képernyőivel.

Ha webböngészőt használ a telepítőprogramhoz csatlakozásra, akkor tényleg teljesen függetlenné válik bármiféle VNC-szoftvertől és operációs rendszertől. Ha a böngésző képes Javát futtatni, akkor bármilyen böngészőt használhat (Firefox, Internet Explorer, Konqueror, Opera stb.) a Linux-rendszer telepítéséhez.

VNC-s telepítés végrehajtása böngészővel:

1. Indítsa el a kedvenc webböngészőjét.
2. Írja be a címsorba a következőt:

   http://*ip_address_of_target*:5801

3. Írja be a VNC-jelszót, amikor a program felszólítja erre. A böngészőablakban most a szokásos helyi telepítés YaST képernyői láthatók.

1.5.2 Telepítés SSH-n keresztül

SSH használatával távolról vezérelheti a linuxos rendszer telepítését bármely SSH-kliensszoftverrel.

Felkészülés az SSH-s telepítésre

A megfelelő szoftvercsomagok (Linux esetében OpenSSH, Windows esetében PuTTY) telepítésén túl még meg kell adni a megfelelő rendszerindítási paramétereket is ahhoz, hogy az SSH-t használhassa telepítésre. Részletek: 1.4.2. - Egyéni rendszerindítási paraméterek használata (33. oldal). Az OpenSSH alapértelmezés szerint telepítve van minden SUSE Linux alapú operációs rendszeren.

Csatlakozás a telepítőprogramhoz

1. Kérje le a telepítési cél IP-címét. Ha fizikailag hozzáfér a célgéphez, akkor használja azt az IP-címet, amelyet a telepítési rutin megadott a konzolon a rendszer indítása után. Ellenkező esetben használja azt az IP-címet, amelyet az adott géphez rendelt a DHCP-kiszolgáló beállításakor.

2. A parancssorban írja be a következő parancsot:

   ```
   ssh -X root@ip_address_of_target
   ```

   Az *ip_address_of_target* helyére a telepítési cél tényleges IP-címét kell írni.

3. Amikor felszólítja a program, hogy adjon meg egy felhasználónevet, írja be, hogy `root`.

4. Jelszónak adja meg azt a jelszót, amely be lett állítva az SSH rendszerindítási paraméterekkel. Sikeres hietelesítés után megjelenik a telepítési cél parancssori promptja.

5. A telepítőprogram indításához írja be, hogy `yast`. Megjelenik egy ablak a szokásos YaST-képernyőkkel (1. fejezet - *Installation with YaST* (↑*Start-Up*)).

2 Speciális lemezbeállítások

A kifinomult rendszerkonfigurációk speciális lemezbeállításokat igényelhetnek. A YaST segítségével az összes szokásos particionálási feladat elvégezhető. A blokkeszközök állandó elnevezéséhez használja a `/dev/disk/by-id/` vagy `/dev/disk/by-uuid` alatti blokkeszközöket. A Logical Volume Management (logikai kötetkezelés, LVM) egy olyan lemezparticionálási séma, amelynek célja, hogy jóval rugalmasabb legyen, mint a szokásos telepítések fizikai particionálása. Pillanatfelvétel funkciója segít az adatmentések egyszerű készítésében. A RAID (Redundant Array of Independent Disks, független lemezek redundáns tömbje) technológia jobb adatintegritást, teljesítményt és hibatűrést kínál.

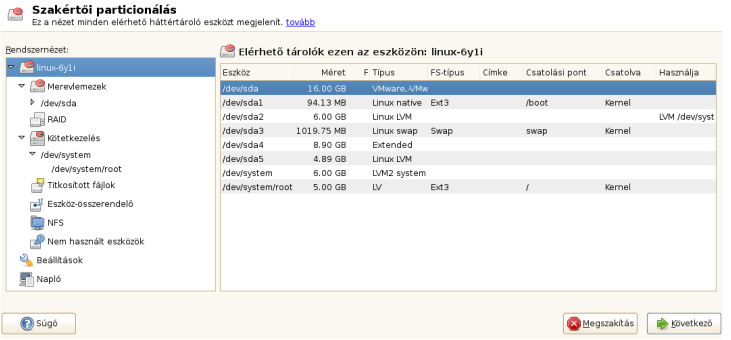
2.1 Particionálás a YaST segítségével

A 2.1. ábra - A YaST particionáló (42. oldal) ábrán látható szakértői párbeszédablakban kézzel módosítható egy vagy több merevlemez particionálása. Partíciók hozhatók létre, törölhetők és szerkeszthetők. Ugyanebből a YaST-modulból érhető el a szoftveres RAID és az LVM konfigurációja.

FIGYELEM: A futó rendszer újraparticionálása

Bár egy telepített rendszer partíciói is módosíthatók, az adatvesztés kockázata rendkívül magas. Kerülje a telepített rendszer újraparticionálását és ha mégis erre szánná magát, előtte feltétlenül mentse el az összes adatot.

2.1. ábra *A YaST particionáló*



Minden csatlakoztatott merevlemez meglévő vagy javasolt partíciói megjelenítésre kerülnek a YaST *Szakértői particionálás* modul párbeszédablakában látható *Elérhető tárolók* listában. A teljes merevlemezek szám nélküli eszközként jelennek meg, például `/dev/sda`. A partíciók ezen eszközök részeként jelennek meg, például `/dev/sda1`. A merevlemezek és partícióik mérete, típusa, fájlrendszere és felcsatolási pontjai szintén láthatók. A csatolási pont azt adja meg, hogy a partíció a Linux-fájlrendszer fastruktúrájában hol kerül felcsatolásra.

Számos funkcionális nézet érhető el a bal oldali *Rendszernézetben*. E nézetekkel gyűjthető információ a meglévő tárolóbeállításokról, illetve itt állíthatók be az olyan funkciók, mint a `RAID`, a `Kötetkezelés`, `Titkosított fájlok` és az `NFS`.

Ha a szakértői párbeszédablakot a telepítés során megnyitja, akkor a szabad lemezterület szintén megjelenik és automatikusan ki lesz választva. Ha több lemezterületet kíván biztosítani az openSUSE számára, akkor a lista aljától kezdve szabadítsa fel a szükséges területet (a merevlemez utolsó partíciójától kezdve az elsőig). Ha például három partícióval rendelkezik, akkor az openSUSE nem használhatja kizárólagosan a másodikat, és nem tartható fenn az első és a harmadik más operációs rendszerek számára.

2.1.1 Partíciótípusok

Minden merevlemez partíciós táblájában négy bejegyzés számára van hely. A partíciós táblában lévő minden bejegyzés vagy egy elsődleges, vagy egy kiterjesztett partíciót jelez. Egy merevlemezen azonban csak egy kiterjesztett partíció lehet.

Az elsődleges partíció egy adott operációs rendszerhez rendelt sávok (fizikai lemezterület) folytonos tartományából áll. Kizárólag elsődleges partíciók használata esetén merevlemezenként négy partíció hozható létre, lévén ennyit enged a partíciós tábla. Ezért lehet szükség kiterjesztett partíciókra. A kiterjesztett partíció szintén a lemezsávok folyamatos tartománya, de ez továbboszthatóúgynevezett *logikai partíciókra*. A logikai partíciók nem igényelnek partícióstábla-bejegyzéseket. Más szavakkal, a kiterjesztett partíció tárolja a logikai partíciókat.

Ha négynél több partícióra van szükség, akkor hozzon létre egy kiterjesztett partíciót, legkésőbb negyedik partícióként. Ezt a kiterjesztett partíciót célszerű a teljes meglévő szabad lemeztartományra kiterjeszteni. A kiterjesztett partícióban ezután hozza létre a kívánt logikai partíciókat. A logikai partíciók maximális száma SCSI-, SATA- és Firewire-lemezeken 15, (E)IDE lemezeken pedig 63. Linux esetén nem számít a használt partíciók típusa. Az elsődleges és logikai partíciók egyaránt kifogástalanul működnek.

2.1.2 Partíció létrehozása

Ha elölről kíván létrehozni egy partíciót, válassza ki a *Merevlemezek* részt, majd egy olyan merevlemezt, amelyen van szabad terület. A tényleges módosítás a *Partíciók* lapon végezhető el:

1. Válassza ki a *Hozzáadás* pontot. Ha több merevlemez van csatlakoztatva, akkor megjelenik egy kiválasztási párbeszédablak, amelyben az új partícióhoz kiválasztható egy merevlemez.

2. Ezután adja meg a partíció típusát (elsődleges vagy kiterjesztett). Maximum négy elsődleges, vagy három elsődleges és egy kiterjesztett partíció hozható létre. A kiterjesztett partícióban több logikai partíció is létrehozható (lásd: 2.1.1. - Partíciótípusok (42. oldal)).

3. Válassza ki a használni kívánt fájlrendszer típusát és egy csatolási pontot. A YaST minden létrehozott partícióhoz javasol egy csatolási pontot. Más (például címke alapján történő) csatolási mód megadásához válassza ki az *fstab-paraméterek* pontot.

4. Ha a rendszer igényli, adjon meg további fájlrendszer-paramétereket. Erre például az állandó eszköznevek érdekében lehet szükség. A használható paraméterek részletes leírása: 2.1.3. - Partíció módosítása (44. oldal).

5 A particionálási beállítások alkalmazásához kattintson az *OK* > *Alkalmazás* gombokra.

Ha a partíciót telepítés közben hozta létre, akkor a telepítés áttekintése képernyőre jut vissza.

2.1.3 Partíció módosítása

Új partíció létrehozásakor vagy meglévő módosításakor különböző paraméterek állíthatók be. Új partíciók esetén a megfelelő paramétereket a YaST állítja be, és ezeket általában nem kell módosítani. Kézi beállításhoz tegye a következőket:

1 Válassza ki a partíciót.

2 Nyomja meg a *Szerkesztés* gombot és állítsa be a paramétereket:

Fájlrendszer-azonosító
: Még ha ezen a ponton nem is kívánja formázni a partíciót, rendeljen hozzá egy fájlrendszer-azonosítót annak biztosítására, hogy a partíció megfelelően bejegyzésre kerüljön. Lehetséges értékek: *Linux*, *Linux csere*, *Linux LVM* és *Linux RAID*.

Fájlrendszer
: Itt változtatható meg a fájlrendszer és formázható meg a partíció. A fájlrendszer módosítása és a partíció formázása visszavonhatatlanul letörli az adatokat a partícióról.

  A cserepartíció egy speciális formátum, az ilyen partíciót a rendszer virtuális memóriaként tudja használni. A cserepartíció mérete legalább 256 MB legyen. Ha azonban megtelik a csereterület, érdemesebb inkább memóriát venni a rendszerbe, nem a csereterület méretét növelgetni.

  A Linux-partíciók alapértelmezett fájlrendszere az Ext3. A ReiserFS, a JFS, az XFS és az Ext3 úgynevezett naplózó fájlrendszer. Ezek a fájlrendszerek összeomlás után nagyon gyorsan helyre tudják állítani a rendszert, mivel az írási folyamatok naplózódnak menet közben. A ReiserFS pedig kifejezetten gyors, ha sok kis fájlt kell kezelni. Az Ext2 nem naplózó fájlrendszer. Ugyanakkor sziklaszilárd, és kiválóan használható kisebb partíciókhoz, mivel nem igényel sok területet a lemezkezeléshez.

Fájlrendszer titkosítása
: Ha bekapcsolja a titkosítást, akkor az adatok titkosított formában íródnak a merevlemezre. Ez növeli a bizalmas adatok biztonságát, de némileg csökkenti a rendszer sebességét, mivel a titkosítás erőforrásokat vesz igénybe. A fájlrendszerek titkosításával kapcsolatos további információ: 36. fejezet - *Partíciók és fájlok titkosítása* (571. oldal).

fstab-paraméterek
: Itt adhatók meg a fájlrendszerek adminisztrációs fájljának (`/etc/fstab`) különböző paraméterei. Az alapértelmezett beállítások a legtöbb rendszer számára megfelelnek. De ha akarja, módosíthatja a fájlrendszer azonosítását eszköznévről kötetcímkére. A kötetcímkében mindenféle karakter használható, kivéve a / és a szóköz.

  Állandó eszköznevekhez használja az *Eszközazonosító*, *UUID* vagy *LABEL* (név) alapján történő csatolást. Az openSUSE rendszerben az állandó eszköznevek alapértelmezés szerint be vannak kapcsolva.

  A *LABEL* alapján történő csatolás esetén adjon megfelelő nevet a partíciónak. Például használhatja a `HOME` partíciónevet egy olyan partíció számára, amelyet a `/home` helyre kíván felcsatolni.

  Ha kvótát kíván használni a fájlrendszeren, akkor használja a *Kvóta támogatásának engedélyezése* csatolási paramétert. Ezt előbb be kell állítani, csak utána lehet kvótákat megadni az egyes felhasználókhoz a YaST *Felhasználók kezelése* moduljában. A felhasználói kvóta beállításáról további információ: 5.3.5. - Managing Quotas (5. fejezet - *Managing Users with YaST*, ↑*Start-Up*).

Csatolási pont
: A fájlrendszer-fastruktúra azon könyvtára, amelyhez a partíció fel lesz csatolva. Választhat a YaST különböző javaslatai közül, vagy megadhat egy másik nevet.

3 A partíció aktiválásához nyomja meg az *OK* > *Alkalmaz* gombot.

MEGJEGYZÉS: Fájlrendszerek átméretezése

Egy meglévő fájlrendszer átméretezéséhez válassza ki a partíciót, majd az *Átméretezés* pontot. Ne feledje, hogy felcsatolt partíciókat nem lehet átméretezni.

A partíció átméretezéséhez a particionáló futtatása előtt le kell csatolni az adott partíciót.

2.1.4 További particionálási tippek

Az alábbi szakasz néhány ötletet és tippet ad a particionálással kapcsolatban, hogy segítsen meghozni a megfelelő döntéseket a rendszer beállításakor.

TIPP: Cilinderek száma

Ne feledje, hogy a különböző particionálási eszközök egy része `0`-val, mások pedig `1`-gyel kezdik a partíció cilindereinek a számozását. A cilinderek számának kiszámításakor mindig használja a legutolsó és a legelső cilinderszám különbségét és adjon hozzá egyet.

`Cserepartíció` (swap) használata

A cserepartíció feladata, hogy megnövelje a fizikailag rendelkezésre álló memóriát. Így megoldható, hogy a ténylegesen rendelkezésre álló RAM-nál több memóriát használjon a rendszer. A 2.4.10-es előtti kernelek memóriakezelő rendszere a cserepartíciót biztonsági tartalékként használta. Ezekben az időkben, ha nem volt legalább kétszer akkora a cserepartíció, mint a rendszerbe beépített RAM mennyisége, akkor a rendszer teljesítménye leromlott. Ez ma már nem igaz, ma már nincsenek ilyen korlátozások.

A Linux a „legrégebben használt” (Least Recently Used, LRU) elv alapján választja ki azokat a lapokat, amelyek a memóriából lemezre mozgathatók. Így a futó alkalmazásoknak több memória jut, és még a gyorsítótáruk is simábban működik.

Ha egy alkalmazás a lehető legtöbb memóriát próbálja meg lefoglalni, akkor gondok léphetnek fel a cserepartícióval. Három fő esetet célszerű megvizsgálni:

Cserepartíció nélküli rendszerek
: Az alkalmazás a bármilyen módon felszabadítható legtöbb memóriát megkapja. Minden gyorsítótár törlődik, ezért a többi alkalmazás lelassul. Néhány perc után a kernel "memóriahiány" miatti folyamatleállító mechanizmusa bekapcsol, és leállítja a folyamatot.

Kis (128–512 MB) cserepartíciójú rendszerek
: Először a rendszer ugyanúgy lelassul, mint a cserepartíció nélküli rendszerek. Az összes fizikai memória elhasználása után a cserepartíció-területet is felhasználja a rendszer. Ezen a ponton a rendszer borzalmasan lelassul, és távolról nem lehet már végrehajtani parancsokat. A cserepartíció merevlemezének sebességétől függően a rendszer 10-15 percig ebben az állapotban marad, amíg a kernel "memóriahiány" miatti folyamatleállító mechanizmusa be nem kapcsol, és megoldja a problémát. Ne feledje, hogy bizonyos mennyiségű csereterületre szükség van ahhoz, hogy a számítógép végre tudja hajtani a „lemezre felfüggesztés” műveletét. Ebben az esetben a cserepartíció méretének elegendően nagynak (512 MB–1GB) kell lennie ahhoz, hogy a memória adatait ki lehessen másolni rá.

Nagy cserepartíciójú rendszerek
: Ebben az esetben általában jobb, ha nincs "elszabadult", a cserepartíciót vadul használó alkalmazás. Ha ugyanis ez a helyzet, a rendszer csak több óra után fog helyreállni. Eközben várhatóan más folyamatokkal is mindenféle probléma fog adódni, például az időtúllépések miatt, és a rendszer állapota nem megjósolható lesz, még akkor sem, ha időközben a hibás folyamatot sikerül leállítani. Ebben az esetben célszerű a gépet minél gyorsabban újraindítani. A nagy cserefájl csak akkor hasznos, ha egy alkalmazás kifejezetten igényli ezt a funkciót. Az ilyen alkalmazások (például adatbázis-kezelők vagy képszerkesztők) gyakran kínálnak lehetőséget arra, hogy közvetlenül kezeljék a merevlemezt. Nagy cserepartíció helyett érdemesebb ezt a lehetőséget használni.

Ha a rendszer nem szabadult el, de egy idő után nagyobb cserepartícióra van szükség, akkor a csereterület gond nélkül megnövelhető. Ha egy partíciót előkészített már cserepartíciónak, akkor vegye fel ezt a partíciót a YaST segítségével. Ha nincs rendelkezésre álló partíció, akkor használható cserefájl is a csereterület méretének megnöveléséhez. A cserefájlok általában lassabbak, mint a partíciók, de mivel a valódi, fizikai memóriához képest mindkettő rendkívül lassú, a gyakorlatban ez a sebességkülönbség nem olyan kiemelkedő fontosságú, mint azt elsőre esetleg gondolni lehetne.

2.1. eljárás *Cserefájl hozzáadása kézzel:*

Cserefájlt az alábbi módon lehet felvenni a futó rendszeren:

1. Hozzon létre egy üres fájlt a rendszeren. Ha például egy 128 MB-os cserefájlt szeretne létrehozni a `/var/lib/swap/swapfile` helyen, akkor adja ki az alábbi parancsokat:

```
mkdir -p /var/lib/swap
dd if=/dev/zero of=/var/lib/swap/swapfile bs=1M count=128
```

2 A cserefájlt inicializáló parancs:

```
mkswap /var/lib/swap/swapfile
```

3 A cserefájlt aktiváló parancs:

```
swapon /var/lib/swap/swapfile
```

A cserefájlt letiltó parancs:

```
swapoff /var/lib/swap/swapfile
```

4 Az aktuális csereterületek az alábbi paranccsal ellenőrizhetők:

```
cat /proc/swaps
```

Ne feledje, hogy e pillanatban ez még csak egy ideiglenes csereterület. A következő újraindítás után már nem használja a rendszer.

5 Ha véglegesíteni szeretné ezt a cserefájlt, vegye fel a következő sort az `/etc/fstab` fájlba:

```
/var/lib/swap/swapfile swap swap defaults 0 0
```

2.1.5 Particionálás és LVM

A szakértői particionálóból a *Kötetkezelés* gomb megnyomására érhető el az LVM konfiguráció. Ha azonban a rendszeren már létezik egy működő LVM-konfiguráció, akkor az automatikusan aktiválódik, amint először belép az LVM-beállítási részbe. Ebben az esetben az aktivált kötetcsoporthoz tartozó partíciót tartalmazó lemezek nem particionálhatók újra, mivel a Linux-kernel nem tudja újra beolvasni a merevlemez módosított partíciós tábláját, ha a lemez egyik partíciója már használatban van. Ha viszont a rendszeren már van egy működő LVM-konfiguráció, akkor alighanem nincs is szükség fizikai újraparticionálásra. Elegendő módosítani a logikai kötetek beállítását.

A fizikai kötetek (PV) elején a kötettel kapcsolatos információ kiíródik a partícióra. Egy ilyen partíció nem LVM-célra történő újbóli hasznosításához felül kell írni a partíción tárolt LVM meta-adat részt. A `system` kötetcsoport és a `/dev/sda2` fizikai

kötet esetében például ez a `dd if=/dev/zero of=/dev/sda2 bs=512 count=1` parancs segítségével hajtható végre.

FIGYELEM: Fájlrendszer rendszerindításhoz

A rendszerindításhoz használt fájlrendszert (root vagy `/boot` fájlrendszer) nem szabad LVM logikai köteten tárolni. Normál fizikai partícióra kell tenni.

2.2 LVM-konfiguráció

Ez a fejezet a logikaikötet-kezelő (LVM) alapelveit és számos körülmények között igen hasznos alapfunkcióit írja le röviden. A 2.2.2. - Az LVM beállítása a YaST segítségével (51. oldal) rész mutatja be, hogy hogyan lehet beállítani az LVM-et a YaST segítségével.

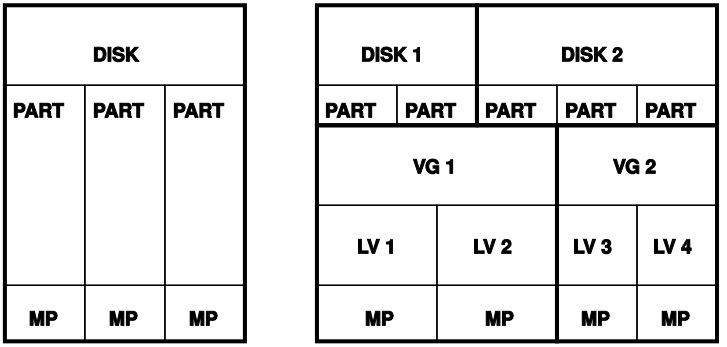
FIGYELEM

Az LVM használata nagyobb kockázatot jelent, például nagyobb valószínűséggel fordulhat elő adatvesztés. További kockázatok: az alkalmazások összeomlása, tápellátási hibák és hibás parancsok. Az LVM kialakítása és a kötetek újrakonfigurálása előtt mentse el az adatokat. Sose dolgozzon biztonsági mentés nélkül.

2.2.1 Az LVM (Logical Volume Manager, logikaikötet-kezelő)

A logikaikötet-kezelő (LVM) lehetővé teszi a merevlemez-terület rugalmas szétosztását több fájlrendszeren. Azért készült, mert néha csak azután derül ki, hogy módosítani kellene a merevlemez felosztását, miután a telepítés során már meg lettek adva a partíciók. Mivel egy futó rendszer partícióinak módosítása bonyolult, az LVM egy virtuális tárolót (kötetcsoport, röviden VG) biztosít, amelyből szükség esetén logikai kötetek (LV) hozhatók létre. Az operációs rendszer ezeket a logikai köteteket használja a fizikai partíciók helyett. A kötetcsoportok több lemezre is kiterjeszthetők, így több lemez vagy ezek részei alkothatnak egyetlen kötetcsoportot. Ily módon az LVM a fizikai lemezterület egyfajta absztrakcióját biztosítja, amelynek segítségével a szegmentálás egyszerűbben és biztonságosabban módosítható, mint a fizikai újraparticionálással. A fizikai particionálással kapcsolatosan az alábbi részek tartalmaznak háttérinformációt: 2.1.1. - Partíciótípusok (42. oldal) és 2.1. - Particionálás a YaST segítségével (41. oldal).

2.2. ábra *A fizikai particionálás és az LVM összehasonlítása*



A következő ábra (2.2. ábra - A fizikai particionálás és az LVM összehasonlítása (50. oldal)) összehasonlítja a fizikai particionálást (bal oldal) és az LVM alapú szegmentálást (jobb oldal). A bal oldalon egyetlen lemez három fizikai partícióra (PART) lett felosztva, mindegyikhez egy csatolási pont (MP) tartozik, hogy az operációs rendszer el tudja érni őket. A jobb oldalon két lemez lett felosztva két, illetve három fizikai partícióra. Ezeken két LVM-kötetcsoport (VG 1 és VG 2) lett megadva. A VG 1 két DISK 1 partíciót és egy DISK 2 partíciót tartalmaz. A VG 2 a maradék két DISK 2 partíciót tartalmazza. Az LVM-ben az egy kötetcsoportba egyesített fizikai lemezpartíciókat fizikai köteteknek (PV) hívják. A kötetcsoportokon belül négy logikai kötet (LV 1 - LV 4) lett megadva, amelyet az operációs rendszer a hozzájuk rendelt csatolási pontokon keresztül használhat. A különböző logikai kötetek közötti határt nem kell más partícióhatárhoz igazítani. Érdemes megfigyelni a példában az LV 1 és LV 2 közötti határt.

Az LVM jellemzői:

- Több merevlemez vagy partíció egyesíthető egy nagy logikai kötetbe.
- Feltéve, hogy a beállítás megfelelő, a logikai kötet (például az `/usr`) a szabad terület elfogyásakor kibővíthető.
- Az LVM használata esetén merevlemezek és újabb logikai kötetek (LV-k) adhatók hozzá egy futó rendszerhez. Ehhez azonban üzem közben cserélhető hardver szükséges, amely képes az ilyen műveletek végrehajtására.
- Bekapcsolható egy sávokra osztott mód is, amely a logikai kötet adatfolyamát több fizikai köteten osztja szét. Ha ezek a fizikai kötetek különböző lemezeken helyez-

kednek el, akkor ez a RAID 0-hoz hasonlóan javíthatja az olvasási és írási teljesítményt.

- A pillanatkép funkció lehetővé teszi a futó rendszer konzisztens biztonsági mentését (különösen kiszolgálók esetén fontos).

Mindezen jellemzők azt jelentik, hogy LVM-et érdemes lehet a fokozottan használt otthoni PC-ken, illetve kis kiszolgálókon használni. Ha az adatok mennyisége folyamatosan növekszik (például az adatbázisok, zenearchívumok vagy a felhasználói könyvtárak), akkor az LVM jó választás lehet. Ez lehetővé teszi a fizikai merevlemeznél nagyobb fájlrendszerek tárolását. Az LVM másik előnye, hogy akár 256 logikai kötet is hozzáadható. Ne feledje azonban, hogy az LVM használata különbözik a hagyományos partíciók használatától. Az LVM beállításával kapcsolatos útmutatás és további információk a hivatalos LVM HOWTO-ban, a `http://tldp.org/HOWTO/LVM-HOWTO/` címen érhetők el.

A 2.6-os kerneltől kezdődően rendelkezésre áll az LVM 2, amely visszamenőlegesen kompatibilis a korábbi LVM-mel és lehetővé teszi a régi kötetcsoportok további használatát. Új kötetcsoportok létrehozásakor döntse el, hogy az új formátumot kívánja használni vagy a visszamenőlegesen kompatibilis verziót. Az LVM 2 nem igényel kerneljavításokat. A 2.6-os kernelbe integrált eszközleképezőt használja. Ez a kernel csak az LVM 2-es változatot támogatja. Éppen ezért az LVM említésekor ebben a részben mindig az LVM 2-re gondolunk.

2.2.2 Az LVM beállítása a YaST segítségével

A YaST LVM-beállító ablaka a YaST Szakértői particionálás (2.1. - Particionálás a YaST segítségével (41. oldal)) részéből érhető el. A szakértői particionálási eszköz lehetővé teszi a meglévő partíciók törlését és módosítását, valamint az LVM-mel használható újak létrehozását. Az első feladat fizikai kötetek létrehozása, amelyek majd tárolják a kötetcsoportokat. Ezután létre kell hozni egy LVM-partíciót, először kiválasztva a merevlemezt, majd a *Létrehozás* > *Ne formázza* pontokra kattintva, és végül kiválasztva a *0x8E Linux LVM*-et, mint a partíció típusát. Az LVM-hez használni kívánt összes partíció létrehozása után az LVM-konfiguráció elindításához kattintson a *Kötetkezelés* gombra.

1. A *Merevlemezek* részben válasszon ki egy merevlemezt.

2. Váltson át a *Partíciók* lapra.

3 Kattintson a *Hozzáadás* gombra, majd írja be a fizikai kötet kívánt méretét.

4 A *Ne formázza a partíciót* pontot megjelölve, állítsa a *Fájlrendszer ID* értékét arra, hogy *0x8E Linux LVM*. Ne csatolja fel ezt a partíciót.

5 Ismételje meg a fenti eljárást addig, amíg létre nem hozta az összes fizikai kötetet a rendelkezésre álló lemezeken.

Kötetcsoportok létrehozása

Ha még nem létezik kötetcsoport, akkor létre kell hozni egyet (2.3. ábra - Kötetcsoport létrehozása (52. oldal)). A *Kötetcsoport hozzáadása* gombbal további csoportok is létrehozhatók, de általában egyetlen kötetcsoport elegendő. Az openSUSE rendszerfájlokat tartalmazó kötetcsoportnak javasolt a `system` nevet adni. A fizikai egység mérete a kötetcsoport fizikai blokkjának méretét adja meg. A kötetcsoportban lévő lemezterület ilyen méretű darabokban kerül kezelésre. Ez az érték alapesetben 4 MB-ra van állítva, amely maximum 256 GB fizikai és logikai kötetméretet tesz lehetővé. Ha 256 gigabájtnál nagyobb logikai kötetekre van szükség, akkor a fizikai egység méretét meg kell növelni, például 8, 16 vagy 32 megabájtra.

2.3. ábra *Kötetcsoport létrehozása*

Az előzőleg létrehozott fizikai köteteket adja hozzá a kötetcsoporthoz: válassza ki őket az egérrel, majd használja a *Hozzáadás* → gombot. Ellenőrizze, hogy a *Kiválasztott fizikai kötetek* rész alsó sorában az eredményül kapott méret megfelelő-e.

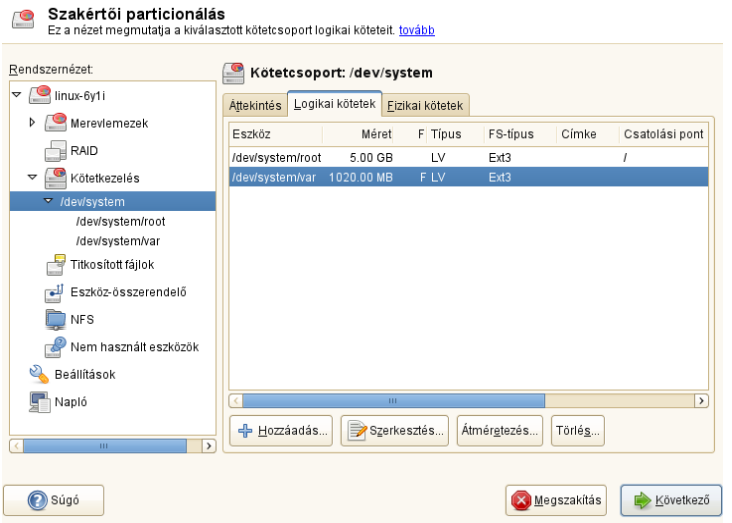
Ha több kötetcsoportot hozott létre, és szeretne hozzáadni vagy eltávolítani fizikai köteteket, akkor válassza ki a kötetcsoportot a *Kötetkezelés* részben. Ezután váltson át az

Áttekintés lapra, majd válassza ki az *Átméretezés* pontot. A megjelenő menüben veheti fel ill. távolíthatja el a kiválasztott kötetcsoport fizikai köteteit.

Logikai kötetek beállítása

Miután a kötetcsoport ki lett töltve fizikai kötetekkel, a következő párbeszédablakban adja meg a logikai köteteket, amelyeket az operációs rendszer fog használni. A bal felső mezőből válassza ki az aktuális kötetcsoportot. Mellette megjelenik az aktuális kötetcsoporton lévő szabad terület. Az alatta lévő lista tartalmazza a kötetcsoport összes logikai kötetét. Megjelenik az összes normál Linux-partíció, amelyhez meg van adva csatolási pont, az összes cserepartíció és a már létező logikai kötetek. Amíg a kötetcsoporton van szabad terület, a *Hozzáadás*, *Szerkesztés* és *Eltávolítás* gombokkal kezelje igény szerint a logikai köteteket. Minden kötetcsoporthoz rendeljen hozzá legalább egy logikai kötetet.

2.4. ábra *Logikai kötetek felügyelete*



Egy új logikai kötet létrehozásához válassza ki a kötetcsoportot a *Kötetkezelés* részben, majd váltson át a *Logikai kötetek* lapra. Ezután kattintson a *Hozzáadás* gombra, és töltse ki a varázslószerű ablakot:

1. Írja be a logikai kötet nevét. A `/home` helyére felcsatolandó kötet esetén praktikus olyan világosan érthető nevet használni, mint a `HOME`.

2. Válassza ki a logikai kötet méretét és a csíkok számát. Ha csak egy fizikai kötetet használ, akkor nincs sok értelme egynél több csíkot választani.

3. Válassza ki a logikai köteten használni kívánt fájlrendszert és a csatolási pontot.

Csíkok használatával a logikai kötet adatfolyama megosztható több fizikai kötet között (csíkozás, striping). Ha ezek a fizikai kötetek különböző lemezeken helyezkednek el, akkor ez általában jobb olvasási és írási teljesítményt eredményez (a RAID 0-hoz hasonlóan). Sávozott logikai kötet azonban csak akkor hozható létre `n` sávval, ha a logikai kötet által igényelt merevlemez-terület egyenletesen feloszthatő `n` fizikai kötetre. Ha például csak két fizikai kötet áll rendelkezésre, akkor három sávból álló logikai kötet nem hozható létre.

FIGYELEM: Sávozás

A YaST ezen a ponton nem tudja ellenőrizni a sávozást érintő bejegyzések helyességét. A hibák csak később látszanak, amikor az LVM ténylegesen kialakításra kerül a lemezen.

Ha beállította az LVM-et, akkor a meglévő logikai kötetek is használhatók. A folytatás előtt ezekhez a logikai kötetekhez is rendeljen hozzá megfelelő csatolási pontokat. A *Tovább* gomb segítségével térjen vissza a YaST Szakértői particionálás ablakába és fejezze be a munkát.

2.3 Szoftveres RAID beállítása

A RAID (redundant array of inexpensive disks, olcsó lemezek redundáns tömbje) nevű technológia célja, hogy több merevlemez-partíciót egy nagy, *virtuális* merevlemezzé szervezzen össze a teljesítmény optimalizálása, az adatok biztonsága vagy mindkettő érdekében. A legtöbb RAID-vezérlő az SCSI protokollt használja, mert több merevlemezt és hatékonyabb módon tud kezelni, mint az IDE protokoll, valamint alkalmasabb a parancsok párhuzamos végrehajtására. Léteznek IDE- és SATA-merevlemezeket használó RAID-vezérlők is. A gyakran igen drága hardveres RAID-vezérlő feladatait szoftverből is meg lehet oldani. Ez azonban elvesz a CPU idejéből és memóriaigénye is van, ezért nem megfelelő megoldás az igazán nagyteljesítményű rendszerekhez.

Az openSUSE lehetővé teszi több merevlemez egyetlen szoftveres RAID-rendszerré egyesítését. A RAID többféle stratégiát is képes alkalmazni a merevlemezek kombiná-

lásához. Ezek mindegyike más jellemzőkkel, célokkal és előnyökkel bír. Ezeket a változatokat szokás *RAID-szintekként* emlegetni.

A szokásos RAID-szintek:

RAID 0
: Ez a szint az adathozzáférés sebességét javítja azáltal, hogy a fájlok blokkjait egynél több lemezre osztja szét. Szigorú értelemben ez nem igazi RAID, hiszen nem redundáns, nem biztosít adatvédelmet, de a *RAID 0* név rajtaragadt az ilyen rendszereken. RAID 0 használatakor két vagy több merevlemez van összekapcsolva. A teljesítmény igen látványos, de akármelyik merevlemez meghibásodik, a teljes RAID-rendszer tönkremegy és elvesznek az adatok.

RAID 1
: Ez a szint megfelelő biztonságot kínál, ugyanis az adatok egy az egyben még egy merevlemezre átmásolódnak. A megoldás másik neve a *merevlemez tükrözése*. Ha a lemez megsérül, a másik meghajtón még mindig rendelkezésre állnak az adatok. Addig, amíg a legutolsó lemez is el nem romlik, az adatok biztonságban vannak. Ha viszont a sérülést nem észlelik, akkor előfordulhat, hogy a sérült adatokat is tükrözi a rendszer a jó lemezre, és így mégiscsak tönkremennek az adatok. Az írási teljesítmény egy kicsit leromlik a másolás során az egyetlen lemezes eléréshez képest (10-20 százalékkal lassúbb), de az olvasási teljesítmény lényegesen jobb bármelyik fizikai merevlemezhez képest, hiszen a megkettőzött adatok párhuzamosan kiolvashatók. Durva közelítésként úgy lehet tekinteni, hogy a RAID 1 közel kétszeres olvasási sebességet biztosít a külön merevlemezekhez képest, és majdnem ugyanazt az írási teljesítményt.

RAID 2 és RAID 3
: Ezek ritkán használt RAID-megvalósítások. A RAID 2 az adatokat nem blokk-, hanem bitszinten választja szét. A RAID 3 esetén bájtonkénti szétválasztás történik, dedikált paritáslemezzel. Ez a szint nem képes egyidejűleg több kérés kiszolgálására. Mindkét szintet nagyon kevés helyen alkalmazzák.

RAID 4
: RAID 4 esetében szintén blokkszintű szétválasztás történik (ugyanúgy, mint a 0. szint esetében), de van egy külön paritáslemez. Ha valamelyik adatlemez meghibásodik, a paritásadatok alapján pótolható. A paritáslemez azonban íráskor rontja a teljesítményt. Ezzel együtt, van ahol RAID 4 rendszereket használnak.

RAID 5

A RAID 5 egy bölcs kompromisszum a 0. és 1. szint között a teljesítmény és a redundancia szempontjából. A használható merevlemez-terület az összes lemezek száma, mínusz egy. Az adatok a RAID 0-hoz hasonlóan el vannak osztva a merevlemezek között. Az egyik partíción *paritásblokkok* készülnek az adatok védelme érdekében. Egymással XOR-kapcsolatban vannak, vagyis a rendszer meghibásodása esetén a megfelelő paritásblokk alapján helyreállíthatók a kiesett adatok. RAID 5 használata esetén viszont éppen ezért egyszerre egynél több merevlemeznek nem szabad meghibásodnia. Ha az egyik lemez elromlik, a lehető leggyorsabban ki kell cserélni az adatvesztés elkerülése érdekében.

További RAID-szintek

Számos további RAID-szintet is kidolgoztak, (RAIDn, RAID 10, RAID 0+1, RAID 30, RAID 50 stb.), amelyek egy része hardvergyártók egyedi megoldása. Ezek a szintek nem túl gyakoriak, ezért itt nem ismertetjük őket.

2.3.1 Szoftveres RAID beállítása a YaST segítségével

A YaST *RAID* beállítására szolgáló modulja az YaST Szakértői particionálás részből érhető el (lásd: 2.1. - Particionálás a YaST segítségével (41. oldal)). Ez a professzionális particionáló eszköz lehetővé teszi a meglévő partíciók módosítását és törlését, valamint a szoftveres RAID-hez használható újak készítését. Itt hozhatja létre a RAID-partíciókat:

1. A *Merevlemezek* részben válasszon ki egy merevlemezt.
2. Váltson át a *Partíciók* lapra.
3. Kattintson a *Hozzáadás* gombra, majd írja be a RAID-partíció kívánt méretét.
4. A *Ne formázza a partíciót* pontot megjelölve, állítsa a *Fájlrendszer ID* értékét arra, hogy *0xFD Linux RAID*. Ne csatolja fel ezt a partíciót.
5. Ismételje meg a fenti eljárást addig, amíg létre nem hozta az összes fizikai kötetet a rendelkezésre álló lemezeken.

RAID 0 és RAID 1 esetében legalább két partícióra van szükség – RAID 1 esetében jellemzően pontosan kettőre, nem többre. RAID 5 használata esetén legalább három partícióra van szükség. Célszerű csak pontosan egyforma méretű partíciókat készíteni.

A RAID-partíciókat külön lemezre készítse, így csökkenthető az adatok elvesztésének a kockázata, ha valamelyik megsérül (RAID 1 és 5), illetve optimalizálható a RAID 0 tömb teljesítménye. A RAID-hez használni kívánt összes partíció létrehozása után kattintson a *RAID* > *RAID hozzáadása* menüpontra a RAID-beállítások megkezdéséhez.

A következő párbeszédablakban válasszon a RAID 0, 1 és 5 szintek közül. Ezután válassza ki a „Linux RAID” vagy „Linux native” típusú partíciókat, amelyeket a RAID-rendszer használni fog. A csere- és DOS-partíciók nem jelennek meg.

2.5. ábra *RAID-partíciók*

Egy korábban még sehová nem rendelt partíciót a kijelölt RAID-kötethez a partícióra, majd a *Hozzáadás* kattintva lehet hozzáadni. Ossza ki az összes, RAID-nek szánt partíciót. Ellenkező esetben a partíciókon található terület üresen marad. Az összes partíció hozzárendelése után kattintson a *Tovább* gombra a rendelkezésre álló *RAID beállítás* kiválasztásához.

A legutolsó lépésben állítsa be a használni kívánt fájlrendszert, valamint a titkosítást és a RAID-kötet csatolási pontját. A beállításokat a *Befejezés* gombbal befejezve a `/dev/md0` eszköz és mások mellett a *RAID* megjelölés látható a szakértői particionáló modulban.

2.3.2 Hibaelhárítás

Azt, hogy a RAID-partíció sérült-e, a `/proc/mdstat` fájl megtekintésével lehet ellenőrizni. Rendszermeghibásodás esetén állítsa le a Linux-rendszert és cserélje ki a hibás merevlemezt egy olyanra, amely ugyanolyan módon van particionálva. Ezután indítsa újra a rendszert, majd írja be az `mdadm /dev/mdX --add /dev/sdX` parancsot, ahol az 'X' helyére a megfelelő eszközazonosítónak kell kerülnie. Így a merevlemez automatikusan integrálódik a RAID-rendszerbe és az tökéletesen helyreáll.

Ne feledje, hogy bár az újjáépítés során hozzáfér minden adathoz, a RAID teljes helyreállításáig csökkent teljesítményt tapasztalhat.

2.3.3 További információk

A szoftveres RAID-del kapcsolatos beállítási utasítások és további részletek a HOWTO dokumentumokban találhatók, a következő címen:

- `http://en.tldp.org/HOWTO/Software-RAID-HOWTO.html`
- `/usr/share/doc/packages/mdadm/Software-RAID.HOWTO.html`

Léteznek Linux RAID levelezési listák is, mint például a `http://marc.theaimsgroup.com/?l=linux-raid`.

II. rész - Szoftverkezelés és -frissítés

Szoftver telepítése és eltávolítása

3

A rendszeren található szoftverek módosításához használja a YaST-ot. A YaST szoftverkezelő eszközével kikereshetők a felvenni vagy eltávolítani kívánt szoftverösszetevők. A YaST az összes függőséget feloldja. Ha olyan csomagokat kíván felvenni a rendszerbe és a YaST-tal kezelni, amelyek nem szerepelnek a telepítési adathordozón, vegyen fel további szoftverforrásokat. A rendszer naprakészen tartásához, a szoftverfrissítések kezeléséhez használja a openSUSE Updater programot.

3.1 Fogalmak

forrás (repository)
: Egy helyi vagy távoli könyvtár, amely csomagokat és a csomagokkal kapcsolatos extra információt (metaadatokat) tartalmaz.

(forrás)álnév (repository alias)
: A különféle zypper-parancsok által a forrásra használt rövid név. Ezt az álnevet a felhasználó választja a forrás felvételekor, és egyedinek kell lennie.

termék (product)
: Egy teljes terméket ábrázol, ilyen például az openSUSE.

minta (pattern)
: A minta egy adott célra szolgáló csomagok telepíthető listája. Ilyen minta például az `Alaprendszer`, amely az openSUSE alapvető rendszerfájljait tartalmazza, vagy a `GNOME alaprendszer`, amelyik a GNOME asztali környezet futtatásához szükséges fájlokat.

csomag (package)
: A csomag egy tömörített, rpm formátumú fájl, amely egy adott program fájljait tartalmazza.

javítás (patch)
: A javítás egy vagy több csomagból áll – teljes csomagokból, vagy patchrpm ill. deltarpm csomagokból –, és bevezethet függőségeket olyan csomagokra vonatkozóan, amelyek még nincsenek telepítve.

feloldható (resolvable)
: A termékekre, mintákra, csomagokra és javításokra használt összefoglaló név. A feloldhatók leggyakoribb fajtája a csomag vagy a javítás.

patchrpm
: A patchrpm csak azokból a fájlokból áll, amelyek az openSUSE 11.1 kiadás óta frissítve lettek. Ennek letöltési mérete általában jóval kisebb, mint a teljes csomagé.

deltarpm
: A deltarpm csak a bináris különbségeket tartalmazza egy csomag két meghatározott verziója között, így ennek a legkisebb a letöltendő mérete. Telepítés előtt az rpm csomagot újra kell építeni a helyi gépen.

3.2 A Qt felület használata

3.2.1 Szoftvertelepítés

A szoftverek RPM-csomagok formájában érhetők el. Minden egyes csomag magát a programot, a konfigurációs fájljait, valamint kiegészítő dokumentációt tartalmaz. Ha további szoftvereket szeretne telepíteni a rendszeren:

1. Kattintson a *Szoftver* > *Szoftverkezelés* pontokra a YaST csomagkezelő elindításához.

2. A keresőmezőbe írja be a telepíteni kívánt szoftver nevét (például azt, hogy `jhead`, ami egy JPEG-metaadatokat kezelő eszköz), vagy nevének egy részét, majd nyomja meg az Enter gombot.

3. A megfelelő nevű csomagok a jobb oldali keretben listázódnak ki. Válassza ki a telepíteni kívánt csomagot. Ha ezzel megvan, további csomagokra is rákereshet és egyszerre is kijelölheti őket telepítésre.

4. Kattintson az *Elfogadás* gombra.

5. Az összes kijelölt csomag telepítése után a YaST rákérdez, hogy kíván-e más csomagokat telepíteni vagy eltávolítani. A YaST bezárásához kattintson a *Nem* gombra.

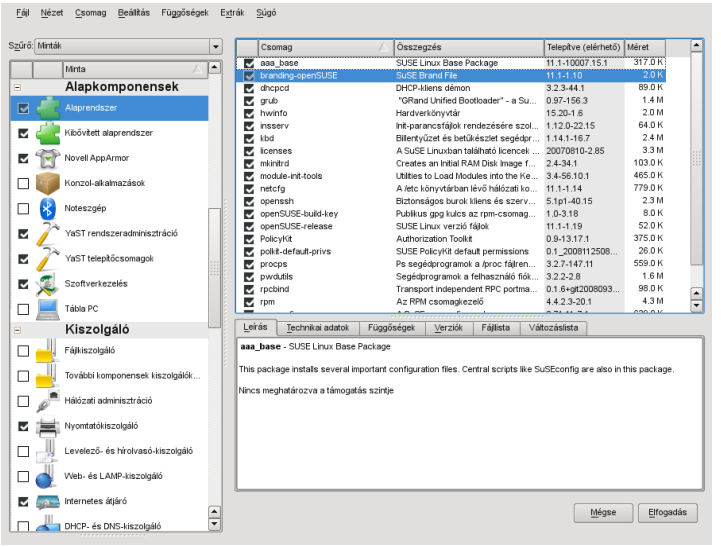
Különféle keresési feltételek megadásával az eredményhalmaz néhány, vagy akár egyetlen csomagra is szűkíthető. Speciális keresési minták is megadhatók helyettesítő karakterek és reguláris kifejezések használatával, *Keresési mód*-ban.

TIPP: Gyorskeresés

A *Keresés* szűrőn túl a csomagkezelő összes listájában használható egy gyorskereső is. Kattintson a megfelelő listára a fókusz odahelyezésére (például a *Csomag* listára) majd írjon be egy betűt, mire a kurzor az első csomagra ugrik, amelynek a neve az adott betűvel kezdődik.

Ha nem ismeri pontosan a szoftver nevét, amelyet keres, még mindig számos módon lehet keresgélni a szoftverkatalógusban. Lehet szűrni minták, csomagcsoportok, nyelvek, források, de még a telepítési összefoglalók alapján is. Szűrjön mintákra, ha egy adott feladatra szolgáló szoftvert keres:

1. A bal felső sarokban látható szűrőlistából válassza ki a *Minták* pontot. Alatta megjelennek a különböző minták.



2 Válassza ki közülük a kívánt mintát. Amikor rákattint egy minta nevére (például az *Alap fejlesztőkörnyezet*), akkor a jobb keretben megjelenik a benne található csomagok listája. Ha megjelöli, akkor a sor elején megváltozik az állapotjelző: az összes csomag állapota *Megtart* vagy *Telepítés* állapotra változik. A szimbólumok és a betűszín-jelentések magyarázata a *Súgó* > *Szimbólumok* részben található.

3 Kattintson az *Elfogadás* gombra.

Szűrhet csomagcsoportokra is. A csomagcsoportok a kategóriáknál részletesebb nézetet biztosítanak a szoftverekről. Sok csomag függ más csomagoktól; ha kiválaszt egy csomagot, akkor szükség lehet további csomagok telepítésére a függőségek feloldásához.

A nyelvek szerinti szűrés a csomagcsoportok szerinti szűréshez hasonlít. A nyelvek nézetben egy adott nyelv támogatásához szükséges lefordított programüzenetek, dokumentációk, speciális betűkészletek és más hasonló csomagok választhatók ki.

A megfelelő forráscsomagok telepítéséhez használja a `zypper`-t. További információ: 7.1.2. - Szoftverek telepítése és eltávolítása a Zypper segítségével (82. oldal).

Használja a telepítés összesítési szűrőjét a telepítésre kijelölt csomagok áttekintéséhez. Kényelmes módszert jelent a biztonsági ellenőrzéshez, ha sok csomag van megjelölve a telepítéshez.

3.2.2 Szoftverfüggőségek ellenőrzése

Az egy adott csomagban található szoftverek lehet, hogy csak akkor működnek tökéletesen, ha egy szükséges másik csomag is telepítve van. Ha hasonló, vagy egyforma funkciójú programok ugyanazt a rendszererőforrást használják, akkor nem szabad őket egyszerre telepíteni, mert ez csomagütközést eredményez.

A csomagkezelő indulásakor megvizsgálja a rendszert és kijelzi a telepített csomagokat. Amikor kiválasztja a telepíteni és eltávolítani kívánt csomagokat, a csomagkezelő automatikusan ellenőrzi a függőségeket és kiválasztja az összes többi szükséges csomagot (függőségek feloldása). Ha ütköző csomagokat választ egyszerre ki, a csomagkezelő figyelmeztet erre és megoldásokat javasol a problémára (ütközések feloldása).

A *Függőségek ellenőrzése* és az *Automatikus ellenőrzés* az információs ablak alatt található. Ha a *Függőségek ellenőrzése* gombra kattint, akkor a csomagkezelő megvizsgálja, hogy az aktuális csomagválaszték eredményez-e bármilyen feloldatlan csomagfüggőséget vagy -ütközést. Ha vannak feloldatlan függőségek, akkor a szükséges további csomagokat automatikusan kiválasztja a rendszer. Csomagütközés esetén a csomagkezelő megnyit egy párbeszédablakot, amely megmutatja az ütközést és különféle megoldásokat javasol a problémára.

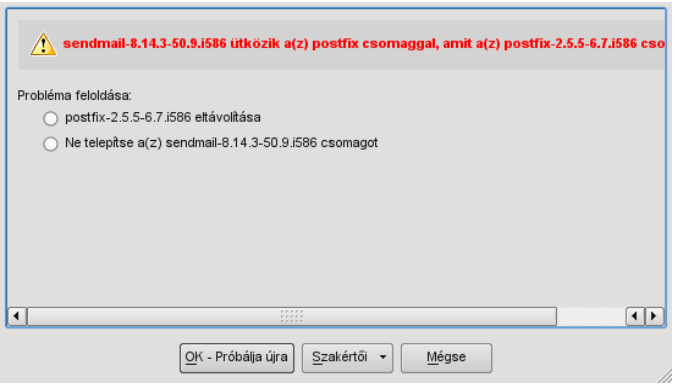
Ha megjelöli az *Automatikus ellenőrzés* pontot, akkor egy csomag állapotának megváltozása automatikus ellenőrzést eredményez. Ez egy igen hasznos funkció, mivel a csomagkiválasztás konzisztenciáját állandóan figyeli a rendszer. Ez azonban erőforrásokat igényel, és lelassíthatja a csomagkezelőt. Éppen ezért az *Automatikus ellenőrzés* alapértelmezés szerint nincs megjelölve. Mindkét esetben konzisztenciaellenőrzés történik, amikor az *Elfogad* gombra kattintva megerősíti a kiválasztást.

Például a `sendmail` és a `postfix` nem lehet egyszerre telepítve. A 3.1. ábra - Csomagütközések kezelése a csomagkezelővel (66. oldal) ábra bemutatja, hogy milyen üzenetet kap ütközés esetén és milyen döntéseket hozhat. A `postfix` már telepítve van. Ennek megfelelően választhatja azt, hogy kihagyja a `sendmail` telepítését, eltávolítja a `postfix` csomagot, vagy vállalja a kockázatot és figyelmen kívül hagyja az ütközést.

FIGYELEM: Csomagütközések kezelése

Hacsak nem rendelkezik bőséges tapasztalatokkal, azt javasoljuk, hogy fogadja meg a YaST tanácsait a csomagütközések kezelésekor. Ha nem így tesz, az ütközés a rendszer stabilitását és funkcionalitását veszélyeztetheti.

3.1. ábra *Csomagütközések kezelése a csomagkezelővel*



3.2.3 Csomagok és szoftverforrások

Ha egy adott szoftverforrásban található csomagokra kíván keresni, akkor használja a *Telepítési források* szűrőt. Az alapértelmezett konfigurációban ez a szűrő az adott telepítési forrásból származó összes csomag listáját jeleníti meg. Ha tovább kívánja szűkíteni a listát, használjon másodlagos szűrőt.

Az adott telepítési forrás összes telepített csomagjának megtekintéséhez válassza ki a *Telepítési források* szűrőt, majd *A telepítés összegzése* menüpontot a *Másodlagos szűrők* közül, és törölje az összes négyzetet, kivéve a *Megtart* jelzésűt.

Ha pont a fordítottja érdekli, és azokat a csomagokat keresi, amelyek nem tartoznak semmilyen forráshoz, szintén használhatja a *Telepítési források* szűrőt, de utána a *Karbantartás nélküli csomagok* pontot válassza ki, mint *Másodlagos szűrő*.

3.2.4 Szoftver törlése

Ha törölni kíván szoftvert a rendszerből, az alábbi módon járjon el:

1. A 3.2.1. - Szoftvertelepítés (62. oldal) részben leírt módon határozza meg a keresési eljárást.

2. A keresési eljárástól függően kiválaszthat egy csomagot, vagy csomagok egy halmazát. Minták esetében mind a két módszer alkalmazható.

3. Kattintson az *Elfogad* gombra, és tekintse meg az eltávolítási folyamatot, vagy ha a YaST függőségre panaszkodna, módosítsa a kijelölést.

3.3 A Gtk felület használata

A rendszeren található szoftverek módosításához használja a YaST-ot. A YaST szoftverkezelő eszközével kikereshetők a felvenni vagy eltávolítani kívánt szoftverösszetevők. A YaST az összes függőséget feloldja. Ha olyan csomagokat kíván felvenni a rendszerbe és a YaST-tal kezelni, amelyek nem szerepelnek a telepítési adathordozón, vegyen fel további szoftverforrásokat. A rendszer naprakészen tartásához, a szoftverfrissítések kezeléséhez használja a openSUSE Updater programot.

3.3.1 Szoftvertelepítés

A szoftverek RPM-csomagok formájában érhetők el. Minden egyes csomag magát a programot, a konfigurációs fájljait, valamint kiegészítő dokumentációt tartalmaz. Ha további szoftvereket szeretne telepíten a rendszeren:

1. Kattintson a *Szoftver* > *Szoftverkezelés* pontokra a YaST csomagkezelő elindításához.

2. A keresőmezőbe írja be a telepíteni kívánt szoftver nevét (például azt, hogy `xpdf`, ami egy PDF-olvasó alkalmazás). A YaST már aközben elkezdi keresni a csomagot, miközben a nevet írja be. A keresés végén válassza ki a kívánt csomagot a fő ablakrészben, majd nyomja meg a *Telepítés* gombot.

3. További csomagokat ugyanilyen módon tud kikeresni és kilistázni.

4 Ha kész, kattintson az *Alkalmaz* gombra a felsorolt csomagok telepítéséhez.

Ha nem ismeri pontosan a szoftver nevét, amelyet keres, még mindig számos módon lehet keresgélni a szoftverkatalógusban. Csoportosíthat például minták, csomagcsoportok, nyelvek és források alapján. Csoportosítson minták alapján, ha egy adott feladatra szolgáló szoftvert keres:

1 A bal felső sarokban látható csoportosító menüből válassza ki a *Minták* pontot. Alatta megjelennek a különböző minták.

2 Válassza ki közülük a kívánt mintát. Amikor rákattint egy minta nevére (például az *Alap fejlesztőkörnyezet*), akkor a jobb keretben megjelenik a benne található csomagok listája. Az *Összes telepítése* pontra kattintva a csomagok jobb oldalon megjelennek az áttekintésben felsorolva.

3 Kattintson az *Alkalmaz* gombra az összes kiválasztott csomag telepítéséhez.

Szűrhet csomagcsoportokra is. A csomagcsoportok a kategóriáknál részletesebb nézetet biztosítanak a szoftverekről. Sok csomag függ más csomagoktól; ha kiválaszt egy csomagot, akkor szükség lehet további csomagok telepítésére a függőségek feloldásához.

A nyelvek szerinti csoportosítás a csomagcsoportok szerinti csoportosításhoz hasonlít. A nyelvek nézetben egy adott nyelv támogatásához szükséges lefordított programüzenetek, dokumentációk, speciális betűkészletek és más hasonló csomagok választhatók ki.

A megfelelő forráscsomagok telepítéséhez használja a `zypper`-t. További információkért lásd: 7.1.2. - Szoftverek telepítése és eltávolítása a Zypper segítségével (82. oldal).

3.3.2 Szoftverfüggőségek ellenőrzése

Az egy adott csomagban található szoftverek lehet, hogy csak akkor működnek tökéletesen, ha egy szükséges másik csomag is telepítve van. Ha hasonló, vagy egyforma funkciójú programok ugyanazt a rendszererőforrást használják, akkor nem szabad őket egyszerre telepíteni, mert ez csomagütközést eredményez.

A csomagkezelő indulásakor megvizsgálja a rendszert és kijelzi a telepített csomagokat. Amikor kiválasztja a telepíteni és eltávolítani kívánt csomagokat, a csomagkezelő automatikusan ellenőrzi a függőségeket és kiválasztja az összes többi szükséges csomagot

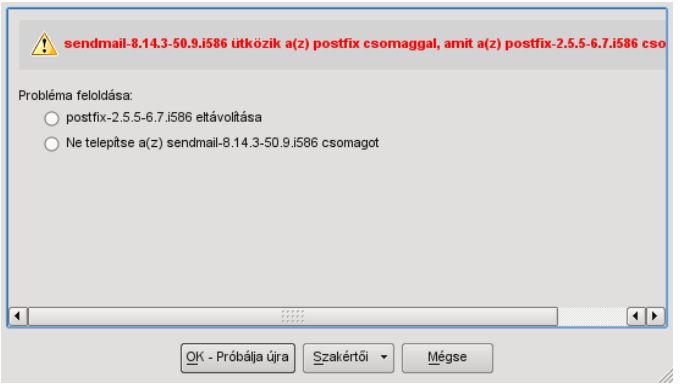
(függőségek feloldása). Ha ütköző csomagokat választ egyszerre ki, a csomagkezelő figyelmeztet erre és megoldásokat javasol a problémára (ütközések feloldása).

Például a `sendmail` és a `postfix` nem lehet egyszerre telepítve. A 3.1. ábra - Csomagütközések kezelése a csomagkezelővel (66. oldal) ábra bemutatja, hogy milyen üzenetet kap ütközés esetén és milyen döntéseket hozhat. A `postfix` már telepítve van. El kell döntenie, hogy a `sendmail`-t telepíti, vagy a `postfix`-et távolítja el.

FIGYELEM: Csomagütközések kezelése

Hacsak nem rendelkezik bőséges tapasztalatokkal, azt javasoljuk, hogy fogadja meg a YaST tanácsait a csomagütközések kezelésekor. Ha nem így tesz, az ütközés a rendszer stabilitását és funkcionalitását veszélyeztetheti.

3.2. ábra *Csomagütközések kezelése a csomagkezelővel*



3.3.3 Csomagok és szoftverforrások

Ha egy adott szoftverforrásban található csomagokra kíván keresni, akkor használja a *Telepítési források* csoportosítási lehetőséget. Ez a nézet egy adott telepítési forrás összes csomagját jeleníti meg.

A kiválasztott telepítési forrás összes telepített csomagjának megjelenítéséhez kattintson a *Telepített* pontra. Először válassza ki az eltávolítani kívánt csomagokat. A fordított művelethez kattintson az *Elérhető* gombra és válassza ki a telepíteni kívánt csomagokat.

3.3.4 Szoftver törlése

Ha törölni kíván szoftvert a rendszerből, az alábbi módon járjon el:

1. A 3.3.1. - Szoftvertelepítés (67. oldal) részben leírt módon határozza meg a keresési eljárást.

2. A *Csomaglista* részben jelölje meg az eltávolítani kívánt csomagokat. Az összes egy kattintással megjelöléséhez kattintson a jobb egérgombbal a *Csomaglista* ablakrészre, és válassza ki az *Összes kijelölése* pontot.

3. Kattintson az *Eltávolítás* gombra.

   Ha olyan csomagot próbál meg eltávolítani, amelyre valamilyen telepített szoftvernek szüksége van, az ütközéskezelő jelzi a függőségi problémákat és az ütközéseket fel kell oldania a 3.3.2. - Szoftverfüggőségek ellenőrzése (68. oldal) részben leírt módon.

   Az összes ütközés feloldása után az eltávolításra jelölt csomagok a jobb oldali *Változások* részben jelennek meg.

4. Kattintson az *Alkalmaz* gombra a *Változások* részben látható műveletek elvégzéséhez.

3.4 Szoftverforrások hozzáadása

Külső gyártók szoftvereinek telepítéséhez vegyen fel külső szoftverforrásokat a rendszerbe. Alapértelmezésben a termékforrás (például az openSUSE-DVD 11.1) és egy ehhez tartozó frissítési forrás van beállítva, ha regisztrálta a rendszert; további információk a regisztrációról: „Registration” szakasz (1. fejezet - *Installation with YaST*, ↑*Start-Up*). Az eredetileg kiválasztott terméktől függően szükség lehet egy külön kiegészítő forrás (fordítások, szótárak stb.) beállítására.

FIGYELEM: Külső szoftverforrások megbízhatóvá nyilvánítása

Külső szoftverforrások forráslistába történő felvétele előtt győződjön meg róla, hogy a forrás megbízható. Az openSUSE nem felelős semmilyen esetleges gondért, amelyet külső gyártók szoftverforrásaiból telepített szoftverek okoznak.

Az integritás biztosításához a szoftverforrások alá lehetnek írva a forrás karbantartójának GPG-kulcsával. Ezek a kulcsok a YaST-ban kezelhetők – további információ: GPG-kulcsok (72. oldal). Új forrás felvételekor a YaST felajánlja a kulcsok importálását. Ellenőrizze ugyanúgy, mint minden más GPG-kulcsot és figyeljen rá, hogy ne változzon. Ha azt észleli, hogy a kulcs megváltozott, akkor valami baj van a forrással és jobban teszi, ha letiltja azt a telepítési források közül, míg ki nem deríti a kulcsmódosítás okát.

Termékforrások felvételéhez vagy kattintson közvetlenül a YaST vezérlőközpont *Szoftver* panelében található *Szoftverforrások* elemre, vagy keresse meg ugyanezt a *Szoftverkezelés*-nél, a következők szerint:

1. A *Szoftverkezelés* kezdő képernyőjén kattintson a bal felső legördülő menü *Források* elemére, majd ezután a *Szerkesztés* lehetőségre a beállított szoftverforrások áttekintéséhez.

2. Kattintson a *Hozzáadás* gombra a forrást tartalmazó adathordozó típusának kiválasztásához (nyelvi kiegészítők esetében pl. *DVD* vagy *USB tároló*). Ezután kattintson a *Tovább* gombra az adathordozó további információinak megjelenítéséhez.

3. A YaST kérni fogja az adathordozó behelyezését.

4. Ha ez megtörtént, erősítse meg a *Folytatás* gombra kattintva. Néhány pillanat múlva a YaST letölti és értelmezi a forrás metaadatait. Ha kész, akkor telepítheti a forrásból származó forrásokat a 3.2.1. - Szoftvertelepítés (62. oldal) ill. 3.3.1. - Szoftvertelepítés (67. oldal) részben leírtak szerint.

Ha az openSUSE Build Service egy forrását szeretné felvenni – például a Mozilla (`http://download.opensuse.org/repositories/mozilla/`) egyik változatát –, akkor használja a YaST *Közösségi források* konfigurációs párbeszédablakát:

1. A *Szoftverkezelés* kezdő képernyőjén kattintson a bal felső legördülő menü *Források* elemére, majd ezután a *Szerkesztés* lehetőségre a beállított szoftverforrások áttekintéséhez.

2. Kattintson a *Hozzáadás* gombra a forrást tartalmazó adathordozó típusának kiválasztásához (Mozilla projektek esetében pl. *Közösségi források*). Majd kattintson a *Tovább* gombra.

3. A források listájában aktiválja a kívánt elemeket (pl. *openSUSE BuildService - Mozilla*).

Hagyja jóvá az *OK* gombbal.

4. Az új szoftverforrás megjelenik a *Beállított szoftverforrások* áttekintésben. Kattintson ismét az *OK* gombra a kiegészítő csomagok telepítéséhez a forrásból a 3.2.1. - Szoftvertelepítés (62. oldal) ill. 3.3.1. - Szoftvertelepítés (67. oldal) részben leírtak szerint.

A *Beállított szoftverforrások* áttekintésben több beállítási lehetőséget talál:

Tulajdonságok
: Alapértelmezésben egy új forrás felvétele után a forrás állapota *Engedélyezett* és az *Automatikus frissítés* aktív. Ez azt jelenti, hogy a YaST automatikusan betölti a frissített metaadatokat és Ön mindig értesülni fog az új változatokról.

  A forrás *priorítása* egy `0` és `99` közötti érték, a `0` jelöli a legmagasabb prioritást. Ha a csomag egynél több forrásban is rendelkezésre áll, akkor a legmagasabb prioritású forrás nyer. Ez rendkívül hasznos, ha szeretne magasabb prioritást adni a helyi forrásoknak (például egy DVD-nek) azért, hogy a rendszer ne töltsön le csomagokat fölöslegesen az internetről még akkor sem, ha azok verziószáma azonos vagy magasabb.

GPG-kulcsok
: A *GPG-kulcsok* elemre kattintva megnyílik a GPG nyilvános kulcsok kezelésre szolgáló felület. Az alsóbb szintű *GPG-kulcsok* párbeszédablakban kézzel lehet kulcsokat felvenni, illetve törölni és szerkeszteni lehet a meglévő kulcsokat.

Frissítés
: A *Frissítés* kiválasztásával többféleképpen is frissítheti a forrás-metaadatokat.

4 Egykattintásos telepítés

Telepíthet szoftvercsomagokat egy webböngészőből is, anélkül, hogy előbb "előfizetne" egy forrásra. Például kikeresheti az openSUSE Build Service-ből (összeállítási szolgáltatás) a telepíteni kívánt szoftvert. Ez az eljárás a *Csomagok keresése* része, és „1-Click Install” (egykattintásos telepítés) névre hallgat.

1. Indítsa el az openSUSE Build Service-t (`http://software.opensuse.org/search`).

2. Keresse ki a telepíteni kívánt csomagot, például az OpenStreetMap szerkesztőt (`josm`), majd a legördülő menüből válassza ki rendszerének verzióját (például `openSUSE 11.1` vagy `SLE_11`).

3. Kattintson a *Keresés* gombra.

4. Az eredménylistából válassza ki a kívánt elemet, majd kattintson a *1-Click Install* gombra.

5. A webböngésző letöltési párbeszédablakában válassza ki a YaST Metacsomag-kezelőt.

6. A *További szoftverforrások* párbeszédablakban válassza ki a forrás beállításait. Ha érdeklik a frissítések, akkor hagyja megjelölve *A feliratkozás megtartása telepítés után ezekre a telepítési forrásokra* pontot. Ha nem, törölje a jelölést.

   Ha megtartja az előfizetést a forrásokra, akkor a többi csomagkezelő eszköz, például a YaST vagy a zypper képes lesz telepíteni vagy frissíteni szoftvereket belőle. Ha kész, kattintson a *Tovább* gombra.

7 Hagyja jóvá a következő, *Telepítendő szoftver* és *Javaslat* című ablakokat a *Tovább* gombbal. Gondosan olvassa el az esetleges figyelmeztetéseket.

8 Írja be a `root` jelszavát, ha ténylegesen telepíteni kívánja a kijelölt szoftverösszetevőket. Számos, az előrehaladást jelző ablak jelenik meg. A „Telepítés sikerült” üzenet megjelenése után kattintson a *Befejezés* gombra.

TIPP: A 1-Click Install funkció letiltása

Ha le akarja tiltani a 1-Click Install funkciót, akkor távolítsa el a `yast2-metapackage-handler` csomagot a YaST segítségével, vagy írja be `root`ként az alábbi parancsokat:

```
rpm -e yast2-metapackage-handler
```

---

5 YaST online frissítés

Az openSUSE folyamatosan készít szoftverbiztonsági javításokat a termékhez. Alapértelmezés szerint a openSUSE Updater szolgál a rendszer naprakészen tartására. További információ az openSUSE Updater-ről: 3.3. - Keeping the System Up-to-date (3. fejezet - *Installing, Removing and Updating Software*, ↑*Start-Up*). Ebben a fejezetben a szoftvercsomagok frissítésére szolgáló másik eszközt mutatjuk be: a YaST Online frissítést.

Az openSUSE aktuális frissítései egy frissítési szoftverforrásból érhetők el. Ha a terméket regisztrálta a telepítés során, akkor a frissítési szoftverforrás már be van állítva. Ha még nem regisztrálta az openSUSE terméket, akkor ezt a YaST-ban a *Szoftver* > *Online frissítések beállítása* részben a *Szakértői* > *Regisztráció a támogatáshoz és a frissítésekhez* pontot kiválasztva teheti meg. Alternatív megoldásként kézzel is felvehet egy frissítési forrást egy megbízhatónak tartott helyről. A források felvételéhez és eltávolításához indítsa el a Forráskezelőt a *Szakértői* > *Szoftverforrások szerkesztése* pont kiválasztásával. A Forráskezelőről további részletek: 3.4. - Szoftverforrások hozzáadása (70. oldal).

Az openSUSE különböző fontosságú frissítéseket biztosít. A `biztonsági` frissítések lényeges biztonsági kockázatokat szüntetnek meg és ezeket feltétlenül telepíteni kell. A `javasolt` frissítések olyan problémákat oldanak meg, amelyekből esetleg bajok származhatnak a számítógépen, míg az `opcionális` frissítések nem biztonsági kérdésekkel kapcsolatosak, vagy bővítéseket kínálnak.

A frissítések és továbbfejlesztések telepítéséhez a YaST segítségével használja a *Szoftver* > *Online frissítés* modult. A rendszerhez elérhető összes új javítás (kivéve az opcionálisakat) azonnal meg is van jelölve telepítésre. Az *Elfogadás* gombra kattintva automatikusan telepítheti ezeket a javításokat. A telepítés végén erősítse meg a *Befejezés* gombbal. A rendszer immár naprakész.

5.1 Javítások telepítése kézzel

Az *Online frissítés* ablak négy részből áll. Az összes elérhető javítás listája baloldalt látható. A kiválasztott javítás leírása a javítások listája alatt jelenik meg. A jobb oszlopban az éppen kiválasztott javításban található csomagok láthatók (egy javítás több csomagból is állhat), alatta pedig a kiválasztott csomag részletes leírása. Opcionálisan a lemezhasználat is megjeleníthető a bal oszlop alján (ez a képernyő alapértelmezés szerint ki van szürkítve – a jobb oldali csúszkával lehet láthatóvá tenni).

A javítási képernyőn az openSUSE elérhető javításai láthatók. A javítások biztonsági fontosság szerint vannak sorbaszedve: `biztonsági`, `javasolt` és `opcionális`. A javítások háromféle nézetben tekinthetők meg. A *Javítási kategória megjelenítése* gombbal lehet váltani a nézetek közt:

Szükséges javítások (alapértelmezett nézet)
: A rendszeren telepített csomagokra vonatkozó, még nem telepített javítások.

Szükségtelen javítások
: Vagy a rendszeren nem telepített csomagokra vonatkozó javítások, vagy olyan javítások, amelyek követelményei már teljesítve vannak (mert valamilyen más forrásból már frissítve vannak).

Minden javítás
: Az openSUSE összes elérhető javítása.

A lista egy bejegyzése egy szimbólumból és a javítás nevéből áll. Az összes lehetséges szimbólum listájának megtekintéséhez nyomja meg a Shift + F1 billentyűt. A `Biztonság` és `Javasolt` javítások által igényelt műveletek automatikusan be vannak állítva előre. Ezek a műveletek az *Automatikus telepítés*, az *Automatikus frissítés* és az *Automatikus törlés*. Az `Opcionális` javítások műveletei nincsenek előre beállítva – kattintson a jobb egérgombbal egy javításra és válassza ki a műveletet a megjelenő listából.

Ha egy naprakész csomagot a frissítési forrástól eltérő, másik forrásból telepít, akkor lehet, hogy a csomag javításának követelményei teljesülnek ezzel a telepítéssel. Ebben az esetben egy pipa jelenik meg a javítás összefoglalása előtt. A javítás addig látható marad a listában, amíg meg nem jelöli telepítésre. Ebben az esetben a javítás telepítése nem fog ténylegesen megtörténni (hiszen a csomag már naprakész), de a javítás úgy lesz megjelölve, mintha telepítve lett volna.

A legtöbb javítás egynél több csomag frissítéseit tartalmazza. Ha az egyes csomagokra vonatkozóan akarja átállítani a műveleteket, akkor kattintson a jobb egérgombbal a csomag nevén a csomagablakban és válassza ki a kívánt műveletet. Ha már minden javítás és csomag a kívánt módon van megjelölve, folytassa az *Elfogad* gombra kattintással.

TIPP: Deltarpm-ek letiltása

Alapértelmezés szerint a frissítések deltarpm-ekként töltődnek le. Mivel az rpm-csomagok újraépítése a deltarpm-ekből memória- és processzorigényes feladat, bizonyos beállítások vagy hardverkonfiguráció esetén szükség lehet a deltarpm-ek használatának letiltására a teljesítmény érdekében. A deltarpm-ek használatának letiltásához az `/etc/zypp/zypp.conf` fájlban a `download.use_deltarpm` paramétert állítsa `false` értékre.

5.2 Automatikus online frissítés

A YaST-tal automatikus frissítés is beállítható. Nyissa meg a *Szoftver > Online frissítések beállítása* pontot. Jelölje meg az *Automatikus online frissítés* pontot, majd válassza ki a frissítés gyakoriságát: *naponta*, *hetente* vagy *havonta*. Egyes javítócsomagok, például a kernel frissítései, mindenképpen megkövetelik a felhasználó beavatkozását. Ezek az automatikus frissítési folyamat leállását eredményezik. Éppen ezért meg kell jelölni az *Interaktív javítások kihagyása* pontot, ha azt akarja, hogy a frissítési eljárás teljesen automatikusan végbemenjen. Ebben az esetben időről időre kézi *Online frissítést* is végezni kell ahhoz, hogy a beavatkozást igénylő javítások is telepítve legyenek.

6 Kiegészítő termékek telepítése

A kiegészítő termékek a rendszer bővítései. Telepíthetők külső gyártók kiegészítő termékei, de az openSUSE speciális rendszerbővítései is, például egy olyan CD, amelyen más nyelvek támogatása vagy bináris illesztőprogramok is találhatók. Egy új kiegészítő telepítéséhez használja a *Szoftver* > *Kiegészítő termék* menüpontot . Többféle termékadathordozó is kiválasztható, CD, FTP, USB-tárolók (pl. USB flash-meghajtók), és helyi könyvtár is megadható. Sőt, kezelhet közvetlenül ISO-fájlokat is. Ha ISO-adathordozót kíván használni, akkor válassza ki a *Helyi ISO lemezkép* pontot, majd töltse ki az *Elérési útvonal az ISO lemezképhez* mezőt. A *Telepítési forrás nevét* nem kötelező megadni.

6.1 Kiegészítők

Új kiegészítőt a következők szerint kell telepíteni:

1. Kattintson a *Szoftver* > *Kiegészítő termék* pontra a telepített kiegészítő termékek megjelenítéséhez.

2. Válassza ki a termék adathordozóját (CD, FTP vagy helyi könyvtár), majd kattintson a *Hozzáadás* gombra. CD-k és DVD-k helyett ISO-lemezképek is használhatók.

3. ISO-lemezkép hozzáadásához válassza ki a *Helyi ISO-lemezkép* pontot, majd kattintson a *Tovább* gombra.

4. Töltse ki az *Elérési útvonal az ISO lemezképhez* és a *Telepítési forrás neve* mezőket. Kattintson a *Tovább* gombra.

5. A kiegészítő adathordozójának sikeres hozzáadása után megjelenik a szoftverkezelő ablaka. Ha a kiegészítő új mintát biztosít, akkor az új elem a *Minták* szűrővel látható. A kijelölt telepítési forrás összes csomagjának megtekintéséhez válassza ki a *Telepítési források* szűrőt, majd a megtekinteni kívánt telepítési forrást. Egy adott kiegészítő csomagjainak csomagcsoportonkénti megjelenítéséhez használja a *Csomagcsoportok* másodlagos szűrőt a YaST Qt felületén.

6.2 Bináris illesztőprogramok

Egyes hardvereszközök bináris illesztőprogramok használatát igénylik a helyes működéshez. Ilyen hardvereszköz birtokában forduljon a kiadási megjegyzésekhez azzal kapcsolatban, hogy léteznek-e bináris illesztőprogramok a rendszerhez. A kiadási megjegyzések elolvasásához nyissa meg a YaST-ot és válassza ki az *Egyéb* > *Kiadási megjegyzések* pontot.

Szoftverkezelés parancssori eszközökkel

7

Ez a fejezet a Zyppert és az RPM-et írja le, a szoftverek kezelésére szolgáló két parancssori eszközt.

7.1 A Zypper használata

A Zypper egy csomagok telepítésére és frissítésére szolgáló parancssoros eszköz. Különösen a távoli szoftverfelügyeleti feladatok végrehajtásánál vagy a szoftverek parancsfájlokból történő kezelésénél hasznosak.

A zypperben van egy beépített súgóáttekintő:

```
zypper help
```

7.1.1 Általános használat

A zypper általános szintaxisa:

```
zypper [globális-kapcsolók] parancs [parancskapcsolók] [paraméterek] ...
```

A zárójeles összetevők használata nem kötelező. A zypper végrehajtásának legegyszerűbb módja, ha begépeli a nevét valamilyen parancs után. Ha például alkalmazni szeretné a rendszertípus összes javítását:

```
zypper update
```

Emellett egy vagy több általános beállítást is kiválaszthat mindössze azzal, ha begépeli azokat a parancs előtt. A `--non-interactive` például azt jelenti, hogy úgy futtatja a parancsot, hogy az ne kérdezzen vissza semmit, fogadjon szót:

```
zypper --non-interactive update
```

Egy adott parancs specifikus beállításainak használatához írja azokat a parancs mögé. Az `--auto-agree-with-licenses` például azt jelenti, hogy a rendszer összes szükséges javítását úgy alkalmazza, hogy a gép ne kérdezzen rá a licencek elfogadására – azok ugyanis mind el vannak olvasva:

```
zypper update --auto-agree-with-licenses
```

A parancsok némelyikéhez több paraméter is szükséges:

```
zypper install mplayer
```

A beállítások némelyike szintén megköveteli valamilyen paraméter megadását. A következő például azt jelenti, hogy a rendszert frissíteni kell az újabb csomagokkal:

```
zypper update -t package
```

A következők együttesen azt jelentik, hogy csak a `factory` forrást használja a program és adjon részletes kimenetet:

```
zypper -v install --repo factory mplayer amarok
```

7.1.2 Szoftverek telepítése és eltávolítása a Zypper segítségével

A regisztrált forrásokból egy csomag telepítéséhez használja a következőt:

```
zypper install csomagnév
```

Helyi vagy távoli RPM közvetlenül is telepíthető:

```
zypper install http://www.example.com/csomagnév.rpm
```

Egy telepített csomag eltávolításához használja a következőt:

```
zypper remove csomagnév
```

FIGYELEM: Ne távolítsa el a rendszer működéséhez nélkülözhetetlen csomagokat

Ne távolítsa el az olyan csomagokat, mint például a `glibc`, `zypper`, `kernel` stb. Ezek a csomagok nélkülözhetetlenek a rendszer működéséhez, és ha hiányoznak, akkor a rendszer leállhat.

A zypper alapértelmezésben megerősítést kér egy kiválasztott csomag telepítése vagy eltávolítása előtt. Ez a tulajdonsága azonban kikapcsolható a `--non-interactive` beállítás megadásával. Ezt a beállítást az aktuális mód (telepítés, eltávolítás vagy frissítés) előtt kell megadni, például:

```
zypper --non-interactive install csomagnév
```

Ez a beállítás lehetőséget ad a zypper használatára parancsfájlokban vagy cron feladatokban.

Ha egy csomag megfelelő forráscsomagját szeretné telepíteni, használja a következőt:

```
zypper source-install csomagnév
```

Ezzel a paranccsal a megadott csomag szerkesztési függőségeit is telepíti. Ha ezt nem szeretné, akkor egészítse ki a `--no-build-deps` kapcsolóval az alábbiak szerint:

```
zypper source-install --no-build-deps csomagnév
```

Ez persze csak akkor működik, ha a forráscsomagokat tartalmazó forrást is felvette a forráslistába. A források hozzáadásával kapcsolatban lásd: 7.1.4. - Források kezelése (84. oldal).

7.1.3 Szoftvertelepítés a Zypper használatával

Kétféle módon frissíthetők szoftverek a zypper használatával. Ha be szeretné építeni az összes hivatalosan kiadott csomagot a rendszerbe, futtassa a következő parancsot:

```
zypper update
```

Ebben az esetben a rendszer relevanciaellenőrzést végez a forrásokban rendelkezésre álló összes javításon, és ha kell, telepíti azokat.

Ha egy forrásban vannak új csomagok, de nincsenek javítások, akkor a `zypper update` hatására semmi észrevehető nem történik. Az összes ilyen csomag telepítéséhez meg kell adni a `package` típus frissítéseinek telepítését:

```
zypper update -t package
```

Egyedi csomagok telepítéséhez használja a telepítési parancsot:

```
zypper install csomagnév
```

A rendelkezésre álló összes új csomag listája a következő paranccsal kérhető le:

```
zypper list-updates -t package
```

7.1.4 Források kezelése

A zypper telepítési és frissítési parancsainak alapjául a források zypper által ismert listája szolgál. A rendszer által ismert összes forrás listájának lekéréséhez használja a következő parancsot:

```
zypper repos
```

Az eredmény valami ilyesmi lesz:

```
#  | Álnév           | Név
   | Bekapcsolva | Frissítés
---+-------------+-----------------------------------------------+-----------+--------
1  | Compiz          | Compiz
   | Igen        | Igen
2  | GNOME:Community | GNOME:Community
   | Igen        | Igen
3  | KDE_Community   | KDE Community
   | Igen        | Igen
4  | openSUSE 11.1-0 | openSUSE 11.1-0
   | Nem         | Nem
5  | repo            | openSUSE BuildService - KDE:Frissítések
   | Igen        | Igen
6  | repo-debug      | openSUSE-11.1-Debug
   | Nem         | Igen
7  | repo-non-oss    | openSUSE-11.1-Non-Oss
   | Igen        | Igen
8  | repo-oss        | openSUSE-11.1-Oss
   | Igen        | Igen
9  | repo-source     | openSUSE-11.1-Source
   | Nem         | Igen
```

```
10 | repo-update      | openSUSE-11.1-Update
   | Igen         | Igen
11 | repo_1           | openSUSE BuildService - KDE:Közösség
   | Igen         | Igen
12 | repo_2           | openSUSE BuildService - OpenOffice.org
   | Igen         | Igen
13 | repo_3          | openSUSE BuildService - Virtualizáció (VirtualBox)
 | Igen         | Igen
14 | repo_5           | openSUSE BuildService - XFCE
   | Igen         | Igen
15 | repo_6           | openSUSE BuildService - Mozilla
   | Igen         | Igen
16 | repo_7           | VideoLan Repository
   | Igen         | Igen
```

Ha el szeretne távolítani egy forrást a listából, akkor használja a `zypper renamerepo` parancsot a törölni kívánt forrás álnevével. A `Main Repository (Non-OSS)` eltávolításához a példából használja a következő parancsot:

```
zypper renamerepo Main Repository (Non-OSS)
```

Forrás felvételéhez:

```
zypper addrepo URI Álnév
```

Az *`URI`* lehet internetes forrás (a rendelkezésre álló források listájának eléréséhez lásd: `http://hu.opensuse.org/Csomagok`) egy könyvtár, egy CD vagy egy DVD is. Az *`Alias`* (álnév) a forrás rövid és egyedi azonosítója. Szabadon megváltoztatható, kivéve, hogy egyedinek kell lennie. A zypper figyelmeztetést jelenít meg, ha olyan álnevet választ, amely már használatban van.

7.1.5 Lekérdezés

Többféle lekérdezési parancs is rendelkezésre áll, például `search`, `info` vagy `what-provides`.

A `search` csomagnevekkel működik és állapotinformációkat (`S`) jelenít meg a kimenet első oszlopában.

Az `info` egy csomagnévvel és egy argumentummal együtt részletes információkat jelenít meg a csomagról.

A `what-provides` *csomag* hasonlít az `rpm -q --whatprovides` *csomag* parancsra, de csak az rpm képes lekérdezni az RPM-adatbázisokat (az összes telepített csomag adatbázisát). A Zypper viszont információt ad bármely forrás szolgáltatóinak képességeiről, nemcsak a telepítettekéről.

Leginkább hibakeresési célt szolgál, hogy rendelkezésre állnak olyan kapcsolók, mint a `--plus-repo`, a `--disable-repositories` vagy a `--disable-system-resolvables`. Akkor használja ezeket, ha csak egyetlen forrásban szeretne keresni. A részletes használati információkért lásd a zypper kézikönyvoldalát (`man zypper`).

7.1.6 A Zypper parancsértelmező használata

Néha több külön zypper parancsot kell egymás után sorban futtatni. Ahhoz, hogy a zypper ne olvassa újra az összes adatbázist az egyes zypper-parancsoknál, a zypper parancsértelmező módban is futtatható:

```
zypper shell
```

Ha a parancsértelmező fut, akkor csak adja ki a zypper parancsokat a megfelelő paraméterekkel:

```
zypper> in zsh
...
zypper> exit
```

A zypper parancsértelmező általában gyorsabban használható, mivel a fontos adatokat memóriában tartja.

A Zypper támogatja a readline könyvtár használatát. Ez azt jelenti, hogy az összes parancssori szerkesztőfunkciót használhatja a Zypper parancsértelmezőben, ami a Bash parancsértelmezőben rendelkezésre áll. A Zypper a `~/.zypper_history` fájlban tartja a parancs előzménylistáját.

7.1.7 További információk

A parancssorból végzett frissítésről további információ a `zypper --help` paranccsal kérhető vagy a `zypper(8)` kézikönyv-oldalán található. Példák és részletes információ: http://hu.opensuse.org/Zypper.

7.2 RPM – a csomagkezelő

Az RPM (Red Hat Package Manager) szolgál a szoftvercsomagok kezelésére. A legfontosabb parancsai az `rpm` és az `rpmbuild`. A sokoldalú RPM-adatbázist lekérdezve részletes információt kaphatnak a felhasználók, a rendszergazdák és a csomagkészítők a telepített szoftverekről.

Alapvetően az `rpm`-nek ötféle működési módja van: szoftvercsomagok telepítése, eltávolítása vagy frissítése; az RPM-adatbázis újraépítése; RPM-bázisok vagy egyedi RPM-archívumok lekérdezése; a csomagok integritásának ellenőrzése; valamint a csomagok aláírása. Az `rpmbuild` parancs használható a tiszta forrásból származó csomagok előállítására.

A telepíthető RPM-archívumok egy speciális bináris formátumot használnak. Az archívumok a telepítendő programfájlokból, valamint bizonyos, az `rpm` által a telepítés során használt, vagy dokumentációs célokból az RPM-adatbázisban tárolt metaadatokból állnak. Az RPM-archívumok szokásos kiterjesztése `.rpm`.

TIPP: Szoftverfejlesztői csomagok

Egyes csomagok esetében a szoftverfejlesztéshez szükséges komponensek (könyvtárak, fejlécfájlok, beillesztendő fájlok stb.) külön csomagokba kerültek. Ezekre a fejlesztői csomagokra csak akkor van szükség, ha saját maga kívánja lefordítani a szoftvert, például a legfrissebb GNOME csomagokat. Az ilyen csomagokat a nevükben található `-devel` karaktersorozat jelzi, mint például az `alsa-devel`, `gimp-devel` vagy a `kdelibs3-devel`.

7.2.1 A csomagok hitelességének ellenőrzése

Az RPM-csomagok GnuPG-aláírással rendelkeznek. Az ujjlenyomatban használt kulcs:

```
1024D/9C800ACA 2000-10-19 SuSE Package Signing Key <build@suse.de>
Key fingerprint = 79C1 79B2 E1C8 20C1 890F  9994 A84E DAE8 9C80 0ACA
```

Az `rpm --checksig` *csomagnév*`-1.2.3.rpm` parancs használható egy RPM-csomag aláírásának ellenőrzésére; arra, hogy valóban a SUSE-tól vagy más, megbízható forrásból származik-e. Ez különösen ajánlott az internetről származó frissítőcsomagok esetében. A SUSE nyilvános csomagaláírási kulcsa általában a `/root/.gnupg/`

könyvtárban található. A kulcs ezenfelül megtalálható az `/usr/lib/rpm/gnupg/` könyvtárban is, hogy a normál felhasználók is ellenőrizhessék az RPM-csomagok aláírását.

7.2.2 Csomagok kezelése: Telepítés, frissítés és eltávolítás

Általában egy RPM-archívum telepítése igen egyszerű: `rpm -i` *`csomag_neve`*`.rpm`. Ez a parancs telepíti a csomagot, de csak akkor, ha a függőségek teljesülnek és nincs ütközés más csomagokkal. Egy hibaüzenet keretében az `rpm` kéri, hogy a telepíteni kívánt csomagok teljesítsék a függőségi követelményeket. A háttérben az RPM-adatbázis garantálja, hogy ne lépjen fel semmilyen ütközés – egy adott fájl csak egy csomaghoz tartozhat. Különféle paraméterekkel az `rpm` kényszeríthető ezen alapértelmezések figyelmen kívül hagyására, de ezt csak szakértőknek ajánljuk. Egyébként a rendszer integritását veszélyezteti, illetve előfordulhat, hogy nem lesz képes frissíteni a rendszert.

A `-U` vagy `--upgrade` és `-F` vagy `--freshen` paraméterek használhatók a csomagok frissítésére, például: `rpm -F` *`csomag_neve`*`.rpm`. Ez a parancs törli a régi változat fájljait és azonnal telepíti az új fájlokat. A kétféle lehetőség közötti különbség az, hogy a `-U` telepít olyan csomagokat, amelyek korábban nem léteztek a rendszerben, a `-F` csupán a meglévő csomagokat frissíti. Frissítéskor az `rpm` a konfigurációs fájlokat is frissíti óvatosan, az alábbi stratégia alkalmazásával:

- Ha a rendszergazda nem módosította a konfigurációs fájlt, akkor az `rpm` telepíti a megfelelő fájl új verzióját. A rendszergazda beavatkozására nincsen szükség.

- Ha a rendszergazda módosította a konfigurációs fájlt a frissítés előtt, akkor az `rpm` elmenti a fájlt `.rpmorig` vagy `.rpmsave` (tartalék fájl) kiterjesztéssel, és telepíti az új csomagban található változatot; de csak akkor, ha az eredetileg telepített fájl és az új változat eltérő. Ebben az esetben hasonlítsa össze az elmentett fájlt (`.rpmorig` vagy `.rpmsave`) az újonnan telepített fájllal és ha szükséges, végezze el az új fájlban a szükséges módosításokat. Ezután feltétlenül törölje az `.rpmorig` és `.rpmsave` fájlokat a jövőbeni frissítések problémáinak elkerülése érdekében.

- Az `.rpmnew` fájlok akkor jelennek meg, ha a konfigurációs fájl már létezik *és* ha a `noreplace` címke lett megadva a `.spec` fájlban.

Frissítés után az `.rpmsave` és `.rpmnew` fájlokat törölni kell az összehasonlítás után, hogy ne zavarják a későbbi frissítéseket. Az `.rpmorig` kiterjesztést akkor használja a program, ha a fájl korábban nem volt ismert az RPM-adatbázisban.

Ellenkező esetben az `.rpmsave` név kerül alkalmazásra. Más szavakkal, az `.rpmorig` egy idegen formátumról RPM-re frissítés eredménye. Az `.rpmsave` egy régebbi RPM-ről egy újabb RPM-re frissítés eredménye. Az `.rpmnew` fájlokból nem derül ki, hogy a rendszergazda módosította-e a konfigurációs fájlt. Az ilyen fájlok listája a `/var/adm/rpmconfigcheck` helyen található. Egyes konfigurációs fájlok (például az `/etc/httpd/httpd.conf`) nem íródnak felül a folyamatos működés fenntartása érdekében.

A `-U` kapcsoló *nem* egyenértékű a `-e` paraméterrel történő eltávolítással és a `-i` paraméterrel történő telepítéssel. Ahol csak lehet, inkább a `-U` paramétert használja.

Egy csomag eltávolításához írja be, hogy `rpm -e` *`csomag_neve`*. Az `rpm` csak akkor törli a csomagot, ha nincsenek feloldatlan függőségek. Elvileg lehetetlen például törölni a Tcl/Tk-t addig, amíg egy másik alkalmazás használja. Még ebben az esetben is, az RPM az adatbázistól kér segítséget. Ha az ilyen törlés – bármilyen okból és akár furcsa körülmények között is – lehetlennek bizonyul, még akkor is, ha *semmilyen* további függőség nincs, akkor célszerű lehet újraépíteni az RPM-adatbázist a `--rebuilddb` paraméter használatával..

7.2.3 Az RPM és a javítások

A rendszer működési biztonságának garantálásához időről időre frissítőcsomagokat kell telepíteni a rendszeren. Korábban egy csomag egy hibáját csak a teljes csomag cseréjével lehett megoldani. A kis fájlokban hibákat tartalmazó nagy csomagok javításai feleslegesen nagy adatmennyiséget eredményeztek. A SUSE RPM azonban lehetővé teszi az egyes csomagok foltozását.

A legfontosabb szempontokat a pine példáján keresztül mutatjuk be:

A javító RPM megfelelő-e a rendszerhez?
: Ennek ellenőrzéséhez először le kell kérdezni a csomag telepített verzióját. A pine esetében erre a következő parancs szolgál:

```
rpm -q pine
pine-4.44-188
```

Ezután ellenőrizni kell, hogy a javító RPM megfelelő-e a pine adott verziójához:

```
rpm -qp --basedon pine-4.44-224.i586.patch.rpm
pine = 4.44-188
pine = 4.44-195
pine = 4.44-207
```

Ez a javítás a pine háromféle verziójához jó. Mivel a telepített verzió is megtalálható a listában, a javítás telepíthető.

Milyen fájlokat cserél le a javítás?

A javítás által érintett fájlok egyszerűen megtekinthetők a javító RPM-ben. Az `rpm -P` paraméterével speciális javítási funkciók választhatók ki. A fájlok az alábbi paranccsal listázhatók:

```
rpm -qpPl pine-4.44-224.i586.patch.rpm
/etc/pine.conf
/etc/pine.conf.fixed
/usr/bin/pine
```

vagy ha a javítás már telepítve van, akkor az alábbival:

```
rpm -qPl pine
/etc/pine.conf
/etc/pine.conf.fixed
/usr/bin/pine
```

Hogyan történik a javító RPM telepítése a rendszerben?

A javító RPM-ek ugyanúgy használhatók, mint a szokásos RPM-ek. Az egyetlen különbség, hogy a javítandó RPM-nek már telepítve kell lennie.

Milyen javítások vannak telepítve a rendszeren és mely csomagokhoz?

A rendszeren telepített összes javítást az `rpm -qPa` parancs listázza ki. Ha csak egyetlen javítás van telepítve egy új rendszeren (mint a fenti példában), akkor a lista így néz ki:

```
rpm -qPa
pine-4.44-224
```

Ha később kíváncsi arra, hogy mely csomagverziók mikor lettek telepítve, ez is lekérdezhető az RPM-adatbázisból. A `pine` esetében ezt az információt a következő paranccsal lehet kiíratni:

```
rpm -q --basedon pine
pine = 4.44-188
```

További információk, így például az RPM javítási funkciójáról az `rpm` és az `rpmbuild` parancsok kézikönyvoldalain olvashatók.

7.2.4 Delta RPM-csomagok

A delta RPM-csomagok egy RPM-csomag régebbi és új változata közötti különbséget tartalmazzák. Egy delta RPM alkalmazása egy régi RPM-en egy teljesen új RPM-et fog eredményezni. Ha nincs meg a régi RPM-példány, a delta RPM a telepített RPM-mel is képes együttműködni. A deltarpm csomagok még a javító RPM-eknél is kisebbek. Ez hasznos, ha a frissítőcsomagokat az interneten keresztül kell elküldeni. A hátránya, hogy a delta RPM-ekkel végzett frissítési műveletek lényegesen jobban megterhelik a CPU-t, mint a sima és javító RPM-ek használata.

A `prepdeltarpm`, `writedeltarpm` és `applydeltarpm` bináris fájlok a delta RPM készlet (`deltarpm` csomag) részei. Ezek segítenek a delta RPM-csomagok elkészítésében és alkalmazásában. Az alábbi parancsokkal készíthető egy `new.delta.rpm`. A következő parancs feltételezi, hogy az `old.rpm` és `new.rpm` rendelkezésre áll:

```
prepdeltarpm -s seq -i info old.rpm > old.cpio
prepdeltarpm -f new.rpm > new.cpio
xdelta delta -0 old.cpio new.cpio delta
writedeltarpm new.rpm delta info new.delta.rpm
```

Végül távolítsa el az `old.cpio`, `new.cpio` és `delta` ideiglenes munkafájlokat.

Az `applydeltarpm` használatával előállítható az új RPM, akár a fájlrendszerből is, ha a régi csomag már telepítve van:

```
applydeltarpm new.delta.rpm new.rpm
```

Vagy pedig a `-r` paraméter használatával származtatható a régi RPM-ből, a fájlrendszer elérése nélkül:

```
applydeltarpm -r old.rpm new.delta.rpm new.rpm
```

A műszaki részletek az `/usr/share/doc/csomagok/deltarpm/README` fájlban olvashatók.

7.2.5 RPM-lekérdezések

A `-q` paraméter megadása esetén az `rpm` rpm lekérdezéseket indít. Megvizsgálható egy adott RPM-archívum (a `-p` paraméterrel) és lekérdezhető a telepített csomagok RPM-adatbázisa. Többféle kapcsoló is használható a kívánt adatok típusának megadására. Lásd: 7.1 táblázat - A legfontosabb RPM-lekérdezési paraméterek (92. oldal).

7.1. táblázat *A legfontosabb RPM-lekérdezési paraméterek*

`-i`	Csomaginformáció
`-l`	Fájllista
`-f FÁJL`	A *FÁJL* fájlt tartalmazó csomag lekérdezése (a *FÁJL* paramétert teljes elérési úttal kell megadni)
`-s`	Fájllista állapotinformációval (magával vonja a `-l` alkalmazását)
`-d`	Csak a dokumentációs fájlok listázása (magával vonja a `-l` alkalmazását)
`-c`	Csak a konfigurációs fájlok listázása (magával vonja a `-l` alkalmazását)
`--dump`	Részletes fájllista (a `-l`, `-c` és `-d` paraméterekkel együttes használathoz)
`--provides`	Azon csomagok funkcióinak listázása, amelyeket egy másik csomag kérhet a `--requires` paraméterrel
`--requires`, `-R`	A csomag által igényelt képességek
`--scripts`	Telepítési parancsfájlok (telepítés előtti, utáni és eltávolító)

Például az `rpm -q -i wget` parancs hatására a 7.1. példa - rpm -q -i wget (93. oldal) által mutatott eredményt kapjuk.

7.1 példa *rpm -q -i wget*

```
Name        : wget                          Relocations: (not relocatable)
Version     : 1.11.4                             Vendor: openSUSE
Release     : 1.22                        Build Date: 2008. dec.  3., szerda,
 07.45.24 CET
Install Date: 2008. dec.  9., kedd, 23.04.48 CET      Build Host: build15
Group       : Productivity/Networking/Web/Utilities   Source RPM:
wget-1.11.4-1.22.src.rpm
Size        : 1530350                          License: GPL v3 or later
Signature   : RSA/8, 2008. dec.  3., szerda, 07.45.34 CET, Key ID
b88b2fd43dbdc284
Packager    : http://bugs.opensuse.org
URL         : http://www.gnu.org/software/wget/
Summary     : A Tool for Mirroring FTP and HTTP Servers
Description :
Wget enables you to retrieve WWW documents or FTP files from a server.
This can be done in script files or via the command line.
[...]
```

A `-f` csak akkor működik, ha a teljes fájlnevet adja meg, elérési úttal együtt. Annyi fáljnevet adhat meg, amenyi csak jólesik. Például az alábbi parancs:

```
rpm -q -f /bin/rpm /usr/bin/wget
```

eredménye a következő:

```
rpm-4.1.1-191
wget-1.9.1-50
```

Ha csak a fájlnév egy része ismert, használjon egy parancsfájlt (7.2. példa - Parancsfájl csomagok kereséséhez (93. oldal)). A részleges fájlnevet adja át paraméterként a parancsfájlnak.

7.2 példa *Parancsfájl csomagok kereséséhez*

```
#! /bin/sh
for i in $(rpm -q -a -l | grep  $1); do
    echo "\"$i\" is in package:"
    rpm -q -f $i
    echo ""
done
```

Az `rpm -q --changelog rpm` parancs egy csomag részletes adatait (frissítések, konfiguráció, módosítások stb.) írja ki. Az előbbi példa az `rpm` csomagról ír ki információt.

A telepített RPM-adatbázis segítségével ellenőrzések is végezhetők. Ezek a `-V`, `-y` vagy `--verify` paraméterrel indíthatók. E paraméter használatakor az `rpm` megjele-

níti egy csomagnak a telepítés óta módosult fájljait. Az `rpm` nyolc karakterszimbólum segítségével jelzi az alábbi módosításokat:

7.2. táblázat *RPM ellenőrzési paraméterek*

`5`	MD5-ellenőrzőösszeg
`S`	Fájlméret
`L`	Szimbolikus lánc
`T`	Módosítás ideje
`D`	Fő- és aleszközszámok
`U`	Tulajdonos
`G`	Csoport
`M`	Mód (jogosultságok és fájltípus)

Konfigurációs fájlok esetében a `c` betű íródik ki. Például az `/etc/wgetrc` (`wget`) módosításainak kiírása:

```
rpm -V wget
S.5....T c /etc/wgetrc
```

Az RPM-adatbázis fájljai a `/var/lib/rpm` könyvtárban találhatók. Ha az `/usr` partíció helyfoglalása 1 GB, akkor ez az adatbázis közel 30 MB-ot foglal, különösen teljes frissítés után. Ha az adatbázis sokkal nagyobb a vártnál, akkor célszerű újraépíteni az adatbázist a `--rebuilddb` paraméter használatával. Előtte azonban mentse el a régi adatbázist. A `cron` és a `cron.daily` parancsfájl napi másolatokat készít az adatbázisról (gzip-pel tömörítve) és a `/var/adm/backup/rpmdb` könyvtárba menti őket. A másolatok számát az `/etc/sysconfig/backup` fájl `MAX_RPMDB_BACKUPS` változója szabályozza (alapértelmezés: `5`). Egy mentés mérete mintegy 1 MB az `/usr` minden 1 GB-jára.

7.2.6 Forráscsomagok telepítése és lefordítása

A forrásfájlokat tartalmazó csomagok `.src.rpm` (source RPM, forrás RPM) kiterjesztéssel rendelkeznek.

TIPP

A forráscsomagok átmásolhatók a telepítési adathordozóról a merevlemezre és a YaST segítségével csomagolhatók ki. A csomagkezelő azonban nem jelzi, hogy telepítve vannak (`[i]`). Ez azért van, mert a forráscsomagok nem kerülnek be az RPM-adatbázisba. Csak az operációs rendszer *telepített* szoftverei vannak felsorolva az RPM-adatbázisban. Egy forráscsomag „telepítésekor" csak a forráskód kerül be a rendszerbe.

Az alábbi könyvtáraknak az `rpm` és `rpmbuild` rendelkezésére kell állniuk az `/usr/src/packages` könyvtárban (hacsak nincsenek megadva egyedi beállítások például az `/etc/rpmrc` fájlban):

`SOURCES`
: az eredeti forrásokhoz (`.tar.bz2` vagy `.tar.gz` fájlok stb.) és a disztribúció-specifikus módosításokhoz (általában `.diff` vagy `.patch` fájlok)

`SPECS`
: a *.spec* fájlokhoz. Ezek az *összeállítási* (build) folyamatot vezérlő meta Makefile fájlokhoz hasonlók

`BUILD`
: az összes forrás kicsomagolva, foltozva és lefordítva található meg ebben a könyvtárban

`RPMS`
: ahol a kész bináris csomagok találhatók

`SRPMS`
: itt találhatók a forrás RPM-ek

Egy forráscsomag YaST-tal történő telepítése közben az összes szükséges összetevő telepítődik az `/usr/src/packages`: könyvtárban: a forrás és a módosítások a `SOURCES`, a vonatkozó `.spec` fájl pedig a `SPECS` könyvtárban.

FIGYELEM

Ne kísérletezzen a rendszerkomponensekkel (`glibc`, `rpm`, `sysvinit` stb.), mivel ez veszélyezteti a rendszer működőképességét.

Az alábbi példa a `wget.src.rpm` csomagot mutatja be. Telepítve a csomagot a YaST-tal, az alábbi listához hasonló fájlok kell, hogy megjelenjenek:

```
/usr/src/packages/SOURCES/nops_doc.diff
/usr/src/packages/SOURCES/toplev_destdir.diff
/usr/src/packages/SOURCES/wget-1.9.1+ipvmisc.patch
/usr/src/packages/SOURCES/wget-1.9.1-brokentime.patch
/usr/src/packages/SOURCES/wget-1.9.1-passive_ftp.diff
/usr/src/packages/SOURCES/wget-LFS-20040909.tar.bz2
/usr/src/packages/SOURCES/wget-wrong_charset.patch
/usr/src/packages/SPECS/wget.spec
```

Az `rpmbuild -b` *X* `/usr/src/packages/SPECS/wget.spec` parancs indítja el a fordítást. Az *X* helyére az összeállítási folyamat különböző szakaszai kerülnek (a részletek a `--help` paraméterrel elindított program kimenetén, vagy az RPM-dokumentációban olvashatók). Alább csak egy egészen rövid magyarázat következik:

`-bp`
: A források előkészítése az `/usr/src/packages/BUILD` könyvtárban: kicsomagolás és foltozás.

`-bc`
: Ugyanaz, mint a `-bp`, de fordítással.

`-bi`
: Ugyanaz, mint a `-bp`, de az összeállított szoftver telepítésével. Vigyázat: ha a csomag nem támogatja a BuildRoot funkciót, akkor előfordulhat, hogy felülíródnak egyes konfigurációs fájlok.

`-bb`
: Ugyanaz, mint a `-bi`, de a bináris csomag létrehozásával. Ha a fordítás sikeres, a bináris fájl az `/usr/src/packages/RPMS` könyvtárban kell, hogy legyen.

`-ba`
: Ugyanaz, mint a `-bb`, de a forrás RPM létrehozásával. Ha a fordítás sikeres, a bináris fájl az `/usr/src/packages/SRPMS` könyvtárban kell, hogy legyen.

`--short-circuit`
: Egyes lépések kihagyása.

A létrehozott bináris RPM most már telepíthető az `rpm -i`, vagy még inkább az `rpm -U` paranccsal.. Az `rpm`-mel telepítve a csomag megjelenik az RPM-adatbázisban.

7.2.7 RPM-csomagok lefordítása a build segítségével

Sok csomag esetében az a veszély, hogy nemkívánatos csomagok is bekerülnek a futó rendszerbe az összeállítási folyamat közben. Ennek megakadályozására használható a `build` parancs, amelyik létrehoz egy jóldefiniált környezetet, amelyben a csomag összeállítása zajlik. E chroot-környezet létrehozásához a `build` parancsfájlnak meg kell adni a teljes csomagfát. Ez a fa biztosítható a merevlemezről, NFS-en keresztül, vagy DVD-ről. A megfelelő helyet a `build --rpms` *`könyvtár`* parancs adja meg. Szemben az `rpm` paranccsal, a `build` parancs a forráskönyvtár SPEC fájlját keresi meg. A wget vadonatúj (a fenti példához hasonló) összeállításához, amennyiben a DVD a rendszerbe a `/media/dvd` ponton van felcsatolva, adja ki a következő parancsot, mint `root` felhasználó:

```
cd /usr/src/packages/SOURCES/
mv ../SPECS/wget.spec .
build --rpms /media/dvd/suse/ wget.spec
```

Létrejön egy minimális környezet a `/var/tmp/build-root` könyvtár alatt. A csomag ebben a környezetben készül el. Befejezés után az eredményül kapott csomagok a `/var/tmp/build-root/usr/src/packages/RPMS` könyvtárban találhatók.

A `build` parancsfájl többféle kiegészítő paraméter használatát is lehetővé teszi. A parancsfájl például előnyben részesíthet saját RPM-eket, kihagyhatja az összeállítási környezet inicializálását, vagy a fenti fázisok közül egyre korlátozhatja az `rpm` parancs használatát. További információ a `build --help` paranccsal, vagy a `build` kézikönyvoldalán érhető el.

7.2.8 Eszközök az RPM-archívumokhoz és az RPM-adatbázishoz

A Midnight Commander (`mc`) képes megjeleníteni az RPM-archívumok tartalmát és kimásolni egy részüket. Az archívumokat virtuális fájlrendszerekként jeleníti meg, amelyekben a Midnight Commander szinte minden szokásos parancsa használható. A `HEADER` például az F3 billentyűvel tekinthető meg. Az archívumstruktúra bejárható a kurzorbillentyűk és az Enter segítségével. Az archívum egyes elemei kimásolhatók az F5 billentyűvel.

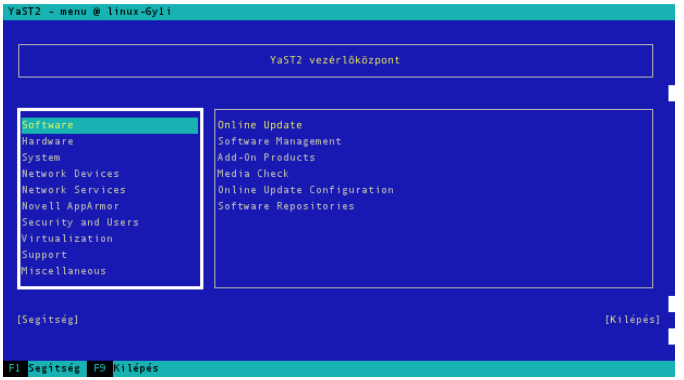
A KDE a kpackage eszközt biztosítja az `rpm` grafikus előtétprogramjaként. YaST-modulként egy teljes funkciókörű csomagkezelő is elérhető (lásd: 3. fejezet - *Szoftver telepítése és eltávolítása* (61. oldal)).

III. rész - Adminisztráció

8 YaST szöveges módban

Ez a rész főként a rendszeradminisztrátorok és -szakértők számára ajánlott, akik nem futtatnak X kiszolgálót a rendszeren, ezért a szöveges alapú telepítési eszközt kell használniuk. Ebben a fejezetben a YaST szöveges módban történő elindításával és működésével kapcsolatos alapvető tudnivalókat írjuk le.

8.1. ábra *A YaST főablaka szöveges módban*



A YaST szöveges módban indításakor először a YaST vezérlőközpont jelenik meg (lásd: 8.1. ábra). A főablak három részből áll. A vastag fehér szegéllyel körülvett bal oldali keret a kategóriákat jellemzi, amelyekhez a különböző modulok tartoznak. Az aktív kategóriát színes háttér jelzi. A vékony fehér szegéllyel körülvett jobb oldali keret az aktív kategóriában rendelkezésre álló modulokat jeleníti meg. Az alsó keret a *Segítség* és a *Kilépés* gombot tartalmazza.

A YaST vezérlőközpont elindításakor a *Szoftver* kategória automatikusan kiválasztásra kerül. A ↓ és ↑ billentyűkkel válthat kategóriát. A kiválasztott kategória egy moduljának elindításához nyomja meg a Tab billentyűt. A modulkiválasztás szegélye vastagra változik. A ↓ és ↑ billentyűkkel válassza ki a kívánt modult. A rendelkezésre álló modulok listájának végiggörgetéséhez tartsa lenyomva a nyíl billentyűket. Egy modul kiválasztásakor a modul címe színes háttéren jelenik meg.

A kívánt modul elindításához nyomja meg az Enter billentyűt. A modulban lévő különböző gombok vagy választómezők különböző színű betűket tartalmaznak (alapértelmezés szerint sárgát). Az Alt + sárga_betű billentyűkombináció segítségével a Tab billentyűvel navigálás helyett közvetlenül is kiválaszthat (megnyomhat) egy gombot. A YaST vezérlőközpontból az Alt + Q billentyűkombinációval, illetve a kategóriáttekintés *Kilépés* menüpontjának kiválasztásával, majd az Enter megnyomásával léphet ki.

8.1 Navigáció a modulokban

A YaST-modul vezérlőelemeinek alábbi leírásában feltételezzük, hogy a funkcióbillentyűk és az Alt billentyűkombinációk működnek, és nincsenek hozzájuk rendelve más globális funkciók. A lehetséges kivételekkel kapcsolatos információt az alábbi rész tartalmaz: 8.2. - A billentyűkombinációk korlátozása (104. oldal).

Navigáció a gombok és választólisták között
: Az egyes gombok, illetve választólistákat tartalmazó keretek között a Tab billentyűvel lépkedhet. A fordított irányban mozgáshoz használja az Alt + Tab vagy Shift + Tab kombinációkat.

Navigáció a választólistákban
: A nyíl billentyűk (↑ és ↓) segítségével lehet navigálni a választólistát tartalmazó aktív keret egyes elemei között. Ha a kereten belüli egyes bejegyzések meghaladják a keret szélességét, akkor a Shift + → és Shift + ← billentyűkombinációkkal lehet vízszintesen jobbra-balra görgetni a keret tartalmát. A Ctrl + E és Ctrl + A billentyűkombináció is használható. Ez a kombináció akkor is használható, ha a → vagy ← megnyomása az aktív keret vagy az aktuális választólista megváltozását eredményezné, mint a vezérlőközpontban.

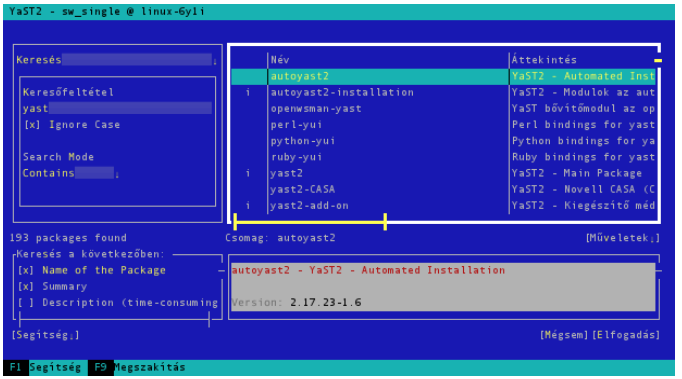
Gombok, választógombok és jelölőnégyzetek
: Az üres szögletes zárójelek (jelölőnégyzetek) vagy üres kerek zárójelek (választógombok) kiválasztásához/megjelöléséhez nyomja meg a szóköz vagy Enter billentyűt. A választógombok és jelölőnégyzetek az Alt + sárga_betű billentyűkom-

binációval közvetlenül is kiválaszthatók. Ebben az esetben nem kell külön az Enter billentyűvel megerősíteni a kijelölést. Ha a Tab billentyű segítségével választ ki egy elemet, akkor a kiválasztott tevékenység végrehajtásához vagy a megfelelő menüpont aktiválásához nyomja meg az Enter billentyűt.

Funkcióbillentyűk
: Az F billentyűk (F1 – F12) lehetővé teszik a különböző gombok gyors elérését. A YaST képernyő alján a rendelkezésre álló funkcióbillentyű-parancsok láthatók. Az aktív YaST-modultól függ, hogy melyik funkcióbillentyű valójában melyik gombra van leképezve, mivel a különböző modulok különböző gombokat kínálnak (Részletek, Információ, Hozzáadás, Törlés stb.). Az F10 billentyűvel az *Elfogadás*, *OK*, *Tovább* és *Befejezés* gombok nyomhatók meg. A YaST súgójának előhívásához használja az F1 billentyűt.

A navigációs fa használata ncurses módban
: Egyes YaST-modulok egy navigációs fát használnak az ablak bal szélén a beállítási párbeszédablakok kiválasztásához. Ncurses módban az Enter billentyűt le kell nyomni a navigációs fában a kijelölt párbeszédablak megjelenítéséhez. Ez szándékosan van így, hogy kevesebb idő menjen el a képernyő újrarajzolására a navigációs fában mozgás közben.

8.2. ábra *A szoftvertelepítési modul*



8.2 A billentyűkombinációk korlátozása

Ha az ablakkezelő globális Alt-kombinációkat használ, akkor elképzelhető, hogy a YaST Alt-kombinációi nem működnek. Az Alt és Shift billentyűket a terminál beállításai is lefoglalhatják.

Alt helyettesítése Esc billentyűvel
: Az Alt billentyűparancsok az Alt helyett az Esc billentyűvel is végrehajthatók. Az Alt + H billentyűkombináció például helyettesíthető az Esc – H billentyűkombinációval. (Először nyomja le az Esc *gombot, majd utána* nyomja meg a H-t.)

Navigáció előre és hátra a Ctrl + F és Ctrl + B billentyűkombinációkkal
: Ha az Alt és Shift kombinációkat az ablakkezelő vagy a terminál lefoglalja, akkor használhatja a Ctrl + F (előre) és Ctrl + B (vissza) billentyűkombinációkat.

A funkcióbillentyűk korlátozása
: Az F billentyűket sok program a saját funkcióihoz használja. Lehet, hogy a terminál lefoglal bizonyos funkcióbillentyűket, ezért elképzelhető, hogy nem használhatók YaST alatt. Egy sima szöveges konzolon azonban az Alt billentyűkombinációknak és a funkcióbillentyűknek mindig teljesen elérhetőnek kell lenniük.

8.3 YaST parancssori paraméterek

A szöveges módú felület mellett a YaST egy tisztán parancssori felületet is biztosít. A YaST parancssori paramétereinek listája a következő paranccsal íratható ki:

```
yast -h
```

8.3.1 Az egyes modulok indítása

Az idő megtakarítása érdekében az egyes YaST-modulok közvetlenül is elindíthatók. Egy modul indításához írja be, hogy:

```
yast <csomag_neve>
```

Az összes modul neve a `yast -l` vagy `yast --list` paranccsal íratható ki. A hálózati modul például a `yast lan` paranccsal indítható.

8.3.2 Csomagok telepítése parancssorból

Ha ismeri egy csomag nevét, és a csomagot bármelyik aktív telepítési forrás biztosítja, akkor a `-i` parancssori paraméterrel telepítheti a csomagot:

```
yast -i <csomag_neve>
```

vagy

```
yast --install <csomag_neve>
```

A *csomag_neve* lehet egy rövid csomagnév, mint például a `gvim`, amely ez esetben függőségellenőrzés után lesz telepítve, vagy lehet egy rpm csomag teljes elérési útja, amely esetben függőségellenőrzés nélkül fut le a telepítés.

Ha olyan parancssori szoftverkezelési segédprogramot szeretne használni, amely a YaST-nál bőségesebb funkcionalitást kínál, fontolja meg a zypper használatát. Ez az új segédprogram ugyanazt a szoftverkezelési függvénytárat használja, ami a YaST csomagkezelő alapja is. A zypper használatának legfontosabb részeit a 7.1. - A Zypper használata (81. oldal) szakasz írja le.

8.3.3 A YaST-modulok parancssori paraméterei

Ahhoz, hogy a YaST funkcióit parancsfájlokban is lehessen használni, a YaST támogatja az egyes modulok használatát is a parancssorból. Nem minden modulnak van parancssori támogatása. Egy modul rendelkezésre álló paramétereinek megjelenítéséhez írja be, hogy:

```
yast <csomag_neve> help
```

Ha egy modul nem biztosít parancssori támogatást, akkor a modul elindul szöveges módban és az alábbi üzenet jelenik meg:

```
This YaST module does not support the command line interface.
```

9 Nyomtatók üzemeltetése

Az openSUSE sokféle nyomtató használatát támogatja; többek hálózati nyomtatókét is. A nyomtatók a YaST használatával és kézzel is beállíthatók. A beállítással kapcsolatos utasítások: 2.5. - Setting Up a Printer (2. fejezet - *Setting Up Hardware Components with YaST*, ↑*Start-Up*). A nyomtatási feladatok elindításához és felügyeletéhez grafikus és parancssoros segédprogramok egyaránt rendelkezésre állnak. Ha a nyomtató nem a várakozásoknak megfelelően működik, tájékozódjon a következő részben: 9.8. - Hibaelhárítás (117. oldal).

Az openSUSE szabványos nyomtatási rendszere a CUPS. A CUPS igen felhasználóorientált. Sok esetben kompatibilis az LPRng rendszerrel, vagy minimális erőfeszítéssel adaptálható. Az LPRng-t az openSUSE csak a kompatibilitás érdekében tartalmazza.

A nyomtatók csoportosíthatók csatoló szerint (például USB vagy hálózati), illetve a nyomtató által használt nyelv szerint. Egy nyomtató vásárlásakor győződjön meg róla, hogy a nyomtató a hardver által támogatott csatolóval (pl. USB vagy párhuzamos port) rendelkezik és megfelelő nyomtatónyelvet használ. A nyomtatók a nyomtatónyelv szerint az alábbi három osztályba sorolhatók:

PostScript-nyomtatók
: A PostScript az a nyomtatónyelv, amelyen Unix/Linux alatt a legtöbb nyomtatási feladat elkészül és amelyet a belső nyomtatási rendszer feldolgoz. Ez a nyelv meglehetősen régi, de nagyon hatékony. Ha a PostScript-dokumentumokat a nyomtató képes közvetlenül feldolgozni, és nem kell a nyomtatási rendszer egyéb szakaszaiban átalakítani, akkor csökken a potenciális hibaforrások száma. Mivel a PostScript-nyomtatókat komolyabb licencköltségek terhelik, ezek a nyomtatók általában drágábbak, mint a PostScript-értelmező nélküliek.

Szabványos nyomtatók (PCL, ESC/P és hasonló nyelvekkel)
: Bár ezek a nyomtatónyelvek igen régiek, továbbra is bővítik őket, hogy lefedjék a nyomtatók új funkcióit. Ismert nyomtatónyelvek esetében a nyomtatási rendszer a Ghostscript segítségével képes átalakítani a PostScript-feladatokat a megfelelő nyomtatónyelvre. Ezt a feldolgozási fázist nevezzük értelmezésnek. A legismertebb ilyen nyelv a PCL, amelyeket elsősorban HP-nyomtatók és klónjaik használnak, illetve az ESC/P, amelyet pedig az Epson-nyomtatók. Ezeket a nyomtatónyelveket általában támogatja a Linux és elfogadható minőségű nyomatot eredményeznek. A nagyon új és speciális nyomtatóknak lehetnek olyan funkciói, amelyekkel a Linux nem tud mit kezdeni, ugyanis a nyílt forráskódú fejlesztők még lehet, hogy dolgoznak e funkciók elérésén. Kivéve a HP által készített HPLIP-et, jelenleg egy nyomtatógyártó sem készít linuxos illesztőprogramokat és teszi azt elérhetővé a Linux-disztribútorok számára nyílt forráskódú licenc keretében. A legtöbb ilyen nyomtató a közepes árkategóriába esik.

Egyedi nyomtatók (rendszerint GDI-nyomtatók)
: Ezek a nyomtatók nem támogatják a szokásos nyomtatónyelvek egyikét sem. A saját, nem dokumentált nyomtatónyelvüket használják, amely a modell egy új kiadásának megjelenésekor változhat. Ezekhez a nyomtatókhoz általában csak windowsos illesztőprogramok állnak rendelkezésre. További információkért lásd: 9.8.1. - Szabványos nyomtatónyelveket nem támogató nyomtatók (118. oldal).

Mielőtt új nyomtatót vásárolna, forduljon az alábbi forrásokhoz és ellenőrizze, hogy milyen mértékben támogatják a megvenni szándékozott nyomtatót:

`http://www.linuxfoundation.org/en/OpenPrinting/`
: Az OpenPrinting.org nyomtatóadatbázisa.

`http://www.cs.wisc.edu/~ghost/`
: A Ghostscript weboldala.

`/usr/share/doc/packages/ghostscript-library/catalog.devices`
: A mellékelt illesztőprogramok

Az online adatbázisok mindig a legfrissebb linuxos támogatási állapotot mutatják. Egy Linux-disztribúció azonban csak a gyártáskor elérhető illesztőprogramokat tudja tartalmazni. Ennek megfelelően, előfordulhat, hogy egy pillanatnyilag „teljesen támogatott” nyomtató az openSUSE legutolsó kiadásának megjelenésekor még nem volt ebben az állapotban. Más szavakkal, az adatbázisok nem hajszálpontosan jelzik az állapotot, de jó közelítést adnak.

9.1 A nyomtatási rendszer munkafolyamata

A felhasználó létrehoz egy nyomtatási feladatot. A nyomtatási feladat egyrészt a kinyomtatandó, másrészt a feladatkezelőnek szánt adatokból (például a nyomtató vagy a nyomtatási sor neve) áll. Harmadrészt, bár ez nem kötelező, a szűrőnek szánt adatokat is tartalmazhat, például nyomtatóspecifikus paramétereket.

Minden nyomtatóhoz létezik legalább egy nyomtatási sor. A nyomtatásisor-kezelő a sorban tartja a nyomtatási feladatokat egészen addig, amíg a kívánt nyomtató készen nem áll az adatok fogadására. Ha a nyomtató készen áll, akkor a nyomtatásisor-kezelő elküldi az adatokat a szűrőbe, a végeredményt pedig a nyomtatóra.

A szűrő a nyomtatást végző alkalmazás által előállított adatokat (általában PostScript vagy PDF, de lehet ASCII, JPEG stb.) alakítja át nyomtatóspecifikus adatokká (PostScript, PCL, ESC/P stb). A nyomtató funkcióit a PPD-fájlok írják le. A PPD-fájlok nyomtatóspecifikus beállításokat tartalmaznak a megfelelő paraméterekkel, amelyekkel ezek a funkciók bekapcsolhatók a nyomtatón. A szűrőrendszer gondoskodik arról, hogy a felhasználó által kiválasztott paraméterek be legyenek kapcsolva.

PostScript-nyomtató használata esetén a szűrőrendszer nyomtatóspecifikus PostScript-állománnyá alakítja az adatokat. Ehhez nincs szükség nyomtatóillesztőre. Nem PostScript-nyomtató használata esetén a szűrőrendszer nyomtatóspecifikus adatokká alakítja az adatokat. Ehhez viszont szükség van a nyomtatónak megfelelő illesztőprogramra. A háttérrendszer a szűrőtől megkapott adatokat továbbadja a nyomtatónak.

9.2 Módszerek és protokollok nyomtatók csatlakoztatására

A nyomtatók többféleképpen is csatlakoztathatók a rendszerhez. A CUPS nyomtatási rendszer beállítása nem tesz különbséget a helyi és a hálózaton keresztül csatlakozó nyomtatók között. Linux alatt a helyi nyomtatókat a nyomtatógyártó által biztosított kézikönyvben leírtak szerint kell csatlakoztatni. A CUPS soros, USB-, párhuzamos és SCSI-kapcsolatokat támogat. A nyomtatók csatlakoztatásáról további információ a támogatási adatbázis (`http://en.opensuse.org/SDB:CUPS_in_a_Nutshell`) *CUPS dióhéjban* című cikkében olvasható.

FIGYELEM: Vezetékes kapcsolatok megváltoztatása egy futó rendszerben

A nyomtatónak a számítógéphez csatlakoztatása közben ne feledje, hogy csak az USB-eszközöket lehet működés közben csatlakoztatni és eltávolítani. A rendszer ill. a nyomtató károsodásának megelőzése érdekében nem USB-csatlakozás esetén a rendszert le kell állítani.

9.3 A szoftver telepítése

A PPD (PostScript printer description, PostScript-nyomtatóleírás) az a számítógépes nyelv, amelyen leírhatók a nyomtató tulajdonságai, például a felbontása, valamint az egyéb jellemzői, például hogy van-e benne duplex egység. Ezekre a leírásokra a CUPS többféle beállításánál is szükség van. PPD-fájl nélkül a nyomtatási adatok „nyers” formátumban kerülnek a nyomtatóra továbbításra, ami általában nem kívánatos. Az openSUSE telepítése során számos PPD-fájl telepítődik.

PostScript-nyomtató beállításának a legjobb módja a megfelelő PPD-fájl beszerzése. Számos PPD-fájl megtalálható a `manufacturer-PPDs` nevű csomagban, amely a normál telepítés részeként automatikusan telepítődik. Lásd 9.7.2. - Különféle csomagok PPD-fájljai (115. oldal) és 9.8.2. - Nincs megfelelő PPD-fájl egy PostScript-nyomtatóhoz (118. oldal).

Az új PPD-fájlok az `/usr/share/cups/model/` könyvtárba menthetők, vagy felvehetők a YaST segítségével is a nyomtatási rendszerbe (lásd: „Adding Drivers with YaST” szakasz (2. fejezet - *Setting Up Hardware Components with YaST*, ↑*Start-Up*)). Következésképpen a PPD-fájl kiválasztható telepítéskor.

Vigyázzon arra, ha a nyomtató gyártója teljes szoftvercsomagokat akar telepíttetni a konfigurációs fájlok módosításán túl. Először is az ilyesfajta telepítés hatására elvész az openSUSE által biztosított támogatás, másodszor lehet, hogy a nyomtatási parancsok másképp viselkednek és a rendszer többé nem képes más gyártók eszközeit helyesen kezelni. Éppen ezért nem ajánlott a gyártók által biztosított szoftverek telepítése.

9.4 Hálózati nyomtatók

A hálózati nyomtatók többféle protokollt is támogatnak, némelyikük akár egyidőben is. Bár a támogatott protokollok többsége szabványosított, egyes gyártók kibővítik (módosítják) a szabványt, mivel olyan rendszereket tesztelnek, amelyek nem tökéletesen valósítják meg a szabványt, vagy mert a szabványból hiányzó funkciókat akarnak biztosítani. Ezután a gyártók bizonyos operációs rendszerekhez biztosítanak illesztőprogramokat és megszüntetik e rendszerek alatt a problémákat. Sajnos, Linux-illesztőprogramokat ritkán adnak a nyomtatókhoz. A jelenlegi helyzet szerint nem lehet nyugodtan feltételezni azt, hogy minden protokoll kifogástalanul működik Linux alatt. Éppen ezért lehet, hogy kísérletezni kell a különféle beállításokkal egy működő konfiguráció kialakításához.

A CUPS a `socket`, `LPD`, `IPP` és `smb` protokollokat támogatja.

socket
: A *socket* egy olyan kapcsolatra utal, amelyben az adatok egy internetes socketbe kerülnek továbbításra, előzetes SSL adat-kézfogás elvégzése nélkül. A leggyakrabban használt socket portszámok a `9100` és a `35`. Az eszköz URI (egységes erőforrás-azonosító) szintaxisa: socket://*a_nyomtató_IP-címe*:*port*, példa: `socket://192.168.2.202:9100/`.

LPD (line printer daemon, sornyomtató démon)
: Az igazoltan sikeres LPD protokollt az RFC 1179 írja le. E protokoll keretében a tényleges nyomtatási adatok előtt a feladatokkal kapcsolatos kiegészítő információ, például a sor azonosítója kerül továbbításra. Éppen ezért, ha az LPD protokoll szolgál az adatok átvitelére, a nyomtatási sor nevét mindig meg kell adni. A különféle nyomtatógyártók megvalósításai általában elég rugalmasak ahhoz, hogy bármilyen nevet elfogadjanak nyomtatási sorként. Ha szükséges, a nyomtató kézikönyve megadja, hogy milyen nevet kell használni. Gyakori az LPT, LPT1, LP1 vagy hasonló nevek használata. Természetesen a CUPS rendszerben egy másik Linux vagy UNIX-gép LPD-sora is beállítható. Az LPD szolgáltatás portszáma `515`. Egy eszköz URI példa:`lpd://192.168.2.202/LPT1`.

IPP (Internet printing protocol, internetes nyomtatási protokoll)
: Az IPP a HTTP protokollra épülő, viszonylag új (1999-es) szabvány. Az IPP használata esetén a többi protokollnál is több feladatspecifikus adat kerül továbbításra. A CUPS belső adatátvitelre az IPP-t használja. Ez a két CUPS-kiszolgáló közötti továbbítási sorok ajánlott protokollja. A nyomtatási sor nevét pontosan kell

megadni ahhoz, hogy az IPP helyesen működjön. Az IPP portszáma `631`. Egy eszköz URI példa: `ipp://192.168.2.202/ps` és `ipp://192.168.2.202/printers/ps`.

SMB (windowsos megosztás)
: A CUPS lehetővé teszi windowsos megosztásokon keresztüli nyomtatást is. Erre az SMB nevű protokoll szolgál. Az SMB által használt portszámok: `137`, `138`, `139`. Egy eszköz URI példa: `smb://user:password@workgroup/smb.example.com/printer`, `smb://user:password@smb.example.com/printer`, and `smb://smb.example.com/printer`.

A nyomtató által támogatott protokollt még a beállítás előtt meg kell állapítani. Ha a gyártó nem biztosítja a szükséges információt, akkor az `nmap` parancs (az `nmap` csomag része) használható a protokoll meghatározására. Az `nmap` a nyitott portokat ellenőrzi. Például:

```
nmap -p 35,137-139,515,631,9100-10000 printerIP
```

9.4.1 A CUPS beállítása parancssori eszközök segítségével

Amellett, hogy a CUPS paraméterei a YaST segítségével is megadhatók egy hálózati nyomtató beállításakor, a CUPS parancssori eszközökkel (pl. `lpadmin`, `lpoptions`) is beállítható. Szükség lesz egy eszköz URI-re, amely a háttérrendszerből (pl. parallel) és paraméterekből áll. A rendszeren érvényes eszköz URI-k meghatározásához adja ki az `lpinfo -v | grep ":/"` parancsot:

```
# lpinfo -v | grep ":/"
direct usb://ACME/FunPrinter%20XL
direct parallel:/dev/lp0
```

Az `lpadmin` paranccsal a CUPS kiszolgálóadminisztrátor osztály- és nyomtatási sorokat vehet fel, törölhet vagy kezelhet. Nyomtatási sor hozzáadásához használja a következő szintaxist:

```
lpadmin -p queue -v device-URI -P PPD-file -E
```

Ekkor az eszköz (-v) *sorként* (-p) áll rendelkezésre a megadott PPD-fájl (-P) használatával. Ez azt jelenti, hogy a nyomtató kézi beállításához ismernie kell a PPD-fájl és az eszköz URI-ját.

A -E ne legyen az első paraméter. A CUPS összes parancsánál az első paraméterként megadott -E titkosított kapcsolatot állít be. A nyomtató engedélyezéséhez a -E paramétert az alábbi példához hasonlóan kell használni:

```
lpadmin -p ps -v parallel:/dev/lp0 -P \
/usr/share/cups/model/Postscript.ppd.gz -E
```

A következő példa egy hálózati nyomtatót állít be:

```
lpadmin -p ps -v socket://192.168.2.202:9100/ -P \
/usr/share/cups/model/Postscript-level1.ppd.gz -E
```

Az lpadmin további paramétereivel kapcsolatban lásd az lpadmin kézikönyvoldalát.

A rendszer telepítése közben bizonyos paramétereket alapértékekre állít be a telepítőprogram. Ezek a beállítások minden egyes nyomtatási feladat esetében módosíthatók (a használt nyomtatási eszköztől függően). Az alapértelmezett értékek módosítására a YaST is használható. Parancssori eszközökkel az alapértelmezett értékek az alábbi módon állíthatók át:

1. Először is írassa ki az összes paramétert:

   ```
   lpoptions -p queue -l
   ```

   példa:

   ```
   Resolution/Output Resolution: 150dpi *300dpi 600dpi
   ```

   Az aktív alapértelmezett értéket az előtte álló csillag (*) karakter azonosítja.

2. Módosítsa a paramétert az lpadmin paranccsal:

   ```
   lpadmin -p queue -o Resolution=600dpi
   ```

3. Ellenőrizze az új beállítást:

   ```
   lpoptions -p queue -l

   Resolution/Output Resolution: 150dpi 300dpi *600dpi
   ```

Ha egy normál felhasználó az `lpoptions` parancsot futtatja, akkor a beállítások az `~/.cups/.lpoptions` fájlba íródnak. A `root` beállítások az `/etc/cups/lpoptions` fájlba íródnak.

9.5 Grafikus nyomtatási felületek

Az olyan eszközök, mint az xpp, vagy a kprinter nevű KDE-program, grafikus felületet biztosítanak a sorok kiválasztásához, valamint a CUPS szabványos paramétereinek, illetve a PPD-fájlból származó nyomtatóspecifikus paraméterek beállításához. A kprinter használható alap nyomtatási felületként nem-KDE alkalmazásokhoz is. Ehhez a `kprinter` vagy `kprinter --stdin` parancsot kell megadni az alkalmazások nyomtatási párbeszédablakában. Azt, hogy a kettő közül melyiket kell használni, az határozza meg, hogy viszi át az alkalmazás az adatokat – egyszerűen próbálja ki, melyik működik. Helyes beállítás esetén az alkalmazás meghívja a kprinter párbeszédablakát minden egyes alkalommal, amikor elküld egy nyomtatási feladatot. A nyomtatási sor tehát a párbeszédablakból választható ki és itt adhat meg egyéb nyomtatási beállításokat is. Ehhez viszont az szükséges, hogy az alkalmazás saját nyomtatóbeállítása ne ütközzön a kprinterével, illetve hogy a nyomtatási paraméterek csak a kprinter segítségével legyenek módosítva, ha már be lettek állítva. További információ a KPrinterről: 7. fejezet - *Managing Print Jobs* (↑*KDE User Guide*).

9.6 Nyomtatás parancssorból

A parancssorból végzett nyomtatáshoz adja ki az `lp -d` *`sor_neve fájlnév`* parancsot úgy, hogy a *`sor_neve`* és a *`fájlnév`* helyére behelyettesíti a megfelelő neveket.

Egyes alkalmazások az `lp` parancsra támaszkodnak a nyomtatás során. Ebben az esetben írja be a megfelelő parancsot az alkalmazás nyomtatási párbeszédablakába (de általában nem kell megadni a *`fájlnév`* paramétert): például `lp -d` *`sor_neve`*.

9.7 A CUPS speciális jellemzői openSUSE alatt

A CUPS némely funkciói átalakításra kerültek az openSUSE rendszerben. Az alábbiakban végigvesszük a legfontosabb módosításokat.

9.7.1 CUPS-kiszolgáló és a tűzfal

Az openSUSE alapértelmezett telepítésének befejezése után a SuSEfirewall2 aktív és a hálózati eszközök úgy vannak beállítva, hogy a bejövő forgalmat blokkoló `külső zónában` legyenek. A CUPS használatakor ezeket az alapértelmezett beállításokat módosítani kell. A SUSEfirewall2 konfigurálásával kapcsolatban további információk: 33.4. - SuSEfirewall2 (536. oldal).

CUPS-kliens

A CUPS kliens általában egy normál, a tűzfal mögötti, megbízható hálózaton belüli munkaállomáson fut. Ebben az esetben ajánlott a hálózati csatolót úgy beállítani, hogy a `belső zónában` legyenek, így a munkaállomás elérhető lesz a hálózaton belül.

CUPS-kiszolgáló

Ha a CUPS-kiszolgáló egy tűzfallal védett, megbízható hálózat része, akkor a hálózati csatolót úgy kell beállítani, hogy a tűzfal `belső zónájában` legyen. Nem célszerű a CUPS-kiszolgálót egy nem megbízható hálózatban beüzemelni, hacsak speciális tűzfalszabályokkal és a CUPS-konfiguráció biztonsági beállításainak alkalmazásával nem gondoskodik a rendszer védelméről.

9.7.2 Különféle csomagok PPD-fájljai

A YaST nyomtatókonfigurációs modulja a CUPS sorait kizárólag az `/usr/share/cups/model` könyvtárban talált PPD-fájlok alapján állítja be. A nyomtatómodellhez tartozó megfelelő PPD-fájlok meghatározásához a YaST összehasonlítja a hardverfelismerés során megállapított gyártó- és modellnevet a rendszer`/usr/share/cups/`

model könyvtárában található PPD-fájlokban lévőkkel. E célból a YaST nyomtatókonfiguráció létrehoz a PPD-fájlokból kinyert gyártó- és modelladatokból egy adatbázist. Egy nyomtató kiválasztásakor megkapja a modellista szerinti gyártónak és modellnek megfelelő PPD-fájlokat.

A kizárólag a PPD-fájlokra épülő, minden más információforrást mellőző beállítás előnye, hogy az /usr/share/cups/model könyvtárban található PPD-fájlok szabadon módosíthatók. A YaST nyomtatókonfigurációs modulja felismeri a változásokat és újragenerálja a gyártó- és modelladatbázist. Ha például csak PostScript-nyomtatókkal rendelkezik, akkor általában nincs szükség a cups-drivers csomag Foomatic PPD-fájljaira, vagy a gutenprint csomag Gutenprint PPD-fájljaira. Ehelyett a PostScript-nyomtatók PPD-fájljai közvetlenül bemásolhatók az /usr/share/cups/model könyvtárba (ha hiányoznának a manufacturer-PPDs csomagból), így optimálisan állíthatók be a meglévő nyomtatók.

A cups csomag CUPS PPD-fájljai

A cups csomagban található általános PPD-fájlok ki lettek bővítve megfelelően átalakított Foomatic PPD-fájlokkal PostScript L 1 és L 2 nyomtatókhoz:

- /usr/share/cups/model/Postscript-level1.ppd.gz
- /usr/share/cups/model/Postscript-level2.ppd.gz

A cups-drivers csomag PPD-fájljai

A nem PostScript nyomtatókhoz általában a Foomatic nyomtatószűrő (foomatic-rip) kerül felhasználásra a Ghostscripttel együtt. A megfelelő Foomatic PPD-fájlokhoz a *NickName: ... Foomatic/Ghostscript driver és a *cupsFilter: ... foomatic-rip bejegyzések tartoznak. Ezek a PPD-fájlok a cups-drivers csomag részei.

A YaST általában előnyben részesíti a manufacturer-PPDs (gyártói PPD-ket tartalmazó) csomagból származó fájlokat. Ha azonban nincs megfelelő manufacturer-PPD fájl, akkor egy *NickName: ... Foomatic ... (javasolt) Foomatic PPD fájl lesz kiválasztva.

A `gutenprint` csomag Gutenprint PPD-fájljai

Számos nem-PostScript nyomtató esetén a `foomatic-rip` helyett a Gutenprint (korábban GIMP-Print) `rastertogutenprint` CUPS-szűrője is használható. Ez a szűrő és a megfelelő Gutenprint PPD-fájlok a `gutenprint` csomagban találhatók. A Gutenprint PPD-fájlok az `/usr/share/cups/model/gutenprint/` könyvtárban találhatók és a `*NickName: ... CUPS+Gutenprint`, valamint `*cupsFilter: ... rastertogutenprint` bejegyzések tartoznak hozzájuk.

A nyomtatógyártók PPD-fájljai a `manufacturer-PPDs` csomagban

A `manufacturer-PPDs` csomag a nyomtatógyártók saját, megfelelően liberális licencfeltételek mellett kiadott PPD-fájljait tartalmazzák. A PostScript-nyomtatókat célszerű a gyártó PPD-fájljával beállítani, mivel ez a fájl lehetővé teszi a PostScript-nyomtató összes funkciójának kihasználását. A YaST előnyben részesíti a `manufacturer-PPDs` (gyártói PPD-ket tartalmazó) csomag PPD-fájljait. A YaST nem tudja használni a `manufacturer-PPDs` csomag PPD-fájlját, ha a modell neve nem egyezik meg. Ez olyankor történhet meg, ha a `manufacturer-PPDs` csomag csak egyetlen PPD-fájlt tartalmaz több, hasonló modellhez, például a Funprinter 12xx sorozat összes tagjához. Ebben az esetben a megfelelő PPD-fájlt kézzel kell kiválasztani a YaST-ban.

9.8 Hibaelhárítás

Az alábbi szakaszok a nyomtatóhardver és -szoftver leggyakoribb problémáit tekintik át, valamint bemutatják a megoldás módját vagy lehetőséget adnak a megkerülésükre. Szó lesz a GDI nyomtatókról, PPD-fájlokról, valamint a portok beállításáról. Szintén tárgyaljuk a leggyakoribb nyomtatási problémákat, a hibás nyomatok és a nyomtatási sorok kezelését.

9.8.1 Szabványos nyomtatónyelveket nem támogató nyomtatók

A szabványos nyomtatónyelveket nem támogató, csak speciális vezérlőszekvenciákkal szabályozható nyomtatókat GDI-nyomtatóknak szokás hívni. Ezek a nyomtatók csak azon operációsrendszer-verziók alatt használhatók, amelyekhez a gyártó biztosít illesztőprogramot. A GDI a Microsoft* által grafikus eszközökhöz kifejlesztett programozási felület. A gyártók általában csak a Windowshoz adnak illesztőprogramot és mivel a Windows-illesztő a GDI-felületet használja, ezeket a nyomtatókat szintén *GDI-nyomtatóknak* szokás hívni. A tényleges problémát nem a programozási felület jelenti, hanem az a tény, hogy a GDI-nyomtatók csak az adott nyomtatómodell egyedi nyomtatónyelvével vezérelhetők.

Egyes nyomtatók átkapcsolhatók, hogy GDI-módban működjenek, vagy a szabványos nyomtatónyelvek valamelyikével. Ha lehetséges, nézze meg a nyomtató kézikönyvét. Bizonyos modelleknél az átkapcsoláshoz szükség van egy speciális Window-szoftverre (figyeljen rá, hogy a Windows-illesztő lehet, hogy minden alkalommal visszaállítja a nyomtatót GDI-módra, ha Windowsból nyomtat). Más GDI-nyomtatókhoz vannak szabványos nyomtatónyelvi bővítőmodulok.

Egyes gyártók egyedi illesztőprogramokat biztosítanak GDI-nyomtatóikhoz. Az egyedi illesztőprogramok hátránya, hogy nincs garancia arra, hogy ezek működnek a telepített nyomtatórendszerrel, és hogy megfelelők a különféle hardverplatformokhoz. A szabványos nyomtatónyelveket támogató nyomtatók ezzel szemben nem függenek a nyomtatási rendszer egy adott változatától, sem a használt hardverplatformtól.

Az egyedi Linux-illesztőprogramok munkára bírása helyett lehet, hogy költséghatékonyabb megoldás egy támogatott nyomtató vásárlása. Ez megoldja az illesztőprogram problémáját egyszer és mindenkorra: nincs többé szükség speciális illesztőprogramok telepítésére és beállítására, valamint a nyomtatási rendszer fejlesztései miatt új illesztőprogram-verziók beszerzésére.

9.8.2 Nincs megfelelő PPD-fájl egy PostScript-nyomtatóhoz

Ha a `manufacturer-PPDs` csomag nem tartalmaz megfelelő PPD-fájlt egy PostScript-nyomtatóhoz, akkor használható a nyomtatógyártó illesztőprogram CD-jén

található PPD-fájl, vagy letölthető egy alkalmas PPD-fájl a nyomtatógyártó weboldaláról.

Ha a PPD-fájl ZIP-archívum (.zip) vagy önkicsomagoló ZIP-archívum (`.exe`) formájában érkezik, akkor csomagolja ki az `unzip` paranccsal. Először tekintse meg a PPD-fájl licencfeltételeit. Ezután a `cupstestppd` segédprogrammal ellenőrizze, hogy a PPD-fájl megfelel-e az „Adobe PostScript Printer Description File Format Specification, version 4.3.” specifikáció előírásainak. Ha a segédprogram „FAIL” eredményt ad vissza, akkor a PPD-fájlban komoly hibák vannak, és komoly hibákra lehet számítani a nyomtatásnál is. A `cupstestppd` által azonosított problémákat lehetőleg meg kell szüntetni. Ha szükséges, kérjen helyes PPD-fájlt a nyomtató gyártójától.

9.8.3 Párhuzamos portok

A legbiztonságosabb megközelítés a nyomtatót közvetlenül az első párhuzamos portra kötni és az alábbi beállításokat megadni a BIOS-ban:

- I/O address (I/O-cím): `378` (hexadecimális)
- Interrupt (megszakítás): mindegy
- Mode (mód): `normal` (normál), `SPP` vagy `output only` (csak kimenet)
- DMA: disabled (letiltva)

Ha a nyomtató a fenti beállítások ellenére sem érhető el a párhuzamos porton, akkor írja be az I/O-címet közvetlenül az `/etc/modprobe.conf` fájlba `0x378` formában. Ha két párhuzamos port van, amelyek I/O-címei `378` és `278` (hexadecimális), akkor ezeket `0x378,0x278` formában adja meg.

Ha a `7.` megszakítás szabad, akkor az az alább bemutatott módon aktiválható (9.1. példa - `/etc/modprobe.conf`: Az első párhuzamos port megszakítási módja (120. oldal)). A megszakítási mód aktiválása előtt ellenőrizze a `/proc/interrupts` fájlban, hogy mely megszakítások vannak már használatban. Csak az éppen használt megszakítások kerülnek megjelenítésre. Ez függhet attól, hogy mely hardverelemek aktívak. A párhuzamos port megszakítását más eszköz nem használhatja. Ha nem biztos a dolgában, használja a lekérdezéses (polling) módot az `irq=none` beállítással.

9.1 példa */etc/modprobe.conf: Az első párhuzamos port megszakítási módja*

```
alias parport_lowlevel parport_pc
options parport_pc io=0x378 irq=7
```

9.8.4 Hálózati nyomtatók csatlakoztatása

Hálózati problémák azonosítása
: Csatlakoztassa a nyomtatót közvetlenül a számítógéphez. Tesztelési célból állítsa be a nyomtatót helyi nyomtatóként. Ha így működik, akkor a probléma a hálózatban lesz.

A TCP/IP-hálózat ellenőrzése
: A TCP/IP-hálózatnak és a névfeloldásnak működnie kell.

Távoli `lpd` ellenőrzése
: Az alábbi paranccsal ellenőrizhető, hogy létesíthető-e TCP-kapcsolat a *`gép neve`* gépen futó `lpd`-vel (port `515`):

  ```
  netcat -z host 515 && echo ok || echo failed
  ```

  Ha az `lpd` felé nem létesíthető kapcsolat, akkor lehet, hogy az `lpd` nem fut, vagy valamilyen gond van a hálózattal.

  A `root` felhasználó nevében adja ki az alábbi parancsot egy (várhatóan jó hosszú) állapotjelentés lekéréséhez a távoli *`host`* gépen található sorról (*`queue`*), feltéve, hogy az `lpd` aktív és a gép elfogadja a kéréseket:

  ```
  echo -e "\004queue" \
  | netcat -w 2 -p 722 host 515
  ```

  Ha az `lpd` nem válaszol, akkor lehet, hogy nem fut, vagy valamilyen gond van a hálózattal. Ha az `lpd` válaszol, akkor a válaszból ki kell derülnie, hogy miért nem lehet nyomtatni a `host` gép sorára (`queue`). Ha a 9.2. példa - Az `lpd` hibaüzenete (120. oldal) példában bemutatotthoz hasonló választ kap, akkor a problémát a távoli `lpd` okozza.

9.2 példa *Az lpd hibaüzenete*

```
lpd: your host does not have line printer access
lpd: queue does not exist
printer: spooling disabled
printer: printing disabled
```

Távoli `cupsd` ellenőrzése

A CUPSD hálózati kiszolgáló alapértelmezésben 30 másodpercenként meghirdeti magát a `631`-es UDP-porton. Így a következő parancs használható annak kiderítésére, hogy működik-e CUPS hálózati kiszolgáló a hálózaton. A parancs végrehajtása előtt győződjön meg róla, hogy leállította a helyi CUPS-démont.

```
netcat -u -l -p 631 & PID=$! ; sleep 40 ; kill $PID
```

Ha létezik nyilvános üzeneteket küldő CUPS hálózati kiszolgáló, akkor a kimenet az alábbi példában bemutatotthoz lesz hasonló: 9.3. példa - A CUPS hálózati kiszolgáló nyilvános üzenete (121. oldal).

9.3 példa *A CUPS hálózati kiszolgáló nyilvános üzenete*

```
ipp://192.168.2.202:631/printers/queue
```

Az alábbi paranccsal ellenőrizhető, hogy létesíthető-e TCP-kapcsolat a *`host`* gépen futó `cupsd`-vel (`631`-es port):

```
netcat -z host 631 && echo ok || echo failed
```

Ha a `cupsd` felé nem létesíthető kapcsolat, akkor lehet, hogy a `cupsd` nem fut, vagy valamilyen gond van a hálózattal. Az `lpstat -h host -l -t` paranccsal lekérhető egy (várhatóan jó hosszú) állapotjelentés a *`host`* gépen található összes sorról, feltéve, hogy a `cupsd` aktív és a gép elfogadja a kéréseket.

A következő paranccsal ellenőrizhető, hogy a *`host`* gépen található sor (*`queue`*) elfogad-e egy mindössze egyetlen soremelés karakterből álló nyomtatási feladatot. Semmi sem kerül kinyomtatásra. A nyomtató esetleg kidob egy üres oldalt.

```
echo -en "\r" \
| lp -d queue -h host
```

Hálózati nyomtató vagy nyomtatókiszolgáló hibaelhárítása

A nyomtatókiszolgáló egységekben (pl. JetDirect) futó nyomtatásisor-kezelők néha problémát jelenthetnek, ha túlságosan sok nyomtatási feladattal kell megküzdeniük. Mivel ezt a nyomtatókiszolgáló egységben működő nyomtatásisor-kezelő okozza, semmit nem lehet tenni vele. Kerülő megoldásként ki lehet hagyni a nyomtatókiszolgáló egységben működő nyomtatásisor-kezelőt, ha közvetlenül, egy TCP-socketen keresztül címzi meg a nyomtatót. Lásd:9.4. - Hálózati nyomtatók (111. oldal)

Ily módon a nyomtatókiszolgáló egység az adatátvitel különböző formái (TCP/IP-hálózat és helyi nyomtatókapcsolat) közötti átalakítóvá egyszerűsödik. A módszer

használatához ismerni kell a nyomtatókiszolgáló egység TCP-portját. Ha a nyomtató a nyomtatókiszolgáló egységhez csatlakozik és be van kapcsolva, akkor ez a TCP-port általában meghatározható az `nmap` csomagban található `nmap` segédprogrammal a nyomtatókiszolgáló egység bekapcsolása után. Az `nmap` *`IP-cím`* például a következő eredményt adhatja egy nyomtatókiszolgáló egység esetében:

```
Port        State       Service
23/tcp      open        telnet
80/tcp      open        http
515/tcp     open        printer
631/tcp     open        cups
9100/tcp    open        jetdirect
```

Ez a kimenet azt jelzi, hogy a nyomtatókiszolgáló egységre csatlakozó nyomtató a `9100`-as TCP socketporton keresztül érhető el. Alapértelmezésben az `nmap` csak az `/usr/share/nmap/nmap-services` fájlban felsorolt ismert portokat ellenőrzi. Az összes lehetséges port ellenőrzéséhez használja az `nmap -p` *`mettől-meddig IP-cím`* parancsot. Ez viszont eltarthat egy darabig. További információt talál az `nmap` parancs kézikönyvoldalán.

Az alábbihoz hasonló paranccsal

```
echo -en "\rHello\r\f" | netcat -w 1 IP-address port
cat file | netcat -w 1 IP-address port
```

küldhet karaktersorozatokat vagy fájlokat közvetlenül a megfelelő portra annak ellenőrzésére, hogy a nyomtató valóban elérhető-e ezen a porton.

9.8.5 Hibás nyomtatás hibaüzenet nélkül

A nyomtatórendszerben a nyomtatási feladat akkor fejeződik be, ha a CUPS háttérrendszer befejezi az adatok elküldését a fogadónak (a nyomtatónak). Ha a fogadón a további feldolgozással probléma van, például a nyomtató nem képes a nyomtatóspecifikus adatok kinyomtatására, a nyomtatási rendszer ezt már nem veszi észre. Ha a nyomtató nem képes a nyomtatóspecifikus adatok kinyomtatására, akkor válasszon a nyomtatónak jobban megfelelő PPD-fájlt.

9.8.6 Letiltott sorok

Ha az adatátvitel a fogadóra több kísérlet után sem sikerül, akkor a CUPS háttérrendszer, például az `USB` vagy a `socket` hibát jelez a nyomtatási rendszer (a `cupsd`) felé. A háttérrendszer dönti el, hogy hány további kísérletet tegyen még, mielőtt visszajelezné, hogy az adatátvitel nem sikerült. Mivel ezek után a további kísérletek hiábavalók, a `cupsd` letiltja az adott sorra nyomtatást. A probléma okának megszüntetése után a rendszergazdának újra engedélyeznie kell a nyomtatást a `cupsenable` paranccsal.

9.8.7 CUPS tallózás: Nyomtatási feladatok törlése

Ha egy CUPS hálózati kiszolgáló meghirdeti a sorait a kliensgépek felé tallózáson keresztül, és egy megfelelő helyi `cupsd` aktív a kliensgépeken, akkor a kliens `cupsd` elfogadja az alkalmazások nyomtatási feladatait és továbbítja őket a kiszolgálón futó `cupsd` felé. Amikor a `cupsd` elfogad egy nyomtatási feladatot, akkor új feladatszámot ad neki. Ez azt jelenti, hogy a kliensgépen a feladat száma nem fog megegyezni a kiszolgáló feladatszámával. Mivel a nyomtatási feladatok jellemzően azonnal továbbítódnak, nem törölhetők a feladatszámmal a kliensgépen, mivel a kliens `cupsd`-je a nyomtatási feladatot befejezettnek tekinti azonnal, ahogy az továbbítódott a kiszolgáló `cupsd`-je felé.

Ahhoz, hogy a nyomtatási feladatot törölni lehessen a kiszolgálón, az `lpstat -h cups.example.com -o` paranccsal állapítsa meg a feladat számát a kiszolgálón, feltéve, hogy a kiszolgáló nem végzett még a feladat kinyomtatásával (nem küldte még el a nyomtatóra). A feladatszám segítségével a kiszolgálón a következő paranccsal törölhető a nyomtatási feladat:

```
cancel -h cups.example.com queue-jobnnumber
```

9.8.8 Hibás nyomtatási feladatok és adatátviteli hibák

A nyomtatási feladatok a sorokban maradnak és a nyomtatásuk folytatódik, hacsak ki és be nem kapcsolja a nyomtatót, valamint újra nem indítja a számítógépet a nyomtatási

folyamat közben. A hibás nyomtatási feladatokat a `cancel` paranccsal lehet eltávolítani a sorból.

Ha egy nyomtatási feladat hibás, vagy hiba történik a gép és a nyomtató közötti kommunikációban, akkor a nyomtató egy csomó papírt ki fog nyomtatni hibás karakterekkel, mert nem lesz képes az adatok helyes értelmezésére. Ennek megelőzéséhez tegye a következőket:

1. A nyomtatás leállításához vegye ki az összes papírt a tintasugaras nyomtatóból, vagy nyissa ki a lézernyomtató papírtálcáját. Egyes nyomtatókon külön gomb is van az éppen folyó nyomtatás megszakítására.

2. Lehet, hogy a nyomtatási feladat még mindig a sorban van, mivel a feladatok csak akkor törlődnek a sorból, ha már teljes egészében el lettek küldve a nyomtatóra. Az `lpstat -o` vagy `lpstat -h cups.example.com -o` paranccsal ellenőrizheti, melyik sor nyomtatása folyik éppen. A nyomtatási feladat törléséhez adja ki a `cancel` *`sor-feladatszám`* vagy `cancel -h cups.example.com` *`sor-feladatszám`* parancsot.

3. Bizonyos adatok még a nyomtatási feladat sorból való törlése után is továbbítódhatnak a nyomtatóra. Ellenőrizze, hogy fut-e a sorért felelős CUPS háttérfolyamat, és ha igen, állítsa le. Például a párhuzamos portra csatlakoztatott nyomtató esetében a `fuser -k /dev/lp0` paranccsal szüntethető meg minden olyan folyamat, amelyik még mindig a nyomtatót (pontosabban a párhuzamos portot) próbálja elérni.

4. Állítsa teljesen alaphelyzetbe a nyomtatót: kapcsolja ki hosszabb időre. Ezután helyezzen bele papírt, majd kapcsolja újra be.

9.8.9 A CUPS nyomtatási rendszer hibaelhárítása

A CUPS nyomtatási rendszer problémái az alábbi eljárással kereshetők meg:

1. Állítsa be az `/etc/cups/cupsd.conf` fájlban a `LogLevel debug` paramétert.

2. Állítsa le a `cupsd` démont.

3 Törölje a `/var/log/cups/error_log*` fájlokat, hogy ne kelljen nagyon nagy naplófájlokban keresgélni.

4 Indítsa el a `cupsd` démont.

5 Ismételje meg a műveletet, ami a hibához vezetett.

6 Ellenőrizze a `/var/log/cups/error_log*` fájlokban található üzeneteket a probléma okának meghatározásához.

9.8.10 További információk

Számos speciális probléma megoldása megtalálható a SUSE támogatási adatbázisában (`http://en.opensuse.org/SDB:SDB`). A vonatkozó cikkek kikereséséhez adja meg az `SDB:CUPS` keresési feltételt.

10 Az X Window rendszer

Az X Window rendszer (X11) a grafikus felhasználói felületek de facto szabványa UNIX alatt. Az X egy hálózatos rendszer, amely lehetővé teszi, hogy az egyik gépen elindított alkalmazások megjelenítésre kerüljenek egy tetszőleges hálózaton (LAN vagy internet) keresztül csatlakoztatott másik gépen. Ez a fejezet az X Window rendszer beállítását és optimalizálási lehetőségeit, valamint a betűkészletek openSUSE alatti használatával kapcsolatos háttérinformációkat írja le.

10.1 Az X Window rendszer kézi beállítása

Alapértelmezés szerint az X Window rendszer beállítása a SaX2 felületen történik (2.2. - Setting Up Graphics Card and Monitor (2. fejezet - *Setting Up Hardware Components with YaST*, ↑*Start-Up*)). A beállítás azonban történhet a konfigurációs fájlok kézi módosításával is.

FIGYELEM: A hibás X-konfiguráció tönkreteheti a hardvert

Az X Window rendszer beállításánál legyen nagyon körültekintő. Sose indítsa el az X Window rendszert addig, amíg a beállítást be nem fejezte. Egy rosszul beállított rendszer javíthatatlan hibát okozhat a hardverben (ez különösen a rögzített frekvenciás monitorokra érvényes). A könyv és az openSUSE szerzői nem vállalnak felelősséget a hibáért. Az itt leírtakat gondosan megvizsgáltuk, de ez nem garantálja, hogy az összes itt megjelenített eljárás helyes és nem károsítja a hardvert.

A `sax2` program létrehozza az `/etc/X11/xorg.conf` fájlt. Ez az X Window rendszer elsődleges konfigurációs fájlja. Itt található meg a grafikus kártyával, egérrel és monitorral kapcsolatos összes beállítás.

FONTOS: Az X -configure használata

Az `X –configure` paranccsal lehet beállítani az X rendszert, ha az openSUSE SaX2 segédprogramjával nem sikerült. Ha a rendszerben egyedi, csak bináris (formában létező) illesztőprogramokat kell használni, akkor az `X –configure` parancs nem fog működni.

Az alábbi bekezdések az `/etc/X11/xorg.conf` konfigurációs fájl szerkezetét írják le. Több szakaszból (section) áll, amelyek mindegyike a beállítás egy adott szempontjával foglalkozik. Minden szakasz a `Section <szakasz_megnevezése>` kulcsszóval kezdődik és az `EndSection` kulcsszóval fejeződik be. Az alábbi konvenció minden szakaszra érvényes:

```
Section "szakasz megnevezése"
  1. bejegyzés
  2. bejegyzés
  n. bejegyzés
EndSection
```

A szakasztípusok listája: 10.1 táblázat - Az /etc/X11/xorg.conf szakaszai (128. oldal).

10.1. táblázat *Az /etc/X11/xorg.conf szakaszai*

Type (típus)	Jelentés
`Files`	Ez a szakasz a betűkészletek és az RGB színtáblázat által használt elérési utakat írja le.
`ServerFlags`	A kiszolgáló viselkedését befolyásoló általános kapcsolók.
`Module`	A kiszolgáló által betöltendő modulok listája.
`InputDevice`	A beviteli eszközök, mint például a billentyűzetek és speciális beviteli eszközök (touchpad, botkormányok, stb.), ebben a szakaszban kerülnek beállításra. A szakasz fontos paraméterei a `Driver`, valamint a `Protocol` és `Device` elemeket megadó

Type (típus)	Jelentés
	beállítások. A számítógéphez csatlakoztatott minden készülékhez jellemzően egy `InputDevice` szakasz tartozik.
`Monitor`	A rendszer által használt monitor. A szakasz fontos elemei az `Identifier` (azonosító), amelyre később a `Screen` definícióban hivatkozunk, a frissítési sebesség (`VertRefresh`), valamint a szinkronizációs frekvenciakorlátok (`HorizSync` és `VertRefresh`). A beállítások MHz, kHz és Hz mértékegységekben vannak megadva. Normális esetben a kiszolgáló visszautasít minden modeline beállítást, amely nem felel meg a monitor specifikációjának. Ez megakadályozza, hogy a monitorra véletlenül túl nagy frekvencia kerüljön.
`Modes`	Az adott képernyőfelbontások modeline paraméterei. Ezek a paraméterek a SaX2 segítségével kiszámíthatók a felhasználó által megadott értékek alapján és az esetek többségében nem kell módosítani őket. Itt lehet beállítani, ha például egy rözített frekvenciájú monitort kíván csatlakoztatni. Az egyedi számértékek jelentésével kapcsolatos részleteket az `/usr/share/doc/howto/en/html/XFree86-Video-Timings-HOWTO` HOWTO fájl tartalmazza (a `howtoenh` csomag része). A VESA-módok kézi kiszámításához használja a `cvt` eszközt. Például egy 1680x1050@60Hz monitor modeline paraméterének kiszámításához adja ki a `cvt 1680 1050 60` parancsot.
`Device`	Ez a szakasz egy adott grafikus kártyát ír le. Erre a leíró nevével hivatkozunk. A jelen szakaszban található paraméterek igen erősen függenek az alkalmazott illesztőprogramtól. Ha például az `i810` illesztőprogramot használja, akkor további információ a `man 4 i810` kézikönyvoldalon található.
`Screen`	Ez a szakasz egy `Monitor` és egy `Device` szakaszt egyesít az X.Org összes szükséges beállításának kialakítása érdekében. A `Display` szakaszban adja meg a képernyőhöz használt vir-

Type (típus)	Jelentés
	tuális képernyő méretét (`Virtual`), a `ViewPort` és a `Modes` elemet. Ne feledje, hogy egyes illesztőprogramok megkövetelik, hogy az összes használt konfiguráció legyen valahol jelen a `Display` szakaszban. Ha például egy noteszgépet használ, de egy olyan külső monitorral, amelynek a felbontása nagyobb, mint a belső LCD-képernyőé, akkor is lehet, hogy fel kell venni egy, a belső LCD által támogatott felbontást a `Modes` sor végére.
`ServerLayout`	Ez a szakasz egy egy- vagy többképernyős beállítás elrendezését adja meg. Ez a szakasz összeköti a beviteli eszközöket (`InputDevice`) és a megjelenítő eszközöket (`Screen`).
`DRI`	A Direct Rendering Infrastructure (közvetlen renderelési infrastruktúra, DRI) információit írja le.

A `Monitor`, `Device` és `Screen` részletesebb leírása a továbbiakban olvasható. A többi szakasszal kapcsolatos információ az `X.Org` és `xorg.conf` kézikönyvoldalán található.

Az `xorg.conf` fájlban több különböző `Monitor` és `Device` szakasz is lehet. Még akár több `Screen` szakasz is megadható. A `ServerLayout` szakasz határozza meg, hogy melyik lesz ténylegesen alkalmazva.

10.1.1 A Screen szakasz

Először tekintsük meg közelebbről a Screen szakaszt, amely egy Monitor és Device szakaszt egyesít, és meghatározza a használandó felbontást és színmélységet. A Screen szakasz az alábbihoz hasonló lehet: 10.1. példa - Az /etc/X11/xorg.conf fájl Screen szakasza (131. oldal).

10.1 példa *Az /etc/X11/xorg.conf fájl Screen szakasza*

```
Section "Screen"❶
  DefaultDepth  16❷
  SubSection "Display"❸
    Depth       16❹
    Modes       "1152x864" "1024x768" "800x600"❺
    Virtual     1152x864❻
  EndSubSection
  SubSection "Display"
    Depth       24
    Modes       "1280x1024"
  EndSubSection
  SubSection "Display"
    Depth       32
    Modes "640x480"
  EndSubSection
  SubSection "Display"
    Depth        8
    Modes       "1280x1024"
  EndSubSection
  Device        "Device[0]"
  Identifier    "Screen[0]"❼
  Monitor       "Monitor[0]"
EndSection
```

❶ A `Section` jelzi a szakasztípust, amely jelen esetben `Screen`.

❷ A `DefaultDepth` beállítás határozza meg az alapértelmezés szerint használt színmélységet, kivéve, ha kifejezetten egy adott színmélységgel lett elindítva az X kiszolgáló.

❸ Minden színmélységhez különböző `Display` alszakaszokat lehet meghatározni.

❹ A `Depth` határozza meg, hogy a jelen `Display` beállításokhoz melyik színmélység tartozzon. A lehetséges értékek a `8`, `15`, `16`, `24` és `32`, bár nem az összes X kiszolgálómodul és felbontás támogatja ezeket az értékeket.

❺ A `Modes` szakasz a lehetséges képernyőfelbontások listáját tartalmazza. Ezt a listát az X kiszolgáló balról jobbra haladva ellenőrzi. Az X kiszolgáló minden egyes felbontáshoz egy megfelelő `Modeline` sort keres a `Modes` szakaszban. A `Modeline` a monitor és a grafikus kártya képességétől függ. A `Monitor` beállítások határozzák meg az eredményül kapott `Modeline` elemet.

Az első megtalált felbontás az `Alapértelmezett mód`. A Ctrl + Alt + szürke + billentyűkombináció segítségével lehet átváltani a lista jobb oldali következő felbontására. A Ctrl + Alt + szürke – billentyűkombinációval pedig az előzőre

(balra) lehet visszaváltani. Ez lehetővé teszi a felbontás módosítását az X futása közben is.

❻ A `Display` alszakasz utolsó sorában lévő `Virtual 1152x864` a virtuális képernyő méretére utal. A virtuális képernyő maximális lehetséges mérete a grafikus kártyán telepített memória mennyiségétől és a kívánt színmélységtől, nem pedig a monitor maximális felbontásától függ. Ha kihagyja ezt a sort, akkor a virtuális felbontás a fizikai felbontással lesz egyenlő. Mivel a modern grafikus kártyák nagy mennyiségű videomemóriával rendelkeznek, nagyon nagy virtuális asztalt biztosító rendszerek hozhatók létre. Elképzelhető azonban, hogy a 3D-funkció a továbbiakban nem használható, ha a videomemória nagy része egy virtuális asztalhoz kerül felhasználásra. Ha a kártya 16 MB video RAM-mal rendelkezik, akkor a virtuális képernyő 8 bites színmélységben akár 4096x4096 pixel is lehet. Különösen gyorsított kártyák esetén nem ajánlatos a teljes memóriát a virtuális képernyőhöz használni, mivel a kártyán lévő memóriába számos betűkészlet és grafikus gyorsítótár is kerül.

❼ Az `Identifier` sor (itt `Screen[0]`) egy meghatározott nevet ad a szakasznak, amellyel egyedi módon lehet rá hivatkozni a következő `ServerLayout` szakaszban. A `Device` és `Monitor` sor a definícióhoz tartozó grafikus kártyát és monitort adja meg. Ezek csak hivatkozások a `Device` és `Monitor` szakaszokra a megfelelő névvel vagy *azonosítókkal*. E szakaszok részletes leírása a továbbiakban olvasható.

10.1.2 A Device szakasz

A Device szakasz egy adott grafikus kártyát ír le. Az `xorg.conf` fájlban tetszőleges számú eszköz bejegyzése adható meg, amelyek neve az `Identifier` kulcsszóval van megkülönböztetve. Az alapszabály az, hogy ha egynél több grafikus kártya van telepítve, akkor a szakaszok egyszerűen sorban kerülnek számozásra. Az első neve `Device[0]`, a másodiké `Device[1]` és így tovább. Az alábbi fájl a számítógép `Device` szakaszának kivonatát jeleníti meg egy Matrox Millennium PCI grafikus kártyával (ahogy a SaX2 beállította):

```
Section "Device"
  BoardName     "MGA2064W"
  BusID         "0:19:0"❶
  Driver        "mga"❷
  Identifier    "Device[0]"
  VendorName    "Matrox"
```

```
  Option        "sw_cursor"
EndSection
```

❶ A `BusID` a PCI vagy AGP kártyahelyre utal, amelyikbe a videokártya be van helyezve. Ez az `lspci` parancs által megjelenített azonosítónak felel meg. Az X kiszolgáló a részleteket decimális formában igényli, de az `lspci` ezeket hexadecimális formában jeleníti meg. A `BusID` értékét a SaX2 automatikusan felismeri.

❷ A `Driver` értékét a SaX2 automatikusan állítja be, ez adja meg, hogy a videokártyához melyik illesztőprogramot használja a rendszer. Ha a kártya egy Matrox Millennium, akkor az illesztőprogram neve `mga`. Az X kiszolgáló ezután a `drivers` alkönyvtárban lévő `Files` szakaszban megadott `ModulePath` elemben keres. Normál telepítés esetén ez az `/usr/lib/xorg/modules/drivers` könyvtár, 64 bites operációs rendszerek esetén pedig az `/usr/lib64/xorg/modules/drivers` könyvtár. A `_drv.o` hozzáadásra kerül a névhez, így az `mga` illesztőprogram esetén az `mga_drv.o` illesztőprogramfájl töltődik be.

Az X kiszolgáló vagy az illesztőprogram viselkedése további opciók segítségével befolyásolható. Példa erre a Device szakasz `sw_cursor` beállítása. Ez letiltja a hardveres egérkurzort és az egérkurzort szoftver segítségével rajzolja ki. Az illesztőprogram-modultól függően különböző lehetőségek állnak rendelkezésre, amelyek az illesztőprogram-modulok leírásaiban találhatók, az `/usr/share/doc/`*`csomag_neve`* könyvtárban. Általánosan érvényes beállítások a kézikönyvoldalakon is találhatók (`man xorg.conf`, `man 4 <illesztőprogram-modul>`, és `man 4 chips`).

Ha a videokártyának több videocsatlakozója is van, akkor a kártya különböző eszközeit be lehet állítani úgy, hogy egyetlen (nagy) nézetet biztosítsanak. A grafikus illesztő ilyen beállításához használja a SaX2 segédprogramot.

10.1.3 A Monitor és a Modes szakasz

A `Device` szakaszhoz hasonlóan a `Monitor` és `Modes` szakaszok egy-egy monitort írnak le. Az `/etc/X11/xorg.conf` konfigurációs fájl tetszőleges számú `Monitor` szakaszt tartalmazhat. A `Monitor` szakasz a `Modes` szakaszra hivatkozik a `UseModes` sorral, ha elérhető. Ha a `Monitor` szakaszban nincsen `Modes` szakasz, akkor az X kiszolgáló a megfelelő értékeket az általános szinkronizációs értékekből számítja ki. A kiszolgálóelrendezés rész adja meg, hogy melyik `Monitor` szakasz az érvényes.

A monitordefiníciókat csak tapasztalt felhasználók állítsák át. A modeline-ok a `Monitor` szakaszok fontos részét alkotják. A modeline-ok adják meg a vízszintes és függőleges időzítést a megfelelő felbontáshoz. A monitortulajdonságok, különösen a megengedett frekvenciák a `Monitor` szakaszban tárolódnak. A normál VESA-módok a `cvt` segédprogrammal állíthatók elő. További információért olvassa el a cvt kézikönyv-oldalát: `man cvt`.

FIGYELEM

Hacsak nem rendelkezik a monitorok és a grafikus kártyák funkcióival kapcsolatos elmélyült tudással, akkor a Modeline szakaszban semmit sem szabad módosítani, mivel ez komolyan károsíthatja a monitort.

Akik saját képernyőleírásokat kívánnak készíteni, igen alaposan kell, hogy ismerjék az `/usr/share/X11/doc` könyvtárban található dokumentációt. A PDF-ek és HTML-oldalak kikereséséhez telepítse a `xorg-x11-doc` csomagot.

A modeline-ok kézi beállítására manapság ritkán van szükség. Ha modern multisync monitort használ, akkor az engedélyezett frekvenciákat és optimális felbontásokat az X kiszolgáló DDC-n keresztül közvetlenül kiolvashatja, amint azt a SaX2 beállításánál leírtuk. Ha ez valamilyen okból nem lehetséges, akkor használja az X kiszolgálóban megadott egyik VESA-módot. Ez a legtöbb grafikuskártya-monitor kombinációval működik.

10.2 Betűkészletek telepítése és beállítása

openSUSE rendszeren a további betűkészletek telepítése nagyon egyszerű. Egyszerűen csak át kell másolni a betűkészleteket az X11 betűkészletek elérési útvonalán belüli tetszőleges könyvtárba (lásd: 10.2.1. - Az X11 alap betűkészletek (136. oldal)). A betűkészletek használatához a telepítési könyvtárnak az `/etc/fonts/fonts.conf` fájlban beállított könyvtárak alkönyvtárának kell lennie (lásd: 10.2.2. - Az Xft (137. oldal)) vagy be kell ágyazni ebbe a fájlba az `/etc/fonts/suse-font-dirs.conf` használatával.

Az alábbiakban egy példát mutatunk az /etc/fonts/fonts.conf fájl részletére. Ez a fájl a normál konfigurációs fájl, amely a legtöbb esetre megfelelő beállításokat tartalmaz. Ez definiálja a mellékelt /etc/fonts/conf.d könyvtárat is. A fontconfig ebből a könyvtárból betölti az összes kétjegyű számmal kezdődő fájlt és szimbolikus láncot. E funkció részletesebb leírása az /etc/fonts/conf.d/README fájlban található.

```
<!-- Font directory list -->
<dir>/usr/share/fonts</dir>
<dir>/usr/X11R6/lib/X11/fonts</dir>
<dir>/opt/kde3/share/fonts</dir>
<dir>/usr/local/share/fonts</dir>
<dir>~/.fonts</dir>
<include ignore_missing="yes">conf.d</include>
```

Az /etc/fonts/suse-font-dirs.conf automatikusan generálódik, hogy behozza a (jellemzően külső fél gyártotta) alkalmazások (például OpenOffice.org, Java vagy Adobe Acrobat Reader) betűkészleteit. Az /etc/fonts/suse-font-dirs.conf szokásos bejegyzései az alábbihoz hasonlóak:

```
<dir>/usr/lib64/ooo-2.0/share/fonts</dir>
<dir>/usr/lib/jvm/java-1_4_2-sun-1.4.2.11/jre/lib/fonts</dir>
<dir>/usr/lib64/jvm/java-1.5.0-sun-1.5.0_07/jre/lib/fonts</dir>
<dir>/usr/X11R6/lib/Acrobat7/Resource/Font</dir>
<dir>/usr/X11R6/lib/Acrobat7/Resource/Font/PFM</dir>
```

További betűkészletek a teljes rendszerre érvényes telepítéséhez másolja át kézzel a betűkészletfájlokat (root felhasználóként) egy megfelelő könyvtárba, mint például az /usr/share/fonts/truetype. A feladat a KDE betűkészlet-telepítőjével is elvégezhető, a KDE vezérlőközpontból. Az eredmény ugyanaz.

A tényleges betűkészletek átmásolása helyett szimbolikus láncok is létrehozhatók. Erre akkor lehet szükség például, ha licencelt betűkészletekkel rendelkezik egy felcsatolt Windows partíción és használni kívánja őket. Ezt követően futtassa le a SuSEconfig --module fonts parancsot.

A SuSEconfig --module fonts a betűkészletek beállítását kezelő /usr/sbin/fonts-config parancsfájlt hajtja végre. A parancsfájl működésének megismeréséhez tekintse meg a parancsfájl kézikönyvoldalát (man fonts-config).

Az eljárás ugyanaz bittérképes, TrueType és OpenType, illetve Type1 (PostScript) betűkészletek esetén. E betűtípusok mindegyike tetszőleges könyvtárba telepíthető.

Az X.Org két teljesen különböző betűrendszert tartalmaz: a régi *X11 alap betűrendszert*, illetve az újonnan kialakított *Xft és fontconfig* rendszert. Az alábbiakban leírjuk a két rendszert röviden.

10.2.1 Az X11 alap betűkészletek

Manapság az X11 alap betűkészletrendszer nem csak bitképes betűkészletek, hanem méretezhető (Type1, TrueType, OpenType és CID kulcsú) betűkészletek használatát is támogatja. A méretezhető betűk támogatása csak élsimítás és részpixel-kirajzolás nélkül támogatott, és a sok nyelv betűalakjait tartalmazó betűkészletek betöltése hosszú időt vehet igénybe. A Unicode-betűkészletek is támogatottak, de használatuk lassú lehet, és több memóriát igényel.

Az X11 alap betűkészletrendszer rendelkezik néhány öröklött gyengeséggel. Elavult rendszer, amely nem terjeszthető ki értelmes módon. A visszamenőleges kompatibilitás érdekében meg kell tartani, de ahol csak lehetséges, a modernebb Xft és fontconfig rendszert kell használni.

A működéshez az X kiszolgálónak tudnia kell, hogy mely betűkészletek állnak rendelkezésére és ezek a rendszerben hol találhatók. Ezt `FontPath` változó kezeli, amely az összes érvényes rendszerbetűkészlet-könyvtár elérési útját tartalmazza. Ezekben a könyvtárakban egy `fonts.dir` nevű fájl a könyvtárban rendelkezésre álló összes betűkészletet felsorolja. A `FontPath` változót az X kiszolgáló állítja elő indításkor. Végigkeresi az `/etc/X11/xorg.conf` konfigurációs fájl minden `FontPath` bejegyzését egy érvényes `fonts.dir` fájl után. Ezek a bejegyzések a `Files` szakaszban találhatók. A tényleges `FontPath` változó az `xset q` parancs segítségével jeleníthető meg. Ez az elérési út futás közben az `xset` parancs segítségével módosítható. További elérési út hozzáadásához használja az `xset +fp <path>` parancsot. A nem kívánt elérési út eltávolításához használja az `xset –fp <path>` parancsot.

Ha az X kiszolgáló már aktív, akkor a felcsatolt könyvtárakban található, frissen telepített betűkészletek az `xset fp rehash` parancs segítségével aktiválhatók. Ezt a parancsot a `SuSEconfig --module fonts` hajtja végre. Mivel az `xset` parancsnak hozzá kell tudnia férni a futó X kiszolgálóhoz, ez csak akkor működik, ha a `SuSEconfig --module fonts` egy olyan parancsértelmezőből van indítva, amelyik hozzá tud férni a futó X kiszolgálóhoz. A legegyszerűbb mód ennek eléréséhez, ha az `su` parancs és a `root` jelszó megadásával szerez `root` jogosultságot. Az `su` átadja az X kiszolgáló elindító felhasználó hozzáférési jogosultságait a `root` parancsértel-

mezőnek. Annak ellenőrzéséhez, hogy a betűkészletek megfelelően telepítésre kerültek-e és hogy rendelkezésre állnak-e az X11 alap betűkészletrendszeren keresztül, az `xlsfonts` parancs segítségével jelenítse meg a rendelkezésre álló betűkészletek listáját.

Az openSUSE alapértelmezés szerint UTF-8 területi beállításokat használ. Éppen ezért a Unicode-betűkészletek a preferáltak (azok, amelyek neve `iso10646-1`-re végződik az `xlsfonts` kimenetében). Az összes Unicode-betűkészlet kiíratható az `xlsfonts | grep iso10646-1` paranccsal. Az openSUSE szinte minden Unicode-betűkészletében megtalálhatók legalább az európai nyelvekhez szükséges (korábban `iso-8859-*`) betűalakok.

10.2.2 Az Xft

Az Xft programozói a kezdetektől fogva biztosították a méretezhető betűkészletek támogatását, beleértve az élsimítást is. Xft használata esetén a betűkészleteket az őket használó alkalmazások állítják elő, nem az X kiszolgáló, mint az X11 alap betűrendszerben. Ily módon a megfelelő alkalmazás hozzá tud férni a tényleges betűkészletfájlokhoz és teljes mértékben szabályozhatja a betűalakok előállítását. Ez képezi a többnyelvű szöveg helyes megjelenítésének alapját. A betűkészletfájlok közvetlen elérése nagyon hasznos a betűkészletek nyomtatáshoz való beágyazásához, mert így ellenőrizhető, hogy a nyomtatási kimenet ugyanúgy néz-e ki, mint a képernyőkimenet.

openSUSE alatt a két asztali környezet (a KDE és a GNOME), a Mozilla és számos más alkalmazás alapértelmezés szerint már az Xft-t használja. Az Xft-t már több alkalmazás használja, mint a régi X11 alap betűrendszert.

Az Xft a fontconfig könyvtárat használja a betűkészletek megkereséséhez és az előállításuk szabályozásához. A fontconfig tulajdonságait az `/etc/fonts/fonts.conf` globális konfigurációs fájl szabályozza. A speciális beállításokat az `/etc/fonts/local.conf` fájlba, illetve a felhasználóspecifikus `~/.fonts.conf` fájlokba kell felvenni. Ezeknek a fontconfig konfigurációs fájloknak az alábbi szöveggel kell kezdődniük:

```
<?xml version="1.0"?>
<!DOCTYPE fontconfig SYSTEM "fonts.dtd">
<fontconfig>
```

és az alábbi szöveggel kell végződniük:

```
</fontconfig>
```

A betűkészletek kereséséhez további könyvtárak az alábbi sorok hozzáfűzésével vehetők fel:

```
<dir>/usr/local/share/fonts/</dir>
```

Erre azonban általában nincs szükség. A felhasználóspecifikus `~/.fonts` alapértelmezés szerint már benne van az `/etc/fonts/fonts.conf` fájlban. Ennek megfelelően további betűkészletek telepítéséhez csak át kell őket másolni a `~/.fonts` fájlba.

A betűkészletek megjelenését befolyásoló szabályok is beilleszthetők. Írja be például az alábbit:

```
<match target="font">
 <edit name="antialias" mode="assign">
  <bool>false</bool>
 </edit>
</match>
```

az összes betűkészlet élsimításának letiltásához, vagy az alábbit:

```
<match target="font">
 <test name="family">
  <string>Luxi Mono</string>
  <string>Luxi Sans</string>
 </test>
 <edit name="antialias" mode="assign">
 <bool>false</bool>
 </edit>
</match>
```

adott betűkészletek élsimításának letiltásához.

A legtöbb alkalmazás alapértelmezés szerint a `sans-serif` (vagy az egyenértékű `sans`), `serif` vagy `monospace` betűkészletnevet használja. Ezek nem valódi betűkészletek, hanem csak álnevek, amelyek a nyelvi beállítástól függően feloldásra kerülnek a megfelelő betűkészletre.

A felhasználók egyszerűen hozzáadhatnak szabályokat a `~/.fonts.conf` fájlhoz ahhoz, hogy ezek az álnevek a kedvenc betűkészletekre legyenek feloldva:

```
<alias>
 <family>sans-serif</family>
 <prefer>
  <family>FreeSans</family>
 </prefer>
</alias>
<alias>
```

```
 <family>serif</family>
 <prefer>
  <family>FreeSerif</family>
 </prefer>
</alias>
<alias>
 <family>monospace</family>
 <prefer>
  <family>FreeMono</family>
 </prefer>
</alias>
```

Mivel alapértelmezés szerint majdnem minden alkalmazás ezeket az álneveket használja, ezek szinte a teljes rendszerre hatással vannak. A kedvenc betűkészletek majdnem mindenütt egyszerűen használhatók anélkül, hogy módosítani kellene az egyes alkalmazások betűkészlet-beállításait.

Az `fc-list` parancs segítségével megjeleníthető, hogy mely betűkészletek vannak telepítve és melyek használhatók. Az `fc-list` például az összes betűkészlet listáját adja vissza. Annak megjelenítéséhez, hogy mely rendelkezésre álló méretezhető betűkészletek (`:scalable=true`) tartalmazzák a héberhez szükséges betűalakot (`:lang=he`), mi ezek neve (`family`), stílusa (`style`), vastagsága (`weight`) és a betűkészleteket tartalmazó fájlok neve, adja ki az alábbi parancsot:

```
fc-list ":lang=he:scalable=true" family style weight
```

A parancs kimenete az alábbi módon néz ki:

```
Lucida Sans:style=Demibold:weight=200
DejaVu Sans:style=Bold Oblique:weight=200
Lucida Sans Typewriter:style=Bold:weight=200
FreeSerif:style=Bold,polkrepko:weight=200
FreeSerif:style=Italic,ležeče:weight=80
FreeSans:style=Medium,navadno:weight=80
DejaVu Sans:style=Oblique:weight=80
FreeSans:style=Oblique,ležeče:weight=80
```

Az `fc-list` parancs segítségével lekérdezhető legfontosabb paraméterek:

10.2. táblázat *Az fc-list paraméterei*

Paraméter	Jelentés és lehetséges értékek
`family`	A betűcsalád neve, például `FreeSans`.

Paraméter	Jelentés és lehetséges értékek
`foundry`	A betűkészlet gyártója, például `urw`.
`style`	A betűkészlet stílusa, például `Medium` (közepes), `Regular` (hagyományos), `Bold` (félkövér), `Italic` (dőlt) vagy `Heavy` (vastag).
`lang`	A betűkészlet által támogatott nyelv, német esetén például `de`, japán esetén `ja`, hagyományos kínai esetén `zh-TW`, egyszerűsített kínai esetén pedig `zh-CN`.
`weight`	A betűkészlet vastagsága, normál betűkészlet esetén `80`, félkövér esetén `200`.
`slant`	A dőltség mértéket jelöli, `0` esetén nem dőlt, `100` esetén dőlt.
`file`	A betűkészletet tartalmazó fájl neve.
`outline`	Körvonalas betűkészlet esetén `igaz`, más betűkészletek esetén `hamis`.
`scalable`	Méretezhető betűkészletek esetén `igaz`, másfajta betűkészletek esetén `hamis`.
`bitmap`	Bitképes betűkészlet esetén `igaz`, más betűkészletek esetén `hamis`.
`pixelsize`	A betűk mérete képpontban. Az fc-list paranccsal kapcsolatban ennek a paraméternek csak bitképes betűkészletek esetén van értelme.

10.3 További információk

Az X11-gyel kapcsolatos további, részletesebb információkért telepítse az `xorg-x11-doc` és `howtoenh` csomagokat. Az X11 fejlesztésével kapcsolatos további információ a projekt weboldalán (`http://www.x.org`) olvasható.

Az `xorg-x11-driver-video` csomag számos illesztőprogramját leírja egy kézikönyvoldal. Ha például a `radeon` illesztőprogramot használja, további információt a `man 4 radeon` oldal tartalmaz.

A külső gyártók illesztőprogramjairól az `/usr/share/doc/packages/<csomag_neve>` könyvtárban kell, hogy legyen információ. Például az `x11-video-nvidiaG01` dokumentációja az `/usr/share/doc/packages/x11-video-nvidiaG01` könyvtárban található a csomag telepítése után.

Rendszerfelügyeleti segédprogramok

11

A rendszer állapotának vizsgálatára számos program és mechanizmus használható; ezek közül mutatunk be néhányat az alábbiakban. Leírunk néhány gyakori, a rutinfeladatok elvégzése során használt segédprogramot is a legfontosabb paraméterekkel együtt.

Minden bemutatott parancsnál megtalálhatók a vonatkozó kimenetek példái is. Ezekben a példákban az első sor maga a parancs (a > vagy # karakterrel jelzett prompt után). A megjegyzéseket szögletes zárójel (`[...]`) jelöli, és ha szükséges, a hosszú sorokat megtörtük. A hosszú sorok sortöréseit visszafelé dőlt törtvonal (`\`) jelzi.

```
# command -x -y
output line 1
output line 2
output line 3 is annoyingly long, so long that \
    we have to break it
output line 3
[...]
output line 98
output line 99
```

A leírásokat rövidre szabtuk, hogy annyi segédprogramról eshessen szó, amennyiről csak lehetséges. A parancsokról további információ a kézikönyvoldalakon (man) olvasható. A legtöbb parancs kiadható a `--help` paraméterrel is; ennek hatására kiírja a használható paraméterek rövid listáját.

11.1 Hibakeresés

11.1.1 A kívánt könyvtár megadása: ldd

Az `ldd` parancs annak megkeresésére használható, hogy milyen dinamikus könyvtárakat tölt be az argumentumként megadott végrehajtható fájl.

```
tux@mercury:~> ldd /bin/ls
        linux-vdso.so.1 =>  (0x00007fffbe7fe000)
        librt.so.1 => /lib64/librt.so.1 (0x00007f55b639d000)
        libacl.so.1 => /lib64/libacl.so.1 (0x00007f55b6195000)
        libc.so.6 => /lib64/libc.so.6 (0x00007f55b5e3d000)
        libpthread.so.0 => /lib64/libpthread.so.0 (0x00007f55b5c21000)
        /lib64/ld-linux-x86-64.so.2 (0x00007f55b65a6000)
        libattr.so.1 => /lib64/libattr.so.1 (0x00007f55b5a1c000)
```

A statikus bináris állományoknak egyetlen dinamikus könyvtárra sincs szükségük.

```
tux@mercury:~> ldd /bin/sash
        not a dynamic executable
tux@mercury:~> file /bin/sash
/bin/sash: ELF 64-bit LSB executable, x86-64, version 1 (SYSV), for GNU/Linux
 2.6.4, statically linked, stripped
```

11.1.2 Egy programfuttatás könyvtárhívásai: ltrace

Az `ltrace` parancs lehetővé teszi egy folyamat könyvtárhívásainak követését. A parancs hasonló módon használható, mint az `strace`. A `-c` paraméter kijelzi a könyvtárhívások számát és időtartamát.

```
tux@mercury:~> ltrace -c find ~
% time     seconds  usecs/call     calls      function
------ ----------- ----------- --------- --------------------
 34.37    6.758937         245     27554 __errno_location
 33.53    6.593562         788      8358 __fprintf_chk
 12.67    2.490392         144     17212 strlen
 11.97    2.353302         239      9845 readdir64
  2.37    0.466754          27     16716 __ctype_get_mb_cur_max
  1.17    0.230765          27      8358 memcpy
[...]
  0.00    0.000036          36         1 textdomain
------ ----------- ----------- --------- --------------------
100.00   19.662715                105717 total
```

11.1.3 Egy programfuttatás rendszerhívásai: strace

Az `strace` segédprogram segít egy futó program összes rendszerhívásának nyomon követésében. Adjon meg egy parancsot a szokásos módon, de az elejére írja oda, hogy `strace`:

```
tux@mercury:~> strace ls
execve("/bin/ls", ["ls"], [/* 61 vars */]) = 0
uname({sys="Linux", node="mercury", ...}) = 0
brk(0)                                  = 0x805c000
access("/etc/ld.so.preload", R_OK)      = -1 ENOENT (No such file or \
    directory)
open("/etc/ld.so.cache", O_RDONLY)      = 3
fstat64(3, {st_mode=S_IFREG|0644, st_size=89696, ...}) = 0
mmap2(NULL, 89696, PROT_READ, MAP_PRIVATE, 3, 0) = 0xb7ef2000
close(3)                                = 0
open("/lib/librt.so.1", O_RDONLY)       = 3
read(3, "\177ELF\1\1\1\0\0\0\0\0\0\0\0\0\3\0\3\0\1\0\0\0000\36\0"..., 512) \
   = 512
fstat64(3, {st_mode=S_IFREG|0755, st_size=36659, ...}) = 0
[...]
stat64(1, {st_mode=S_IFCHR|0620, st_rdev=makedev(136, 0), ...}) = 0
mmap2(NULL, 4096, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) \
    = 0xb7ca7000
write(1, "bin  Desktop  Documents  music\tM"..., 55bin  Desktop  Documents \
   \  music       Music  public_html  tmp
) = 55
close(1)                                = 0
munmap(0xb7ca7000, 4096)                = 0
exit_group(0)                           = ?
```

Egy adott fájl megnyitására történt kísérletek nyomon követéséhez például írja be a következőt:

```
tux@mercury:~> strace -e open ls .bashrc
open("/etc/ld.so.cache", O_RDONLY)      = 3
open("/lib/librt.so.1", O_RDONLY)       = 3
open("/lib/libacl.so.1", O_RDONLY)      = 3
open("/lib/libc.so.6", O_RDONLY)        = 3
open("/lib/libpthread.so.0", O_RDONLY)  = 3
open("/lib/libattr.so.1", O_RDONLY)     = 3
[...]
```

Az összes leszármazott folyamat nyomon követéséhez használja a `-f` paramétert. Az strace viselkedése és kimeneti formátumai nagymértékben szabályozhatók. További információ: `man strace`.

11.2 Fájlok és fájlrendszerek

11.2.1 Fájltípus meghatározása: fájl

A `file` meghatározza egy fájl (vagy fájlok listájának a) típusát az `/etc/magic` fájl alapján.

```
tux@mercury:~> file /usr/bin/file
/usr/bin/file: ELF 64-bit LSB executable, x86-64, version 1 (SYSV), \
    for GNU/Linux 2.6.4, dynamically linked (uses shared libs), stripped
```

A `-f` *`lista`* paraméter a megvizsgálandó fájlnevek listáját tartalmazó fájlt határoz meg. A `-z` paraméter hatására a `file` tömörített fájlok belsejébe is belenéz:

```
tux@mercury:~> file /usr/share/man/man1/file.1.gz
usr/share/man/man1/file.1.gz: gzip compressed data, from Unix, max compression
tux@mercury:~> file -z /usr/share/man/man1/file.1.gz
/usr/share/man/man1/file.1.gz: ASCII troff or preprocessor input text \
    (gzip compressed data, from Unix, max compression)
```

11.2.2 Fájlrendszerek és használatuk: mount, df és du

A `mount` parancs megmutatja, melyik fájlrendszer (eszköz és típus) van csatolva és melyik ponton:

```
tux@mercury:~> mount
/dev/sda3 on / type reiserfs (rw,acl,user_xattr)
proc on /proc type proc (rw)
sysfs on /sys type sysfs (rw)
udev on /dev type tmpfs (rw)
devpts on /dev/pts type devpts (rw,mode=0620,gid=5)
/dev/sda1 on /boot type ext2 (rw,acl,user_xattr)
/dev/sda4 on /local type reiserfs (rw,acl,user_xattr)
/dev/fd0 on /media/floppy type subfs (rw,nosuid,nodev,noatime,fs=floppyfss,p
```

A fájlrendszerek teljes kihasználtságáról a `df` paranccsal kaphat információt. A `-h` (vagy `--human-readable`) paraméter az átlagos felhasználó számára érthető formába önti a kimenetet.

```
tux@mercury:~> df -h
Filesystem            Size  Used Avail Use% Mounted on
/dev/sda3              11G  3.2G  6.9G  32% /
udev                  252M  104K  252M   1% /dev
/dev/sda1              16M  6.6M  7.8M  46% /boot
/dev/sda4              27G   34M   27G   1% /local
```

Egy adott könyvtárban az alkönyvtárakban található fájlok összméretének megjelenítéséhez adja ki a `du` parancsot. A `-s` paraméter elnyomja a részletes adatok kimenetét. Megint csak, a `-h` könnyen érthető formába önti az adatokat:

```
tux@mercury:~> du -sh /local
1.7M    /local
```

11.2.3 További információk az ELF bináris állományokról

A bináris állományok tartalma a `readelf` segédprogrammal olvasható. Ez még a más hardverarchitektúrákhoz készült ELF-fájlokkal is működik.

```
tux@mercury:~> readelf --file-header /bin/ls
ELF Header:
  Magic:   7f 45 4c 46 02 01 01 00 00 00 00 00 00 00 00 00
  Class:                             ELF64
  Data:                              2's complement, little endian
  Version:                           1 (current)
  OS/ABI:                            UNIX - System V
  ABI Version:                       0
  Type:                              EXEC (Executable file)
  Machine:                           Advanced Micro Devices X86-64
  Version:                           0x1
  Entry point address:               0x402430
  Start of program headers:          64 (bytes into file)
  Start of section headers:          98616 (bytes into file)
  Flags:                             0x0
  Size of this header:               64 (bytes)
  Size of program headers:           56 (bytes)
  Number of program headers:         9
  Size of section headers:           64 (bytes)
  Number of section headers:         31
  Section header string table index: 30
```

11.2.4 Fájltulajdonságok: stat

A `stat` parancs megjeleníti a fájltulajdonságokat:

```
tux@mercury:~> stat /etc/profile
  File: '/etc/profile'
  Size: 8080            Blocks: 16         IO Block: 4096   regular file
Device: 806h/2054d      Inode: 64942       Links: 1
Access: (0644/-rw-r--r--)  Uid: (    0/    root)   Gid: (    0/    root)
Access: 2007-07-16 23:28:18.000000000 +0200
Modify: 2006-09-19 14:45:01.000000000 +0200
Change: 2006-12-05 14:54:55.000000000 +0100
```

A `--filesystem` paraméter részletesen megadja annak a fájlrendszernek a tulajdonságait, amelyben a megadott fájl található:

```
tux@mercury:~> stat /etc/profile --filesystem
  File: "/etc/profile"
    ID: 0        Namelen: 255     Type: reiserfs
Block size: 4096       Fundamental block size: 4096
Blocks: Total: 2622526    Free: 1809771    Available: 1809771
Inodes: Total: 0          Free: 0
```

11.3 Hardverinformáció

11.3.1 PCI erőforrások: lspci

Az `lspci` parancs felsorolja a PCI-erőforrásokat:

```
mercury:~ # lspci
00:00.0 Host bridge: Intel Corporation 82845G/GL[Brookdale-G]/GE/PE \
    DRAM Controller/Host-Hub Interface (rev 01)
00:01.0 PCI bridge: Intel Corporation 82845G/GL[Brookdale-G]/GE/PE \
    Host-to-AGP Bridge (rev 01)
00:1d.0 USB Controller: Intel Corporation 82801DB/DBL/DBM \
    (ICH4/ICH4-L/ICH4-M) USB UHCI Controller #1 (rev 01)
00:1d.1 USB Controller: Intel Corporation 82801DB/DBL/DBM \
    (ICH4/ICH4-L/ICH4-M) USB UHCI Controller #2 (rev 01)
00:1d.2 USB Controller: Intel Corporation 82801DB/DBL/DBM \
    (ICH4/ICH4-L/ICH4-M) USB UHCI Controller #3 (rev 01)
00:1d.7 USB Controller: Intel Corporation 82801DB/DBM \
    (ICH4/ICH4-M) USB2 EHCI Controller (rev 01)
00:1e.0 PCI bridge: Intel Corporation 82801 PCI Bridge (rev 81)
00:1f.0 ISA bridge: Intel Corporation 82801DB/DBL (ICH4/ICH4-L) \
    LPC Interface Bridge (rev 01)
00:1f.1 IDE interface: Intel Corporation 82801DB (ICH4) IDE \
```

```
    Controller (rev 01)
00:1f.3 SMBus: Intel Corporation 82801DB/DBL/DBM (ICH4/ICH4-L/ICH4-M) \
    SMBus Controller (rev 01)
00:1f.5 Multimedia audio controller: Intel Corporation 82801DB/DBL/DBM \
    (ICH4/ICH4-L/ICH4-M) AC'97 Audio Controller (rev 01)
01:00.0 VGA compatible controller: Matrox Graphics, Inc. G400/G450 (rev 85)
02:08.0 Ethernet controller: Intel Corporation 82801DB PRO/100 VE (LOM) \
    Ethernet Controller (rev 81)
```

A `-v` paraméter használata részletesebb felsorolást eredményez:

```
mercury:~ # lspci -v
[...]
02:08.0 Ethernet controller: Intel Corporation 82801DB PRO/100 VE (LOM)\
    Ethernet Controller (rev 81)
        Subsystem: Fujitsu Siemens Computer GmbH: Unknown device 1001
        Flags: bus master, medium devsel, latency 66, IRQ 11
        Memory at d1000000 (32-bit, non-prefetchable) [size=4K]
        I/O ports at 3000 [size=64]
        Capabilities: [dc] Power Management version 2
```

Az eszközök nevének feloldásáról az `/usr/share/pci.ids` ad információt. Az ebben a fájlban fel nem sorolt PCI-azonosítók „Unknown device” (ismeretlen eszköz) megjelölést kapnak.

A `-vv` paraméter minden, egy program által lekérdezhető információt megad. Tisztán numerikus értékek megadásához a `-n` paramétert kell használni.

11.3.2 USB-eszközök: lsusb

Az `lsusb` parancs kilistázza az összes USB-eszközt. A `-v` paraméter hatására részletesebb listát ír ki. A részletes adatokat a `/proc/bus/usb/` könyvtárból olvassa a program. A következőkben az `lsusb` parancs kimenete látható, a következő csatlakoztatott USB-eszközök esetén: USB elosztó, pendrive, merevlemez és egér.

```
mercury:/ # lsusb
Bus 004 Device 007: ID 0ea0:2168 Ours Technology, Inc. Transcend JetFlash \
    2.0 / Astone USB Drive
Bus 004 Device 006: ID 04b4:6830 Cypress Semiconductor Corp. USB-2.0 IDE \
    Adapter
Bus 004 Device 005: ID 05e3:0605 Genesys Logic, Inc.
Bus 004 Device 001: ID 0000:0000
Bus 003 Device 001: ID 0000:0000
Bus 002 Device 001: ID 0000:0000
Bus 001 Device 005: ID 046d:c012 Logitech, Inc. Optical Mouse
Bus 001 Device 001: ID 0000:0000
```

11.4 Hálózatok

11.4.1 A hálózat állapotának megjelenítése: netstat

A `netstat` a hálózati kapcsolatokat, az útválasztási táblát (`-r`), a csatolókat (`-i`), a maszkolási kapcsolatokat (`-M`), a multicast-tagságokat (`-g`) és hálózati statisztikákat (`-s`) jeleníti meg.

```
tux@mercury:~> netstat -r
Kernel IP routing table
Destination     Gateway         Genmask         Flags  MSS Window  irtt Iface
192.168.2.0     *               255.255.254.0   U        0 0          0 eth0
link-local      *               255.255.0.0     U        0 0          0 eth0
loopback        *               255.0.0.0       U        0 0          0 lo
default         192.168.2.254   0.0.0.0         UG       0 0          0 eth0
```

```
tux@mercury:~> netstat -i
Kernel Interface table
Iface   MTU Met   RX-OK RX-ERR RX-DRP RX-OVR  TX-OK TX-ERR TX-DRP TX-OVR Flg
eth0   1500   0 1624507 129056      0      0   7055      0      0      0 BMNRU
lo    16436   0   23728      0      0      0  23728      0      0      0 LRU
```

A hálózati kapcsolatok és statisztikák megjelenítésekor megadható a megjeleníteni kívánt sockettípus: TCP (`-t`), UDP (`-u`) vagy nyers (`-r`). A `-p` paraméter a programok PID-jét és nevét jeleníti meg, amelyekhez az egyes socketek tartoznak.

Az alábbi példa kiírja az összes TCP-kapcsolatot, illetve az e kapcsolatokat használó programokat.

```
mercury:~ # netstat -t -p
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address  Foreign Address       State       PID/Pro

tcp      0      0 mercury:33513    www.novell.com:www-http ESTABLISHED 6862/fi
tcp      0    352 mercury:ssh      mercury2.:trc-netpoll     ESTABLISHED
19422/s
tcp      0      0 localhost:ssh  localhost:17828         ESTABLISHED -
```

A következőkben pedig a TCP protokoll statisztikái láthatók:

```
tux@mercury:~> netstat -s -t
Tcp:
    2427 active connections openings
    2374 passive connection openings
```

```
    0 failed connection attempts
    0 connection resets received
    1 connections established
    27476 segments received
    26786 segments send out
    54 segments retransmited
    0 bad segments received.
    6 resets sent
[...]
    TCPAbortOnLinger: 0
    TCPAbortFailed: 0
    TCPMemoryPressures: 0
```

11.5 A /proc fájlrendszer

A `/proc` fájlrendszer egy pszeudo-fájlrendszer, amelyben a kernel tárol fontos információkat virtuális fájlok formájában. A CPU típusa például ezzel a paranccsal jeleníthető meg:

```
tux@mercury:~> cat /proc/cpuinfo
processor       : 0
vendor_id       : GenuineIntel
cpu family      : 15
model           : 4
model name      : Intel(R) Pentium(R) 4 CPU 3.40GHz
stepping        : 3
cpu MHz         : 2800.000
cache size      : 2048 KB
physical id     : 0
[...]
```

A megszakítások kiosztása és használata a következő paranccsal kérdezhető le:

```
tux@mercury:~> cat /proc/interrupts
           CPU0
  0:    3577519          XT-PIC  timer
  1:        130          XT-PIC  i8042
  2:          0          XT-PIC  cascade
  5:     564535          XT-PIC  Intel 82801DB-ICH4
  7:          1          XT-PIC  parport0
  8:          2          XT-PIC  rtc
  9:          1          XT-PIC  acpi, uhci_hcd:usb1, ehci_hcd:usb4
 10:          0          XT-PIC  uhci_hcd:usb3
 11:      71772          XT-PIC  uhci_hcd:usb2, eth0
 12:     101150          XT-PIC  i8042
 14:      33146          XT-PIC  ide0
 15:     149202          XT-PIC  ide1
NMI:          0
LOC:          0
```

```
ERR:          0
MIS:          0
```

Néhány fontos fájl és tartalma:

`/proc/devices`
: a rendelkezésre álló eszközök

`/proc/modules`
: a betöltött kernelmodulok

`/proc/cmdline`
: kernel paranccsor

`/proc/meminfo`
: részletes adatok a memóriahasználatról

`/proc/config.gz`
: a jelenleg futó kernel `gzip`-pel tömörített konfigurációs fájlja

További információ az`/usr/src/linux/Documentation/filesystems/proc.txt` szövegfájlban található (ez a fájl a `kernel-source` csomag telepítése után érhető el). A jelenleg futó folyamatok adatai a `/proc/`*NNN* könyvtárakban találhatók meg, ahol az *NNN* a vonatkozó folyamatok folyamatazonosítója (PID-je). A folyamatok saját jellemzőiket a `/proc/self/` könyvtárakban találhatják meg:

```
tux@mercury:~> ls -l /proc/self
lrwxrwxrwx 1 root root 64 2007-07-16 13:03 /proc/self -> 5356
tux@mercury:~> ls -l /proc/self/
total 0
dr-xr-xr-x 2 tux users 0 2007-07-16 17:04 attr
-r-------- 1 tux users 0 2007-07-16 17:04 auxv
-r--r--r-- 1 tux users 0 2007-07-16 17:04 cmdline
lrwxrwxrwx 1 tux users 0 2007-07-16 17:04 cwd -> /home/tux
-r-------- 1 tux users 0 2007-07-16 17:04 environ
lrwxrwxrwx 1 tux users 0 2007-07-16 17:04 exe -> /bin/ls
dr-x------ 2 tux users 0 2007-07-16 17:04 fd
-rw-r--r-- 1 tux users 0 2007-07-16 17:04 loginuid
-r--r--r-- 1 tux users 0 2007-07-16 17:04 maps
-rw------- 1 tux users 0 2007-07-16 17:04 mem
-r--r--r-- 1 tux users 0 2007-07-16 17:04 mounts
-rw-r--r-- 1 tux users 0 2007-07-16 17:04 oom_adj
-r--r--r-- 1 tux users 0 2007-07-16 17:04 oom_score
lrwxrwxrwx 1 tux users 0 2007-07-16 17:04 root -> /
-rw------- 1 tux users 0 2007-07-16 17:04 seccomp
-r--r--r-- 1 tux users 0 2007-07-16 17:04 smaps
```

```
-r--r--r-- 1 tux users 0 2007-07-16 17:04 stat
[...]
dr-xr-xr-x 3 tux users 0 2007-07-16 17:04 task
-r--r--r-- 1 tux users 0 2007-07-16 17:04 wchan
```

A végrehajtható fájlok és könyvtárak címhozzárendelését a `maps` fájl tartalmazza:

```
tux@mercury:~> cat /proc/self/maps
08048000-0804c000 r-xp 00000000 03:03 17753      /bin/cat
0804c000-0804d000 rw-p 00004000 03:03 17753      /bin/cat
0804d000-0806e000 rw-p 0804d000 00:00 0          [heap]
b7d27000-b7d5a000 r--p 00000000 03:03 11867      /usr/lib/locale/en_GB.utf8/
b7d5a000-b7e32000 r--p 00000000 03:03 11868      /usr/lib/locale/en_GB.utf8/
b7e32000-b7e33000 rw-p b7e32000 00:00 0
b7e33000-b7f45000 r-xp 00000000 03:03 8837       /lib/libc-2.3.6.so
b7f45000-b7f46000 r--p 00112000 03:03 8837       /lib/libc-2.3.6.so
b7f46000-b7f48000 rw-p 00113000 03:03 8837       /lib/libc-2.3.6.so
b7f48000-b7f4c000 rw-p b7f48000 00:00 0
b7f52000-b7f53000 r--p 00000000 03:03 11842      /usr/lib/locale/en_GB.utf8/
[...]
b7f5b000-b7f61000 r--s 00000000 03:03 9109       /usr/lib/gconv/gconv-module
b7f61000-b7f62000 r--p 00000000 03:03 9720       /usr/lib/locale/en_GB.utf8/
b7f62000-b7f76000 r-xp 00000000 03:03 8828       /lib/ld-2.3.6.so
b7f76000-b7f78000 rw-p 00013000 03:03 8828       /lib/ld-2.3.6.so
bfd61000-bfd76000 rw-p bfd61000 00:00 0          [stack]
ffffe000-fffff000 ---p 00000000 00:00 0          [vdso]
```

11.5.1 procinfo

A `/proc` fájlrendszer fontos adatainak összefoglalására szolgál a `procinfo` parancs:

```
tux@mercury:~> procinfo
Linux 2.6.18.8-0.5-default (geeko@buildhost) (gcc 4.1.2 20061115) #1 2CPU

Memory:      Total        Used        Free      Shared     Buffers
Mem:       2060604     2011264       49340           0      200664
Swap:      2104472         112     2104360

Bootup: Tue Jul 10 10:29:15 2007    Load average: 0.86 1.10 1.11 3/118 21547

user  :       2:43:13.78   0.8%  page in :   71099181  disk 1:  2827023r 968
nice  :   1d 22:21:27.87  14.7%  page out:  690734737
system:      13:39:57.57   4.3%  page act:  138388345
IOwait:      18:02:18.59   5.7%  page dea:   29639529
hw irq:       0:03:39.44   0.0%  page flt: 9539791626
sw irq:       1:15:35.25   0.4%  swap in :         69
idle  :   9d 16:07:56.79  73.8%  swap out:        209
uptime:   6d 13:07:11.14         context :  542720687

irq  0: 141399308 timer          irq 14:   5074312 ide0
```

```
irq  1:     73784 i8042          irq 50:   1938076 uhci_hcd:usb1, ehci_
irq  4:         2                irq 58:         0 uhci_hcd:usb2
irq  6:         5 floppy [2]     irq 66:    872711 uhci_hcd:usb3, HDA I
irq  7:         2                irq 74:        15 uhci_hcd:usb4
irq  8:         0 rtc            irq 82: 178717720 0         PCI-MSI  e
irq  9:         0 acpi           irq169:  44352794 nvidia
irq 12:         3                irq233:   8209068 0         PCI-MSI  l
```

Az összes információ megjelenítéséhez használja a `-a` paramétert. A `-nN` paraméter minden *N* másodpercben frissíti az adatokat. Ebben az esetben a program lezárásához nyomja meg a Q billentyűt.

Alapértelmezésben az összesített adatok kerülnek megjelenítésre. A `-d` paraméter különbségi értékeket szolgáltat. A `procinfo -dn5` az utolsó öt másodpercben módosult adatokat jeleníti meg:

11.6 Folyamatok

11.6.1 Folyamatközi kommunikáció: ipcs

Az `ipcs` parancs megadja az aktuálisan használt IPC-erőforrások listáját:

```
------ Shared Memory Segments --------
key        shmid      owner     perms      bytes      nattch     status
0x00000000 58261504   tux    600        393216     2          dest
0x00000000 58294273   tux    600        196608     2          dest
0x00000000 83886083   tux    666        43264      2
0x00000000 83951622   tux    666        192000     2
0x00000000 83984391   tux    666        282464     2
0x00000000 84738056   root      644        151552     2          dest

------ Semaphore Arrays --------
key        semid      owner     perms      nsems
0x4d038abf 0          tux    600        8

------ Message Queues --------
key        msqid      owner      perms      used-bytes   messages
```

11.6.2 Folyamatlista: ps

A `ps` parancs folyamatlistát készít. A legtöbb paraméter mínuszjel nélkül is megadható. A `ps --help` parancs egy rövidített súgóoldalt jelenít meg, a kézikönyvoldalon pedig részletes súgó található.

Az összes folyamat kiíratásához a felhasználói és parancssori információkkal adja ki a `ps axu` parancsot:

```
tux@mercury:~> ps axu
USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.0  0.0    696   272 ?        S    12:59   0:01 init [5]
root         2  0.0  0.0      0     0 ?        SN   12:59   0:00 [ksoftirqd
root         3  0.0  0.0      0     0 ?        S<   12:59   0:00 [events
[...]
tux    4047  0.0  6.0 158548 31400 ?        Ssl  13:02   0:06 mono-best
tux    4057  0.0  0.7   9036  3684 ?        Sl   13:02   0:00 /opt/gnome
tux    4067  0.0  0.1   2204   636 ?        S    13:02   0:00 /opt/gnome
tux    4072  0.0  1.0  15996  5160 ?        Ss   13:02   0:00 gnome-scre
tux    4114  0.0  3.7 130988 19172 ?        SLl  13:06   0:04 sound-juic
tux    4818  0.0  0.3   4192  1812 pts/0    Ss   15:59   0:00 -bash
tux    4959  0.0  0.1   2324   816 pts/0    R+   16:17   0:00 ps axu
```

Annak ellenőrzésére például, hogy hány `sshd` folyamat fut, használja a `-p` paramétert a `pidof` paranccsal, amelyik megjeleníti az adott folyamat folyamatazonosítóját (PID-jét).

```
tux@mercury:~> ps -p $(pidof sshd)
  PID TTY      STAT   TIME COMMAND
 3524 ?        Ss     0:00 /usr/sbin/sshd -o PidFile=/var/run/sshd.init.pid
 4813 ?        Ss     0:00 sshd: tux [priv]
 4817 ?        R      0:00 sshd: tux@pts/0
```

A folyamatlista az igényeknek megfelelően formázható. A `-L` paraméter visszaadja a kulcsszavak listáját. Adja meg a következő parancsot a folyamatok kiíratásához, memóriahasználat szerint rendezve:

```
tux@mercury:~> ps ax --format pid,rss,cmd --sort rss
  PID   RSS CMD
    2     0 [ksoftirqd/0]
    3     0 [events/0]
    4     0 [khelper]
    5     0 [kthread]
   11     0 [kblockd/0]
   12     0 [kacpid]
  472     0 [pdflush]
  473     0 [pdflush]
[...]
```

```
 4028 17556 nautilus --no-default-window --sm-client-id default2
 4118 17800 ksnapshot
 4114 19172 sound-juicer
 4023 25144 gnome-panel --sm-client-id default1
 4047 31400 mono-best --debug /usr/lib/beagle/Best.exe --autostarted
 3973 31520 mono-beagled --debug /usr/lib/beagle/BeagleDaemon.exe --bg --aut
```

11.6.3 Folyamatfa: pstree

A `pstree` parancs fa formában állítja elő a folyamatok listáját:

```
tux@mercury:~> pstree
init-+-NetworkManagerD
     |-acpid
     |-3*[automount]
     |-cron
     |-cupsd
     |-2*[dbus-daemon]
     |-dbus-launch
     |-dcopserver
     |-dhcpcd
     |-events/0
     |-gpg-agent
     |-hald-+-hald-addon-acpi
     |      `-hald-addon-stor
     |-kded
     |-kdeinit-+-kdesu---su---kdesu_stub---yast2---y2controlcenter
     |         |-kio_file
     |         |-klauncher
     |         |-konqueror
     |         |-konsole-+-bash---su---bash
     |         |         `-bash
     |         `-kwin
     |-kdesktop---kdesktop_lock---xmatrix
     |-kdesud
     |-kdm-+-X
     |     `-kdm---startkde---kwrapper
[...]
```

A `-p` paraméter hozzáadja a folyamatazonosítót egy adott névhez. Ha a parancssorokat is szeretné megjeleníteni, használja a `-a` paramétert:

11.6.4 Folyamatok: top

A `top` parancs (a "table of processes", folyamattábla kifejezésből) megjelenít egy folyamatlistát, amely két másodpercenként frissül. A program lezárásához nyomja meg

a Q gombot. A `-n 1` paraméter a folyamatlista egyetlen megjelenése után lezárja a programot. Az alábbiakban egy példa a `top -n 1` parancs kimenetére:

```
tux@mercury:~> top -n 1
top - 17:06:28 up  2:10,  5 users,  load average: 0.00, 0.00, 0.00
Tasks:  85 total,   1 running,  83 sleeping,   1 stopped,   0 zombie
Cpu(s):  5.5% us,  0.8% sy,  0.8% ni, 91.9% id,  1.0% wa,  0.0% hi,  0.0% si
Mem:    515584k total,   506468k used,     9116k free,    66324k buffers
Swap:   658656k total,        0k used,   658656k free,   353328k cached

  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
    1 root      16   0   700  272  236 S  0.0  0.1   0:01.33 init
    2 root      34  19     0    0    0 S  0.0  0.0   0:00.00 ksoftirqd/0
    3 root      10  -5     0    0    0 S  0.0  0.0   0:00.27 events/0
    4 root      10  -5     0    0    0 S  0.0  0.0   0:00.01 khelper
    5 root      10  -5     0    0    0 S  0.0  0.0   0:00.00 kthread
   11 root      10  -5     0    0    0 S  0.0  0.0   0:00.05 kblockd/0
   12 root      20  -5     0    0    0 S  0.0  0.0   0:00.00 kacpid
  472 root      20   0     0    0    0 S  0.0  0.0   0:00.00 pdflush
  473 root      15   0     0    0    0 S  0.0  0.0   0:00.06 pdflush
  475 root      11  -5     0    0    0 S  0.0  0.0   0:00.00 aio/0
  474 root      15   0     0    0    0 S  0.0  0.0   0:00.07 kswapd0
  681 root      10  -5     0    0    0 S  0.0  0.0   0:00.01 kseriod
  839 root      10  -5     0    0    0 S  0.0  0.0   0:00.02 reiserfs/0
  923 root      13  -4  1712  552  344 S  0.0  0.1   0:00.67 udevd
 1343 root      10  -5     0    0    0 S  0.0  0.0   0:00.00 khubd
 1587 root      20   0     0    0    0 S  0.0  0.0   0:00.00 shpchpd_event
 1746 root      15   0     0    0    0 S  0.0  0.0   0:00.00 w1_control
 1752 root      15   0     0    0    0 S  0.0  0.0   0:00.00 w1_bus_master1
 2151 root      16   0  1464  496  416 S  0.0  0.1   0:00.00 acpid
 2165 messageb  16   0  3340 1048  792 S  0.0  0.2   0:00.64 dbus-daemon
 2166 root      15   0  1840  752  556 S  0.0  0.1   0:00.01 syslog-ng
 2171 root      16   0  1600  516  320 S  0.0  0.1   0:00.00 klogd
 2235 root      15   0  1736  800  652 S  0.0  0.2   0:00.10 resmgrd
 2289 root      16   0  4192 2852 1444 S  0.0  0.6   0:02.05 hald
 2403 root      23   0  1756  600  524 S  0.0  0.1   0:00.00 hald-addon-acpi
 2709 root      19   0  2668 1076  944 S  0.0  0.2   0:00.00 NetworkManagerD
 2714 root      16   0  1756  648  564 S  0.0  0.1   0:00.56 hald-addon-stor
```

Ha megnyomja az F billentyűt a `top` futtatása közben, akkor megjelenik egy menü, amellyel jelentősen módosítható a kimenet formátuma.

A `-U` *`UID`* paraméter csak egy adott felhasználóhoz rendelt folyamatokat figyeli. Helyettesítse be az *`UID`* értéket a felhasználó azonosítójával. A `top -U $(id -u)` parancs visszaadja a felhasználó azonosítóját a felhasználónév alapján, és megjeleníti a folyamatait.

11.6.5 Egy folyamat nice értékének módosítása: nice és renice

A kernel azt, hogy mely folyamatok igényelnek több CPU-időt, mint a többiek, a folyamat úgynevezett 'nice'-szintje ("kedvessége") alapján állapítja meg. Mennél magasabb a folyamat nice-szintje, annál kevesebb CPU-időt vehet el más folyamatoktól. A nice értékek -20-tól (ez a legalacsonyabb „nice” szint) 19-ig mehetnek. Negatív értékeket csak a `root` állíthat be.

A nice-szint módosítása hasznos például, ha egy rendszeren, amelyen egyéb feladatok is futnak, egy nagy, nem időkritikus folyamatot futtat, amely sokáig tart és sok CPU-időt igényel (ilyen például a kernelfordítás). Egy ilyen folyamat nice-szintjének „emelésével” garantálható, hogy a többi feladat, például a webkiszolgáló, magasabb prioritást élvezhet.

A `nice` paraméterek nevű meghívása kiírja az aktuális nice-értéket.

```
tux@mercury:~> nice
0
```

A `nice` *`parancs_neve`* parancs 10-zel megnöveli az adott parancs nice-értékét. A `nice –n` *`szint parancs_neve`* paranccsal az előzőhöz képest relatíve módosítható az adott parancs nice-értéke.

Egy folyamat nice-értékének módosításához használja a `renice` *`prioritás`* `–p` *`folyamatazonosító`* parancsot, például:

```
renice +5 3266
```

Egy adott felhasználó összes folyamatának a `–u` *`felhasználó_neve`* paranccsal lehet módosítani a nice-értékét. A folyamatcsoportok nice-értékének módosításához használja a `–g` *`folyamatcsoport_azonosítója`* parancsot.

11.7 Rendszeradatok

11.7.1 Memóriahasználat: free

A `free` segédprogram megvizsgálja a RAM-használatot. A kimenetben mind a szabad, mind a használt memória (és a csereterületek) részletes adatai láthatók:

```
tux@mercury:~> free
             total       used       free     shared    buffers     cached
Mem:       2062844    2047444      15400          0     129580     921936
-/+ buffers/cache:     995928    1066916
Swap:      2104472          0    2104472
```

A `-b`,`-k`,`-m`,`-g` paraméterek a kimenetet bájtokban, kilobájtokban, megabájtokban ill. gigabájtokban jelenítik meg. A `-d késleltetés` paraméter hatására a képernyő *`késleltetés`* másodpercenként frissül. A `free -d 1.5` parancs például másfél másodpercenként frissíti a képernyőt.

11.7.2 Adott fájlokat használó felhasználók: fuser

Ez a parancs annak eldöntésére lehet hasznos, hogy jelenleg milyen folyamatok vagy felhasználók használnak bizonyos fájlokat. Tegyük fel például, hogy le szeretné csatolni az `/mnt` könyvtárhoz csatolt fájlrendszert. Az `umount` parancs kimenete: "device is busy" (az eszköz foglalt). Ekkor az `fuser` paranccsal meg lehet állapítani, mely folyamatok is használják pillanatnyilag az eszközt:

```
tux@mercury:~> fuser -v /mnt/*

                     USER        PID ACCESS COMMAND
/mnt/notes.txt       tux     26597 f....  less
```

A `less` folyamat lezárását követően (amely egy másik terminálon futott), a fájlrendszer sikeresen lecsatolható.

11.7.3 Kernel gyűrűpuffer: dmesg

A Linux-kernel számos üzenetet tárol egy gyűrűpufferben. Ezen üzenetek megtekintésére szolgál a `dmesg` parancs:

```
$ dmesg
[...]
end_request: I/O error, dev fd0, sector 0
subfs: unsuccessful attempt to mount media (256)
e100: eth0: e100_watchdog: link up, 100Mbps, half-duplex
NET: Registered protocol family 17
IA-32 Microcode Update Driver: v1.14 <tigran@veritas.com>
microcode: CPU0 updated from revision 0xe to 0x2e, date = 08112004
IA-32 Microcode Update Driver v1.14 unregistered
bootsplash: status on console 0 changed to on
NET: Registered protocol family 10
Disabled Privacy Extensions on device c0326ea0(lo)
IPv6 over IPv4 tunneling driver
powernow: This module only works with AMD K7 CPUs
bootsplash: status on console 0 changed to on
```

A régebbi események a `/var/log/messages` és `/var/log/warn` fájlokban vannak naplózva.

11.7.4 Nyitott fájlok listája: lsof

Egy adott folyamatazonosítóval (*PID*) rendelkező folyamathoz tartozó összes nyitott fájl listájának megtekintéséhez használja a `-p` paramétert. Ha például látni szeretné az aktuális parancsértelmező által használt összes fájlt, írja be a következőket:

```
tux@mercury:~> lsof -p $$
COMMAND  PID   USER   FD   TYPE DEVICE    SIZE   NODE NAME
bash    5552 tux  cwd    DIR    3,3    1512 117619 /home/tux
bash    5552 tux  rtd    DIR    3,3     584      2 /
bash    5552 tux  txt    REG    3,3  498816  13047 /bin/bash
bash    5552 tux  mem    REG    0,0       0 [heap] (stat: No such
bash    5552 tux  mem    REG    3,3  217016 115687 /var/run/nscd/passwd
bash    5552 tux  mem    REG    3,3  208464  11867 /usr/lib/locale/en_GB.
bash    5552 tux  mem    REG    3,3  882134  11868 /usr/lib/locale/en_GB.
bash    5552 tux  mem    REG    3,3 1386997   8837 /lib/libc-2.3.6.so
bash    5552 tux  mem    REG    3,3   13836   8843 /lib/libdl-2.3.6.so
bash    5552 tux  mem    REG    3,3  290856  12204 /lib/libncurses.so.5.5
bash    5552 tux  mem    REG    3,3   26936  13004 /lib/libhistory.so.5.1
bash    5552 tux  mem    REG    3,3  190200  13006 /lib/libreadline.so.5.
bash    5552 tux  mem    REG    3,3      54  11842 /usr/lib/locale/en_GB.
bash    5552 tux  mem    REG    3,3    2375  11663 /usr/lib/locale/en_GB.
bash    5552 tux  mem    REG    3,3     290  11736 /usr/lib/locale/en_GB.
```

```
bash    5552 tux  mem    REG    3,3      52  11831 /usr/lib/locale/en_GB.
bash    5552 tux  mem    REG    3,3      34  11862 /usr/lib/locale/en_GB.
bash    5552 tux  mem    REG    3,3      62  11839 /usr/lib/locale/en_GB.
bash    5552 tux  mem    REG    3,3     127  11664 /usr/lib/locale/en_GB.
bash    5552 tux  mem    REG    3,3      56  11735 /usr/lib/locale/en_GB.
bash    5552 tux  mem    REG    3,3      23  11866 /usr/lib/locale/en_GB.
bash    5552 tux  mem    REG    3,3   21544   9109 /usr/lib/gconv/gconv-m
bash    5552 tux  mem    REG    3,3     366   9720 /usr/lib/locale/en_GB.
bash    5552 tux  mem    REG    3,3   97165   8828 /lib/ld-2.3.6.so
bash    5552 tux    0u   CHR  136,5             7 /dev/pts/5
bash    5552 tux    1u   CHR  136,5             7 /dev/pts/5
bash    5552 tux    2u   CHR  136,5             7 /dev/pts/5
bash    5552 tux  255u   CHR  136,5             7 /dev/pts/5
```

A speciális `$$` parancsértelmező-változót használtuk, amelynek az értéke az aktuális parancsértelmező folyamatazonosítója.

Az `lsof` parancs paraméterek nélkül kiadva minden éppen nyitott fájlt felsorol. Mivel gyakran fájlok ezrei vannak nyitva, mindegyiket ritkán érdemes kilistázni. Az összes fájl listája azonban a keresési funkciókkal kombinálva hasznos listákat eredményez. Ilyen például az összes karakteres eszköz listája:

```
tux@mercury:~> lsof | grep CHR
bash      3838     tux    0u      CHR  136,0                2 /dev/pts/0
bash      3838     tux    1u      CHR  136,0                2 /dev/pts/0
bash      3838     tux    2u      CHR  136,0                2 /dev/pts/0
bash      3838     tux  255u      CHR  136,0                2 /dev/pts/0
bash      5552     tux    0u      CHR  136,5                7 /dev/pts/5
bash      5552     tux    1u      CHR  136,5                7 /dev/pts/5
bash      5552     tux    2u      CHR  136,5                7 /dev/pts/5
bash      5552     tux  255u      CHR  136,5                7 /dev/pts/5
X         5646       root  mem       CHR    1,1            1006 /dev/mem
lsof      5673     tux    0u      CHR  136,5                7 /dev/pts/5
lsof      5673     tux    2u      CHR  136,5                7 /dev/pts/5
grep      5674     tux    1u      CHR  136,5                7 /dev/pts/5
grep      5674     tux    2u      CHR  136,5                7 /dev/pts/5
```

11.7.5 Kernel és udev eseménysorozat-megjelenítő: udevadm monitor

Az `udevadm monitor` a kernel üeventeket és az udev szabályok által kibocsátott eseményeket figyeli és kinyomtatja az eseményben érintett eszköz elérési útját (DEV-

PATH) a konzolra. Egy USB-pendrive csatlakoztatásával kapcsolatos események sorozata:

```
UEVENT[1138806687] add@/devices/pci0000:00/0000:00:1d.7/usb4/4-2/4-2.2
UEVENT[1138806687] add@/devices/pci0000:00/0000:00:1d.7/usb4/4-2/4-2.2/4-2.2
UEVENT[1138806687] add@/class/scsi_host/host4
UEVENT[1138806687] add@/class/usb_device/usbdev4.10
UDEV  [1138806687] add@/devices/pci0000:00/0000:00:1d.7/usb4/4-2/4-2.2
UDEV  [1138806687] add@/devices/pci0000:00/0000:00:1d.7/usb4/4-2/4-2.2/4-2.2
UDEV  [1138806687] add@/class/scsi_host/host4
UDEV  [1138806687] add@/class/usb_device/usbdev4.10
UEVENT[1138806692] add@/devices/pci0000:00/0000:00:1d.7/usb4/4-2/4-2.2/4-2.2
UEVENT[1138806692] add@/block/sdb
UEVENT[1138806692] add@/class/scsi_generic/sg1
UEVENT[1138806692] add@/class/scsi_device/4:0:0:0
UDEV  [1138806693] add@/devices/pci0000:00/0000:00:1d.7/usb4/4-2/4-2.2/4-2.2
UDEV  [1138806693] add@/class/scsi_generic/sg1
UDEV  [1138806693] add@/class/scsi_device/4:0:0:0
UDEV  [1138806693] add@/block/sdb
UEVENT[1138806694] add@/block/sdb/sdb1
UDEV  [1138806694] add@/block/sdb/sdb1
UEVENT[1138806694] mount@/block/sdb/sdb1
UEVENT[1138806697] umount@/block/sdb/sdb1
```

11.8 Felhasználó adatai

11.8.1 Ki mit csinál: w

A `w` parancs megjeleníti, hogy ki van bejelentkezve a rendszerre és ki mit csinál éppen. Például:

```
tux@mercury:~> w
 14:58:43 up 1 day,  1:21,  2 users,  load average: 0.00, 0.00, 0.00
USER     TTY        LOGIN@   IDLE   JCPU   PCPU WHAT
tux      :0        12:25   ?xdm?   1:23   0.12s /bin/sh /usr/bin/startkde
root     pts/4     14:13    0.00s  0.06s  0.00s w
```

Ha a felhasználók bármelyike távolról jelentkezett be, akkor a `-f` megjeleníti a számítógépeket, amelyekről a kapcsolatot létesítették.

11.9 Idő és dátum

11.9.1 Időmérés a time paranccsal

A parancsok által felhasznált idő a `time` segédprogrammal mérhető. Ez a segédprogram két verzióban létezik: mint egy parancsértelmező beépített része, és mint program (`/usr/bin/time`).

```
tux@mercury:~> time find . > /dev/null

real    0m4.051s
user    0m0.042s
sys     0m0.205s
```

A rendszer frissítése és módosításai

12

Egy meglévő rendszer frissíthető anélkül, hogy teljesen újra kellene telepíteni. Kétféle frissítési módszer létezik: *az egyes szoftvercsomagok frissítése* és a *teljes rendszer frissítése*.

12.1 A rendszer frissítése

A szoftverek jellemzően minden egyes verziójukban egyre nagyobbra „nőnek”. Éppen ezért frissítés előtt érdemes szemügyre venni a rendelkezésre álló területet a `df` paranccsal. Ha sejti, hogy nem lesz elég a merevlemez-terület, akkor mentse el az adatokat a frissítés előtt és particionálja újra a rendszert. Nincs általános ökölszabály arra nézve, hogy mekkorának kell lenniük az egyes partícióknak. A helyigény az Ön saját partíciós profiljától, a kiválasztott szoftverektől és a rendszer verziószámától függ.

12.1.1 Előkészületek

Frissítés előtt másolja át a régi konfigurációs fájlokat egy másik adathordozóra, például szalagra, cserélhető merevlemezre, vagy USB-meghajtóra. Ez elsősorban az `/etc` könyvtár fájljaira, illetve a `/var` könyvtár bizonyos alkönyvtáraira és fájljaira vonatkozik. Célszerű lementeni a `/home` könyvtárban található felhasználói adatokat (a `HOME`, azaz saját könyvtárakat) is. Ezeket az adatokat `root` felhasználóként mentse el. Csak a `root` jogosult az összes helyi fájl olvasására.

A frissítés megkezdése előtt jegyezze fel a gyökérpartíciót. A `df /` parancs kiírja a gyöképartíció eszköznevét. A következő példában (12.1. példa - Listázás a `df -h` paranccsal (166. oldal)) a leírandó gyökérpartíció a `/dev/sda3` (ez a fájlrendszer `/` része).

12.1 példa *Listázás a df -h paranccsal*

```
Filesystem      Size  Used Avail Use% Mounted on
/dev/sda3        74G   22G   53G  29% /
udev            252M  124K  252M   1% /dev
/dev/sda5       116G  5.8G  111G   5% /home
/dev/sda1        39G  1.6G   37G   4% /windows/C
/dev/sda2       4.6G  2.6G  2.1G  57% /windows/D
```

12.1.2 Lehetséges problémák

Ha egy alapértelmezett rendszert frissít az előző verzióról erre a verzióra, akkor a YaST kikeresi a szükséges változtatásokat és végrehajtja őket. A testreszabás mértékétől függően azonban egyes lépések, vagy akár a teljes frissítési folyamat meghiúsulhat, és lehet, hogy vissza kell másolni majd az elmentett adatokat. Itt megemlítünk néhány további dolgot, amit érdemes ellenőrizni a rendszer frissítésének megkezdése előtt.

A passwd és group fájlok ellenőrzése az /etc könyvtárban

A rendszer frissítése előtt győződjön meg róla, hogy az `/etc/passwd` és `/etc/group` fájlok nem tartalmaznak szintaktikai hibákat. E célból `root` felhasználóként indítsa el a `pwck` és `grpck` ellenőrző segédprogramot, és ha hibát észlel, javítsa azokat.

PostgreSQL

A PostgreSQL (`postgres`) frissítése előtt mentse le az adatbázisokat. Tekintse meg a `pg_dump` kézikönyvoldalát (man). Erre csak akkor van szükség, ha a PostgreSQL-t ténylegesen használta is a frissítés előtt.

12.1.3 Frissítés a YaST segítségével

Az 12.1.1. - Előkészületek (165. oldal) előkészületi eljárásait követve most már frissíthető a rendszer:

1. Indítsa el a rendszert ugyanúgy, mint az új telepítés esetében (1.4. - System Start-Up for Installation (1. fejezet - *Installation with YaST*, ↑*Start-Up*)). A YaST-ban válasszon ki egy nyelvet és válassza ki a *Telepítési mód* párbeszédablakban a *Frissítés* menüpontot. Ne válassza az *Új telepítés* menüpontot. Vegyen fel forrásokat azért, hogy az összes lehetséges szoftver biztosan frissüljön, amikor csak lehetséges. A forrásokról további információk: 1.7.1. - Add-On Products (1. fejezet - *Installation with YaST*, ↑*Start-Up*).

2. A YaST megállapítja, hogy van-e egynél több gyökérpartíció. Ha csak egy van, folytatja a következő lépéssel. Ha több van, akkor válassza ki a megfelelő partíciót és erősítse meg a *Tovább* gomb megnyomásával. (A `/dev/sda3` volt kiválasztva a 12.1.1. - Előkészületek (165. oldal) részben található példában.) A YaST beolvassa a partíció régi `fstab` fájlját és annak alapján elemzi, majd felcsatolja a felsorolt fájlrendszereket.

3. Ha voltak előzőleg használt források, akkor ellenőrizze azokat. Engedélyezze az összes olyan forrást, amit továbbra is használni kíván, és frissítse az ezekből származó külső gyártós szoftvereket. Kattintson az *Állapot átkapcsolása* pontra a lista minden szükséges eleménél.

4. Ha a frissítési folyamat során a fentiekben ajánlottak szerint felvette a forrásokat, akkor most aktiválhatja azokat, amelyek ténylegesen érdekesek.

5. A *Telepítési beállítások* párbeszédablakban módosítsa a beállításokat az igényeknek megfelelően. Normál esetben nyugodtan lehet az alapértelmezett beállításokat úgy hagyni, ahogy vannak, de ha bővíteni kívánja a rendszert, akkor jelölje meg a *Szoftverválaszték* almenüjeiben megjelölt csomagokat, vagy vegyen fel támogatást további nyelvekhez.

   Van lehetőség a különféle rendszerkomponensek elmentésére is. A biztonsági mentések kiválasztása lelassítja a frissítési folyamatot. Akkor használja ezt a lehetőséget, ha a közelmúltban nem készített biztonsági mentést.

6. Erősítse meg szándékát a *Frissítés megkezdése* gombra kattintva.

Amikor az alapszintű frissítések telepítése befejeződött, tesztelje az internetkapcsolatot, ahogy azt a YaST párbeszédablak ajánlja. A YaST legvégül frissíti a maradék szoftvereket, felajánlja a Novell Customer Center beállítását és megjeleníti a kiadási megjegyzéseket. A YaST konfiguráció írásának befejezéséhez kattintson a *Befejezés* gombra.

További Novell Customer Center információ: „Registration” szakasz (1. fejezet - *Installation with YaST*, ↑*Start-Up*).

12.1.4 Egyedi csomagok frissítése

A teljes frissített környezettől függetlenül mindig frissíthetők az egyedi csomagok is. Ettől kezdve azonban az Ön felelőssége annak biztosítása, hogy a rendszer konzisztens maradjon. Frissítési tanácsok: `http://www.novell.com/linux/download/updates/`.

Válassza ki az összetevőket a YaST csomagválasztási listájából igény szerint. Ha a rendszer általános működéséhez szükséges csomagot választ, a YaST figyelmeztető üzenetet jelenít meg. Az ilyen csomagok csak frissítési módban frissíthetők. Sok csomag tartalmaz például *megosztott függvénytárakat*. Ha ezeket a programokat és alkalmazásokat a futó rendszeren frissítené, az hibát okozhatna.

12.2 Szoftverváltozások az egyes verziók között

Az alábbiakban részletesen áttekintjük, hogy mi is változott az előző verziók óta. Az összegzésben jelezzük, ha például teljesen átalakultak az alapbeállítások, ha a konfigurációs fájlok más helyre kerültek, vagy ha a megszokott alkalmazások lényeges mértékben változtak. Megemlítjük az összes lényeges módosítást, amely akár a felhasználók, akár a rendszergazda napi munkáját befolyásolja.

Ha egy adott változattal kapcsolatban valamilyen problémára derül fény vagy speciális kérdések vetődnek fel, akkor ez bekerül az online dokumentációba. A hivatkozásokat lásd alább. Az egyedi csomagok fontos frissítései a `http://www.novell.com/products/linuxprofessional/downloads/` weboldalon érhetők el a YaST Online frissítés eszközével. További információkért lásd: 5. fejezet - *YaST online frissítés* (75. oldal).

12.2.1 10.1 - 10.2

Keresse a „Hibák” szócikket az openSUSE wikiben, a következő címen: `http://en.opensuse.org/Bugs`.

A normál kernel

A `kernel-default` csomag tartalmazza az egy- és többprocesszoros rendszerek normál kernelét is. A kernel beépített SMP-támogatással rendelkezik és az egyprocesszoros rendszereken minimális többletterheléssel fut. Már nincs `kernel-smp` csomag.

Kiegészítő adathordozó egyéb nyelvekkel

Ha jobb támogatást szeretne valamelyik 2. rétegbeli nyelvhez, akkor vegye be a kiegészítő adathordozót a telepítési források listájába. 2. rétegbeli nyelveknek nevezünk minden nyelvet, kivéve az 1. rétegbeli nyelveket: az angolt, a franciát, a németet, az olaszt, a spanyolt, a brazil portugált, az egyszerűsített és hagyományos kínait, a japánt és a csehet. Az 1. rétegbeli nyelvek támogatása a szabványos adathordozókészleten található.

12.2.2 10.2 - 10.3

Tájékozódjon az openSUSE wiki `Hibák` szócikkéből, a következő weboldalon: `http://en.opensuse.org/Bugs`.

Szöveges telepítési minta

A szöveges telepítési minta hatóköre igen korátozott. Kiegészítő szoftverek hozzáadása nélkül nem ajánlott a minta telepítése. Csomagok hozzáadása más mintákból. A minta feladata, hogy legyen egy valódi hardveren futó minimális indítható rendszer. Ezt elindítva egy többfelhasználós rendszert kap, amely helyi bejelentkezési és hálózati beállítási szolgáltatásokat kínál, valamint rendelkezik az alapértelmezett fájlrendszerekkel. Alapértelmezésben semmilyen szolgáltatás nincs engedélyezve és csak a telepítés során szükséges YaST-modulok vannak telepítve.

Kiegészítő szoftverforrások hozzáadása a telepítés során

Amikor a telepítés végén beállította a frissítési konfigurációt, a YaST felajánlja a következő három szoftverforrás felvételét kiegészítő telepítés forrásként:

- Az „oss” forrás a teljes FTP-disztribúciót tartalmazza, beleértve további, a CD-ken található csomagokat is.
- A „non-oss” forrás jogvédett vagy nem nyílt forráskódú licenccel használható szoftvereket tartalmaz.
- A „debug” forrás a programok és könyvtárak hibakereséséhez, valamint a visszakövetéshez használható debuginfo csomagokat tartalmazza. Hiba esetén ez a kiegészítő információ segít a megfelelő hibajelentések írásában.

Az „oss” forrás RPM-jeinek helye: `http://download.opensuse.org/distribution/10.3/src-oss`, a „non-oss” forrás RPM-jeinek helye: `http://download.opensuse.org/distribution/10.3/src-non-oss`.

Honosítási támogatás

Az egy CD-s telepítési adathordozó (GNOME vagy KDE) csak amerikai angol nyelvi támogatást tartalmaz.

A többi nyelv támogatása külön érhető el. Ha Önnek más nyelvek is érdekesek, akkor a fordításokhoz külön online forrásokat kell felvennie. A „Kiegészítő szoftverforrások hozzáadása a telepítés során” szakasz (170. oldal) részben említett „oss” például egy ilyen forrás.

AppArmor 2.1

Az új funkciókról bővebben: `http://en.opensuse.org/AppArmor/Changes_AppArmor_2_1`

A szintaxis mostantól megkülönbözteti a könyvtárakat a fájloktól. Bekerült néhány kisebb szintaktikai hibajavítás.

Változások történtek a change_hat események és információk jelentéskészítésénél. A naplóüzenetek és profilállapot (a via /proc/<pid>/attr/current fájlban található) jelentése mostantól: `/profile//hat`.

A rendszer egy új change_profile irányelv-specifikációval bővült. A change_profile hasonló a change_hat-hez, de lehetővé teszi az összes profil módosítását (a "kalap"-okat is). A módosítható profilokat meg kell határozni, ez az egyetlen korlátozás. Egy kalap módosításához a change_profile segítségével, a kalap nevét is meg kell adni, a profil és a kalap nevét `//` karakterrel elválasztva.

A GAIM új neve Pidgin

A GAIM azonnali üzenettovábbító program új nevet kapott, mostantól Pidginnek hívják.

A KDE és a GNOME új helye

A GNOME 2 az openSUSE 10.3 óta az `/usr` fájlrendszerbe telepítődik, mostantól a KDE 4 is követi ebben. A KDE 3 kompatibilitási okokból az `/opt` fájlrendszerben marad.

A frissítés megkezdése előtt győződjön meg róla, hogy az `/usr` fájlrendszerben elég üres hely van. (Kb. 2,5 gigabájtra van szüksége mind a két asztali környezetnek.) Ha az `/usr` alatt nincs elég hely, akkor méretezze át vagy rendezze át a partíciókat.

A Berkeley DB változásai érintik az OpenLDAP kiszolgálót

A Berkeley adatbázis 4.3-as és 4.4-es változatánál más a lemezen található naplófájlok formátuma. Emiatt a rendszer frissítése után a telepített OpenLDAP kiszolgáló nem tud elindulni.

Ennek a problémának a kiküszöböléséhez exportálja a meglévő LDAP-adatbázisokat a `slapcat` segédprogrammal még a rendszerfrissítés megkezdése *előtt*, majd importálja vissza az adatokat a frissítés után a `slapadd` eszközzel. Egy már frissített gépen az LDP Server a következőképpen bírható működésre:

1. Állítsa le az LDAP-kiszolgálót.

2. Távolítsa el az összes `_db.` karakterekkel kezdődő fájlt az adatbáziskönyvtárból.

3. Indítsa újra az LDAP-kiszolgálót.

libata IDE-eszközökhöz

A libata az első merevlemezhez a `/dev/sda` fájlrendszert használja a `/dev/hda` helyett. Mostantól nem automatikus a 15-nél több partícióval rendelkező lemezek kezelése. A libata támogatás letiltható, ha a rendszerindítás a következő kernelparaméterrel történik:

```
hwprobe=-modules.pata
```

Innentől újra láthatja a 15 fölötti összes partíciót, illetve használhatja azokat a telepítéshez.

A titkosított partíciók létesítésének változásai

A `boot.crypto` mögötti háttértechnológia `cryptoloop`-ról `dm-crypt`-re változott.

Minden régi `/etc/cryptotab` partíció módosítás nélkül futtatható az openSUSE 10.3 változatán (a `hd`*X*-ről `sd`*X*-re történő átnevezésekkel kapcsolatban a libata változásai miatt adódhatnak gondok —lásd: „libata IDE-eszközökhöz” szakasz (172. oldal)). Emellett a rendszer mostantól támogatja az `/etc/crypttab` használatát (figyeljen a hiányzó `o` betűre!), amibe a LUKS kötetek támogatása is beletartozik. Az előző kiadásokkal szemben a `boot.crypto` alapértelmezésben nincs engedélyezve. Ennek engedélyezéséről a YaST gondoskodik, ha azzal csinál titkosított kötetet. Kézzel is engedélyezhető, a következő parancs használatával:

```
chkconfig boot.crypto on
```

A cryptoloop továbbra is használható a `losetup` és a `mount` segítségével. Mivel elhagytuk a primitív loop-AES javítást a util-linux csomagból, az `losetup` néhány paramétere (mint az `itercountk` és a `pseed`) már nem létezik. Ha ezeknek a beállításoknak bármelyike szerepel az `/etc/fstab` fájlban, akkor az eszköz többé nem csatolható fel közvetlenül. Helyezze át ezeket a beállításokat az `/etc/crypttab` fájlba, ahol a `boot.crypto` tartalmazza a szükséges kompatibilitási kódot.

A kvótatámogatás engedélyezése

Mostantól a felhasználói fiókokhoz kvóták állíthatók be a YaST-on belül. Ez a funkció a *Kvótatámogatás engedélyezése* jelölőnégyzet kijelölésével aktiválható az fstab beállításoknál, a telepítés első szakaszában, a particionálásnál. Ez gondoskodik róla, hogy a rendszerindításkor lefusson az `/etc/init.d/boot.quota` parancsfájl. A második szakaszban a felhasználói fiókok speciális beállításai biztosítják a quota modult, ha a kvótaszabályok be vannak állítva.

Ha a telepítés után, a futó rendszeren a particionálóban engedélyezi a kvótatámogatást, akkor vagy újra kell indítani a rendszert vagy kézzel fel kell csatolni az érintett partíciókat és `root`-ként végre kell hajtani a következő parancsot:

```
/etc/init.d/boot.quota restart
```

Zeroconf

A Zeroconf szolgáltatás – amelyet ezen kívül Bonjour, Multicast DNS, mDNS vagy DNS-SD néven is ismernek – mostantól az Avahi csomag része, nem az mDNSResponderé. Az mDNSResponder azonban továbbra is rendelkezésre áll és a howl kompatibilitási könyvtárak is elérhetők.

Ha engedélyezni szeretné az mDNS-t az összes hálózati csatolóhoz, használja a *Zeroconf/Bonjour Multicast DNS* SuSEfirewall2 szabályt.

Régebbi Intel grafikus lapkák

A régebbi Intel grafikus lapkák támogatását két illesztőprogram látja el: az i810 és az intel. Mivel komoly igény volt az olyan funkciók iránt, mint a natív módú (és többé nem a VESA BIOS alapú) beállítás és az RANDR 1.2 támogatás, az intel illesztőprogram az openSUSE 10.3-on alapértelmezett.

Az openSUSE 10.3-as változatára frissítéskor az i810 illesztőprogramot a rendszer nem cseréli le az intel illesztőprogramra. Ha át szeretne állni az intel illesztőprogramra, használja a `sax2 -r` parancsot.

Az intel illesztőprogram még mindig nem olyan stabil, mint az i810. A `sax2 -r -m 0=i810` paranccsal állhat vissza az i810-re, ha olyan problémákat észlel, amelyeket

azelőtt nem tapasztalt. Ezekben az esetekben érdemes lehet hibajelentést nyitni az intel illesztőprogrammal kapcsolatban.

Intel WiFi-illesztőprogramok

Jelenleg két illesztőprogam áll rendelkezésre: a hagyományos, alapértelmezésként települő `ipw3945`, illetve alternatív megoldásként az új `iwlwifi` illesztő. Figyeljen a következő buktatókra:

- Az `ipw3945` működik a rejtett hálózatok esetében, de nem éli túl a felfüggesztés/folytatási ciklust.
- Az `iwlwifi` nem működik a rejtett hálózatokkal, de támogatja a felfüggesztési/folytatási ciklusokat.

Az alapértelmezés a YaST használatával módosítható. Kattintson a *Szoftver* > *Szoftverkezelés* lehetőségre és távolítsa el az `ipw3945d` csomagot. Ettől kezdve automatikusan az alternatívát jelentő `iwlwifi` illesztőprogram lesz kiválasztva a telepítéshez.

Eszközök optikai lemezek (CD-ROM és DVD) írásához

Ebből a disztribúcióból kikerült a cdrecord csomag. A cdrkit projekt új wodim, genisoimage és icedax csomagjai használhatók adatrögzítésre vagy audio-CD-k készítésére azokon a CD-írókon, amelyek megfelelnek az Orange Book szabványnak. A következő bináris állományok új nevet kaptak:

- cdrecord helyett wodim
- readcd helyett readom
- mkisofs helyett genisoimage
- cdda2wav helyett icedax

Ha az alkalmazása a régi neveken nyugszik, akkor telepítse a cdrkit-cdrtools-compat csomagot. Érdemes azonban az ügyféloldali alkalmazásokban gondoskodni a wodim natív használatának támogatásáról, mert tartalmaz tökéletesítéseket:

- Egy eszköz megadására a legjobb módszer a `dev=/dev/cdrecorder`, `dev=/dev/hdc`, `dev=/dev/sr0` stb.
- A rendelkezésre álló eszközök a `wodim –devices` használatával listázhatók.
- Nincs szükség a suid root parancsra.

Ha ilyen ügyféloldali alkalmazás vagy parancsfájl karbantartását végzi, érdemes számításba venni a natív wodim támogatás beépítését.

DVD-k írásához használja a `growisofs` alkalmazást. A grafikus felület ezt észrevétlenül kezeli.

KDE 4 alkalmazások elérési útvonala

Ha az induló openSUSE 10.3 telepítésnél nem telepítette a KDE asztali környezetet, akkor telepítse később a KDE Base System és KDE 4 Base System mintákat. Alapértelmezésként a rendszer a KDE 4 alkalmazáselérési útvonalat használja. Ha egy KDE-alkalmazást - pl. Konqueror - indít, akkor a KDE 3 változat helyett a Konqueror KDE 4 változata fog betöltődni.

MP3 fájlok lejátszása a Kaffeine szoftverben

Ha megnyit egy MP3 fájlt a Kaffeine alkalmazásban, akkor hibaüzenetet fog kapni, amely szerint a lejátszáshoz szükséges szoftver nincs telepítve. Ezután az openSUSE felajánlja, hogy keres egy megfelelő kodeket, amely a YaST-tal telepíthető. Az alrendszer is átállítható a Xine-ről Gstreamer-re a *Beállítások* > *Lejátszó alrendszer* menüpontra kattintva, az MP3-támogatás biztosításához.

12.2.3 10.3 - 11.0

Tájékozódjon az openSUSE wiki `Hibák` szócikkéből, a következő weboldalon: `http://en.opensuse.org/Bugs`.

A sysstat új lemezformátuma

A sysstat csomagnak a 11.0-s verzióban megjelent új funkciói miatt meg kellett változtatni a lemezen tárolt adatfájlok formátumát. A sysstat csomag frissítése után a régi összegyűjtött adatok már nem használhatók.

IV. rész - Rendszer

32 és 62 bites alkalmazások 64 bites rendszerkörnyezetben

13

Az openSUSE 64 bites platformokon is használható. Ez azonban nem jelenti feltétlenül azt, hogy az összes mellékelt alkalmazás is át lett írva 64 bites platformra. Az openSUSE támogatja 32 bites alkalmazások használatát 64 bites rendszerkörnyezetben. Ez a fejezet röviden áttekinti, hogy ez a támogatás hogyan is lett megvalósítva a 64 bites openSUSE platformokon. Bemutatjuk, hogyan történik a 32 bites alkalmazások végrehajtása (futási támogatás), illetve hogyan kell lefordítani a 32 bites alkalmazásokat, hogy egyaránt lehessen őket futtatni mind 32, mind 64 bites rendszerkörnyezetekben. Található továbbá itt információ a kernel API-ról is, valamint magyarázat arról, hogy hogyan futnak a 32 bites alkalmazások 64 bites kernel alatt.

A 64 bites amd64 és Intel 64 platformokhoz készült openSUSE úgy lett kialakítva, hogy a meglévő 32 bites alkalmazások a 64 bites környezetben a „dobozból kivéve”, azonnal futnak. Ez a támogatás azt jelenti, hogy a preferált 32 bites alkalmazások továbbra is használhatók, nem kell várni a megfelelő 64 bites átírás megjelenésére.

13.1 Futási támogatás

FONTOS: Alkalmazásverziók közötti ütközések

Ha egy alkalmazás 32 és 64 bites környezethez egyaránt rendelkezésre áll, mindkét verzió egyidejű telepítése valószínűleg problémát okoz. Ilyen esetben válasszon a verziók közül, majd azt telepítse és használja.

Kivételt jelentenek e szabály alól az ún. PAM-ok (pluggable authentication module, cserélhető hitelesítési modulok). Az a PAM (cserélhető hitelesítési

modulok) rendszert használja a hitelesítési folyamatban a felhasználó és az alkalmazás közötti rétegként. 32 bites alkalmazásokat is futtató 64 bites operációs rendszeren feltétlenül szükséges a PAM-modulok mindkét verzióját telepíteni.

A megfelelő végrehajtás érdekében minden alkalmazás függvénytárakat igényel. Sajnos, a könyvtárak 32 és 64 bites változatainak neve megegyezik. Ezeket valamilyen más módon kell megkülönböztetni.

A 32 bites verzióval való kompatibilitás fenntartása érdekében a függvénytárak ugyanott tárolódnak, mint a 32 bites környezetben. A `libc.so.6` 32 bites verziója 32 és 64 bites környezetben egyaránt a `/lib/libc.so.6` könyvtárban található.

A 64 bites függvénytárak és objektumfájlok a `lib64` nevű könyvtárban találhatók. A 64 bites objektumfájlok, amelyeket általában a `/lib` és `/usr/lib` könyvtárban keresnénk, a `/lib64` és `/usr/lib64` könyvtárban találhatók. Ez azt jelenti, hogy a `/lib` és `/usr/lib` alatt van hely a 32 bites könyvtárak számára, így mindkét verzió fájlneve változatlan marad.

A szómérettől független adatokat tartalmazó 32 bites `/lib` könyvtárak alkönyvtárai nem kerülnek áthelyezésre. Ez a séma megfelel az LSB (Linux Standards Base) és FHS (File System Hierarchy Standard) előírásoknak.

13.2 Szoftverfejlesztés

32 és 64 bites objektumok egyaránt előállíthatók a biarch fejlesztőkészlet-lánccal. Az alapértelmezés a 64 bites objektumok fordítása. 32 bites objektumok speciális jelzők használatával állíthatók elő. GCC esetén ez a speciális jelző az `-m32`.

Az összes header fájlt architektúrafüggetlen formátumban kell megírni. A telepített 32 és 64 bites függvénytáraknak rendelkezniük kell a telepített header fájloknak megfelelő API-val (alkalmazásprogramozási felület). A normál openSUSE környezet ennek az alapelvnek megfelelően került kialakításra. Kézzel frissített függvénytárak esetén ezeket a problémákat önállóan kell megoldani.

13.3 Szoftverfordítás biarch platformokon

Ha egy biarch architektúrán más architektúrára akar bináris fájlokat készíteni, akkor telepíteni kell a második architektúra megfelelő függvénytárait. Az ilyen csomagok neve `rpmname-32bit`. Az `rpmname-devel` csomagok megfelelő header fájljaira és függvénytáraira, illetve az `rpmname-devel-32bit` fejlesztési függvénytáraira is szükség van a második architektúrához.

A legtöbb nyílt forrású program egy `autoconf` alapú programkonfigurációt használ. Ha az `autoconf` parancs segítségével kíván beállítani egy programot a második architektúrához, a `configure` parancsfájl megfelelő környezeti változókkal futtatásával írja felül az `autoconf` normál fordító- és linkerbeállításait.

Az alábbi példa egy x86_64 rendszert mutat be, amelyen x86 a második architektúra.

1. 32 bites fordító használata:

```
CC="gcc -m32"
```

2. A linker utasítása 32 bites objektumok feldolgozására (mindig a gcc használata a linker előtétjeként):

```
LD="gcc -m32"
```

3. Az assembler beállítása 32 bites objektumok előállítására:

```
AS="gcc -c -m32"
```

4. Annak megadása, hogy a `libtool` függvénytárai és egyebei az `/usr/lib` könyvtárból kerüljenek ki:

```
LDFLAGS="-L/usr/lib"
```

5. Annak megadása, hogy a függvénytárak a `lib` alkönyvtárban tárolódjanak:

```
--libdir=/usr/lib
```

6. Annak megadása, hogy a 32 bites X függvénytárak kerüljenek alkalmazásra:

```
--x-libraries=/usr/lib/xorg
```

Nincs szükség az összes változóra minden programhoz. Használja őket az adott programnak megfelelően.

```
CC="gcc -m32"            \
LDFLAGS="-L/usr/lib;"  \
        .configure       \
          --prefix=/usr  \
          --libdir=/usr/lib
make
make install
```

13.4 Kernelspecifikációk

Az x86_64 64 bites kernelei 64 és 32 bites kernel ABI-t (alkalmazás bináris csatoló) is tartalmaznak. Az utóbbi a megfelelő 32 bites kernel ABI-jával azonos. Ez azt jelenti, hogy a 32 bites alkalmazás ugyanúgy tud kommunikálni a 64 bites kernellel, mint a 32 bites kernellel.

Egy 64 bites kernel rendszerhívásainak 32 bites emulációja nem támogatja a rendszerprogramok által használt API-k nagy részét. Ez a platformtól függ. Ez azt jelenti, hogy csak néhány alkalmazást, például az `lspci`-t kell lefordítani.

Egy 64 bites kernel csak speciálisan ehhez a kernelhez lefordított 64 bites kernelmodulokat tud betölteni. A 32 bites kernelmodulok nem használhatók.

TIPP

Néhány alkalmazás külön kernel által betölthető modulokat igényel. Ha ilyen 32 bites alkalmazást kíván használni egy 64 bites rendszerkörnyezetben, akkor keresse meg az alkalmazás gyártóját és a Novellt annak ellenőrzéséhez, hogy a kernel által betölthető modul 64 bites verziója és a kernel API 32 bites lefordított verziója rendelkezésre áll-e ehhez a modulhoz.

Linux-rendszerek indítása és beállítása

14

A Linux-rendszerek indítása összetett folyamat. A hardvert magát a BIOS inicializálja, majd utána a rendszertöltő segítségével elindítja a kernelt. E pont után a rendszerindítási folyamatot teljes egészében az operációs rendszer veszi át, az init és a futási szintek használatával. A futási szintek segítségével be lehet állítani a mindennapos használathoz, illetve a rendszer karbantartására szolgáló konfigurációkat.

14.1 A Linux rendszerindítási folyamata

A Linux rendszerindítási folyamata több szintből áll, amelyek mindegyikét más és más komponens végzi. Az alábbi lista röviden összefoglalja a rendszerindítási folyamatot és bemutatja az érintett fő komponensek jellemzőit.

1. **BIOS** A számítógép bekapcsolása után a BIOS inicializálja a képernyőt és billentyűzetet, majd teszteli a fő memóriát. Eddig a pontig a gép még semmilyen tömegtároló eszközhöz nem fért hozzá. Ezután az aktuális dátum és idő, illetve a legfontosabb perifériákra vonatkozó adatok betöltődnek a CMOS-ból. Az első merevlemez és annak geometriájának felismerése után a BIOS átadja a rendszervezérlést a rendszertöltőnek.

2. **Rendszertöltő** Az első merevlemez első 512 bájtos fizikai adatszektora betöltésre kerül a fő memóriába és a szektor elején található *rendszertöltő* átveszi az irányítást. A rendszertöltő által végrehajtott parancsok határozzák meg az indítási folyamat további részét. Az első merevlemez első 512 bájtját éppen ezért *Master*

Boot Record-nak (fő rendszertöltő rekord, MBR) hívjuk. A rendszertöltő ezután átadja az irányítást az aktuális operációs rendszernek, ebben az esetben a Linux-kernelnek. A GRUB-bal, a Linux rendszertöltőjével kapcsolatos további információ: 15. fejezet - *A rendszertöltő* (201. oldal)

3. **Kernel és initrd** A rendszervezérlés átadásához a rendszertöltő betölti a memóriába a kernelt és egy kezdeti, RAM alapú fájlrendszert (initramfs). Az initramfs tartalmát a kernel közvetlenül képes használni. Az initramfs része egy kisméretű, init nevű végrehajtható fájlt, amelyik a valódi root fájlrendszer felcsatolását végzi. Ha speciális hardverillesztő programokra van szükség még a fő tárolóeszköz elérése előtt, akkor annak szerepelnie kell az initramfs-ben. Az initramfs-sel kapcsolatos további információ: 14.1.1. - initramfs (184. oldal).

4. **init az initramfs-ben** Ez a program végzi el a megfelelő root fájlrendszer felcsatolásához szükséges összes műveletet: megfelelő kernelfunkciókat biztosít a használni kívánt fájlrendszerhez, illetve eszköz-illesztőprogramokat a tárolóvezérlőkhöz. Ha sikerült megtalálni, a root fájlrendszeren hibaellenőrzés történik, majd felcsatolja a rendszer. Ha ez is sikerült, akkor az initramfs törlődik és elindul a root fájlrendszeren lévő init program. További információ az init-ről: 14.1.2. - init az initramfs-ben (185. oldal) További információ az udev-ről: 17. fejezet - *Dinamikus kerneleszköz-felügyelet az udev segítségével* (237. oldal).

5. **init** Az init kezeli a rendszer tényleges indítását és lehetővé teszi különböző funkcionalitást biztosító szintek használatát. Az init részletes leírása: 14.2. - Az init folyamat (187. oldal)

14.1.1 initramfs

Az initramfs egy kisméretű cpio archívum, amelyet a kernel be tud tölteni a RAM-lemezre. Egy minimális Linux-rendszer található benne, amelyik lehetővé teszi programok végrehajtását még a tényleges root fájlrendszer felcsatolása előtt. Ezt a minimális Linux-rendszert BIOS-rutinok töltik be a memóriába. Az elegendő memórián kívül nincs egyéb hardverkövetelménye. Az initramfs-ben kell, hogy szerepeljen egy init nevű végrehajtható fájl, amely a root fájlrendszeren található tényleges init programot hajtja végre, hogy a rendszerindítási folyamat folytatódhasson.

A root fájlrendszer felcsatolása és az operációs rendszer elindítása előtt a kernelnek a root fájlrendszert tartalmazó eszköz eléréséhez szüksége van a megfelelő illesztőprogramokra. Lehet, hogy speciális illesztőprogramokra van szükség bizonyos típusú me-

revlemez-meghajtók vagy éppen a hálózati fájlrendszer eléréséhez. Az initramfs-ben található init be is töltheti a root fájlrendszerhez szükséges modulokat. A modulok betöltése után az udev biztosítja az initramfs-nek a szükséges eszközöket. A rendszerindítási folyamat későbbi részében, a root fájlrendszerre átváltás után újra kell generálni az eszközöket. Ezt a `boot.udev` végzi az `udevtrigger` parancs kiadásával.

Ha meg kell változtatni egy telepített rendszerben a hardvert (például a merevlemezeket), és az új hardver használatához más illesztőprogramokra van szükség, mint ami a kernel számára rendszerindításkor rendelkezésre áll, akkor frissíteni kell az initramfs-t. Ez ugyanúgy történik, mint az elődje, az initrd esetén: meg kell hívni az `mkinitrd` parancsot. Az `mkinitrd` paraméterek nélküli kiadása esetén egy initramfs jön létre. Az `mkinitrd -R` parancs pedig initrd-t hoz létre. Az openSUSE alatt a betöltendő modulokat az `/etc/sysconfig/kernel` fájlban található `INITRD_MODULES` változó adja meg. Telepítés után ez a változó automatikusan beállításra kerül a megfelelő értékre. A modulok pontosan abban a sorrendben lesznek betöltve, ahogy az `INITRD_MODULES` változóban meg vannak adva. Ez csak akkor fontos, ha a `/dev/sd` eszközfájlok megfelelő beállítására támaszkodik. Modern rendszerekben azonban használhatók a `/dev/disk/` alatti eszközfájlok is. Ezek több, `by-id`, `by-path` és `by-uuid` nevű könyvtárra vannak szétosztva, de mindig ugyanazt a lemezt ábrázolják. Ez telepítéskor is lehetséges a megfelelő mount paraméter megadásával.

FONTOS: Az initramfs vagy initrd frissítése

A rendszertöltő ugyanúgy tölti be az initramfs-t és initrd-t, mint a kernel. Az initramfs és initrd frissítése után a GRUB-ot nem kell újratelepíteni, mivel a GRUB indításkor a könyvtárban megkeresi a megfelelő fájlt.

14.1.2 init az initramfs-ben

Az initramfs-en található init fő célja a valódi root fájlrendszer felcsatolásának és elérésének előkészítése. Az aktuális rendszerkonfigurációtól függően az init az alábbi feladatokért felelős.

Kernelmodulok betöltése
: A hardverkonfigurációtól függően a számítógép hardverkomponenseinek (amelyek közül a legfontosabb a merevlemez) az eléréséhez speciális illesztőprogramokra lehet szükség. A végleges root fájlrendszer eléréséhez a kernelnek be kell töltenie a megfelelő fájlrendszer-illesztőprogramokat.

Blokk-speciális fájlok biztosítása

Minden egyes betöltött modulhoz a kernel eszközeseményeket generál. Ezeket az eseményeket az udev kezeli és hozza létre a blokk-speciális fájlokat a RAM-fájlrendszerben a `/dev` alatt. E speciális fájlok nélkül a fájlrendszer és a többi eszköz nem lenne elérhető.

RAID- és LVM-beállítások kezelése

Ha a rendszer úgy lett beállítva, hogy a root fájlrendszert RAID- vagy LVM-köteteken tárolja, akkor az init beállítja az LVM-et vagy a RAID-et, hogy a root fájlrendszer később elérhető legyen. További információ a RAID-ről és az LVM-ről: 2. fejezet - *Speciális lemezbeállítások* (41. oldal).

Hálózati beállítások

Ha a rendszer egy hálózaton (NFS-en) keresztül felcsatolt root fájlrendszer használatára lett beállítva, akkor ahhoz, hogy a root fájlrendszer később biztosan elérhető legyen, az init-nek ellenőriznie kell, hogy be vannak-e töltve és be vannak-e állítva a megfelelő hálózati illesztőprogramok.

Amikor az init a kezdeti rendszerindítás során, a telepítési folyamat részeként kerül meghívásra, akkor a feladatai különböznek a korábban említettektől:

Telepítési adathordozó megkeresése

A telepítési folyamat elindításakor a gép a telepítési adathordozóról a YaST telepítő segítségével betölt egy telepítési kernelt és egy speciális initrd-t. A RAM-fájlrendszerben futó YaST telepítőnek ismernie kell a telepítési adathordozó tényleges helyét, hogy elérhesse és telepíthesse az operációs rendszert.

Hardverfelismerés kezdeményezése és a megfelelő kernelmodulok betöltése

A rendszerindítási folyamat minimális illesztőprogram-készlettel indul (lásd 14.1.1. - initramfs (184. oldal)), amely a legtöbb hardverkonfigurációval használható. Az init elindít egy kezdeti hardverkeresési folyamatot, amely meghatározza a hardverkonfigurációhoz megfelelő illesztőprogramokat. A rendszerindítási folyamathoz szükséges modulok nevei az `/etc/sysconfig/kernel` fájl `INITRD_MODULES` változójába íródnak. Ezekből a nevekből generálódik a rendszer indításához szükséges egyéni initramfs. Ha a modulok rendszerindításhoz nem, de a coldplughoz szükségesek, akkor a modulok az `/etc/sysconfig/hardware/hwconfig-*` fájlokba íródnak. Az ebben a könyvtárban található összes eszközt a rendszerindítási folyamat inicializálja.

A telepítési vagy mentőrendszer betöltése
: A hardver megfelelő felismerése és a megfelelő illesztőprogramok betöltése után, illetve miután az udev létrehozta az eszközök speciális fájljait, az init elindítja az aktuális YaST telepítőt tartalmazó telepítőrendszert, illetve a mentőrendszert.

A YaST indítása
: Az init végül elindítja a YaST-ot, amely elkezdi a csomagok telepítését és a rendszer beállítását.

14.2 Az init folyamat

Az init program az 1-es folyamatszámú folyamat. Ez felelős a rendszer megfelelő inicializálásáért. Az init folyamatot közvetlenül a kernel indítja el és nem is hat rá a 9-es szignál, amely normál esetben leállítja a folyamatokat. Minden más folyamat az init vagy valamelyik leszármazott folyamatának leszármazottja.

Az init beállításai központilag vannak megadva az `/etc/inittab` fájlban. Itt vannak beállítva a *futási szintek* is (lásd 14.2.1. - Futási szintek (187. oldal)). Szintén ez a fájl határozza meg, hogy az egyes futási szinteken mely szolgáltatások és démonok álljanak rendelkezésre. Az `/etc/inittab` bejegyzéseitől függően az init számos parancsfájlt lefuttat. Alapértelmezés szerint a rendszerindítás után elsőként elinduló parancsfájl az `/etc/init.d/boot`. A rendszerinicializálási szakasz befejeztével a rendszer az `/etc/init.d/rc` parancsfájllal megváltoztatja a futási szintet az alapértelmezettre. Az áttekinthetőség érdekében e parancsfájlok (ún. *init parancsfájlok*) mindegyike az `/etc/init.d` könyvtárban található (lásd: 14.2.2. - Init parancsfájlok (190. oldal)).

A rendszerindítás és -leállítás teljes folyamatát az init tartja karban. E nézőpontból a kernel egy háttérfolyamatnak tekinthető, amelynek feladata az összes folyamat vezérlése és karbantartása, valamint a CPU-idő és a hardverhozzáférés beállítása a többi programtól érkező kéréseknek megfelelően.

14.2.1 Futási szintek

A Linux-rendszerekben a *futási szintek* határozzák meg a rendszer elindításának módját és a futó rendszerben rendelkezésre álló szolgáltatásokat. Rendszerindítás után a rendszer az `/etc/inittab` fájl `initdefault` sorában megadott módon kerül indításra. Ez általában `3` vagy `5`. Lásd:14.1 táblázat - A használható futási szintek (188. oldal). A

futási szint a rendszerindítás közben is megadható (például a rendszerindítási promptnál). Azokat a paramétereket, amelyeket nem közvetlenül a kernel értékel ki, az init kapja meg. Ha például 3-as szinten akarja indítani a rendszert, akkor a rendszerindítási promptnál adja meg a 3 paramétert (egyetlen hármast).

14.1. táblázat *A használható futási szintek*

Futási szint	Leírás
0	Rendszerleállás
S vagy 1	Egyfelhasználós mód
2	Több helyi felhasználós mód távoli hálózat (például NFS) nélkül
3	Teljes többfelhasználós mód hálózattal
4	*Felhasználó által meghatározható*: ez le van tiltva addig, amíg a rendszergazda be nem állítja ezt a futási szintet.
5	Teljes többfelhasználós mód hálózattal és X képernyőkezelővel – KDM (alapértelmezett), GDM vagy XDM
6	A rendszer újraindítása

FONTOS: Kerülje a 2-es futási szint használatát NFS-en keresztül felcsatolt partícióval.

A 2-es futási szintet nem kell használni, ha a rendszer NFS-en keresztül csatolja fel az `/usr` partíciót. Mivel az NFS szolgáltatás a 2-es futási szinten (több helyi felhasználós mód távoli hálózat nélkül) nem elérhető, a rendszer működése problémássá válhat, ha fontos program- vagy függvénytárfájlok hiányoznak.

A rendszer futása közben a futási szint a `telinit` paranccsal módosítható, a kívánt szint számát paraméterként megadva. Erre csak a rendszergazda jogosult. Az alábbi listában összefoglaljuk a futási szintekkel kapcsolatos legfontosabb parancsokat.

`telinit 1` vagy `shutdown now`
: A rendszer *egyfelhasználós módba* vált. Ez a mód rendszerkarbantartásra és -adminisztrációra használható.

`telinit 3`
: Elindul az összes lényeges program (a hálózat is), a normál felhasználók bejelentkezhetnek és X grafikus környezet nélkül használhatják a rendszert.

`telinit 5`
: A grafikus környezet is bekapcsolódik. Általában elindul egy képernyőkezelő, mint az XDM, GDM vagy KDM. Az automatikus bejelentkezés engedélyezése esetén a helyi felhasználó automatikusan bejelentkezik az előre kiválasztott ablakkezelőbe (GNOME, KDE, vagy bármely másik ablakkezelő).

`telinit 0` vagy `shutdown -h now`
: A rendszer leáll.

`telinit 6` vagy `shutdown -r now`
: A rendszer leáll, majd újraindul.

Az összes szokásos módon telepített openSUSE rendszerben az `5`-ös futási szint az alapértelmezett beállítás. A felhasználók közvetlenül a grafikus felületen jelentkeznek be, vagy az alapértelmezett felhasználót automatikusan bejelentkezteti a rendszer. Ha az alapértelmezett futási szint a `3`, akkor az `5`-ös szintre váltás előtt az X Window rendszert megfelelően be kell állítani (lásd: 10. fejezet - *Az X Window rendszer* (127. oldal)). Ha ez megtörtént, akkor a `telinit 5` parancs kiadásával ellenőrizze, hogy a rendszer megfelelően működik-e. Ha minden a várakozásnak megfelelően működik, akkor a YaST segítségével az alapértelmezett futási szint `5`-re állítható.

FIGYELEM: Az /etc/inittab fájl hibái sikertelen rendszerindítást eredményezhetnek.

Ha az `/etc/inittab` fájl megsérül, akkor elképzelhető, hogy a rendszer nem indul el megfelelően. Éppen ezért legyen nagyon körültekintő az `/etc/inittab` fájl módosításakor. Mindig olvastassa újra az init-tel az `/etc/inittab` fájlt: adja ki a `telinit q` parancsot a gép újraindítása előtt.

A futási szintek módosításakor általában két dolog történik. Először elindulnak az aktuális futási szinthez tartozó leállító parancsfájlok, amelyek bezárják az aktuális futási

szint működéséhez szükséges fontos programokat. Majd ezután elindulnak az új futási szint indító parancsfájljai. Itt a legtöbb esetben jónéhány program elindításra kerül. A 3-asról 5-ös szintre módosításkor például az alábbiak történnek:

1. Az adminisztrátor (`root`) a `telinit 5` parancs kiadásával utasítja az init-et a másik futási szintre váltásra.

2. Az init megvizsgálja az aktuális futási szintet (`runlevel`) és megállapítja, hogy az `/etc/init.d/rc` fájlt az új futási szint paraméterként megadásával kell elindítania.

3. Az `rc` ezután meghívja az aktuális futási szint leállító parancsfájljai közül azokat, amelyekhez az új futási szinten nem tartozik indító parancsfájl. A jelen példában ezek az `/etc/init.d/rc3.d` könyvtárban található parancsfájlok (az előző futási szint a 3-as volt) közül azok, amelyek neve `K` betűvel kezdődik. A `K` betű utáni szám határozza meg a parancsfájlok `stop` paraméterrel futtatásának a sorrendjét, ugyanis bizonyos függőségeket figyelembe kell venni.

4. Legutoljára pedig elindulnak az új futási szint indító parancsfájljai. A jelen példában ezek az `/etc/init.d/rc5.d` könyvtárban található, `S` betűvel kezdődő nevű fájlok. A parancsfájlok indításának sorrendjét megint az `S` utáni szám határozza meg.

Ha ugyanarra a futási szintre vált át, mint az éppen aktuális, akkor az init ellenőrzi az`/etc/inittab` és csupán a módosításoknak megfelelő lépéseket teszi meg (például elindítja a `getty` programot egy másik csatolón). Ugyanez az eredménye a `telinit q` parancs kiadásának is.

14.2.2 Init parancsfájlok

Az `/etc/init.d` könyvtárban kétféle parancsfájl található:

Az init által közvetlenül végrehajtott parancsfájlok
: Ez csak a rendszerindítási folyamat közben, vagy egy azonnali rendszerleállítás kezdeményezésekor áll fenn (áramellátási hiba esetén, vagy ha a felhasználó megnyomja a Ctrl + Alt + Del billentyűkombinációt). E parancsfájlok végrehajtását az `/etc/inittab` szabályozza.

Az init által közvetetten végrehajtott parancsfájlok

Ezek a futási szint módosításakor futnak le, és mindig az `/etc/init.d/rc` fő parancsfájlt hívják meg, amely garantálja az érintett parancsfájlok megfelelő sorrendjét.

Az összes parancsfájl az `/etc/init.d` könyvtárban található. A rendszerindításkor lefutó parancsfájlok szimbolikus láncokon keresztül kerülnek meghívásra az `/etc/init.d/boot.d` alkönyvtárból. A futási szint módosítására szolgáló parancsfájlok szintén szimbolikus láncokon keresztül kerülnek meghívásra az egyik alkönyvtárból (`/etc/init.d/rc0.d`-től `/etc/init.d/rc6.d`-ig). Ez csak a jobb átláthatóság érdekében van így, valamint hogy ne duplázódjanak a parancsfájlok, ha több futási szinten is használja őket a rendszer. Mivel minden parancsfájl végrehajtható indítási és leállítási parancsfájlként is, ezeknek a parancsfájloknak meg kell érteniük a `start` és `stop` paramétereket. A parancsfájlok a `restart`, `reload`, `force-reload` és `status` paraméterekre is reagálnak. Az egyes paraméterek leírása: 14.2 táblázat - A használható init parancsfájl-paraméterek (191. oldal). Az init által közvetlenül futtatott parancsfájlok nem rendelkeznek ilyen hivatkozásokkal. Ezek szükség esetén a futási szinttől függetlenül futnak le.

14.2. táblázat *A használható init parancsfájl-paraméterek*

Paraméter	Leírás
`start`	A szolgáltatás elindítása.
`stop`	A szolgáltatás leállítása.
`restart`	Ha a szolgáltatás fut, leállítja, majd újraindítja. Ha nem fut, akkor elindítja.
`reload`	Újratölti a konfigurációt a szolgáltatás leállítása és újraindítása nélkül.
`force-reload`	Újratölti a konfigurációt, ha a szolgáltatás támogatja ezt. Ellenkező esetben ugyanúgy viselkedik, mintha a `restart` paraméter lett volna megadva.
`status`	Megjeleníti a szolgáltatás aktuális állapotát.

A futásiszint-specifikus alkönyvtárban található láncok segítségével a parancsfájlok több futási szinthez is rendelhetők. Csomagok telepítésekor vagy eltávolításakor ezek a hivatkozások az insserv program segítségével adhatók hozzá vagy távolíthatók el (vagy az `/usr/lib/lsb/install_initd` parancsfájl segítségével, amely szintén ezt a programot hívja meg). Részletes információt erről az insserv(8) kézikönyvoldala tartalmaz.

E beállítások mindegyikét lehet módosítani a YaST modul segítségével is. Ha ellenőrizni kell parancssorban az állapotot, akkor használja a chkconfig eszközt. Ennek leírását a chkconfig(8) kézikönyvoldal tartalmazza.

Most pedig az elsőként vagy utolsóként elindított rendszerindító ill. -leállító parancsfájlok rövid leírása, valamint a karbantartási parancsfájl rövid bemutatása következik.

`boot`
: A rendszernek az init programmal történő közvetlen elindítása során kerül végrehajtásra. Független a kiválasztott futási szinttől és csak egyszer kerül végrehajtásra. Itt kerül felcsatolásra a `/proc` és `/dev/pts` fájlrendszer, illetve aktiválásra a blogd (rendszerindítás-naplózó démon). A rendszer frissítés vagy telepítés utáni első indításakor a kezdeti rendszerkonfiguráció kerül elindításra.

  A boot és rc minden más szolgáltatás előtt indítja el a blogd démont. A blogd a fenti parancsfájlok által elindított tevékenységek végrehajtása (bizonyos parancsfájlok futtatása, például a blokk-speciális fájlok elérhetővé tétele) után kerül leállításra. A blogd a képernyőkimenetet a `/var/log/boot.msg` naplófájlba írja, de csak akkor, ha a `/var` írható-olvasható módban van felcsatolva. Ellenkező esetben a blogd puffereli az adatokat, amíg a `/var` rendelkezésre nem áll. A blogdvel kapcsolatos további információ a blogd(8) kézikönyvoldalon található.

  A `boot` parancsfájl felelős az `/etc/init.d/boot.d` könyvtárban található, `S` betűvel kezdődő nevű parancsfájlok elindításáért. Itt történik meg a fájlrendszerek ellenőrzése és szükség esetén a hurokeszközök beállítása. A rendszeridő beállítása is megtörténik. Ha hiba történik a fájlrendszer automatikus ellenőrzése és kijavítása közben, akkor a rendszeradminisztrátor a root jelszó megadása után közbeavatkozhat. A legutoljára végrehajtott parancsfájl a `boot.local`.

`boot.local`
: Ebben a fájlban további, a rendszerindításkor, még az adott futási szintre váltás előtt végrehajtandó parancsok adhatók meg. Sok tekintetben hasonlít a DOS-rendszerek `AUTOEXEC.BAT` fájljára.

`halt (leállás)`
: Ez a parancsfájl csak 0-ás vagy 6-os futási szintre váltáskor hajtódik végre. Vagy `halt` (leállítás), vagy `reboot` (újraindítás) formájában van végrehajtva. A `halt` meghívási módjától függ, hogy a rendszer leállítása vagy újraindítása történik. Ha a leállítás során speciális parancsokat is végre kell hajtani, akkor ezeket a `halt.local` parancsfájlba kell beírni.

`rc`
: Ez a parancsfájl meghívja az aktuális futási szint megfelelő leállító parancsfájljait és elindítja az újonnan kiválasztott futási szint indító parancsfájljait. Az `/etc/init.d/boot` parancsfájlhoz hasonlóan, ezt a parancsfájlt is az `/etc/inittab` hívja meg, a kívánt futási szintet megadva paraméterként.

Saját parancsfájlok is létrehozhatók és egyszerűen beilleszthetők a fent leírt sémába. Az egyedi parancsfájlok formázásával, elnevezésével és rendszerezésével kapcsolatos információt az LSB-specifikáció, valamint az `init`, `init.d`, `chkconfig` és `insserv` kézikönyvoldalak tartalmaznak. Érdemes megtekinteni a `startproc` és `killproc` kézikönyvoldalat is.

FIGYELEM: A hibás init parancsfájlok lefagyaszthatják a rendszert.

A hibás init parancsfájlok lefagyaszthatják a gépet. Az ilyen parancsfájlokat nagy körültekintéssel szabad csak módosítani, ha lehetséges, szigorú tesztelésnek kitéve a többfelhasználós környezetben. Az init parancsfájlokkal kapcsolatos további hasznos információ: 14.2.1. - Futási szintek (187. oldal).

Ha egy adott programhoz vagy szolgáltatáshoz készít egyéni init parancsfájlt, használja az`/etc/init.d/skeleton` fájlt sablonként. Mentse el a fájl egy példányát új néven, majd módosítsa a megfelelő program- és fájlneveket, elérési utakat és egyéb részleteket. A parancsfájl természetesen tovább finomítható, hogy az init eljárás a megfelelő műveleteket indítsa el.

A skeleton fájl másolatának elején látható `INIT INFO` blokk a parancsfájl kötelező része, és feltétlenül módosítani kell. Lásd:14.1. példa - Egy minimális INIT INFO blokk (194. oldal)

14.1 példa *Egy minimális INIT INFO blokk*

```
### BEGIN INIT INFO
# Provides:          FOO
# Required-Start:    $syslog $remote_fs
# Required-Stop:     $syslog $remote_fs
# Default-Start:     3 5
# Default-Stop:      0 1 2 6
# Description:       Start FOO to allow XY and provide YZ
### END INIT INFO
```

Az `INFO` blokk első sorában a `Provides:` rész után adja meg az init parancsfájl által vezérelt program vagy szolgáltatás nevét. A `Required-Start:` és `Required-Stop:` sorokban adja meg az összes szolgáltatást, amelyet az adott szolgáltatás elindítása vagy leállítása előtt el kell indítani vagy le kell állítani. Ez az információ később kerül felhasználásra a futásiszint-könyvtárakban található parancsfájlnevek számozásának előállításakor. A `Default-Start:` és `Default-Stop:` szakaszban adja meg azokat a futási szinteket, amelyekben a szolgáltatást automatikusan el kell indítani, illetve le kell állítani. Végül a `Description:` részben adja meg a kérdéses szolgáltatás rövid leírását.

A futásiszint-könyvtárak (`/etc/init.d/rc?.d/`) és az `/etc/init.d/` könyvtárban található parancsfájlok közötti lánc létrehozásához adja ki az `insserv` *`új_parancsfájl_neve`* parancsot. Az insserv program kiértékeli az `INIT INFO` fejlécet és létrehozza a futásszint-könyvtárakban (`/etc/init.d/rc?.d/`) található parancsfájlok elindításához és leállításához szükséges láncokat. A program a megfelelő indítási és leállítási sorrendre is figyel: az egyes futási szinteken megfelelően számozza a láncok neveit. Ha inkább egy grafikus eszközzel kívánja létrehozni az ilyen láncokat, akkor használja a YaST által biztosított szerkesztőt (14.2.3. - Rendszerszolgáltatások (futási szintek) beállítása a YaST segítségével (195. oldal)).

Ha az `/etc/init.d/` könyvtárban már meglévő parancsfájlt kell integrálni egy meglévő futtásiszint-sémába, akkor a futásiszint-könyvtárakban rögtön létrehozhatók a láncok, akár az insserv segítségével, akár a YaST futásszint-szerkesztőjében a megfelelő szolgáltatás engedélyezésével. A módosítások a következő újraindításkor kerülnek alkalmazásra – az új szolgáltatás automatikusan el fog indulni.

A láncokat ne állítsa be kézzel. Ha az `INFO` blokkban valami nem jól van megadva, akkor problémák fognak felmerülni az `insserv` parancs későbbi, más szolgáltatásra vonatkozó futtatásakor. A kézzel felvett szolgáltatás törlődni fog a parancsfájlra vonatkozó `insserv` következő futtatásakor.

14.2.3 Rendszerszolgáltatások (futási szintek) beállítása a YaST segítségével

A YaST-modul elindítása után (*YaST* > *Rendszer* > *Rendszerszolgáltatások (futási szintek)* megjelenik a rendelkezésre álló szolgáltatások áttekintő listája és a szolgáltatások aktuális állapota (engedélyezett/letiltott). Döntse el, hogy a modult *Egyszerű módban* vagy *Szakértői módban* kívánja használni. Az alapértelmezett *Egyszerű mód* a legtöbb célnak megfelelő. A bal oldali oszlop a szolgáltatás nevét, a középső az aktuális állapotát, a jobb oldali pedig egy rövid leírást jelenít meg. A kiválasztott szolgáltatáshoz az ablak alsó részében egy részletesebb leírás jelenik meg. A szolgáltatás engedélyezéshez a táblázatban válassza azt ki, majd kattintson az *Engedélyezés* menüpontra. A szolgáltatás ugyanezekkel a lépésekkel tiltható le.

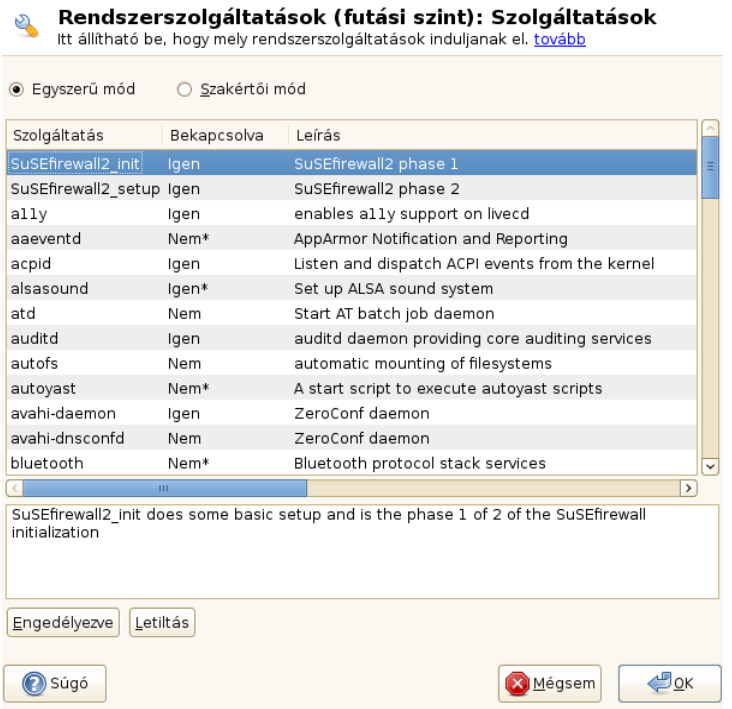
Ha finomabban kívánja szabályozni a futási szinteket, amelyben a szolgáltatás elindításra vagy leállításra kerül, illetve ha az alapértelmezett futási szintet kívánja módosítani, akkor először válassza ki a *Szakértői mód* menüpontot. Ebben a módban a párbeszédablak az alapértelmezett futási szintet („initdefault”, az a futási szint, amelyen a rendszer alapértelmezés szerint elindul) jeleníti meg legfelül. Normális esetben az openSUSE rendszer alapértelmezett futási szintje az 5 (teljes többfelhasználós mód hálózattal és X rendszerrel). Értelmes alternatíva lehet a 3-as futási szint (teljes többfelhasználós mód hálózattal).

A YaST párbeszédablak segítségével kiválasztható egy másik futási szint, mint új alapértelmezett érték (14.1 táblázat - A használható futási szintek (188. oldal)). Az ablakban lévő táblázat segítségével letilthatók és engedélyezhetők az egyes szolgáltatások és démonok. A táblázat felsorolja a rendelkezésre álló szolgáltatásokat és démonokat, megjeleníti, hogy pillanatnyilag engedélyezve vannak-e a rendszeren, és ha igen, akkor mely futási szintekhez. Ha az egér segítségével kiválasztotta az egyik sort, akkor jelölje meg azon futási szintek melletti négyzetet (*B*, *0*, *1*, *2*, *3*, *5*, *6* és *S*), amelyeken a kiválasztott szolgáltatást vagy démont futtani kívánja. A 4-es futási szint nincs megadva, így létre lehet hozni egy egyedi futási szintet. A táblázatos áttekintés alatt az éppen kiválasztott szolgáltatás vagy démon rövid leírása látható.

FIGYELEM: A hibás futásiszint-beállítások tönkretehetik a rendszert.

A hibás futásiszint-beállítások a rendszert használhatatlanná tehetik. Csak akkor alkalmazzon egy módosítást, ha tisztában van a következményekkel.

14.1. ábra *Rendszerszolgáltatások (futási szint)*



Az *Indítás, Leállítás vagy Frissítés* menüpontok segítségével állapítsa meg, hogy a szolgáltatást kell-e aktiválni. Az *Állapot frissítése* gomb megnyomására a rendszer ellenőrzi az aktuális állapotot. A *Beállítás vagy Visszaállítás* gombokkal megadható, hogy a módosítások alkalmazásra kerüljenek-e a rendszeren, vagy a beállítások visszaállításra kerüljenek-e a futásiszint-szerkesztő elindítása előtt érvényes értékekre. A *Befejezés* gomb megnyomására a program lemezre menti a módosított beállításokat.

14.3 Rendszerkonfiguráció az /etc/sysconfig fájl segítségével

Az openSUSE legfőbb beállításai az `/etc/sysconfig` könyvtárban található konfigurációs fájlok segítségével adhatók meg. Az `/etc/sysconfig` könyvtárban lévő egyes fájlokat csak azok a parancsfájlok olvassák, amelyekhez tartoznak. Ez biztosítja,

hogy például a hálózati beállításokat csak a hálózattal kapcsolatos parancsfájlok elemezzék.

A rendszerkonfiguráció kétféleképpen módosítható. Használható a YaST sysconfig-szerkesztője, illetve a konfigurációs fájlok kézzel is módosíthatók.

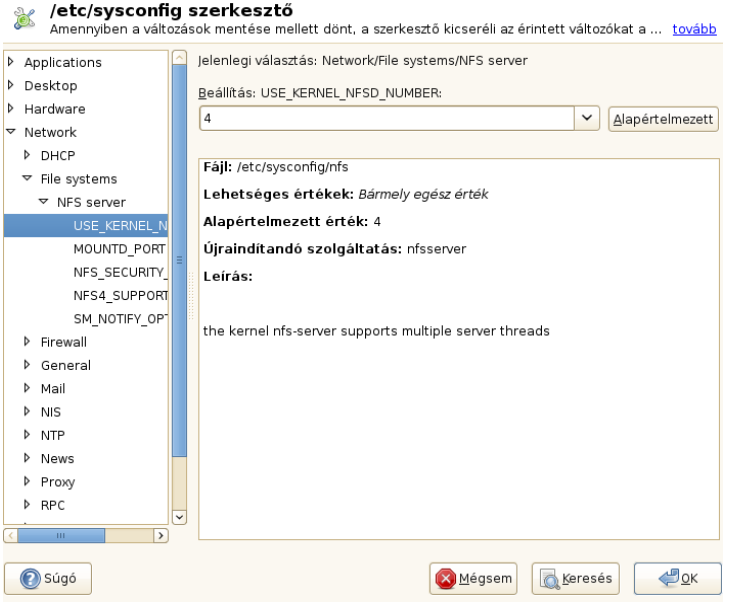
14.3.1 A rendszerkonfiguráció módosítása a YaST sysconfig-szerkesztőjével

A YaST sysconfig-szerkesztője egyszerűen kezelhető felületet biztosít a rendszerkonfiguráció módosításához. Anélkül, hogy tisztában lenne a módosítandó konfigurációs változó tényleges helyével, használhatja a modul beépített keresési funkcióját; igény szerint módosíthatja a konfigurációs változók értékét; és hagyhatja, hogy a YaST végezze el a tényleges módosításokat a `sysconfig`-ban beállított értékek függvényében, majd indítsa újra a szolgáltatásokat.

FIGYELEM: Az `/etc/sysconfig/*` fájlok módosítása tönkreteheti a telepített rendszert.

Megfelelő tapasztalat és ismeretek hiányában ne módosítsa az `/etc/sysconfig` könyvtár fájljait. Szó szerint tönkreteheti vele a rendszert. Az `/etc/sysconfig` könyvtárban lévő fájlok egy rövid megjegyzést tartalmaznak minden változóhoz, amelyben leírják a hatásukat.

14.2. ábra *Rendszerkonfiguráció a sysconfig-szerkesztő segítségével*



A YaST sysconfig párbeszédablak három részre van osztva. A párbeszédablak bal oldali része a beállítható változók fanézetét jeleníti meg. Egy változó kiválasztásakor a jobb oldali rész az aktuális kijelölést és a változó aktuális értékét jeleníti meg. A harmadik ablak alul röviden leírja a változó célját, lehetséges értékeit, alapértelmezett értékét, valamint a konfigurációs fájlt, amelyből a változók származik. A párbeszédablak arról is szolgáltat információt, hogy a változó módosítása után mely konfigurációs parancsfájl lesz végrehajtva és hogy a módosítás eredményeképp melyik új szolgáltatás lesz elindítva. A YaST felszólít a módosítások megerősítésére és értesít arról, hogy mely parancsfájlok kerülnek végrehajtásra, miután a *Befejezés* kiválasztásával kilépett a párbeszédablakból. A most kihagyni kívánt szolgáltatásokat és parancsfájlokat is válassza ki, hogy később azokat is el lehessen majd indítani. A YaST automatikusan érvényesíti az összes módosítást és újraindítja az érintett szolgáltatásokat, hogy a módosítások érvényre jussanak.

14.3.2 A rendszerkonfiguráció kézi módosítása

A rendszerkonfiguráció kézi módosításához az alábbi lépéseket kell követni.

1. Váltson át a `root` felhasználóra.
2. Állítsa át a rendszert egyfelhasználós módba (1-es futási szint) a `telinit 1` paranccsal.
3. Módosítsa igény szerint a konfigurációs fájlokat egy tetszés szerinti szerkesztőprogrammal.

   Ha nem a YaST segítségével módosítja az `/etc/sysconfig` könyvtár konfigurációs fájljait, akkor ügyeljen rá, hogy az üres változóértékeket két idézőjel ábrázolja (`KEYTABLE=""`) és hogy a szóközt tartalmazó értékek idézőjelek közé legyenek zárva. A csak egy szóból álló értékek esetén nincs szükség idézőjelre.
4. Futtassa le a `SuSEconfig` parancsot, hogy a módosítások alkalmazásra kerüljenek.
5. Állítsa vissza a rendszert a korábbi futási szintre a `telinit` *`alapértelmezett_futási_szint`* parancs segítségével. Az *`alapértelmezett_futási_szint`* helyére a rendszer alapértelmezett futási szintjét írja. Ha teljes többfelhasználós módba kíván visszatérni hálózattal és X képernyőkezelővel, akkor írjon `5`-öst, ha teljes többfelhasználós módba kíván visszatérni hálózattal (X nélkül), akkor írjon `3`-ast.

Ez az eljárás főként a rendszerszintű beállítások – például a hálózati konfiguráció – módosítása esetén lényeges. A kis módosításokhoz nem kell egyfelhasználós módba lépni, bár ez biztosan garantálja, hogy az összes érintett program megfelelő módon újraindul.

TIPP: Automatizált rendszerkonfiguráció beállítása

A SuSEconfig által végrehajtott automatikus konfiguráció letiltásához az `/etc/sysconfig/suseconfig` fájlban található `ENABLE_SUSECONFIG` változót

állítsa `no` értékre. Ha a SUSE telepítéstámogatást használni kívánja, akkor ne tiltsa le a SuSEconfig-ot. Az automatikus konfiguráció részlegesen is letiltható.

15 A rendszertöltő

Ez a fejezet a GRUB, az openSUSE-ban használt rendszertöltő beállítását írja le. A beállítások megadásához egy speciális YaST-modul áll rendelkezésre. Ha nincs tisztában a Linux indításával, akkor némi háttérinformáció megszerzéséhez olvassa el az alábbi részeket. A fejezet kitér néhány, a GRUB segítségével való indítás során gyakran fellépő problémára és ezek megoldására is.

Ez a fejezet az indításkezelésre és a GRUB rendszertöltő beállítására koncentrál. A rendszerindítási folyamat részletesebb leírása: 14. fejezet - *Linux-rendszerek indítása és beállítása* (183. oldal) A rendszertöltő jelenti a gép (a BIOS) és az operációs rendszer (openSUSE) közös felületét. A rendszertöltő konfigurációja adja meg az elindítandó operációs rendszert és beállításait.

Az alábbi kifejezések sűrűn előfordulnak a fejezetben és szükség lehet a rövid magyarázatukra:

Master Boot Record
: Az MBR struktúráját egy operációsrendszer-független egyezmény határozza meg. Az első 446 bájt a programkód számára van lefoglalva. Ezek jellemzően a rendszertöltő, vagy egy operációsrendszer-választó programot tartalmazzák. A következő 64 bájt a maximum négy bejegyzéssel rendelkező partíciós táblának biztosít területet (lásd .). A partíciós tábla a merevlemez és a fájlrendszertípus particionálásával kapcsolatos adatokat tartalmazza. Az operációs rendszernek erre a táblázatra a merevlemez kezeléséhez van szüksége. Az MBR-ben hagyományos, általános kód található, és a partíciók közül pontosan egyet szabad és kell *aktívnak* megjelölni. Az MBR utolsó két bájtjának tartalmaznia kell egy statikus „mágikus számot” (AA55). Ha az MBR más értéket tartalmaz, akkor bizonyos BIOS-ok érvénytelennek tekintik, és nem hajlandók rendszerindításhoz használni.

Rendszerindító szektorok

A rendszerindító szektorok a merevlemez-partíciók első szektorai a kiterjesztett partíciók kivételével, amely más partíciók „tárolójaként” működik. Ezek a rendszerindító szektorok 512 bájt területet biztosítanak a megfelelő partíción telepített operációs rendszer indításához használt kódhoz. Ez a formázott DOS, Windows és OS/2 partíciók rendszerindító szektoraira érvényes, amelyek a fájlrendszer néhány fontos alapadatát tartalmazzák. Ezzel szemben a Linux-partíciók rendszerindító szektorai a fájlrendszer beállítása után kezdetben üresek (kivéve az XFS fájlrendszert). Éppen ezért egy Linux-partíció magától nem indítható el abban az esetben sem, ha egy kernelt és egy érvényes root fájlrendszert tartalmaz. A rendszer indítására szolgáló érvényes kóddal rendelkező rendszerindító-szektor ugyanazzal a mágikus számmal rendelkezik, mint az MBR az utolsó két bájtban (`AA55`).

15.1 Rendszerindítás a GRUB segítségével

A GRUB (Grand Unified Bootloader) két részből áll. Az első rész (stage 1) 512 bájtot tartalmaz, amelynek az összes feladata a rendszertöltő második részének (stage2) betöltése. Ezt követően a második rész (stage 2) kerül betöltésre. Ez a rész tartalmazza a rendszertöltő lényegi részét.

Egyes konfigurációkban egy köztes (1.5-ös) szakasz is használható, amelyik kikeresi és betölti a stage2-t a megfelelő fájlrendszerből. Hacsak lehetséges, az alapértelmezett telepítés ezt a módszert alkalmazza, illetve ez történik a GRUB YaST-tal történő beállításakor is.

A stage 2 többféle fájlrendszert képes kezelni. Jelenleg az Ext2, Ext3, ReiserFS, Minix és a Windows által használt DOS FAT fájlrendszer támogatott. Bizonyos mértékben az XFS és UFS, valamint a BSD-rendszerek által használt FFS is támogatott. A 0.95-ös verzió óta a GRUB az „El Torito” specifikációnak megfelelő, ISO 9660 szabványú fájlrendszert tartalmazó CD-ről vagy DVD-ről is el tudja indítani a rendszert. A GRUB még a rendszer indítása előtt el tudja érni a támogatott BIOS-lemezeszközök (a BIOS által felismert hajlékonylemezek és merevlemezek, CD- és DVD-meghajtók) fájlrendszereit. A GRUB konfigurációs fájl (`menu.lst`) módosításai miatt az indításkezelőt nem kell többé újratelepíteni. A rendszer indításakor a GRUB újratölti a menüfájlt az érvényes elérési utakkal, valamint a kernel vagy a kezdeti memóriaeszköz (`initrd`) partícióadataival és megkeresi a fájlokat.

A GRUB tényleges konfigurációja az alább leírt három fájlra épül:

`/boot/grub/menu.lst`
: Ez a fájl a GRUB segítségével indítható partíciókkal és operációs rendszerekkel kapcsolatos összes információt tartalmazza. Ezen adatok nélkül a GRUB parancssor megkérdezik a felhasználótól, hogy hogyan folytassa (ennek részletei: „Menüpontok szerkesztése a rendszerindítási folyamat során” szakasz (208. oldal)).

`/boot/grub/device.map`
: Ez a fájl fordítja le a GRUB és a BIOS-jelölés eszközneveit Linux-eszköznevekre.

`/etc/grub.conf`
: Ez a fájl tartalmazza a paramétereket és opciókat, amelyekre a GRUB-nak a rendszertöltő megfelelő betöltéséhez szüksége van.

A GRUB sokféleképp vezérelhető. A grafikus menüből kiválaszthatók a meglévő konfiguráció rendszerindítási bejegyzései (nyitóképernyő). A beállítás a `menu.lst` fájlból kerül betöltésre.

A GRUB-ban az indítás előtt az összes rendszerindítási paraméter módosítható. Így például kijavítható a menüfájl szerkesztésekor fellépő hiba. A rendszerindító parancsok interaktív módon is betölthetők egy bemeneti prompt segítségével (lásd „Menüpontok szerkesztése a rendszerindítási folyamat során” szakasz (208. oldal)). A GRUB a rendszerindítás előtt biztosítja a kernel és az `initrd` helymeghatározásának lehetőségét. Ezen a módon akár egy olyan telepített operációs rendszer is elindítható, amelyhez nincs bejegyzés a rendszertöltő konfigurációjában

A GRUB-nak valójában két verziója létezik: egy rendszertöltő és egy normál Linux-program az `/usr/sbin/grub` könyvtárban. Ezt a programot *GRUB-parancsértelmezőnek* hívjuk. Emulálja a GRUB-ot a telepített rendszeren és használható akár a GRUB telepítésére, akár az új beállítások kipróbálására az éles bevezetés előtt. Az a funkció, amely a GRUB-ot telepíti rendszertöltőként a merevlemezen vagy hajlékonylemezen, integrált része a GRUB-nak az `install` és `setup` parancsok formájában. Ez elérhető a GRUB-parancsértelmezőben a Linux betöltésekor.

15.1.1 A GRUB rendszerindító menü

A rendszerindító menüt megjelenítő grafikus nyitóképernyő a `/boot/grub/menu.lst` GRUB konfigurációs fájlra épül, amely tartalmazza az összes partícióval és operációs rendszerrel kapcsolatos információt, amely a menü segítségével elindítható.

A rendszer minden indításakor a GRUB betölti a menüfájlt a fájlrendszerből. Ez azt jelenti, hogy a fájl módosítása után a GRUB -ot nem kell újratelepíteni. A YaST rendszertöltő segítségével módosítsa a GRUB-konfigurációt (15.2. - A rendszertöltő beállítása a YaST használatával (211. oldal)).

A menüfájl parancsokat tartalmaz. A szintaxis nagyon egyszerű. Minden sor egy parancsot tartalmaz, amelyet szóközzel elválasztott opcionális paraméterek követnek, mint a parancsértelmezőben. Történeti okokból néhány parancs első paramétere elé = tehető. A megjegyzéseket egy kettőskereszt (#) vezeti be.

A menüáttekintésben a menüpontok azonosításához minden bejegyzéshez adjon meg egy `title` bejegyzést. A `title` kulcsszót követő szöveg (a szóközöket is beleértve) választható menüpontként jelenik meg a menüben. A menüpont kiválasztásakor minden parancs végrehajtásra kerül a következő `title` bejegyzésig.

A legegyszerűbb eset más operációs rendszerek rendszertöltőire történő átirányítás. A parancs a `chainloader` és az argumentum általában a másik partíció rendszerindító blokkja, GRUB-blokkjelölésben. Például:

```
chainloader (hd0,3)+1
```

A GRUB eszközneveinek leírása: „Merevlemezek és partíciók névkonvenciói” szakasz (205. oldal). A fenti példa az első merevlemez negyedik partíciójának első blokkját adja meg.

A `kernel` parancs segítségével adható meg egy kernelképfájl. Az első argumentum a partícióban lévő kernelképfájl elérési útja. A többi argumentum a parancssorban kerül a kernelnek átadásra.

Ha a kernel nem rendelkezik beépített segédprogramokkal a gyökérpartíció eléréséhez, vagy ha egy frissebb kiadású, speciális hotplug-funkciókat alkalmazó Linux-rendszert használ, az `initrd` fájlt egy külön GRUB -parancs segítségével kell megadni, amelynek egyetlen argumentuma az `initrd` fájl elérési útja. Mivel az `initrd` betöl-

tési címe beíródik a betöltött kernelképbe, az `initrd` parancsnak közvetlenül a `kernel` parancsot kell követnie.

A `root` parancs leegyszerűsíti a kernel és az initrd fájlok megadását. A `root` egyetlen argumentuma egy eszköz vagy egy partíció. Ez az eszköz lesz felhasználva az összes kernelhez, `initrd` fájlhoz és egyéb elérési utakhoz, amelyekhez explicit módon nincs megadva eszköz, a következő `root` parancsig.

A `boot` parancs minden menübejegyzés végére odaértendő, nem kell külön beírni a menüfájlba. Ha azonban a GRUB-ot interaktív módon használja a rendszerindításhoz, akkor a `boot` parancsot meg kell adni a végén. Maga a parancs nem rendelkezik argumentumokkal. Ez egyszerűen csak elindítja a betöltött kernelképet vagy a megadott láncbetöltőt.

A menübejegyzések elkészítése után jelölje meg az egyiket `alapértelmezett` bejegyzésként. Ellenkező esetben az első bejegyzés (`0` bejegyzés) lesz az. Egy időkorlát is megadható (másodpercben), amely után az alapértelmezett bejegyzést el kell indítani. A `timeout` (időkorlát) és `default` (alapértelmezett érték) általában megelőzi a menübejegyzéseket. Egy példafájl leírása a következő helyen található: „Egy példa menüfájl” szakasz (206. oldal).

Merevlemezek és partíciók névkonvenciói

A GRUB merevlemezekhez és partíciókhoz használt névkonvenciói eltérnek a normál Linux-eszközökétől. Jobban hasonlít a BIOS által használt megoldáshoz, a lemezek egyszerű megszámozásához, a szintaxis pedig egyes BSD-leszármazottakéra hasonlít. A GRUB-ban a partíciók számozása nullával kezdődik. Következésképp a (`hd0,0`) az első merevlemez első partíciója. Egy általános asztali gépen, amelyre egy merevlemez van csatlakoztatva elsődleges masterként, a megfelelő Linux-eszköznév a `/dev/sda1`.

A négy lehetséges elsődleges partícióhoz a `0-3` partíciószám van rendelve. A logikai partíciók számozása `4`-től kezdődik:

```
(hd0,0)    first primary partition of the first hard disk
(hd0,1)    second primary partition
(hd0,2)    third primary partition
(hd0,3)    fourth primary partition (usually an extended partition)
(hd0,4)    first logical partition
(hd0,5)    second logical partition
```

Mivel a BIOS-eszköztől függ, a GRUB nem tesz különbséget az IDE-, SATA-, SCSI- és hadveres RAID-eszközök között. A BIOS által felismert merevlemezek és más vezérlők a BIOS-ban lévő rendszerindítási szekvenciának megfelelően számozódnak.

Sajnos, gyakran nem lehet pontosan leképezni a Linux-eszközneveket BIOS-eszköznevekre. Egy algoritmus segítségével állítja elő a leképezést és menti el a `device.map`, amely szükség esetén szerkeszthető. A `device.map` fájllal kapcsolatos információt a következő rész tartalmaz: 15.1.2. - A device.map fájl (209. oldal).

Egy teljes GRUB elérési út zárójelek közé írt eszköznévből és a megadott partíció fájlrendszerén található fájl elérési útjából áll. Az elérési út törtvonallal kezdődik. Az indítható kernel például az alábbi módon adható meg egy olyan rendszeren, amely egy IDE-merevlemezt tartalmaz és ennek első partícióján Linux található:

```
(hd0,0)/boot/vmlinuz
```

Egy példa menüfájl

Az alábbi példa a GRUB-menüfájl szerkezetét mutatja be. A mintarendszerben legyen a `/dev/sda5` alatt egy Linux indító partíció, a `/dev/sda7` alatt egy root partíció és a `/dev/sda1` alatt egy Windows-rendszer.

```
gfxmenu (hd0,4)/boot/message
color white/blue black/light-gray
default 0
timeout 8

title linux
   root (hd0,4)
   kernel /boot/vmlinuz root=/dev/sda7 vga=791 resume=/dev/sda9
   initrd /boot/initrd

title windows
   rootnoverify (hd0,0)
   chainloader +1

title floppy
   rootnoverify (hd0,0)
   chainloader (fd0)+1

title failsafe
   root (hd0,4)
   kernel /boot/vmlinuz.shipped root=/dev/sda7 ide=nodma \
   apm=off acpi=off vga=normal nosmp maxcpus=0 3 noresume
   initrd /boot/initrd.shipped
```

Az első blokk a nyitóképernyő konfigurációját adja meg:

gfxmenu (hd0,4)/boot/message
: A `message` háttérkép a `/dev/sda5` partíció /boot könyvtárában található.

color white/blue black/light-gray
: Színséma: fehér (előtér), kék (háttér), fekete (kiválasztás) és világosszürke (a kiválasztás háttere). A színséma nincs hatással a nyitóképernyőre, csak a testreszabható GRUB-menüre, amely akkor jelenik meg, ha az Esc billentyűvel kilép a nyitóképernyőből.

default 0
: Alapértelmezés szerint az első menübejegyzés, a `title linux` lesz elindítva.

timeout 8
: Ha a rendszer nyolc másodpercig nem kap utasítást a felhasználótól, akkor a GRUB automatikusan elindítja az alapértelmezett bejegyzést. Az automatikus indítás kikapcsolásához törölje a `timeout` sort. A `timeout 0` megadása esetén a GRUB azonnal elindítja az alapértelmezett bejegyzést.

A második és legnagyobb blokk a különböző indítható operációs rendszereket jeleníti meg. Az egyes operációs rendszereket tartalmazó rész elejét a `title` kulcsszó jelzi.

- Az első bejegyzés (`title linux`) az openSUSE indításáért felelős. A kernel (`vmlinuz`) az első merevlemez első logikai partíciójában (az indítási partíció) található. Itt adhatók meg a kernelparaméterek, mint például a root partíció és a VGA mód. A root partíció a Linux névkonvenciójának megfelelően van megadva (`/dev/sda7/`), mivel ezt az információt a kernel olvassa és a GRUB-nak nincs rá szüksége. Az `initrd` szintén az első merevlemez első logikai partíciójában található.

- A második bejegyzés a Windows betöltéséért felelős. A Windows az első merevlemez első partíciójáról töltődik be (`hd0,0`). A `chainloader +1` parancs hatására a GRUB elolvassa és végrehajtja a megadott partíció első szektorát.

- A következő bejegyzés hajlékonylemezről történő indítást tesz lehetővé a BIOS-beállítások módosítása nélkül.

- A `failsafe` indítási opció a Linuxot olyan kernelparaméterekkel indítja el, amelyek segítségével a Linux problémás rendszereken is elindulhat.

A menüfájl szükség esetén bármikor módosítható. A GRUB a következő rendszerindítás során a módosított beállításokat használja. A fájl a YaST segítségével vagy egy tetszőleges szerkesztővel bármikor szerkeszthető. A GRUB szerkesztési funkciójával ideiglenes módosítások is végezhetők interaktív módon. Lásd:„Menüpontok szerkesztése a rendszerindítási folyamat során” szakasz (208. oldal)

Menüpontok szerkesztése a rendszerindítási folyamat során

A grafikus rendszerindító menüben a nyíl billentyűk segítségével válassza ki az indítandó operációs rendszert. Linux rendszer választása esetén az indítási promptnál további indítási paraméterek is megadhatók. Az egyes menübejegyzések közvetlen szerkesztéséhez nyomja meg az Esc gombot a nyitóképernyő elhagyásához, majd az E billentyűt. Az ilyen módosítás csak az aktuális indítási folyamatra érvényes és nem kerül véglegesen alkalmazásra.

FONTOS: Billentyűzetkiosztás az indítási folyamat során

Rendszerindításkor csak az US billentyűzetkiosztás áll rendelkezésre (lásd „US Keyboard Layout” ábra (↑*Start-Up*)).

A menübejegyzések szerkesztése segíthet egy hibás, már nem indítható rendszer megjavításában, mivel a rendszertöltő hibás konfigurációs fájlja kikerülhető a paraméterek kézi megadásával. A paraméterek kézi megadása a rendszerindítási folyamat során hasznos akkor is, ha új beállításokat akar kipróbálni az eredeti rendszer befolyásolása nélkül.

A szerkesztési mód aktiválása után a nyíl billentyűk segítségével válassza ki a menübejegyzést, amelynek szerkeszteni kívánja a konfigurációját. A konfiguráció szerkeszthetővé tétele érdekében nyomja meg még egyszer az E billentyűt. Ily módon módosíthatja a nem megfelelő partíció vagy elérési út részleteit, mielőtt azok negatív hatással lennének a rendszerindítási folyamatra. A szerkesztési módból kilépéshez és a menühöz visszatéréshez nyomja az Enter billentyűt. Utána a bejegyzés indításához nyomja meg a B billentyűt. A további lehetséges műveleteket az alul látható súgószöveg mutatja.

A módosított rendszerindítási opciók állandó megadásához és a kernelhez továbbításához `root` felhasználóként nyissa meg a `menu.lst` fájlt, majd a meglévő sorhoz szóközzel elválasztva fűzze hozzá a megfelelő kernelparamétereket:

```
title linux
   root(hd0,0)
   kernel /vmlinuz root=/dev/sda3 additional parameter
   initrd /initrd
```

A rendszer következő indításakor a GRUB automatikusan alkalmazza az új paramétereket. Ez a módosítás a YaST rendszertöltő modul segítségével is végrehajtható. Szóközökkel elválasztva fűzze hozzá az új paramétereket a meglévő sorhoz.

15.1.2 A device.map fájl

A `device.map` fájl a GRUB eszközneveit képezi le Linux-eszköznevekre. IDE- és SCSI-merevlemezeket egyaránt tartalmazó vegyes rendszerben a GRUB egy speciális eljárás segítségével megpróbálja kideríteni az indítási sorrendet, mivel a GRUB nem tud hozzáférni az indítási sorrenddel kapcsolatos BIOS-információhoz. A GRUB az elemzés eredményét elmenti a `/boot/grub/device.map` fájlba. Egy olyan rendszer esetén, amelynek BIOS-ban lévő indítási sorrendjében az IDE a SCSI előtt van, a `device.map` az alábbi módon jelenhet meg:

```
(fd0)  /dev/fd0
(hd0)  /dev/sda
(hd1)  /dev/sdb
```

Mivel az IDE-, SCSI- és egyéb merevlemezek sorrendje különböző tényezőktől függ és a Linux nem tudja azonosítani a leképezést, a `device.map` fájlban lévő sorrend kézzel is beállítható. Amennyiben a rendszerindítás során problémákat észlel, ellenőrizze, hogy a fájlban lévő sorrend megfelel-e a BIOS-ban lévő sorrendnek, és ha szükséges, az ideiglenes módosításhoz használja a GRUB-parancsértelmezőt. A Linux-rendszer elindítása után a `device.map` fájl a YaST rendszertöltő modul vagy egy tetszőleges szerkesztőprogram segítségével módosítható.

A `device.map` fájl kézzel történő módosítása után az alábbi parancs végrehajtásával telepítse újra a GRUB-ot. A parancs hatására a `device.map` újra betöltődik és a `grub.conf` fájlban megjelenített parancsok végrehajtódnak:

```
grub --batch < /etc/grub.conf
```

15.1.3 Az /etc/grub.conf fájl

A GRUB harmadik fontos konfigurációs fájlja (a `menu.lst` és a `device.map` mellett) az `/etc/grub.conf`. Ez a fájl tartalmazza a paramétereket és opciókat, amelyekre a GRUB-nak a rendszertöltő megfelelő betöltéséhez szüksége van:

```
setup --stage2=/boot/grub/stage2 --force-lba (hd0,1) (hd0,1)
   quit
```

Ez a parancs azt jelzi a GRUB-nak, hogy automatikusan telepítse a rendszertöltőt az első merevlemez második partíciójára (hd0,1), az ugyanezen a partíción található rendszerindító képfájlok használatával. A `--stage2=/boot/grub/stage2` paraméter a `stage2` rendszerkép egy felcsatolt fájlrendszerről való telepítéséhez szükséges. Egyes BIOS-okban rossz az LBA-támogatás megvalósítása. A `--force-lba` paraméterrel ez figyelmen kívül hagyható.

15.1.4 Rendszerindítási jelszó beállítása

Bár az operációs rendszer indítása előtt kerül elindításra, a GRUB lehetővé teszi a fájlrendszerek elérését. A root jogosultsággal nem rendelkező felhasználók elérhetik a Linux-rendszer azon fájljait, amelyhez a rendszer indítása után már nem férhetnek hozzá. Az ilyen típusú hozzáférés letiltásához illetve annak megakadályozásához, hogy a felhasználók bizonyos operációs rendszereket elindítsanak, állítson be egy rendszerindítási jelszót.

FONTOS: Rendszerindítási jelszó és a nyitóképernyő

Ha használ rendszerindítási jelszót a GRUB-hoz, akkor a szokásos nyitóképernyő nem jelenik meg.

Rendszerindítási jelszó beállításához `root` felhasználóként a következőképpen kell eljárni:

1. A root promptnál titkosítsa a jelszót a grub-md5-crypt használatával:

```
# grub-md5-crypt
Password: ****
Retype password: ****
Encrypted: $1$lS2dv/$JOYcdxIn7CJk9xShzzJVw/
```

2 Illessze be a titkosított karaktersorozatot a `menu.lst` globális részébe:

```
gfxmenu (hd0,4)/message
color white/blue black/light-gray
default 0
timeout 8
password --md5 $1$lS2dv/$JOYcdxIn7CJk9xShzzJVw/
```

A GRUB-parancsok ezután a rendszerindítási promptnál csak a P billentyű lenyomása és a jelszó megadása után hajthatók végre. A felhasználók azonban továbbra is elindíthatják a rendszerindítás menüben lévő összes operációs rendszert.

3 Annak megakadályozásához, hogy a rendszerindítás menüben lévő operációs rendszerek egy részét el lehessen indítani, a `menu.lst` fájl minden olyan részéhez hozzá kell adni a `lock` bejegyzést, amelyeket jelszóval kíván védeni. Például:

```
title linux
   kernel (hd0,4)/vmlinuz root=/dev/sda7 vga=791
   initrd (hd0,4)/initrd
   lock
```

Ha a rendszer újraindítása után a rendszerindítás menüben a Linux-bejegyzést választotta, az alábbi hibaüzenet jelenik meg:

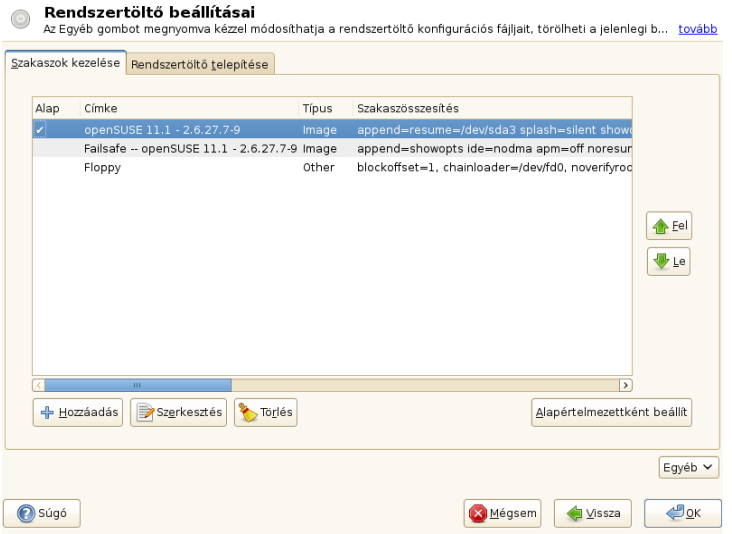
```
Error 32: Must be authenticated
```

A menübe belépéshez nyomja meg az Enter billentyűt. A jelszóprompt megnyitásához nyomja meg a P billentyűt. A jelszó megadása és az Enter megnyomása után a kiválasztott operációs rendszernek (ebben az esetben a Linuxnak) el kell indulnia.

15.2 A rendszertöltő beállítása a YaST használatával

A rendszertöltő beállításának legegyszerűbb módjaz openSUSE rendszeren a YaST megfelelő moduljának a használata. A YaST vezérlőközpontban válassza ki a *Rendszer* > *Rendszertöltő beállítása* menüpontot. Megjelennek a rendszer aktuális rendszertöltő-beállításai és itt végezhetők el a kívánt módosítások. Lásd: 15.1. ábra - A rendszertöltő beállításai (212. oldal)

15.1. ábra *A rendszertöltő beállításai*



Az adott operációs rendszer rendszertöltő-szakaszainak szerkesztéséhez, módosításához és törléséhez használja a *Szakaszok kezelése* lapot. Egy beállítás hozzáadásához kattintson a *Hozzáadás* gombra. Egy meglévő beállítás értékének módosításához válassza ki azt az egérrel és kattintson a *Szerkesztés* gombra. Egy meglévő bejegyzés törléséhez válassza ki azt és kattintson a *Törlés* gombra. Ha nem ismeri a rendszertöltő beállításait, akkor először olvassa el ezt a részt: 15.1. - Rendszerindítás a GRUB segítségével (202. oldal)

A rendszertöltő típusával, helyével és speciális beállításaival kapcsolatos beállítások megtekintéséhez és módosításához használja a *Rendszertöltő telepítése* lapot.

A speciális konfigurációs beállítások az *Egyéb* gombra kattintva a legördülő menüben érhetők el. A GRUB konfigurációs fájljai a beépített szerkesztővel módosíthatók (ennek részletei: 15.1. - Rendszerindítás a GRUB segítségével (202. oldal)) Törölheti a meglévő konfigurációt és létrehozhat egy újat (*Kezdés elölről*), illetve hagyhatja, hogy a YaST ajánljon egyet (*Javaslat egy új konfigurációhoz*). A konfiguráció lemezre is írható vagy onnan újraolvasható. A telepítéskor elmentett elsődleges rendszerindítási rekord (master boot record, MBR) visszaállításához válassza a *Merevlemez MBR-jének visszaállítása* lehetőséget.

15.2.1 Az alapértelmezett rendszerindító bejegyzés módosítása

Az alapértelmezésben elindított rendszer megváltoztatásához tegye a következőket:

15.1. eljárás *Az alapértelmezett rendszer beállítása*

1. Nyissa ki a *Munkamenet-felügyelet* lapot.
2. Válassza ki a kívánt bejegyzést a listából.
3. Kattintson a *Beállítás alapértelmezettként* lehetőségre.
4. A változások aktiválásához kattintson a *Kész* gombra.

15.2.2 A rendszertöltő helyének módosítása

A rendszertöltő helyének megváltoztatásához a következőket kell tennie:

15.2. eljárás *Válassza ki a Rendszertöltő helye lehetőséget*

1. Válassza ki a *Rendszertöltő telepítése* lapot, majd válasszon egyet a következő lehetőségek közül a *Rendszertöltő helye* mezőben:

   Rendszerindítás a rendszerindító partícióról
   : A `/boot` partíció rendszerindító szektora.

   Rendszerindítás kiterjesztett partícióról
   : Ez a kiterjesztett partíció tárolójába telepíti a rendszertöltőt.

   Rendszerindítás az elsődleges rendszerindítási rekord használatával
   : Ez az első lemez MBR-ébe telepíti a rendszertöltőt (a BIOS-ban előre beállított rendszerindítási sorrend szerint).

   Rendszerindítás a root partícióból
   : Ez a `/` partíció rendszerindító szektorába telepíti a rendszertöltőt.

Egyedi rendszerindító partíció
Ez a lehetőség a rendszertöltő helyének kézi megadásához használható.

2 A módosítások alkalmazásához kattintson a *Kész* gombra.

15.2.3 A rendszertöltő időkorlátjának módosítása

A rendszertöltő nem azonnal indítja el az alapértelmezett rendszert. Az időkorláton belül kiválaszthatja az elindítani kívánt rendszert vagy beírhat bizonyos kernelparamétereket. A rendszertöltő időkorlátjának megadásához tegye a következőket:

15.3. eljárás *A rendszertöltő időkorlátjának módosítása*

1 Nyissa meg a *Rendszertöltő telepítése* lapot.

2 Kattintson a *Rendszertöltő beállítások* gombra.

3 Módosítsa az *Időkorlát másodpercben* értékét egy új szám beírásával, a megfelelő nyílra kattintva az egérrel vagy a billentyűzet nyíl gombjaival.

4 Kattintson az *OK* gombra.

5 A módosítások mentéséhez kattintson a *Kész* gombra.

15.2.4 Rendszerindítási jelszó beállítása

Ennek a YaST modulnak a használatával megadhat egy jelszót is a rendszerindítás levédéséhez. Ez újabb biztonsági fokozatot jelent.

15.4. eljárás *Rendszertöltő jelszó megadása*

1 Nyissa meg a *Rendszertöltő telepítése* lapot.

2 Kattintson a *Rendszertöltő beállítások* gombra.

3 Adja meg a jelszót a *Jelszó a menüfelülethez* mezőben.

4 Kattintson az *OK* gombra.

5 A módosítások mentéséhez kattintson a *Kész* gombra.

15.2.5 A lemezek sorrendjének módosítása

Ha a számítógépben egynél több merevlemez található, akkor megadható a lemezek indítási sorrendje, a gép BIOS-beállításaihoz igazodóan (lásd: 15.1.2. - A device.map fájl (209. oldal)). Ennek lépései:

15.5. eljárás *A lemezek sorrendjének beállítása*

1 Nyissa meg a *Rendszertöltő telepítése* lapot.

2 Kattintson a *Rendszertöltő telepítésének részletei* gombra.

3 Ha egynél több lemez látható felsorolva, akkor válassza ki az egyiket, majd kattintson a *Fel* vagy *Le* pontra a megjelenített lemezek átrendezéséhez.

4 A módosítások mentéséhez kattintson az *OK* gombra.

5 A módosítások mentéséhez kattintson a *Kész* gombra.

15.2.6 Speciális beállítások

A speciális rendszerindítási beállítások a *Rendszertöltő telepítése* > *Rendszertöltő paraméterei* részben állíthatók be. Általában nincs szükség az alapértelmezett beállítások módosítására.

Rendszertöltő partíció aktiválása
: Aktiválja a rendszertöltőt tartalmazó partíciót. Egyes régebbi operációs rendszerek, például a Windows 98, kizárólag aktív partícióról tudnak csak elindulni.

Nyomkövetési jelző
: A GRUB-ot nyomkövetési módban indítja el, amelyben kiír a lemez műveleteivel kapcsolatos üzeneteket.

MBR helyettesítése általános kóddal
: Az aktuális MBR-t általános, operációs rendszertől független kóddal helyettesíti.

Menü elrejtése rendszerindításkor
: Elrejti a rendszerindító menüt és az alapértelmezett bejegyzést indítja el.

Megbízható GRUB használata
: A megbízható számítástechnikával kapcsolatos funkciókat támogató Megbízható GRUB-ot indítja el.

Soros kapcsolat paraméterei
: Ha a gépet soros kapcsolatos keresztül vezérli, akkor megadhatja, melyik COM-portot kívánja használni, milyen sebességgel. Ilyenkor a *Terminál definíció* értéke is „serial” kell, hogy legyen. További részletekért adja ki az `info grub` parancsot, vagy látogasson el a `http://www.gnu.org/software/grub/manual/grub.html` webhelyre.

Terminál definíció
: Ha soros konzolon keresztül indítja a rendszert, akkor írja be, hogy „serial”, ellenkező esetben hagyja üresen. Ebben az esetben meg kell adni a *Soros kapcsolat paraméterei*-t is.

15.2.7 A rendszertöltő típusának módosítása

Adja meg a rendszertöltő típusát a *Rendszertöltő telepítése* lapon. Az openSUSE alapértelmezett rendszertöltője a GRUB. LILO használatához tegye a következőket:

15.6. eljárás *A rendszertöltő típusának módosítása*

1. Válassza ki a *Rendszertöltő telepítése* lapot.
2. A *Rendszertöltő*-nél válassza ki a *LILO* lehetőséget.
3. A megnyíló párbeszédablakban válassza ki a következő műveletek valamelyikét:

   Új konfiguráció ajánlása
   : A YaST ajánljon új konfigurációt.

Az aktuális konfiguráció átalakítása.
: A YaST alakítsa át az aktuális konfigurációt A konfiguráció átalakítása során bizonyos beállítások elveszhetnek.

Teljesen új konfiguráció készítése.
: Egyedi konfiguráció írása. Ez a művelet nem érhető el az openSUSE telepítése során.

Lemezre mentett konfiguráció olvasása.
: Saját `/etc/lilo.conf` betöltése. Ez a művelet nem érhető el az openSUSE telepítése során.

4. A módosítások mentéséhez kattintson az *OK* gombra.

5. A változások érvényre juttatásához kattintson a *Kész* gombra.

Az átalakítás során a régi GRUB konfigurációt a rendszer elmenti a lemezre. Ennek használatához egyszerűen állítsa vissza a rendszertöltő típusát GRUB értékre és válassza az *Átalakítás előtt elmentett konfiguráció visszaállítása* lehetőséget. Ez a művelet csak a már telepített rendszereken végezhető el.

MEGJEGYZÉS: Egyedi rendszertöltő

Ha más rendszertöltőt szeretne használni, mint a GRUB vagy a LILO, válassza a *Ne kerüljön telepítésre rendszertöltő* lehetőséget. Mielőtt ezt választaná, gondosan olvassa el a saját rendszertöltőjének dokumentációját!

15.3 A Linux-rendszertöltő eltávolítása

A YaST segítségével eltávolítható a Linux rendszertöltő, és az MBR visszaállítható a Linux telepítése előtti állapotba. A telepítés során a YaST automatikusan létrehoz egy biztonsági mentést az eredeti MBR-ről és kérésre visszaállítja azt.

A GRUB eltávolításához indítsa el a YaST rendszertöltő modult (*Rendszer > Rendszertöltő beállítása*). Válassza ki az *Egyéb > A merevlemez MBR-ének visszaállítása* menüpontot, majd erősítse meg az *Igen, írja felül* gombbal.

15.4 Rendszerindító CD-k készítése

Ha problémák lépnek fel a rendszertöltővel végzett indításkor, vagy ha a rendszertöltő nem telepíthető a merevlemez vagy kislemez MBR-jére, akkor létre lehet hozni egy indítható CD-t a Linux indításához szükséges összes fájllal. Ehhez egy telepített CD-íróra van szükség.

Az indítható CD-ROM létrehozásához a GRUB segítségével csupán a *stage2* egy `stage2_eltorito` nevű, speciális formájára van szükség, illetve igény esetén egy testreszabott `menu.lst` fájlra. A klasszikus `stage1` és `stage2` fájlokra nincs szükség.

15.7. eljárás *Rendszerindító CD-k készítése*

1. Váltson át abba a könyvtárba, amelyben az ISO-rendszerképfájl elő lesz állítva, például: `cd /tmp`

2. Hozzon létre egy alkönyvtárat a GRUB számára, és váltson át a frissen létrehozott `iso` könyvtárba:

   ```
   mkdir -p iso/boot/grub && cd iso
   ```

3. A kernelt, valamint a `stage2_eltorito`, `initrd`, `menu.lst` és `message` fájlokat másolja át az `iso/boot/` könyvtárba:

   ```
   cp /boot/vmlinuz boot/
   cp /boot/initrd boot/
   cp /boot/message boot/
   cp /usr/lib/grub/stage2_eltorito boot/grub
   cp /boot/grub/menu.lst boot/grub
   ```

4. Állítsa be a `/boot/grub/menu.lst` elérési út bejegyzéseit, hogy azok a CD-ROM eszközre mutassanak Ehhez cserélje le a merevlemezek `(hdx,y)` formátumú eszközneveit az elérési utakban arra, hogy `cd`, vagyis a CD-ROM meghajtó eszköznevére. Lehet, hogy módosítania kell az üzenetfájl, a kernel és az initrd elérési útjait is – ezeknek rendre a `/boot/message`, `/boot/vmlinuz` és `/boot/initrd` helyekre kell mutatniuk. A módosítások után a `menu.lst` fájl az alábbihoz hasonló képet kell, hogy mutasson:

   ```
   timeout 8
   default 0
   gfxmenu (cd)/boot/message
   ```

```
title Linux
   root (cd)
   kernel /boot/vmlinuz root=/dev/sda5 vga=794 resume=/dev/sda1 \
   splash=verbose showopts
   initrd /boot/initrd
```

A `splash=verbose` helyett használja a `splash=silent` beállítást, hogy ne jelenjenek meg az üzenetek a rendszerindítási folyamat közben.

5 Hozza létre az ISO-képfájlt az alábbi paranccsal:

```
genisoimage -R -b boot/grub/stage2_eltorito -no-emul-boot \
-boot-load-size 4 -boot-info-table -iso-level 2 -input-charset utf-8 \
-o grub.iso /tmp/iso
```

6 A preferált segédprogram segítségével írja az eredményül kapott `grub.iso` fájlt egy CD-re. Ne adatfájlként írja ki az ISO-képfájlt; használja a segédprogram képfájlmásoló funkcióját.

15.5 A grafikus SUSE képernyő

Ha a `vga=`*`érték`* kernelparamétert használja, akkor a grafikus SUSE képernyő jelenik meg az első konzolon. A YaST segítségével történő telepítés esetén ez az opció automatikusan aktiválódik a kiválasztott felbontásnak és grafikus kártyának megfelelően. A SUSE képernyő háromféleképpen tiltható le, ha szükséges:

A SUSE képernyő szükség szerinti letiltása
: A grafikus képernyő letiltásához a parancssorban adja ki az `echo 0 >/proc/splash` parancsot. Az újbóli aktiváláshoz adja ki az `echo 1 >/proc/splash` parancsot.

A SUSE képernyő alapértelmezés szerinti letiltása.
: Adja hozzá a `splash=0` kernelparamétert a rendszertöltő beállításaihoz. További információ: 15. fejezet - *A rendszertöltő* (201. oldal). Ha a szöveges módot preferálja, amely a korábbi verziók alapértelmezett beállítása volt, akkor állítsa be a `vga=normal` értéket.

A SUSE képernyő teljes letiltása.
: Fordítson le egy új kernelt és a *keretpuffer támogatása* részben tiltsa le a *Nyitóképernyő használata rendszerindítási logó helyett* opciót.

TIPP

A kernel keretpuffer támogatásának letiltása a nyitóképernyőt is automatikusan letiltja. A SUSE egyéni kernel használatakor nem tud támogatást biztosítani a rendszerhez.

15.6 Hibaelhárítás

Ez a rész a GRUB segítségével való rendszerindítás néhány gyakori problémáját sorolja fel és röviden leírja a lehetséges megoldásokat. A problémák egy részével a Támogatási adatbázis `http://en.opensuse.org/SDB:SDB` cikkei foglalkoznak. A keresési párbeszédablaka segítségével keressen rá néhány kulcsszóra, mint például a *GRUB*, a *rendszerindítás* és a *rendszertöltő*.

A GRUB és az XFS
: Az XFS a partícióindító blokkban nem hagy helyet a `stage1` számára. Ezért a rendszertöltő helyeként nem szabad megadni XFS partíciót. Ez a probléma egy külön indítási partíció létrehozásával oldható meg, amely nem XFS-sel van formázva.

A GRUB GRUB Geom Error hibát jelent
: A GRUB a rendszer indításakor ellenőrzi a csatlakoztatott merevlemezek geometriáját. Bizonyos esetekben a BIOS inkonzisztens információt ad vissza és a GRUB GRUB Geom Error hibát jelez. Ebben az esetben frissítse a BIOS-t.

  A GRUB akkor is ezt a hibaüzenetet adja vissza, ha a Linux a BIOS-ban nem bejegyzett merevlemezre lett telepítve. A rendszertöltő *stage1* része megtalálható és megfelelően betöltésre került, de a *stage2* nem található. Ez a probléma az új hardver BIOS-ban való bejegyzésével megoldható.

Nem indul el a több merevlemezt tartalmazó rendszer
: Elképzelhető, hogy a YaST a telepítés során rosszul határozta meg a merevlemezek indítási sorrendjét (és ez nem lett kijavítva). A GRUB az IDE-lemezre `hd0`-ként és az SCSI-lemezre `hd1`-ként hivatkozhat, pedig a BIOS-ban lévő indítási sorrend fordított (SCSI *előtt* IDE).

  Ebben az esetben az indítási folyamat során a GRUB-parancssor segítségével javítsa ki a merevlemezeket. A rendszer indulása után az új leképezés állandósítása érde-

kében módosítsa a `device.map` fájlt. Ezután a `/boot/grub/menu.lst` és `/boot/grub/device.map` fájlokban ellenőrizze a GRUB-eszközneveket, majd az alábbi parancs segítségével telepítse újra a rendszertöltőt:

```
grub --batch < /etc/grub.conf
```

Windows indítása a második merevlemezről
: Néhány operációs rendszer, mint például a Windows, csak az első merevlemezről indítható. Ha egy ilyen operációs rendszer nem az első merevlemezre van telepítve, akkor a megfelelő menübejegyzés logikailag módosítható.

```
...
title windows
   map (hd0) (hd1)
   map (hd1) (hd0)
   chainloader(hd1,0)+1
...
```

Ebben a példában a Windows a második merevlemezről lesz elindítva. E célból a merevlemezek logikai sorrendje a `map` paranccsal meg lett változtatva. Ez a módosítás nem befolyásolja a GRUB-menüfájl logikáját. A `chainloader` számára a második merevlemezt kell megadni.

15.7 További információk

A GRUB-bal kapcsolatos bővebb információ a `http://www.gnu.org/software/grub/` címen található. Érdemes elolvasni a `grub` info oldalait is. A speciális esetekkel kapcsolatos tudnivalók eléréséhez a `http://www.opensuse.org/` címen található Támogatási adatbázisban rákereshet az „SDB:GRUB” kifejezésre.

16 Speciális rendszerjellemzők

Ez a fejezet a különféle szoftvercsomagokról, a virtuális konzolokról, valamint a billentyűzetkiosztásról tartalmaz információt. Szó lesz olyan szoftverkomponensekről, mint a `bash`, a `cron` és a `logrotate`, mivel ezek megváltoztak vagy bővültek a legutóbbi kiadási ciklusokban. Még akkor is, ha kicsik, vagy csekély fontosságúak, előfordulhat, hogy a felhasználók meg kívánják változtatni az alapértelmezett viselkedésüket, mivel ezek az összetevők jellemzően igen szorosan vannak csatolva a rendszerhez. A fejezet végén egy külön szakasz szól a nyelv- és országspecifikus beállításokról (I18N és L10N).

16.1 Információ speciális szoftvercsomagokról

A `bash`, a `cron`, a `logrotate`, a `locate`, az `ulimit` és a `free` programok, illetve a `resolv.conf` fájl nagyon fontosak a rendszergazdák és sok felhasználó számára. A kézikönyvoldalak és az info oldalak hasznos forrás a parancsokkal kapcsolatban, de nem mindig érhető el mind a kettő. A GNU Emacs egy népszerű, nagyon jól konfigurálható szövegszerkesztő.

16.1.1 A bash csomag és az /etc/profile

A bash az alapértelmezett parancsértelmező. Bejelentkezési parancsértelmezőként használva különféle inicializáló fájlokat olvas be. A bash az itt látható sorrendben dolgozza fel őket.

1. `/etc/profile`
2. `~/.profile`
3. `/etc/bash.bashrc`
4. `~/.bashrc`

A felhasználók saját bejegyzéseket készíthetnek a `~/.profile` és `~/.bashrc` fájlokban. E fájlok helyes feldolgozásának biztosításához át kell másolni az `/etc/skel/.profile` vagy `/etc/skel/.bashrc` alapbeállításokat a felhasználó saját könyvtárába. Célszerű a beállításokat egy frissítés után átmásolni az `/etc/skel` könyvtárból. Hajtsa végre az alábbi parancsokat a személyes beállítások elvesztésének megakadályozására:

```
mv ~/.bashrc ~/.bashrc.old
cp /etc/skel/.bashrc ~/.bashrc
mv ~/.profile ~/.profile.old
cp /etc/skel/.profile ~/.profile
```

A személyes beállításokat ezután vissza kell másolni a `*.old` fájlokból.

16.1.2 A cron csomag

A parancsok időzített, rendszeres futtatásához a háttérben a cron nevű eszköz használható. A cron speciálisan formázott időzítő táblázatokat használ. Egy részüket a rendszer tartalmazza, de a felhasználók maguk is készíthetnek táblázatokat, ha szükséges.

A cron-táblázatok a `/var/spool/cron/tabs` könyvtárban találhatók. Az `/etc/crontab` egy rendszerszintű cron- (időzítési) táblázat. A parancsot futtató felhasználó nevét közvetlenül az időzítés megadása után kell beírni. A 16.1. példa - Példa az /etc/crontab egy bejegyzésére (224. oldal) esetében ez a `root`. Az `/etc/cron.d` könyvtárban található csomagspecifikus táblázatok ugyanezt a formátumot használják. További információk a `cron` kézikönyvoldalán (`man cron`) olvashatók.

16.1 példa *Példa az /etc/crontab egy bejegyzésére*

```
1-59/5 * * * *   root   test -x /usr/sbin/atrun && /usr/sbin/atrun
```

Az `/etc/crontab` nem dolgozható fel a `crontab -e` paranccsal. Közvetlenül egy szerkesztőbe kell betölteni, módosítani, majd elmenteni.

Néhány csomag parancsfájlokat telepít az `/etc/cron.hourly`, `/etc/cron.daily`, `/etc/cron.weekly` és `/etc/cron.monthly` könyvtárakba, amelyek végrehajtását az `/usr/lib/cron/run-crons` szabályozza. Az `/usr/lib/cron/run-crons` tizenöt percenként fut le a fő táblázat (`/etc/crontab`) alapján. Ez garantálja, hogy az esetleg elhanyagolt folyamatok is megfelelő időben le legyenek futtatva.

Az `hourly` (óránkénti), `daily` (napi) és egyéb periodikus rendszerkarbantartási feladatok egyéni időben történő futtatásához távolítsa el rendszeresen az időbélyegfájlokat az `/etc/crontab` fájlba megfelelő bejegyzéseket felvéve (lásd: 16.2. példa - /etc/crontab: Az időbélyegfájlok eltávolítása (225. oldal), amely az `hourly`, vagyis az óránkénti bejegyzéseket távolítja el minden teljes óra előtt, a `daily` bejegyzéseket pedig naponta egyszer, hajnal 2:14-kor stb).

16.2 példa */etc/crontab: Az időbélyegfájlok eltávolítása*

```
59 *  * * *     root  rm -f /var/spool/cron/lastrun/cron.hourly
14 2  * * *     root  rm -f /var/spool/cron/lastrun/cron.daily
29 2  * * 6     root  rm -f /var/spool/cron/lastrun/cron.weekly
44 2  1 * *     root  rm -f /var/spool/cron/lastrun/cron.monthly
```

Alternatív megoldásként állítsa be az `/etc/sysconfig/cron` fájlban a `DAILY_TIME` értékét arra az időre, amikor a `cron.daily` induljon. A `MAX_NOT_RUN` beállítás garantálja, hogy a napi feladatok meg legyenek jelölve futásra, még akkor is, ha a felhasználó hosszabb ideig nem kapcsolta be a számítógépét a meghatározott `DAILY_TIME` időpontban. A `MAX_NOT_RUN` változó maximális értéke 14 nap.

A napi rendszerkarbantartási feladatok az átláthatóság kedvéért több parancsfájlba lettek szétosztva. Ezeket az `aaa_base` csomag tartalmazza. Az `/etc/cron.daily` fájlban található például a `suse.de-backup-rpmdb`, `suse.de-clean-tmp` és a `suse.de-cron-local`.

16.1.3 Naplófájlok: A logrotate csomag

A kernel és egy sor rendszerszolgáltatás (*démon*) rendszeresen rögzítik a rendszer állapotát és bizonyos eseményeket naplófájlokba. Ily módon a rendszergazda bármikor tudja ellenőrizni a rendszer állapotát, könnyebben felismerheti a hibákat vagy hibás működést, és precízen azonosítani tudja a problémákat. Ezek a naplófájlok jellemzően

a `/var/log` könyvtárban tárolódnak és napról napra több helyet foglalnak el. A `logrotate` csomag segít e fájlok méretének kézben tartásában.

A logrotate beállítása az `/etc/logrotate.conf` fájlban történik. Az `include` utasítás adja meg elsősorban a további beolvasandó fájlokat. A naplófájlokat előállító programok saját konfigurációs fájlokat telepítenek az `/etc/logrotate.d` könyvtárba. Például ilyen programok részei az `apache2` (`/etc/logrotate.d/apache2`) és a `syslogd` (`/etc/logrotate.d/syslog`) csomagoknak.

16.3 példa *Példa az /etc/logrotate.conf fájlra*

```
# see "man logrotate" for details
# rotate log files weekly
weekly

# keep 4 weeks worth of backlogs
rotate 4

# create new (empty) log files after rotating old ones
create

# uncomment this if you want your log files compressed
#compress

# RPM packages drop log rotation information into this directory
include /etc/logrotate.d

# no packages own lastlog or wtmp - we'll rotate them here
#/var/log/wtmp {
#    monthly
#    create 0664 root utmp
#    rotate 1
#}

# system-specific logs may be also be configured here.
```

A működését a cron szabályozza és naponta az `/etc/cron.daily/logrotate` hívja meg.

FONTOS

A `create` utasítás beolvassa a rendszergazda összes beállítását az `/etc/permissions*` fájlokból. Ügyeljen rá, hogy a saját módosításokból ne származzon ütközés.

16.1.4 A locate parancs

A locate parancs, amellyel a fájlok gyorsan megkereshetők, nincsen benne a szokásosan telepített szoftverek listájában. Ha hiányozna, telepítse a `findutils-locate` csomagot. Az updatedb folyamat automatikusan elindul minden éjszaka, vagy mintegy 15 perccel a rendszer elindítása után.

16.1.5 Az ulimit parancs

Az `ulimit` (*user limits*, azaz felhasználói korlátozások) paranccsal lehet beállítani és megjeleníteni a rendszererőforrásokra vonatkozó korlátozásokat. Az `ulimit` parancs különösen hasznos az alkalmazások rendelkezésére álló memória korlátozásában. Így megakadályozható, hogy egy alkalmazás túlságosan sok memóriát használjon el, ami esetleg lefagyaszthatná a rendszert.

Az `ulimit` különféle paraméterekkel használható. A memóriahasználat korlátozására használja az 16.1 táblázat - `ulimit`: Felhasználói erőforrások korlátozása (227. oldal) táblázatban bemutatott paramétereket.

16.1. táblázat *ulimit: Felhasználói erőforrások korlátozása*

`-m`	a maximális rezidens halmaz mérete
`-v`	a parancsértelmező számára rendelkezésre álló maximális virtuális memória
`-s`	a verem maximális mérete
`-c`	a létrehozott core fájlok maximális mérete
`-a`	minden aktuális korlát jelentésre kerül

A rendszerszintű beállítások az `/etc/profile` fájlban adhatók meg. Itt lehet engedélyezni a core fájlok létrehozását, amelyekre a programozóknak van szükségük a *hibakereséshez*. A normál felhasználók nem növelhetik meg a rendszergazda által az `/etc/profile` fájlban megadott értékeket, de készíthetnek bejegyzéseket a saját `~/.bashrc` fájljukban.

16.4 példa *ulimit: A ~/.bashrc beállításai*

```
# Limits maximum resident set size (physical memory):
ulimit –m 98304

# Limits of virtual memory:
ulimit –v 98304
```

A memória mennyiségét kilobájtban kell megadni. Részletesebb információ a `man bash` kézikönyvoldalon található.

FONTOS

Nem minden parancsértelmező támogatja az `ulimit` direktíváit. A PAM (például a `pam_limits`) átfogó finomhangolási lehetőségeket biztosít, ha meg kell birkózni ezekkel a korlátozásokkal.

16.1.6 A free parancs

A `free` parancs egy kicsit félrevezető lehet, ha azt kell kideríteni, hogy mennyi RAM-ot is használ éppen a rendszer. A kérdéses információ egyébként a `/proc/meminfo` fájlban található. Manapság, egy olyan modern operációs rendszert használva, mint a Linux, igazából nem kell a rendelkezésre álló memória mennyiségével foglalkozni. A *rendelkezésre álló memória* fogalma még az egyesített memóriakezelés előtti időkből származik. Valójában a Linux esetén is igaz a *szabad memória rossz memória* szabály. A Linux mindig is arra törekedett, hogy kiegyensúlyozza a különböző átmeneti és gyorsítótárakat anélkül, hogy valójában hagyna memóriát parlagon heverni.

A kernel tulajdonképpen semmilyen közvetlen információval nem rendelkezik az egyes alkalmazásokról vagy felhasználói adatokról. Az alkalmazásokat és a felhasználói adatokat egy *lapozási gyorsítótáron* (page cache) keresztül kezeli. Ha kezd fogyni a memória, akkor annak egyes részei a cserepartícióra vagy fájlokba íródnak, ahonnan az `mmap` parancs segítségével olvashatók be (lásd `man mmap`).

A kernel más gyorsítótárakat is tartalmaz. llyen például a *slab cache*, amelyben a hálózati hozzáféréshez szükséges tárolók találhatók. Mindez talán megmagyarázza a `/proc/meminfo` fájl számlálói közötti eltéréseket. A legtöbb, bár nem az összes, elérhető a `/proc/slabinfo`-n keresztül.

16.1.7 Az /etc/resolv.conf fájl

A tartománynevek feloldása az `/etc/resolv.conf` fájlon keresztül történik.További információk: 22. fejezet - *A DNS (tartománynévrendszer, Domain Name System)* (343. oldal).

Ezt a fájlt kizárólag az `/sbin/modify_resolvconf` parancsfájl frissíti, és semmilyen más programnak nincs jogosultsága az `/etc/resolv.conf` közvetlen módosítására. E szabály következetes betartásával garantálható csak, hogy a rendszer hálózati beállításai és az érintett fájlok konzisztens állapotban maradjanak.

16.1.8 Kézikönyvoldalak (man) és info oldalak

Egyes GNU-alkalmazások (például a tar) esetében a kézikönyvoldalakat már nem tartja karban senki. E parancsok esetében a `--help` paraméterrel lehet gyors áttekintést kapni, illetve az info oldalak tartalmaznak részletesebb magyarázatot. Az info a GNU hiperszöveg-kezelő rendszere. A rendszerről bemutatkozó szöveget az `info info` parancs beírásával kaphat. Az info oldalak az Emacs segítségével is megtekinthetők az `emacs -f info` parancs beírásával, vagy a konzolban közvetlenül beírt `info` paranccsal. Az info oldalak megtekintéséhez használható még a tkinfo, az xinfo, valamint a súgórendszer.

16.1.9 A GNU Emacs beállításai

A GNU Emacs egy összetett munkakörnyezet. Az alábbi részben áttekintjük, hogyan kerülnek feldolgozásra a konfigurációs fájlok a GNU Emacs indításakor. További információ a `http://www.gnu.org/software/emacs/` oldalon található.

Indításkor az Emacs számos fájlt beolvas, amelyek a felhasználó, a rendszergazda, valamint a testreszabó vagy előzetesen beállító disztribútor beállításait tartalmazzák. A `~/.emacs` fájl az egyes felhasználók saját könyvtáraiban kerül telepítésre, az `/etc/skel` sablon alapján. A `.emacs` az `/etc/skel/.gnu-emacs` fájlt olvassa be. A program testreszabásához másolja át a `.gnu-emacs` fájlt a saját könyvtárába (a `cp /etc/skel/.gnu-emacs ~/.gnu-emacs` paranccsal) és ott végezze el a kívánt beállításokat.

A `.gnu-emacs` a `~/.gnu-emacs-custom` fájlt mint `custom-file` adja meg. Ha a felhasználók módosítják a beállításokat az Emacs `customize` utasításaival, akkor ezek a `~/.gnu-emacs-custom` fájlba mentődnek el.

openSUSE alatt az `emacs` csomag telepíti a `site-start.el` fájlt az `/usr/share/emacs/site-lisp` könyvtárban. A `site-start.el` fájl az `~/.emacs` fájl előtt töltődik be. A `site-start.el` több más dolog mellett arról gondoskodik, hogy az Emacs kiegészítő csomagjaival, például a `psgml` csomaggal együtt kapott speciális konfigurációs fájlok automatikusan betöltődjenek. Az ilyen típusú konfigurációs fájlok szintén az `/usr/share/emacs/site-lisp` könyvtárban találhatók, és a nevük mindig úgy kezdődik, hogy `suse-start-`. A helyi rendszergazda a `default.el` fájlban adhat meg az egész rendszerre érvényes beállításokat.

Ezekről a fájlokról további információ az Emacs info fájljában, az *Init File* részben található: `info:/emacs/InitFile`. Itt arról is olvashat, hogyan lehet letiltani ezeknek a fájloknak a betöltését (ha szükséges).

Az Emacs komponensei több csomagba vannak osztva:

- Az alapcsomag az `emacs`.
- `emacs-x11` (általában telepítésre kerül): a program *X11-támogatással*.
- `emacs-nox`: a program X11-támogatás *nélkül*.
- `emacs-info`: online dokumentáció info formátumban.
- `emacs-el`: a lefordítatlan könyvtárfájlok Emacs Lispben. Ezek nem szükségesek a futtatáshoz.
- Igény esetén számos kiegészítő csomag is telepíthető: `emacs-auctex` (LaTeX-hez), `psgml` (SGML-hez és XML-hez), `gnuserv` (kliens- és kiszolgálóműveletekhez) és még sokminden más.

16.2 Virtuális konzolok

A Linux egy többfeladatos és többfelhasználós operációs rendszer. Ennek előnyeit előbb-utóbb értékelni fogjuk, még akkor is, ha számítógépünket csak egyedül használjuk.

Szöveges módban hat virtuális konzol áll rendelkezésre. Ezek között az Alt + F1 – Alt + F6 billentyűkombinációkkal lehet váltani. A hetedik konzol az X, a grafikus felület számára van lefoglalva, a tizedik pedig a kernel üzeneteit jeleníti meg. Az `/etc/inittab` fájl módosításával több vagy kevesebb konzol is beállítható.

Ha a grafikus felületről kíván átkapcsolni egy szöveges konzolra az X leállítása nélkül, használja a Ctrl + Alt + F1 – Ctrl + Alt + F6 billentyűkombinációkat. A szöveges képernyőről az Alt + F7 lenyomásával lehet visszatérni az X környezet alá.

16.3 Billentyűzet-leképezés

A programok billentyűzet-leképezésének szabványosítása érdekében az alábbi fájlok módosításra kerültek:

```
/etc/inputrc
/etc/X11/Xmodmap
/etc/skel/.Xmodmap
/etc/skel/.exrc
/etc/skel/.less
/etc/skel/.lesskey
/etc/csh.cshrc
/etc/termcap
/usr/lib/terminfo/x/xterm
/usr/share/X11/app-defaults/XTerm
/usr/share/emacs/VERSION/site-lisp/term/*.el
```

Ezek a változások csak azokat az alkalmazásokat érintik, amelyek a `terminfo` bejegyzéseit használják, vagy amelyek konfigurációs fájljai közvetlenül kerülnek módosításra (`vi`, `less` stb). A szállított rendszer részét nem képező alkalmazásokban ezekhez az alapértelmezésekhez kell igazodni.

X alatt az összetétel billentyű (multikey) a Ctrl + Shift (jobb) segítségével érhető el. Tekintse meg továbbá az `/etc/X11/Xmodmap` vonatkozó bejegyzését.

További beállítások az X Keyboard Extension (XKB) segítségével lehetségesek. Ezt a kiterjesztést használja a GNOME (gswitchit) és KDE (kxkb) asztali környezet is.

TIPP: További információk

Az XKB-ről az `/etc/X11/xkb/README` és a benne felsorolt dokumentumok tartalmaznak információt.

Részletes információ a kínai, japán és koreai (CJK) karakterek beviteléről Mike Fabian oldalán olvasható: http://www.suse.de/~mfabian/suse-cjk/input.html.

16.4 Nyelv- és országspecifikus beállítások

A rendszer igen nagy mértékben lokalizálható és igen rugalmasan a helyi igényekhez igazítható. Más szavakkal, a nemzetközi igényekhez alakítás (*internationalization, I18N*) lehetővé teszi az egyedi honosítást (*localization, L10N*). Az I18N és L10N rövidítések az angol szavak első és utolsó betűjéből, illetve a kihagyott betűk számából származnak.

A beállításokat az `/etc/sysconfig/language` fájlban található `LC_` változókkal lehet megadni. Ezek nemcsak a *nemzeti nyelv támogatására* vonatkoznak, hanem az *Üzenetek* (nyelv), *Karakterkészlet*, *Rendezési sorrend*, *Dátum és idő*, *Számok* és a *Pénznem* beállítására is. A kategóriák mindegyike megadható közvetlenül a saját változójával, vagy közvetve, a `language` fájl egy fő változójával (lásd a `man locale` kézikönyvoldalt).

`RC_LC_MESSAGES`, `RC_LC_CTYPE`, `RC_LC_COLLATE`, `RC_LC_TIME`, `RC_LC_NUMERIC`, `RC_LC_MONETARY`
: Ezek a változók az `RC_` előtag nélkül kerülnek átadásra a parancsértelmezőnek, és ezek szabályozzák a fenti kategóriákat. Az érintett parancsértelmező-profilok listája alább látható. Az aktuális beállítások a `locale` paranccsal jeleníthetők meg.

`RC_LC_ALL`
: Ez a változó (ha be van állítva) felülírja a fent említett változók értékét.

`RC_LANG`
: Ha a fenti változók egyike sincs beállítva, a rendszer ezt használja maradék lehetőségként. Alapértelmezésben csak az `RC_LANG` változó van beállítva. Így egyszerűbb a felhasználóknak beírniuk a saját értékeiket.

ROOT_USES_LANG
: Egy yes vagy no értékű változó. Ha az értéke yes, akkor a root mindig a POSIX környezetben dolgozik.

A többi változó a YaST sysconfig-szerkesztőjével állítható be (lásd: 14.3.1. - A rendszerkonfiguráció módosítása a YaST sysconfig-szerkesztőjével (197. oldal)). Az ilyen változók értéke egy nyelvkódból, egy országkódból, egy kódolásból és egy módosítóból áll. Az egyes elemeket speciális karakterek kötik össze:

```
LANG=<language>[[_<COUNTRY>].<Encoding>[@<Modifier>]]
```

16.4.1 Néhány példa

A nyelv és az ország kódját mindig egyszerre kell állítani. A nyelv megadása az ISO 639-es szabványt követi (http://www.evertype.com/standards/iso639/iso639-en.html és http://www.loc.gov/standards/iso639-2/). Az országkódokat az ISO 3166 sorolja fel (http://www.din.de/gremien/nas/nabd/iso3166ma/codlstp1/en_listp1.html).

Csak olyan értékeket célszerű megadni, amelyhez használható leírófájlok találhatók az /usr/lib/locale könyvtárban. További leírófájlok létrehozhatók az /usr/share/i18n könyvtár fájljaiból a localedef paranccsal. A leírófájlok a glibc-i18ndata csomag részei. Az en_US.UTF-8 (angol nyelvű, Egyesült Államok) leírófájlja például a következő paranccsal hozható létre:

```
localedef -i en_US -f UTF-8 en_US.UTF-8
```

LANG=en_US.UTF-8
: Ez az alapértelmezett beállítás, ha a telepítés során az amerikai angol a kiválasztott nyelv. Ha más nyelvet választott, az a nyelv kerül bekapcsolásra, de a karakterkódolás továbbra is UTF-8.

LANG=en_US.ISO-8859-1
: Ez angol nyelvet állít be, az ország az Egyesült Államok, a karakterkódolás pedig ISO-8859-1. Ez a karakterkészlet nem támogatja az euro pénznem jelét, de hasznos lehet olyan programok esetében, amelyek még nincsenek felkészítve az UTF-8 kódolás használatára. A karakterkészletet megadó karaktersorozatot (ami

a jelen esetben az ISO-8859-1) ezután a programok, például az Emacs értékeli ki.

LANG=en_IE@euro
: A fenti példa kifejezetten tartalmazza az euro karaktert egy nyelvi beállításban. Szigorúan véve ez a beállítás mára túlhaladott, hiszen az UTF-8 szintén tartalmazza az euro szimbólumot. Csak akkor hasznos, ha a használni kívánt alkalmazás nem támogatja az UTF-8 kódolást, csak az ISO-8859-15-öt.

A SuSEconfig beolvassa az /etc/sysconfig/language könyvtárban található fájlokat és az /etc/SuSEconfig/profile, valamint az /etc/SuSEconfig/csh.cshrc helyekre írja ki a szükséges módosításokat. Az /etc/SuSEconfig/profile az /etc/profile-t olvassa vagy használja *forrásul*. Az /etc/SuSEconfig/csh.cshrc-t az /etc/csh.cshrc használja forrásul. Ennek hatására a beállítások az egész rendszerre kiterjedően elérhetővé válnak.

A felhasználók felülbírálhatják a rendszer alapértelmezett értékeit, ha módosítják saját ~/.bashrc fájljaikat. Ha például a rendszerszintű en_US beállítás helyett a programok üzeneteit spanyolul akarják látni, akkor az LC_MESSAGES=es_ES beállítást kell megadniuk.

16.4.2 A nyelvi támogatás beállításai az ~/.i18n fájlokban

Ha nincs megelégedve a rendszer területi beállításaival, akkor módosítsa az ~/.i18n fájl beállításait a Bash parancsnyelvi szintaxisának megfelelően. A ~/.i18n bejegyzései felülírják a rendszer /etc/sysconfig/language helyen lévő alapértelmezett beállításait. Használja ugyanazokat a változóneveket, csak az RC_ név prefixumot hagyja el (például az RC_LANG helyett használja a LANG változót:

```
LANG=cs_CZ.UTF-8
LC_COLLATE=C
```

16.4.3 A nyelvi támogatás beállításai

Az alapszabály az, hogy az *Üzenetek* kategóriába eső fájlok csak a megfelelő nyelvi könyvtárban (például en) tárolódnak, hogy legyen mire visszalépni. Ha a LANG változót

az en_US értékre állítja, viszont nem létezik az /usr/share/locale/en_US/LC_MESSAGES könyvtárban a message fájl, akkor a rendszer az /usr/share/locale/en/LC_MESSAGES fájlhoz tér vissza.

Visszalépési lánc is megadható, például bretonról franciára, vagy galíciairól spanyolra, és onnan portugálra:

```
LANGUAGE="br_FR:fr_FR"

LANGUAGE="gl_ES:es_ES:pt_PT"
```

Így állíthatók be a norvég variánsok (a Nynorsk és a Bokmål, további visszalépéssel a sima no beállításra):

```
LANG="nn_NO"

LANGUAGE="nn_NO:nb_NO:no"
```

vagy

```
LANG="nb_NO"

LANGUAGE="nb_NO:nn_NO:no"
```

Ügyeljünk arra, hogy a norvég nyelv használata esetén az LC_TIME kezelése is eltér.

Egy lehetséges probléma, ha az ezres elválasztó karaktert nem helyesen ismeri fel a rendszer. Ez akkor fordul elő, ha a LANG értéke csak egy kétbetűs nyelvi kódra van állítva (pl. de), de a glibc által használt leírás az /usr/share/lib/de_DE/LC_NUMERIC helyen található. Ilyenkor az LC_NUMERIC változót de_DE értékre kell állítani, hogy az elválasztódefinícót helyesen lássa a rendszer.

16.4.4 További információk

- *A GNU C Library referencia-kézikönyv* „Területi beállítások és lokalizálás” c. fejezete. A glibc-info része.
- A Markus Kuhn által írt *UTF-8 and Unicode FAQ for Unix/Linux*. Jelenleg a http://www.cl.cam.ac.uk/~mgk25/unicode.html címen található.

- *Unicode-Howto*, amelyet Bruno Haible írt:`/usr/share/doc/howto/en/html/Unicode-HOWTO.html`.

Dinamikus kerneleszköz-felügyelet az udev segítségével

17

A kernel képes a futó rendszer szinte bármely eszközének hozzáadására és eltávolítására. Az eszközök állapotának változását (vagyis hogy az eszközt behelyezték, vagy eltávolították) továbbítani kell a felhasználói területre (userspace) is. Az eszközöket csatlakoztatás és azonosítás után azonnal be kell állítani. Egy adott eszköz használóit értesíteni kell az eszköz állapotának minden megváltozásáról. Az udev biztosítja a szükséges infrastruktúrát ahhoz, hogy az eszközcsomópontfájlokat és a szimbolikus láncokat dinamikusan lehessen kezelni a `/dev` könyvtárban. Az udev-szabályok egyfajta módszert biztosítanak a külső eszközöknek a kernel eszközesemény-feldolgozásba becsatlakoztatásához. Ily módon testreszabható az udev eszközkezelése: például végrehajthatók meghatározott parancsfájlok a kernel eszközkezelésének részeként, vagy kérhetők és importálhatók további adatok kiértékelésre az eszközkezelés közben.

17.1 A /dev könyvtár

A `/dev` könyvtárban található eszközcsomópontok biztosítanak hozzáférést a megfelelő kernel eszközökhöz. Az udev használata esetén a `/dev` könyvtár a kernel aktuális állapotát tükrözi. Minden kerneleszközhöz pontosan egy eszközfájl tartozik. Ha az eszközt lekapcsolják a rendszerről, akkor az eszközcsomópont is eltűnik.

A `/dev` könyvtár tartalma egy ideiglenes fájlrendszeren található, és a rendszer minden egyes indulásakor újból létrejönnek a rajta található fájlok. Az itt kézzel létrehozott vagy szándékosan módosított fájlok nem élik túl az újraindítást. Azokat a statikus fájlokat és könyvtárakat, amelyeknek állandóan jelen kell lenniük a `/dev` könyvtárban,

függetlenül a hozzá tartozó kerneleszköz állapotától, a `/lib/udev/devices` könyvtárba lehet helyezni. A rendszer indításakor ennek a könyvtárnak a tartalma átmásolódik a `/dev` könyvtárba, ugyanazokkal a tulajdonosokkal és jogosultságokkal, mint amelyekkel a fájlok a `/lib/udev/devices` könyvtárban rendelkeztek.

17.2 Kernel uevent-ek és az udev

Az eszközökről információt a sysfs fájlrendszer biztosít. A kernel által felismert és inicializált minden eszközhöz létrejön egy könyvtár az eszköz nevével. Ez az eszközspecifikus jellemzőket tároló attribútumfájlokat tartalmaz.

Minden egyes alkalommal, amikor egy eszközt felvesznek vagy eltávolítanak, a kernel egy uevent eseményt küld, hogy értesítse az udev-et a változásról. Az udev démon indulás után elolvassa és feldolgozza az `/etc/udev/rules.d/*.rules` fájlok összes szabályát és a memóriában tartja őket. Ha a szabályfájlok módosulnak, bővülnek vagy törlődnek, a démon az `udevadm control reload_rules` parancs hatására képes frissíteni a memóriában tárolt szabályokat. Ugyanez történik az `/etc/init.d/boot.udev reload` parancs futtatásakor. További részletek az udev-szabályokról és szintaxisukról: 17.6. - A kernel eszközesemény-kezelésének befolyásolása udev-szabályokkal (241. oldal).

Minden fogadott esemény összehasonlítódik a meglévő szabályokkal. A szabályok felvehetnek vagy módosíthatnak eseménykörnyezeti kulcsokat, kérhetnek egy adott nevet a létrehozandó eszközcsomópontnak, felvehetnek a csomópontra mutató symlinkeket, illetve felvehetnek az eszközcsomópont létrehozása után futtatandó programokat. Az illesztőprogram alap uevent eseményei egy kernel netlink socketen keresztül érkeznek.

17.3 Illesztőprogramok, kernelmodulok és eszközök

A kernel busz-illesztőprogramjai felderítik az eszközöket. Minden egyes felismert eszközhöz a kernel létrehoz egy belső eszközstruktúrát és az illesztőprogram magja egy ueventet küld az udev démonnak. A buszeszközök egy speciálisan kialakított azonosítóval azonosítják magukat, amely leírja az eszköz fajtáját is. Általában ezek az

azonosítók a gyártó és a termék azonosítójából, és egyéb, az alrendszerre jellemző értékből állnak. Minden busz saját sémát használ az azonosítók kialakítására. Ez a MODALIAS. A kernel fogja az eszköz adatait, előállítja a MODALIAS azonosítót belőle, és elküldi az eseménnyel együtt. Egy USB-egér esetén például ez így néz ki:

```
MODALIAS=usb:v046DpC03Ed2000dc00dsc00dp00ic03isc01ip02
```

Minden egyes eszköz-illesztőprogram tartalmazza az általa kezelni képes eszközök ismert neveinek listáját. Ez a lista magában a kernelmodul-fájlban található. A depmod program kiolvassa az azonosítólistákat és létrehozza belőle a `modules.alias` fájlt a kernel `/lib/modules` könyvtárában, az összes éppen rendelkezésre álló modulhoz. Ezzel az infrastruktúrával egy modul betöltése mindössze annyiból áll, hogy meg kell hívni a `modprobe`-ot minden olyan eseményhez, amelyben van `MODALIAS` kulcs. A `modprobe $MODALIAS` meghívásakor összeveti az eszközhöz kialakított nevet a modul által biztosított nevek listájával. Ha van egyező bejegyzés, akkor az a modul betöltődik. Mindezt az udev aktiválja és automatikusan történik.

17.4 Rendszerindítás és az eszközök kezdeti beállítása

Minden olyan eszközesemény, amely a rendszerindítási folyamat során még az udev démon futása előtt történik, elveszik, hiszen az ezeket az eseményeket kezelő infrrastruktúra a gyökér fájlrendszeren lakik, és az ebben az időben még nem érhető el. E veszteség fedezésére a kernel egy `uevent` nevű fájlt biztosít a sysfs fájlrendszer minden eszközéhez. A fájlba az `add` parancsot írva a kernel újraküldi ugyanazt az eseményt, amely elveszett a rendszerindítás közben. A `/sys` `uevent` fájljain egy egyszerű ciklust végrehajtva az összes esemény újragenerálható az eszközcsomópontok létrehozásához és az eszközök beállításához.

Például lehetséges, hogy rendszerindítás közben a jelen lévő USB-egeret nem inicializálja helyesen a korai rendszerindítási logika, mivel az illesztőprogram azon a ponton még nem áll rendelkezésre. Az eszköz felderítésének az eseménye elvész és nem sikerül kernelmodult találni az eszközhöz. Az esetlegesen csatlakoztatott eszközök kézi keresgélése helyett az udev egyszerűen újrakéri az összes eszközeseményt a kerneltől azután, hogy a gyökér fájlrendszer elérhetővé vált, úgyhogy az USB-egér eszköz eseménye egész egyszerűen lefut még egyszer. Most már meglesz a szükséges kernelmodul a felcsatolt gyökér fájlrendszerben, és az USB-egér gond nélkül inicializálható.

A felhasználói területen nincs látható különbség egy eszköz coldplug-sorozata és az eszköz futási időben történő felderítése között. Mindkét esetben ugyanazokat a szabályokat használja a rendszer az ellenőrzéshez és ugyanazok a beállított programok futnak le.

17.5 A futó udev démon figyelése

Az illesztőprogram alapeseményeinek és az udev-eseményfolyamatok időzítéseinek vizualizálására az `udevadm monitor` program használható.

```
UEVENT[1185238505.276660] add   /devices/pci0000:00/0000:00:1d.2/usb3/3-1
(usb)
UDEV  [1185238505.279198] add   /devices/pci0000:00/0000:00:1d.2/usb3/3-1
(usb)
UEVENT[1185238505.279527] add
/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0 (usb)
UDEV  [1185238505.285573] add
/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0 (usb)
UEVENT[1185238505.298878] add
/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/input10 (input)
UDEV  [1185238505.305026] add
/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/input10 (input)
UEVENT[1185238505.305442] add
/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/input10/mouse2 (input)
UEVENT[1185238505.306440] add
/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/input10/event4 (input)
UDEV  [1185238505.325384] add
/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/input10/event4 (input)
UDEV  [1185238505.342257] add
/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/input10/mouse2 (input)
```

Az `UEVENT` sorok a kernel által a netlinken keresztül küldött eseményeket jelzik. Az `UDEV` sorok a befejezett udev eseménykezelőket mutatják. Az időzítés mikroszekundumban van megadva. Az `UEVENT` és az `UDEV` közötti idő az az idő, amíg az udev feldolgozta az eseményt, vagy amíg az udev démon késleltette a végrehajtását, hogy szinkronizálja az eseményt kapcsolódó, már futó eseményekkel. Például a merevlemez-partíciók eseményei mindig megvárják, hogy a fő lemezeszköz-esemény befejeződjön, mert a partícióesemények használhatják azokat az adatokat, amelyeket a fő lemezesemény lekért a hardvertől.

Az `udevadm monitor --env` parancs a teljes eseménykörnyezetet megjeleníti.

```
ACTION=add
DEVPATH=/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/input10
SUBSYSTEM=input
```

```
SEQNUM=1181
NAME="Logitech USB-PS/2 Optical Mouse"
PHYS="usb-0000:00:1d.2-1/input0"
UNIQ=""
EV=7
KEY=70000 0 0 0 0
REL=103
MODALIAS=input:b0003v046DpC03Ee0110-e0,1,2,k110,111,112,r0,1,8,amlsfw
```

Az udev a rendszernaplóba (syslog) is küld üzeneteket. Az alapértelmezett syslog-prioritást, amely szabályozza, hogy mely üzenetek kerüljenek be a naplóba, az udev `/etc/udev/udev.conf` konfigurációs fájlja adja meg. A futó démon naplóprioritása az `udevadm control log_priority=`*`szint/szám`* paranccsal változtatható meg.

17.6 A kernel eszközesemény-kezelésének befolyásolása udev-szabályokkal

Az udev-szabályok az esemény bármely tulajdonságát vizsgálhatják, amelyet a kernel ad az eseményhez, vagy amelyet a kernel a `sysfs` fájlba exportál. A szabály kérhet további információkat is külső programoktól. Minden esemény összevetésre kerül a meglévő szabályokkal. A szabályok az `/etc/udev/rules.d` könyvtárban találhatók.

A szabályfájl minden egyes sora legalább egy kulcs-érték párt tartalmaz. Kétféle kulcs létezik, egyezési és hozzárendelési kulcsok. Ha az összes egyezési kulcs megegyezik az értékeikkel, akkor a szabály alkalmazva lesz és a hozzárendelési kulcsok megkapják a megadott értéket. Egy illeszkedő szabály megadhatja az eszközcsomópont nevét, felvehet a csomópontra mutató symlinkeket, vagy lefuttathat egy adott programot az eseménykezelés részeként. Ha egyetlen illeszkedő szabály sem található, akkor az alapértelmezett eszközcsomópont-nevet használja a rendszer az eszközcsomópont létrehozására. A szabály szintaxisát és az adatok vizsgálatára vagy importálására használható kulcsokat az udev kézikönyvoldala írja le részletesen. Az alábbi példaszabályok bemutatják az udev szabályszintaxisának legfontosabb elemeit. A példaszabályok mind az `/etc/udev/rules.d/50-udev-default.rules` alatt található alapértelmezett udev-halmazból lettek véve.

17.1 példa *Példa udev-szabályok*

```
# console
KERNEL=="console", MODE="0600", OPTIONS="last_rule"

# serial devices
KERNEL=="ttyUSB*", ATTRS{product}=="[Pp]alm*Handheld*", SYMLINK+="pilot"

# printer
SUBSYSTEM=="usb", KERNEL=="lp*", NAME="usb/%k", SYMLINK+="usb%k", GROUP="lp"

# kernel firmware loader
SUBSYSTEM=="firmware", ACTION=="add", RUN+="firmware.sh"
```

A `console` szabály három kulcsból áll: egy illesztési kulcsból (`KERNEL`) és két hozzárendelési kulcsból (`MODE`, `OPTIONS`). A `KERNEL` illesztési szabály végigkeresi az eszközlistát `console` típusú eszközök után. Csak a pontos egyezések számítanak találatnak a szabály végrehajtását illetően. A `MODE` kulcs speciális jogosultságokat rendel az eszközcsomóponthoz, a jelen esetben olvasási és írási jogosultságokat kizárólag az eszköz tulajdonosa számára. Az `OPTIONS` kulcs hatására ez a szabály lesz az utolsó, amelyet a rendszer az ilyen típusú eszközökre alkalmaz. Még ha később akad is szabály, amelyik megfelelne az eszköztípusnak, semmilyen hatásuk nem lesz.

A `serial devices` szabály már nem része az `50-udev-default.rules` fájlnak, de érdemes vetni rá egy pillantást. Két illesztési kulcsból (`KERNEL` és `ATTRS`) és egy hozzárendelési kulcsból (`SYMLINK`) áll. A `KERNEL` kulcs végigkeresi az eszközlistát `ttyUSB` típusú eszközök után. A `*` helyettesítő karakter használata miatt ez a kulcs több ilyen eszközt is megtalál. A második illesztési kulcs, az `ATTRS`, ellenőrzi, hogy a `sysfs product` attribútumfájlja bármely `ttyUSB` eszközre vonatkozóan tartalmaze egy bizonyos karaktersorozatot. A hozzárendelési kulcs (`SYMLINK`) hatására létrejön egy szimbolikus lánc erre az eszközre a `/dev/pilot` alatt. A kulcsban használt operátor (+=) azt jelenti az udev számára, hogy ezt a műveletet kiegészítésképpen hajtsa végre, még akkor is, ha korábbi vagy későbbi szabályok más szimbolikus láncokat hoznának létre. Mivel a szabályban két illesztési kulcs van, csak akkor lesz alkalmazva, ha mind a két feltétel teljesül.

A `printer` szabály az USB-nyomtatókra vonatkozik, és két illesztési kulcsot tartalmaz (`SUBSYSTEM` and `KERNEL`). A teljes szabály alkalmazásához mindkettőnek teljesülnie kell. Három hozzárendelési kulcs foglalkozik az eszköztípus elnevezésével (`NAME`), a szimbolikus eszközlánc létrehozásával (`SYMLINK`) és az eszköztípus csoporttagságával (`GROUP`). A `*` helyettesítő karakter hatására a `KERNEL` kulcs több `lp` nyomtatóeszközt

is megtalál. Helyettesítések vannak mind a `NAME`, mind a `SYMLINK` kulcsban, hogy ezek a karaktersorozatok kibővüljenek a belső eszköznévre. Például az első `lp` USB-nyomtató szimbolikus lánca a `/dev/usblp0` lesz.

A `kernel firmware loader` szabály hatására az udev további firmware-t tölt be futás közben egy külső segédparancsfájl használatával. A `SUBSYSTEM` illesztési kulcs a `firmware` alrendszert keresi ki. Az `ACTION` kulcs ellenőrzi, hogy a `firmware` alrendszerhez tartozó eszköz fel lett-e véve. A `RUN+=` kulcs indítja a `firmware.sh` parancsfájl végrehajtását a betöltendő firmware kikereséséhez.

Néhány jellemző egységes az összes szabályban:

- Mindegyik szabály egy vagy több vesszővel elválasztott kulcs-érték párból áll.
- A kulcs műveletét az operátor határozza meg. Az udev-szabályok többféle operátort is támogatnak.
- Minden megadott értéket idézőjelek közé kell tenni.
- A szabályfájl minden sora egy-egy szabályt ábrázol. Ha egy szabály hosszabb lenne egy sornál, akkor a `\` karakterrel lehet összekapcsolni az egymás utáni sorokat, pontosan úgy, mint a parancsértelmezőben.
- Az udev-szabályok a parancsértelmezőhöz hasonló mintaillesztést támogatnak, a `*`, `?` és `[]` helyettesítő karakterek/minták alkalmazásával.
- Az udev-szabályok támogatják a helyettesítéseket.

17.6.1 Operátorok használata az udev-szabályokban

A kulcsok létrehozásakor többféle operátor közül is lehet választani, a létrehozni kívánt kulcs típusától függően. Az illesztési kulcsok jellemzően arra szolgálnak, hogy kikeressenek egy értéket, amely vagy pontosan megegyezik, vagy éppenhogy nem egyezik meg a kereséshez megadott értékkel. Az illesztési kulcsok az alábbi operátorok valamelyikét tartalmazhatják:

==
: Egyenlőség vizsgálata. Ha a kulcs keresési mintát tartalmaz, akkor a mintának megfelelő összes eredmény érvényesnek számít.

!=
: Nem egyenlőség (eltérés) vizsgálata. Ha a kulcs keresési mintát tartalmaz, akkor a mintának megfelelő összes eredmény érvényesnek számít.

A hozzárendelési kulcsok az alábbi operátorok valamelyikét tartalmazhatják:

=
: Érték hozzárendelése egy kulcshoz. Ha a kulcs korábban értékek egy listáját tartalmazta, akkor a kulcs visszaáll és csak ez az egy érték lesz hozzárendelve.

+=
: Érték hozzáadása egy bejegyzések listáját tartalmazó kulcshoz.

:=
: Végső érték hozzáadása. Minden későbbi szabály módosítását letiltja.

17.6.2 Helyettesítések használata az udev-szabályokban

Az udev-szabályok támogatják a helykitöltők és helyettesítések használatát. Ugyanúgy használhatja őket, mint bármilyen más parancsfájlban. Az udev-szabályokban az alábbi helyettesítések használhatók:

`%r`, `$root`
: Az eszközkönyvtár, alapértelmezés szerint a `/dev`.

`%p`, `$devpath`
: A `DEVPATH` változó értéke.

`%k`, `$kernel`
: A `KERNEL` értéke vagy a belső eszköznév.

`%n`, `$szám`
: Az eszköz száma.

`%N`, `$tempnode`
: Az eszközfájl ideiglenes neve.

`%M`, `$major`
: Az eszköz fő száma.

`%m`, `$minor`
: Az eszköz alszáma.

`%s{`*`attribútum`*`}`, `$attr{`*`attribútum`*`}`
: Egy `sysfs` attribútum értéke (amelyet az *`attribútum`* határoz meg).

`%E{`*`változó`*`}`, `$attr{`*`változó`*`}`
: Egy környezeti változó értéke (amelyet a *`változó`* ad meg).

`%c`, `$eredmény`
: A `PROGRAM` kimenete.

`%%`
: A `%` karakter.

`$$`
: A `$` karakter.

17.6.3 udev illesztési kulcsok használata

Az illesztési kulcsok írják le azokat a feltételeket, amelyeknek teljesülniük kell ahhoz, hogy az udev-szabályok alkalmazhatók legyenek. Az alábbi illesztési kulcsok használhatók:

`ACTION`
: Az eseményművelet neve, például `add` vagy `remove` egy eszköz hozzáadásához vagy eltávolításához.

`DEVPATH`
: Az eseményeszköz eszköz elérési útja, például `DEVPATH=/bus/pci/drivers/ipw3945` az ipw3945 illesztőprogrammal kapcsolatos összes esemény kikereséséhez.

KERNEL
: Az esemény eszközének belső (kernel) neve.

SUBSYSTEM
: Az esemény eszközének alrendszere, például SUBSYSTEM=usb az összes USB-eszközzel kapcsolatos eseményhez.

ATTR{*fájlnév*}
: Az esemény eszközének sysfs attribútumai. A fájlnév vendor attribútumában található karaktersorozat kereséséhez használható, például ATTR{vendor}=="On[sS]tream".

KERNELS
: Végigkeresteti az udev-vel az eszköz elérési utat felfelé egy illeszkedő eszköznév után.

SUBSYSTEMS
: Végigkeresteti az udev-vel az eszköz elérési utat felfelé egy illeszkedő alrendszernév után.

DRIVERS
: Végigkeresteti az udev-vel az eszköz elérési utat felfelé egy illeszkedő eszköz-illesztőprogram után.

ATTRS{*fájlnév*}
: Végigkeresteti az udev-vel az eszköz elérési utat felfelé egy illeszkedő sysfs attribútumértékű eszköz után.

ENV{*kulcs*}
: Egy környezeti változó értéke, például ENV{ID_BUS}="ieee1394" a FireWire busz azonosítóval kapcsolatos események kikereséséhez.

PROGRAM
: Végrehajtat az udev-vel egy külső programot. A sikerhez a programnak nulla kilépési kóddal kell visszatérnie. A program (a standard kimenetre írt) kimenete a RESULT kulcsban érhető el.

RESULT
: A legutolsó PROGRAM hívás kimenetének felel meg. Használhatja ezt a kulcsot ugyanabban a szabályban, mint amelyikben a PROGRAM kulcsot, de lehet egy későbbiben is.

17.6.4 Az udev hozzárendelési kulcsainak használata

Szemben a fent leírt illesztési kulcsokkal, a hozzárendelési kulcsok nem a teljesítendő feltételeket írják le, hanem értékeket, neveket és műveleteket rendelnek az udev által kezelt eszközcsomópontokhoz.

NÉV
: A létrehozandó eszközcsomópont neve. Miután a szabály beállította a csomópont nevét, a csomópontra vonatkozó összes többi NAME kulcs figyelmen kívül marad.

SYMLINK
: A létrehozandó csomóponttal kapcsolatos szimbolikus lánc neve. Több illesztési szabály is megadható szimbolikus láncok létrehozására az eszközcsomóponttal együtt. Több szimbolikus lánc is megadható egy csomópothoz egy szabályban, szóközzel elválasztva a szimbolikus láncok neveit.

OWNER, GROUP, MODE
: Egy új eszközcsomópont jogosultságai. Az itt megadott értékek felülírják a befordított értékeket.

ATTR{*key*}
: Az esemény eszközének sysfs attribútumába írandó értéket adja meg. Az == operátor használata esetén ez a kulcs használható egy sysfs attribútum értékének vizsgálatára is.

ENV{*kulcs*}
: Kiexportáltat az udev-vel egy változót a környezetbe. Az == operátor használata esetén ez a kulcs használható egy környezeti változó értékének vizsgálatára is.

RUN
: Felvetet az udev-vel egy programot az eszközhöz végrehajtandó programok listájába. Ügyeljen rá, hogy ezek igen rövid feladatok legyenek, hogy ne blokkolják az eszköz későbbi eseményeit.

LABEL
: Egy címkét ad meg, amelyre majd a GOTO ugrani tud.

GOTO
: Kihagyat az udev-vel egy sor szabályt, és azzal folytatja, amelynek a címkéjére a GOTO kulcs hivatkozik.

IMPORT{*típus*}
: Betölt változókat az esemény környezetébe (például egy külső program kimenetét). Az udev többféle típusú változót képes importálni. Ha nincs típus megadva, akkor az udev megpróbálja meghatározni a típust a fájljogosultságok végrehajtás bitje alapján.

  - A program hatására az udev végrehajt egy külső programot és beimportálja annak kimenetét.
  - A file hatására az udev egy szövegfájlt importál.
  - A parent hatására az udev a szülő eszközből importálja a tárolt kulcsokat.

WAIT_FOR_SYSFS
: Arra utasítja az udev-et, hogy várja meg, hogy létrejöjjön a megadott sysfs fájl egy adott eszközhöz, például a WAIT_FOR_SYSFS="ioerr_cnt" hatására az udev megvárja, amíg létrejön az ioerr_cnt fájl.

KAPCSOLÓK
: Az OPTION kulcsnak többféle értéke is lehet:

  - A last_rule hatására az udev figyelmen kívül hagyja az összes későbbi szabályt.
  - Az ignore_device hatására az udev az egész eseményt figyelmen kívül hagyja.

- Az `ignore_remove` hatására az udev figyelmen kívül hagyja az eszköz összes későbbi eseményét.

- Az `all_partitions` hatására az udev eszközcsomópontokat készít egy blokkeszköz minden rendelkezésre álló partíciója számára.

17.7 Állandó eszköz-elnevezés

A dinamikus eszközkönyvtár és az udev szabályinfrastruktúrája lehetővé teszi az összes lemezes eszköz állandó elnevezését – függetlenül attól, hogy milyen sorrendben ismerte fel őket a rendszer, vagy milyen kapcsolatot használ az adott eszköz. A kernel által létrehozott minden megfelelő blokkeszközt olyan eszközök vizsgálnak, amelyek speciális ismeretekkel rendelkeznek bizonyos buszokról, meghajtótípusokról vagy fájlrendszerekről. A kernel által biztosított dinamikus eszközcsomópont-név mellett az udev az eszközre mutató állandó szimbolikus láncok osztályait is fenntartja.

```
/dev/disk
|-- by-id
|   |-- scsi-SATA_HTS726060M9AT00_MRH453M4HWHG7B -> ../../sda
|   |-- scsi-SATA_HTS726060M9AT00_MRH453M4HWHG7B-part1 -> ../../sda1
|   |-- scsi-SATA_HTS726060M9AT00_MRH453M4HWHG7B-part6 -> ../../sda6
|   |-- scsi-SATA_HTS726060M9AT00_MRH453M4HWHG7B-part7 -> ../../sda7
|   |-- usb-Generic_STORAGE_DEVICE_02773 -> ../../sdd
|   `-- usb-Generic_STORAGE_DEVICE_02773-part1 -> ../../sdd1
|-- by-label
|   |-- Photos -> ../../sdd1
|   |-- SUSE10 -> ../../sda7
|   `-- devel -> ../../sda6
|-- by-path
|   |-- pci-0000:00:1f.2-scsi-0:0:0:0 -> ../../sda
|   |-- pci-0000:00:1f.2-scsi-0:0:0:0-part1 -> ../../sda1
|   |-- pci-0000:00:1f.2-scsi-0:0:0:0-part6 -> ../../sda6
|   |-- pci-0000:00:1f.2-scsi-0:0:0:0-part7 -> ../../sda7
|   |-- pci-0000:00:1f.2-scsi-1:0:0:0 -> ../../sr0
|   |-- usb-02773:0:0:2 -> ../../sdd
|   |-- usb-02773:0:0:2-part1 -> ../../sdd1
`-- by-uuid
    |-- 159a47a4-e6e6-40be-a757-a629991479ae -> ../../sda7
    |-- 3e999973-00c9-4917-9442-b7633bd95b9e -> ../../sda6
    `-- 4210-8F8C -> ../../sdd1
```

17.8 Az udev által használt fájlok

`/sys/*`
: A Linux kernel által biztosított virtuális fájlrendszer, amely exportálja az összes ismert eszközt. Az udev ezt az információt használja eszközcsomópontok létrehozására a `/dev` alatt.

`/dev/*`
: Dinamikusan létrehozott eszközcsomópontok és statikus tartalom, rendszerindításkor átmásolva a `/lib/udev/devices/*` alól.

Az udev infrastruktúra kulcsfontosságú elemeit az alábbi fájlok és könyvtárak tartalmazzák:

`/etc/udev/udev.conf`
: A fő udev konfigurációs fájl.

`/etc/udev/rules.d/*`
: udev eseményillesztési szabályok.

`/lib/udev/devices/*`
: Statikus `/dev` tartalom.

`/lib/udev/*`
: Az udev-szabályokból meghívott segítő programok.

17.9 További információk

További információ az udev infrastruktúráról a következő kézikönyvoldalakon olvasható:

udev
: Általános információ az udevről, a kulcsokról, szabályokról és más fontos konfigurációs kérdésekről.

udevadm
: Az udevadm használható az udev futási idejű viselkedésének szabályozására, kernelesemények kérésére, az eseménysor kezelésére, valamint egyszerű hibakeresési mechanizmusok biztosítására.

udevd
: Információ az udev eseménykezelő démonjáról.

Hozzáférés-vezérlési listák Linuxban

18

A fájlrendszer-objektumok védelmére a hagyományos jogosultságok kiterjesztéseként használhatók POSIX ACL-ek (hozzáférés-vezérlési listák) is. Az ACL-ek segítségével a jogosultságok rugalmasabban definiálhatóak, mint ahogy azt a hagyományos jogosultsági fogalmak engednék.

A *POSIX ACL* elnevezés azt sugallja, hogy ez egy igazi POSIX- (*portable operating system interface*) szabvány. A vonatkozó szabványtervezeteket – POSIX 1003.1e és POSIX 1003.2c – azonban több okból is visszavonták. Ennek ellenére a UNIX-családhoz tartozó számos rendszeren megtalálható ACL-ek ezekre a tervezetekre épülnek és a fájlrendszer ACL-ek megvalósítása – ahogy a jelen fejezetben le van írva – ezeket a szabványokat követi. Ezek a következő címen tekinthetők meg: `http://wt.xpilot.org/publications/posix.1e/`.

18.1 Hagyományos fájljogosultságok

A hagyományos fájljogosultságokról részletes információ található a GNU Coreutils info oldalán, a *Fájljogosultságok* pontban (`info coreutils "File permissions"`). Speciálisabb lehetőséget biztosítanak a setuid, a setgid és a sticky (ragadós) bitek.

18.1.1 A setuid bit

Egyes esetekben a hozzáférési jogosultságok túlságosan korlátozók lehetnek. Éppen ezért a Linux extra beállításokkal lehetővé teszi az aktuális felhasználó és csoport ide-

iglenes megváltoztatását egy-egy adott műveletre. A `passwd` program például normál esetben root jogosultságot igényel az `/etc/passwd` fájl eléréséhez. Ez a fájl fontos, bizalmas információkat tartalmaz, például a felhasználók home könyvtárait, illetve a felhasználói és csoportazonosítókat. Egy normál felhasználó tehát nem lenne képes megváltoztatni a jelszavát és használni a `passwd` programot, hiszen túlságosan veszélyes lenne minden felhasználó számára közvetlen hozzáférést adni ehhez a fájlhoz. E probléma egy lehetséges megoldását kínálja a *setuid* mechanizmus. A setuid (set user ID, "felhasználói azonosító beállítása") egy olyan speciális fájlattribútum, amelyik arra utasítja a rendszert, hogy az így megjelölt programokat egy meghatározott felhasználói azonosító (UID) nevében hajtsa végre. Vegyük példának ismét a `passwd` parancsot:

```
-rwsr-xr-x  1 root shadow 80036 2004-10-02 11:08 /usr/bin/passwd
```

A felhasználói jogosultságok között látható a setuid bitet jelző `s` karakter. A setuid bit beállítása miatt a `passwd` programot minden felhasználó a `root` nevében futtatja.

18.1.2 A setgid bit

A setuid bit felhasználókra vonatkozik. Létezik egy párja, amelyik viszont a csoportokra: ez a *setgid* bit. Egy olyan program, amelyhez ezt a bitet beállítják, azon csoport azonosítója (GID) alatt fog futni, amelyikkel elmentették, függetlenül attól, hogy melyik felhasználó indítja el. Éppen ezért egy olyan könyvtárban, amelynek be van állítva a setgid bitje, az összes újonnan létrehozott fájl és alkönyvtár ahhoz a csoporthoz lesz rendelve, amelyhez a könyvtár maga is tartozik. Vegyük a következő példát:

```
drwxrws--- 2 tux archive 48 Nov 19 17:12  backup
```

Az `s` karakter jelzi, hogy a setgid bit be lett állítva a csoportjogosultságokhoz. A könyvtárat a könyvtár tulajdonosa és az `archive` csoport tagjai érhetik el. Azok a felhasználók, akik nem a csoport tagjai, „leképződnek” a megfelelő csoportra. Az összes kiírt fájl tényleges csoportazonosítója az `archive` lesz. Például egy mentést végző program, amely az `archive` csoportazonosító nevében fut, elérheti ezt a könyvtárat root jogosultságok nélkül is.

18.1.3 A sticky (ragadós) bit

A harmadik speciális jelző a *sticky (ragadós) bit*. Ennek a szerepe függ attól, hogy egy végrehajtható programra vagy egy könyvtárra van beállítva. Ha egy programhoz tartozik, akkor az így megjelölt fájl RAM-ba töltődik, hogy ne kelljen minden egyes használatkor

a merevlemezről betölteni. Az attribútum ilyen használata ma már ritka, mert a modern merevlemezek elég gyorsak. Ha egy könyvtárhoz van rendelve, akkor megakadályozza, hogy a felhasználók törölhessék egymás fájljait. Jellemzően például a `/tmp` és `/var/tmp` könyvtárakon szokás használni:

```
drwxrwxrwt 2 root root 1160 2002-11-19 17:15 /tmp
```

18.2 Az ACL-ek előnyei

A Linux-rendszer fájlobjektumaihoz hagyományosan három jogosultsághalmaz van megadva. Olvasási (read, `r`), írási (write, `w`), és végrehajtási (execute, `x`) jogosultságokat kaphat mind a három felhasználótípus: – a fájl tulajdonosa, a csoport és az összes többi felhasználó. Megadható továbbá a *felhasználói azonosító beállítása* (setuid), a *csoport-azonosító beállítása* (setgid) és a *sticky* (ragadós) bit. Ezek az alapelvek a legtöbb gyakorlati esethez teljesen megfelelők. Összetettebb helyzetek vagy speciális alkalmazások esetén azonban a rendszeradminisztrátoroknak korábban számos trükköt kellett alkalmazniuk a hagyományos jogosultsági alapelvek korlátainak megkerüléséhez.

Az ACL-ek olyan helyzetekben használhatók, amelyek a hagyományos fájljogosultság fogalmának kiterjesztését igénylik. Lehetővé teszik a jogosultságok egyedi felhasználókhoz vagy csoportokhoz rendelését akkor is, ha ezek nem egyeznek meg az eredeti tulajdonossal vagy csoporttulajdonossal. A hozzáférés-vezérlési lista a Linux-kernel funkciója, és jelenleg a ReiserFS, Ext2, Ext3, JFS és XFS fájlrendszerek támogatják. ACL-ek használatával az összetett helyzetek is megoldhatók anélkül, hogy alkalmazásszinten kellene megvalósítani összetett jogosultsági modelleket.

Az ACL-ek előnye egyértelmű olyan helyzetekben, mint például egy Windows-kiszolgáló Linux-kiszolgálóval helyettesítése. A csatlakoztatott munkaállomások egy része továbbra is Windows alatt futhat, akár az áttérés után is. A Linux-rendszer Samba segítségével fájl- és nyomtatási szolgáltatásokat biztosít a Windows-kliensek számára. Mivel a Samba támogatja a hozzáférés-vezérlési listák használatát, a felhasználói jogosultságok a grafikus felhasználói felületen a Linux-kiszolgálón és Windowson is beállíthatók (csak Windows NT és újabb rendszerek esetén). A `winbindd` program segítségével olyan felhasználókhoz is rendelhetők jogosultságok, akik csak a Windows-tartományban léteznek és nem rendelkeznek azonosítóval a Linux-kiszolgálón.

18.3 Meghatározások

felhasználói osztály
: A hagyományos POSIX jogosultsági elv a fájlrendszeren belül három felhasználói *osztályt* használ a jogosultságok hozzárendeléséhez: ezek a tulajdonos, a tulajdonoscsoport és az egyéb felhasználók. Három jogosultsági bit állítható be a felhasználói osztályokhoz: az olvasás (`r`), írás (`w`), és végrehajtás (`x`) jelzésére.

hozzáférési ACL
: A fájlrendszer-objektumok (fájlok és könyvtárak) felhasználói és csoporthozzáférési jogosultságait a hozzáférési ACL-ek határozzák meg.

alapértelmezett ACL
: Az alapértelmezett ACL-ek csak a könyvtárakra alkalmazhatók. Ezek határozzák meg, hogy egy fájlrendszer-objektum milyen jogosultságokat örököl a szülőkönyvtártól a létrehozása során.

ACL-bejegyzés
: Minden hozzáférés-vezérlési lista ACL-bejegyzésekből áll. Az ACL-bejegyzések egy típust tartalmaznak, egy minősítőt ahhoz a felhasználóhoz vagy csoporthoz, amelyre a bejegyzés hivatkozik, valamint egy jogosultsághalmazt. Bizonyos bejegyzéstípusok esetén a csoport vagy felhasználó minősítése nincs megadva.

18.4 ACL-ek kezelése

Az 18.1 táblázat - ACL-bejegyzéstípusok (257. oldal) szakasz foglalja össze a hat lehetséges ACL-bejegyzést, amelyek mindegyike egy adott felhasználó vagy felhasználói csoport jogosultságait adja meg. A *tulajdonos* bejegyzés a fájlt vagy könyvtárat birtokló felhasználó jogosultságait adja meg. A *tulajdonoscsoport* bejegyzés adja meg a fájlt birtokló csoport jogosultságait. Az adminisztrátor (superuser) a `chown` vagy `chgrp` parancs segítségével megváltoztathatja a tulajdonost vagy a tulajdonoscsoportot. Ez esetben a tulajdonos és a tulajdonoscsoport bejegyzés az új tulajdonosra és tulajdonoscsoportra hivatkozik. A *megnevezett felhasználó* bejegyzések a minősítő mezőben megadott felhasználó jogosultságait adják meg. A *megnevezett csoport* bejegyzések a minősítő mezőben megadott csoport jogosultságait adják meg. Csak a megnevezett felhasználó és csoport bejegyzések rendelkeznek nem üres minősítőmezővel. Az *other* (egyéb) bejegyzés a maradék felhasználók jogosultságait adja meg.

A *mask* (maszk) bejegyzés tovább korlátozza a megnevezett felhasználó, megnevezett csoport és tulajdonoscsoport bejegyzések által megadott jogosultságokat: azt adja meg, hogy e bejegyzések mely jogosultságai érvényesek és melyek vannak maszkolva. Ha a jogosultságok az említett bejegyzések egyikében és a maszkban egyaránt léteznek, akkor ezek érvényesek. A csak a maszkban vagy csak az aktuális bejegyzésben lévő jogosultságok nem érvényesek – ezek a jogosultságok nem lesznek megadva. A tulajdonos és tulajdonoscsoport részben megadott bejegyzések mindig érvényesek. A következő példa (18.2 táblázat - Hozzáférési jogosultságok maszkolása (257. oldal)) ezt a mechanizmust illusztrálja.

Az ACL-eknek két alapvető osztálya van: a *minimális* ACL csak a tulajdonos, tulajdonoscsoport és az egyéb típusok bejegyzéseit tartalmazza, amely a fájlok és könyvtárak szokásos jogosultsági bitjeinek felelnek meg. A *kiterjesztett* ACL ennél többet foglal magában. Tartalmaznia kell egy maszk bejegyzést és tartalmazhat több megnevezett felhasználó és megnevezett csoport típust is.

18.1. táblázat *ACL-bejegyzéstípusok*

Típus	Szöveges forma
tulajdonos	`user::rwx`
megnevezett felhasználó	`user:name:rwx`
tulajdonoscsoport	`group::rwx`
megnevezett csoport	`group:name:rwx`
maszk	`mask::rwx`
egyéb	`other::rwx`

18.2. táblázat *Hozzáférési jogosultságok maszkolása*

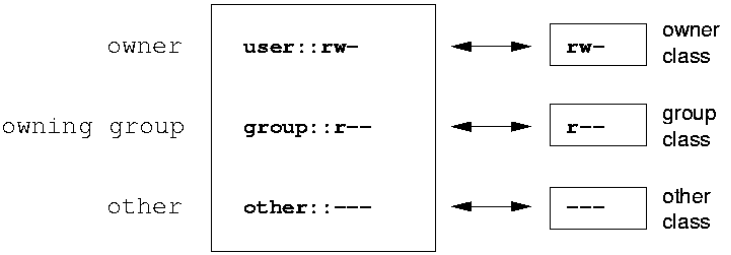
Bejegyzés típusa	Szöveges forma	Jogosultságok
megnevezett felhasználó	`user:geeko:r-x`	`r-x`

Bejegyzés típusa	Szöveges forma	Jogosultságok
maszk	`mask::rw-`	`írható-olvasható-`
	hatályos jogosultságok:	`r--`

18.4.1 ACL-bejegyzések és fájlmód-jogosultságbitek

A 18.1. ábra - Minimális ACL: Az ACL-bejegyzések és a jogosultságbitek összehasonlítása (258. oldal) és a 18.2. ábra - Kiterjesztett ACL: Az ACL-bejegyzések és a jogosultságbitek összehasonlítása (259. oldal) ábrák a minimális és a kiterjesztett ACL-eket ábrázolják. Az ábrák három blokkba vannak rendezve – a bal oldali blokk az ACL-bejegyzések típusspecifikációját, a középső egy minta ACL-t, a jobb oldali pedig a szokásos jogosultság-alapelvnek megfelelő jogosultságbiteket jeleníti meg, mint ahogy azt például az `ls -l` parancs is kiírná. A *tulajdonos osztály* jogosultságai mindkét esetben a tulajdonos ACL-bejegyzésnek vannak megfeleltetve. Az *egyéb osztály* jogosultságai a megfelelő ACL-bejegyzésnek vannak megfeleltetve. A *csoportosztály* jogosultságok megfeleltetése azonban a két esetben eltér.

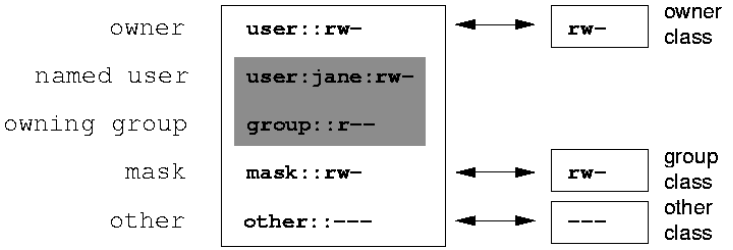
18.1. ábra *Minimális ACL: Az ACL-bejegyzések és a jogosultságbitek összehasonlítása*



Minimális – maszk nélküli – ACL esetén a csoport osztály jogosultságai a tulajdonos-csoport ACL-bejegyzésre vannak leképezve. Ez a következő ábrán látható: 18.1. ábra - Minimális ACL: Az ACL-bejegyzések és a jogosultságbitek összehasonlítása (258. oldal). Kiterjesztett – maszkolt – ACL esetén a csoportosztály jogosultságai a maszk bejegyzésnek vannak megfeleltetve. Ez a következő ábrán látható: 18.2. ábra -

Kiterjesztett ACL: Az ACL-bejegyzések és a jogosultságbitek összehasonlítása (259. oldal).

18.2. ábra *Kiterjesztett ACL: Az ACL-bejegyzések és a jogosultságbitek összehasonlítása*



Ez a leképezési módszer biztosítja az alkalmazások zökkenőmentes együttműködését az ACL-támogatás alkalmazásától függetlenül. A jogosultságbitek által megadott hozzáférési jogosultságok jelentik az ACL-lel megadott további „finombeállítások” felső korlátját. Az ACL tükrözi a jogosultságbitek módosítását és fordítva.

18.4.2 Hozzáférési ACL-lel rendelkező könyvtár

A parancssori `getfacl` és `setfacl` parancsokkal lehet kezelni az ACL-eket. A parancsok használatát az alábbi példa mutatja be.

A könyvtár létrehozása előtt az `umask` parancs segítségével adja meg, hogy a fájlobjektumok létrehozásakor mely hozzáférési jogosultságokat kell maszkolni. Az `umask 027` parancs az alapértelmezett jogosultságot úgy állítja be, hogy a tulajdonosnak az összes jogosultságot biztosítja (`0`), , a csoport írási jogosultsága le van tiltva (`2`), az egyéb felhasználók pedig semmilyen jogosultsággal nem rendelkeznek (`7`). Az `umask` ténylegesen maszkolja a megfelelő jogosultságbiteket vagy kikapcsolja őket. Részletes leírást az `umask` kézikönyvoldal tartalmaz.

Az `mkdir mydir` parancs létrehozza a `mydir` könyvtárat az `umask` által megadott alapértelmezett jogosultságokkal. Az `ls -dl mydir` parancs segítségével ellenőrizhető, hogy az összes jogosultság megfelelően lett-e megadva. A példa kimenete:

```
drwxr-x--- ... tux project3 ... mydir
```

A `getfacl mydir` parancs segítségével ellenőrizze az ACL kezdeti állapotát. Ez az alábbihoz hasonló kimenetet eredményez:

```
# file: mydir
# owner: tux
# group: project3
user::rwx
group::r-x
other::---
```

Az első három kimeneti sor a könyvtár nevét, tulajdonosát és tulajdonoscsoportját adja meg. A következő három sor a tulajdonos, tulajdonoscsoport és egyéb ACL-bejegyzéseket tartalmazza. E minimális ACL esetén a `getfacl` parancs nem állít elő olyan információt, amely az `ls` segítségével ne lenne látható.

Módosítsa az ACL-t és adjon olvasási, írási és végrehajtási jogosultságot még a `geeko` felhasználónak és a `mascots` csoportnak:

```
setfacl -m user:geeko:rwx,group:mascots:rwx mydir
```

A `-m` paraméter hatására a `setfacl` módosítja a meglévő ACL-t. A következő argumentum a módosítandó ACL-bejegyzéseket jelzi (a több bejegyzés vesszővel van elválasztva). Az utolsó rész a könyvtár nevét adja meg, amelyen ezeket a módosításokat végre kell hajtani. A `getfacl` parancs segítségével megjeleníthető az eredményül kapott ACL.

```
# file: mydir
# owner: tux
# group: project3
user::rwx
user:geeko:rwx
group::r-x
group:mascots:rwx
mask::rwx
other::---
```

A `geeko` felhasználóhoz és a `mascots` csoporthoz létrehozott bejegyzések mellett egy maszk bejegyzés is létrejött. Ez a maszk bejegyzés automatikusan beállításra kerül, így az összes jogosultság érvényes. A `setfacl` parancs automatikusan átalakítja a maszk bejegyzéseket a módosított beállításokra, hacsak a `-n` paraméterrel le nem tiltja ezt a funkciót. A maszk határozza meg a csoport osztályban lévő bejegyzések maximális érvényes hozzáférési jogosultságait. Ez a megnevezett felhasználót, megnevezett csoportot és a tulajdonoscsoportot foglalja magában. Az `ls -dl mydir` paranccsal megjelenített csoportosztály jogosultságbitek mostantól a `mask` bejegyzésnek felelnek meg.

```
drwxrwx---+ ... tux project3 ... mydir
```

A kimenet első oszlopa egy további + jelet tartalmaz, jelezve, hogy az elemhez egy *kiterjesztett* ACL tartozik.

Az `ls` parancs kimenetének megfelelően a maszkbejegyzés jogosultságai írási hozzáférést is tartalmaznak. Az ilyen jogosultságbitek hagyományosan azt jelentenék, hogy a tulajdonoscsoport (jelen esetben a `project3`) szintén rendelkezik írási hozzáféréssel a `mydir` könyvtárhoz. A tulajdonoscsoport érvényes hozzáférési jogosultságai azonban a tulajdonoscsoporthoz és a maszkhoz megadott jogosultságok átfedő részének felelnek meg – amely a mi példánkban `r-x` (lásd: 18.2 táblázat - Hozzáférési jogosultságok maszkolása (257. oldal)). Ami a példában levő tulajdonoscsoport érvényes jogosultságát illeti, semmi nem változik az ACL-bejegyzések hozzáadása után sem.

A `setfacl` vagy `chmod` parancs segítségével módosítsa a maszkbejegyzést. Használja például a `chmod g-w mydir` parancsot. Az `ls -dl mydir` ezután a következőt jeleníti meg:

```
drwxr-x---+ ... tux project3 ... mydir
```

A `getfacl mydir` parancs kimenete a következő:

```
# file: mydir
# owner: tux
# group: project3
user::rwx
user:geeko:rwx          # effective: r-x
group::r-x
group:mascots:rwx       # effective: r-x
mask::r-x
other::---
```

Miután a `chmod` parancs segítségével eltávolította az írási jogosultságot a csoportosztály bitek közül, az `ls` parancs kimenete elegendő ahhoz, hogy észrevegyük, hogy a maszkbiteket megfelelően módosítani kell: az írási jogosultság a `mydir` tulajdonosára van korlátozva. A `getfacl` kimenete megerősíti ezt. Ez a kimenet az összes olyan bejegyzéshez tartalmaz megjegyzést, amelyben a tényleges jogosultságbitek nem felelnek meg az eredeti jogosultságoknak, mivel ezek a maszkbejegyzésnek megfelelően szűrve vannak. Az eredeti jogosultságok a `chmod g+w mydir` parancs segítségével bármikor visszaállíthatók.

18.4.3 Alapértelmezett ACL-lel rendelkező könyvtár

A könyvtárak rendelkezhetnek egy alapértelmezett ACL-lel. Ez egy speciális ACL, amely megadja, hogy a könyvtár objektumai létrehozásukkor milyen hozzáférési jogosultságokat örökölnek meg. Az alapértelmezett ACL az alkönyvtárakra és fájlokra egyaránt érvényes.

Az alapértemezett ACL hatásai

A könyvtár alapértelmezett ACL-jének jogosultságai kétféleképp kerülhetnek át a könyvtárban található alkönyvtárakra és fájlokra:

- Az alkönyvtár örökli a szülőkönyvtár alapértelmezett ACL-jét alapértelmezett és hozzáférési ACL-ként egyaránt.
- A fájl örökli az alapértelmezett ACL-t hozzáférési ACL-ként.

Minden fájlrendszer-objektumot létrehozó rendszerhívás egy `mode` paramétert használ, amely megadja az újonnan létrehozott fájlrendszer-objektum jogosultságait. Ha a szülőkönyvtár nem rendelkezik alapértelmezett ACL-lel, akkor az `umask` által megadott jogosultságbitek a `mode` paraméter által átadott jogosultságokból vonódnak ki, és az eredmény hozzárendelődik az új objektumhoz. Ha a szülőkönyvtár rendelkezik alapértelmezett ACL-lel, akkor az új objektumhoz rendelt jogosultságbitek a `mode` paraméter jogosultságainak átfedő részének és az alapértelmezett ACL-ben megadottaknak felelnek meg. Az `umask` paramétert ebben az esetben a rendszer figyelmen kívül hagyja.

Az alapértelmezett ACL-ek alkalmazása

Az alábbi három példa a könyvtárak és az alapértelmezett ACL-ek legjellemzőbb alkalmazásait mutatja be:

1. Az alábbi parancs segítségével adjon hozzá egy alapértelmezett ACL-t a meglévő `mydir` könyvtárhoz:

   ```
   setfacl –d –m group:mascots:r–x mydir
   ```

A `setfacl` parancs `-d` paramétere következtében a `setfacl` az alábbi módosításokat (`-m` kapcsoló) hajtja végre az alapértelmezett ACL-en.

A parancs eredménye a következő:

```
getfacl mydir

# file: mydir
# owner: tux
# group: project3
user::rwx
user:geeko:rwx
group::r-x
group:mascots:rwx
mask::rwx
other::---
default:user::rwx
default:group::r-x
default:group:mascots:r-x
default:mask::r-x
default:other::---
```

A `getfacl` a hozzáférési és alapértelmezett ACL-t is visszaadja. Az alapértelmezett ACL-t a `default` szóval kezdődő sorok alkotják. Annak ellenére, hogy a `setfacl` parancsot csak az alapértelmezett ACL `mascots` csoportjának egy bejegyzésére hajtotta végre, a `setfacl` a hozzáférési ACL összes többi bejegyzését is automatikusan lemásolja egy érvényes alapértelmezett ACL létrehozása érdekében. Az alapértelmezett ACL-ek nincsenek azonnal hatással a hozzáférési jogosultságokra. Csak a fájlrendszer-objektumok létrehozásakor jutnak érvényre. Ezek az új objektumok csak a szülőkönyvtár alapértelmezett ACL-jétől örökölnek jogosultságokat.

2. A következő példában az `mkdir` parancs segítségével a `mydir` könyvtárban létrehozunk egy alkönyvtárat, amely örökli az alapértelmezett ACL-t.

```
mkdir mydir/mysubdir

getfacl mydir/mysubdir

# file: mydir/mysubdir
# owner: tux
# group: project3
user::rwx
group::r-x
group:mascots:r-x
mask::r-x
other::---
default:user::rwx
```

```
default:group::r-x
default:group:mascots:r-x
default:mask::r-x
default:other::---
```

A működésnek megfelelően, az újonnan létrehozott `mysubdir` alkönyvtár a szülőkönyvtár alapértelmezett ACL-jéből származó jogosultságokkal rendelkezik. A `mysubdir` hozzáférési ACL-je a `mydir` könyvtár alapértelmezett ACL-jének pontos mása. Az alapértelmezett ACL, amelyet a könyvtár átad az alárendelt objektumoknak, szintén ugyanaz.

3. A `touch` parancs segítségével hozzon létre egy fájlt a `mydir` könyvtárban, például így: `touch mydir/myfile`. Az `ls -l mydir/myfile` parancs ezután az alábbit jeleníti meg:

```
-rw-r-----+ ... tux project3 ... mydir/myfile
```

A `getfacl mydir/myfile` kimenete az alábbi:

```
# file: mydir/myfile
# owner: tux
# group: project3
user::rw-
group::r-x          # effective:r--
group:mascots:r-x   # effective:r--
mask::r--
other::---
```

A `touch` az új fájlok létrehozásakor egy `0666` értékű `mode` paramétert használ, ami azt jelenti, hogy a létrehozott fájlokhoz az összes felhasználó írási és olvasási jogosultságot kap, feltéve, hogy az `umask` vagy az alapértelmezett ACL nem adnak meg egyéb megszorításokat (lásd „Az alapértemezett ACL hatásai” szakasz (262. oldal)). Ez a gyakorlatban azt jelenti, hogy a `mode` értékben lévő hozzáférési jogosultságok eltávolításra kerültek a megfelelő ACL-bejegyzésekből. Bár a csoportosztály ACL-bejegyzéséből nem kerültek eltávolításra jogosultságok, a maszk bejegyzés módosult, hogy maszkolja a `mode` paraméterben be nem állított jogosultságokat.

Ez a megközelítés biztosítja az alkalmazások – például a fordítóprogramok – és az ACL-ek zökkenőmentes együttműködését. Létre lehet hozni korlátozott hozzáférési jogosultságú fájlokat, amelyek később végrehajthatóként jelölhetők meg. A `mask` mechanizmus garantálja, hogy ezeket azután a megfelelő felhasználók és csoportok végrehajthassák.

18.4.4 Az ACL ellenőrzési algoritmusa

Az ellenőrzési algoritmus azelőtt kerül alkalmazásra, hogy a folyamat vagy alkalmazás hozzáférést kapna egy ACL-lel védett fájlrendszer-objektumhoz. Alapszabályként az ACL-bejegyzések az alábbi sorrendben kerülnek megvizsgálásra: tulajdonos, megnevezett felhasználó, tulajdonoscsoport vagy megnevezett csoport és egyéb. A hozzáférés a folyamathoz legjobban megfelelő bejegyzésnek megfelelően kerül kezelésre. A jogosultságok nem halmozódnak.

A dolgok sokkal bonyolultabbá válnak, ha a folyamat több csoporthoz tartozik, és több csoportbejegyzésnek is megfelel. Egy bejegyzés véletlenszerűen kerül kiválasztásra a szükséges jogosultságokkal rendelkező megfelelő bejegyzések közül. Lényegtelen, hogy mely bejegyzések aktiválják a „hozzáférés megadva” végső eredményt. Ehhez hasonlóan, ha egyik megfelelő csoport bejegyzés sem tartalmazza a szükséges jogosultságokat, akkor egy véletlenszerűen kiválasztott bejegyzés aktiválja a végső eredményt: „hozzáférés megtagadva”.

18.5 ACL-támogatás az alkalmazásokban

ACL-ek segítségével a modern alkalmazások követelményeinek megfelelő igen összetett jogosultsági helyzetek is leírhatók. A hagyományos jogosultsági alapelv és az ACL-ek jól kombinálhatók. Az alap fájlparancsok (`cp`, `mv`, `ls` stb.) támogatják az ACL-ek használatát, csakúgy, mint a Samba és a Konqueror.

Számos szerkesztő és fájlkezelő továbbra sem kezeli az ACL-eket. Az Emacs használatával történő másoláskor például elvesznek a fájlok ACL-jei. Ha a fájlokat egy szerkesztőben módosítja, akkor a fájlok ACL-jei bizonyos esetekben megőrzésre kerülnek, máskor pedig nem, a szerkesztő által használt mentési módtól függően. Ha a szerkesztő az eredeti fájlba írja a módosításokat, akkor a hozzáférési ACL megőrzésre kerül. Ha a szerkesztő a frissített tartalmat egy új fájlba menti, amely utána átneveződik a régi fájl nevére, akkor az ACL-ek elveszhetnek, hacsak a szerkesztő nem támogatja az ACL-eket. A star archiváló kivételével pillanatnyilag nincs más mentési alkalmazás, amely az ACL-eket megőrizné.

18.6 További információk

Az ACL-ekkel kapcsolatos részletes információ a következő címen érhető el: `http://acl.bestbits.at/`. Lásd még: `getfacl(1)`, `acl(5)` és `setfacl(1)` kézikönyv- (man-) oldalai.

19 Hitelesítés PAM használatával

A Linux a PAM (Pluggable Authentication Modules, cserélhető hitelesítési modulok) rendszert használja a hitelesítési folyamatban a felhasználó és az alkalmazás közötti rétegként. A PAM-modulok rendszerszinten állnak rendelkezésre, így akármelyik alkalmazás kérheti őket. Ez a fejezet leírja a moduláris hitelesítési mechanizmus működését és beállításának módját.

A rendszergazdák és a programozók gyakran kívánják korlátozni a hozzáférést a rendszer egyes részeihez, illetve korlátozni az alkalmazások bizonyos funkcióinak használatát. PAM nélkül az alkalmazásokat minden egyes új hitelesítési mechanizmushoz (például LDAP, Samba vagy Kerberos) hozzá kell igazítani. Ez a folyamat azonban meglehetősen időigényes és a hibázás esélyét rejti. E hátrányok elkerülésének egyik módja az alkalmazások és a hitelesítési mechanizmusok szétválasztása, és az utóbbi központilag felügyelt modulokba irányítása. Így minden egyes alkalommal, ha egy új hitelesítési séma kerül bevezetésre, elegendő a megfelelő PAM-modult elkészíteni vagy adaptálni.

A PAM mechanizmusát használó programok mindegyikének van egy saját konfigurációs fájlja az `/etc/pam.d/`*`programnév`* könyvtárban. Ezek a fájlok határozzák meg a hitelesítéshez használt PAM-modulokat. Létezik továbbá egy globális konfigurációs fájl a legtöbb PAM-modulhoz az `/etc/security` könyvtárban, amely meghatározza a modulok pontos viselkedését (ilyen például a `pam_env.conf` és a `time.conf`). A PAM-modulokat használó alkalmazások ténylegesen egy sor PAM-funkciót hívnak meg, amelyek azután feldolgozzák a különféle konfigurációs fájlokban található adatokat és az eredményt visszaadják a hívó alkalmazásnak.

A PAM-modulok létrehozásának és karbantartásának elősegítéséhez az `auth`, `account`, `password` és `session` modulokhoz általános alapértelmezett konfigurá-

ciós fájlok lettek bevezetve. Ezek az egyes alkalmazások PAM-konfigurációjából vannak véve. Az általános PAM-konfigurációs modulok (`common-*`) így átmásolódnak az összes PAM konfigurációs fájlba anélkül, hogy a rendszergazdának magának kéne frissítenie az egyes PAM konfigurációs fájlokat.

Az általános közös PAM konfigurációs fájlok karbantartása a pam-config eszközzel történik. Ez az eszköz automatikusan hozzáadja az új modulokat a konfigurációhoz, módosítja a meglévők beállításait, illetve törli a modulokat vagy a konfigurációs beállításokat. A PAM-konfigurációk karbantartásához nem vagy csak nagyon kevés kézi beavatkozásra van szükség.

19.1 A PAM konfigurációs fájlok szerkezete

A PAM konfigurációs fájlok minden egyes sora maximum négy oszlopból állhat:

```
<Type of module> <Control flag> <Module path> <Options>
```

A PAM-modulok egymásra épülve kerülnek feldolgozásra. A különféle típusú moduloknak különböző feladataik vannak: az egyik modul például ellenőrzi a jelszót, a másik azt a helyet, ahonnan a rendszert elérték, egy harmadik pedig lehet, hogy felhasználóspecifikus beállításokat vizsgál meg. A PAM négyféle modultípust különböztet meg:

`auth`
: Az ilyen típusú modulok feladata a felhasználó azonosságának ellenőrzése. Hagyományosan ez jelszóellenőrzéssel történik, de használhatók például intelligens kártyák vagy különféle biometriai eszközök (ujjlenyomat- vagy szivárványhártya-ellenőrzés) is.

`account`
: Az ilyen típusú modulok ellenőrzik, hogy a felhasználó rendelkezik-e általános engedéllyel a kért szolgáltatás használatára. Például ilyen ellenőrzésre van szükség ahhoz, hogy senki ne léphessen be egy lejárt felhasználói fiók azonosítójával.

`password`
: Az ilyen típusú modulok feladata, hogy lehetővé tegyék a hitelesítési tokenek cseréjét. A legtöbb esetben ez egy jelszót jelent.

`session`
: Az ilyen típusú modulok felelősek a felhasználói munkamenetek kezeléséért és beállításáért. A hitelesítés előtt és után kerülnek elindításra, hogy feljegyezzék a bejelentkezési kísérleteket a rendszernaplókba, valamint beállítsák a felhasználó egyedi környezetét (postafiókok, saját könyvtár, rendszerkorlátok stb).

A második oszlop az elindított modulok viselkedését befolyásoló vezérlő jelzőket tartalmaz:

`required`
: Az ilyen jelzőjű modulok feldolgozásának sikeresen végbe kell mennie ahhoz, hogy a hitelesítés folytatódjon. Egy `required` jelzőjű modul sikertelen futása esetén az ilyen jelzőjű összes többi modul feldolgozásra kerül, mielőtt a felhasználó üzenetet kapna a hitelesítési kísérlet sikertelenségéről.

`requisite`
: Hasonlóan a `required` jelzőjű modulokhoz, az ilyen jelzőjű modulok feldolgozásának sikeresen végbe kell mennie. Egy ilyen jelzőjű modul sikertelen futása esetén azonban a felhasználó azonnal üzenetet kap és a rendszer a további modulokat nem dolgozza fel. Sikeres végrehajtás esetén feldolgozásra kerülnek a további modulok, hasonlóan a `required` jelzőhöz. A `requisite` jelző alapszintű szűrőként használható, amely a helyes hitelesítés alapvető fontosságú feltételeinek meglétét ellenőrzi.

`sufficient`
: Az ilyen jelzőjű modul sikeres feldolgozása esetén a hívó alkalmazás azonnal üzenetet kap a sikerről és a többi modul már nem is kerül feldolgozásra, feltéve, hogy nem volt korábbi `required` jelzőjű sikertelen modul. A `sufficient` jelzőjű modul sikertelen feldolgozása nem jár közvetlen következményekkel, hiszen minden további modul a megfelelő sorrendben végrehajtásra kerül.

`optional`
: Az ilyen jelzőjű modulok sikertelensége vagy sikere nem jár semmilyen direkt következménnyel. Ez olyan modulok esetén hasznos, amelyeknek csak egy üzenetet kell megjeleníteniük (például jelezni a felhasználónak, hogy levele érkezett), egyéb teendők nélkül.

include
: Ha ez a jelző meg van adva, akkor a paraméterként megadott fájl beszúrásra kerül ezen a helyen.

A modul elérési útját nem kell külön megadni, amennyiben a modul az alapértelmezett könyvtárban található (`/lib/security`, az openSUSE, által támogatott 64 bites platformokon a könyvtár neve `/lib64/security`). A negyedik oszlop az adott modul esetleges paramétereit tartalmazza. Ilyen lehet például a `debug` (a hibakeresés engedélyezése) vagy a `nullok` (üres jelszavak használatának engedélyezése).

MEGJEGYZÉS: 32 és 64 bites vegyes telepítések

64 bites operációs rendszer használatakor a 32 bites alkalmazásokhoz is készíthető futtatókörnyezet. Ha ezt szeretné, akkor az új modulok telepítésekor győződjön meg róla, hogy a megfelelő PAM-modulok mindkét változatát telepítette.

19.2 Az sshd PAM-konfigurációja

A PAM működésének illusztrálására tekintsük át az sshd PAM-konfigurációját gyakorlati példaként:

19.1 példa *Az sshd PAM-konfigurációja*

```
#%PAM-1.0
auth     required       pam_nologin.so
auth     include        common-auth
account  include        common-account
password include        common-password
session  required       pam_loginuid.so
session  include        common-session
# Enable the following line to get resmgr support for
# ssh sessions (see /usr/share/doc/packages/resmgr/README)
#session  optional      pam_resmgr.so fake_ttyname
```

Az első modul neve `pam_nologin`. Ez ellenőrzi, hogy létezik-e az `/etc/nologin` fájl. Ha igen, akkor csak a `root` felhasználó jelentkezhet be.

Egy alkalmazás (jelen esetben az sshd) tipikus PAM-konfigurációja négy include utasítást tartalmaz, amelyek a négy modultípus konfigurációs fájljaira utalnak: `common-auth`, `common-account`, `common-password` és `common-session`. Ez a négy fájl tartalmazza az egyes modultípusok alapértelmezett konfigurációját. Ha beágyazva használja ezeket ahelyett, hogy az egyes modulokat külön adná hozzá a megfelelő PAM-konfigurációhoz, akkor a PAM-konfiguráció automatikusan frissülni fog, ha a rendszergazda módosítja az alapértelmezett értékeket. Régebben kézzel kellett

módosítani minden alkalmazás konfigurációs fájlját, ha a PAM-ban változások történtek, vagy egy új alkalmazás lett telepítve. Most már a PAM-konfiguráció és az összes módosítása öröklődik az alapértelmezett konfigurációs fájlokon keresztül.

Az első beágyazott fájl (a `common-auth`) két `auth` típusú modult hív meg: a `pam_env.so` és a `pam_unix2.so` modulokat. Lásd:19.2. példa - Az `auth` szakasz alapértelmezett konfigurációja (271. oldal)

19.2 példa *Az auth szakasz alapértelmezett konfigurációja*

```
auth    required        pam_env.so
auth    required        pam_unix2.so
```

Az első, a `pam_env` az `/etc/security/pam_env.conf` fájlt tölti be a fájlban megadott környezeti változók beállításához. Így például beállítható a `DISPLAY` változó a helyes értékre, mivel a `pam_env` modul tudja, hogy a bejelentkezés honnan történik. A második, a `pam_unix2` összeveti a felhasználó bejelentkezési azonosítóját és jelszavát az `/etc/passwd` és az `/etc/shadow` fájlokban tároltakkal.

Az összes `auth` modul feldolgozásra kerül, mielőtt az sshd bármilyen visszajelzést kapna arról, hogy a bejelentkezés sikerült-e. Figyelembe véve, hogy az összes modul `required` vezérlő jelzővel rendelkezik, ahhoz, hogy az sshd pozitív eredményt kapjon vissza, mindegyikük feldolgozásának sikeresen végbe kell mennie. Ha a modulok közül csak egy is sikertelen, az összes modul feldolgozásra kerül, majd ezután kap értesítést az sshd a negatív eredményről.

Miután az összes `auth` típusú modul sikeresen feldolgozásra került, egy újabb beágyazási (include) utasítás következik, amint azt az ábra (19.3. példa - Az `account` szakasz alapértelmezett konfigurációja (271. oldal)) mutatja. A `common-account` csak egy modult tartalmaz, ez a `pam_unix2`. Ha a `pam_unix2` azt az eredményt adja vissza, hogy a felhasználó létezik, az sshd kap egy üzenetet a sikerről, és a következő modulköteg (`password`) kerül feldolgozásra: 19.4. példa - A `password` szakasz alapértelmezett konfigurációja (271. oldal).

19.3 példa *Az account szakasz alapértelmezett konfigurációja*

```
account required        pam_unix2.so
```

19.4 példa *A password szakasz alapértelmezett konfigurációja*

```
password requisite       pam_pwcheck.so  nullok cracklib
password required        pam_unix2.so    nullok use_authtok
```

Az sshd PAM-konfigurációja megint csupán egy include utasítást tartalmaz, amely a `password` moduloknak a `common-password` helyen található alapértelmezett konfigurációjára hivatkozik. Ezeknek a moduloknak sikeresen le kell futniuk (`requisite` és `required` vezérlő jelző) minden alkalommal, ha az alkalmazás egy hitelesítési token módosítását kéri.

A jelszó vagy valamilyen más hitelesítési token megváltoztatása biztonsági ellenőrzést igényel. Ezt a `pam_pwcheck` modul végzi. Az utána használt `pam_unix2` modul áthoz minden régi és új jelszót a `pam_pwcheck` modulból, így a felhasználónak nem kell újra hitelesítenie magát a jelszó megváltozatása után. Ez az eljárás lehetetlenné teszi a `pam_pwcheck` által végzett ellenőrzések megkerülését. Ha az `account` vagy az `auth` típusok úgy vannak beállítva, hogy jelezzék a lejárt jelszavakat, akkor a `password` modulokat is használni kell.

19.5 példa *A session szakasz alapértelmezett konfigurációja*

```
session required        pam_limits.so
session required        pam_unix2.so
session optional        pam_umask.so
```

Utolsó lépésként a `session` típusú modulok (ezek a `common-session` fájlba vannak beágyazva) kerülnek meghívásra a munkamenet beállítására az adott felhasználónak megfelelően. A `pam_limits` modul betölti az `/etc/security/limits.conf` fájlt, amely korlátokat szabhat meg bizonyos rendszererőforrások használatával kapcsolatban. A `pam_unix2` modul újra feldolgozára kerül. A `pam_umask` modul a fájl mód létrehozási maszk beállítására használható. Mivel ez a modul `optional` jelzővel van ellátva, a hibája nem befolyásolja a teljes munkamenet-modulverem sikeres végrehajtását. A `session` modulok a felhasználó kijelentkezésekor másodszor is meghívódnak.

19.3 A PAM-modulok beállítása

A PAM-modulok némelyike konfigurálható. A megfelelő konfigurációs fájlok az `/etc/security` könyvtárban találhatók. Az alábbi szakasz az sshd példával kapcsolatos `pam_env.conf` és `limits.conf` konfigurációs fájlokat írja le röviden.

19.3.1 pam_env.conf

Ez a fájl használható a felhasználók számára egy szabványosított környezet kialakítására, amely beállításra kerül a `pam_env` modul minden egyes meghívásánál. Ebben az esetben az előre beállított környezeti változók a következő szintaxissal adhatók meg:

```
VARIABLE  [DEFAULT=[value]]  [OVERRIDE=[value]]
```

`VARIABLE`
: A beállítani kívánt környezeti változó neve.

`[DEFAULT=[érték]]`
: A rendszergazda által beállítani kívánt alapérték.

`[OVERRIDE=[érték]]`
: A `pam_env` által lekérdezhető és beállítható, az alapértelmezett értéket felülírható értékek.

Egy igen hétköznapi példa, ahol az alapértelmezett értéket felül kell írnia a `pam_env` modulnak, a `DISPLAY` változó, amelyik minden egyes távoli bejelentkezéskor módosításra kerül. Ez a következő ábrán látható: 19.6. példa - pam_env.conf (273. oldal).

19.6 példa *pam_env.conf*

```
REMOTEHOST      DEFAULT=localhost OVERRIDE=@{PAM_RHOST}
DISPLAY         DEFAULT=${REMOTEHOST}:0.0 OVERRIDE=${DISPLAY}
```

Az első sor beállítja a `REMOTEHOST` változót a `localhost` értékre, és ez lesz mindig használva, ha a `pam_env` nem tud kideríteni más értéket. A `DISPLAY` változó pedig tartalmazza a `REMOTEHOST` értékét. A további beállítási lehetőségek az `/etc/security/pam_env.conf` fájlban található megjegyzésekből ismerhetők meg.

19.3.2 limits.conf

Rendszerkorlátok egy felhasználóra vagy felhasználói csoportra a `limits.conf` fájlban állíthatók be, amelyet a `pam_limits` modul olvas ki. A fájlban fix korlátok is beállíthatók (ezeket semmilyen körülmények között nem lehet meghaladni), illetve lágy korlátok, amelyek ideiglenesen túlléphetők. A szintaxis és a rendelkezésre álló

paraméterek megismeréséhez olvassa el az `/etc/security/limits.conf` fájl megjegyzéseit.

19.4 PAM konfigurálás a pam-config használatával

A pam-config eszköz segítséget ad a `/etc/pam.d/common-*-pc` alatt található általános PAM konfigurációs fájlok beállításához, valamint bizonyos alkalmazási beállítások elvégzéséhez. A támogatott modulok listája a `pam-config --list-modules` paranccsal kérhető le. Használja a `pam-config` parancsot a PAM konfigurációs fájlok karbantartásához. Ezzel új modulokkal egészítheti ki a PAM-konfigurációt, törölhet más modulokat vagy módosíthatja a modulok beállításait. Az általános PAM konfigurációs fájlok megváltoztatásakor nincs szükség az egyes alkalmazások PAM-beállításainak kézi hangolására.

A pam-config egy egyszerű, valós felhasználási módja a következőket tartalmazhatja:

1. **Egy friss UNIX-stílusú PAM-konfiguráció automatikus létrehozása.** Hagyja, hogy a pam-config létrehozza a lehető legegyszerűbb beállítást, amit majd később kiterjeszthet. A `pam-config --create` parancs létrehoz egy egyszerű UNIX hitelesítési konfigurációt. A nem a pam-config által karbantartott, már létező konfigurációs fájlok felülíródnak, de a rendszer `*.pam-config-backup` néven megtartja ezek biztonsági másolatát.

2. **Új hitelesítési metódus hozzáadása.** Egy új hitelesítési metódus (például az LDAP) hozzáadása a PAM-modulokhoz egyszerűen a `pam-config --add --ldap` parancs használatával történik. Az LDAP az összes megfelelő helyen hozzáadásra kerül a `common-*-pc` PAM konfigurációs fájlokhoz.

3. **Hibakeresés hozzáadása tesztcélból.** Ha meg akar győződni róla, hogy az új hitelesítési eljárás a terveknek megfelelően működik, akkor kapcsolja be a hibakeresést az összes PAM-mal kapcsolatos műveletnél. A `pam-config --add --ldap-debug` bekapcsolja az LDAP-val kapcsolatos PAM-műveletek hibakeresését. Keresse meg a hibakeresés kimenetét a `/var/log/messages` fájlban.

4 **A beállítások lekérdezése.** Az új PAM-beállítások végleges alkalmazása előtt ellenőrizze, hogy minden hozzáadni kívánt elemet tartalmaznak-e. A `pam-config --query --`*`modul`* kilistázza a lekérdezett PAM-modul típusát és beállításait.

5 **A hibakeresési beállítások eltávolítása.** Befejezésként, ha teljesen elégedett a teljesítménnyel, törölje ki a hibakeresési beállítást. A `pam-config --delete --ldap-debug` kikapcsolja az LDAP-hitelesítés hibakeresését. Ha más moduloknál is bekapcsolta a hibakeresést, akkor hasonló parancsokkal azokat is törölje.

Ha a PAM konfigurációs fájlokat előzmények nélkül hozta létre a `pam-config --create` paranccsal, akkor a `common-*` fájlokról szimbolikus hivatkozások mutatnak a `common-*-pc` fájlokra. A pam-config csak a `common-*-pc` konfigurációs fájlokat módosítja. E szimbolikus hivatkozások törlésével hatékonyan letiltható a pam-config, mivel a pam-config csak a `common-*-pc` fájlokon működik, ezeknek pedig a szimbolikus hivatkozások nélkül semmilyen hatása nincs.

A `pam-config` parancsról és a beállításokról további információkat a `pam-config` és `pam-config(8)` kézikönyv-oldalakon talál.

19.5 További információk

A telepített rendszer `/usr/share/doc/packages/pam` könyvtárában az alábbi dokumentációs anyagok találhatók:

README fájlok
: A könyvtár legfelső szintjén néhány általános README fájl található. A `modules` alkönyvtárban a rendelkezésre álló PAM-modulok README fájljai találhatók.

A Linux-PAM rendszergazda kézikönyve (The Linux-PAM System Administrators' Guide)
: Ez a dokumentum mindent tartalmaz, amit csak egy rendszergazdának tudnia kellhet a PAM-ról. Témakörök sokaságát öleli fel, a konfigurációs fájlok szintaxisától kezdve egészen a PAM biztonsági aspektusáig. A dokumentum PDF-fájlként, HTML-formátumban és sima szövegként is megtalálható.

A Linux-PAM modul írók kézikönyve (The Linux-PAM Module Writers' Manual)
: Ez a dokumentum a témakört a fejlesztők szemszögéből tekinti át, részletes információt adva arról, hogyan készíthetők a szabványnak megfelelő PAM-modulok. A dokumentum PDF-fájlként, HTML-formátumban és sima szövegként is megtalálható.

Linux-PAM alkalmazásfejlesztők kézikönyve (The Linux-PAM Application Developers' Guide)
: Ez a dokumentum mindent tartalmaz a PAM-könyvtárakat használni kívánó alkalmazásfejlesztők számára. A dokumentum PDF-fájlként, HTML-formátumban és sima szövegként is megtalálható.

A PAM kézikönyv-oldalak
: A PAM általában is, de az egyes modulok is kézikönyv-oldalakkal együtt állnak rendelkezésre. Ezek jól használható áttekintést nyújtanak a vonatkozó összetevők funkcionalitásáról.

Thorsten Kukuk számos PAM-modult készített SUSE LINUX alá, és ezekhez leírást is mellékelt. Ezek helye: `http://www.suse.de/~kukuk/pam/`.

V. rész - Szolgáltatások

20 A hálózatkezelés alapjai

A Linux biztosítja a szükséges hálózatkezelési eszközöket és szolgáltatásokat az összes típusú hálózati struktúrába való integrálhatóság érdekében. Az alábbiakban leírjuk a Linux által legszélesebb körben alkalmazott TCP/IP protokoll különféle szolgáltatásait és funkcióit. A hálózati kártyákkal, modemmel vagy egyéb eszközökkel történő hálózatelérés mind-mind beállítható a YaST segítségével. Manuális konfiguráció is lehetséges. Ebben a fejezetben csak a legalapvetőbb mechanizmusokról írunk és a legfontosabb hálózati konfigurációs fájlokat tekintjük át.

A Linux és más operációs rendszerek alapvetően a TCP/IP protokollt használják. Pontosabban szólva, ez nem is egy egyedülálló hálózati protokoll, sokkal inkább egy különféle szolgáltatásokat nyújtó hálózati protokollcsalád. A 20.1 táblázat - A TCP/IP protokollcsalád különféle protokolljai (280. oldal) ábrán felsorolt protokollok két gép közötti TCP/IP alapú adatcserére szolgálnak. A TCP/IP protokollcsalád segítségével összekapcsolt hálózatok egy világméretű hálózatot alkotnak, az „internetet.”

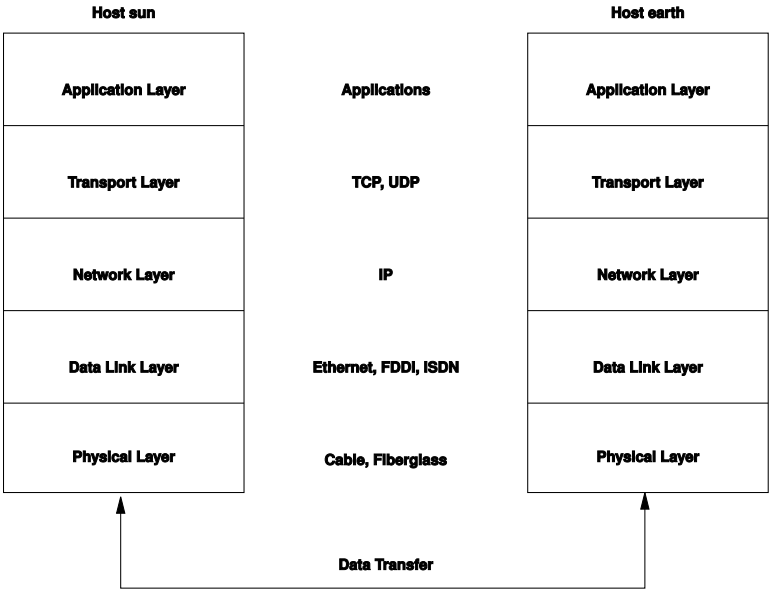
Az RFC a *Request for Comments* (megjegyzések kérése) kifejezés rövidítése. Az RFC-k a különféle internetes protokollokat, illetve az operációs rendszerek és alkalmazások számára a megvalósítási eljárásaikat leíró dokumentumok. Az RFC dokumentumok leírják az internetes protokollok beállításának módját is. A protokollokkal kapcsolatos ismeretek bővítése érdekében érdemes elolvasni a megfelelő RFC dokumentumokat. Ezek a `http://www.ietf.org/rfc.html` címen olvashatók.

20.1. táblázat *A TCP/IP protokollcsalád különféle protokolljai*

Protokoll	Leírás
TCP	Transmission Control Protocol: Kapcsolatorientált, biztonságos protokoll. A továbbítandó adatok először az alkalmazáshoz továbbítódnak, mint adatfolyam, és az operációs rendszer alakítja őket át a megfelelő formátumra. Az adat a célgépen futó megfelelő alkalmazáshoz mindig az eredetileg elküldött adatfolyam formájában érkezik meg. A TCP megállapítja, hogy veszett-e el adat az átvitel során, illetve hogy az adatok sorrendje összekeveredett-e. A TCP ott kerül alkalmazásra, ahol az adatok sorrendje fontos.
UDP	User Datagram Protocol: Kapcsolat nélküli, nem biztonságos protokoll. Az adatok az alkalmazás által előállított csomagok formájában kerülnek továbbításra. A fogadó félhez érkező adatok sorrendje nem garantált, adatvesztés is előfordulhat. Az UDP a rekordorientált alkalmazások számára hasznos. Előnye a TCP-vel szemben a kisebb késleltetés.
ICMP	Internet Control Message Protocol: Ez igazából nem a végfelhasználóknak szánt protokoll, hanem egy különleges vezérlési protokoll, amely hibajelentéseket biztosít, illetve képes ellenőrizni a TCP/IP-adatátvitelben résztvevő gépek viselkedését. Ezenkívül van egy egyedi visszhang üzemmódja is, amelyet például a ping program használ.
IGMP	Internet Group Management Protocol: Ez a protokoll szabályozza a gép viselkedését IP multicast (többesszórás) használata közben.

A 20.1. ábra - A TCP/IP egyszerűsített rétegmodellje (281. oldal) jól mutatja, hogy az adatcsere több szinten, rétegben zajlik: A tényleges hálózati réteg az IP (Internet Protocol) alapú, nem biztonságos adatátvitel. A TCP (transmission control protocol) az IP protokollra épül rá, és azt használva valósít meg biztonságos adatátvitelt. Az IP-réteg maga is ráépül egy legalsó, hardverszintű protokollra, mint amilyen például az Ethernet.

20.1. ábra *A TCP/IP egyszerűsített rétegmodellje*



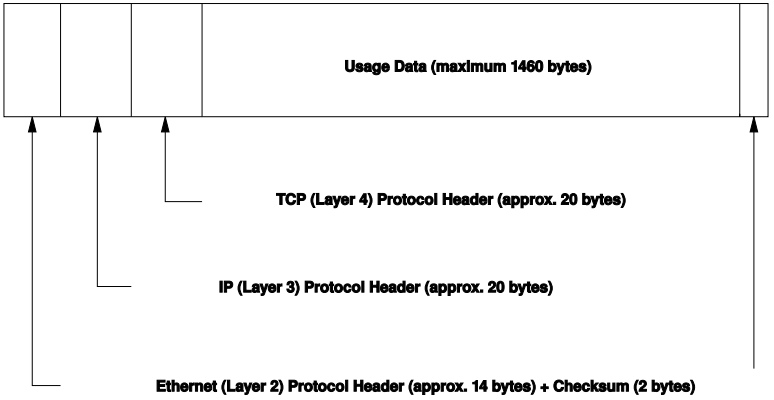
Az ábrán minden rétegre egy vagy két példát láthatunk. A rétegek az *absztrakciós szinteknek* megfelelően vannak elrendezve. A legalsó szinten a hardverhez közeli réteg található. A legfelső réteg ezzel szemben már szinte teljesen elvonatkoztat a hardversajátosságoktól. Minden rétegnek megvan a saját speciális funkciója. Az egyes rétegek szerepe általában kiderül a leírásukból. Az adatkapcsolati és a fizikai rétegek jelentik a használt fizikai hálózatot (például Ethernet).

A hardverközeli protokollok szinte mindegyike csomagalapú megoldást alkalmaz. Az átvinni kívánt adatok *csomagokba* szerveződnek, mivel egyszerre nem küldhető el mind. Egy TCP/IP csomag mérete maximum 64 kilobájt lehet. A csomagok általában ennél azonban sokkal kisebbek, mert a hálózati hardver korlátozó tényezőt jelent. Az adatcsomag maximális mérete például egy Ethernet-szegmensben 1500 bájt. A TCP/IP-csomag mérete maximum ekkora lehet, ha az adatok Ethernet-hálózaton keresztül kerülnek továbbításra. Ha több adatot szeretnénk továbbítani, akkor az operációs rendszernek több adatcsomagot kell elküldenie.

Hogy a rétegek elvégezhessék a nekik szánt feladatot, minden réteg számára kiegészítő információt kell elmenteni az adatcsomagokba. Ez az információ a csomag *fejlécében* található. Minden réteg egy rövid adatblokkot, ún. protokollfejlécet fűz a csomagok elejére. A 20.2. ábra - TCP/IP Ethernet-csomag (282. oldal) ábra egy TCP/IP adatcsomag

továbbítására mutat példát Ethernet-kábelen. Az ellenőrző összeg nem a csomag elején, hanem a végén található. Ez leegyszerűsíti a hálózati hardver dolgát.

20.2. ábra *TCP/IP Ethernet-csomag*



Amikor egy alkalmazás adatokat küld a hálózaton keresztül, az adatok a fizikai réteg kivételével olyan rétegeken haladnak keresztül, amelyeket a Linux-kernel tartalmaz. Minden réteg felelős azért, hogy az adatokat előkészítse a következő réteg számára. Az adatok tényleges elküldéséért a legalacsonyabb réteg felelős. Adatok fogadása esetén az egész folyamat fordítva zajlik le. A rétegek olyanok, mint egy hagyma: az egyes rétegekben a protokolfejlécek leválasztásra kerülnek a szállított adatokról. Végül a szállítási réteg felelős azért, hogy a célgép alkalmazásai számára felhasználható adatokat állítson elő. Mindez azt jelenti, hogy egy réteg csak a közvetlenül felette és alatta lévő rétegekkel kommunikálhat. Az alkalmazásoknak mindegy, hogy az adat egy 100 megabit/másodperc sebességű FDDI hálózaton, vagy egy 56 kilobit/másodperces modemen keresztül érkezik. Az adatvonalnak is mindegy, hogy milyen adatokat továbbít, feltéve, hogy azok formátuma megfelelő.

20.1 IP-címek és útválasztás

Az alábbi szakaszban csak az IPv4 hálózatokkal foglalkozunk. Az IPv4-et felváltó IPv6 protokollal kapcsolatos további információ: 20.2. - IPv6 – az internet következő generációja (285. oldal).

20.1.1 IP-címek

Az internet minden egyes számítógépe saját 32 bites címmel rendelkezik. Ezt a 32 bitet (azaz 4 bájtot) általában a következő példa második sorában látható módon írjuk: 20.1. példa - IP-címek leírása (283. oldal).

20.1 példa *IP-címek leírása*

```
IP Address (binary):  11000000 10101000 00000000 00010100
IP Address (decimal):      192.     168.       0.      20
```

Decimális formában a négy bájtot tízes számrendszerben ábrázoljuk, pontokkal elválasztva. IP-címe egy gépnek, illeve egy hálózati csatolónak lehet (és kell lennie). Ez az IP-cím a világon sehol máshol nem használható. A szabály alól vannak bizonyos kivételek, de a következő részekben ezek jelentősége elhanyagolható.

Az IP-címben látható pontok egy hierarchikus rendszerre utalnak. Az 1990-es évekig az IP-címek szigorúan osztályokba voltak sorolva. Ez a rendszer azonban túlságosan merevnek bizonyultak, ezért beszüntették a használatát. Napjainkban ezért az *osztálynélküli útválasztást* (CIDR, classless interdomain routing) használjuk.

20.1.2 Hálózati maszkok és útválasztás

A hálózati maszk az alhálózat címtartományát adja meg. Az azonos alhálózaton lévő gépek közvetlenül el tudják egymást érni. A különböző alhálózatban lévő gépeknek szükségük van az átjáró címére, amely kezeli az alhálózat és a világ többi része közötti forgalmat. Annak ellenőrzéséhez, hogy két IP-cím ugyanabban az alhálózatban van-e, egyszerűen hozza „ÉS” kapcsolatba a két címet és a hálózati maszkot. Ha az eredmények megegyeznek, akkor mindkét IP-cím azonos helyi hálózatban található. Ha az eredmények különböznek, akkor az IP-cím távoli, és a távoli csatoló csak átjárón keresztül érhető el.

A hálózati maszk működésének megértéséhez tekintse meg a következő részt: 20.2. példa - IP-címek és hálózati maszkok összekapcsolása (284. oldal). A hálózati maszk 32 bitből áll, amely mutatja, hogy az IP-cím mekkora része tartozik a hálózathoz. Az `1`-es bitek jelzik, hogy az IP-cím megfelelő bitje a hálózathoz tartozik. A `0`-ás bitek az alhálózatban lévő biteket jelzik. Ez azt jelenti, hogy minél több `1`-es bit van, annál kisebb az alhálózat. Mivel a hálózati maszk mindig számos egymást követő `1`-es bitből áll, a hálózati maszkban lévő bitek egyszerűen megszámolhatók. 20.2. példa - IP-címek és

hálózati maszkok összekapcsolása (284. oldal) esetében az első 24 bitet tartalmazó hálózat a következőképp is leírható: `192.168.0.0/24`.

20.2 példa *IP-címek és hálózati maszkok összekapcsolása*

```
IP address (192.168.0.20):  11000000 10101000 00000000 00010100
Netmask   (255.255.255.0):  11111111 11111111 11111111 00000000
----------------------------------------------------------------
Result of the link:         11000000 10101000 00000000 00000000
In the decimal system:           192.     168.       0.       0

IP address (213.95.15.200): 11010101 10111111 00001111 11001000
Netmask    (255.255.255.0): 11111111 11111111 11111111 00000000
----------------------------------------------------------------
Result of the link:         11010101 10111111 00001111 00000000
In the decimal system:           213.      95.      15.       0
```

Egy másik példa: az ugyanarra az Ethernet-kábelre csatlakozó gépek rendszerint egy alhálózatban találhatók és közvetlenül elérhetők. Ha az Ethernet-hálózatot kapcsolók (switch) vagy hidak (bridge) osztják fel, ezek a gépek még mindig közvetlenül elérhetők.

A helyi alhálózaton kívüli IP-címek csak akkor érhetők el, ha egy átjáró be van állítva a célhálózathoz. A legáltalánosabb esetben csak egy átjáró van, amely az összes külső forgalmat kezeli. Azonban a különböző alhálózatokhoz több átjáró is beállítható.

Átjáró megadása esetén az IP-csomagok a megfelelő átjárón keresztül továbbítódnak. Az átjárók ugyanúgy továbbítják a csomagokat –géptől gépig –, amíg az eléri a címzett gépet vagy a csomag TTL-je (time to live – élettartam) le nem jár.

20.2. táblázat *Speciális címek*

Címtípus	Leírás
Hálózati alapcím	Ez a hálózati maszk és bármely hálózati cím ÉS kapcsolata, ahogy az a következő példa `Eredmények` részben látható: 20.2. példa - IP-címek és hálózati maszkok összekapcsolása (284. oldal). Ez a cím nem rendelhető egy géphez sem.
Nyilvános (broadcast) cím	Ez lényegében azt jelenti, hogy az „Alhálózat minden gépe.” Ezt úgy állítjuk elő, hogy a hálózati maszkot bináris formátumra alakítjuk és a hálózati alapcímmel logikai VAGY kapcsolatba

Címtípus	Leírás
	hozzuk. A fenti példa eredménye így 192.168.0.255. Ez a cím egy géphez sem rendelhető.
Helyi gép	A `127.0.0.1` cím szigorúan a „loopback eszköz” számára van kijelölve. Ezen a címen keresztül kapcsolat létesíthető a saját géppel.

Mivel az IP-címek az egész világon egyediek, nem szabad ötletszerűen kitalált címekkel csatlakozni a világhálóra. Három címtartomány van fenntartva saját, zárt célokra szánt, IP alapú hálózat kialakítására. Bizonyos trükkök alkalmazása nélkül ezekkel a címekel nem lehetséges az internet felé kapcsolatot létesíteni, hiszen ezek a címek nem kerülnek továbbításra az interneten. Ezeket a címtartományokat az RFC 1597 definiálja és a 20.3 táblázat - IP-címtartományok privát felhasználásra (285. oldal) mutatja be őket.

20.3. táblázat *IP-címtartományok privát felhasználásra*

Hálózat/hálózati maszk	Tartomány
`10.0.0.0/255.0.0.0`	`10.x.x.x`
`172.16.0.0/255.240.0.0`	`172.16.x.x – 172.31.x.x`
`192.168.0.0/255.255.0.0`	`192.168.x.x`

20.2 IPv6 – az internet következő generációja

A WWW (World Wide Web) megjelenése miatt az interneten keresztül, TCP/IP segítségével kommunikáló gépek száma robbanásszerűen megnőtt az elmúlt tizenöt évben. Mióta Tim Berners-Lee a CERN-nél (`http://public.web.cern.ch`) 1990-ben kitalálta a WWW-t, az internetre kapcsolódó gépek száma néhány ezerről megközelítőleg százmillióra nőtt.

Amint már említettük, egy IPv4 cím mindössze 32 bitet tartalmaz. Hálózatszervezési okokból az IP-címek egy része nem is használható – így azután sok IP-cím elvész. Egy alhálózaton belül rendelkezésre álló címek száma úgy számítható ki, ha a kettőt az alhálózat bitjeinek száma szerinti hatványra emeljük, majd az így kapott számból kivonunk kettőt. Az alhálózatban tehát 2, 6 vagy 14 cím használható. Ahhoz tehát, hogy például 128 gépet az internetre kapcsoljuk, egy 256 IP-címmel rendelkező alhálózatra van szükség. A címek közül csak 254 használható, mivel az alhálózat struktúrájának kialakításához két IP-címre szükség van: a broadcast és a hálózati alapcímre.

A potenciális címhiány leküzdése érdekében a ma elterjedt IPv4 protokoll alatt olyan eljárásokat szokás használni, mint a DHCP vagy a NAT (network address translation, hálózati címfordítás). Mivel a privát és nyilvános címek szigorúan el vannak különítve, ezek a módszerek valóban alkalmasak a hiány enyhítésére. Az eljárás hátránya a bonyolultabb beállítás és a nagyobb rendszerkarbantartási munka. Egy IPv4 kliensgép beállításához egy sor címadatra van szükség: a gép IP-címére, hálózati maszkjára, az átjáró címére és esetleg a névkiszolgáló címére. Ezeket az adatokat ismerni kell, nem lehet őket egyszerűen leszármaztatni valahonnan máshonnan.

Az IPv6 mind a címek hiányának, mind a bonyolult beállításnak a problémáját megszünteti. A következő szakaszokban részletesebben bemutatjuk az IPv6 továbbfejlesztéseit és előnyeit, illetve beszélünk a régi protokollról az újra átállásról.

20.2.1 Előnyök

Az új protokoll legfontosabb és leginkább szembetűnő előnye a felhasználható címtér rendkívüli bővülése. Egy IPv6-cím a hagyományos 32 bit helyett 128 bites értékekből áll. Ez azt jelenti, hogy akár több trillió IP-cím használható.

Az IPv6 címek azonban nem csak hosszukban különböznek elődeiktől. Belső szerkezetük is más, így a címek információt tartalmazhatnak azokról a rendszerekről és hálózatokról is, amelyekhez tartoznak. További részletek erről: 20.2.2. - Címtípusok és címzési rendszer (288. oldal).

Az új protokoll további előnyei:

Automatikus beállítás
: Az IPv6 hálózatban valóban működik az „azonnali használat” (plug and play), vagyis egy újonnan telepített rendszer bármiféle kézi beállítás nélkül is beilleszkedik a (helyi) hálózatba. Az új gép egy automatikus beállítási mechanizmus segítségével,

a szomszéd útválasztóktól egy *neighbor discovery* (ND) nevű protokoll segítségével megkapott adatokból deríti ki saját címét. Ez a beállítás a rendszergazda közreműködése nélkül történik, és központi IP-címkiosztó kiszolgáló beállítására sincs szükség – újabb előny az IPv4-gyel szemben, ahol az automatikus címkiosztáshoz DCHP címkiszolgálót kell beüzemelni.

Mobilitás
: Az IPv6 lehetővé teszi, hogy egy hálózati csatolóhoz egyidőben több címet rendeljünk. Így a felhasználók könnyen elérhetnek különböző hálózatokat is, hasonlóan a mobiltelefon-szolgáltatók által kínált barangolási (roaming) szolgáltatáshoz: ha mobiltelefonunkkal kimegyünk külföldre, akkor a megfelelő területre érve a telefon automatikusan kiválaszt egy ottani szolgáltatót. Ez azt jelenti, hogy bárhol is legyünk, mindig ugyanazon a telefonszámon vagyunk elérhetők és úgy tudunk onnan telefonálni, mintha otthon lennénk.

Biztonságos kommunikáció
: Az IPv4 alatt a hálózati biztonság egy kiegészítő funkció. Az IPv6-nak az IPSec alapú titkosítás már szerves része, így két rendszer kommunikálhat egy biztonságos ún. alagúton (tunnel) keresztül anélkül, hogy az internetről bárki le tudná hallgatni.

Visszamenőleges kompatibilitás
: A teljes internet átállítása lehetetlen egyik pillanatról a másikra IPv4-ről IPv6-ra. Épp ezért nagyon fontos, hogy a két rendszer egyszerre működhessen ne csak az interneten, hanem akár egyetlen gépen belül is. Ezt a kompatibilis címek (az IPv4 címek egyszerűen átalakíthatók IPv6-címekké), és különféle alagutak alkalmazása biztosítja. Lásd: 20.2.3. - IPv4 és IPv6 együtt (292. oldal). Ezek kívül a rendszer használhat egy *dual stack IP* (kettős protokollcsomag) nevű technikát is, amely egyidőben támogatja mindkét protokollt, vagyis két teljesen különálló hálózati alrendszert használnak és a két protokollverzió semmilyen hatással nincs egymásra.

Testreszabott szolgáltatások többesszórás (multicasting) segítségével
: IPv4 alatt egyes szolgáltatások (például az SMB) a helyi hálózat minden gépének elküldi a csomagjait nyilvános (broadcast) üzenetekben. Az IPv6 jóval finomabb felosztást tesz lehetővé: a kiszolgálók az egyes gépeket *többesszórás* (multicasting, szokták differenciált sugárzás néven is emlegetni) segítségével is elérhetik – vagyis csak egy adott csoportba tartozó gépeket címeznek meg, szemben az összes gépnek szóló *nyilvános* (broadcast) vagy az egyetlen gépnek szóló *unicast* üzenetekkel. Az, hogy mely gépek kerülnek egy csoportként megcímzésre, a tényleges alkalmazástól függ. Vannak azonban előre meghatározott multicast-csoportok is,

például az összes névkiszolgáló (*all name servers multicast group*, vagy az összes útválasztó (*all routers multicast group*).

20.2.2 Címtípusok és címzési rendszer

Amint már említettük, a jelenlegi IP protokoll fogyatékossága két fontos területen szembetűnő: egyrészt lassan elfogynak a rendelkezésre álló IP-címek, másrészt egyre bonyolultabb és kényelmetlenebb feladat a hálózati beállítások és az útválasztótáblák karbantartása. Az IPv6 az első problémát a címtér 128 bitre bővítésével oldja meg. A második probléma megoldását a hierarchikus címszerkezet, az új, intelligens címkiosztási eljárások és az ún. *multihoming* jelenti (egy csatolóhoz több cím is rendelhető a különböző hálózatok eléréséhez).

IPv6 esetén az alábbi háromféle címtípust különböztetjük meg:

Unicast (egyesszórás, egyedi sugárzás)
: Az ilyen típusú címek pontosan egy hálózati csatolóhoz tartoznak. Az ilyen című csomagok kizárólag egy címzetthez érkeznek meg. Ennek megfelelően a unicast címek arra szolgálnak, hogy a csomagok a helyi hálózat vagy az internet egyes gépeihez eljussanak.

Multicast (többesszórás, differenciált sugárzás)
: Az ilyen típusú címek hálózati csatolók egy adott csoportjára vonatkoznak. Az ilyen című csomagok a csoport összes tagjához kézbesítésre kerülnek. A multicast-címeket elsősorban bizonyos hálózati szolgáltatások használják arra, hogy adott gépcsoportokat könnyen és egyszerűen el tudjanak érni.

Anycast (nem differenciált üzenetek)
: Az ilyen típusú címek csatolók egy adott csoportjára vonatkoznak. Az ilyen című csomagok a csoportnak a használt útválasztási protokoll elvei szerint a küldő félhez legközelebbi tagjához érkeznek. Az anycast címeket arra használjuk, hogy egyszerűbb legyen megtalálni az adott hálózati területen egy bizonyos szolgáltatást nyújtó kiszolgálókat. Az ugyanolyan típusú kiszolgálók mind ugyanazzal az anycast-címmel rendelkeznek. Amikor egy gép kér egy bizonyos szolgáltatást, az a kiszolgáló fog rá válaszolni, amelyik az útválasztási protokoll szerint a legközelebb található a küldő géphez. Ha ez a kiszolgáló bármi oknál fogva kiesne, akkor a protokoll automatikusan a következő legközelebbi kiszolgálót választja, majd a harmadikat stb.

Egy IPv6-cím nyolc darab négyszámjegyű mezőből áll, amelyek mindegyike 16 bitet ábrázol, hexadecimális jelöléssel. A mezőket kettőspont (`:`) választja el. A mezők elején álló nulla bájtokat ki lehet hagyni, a mezőn belül, vagy annak végén azonban ez tilos. Amennyiben egymás után több mint négy nulla bájt szerepel, akkor ezek dupla kettősponttal rövidíthetők. Egy címen belül azonban csak egyszer alkalmazható a `::` jelölés. Az összevonás lehetőségeit a 20.3. példa - Példák ugyanazon IPv6-cím írásmódjára (289. oldal) táblázat mutatja, ahol mindhárom sor ugyanazt a címet jelenti.

20.3 példa *Példák ugyanazon IPv6-cím írásmódjára*

```
fe80 : 0000 : 0000 : 0000 : 0000 : 10 : 1000 : 1a4
fe80 :    0 :    0 :    0 :    0 : 10 : 1000 : 1a4
fe80 :                           : 10 : 1000 : 1a4
```

Az IPv6-címek minden egyes részének külön szerepe van. Az első bájtok képezik az előtagot (prefix) és határozzák meg a cím típusát. A középső rész a cím hálózati része, de előfordulhat, hogy ez nincs használva. Az utolsó rész azonosítja az egyes gépet. A hálózati maszkot IPv6 alatt a prefix hossza határozza meg, amelyet az IP-cím végén jelzünk egy törtvonallal elválasztva. 20.4. példa - Az előtag hosszát megadó IPv6-cím (289. oldal) ábra például azt mutatja, hogy az első 64 bit a hálózati szegmenst, az utolsó 64 bit pedig a gépazonosítót határozza meg. Más szavakkal a `64` azt jelenti, hogy a hálózati maszkot balról 64 darab 1-es bittel kell kitölteni. Az IPv4-nél megszokott módon, a hálózati maszk és az IP-cím ÉS kapcsolata határozza meg, hogy egy gép ugyanahhoz, vagy egy másik alhálózathoz tartozik-e

20.4 példa *Az előtag hosszát megadó IPv6-cím*

```
fe80::10:1000:1a4/64
```

Az IPv6 különböző jelentésű előtagokat ismer. Ezek egy részét a 20.4 táblázat - Különféle IPv6-előtagok (289. oldal) mutatja.

20.4. táblázat *Különféle IPv6-előtagok*

Előtag (hexa)	Meghatározás
`00`	IPv4-címek és IPv6-on keresztüli IPv4 (IPv4 over IPv6), kompatibilis címek. Ezek feladata a kompatibilitás fenntartása az IPv4-gyel. Használatukhoz az szükséges, hogy az útválasztó át tudja alakítani az IPv6-címeket IPv4-címekké. Számos speciális cím (például a loopback eszköz) is ezzel az előtaggal rendelkezik.

Előtag (hexa)	Meghatározás
Az első számjegy `2` vagy `3`	Aggregálható általános unicast-címek (aggregatable global unicast addresses). Ahogy az IPv4 esetében, egy csatoló itt is hozzárendelhető egy adott alhálózathoz. Jelenleg a következő címterek vannak lefoglalva: `2001::/16` (éles minőségű címtér, production quality address space) és `2002::/16` (6to4 címtér, 6to4 address space).
`fe80::/10`	Link-local (adatkapcsolati szinten helyi) címek. Az ilyen előtaggal rendelkező címeken nem kerül alkalmazásra útválasztás, vagyis csak ugyanazon alhálózaton belül érhetők el.
`fec0::/10`	Site-local (telephelyi szinten helyi) címek. Ezek a címek ugyan áthaladhatnak az útválasztón, de csak azon szervezet hálózatán belül, amelyhez tartoznak Az IPv6-ban ezek a címek felelnek meg az eddigi magánhálózati címtérnek (mint pl. a `10.x.x.x`).
`ff`	Ezek a multicast-címek.

Az unicast-címek három fő részből állnak:

Public Topology (nyilvános topológia)
: A cím első része (amely többek között a fent említett előtagok egyikét is tartalmazza) felelős a csomag forgalomirányításáért a nyilvános interneten. Tartalmaz például információt az internet-hozzáférést biztosító szolgáltatóról vagy szervezetről is.

Site Topology (telephely-topológia)
: A második rész forgalomirányítási adatokat tartalmaz arról, hogy melyik alhálózatba kell a csomagokat továbbítani.

Interface ID (Csatolóazonosító)
: A harmadik rész azonosítja a csatolót, amelyre továbbítani kell a csomagot. Ez lehetővé teszi, hogy a MAC-cím az IPv6-cím része legyen. Mivel a MAC-cím az egész világon egyedi (a hardvergyártók rögzítik az eszközben), lényegesen leegyszerűsödik a beállítási folyamat. Az első 64 címbit egy úgynevezett `EUI-64` tokent képez, amelynek a legutolsó 48 bitje a MAC-cím, a maradék 24 bit pedig speciális információt tartalmaz a token típusáról. Ez lehetővé teszi, hogy olyan eszközökhöz

is lehessen `EUI-64` tokent hozzárendelni, melyek nem rendelkeznek MAC-címmel (pl. PPP- és ISDN-kapcsolatok).

A unicast-címek alapvető felépítéséből adódóan az IPv6 ötfajta unicast-címet különböztet meg:

`::` (nem megadott)
: Ezt a címet akkor használja forráscímként egy gép, amikor a csatoló első alkalommal aktiválódik – és amikor a cím egyéb módon még nem határozható meg

`::1` (loopback)
: A loopback (hurok, sajátgép) eszköz címe.

IPv4-kompatibilis címek
: Az IPv6-cím az IPv4-címből és egy 96 db nulla bitet tartalmazó előtagból áll. Ez a fajta kompatibilitási cím elsősorban alagutak kialakítására (tunneling) használatos (lásd: 20.2.3. - IPv4 és IPv6 együtt (292. oldal)). Az IPv6- és IPv4-gépek így olyan gépekkel is tudnak kommunikálni, amelyek egy tiszta IPv4-hálózatban találhatók.

IPv6-ra leképezett IPv4-címek
: Ez a fajta cím egy tiszta IPv4-címet ad meg IPv6-jelöléssel.

Helyi címek
: Helyi használatra kétféle címtípus áll rendelkezésre:

  link-local (adatkapcsolati szinten helyi)
  : Ez a fajta cím csak az adott helyi alhálózaton belül használható. Az ilyen típusú forrás- vagy célcímmel rendelkező csomagok nem kerülnek továbbításra az internet vagy más alhálózatok felé. Ezek a címek egy speciális előtagot tartalmaznak (`fe80::/10`), valamint a hálózati kártya azonosítóját. A középső rész csupa nulla bájt. Az ilyen típusú címek az ugyanazon alhálózat más gépeivel folytatott kommunikációra szolgálnak az automatikus beállítás során.

  site-local (telephelyi szinten helyi)
  : Az ilyen címtípusú csomagok átirányíthatók más alhálózatokra, de a szélesebb értelemben vett internetre nem – az adott szervezet hálózatán belül kell maradniuk. Ezek a címek jellemzően intraneteken és az IPv4-ben meghatározott magánhálózati címek helyett használhatók. A speciális előtag (`fec0::/10`), és a csatolóazonosító mellett egy 16 bites mezőt tartalmaznak, amely az alhálózatot azonosítja. A többi mező értéke nulla.

Az IPv6 egy teljesen új funkciója, hogy egy hálózati csatoló rendszerint több IP-címet is kaphat. Ennek az az előnye, hogy így több hálózathoz is hozzá lehet férni egyszerre, ugyanazzal a csatolóval. E hálózatok egyike a MAC-cím és egy ismert előtag segítségével teljesen automatikusan beállítható, így az IPv6 rendszer indítását követően a helyi hálózat összes gépe azonnal elérhető (a link-local cím segítségével). Mivel a MAC-cím az IP-cím része, ezért biztos, hogy minden cím egyedi lesz. A címben egyedül a *site topology* (telephely-topológia) és a *public topology* (nyilvános topológia) paraméterek változhatnak attól függően, hogy a gép éppen melyik hálózaton belül működik.

Ahhoz, hogy egy gép több hálózat között mozoghasson, legalább két címre van szüksége. Ezek egyike, az *otthoni cím* (home address) a csatolóazonosító mellett az otthoni hálózat azonosítóját is tartalmazza (valamint a megfelelő előtagot). Az otthoni cím statikus, ezért általában nem kerül módosításra. Az újdonság az, hogy a mozgó, mobil gépnek szánt minden egyes csomag elküldhető rá, függetlenül attól, hogy a gép valóban az otthoni hálózatban működik, vagy teljesen máshol. Ezt az IPv6-ban bevezetett két vadonatúj funkció teszi lehetővé: az *állapot nélküli automatikus konfiguráció* (stateless autoconfiguration) és a *szomszédok felderítése* (neighbor discovery). A mobil eszközök az otthoni címen kívül további címekkel is rendelkezhetnek, amelyek abból a hálózatból származnak, amelyben éppen találhatók. Ezeket *care-of* (postai küldeményeken használt rövidítés, vki címén) címeknek hívjuk. Az otthoni hálózatban egy olyan szolgáltatásnak kell futnia, mely automatikusan a megfelelő hálózatba továbbítja a távol lévő gép otthoni címére küldött csomagokat. IPv6-környezetben ezt a funkciót az ún. *home agent* (otthoni ügynök) látja el, amely minden, a mobil gép otthoni címére küldött csomagot egy alagúton keresztül a gép aktuális care-of címére továbbít. A care-of címre küldött csomagok persze mindenféle kitérő nélkül közvetlenül a mobil eszközre kerülnek továbbításra.

20.2.3 IPv4 és IPv6 együtt

Az internetre csatlakozó összes gép átállítása IPv4-ről IPv6-ra csak fokozatosan történhet. Egy ideig a két protokoll párhuzamosan fog létezni. Egy rendszeren belül az együttes működés *kettős protokollcsomag* (dual stack) megvalósításával garantálható. Továbbra is fennállnak azonban azok a problémák, hogy hogyan tudnak IPv6-gépek IPv4-gépekkel kommunikálni, illetve hogyan továbbíthatók IPv6-csomagok a jelenlegi, túlnyomórészt IPv4 alapú hálózatokban. A legjobb megoldást az alagutak (tunneling) és a kompatibilitási címek használata jelenti (lásd: 20.2.2. - Címtípusok és címzési rendszer (288. oldal)).

A világméretű IPv4-hálózatban egyelőre elszigetelt IPv6-hálózatok alagutakon keresztül cserélhetik ki adataikat: az IPv6-adatok IPv4-csomagokba kerülnek beágyazásra, hogy

az IPv4-hálózaton keresztül továbbíthatók legyenek. Két IPv4-gép ilyen kapcsolatát *alagútnak* (tunnel) nevezzük. Ehhez a csomagoknak tartalmaznia kell az IPv6-célcímet (vagy annak megfelelő előtagját) és az alagút fogadó végén található célgép IPv4-címét. Egy alapszintű alagút manuálisan is beállítható, ha a gépek rendszergazdái megegyeznek. Ezt *statikus alagútnak* (static tunneling) is hívják.

A statikus alagutak beállítása és karbantartása azonban gyakran túlságosan munkaigényes a mindennapos kommunikációban használathoz. Éppen ezért az IPv6 három különböző módszet is kínál *dinamikus alagutak* (dynamic tunneling) kialakításához:

6over4
: Az IPv6-csomagok automatikusan IPv4-csomagokká kerülnek átalakításra, és olyan IPv4-hálózaton keresztül kerülnek továbbításra, amelyik képes multicast-üzenetek továbbítására. Az IPv6 úgy érzékeli, hogy a teljes hálózat (az internet) egyetlenegy óriási helyi hálózat (LAN). Ezzel az eljárással automatikusan ki lehet deríteni az IPv4 alagút végpontját. Ez az eljárás azonban rosszul méretezhető, valamint az IPv4 multicast használata messze nem terjedt el széles körben az interneten. Ez tehát elsősorban kisebb vállalati vagy szervezeti hálózatokban jelent megoldást, ahol rendelkezésre áll multicast. A módszer leírása az RFC 2529-ben található meg.

6to4
: Ennél az eljárásnál az IPv6-címekből automatikusan IPv4-címek kerülnek előállításra, így az elszigetelt IPv6-hálózatok egy IPv4-hálózaton kereszül tudnak egymással kommunikálni. A gyakorlatban azonban az elszigetelt IPv6-gépek és az internet közötti kommunikáció nem problémamentes. A módszert az RFC 3056 írja le.

IPv6 Tunnel Broker (alagútbróker)
: E módszer használatához speciális kiszolgálókra van szükség, amelyek dedikált alagutakat biztosítanak az IPv6-gépek számára. Ezt a módszert az RFC 3053 írja le.

20.2.4 IPv6 beállítása

Az IPv6 beállításához általában semmit nem kell tenni az egyes munkaállomásokon. Az IPv6 alapértelmezésben engedélyezett. A telepítés során ez azonban letiltható a következő részben leírt hálózati konfigurációs lépésekben: „Network Configuration” szakasz (1. fejezet - *Installation with YaST*, ↑*Start-Up*). Az IPv6 telepített rendszeren történő letiltásához vagy engedélyezéséhez használja a YaST *Hálózati beállítások* modulját. Az *Általános beállítások* lapon igény szerint jelölje meg az *IPv6 engedélye-*

zése lehetőséget. Az IPv6 manuális engedélyezéséhez adja ki a `modprobe ipv6` parancsot `root` felhasználóként.

Az IPv6 automatikus konfigurációs funkciójának köszönhetően a hálózati kártya kap egy címet a *link-local* hálózatból. Általában a munkaállomásokon nincs szükség az útválasztási táblák felügyeletére. A munkaállomás lekérdezheti a hálózati útválasztókat az *útválasztó-meghirdetési protokoll* (router advertisement protocol) segítségével, hogy megtudja, milyen előtagot és átjárókat kell használnia. IPv6-útválasztó az radvd programmal állítható be. Ez a program értesíti a munkaállomásokat, hogy milyen előtagot használjanak az IPv6-címekhez, illetve mely útválasztókat használják. Ennek alternatívájaként a zebra/quagga nevű program használható a címek és az útválasztás automatikus beállításához.

Azzal kapcsolatban, hogyan állíthatók be az egyes alagutak az `/etc/sysconfig/network` fájlok segítségével, olvassa el az ifcfg-tunnel(5) parancs man oldalait.

20.2.5 További információk

A fenti áttekintés temészetesen nem térhetett ki az IPv6 minden részletére. Az új protokoll mélyebb megismeréséhez az alábbi online dokumentációt és könyveket ajánljuk:

`http://www.ipv6.org/`
: Jó kezdőpont mindenhez, ami az IPv6-tal kapcsolatos.

`http://www.ipv6day.org`
: Minden információt tartalmaz, amire a saját IPv6-hálózat kialakításához szükség lehet.

`http://www.ipv6-to-standard.org/`
: Az IPv6-ra felkészített eszközök listája.

`http://www.bieringer.de/linux/IPv6/`
: Linux-IPv6-HOWTO és számos további, a témakörrel kapcsolatos hivatkozás.

2640-es RFC
: Az IPv6 alapvető RFC-je.

IPv6 Essentials
: A témakör összes fontos részletét leíró könyv. Silvia Hagen: *IPv6 Essentials* (ISBN 0-596-00125-8).

20.3 Névmegfeleltetés

A DNS segít hozzárendelni egy IP-címet egy vagy több névhez, illetve hozzárendelni egy nevet egy IP-címhez. Linux alatt ezt az átalakítást általában egy speciális szoftver, a bind végzi. Azt a gépet, amelyik ezt az átalakítást végzi *névkiszolgálónak* (name server) nevezzük. A nevek hierarchikus rendszert alkotnak, és a név egyes elemei pontokkal vannak elválasztva. A névhierarchia egyébként teljesen független a fentebb leírt IP-cím hierarchiától.

Vizsgáljunk meg egy teljes nevet, legyen ez mondjuk a `jupiter.example.com`. A név a `gépnév.tartomány` formát követi. A teljes név, az úgynevezett *teljes képzésű név* ((fully qualified domain name, FQDN), egy gépnévből és egy tartományrészből áll (`example.com`). Ez utóbbinak része a *legfelső szintű tartomány* (top level domain) vagy TLD (`hu`).

A TLD-k meghatározása történelmi okok miatt meglehetősen zavarossá vált. Hagyományosan a hárombetűs tartományneveket az USA-ban használták. A világ többi részén a kétbetűs ISO nemzeti kód volt a szabvány. 2000 óta három betűnél hosszabb TLD-ket is létrehoztak, melyek a szakterületek szerinti felosztást célozzák meg (például: `.info`, `.name`, `.museum`).

Az internet korai időszakában (1990 előtt) az `/etc/hosts` fájlt használták az interneten elérhető gépek neveinek tárolására. Ez azonban hamar használhatatlannak bizonyult, mivel az internetet elérő gépek száma igen gyorsan nőtt. Éppen ezért egy decentralizált adatbázis készült a gépnevek széles körben elosztott tárolására. Ennek az adatbázisnak, hasonlóan a fentebb említett névkiszolgálóhoz, nem kell az interneten elérhető összes gépről adatokat tartalmaznia, hanem kéréssel fordulhat más névkiszolgálókhoz.

A hierarchia legfelső részén a *gyökér névkiszolgálók* (root name servers) találhatók. A legfelső szintű tartományokat ezek a gyökér névkiszolgálók kezelik, amelyeket a Network Information Center (NIC) nevű hálózati információs központ működtet. Minden gyökér névkiszolgáló ismeri az egyes legfelső szintű tartományokért felelős névkiszolgálókat. További információ a legfelső szintű NIC-ekről a `http://www.internic.net` címen található.

A DNS jóval többet tud az egyszerű névfeloldásnál. A névkiszolgáló azt is tudja, hogy melyik gép fogadja a teljes tartomány elektronikus leveleit – vagyis melyik a *levélcserélő* (mail exchanger, MX).

Ahhoz, hogy egy gép megfelelően fel tudjon oldani egy IP-címet, legalább egy névkiszolgáló IP-címét ismernie kell. Egy ilyen névkiszolgáló egyszerűen megadható a YaST segítségével. Modemes elérés esetén lehet, hogy egyáltalán nem kell kézzel beállítani névkiszolgálót. A betárcsázós (dial-up) protokollon keresztül a szolgáltató automatikusan biztosítja a névkiszolgáló címét a kapcsolat létrejöttekor. Az openSUSE névkiszolgálójának beállítását a „Kiszolgálónév és DNS beállítása” szakasz (306. oldal) rész írja le. A saját névkiszolgáló beállításának leírása: 22. fejezet - *A DNS (tartománynévrendszer, Domain Name System)* (343. oldal).

A `whois` protokoll szorosan kapcsolódik a DNS-hez. Ezzel a programmal gyorsan kikereshető, ki is felelős egy adott tartományért.

MEGJEGYZÉS: MDNS és .local tartománynevek

A `.local` legfelső szintű tartománynevet a feloldó link-local (adatkapcsolati szinten helyi) tartománynak tekinti. A DNS-kérések a normál DNS-kérések helyett multicast DNS-kérésekként lesznek elküldve. Ha már használja a `.local` tartományt a névkiszolgáló konfigurációjában, akkor ezt a beállítást ki kell kapcsolni az `/etc/host.conf` fájlban. Olvassa továbbá el a `host.conf` kézikönyvoldalt is.

Ha ki akarja kapcsolni az MDNS funkciót telepítés közben, akkor használja a `nomdns=1` rendszerindítási paramétert.

További információ a multicast DNS-ről: `http://www.multicastdns.org`.

20.4 Hálózati kapcsolat beállítása a YaST segítségével

A Linux számos hálózatkezelési típust támogat. Ezek többsége eltérő eszközneveket használ, és a konfigurációs fájlok a fájlrendszer különféle helyein elszórva találhatók. A manuális hálózati beállítás részletes áttekintését lásd: 20.6. - Hálózati kapcsolat kézi beállítása (318. oldal).

Noteszgépen telepítéskor, amelyen a NetworkManager alapértelmezés szerint bekapcsolódik, a YaST beállítja az összes észlelt csatolót. Más gépeken csak az első aktív csatoló (amelyikbe van dugva hálózati kábel) lesz automatikusan beállítva. A telepített rendszeren bármikor beállítható további hardver. A következő részek az openSUSE által támogatott hálózati kapcsolatok hálózati beállítását írják le.

20.4.1 Hálózati kártya beállítása a YaST segítségével

A vezetékes vagy vezetéknélküli hálózati kártya beállításához válassza ki a YaST *Hálózati eszközök* > *Hálózati beállítások* menüpontját. A modul elindítása után a YaST megjeleníti a *Hálózati beállítások* párbeszédablakot, amelynek négy lapja van: *Általános beállítások*, *Áttekintés*, *Gépnév/DNS* és *Útválasztás*.

Az *Általános beállítások* lapon az általános hálózati beállítások láthatók, például a NetworkManager használatának engedélyezése, az IPv6 és az általános DHCP-beállítások. További információkért lásd: „Az általános hálózati beállítások megadása ” szakasz (298. oldal).

Az *Áttekintés* lap a telepített hálózati kártyákról nyújt információt. A folyamat során megfelelően felismert kártyák a nevükkel együtt jelennek meg itt. Ebben a párbeszédablakban állíthat be egy új hálózati kártyát vagy módosíthat egy meglévő konfigurációt. Az automatikusan fel nem ismert hálózati kártyák beállításának leírása: „Nem felderített hálózati kártya beállítása” szakasz (305. oldal). Egy már beállított kártya konfigurációjának módosítása: „Hálózati kártya beállításának módosítása” szakasz (299. oldal).

A *Gépnév/DNS* lapon lehet beállítani a gép gépnevét és elnevezni a használandó kiszolgálókat. További információkért lásd: „Kiszolgálónév és DNS beállítása” szakasz (306. oldal).

Az *Útválasztás* lapon lehet beállítani az útválasztást. További információkért lásd: „Útválasztás beállítása” szakasz (307. oldal).

20.3. ábra *Hálózati beállítások*

Az általános hálózati beállítások megadása

A YaST *Hálózati beállítások* modul *Általános beállítások* lapján adhatók meg a legfontosabb általános hálózati beállítások, például a NetworkManager használatának engedélyezése, az IPv6- és a DHCP-kliensbeállítások. Ezek a beállítások az összes hálózati csatolóra egyformán vonatkoznak.

A *Hálózatbeállítási módszer* részben válassza ki, hogyan történjen a hálózati kapcsolatok kezelése. Ha azt szeretné, hogy egy NetworkManager asztali kisalkalmazás felügyelje az összes csatoló kapcsolatát, válassza ki a *Felhasználó által vezérelt, NetworkManagerrel* lehetőséget. Ez a beállítás igen alkalmas többféle vezetékes és vezetéknélküli hálózat közötti kapcsolgatásra. Ha nem használ asztali környezetet (GNOME-ot vagy KDE-t),

vagy a számítógép egy Xen-kiszolgáló, virtuális rendszer, vagy hálózati szolgáltatásokat biztosít (például DHCP vagy DNS), akkor válassza a *Hagyományos módszer (ifup)* lehetőséget. A NetworkManager-rel kapcsolatos további tudnivalók: 10. fejezet - *Using NetworkManager* (↑*Start-Up*).

Az *IPv6 protokoll beállítása* részben adja meg, hogy kívánja-e használni az IPv6 protokollt. Nincs akadálya együtt használni az IPv6 és IPv4 protokollokat. Alapértelmezés szerint az IPv6 be van kapcsolva. Olyan hálózatokon azonban, amelyeken nem használják az IPv6 protokollt, a válaszidők jobbak lehetnek, ha az IPv6 protokoll le van tiltva. Az IPv6 letiltásához törölje az *IPv6 engedélyezése* beállítás megjelölését. Ennek hatására nem töltődik be automatikusan az IPv6 kernelmodulja. A módosítások újraindítás után lépnek életbe.

A *DHCP-kliens beállítások* részben adhatók meg a DHCP-kliens beállításai. Ha azt szeretné, hogy a DHCP-kliens azt kérje a kiszolgálótól, hogy mindig nyilvános üzenetekben küldje a válaszait, jelölje meg a *Nyilvános (broadcast) válasz igénylése* pontot. Erre szükség lehet, ha a gép gyakran mozog különböző hálózatok között. A *DHCP-kliensazonosító* egy adott hálózat minden egyes DHCP-kliensén eltérő kell, hogy legyen. Ha üresen hagyja, akkor alapértelmezés szerint a hálózati csatoló hardvercíme lesz. Ha azonban több virtuális gépet futtat ugyanazon a hálózati csatolón, vagyis ugyanazon a hardvercímen, akkor itt meg kell adni egyedi neveket.

A *Küldendő gépnév* a dhcpcd által a DHCP-kiszolgálónak küldött üzenetekben, a gépnév paramétermezőben használandó karaktersorozatot adja meg. Egyes DHCP-kiszolgálók frissítik a névkiszolgáló zónáit (a normál és fordított bejegyzéseket) e név alapján (dinamikus DNS). Ezenfelül néhány DHCP-kiszolgáló elvárja, hogy a kliensektől érkező DHCP-üzenetek *Küldendő gépnév* paramétermezője egy meghatározott karaktersorozatot tartalmazzon. Hagyja `AUTO` értéken az aktuális (az `/etc/HOSTNAME` részben definiált) gépnév elküldéséhez. Amennyiben a paramétermezőt üresen hagyja, a kliens semmilyen gépnevet nem küld. Ha nem kívánja módosítani az alapértelmezett útvonalat a DHCP-től érkező információ alapján, akkor törölje az *Alapértelmezett útvonal megváltoztatása DHCP-n keresztül* pontot.

Hálózati kártya beállításának módosítása

Egy hálózati kártya beállításának módosításához válassza ki a kártyát a YaST *Hálózati beállítások* > *Áttekintés* lapján, majd kattintson a *Szerkesztés* gombra. Megjelenik a *Hálózati címek beállítása* párbeszédablak, amelynek *Általános*, *Cím* és *Hardver* lapjain

megadhatja a kártya beállításait. A vezetéknélküli kártya beállításával kapcsolatos információ: 30.1.2. - Beállítás a YaST segítségével (507. oldal).

IP-címek beállítása

A hálózati kártya IP-címét, illetve az IP-cím meghatározásának módját a *Hálózati kártya beállítása* párbeszédablak *Cím* lapján lehet beállítani. IPv4- és IPv6-címek egyaránt használhatók. A hálózati kártyához a *Nincs IP-cím* érték (ami az eszközök nyalábolásakor hasznos), *Statikusan hozzárendelt IP-címek* (IPv4 vagy IPv6), illetve a *DHCP* és/vagy *Zeroconf* segítségével kiosztott *Dinamikus címek* állíthatók be.

Dinamikus címek használata esetén adja meg, hogy *csak DHCP 4*-et kíván használni (IPv4 esetén), *csak DHCP 6*-ot (IPv6 esetén), vagy *DHCP 4-es és 6-os verzió*-t.

Ha lehetséges, akkor a telepítéskor működő kapcsolattal rendelkező első hálózati kártya automatikusan DHCP-n keresztüli automatikus címhozzárendelésre lesz beállítva. Noteszgépek esetén, ahol a NetworkManager alapértelmezés szerint aktív, az összes hálózati kártya be lesz állítva.

Szintén DHCP-t kell használni, ha DSL-kapcsolattal rendelkezik, de az ISP (internetszolgáltató) nem adott statikus IP-címet. Ha a DHCP használata mellett döntött, akkor állítsa be a részleteket a YaST hálózatikártya-konfigurációs moduljában, a *Hálózati beállítások* párbeszédablak *Általános beállítások* lapján, a *DHCP-kliens beállítások* részben. A *Nyilvános (broadcast) válasz igénylése* részben adja meg, hogy a DHCP-kliens mindig nyilvános (broadcast) üzenetekben kérje-e a kiszolgálótól a válaszokat. Erre a hálózatokat gyakran váltó, mobil gépek esetében lehet szükség. Ha virtuális gépeket működtet, ahol a különböző gépek ugyanazon a csatolón keresztül kommunikálnak, akkor a megkülönböztetésükhöz szükség van egy *DHCP-kliensazonosítóra*.

A DHCP jó választás a kliensek konfigurációja során, de kiszolgálók beállítása esetén nem ideális megoldás. Statikus IP-cím beállítása:

1. Válasszon ki egy kártyát a YaST hálózati kártya beállítására szolgáló moduljának *Áttekintés* lapján a felderített kártyák listájában, majd kattintson a *Szerkesztés* gombra.

2. A *Cím* lapon válassza ki a *Statikusan hozzárendelt IP-címek* pontot.

3 Írja be az *IP-cím* értékét. IPv4- és IPv6-címek egyaránt használhatók. Az *Alhálózati maszk* mezőbe írja be a hálózati maszk értékét. Ha IPv6-címet használ, akkor az *Alhálózati maszk*-ot `/64` formátumban adja meg.

   Beírhat egy teljesen megadott *Gépnevet* is a címhez, amely be fog íródni az `/etc/hosts` konfigurációs fájlba.

4 Kattintson a *Tovább* gombra.

5 A beállítás aktiválásához kattintson a *Befejezés* gombra.

Statikus cím használata esetén névkiszolgálók és az alapértelmezett átjáró nem lesz automatikusan beállítva. A névkiszolgálók beállításához kövesse az „Kiszolgálónév és DNS beállítása” szakasz (306. oldal) részben leírtakat. Egy átjáró beállításához kövesse a „Útválasztás beállítása” szakasz (307. oldal) részben leírtakat.

Aliasok beállítása

Ha nem használja a NetworkManagert, akkor egy hálózati eszköznek egynél több IP-címe (úgynevezett aliasa, másodlagos címe) is lehet. Hálózati kártya alias beállítása:

1 Válasszon ki egy kártyát a YaST hálózati kártya beállítására szolgáló moduljának *Áttekintés* lapján a felderített kártyák listájában, majd kattintson a *Szerkesztés* gombra.

2 A *Cím* > *További címek* lapon kattintson a *Hozzáadás* gombra.

3 Adjon meg egy *Álnevet*, egy *IP-címet* majd a *Hálózati maszkot*. Az alias nevébe ne írja be a csatoló nevét.

4 Kattintson az *OK* gombra.

5 Kattintson a *Tovább* gombra.

6 A beállítás aktiválásához kattintson az *OK* gombra.

Az eszköznév és az udev-szabályok módosítása

Ha szükséges, a hálózati kártya eszközneve megváltoztatható. Szintén beállítható, hogy a hálózati kártyát felismerje-e az udev a hardvercím (MAC-cím) vagy a buszazonosító

alapján. Ez utóbbi beállítás nagy kiszolgálókban előnyös, ahol leegyszerűsíti a kártyák üzem közbeni cseréjét. Ezek a paraméterek YaST segítségével a következőképp állíthatók be:

1. Válasszon ki egy kártyát a YaST *Hálózati beállítások* moduljának *Áttekintés* lapján a felderített kártyák listájában, majd kattintson a *Szerkesztés* gombra.

2. Lépjen át a *Hardver* lapra. Az aktuális eszköznév az *Udev szabályok* részben látható. Kattintson a *Módosítás* gombra.

3. Válassza ki, hogy az udev a kártyát *MAC-cím* vagy *Buszazonosító* alapján azonosítsa. Az aktuális MAC-cím és buszazonosító a párbeszédablakban látható.

4. Az eszköz nevének megváltoztatásához jelölje meg az *Eszköznév megváltoztatása* pontot és írja át a nevet.

5. Kattintson az *OK*, majd a *Tovább* gombra.

6. A beállítás aktiválásához kattintson a *Befejezés* gombra.

Hálózatikártya-kernelmodul megváltoztatása

Egyes hálózati kártyákhoz többféle kernelmodul (illesztőprogram) is használható. Ha a kártyát már beállította a YaST-tal, akkor a rendelkezésre álló, alkalmas modulok közül egy listából választhatja ki a kívánt kernelmodult. A kernelmodulhoz paraméterek is megadhatók. Ezek a paraméterek YaST segítségével a következőképp állíthatók be:

1. Válasszon ki egy kártyát a YaST Hálózati beállítások moduljának *Áttekintés* lapján a felderített kártyák listájában, majd kattintson a *Szerkesztés* gombra.

2. Lépjen át a *Hardver* lapra.

3. A *Modulnév* mezőben válassza ki a használni kívánt kernelmodult. A *Paraméterek* mezőben adja meg a kijelölt modul paramétereit, `paraméter=érték` formátumban. Ha több paramétert kell megadni, szóközökkel válassza el őket.

4. Kattintson az *OK*, majd a *Tovább* gombra.

5. A beállítás aktiválásához kattintson a *Befejezés* gombra.

Hálózati eszköz aktiválása

A hagyományos ifup módszer használata esetén az eszköz beállítható, hogy rendszerindításkor, kábelcsatlakoztatáskor, a kártya felderítésekor vagy sose induljon el, illetve manuálisan legyen indítható. Az eszközindítás módosításához tegye a következőket:

1. A YaST-ban válassza ki a kártyát a felderített kártyák listájából a *Hálózati eszközök* > *Hálózati beállítások* részben, majd kattintson a *Szerkesztés* gombra.

2. Az *Általános* lap *Eszköz aktiválása* menüpontjában válassza ki a kívánt bejegyzést.

   Ha rendszerindításkor kívánja elindítani az eszközt, akkor jelölje meg a *Rendszerindításkor* pontot. Ha a csatoló figyelje a fizikai kapcsolatot, akkor használja a *Kábeles kapcsolat esetén* lehetőséget. Az *Üzem közbeni csatlakoztatáskor* pont megjelölése esetén a csatoló a lehető leghamarabb aktiválódik. Ez hasonlít a *Rendszerindításkor* beállításhoz, az egyetlen tényleges különbség annyi, hogy nem jelez hibát, ha a csatoló rendszerindításkor még nincs jelen. A *Kézzel* beállítás esetén Ön vezérelheti kézzel a csatolót, az `ifup` vagy a KInternet segítségével. A *Soha* beállítás kiválasztása esetén az eszköz egyáltalán nem fog elindulni. Az *NFSroot használatakor* beállítás is hasonló, mint a *Rendszerindításkor*, de a csatoló nem áll le az `rcnetwork stop` parancs hatására. Akkor használja ezt, ha NFS vagy iSCSI gyökér fájlrendszert használ.

3. Kattintson a *Tovább* gombra.

4. A beállítás aktiválásához kattintson a *Befejezés* gombra.

Általában a hálózati csatolók aktiválására és deaktiválására csak a rendszergazda jogosult. Ha azt akarja, hogy a felhasználók is tudják aktiválni a csatolót a KInterneten keresztül, akkor jelölje meg a *Felhasználó által, KInterneten keresztül vezérelt* pontot.

Maximális átviteli egység beállítása

A csatolóhoz beállítható a maximális átviteli egység (maximum transmission unit, MTU). Az MTU a legnagyobb csomagméretet jelöli, bájtokban megadva. A nagyobb MTU a sávszélesség jobb kihasználását eredményezi. A nagyon nagy csomagok azonban eltömhetik egy időre a lassabb csatolókat, így megnövelik a többi csomag késését.

1. A YaST-ban válassza ki a kártyát a felderített kártyák listájából a *Hálózati eszközök* > *Hálózati beállítások* részben, majd kattintson a *Szerkesztés* gombra.

2 Az *Általános* lapon válassza ki a kívánt pontot az *MTU beállítása* listából.

3 Kattintson a *Tovább* gombra.

4 A beállítás aktiválásához kattintson a *Befejezés* gombra.

Tűzfal beállítása

Anélkül, hogy meg kellene adni a részletes tűzfalbeállítást a 33.4.1. - Tűzfal beállítása a YaST segítségével (537. oldal) részben leírt módon, az eszközbeállítás részeként meghatározhatja az eszköz alapvető tűzfalbeállítását. A következő műveleteket hajtsa végre:

1 Nyissa meg a YaST *Hálózati eszközök* > *Hálózati beállítások* modulját. Az *Áttekintés* lapon válasszon ki egy kártyát a felderített kártyák listájából, majd kattintson a *Szerkesztés* gombra.

2 Lépjen a *Hálózati beállítások* párbeszédablak *Általános* lapjára.

3 Határozza meg a tűzfalzónát, amelyhez a csatolót hozzá kell rendelni. A következő lehetőségek használhatók:

Tűzfal kikapcsolva
: Ez a beállítás csak akkor látható, ha a tűzfal ki van kapcsolva és egyáltalán nem is fut. Csak akkor használja ezt a beállítást, ha a gép egy nagyobb, külső tűzfallal védett hálózat része.

Automatikus zónakiosztás
: Ez a beállítás csak akkor látható, ha a tűzfal be van kapcsolva. A tűzfal fut és a csatoló automatikusan hozzárendelődik egy tűzfalzónához. Az ilyen csatolókhoz az `any` kulcsszóval megjelölt, illetve a külső zóna lesz hozzárendelve.

Belső zóna (Védtelen)
: A tűzfal fut, de nem kényszerít ki semmilyen szabályt a csatoló védelme érdekében. Akkor használja ezt a beállítást, ha a gép egy nagyobb, külső tűzfallal védett hálózat része. Akkor is hasznos, ha a gépben több hálózati csatoló található és a csatolók a belső hálózathoz csatlakoznak.

Demilitarizált zóna
: A demilitarizált zóna egy további védelmi vonal a belső hálózat és a (rosszindulatú) internet előtt. A zónához rendelt gépek a belső hálózatról és az internetről is elérhetők, de a belső hálózat nem érhető el.

Külső zóna
: A tűzfal fut a csatolón, és teljesen védi azt más – feltételezhetően rosszindulatú – hálózati forgalom ellen. Ez az alapértelmezett beállítás.

4 Kattintson a *Tovább* gombra.

5 Aktiválja a konfigurációt az *OK* gombra kattintással.

Nem felderített hálózati kártya beállítása

Lehet, hogy a kártyát nem sikerül helyesen felismerni. Ebben az esetben a kártya nem kerül bele a felderített kártyák listájába. Ha biztos benne, hogy a rendszer tartalmazza a kártya illesztőprogramját, akkor beállíthatja a kártyát kézzel. Nem felderített hálózati kártya beállításához tegye a következőket:

1 A YaST *Hálózati eszközök* > *Hálózati beállítások* > *Áttekintés* párbeszédablakában kattintson a *Hozzáadás* gombra.

2 A *Hardver* párbeszédablakban válassza ki a csatoló *Eszköztípusát* a lehetőségek közül, és adja meg a *Konfiguráció nevét*. Ha a hálózati kártya PCMCIA- vagy USB-eszköz, akkor jelölje meg a megfelelő négyzetet és lépjen ki a párbeszédablakból a *Tovább* gombra kattintással. Ellenkező esetben megadhatja a kártyához használandó kernelmodul *Modulnevét*, illetve ha szükséges, annak *Paramétereit*.

3 Kattintson a *Tovább* gombra.

4 Állítsa be a szükséges paramétereket, például az IP-címet, az eszköz aktiválását, illetve a csatolóhoz rendelt tűzfalzónát az *Általános*, *Cím* és *Hardver* lapokon. További információ a beállításokról: „Hálózati kártya beállításának módosítása” szakasz (299. oldal).

5 Ha a csatoló választott eszköztípusa *Vezetéknélküli*, akkor a következő párbeszédablakban állítsa be a vezetéknélküli kapcsolatot.

6 Kattintson a *Tovább* gombra.

7 Az új hálózati beállítás aktiválásához kattintson az *OK* gombra.

Kiszolgálónév és DNS beállítása

Ha nem módosította a telepítés során a hálózati beállítást és a vezetékes hálózati kártya már elérhető volt, akkor a gépnév automatikusan be lett állítva a számítógépen és a DHCP aktiválva lett. Ugyanez érvényes a névszolgáltatásra, amelyekre a gépnek szüksége van, hogy be tudjon illeszkedni a hálózati környezetbe. Ha DHCP-t használ a hálózati cím beállításához, akkor a tartománynév-kiszolgálók listáját a rendszer automatikusan kitölti a megfelelő adatokkal. Ha a statikus beállítást részesíti előnyben, akkor állítsa be ezeket az értékeket kézzel.

A számítógép nevének módosítása és a névkiszolgáló keresési listájának beállítása:

1 Menjen a YaST *Hálózati beállítások* > *Gépnév/DNS* lapjára a *Hálózati eszközök* modulban.

2 Adja meg a *Gépnév* és ha szükséges, a *Tartománynév* értékét. A tartománynév különösen fontos, ha a gép levelezési kiszolgálóként működik. Ne feledje, hogy a gépnév globális beállítás, és az összes beállított hálózati csatolóra érvényes lesz.

   Ha DHCP-vel kér IP-címet, akkor a számítógép gépnevét a DHCP automatikusan beállítja. Ezt a fajta működést szükséges lehet letiltani, ha többféle hálózathoz csatlakozik, mert azok más-más gépneveket rendelhetnek a számítógéphez, és a grafikus asztali környezetet megzavarhatja, ha menet közben megváltozik a gépnév. A DHCP-s gépnévkérés letiltásához törölje a *Gépnév módosítása DHCP-n keresztül* pontot.

   Ha DHCP-vel kér IP-címet, akkor a gépnév alapértelmezés szerint beíródik az `/etc/hosts` fájlba és a `127.0.0.2` IP-címre fog feloldódni. Ennek letiltásához törölje a *Gépnév bejegyzése az /etc/hosts fájlba* beállítást, de ne feledje, hogy a gépnév aktív hálózat nélkül nem lesz feloldható.

3 A *DNS-beállítások módosítása* részben válassza ki a DNS-beállítások módosításának módját (névkiszolgálók, keresési lista, az `/etc/resolv.conf` fájl tartalma).

   Az *Alapértelmezett irányelv használata* beállítás megjelölése esetén a konfigurációt a `netconfig` parancsfájl fogja kezelni, amely a statikusan (a YaST-ban

vagy a konfigurációs fájlokban) megadott adatokat egyesíti a dinamikusan (a DHCP-kliens vagy a NetworkManager által) beállított adatokkal. Az alapértelmezett irányelv a legtöbb esetben megfelelő.

A *Csak kézzel* paraméter megjelölése esetén a `netconfig` nem módosíthatja az `/etc/resolv.conf` fájl tartalmát. A fájl kézzel természetesen szerkeszthető.

Az *Egyedi irányelv* pont megjelölése esetén meg kell adni az összefésülést szabályozó *Egyedi irányelvszabályok* karaktersorozatot. Ez a karaktersorozat az érvényes beállítási forrásnak számító csatolónevek vesszővel elválasztott listáját tartalmazza. A teljes csatolónevek mellett egyszerű helyettesítő karakterek is használhatók, több csatoló megjelölésére. Például az `eth* ppp?` elsőként az összes eth-csatolót tekinti célnak, majd utána a ppp0-ppp9 csatolókat. Két speciális irányelvérték jelöli, hogyan legyenek alkalmazva az `/etc/sysconfig/network/config` fájlban megadott statikus beállítások:

`STATIC`
: A statikus beállításokat össze kell fésülni a dinamikus beállításokkal.

`STATIC_FALLBACK`
: A statikus beállításokat akkor kell használni, ha nincsenek dinamikus beállítások.

További információ: `man 8 netconfig`.

4. Adja meg a *Névkiszolgálók* értékeit, majd töltse ki a *Tartomány keresése* listát. A névkiszolgálókat kötelező IP-címmel megadni (például 192.168.1.116), nem pedig gépnevekkel. A *Tartomány keresése* lapon megadott nevek a tartománynév nélkül megadott gépnevek feloldására használt tartománynevek. Ha a *Tartomány keresése* részben egynél több tartománynevet akar megadni, akkor válassza el őket vesszőkkel vagy szóközszerű karakterekkel.

5. A beállítás aktiválásához kattintson a *Befejezés* gombra.

Útválasztás beállítása

Ahhoz, hogy a gép kommunikálni tudjon más gépekkel és más hálózatokkal, útválasztási adatokat kell megadni, hogy a hálózati forgalom a megfelelő útvonalon haladjon.

DHCP használata esetén ezeket az adatokat a gép automatikusan megkapja. Statikus beállítás esetén ezeket az adatokat kézzel kell megadni.

1. A YaST-ban lépjen be a *Hálózati beállítások* > *Útválasztás* részbe.

2. Adja meg az *Alapértelmezett átjáró* IP-címét. Az alapértelmezett átjáró minden lehetséges célnak megfelel, de ha van más bejegyzés, amely megfelel az adott címnek, akkor azt használja az alapértelmezett útvonal helyett.

3. További bejegyzéseket az *Útválasztó tábla* részben lehet megadni. Adja meg a *Cél* hálózat IP-címét, az *Átjáró* IP-címét és a *Hálózati maszk* értékét. Válassza ki az *Eszközt*, amelyen keresztül az adott hálózatra a forgalom áthalad (a mínusz jel jelentése a minden eszköz). Az értékek kihagyásához használjon mínusz jelet –. Egy alapértelmezett átjáró felvételéhez adja meg a `default` értéket a *Cél* mezőben.

   MEGJEGYZÉS

   Ha egynél több alapértelmezett útvonalat ad meg, akkor lehetséges a metric paraméterrel prioritást adni az egyes utaknak. A metric paraméter megadásához a *Paraméterek* részben írja be, hogy `– metric` *`szám`*. A legmagasabb értékű útvonal lesz az alapértelmezett. Ha a hálózati eszközt lekapcsolják, akkor az útvonal törlődik és a rendszer a következő útvonalat fogja használni. A jelenlegi kernel azonban nem tudja a metric paramétert használni statikus útválasztás esetén. Erre csak az útválasztó démonok, például a multipathd képes.

4. Ha a rendszer útválasztó, akkor kapcsolja be az *IP továbbítás* lehetőséget a *Hálózati beállítások* ablakban.

5. A beállítás aktiválásához kattintson a *Befejezés* gombra.

20.4.2 Modem

A modem beállítása a YaST vezérlőközpont *Hálózati eszközök* > *Modem* részében érhető el. Ha a modem felismerése nem sikerült automatikusan, akkor nyissa meg a kézi beállításra szolgáló párbeszédablakot a *Hozzáadása* menüpontra kattintással. A csatolót, amelyhez a modem csatlakozik, a *Modemeszközök* részben lehet megadni.

TIPP: CDMA- és GPRS-modemek

A támogatott CDMA- és GPRS-modemek ugyanúgy a YaST *Modem* moduljával állíthatók be, mint a normál modemek.

20.4. ábra *Modembeállítások*

Alközpont (private branch exchange, PBX) használata esetén egy tárcsázási előtag megadására is szükség lehet. Ez gyakran egy nulla. Ezt az alközpont leírásából, vagy a megfelelő szabályzatból tudhatja meg. Azt is válassza ki, hogy hangfrekvenciás vagy hagyományos (megszakításos) tárcsázást kíván használni, illetve hogy a modem várjon-e tárcsahangra. Ha a modem alközponthoz csatlakozik, akkor az utóbbi beállítást nem szabad bekapcsolni.

A *Részletek* alatt állítsa be a baudsebességet és a modem inicializáló karaktersorozatait. Csak akkor változtassa meg ezeket a beállításokat, ha a modem nem került automatikusan felismerésre vagy ha speciális beállításokat igényel ahhoz, hogy az adatátvitel működjön. ISDN terminéladapterek esetén általában ez a helyzet. Az *OK* gombra kattintva lépjen ki a párbeszédablakból. Ha a modem vezérlését a root jogosultságok nélküli, normál felhasználók számára is engedélyezni kívánja, jelölje meg a *Felhasználó által, KInternéten keresztül vezérelt* pontot. Ily módon az adminisztrátori jogosultsággal nem rendelkező felhasználó is aktiválhat vagy letilthat egy csatolót. A *Tárcsázási előtag reguláris kifejezés* részben adjon meg egy reguláris kifejezést. A KInternetnek a felhasználó által módosítható *Elővválasztó* értéke meg kell, hogy feleljen ennek a reguláris kifejezés-

nek. Ha a mező üres marad, akkor a felhasználó adminisztrátori jogosultságok nélkül nem tud beállítani másik *Előválasztó* értéket.

A következő párbeszédablakban válassza ki az ISP-t (internetszolgáltatót). Ha az országban működő ISP-k előre meghatározott listájából kíván választani, akkor válassza ki az *Ország* menüpontot. Másik lehetőség, ha az *Új* elemre kattintással megnyit egy párbeszédablakot, amelyben megadhatók az ISP adatai. Ez a behívó kapcsolat és az ISP nevének, valamint az ISP által biztosított bejelentkezési név és jelszó megadását jelenti. Engedélyezze a *Mindig kérdezzen rá a jelszóra* lehetőséget, ha azt szeretné, hogy a jelszót minden csatlakozáskor meg kelljen adni.

Az utolsó párbeszédablakban további kapcsolati beállításokat adhat meg:

Automatikus kapcsolódás
: Ha engedélyezi az *automatikus kapcsolódást*, akkor adjon meg legalább egy névkiszolgálót. Ezt a funkciót csak akkor használja, ha az internetkapcsolat olcsó, mivel vannak programok, amelyek rendszeres időközönként kérnek adatokat az internetről.

DNS módosítása kapcsolódáskor
: Ez a négyzet alapértelmezés szerint be van jelölve, amelynek hatására a névkiszolgáló címe az internetre csatlakozáskor mindig frissítésre kerül.

DNS automatikus lekérése
: Ha a szolgáltató csatlakozás után nem küldi el a tartomány névkiszolgálóját, akkor tiltsa le ezt a beállítást és adja meg kézzel a DNS-re vonatkozó adatokat.

Automatikus újracsatlakozás
: Ha ez a paraméter meg van adva, akkor a kapcsolat megszakadás után automatikusan helyre lesz állítva.

Prompt letiltása
: Ez a beállítás letiltja a telefonos kiszolgáló üzeneteinek felismerését. Ha a kapcsolat nagyon lassan, vagy egyáltalán nem épül fel, próbálkozzon meg ezzel a beállítással.

Külső tűzfalcsatoló
: A beállítást megjelölve engedélyezésre kerül a tűzfal, amely a csatolót külsőként állítja be. Ezáltal a rendszer az internetkapcsolat fennállása alatt védve van a külső támadások ellen.

Tétlenségi időkorlát(másodperc)
: Ezzel a beállítással lehet megadni egy hálózati tétlenségi időkorlátot, amely után a modem automatikusan megszakítja a kapcsolatot.

IP részletek
: Megnyitja a címbeállító párbeszédablakot. Ha az ISP nem rendel dinamikus IP-címet a géphez, akkor tiltsa le a *Dinamikus IP-cím* lehetőséget, majd adja meg a gép helyi és távoli IP-címét. Ezt az információt az internet-szolgáltatótól kérje. Hagyja az *Alapértelmezett útvonal* lehetőséget megjelölve, majd az *OK* gomb megnyomásával zárja be a párbeszédablakot.

A *Következő* gomb visszavisz az eredeti párbeszédablakhoz, amely a modembeállítás összefoglalását jeleníti meg. A *Kész* gomb segítségével zárja be a párbeszédablakot.

20.4.3 ISDN

A modul segítségével állíthat be a rendszerhez egy vagy több ISDN-kártyát. Ha a YaST nem ismeri fel az ISDN-kártyát, akkor kattintson az *ISDN-eszközök* lapon a *Hozzáadás* gombra és válassza ki kézzel a kártyát. Több csatoló is használható, de sok ISP csak egy csatolóhoz állítható be. A következő párbeszédablakokban adja meg a kártya megfelelő működéséhez szükséges ISDN-beállításokat.

20.5. ábra *ISDN beállítása*

A következő párbeszédablakban (20.5. ábra - ISDN beállítása (311. oldal)) válassza ki a használni kívánt protokollt. Az alapértelmezett az *Euro-ISDN (EDSS1)*, de régebbi és nagyobb alközpontok esetében az *1TR6* menüpontot kell kiválasztani. Az Egyesült Államokban az *NI1* elem a megfelelő. A megfelelő mezőben válassza ki az országot. Ezután a mellette levő mezőben megjelenik a megfelelő országkód. Végül adja meg a *Körzetszám* és az *Előtag* értékét (ha szükséges). Ha nem akarja naplózni a teljes ISDN-forgalmat, akkor törölje az *ISDN-napló indítása* pontot.

Az *Eszköz aktiválása* határozza meg, hogyan kell az ISDN-csatolót elindítani: a *Rendszerindításkor* hatására az ISDN-illesztőprogram minden rendszerindításkor inicializálásra kerül. *Kézzel* mód esetén az ISDN-illesztőprogramot `root` felhasználóként kell betölteni az `rcisdn start` parancs segítségével. A PCMCIA- vagy USB-eszközökhöz használt *Hotplug* az eszköz csatlakoztatása után tölti be az illesztőprogramot. Ha minden beállítást megadott, nyomja meg az *OK* gombot.

A következő párbeszédablakban adja meg az ISDN-kártya csatolótípusát és adja hozzá az ISP-ket egy meglévő csatolóhoz. A csatolók `SyncPPP` vagy `RawIP` típusúak lehetnek, de a legtöbb ISP `SyncPPP` módban működik, úgyhogy ennek leírása következik most.

20.6. ábra *ISDN csatoló beállítása*

A *Saját telefonszám* az adott beállítástól függ:

Közvetlenül a telefonkimenethez csatlakoztatott ISDN-kártya
: A szabványos ISDN-vonal három telefonszámot (többszörös előfizetői szám vagy MSN) biztosít. Ha az előfizető többet kér, akkor maximum tíz adható neki. Itt az egyik MSN-t kell megadni, de körzetszám nélkül. Ha rossz számot ad meg, akkor a telefonszolgáltató automatikusan az ISDN-vonalhoz elsőként hozzárendelt MSN-hez lép vissza.

Telefon-alközponthoz csatlakoztatott ISDN-kártya
: A konfiguráció a telepített berendezéstől függően változhat:

1. Az otthoni használatra kialakított kisebb alközpontok általában Euro-ISDN (EDSS1) protokollt használnak a belső hívásokhoz. Ezek az alközpontok egy belső S0 busszal rendelkeznek és belső számokat használnak a hozzájuk csatlakoztatott berendezésekhez.

   Használja az egyik belső számot MSN-ként. Legalább az egyik alközpont MSN-jét tudni kell használni: azét, amelyiken engedélyezve lett a közvetlen külső tárcsázás. Ha nem működik, akkor próbálja meg a nullát. További információért tekintse meg az alközponthoz biztosított dokumentációt.

2. A vállalatok számára tervezett nagyobb alközpontok általában az 1TR6 protokollt használják a belső hívásokhoz. Ezek MSN-jét EAZ-nek hívják és általában a közvetlenül hívható mellékkel egyeznek meg. Linux alatti beállítás esetén az EAZ utolsó számjegyének beírása elegendő kell, hogy legyen. Ha ez nem működik, érdemes végigpróbálni 1 és 9 közötti számokkal.

Annak érdekében, hogy a kapcsolat a következő fizetési egység előtt lebontásra kerüljön, jelölje meg a *Fizetendő egységek alapján* négyzetet. Ne feledje el, hogy ez nem minden internet-szolgáltatónál működik. A csatornakötegelés (multilink PPP) is engedélyezhető a megfelelő négyzet megjelölésével. Végül a *Külső tűzfalcsatoló* és a *Tűzfal újraindítása* kiválasztásával engedélyezheti a tűzfalat az adott kapcsolaton. Ha engedélyezni kívánja a normál, root jogosultság nélküli felhasználóknak is, hogy aktiválhassák vagy deaktiválhassák a csatolót, akkor jelölje meg a *Felhasználó által, KInterneten keresztül vezérelt* pontot.

A *Részletek* gomb megnyomására megnyílik egy párbeszédablak, amelyben még összetettebb kapcsolódási megoldásokat állíthat be, de ez a normál, otthoni felhasználók számára nem érdekes. Az *OK* gomb kiválasztásával lépjen ki a *Részletek* párbeszédablakból.

A következő párbeszédablakban adja meg az IP-címmel kapcsolatos beállításokat. Ha a szolgáltatótól nem kapott statikus IP-címet, akkor jelölje meg a *Dinamikus IP-cím* lehetőséget. Ellenkező esetben a mezőkbe írja be a gép helyi IP-címét és a távoli IP-címet az ISP által megadott adatok alapján. Ha ez a csatoló lesz az internet felé vezető alapértelmezett útvonal, akkor jelölje meg az *Alapértelmezett útvonal* lehetőséget. Minden gépen csak egy alapértelmezett útvonal lehet. A *Tovább* gomb kiválasztásával lépjen ki a párbeszédablakból.

A következő párbeszédablak segítségével állítsa be az országot és válasszon ki egy szolgáltatót. A listában csak a hívással választható (call-by-call) szolgáltatók láthatók. Ha a szolgáltató nem szerepel a listában, akkor nyomja meg az *Új* gombot. Erre megnyílik *A szolgáltató paraméterei* párbeszédablak, amelyben meg kell adni az ISP részletes adatait. A telefonszám megadásakor a számjegyek közé ne írjon szóközt vagy vesszőt. Végül az ISP által megadott módon írja be a bejelentkezési nevet és jelszót. Ha kész, nyomja meg a *Tovább* gombot.

Ha egy önálló munkaállomáson kapcsolja be az *Automatikus kapcsolódást*, akkor adja meg a névkiszolgálót (DNS-kiszolgálót). A legtöbb ISP támogatja a dinamikus DNS használatát, ami azt jelenti, hogy a névkiszolgáló IP-címét minden kapcsolódáskor az ISP küldi el. Egyetlen munkaállomás esetén azonban akkor is be kell írni egy helykitöltő címet, mint például `192.168.22.99`. Ha az ISP nem támogatja a dinamikus DNS-t, akkor adja meg kézzel az ISP névkiszolgálójának IP-címét. Ha igény van rá, a kapcsolathoz megadható egy időkorlát – ennyi (másodperc) hálózati inaktivitás után a kapcsolat automatikusan megszakad. Erősítse meg a beállításokat a *Tovább* gomb megnyomásával. A YaST megjeleníti a beállított csatolók összegzését. A beállítások aktiválásához nyomja meg a *Befejezés* gombot.

20.4.4 Kábelmodem

Néhány országban általános az internet kábeltévé-hálózaton keresztüli elérése. A kábeltévé-előfizető általában kap egy modemet, amely az egyik oldalon az antennakábelhez van csatlakoztatva, a másikon pedig egy számítógép hálózati kártyájához (egy 10BaseTG csavart érpárú kábellel). A kábelmodem ezután egy dedikált, fix IP-című internetkapcsolatot biztosít.

Az ISP által megadott utasításoktól függően a hálózati kártya beállításakor válassza ki a *Dinamikus címek* vagy *Statikusan hozzárendelt IP-címek* lehetőséget. Jelenleg a legtöbb szolgáltató DHCP-t használ. Egy statikus IP-cím gyakran egy speciális üzleti csomag része.

További információ a kábelmodemek beállításáról a Támogatási adatbázis megfelelő cikkében olvasható, amely online a http://en.opensuse.org/SDB:Setting_Up_an_Internet_Connection_via_Cable_Modem_with_SuSE_Linux_8.0_or_Higher címen érhető el.

20.4.5 DSL

A DSL-eszköz beállításához a YaST *Hálózati eszközök* szakaszban válassza ki a *DSL* modult. Ez a YaST modul több párbeszédablakból áll, amelyben a DSL-kapcsolat paraméterei adhatók meg az alábbi protokollok egyike alapján:

- PPP over Ethernet (PPPoE)
- PPP over ATM (PPPoATM)
- CAPI for ADSL (Fritz Cards)
- Point-to-Point Tunneling Protocol (PPTP) – Ausztria

A *DSL-beállítások áttekintése* párbeszédablak *DSL-eszközök* lapján látható a telepített DSL-eszközök listája. A DSL-eszköz beállításának módosításához válassza ki a listából az eszközt, majd kattintson a *Szerkesztés* gombra. Ha a *Hozzáadás* gombra kattint, akkor kézzel állíthat be egy új DSL-eszközt.

A PPPoE-re vagy PPTP-re épülő DSL-kapcsolat konfigurációjához a megfelelő hálózati kártyának már beállítottnak kell lennie. Ha ezt még nem tette meg, akkor állítsa be a kártyát a *Hálózati kártyák beállítása* részben leírtaknak megfelelően (lásd: 20.4.1. - Hálózati kártya beállítása a YaST segítségével (297. oldal)). DSL-kapcsolat esetén a címek automatikusan kioszthatók, de nem DHCP-n keresztül, éppen ezért a *Dinamikus címek* beállítás nem használható. Ehelyett a csatolóhoz adjon meg egy statikus helykitöltő címet, mint például a `192.168.22.1`. Az *Alhálózati maszk* mezőben adja meg a `255.255.255.0` értéket. Önálló munkállomás beállításakor hagyja az *Alapértelmezett átjáró* mezőt üresen.

TIPP

Az *IP-cím* és az *Alhálózati maszk* menüpontban lévő értékek csak helykitöltők. Ezek csak a hálózati kártya inicializálásához szükségesek és semmi közük a valódi DSL-kapcsolathoz.

A DSL-beállítás megkezdéséhez (20.7. ábra - DSL beállítása (316. oldal)) először válassza ki a *PPP módot* és az *Ethernet-kártyát*, amelyhez a DSL-modem csatlakozik (a legtöbb esetben ez az `eth0`). Az *Eszköz aktiválása* mezőben adja meg, hogy a DSL-kapcsolatot ki kell-e építeni a rendszerindítási folyamat során. Kattintson a *Felhasználó által, KInterneten keresztül vezérelt* pontra, ha engedélyezni kívánja a normál, root jogosultság nélküli felhasználóknak is, hogy aktiválhassák vagy deaktiválhassák a csatolót a KInternet segítségével.

A párbeszédablakban kiválaszthatja az országot, majd választhat az ott működő számos ISP közül. A DSL-konfiguráció következő párbeszédablakainak részletei az eddigi beállításoktól függenek, ezért csak röviden említjük a következő bekezdésekben. A beállítások részletes leírását a párbeszédablakokban rendelkezésre álló részletes súgó tartalmazza.

20.7. ábra *DSL beállítása*

Ha egy önálló munkaállomáson kapcsolja be az *Automatikus kapcsolódást*, akkor adja meg a névkiszolgálót (DNS-kiszolgálót). A legtöbb ISP támogatja a dinamikus DNS használatát, ami azt jelenti, hogy a névkiszolgáló IP-címét minden kapcsolódáskor az ISP küldi el. Egyetlen munkaállomás esetén azonban akkor is be kell írni egy helykitöltő

címet, például a `192.168.22.99`. Ha az ISP nem támogatja a dinamikus DNS-t, akkor adja meg kézzel az ISP névkiszolgálójának az IP-címét.

A *Tétlenségi időkorlát (másodperc)* azt az időt adja meg, amennyi hálózati tétlenség után a kapcsolat automatikusan megszakításra kerül. A célszerű időkorlát hatvan és háromszáz másodperc között van. Ha az *Automatikus kapcsolódás* le van tiltva, akkor az automatikus szétkapcsolás megakadályozása érdekében érdemes az időkorlátot nullára állítani.

A T-DSL konfigurációja nagyon hasonlít a DSL beállításához. Csak válassza ki a *T-Online*-t szolgáltatóként és a YaST megnyitja a T-DSL konfigurációs párbeszédablakot. Ebben a párbeszédablakban adja meg a T-DSL-hez szükséges további információt – a vonalazonosítót, a T-Online számát, a felhasználói kódot és a jelszót. Ezek a T-DSL-re előfizetés után megkapott adatok közt vannak.

20.5 NetworkManager

A NetworkManager ideális megoldás egy mobil munkaállomáshoz. A NetworkManager használata esetén nem kell törődni a hálózati csatolók újrakonfigurálásával: nyugodtan válthat a hálózatok között, ha más helyre megy. A NetworkManager képes automatikusan csatlakozni az ismert WLAN-hálózatokhoz. Ha két vagy több kapcsolat is lehetséges, akkor tud a gyorsabbikhoz csatlakozni.

A NetworkManager azonban nem tökéletes megoldás minden helyzetre, ezért továbbra is van lehetőség a választásra a hálózati kapcsolatok hagyományos kezelése (ifup) és a NetworkManager között. Ha a NetworkManager segítségével akarja kezelni a hálózati kapcsolatokat, akkor kapcsolja be a NetworkManagert a YaST Hálózati beállítások moduljában, az 10.2. - Enabling NetworkManager (10. fejezet - *Using NetworkManager*, ↑*Start-Up*) részben leírt módon. Példahelyzetek listája, valamint a NetworkManager beállításának és használatának részletes leírása: 10. fejezet - *Using NetworkManager* (↑*Start-Up*).

A hálózati kapcsolatok kezelésére szolgáló módszer kiválasztása után állítsa be a hálózati kártyát DHCP-n keresztüli automatikus konfigurációval vagy egy statikus IP-címmel, illetve állítsa be a modemet. A YaST-tal elvégezhető hálózati beállítások részletes leírása: 20.4. - Hálózati kapcsolat beállítása a YaST segítségével (297. oldal) és 30.1. - Vezetéknélküli LAN (503. oldal). A támogatott vezetéknélküli kártyák közvetlenül a NetworkManager-ben állíthatók be, a KDE vagy GNOME NetworkManager-kisalkalmazásainak segítségével.

Néhány különbség az ifup és a NetworkManager között:

`root` jogosultságok
: Ha a NetworkManagert használja a hálózat beállítására, akkor bármikor egyszerűen válthatja, állíthatja le és indíthatja el a hálózati kapcsolatokat, magából az asztali környezetből, egy kisalkalmazás segítségével. A NetworkManager lehetővé teszi a vezetéknélküli kapcsolatok közötti váltást, illetve ezek beállítását anélkül, hogy `root` jogosultságra lenne szükség. Éppen ezért a NetworkManager ideális megoldás egy mobil munkaállomáshoz.

  A hagyományos konfiguráció (ifup) is biztosít lehetőséget a kapcsolatok átváltására, elindítására és leállítására, a felhasználó közreműködésével vagy anélkül (ide tartoznak például a felhasználó által felügyelt eszközök), de a használatához mindig `root` jogosultság szükséges, ha módosítani kell egy hálózati eszközön vagy a beállításain. Ez gyakran jelent problémát pontosan a mobil számítástechnikában, hiszen előre lehetetlen az összes elképzelhető kapcsolatot beállítani.

A hálózati kapcsolatok típusai
: Mind a hagyományos konfiguráció, mind a NetworkManager képes kezelni a hálózati kapcsolatokat akár vezetéknélküli (WEP, WPA-PSK és WPA-Enterprise eléréssel), akár telefonos, akár vezetékes hálózatokon, DHCP használatával és statikus beállításokkal egyaránt. Támogatják a VPN-en keresztül történő csatlakozást is.

  A NetworkManager megpróbálja a számítógépet folyamatosan csatlakoztatva tartani, a lehető legjobb kapcsolat használatával. Ha van, akkor a leggyorsabb vezetékes kapcsolatot használja. Ha a vezetékes hálózati kapcsolat megszakad, akkor megpróbál újracsatlakozni. Képes kiválasztani vezetéknélküli kapcsolatok listájából a legjobb jelerősségű hálózatot, és automatikusan azt használni a csatlakozáshoz. Ugyanezt megvalósítani az ifup használatával nem kevés beállítást igényel.

20.6 Hálózati kapcsolat kézi beállítása

A hálózati szoftver kézi beállításának mindig az utolsó alternatívának kell lennie. A YaST használata javasolt. A hálózati konfigurációval kapcsolatos háttérinformáció azonban a YaST segítségével végzett munkát is elősegítheti.

Amikor a kernel észlel egy hálózati kártyát és létrehozza a hozzá tartozó hálózati csatolót, akkor az eszköznek a felderítés, vagy a kernelmodulok betöltésének sorrendje alapján rendel nevet. Az alapértelmezett kernel-eszköznevek csak nagyon egyszerű és igen

szabályozott hardverkörnyezetekben eredményeznek kiszámítható eszközneveket. Az olyan rendszereken, amelyek lehetővé teszik a hardver üzem közbeni hozzáadását és eltávolítását, illetve támogatják az eszközök automatikus konfigurációját, nem várható el, hogy a kernel minden egyes újraindításkor következetesen ugyanúgy osztja ki az eszközneveket.

Az összes rendszerkonfigurációs eszköz azonban számít a következetes eszköznevekre. Ezt a problémát oldja meg az udev. Az udev egy adatbázist tárol az ismert hálózati csatolókról, és a csatolókat a kernel által kiosztott nevükről az adatbázisban tárolt, állandó névre nevezi át. A hálózati csatolók udev-adatbázisa az `/etc/udev/rules.d/70-persistent-net.rules` fájlban tárolódik. A fájl minden egyes sora egy hálózati csatolót ír le és határozza meg állandó nevét. A rendszergazdák a kiosztott neveket a `NAME=""` bejegyzések módosításával változtathatják meg. Miután a hálózati eszköz átneveződött az udev által beállított névre, az `ifup` parancs alkalmazza a rendszer beállításait a csatolóra.

A 20.5 táblázat - Kézi hálózatkonfigurációs parancsfájlok (319. oldal) táblázat összefoglalja a hálózati konfigurációban résztvevő legfontosabb parancsfájlokat.

20.5. táblázat *Kézi hálózatkonfigurációs parancsfájlok*

Parancs	Funkció
`if{up,down,status}`	Az `if*` parancsfájlok meglévő hálózati csatolókat indítanak el vagy visszaadják a megadott csatoló állapotát. További információt az `ifup` kézikönyvoldala tartalmaz.
`rcnetwork`	Az `rcnetwork` parancsfájl használható az összes vagy csak egy adott hálózati csatoló elindítására, leállítására vagy újraindítására. Az `rcnetwork stop` parancs leállítja, az `rcnetwork start` elindítja, az `rcnetwork restart` parancs pedig újraindítja a hálózati csatolókat. Ha csak egy adott csatolót akar elindítani, leállítani vagy újraindítani, akkor a parancs után írja be a csatoló nevét, tehát például `rcnetwork restart eth0`. Ha nincs megadva csatoló, akkor a tűzfal is leáll, elindul vagy újraindul az összes hálózati

Parancs	Funkció
	csatolóval együtt. Az `rcnetwork status` parancs megjeleníti a csatolók állapotát, IP-címeit, valamint hogy fut-e DHCP-kliens. Az `rcnetwork stop-all-dhcp-clients` és `rcnetwork restart-all-dhcp-clients` parancsokkal lehet leállítani, illetve újraindítani a hálózati csatolókon futó DHCP-klienseket.

Az udev-alrendszerrel és az állandó eszköznevekkel kapcsolatos további információ: 17. fejezet - *Dinamikus kerneleszköz-felügyelet az udev segítségével* (237. oldal).

20.6.1 Konfigurációs fájlok

Ez a rész áttekintést nyújt a hálózati konfigurációs fájlokról, és bemutatja céljukat, valamint az általuk használt formátumot.

/etc/sysconfig/network/ifcfg-*

Ezek a fájlok tartalmazzák a hálózati csatolók beállításait. Olyan adatokat tartalmaznak, mint például az indítási mód és az IP-cím. A lehetséges paramétereket az `ifup` kézikönyvoldala tartalmazza. Ezen felül a `dhcp`, `wireless` és `config` fájlok változói használhatók az `ifcfg-*` fájlokban, ha egy általános beállítást kell használni egyetlen csatolóhoz.

/etc/sysconfig/network/{config, dhcp, wireless}

A `config` fájl az `ifup`, `ifdown` és `ifstatus` viselkedésének általános beállításait tartalmazza. A `dhcp` a DHCP, a `wireless` pedig a vezeték nélküli LAN kártyák beállításait tartalmazza. A három konfigurációs fájlban lévő változók megjegyzésekkel vannak ellátva és az `ifcfg-*` fájlokban is használhatók, amelyben nagyobb prioritást kapnak.

/etc/sysconfig/network/{routes,ifroute-*}

Itt van megadva a TCP/IP-csomagok statikus útválasztása. A különböző rendszerek által igényelt statikus utak az `/etc/sysconfig/network/routes` fájlban adhatók meg: a gép felé menő utak, a gép felé átjárón keresztül menő utak és a hálózat felé menő utak. Minden egyedi útválasztást igénylő csatolóhoz adjon meg egy további konfigurációs fájlt: `/etc/sysconfig/network/ifroute-*`. A `*` helyére írja be a csatoló nevét. Az útválasztási konfigurációs fájlok bejegyzései az alábbi módon néznek ki:

```
# Destination     Dummy/Gateway     Netmask            Device
#
127.0.0.0         0.0.0.0           255.255.255.0      lo
204.127.235.0     0.0.0.0           255.255.255.0      eth0
default           204.127.235.41    0.0.0.0            eth0
207.68.156.51     207.68.145.45     255.255.255.255    eth1
192.168.0.0       207.68.156.51     255.255.0.0        eth1
```

Az út célját az első oszlop tartalmazza. Ez az oszlop tartalmazhatja egy hálózat vagy gép IP-címét, illetve *elérhető* névkiszolgálók esetén a teljes képzésű hálózati vagy gépnevet.

A második oszlop az alapértelmezett átjárót tartalmazza, vagy egy olyan átjárót, amelyen keresztül egy gép vagy hálózat elérhető. A harmadik oszlop egy átjáró mögötti hálózatok vagy gépek hálózati maszkját tartalmazza. Egy átjáró mögötti gép maszkja például `255.255.255.255` lehet.

Az utolsó oszlop a helyi géphez csatlakozott hálózatok számára fontos, mint amilyen a loopback, Ethernet, ISDN, PPP és dummy eszköz. Itt meg kell adni az eszköz nevét.

Egy (opcionális) ötödik oszlop segítségével megadható az út típusa. Azoknak az oszlopoknak, amelyek nem szükségesek, mínusz jelet (–) kell tartalmazniuk annak biztosítása érdekében, hogy az elemző megfelelően értelmezze a parancsot. További részleteket a `routes(5)` man oldal tartalmaz.

/etc/resolv.conf

Ebben a fájlban van megadva a domain, amelyhez a gép tartozik (`search` kulcsszó). Az elérendő névkiszolgáló állapotát is megjeleníti (`nameserver` kulcsszó). Több tartománynév is megadható a fájlban. Egy nem teljes képzésű név feloldásakor kísérlet történik egy ilyen név létrehozására az egyes `search` bejegyzések csatolásával. Több névkiszolgáló több sorban adható meg, amelyek mindegyike a `nameserver` szóval

kell, hogy kezdődjön. A megjegyzések elé # jelet kell írni. A 20.5. példa - /etc/resolv.conf (322. oldal) bemutatja, hogyan nézhet ki egy /etc/resolv.conf fájl.

Az /etc/resolv.conf fájlt azonban nem szabad kézzel módosítani. Ezt a netconfig parancsfájl állítja elő. Statikus DNS-beállítások YaST nélküli megadásához kézzel kell módosítani a megfelelő változókat az /etc/sysconfig/network/config fájlban: NETCONFIG_DNS_STATIC_SEARCHLIST (DNS-tartománynevek listája gépnevek kikereséséhez), NETCONFIG_DNS_STATIC_SERVERS (névkiszolgáló IP-címek listája gépnevek kikereséséhez), és NETCONFIG_DNS_FORWARDER (a beállítandó DNS-továbbító nevét adja meg). A DNS-konfiguráció letiltásához a netconfig használatával állítsa be a NETCONFIG_DNS_POLICY='' értéket. További információ a netconfig-ról: man 8 netconfig.

20.5 példa */etc/resolv.conf*

```
# Our domain
search example.com
#
# We use dns.example.com (192.168.1.116) as nameserver
nameserver 192.168.1.116
```

Néhány szolgáltatás, mint például a pppd (wvdial), ipppd (isdn), dhcp (dhcpcd és dhclient) és a pcmcia módosítja az /etc/resolv.conf fájlt a modify_resolvconf parancsfájllal. Ha az /etc/resolv.conf fájlt a parancsfájl ideiglenesen módosította, akkor egy előre megadott megjegyzést, amely a módosító szolgáltatással kapcsolatos információt biztosítja, az eredeti fájl biztonsági mentésének helyét, és az automatikus módosítási mechanizmus kikapcsolásának módját tartalmazza. Ha az /etc/resolv.conf fájl többször módosításra került, akkor a fájl a módosításokat beágyazott formában tartalmazza. Ezek tisztán eltávolíthatók még abban az esetben is, ha az eltávolítás sorrendje eltér a módosításokétól. A szolgáltatások, amelyeknek szükségük van erre a rugalmasságra: isdn és pcmcia.

Ha egy szolgáltatás nem normál, tiszta módon áll le, a modify_resolvconf segítségével visszaállítható az eredeti fájl. Rendszerindításkor ellenőrzésre kerül, hogy maradt-e nem eltávolított, módosított resolv.conf például rendszerösszeomlás után, és ez esetben az eredeti (nem módosított) resolv.conf visszaállításra kerül.

A YaST a modify_resolvconf check parancs segítségével ellenőrzi, hogy a resolv.conf módosítva lett-e, majd figyelmezteti a felhasználót, hogy ezek a mó-

dosítások a fájl visszaállítása után elvesznek. Ettől eltekintve a YaST nem használja a `modify_resolvconf` fájlt, amely azt jelenti, hogy a `resolv.conf` YaST segítségével történő módosításának hatása megegyezik a kézi módosításával. Mindkét esetben a módosítások hatása állandó. Az említett szolgáltatások által igényelt módosítások csak ideiglenesek.

/sbin/netconfig

A `netconfig` egy moduláris eszköz a további hálózati beállítások kezeléséhez. A statikusan beállított paramétereket egyesíti az automatikus beállítási mechanizmusokkal, mint a DHCP vagy PPP, egy előre meghatározott irányelvnek megfelelően. A szükséges módosítások úgy végződnek el a rendszeren, hogy meghívódnak az egy adott konfigurációs fájl módosításáért felelős netconfig-modulok, majd újraindul a szolgáltatás (vagy valamilyen hasonló módszer).

A `netconfig` három fő műveletet ismer:

`modify` (módosítás)
: A `netconfig modify` parancs módosítja az aktuális csatolót és a szolgáltatásspecifikus dinamikus beállításokat, majd frissíti a hálózati konfigurációt. A netconfig a beállításokat a standard bemenetről vagy a `--lease-file` *`fájlnév`* paraméterrel megadott fájlból olvassa, és belsőleg eltárolja a rendszer újraindításáig vagy a következő módosítási vagy eltávolítási műveletig. Az ugyanazon csatoló-szolgáltatás kombináció már meglevő beállításai felülíródnak. A csatolót a `-i` *`csatolónév`* paraméter adja meg. A szolgáltatást a `-s` *`szolgáltatásnév`* paraméter adja meg.

`remove` (eltávolítás)
: A `netconfig remove` parancs eltávolítja a módosítás művelet által felvett dinamikus beállításokat a megadott csatoló-szolgáltatás kombinációról és frissíti a hálózati beállításokat. A csatolót a `-i` *`csatolónév`* paraméter adja meg. A szolgáltatást a `-s` *`szolgáltatásnév`* paraméter adja meg.

`update` (frissítés)
: A `netconfig update` parancs frissíti a hálózati konfigurációt az aktuális beállításokkal. Ez akkor hasznos, ha az irányelv vagy a statikus konfiguráció változott meg.

A netconfig-irányelv és a statikus konfigurációs beállítások megadhatók kézzel, a YaST használatával, vagy a NetworkManagerrel az `/etc/sysconfig/network/config` fájlban. A DHCP-hez és PPP-hez hasonló automatikus konfigurációs eszközök dinamikus beállításait közvetlenül ezek az eszközök továbbítják a `netconfig modify` és `netconfig remove` műveletekkel.

További információ a `netconfig`-ról: `man 8 netconfig`.

/etc/hosts

Ebben a fájlban (20.6. példa - `/etc/hosts` (324. oldal)) az IP-címek gépnevekhez vannak rendelve. Ha nincs névkiszolgáló, akkor minden gépet, amelyen be van állítva IP-kapcsolat, fel kell itt tüntetni. A fájlban minden géphez adjon meg egy sort, amely az IP-címet, a teljes képzésű gépnevet és a gépnevet tartalmazza. Az IP-címnek a sor elején kell lennie és a bejegyzéseket üres helyek és tabulátorok tagolják. A megjegyzések előtt mindig # jel található.

20.6 példa */etc/hosts*

```
127.0.0.1 localhost
192.168.2.100 jupiter.example.com jupiter
192.168.2.101 venus.example.com venus
```

/etc/networks

A hálózati nevek itt kerülnek átalakításra hálózati címekké. A formátum a `hosts` fájlhoz hasonló azzal a kivétellel, hogy a hálózati nevek megelőzik a címeket. Lásd:20.7. példa - `/etc/networks` (324. oldal)

20.7 példa */etc/networks*

```
loopback      127.0.0.0
localnet      192.168.0.0
```

/etc/host.conf

A névfeloldást – a gép- és hálózati nevek lefordítását a *resolver* könyvtáron keresztül – ez a fájl vezérli. Ezt a fájlt csak a libc4 vagy libc5 függvénytárhoz csatolt programok használják. Az aktuális glibc programok esetén tekintse meg az `/etc/nsswitch.conf` beállításait. A paraméternek mindig egyedül kell állnia a saját sorában. A

megjegyzéseket # jel előzi meg. 20.6 táblázat - Az /etc/host.conf paraméterei (325. oldal) táblázat a használható paramétereket jeleníti meg. Egy minta `/etc/host.conf` fájlt mutat be a 20.8. példa - `/etc/host.conf` (325. oldal).

20.6. táblázat *Az /etc/host.conf paraméterei*

order *hosts*, *bind*	Meghatározza, hogy a szolgáltatások milyen sorrendben érik el a névfeloldást. A használható argumentumok (üres hellyel vagy vesszőkkel elválasztva): *hosts*: Az `/etc/hosts` fájlt keresi *bind*: Hozzáfér egy névkiszolgálóhoz *nis*: NIS-t használ
multi *on*/*off*	Azt határozza meg, hogy az `/etc/hosts` fájlban megadott gép rendelkezhet-e több IP-címmel.
nospoof *on* spoofalert *on*/*off*	Ezek a paraméterek a névkiszolgáló *hamisítására* vannak hatással, de nem befolyásolják a hálózati konfigurációt.
trim *tartománynév*	A gépnévfeloldás után a megadott tartománynév le van választva a gépnévtől (feltéve, hogy a gépnév tartalmazta a tartománynevet). Ez az opció akkor hasznos, ha csak a helyi tartomány nevei vannak az `/etc/hosts` fájlban, de a csatolt tartományneveket továbbra is fel kell ismerni.

20.8 példa */etc/host.conf*

```
# We have named running
order hosts bind
# Allow multiple address
multi on
```

/etc/nsswitch.conf

A GNU C Library 2.0 bevezetése együtt jár a *Name Service Switch* (NSS) bevezetésével. Részletes információt az `nsswitch.conf(5)` kézikönyvoldala és a *The GNU C Library Reference Manual* tartalmaz.

A lekérdezések sorrendje az `/etc/nsswitch.conf` fájlban van megadva. A 20.9. példa - `/etc/nsswitch.conf` (326. oldal) egy példa `nsswitch.conf` fájlt mutat. A megjegyzéseket a # jel vezeti be. Ebben a példában a `hosts` adatbázis alatti bejegyzések azt jelentik, hogy kérés lett küldve DNS-en keresztül az `/etc/hosts` (`fájlok`) fájlhoz.

20.9 példa */etc/nsswitch.conf*

```
passwd:     compat
group:      compat

hosts:      files dns
networks:   files dns

services:   db files
protocols:  db files

netgroup:   files
automount:  files nis
```

Az NSS-en keresztül elérhető „adatbázisok” listája: 20.7 táblázat - Az /etc/nsswitch.conf fájlon keresztül elérhető adatbázisok (326. oldal). Ezen felül az `automount`, `bootparams`, `netmasks` és `publickey` várható a közeli jövőben. Az NSS adatbázisok konfigurációs beállításait tekinti át a 20.8 táblázat - NSS-„adatbázisok” beállítási lehetőségei (327. oldal).

20.7. táblázat *Az /etc/nsswitch.conf fájlon keresztül elérhető adatbázisok*

`aliasok`	A `sendmail` által megvalósított e-mail aliasok; lásd: `man 5 aliases`.
`ethers`	Ethernet-címek.
`csoport`	Felhasználói csoportok, a `getgrent` használja. Lásd még a `group` man kézikönyvoldalát.
`hosts`	Gépnevek és IP-címek, a `gethostbyname` és hasonló funkciók használják.
`netgroup`	Érvényes gép- és felhasználói listák a hálózatban a hozzáférési jogosultságok vezérléséhez; lásd: `netgroup(5)` man oldal.

networks	A getnetent által használt hálózatnevek és címek.
passwd	A getpwent által használt felhasználói jelszavak; lásd a passwd(5) kézikönyvoldalát.
protocols	A getprotoent által használt hálózati protokollok; lásd a protocols(5) kézikönyvoldalát.
rpc	A getrpcbyname és hasonló funkciók által használt távoli eljáráshívásnevek és címek.
services	A getservent által használt hálózati szolgáltatások.
shadow	A getspnam által használt shadow-jelszavak és felhasználók; lásd a shadow(5) kéizkönyvoldalát.

20.8. táblázat *NSS-„adatbázisok” beállítási lehetőségei*

files	fájlok, például az /etc/aliases közvetlen elérése
db	elérés adatbázison keresztül
nis, nisplus	NIS, lásd még: 25. fejezet - *A NIS használata* (387. oldal)
dns	csak a hosts és networks kiterjesztéseként használható
compat	csak a passwd, shadow, és group kiterjesztéseként használható

/etc/nscd.conf

Ez a fájl állítja be az nscd-t (name service cache daemon, névkiszolgáló-gyorsítótárdémon). Lásd az nscd(8) és nscd.conf(5) kézikönyvoldalát. Alapértelmezés szerint a passwd és groups rendszerbejegyzéseit az nscd ideiglenesen tárolja. Ez a címtárszolgáltatások – például NIS és LDAP – teljesítménye miatt fontos, mivel ellenkező esetben a hálózati kapcsolatot kell használni a nevek és csoportok eléréséhez A hosts alapértelmezés szerint nem kerül ideiglenesen tárolásra, mivel az nscd-nek a gépeket

ideiglenesen tároló mechanizmusa miatt a helyi rendszer nem tud megbízni a normál és visszirányú ellenőrzésekben. Ahelyett, hogy az nscd tároltatná ideiglenesen a neveket, állítson be egy ideiglenes tárolást végző DNS-kiszolgálót.

A `passwd` ideiglenes tárolása aktív, akkor általában tizenöt másodpercig tart az újonnan hozzáadott helyi felhasználó felismerése. A várakozási idő lecsökkenthető, ha az nscd-t az `rcnscd restart` parancs segítségével újraindítja.

/etc/HOSTNAME

A gépnevet tartalmazza a csatolt tartománynév nélkül. Ezt a fájlt számos parancsfájl olvassa a gép indulása során. Elképezlhető, hogy csak egy sort tartalmaz, amelyben a gépnév van beállítva.

20.6.2 A konfiguráció tesztelése

A konfigurációt a konfigurációs fájlba írás előtt tesztelheti. Állítsa be a tesztkonfigurációt az `ip` parancs segítségével. A kapcsolat a `ping` paranccsal tesztelhető. A régi konfigurációs eszközök, az `ifconfig` és a `route`, szintén rendelkezésre áll.

Az `ip`, `ifconfig` és a `route` parancs közvetlenül módosítja a hálózati konfigurációt a konfigurációs fájlba való mentés nélkül. Ha a konfigurációt nem a megfelelő konfigurációs fájlokban adta meg, akkor a módosított hálózati konfiguráció a rendszer újraindításakor elveszik.

Hálózati csatoló beállítása ip-vel

Az `ip` az útválasztás, a hálózati eszközök, az irányelv-továbbítás és a csatornák megjelenítésére és beállítására szolgáló eszköz. A régebbi eszközök, az ifconfig és a route helyettesítésére alakították ki.

Az `ip` egy igen összetett eszköz. Az általános szintaxis: `ip` *`opciók objektum parancs`*. A következő objektumok használhatók:

link (csatolás)
: Az objektum egy hálózati eszközt ábrázol.

TCP/IP:
: Az objektum az eszköz IP-címét ábrázolja.

neighbour (szomszéd)
: Az objektum egy ARP vagy NDISC gyorsítótár-bejegyzést ábrázol.

router (útvonal)
: Az objektum az útválasztási tábla bejegyzést ábrázolja.

rule (szabály)
: Az objektum az útválasztási irányelv adatbázisban lévő szabályt ábrázolja.

maddress
: Az objektum egy multicast-címet ábrázol.

mroute
: Az objektum egy multicast útválasztási gyorsítótár bejegyzést ábrázol.

tunnel (alagút)
: Az objektum IP-n keresztüli alagutat ábrázol.

Ha nincs parancs megadva, akkor az alapértelmezett parancs kerül felhasználásra. Ez általában a `list`.

Módosítsa az eszköz állapotát az `ip link set` *`eszköznév parancs`* paranccsal. Az eth0 eszköz letiltásához például adja ki az `ip link set eth0 down` parancsot. Az újbóli aktiváláshoz használja az `ip link set eth0 up` parancsot.

Az eszközt aktiválás után beállíthatja. Az IP-cím beállításához használja az `ip addr add` *`ip_cím`* `+ dev` *`eszköznév`* parancsot. Az eth0 csatolóhoz 192.168.12.154/30 beállítása például normál üzenetszórással (`brd` opció) az alábbi módon történhet: adja ki az `ip addr add 192.168.12.154/30 brd + dev eth0` parancsot.

Működő kapcsolathoz az alapértelmezett átjárót is be kell állítani. A rendszer átjárójának beállításához adja ki az `ip route add átjáró_ip_címe` parancsot. Az IP-cím másik címre fordításához használjon `nat`-ot: az `ip route add nat ip_cím via másik_ip_cím`.

Az összes eszköz megjelenítéséhez használja az `ip link ls` parancsot. Ha csak a futó csatolókat kívánja megjeleníteni, akkor használja az `ip link ls up` parancsot.

Az eszköz csatolóstatisztikájának kinyomtatásához adja ki az `ip -s link ls eszköznév` parancsot. Az eszközök címének megjelenítéséhez adja ki az `ip addr` parancsot. Az `ip addr` kimenetében az eszközök MAC-címével kapcsolatos információt is talál. Az összes út megjelenítéséhez használja az `ip route show` parancsot.

Az ip használatával kapcsolatos információért adja ki az `ip help` parancsot, vagy tekintse meg az `ip(8)` kézikönyvoldalát. A `help` opció az összes ip objektumhoz rendelkezésre áll. Ha például az `ip addr` súgóját kívánja elolvasni, akkor adja ki az `ip addr help` parancsot. Az ip leírása az `/usr/share/doc/packages/iproute2/ip-cref.pdf` fájlban található.

Kapcsolat tesztelése a ping paranccsal

A `ping` parancs egy általános eszköz a TCP/IP kapcsolat működésének tesztelésére. Ez az ICMP protokollal kis adatcsomagot, ECHO_REQUEST datagramot küld a célgépnek, és azonnal választ kér. Ha ez működik, akkor a `ping` egy üzenetet jelenít meg, amely jelzi, hogy a hálózati kapcsolat alapszinten működik.

A `ping` nem csak a két számítógép közötti kapcsolat működését teszteli. A kapcsolat minőségével kapcsolatos alapszintű információt is biztosít. A 20.10. példa - A ping parancs kimenete (331. oldal) példát mutat a `ping` kimenetére. A sorok – az első kivételével – az átvitt csomagokkal, csomagvesztéssel és a `ping` teljes futási idejével kapcsolatos kapcsolatos adatokat tartalmaznak.

Célként megadhat gépnevet vagy IP-címet, például: `ping example.com` vagy `ping 192.168.3.100`. A program addig küld csomagokat, amíg meg nem nyomja a Ctrl + C billentyűkombinációt.

Ha csak a kapcsolat működését kívánja ellenőrizni, akkor a `-c` kapcsolóval korlátozhatja a csomagok számát. A ping három csomagra korlátozásához például adja ki a `ping -c 3 example.com` parancsot.

20.10 példa *A ping parancs kimenete*

```
ping -c 3 example.com
PING example.com (192.168.3.100) 56(84) bytes of data.
64 bytes from example.com (192.168.3.100): icmp_seq=1 ttl=49 time=188 ms
64 bytes from example.com (192.168.3.100): icmp_seq=2 ttl=49 time=184 ms
64 bytes from example.com (192.168.3.100): icmp_seq=3 ttl=49 time=183 ms
--- example.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2007ms
rtt min/avg/max/mdev = 183.417/185.447/188.259/2.052 ms
```

Az alapértelmezett időtartam a két csomag között egy másodperc. Az időtartam a ping `-i` kapcsolójával módosítható. A ping időtartamának tíz másodpercre növeléséhez adja ki a `ping -i 10 example.com` parancsot.

Több hálózati eszközzel rendelkező rendszerben hasznos lehet a ping csomagot adott csatolócímen keresztül küldeni. Ehhez használja a `-I` kapcsolót a kiválasztott eszköz nevével, például: `ping -I wlan1 example.com`.

A ping parancs kapcsolóival és használatával kapcsolatos információért adja ki a `ping -h` parancsot, vagy tekintse meg a `ping (8)` kézikönyvoldalát.

Hálózat beállítása az ifconfig segítségével

Az `ifconfig` egy hagyományos hálózatkonfigurációs eszköz. Az ip-vel ellentétben ez csak csatolókonfigurációhoz használható. Az útválasztás beállításához használja a `route` parancsot.

MEGJEGYZÉS: ifconfig és ip

Az ifconfig program elavult. Használja inkább az ip-t.

Argumentumok nélkül az ipconfig az aktuális aktív csatolók állapotát mutatja meg. Az ábrán (20.11. példa - Az ifconfig parancs kimenete (332. oldal)) láthatóan az ifconfig jó elrendezésű és részletes kimenettel rendelkezik. A kimenet az eszköz MAC-címével kapcsolatos adatokat is tartalmaz. Ez a `HWaddr` érték az első sorban.

20.11 példa *Az ifconfig parancs kimenete*

```
eth0      Link encap:Ethernet  HWaddr 00:08:74:98:ED:51
          inet6 addr: fe80::208:74ff:fe98:ed51/64 Scope:Link
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:634735 errors:0 dropped:0 overruns:4 frame:0
          TX packets:154779 errors:0 dropped:0 overruns:0 carrier:1
          collisions:0 txqueuelen:1000
          RX bytes:162531992 (155.0 Mb)  TX bytes:49575995 (47.2 Mb)
          Interrupt:11 Base address:0xec80

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:8559 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8559 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:533234 (520.7 Kb)  TX bytes:533234 (520.7 Kb)

wlan1     Link encap:Ethernet  HWaddr 00:0E:2E:52:3B:1D
          inet addr:192.168.2.4  Bcast:192.168.2.255  Mask:255.255.255.0
          inet6 addr: fe80::20e:2eff:fe52:3b1d/64 Scope:Link
          UP BROADCAST NOTRAILERS RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:50828 errors:0 dropped:0 overruns:0 frame:0
          TX packets:43770 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:45978185 (43.8 Mb)  TX bytes:7526693 (7.1 MB)
```

Az ifconfig használatával és kapcsolóival kapcsolatos információért adja ki az `ifconfig –h` parancsot, vagy használja az `ifconfig (8)` kézikönyvoldalát.

Útválasztás beállítása a route paranccsal

A `route` az IP útválasztási tábla kezelésére szolgáló program. Ennek segítségével megjeleníthető az útválasztási konfiguráció, illetve utak vehetők fel és távolíthatók el.

MEGJEGYZÉS: route és ip

A route program elavult. Használja inkább az ip-t.

A route különösen akkor hasznos, ha az útválasztási konfigurációval kapcsolatos gyors és érthető adatokra van szüksége az útválasztással kapcsolatos problémák meghatározásához. Az aktuális útválasztási konfiguráció megjelenítéséhez adja ki a `route –n` parancsot `root` felhasználóként.

20.12 példa *A route -n parancs kimenete*

```
route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
10.20.0.0       *               255.255.248.0   U         0 0          0 eth0
link-local      *               255.255.0.0     U         0 0          0 eth0
loopback        *               255.0.0.0       U         0 0          0 lo
default         styx.exam.com   0.0.0.0         UG        0 0          0 eth0
```

A route használatával és kapcsolóival kapcsolatos információért adja ki a `route -h` parancsot, vagy tekintse meg a `route (8)` kézikönyvoldalát.

20.6.3 Indító parancsfájlok

A fentebb említett konfigurációs beállítási fájloktól függetlenül számos parancsfájl létezik, amely hálózati programot tölt be a gép rendszerindítása alatt. Ezek azonnal elindulnak, amint a gép az egyik *többfelhasználós futási szintre* kapcsol. A parancsfájlok egy részének leírása: 20.9 táblázat - Néhány indító parancsfájl a hálózati programokhoz (333. oldal).

20.9. táblázat *Néhány indító parancsfájl a hálózati programokhoz*

`/etc/init.d/network`	Ez a parancsfájl kezeli a hálózati csatolók beállítását. Ha a `network` szolgáltatás nincs elindítva, akkor egyetlen hálózati csatoló sem él.
`/etc/init.d/xinetd`	Elindítja az xinetd-t. Az xinetd a kiszolgálószolgáltatásokat elérhetővé tudja tenni a rendszeren. Egy FTP kapcsolat kezdeményezésekor például el tudja indítani a vsftpd-t.
`/etc/init.d/portmap`	Elindítja az RPC-kiszolgáló számára szükséges portleképezőt, például egy NFS-kiszolgálót.
`/etc/init.d/nfsserver`	Elindítja az NFS kiszolgálót.
`/etc/init.d/postfix`	Vezérli a postfix folyamatot.

`/etc/init.d/ypserv`	Elindítja a NIS-kiszolgálót.
`/etc/init.d/ypbind`	Elindítja a NIS-klienst.

20.7 Az smpppd behívósegéd

Sok otthoni felhasználó nem rendelkezik dedikált internetkapcsolattal. Ehelyett általában behívó kapcsolatot használnak. A behívási módszertől függően (ISDN vagy DSL) a kapcsolatot az ipppd vagy a pppd vezérli. Az internetre feljelentkezéshez alig kell többet tenni, mint elindítani helyesen ezeket a programokat.

Ha átalánydíjas kapcsolattal rendelkezik, ami nem jelent többletköltséget behívásos kapcsolat esetén sem, egyszerűen indítsa el a megfelelő démont. A behívásos kapcsolat egy KDE-kisalkalmazás vagy a parancssori felület segítségével felügyelhető. Ha az internetes átjáró nem a saját gép, akkor lehet, hogy a behívásos kapcsolatot egy hálózati gép segítségével kívánja irányítani.

Itt kerül a képbe az smpppd. Egységes felületet biztosít a segédprogramok számára és két irányban működik. Először is beprogramozza a szükséges pppd-t vagy ipppd-t és vezérli azok behívási tulajdonságait. Másodszor a felhasználói programok számára elérhetővé teszi a különböző szolgáltatókat és továbbít bizonyos információkat a kapcsolat aktuális állapotával kapcsolatban. Mivel az smpppd hálózaton keresztül is vezérelhető, egy magánjellegű alhálózatban teljesen megfelel a munkaállomásról az internet felé irányuló behívó kapcsolatok kezelésére.

20.7.1 Az smpppd beállítása

A YaST automatikusan beállítja az smpppd által biztosított kapcsolatokat. A tényleges behívóprogramok, a KInternet és cinternet szintén előre beállításra kerültek. Kézi beállításra csak az smpppd olyan további funkcióinak beállításához van szükség, mint például a távoli vezérlés.

Az smpppd konfigurációs fájlja az `/etc/smpppd.conf`. Alapértelmezés szerint ez nem engedélyezi a távoli vezérlést. A konfigurációs fájl legfontosabb beállításai:

open-inet-socket = *yes|no*

Az smpppd hálózatról történő vezérléséhez ezt a beállítást `yes` értékre kell állítani. Az smpppd a `3185`-ös porton figyel. Ha a paraméter értéke `yes`, akkor a `bind-address`, `host-range` és `password` paramétert is megfelelően be kell állítani.

bind-address = *ip-cím*

Ha a hoszt több IP-címmel rendelkezik, akkor ennek a paraméternek a használata határozza meg, hogy az smpppd-nek mely IP-címen kell fogadnia a kapcsolatokat. Alapértelmezésben a rendszer az összes porton figyel.

host-range = *min ip max ip*

A `host-range` paraméter egy hálózati tartományt ad meg. A tartományon belüli IP-címmel rendelkező gépek számára engedélyezett a hozzáférés az smpppd-hez. A tartományon kívüli gépek hozzáférése le van tiltva.

password = *jelszó*

Jelszó hozzárendelésével a kliensek hozzáférése korlátozható a hitelesített gépekre. Mivel azonban ez egy sima szöveges jelszó, nem szabad túlbecsülni az általa nyújtott biztonságot. Ha nincs jelszó megadva, akkor az összes kliens hozzáférhet az smpppd-hez.

slp-register = *yes|no*

Ezzel a paraméterrel az smpppd szolgáltatás meghirdethető a hálózatban SLP protokollon keresztül.

Az smpppd-vel kapcsolatos információ az `smpppd(8)` és `smpppd.conf(5)` kézikönyvoldalon érhető el.

20.7.2 Kinternet és cinternet beállítása távoli használathoz

A kinternet és a cinternet segítségével vezérelhető a helyi vagy távoli smpppd. A cinternet a grafikus Kinternet parancssori megfelelője. Ezeknek a segédprogramoknak a távoli smpppd-vel való használatához kézzel vagy a kinternet segítségével módosítsa az `/etc/smpppd-c.conf` konfigurációs fájlt. Ez a fájl csak négy paramétert tartalmaz:

sites = *helyek listája*
: Itt kell megadni a felületek számára, hogy az smpppd-t hol kell keresni. A felületek az itt megadott sorrendben próbálják végig a lehetőségeket. A `local` (helyi) beállítás a helyi smpppd-vel való kapcsolat létesítését írja elő. A `gateway` paraméter az átjárón lévő smpppd-re mutat. A `config-file` paraméter azt jelzi, hogy az `/etc/smpppd-c.conf` fájlban található `server` és `port` paraméterekkel megadott smpppd-hez kell csatlakozni. Az `slp` a felületeket egy SLP-n keresztül megtalált smpppd-hez kapcsolódásra készteti.

server = *kiszolgáló*
: Itt adja meg azt a gépet, amelyen az smpppd fut.

port = *port*
: Itt adja meg azt a portot, amelyen az smpppd elérhető.

password = *jelszó*
: Adja meg az smpppd-hez kiválasztott jelszót.

Ha az smpppd aktív, akkor most már megpróbálhat csatlakozni hozzá, például a `cinternet --verbose --interface-list` parancs segítségével. Ha itt nehézségei vannak, akkor tekintse meg az `smpppd-c.conf(5)` és `cinternet(8)` kézikönyvoldalt.

SLP-szolgáltatások a hálózatban

21

Az *SLP-t* (Service Location Protocol, szolgáltatáshely-protokoll) a helyi hálózatban lévő hálózati kliensek beállításának egyszerűsítésére fejlesztették ki. A hálózati kliens beállításához, a szükséges szolgáltatásokat is beleértve, az adminisztrátornak részletesen ismernie kell a hálózat kiszolgálóit. Az SLP értesíti az adott szolgáltatás elérhetőségéről a helyi hálózat minden kliensét. Az SLP-t támogató alkalmazások fel tudják használni a szétosztott információt és automatikusan beállíthatók.

Az openSUSE támogatja az SLP-n keresztül kínált telepítési források használatát a telepítéshez, és számos integrált SLP-támogatással rendelkező rendszerszolgáltatást biztosít. A YaST és Konqueror egyaránt rendelkezik a megfelelő bemeneti felülettel az SLP-hez. Az SLP használatával központi szolgáltatások biztosíthatók a hálózati kliensek számára: például egy telepítőkiszolgáló, fájlkiszolgáló vagy nyomtatókiszolgáló.

FONTOS: SLP-támogatás openSUSE alatt

Az SLP-támogatást kínáló szolgáltatások a következők: cupsd, rsyncd, ypserv, openldap2, ksysguardd, saned, kdm vnc login, smpppd, rpasswd, postfix és sshd (fishen keresztül).

21.1 Telepítés

Alapértelmezés szerint csak az SLP-kliens és az slptools van telepítve. Ha SLP-n keresztül kíván szolgáltatásokat meghirdetni, telepítse az `openslp-server` csomagot. A csomag telepítéséhez indítsa el a YaST-ot, majd válassza ki a *Szoftver* > *Szoftvertelepítés* modult. Most válassza ki a *Szűrő* > *Minták* lehetőséget, majd az *Egyéb Kiszol-*

gáló menüpontot. Válassza ki az `openslp-server` csomagot. A telepítési folyamat befejezéséhez erősítse meg a kívánt csomagok telepítését.

21.2 SLP aktiválása

Ahhoz, hogy SLP-vel meg lehessen hirdetni szolgáltatásokat, az slpd démonnak futnia kell a rendszeren. Ha a gép csak kliensként fog működni és nem biztosít szolgáltatásokat, akkor felesleges az slpd futtatása. Az openSUSE alatt futó legtöbb szolgáltatáshoz hasonlóan az slpd démont is külön `inicializációs` (init) parancsfájlok vezérlik. Telepítés után a démon alapértelmezés szerint inaktív. Ideiglenes aktiválásához futtassa le az `rcslpd start` parancsot a `root` felhasználó nevében, illetve a leállításhoz adja ki az `rcslpd stop` parancsot. A `restart` vagy `status` paraméter használatával újraindítást ill. állapotellenőrzést hajthat végre. Ha az slpd-nek alapértelemzés szerint aktívnak kell lennie a rendszerindítás után, akkor engedélyezze az slpd-t a YaST *Rendszer* > *Rendszerszolgáltatások (futási szint)* menüpontjával, vagy futtassa le az `insserv slpd` parancsot egyszer `root` felhasználóként. Ennek hatására bekerül az slpd a rendszerindításkor elindítandó szolgáltatások listájába.

21.3 SLP felhasználói felületek openSUSE alatt

A hálózatban meghirdetett szolgáltatások SLP segítségével történő megkereséséhez használja az SLP felhasználói felületet. Az openSUSE számos felhasználói felületet tartalmaz:

slptool
: Az slptool egy egyszerű parancssori program SLP-kérések kiadására a hálózatban, vagy egyedi szolgáltatások meghirdetésére. Az `slptool --help` parancs elsorolja az összes rendelkezésre álló lehetőséget és funkciót. Az slptool az SLP-adatokat feldolgozó parancsfájlokból is meghívható. Például ha ki akarja keresni az összes, magát a hálózatban meghirdető időkiszolgálót, akkor írja be az alábbi parancsot:

```
slptool findsrvs service:ntp
```

Konqueror
: Ha hálózati böngészőnek használjuk, a Konqueror képes a helyi hálózat összes rendelkezésre álló SLP-szolgáltatásának megjelenítésére az `slp:/` protokolljelöléssel. A megfelelő szolgáltatással kapcsolatos részletes információért kattintson a főablakban lévő ikonokra. Ha a Konquerort `service:/` protokolljelöléssel használja, kattintson egyszer a böngészőablak megfelelő ikonjára a kapcsolat megteremtéséhez a kiválasztott szolgáltatással.

21.4 Telepítés SLP-n keresztül

Ha telepítési kiszolgálót is kíván biztosítani a hálózaton, az openSUSE telepítési adathordozól használatával, ez a szolgáltatás is meghirdethető SLP-n keresztül. Ennek részletes leírása: 1.2. - A telepítési forrásokat tároló kiszolgáló beállítása (12. oldal). Ha az SLP-telepítést választja ki, akkor a linuxrc a kiválasztott rendszerindítási adathordozóról való indulás után küld egy SLP-lekérdezést, és megjeleníti a talált forrásokat.

21.5 Szolgáltatások meghirdetése SLP használatával

Az openSUSE számos alkalmazása rendelkezik már integrált SLP támogatással a `libslp` függvénytár használatával. Ha egy szolgáltatás nem SLP-támogatással került lefordításra, akkor az alábbi módszerek egyikével tehető elérhetővé:

Statikus regisztráció az `/etc/slp.reg.d` könyvtárban
: Minden új szolgáltatáshoz hozzon létre egy külön regisztrációs fájlt. A következő példában egy lapolvasó szolgáltatás regisztrálására szolgáló fájl látható:

```
## Register a saned service on this system
## en means english language
## 65535 disables the timeout, so the service registration does
## not need refreshes
service:scanner.sane://$HOSTNAME:6566,en,65535
watch-port-tcp=6566
description=SANE scanner daemon
```

A fájl legfontosabb sora a *szolgáltatás URL*-jét tartalmazó sor, amely a `service:` szóval kezdődik. Ez tartalmazza a szolgáltatástípust (`scanner.sane`) és a címet,

amelyen a szolgáltatás elérhető a kiszolgálón. A *$HOSTNAME* automatikusan behelyettesítésre kerül a teljes gépnévvel. Ezután a megfelelő szolgáltatás TCP-portjának a neve következik kettősponttal elválasztva. Ezt követően adja meg a szolgáltatás nyelvét és a regisztráció időtartamát másodpercben. Ezeket a szolgáltatás URL-jétől vesszővel kell elválasztani. A regisztráció időtartamának `0` és `65535` közötti értéknek kell lennie. A `0` megakadályozza a regisztrációt. A `65535` megszünteti az összes korlátozást.

A regisztrációs fájl a `watch-port-tcp` és `description` változókat is tartalmazza. A `watch-port-tcp` ahhoz köti az SLP-szolgáltatás meghirdetését, hogy a megfelelő szolgáltatás aktív-e (az slpd ellenőrzi a szolgáltatás állapotát). A második változó a szolgáltatás pontosabb leírását tartalmazza, ami a megfelelő böngészőkben meg is jeleníthető.

Statikus regisztráció az `/etc/slp.reg` használatával
: Az egyetlen különbség e módszer és az `/etc/slp.reg.d` használata között, hogy az összes szolgáltatás egy központi fájlba van gyűjtve.

Dinamikus regisztráció az slptool segítségével
: Ha egy szolgáltatást dinamikusan kell bejegyezni, konfigurációs fájlok nélkül, használja az slptool parancssori segédprogramot. Ugyanez a segédprogram használható egy meglévő szolgáltatás bejegyzésének megszüntetésére anélkül, hogy újra kéne indítani az slpd démont.

21.6 További információk

Az alábbi forrásokból további információhoz juthat az SLP-vel kapcsolatban:

RFC 2608, 2609, 2610
: Az RFC 2608 általában az SLP definíciójával foglalkozik. Az RFC 2609 a használt szolgáltatási URL-ek szintaxisával foglalkozik részletesebben, az RFC 2610 pedig az SLP-n keresztül megvalósított DHCP-vel.

`http://www.openslp.org/`
: Az OpenSLP projekt honlapja.

`/usr/share/doc/packages/openslp`
: Ez a könyvtár tartalmazza az SLP-hez rendelkezésre álló összes dokumentációt, az openSUSE-ot részletesen ismertető `README.SuSE` fájlt is beleértve, továbbá a fent említet RFC-ket és a két bevezető HTML dokumentumot is beleértve. Az SLP-funkciókat használni kívánó programozók további információt az `openslp-devel` csomagban lévő *Programozói kézikönyvben* találhatnak.

A DNS (tartománynévrendszer, Domain Name System)

22

A DNS (tartománynévrendszer) a tartomány- és gépneveket IP-címekké alakító rendszer. A 192.168.2.100 IP-cím például a `jupiter` gépnévhez lehet rendelve. Egy saját névkiszolgáló beállítása előtt olvassa el az általános tudnivalókat a DNS-ről: 20.3. - Névmegfeleltetés (295. oldal). Az alábbi konfigurációs példák a BIND-ra hivatkoznak.

22.1 DNS-terminológia

Zóna (zone)
: A tartomány névtere zónáknak nevezett részekre van osztva. Az `example.com` például a `com` tartomány `example` nevű részét, vagy zónáját jelenti.

DNS-kiszolgáló
: A DNS-kiszolgáló egy olyan kiszolgáló, amelyik egy adott tartomány név- és IP-adatait kezeli. Működhet egy elsődleges DNS-kiszolgáló az elsődleges zónához, egy másodlagos kiszolgáló a másodlagos zónához, vagy egy másodlagos kiszolgáló zónák nélkül, csak gyorsítótárazáshoz.

  Elsődleges zóna DNS-kiszolgálója
  : Az elsődleges (master) zóna tartalmazza a hálózat összes gépét, és az elsődleges zóna a DNS-kiszolgálón tartalmazza a legfrissebb adatokat a tartomány összes gépéről.

Másodlagos zóna DNS-kiszolgáló
: A másodlagos zóna az elsődleges zóna másolata. A másodlagos zóna DNS-kiszolgálója a zónaadatokat az elsődleges kiszolgálótól kapja, ún. zónatranszfer-műveletek keretében. A másodlagos zóna DNS-kiszolgálója hatályos adatokat szolgáltat a zónáról, feltéve, hogy érvényes (nem lejárt) zónaadatokkal rendelkezik. Ha a másodlagos kiszolgáló nem tudja lekérni a zónaadatokat, akkor abbahagyja a zónára vonatkozó kérések kiszolgálását.

Továbbító (forwarder)
: A továbbítók olyan DNS-kiszolgálók, amelyekhez a saját DNS-kiszolgáló továbbítani tudja az olyan kéréseket, amelyeket maga nem tud megválaszolni. Arra, hogy ugyanazon konfiguráción belül többféle konfigurációs forrást is meg lehessen adni, a `netconfig` használható (lásd még: `man 8 netconfig`).

Rekord
: A rekordok tárolják az adatokat a nevekről és az IP-címekről. A támogatott rekordtípusokat és szintaxisukat a BIND dokumentációja írja le. Néhány fontosabb rekord:

  NS rekord
  : Az NS rekord mondja meg a névkiszolgálók számára, hogy egy adott tartományzónáért mely gépek felelősek.

  MX rekord
  : Az MX (mail exchange, levélcsere) rekordok írják le, hogy mely gépek felelősek az adott zónával kapcsolatos levelek irányításáért az interneten.

  SOA rekord
  : A SOA (Start of Authority, jogosultság kezdete) rekord a zónafájl első rekordja. A SOA rekord akkor használatos, amikor a DNS szinkronizálja az adatokat több gép között.

22.2 Telepítés

A DNS-kiszolgáló telepítéséhez indítsa el a YaST-ot és válassza ki a *Szoftver* > *Szoftver telepítése és eltávolítása* menüpontot. Válassza ki a *Szűrő* > *Minták* menüpontot, majd a *DHCP- és DNS-kiszolgáló* pontot. A telepítési folyamat befejezéséhez erősítse meg a függő csomagok telepítését.

22.3 Beállítás a YaST segítségével

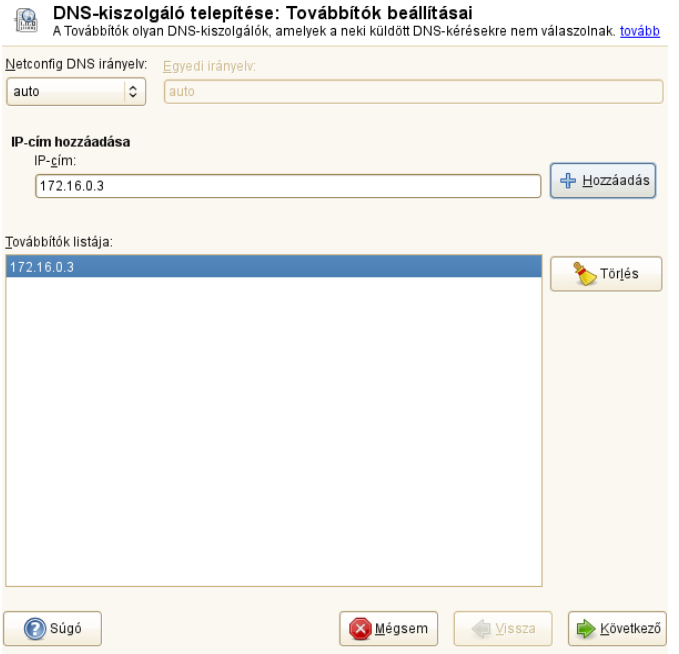
A YaST DNS-modulja segítségével be lehet állítani egy DNS-kiszolgálót a helyi hálózaton. A modul első indításakor megjelenik egy varázsló, és feltesz néhány alapkérdést a kiszolgáló felügyeletével kapcsolatban. A kezdeti beállítás egy alap kiszolgálókonfigurációt hoz létre, amely a legfontosabb feladatokat már képes ellátni. A szakértői módban a speciális konfigurációs feladatok is elvégezhetők.

22.3.1 Beállító varázsló

A varázsló három lépésből (párbeszédablakból) áll. A párbeszédablakok megfelelő helyein be lehet lépni a szakértői beállítási módba.

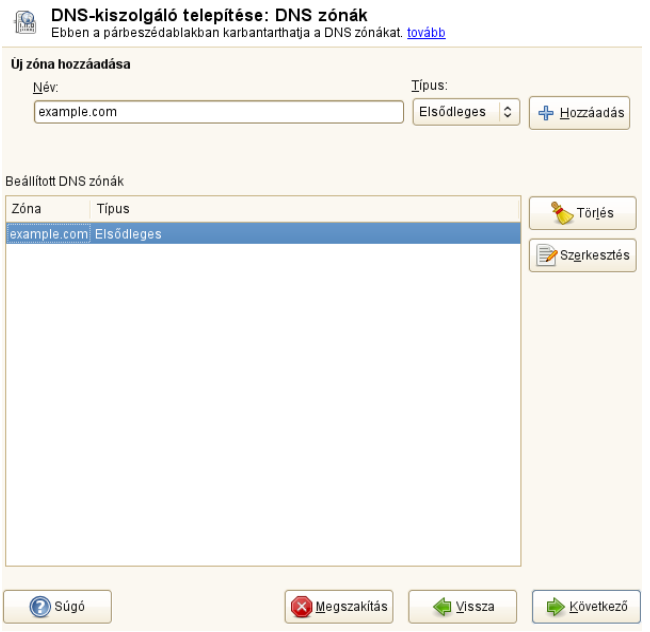
1. A modul első elindításakor megjelenik a *Továbbítók beállításai* párbeszédablak (22.1. ábra - DNS-kiszolgáló telepítése: Továbbítók beállításai (346. oldal)). A *Netconfig DNS irányelv* határozza meg, hogy az eszközök biztosítanak-e továbbítókat, vagy van saját *Továbbítók listája*. További információ a netconfigról: `man 8 netconfig`.

22.1. ábra *DNS-kiszolgáló telepítése: Továbbítók beállításai*



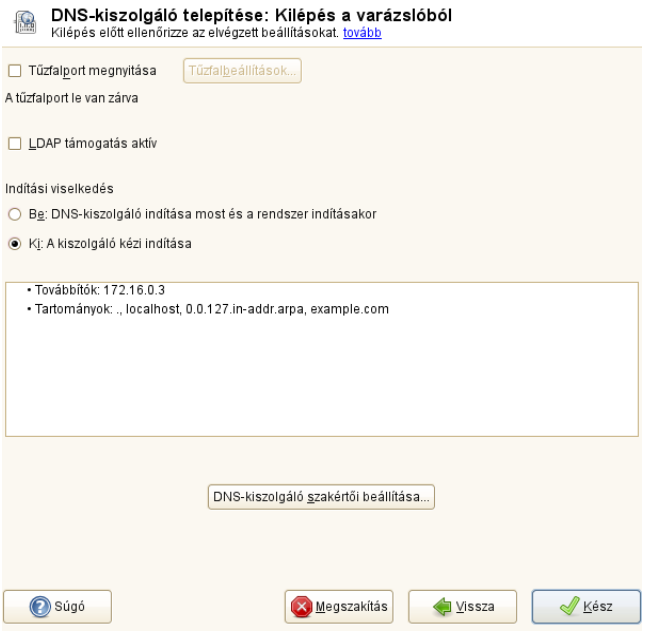
2 A *DNS-zónák* párbeszédablak több részből áll, és ez felelős a 22.6. - Zónafájlok (361. oldal) részben leírt zónafájlok kezeléséért. Új zóna létrehozásához a *Zóna neve* mezőben adjon meg egy nevet. Visszirányú zóna felvétele esetén a névnek az `.in-addr.arpa` karaktersorozatra kell végződnie. Végül válassza ki a *Zónatípust* – elsődleges (master) vagy másodlagos (slave) – (lásd: 22.2. ábra - DNS-kiszolgáló telepítése: DNS-zónák (347. oldal)). A meglévő zóna egyéb beállításainak módosításához kattintson a *Zóna szerkesztése* gombra. A zóna eltávolításához kattintson a *Zóna törlése* gombra.

22.2. ábra *DNS-kiszolgáló telepítése: DNS-zónák*



3 Az utolsó párbeszédablakban nyithatja meg a telepítés során aktivált tűzfal portjait a DNS-szolgáltatás számára a *Tűzfalport megnyitása* pont megjelölésével. Utána határozza meg, hogy a DNS-t el kell-e indítani (*Be* vagy *Ki*). Az LDAP-támogatás is aktiválható. Lásd: 22.3. ábra - DNS-kiszolgáló telepítése: A varázsló használatának befejezése (348. oldal).

22.3. ábra *DNS-kiszolgáló telepítése: A varázsló használatának befejezése*



22.3.2 Szakértői beállítások

A modul elindítása után a YaST megnyit egy ablakot, amely számos beállítási lehetőséget jelenít meg. A beállítások megadására létrejön egy DNS-kiszolgálókonfiguráció, amelynek a legfontosabb funkciói már működnek:

Indítás

Az *Indítás* részben lehet beállítani, hogy a DNS-kiszolgáló elinduljon-e rendszerindításkor, vagy kézzel legyen elindítva. A DNS-kiszolgáló azonnali elindításához nyomja meg a *DNS-kiszolgáló indítása most* gombot. A DNS kiszolgáló leállításához nyomja meg a *DNS-kiszolgáló leállítása most* gombot. Az aktuális beállítások mentéséhez nyomja meg a *Beállítások mentése és a DNS-kiszolgáló újraindítása most* gombot. A *Tűzfalport megnyitása* ablakban megnyitható a tűzfal DNS-portja, a *Tűzfalbeállítások* segítségével pedig módosíthatók a tűzfalbeállítások.

Az *LDAP-támogatás aktív* négyzet megjelölése esetén a zónafájlokat egy LDAP-adatbázis felügyeli. Az LDAP-adatbázisba írt zónaadat-módosításokat a DNS-kiszolgáló újraindításkor vagy a konfiguráció ismételt betöltésére való felszólításkor veszi át.

Továbbítók

Ha a helyi DNS-kiszolgáló nem tud megválaszolni egy kérést, akkor megpróbálja azt továbbítani egy *Továbbító* felé, amennyiben így lett beállítva. A továbbító kézzel vehető fel a *Továbbítók listája* részbe. Ha a továbbító nem statikusan van megadva (ilyen a helyzet például telefonos kapcsolatok esetében), akkor a konfigurációt a *netconfig* kezeli. További információ a netconfigról: `man 8 netconfig`. kiszolgáló

A legfontosabb beállítások

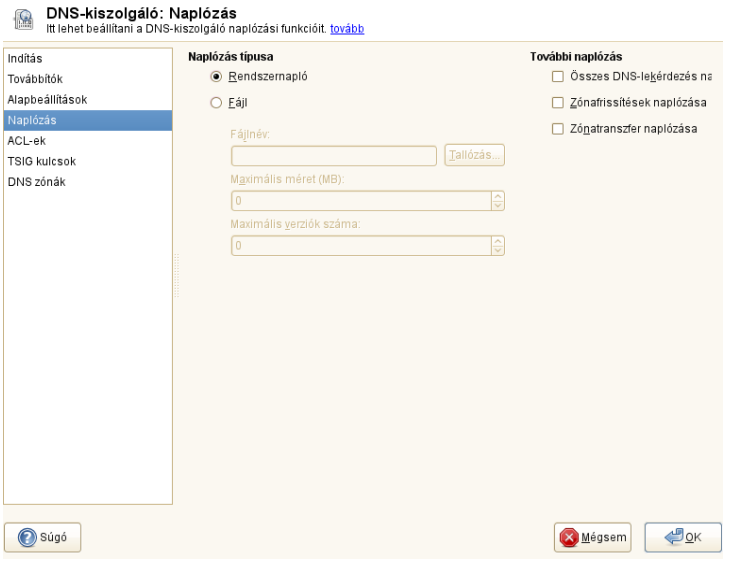
Ebben a részben adja meg a kiszolgáló legfontosabb beállításait. Az *Opciók* menüben válassza ki a kívánt elemet, majd a megfelelő beviteli mezőben adja meg az értékét. A *Hozzáadás* gomb megnyomásával vegye fel az új bejegyzést.

Naplózás

A *Naplózás* részben állítható be, hogy DNS-kiszolgáló mit naplózzon és hogyan. A *Naplózás típusa*alatt adja meg, hogy a DNS-kiszolgáló hova írja a naplóadatokat. A *Rendszernapló* kiválasztása esetén a `/var/log/messages` rendszerszintű naplófájl kerül használatra, vagy a *Fájl* gombbal megadható egy másik fájl. Az utóbbi esetben adja meg a maximális fájlméretet (megabájtban) és a tárolandó naplófájlok számát.

További lehetőségek a *További naplózás* részben érhetők el. Az *Összes DNS-lekérdezés naplózása* megjelölése esetén *minden* lekérdezés naplózásra kerül. Ebben az esetben a naplófájl nagyon nagyra nőhet. Éppen ezért a hibakeresést leszámítva nem túl jó ötlet a funkció bekapcsolása. A zónafrissítés során a DHCP- és DNS-kiszolgáló közötti adatforgalom naplózásához egedélyezze a *Zónafrissítések naplózása* lehetőséget. Az elsődleges és másodlagos kiszolgálók közötti zónatranszfer adatforgalmának naplózása a *Zónatranszferek naplózása* lehetőséggel engedélyezhető. Lásd: 22.4. ábra - DNS-kiszolgáló: Naplózás (350. oldal).

22.4. ábra *DNS-kiszolgáló: Naplózás*



ACL-ek használata

Ebben az ablakban lehet megadni a hozzáférési megszorítások betartatása érdekében ACL-eket (hozzáférés-vezérlési listákat). A *Név* mezőben adjon meg egy nevet, az *Érték* mezőben adjon meg egy IP-címet (hálózati maszkkal, vagy anélkül) az alábbi módon:

```
{ 10.10/16; }
```

A konfigurációs fájl szintaxisa megköveteli, hogy a cím pontosvesszővel végződjön és kapcsos zárójelek határolják.

TSIG-kulcsok

A TSIG-k (tranzakció-aláírások) fő célja a DHCP- és DNS-kiszolgálók közötti kommunikáció biztonságossá tétele. A TSIG-kulcsok bemutatása: 22.8. - Biztonságos tranzakciók (366. oldal)

TSIG-kulcs előállításához a *Kulcsazonosító* mezőben adjon meg egy egyedi nevet és adja meg a fájlt, amelyben a kulcsot tárolni kívánja (*Fájlnév*). A *Hozzáadás* gombra kattintva erősítse meg a beállításokat.

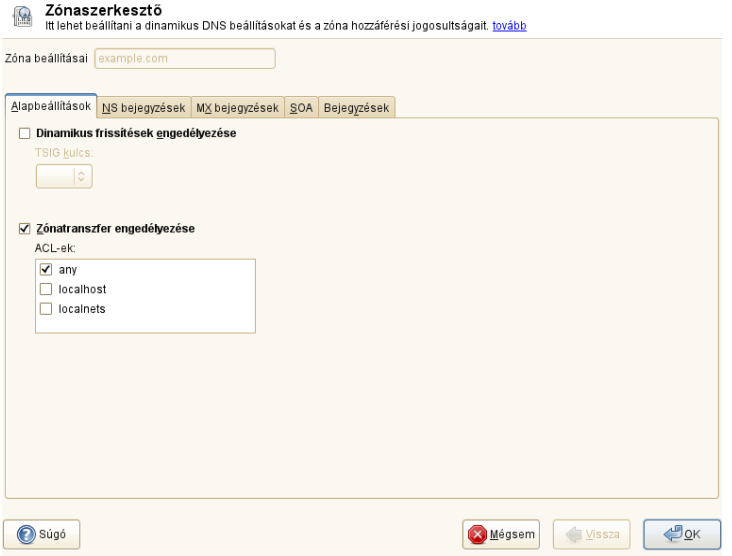
Egy már korábban létrehozott kulcs használatához hagyja üresen a *Kulcsazonosító* mezőt, majd a *Fájlnév* mezőben válassza ki a tároláshoz használt fájlt. Végül nyomja meg a *Hozzáadás* gombot.

Másodlagos zóna hozzáadása

Egy másodlagos zóna hozzáadásához válassza ki a *DNS zónák* részt, adja meg a zóna típusát *Másodlagos*, írja be az új zóna nevét, majd kattintson a *Hozzáadás* gombra.

A *Zónaszerkesztőben* az *Elsődleges (master) DNS-kiszolgáló IP* mezőben adja meg az elsődleges kiszolgálót, ahonnan a másodlagos kiszolgáló majd veszi az adatokat. A kiszolgáló hozzáférésének korlátozásához válassza ki a lista valamelyik ACL-jét. Lásd: 22.5. ábra - DNS-kiszolgáló: Másodlagos zóna szerkesztő (351. oldal).

22.5. ábra *DNS-kiszolgáló: Másodlagos zóna szerkesztő*



Elsődleges zóna hozzáadása

Egy elsődleges zóna hozzáadásához válassza ki a *DNS zónák* részt, adja meg a zóna típusát *Elsődleges*, írja be az új zóna nevét, majd kattintson a *Hozzáadás* gombra.

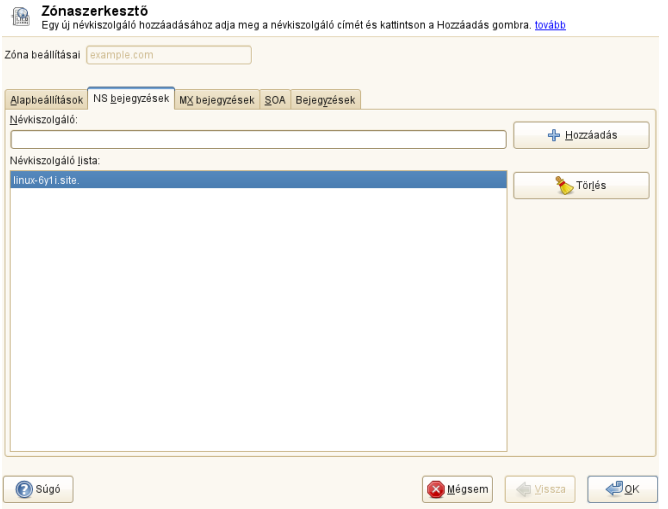
Elsődleges zóna módosítása

Egy elsődleges zóna módosításához válassza ki a *DNS zónák* részt, válassza ki a táblázatból az elsődleges zónát, majd kattintson a *Szerkesztés* gombra. A párbeszédablak több lapból áll: *Alapbeállítások* (ez jelenik meg elsőként), *NS bejegyzések*, *MX bejegyzések*, *SOA* és *Bejegyzések*.

Az Alapbeállítások párbeszédablakban válassza ki, hogy engedélyezi-e a zónatranszfereket. Annak megadásához, hogy ki tölthet le zónákat, válassza ki a megfelelő ACL-eket.

Zónaszerkesztő (NS bejegyzések)
: Ebben a párbeszédablakban alternatív névkiszolgálóneveket lehet megadni a megadott zónákhoz. Ellenőrizze, hogy a saját névkiszolgálónév benne van-e a listában. Egy bejegyzés hozzáadásához a *Névkiszolgáló* mezőben adja meg a nevét, majd nyomja meg a *Hozzáadás* gombot. Lásd: 22.6. ábra - DNS-kiszolgáló: Zónaszerkesztő (NS bejegyzések) (352. oldal).

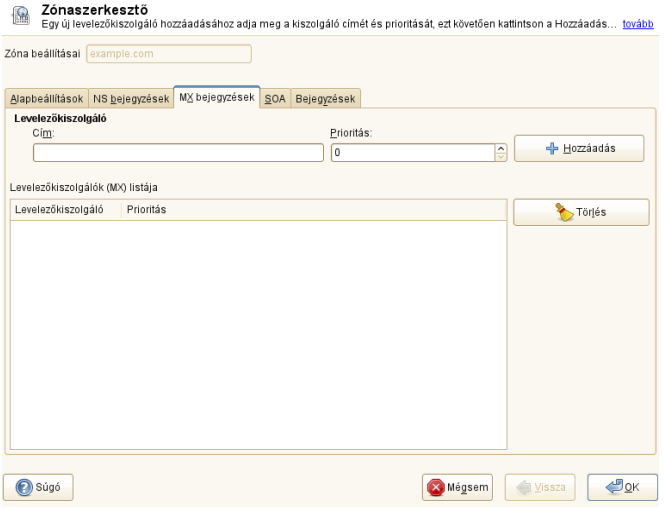
22.6. ábra *DNS-kiszolgáló: Zónaszerkesztő (NS bejegyzések)*



Zónaszerkesztő (MX bejegyzések)
: Ha fel kíván venni egy levelezőkiszolgálót az aktuális zóna meglévő listájába, akkor írja be a megfelelő címet és prioritásértéket. Ezután nyomja meg a *Hozzáadás*

gombot. Lásd: 22.7. ábra - DNS-kiszolgáló: Zónaszerkesztő (MX bejegyzések) (353. oldal).

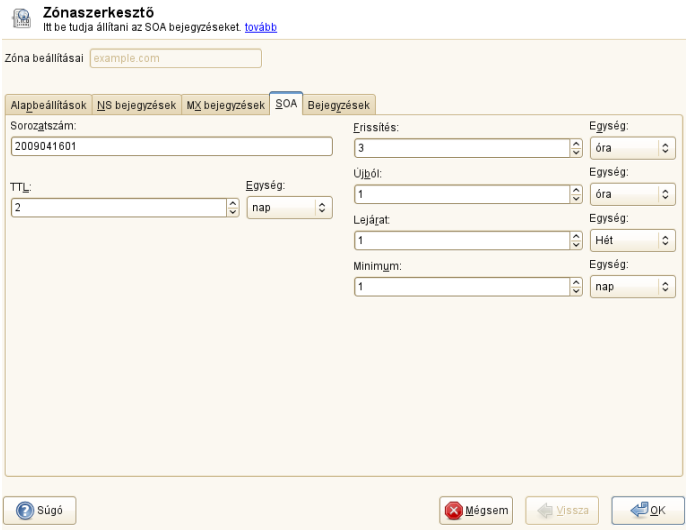
22.7. ábra *DNS-kiszolgáló: Zónaszerkesztő (MX bejegyzések)*



Zónaszerkesztő (SOA)

Ezen az oldalon lehet SOA (start of authority, jogosultság kezdete) bejegyzéseket létrehozni. Az egyes lehetőségek leírása: 22.6. példa - A /var/lib/named/example.com.zone fájl (361. oldal)

22.8. ábra *DNS-kiszolgáló: Zónaszerkesztő (SOA)*



Zónaszerkesztő (bejegyzések)
: Ebben a párbeszédablakban szabályozható a névfeloldás. A *Bejegyzés kulcsa* menüpontban adja meg a gépnevet, majd válassza ki a típusát. Az *A bejegyzés* a fő bejegyzést ábrázolja. Ennek értéke IP-cím kell, hogy legyen. A *CNAME* egy másodlagos név. A részletes vagy részleges bejegyzések esetén használja az *NS* vagy *MX* típust, amelyek az *NS bejegyzések* és *MX bejegyzések* lapokon megadott információt terjesztik ki. Ez a három típus egy meglévő A rekordra kerül feloldásra. A *PTR* a fordított zónákhoz való. Pont az `A` rekord fordítottja, például:

```
hostname.example.com. IN A 192.168.0.1
1.0.168.192.in-addr.arpa IN PTR hostname.example.com.
```

22.4 A BIND névkiszolgáló elindítása

Az openSUSE rendszeren a BIND (*Berkeley Internet name domain*) névkiszolgáló előre be van állítva, így akár közvetlenül a telepítés után gond nélkül elindítható. Ha már rendelkezik egy működő internetkapcsolattal és az `/etc/resolv.conf` fájlban a `localhost` bejegyzéshez beírta a `127.0.0.1` névkiszolgálócímet, akkor máris rendelkezik egy működő névfeloldással anélkül, hogy a szolgáltató DNS-ét ismerné. A BIND ekkor a névfeloldást a root névkiszolgálón keresztül hajtja végre, ez viszont

meglehetősen lassú folyamat. Célszerűbb beírni a szolgáltató DNS-kiszolgálójának címét az `/etc/named.conf` konfigurációs fájlba a `forwarders` részbe a hatékony és biztonságos névfeloldás biztosítása érdekében. Ha ez működik, akkor a névkiszolgáló *csak ideiglenesen tároló</emphasis> (caching-only)* névkiszolgálóként működik. Teljeskörű DNS-kiszolgálóvá akkor válik, ha beállít egy saját zónát. Egy egyszerű példa az `/usr/share/doc/packages/bind/config` könyvtárban található dokumentációban olvasható.

TIPP: A névkiszolgáló-adatok automatikus igazítása

Az internet- vagy hálózati kapcsolat típusától függően a névkiszolgáló adatai automatikusan a meglévő állapotokhoz igazíthatók. Ehhez állítsa az `/etc/sysconfig/network/config` fájlban lévő `MODIFY_NAMED_CONF_DYNAMICALLY` változót `yes` értékre.

Ne állítson be hivatalos tartományokat addig, amíg egy felelős intézmény ki nem osztja őket. Még ha rendelkezik is saját tartománnyal, ha azt a szolgáltató felügyeli, ne állítson be rá névfeloldást házon belül, mert akkor a BIND nem fogja továbbítani a kéréseket ehhez a tartományhoz. A szolgáltatónál lévő webkiszolgáló például ilyenkor nem lenne elérhető a tartományból.

A névkiszolgáló elindításához adja ki az `rcnamed start` parancsot `root` felhasználóként. Ha a „done” üzenet jelenik meg a jobb oldalon zölddel, a névkiszolgáló nevével, akkor az elindítás sikeresen megtörtént. A `host` vagy `dig` programok segítségével tesztelje azonnal a névkiszolgálót a helyi rendszeren, amelynek a `localhost` értéket kell visszaadnia alapértelmezett kiszolgálóként a `127.0.0.1` címmel. Ha nem ez a helyzet, akkor az `/etc/resolv.conf` valószínűleg helytelen névkiszolgáló-bejegyzést tartalmaz, vagy a fájl nem is létezik. Az első teszteléskor adja ki a `host 127.0.0.1` parancsot, amelynek mindig működnie kell. Ha hibaüzenetet kap, akkor az `rcnamed status` parancs segítségével nézze meg, hogy a kiszolgáló pillanatnyilag fut-e. Ha a névkiszolgáló nem indul el vagy nem a várt módon viselkedik, akkor ennek oka általában a `/var/log/messages` hibafájlban megtalálható.

Ha továbbítóként a szolgáltató névkiszolgálóját vagy egy a hálózaton már futó névkiszolgálót kívánja használni, akkor a `forwarders` alatt lévő `options` részbe írja be a megfelelő IP-címet vagy -címeket. A példában (22.1. példa - Továbbítási beállítások a named.conf fájlban (356. oldal)) látható címek helyett természetesen a valódi címeket kell használni. A bejegyzések az Ön beállításainak feleljenek meg.

22.1 példa *Továbbítási beállítások a named.conf fájlban*

```
options {
        directory "/var/lib/named";
        forwarders { 10.11.12.13; 10.11.12.14; };
        listen-on { 127.0.0.1; 192.168.1.116; };
        allow-query { 127/8; 192.168/16 };
        notify no;
        };
```

Az `options` bejegyzést a zóna, a `localhost` és `0.0.127.in-addr.arpa` bejegyzései követik. A `type hint` bejegyzésnek a „.” alatt mindig jelen kell lennie. A kapcsolódó fájlokat nem kell módosítani, működniük kell, ahogy vannak. Győződjön meg róla, hogy minden bejegyzést „;” (pontosvessző) zár le és a kapcsos zárójelek a megfelelő helyen vannak. Az `/etc/named.conf` konfigurációs fájl vagy a zónafájlok módosítása után az `rcnamed reload` parancs segítségével utasítsa a BIND-ot, hogy olvassa újra be őket. Ugyanez az eredmény érhető el, ha a névkiszolgálót leállítja, majd az `rcnamed restart` parancs segítségével újraindítja. Az `rcnamed stop` parancs segítségével a kiszolgáló bármikor leállítható.

22.5 Az /etc/named.conf konfigurációs fájl

A BIND névkiszolgáló a beállításait az `/etc/named.conf` fájl tárolja. A tartományok zónaadatai – a gépnevek, IP-címek stb. – külön fájlokban tárolódnak a `/var/lib/named` könyvtárban. Alább részletesen is leírjuk a fájl beállításait.

Az `/etc/named.conf` két fő területre oszlik. Az egyik, az `options` kulcsszóval kezdődő rész az általános beállításokat, a `zone` kulcsszóval kezdődő rész az egyes tartományok zónabejegyzéseit tartalmazza. A `logging` rész és az `acl` (hozzáférés-vezérlési lista) szakaszok nem kötelezők. A megjegyzéssorok `#` vagy `//` jellel kezdődnek. Az 22.2. példa - Egyszerű /etc/named.conf fájl (357. oldal) egy minimális `/etc/named.conf` fájlt mutat be.

22.2 példa *Egyszerű /etc/named.conf fájl*

```
options {
        directory "/var/lib/named";
        forwarders { 10.0.0.1; };
        notify no;
};

zone "localhost" in {
       type master;
       file "localhost.zone";
};

zone "0.0.127.in-addr.arpa" in {
        type master;
        file "127.0.0.zone";
};

zone "." in {
        type hint;
        file "root.hint";
};
```

22.5.1 A legfontosabb beállítási lehetőségek

directory "*fájlnév*";
: Azt a könyvtárat adja meg, amelyben a BIND a zónaadatokat tartalmazó fájlokat keresi. Ez általában a `/var/lib/named`.

forwarders { *ip-cím*; };
: Azokat a névkiszolgálókat adja meg (általában a szolgáltatóét), amelyhez a DNS-kéréseket továbbítani kell, ha közvetlenül nem oldhatók fel. Az *ip-cím* helyére írjon be egy IP-címet (hasonlót, mint a `192.168.1.116`).

forward first;
: Minden DNS-kérést előbb továbbít, mielőtt megpróbálná a root névkiszolgálók segítségével feloldani. Ha a `forward first` helyett `forward only` szerepel, akkor a kérések kizárólag továbbításra kerülnek, egyáltalán nem kerülnek elküldésre a root névkiszolgálókhoz. Ennek tűzfal használata esetén van kiemelt szerepe.

listen-on port 53 { 127.0.0.1; *ip-cím*; };
: Meghatározza, hogy a BIND melyik hálózati csatolón és porton fogadja a kliensкéréseket. A `port 53` értéket nem kell külön megadni, mivel az `53` az alapértelmezett port. A helyi géptől érkező kérések engedélyezéséhez írja be a `127.0.0.1`

címet. Ha ez a bejegyzés teljesen ki van hagyva, akkor alapértelmezés szerint az összes csatoló használatra kerül.

listen-on-v6 port 53 {any; };
: Azt adja meg, hogy a BIND melyik porton figyelje az IPv6-klienskéréseket. Az `any` egyetlen alternatívája a `none`. IPv6 esetén a kiszolgáló csak helyettesítő karakteres (wildcard) címeket tud fogadni.

query-source address * port 53;
: Ez a bejegyzés akkor szükséges, ha a tűzfal blokkolja a kimenő DNS-kéréseket. Ezt azt jelzi a BIND számára, hogy a kéréseket külsőleg az 53-as portról küldje el, ne az 1024 fölötti portokról.

query-source-v6 address * port 53;
: Azt adja meg, hogy a BIND melyik portot használja az IPv6-lekérdezésekhez.

allow-query { 127.0.0.1; *net*; };
: Megadja a hálózatokat, amelyről a kliensek DNS-kéréseket tudnak küldeni. A *net* bejegyzést cserélje le a `192.168.2.0/24` címhez hasonlóra. A végén szereplő `/24` a hálózati maszk rövid alakja, ebben az esetben a `255.255.255.0`.

allow-transfer ! *;;
: Azt szabályozza, hogy mely gépek kérhetnek zónatranszfert. Ebben a példában `! *` miatt minden kérés visszautasításra kerül. E bejegyzés nélkül korlátozás nélkül bárhonnan kérhető zónatranszfer.

statistics-interval 0;
: E bejegyzés hiányában a BIND a `/var/log/messages` fájlban óránként sok sornyi statisztikai bejegyzést állít elő. A statisztikák teljes elhagyásához állítsa az értéket 0-ra vagy adjon meg egy intervallumot percben.

cleaning-interval 720;
: Ez a paraméter azt szabályozza, hogy a BIND mennyi idő után ürítse ki az ideiglenes tárolóját. Minden ürítés egy bejegyzést hoz létre a `/var/log/messages` fájlban. Az idő percben van megadva. Az alapértelmezett érték 60 perc.

interface-interval 0;
: A BIND rendszeres időközönként végigkeresi a hálózati eszközöket, hiszen megjelenhetnek újak, vagy megszűnhetnek régiek. `0` érték megadása esetén ez nem

történik meg: a BIND csak az induláskor észlelt csatolókat figyeli. Ellenkező eseben megadható egy perc alapú intervallum. Az alapértelmezett érték hatvan perc.

notify no;
: A `no` érték azt jelzi, hogy más névkiszolgáló nem kap értesítést a zónaadatok módosításáról és a névkiszolgáló újraindításáról.

22.5.2 Naplózás

A BIND-ban részletesen megadható, hogy mi, hogyan és hova kerüljön naplózásra. Normális esetben az alapértelmezett beállítások megfelelők. A 22.3. példa - Bejegyzés a naplózás letiltásához (359. oldal) a bejegyzés legegyszerűbb formáját mutatja be, amely a naplózást teljesen letiltja.

22.3 példa *Bejegyzés a naplózás letiltásához*

```
logging {
        category default { null; };
};
```

22.5.3 Zónabejegyzések

22.4 példa *Az example.com zónabejegyzései*

```
zone "example.com" in {
      type master;
      file "example.com.zone";
      notify no;
};
```

A `zone` után adja meg az adminisztrálandó tartomány nevét (`example.com`), amelyet az `in` kulcsszó követ, valamint a lényeges beállítások blokkja zárójelek között (22.4. példa - Az example.com zónabejegyzései (359. oldal)). Egy *másodlagos zóna* megadásához állítsa a `type` paramétert `slave` értékre és adja meg a névkiszolgálót, amely `elsődleges` névkiszolgálóként felügyeli ezt a zónát (22.5. példa - example.net zónabejegyzése (360. oldal)). Ez az elsődleges kiszolgáló egy másik tartománynak lehet másodlagos névkiszolgálója.

22.5 példa *example.net zónabejegyzése*

```
zone "example.net" in {
      type slave;
      file "slave/example.net.zone";
      masters { 10.0.0.1; };
};
```

A zónaparaméterek:

type master;
: A `master` kulcsszó jelzi a BIND számára, hogy ezt a zónát ez a helyi névkiszolgáló kezeli. . Ehhez persze megfelelő formátumban létre kell hozni a zónafájlt.

type slave;
: Ez a zóna egy másik kiszolgálóról kerül áthozásra. Ez csak `elsődleges` kiszolgálókkal együtt használható.

type hint;
: A `.` zóna, amely `hint` típusú, a gyökér névkiszolgálók megadására szolgál. Ezt a zónadefiníciót nem kell módosítani.

`example.com.zone` vagy „slave/example.net.zone” fájl;
: Ez a bejegyzés azt a fájlt adja meg, amelyben a tartomány zónaadatai találhatók. Másodlagos névkiszolgálók esetében nem szükséges ez a fájl, mivel ezek az adatok más névkiszolgálótól érkeznek. Az elsődleges (master) és másodlagos (slave) fájlok megkülönböztetése érdekében a slave fájlokhoz használja a `slave` könyvtárat.

masters { *`kiszolgáló-ip-cím`*; };
: Ez a bejegyzés csak másodlagos zónákhoz szükséges. Megadja, hogy a zónafájlokat mely névkiszolgálóról kell átvinni.

allow-update {! *; };
: Ez a beállítás vezérli a külső írási hozzáférést, amely lehetővé teszi a kliensek számára DNS-bejegyzések létrehozását – biztonsági okokból ez általában nem kívánatos. E bejegyzés hiányában a zónafrissítés egyátalán nem lehetséges. A fenti bejegyzés ugyanezt eredményezi, mivel a `! * *` letiltja az ilyen műveleteket.

22.6 Zónafájlok

Kétféle típusú zónafájl létezik: az egyik IP-címeket rendel a gépnevekhez, a másik a fordítottját csinálja: gépnevet ad meg az IP-címhez.

TIPP: A pont karakter használata a zónafájlokban

A `.` karakternek fontos jelentése van a zónafájlokban. Ha a gépnevek lezáró `.` végződés nélkül vannak megadva, akkor kiegészülnek a zóna nevével. A teljes tartománynévvel megadott teljes gépneveknek `.` karakterrel kell végződniük, hogy a tartomány ne legyen még egyszer hozzájuk fűzve. A hiányzó vagy rossz helyen megadott pont eredményezi a névkiszolgáló konfigurációs hibáinak nagy részét.

Az első esetben tételezzük fel, hogy a `example.com.zone` zónafájl a `example.com` tartományért felelős (22.6. példa - A /var/lib/named/example.com.zone fájl (361. oldal)).

22.6 példa *A /var/lib/named/example.com.zone fájl*

```
1.  $TTL 2D
2.  example.com. IN SOA      dns  root.example.com. (
3.               2003072441  ; serial
4.               1D          ; refresh
5.               2H          ; retry
6.               1W          ; expiry
7.               2D )        ; minimum
8.
9.               IN NS       dns
10.              IN MX       10 mail
11.
12. gate         IN A        192.168.5.1
13.              IN A        10.0.0.1
14. dns          IN A        192.168.1.116
15. mail         IN A        192.168.3.108
16. jupiter      IN A        192.168.2.100
17. venus        IN A        192.168.2.101
18. saturn       IN A        192.168.2.102
19. mercury      IN A        192.168.2.103
20. ntp          IN CNAME    dns
21. dns6         IN A6  0    2002:c0a8:174::
```

1. sor:

   A `$TTL` az alapértelmezett TTL (time to live, élettartam) értéket adja meg, amely a fájl összes bejegyzésére érvényes. Ebben a példában a bejegyzések két napig érvényesek (`2 D`).

2. sor:

   Itt kezdődik a SOA vezérlőrekord:

   - Az adminisztrálandó tartomány neve az első pozícióban `example.com`. Ez `.`-ra végződik, mivel ellenkező esetben a zóna másodszor is hozzáfűzésre kerülne. Alternatívaként a `@` karakter is megadható itt, amely esetben a zóna az `/etc/named.conf` fájl megfelelő bejegyzéséből kerül kibontásra.

   - Az `IN SOA` után a zónáért felelős elsődleges (master) névkiszolgáló neve található. A `dns`-ről `dns.example.com`-ra egészül ki, mivel nem `.` karakterre végződik.

   - A névkiszolgálóért felelős személy e-mail címe következik. Mivel a `@` jel speciális jelentéssel rendelkezik, itt is `.` karaktert kell használni. A `root@example.com` esetén a bejegyzést `root.example.com.` formában kell megadni. A végén ki kell tenni a `.` karaktert, hogy a zóna ne kerüljön hozzáfűzésre.

   - A `(` és `)` közötti sorok a SOA rekordhoz tartoznak.

3. sor:

   A `sorszám` egy tetszőleges szám, amely a fájl minden módosításakor növekszik. Ennek segítségével informálhatók a másodlagos (slave) névkiszolgálók a módosításokról. A szokásos formátum egy tízjegyű dátum és egy növekvő sorozatszám együttese ÉÉÉÉHHNNSS formában.

4. sor:

   A `frissítési gyakoriság` (refresh rate) azt adja meg, hogy a másodlagos névkiszolgáló mennyi időnként ellenőrizze a zóna `sorszámát`. Ebben az esetben naponta.

5. sor:

   A `újrapróbálkozások gyakorisága` (retry rate) megadja, hogy a másodlagos kiszolgáló hiba esetén mennyi idő után kísérli meg újból az elsődleges kiszolgáló elérését. Itt két óra van beállítva.

6. sor:

A `lejárat ideje` (expiration time) azt az időkorlátot adja meg, amelynek eltelte után a másodlagos névkiszolgáló törli a gyorsítótárban tárolt adatokat, amennyiben nem tudja újból elérni az elsődleges kiszolgálót. Itt egy hét van beállítva.

7. sor:

A SOA rekord utolsó bejegyzése megadja a `negatív tárolási TTL` értékét – ez az az idő, ameddig a más kiszolgálóktól érkező, nem feloldott DNS-kérések eredményei tárolásra kerülnek.

9. sor:

Az `IN NS` sor a tartományért felelős névkiszolgálót adja meg. A `dns` kiegészül a `dns.example.com` címre, hiszen nem áll a végén `.` karakter. Több hasonló sor is lehet – egy az elsődleges, és egy-egy a másodlagos névkiszolgálókhoz. Ha az `/etc/named.conf` fájlban a `notify` paraméter értéke nem `no`, akkor az itt megjelenített névkiszolgálók értesítést kapnak a zónaadatok módosításáról.

10. sor:

Az MX bejegyzés a levelezőkiszolgálót adja meg, amely fogadja, feldolgozza és továbbítja az e-mail üzeneteket a `example.com` tartományhoz. Ebben a példában ez a `mail.example.com` gép. A gépnév előtti szám egy úgynevezett preferenciaérték. Ha több MX bejegyzés is van, akkor a legkisebb értékkel rendelkező levelezőkiszolgáló kapja meg először a levelet, de nem sikerül neki kézbesíteni, akkor a küldő a következő értékűvel próbálkozik.

12–19 sor:

Ezek maguk a címrekordok, amelyekben egy vagy több IP-cím van hozzárendelve gépnevekhez. A nevek itt `.` nélkül kerülnek megjelenítésre, mivel nem tartalmazzák a tartományt, így a `example.com` mindegyikhez hozzáfűzésre kerül. A `gate` géphez két IP-cím van hozzárendelve, mivel két hálózati kártyával rendelkezik. Ha a cím hagyományos (IPv4), akkor a rekord `A`-val van megjelölve. Ha a cím egy IPv6-cím, akkor a bejegyzés `A6 0`-val van megjelölve . Az IPv6-címekhez korábban az `AAAA` jelsort használták, de ez mára elavult.

MEGJEGYZÉS: IPv6-szintaxis

Az IPv6 bejegyzés szintaxisa valamelyest eltér az IPv4-étől. A töredezettség elkerülése érdekében kötelező információt adni a cím előtt a kihagyott bi-

tekről. Ezt az információt még akkor is meg kell adni, ha egy egyáltalán nem töredezett címet kíván használni. A következő szintaxisú AAAA bejegyzéshez

```
pluto IN            AAAA 2345:00C1:CA11:0001:1234:5678:9ABC:DEF0
pluto IN            AAAA 2345:00D2:DA11:0001:1234:5678:9ABC:DEF0
```

Információt kell adni a hiányzó bitekről IPv6-formátumban. Mivel a fenti példa teljes (egy bit sem hiányzik belőle), a bejegyzés A6-formátuma:

```
pluto  IN            A6 0 2345:00C1:CA11:0001:1234:5678:9ABC:DEF0
pluto  IN            A6 0 2345:00D2:DA11:0001:1234:5678:9ABC:DEF0
```

---

20. sor:

Az `ntp` másodlagos név használható a `dns` megcímzéséhez (a `CNAME` rövidítés a *canonical name*, azaz kanonikus névből származik).

Az `in-addr.arpa` pszeudotartomány használható a fordított kereséshez, ha IP-címek alapján keresünk gépneveket. Ez a cím hálózati részéhez kerül hozzáfűzésre fordított sorrendben. A `192.168` cím tehát a `168.192.in-addr.arpa` címmé alakítódik át. Lásd: 22.7. példa - Fordított keresés (364. oldal).

22.7 példa *Fordított keresés*

```
1.  $TTL 2D
2.  168.192.in-addr.arpa.   IN SOA dns.example.com. root.example.com. (
3.                          2003072441      ; serial
4.                          1D              ; refresh
5.                          2H              ; retry
6.                          1W              ; expiry
7.                          2D )            ; minimum
8.
9.                          IN NS           dns.example.com.
10.
11. 1.5                     IN PTR          gate.example.com.
12. 100.3                   IN PTR          www.example.com.
13. 253.2                   IN PTR          cups.example.com.
```

1. sor:

A $TTL az általános TTL-t adja meg, amely az összes itt szereplő bejegyzésre érvényes.

2. sor:

A konfigurációs fájlnak fordított keresést kell kezdenie a `192.168` hálózatra vonatkozóan. Mivel a zóna neve `168.192.in-addr.arpa`, ezért nem szabad

hozzáfűzni a gépnevekhez. Az összes gépnév teljes formában van megadva – tartománnyal és egy lezáró `.` karakterrel. A fennmaradó bejegyzések az előző `example.com` példában leírtaknak megfelelőek.

3–7. sor:
Lásd a `example.com` előző példáját.

9. sor:
Ez a sor újra a zónáért felelős névszert adja meg. Ebben az esetben a név teljes formában kerül megadásra a tartománnyal és `.` karakterrel a végén.

11–13. sor:
Ezek mutató bejegyzések, amelyek a megfelelő gépek IP-címeire mutatnak. A sor elején csak az IP-cím utolsó része van megadva, lezáró `.` karakter nélkül. A zóna hozzáadása (`.in-addr.arpa` nélkül) az összes IP-címet eredményezi, fordított sorrendben.

Normális esetben a BIND különböző verziói közötti zónatranszfernek probléma nélkül le kell zajlania.

22.7 A zónaadatok dinamikus frissítése

A *dinamikus frissítés* kifejezés egy olyan műveletre utal, amely hozzáadja, módosítja vagy törli az elsődleges kiszolgáló zónafájljaiban lévő bejegyzéseket. A mechanizmus leírását az RFC 2136 tartalmazza. A dinamikus frissítés minden zónabejegyzéséhez egyénileg kerül beállításra egy opcionális `allow-update` vagy `update-policy` szabály hozzáadásával. A dinamikusan frissített zónákat nem szabad kézzel szerkeszteni.

A frissítendő bejegyzések az `nsupdate` parancs segítségével továbbítódnak a kiszolgálóhoz. A parancs pontos szintaxisához tekintse meg az nsupdate kézikönyvoldalát (`man 8 nsupdate`). Biztonsági okokból az ilyen frissítést TSIG-kulcsok segítségével kell végrehajtani (lásd 22.8. - Biztonságos tranzakciók (366. oldal)).

22.8 Biztonságos tranzakciók

Biztonságos tranzakciók a tranzakciók aláírásával (TSIG) és megosztott titkos kulcsok alkalmazásával (TSIG-kulcsok) készíthetők. Ez a rész az ilyen kulcsok előállításának és használatának módját írja le.

A biztonságos tranzakciókra a különböző kiszolgálók közötti kommunikációhoz és a zónaadatok dinamikus frissítése érdekében van szükség. A kulcsokon alapuló hozzáférésvezérlés sokkal biztonságosabb, mint a csak IP-címekre épülő vezérlés.

Az alábbi parancs segítségével állítson elő egy TSIG-kulcsot (részletes leírásért tekintse meg a `man dnssec-keygen` parancs által megjelenített kézikönyvoldalt):

```
dnssec-keygen -a hmac-md5 -b 128 -n HOST host1-host2
```

Ez két fájlt hoz létre az alábbihoz hasonló névvel:

```
Khost1-host2.+157+34265.private Khost1-host2.+157+34265.key
```

A kulcs maga (például az `ejIkuCyyGJwwuN3xAteKgg==` karaktersorozat) mindkét fájlban megtalálható. A tranzakcióhoz a második fájlt (`Khost1-host2.+157+34265.key`) át kell vinni a távoli gépre, lehetőleg biztonságos módon (például scp segítségével). A `host1` és `host2` közötti biztonságos kommunikáció engedélyezéséhez a távoli kiszolgálón az `/etc/named.conf` fájlban meg kell adni a kulcsot:

```
key host1-host2. {
 algorithm hmac-md5;
 secret ";ejIkuCyyGJwwuN3xAteKgg==;
};
```

FIGYELEM: Az `/etc/named.conf` fájljogosultságai

Ellenőrizze, hogy az `/etc/named.conf` fájl jogosultságai megfelelően korlátozva vannak-e. A fájl alapértelmezett jogosultságértéke `0640`, a tulajdonos a `root`, a csoport pedig a `named`. Egy olyan megoldás is lehetséges, hogy a kulcsokat egy külön, korlátozott jogosultságokkal rendelkező fájlba helyezi, amely az `/etc/named.conf` fájlból kerül betöltésre. Egy külső fájl beágyazása:

```
include  "filename"
```

A `filename` helyére a kulcsokat tartalmazó fájl abszolút elérési útját kell beírni.

Annak engedélyezéséhez, hogy a `host1` kiszolgáló használhassa a kulcsot a `host2` kiszolgálóhoz (amely ebben a példában a `10.1.2.3` címmel rendelkezik), a kiszolgáló `/etc/named.conf` fájljának tartalmaznia kell az alábbi szabályt:

```
server 10.1.2.3 {
  keys { host1-host2. ;};
};
```

Hasonló bejegyzéseket a `host2` konfigurációs fájljába is kell írni.

A biztonságos tranzakciók kialakításához az IP-címekhez és -címtartományokhoz megadott ACL-eken (hozzáférés-vezérlési listák – nem összekeverendő a fájlrendszer ACL-ekkel) kívül TSIG-kulcsokat is meg kell adni. A megfelelő bejegyzés az alábbihoz hasonlóan néz ki:

```
allow-update { key host1-host2. ;};
```

A témakör részletesebb leírását a *BIND Administrator Reference Manual* `update-policy` része tartalmazza.

22.9 Biztonságos DNS

A DNSSEC (biztonságos DNS) leírását az RFC 2535 tartalmazza. A DNSSEC-hez rendelkezésre álló eszközöket a BIND kézikönyv tárgyalja.

Egy biztonságos zónának egy vagy több zónakulccsal kell rendelkeznie. Ezek a `dnssec-keygen` paranccsal generálhatók, a gépkulcsokhoz hasonlóan. A kulcsok a DSA titkosítási algoritmus segítségével készülnek. Az előállított nyilvános kulcsokat az `$INCLUDE` szabály segítségével a megfelelő zónafájlban kell megadni.

A `dnssec-makekeyset` parancs segítségével az előállított kulcsok egy halmazba kerülnek, amelyet azután biztonságos módon át kell küldeni a szülőzónához. A szülőn a halmaz a `dnssec-signkey` parancs segítségével íródik alá.. A parancs által előállított fájlokat ezután a zónák aláráírásához használja a rendszer a `dnssec-signzone` paranccsal, amely végül előállítja a fájlokat, amelyeket minden zóna `/etc/named.conf` fájljának tartalmaznia kell.

22.10 További információ

További információért tekintse meg a `bind-doc` csomag *BIND Administrator Reference Manual* című kézikönyvét, amely az `/usr/share/doc/packages/bind/` könyvtárban található. Érdemes elolvasni a kézikönyv által hivatkozott RFC-ket és a BIND man oldalait is. Az `/usr/share/doc/packages/bind/README.SuSE` fájl az openSUSE rendszeren működő BIND-kiszolgálóval kapcsolatos legfrissebb információt tartalmazza.

23

DHCP

A *dinamikus gépkonfigurációs protokoll* (dynamic host configuration protocol, DHCP) célja, hogy a hálózati beállítások központilag, egy kiszolgálóról kerüljenek kiosztásra ahelyett, hogy minden munkaállomást helyileg kellene beállítani. A DHCP használatára beállított gép nem tudja szabályozni a saját statikus IP-címét. Ehelyett a kiszolgáló útmutatásai szerint teljesen automatikusan beállítja magát. Ha a NetworkManagert használja a kliensoldalon, akkor a kliensen egyáltalán semmit nem kell beállítani. Ez akkor hasznos, ha folyamatosan változik a környezet, de egyszerre csak egy csatoló aktív. DHCP-kiszolgálót futtató gépen soha ne használja a NetworkManagert.

A DHCP használatának egyik módja, hogy a kiszolgáló minden klienst azonosít a hálózati kártya hardvercímével (amely a legtöbb esetben rögzített), majd csatlakozáskor ugyanazokat a beállításokat adja meg a kliens számára. A DHCP azonban úgy is beállítható, hogy a kiszolgáló dinamikusan rendeljen címet az egyes kliensekhez egy erre a célra lefoglalt címkészletből. Ez utóbbi esetben is, a DHCP-kiszolgáló minden kérés esetén megpróbálja mindig ugyanazt a címet rendelni a klienshez, még hosszabb idő eltelte után is. Ez természetesen csak akkor működik, ha a hálózatban nincs több kliens, mint cím.

Mindez azt jelenti, hogy a DHCP kétféleképpen is leegyszerűsítheti a rendszergazdák életét. A címekkel és hálózati konfigurációval kapcsolatos változtatások, a nagyobbak is, a kiszolgáló konfigurációs fájljának módosításával központilag elvégezhetők. Ez sokkal kényelmesebb, mint a munkaállomások egyenkénti átkonfigurálása. A gépek hálózatba szervezése is sokkal egyszerűbb, különösen az új gépeké, mivel ezek a címkészletből automatikusan kaphatnak IP-címet. A megfelelő hálózati beállítások lekérése a DHCP-kiszolgálótól különösen hasznos megoldás a folyton más és más hálózatokban használt noteszgépek esetén.

A jelen fejezetben a DHCP-kiszolgáló ugyanazon az alhálózaton fut, mint a munkaállomások (192.168.2.0/24) és 192.168.2.1 az átjáró. Fix IP-címe van (192.168.2.254) és két címtartományt szolgál ki: 192.168.2.10 – 192.168.2.20 és 192.168.2.100 – 192.168.2.200.

A DHCP-kiszolgáló a kliens számára nemcsak az IP-címet és a hálózati maszkot tudja kiosztani, hanem akár a gép- és tartománynevet, valamint az átjáró és a névkiszolgáló címét is. A DHCP lehetővé teszi számos további paraméter központi beállítását is. Be lehet állítani például egy időkiszolgálót, amelytől a kliensek lekérdezhetik az aktuális időt, vagy egy nyomtatókiszolgálót is.

23.1 DHCP-kiszolgáló beállítása a YaST segítségével

FONTOS: LDAP-támogatás

Az openSUSE jelen verziójában a YaST DHCP-modul beállítható úgy is, hogy a kiszolgáló konfigurációját helyileg tárolja (azon a gépen, amelyik a DHCP-kiszolgálót futtatja), de úgy is, hogy a konfigurációs adatokat egy LDAP-kiszolgáló kezelje. Ha LDAP-t kíván használni, akkor még a DHCP-kiszolgáló konfigurálása előtt állítsa be az LDAP-környezetet.

A YaST DHCP-moduljával saját DHCP-kiszolgáló állítható be a helyi hálózat számára. A modul használható egyszerű és szakértői módban is.

23.1.1 Kezdeti beállítás (varázsló)

A modul első használatakor egy beállító varázsló indul el, amelyben néhány alapvető döntést kell meghozni a kiszolgáló felügyeletével kapcsolatban. Ezzel a kezdeti beállítási folyamattal kialakítható egy alapszintű DHCP-kiszolgáló, amely a legfontosabb funkciókat biztosítja. A szakértői módban a speciálisabb beállítások is megadhatók.

A hálózati kártya kiválasztása
: Az első lépésben a YaST megkeresi a rendelkezésre álló hálózati csatolókat, majd megjeleníti őket egy listában. A listából válassza ki azt a csatolót, amelyen a DHCP-kiszolgálónak figyelnie kell, majd kattintson a *Hozzáadás* gombra. Ezután a tűzfal

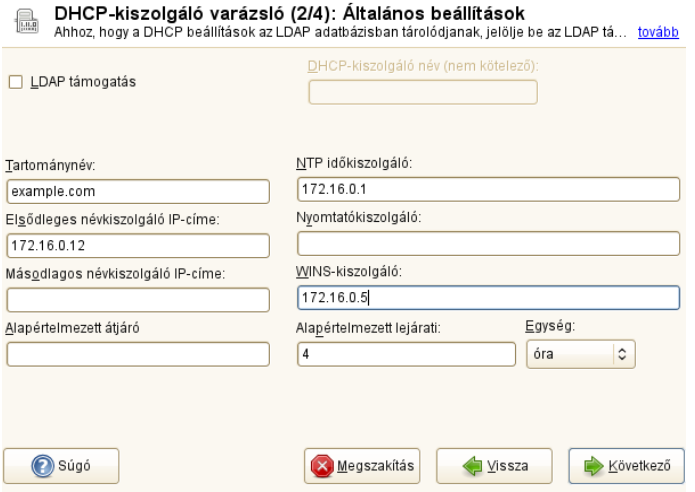
kinyitásához jelölje meg a *Tűzfal kinyitása a kijelölt csatolóhoz* lehetőséget. Lásd: 23.1. ábra - DHCP-kiszolgáló: A hálózati csatoló kiválasztása (371. oldal).

23.1. ábra *DHCP-kiszolgáló: A hálózati csatoló kiválasztása*

Általános beállítások

A jelölőnégyzettel adja meg, hogy a DHCP-beállítások automatikusan egy LDAP-kiszolgálón tárolódjanak-e. A beviteli mezőkben adja meg a DHCP-kiszolgáló által kezelendő összes kliens hálózati jellemzőit. Ezek a jellemzők a tartománynév, az időkiszolgáló címe, az elsődleges és másodlagos névkiszolgáló címe, a nyomtató- és WINS-kiszolgáló címe (Windows- és Linux-klienseket egyaránt tartalmazó vegyes hálózat esetén), az átjáró címe és a lejárati idő. Lásd: 23.2. ábra - DHCP-kiszolgáló: Általános beállítások (372. oldal).

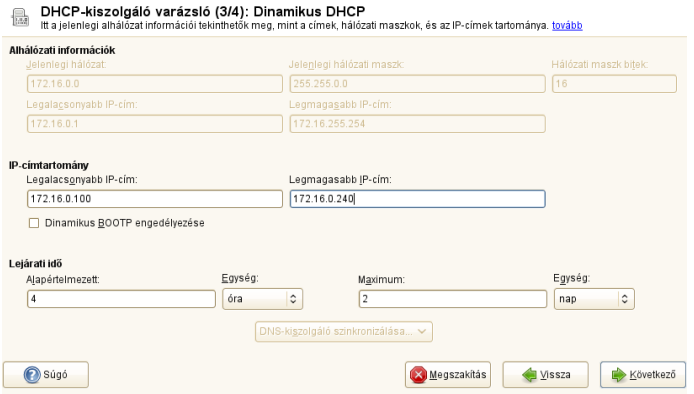
23.2. ábra *DHCP-kiszolgáló: Általános beállítások*



Dinamikus DHCP

Ebben a lépésben állíthatja be, hogy a dinamikus IP-cím hogyan legyen hozzárendelve a kliensekhez. Ehhez adjon meg egy IP-tartományt, amelyből a kiszolgáló címeket tud rendelni a DHCP-kliensekhez. Az összes címre ugyanannak a hálózati maszknak kell vonatkoznia. Adja meg a lejárati időt is, ameddig a kliens megtarthatja az IP-címet anélkül, hogy a használat hosszabbítását kellene kérnie. Nem kötelező, de a maximális lejárati idő is megadható – az az időtartam, ameddig a kiszolgáló fenntart egy IP-címet az adott kliens számára. Lásd: 23.3. ábra - DHCP-kiszolgáló: Dinamikus DHCP (373. oldal).

23.3. ábra *DHCP-kiszolgáló: Dinamikus DHCP*

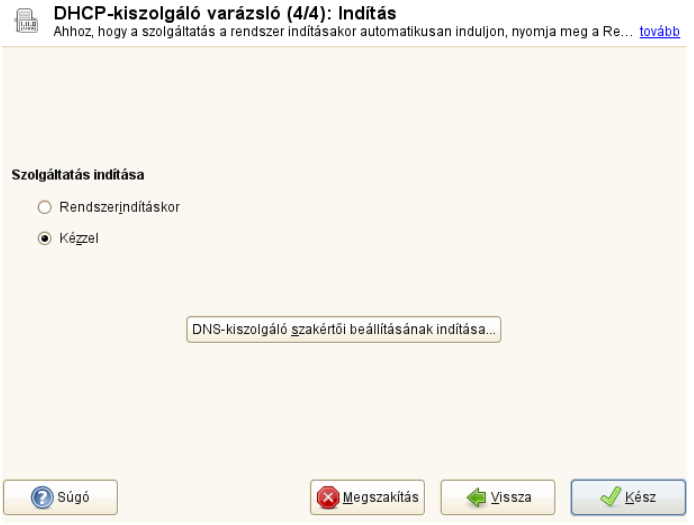


A beállítás befejezése és az indítási mód beállítása

A konfigurációs varázsló harmadik része után megjelenik az utolsó párbeszédablak, amelyben megadható, hogy a DHCP-kiszolgálót hogyan kell elindítani. Itt meghatározható, hogy a rendszer betöltése után a DHCP-kiszolgáló automatikusan elinduljon-e, vagy szükség esetén kézzel kell elindítani (például tesztelési célokból).

A kiszolgáló beállításának befejezéséhez kattintson a *Befejezés* gombra. Lásd: 23.4. ábra - DHCP-kiszolgáló: Indítás (373. oldal).

23.4. ábra *DHCP-kiszolgáló: Indítás*



23.2 DHCP-szoftvercsomagok

openSUSE alatt DHCP-kiszolgáló és DHCP-kliens egyaránt rendelkezésre áll. A rendelkezésre álló DHCP-kiszolgáló a dhcpd (az Internet Software Consortium tette közzé). A kliensoldalon válasszon a két különböző DHCP-kliensprogram közül: `dhcp-client` (szintén az ISC-től) és a DHCP kliensdémon a `dhcpcd` csomagban.

Az openSUSE alapértelmezés szerint a dhcpcd-t telepíti. A program kezelése nagyon egyszerű és a DHCP-kiszolgáló figyelése érdekében minden rendszerindításkor automatikusan elindításra kerül. Nincs szükség konfigurációs fájlra és a legtöbb szokásos kialakításban azonnal használható. Összetettebb helyzetekben használja az ISC dhcp-client-et, amelyet az `/etc/dhclient.conf` konfigurációs fájl vezérel.

23.3 A dhcpd DHCP-kiszolgáló

Minden DHCP-rendszer központi része a dinamikus gépkonfigurációs protokollt kezelő démon. A kiszolgáló *kiosztja* a címeket, majd az `/etc/dhcpd.conf` konfigurációs fájlban megadott beállításoknak megfelelően figyeli a használatukat. A fájlban lévő paraméterek és értékek módosításával a rendszergazda többféleképp befolyásolhatja a program viselkedését. A 23.1. példa - Az /etc/dhcpd.conf konfigurációs fájl (374. oldal) példa egy egyszerű `/etc/dhcpd.conf` példafájlt mutat be.

23.1 példa *Az /etc/dhcpd.conf konfigurációs fájl*

```
default-lease-time 600;         # 10 minutes
max-lease-time 7200;            # 2  hours

option domain-name "example.com";
option domain-name-servers 192.168.1.116;
option broadcast-address 192.168.2.255;
option routers 192.168.2.1;
option subnet-mask 255.255.255.0;

subnet 192.168.2.0 netmask 255.255.255.0
 {
  range 192.168.2.10 192.168.2.20;
  range 192.168.2.100 192.168.2.200;
 }
```

Ez az egyszerű konfigurációs fájl elegendő ahhoz, hogy a DHCP-kiszolgáló IP-címeket osszon ki a hálózatban. Figyeljen arra, hogy minden sor végén legyen pontosvessző, mivel ellenkező esetben a dhcpd nem lesz elindítva.

A példafájl három részre osztható. Az első megadja, hogy egy IP-cím alapértelmezés szerint hány másodpercig marad a kérő kliensnél (`default-lease-time`), mielőtt megújítást kéne alkalmazni. A szakasz a maximális időszakot is megadja, ameddig a gép a DHCP-kiszolgáló által hozzárendelt IP-címet megújítás kérése nélkül megtarthatja (`max-lease-time`).

A második részben néhány alapvető hálózati paraméter van megadva általánosságban:

- Az `option domain-name` sor a hálózat alapértelmezett tartományát adja meg.
- Az `option domain-name-servers` bejegyzéssel maximum három érték adható meg az IP-címeket gépnevekre (és vissza) alakító DNS-kiszolgálókhoz. Ideális eseten még a DHCP beállítása előtt kell beüzemelni egy névkiszolgálót a saját gépen vagy a hálózat egy másik részén. Célszerű, ha a névkiszolgáló egy gépnevet is megad minden dinamikus címhez és viszont. A névkiszolgáló beállításának leírása: 22. fejezet - *A DNS (tartománynévrendszer, Domain Name System)* (343. oldal).
- Az `option broadcast-address` sor adja meg a kérést küldő kliens által használandó üzenetszórási címet.
- Az `option routers` segítségével utasítható a kiszolgáló, hogy hova küldje az adatcsomagokat, amelyek nem kézbesíthetők a helyi hálózaton lévő gépnek (a megadott forrás- és célgépcímnek, valamint az alhálózati maszknak megfelelően). A legtöbb esetben, különösen kisebb hálózatokban, ez az útválasztó ugyanaz, mint az internetátjáró.
- Az `option subnet-mask` segítségével adja meg a klienshez rendelt hálózati maszkot.

A fájl utolsó részében a hálózatot lehet megadni, az alhálózati maszkot is beleértve. A befejezéshez adjon meg egy címtartományt, amelyből a DHCP-démon IP-címeket oszthat. A 23.1. példa - Az /etc/dhcpd.conf konfigurációs fájl (374. oldal) példában a kliensek `192.168.2.10` és `192.168.2.20`, valamint `192.168.2.100` és `192.168.2.200` közötti címet kaphatnak.

E pár sor módosítása után az `rcdhcpd start` paranccsal már aktiválható a DHCP-démon, amely azonnal használható. Az `rcdhcpd check-syntax` parancs segítségével hajtson végre egy rövid szintaxisellenőrzést. Ha váratlan problémákat észlel a konfigurációban – a kiszolgáló hibával leáll, vagy indításkor nem ad vissza `done` értéket –, akkor a `/var/log/messages` fő rendszernaplóban vagy a 10-es konzolon (Ctrl + Alt + F10) látható információ segítségével meg kell tudnia találni a hiba okát.

Egy alapértelmezett openSUSE rendszeren a DHCP-démon biztonsági okokból chroot környezetben indul el. A konfigurációs fájlokat át kell másolni a chroot környezetbe, hogy a démon meg tudja találni őket. Általában emiatt nem kell aggódni, mivel az `rcdhcpd start` parancs automatikusan átmásolja a fájlokat.

23.3.1 Statikus IP-címekkel rendelkező kliensek

Amint már említettük, a DHCP képes adott klienshez mindig ugyanazt az előre meghatározott, statikus címet rendelni. Az explicit módon kiosztott címeknek mindig prioritása van a tárolóból származó dinamikus címekkel szemben. Továbbá egy statikus cím nem jár le úgy, mint a dinamikus, vagyis ha például nem áll rendelkezésre elég cím, a kiszolgáló nem osztja ki másnak.

Egy statikus címmel rendelkező kliens azonosításához a dhcpd a hardvercímet használja, amely hálózati eszközök azonosítására szolgáló globálisan egyedi, hat hexadecimális számpárból álló rögzített numerikus kód (például `00:30:6E:08:EC:80`). Ha a megfelelő sorok (egy példa: 23.2. példa - A konfigurációs fájl kiegészítései (376. oldal), hozzáadásra kerülnek a korábbi példa 23.1. példa - Az /etc/dhcpd.conf konfigurációs fájl (374. oldal) konfigurációs fájljaihoz, akkor a DHCP-démon minden helyzetben ugyanazt az adathalmazt rendeli hozzá a megfelelő klienshez.

23.2 példa *A konfigurációs fájl kiegészítései*

```
host jupiter {
hardware ethernet 00:30:6E:08:EC:80;
fixed-address 192.168.2.100;
}
```

Az első sorban a megfelelő kliens (`host` *`gépnév`*, itt `jupiter`) a másodikban pedig a MAC-cím van megadva. Linux-gépeken ez a cím az `ip link show` parancs segít-

ségével határozható meg, amelyet a hálózati eszköz követ (például `eth0`). A kimenetnek az alábbihoz hasonlónak kell lennie:

```
link/ether 00:30:6E:08:EC:80
```

A fenti példában a `00:30:6E:08:EC:80` MAC-című hálózati kártyával rendelkező kliensnek a `192.168.2.100` IP-cím és a `jupiter` gépnév kerül automatikusan hozzárendelésre. A megadandó hardver típusa a legtöbb esetben `ethernet` , de az IBM rendszereken gyakran található `token-ring` is támogatott.

23.3.2 Az openSUSE verzió

A biztonság javítása érdekében az ISC DHCP-kiszolgáló openSUSE verzióját az Ari Edelkind által alkalmazott non-root/chroot javítással szállítjuk. Ez lehetővé teszi, hogy a dhcpd `nobody` felhasználói azonosítóval és chroot környezetben fusson (`/var/lib/dhcp`). Ehhez a `dhcpd.conf` konfigurációs fájlnak a `/var/lib/dhcp/etc` könyvtárban kell lennie. Az init parancsfájl indításkor automatikusan átmásolja az összes fájlt ebbe a könyvtárba.

Az `/etc/sysconfig/dhcpd` fájlban lévő bejegyzések segítségével szabályozható a kiszolgáló viselkedése e funkciót illetően. A dhcpd chroot környezet nélküli futtatásához a `DHCPD_RUN_CHROOTED` fájlban lévő `/etc/sysconfig/dhcpd` változót állítsa „no” értékre.

Ahhoz, hogy a dhcpd chroot környezetben futva is feloldhassa a gépneveket, további konfigurációs fájlokat is át kell másolni:

- `/etc/localtime`
- `/etc/host.conf`
- `/etc/hosts`
- `/etc/resolv.conf`

Ezek a fájlok az init parancsfájl indításakor átmásolódnak a`/var/lib/dhcp/etc/` könyvtárba. Ne feledkezzen meg ezen példányok megváltoztatásáról, ha szükség van rá, mert dinamikusan módosítják őket az `/etc/ppp/ip-up`-hoz hasonló parancsfájlok.

Nem kell ugyanakkor aggódni emiatt, ha a konfigurációs fájl csak IP-címeket ad meg (gépnevek helyett).

Ha a konfiguráció további, a chroot környezetbe átmásolandó fájlokat tartalmaz, akkor ezeket az `/etc/sysconfig/dhcpd` fájl `DHCPD_CONF_INCLUDE_FILES` változóiban kell megadni. Annak biztosításához, hogy a DHCP naplózási funkciója a syslog démon újraindítása után is működjön, az `/etc/sysconfig/syslog` fájlban a `SYSLOGD_ADDITIONAL_SOCKET_DHCP` alatt található plusz egy bejegyzés.

23.4 További információ

A DHCP-vel kapcsolatos további információ az *Internet Systems Consortium* webhelyén érhető el (`http://www.isc.org/products/DHCP/`). A `dhcpd`, `dhcpd.conf`, `dhcpd.leases` és `dhcp-options` kézikönyvoldala is biztosít hasznos tudnivalókat.

24 Időszinkronizálás NTP-vel

Az NTP (Network Time Protocol) a rendszer idejének hálózaton keresztüli szinkronizálására szolgáló protokoll. Az első lehetőség, hogy a gép lekéri az időt egy megbízható időforrásnak számító kiszolgálóról. A második lehetőség, hogy a gép maga is időforrásként működik a hálózat más számítógépei számára. Tehát az NTP feladata az abszolút idő fenntartása és a rendszeridő szinkronizálása a hálózat összes gépén.

A pontos rendszeridő fenntartása számos helyzetben fontos. A beépített hardveróra (BIOS) gyakran nem felel meg az alkalmazások – például adatbázisok – követelményeinek. A rendszeridő kézi javítása számos problémához vezethet, egy visszafelé ugrás például a kritikus alkalmazások hibás működését eredményezheti. A hálózatban általában az összes gép rendszeridejét szinkronizálni kell, de a kézi időbeállítás nem jó megközelítés. Az xntp megfelelő mechanizmust biztosít e problémák megoldásához. A hálózat megbízható időkiszolgálói segítségével folyamatosan kiigazítja a rendszeridőt. Lehetővé teszi továbbá a helyi referenciaórák – például rádióvezérelt órák – használatát.

24.1 NTP-kliens beállítása YaST segítségével

Az xntp előre megadott beállítása, hogy időreferenciaként a számítógép saját óráját használja. A BIOS-óra használata azonban csak tartalék megoldás arra az esetre, ha nem áll rendelkezésre pontosabb időforrás. A YaST megkönnyíti az NTP-kliens beállítását. Tűzfal nélküli rendszer esetén használja a gyors vagy a szakértői beállítást. Tűzfallal védett rendszer esetén a szakértői beállítás meg tudja nyitni a SuSEfirewall2 szükséges portjait.

24.1.1 Az NTP-kliens gyors beállítása

Az NTP-kliens gyors beállítása (*Hálózati szolgáltatások* > *NTP beállítás*) mindössze két párbeszédablakból áll. Az első párbeszédablakban állíthatja be az xntpd indítási módját és a lekérdezendő kiszolgálót. Ahhoz, hogy az xntpd a rendszerindításkor automatikusan elinduljon, kattintson a *Most és rendszerindításkor* menüpontra. Majd adja meg az *NTP-kiszolgáló beállítások* értékeit. A `0.opensuse.pool.ntp.org`, `1.opensuse.pool.ntp.org`, `2.opensuse.pool.ntp.org` vagy `3.opensuse.pool.ntp.org` előre ki van jelölve. Kattintson a *Véletlen kiszolgáló használata a pool.ntp.org-ból* pontra, ha nem akar előre megadott időkiszolgálót használni. Alternatív megoldásként kattintson a *Kiválasztás* gombra egy második párbeszédablak megjelenítéséhez, amelyben kiválaszthatja a hálózatnak legmegfelelőbb időkiszolgálót.

24.1. ábra *YaST: NTP-beállítások*

A legördülő *Kiválasztás* párbeszédablakban adja meg, hogy az időszinkronizálás a helyi hálózat időkiszolgálója (*Helyi NTP-kiszolgáló*) segítségével történjen, vagy egy, a helyi időzónát kezelő internetes időkiszolgálóval (*Nyilvános NTP-kiszolgáló*). Helyi időkiszolgáló esetén kattintson a *Kikeresés* menüpontra; ez elindít egy, a hálózat rendelkezésre álló időkiszolgálóira vonatkozó SLP-lekérdezést. A keresési eredmények listájában válassza ki a legmegfelelőbb időkiszolgálót és az *OK* gomb segítségével lépjen ki a párbeszédablakból. Nyilvános időkiszolgáló esetén a *Nyilvános NTP-kiszolgáló* alatti listában válassza ki az országot (az időzónát) és a megfelelő kiszolgálót, majd az *OK* gomb segítségével lépjen ki a párbeszédablakból. A fő párbeszédablakban a *Teszt* menüpont segítségével tesztelje a kiválasztott kiszolgáló rendelkezésre állását és a *Befejezés* menüponttal lépjen ki a párbeszédablakból.

24.1.2 NTP-kliens szakértői beállítása

Az NTP-kliens szakértői beállítása az *NTP beállítás* modul fő párbeszédablakában található *Szakértői beállítás* gombbal érhető el (24.1. ábra - YaST: NTP-beállítások (380. oldal)), miután a gyors beállításban leírt módon már kiválasztotta az indítási módot.

24.2. ábra *Szakértői NTP-beállítások: Általános beállítások*

Az NTP-kliens beállítható kézzel, de úgy is, hogy automatikusan lekérje a hálózatban elérhető NTP-kiszolgálók listáját DHCP-n keresztül. A *Beállítás DHCP-vel* pont megjelölése esetén az alábbi ismertetett kézi beállítások nem használhatók.

A kiszolgálók és a kliens egyéb lekérdezendő időforrásainak listája az *Általános beállítások* lapon látható. A *Hozzáadás*, *Szerkesztés* és *Törlés* gomb segítségével igény szerint módosíthatja a listát. A *Napló megtekintése* gomb megnyomására megtekinthetők a kliens naplófájljai.

Új időforrás hozzáadásához kattintson a *Hozzáadás* menüpontra. A következő párbeszédablakban válassza ki a forrás típusát, amellyel az időszinkronizációt végre kell hajtani. A következő lehetőségek használhatók:

Kiszolgáló
: Egy újabb párbeszédablakban (24.1.1. - Az NTP-kliens gyors beállítása (380. oldal)) kiválasztható az NTP-kiszolgáló. Jelölje meg az *Ezt a gépet használja kezdeti*

szinkronizációra négyzetet, ha azt kívánja, hogy rendszerindításkor a kiszolgáló és a kliens között az időadatok szinkronizálásra kerüljenek. Az *Opciók* menüpontban az xntpd további beállításai adhatók meg.

A *Hozzáférés-felügyeleti beállítások* részben korlátozható, hogy milyen műveleteket végezhet a távoli számítógép a démont futtató saját számítógépen. Ez a beállítás csak akkor érhető el, ha megjelölte az *NTP-szolgáltatás korlátozása csak a beállított kiszolgálókra* pontot a *Biztonsági beállítások* lapon. A beállítások az `/etc/ntp.conf` `restrict` szakaszainak felelnek meg. Például a `nomodify notrap noquery` megtiltja a kiszolgálónak, hogy módosíthassa a számítógép NTP-beállításait, és letiltja az NTP-démon trap (távoli eseménynaplózási) funkcióját. Ezeket a korlátozásokat célszerű beállítani az olyan gépeken, amelyeket nem teljes mértékben saját maga kezel (mert például kint vannak az interneten).

Részletes információ az `/usr/share/doc/packages/xntp-doc` (az `xntp-doc` csomag része) fájlban található.

Társkiszolgáló
: A társkiszolgáló (peer) egy olyan gép, amellyel szimmetrikus kapcsolat kerül kiépítésre: időkiszolgálóként és kliensként is működik. Ha egy kiszolgáló helyett társkiszolgálót kíván használni ugyanabban a hálózatban, akkor adja meg a megfelelő rendszer címét. A párbeszédablak további része megegyezik a *Kiszolgáló* párbeszédablakkal.

Rádióóra
: Ha a rendszerben rádióórát kíván használni az időszinkronizációhoz, akkor ebben a párbeszédablakban adja meg az óra típusát, az egység számát, az eszköz nevét és az egyéb beállításokat. Az illesztőprogram finomhangolásához válassza ki az *Illesztőprogram finomhangolása* lehetőséget. A helyi rádióórák működéséről részletes információt az `/usr/share/doc/packages/xntp-doc/refclock.html` fájl tartalmaz.

Nyilvános szórás (broadcast)
: Az időinformáció és a lekérdezések üzenetszórással (broadcast) is továbbíthatók a hálózatban. Ebben a párbeszédablakban adja meg a címet, amelyre a nyilvános üzeneteket küldeni kell. Csak akkor aktiválja a nyilvános szórást, ha van megbízható időforrás, mint amilyen például egy rádiós vezérlésű óra.

Nyilvános csomagok fogadása

Ha azt kívánja, hogy a kliens az információt nyilvános üzenetek formájában kapja meg, akkor ezekben a mezőkben adja meg a címet, amelyről a megfelelő csomagokat fogadni kell.

24.3. ábra *Szakértői NTP-beállítások: Biztonsági beállítások*

A *Biztonsági beállítások* lapon adja meg, hogy az xntpd démon "chroot jail"-módban induljon-e. Az *NTP démon futtatása Chroot környezetben* lehetőség alapértelmezésben aktív. Ez megnöveli a biztonságot egy xntpd-n keresztüli támadás esetén, mivel megakadályozza, hogy a támadó a teljes rendszert veszélyeztesse.

Az *NTP-szolgáltatás korlátozása csak a beállított kiszolgálókra* beállítás megnöveli a rendszer biztonságát, mivel megtiltja a távoli számítógépeknek, hogy megtekintsék és módosítsák a gép NTP-beállításait, illetve használják a távoli eseménynaplózási (trap) funkciót. Bekapcsolás után ezek a korlátozások minden távoli számítógépre vonatkozni fognak, hacsak felül nem írja az egyes gépek hozzáférés-vezérlési beállításait az *Álta-*

lános beállítások lap időforrás-listájában. Minden egyéb távoli számítógép számára csupán a helyi idő lekérdezése engedélyezett.

Engedélyezze a *Tűzfalport megnyitása* lehetőséget, ha a SuSEfirewall aktív (ez az alapértelmezett beállítás). Ha a portot zárva hagyja, akkor nem létesíthető kapcsolat az időkiszolgálóval.

24.2 Az xntp beállítása a hálózatban

Az időkiszolgáló használatának legegyszerűbb módja egy lekérdezhető időkiszolgáló paramétereinek beállítása. Ha például az `ntp.example.com` nevű időkiszolgáló elérhető a hálózatban, akkor adja hozzá a nevét az `/etc/ntp.conf` fájlhoz a következő sor hozzáfűzésével:

```
server ntp.example.com
```

Több időkiszolgáló hozzáadásához vegyen fel további sorokat a `server` kulcsszóval. Miután megtörtént az xntpd inicializálása az `rcntpd start` paranccsal, körülbelül egy óráig tart az idő stabilizálása. Létrejön egy úgynevezett csúszási (drift) fájl a helyi számítógépóra igazításához. A csúszási fájl segítségével kiszámítható a hardveróra szisztematikus hibája. A javítás azonnal alkalmazásra kerül, és a rendszeridő nagyobb stabilitását eredményezi.

Az NTP-mechanizmust a kliensek kétféleképp használhatják: Az első lehetőség, hogy a kliens rendszeres időközönként lekéri az időt egy ismert kiszolgálóról. Sok kliens esetén ez azonban nagyon nagy terhelést jelenthet a kiszolgáló számára. A második lehetőség, hogy a kliens a hálózat üzenetszóró időkiszolgálói által küldött NTP üzenetszórási üzenetekre vár. A megközelítés hátránya, hogy a kiszolgáló minősége nem ismert, és a rossz információt küldő kiszolgáló súlyos problémákat okozhat.

Ha az idő üzenetszórással kerül szétosztásra, akkor nincs szükség a kiszolgáló nevére. Ebben az esetben az `/etc/ntp.conf` konfigurációs fájlba írja be a `broadcastclient` sort. Egy vagy több ismert időkiszolgáló kizárólagos használatához a `servers` szóval kezdődő sorban adja meg ezeknek a nevét.

24.3 Helyi referenciaóra beállítása

Az xntp szoftvercsomag illesztőprogramokat tartalmaz helyi referenciaórák csatlakoztatásához. A támogatott órák listáját az `xntp-doc` csomag `/usr/share/doc/packages/xntp-doc/refclock.html` fájlja tartalmazza. Minden illesztőprogramhoz egy szám van rendelve. Az xntp-ben a tényleges beállítás pszeudo IP-címek segítségével történik. Az `/etc/ntp.conf` fájlban úgy vannak megadva az órák, mintha a hálózatban lennének. Erre a célra egy speciális IP-cím van hozzájuk rendelve `127.127.`*t*`.`*u* formátumban. A *t* az óra típusát jelzi és meghatározza, hogy mely illesztőprogram kerül alkalmazásra, az *u* pedig az egységet, amely meghatározza a használt felületet.

Az egyedi illesztőprogramok általában speciális paraméterekkel rendelkeznek, amelyek leírják a konfiguráció részleteit. Az `/usr/share/doc/packages/xntp-doc/drivers/driver`*NN*`.html` (amelyben az *NN* az illesztőprogramok száma) az adott óratípusról ad információt. A „8-as típusú” órához (soros csatolón keresztül használt rádiós óra) például szükség van egy kiegészítő módra, amely pontosabban leírja az órát. A Conrad DCF77 vevőmodulok módja az 5-ös. Ahhoz, hogy ez az óra legyen az elsődleges referencia, adja meg a `prefer` kulcsszót. A Conrad DCF77 vevőmodul teljes `server` sora az alábbi lenne:

```
server 127.127.8.0 mode 5 prefer
```

A többi óra ugyanezt a mintát követi. Az `xntp-doc` csomag telepítése után az `/usr/share/doc/packages/xntp-doc` könyvtárban rendelkezésre áll az xntp dokumentáció. Az `/usr/share/doc/packages/xntp-doc/refclock.html` fájl hivatkozásokat biztosít az illesztőprogram-paramétereket leíró oldalakhoz.

25 A NIS használata

Amint a hálózat egyre több UNIX-rendszere kíván hozzáférni a közös erőforrásokhoz, fontossá válik, hogy a felhasználói és csoportazonosítók a hálózat összes gépén megegyezzenek. A hálózatnak a felhasználók számára átlátszónak kell lennie: bármelyik gépet is használják, mindig ugyanabban a környezetben kell, hogy találják magukat. Ez a NIS és NFS szolgáltatások segítségével érhető el. Az NFS fájlrendszereket ajánl ki a hálózatban (27. fejezet - *Fájlrendszer megosztása NFS-sel* (435. oldal)).

A NIS (Network Information Service, hálózati információs szolgáltatás) egy adatbázis-szerű szolgáltatás, amely az `/etc/passwd`, `/etc/shadow` és `/etc/group` fájlok tartalmához biztosít hozzáférést a hálózatokban. A NIS más célokra is használható (például az `/etc/hosts` vagy `/etc/services` fájlok elérhetővé tételére), azonban ez a fejezet ezzel már nem foglalkozik. Az emberek gyakran *YP*-ként is emlegetik a NIS-t, mivel hasonlóan működik, mint egy hálózatos „szaknévsor” (Yellow Pages).

25.1 NIS-kiszolgálók beállítása

A NIS-információ szétosztásához a hálózaton használható egyetlen kiszolgáló (az úgynevezett *elsődleges*, vagy master), amely kiszolgálja az összes klienst, de használhatók másodlagos (slave) NIS-kiszolgálók is, amelyek az elsődlegestől kapott adatokat továbbítják a saját klienseik felé.

- Ha csak egy NIS-kiszolgálót akar beállítani a hálózaton, folytassa az 25.1.1. - Elsődleges NIS-kiszolgáló beállítása (388. oldal) résszel.

- Ha az elsődleges NIS-kiszolgáló adatait exportálnia kell a másodlagos kiszolgálók felé, akkor állítsa be az elsődleges kiszolgálót az 25.1.1. - Elsődleges NIS-kiszolgáló beállítása (388. oldal) részben leírt módon, majd állítsa be az alhálózatok másodlagos kiszolgálóit a 25.1.2. - Másodlagos NIS-kiszolgáló beállítása (393. oldal) részben leírt módon.

25.1.1 Elsődleges NIS-kiszolgáló beállítása

Egy elsődleges NIS-kiszolgáló beállítása az alábbi lépésekből áll:

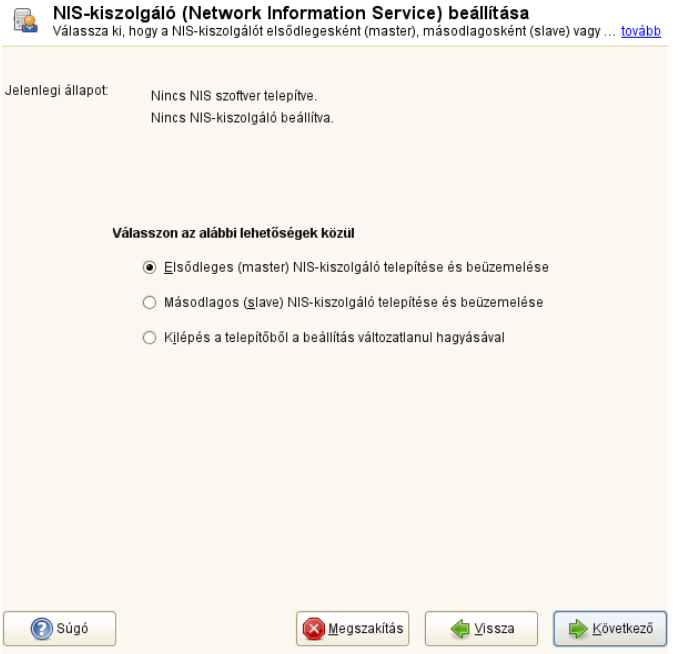
1. Indítsa el a *YaST* > *Hálózati szolgáltatások* > *NIS-kiszolgáló* modulját.

2. Ha csak egy NIS-kiszolgáló van a hálózatban, vagy ez a kiszolgáló lesz az elsődleges a többi másodlagos NIS-kiszolgáló számára, akkor válassza ki a *Elsődleges (master) NIS-kiszolgáló telepítése és beüzemelése* pontot. A YaST telepíti a szükséges csomagokat.

TIPP

Ha a NIS-kiszolgálószoftver már telepítve van a gépen, indítsa el az elsődleges NIS-kiszolgáló létrehozását az *Elsődleges (master) NIS-kiszolgáló létrehozása* pontra kattintással.

25.1. ábra *NIS-kiszolgáló beállítása*



3 Adja meg a legfontosabb NIS-jellemzőket:

3a Írja be a NIS-tartománynevet.

3b Adja meg, hogy a gép egyben NIS-kliens-e, vagyis a felhasználói bejelentkezhetnek és elérhetik a NIS-kiszolgáló adatait. Erre az *Ez a gép egyben NIS-kliens* beállítás szolgál.

Az *Engedélyezi a jelszavak megváltoztatását* pont kiválasztása esetén a hálózati felhasználók (a helyiek és a NIS-kiszolgáló által kezeltek egyaránt) módosíthatják jelszavaikat a NIS-kiszolgálón (az `yppasswd` paranccsal). Ennek hatására aktívvá válnak az *Engedélyezi a GECOS mező megváltoztatását* és az *Engedélyezi a bejelentkezési burok megváltoztatását* pontok. A „GECOS” azt jelenti, hogy a felhasználók a nevüket és címüket is módosíthatják az `ypchfn` paranccsal. A „SHELL” hatására a felhasználók módosíthatják az alapértelmezett parancsértelmezőjüket az `ypchsh` paranccsal; át-

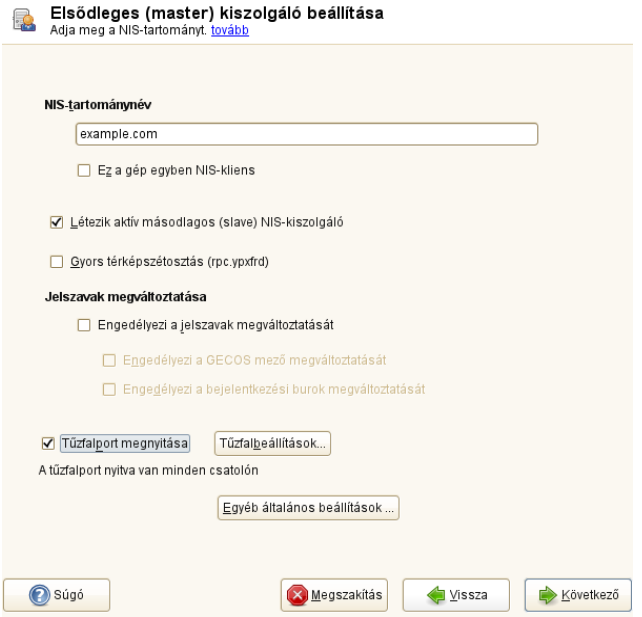
válthatnak például bash-ról sh-ra. Az új parancsértelmező az `/etc/shells` fájlban megadottak egyike kell, hogy legyen.

3c Ha a NIS-kiszolgáló más alhálózatok másodlagos kiszolgálóinak elsődleges kiszolgálójaként fog működni, akkor jelölje meg a *Létezik aktív másodlagos (slave) NIS-kiszolgáló* pontot.

A *Gyors térképszétosztás* beállítás csak a *Létezik aktív másodlagos (slave) NIS-kiszolgáló* használata esetén hasznos. Ez a beállítás felgyorsítja a térképek továbbítását a másodlagos kiszolgálókra.

3d A *Tűzfalport megnyitása* megjelölése esetén a YaST kinyitja a tűzfalat a NIS-kiszolgáló számára.

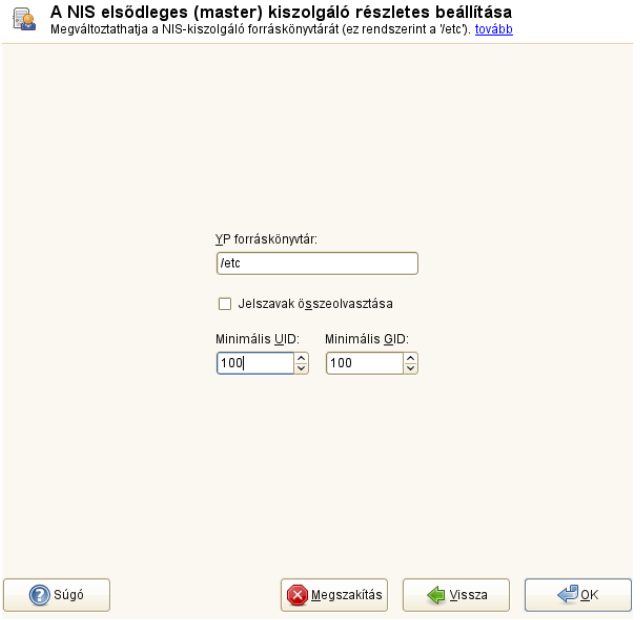
25.2. ábra *Elsődleges kiszolgáló beállítása*



3e Lépjen ki a párbeszédablakból a *Tovább* gombbal, vagy kattintson az *Egyéb általános beállítások* pontra a további beállítások elvégzéséhez. Az *Egyéb általános beállítások* közé tartozik a NIS-kiszolgáló forráskönyvtárának megváltoztatása (alapértelmezés szerint az `/etc`). Szintén itt fésülhetők

össze a jelszavak. Válassza az *Igen* lehetőséget a felhasználói adatbázis a rendszer hitelesítési fájljai (`/etc/passwd`, `/etc/shadow` és `/etc/group`) alapján előállításához. Szintén adja meg, hogy mi legyen a legkisebb felhasználó- és csoportazonosító, amelyet a NIS kioszt. Kattintson az *OK* gombra a beállítások érvényesítéséhez és az előző képernyőhöz visszatéréshez.

25.3. ábra *NIS-kiszolgáló könyvtárának megváltoztatása és fájlok szinkronizálása*

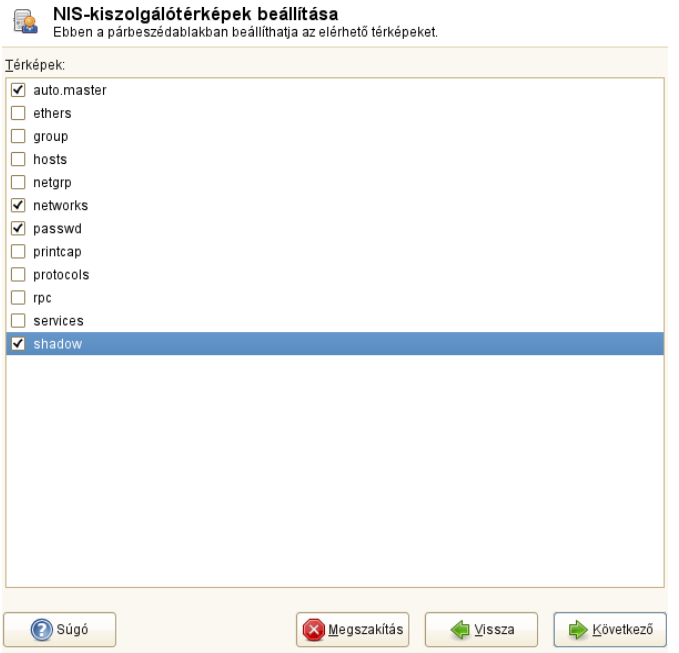


4 Ha előzőleg bekapcsolta a *Létezik aktív másodlagos (slave) NIS-kiszolgáló* beállítást, akkor most írja be a másodlagos gépek gépneveit, majd kattintson a *Tovább* gombra.

5 Ha nem használ másodlagos kiszolgálókat, akkor azok beállítása kimarad, és közvetlenül az adatbázis-beállító párbeszédablak következik. Itt adhatók meg a *térképek* (map), a NIS-kiszolgálóról a kliensre küldendő részleges adatbázisok. Az alapértelmezett beállítások általában megfelelők. Lépjen ki a párbeszédablakból a *Tovább* gombra kattintva.

6 Jelölje meg, mely térképek legyenek elérhetők, majd kattintson a *Tovább* gombra a folytatáshoz.

25.4. ábra *NIS-kiszolgáló térképek beállítása*

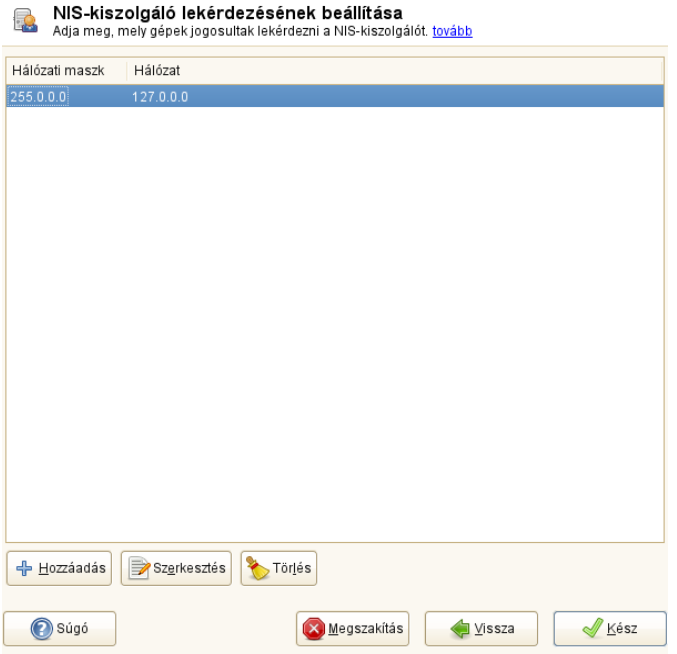


7 Adja meg a gépeket, amelyek jogosultak lekérdezni a NIS-kiszolgálót. A megfelelő gombokra kattintva veheti fel, módosíthatja és törölheti a gépeket. Adja meg, milyen hálózati kérések küldhetők el a NIS-kiszolgálónak. Általában ez a belső hálózat. Ebben az esetben a következő két bejegyzésnek kell látszania:

```
255.0.0.0       127.0.0.0
0.0.0.0         0.0.0.0
```

Az első bejegyzés engedélyezi a kapcsolatot magáról a gépről (a NIS-kiszolgálóról). A második engedélyezi az összes gép számára, hogy kéréseket küldjön a kiszolgálónak.

25.5. ábra *NIS-kiszolgáló kérési jogosultságok beállítása*



8 Kattintson a *Befejezés* gombra a módosítások elmentéséhez és a beállításokból kilépéshez.

25.1.2 Másodlagos NIS-kiszolgáló beállítása

További *másodlagos NIS-kiszolgálók* beállításához kövesse az alábbi lépéseket:

1 Indítsa el a *YaST* > *Hálózati szolgáltatások* > *NIS-kiszolgáló* modulját.

2 Válassza ki a *Másodlagos (slave) NIS-kiszolgáló telepítése és beállítása* pontot, majd kattintson a *Tovább* gombra.

TIPP

Ha a NIS-kiszolgálószoftver már telepítve van a gépen, akkor a másodlagos NIS-kiszolgáló létrehozásához kattintson a *Másodlagos (slave) NIS-kiszolgáló létrehozása* pontra.

3 Adja meg a másodlagos NIS-kiszolgáló legfontosabb beállításait:

3a Adja meg a NIS-tartományt.

3b Adja meg az elsődleges kiszolgáló gépnevét vagy IP-címét.

3c Jelölje meg az *Ez a gép egyben NIS-kliens* pontot, ha engedi kívánja a felhasználók bejelentkezését ezen a kiszolgálón.

3d Módosítsa a tűzfal beállításait a *Tűzfalport megnyitása* pont megjelölésével.

3e Kattintson a *Tovább* gombra.

4 Adja meg a gépeket, amelyek jogosultak lekérdezni a NIS-kiszolgálót. A megfelelő gombokra kattintva veheti fel, módosíthatja és törölheti a gépeket. Adja meg, milyen hálózati kérések küldhetők el a NIS-kiszolgálónak. Általában ez minden gép. Ebben az esetben a következő két bejegyzésnek kell látszania:

```
255.0.0.0     127.0.0.0
0.0.0.0       0.0.0.0
```

Az első bejegyzés engedélyezi a kapcsolatot magáról a gépről (a NIS-kiszolgálóról). A második bejegyzés engedi ugyanazon alháló minden gépe számára, hogy kéréseket küldjön a kiszolgálónak.

5 Kattintson a *Befejezés* gombra a módosítások elmentéséhez és a beállításokból kilépéshez.

25.2 NIS-kliensek beállítása

Annak beállítására, hogy a munkaállomás NIS-t használjon, a YaST *NIS-kliens* modulja szolgál. Adja meg, hogy a gép statikus IP-címmel rendelkezzen, vagy a DHCP által

kiadottat kapja. A DHCP a NIS-tartományt és a NIS-kiszolgálót is megadja. További információ a DHCP-ről: 23. fejezet - *DHCP* (369. oldal). Statikus IP-cím használata esetén adja meg a NIS-tartományt és a NIS-kiszolgálót kézzel. Lásd:25.6. ábra - NIS-kiszolgáló tartományának és címének beállítása (396. oldal). A *Keresés* hatására a YaST aktív NIS-kiszolgálót keres a teljes hálózaton. A helyi hálózat méretétől függően ez időigényes folyamat lehet. A *Nyilvános keresés (broadcast)* parancs NIS-kiszolgálót keres a helyi hálózaton, ha a megadott kiszolgálók nem tudnak válaszolni.

Több kiszolgáló is megadható, ha megadja *A NIS-kiszolgálók IP-címei* mezőben a címeket, szóközzel elválasztva.

A helyi telepített rendszertől függően az automounter aktiválására is szükség lehet. Ez a lehetőség szükség esetén további szoftvereket is telepít.

A szakértői beállításokban tiltsa le a *Válasz távoli gépeknek* lehetőséget, ha nem kívánja, hogy más gép le tudja kérdezni a kliens által használt kiszolgálót. A *Nem elérhető kiszolgáló* lehetőség megjelölése esetén a kliens válaszokat fogadhat jogosulatlan porton keresztül kommunikáló kiszolgálótól is. További információt a `man ypbind` paranccsal kaphat.

A beállítások megadása után kattintson a *Befejezés* gombra a beállítások mentéséhez és a YaST vezérlőközponthoz való visszatéréshez.

25.6. ábra *NIS-kiszolgáló tartományának és címének beállítása*

LDAP – címtárszolgáltatás

26

Az LDAP (Lightweight Directory Access Protocol, egyszerűsített címtárhozzáférési protokoll) egy címtárak, címjegyzékek elérésére és karbantartására szolgáló protokollcsalád. Az LDAP sokféle feladatra használható, például a felhasználók és csoportok felügyeletének központosítására, a rendszerkonfigurációs adatok kezelésének megkönnyítésére, vagy akár egyszerű címjegyzékek kezelésére. Ebben a fejezetben áttekintjük az LDAP működésének alapjait, valamint azt, hogy hogyan is kezelhetők egy LDAP-címtárban tárolt adatok a YaST segítségével. Az LDAP-protokollnak számos megvalósítása van, ez a fejezet azonban kizárólag az OpenLDAP megvalósítással foglalkozik.

Hálózati környezetben rendkívül nagy jelentőségű a fontos adatok szervezettségének fenntartása és gyors elérése. Ebben segít egy címtárszolgáltatás, amely – hasonlóan például a szaknévsorhoz – az adatokat jól szervezett, gyorsan kereshető formában teszi elérhetővé.

Ideális esetben egy központi kiszolgáló tárolja az adatokat egy címtárban és osztja szét a klienseknek egy meghatározott protokoll segítségével. Az adatok úgy vannak szervezve, hogy az alkalmazások széles skálája számára elérhetők legyenek. Nem kell tehát minden egyes naptárprogramhoz és e-mail klienshez külön adatbázist fenntartani – elegendő egyetlen, jól karbantartott központi adattárat használni. Így sokkal kisebb fáradsággal, sokkal pontosabban karbantarthatók az adatok. Az LDAP-hoz hasonló nyílt, szabványos protokollok használata segít abban, hogy a lehető legtöbb kliensalkalmazás képes legyen az adatok elérésére.

Címtár alatt egy gyors, kifejezetten a hatékony olvasásra és keresésre optimalizált adatbázistípust értünk:

- A sok egyidejű olvasási hozzáférés érdekében a frissítések száma általában nagyon alacsony az olvasási hozzáférésekhez képest, és az írási hozzáférés gyakran csekély számú frissítésre van korlátozva, csak az adminisztrációs jogokkal rendelkező felhasználók számára. Emlékeztetőül: a hagyományos adatbázisokat arra optimalizálják, hogy rövid idő alatt a lehető legnagyobb adatmennyiséget legyenek képesek fogadni.

- Statikus adatok karbantartásakor ritkán kell frissíteni a meglévő adatokat. Dinamikus adatok használatakor – különösen, ha például bankszámlákról vagy könyvelésről van szó – az adatok konzisztenciája az elsődleges szempont. Egy pénzügyi műveletnél például nem elég, hogy az egyik fél számláját ugyanannyival növeljük, mint amennyivel a másikét csökkentjük: a műveleteket egyidejűleg kell végrehajtani egy *tranzakción* belül az adatállomány egyensúlyának fenntartása érdekében. A hagyományos adatbázisok egyik legfontosabb funkciója az ilyen tranzakciók támogatása. Az LDAP-címtáraknál általában elfogadható az adatok rövid ideig tartó inkonzisztenciája. Az LDAP-címtáraknál nincsenek olyan szigorú konzisztencia-előírások, mint a relációs adatbázisoknál.

A címtárszolgáltatások – például az LDAP – felépítése nem az összetett frissítési vagy lekérdezési mechanizmusokra lett optimalizálva. A fő szempont a gyors és egyszerű hozzáférés biztosítása a szolgáltatást kérő alkalmazások számára.

26.1 LDAP vagy NIS?

A UNIX-rendszergazdák hagyományosan a NIS nevű szolgáltatást használják a névfeloldáshoz és az adatok szétosztásához a hálózatban. Az `/etc` könyvtárban lévő fájlok és a `group`, `hosts`, `mail`, `netgroup`, `networks`, `passwd`, `printcap`, `protocols`, `rpc` valamint `services` könyvtár konfigurációs adatait a klinesek osztják szét a hálózatban. Ezek a fájlok könnyedén karbantarthatók, hiszen egyszerű szövegfájlok. Nagyobb mennyiségű adat kezelése azonban jóval bonyolultabb, ugyanis a NIS-ben nincs különösebb strukturáltság. A NIS csak UNIX-platformokhoz készült. Ez azt jelenti, hogy nem alkalmas heterogén hálózatok központi adminisztrációs eszközének.

Szemben a NIS-sel, az LDAP szolgáltatás használata nem korlátozódik tisztán UNIX-hálózatokra. A windowsos kiszolgálók (a Windows 2000 óta) támogatják az LDAP felhasználását címtárszolgáltatásként. A fent említett alkalmazásfeladatok nem UNIX-rendszereken is támogatottak.

Az LDAP alapelve minden központilag felügyelendő adatstruktúrára alkalmazható. Néhány példaalkalmazás:

- Alkalmazás a NIS szolgáltatás kiváltására
- Levéltovábbítás (postfix, sendmail)
- Címjegyzék levelezőprogramokhoz (például Mozilla, Evolution vagy Outlook)
- BIND9 névkiszolgáló zónaleírásának adminisztrációja
- Felhasználóhitelesítés Samba segítségével heterogén hálózatokban

A lista szabadon bővíthető, ugyanis az LDAP, szemben a NIS-sel, szabadon kiterjeszthető. A világosan definiált adatstruktúra leegyszerűsíti a nagy adathalmazok kezelését azáltal, hogy könnyebbé és hatékonyabbá teszi a kereséseket.

26.2 Az LDAP-címtárfa szerkezete

Az LDAP-kiszolgáló működésének és az adattárolás módjának jobb megismeréséhez meg kell érteni a kiszolgáló adatszervezési módját, valamint azt, hogy a szerkezet segítségével az LDAP tudja biztosítani a szükséges adatok gyors elérését. Az LDAP-beállítás megfelelő működéséhez az alapvető LDAP-terminológiát ismernie kell. Ez a rész az LDAP-címtárfa alapvető elrendezését mutatja be, és bemutatja az LDAP-vel kapcsolatban használt legfontosabb kifejezéseket. Ha rendelkezik LDAP háttérismerettel, és csak az LDAP-környezet openSUSE rendszeren való beállításával kíván foglalkozni, akkor hagyja ki ezt a bevezető részt. Folytassa az olvasást a 26.3. - LDAP-kiszolgáló beállítása YaST segítségével (403. oldal) vagy 26.7. - LDAP-kiszolgáló beállítása kézzel (422. oldal) helyeken.

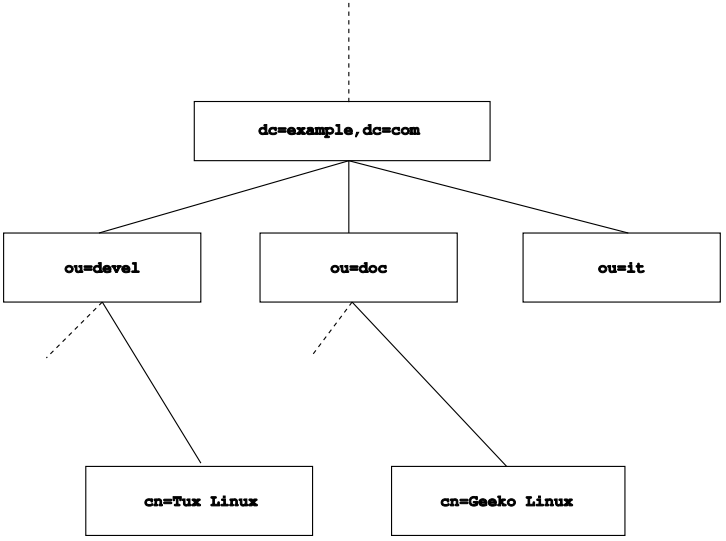
Az LDAP-címtárak faszerkezetre épülnek. A címtár minden bejegyzésének (objektumának) meghatározott helye van a hierarchiában. Ezt a hierarchiát az X.500 szabvány elnevezésével *címtárinformációs fának* (directory information tree, röviden DIT) hívjuk. A keresett bejegyzés teljes elérési útját, amely egyértelműen azonosítja, *megkülönböztetett névnek* vagy DN-nek (distinguished name) hívjuk. A bejegyzés elérési útja mentén lévő csomópontok neve *relatív megkülönböztetett név* vagy RDN (relative distinguished name). Az objektumok általában két fő típusba sorolhatók:

konténer (container)
: Ezek az objektumok maguk is tartalmazhatnak további objektumokat. Ilyen objektumosztályok a `root` (a címtárfa gyökéreleme, amely igazából nem is létezik), a `c` (ország), az `ou` (szervezeti egység) és a `dc` (tartománykomponens). A modell igazából nagyban hasonlít egy fájlrendszer könyvtáraira (mappáira).

levél (leaf)
: Ezek az objektumok egy ág legvégén helyezkednek el, alattuk már nincsenek további objektumok. Néhány példa: `person` (személy), `InetOrgPerson` (személy kifejezetten internetes és vállalati attribútumokkal) és `groupofNames` (nevek csoportja).

A címtárhierarchia legtetején a root gyökérelem található: `root`. Ennek alárendelt elemei a következők lehetnek: `c` (country, ország), `dc` (domain component, tartománykomponens) vagy `o` (organization, szervezet). Az LDAP-címtárfa felépítését sokkal egyszerűbb egy ábrán bemutatni: 26.1. ábra - Az LDAP-címtár szerkezete (400. oldal).

26.1. ábra *Az LDAP-címtár szerkezete*



Az ábrán egy képzeletbeli címtárinformációs fa látható. Három szinten láthatók bejegyzések. Minden bejegyzés a kép egy mezőjének felel meg. A képzeletbeli `Geeko Linux` nevű SUSE-alkalmazott teljes, érvényes *megkülönböztetett neve* ebben az

esetben `cn=Geeko Linux,ou=doc,dc=example,dc=com`. Ez úgy keletkezik, hogy a `cn=Geeko Linux` RDN-hez (relatív megkülönböztetett névhez) hozzáadjuk az előző bejegyzés megkülönböztetett nevét (`ou=doc,dc=example,dc=com`).

Azt, hogy milyen típusú objektumok tárolhatók a DIT-ben, a *séma* határozza meg. Az objektum jellegét pedig az *objektumosztály* határozza meg. Az objektumosztály definiálja, hogy egy adott objektumnak milyen kötelező és opcionális attribútumai vannak. A sémának tehát minden, a kívánt alkalmazási helyzetben használt objektumosztály és attribútum definícióját tartalmaznia kell. Létezik néhány általános séma (lásd: RFC 2252 és 2256). Az LDAP RFC definiál néhány általánosan használt sémát lásd pl. RFC 4519). Ezenfelül további sémák is elérhetők számos más alkalmazási helyzethez (pl. Samba, NIS helyettesítése stb.). Létrehozhatók azonban egyedi sémák is, illetve több, egymást kiegészítő séma is használható, ha ezt követeli meg a környezet, amelyben az LDAP-kiszolgálónak működnie kell.

A 26.1 táblázat - Általánosan használt objektumosztályok és attribútumok (401. oldal) táblázat röviden bemutatja a példában használt `core.schema` és `inetorgperson.schema` objektumosztályt, kötelező attribútumaikat és az attribútumok érvényes értékeit.

26.1. táblázat *Általánosan használt objektumosztályok és attribútumok*

Objektumosztály	Jelentés	Példabejegyzés	Kötelező attribútumok
dcObject	*domainComponent* (tartomány-névkomponensek)	pelda	dc
organizationalUnit	*organizationalUnit* (szervezeti egység)	doc	ou
inetOrgPerson	*inetOrgPerson* (intranetes vagy internetes személyes adatok)	Geeko Linux	sn és cn

A 26.1. példa - A schema.core kivonata (402. oldal) a sémadirektíva egy részét mutatja be, magyarázatokkal együtt (sorszámozás csak a magyarázat érdekében).

26.1 példa *A schema.core kivonata*

```
#1 attributetype (2.5.4.11 NAME ( 'ou' 'organizationalUnitName')
#2        DESC 'RFC2256: organizational unit this object belongs to'
#3        SUP name )

...
#4 objectclass ( 2.5.6.5 NAME 'organizationalUnit'
#5        DESC 'RFC2256: an organizational unit'
#6        SUP top STRUCTURAL
#7        MUST ou
#8 MAY (userPassword $ searchGuide $ seeAlso $ businessCategory
    $ x121Address $ registeredAddress $ destinationIndicator
    $ preferredDeliveryMethod $ telexNumber
    $ teletexTerminalIdentifier $ telephoneNumber
    $ internationaliSDNNumber $ facsimileTelephoneNumber
    $ street $ postOfficeBox $ postalCode $ postalAddress
    $ physicalDeliveryOfficeName
    $ st $ l $ description) )
    ...
```

A példában az `organizationalUnitName` attribútumtípust és a hozzá tartozó `organizationalUnit` objektumosztályt tekintjük meg. Az 1. sor az attribútum nevét, az egyedi OID-t (numerikus *objektumazonosító*) és az attribútum rövidítését tartalmazó OID.

A 2. sor egy rövid leírást ad az attribútumról a `DESC` kulcsszó után. Megemlíti a vonatkozó RFC-t, amelyre a definíció épül. A 3. sorban a `SUP` kulcsszó jelzi a felsőbb szintű attribútumtípust, amelyhez ez az attribútum tartozik.

Az `organizationalUnit` objektumosztály definíciója a 4. sorban kezdődik, ugyanúgy, mint az attribútum definíciójában, egy OID-vel és az objektumosztály nevével. Az 5. sor az objektumosztály rövid leírását tartalmazza. A 6. sor a `SUP top` bejegyzéssel jelzi, hogy ez az objektumosztály nem másik osztály alárendeltje. A 7. sor a `MUST` kulcsszótól kezdődően felsorolja az összes olyan attribútumtípust, amelyet az `organizationalUnit` típusú objektumok esetében kötelező megadni. A 8. sor a `MAY` kulcsszótól kezdődően megjeleníti az összes attribútumtípust, amely az objektumosztályban használható.

A sémák használatáról egészen kiváló bevezetést olvashat az OpenLDAP dokumentációjában. Ha a csomag már telepítve van, akkor a dokumentáció az `/usr/share/doc/packages/openldap2/admin-guide/index.html` fájlban tekinthető meg.

26.3 LDAP-kiszolgáló beállítása YaST segítségével

Az LDAP-kiszolgáló beállításához is használható a YaST. Az LDAP-kiszolgáló nemcsak a felhasználói fiók adatait tudja kezelni, hanem egyéb adatokat is – például a levelezés, vagy akár a DNS- és DHCP-kiszolgálók beállításait.

MEGJEGYZÉS: Az LDAP-objektumok nagybetűvel írása

A YaST LDAP-moduljai korábban nagybetűvel írták az összes létrehozott és megjelenített LDAP-objektum nevét. A YaST most már a névséma szerinti helyes jelölést alkalmazza.

26.2. ábra *YaST LDAP-kiszolgáló beállítás*

26.3. ábra *YaST LDAP-kiszolgáló – Új adatbázis*

Ha az LDAP-kiszolgálóval kívánja kezelni a felhasználói adatokat, akkor ellenőrizze, hogy telepítve van-e a `yast2-ldap-server` és `openldap2` csomag, illetve azok a csomagok, amelyektől függenek. Ezután folytassa az alábbi módon:

1. Jelentkezzen be `root` felhasználóként.
2. Indítsa el a YaST-ot és válassza ki a *Hálózati szolgáltatások* > *LDAP-kiszolgáló* részt a konfigurációs varázsló elindításához.
3. Adja meg az LDAP-kiszolgáló *Általános beállításait* (ezek a beállítások később módosíthatók, lásd: 26.2. ábra - YaST LDAP-kiszolgáló beállítás (403. oldal):
   - **3a** Adja meg, hogy az LDAP elinduljon-e.
   - **3b** Ahhoz, hogy az LDAP-kiszolgáló a szolgáltatásait SLP-n keresztül hirdesse meg, jelölje meg a *Regisztrálás egy SLP-démonnál* pontot.

3c Töltse ki a *Tűzfalbeállítások* részt.

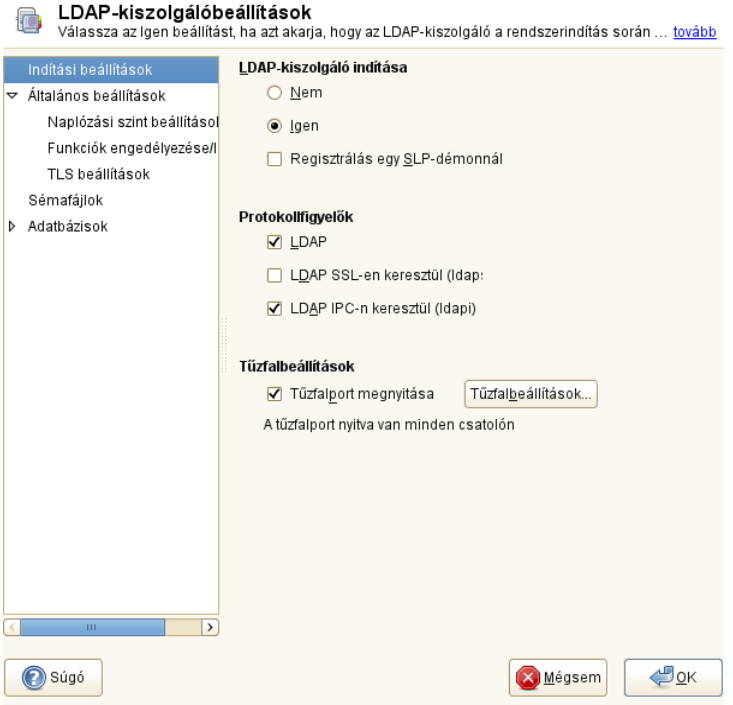
3d Kattintson a *Tovább* gombra.

4 Fontolja meg a *TLS engedélyezése* pont bekapcsolását. A TLS egy titkosítási technológia. További információ: 4. Lépés (407. oldal).

5 Ellenőrizze az *Adatbázis-beállításokat*, töltse ki az *LDAP adminisztrátori jelszó* értékét, majd kattintson a *Tovább* gombra – lásd: 26.2. ábra - YaST LDAP-kiszolgáló beállítás (403. oldal).

6 Ellenőrizze az *LDAP-kiszolgálóbeállításokat*, majd nyomja meg a *Befejezés* gombot a konfigurációs varázslóból kilépéshez.

26.4. ábra *YaST LDAP-kiszolgáló beállítás*



A módosításhoz vagy további beállításokhoz indítsa el újra az LDAP-kiszolgáló modult, majd az albejegyzések megnyitásához bontsa ki az *Általános beállítások* részt, a bal képernyőrészben – lásd: 26.4. ábra - YaST LDAP-kiszolgáló beállítás (405. oldal):

1. A *Naplózási szint beállítások* részben adja meg, hogy az LDAP-kiszolgáló milyen részletességgel naplózzon. A listából válassza ki az igényeknek legmegfelelőbb naplózási beállításokat. Minél több dolgot kapcsol be, annál nagyobbra fognak nőni a naplófájlok.

2. A *Funkciók engedélyezése/letiltása* részben határozza meg, hogy az LDAP-kiszolgáló milyen kapcsolattípusokat engedjen meg. Az alábbiak közül választhat:

   LDAPv2 kötési (bind) kérések
   : Ez az beállítás engedélyezi a kliens felől a protokoll előző verziójának (LDAPv2) használatával érkező kapcsolatkéréseket (bind kérések).

   Anonymous kötés ha a hitelesítési adatok nem üresek
   : Az LDAP-kiszolgáló alapesetben elutasít minden üres hitelesítési adatokkal (DN vagy jelszó) érkező hitelesítési kísérletet. A beállítás engedélyezése azonban lehetővé teszi a csatlakozást jelszóval, DN nélkül anonim kapcsolat létesítéséhez.

   Nem hitelesített kötés ha a DN nem üres
   : E pont megjelölése esetén lehetőség lesz hitelesítés nélkül (anonim módon) csatlakozni, DN megadásával, de jelszó nélkül.

   Feldolgozandó nem hitelesített frissítési műveletek
   : E pont megjelölése esetén a nem hitelesített frissítési műveletek is engedélyezettek. A hozzáférést ACL-ekkel és más szabályokkal kell korlátozni (lásd: 26.7.1. - Az slapd.conf általános direktívái (422. oldal)).

3. Ezután a *Funkciók engedélyezése/letiltása* részben adja meg, hogy az LDAP-kiszolgáló milyen jelzőket ne engedjen. Az alábbiak közül választhat:

   Anonymous kötési kérés elfogadása

   Egyszerű kötés hitelesítésének letiltása

   Anonymous-állapot kikényszerítésének tiltása StartTLS művelet fogadásakor

   StartTLS műveletek tiltása hitelesítés után

4 A kliens és a kiszolgáló közötti biztonságos kommunikáció beállításához folytassa a *TLS beállítások* résszel:

4a Jelölje meg a *TLS engedélyezése* pontot a kliens és a kiszolgáló közötti kommunikációban a TLS és SSL protokollok engedélyezéséhez.

4b Vagy a *Tanúsítvány importálása* részben adja meg a tanúsítvány pontos elérési útját, vagy engedélyezze az *Általános kiszolgálótanúsítvány használatát*. Ha az *Általános kiszolgálótanúsítvány használata* nem lehetséges, mert a telepítés során nem lett generálva, akkor először a *CA-kezelőmodul elindítása* résszel kell kezdeni – további információ: 35.2. - YaST CA-felügyeleti modulok (558. oldal).

A párbeszédablak bal részén látható *Sémafájlok* részt kiválasztva veheti fel a kiszolgáló konfigurációjában alkalmazandó sémafájlokat. Az alapértelmezett sémafájlok használata esetén a kiszolgáló a YaST felhasználóifiók-adatok forrásaként működhet.

A YaST lehetővé teszi a hagyományos sémafájlok használatát (ezek általában `.schema` kiterjesztésűek), illetve az OpenLDAP LDIF sémaformátumát követő, sémadefiníciókat tartalmazó LDIF fájlok használatát.

26.5. ábra *YaST LDAP-kiszolgáló beállítás*

Az LDAP-kiszolgáló által kezelt adatbázisok beállítása:

1. Válassza ki a párbeszédablak bal részében látható *Adatbázisok* pontot.

2. Kattintson az *Adatbázis hozzáadása* pontra az új adatbázis hozzáadásához.

3. Adja meg a szükséges adatokat.

   Alap (base) DN
   : Adja meg az LDAP-kiszolgáló alap DN-jét.

   Adminisztrátori DN
   : Írja be a kiszolgálóért felelős rendszergazda DN-jét. Ha megjelöli az *és* pontot, akkor csak a rendszergazda `cn`-jét kell megadni, a többit a rendszer automatikusan hozzáfűzi.

LDAP adminisztrátori jelszó
: Adja meg a rendszergazda jelszavát.

Adatbázis használata alapértelmezettként az OpenLDAP-kliensek számára
: Ha kívánja, megjelölheti a kényelem érdekében ezt a pontot is.

4 A következő párbeszédablakban kapcsolja be a jelszókezelési irányelvek használatát az LDAP-kiszolgáló extra védelme érdekében:

4a Jelölje meg a *Jelszóirányelvek engedélyezése* pontot. Ezután megadhat jelszóirányelveket.

4b Jelölje meg a *Nyíltszöveges jelszavak kivonatolása* pontot, ha azt szeretné, hogy a jelszavak hozzáadásakor vagy módosításakor, a nyílt szövegben megadott jelszavakból az adatbázisba írás előtt képződjön egy kivonat.

4c A *"Fiók zárolása" állapot megjelenítése* egy hasznos hibaüzenetet eredményez, ha zárolt fiókok nevében érkeznek kapcsolódási kérések.

FIGYELEM: Zárolt fiókok nagy biztonságot igénylő környezetekben

Ne használja a "*Fiók zárolása*" *állapot megjelenítése* beállítást, ha a környezet magas biztonsági fokot igényel, mivel a „Zárolt fiók” hibaüzenet olyan bizalmas adatokat tartalmazhat, amellyel egy potenciális támadó visszaélhet.

4d Adja meg az alapértelmezett irányelvobjektum DN-jét. Adja meg a DN-t, ha nem a YaST által javasoltat kívánja használni. Ellenkező esetben fogadja el az alapértelmezett beállításokat.

5 Fejezze be az adatbázis beállítását a *Befejezés* gombra kattintással.

Ha nem akar használni jelszóirányelveket, akkor a kiszolgáló ezen a ponton már készen is áll a működésre. Ha beállította a jelszóirányelvek használatát, akkor folytassa a jelszóirányelvek részletes beállításával. Ha egy olyan jelszóirányelv-objektumot választott ki, amelyik még nem létezik, akkor a YaST létrehoz egyet:

1 Adja meg az LDAP-kiszolgáló jelszavát. Az *Adatbázisok* alatti navigációs fában bontsa ki az adatbázis-objektumot, és jelölje meg a *Jelszóirányelv beállítása* pontot.

2 Győződjön meg róla, hogy a *Jelszóirányelvek engedélyezése* pont meg van jelölve. Ezután kattintson az *Irányelv szerkesztése* pontra.

3 Állítsa be a jelszómódosítási irányelveket:

3a Adja meg, hány jelszó tárolódjon a jelszó előzményeiben. Az elmentett jelszavak nem használhatók.

3b Adja meg, hogy a felhasználók módosíthatják-e a jelszavaikat, illetve hogy kötelező-e módosítaniuk a jelszavaikat, ha azt a rendszergazda alaphelyzetbe állította. Opcionálisan beállítható az is, hogy a jelszómódosításnál meg kelljen-e adni a régi jelszót.

3c Adja meg, hogy a jelszavak minőségét vizsgálja-e, és ha igen, milyen mértékben vizsgálja a rendszer. Adja meg a minimális jelszóhosszat (ellenkező esetben a jelszó nem érvényes). Ha megjelöli az *Ellenőrizhetetlen jelszavak elfogadása* pontot, akkor a felhasználók használhatnak titkosított jelszavakat, de ilyenkor a minőségellenőrzés nem végezhető el. Ha a *Csak ellenőrzött jelszavak elfogadása* pontot jelöli meg, akkor csak a minőségellenőrzésen átment jelszavak lesznek érvényesek.

4 Állítsa be a jelszavak elévülésére vonatkozó irányelveket:

4a Határozza meg a jelszavak minimális korát (ennyi időnek muszáj eltelnie két érvényes jelszóváltás között) és a jelszavak maximális korát.

4b Adja meg, hogy mennyi idővel korábban figyelmeztessen a rendszer a jelszó tényleges lejáratára.

4c Adja meg, hányszor lehet használni egy lejárt jelszót, mielőtt az visszavonhatatlanul lejárna.

5 Állítsa be a zárolási irányelveket:

5a Kapcsolja be a jelszavak zárolását.

5b Adja meg, hány sikertelen kapcsolódás után zárolódjon a jelszó.

5c Adja meg a jelszózárolás időtartamát.

5d Határozza meg, hogy mennyi ideig tárolódjanak a jelszóhibák a gyorsítótárban, mielőtt törlődnének.

6 Érvényesítse a jelszóirányelv-beállításokat az *OK* gombra kattintással.

Egy már korábban létrehozott adatbázis módosításához válassza ki annak alap DN-jét a bal oldali fából. Az ablak jobb oldalán a YaST megjelenít egy, az új adatbázis létrehozásához használthoz hasonló párbeszédablakot – azzal a jelentős különbséggel, hogy az alap DN nem módosítható, így szürkével jelenik meg.

Miután a *Befejezés* gombra kattintva elhagyta a párbeszédablakot, az LDAP-kiszolgáló alapszintű konfigurációja készen áll a használatra. A beállítás finomhangolásához használja az OpenLDAP dinamikus konfigurációs háttérprogramját.

Az OpenLDAP dinamikus konfigurációs háttérprogramja a konfigurációt magát is egy LDAP-adatbázisban tárolja. Az adatbázis egy sor `.ldif` fájlból áll az`/etc/openldap/slapd.d` könyvtárban. Nincs szükség e fájlok közvetlen elérésére. A beállítások eléréséhez használhatja a YaST LDAP-kiszolgáló modulját (a `yast2-ldap-server` csomag), vagy egy LDAP-kliensprogramot, mint az `ldapmodify` vagy az `ldapsearch`. További információ az OpenLDAP dinamikus konfigurációjáról az OpenLDAP Adminisztrátori kézikönyvben található.

26.4 LDAP-kliens beállítása YaST segítségével

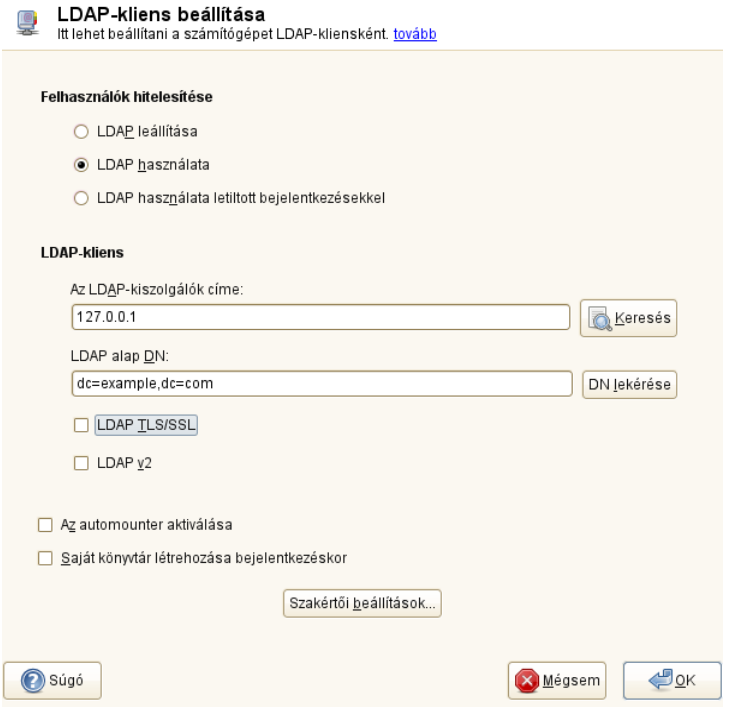
A YaST tartalmaz egy modult az LDAP alapú felhasználófelügyelet beállításához. Ha nem engedélyezi ezt a szolgáltatást a telepítés során, akkor indítsa el a modult a *Hálózati szolgáltatások* > *LDAP-kliens* menüpont kiválasztásával. A YaST automatikusan engedélyezi a PAM és NSS megfelelő módosításait, amelyekre az LDAP használatához szükség van és telepíti a szükséges fájlokat. Egyszerűen csak csatlakoztassa a klienst a kiszolgálóhoz és hagyja, hogy a YaST a felhasználókat LDAP-n keresztül kezelje. Az alapvető beállítás leírása: 26.4.1. - Alapbeállítások (412. oldal).

A YaST LDAP-kliens segítségével átalakíthatja a felhasználói és csoportadminisztrációra szolgáló YaST-modulokat. Ez magában foglalja az új felhasználók és csoportok alapértelmezett beállításainak, valamint felhasználóhoz vagy csoporthoz rendelt attribútumok számának és viselkedésének módosítását. Az LDAP felhasználófelügyelet lényegesen több, másféle attribútumok hozzárendelését teszi lehetővé a felhasználókhoz és csoportokhoz, mint a hagyományos felhasználó- és csoportfelügyeleti megoldások. Ennek leírása: 26.4.2. - A YaST csoport- és felhasználófelügyeleti moduljainak beállítása (416. oldal).

26.4.1 Alapbeállítások

Az alap LDAP klienskonfiguráció párbeszédablak (26.6. ábra - YaST: LDAP-kliens beállítása (412. oldal)) megjelenik a telepítés során, ha az LDAP felhasználófelügyeletet választja, vagy ha a telepített rendszeren kiválasztja a YaST vezérlőközpont *Hálózati szolgáltatások* > *LDAP-kliens* menüpontot.

26.6. ábra *YaST: LDAP-kliens beállítása*



A gép felhasználóinak OpenLDAP-kiszolgálón történő hitelesítéséhez és az OpenLDAP-n keresztüli felhasználófelügyelet engedélyezéséhez tegye a következőket:

1. Az LDAP használatának engedélyezéséhez kattintson az *LDAP használata* lehetőségre. Ha LDAP-hitelesítést kíván használni, de nem szeretné, hogy más felhasználók bejelentkezzenek a kliensre, akkor válassza inkább az *LDAP használata letiltott bejelentkezésekkel* lehetőséget.

2. Adja meg a használandó LDAP-kiszolgáló IP-címét.

3. Az LDAP-kiszolgálón a keresési alap kiválasztásához adja meg az *LDAP alap DN*-t. Az alap DN automatikus lekéréséhez kattintson a *DN lekérése* menüpontra. A YaST ezután a fent megadott kiszolgálócímen LDAP-adatbázist keres. A YaST által biztosított keresési eredemények közül válassza ki a megfelelő alap DN-t.

4. Ha a kiszolgálóval TLS-sel vagy SSL-lel védett kommunikációt kíván kialakítani, akkor válassza ki az *LDAP TLS/SSL* lehetőséget.

5. Ha az LDAP-kiszolgáló továbbra LDAPv2-t használ, akkor explicit módon engedélyezze a protokollváltozat használatát a *2-es LDAP verzió* lehetőség kiválasztásával.

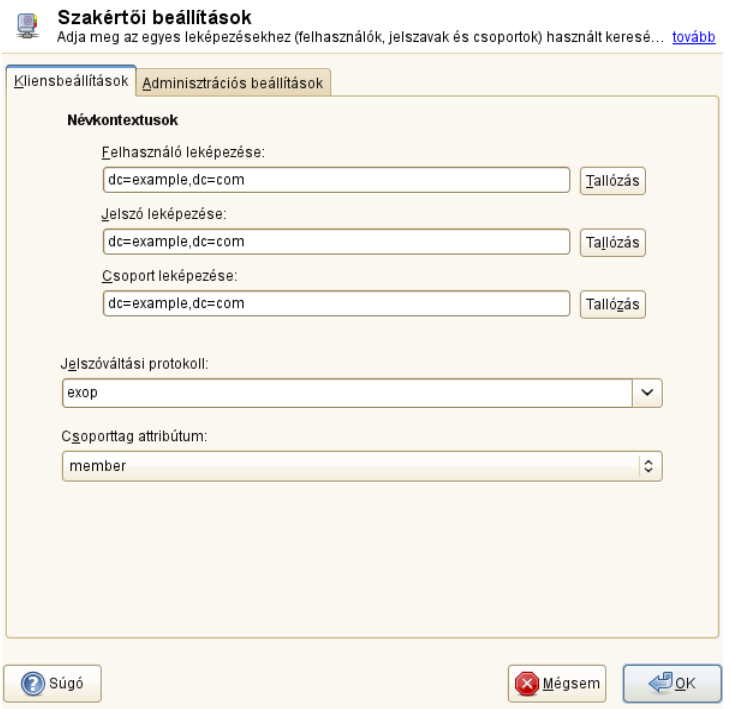
6. Válassza ki *Az automounter aktiválása* menüpontot a távoli könyvtárak - mint például a távolról felügyelt `/home` - felcsatolásához a kliensen.

7. Válassza ki a *Saját könyvtár létrehozása bejelentkezéskor* menüpontot, hogy a felhasználó saját könyvtára automatikusan létrejöjjön a felhasználó első bejelentkezésekor.

8. A beállítások alkalmazásához kattintson a *Befejezés* gombra.

A kiszolgáló adatainak módosításához adminisztrátor felhasználóként kattintson a *Szakértői beállítások* gombra. A következő párbeszédablak két részből áll: Lásd:26.7. ábra - YaST: Szakértői beállítás (414. oldal)

26.7. ábra *YaST: Szakértői beállítás*



1 A *Kliensbeállítások* lapon a következő beállításokat az igényeinek megfelelően adja meg:

1a Ha a felhasználók, jelszavak és csoportok keresési alapja eltér az *LDAP alap DN* részben megadott globális keresési alaptól, akkor adja meg ezeket az eltérő névkontextusokat itt, a *Felhasználó leképezése*, *Jelszó leképezése* és *Csoport leképezése* mezőkben.

1b Adja meg a jelszómódosítási protokollt. A jelszóváltozásakor alkalmazandó szabványos módszer az exop, amely az RFC 3062-ben leírt módon módosítja a jelszót (csak az új jelszó kerül elküldésre). Ezzel és más beállításokkal kapcsolatos részletekért tekintse meg a `pam_ldap` kézikönyvoldalt.

1c Adja meg a *Csoporttag attribútum*-hoz használandó LDAP-csoportot. Ennek alapértelmezett értéke a `member`.

2 A *Felügyeleti beállítások* menüpontban adja meg a következő beállításokat:

2a Adja meg a felhasználófelügyeleti adatok tárolásának alapját a *Beállítás alap DN* menüpontban.

2b Adja meg az *Adminisztrátori DN* megfelelő értékét. Ennek a DN-nek meg kell egyeznie az `/etc/openldap/slapd.conf` fájlban megadott `rootdn` értékkel annak engedélyezéséhez, hogy ez az adott felhasználó módosítani tudja az LDAP-kiszolgálón tárolt adatokat. Adja meg a teljes DN-t (például: `cn=Administrator,dc=example,dc=com`) vagy aktiválja a *Alap DN hozzáfűzése* lehetőséget ahhoz, hogy az alap DN automatikusan hozzáadásra kerüljön a `cn=Administrator` beírásakor.

2c Jelölje be az *Alapértelmezett konfigurációs objektumok létrehozása* lehetőséget az alap konfigurációs objektumok létrehozásához a kiszolgálón az LDAP-n keresztüli felhasználófelügyelet engedélyezéséhez.

2d Ha a kliensgépnek a saját könyvtárak fájlkiszolgálójaként kell működnie a hálózatban, akkor jelölje be a *Saját könyvtárak ezen a gépen* lehetőséget.

2e A *Jelszóirányelv* részben kiválaszthatja, hozzáadhatja, törölheti vagy módosíthatja a használandó jelszóirányelvet. A jelszóirányelvek YaST segítségével történő konfigurációja az LDAP-kiszolgálóbeállítás része.

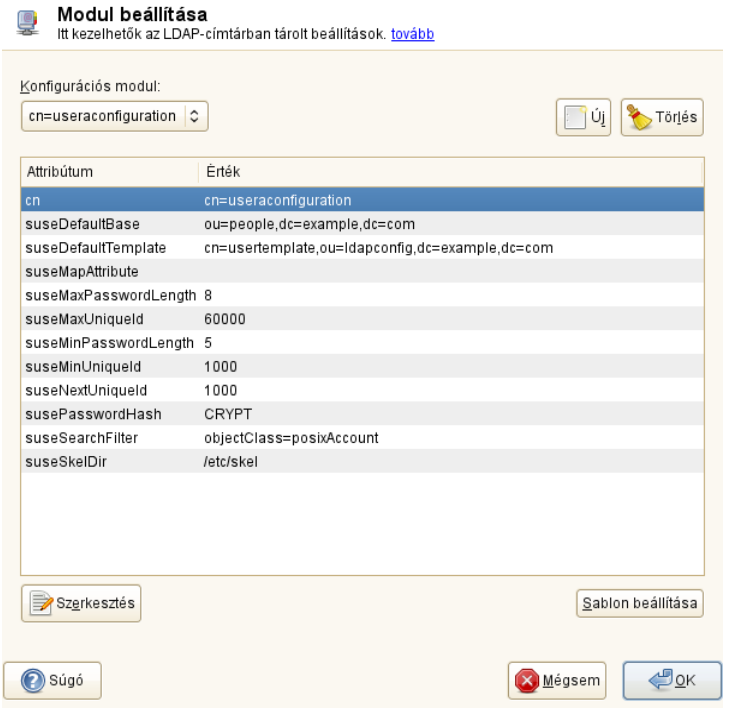
2f Kattintson az *Elfogadás* gombra a *Szakértői beállítás* elhagyásához, majd a *Befejezés* gombra a beállítások alkalmazásához.

A *Felhasználókezelési konfiguráció beállítása* menüpont segítségével módosíthatja az LDAP-kiszolgáló bejegyzéseit. A kiszolgálón lévő konfigurációs modulok elérése a kiszolgálón tárolt ACL-ek és ACI-k szerint biztosított. Kövesse a következő eljárásokat: 26.4.2. - A YaST csoport- és felhasználófelügyeleti moduljainak beállítása (416. oldal).

26.4.2 A YaST csoport- és felhasználófelügyeleti moduljainak beállítása

A YaST LDAP-kliens segítségével a YaST modulok módosíthatók a felhasználó- és csoportfelügyelethez, valamint ezek szükség szerint kiterjeszthetők. Adjon meg sablonokat alapértelmezett értékekkel az egyéni attribútumokhoz az adatregisztráció egyszerűsítése érdekében. Az itt létrehozott előre megadott beállításokat az LDAP-címtár LDAP-objektumokként tárolja. A felhasználói adatok regisztrációja továbbra is a felhasználó- és csoportkezelésre szolgáló normál YaST modulokkal történik. A regisztrált adatok LDAP-objektumok formájában kerülnek tárolására a kiszolgálón.

26.8. ábra *YaST: modul beállítása*



A modulkonfigurációhoz tartozó párbeszédablak (26.8. ábra - YaST: modul beállítása (416. oldal)) lehetővé teszi új modulok létrehozását, a meglévő konfigurációs modulok

kiválasztását és módosítását, valamint az ilyen modulok sablonjainak tervezését és módosítását.

Új konfigurációs modul létrehozásához tegye a következőket:

1. Az *LDAP-kliens beállítása* részben kattintson a *Szakértői beállítások* pontra, majd nyissa meg az *Adminisztrációs beállítások* lapot. Kattintson a *Felhasználókezelési konfiguráció beállítása* pontra, és adja meg az LDAP-kiszolgáló azonosító adatait.

2. Kattintson az *Új* lehetőségre, és válassza ki a létrehozandó modul típusát. A felhasználói konfigurációs modulhoz válassza ki a `suseuserconfiguration`, a csoportkonfigurációhoz pedig a `susegroupconfiguration` lehetőséget.

3. Az új sablonhoz válasszon nevet. A tartalom nézetben ezután megjelenik egy táblázat, amelyben a modulban engedélyezett összes attribútum látható a hozzájuk rendelt értékekkel. Az összes beállított attribútumon túl a lista tartalmazza az aktuális séma által engedélyezett, de jelenleg nem használt egyéb attribútumokat is.

4. Fogadja el az előre beállított értékeket, vagy módosítsa a csoport- és felhasználókonfiguráció alapértelmezéseit: válassza ki a kívánt attribútumot, nyomja meg a *Szerkesztés* gombot, majd írja be az új értéket. A modul átnevezéséhez egyszerűen csak a modul `cn` attribútumát kell módosítani. A *Törlés* gomb megnyomására a jelenleg kiválasztott modul törlődik.

5. Az *OK* gomb megnyomása után az új modul bekerül a kiválasztás menübe.

A csoport- és felhasználóadminisztrációs YaST-modulok értelmes alapértékekkel kitöltött sablonokat tartalmaznak. Egy konfigurációs modulhoz rendelt sablon szerkesztése:

1. A *Modul beállítása* párbeszédablakban kattintson a *Sablon beállítása* menüpontra.

2. Igény szerint határozza meg a sablonhoz rendelt általános attribútumok értékeit. Üresen is hagyhat közülük néhányat. Az üres attribútumok törlődnek az LDAP-kiszolgálóról.

3. Módosítsa, törölje vagy vegye fel az új objektumok (az LDAP-címtárfa felhasználó- vagy csoportkonfigurációs objektumainak) új alapértelmezett értékeit.

26.9. ábra *YaST: Objektumsablon beállítása*

Csatlakoztassa a sablont a moduljához: állítsa a modul `susedefaulttemplate` attribútumának értékét a módosított sablon DN-jére.

TIPP

Az attribútum alapértelmezett értékei létrehozhatók másik attribútumokból is, ha abszolút érték használata helyett egy változót használ. Új felhasználó létrehozásakor például a `cn=%sn %givenName` automatikusan létrejön az `sn` és `givenName` attribútumértékéből.

Ha az összes modul és sablon megfelelően be van állítva és futásra kész, akkor a YaST segítségével az új csoportok és felhasználók a szokásos módon bejegyezhetők.

26.5 LDAP felhasználók és csoportok beállítása a YaST segítségével

A felhasználói és csoportadatok tényleges regisztrációja alig különbözik az LDAP nélküli eljárástól. A következő rövid útmutató a felhasználók adminisztrációjával kapcsolatos. A csoportok adminisztrálásának folyamata hasonló.

1 Nyissa meg a YaST felhasználói adminisztrációs modulját a *Biztonság és felhasználók* > *Felhasználók és csoportok kezelése* menüpontokkal.

2 A *Szűrő beállítása* menüpont segítségével korlátozhatja a felhasználók nézetét az LDAP-felhasználókra és megadhatja a Root DN jelszavát.

3 Kattintson a *Hozzáadás* menüpontra és adja meg az új felhasználó konfigurációját. Egy párbeszédpanel nyílik meg négy lappal:

3a Adja meg a felhasználónevet, a bejelentkezési azonosítót és a jelszót a *Felhasználói adatok* lapon.

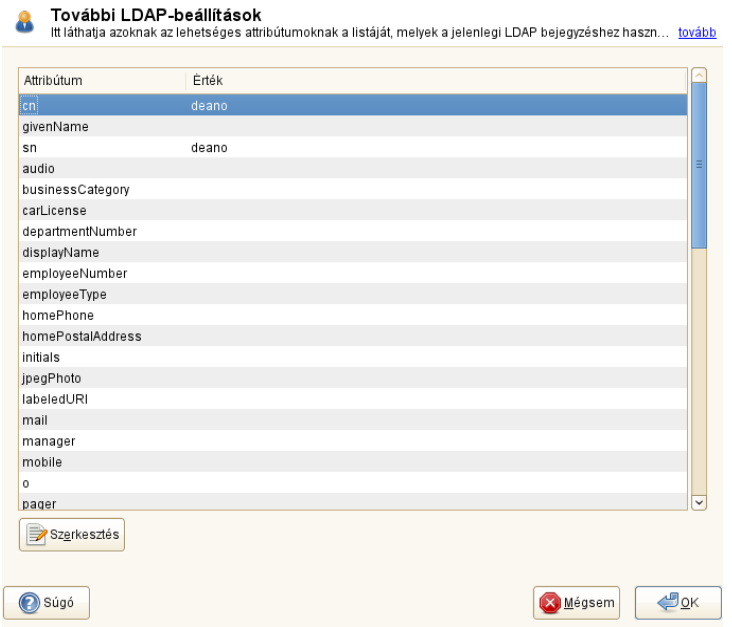
3b Tekintse meg a *Részletek* lapot az új felhasználó csoporttagságára, bejelentkezési parancsértelmezőjére és saját könyvtárára vonatkozóan. Szükség esetén módosítsa az alapértelmezéseket az igényeinek jobban megfelelő értékekre. Az alapértelmezett értékek, valamint a jelszóbeállítások értékei a következő leírt eljárással adhatók meg: 26.4.2. - A YaST csoport- és felhasználófelügyeleti moduljainak beállítása (416. oldal).

3c Módosítsa vagy fogadja el az alapértelmezett *Jelszóbeállításokat*

3d Lépjen a *Bővítőmodulok* lapra, válassza ki az LDAP-bővítőmodult, majd kattintson az *Indítás* lehetőségre az új felhasználóhoz rendelt további LDAP attribútumok beállításához (lásd: 26.10. ábra - YaST: További LDAP-beállítások (420. oldal)).

4 A beállítások alkalmazásához és a felhasználói beállítások elhagyásához nyomja meg az *OK* gombot.

26.10. ábra *YaST: További LDAP-beállítások*



A felhasználófelügyelet kezdeti beviteli űrlapján találhatók *LDAP beállítási lehetőségek*. Itt meg lehet adni LDAP keresési szűrőket a meglévő felhasználók halmazára, valamint át lehet lépni az LDAP-felhasználók és csoportok beállítási moduljába a *LDAP felhasználók és csoportok beállítása* menüponttal.

26.6 Tallózás az LDAP-címtárfában

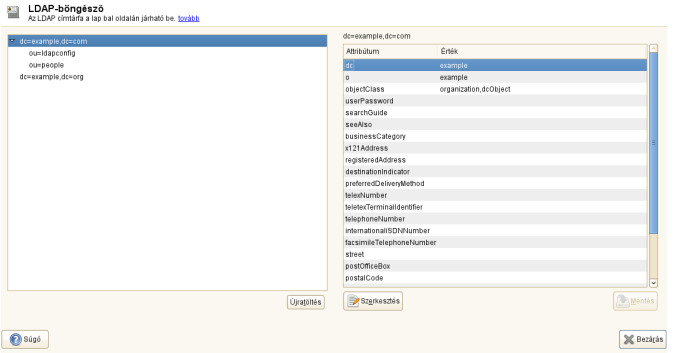
Az LDAP-címtárfa és az összes bejegyzésének kényelmes tallózásához használja a YaST LDAP-böngészőjét:

1. Jelentkezzen be `root` felhasználóként.
2. Válassza ki a *YaST* > *Hálózati szolgáltatások* > *LDAP-böngésző* menüpontot.
3. Adja meg az LDAP-kiszolgáló címét, az Adminisztrátori DN-t, valamint a kiszolgáló RootDN-jéhez tartozó jelszót, ha a kiszolgálón tárolt adatokat olvasni és írni is szeretné.

   Vagy válassza az *Anonim hozzáférés* lehetőséget, és ne adjon meg jelszót, ekkor csak olvashatja a címtárat.

   Az *LDAP-címtárfa* a lap bal oldalán járható be. Az alelemek megjelenítéséhez kattintson a kívánt elemre.

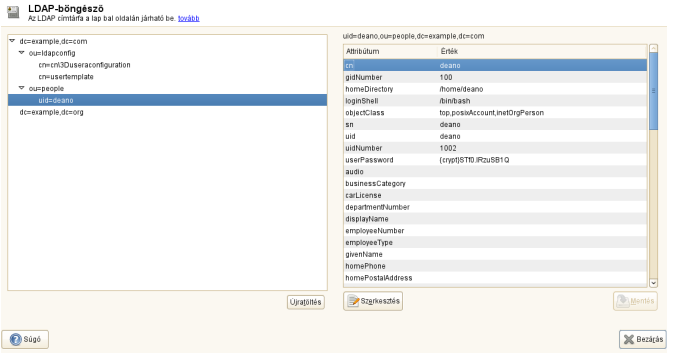
26.11. ábra *Tallózás az LDAP-címtárfában*



4. Egy bejegyzés részletes megjelenítéséhez válassza ki a bejegyzést az *LDAP-fa* nézetben.

   A bejegyzéshez tartozó attribútumok és értékek megjelennek.

26.12. ábra *Bejegyzésadatok tallózása*



5 Az attribútumok értékének módosításához válassza ki az attribútumot, kattintson a *Szerkesztés* menüpontra, adja meg az új értéket, kattintson a *Mentés* gombra és adja meg a Root DN jelszót, amikor a rendszer ezt kéri.

6 Hagyja el az LDAP-böngészőt a *Bezárás* menüponttal.

26.7 LDAP-kiszolgáló beállítása kézzel

A telepített rendszerben található egy teljes konfigurációs fájl az LDAP-kiszolgáló számára, amely az `/etc/openldap/slapd.conf`. Az alábbiakban röviden leírjuk az egyes bejegyzéseket és elmagyarázzuk az esetleg szükséges módosításokat. A kettőskereszt (#) karakter után írt bejegyzések nem aktívak. Az aktiválásukhoz törölni kell ezt a megjegyzés karaktert.

26.7.1 Az slapd.conf általános direktívái

26.2 példa *slapd.conf: Beágyazási direktíva sémákhoz*

```
include         /etc/openldap/schema/core.schema
include         /etc/openldap/schema/cosine.schema
include         /etc/openldap/schema/inetorgperson.schema
include         /etc/openldap/schema/rfc2307bis.schema
include         /etc/openldap/schema/yast.schema
```

Az `slapd.conf` első direktívája (26.2. példa - slapd.conf: Beágyazási direktíva sémákhoz (422. oldal)) azt a sémát adja meg, amelynek alapján az LDAP-címtár szerveződik. A `core.schema` bejegyzés kötelező. A további szükséges sémákat ehhez a direktívához kell fűzni. Ezzel kapcsolatos információ a mellékelt OpenLDAP-dokumentációban található.

26.3 példa *slapd.conf: pidfile és argsfile*

```
pidfile /var/run/slapd/slapd.pid
argsfile /var/run/slapd/slapd.args
```

Ez a két fájl tartalmazza az `slapd` folyamat PID-jét (folyamatazonosítóját) és egyes paramétereit, amelyekkel el lett indítva. Itt nincs szükség módosításra.

26.4 példa *slapd.conf: Hozzáférés-vezérlés*

```
# Sample Access Control
#       Allow read access of root DSE
# Allow self write access
#       Allow authenticated users read access
#       Allow anonymous users to authenticate
# access to dn="" by * read
  access to * by self write
               by users read
               by anonymous auth
#
# if no access controls are present, the default is:
#       Allow read by all
#
# rootdn can always write!
```

A 26.4. példa - slapd.conf: Hozzáférés-vezérlés (423. oldal) ábrán látható az `slapd.conf` azon részlete, amely a kiszolgáló LDAP-címtárának hozzáférési jogosultságait szabályozza. Az `slapd.conf` általános részében megadott beállítások addig érvényesek, amíg az adatbázis-specifikus részben egy egyéni hozzáférési szabály felül nem írja őket. Ezek felülírják az általános deklarációkat. Az itt látható módon, minden felhasználó jogosult olvasni a címtárat, de csak a rendszergazda (`rootdn`) jogosult írni bele. Az LDAP hozzáférés-vezérlése meglehetősen összetett folyamat. Az alábbi tanácsok talán segítenek:

- Minden hozzáférési szabály az alábbi módon épül fel:

  ```
  access to <what> by <who> <access>
  ```

- A *what* helyére kell írni azt az objektumot vagy attribútumot, amelyhez a hozzáférést engedélyezi. A független címtárágakat külön szabályokkal kell védeni, explicit módon. Reguláris kifejezések használatával a címtárfa több része is feldolgozható egyetlen szabállyal. Az `slapd` a szabályokat abban a sorrendben értékeli ki, ahogy azok a konfigurációs fájlban szerepelnek. Az általánosabb szabályokat a speciálisabbak után kell venni – az `slapd` az első illeszkedő szabályt fogja alkalmazni és a többit figyelmen kívül hagyja.

- A *who* helyére kerül az, hogy ki kap hozzáférést a *what* részhez. Itt is használhatók reguláris kifejezések. Megint csak, az `slapd` megszakítja a `who` rész kiértékelését az első illeszkedésnél, tehát a specifikusabb szabályokat az általánosabbak elé kell venni. A 26.2 táblázat - Felhasználói csoportok és hozzáférési jogaik (424. oldal) táblázatban felsorolt lehetőségek használhatók.

26.2. táblázat *Felhasználói csoportok és hozzáférési jogaik*

Címke	Hatókör
`*`	Minden felhasználó, kivétel nélkül
`anonymous`	A nem hitelesített, („anonim”) felhasználók
`users`	A hitelesített felhasználók
`self`	A célobjektumhoz csatlakozó felhasználók
`dn.regex=<regex>`	A reguláris kifejezésnek megfelelő felhasználók

- Az *access* helyére a hozzáférés típusa kerül. 2A 26.3 táblázat - Hozzáférés típusa (424. oldal) táblázatban felsorolt lehetőségek használhatók.

26.3. táblázat *Hozzáférés típusa*

Címke	Hozzáférési kör
`none`	Nincs hozzáférés

Címke	Hozzáférési kör
`auth`	A kiszolgálóhoz kapcsolódás
`compare`	Összehasonlítási hozzáférés
`search`	Jogosultság keresési szűrők használatára
`read`	Olvasási hozzáférés
`write`	Írási hozzáférés

Az `slapd` összehasonlítja a kliens által kért hozzáférési jogokat az `slapd.conf` fájlban megadottakkal. A kliens akkor kap hozzáférést, ha a szabályok a kértnél magasabb vagy azzal egyenlő hozzáférést engedélyeznek. Ha a kliens magasabb szintű hozzáférést kér, mint amit a szabályok engedélyeznek, akkor a kiszolgáló megtagadja a hozzáférést.

A 26.5. példa - slapd.conf: Példa hozzáférés-vezérlésre (425. oldal) ábrán egy egyszerű hozzáférés-vezérlési beállítás látható, amely önkényesen alakítható reguláris kifejezések használatával.

26.5 példa *slapd.conf: Példa hozzáférés-vezérlésre*

```
access to  dn.regex="ou=([^,]+),dc=example,dc=com"
by dn.regex="cn=Administrator,ou=$1,dc=example,dc=com" write
by user read
by * none
```

Ez a szabály azt jelenti, hogy csak a megfelelő rendszergazdának van írási joga egy `ou` (szervezeti egység) bejegyzéshez. A többi hitelesített felhasználó olvasási jogot kap, mindenki más pedig semmilyet.

TIPP: Hozzáférési szabályok kialakítása

Ha nincs `access to` szabály, vagy illeszkedő `by` direktíva, akkor a hozzáférés meg lesz tagadva. Csak a kifejezetten megadott hozzáférési jogok lesznek megadva. Ha egyáltalán nincsenek szabályok megadva, akkor az alapelv az, hogy a rendszergazda kap írási jogot, és mindenki más olvasásit.

Részletes információ és az LDAP hozzáférési jogok példakonfigurációja a telepített `openldap2` csomag online dokumentációjában található.

Azon túl, hogy a központi kiszolgálókonfigurációs fájl (az `slapd.conf`) segítségével beállíthatók hozzáférési jogok, létezik az úgynevezett hozzáférés-vezérlési információ (access control information, ACI) funkció is. Az ACI lehetővé teszi az egyes objektumok hozzáférési adatainak tárolását magában az LDAP-címtárfában. Ez a fajta hozzáférés-vezérlés még nem nagyon elterjedt, és még maguk a fejlesztők is kísérletinek tekintik. További információ: http://www.openldap.org/faq/data/cache/758.html.

26.7.2 Az slapd.conf adatbázis-specifikus direktívái

26.6 példa *slapd.conf: adatbázis-specifikus direktívák*

```
database bdb❶
suffix "dc=example,dc=com"❷
checkpoint      1024    5❸
cachesize       10000❹
rootdn "cn=Administrator,dc=example,dc=com"❺
# Cleartext passwords, especially for the rootdn, should
# be avoided.  See slappasswd(8) and slapd.conf(5) for details.
# Use of strong authentication encouraged.
rootpw secret❻
# The database directory MUST exist prior to running slapd AND
# should only be accessible by the slapd/tools. Mode 700 recommended.
directory /var/lib/ldap❼
# Indices to maintain
index   objectClass     eq❽
overlay ppolicy❾
ppolicy_default "cn=Default Password Policy,dc=example,dc=com"
ppolicy_hash_cleartext
ppolicy_use_lockout
```

❶ Az adatbázis típusa (a jelen esetben egy Berkeley adatbázis) a szakasz első sorában van beállítva (lásd: 26.6. példa - slapd.conf: adatbázis-specifikus direktívák (426. oldal)).

❷ A `suffix` (utótag) rész határozza meg, hogy ez a kiszolgáló az LDAP-címtárfa mely részéért felelős.

❸ A `checkpoint` (ellenőrzőpont) határozza meg azt az adatmennyiséget (kilobájtban), amelyik a tranzakciós naplóban marad, mielőtt az a tényleges adatbázisba íródna, illetve a két írási művelet közötti időt (percben).

❹ A `cachesize` (gyorsítótár mérete) paraméter adja meg, hogy hány objektum tárolódik az adatbázis gyorsítótárában.

❺ A `rootdn` adja meg, hogy ki rendelkezik rendszergazdai jogokkal a kiszolgálót illetően. Az itt megadott felhasználónak nem kell LDAP-bejegyzéssel rendelkeznie, és nem is kell léteznie normál felhasználóként.

❻ A `rootpw` paraméter adja meg a rendszergazda jelszavát. A `secret` használata helyett megadható a `slappasswd` által a rendszergazdai jelszóból készített kivonat is.

❼ A `directory` direktíva adja meg a fájlrendszer azon könyvtárát, amelyben a kiszolgálón az adatbázis könyvtárai tárolódnak.

❽ Az utolsó direktíva, az `index objectClass eq` azt jelenti, hogy index készül minden objektumosztályról. A tapasztalat szerint a felhasználók által leggyakrabban keresett attribútumok is felvehetők ide.

❾ Az `overlay ppolicy` jelszókezelési mechanizmusok egy rétegével bővíti a rendszert. A `ppolicy_default` adja meg a használandó pwdPolicy objektum DN-jét, ha egy adott felhasználói bejegyzésre semmilyen más irányelv nem vonatkozik. Ha nincs specifikus irányelv egy adott bejegyzéshez, és nincs alapértelmezés sem, akkor semmilyen irányelv nem lesz érvényesítve. A `ppolicy_hash_cleartext` azt adja meg, hogy a hozzáadási és módosítási kérések nyílt szövegű jelszavaiból először kivonat készül, mielőtt az adatbázisban tárolódnának. E paraméter használata esetén célszerű letiltani az összehasonlítási, keresési és olvasási hozzáférést a `userPassword` attribútumhoz a címtár összes felhasználója számára, mivel a `ppolicy_hash_cleartext` sérti az X.500/LDAP információs modellt. A `ppolicy_use_lockout` meghatározott hibakódot küld, amikor egy kliens egy zárolt fiókhoz próbál csatlakozni. Kiemelt biztonságú rendszerekben érdemes letiltani ezt a funkciót, mivel a hibakódból a támadók esetleg értékes információt nyerhetnek ki.

Az adatbázisra vonatkozóan itt megadott egyéni `Access` szabályok felülírják az általános `Access` szabályokat.

26.7.3 A kiszolgálók elindítása és leállítása

Az LDAP-kiszolgálót a teljes beállítása, és a 26.8. - LDAP-adatok kézi adminisztrációja (428. oldal) részben leírtak szerint az összes szükséges bejegyzés felvétele után a `root` tudja elindítani az `rcldap start` paranccsal. A kiszolgáló kézi leállításához írja be, hogy `rcldap stop`. A futó LDAP-kiszolgáló állapotáról információ az `rcldap status` paranccsal kérhető.

A YaST futásiszint-szerkesztője (14.2.3. - Rendszerszolgáltatások (futási szintek) beállítása a YaST segítségével (195. oldal)) is használható a kiszolgáló automatikus elindításához és leállításához a rendszer indításakor és leállításakor. Lehet továbbá megfelelő hivatkozásokat készíteni az indító és leállító parancsfájlokra az `insserv` paranccsal egy konzolból (ennek leírása: 14.2.2. - Init parancsfájlok (190. oldal)).

26.8 LDAP-adatok kézi adminisztrációja

Az OpenLDAP egy sor eszközt kínál az LDAP-címtár adatainak adminisztrációjához. Az alábbiakban bemutatjuk az adatok felvételére, törlésére, keresésére és módosítására szolgáló négy legfontosabb eszközt.

26.8.1 Adatok beszúrása egy LDAP-címtárba

Ha az LDAP-kiszolgáló konfigurációja helyes az `/etc/openldap/slapd.conf` fájlban és a kiszolgáló készen áll a működésre (megfelelő `suffix`, `directory`, `rootdn`, `rootpw` és `index` bejegyzéseket tartalmaz), akkor következhet a bejegyzések beírása. Az OpenLDAP erre az `ldapadd` parancsot biztosítja. Ha lehetséges, gyakorlati okokból érdemes csoportosan felvenni az adatbázisba az objektumokat. Az LDAP ehhez az LDIF adatformátumot (LDAP adatcsere formátumot) kínálja. Egy LDIF fájl egy egyszerű szövegfájl, amelyben tetszés szerinti számú attribútum-érték pár szerepelhet. A használható objektumosztályokkal és attribútumokkal kapcsolatban forduljon az `slapd.conf` fájlban deklarált sémafájlokhoz. A 26.1. ábra - Az LDAP-címtár szerkezete (400. oldal) példa durva keretrendszerének előállítására szolgáló LDIF fájl valahogy így nézne ki: 26.7. példa - Példa egy LDIF fájlra (429. oldal).

FONTOS: LDIF fájlok kódolása

Az LDAP az UTF-8 (Unicode) kódolást használja. Az ékezetes betűket ennek megfelelően kell kódolni. Olyan szövegszerkesztőt használjon, amelyik támogatja az UTF-8 használatát. Ilyen például a Kate, vagy az Emacs friss verziói. Ellenkező esetben kerülje az ékezetes betűk és más speciális karakterek használatát, vagy használja a `recode` parancsot a bemenet UTF-8 kódtáblára alakításához.

26.7 példa *Példa egy LDIF fájlra*

```
# The Organization
dn: dc=example,dc=com
objectClass: dcObject
objectClass: organization
o: Example dc: example

# The organizational unit development (devel)
dn: ou=devel,dc=example,dc=com
objectClass: organizationalUnit
ou: devel

# The organizational unit documentation (doc)
dn: ou=doc,dc=example,dc=com
objectClass: organizationalUnit
ou: doc

# The organizational unit internal IT (it)
dn: ou=it,dc=example,dc=com
objectClass: organizationalUnit
ou: it
```

Mentse el a fájlt `.ldif` kiterjesztéssel, majd küldje el a kiszolgálóhoz az alábbi paranccsal:

```
ldapadd -x -D <dn of the administrator> -W -f <file>.ldif
```

A jelen esetben az `-x` paraméter kikapcsolja az SASL-hitelesítést. A `-D` azt a felhasználót jelzi, aki meghívja a műveletet. Itt a rendszergazda érvényes DN-jét kell megadni, ugyanúgy, ahogy az az `slapd.conf` fájlban meg van adva. A jelen példában ez a `cn=Administrator,dc=example,dc=com`. A `-W` hatására a jelszót nem nyílt szövegként kell beírni a parancssorban, hanem külön. Ez a jelszó az, amit korábban az `slapd.conf` fájlban a `rootpw` direktívánál adott meg. A `-f` paraméter a fájlnevet adja át. Az `ldapadd` használatának részletei: 26.8. példa - ldapadd és az example.ldif fájl (430. oldal).

26.8 példa *ldapadd és az example.ldif fájl*

```
ldapadd -x -D cn=Administrator,dc=example,dc=com -W -f example.ldif

Enter LDAP password:
adding new entry "dc=example,dc=com"
adding new entry "ou=devel,dc=example,dc=com"
adding new entry "ou=doc,dc=example,dc=com"
adding new entry "ou=it,dc=example,dc=com"
```

Az egyes felhasználók adatait külön LDIF fájlokban is el lehet készíteni. A 26.9. példa - Tux LDIF-adatai (430. oldal) fájl használata esetén `Tux` bekerül az új LDAP-címtárba.

26.9 példa *Tux LDIF-adatai*

```
# coworker Tux
dn: cn=Tux Linux,ou=devel,dc=example,dc=com
objectClass: inetOrgPerson
cn: Tux Linux
givenName: Tux
sn: Linux
mail: tux@example.com
uid: tux
telephoneNumber: +49 1234 567-8
```

Egy LDIF fájlban tetszés szerinti számú objektum lehet. Egyszerre akár teljes címtárfa-ágakat is fel lehet venni a kiszolgálóra, de külön objektumokat is, mint a példában látható. Ha bizonyos adatokat viszonylag gyakran kell módosítani, akkor célszerű finoman felosztani az egyes objektumokat.

26.8.2 Az LDAP-címtár adatainak módosítása

Az adatok módosítására az `ldapmodify` parancs szolgál. Ennek legegyszerűbb módja a megfelelő LDIF fájl módosítása és a módosított fájl átküldése az LDAP-kiszolgálónak. Például ha meg akarja változtatni Tux kolléga telefonszámát `+49 1234 567-8`-ról `+49 1234 567-10`-re, akkor módosítsa az LDIF fájlt így: 26.10. példa - Módosított tux.ldif LDIF fájl (430. oldal).

26.10 példa *Módosított tux.ldif LDIF fájl*

```
# coworker Tux
dn: cn=Tux Linux,ou=devel,dc=example,dc=com
changetype: modify
replace: telephoneNumber
telephoneNumber: +49 1234 567-10
```

Importálja a módosított fájlt az LDAP-címtárba az alábbi paranccsal:

```
ldapmodify -x -D cn=Administrator,dc=example,dc=com -W -f tux.ldif
```

Alternatív megoldásként az attribútumok átadhatók közvetlenül, paraméterként is az `ldapmodify` parancsnak. Ennek módja a következő:

1. Indítsa el az `ldapmodify` parancsot és írja be a jelszavát:

   ```
   ldapmodify -x -D cn=Administrator,dc=example,dc=com -W
   Enter LDAP password:
   ```

2. Írja be a módosításokat, és ügyeljen az alább leírt szintaxisra:

   ```
   dn: cn=Tux Linux,ou=devel,dc=example,dc=com
   changetype: modify
   replace: telephoneNumber
   telephoneNumber: +49 1234 567-10
   ```

Az `ldapmodify` parancsról és szintaxisáról az `ldapmodify` kézikönyvoldalon olvashat részletesen.

26.8.3 LDAP-címtár adatainak keresése vagy kiolvasása

Az OpenLDAP az `ldapsearch` parancsori eszközt biztosítja az LDAP-címtárak adatainak keresésére és kiolvasására. Egy egyszerű lekérdezés az alábbi szintaxist követi:

```
ldapsearch -x -b dc=example,dc=com "(objectClass=*)"
```

A `-b` paraméter adja meg a keresés alapját – a fának azt a részét, amelyben a keresés történik. A jelen esetben ez a `dc=example,dc=com`. Egy finomabb keresés végrehajtásához az LDAP-címtárfa meghatározott részeiben (például csak a `devel` osztályon belül), adja át ezt a szakaszt az `ldapsearch` parancsnak a `-b` paraméterrel. A `-x` paraméter egyszerű hitelesítést kér. Az `(objectClass=*)` azt jelenti, hogy a címtár minden objektumát ki kell olvasni. Ez a paraméter használható egy újonnan létrehozott címtárfában annak ellenőrzésére, hogy a bejegyzések sikeresen rögzítve lettek-e, és a kiszolgáló az elvárásoknak megfelelően reagál-e. Az `ldapsearch` parancs használatáról további részletek a megfelelő kézikönyvoldalon olvashatók (ldapsearch(1)).

26.8.4 Adatok törlése egy LDAP-címtárból

A nem kívánt bejegyzések törlésére az `ldapdelete` parancs szolgál. Ennek szintaxisa a fenti többi parancshoz hasonló. Például `Tux Linux` teljes bejegyzésének törléséhez adja ki az alábbi parancsot:

```
ldapdelete -x -D cn=Administrator,dc=example,dc=com -W cn=Tux \
Linux,ou=devel,dc=example,dc=com
```

26.9 További információk

A fejezetben szándékosan nem esett szó bonyolultabb esetekről – például az SASL beállításáról vagy egy replikációt végző LDAP-kiszolgáló üzembe helyezéséről, amely több alárendelt rendszer között osztja el a terhelést. Mindkét téma részletes leírását megtalálja az *OpenLDAP 2.2 Adminisztrátori kézikönyvben*.

Az OpenLDAP projekt weboldala átfogó dokumentációt biztosít a kezdő és haladó LDAP felhasználók számára egyaránt:

OpenLDAP Faq-O-Matic
: Az OpenLDAP telepítésével, beállításával és használatával kapcsolatos gazdag kérdés-válasz gyűjtemény. A következő címen érhető el: `http://www.openldap.org/faq/data/cache/1.html`.

Gyors üzembehelyezési segédlet
: Az első LDAP-kiszolgáló telepítésének rövid, lépésenkénti útmutatója. Ez a `http://www.openldap.org/doc/admin22/quickstart.html` címen, illetve telepített rendszeren az `/usr/share/doc/packages/openldap2/admin-guide/quickstart.html` fájlban érhető el.

OpenLDAP 2.2 Adminisztrátori kézikönyv
: Az LDAP beállításával kapcsolatos összes fontos aspektus részletes bemutatása, a hozzáférés-felügyeletet és a titkosítást is beleértve. Tekintse meg a `http://www.openldap.org/doc/admin22/`, illetve telepített rendszeren az `/usr/share/doc/packages/openldap2/admin-guide/index.html` oldalt.

Az LDAP bemutatása

Az LDAP alapelveinek részletes, általános bemutatása: http://www.redbooks.ibm.com/redbooks/pdfs/sg244986.pdf.

LDAP-vel kapcsolatos nyomtatott irodalom:

- Gerald Carter: *LDAP System Administration* (ISBN 1-56592-491-6)
- Howes, Smith és Good: *Understanding and Deploying LDAP Directory Services* (ISBN 0-672-32316-8)

Az LDAP-témakör alapvető referenciaanyagai a megfelelő RFC-k (request for comment): 2251 - 2256.

Fájlrendszer megosztása NFS-sel

27

A fájlrendszerek hálózaton keresztüli megosztása és terjesztése általános feladat vállalati környezetekben. Az `NFS` kipróbált rendszer, amely együttműködik a `NIS` protokollal. Ha biztonságosabb protokollra van szüksége, amely együttműködik az `LDAP` címtárral és Kerberosszal védhető, akkor tekintse meg az `NFSv4`-et.

Az NFS a NIS-sel együttműködik, hogy átlátszóvá tegye a hálózatot a felhasználók számára. Az NFS segítségével a fájlrendszereket lehet megosztani a hálózat gépei között. Megfelelő beállítás esetén mindegy, hogy a felhasználó melyik terminálon jelentkezik be, mindig ugyanabban a környezetben találja magát.

Csakúgy, mint a NIS, az NFS is egy kliens-kiszolgáló alapú szolgáltatás. Egy gép betöltheti mindkét szerepet – fájlrendszereket szolgáltathat a hálózaton (exportálás) és felcsatolhat fájlrendszereket más gépekről (importálás).

FONTOS: Igény a DNS-re

Az exportálás elvileg végrehajtható csak IP-címekkel. Az időtúllépések elkerüléséhez azonban szükség van egy működő DNS-rendszerre. Ez legalább a naplózáshoz szükséges, mivel a mountd démon végez fordított keresést.

27.1 A szükséges szoftver telepítése

Ha a gépet NFS-kliensként kívánja beállítani, akkor nem kell telepíteni további szoftvert. Az NFS-kliens beállításához szükséges összes csomag alapértelmezésben telepítésre kerül.

Az NFS-kiszolgáló azonban nem része az alapértelmezett telepítésnek. Az NFS-kiszolgálószoftver telepítéséhez indítsa el a YaST-ot és válassza ki a *Szoftver* > *Szoftver telepítése és eltávolítása* menüpontot. Ezt követően válassza ki a *Szűrő* > *Minták* lehetőséget, majd az *Egyéb kiszolgáló* menüpontot, vagy a *Keresés* lehetőséggel keressen rá az `NFS` kifejezésre és válassza ki az NFS-kiszolgáló csomagját. A telepítési folyamat befejezéséhez erősítse meg a csomagok telepítését.

27.2 Fájlrendszerek importálása YaST segítségével

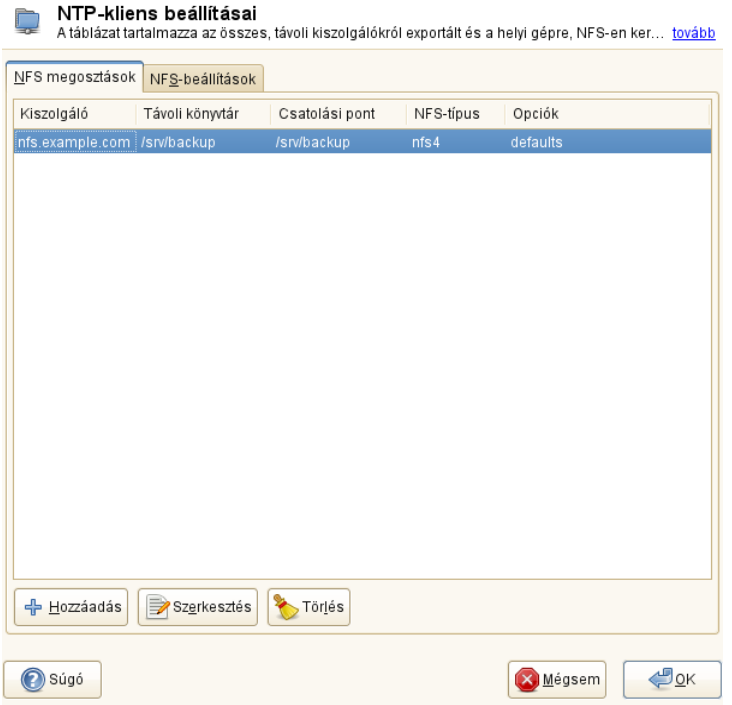
Az erre jogosult felhasználók felcsatolhatják az NFS-könyvtárakat egy NFS-kiszolgálóról a saját könyvtárfájukba. Ez a YaST *NFS-kliens* moduljával hajtható végre. Kattintson a *Hozzáadás* gombra, majd adja meg az NFS-kiszolgáló gépnevét, az importálandó könyvtárakat, valamint a csatolási pontot, amelyen a könyvtár helyileg felcsatolásra kerül. A módosítások akkor lépnek életbe, ha az első párbeszédablakban rákattint a *Befejezés* gombra.

Az *NFS-beállítások* lapon kattintson a *Tűzfalport megnyitása* pontra annak érdekében, hogy a tűzfal engedélyezze a szolgáltatás elérését a távoli számítógépekről. A tűzfal állapota a jelölőnégyzet mellett látható. NFSv4 használata esetén győződjön meg róla, hogy az *NFSv4 engedélyezése* meg van jelölve, és az *NFSv4 tartománynév* ugyanazt az értéket tartalmazza, mint amelyet az NFSv4-kiszolgáló használ. Az alapértelmezett tartomány a `localdomain`.

A módosítások elmentéséhez nyomja meg az *OK* gombot. Lásd: 27.1. ábra - NFS-kliens beállítása YaST segítségével (437. oldal)

A konfiguráció beíródik az `/etc/fstab` könyvtárba és a megadott fájlrendszer felcsatolódik. Ha a YaST konfigurációs klienst elindítja egy későbbi időpontban, akkor az a meglévő konfigurációt kiolvassa a fájlból.

27.1. ábra *NFS-kliens beállítása YaST segítségével*



27.3 Fájlrendszerek manuális importálása

A fájlrendszerek manuálisan is importálhatók az NFS-kiszolgálóból. Ennek előfeltétele egy futó RPC portleképező, amely az `rcrpcbind start` parancs `root` felhasználóként kiadásával indítható el. Ha ez az előfeltétel teljesül, a távoli exportált fájlrendszerek ugyanúgy csatolhatók fel a fájlrendszeren, mint a helyi merevlemezek, a `mount` parancs segítségével:

```
mount host:remote-path local-path
```

Ha például az nfs.example.com gépen lévő felhasználói könyvtárakat kell importálni, akkor használja a következő parancsot:

```
mount nfs.example.com:/home /home
```

27.3.1 Az automount szolgáltatás használata

A szokásos helyi eszközcsatolásokhoz hasonlóan az autofs démon távoli fájlrendszerek automatikus csatolásához is használható. Ehhez adja hozzá a következő bejegyzést az `/etc/auto.master` fájlhoz:

```
/nfsmounts /etc/auto.nfs
```

Ezután az `/nfsmounts` könyvtár a kliensen lévő összes NFS-sel csatolt fájlrendszer gyökere lesz, ha az `auto.nfs` fájl megfelelően létre lett hozva. Az `auto.nfs` név választásának kényelmi oka van, de tetszőleges név megadható. A kiválasztott fájlban (ha nem létezik, hozza létre) hozzon létre egy bejegyzést az összes NFS-sel csatolt fájlrendszerhez, a következő példában látható módon:

```
localdata –fstype=nfs server1:/data
nfs4mount –fstype=nfs4 server2:/
```

Aktiválja a beállításokat az `rcautofs start` paranccsal. Ehhez például az `/nfsmounts/localdata`, a server1 `/data` könyvtára NFS, a server2 `/nfsmounts/nfs4mount` könyvtára pedig az NFSv4 segítségével kerül felcsatolásra.

Ha az `/etc/auto.master` fájl az autofs szolgáltatás futása közben módosul, akkor az automountert újra kell indítani a módosítások életbe léptetése érdekében. Ezt az `rcautofs restart` paranccsal hajtsa végre.

27.3.2 Az /etc/fstab manuális módosítása

Egy NFSv3 segítségével csatolt könyvtár szokásos bejegyzése az `/etc/fstab` fájlban így néz ki:

```
nfs.example.com:/data /local/path nfs rw,noauto 0 0
```

Az NFSv4-csatolások az `/etc/fstab` fájlhoz manuálisan is hozzáadhatók. E csatolások esetén az `nfs` helyett `nfs4` értéket használjon a harmadik oszlopban, és ügyeljen rá, hogy a távoli fájlrendszer után `/` karaktert adjon meg (a példában *`nfs.example.com:/`*) után az első oszlopban. Egy NFSv3 segítségével csatolt könyvtár szokásos bejegyzése az `/etc/fstab` fájlban így néz ki:

```
nfs.example.com:/ /local/pathv4 nfs4 rw,noauto 0 0
```

A `noauto` paraméter megakadályozza, hogy a fájlrendszer automatikusan fel legyen csatolva a rendszer indulásakor. Ha a fájlrendszert kézzel kívánja felcsatolni, akkor a parancs lerövidíthető a csatoláshoz és ilyenkor csak a csatolási pontot kell megadni, így:

```
mount /local/path
```

Ügyeljen rá, hogy ha nem adja meg a `noauto` paramétert, akkor a rendszer indulásakor e fájlrendszerek csatolását a rendszer inicializációs parancsfájljai fogják elvégezni.

27.4 Fájlrendszerek exportálása YaST segítségével

A YaST segítségével a hálózat egyik gépe beállítható NFS-kiszolgálónak – ez egy olyan kiszolgáló, amely a könyvtárakat és fájlokat exportálja az összes olyan gépre, amely számára engedélyezik e fájlok elérését. Így például egy csoport összes felhasználója számára biztosíthatók alkalmazások anélkül, hogy azokat helyileg telepíteni kéne minden gépen. Ilyen kiszolgáló telepítéséhez indítsa el a YaST-ot és válassza ki a *Hálózati szolgáltatások* > *NFS-kiszolgáló* menüpontot. Megjelenik egy, az 27.2. ábra - NFS-kiszolgálókonfigurációs eszköz (440. oldal) ábrán látható párbeszédablak.

27.2. ábra *NFS-kiszolgálókonfigurációs eszköz*

Következő lépésként válassza ki az *NFS-kiszolgáló indítása* pontot és adja meg az *NFSv4-tartomány nevét*.

Kattintson a *GSS biztonság engedélyezése* gombra, ha a kiszolgálóhoz biztonságos hozzáférésre van szüksége. Ennek előfeltétele, hogy a Kerberos telepítve legyen a tartományban, továbbá a kiszolgáló és a kliensek is támogassák a Kerberost. Kattintson a *Tovább* gombra.

A felső szövegmezőben adja meg az exportálandó könyvtárakat. Alul adja meg a gépeket, amelyek számára hozzáférést kell biztosítani ezekhez a könyvtárakhoz. Ezt a párbeszédablakot az 27.3. ábra - NFS-kiszolgáló beállítása YaST segítségével (441. oldal) ábra mutatja. Az ábra olyan példahelyzetet mutat, amelyben az NFSv4 az előző párbeszédablakban engedélyezve lett. A jobb oldalon megjelennek a `Csatlakoztatott kiszolgálók`. További részleteket a bal oldali ablakrészben látható súgó tartalmaz. A párbeszédablak alsó részében minden géphez négy lehetőség állítható be: `egyes gép`, `hálózati csoportok`, `dzsókernevek` és `IP-hálózatok`. A lehetőségek

részletesebb leírását az `exports` kézikönyvoldala tartalmazza. A beállítás befejezéséhez kattintson a *Befejezés* gombra.

27.3. ábra *NFS-kiszolgáló beállítása YaST segítségével*

FONTOS: Automatikus tűzfalbeállítás

Ha van a rendszeren aktív tűzfal (SuSEfirewall2), akkor a YaST a *Tűzfalport megnyitása* lehetőség kiválasztására átalakítja a tűzfal konfigurációját és engedélyezi az `nfs` szolgáltatást.

27.4.1 NFSv4-kliensek exportálása

Jelölje meg az *NFSv4 engedélyezése* lehetőséget az NFSv4-kliensek támogatásához. Az NFSv3-kliensek továbbra is hozzá tudnak férni a kiszolgáló exportált könyvtáraihoz,

amennyiben azok megfelelően lettek exportálva. Ennek részletes leírása: 27.4.3. - v3 és v4 exportok együttes használata (445. oldal).

Az NFSv4 aktiválása után adjon meg egy megfelelő tartománynevet. Győződjön meg róla, hogy a beírt név megegyezik az adott kiszolgálót elérő valamelyik NFSv4-kliens `/etc/idmapd.conf` fájljában lévővel. Ez az idmapd szolgáltatás paramétere, amely az NFSv4 támogatáshoz (a kiszolgálón és kliensen egyaránt) szükséges. Ha nincsenek különleges igényei, akkor hagyja meg az alapértelmezett (`localdomain`) beállítást. További információkért lásd: 27.7. - További információk (450. oldal).

Kattintson a *Tovább* gombra. A következő párbeszédablak két részre van osztva. A felső részben két oszlop található, *Könyvtárak* és *Csatlakoztatott kiszolgálók* néven. A *Könyvtárak* egy közvetlenül szerkeszthető oszlop, amely az exportálandó könyvtárakat sorolja fel.

Rögzített klienshalmaz esetén kétféle könyvtár exportálható – pszeudo-root fájlrendszerként viselkedő, illetve a pszeudo-fájlrendszer bármely alkönyvtárához rendelt könyvtár. Ez a pszeudo-fájlrendszer kiindulási pontként szolgál: ezalatt található az adott klienshalmaz összes exportált fájlrendszere. Egy klienshez vagy a kliensek halmazához a kiszolgálón csak egy könyvtár állítható be pszeudo-rootként az exportáláshoz. A kliens számára több könyvtár úgy exportálható, ha a könyvtárakat a pszeudo-root egyik meglévő alkönyvtárához rendeli.

27.4. ábra *Könyvtárak exportálása NFSv4 segítségével*

A párbeszédablak alsó részében adja meg az adott könyvtár kliensét (dzsókernév) és exportálási lehetőségeit. Miután a felső részben felvett egy könyvtárat, automatikusan megjelenik egy másik párbeszédablak a kliens és a beállítási adatok megadásához. Ezután új kliens (klienshalmaz) hozzáadásához kattintson a *Gép hozzáadása* menüpontra.

A megjelenő kis párbeszédablakban adja meg a gép dzsókernevét. Minden géphez négyféle dzsókernév állítható be: egyetlen gép (név vagy IP-cím), hálózati csoportok, dzsókernév (a `*` például azt jelenti, hogy az összes gép el tudja érni a kiszolgálót), és az IP-hálózatok. A *Beállítások* menüben adja meg az `fsid=0` értéket a beállítások vesszővel elválasztott listájában a könyvtár pszeudo-rootként történő beállításához. Ha a könyvtárat egy másik, már beállított pszeudo-root alatt lévő könyvtárhoz kell rendelni, akkor győződjön meg róla, hogy a cél hozzárendelési útvonal a beállításlistában `bind=/target/path` formátumban van megadva.

Tételezzük fel például, hogy az `/exports` könyvtár lett kiválasztva pszeudo-root könyvtárként a kiszolgálóhoz hozzáférő összes kliens számára. Vegye fel ezt a felső

részben és győződjön meg róla, hogy a könyvtárhoz megadott beállítás tartalmazza az `fsid=0` értéket. Ha van másik könyvtár, a `/data`, amelyet szintén NFSv4-gyel kell exportálni, akkor vegye fel ezt a könyvtárat is a felső részben. A beállítások megadása során győződjön meg róla, hogy a `bind=/exports/data` megtalálható a listában, és hogy az `/exports/data` az `/exports` már meglévő alkönyvtára. A *Csatlakoztatott kiszolgálók* rész a `bind=/target/path` minden módosítását tükrözi, legyen az akár törlés, hozzáadás vagy az érték módosítása. Ez az oszlop nem közvetlenül szerkeszthető, hanem összegzi a könyvtárakat és azok jellemzőit. Ha minden adatot beírt, kattintson a *Befejezés* gombra a beállítás befejezéséhez, illetve az *Indítás* gombra a szolgáltatás újraindításához.

27.4.2 NFSv3- és NFSv2-exportok

Mielőtt a *Tovább* gombra kattintana, győződjön meg róla, hogy az *NFSv4 engedélyezése* nincs bejelölve a kezdeti párbeszédablakban.

A következő párbeszédablak két részre van osztva. A felső szövegmezőben adja meg az exportálandó könyvtárakat. Alul adja meg a gépeket, amelyek számára hozzáférést kell biztosítani ezekhez a könyvtárakhoz. Minden géphez négyféle dzsókernév állítható be: egyetlen gép (név vagy IP-cím), hálózati csoportok, dzsókernév (a `*` például azt jelenti, hogy az összes gép el tudja érni a kiszolgálót), és az IP-hálózatok.

Ezt a párbeszédablakot az 27.5. ábra - Könyvtárak exportálása NFSv2 és v3 segítségével (445. oldal) ábra mutatja. A lehetőségek átfogóbb magyarázatát a `man exports` parancs kimenete tartalmazza. A beállítás befejezéséhez kattintson a *Befejezés* gombra.

27.5. ábra *Könyvtárak exportálása NFSv2 és v3 segítségével*

27.4.3 v3 és v4 exportok együttes használata

Az NFSv3- és NFSv4-exportok együtt is jelen lehetnek a kiszolgálón. Az NFSv4-támogatás engedélyezése után a kezdeti beállítási párbeszédablakban azokat az exportokat, amelyekhez az `fsid=0` és `bind=/target/path` nincs megadva a beállításlistában, a rendszer v3 exportoknak tekinti. Tekintse meg a következő példát: 27.3. ábra - NFS-kiszolgáló beállítása YaST segítségével (441. oldal). Ha a *Könyvtár hozzáadása* paranccsal felvesz egy újabb könyvtárat (például a `/data2`-t), akkor a megfelelő beállításlistában ne adja meg az `fsid=0` vagy `bind=/target/path` értéket. Ebben az esetben ez az export v3-exportként viselkedik.

FONTOS

Automatikus tűzfalbeállítás

Ha a rendszeren aktív a SuSEfirewall2, akkor a YaST a `Tűzfalport megnyitása` lehetőség kiválasztására átalakítja a tűzfal konfigurációját és engedélyezi az *nfs* szolgáltatást.

27.5 Fájlrendszer manuális exportálása

Az NFS exportálási szolgáltatás konfigurációs fájljai: `/etc/exports` és `/etc/sysconfig/nfs`. Ezen fájlokon felül még az `/etc/idmapd.conf` szükséges az NFSv4-kiszolgáló beállításához. A szolgáltatások indításához vagy újraindításához futtassa az `rcnfsserver restart` parancsot. Ez elindítja az `rpc.idmapd`-t is, ha az `/etc/sysconfig/nfs` fájlban az NFSv4 be van állítva. Az NFS-kiszolgáló használatához szükség van egy működő RPC-portleképezőre. Ezért a portleképező szolgáltatást is indítsa el vagy indítsa újra az `rcrpcbind restart` paranccsal.

27.5.1 Fájlrendszerek exportálása NFSv4 segítségével

Az NFSv4 az NFS protokoll openSUSE rendszeren rendelkezésre álló legújabb változata. A könyvtárak beállítása az NFSv4 változattal történő exportáláshoz kissé eltér az előző NFS-változatoktól.

Az /etc/exports fájl

A fájl bejegyzések listájából áll. Minden bejegyzés egy könyvtárat jelöl, amely meg van osztva, illetve a megosztás módját is jelzi. Az `/etc/exports` egy szokásos bejegyzése a következőkből áll:

```
/shared/directory host(option_list)
```

Például:

```
/export 192.168.1.2(rw,fsid=0,sync)
/data 192.168.1.2(rw,bind=/export/data,sync)
```

E könyvtárak – az úgynevezett pszeudo-root fájlrendszer – esetén az `fsid=0` kell, hogy szerepeljen a paraméterlistában. Itt a `192.168.1.2` IP-címet használjuk. Használhatja a gép nevét, illetve megadhat a gépek halmazát jelző dzsókernevet (`*.abc.com`, `*` stb.) vagy hálózati csoportokat.

Kliensek rögzített halmaza esetén csak két könyvtártípus exportálható NFSv4 segítségével:

- Pszeudo-root fájlrendszerként kiválasztott egyetlen könyvtár. Ebben a példában az `/export` a pszeudo-root könyvtár, mivel az `fsid=0` meg van adva a bejegyzéshez a beállításlistában.
- A pszeudo-fájlrendszer egy meglévő alkönyvtárához rendelt könyvtárak. A fenti példában a `/data` olyan könyvtár, amely az `/export` pszeudo-fájlrendszer meglévő alkönyvtárához (`/export/data`) van rendelve.

A pszeudo-fájlrendszer a legfelső szintű könyvtár: ez alatt található az összes NFSv4-gyel exportált fájlrendszer. Egy adott klienshez vagy kliensek adott halmazához a kiszolgálón csak egy könyvtár állítható be pszeudo-rootként az exportáláshoz. Ehhez a klienshez vagy klienshalmazhoz több könyvtár egyszerre úgy exportálható, ha azokat a pszeudo-root meglévő alkönyvtárához rendeli.

/etc/sysconfig/nfs

Ez a fájl tartalmaz néhány paramétert, amelyek meghatározzák az NFSv4 kiszolgáló démon viselkedését. Az NFSv4_SUPPORT paraméternek 'yes' értéket kell adni. Ez a paraméter határozza meg, hogy az NFS-kiszolgáló támogatja-e az NFSv4-exportokat és -klienseket.

/etc/idmapd.conf

A Linux gép minden használójának rendelkeznie kell névvel és azonosítóval. Az idmapd végzi a név-azonosító leképezést a kiszolgáló NFSv4-kéréseihez, illetve válaszol a kliensnek. NFSv4 esetén ennek a kiszolgálón és a kliensen is futnia kell, mivel az NFSv4 csak neveket használ a saját kommunikációjában.

Győződjön meg róla, hogy rendelkezésre áll egy egységes módszer a felhasználónevek és azonosítók (uid) felhasználókhoz rendelésére azokon a gépeken, amelyeken a fájl-

rendszereket NFS-sel osztják meg. Ez NIS, LDAP vagy a tartomány egyéb egységes tartományhitelesítési mechanizmusa segítségével oldható meg.

A megfelelő működés érdekében a klienshez és kiszolgálóhoz tartozó `Tartomány` (Domain) paraméter értékének meg kell egyeznie az adott fájlban. Ha nem biztos a dolgában, hagyja a tartományt a `localdomain` értéken mind a kiszolgáló, mind a kliens fájljaiban. Példa a konfigurációs fájlra:

```
[General]

Verbosity = 0
Pipefs-Directory = /var/lib/nfs/rpc_pipefs
Domain = localdomain

[Mapping]

Nobody-User = nobody
Nobody-Group = nobody
```

Csak akkor módosítsa ezeket a paramétereket, ha pontosan tudja, mit csinál. További részleteket az `idmapd` és `idmapd.conf` kézikönyvoldala tartalmaz: `man idmapd`, `man idmapd.conf`.

Szolgáltatások elindítása és leállítása

Az `/etc/exports` vagy `/etc/sysconfig/nfs` módosítása után indítsa el vagy indítsa újra az NFS-kiszolgáló szolgáltatást az `rcnfsserver restart` parancs segítségével. Az `/etc/idmapd.conf` módosítása után töltse újra a konfigurációs fájlt a következő paranccsal: `killall -HUP rpc.idmapd`.

Ha a szolgáltatásnak rendszerindításkor el kell indulnia, akkor futtassa le a `chkconfig nfsserver on` parancsot.

27.5.2 Fájlrendszerek exportálása NFSv2 és NFSv3 segítségével

Ez csak az NFSv3- és NFSv2-exportokra vonatkozik. Az NFSv4-exportokról az 27.4.1. - NFSv4-kliensek exportálása (441. oldal) rész szól.

A fájlrendszerek NFS-en keresztüli exportálásához két konfigurációs fájlt kell módosítani: az `/etc/exports` és `/etc/sysconfig/nfs` fájlokat. Az `/etc/exports` fájl bejegyzéseinek szokásos formátuma:

```
/shared/directory host(list_of_options)
```

Például:

```
/export 192.168.1.2(rw,sync)
```

Itt az `/export` könyvtár meg van osztva a 192.168.1.2 géppel, az `rw,sync` beállításlistával. Ez az IP-cím helyettesíthető a kliens nevével vagy kliensek halmazával dzsókernév (például a `*.abc.com`) vagy akár hálózati csoportok használatával.

A beállítások és jelentésük részletes magyarázatát az `exports` kézikönyvoldala (`man exports`) tartalmazza.

Az `/etc/exports` vagy `/etc/sysconfig/nfs` módosítása után indítsa és vagy indítsa újra az NFS szolgáltatást az `rcnfsserver restart` parancs segítségével.

27.6 NFS és Kerberos

Ha az NFS-hez Kerberos-hitelesítést kíván használni, akkor a GSS biztonságot engedélyezni kell. Ehhez válassza ki a *GSS biztonság engedélyezése* menüpontot a kezdeti YaST párbeszédablakban. E funkció használatához szükség van egy működő Kerberos kiszolgálóra. A YaST nem állítja be a kiszolgálót, csak felhasználja a rendelkezésre álló funkcionalitást. Ha Kerberos alapú hitelesítést kíván használni a YaST-konfiguráció mellett, akkor az NFS-beállítások futtatása előtt legalább az alábbi lépéseket el kell végeznie:

1. Győződjön meg róla, hogy a kiszolgáló és a kliens ugyanabban a Kerberos-tartományban található. Ez azt jelenti, hogy ugyanazt a KDC (Key Distribution Center – Kulcselosztó központ) kiszolgálót érik el és ugyanazon a `krb5.keytab` fájlon osztoznak (ennek alapértelmezett helye minden gépen: `/etc/krb5.keytab`).

2. Indítsa el a gssd szolgáltatást a kliensen az `rcgssd start` parancs segítségével.

3. Indítsa el az svcgssd szolgáltatást a kiszolgálón az `rcsvcgssd start` parancs segítségével.

A Kerberosszal védett NFS beállításával kapcsolatos információt a következő hivatkozásokon talál: 27.7. - További információk (450. oldal).

27.7 További információk

Az `exports`, `nfs` és `mount` parancsok kézikönyvoldalán túl az NFS-kiszolgáló és -kliens beállításával kapcsolatos információ az `/usr/share/doc/packages/nfsidmap/README` fájlban található. Online dokumentációt a következő webes dokumentumok tartalmaznak:

- A részletes műszaki dokumentáció online változata a SourceForge [`http://nfs.sourceforge.net/`]-on található.
- A Kerberosszal védett NFS beállításával kapcsolatos útmutatást a következő címen talál: NFS Version 4 Open Source Reference Implementation [`http://www.citi.umich.edu/projects/nfsv4/linux/krb5-setup.html`].
- Ha az NFSv4-gyel kapcsolatban kérdései vannak, akkor forduljon a Linux NFSv4 Gyakran ismételt kérdések [`http://www.citi.umich.edu/projects/nfsv4/linux/faq/`] dokumentumhoz.

28 Az Apache HTTP kiszolgáló

A http://www.netcraft.com/ címen olvasható felmérés szerint, több mint 70 százalékos részesedésével az Apache HTTP kiszolgáló (Apache) a világ legnépszerűbb webkiszolgálója. Az Apache, amelyet az Apache Software Foundation (http://www.apache.org/) fejleszt, a legtöbb operációs rendszeren elérhető. Az openSUSE az Apache 2.2-es verzióját tartalmazza. A jelen fejezetben bemutatjuk a webkiszolgáló telepítését és beállítását; az SSL, a CGI és más modulok használatát; valamint az Apache webkiszolgálóval kapcsolatos hibaelhárítást.

28.1 Gyorskalauz

E szakasz alapján az Apache gyorsan beüzemelhető és használatba vehető. Az Apache telepítésére és beállítására csak a `root` jogosult.

28.1.1 Követelmények

Az Apache webkiszolgáló telepítése előtt győződjön meg róla, hogy az alábbi követelmények teljesülnek:

1. A gépen a hálózat helyesen be van állítva. További információ erről a témakörről: 20. fejezet - *A hálózatkezelés alapjai* (279. oldal).

2. A gépen az idő pontosságát egy időkiszolgálóval való szinkronizálás biztosítja. Ez azért szükséges, mert a HTTP protokoll egyes részei függenek a helyes időtől.

További ismeretek erről a témakörről a 24. fejezet - *Időszinkronizálás NTP-vel* (379. oldal) részben találhatók.

3. A legfrissebb lbiztonsági frissítések telepítve vannak. Ha kétségei lennének, futtassa le a YaST Online frissítést.

4. A webkiszolgáló alapértelmezett portjának (a 80-as port) nyitva kell lennie a tűzfalon. Ehhez állítsa be a SUSEFirewall2-t úgy, hogy az engedje a *HTTP kiszolgáló* szolgáltatást a külső zónában. Ez elvégezhető a YaST segítségével. Ennek részletes leírása: 33.4.1. - Tűzfal beállítása a YaST segítségével (537. oldal).

28.1.2 Telepítés

Az Apache a openSUSE rendszeren alapértelmezés szerint nincs telepítve. A telepítéséhez indítsa el a YaST-ot, majd válassza ki a *Szoftver* > *Szoftvertelepítés* modult. Ezután válassza ki a *Szűrő* > *Minták* részt, és ott a *Kiszolgálófunkciók* szakaszban a *Web és LAMP kiszolgáló* részt. A telepítési folyamat befejezéséhez erősítse meg a függő csomagok telepítését.

Az Apache egy szokásos, előre definiált, „azonnal használható” konfigurációval kerül telepítésre. A telepítés során felkerül a többprocesszoros `apache2-prefork` modul, valamint a PHP5 modul is. A modulokkal kapcsolatos további információ: 28.4. - Modulok telepítése, aktiválása és beállítása (471. oldal).

28.1.3 Indítás

Az Apache indításához, illetve annak biztosításához, hogy rendszerindításkor az Apache is automatikusan elinduljon, futtassa a YaST-ot és válassza ki a *Rendszer* > *Rendszerszolgáltatások (futási szint)* részt. Keresse ki az *apache2* pontot, majd *engedélyezze* a szolgáltatást. A webkiszolgáló azonnal elindul. A módosítások elmentéséhez nyomja meg a *Befejezés* gombot. A rendszer úgy lesz beállítva, hogy a 3-as és 5-ös futási szinteken rendszerindításkor az Apache is automatikusan elinduljon. További információ a openSUSE futási szintjeiről és a YaST futásiszint-szerkesztőjének leírása: 14.2.3. - Rendszerszolgáltatások (futási szintek) beállítása a YaST segítségével (195. oldal).

Az Apache a parancsértelmezőből történő indításához írja be, hogy `rcapache2 start`. Annak biztosításához, hogy az Apache automatikusan elinduljon a 3-as és 5-ös futási szinteken, használja a `chkconfig -a apache2` parancsot.

Ha nem kapott hibaüzeneteket az Apache indításakor, akkor a webkiszolgálónak mostanra futnia kell. Indítson el egy böngészőt és írja be, hogy `http://localhost/`. Egy Apache tesztoldalnak kell megjelennie, „It works!” (működik) felirattal. Ha nem ez az oldal jelenik meg, forduljon az alábbi részhez: 28.8. - Hibaelhárítás (491. oldal).

Most, hogy a webkiszolgáló fut, felveheti saját dokumentumait, módosíthatja a konfigurációt az igényeknek megfelelően, vagy éppen kibővítheti a funkcionalitást további modulok telepítésével.

28.2 Az Apache beállítása

A openSUSE Apache kiszolgálója kétféleképpen is beállítható: a YaST segítségével vagy kézzel. A kézi beállítás részletesebb lehet, de a YaST GUI használata jóval kényelmesebb.

FONTOS: A konfiguráció módosítása

Az Apache legtöbb konfigurációs értékének módosítása csak az Apache újraindítása vagy újra betöltése után lép életbe. Ez a YaST használatakor automatikusan megtörténik, ha a beállítást úgy fejezi be, hogy a *HTTP szolgáltatás* értéke *Engedélyezett*. A kézi újraindítás módját a 28.3. - Az Apache elindítása és leállítása (469. oldal) rész írja le. A legtöbb konfigurációs módosításhoz csak újra kell tölteni az Apache programot az `rcapache2 reload` paranccsal.

28.2.1 Az Apache kézi beállítása

Az Apache kézi beállítása esetén a sima szöveges konfigurációs fájlokat kézzel kell módosítani a `root` felhasználó nevében.

Konfigurációs fájlok

Az Apache konfigurációs fájljai két helyen találhatók:

- `/etc/sysconfig/apache2`
- `/etc/apache2/`

/etc/sysconfig/apache2

Az `/etc/sysconfig/apache2` könyvtárban találhatók az Apache egyes globális beállításai, például a betöltendő modulok, további figyelembe veendő konfigurációs fájlok, a kiszolgáló indításakor figyelembe veendő jelzők, illetve a parancssorba beírandó jelzők. A fájl minden beállítási lehetősége alaposan le van írva, ezért itt nem foglalkozunk velük. Egy általános célú webkiszolgálóhoz az `/etc/sysconfig/apache2` fájl beállításai mindenféle konfigurációs igényhez meg kell, hogy feleljenek.

/etc/apache2/

Az `/etc/apache2/` könyvtárban található az Apache összes többi konfigurációs fájlja. Az alábbiakban leírjuk az egyes fájlok szerepeit. Minden egyes fájlban többféle beállítási lehetőség (másik gyakori nevén *direktíva*) található. Az egyes fájlok minden beállítási lehetősége alaposan le van írva, ezért itt nem foglalkozunk velük.

Az Apache konfigurációs fájlok az alábbi módon szerveződnek:

```
/etc/apache2/
 |
 |- charset.conv
 |- conf.d/
 |   |
 |   |- *.conf
 |
 |- default-server.conf
 |- errors.conf
 |- httpd.conf
 |- listen.conf
 |- magic
 |- mime.types
 |- mod_*.conf
 |- server-tuning.conf
 |- ssl.*
 |- ssl-global.conf
 |- sysconfig.d
 |   |
 |   |- global.conf
 |   |- include.conf
 |   |- loadmodule.conf . .
 |
 |- uid.conf
 |- vhosts.d
 |   |- *.conf
```

Az /etc/apache2/ Apache-konfigurációs fájljai

`charset.conv`
: Az egyes nyelvekhez használt karakterkészleteket adja meg. Ne módosítsa.

`conf.d/*.conf`
: Más modulok által felvett konfigurációs fájlok. Ezek a konfigurációs fájlok szükség esetén a virtuális gépek beállításánál használhatók. Példák a `vhosts.d/vhost.template` fájlban láthatók. Használatukkal eltérő modulkészletek állíthatók be az egyes virtuális gépekhez.

`default-server.conf`
: Általános beállítások az összes virtuális géphez, ésszerű alapértelmezésekkel. Az értékek módosítása helyett írja felül őket egy virtuálisgép-konfigurációval.

`errors.conf`
: Azt szabályozza, hogyan reagáljon az Apache a hibákra. Az összes virtuális gépre vonatkozóan az üzenetek testreszabásához ezt a fájlt kell módosítani. Egyébként ezeket a direktívákat a virtuálisgép-beállításoknál egyenként lehet felülírni.

`httpd.conf`
: Az Apache kiszolgáló fő konfigurációs fájlja. Kerülje ennek a fájlnak a módosítását. Leginkább csak beágyazó utasításokat és általános beállításokat tartalmaz. Az általános beállításokat inkább az itt felsorolt konfigurációs fájlokban írja felül. A gépspecifikus beállításokat (például a fő dokumentumkönyvtárat) a virtuálisgép-konfigurációkban módosítsa.

`listen.conf`
: Az Apache kiszolgálót meghatározott IP-címekhez és portokhoz rendeli. Szintén itt kell beállítani a név alapú virtuálisgép-kezelést (lásd: „Név alapú virtuális gépek” szakasz (458. oldal)).

`magic`
: A mime_magic modul adatai, amely segít az Apache-nak automatikusan meghatározni egy ismeretlen fájl típusát. Ne módosítsa.

`mime.types`
: A rendszer által ismert MIME-típusok (ez valójában csak egy hivatkozás az `/etc/mime.types` fájlra). Ne módosítsa. Ha további, itt még fel nem sorolt MIME-tí-

pusokra van szükség, akkor azokat a `mod_mime-defaults.conf` fájlba vegye fel.

`mod_*.conf`
: Az alapértelmezés szerint telepített modulok konfigurációs fájljai. Részletek: 28.4. - Modulok telepítése, aktiválása és beállítása (471. oldal). Ne feledje, hogy az opcionális modulok konfigurációs fájljai a `conf.d` könyvtárban találhatók.

`server-tuning.conf`
: A különféle MPM-ek (lásd: 28.4.4. - Többprocesszoros modulok (MPM) (476. oldal)) konfigurációs direktíváit, valamint az Apache teljesítményét szabályozó általános konfigurációs beállításokat tartalmazza. Ha módosítja, feltétlenül alaposan tesztelje le a webkiszolgáló működését.

`ssl-global.conf` és `ssl.*`
: Globális SSL-konfigurációs és SSL-tanúsítványadatok. Részletek: 28.6. - Biztonságos webkiszolgáló beállítása SSL használatával (482. oldal).

`sysconfig.d/*.conf`
: Az `/etc/sysconfig/apache2` fájlból automatikusan előállított konfigurációs fájlok. Ne módosítsa ezeket a fájlokat –helyettük módosítsa az `/etc/sysconfig/apache2` fájlt. Ebbe a könyvtárba ne tegyen más konfigurációs fájlokat.

`uid.conf`
: Azt határozza meg, mely felhasználó- és csoportazonosító alatt fusson az Apache. Ne módosítsa.

`vhosts.d/*.conf`
: A virtuális gépek beállításai ide kerüljenek. A könyvtár tartalmaz sablonfájlokat SSL-es és SSL nélküli virtuális gépek számára egyaránt. Minden `.conf`-ra végződő nevű fájl automatikusan bekerül az Apache konfigurációjába. Részletek: „Virtuális gépek konfigurációja” szakasz (456. oldal).

Virtuális gépek konfigurációja

A *virtuális gép* kifejezés az Apache-nak arra a képességére utal, hogy képes több URI-t (univerzális erőforrás-azonosítót) kiszolgálni ugyanarról a fizikai gépről. Ez azt jelenti,

hogy több tartományt , tehát például a www.example.com és www.example.net tartományokat is képes kiszolgálni egyetlen fizikai gépen futó ugyanazon webkiszolgáló.

Bevált gyakorlat a virtuális gépek használata az adminisztráció megkönnyítése (hiszen csak egyetlen webkiszolgálót kell karbantartani) és a hardverköltségek leszorítása érdekében (nincs szükség külön kiszolgálóra minden egyes tartományhoz). A virtuális gépek lehetnek név alapúak, IP alapúak és port alapúak.

Az összes meglévő virtuális gép kilistázásához használja a `httpd2 -S` parancsot. Ennek kimenete az alapértelmezett kiszolgáló és az összes virtuális gép listája, IP-címeikkel és a portokkal együtt, amelyeken figyelnek. A lista ezenfelül tartalmaz egy bejegyzést mindegyik virtuális géphez, amely a konfigurációs fájlok helyét mutatja.

A virtuális gépek a YaST segítségével is beállíthatók (lásd: „Virtuális gépek” szakasz (465. oldal)), de a konfigurációs fájlok kézzel is módosíthatók. Alapértelmezés szerint a openSUSE rendszerben található Apache úgy van előkészítve, hogy egy virtuális géphez az `/etc/apache2/vhosts.d/` egy konfigurációs fájlja tartozik. A könyvtár összes `.conf` kiterjesztésű fájlja automatikusan bekerül a konfigurációba. A basic template for a virtual host is provided in this directory (`vhost.template` or `vhost-ssl.template` for a virtual host with SSL support).

TIPP: Mindig hozzon létre virtuális gépeket

Célszerű mindig virtuális gépeket készíteni, még akkor is, ha a webkiszolgáló csak egyetlen tartományt szolgál ki. Ebben az esetben ugyanis nemcsak a tartományspecifikus beállítások kerülnek egy fájlba, hanem bármikor egyszerűen vissza lehet állni egy működő alapkonfigurációra a virtuális gép konfigurációs fájljának áthelyezésével, törlésével vagy átnevezésével. Ugyanezen okokból érdemes külön konfigurációs fájlokat készíteni az egyes virtuális gépekhez.

A `<VirtualHost></VirtualHost>` szakasz tartalmazza az adott tartományra vonatkozó adatokat. Amikor az Apache egy kérést fogad egy klienstől egy már definiált virtuális gépre vonatkozóan, akkor az e szakaszban található direktívákat fogja használni. Szinte minden direktíva használható virtuálisgép-környezetben. További részletek az Apache beállítási lehetőségeivel kapcsolatban: `http://httpd.apache.org/docs/2.2/mod/quickreference.html`.

Név alapú virtuális gépek

Név alapú virtuális gépek használata esetén egy IP-címhez egynél több webhely is tartozhat. Az Apache a kliens által küldött HTTP-fejlécben található "host" mező alapján rendeli össze a kérést a virtuálisgép-definíciók között található megfelelő `ServerName` bejegyzéssel. Ha nincs megfelelő `ServerName` bejegyzés, akkor viszont az elsőként megadott virtuális gépet fogja használni alapértelmezésként.

A `NameVirtualHost` direktíva jelzi az Apache számára, hogy mely IP-címeken (és esetleg mely portokon) kell figyelnie a klienskérések HTTP-fejlécében a tartománynevet is. Ezt a lehetőséget az `/etc/apache2/listen.conf` konfigurációs fájlban kell beállítani.

Az első paraméter lehet egy teljesen megadott tartománynév, de célszerűbb az IP-címet használni. A második paraméter a portszám, amely elhagyható. Alapértelmezés szerint az Apache a 80-as portot használja, amelyet egyébként a `Listen` direktívával lehet beállítani.

A `*` helyettesítő karakter használható mind az IP-cím, mind a portszám esetében, és azt jelenti, hogy minden csatolón érkezhetnek kérések. Az IPv6-címeket szögletes zárójelekbe kell tenni.

28.1 példa *A név alapú VirtualHost bejegyzések fajtái*

```
# NameVirtualHost IP-address[:Port]
NameVirtualHost 192.168.3.100:80
NameVirtualHost 192.168.3.100
NameVirtualHost *:80
NameVirtualHost *
NameVirtualHost [2002:c0a8:364::]:80
```

Név alapú virtuális gép beállításakor a nyitó `VirtualHost` címke paraméterként kapja a korábban a `NameVirtualHost` sorban beállított IP-címet vagy teljesen megadott tartománynevet. A `NameVirtualHost` direktívában korábban megadott portszám elhagyható.

A * helyettesítő karakter szintén használható az IP-cím helyett. Ez a szintaxis csak akkor használható, ha korábban helyettesítő karaktert használt, `NameVirtualHost *` módon. Ha IPv6-címeket használ, azokat szögletes zárójelekbe kell tenni.

28.2 példa *Név alapú VirtualHost direktívák*

```
<VirtualHost 192.168.3.100:80>
  ...
</VirtualHost>

<VirtualHost 192.168.3.100>
  ...
</VirtualHost>

<VirtualHost *:80>
  ...
</VirtualHost>

<VirtualHost *>
  ...
</VirtualHost>

<VirtualHost [2002:c0a8:364::]>
  ...
</VirtualHost>
```

IP alapú virtuális gépek

Ha így állít be virtuális gépeket, akkor egy géphez több IP-címnek is kell tartoznia. Egy Apache-példány több tartományt is kiszolgál, amelyek mindegyikéhez különböző IP-cím tartozik.

A fizikai kiszolgálón minden egyes IP alapú virtuális géphez külön IP-címnek kell tartoznia. Ha a gépben fizikailag nincs több hálózati kártya, akkor virtuális hálózati csatolók (másodlagos IP-címek) is használhatók.

Az alábbi példában bemutatunk egy Apache-rendszert, amelyik az `192.168.3.100` IP-című gépen fut, de két további IP-címen (`192.168.3.101` és `192.168.3.102`) két tartományt szolgál ki. Egy külön `VirtualHost` blokkra van szükség mindegyik virtuális kiszolgálóhoz.

28.3 példa *IP alapú VirtualHost direktívák*

```
<VirtualHost 192.168.3.101>
  ...
</VirtualHost>

<VirtualHost 192.168.3.102>
  ...
</VirtualHost>
```

Itt a `VirtualHost` direktívák csak a `192.168.3.100` címtől eltérő csatolókhoz vannak megadva. Ha megad egy `Listen` direktívát a `192.168.3.100` címhez, akkor egy külön IP alapú virtuális gépet létre kell hozni, amelyik válaszol az adott csatolóra érkező HTTP-kérésekre – ellenkező esetben az Apache az (`/etc/apache2/default-server.conf`) fájlban megadott alapértelmezett direktívákat fogja használni.

Virtuális gépek alapszintű beállításai

Ahhoz, hogy a virtuális gép működjön, legalább az alábbi direktívákat be kell állítani minden egyes virtuális gép konfigurációjában. További részletek az `/etc/apache2/vhosts.d/vhost.template` sablonfájlban találhatók.

`Kiszolgálónév`
: A teljesen megadott tartománynév, amelyen a gép megszólítható.

`DocumentRoot`
: Annak a könyvtárnak az elérési útja, ahonnan az Apache-nak ki kell szolgálnia az adott gép fájljait. Biztonsági okokból alapértelmezés szerint tiltott a teljes fájlrendszerhez való hozzáférés, így ezt a könyvtárat külön engedélyezni kell egy `Directory` szakasszal.

`ServerAdmin`
: A kiszolgáló rendszergazdájának e-mail címe. Ez a cím megjelenik például az Apache által előállított oldalakon.

`ErrorLog`
: A virtuális gép hibanaplófájlja. Bár nem kötelező külön hibanaplót készíteni minden egyes virtuális géphez, ez a szokásos gyakorlat, hiszen lényegesen megkönnyíti a hibák keresését. A `/var/log/apache2/` az alapértelmezett könyvtár, ahová az Apache naplófájljai kerülnek.

`CustomLog`
: A virtuális gép hozzáférésinapló-fájlja. Bár nem kötelező külön hozzáférési naplót készíteni minden egyes virtuális géphez, ez a szokásos gyakorlat, mert megkönnyíti a gépenkénti hozzáférési statisztikák készítését. A `/var/log/apache2/` az alapértelmezett könyvtár, ahová az Apache naplófájljai kerülnek.

Amint feljebb már említettük, biztonsági okokból alapértelmezés szerint tiltott a teljes fájlrendszerhez való hozzáférés. Éppen ezért külön kell engedélyezni azokat a könyvtárakat, ahová az Apache által kiszolgálandó fájlok kerültek – például a `DocumentRoot` könyvtárat.

```
<Directory "/srv/www/www.example.com/htdocs">
  Order allow,deny
  Allow from all
</Directory>
```

A teljes konfigurációs fájl így néz ki:

28.4 példa *Alapszintű VirtualHost beállítások*

```
<VirtualHost 192.168.3.100>
  ServerName www.example.com;
  DocumentRoot /srv/www/www.example.com/htdocs
  ServerAdmin webmaster@example.com
  ErrorLog /var/log/apache2/www.example.com_log
  CustomLog /var/log/apache2/www.example.com-access_log common
  <Directory "/srv/www/www.example.com/htdocs">
    Order allow,deny
    Allow from all
  </Directory>
</VirtualHost>
```

28.2.2 Az Apache beállítása a YaST segítségével

A webkiszolgáló a YaST-tal történő beállításához indítsa el a YaST-ot és válassza ki a *Hálózati szolgáltatások* > *HTTP-kiszolgáló* elemet. A modul első indításakor megjelenik a `HTTP-kiszolgáló varázsló`, és feltesz néhány alapkérdést a kiszolgáló felügyeletével kapcsolatban. A varázsló befejezése után a „HTTP-kiszolgáló beállítások” szakasz (466. oldal) párbeszédablak indul el minden egyes alkalommal, amikor meghívja a *HTTP-kiszolgáló* modult.

A HTTP-kiszolgáló varázsló

A HTTP-kiszolgáló varázsló öt lépésből áll. A párbeszédablak utolsó lépésében beléphet a szakértői beállítások közé, ha még speciálisabb beállításokra van szükség.

Hálózati eszköz kiválasztása

Itt kell megadni a hálózati csatolókat és portokat, amelyeken az Apache figyelni fogja a bejövő kéréseket. A meglévő hálózati csatolók és IP-címeik tetszés szerinti kombinációja használható. Mindhárom tartomány (jól ismert portok, bejegyzett portok és dinamikus/privát portok) egyéb szolgáltatások által nem foglalt portjai használhatók. Az alapértelmezett beállítás a minden hálózati csatolón (IP-címen), a 80-as porton történő figyelés.

Jelölje meg a *Tűzfal megnyitása a kijelölt portokon* beállítást a webkiszolgáló által figyelt portok megnyitásához a tűzfalon. Erre szükség van ahhoz, hogy a webkiszolgáló valóban elérhető legyen a hálózaton (legyen akár LAN, WAN, akár a nyilvános internet). A port zárva tartásának csak olyan teszthelyzetekben van értelme, ahol senkinek nem kell kívülről elérnie a webkiszolgálót. Ha egynél több hálózati csatoló van a gépben, akkor kattintson a *Tűzfalbeállítások* pontra és adja meg, mely csatoló(ko)n mely port(ok) legyen(ek) megnyitva.

Kattintson a *Tovább* gombra a beállítások folytatásához.

Modulok

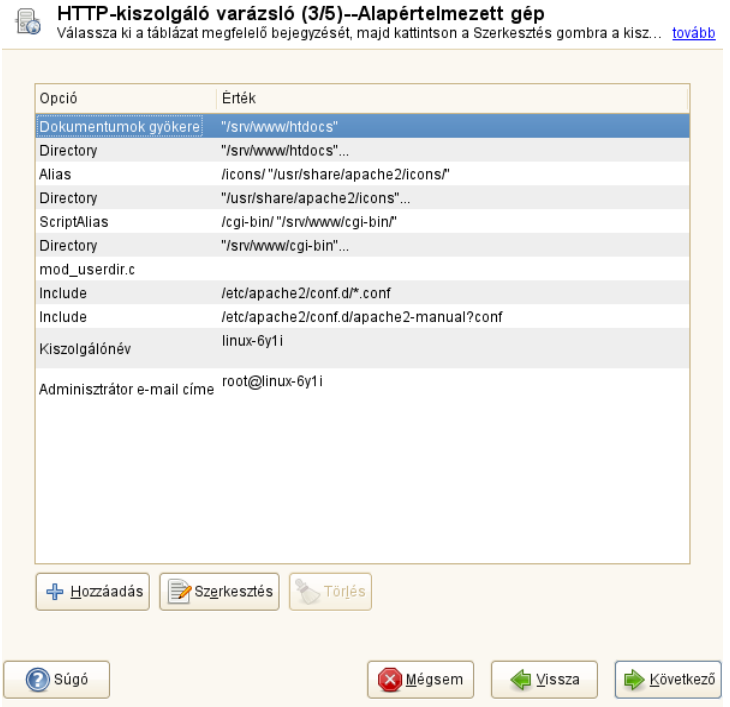
A *Modulok* részben lehet be- és kikapcsolni a webkiszolgáló által támogatandó parancsnyelveket. A többi modul be- és kikapcsolásának leírása: „Kiszolgálómodulok” szakasz (468. oldal). Kattintson a *Tovább* gombra a következő párbeszédablakra lépéshez.

Alapértelmezett gép

Ezek a beállítások az alapértelmezett webkiszolgálóra vonatkoznak. Amint az a „Virtuális gépek konfigurációja” szakasz (456. oldal) részben is olvasható, az Apache képes egyetlen fizikai gépről több virtuális gépet kiszolgálni. A konfigurációs fájlban elsőként megadott virtuális gépet szokás az *alapértelmezett gépnek* hívni. Minden egyes virtuális gép megörökli az alapértelmezett gép konfigurációját.

A gép beállításainak (más szavakkal, *direktíváinak*) módosításához válassza ki a táblázat megfelelő bejegyzését, majd kattintson a *Szerkesztés* gombra. Új direktívák felvételéhez kattintson a *Hozzáadás* gombra. Egy direktíva törléséhez válassza ki és kattintson a *Törlés* gombra.

28.1. ábra *HTTP kiszolgáló varázsló: Alapértelmezett gép*



Itt láthatók a kiszolgáló alapértelmezett beállításai.

`Document Root`
: Annak a könyvtárnak az elérési útja, ahonnan az Apache kiszolgálja az adott gép fájljait. Az alapértelmezett hely az `/srv/www/htdocs`.

`Alias`
: Az `Alias` direktívák használatával az URL-ek megfeleltethetők a fizikai fájlrendszer egyes helyeinek. Ez azt jelenti, hogy ha egy bizonyos útvonal kívül is esne a `Document Root`-ban megadott helyet, akkor is elérhető a fájlrendszer ezen része, az URL-t ennek megfeleltetve.

  Az openSUSE alapértelmezett `Alias /icons` beállítása az `/usr/share/apache2/icons` könyvtárra mutat, innen veszi az Apache ikonjait a könyvtárindex-nézet megjelenítéséhez.

`ScriptAlias`

Az `Alias` direktívához hasonlóan, a `ScriptAlias` direktíva is egy bizonyos URL-t a fájlrendszer egy adott részéhez rendel. A különbség az, hogy a `ScriptAlias` esetén a célkönyvtár CGI-parancsfájlokat tartalmaz, vagyis a CGI-parancsfájlokat erről a helyről szabad csak végrehajtani.

`Directory`

A `Directory` direktívával egy sor olyan beállítást lehet megadni, amelyek csak a megadott könyvtárra vonatkoznak.

Itt vannak beállítva az `/usr/share/apache2/icons` és az `/srv/www/cgi-bin` könyvtárak hozzáférési és megjelenítési jellemzői. Nincs szükség az alapértelmezett értékek megváltoztatására

`Include`

Az include utasítással további konfigurációs fájlok adhatók meg. Két `Include` direktíva már előre be van állítva: az `/etc/apache2/conf.d/` az a könyvtár, amely a külső modulok konfigurációs fájljait tartalmazza. Ezzel a beállítással a könyvtár minden `.conf` kiterjesztésű fájlja beágyazásra kerül. A második direktíva az jelenti, hogy az `/etc/apache2/conf.d/apache2-manual.conf` fájl, az `apache2-manual` konfigurációs fájl legyen beágyazva.

`Kiszolgáló neve`

Ez adja meg az alapértelmezett URL-t, amelyen a kliensek elérik a webkiszolgálót. Használja a webkiszolgáló elérésére szolgáló teljesen megadott tartománynevet (`http://`*`FQDN`*`/`), vagy az IP-címét. Itt nem választhat teljesen önkényesen nevet – a kiszolgálónak ezen a néven kell „ismertnek” lennie.

`Adminisztrátor e-mail címe`

A kiszolgáló rendszergazdájának e-mail címe. Ez a cím megjelenik például az Apache által előállított oldalakon.

Az *Alapértelmezett gép* lépés befejezése után kattintson a *Tovább* gombra a beállítás folytatásához.

Virtuális gépek

Ebben a lépésben a varázsló megjeleníti a már beállított virtuális gépek listáját (lásd: „Virtuális gépek konfigurációja” szakasz (456. oldal)). Ha nem végzett kézi módosításokat a YaST HTTP varázslójának elindítása előtt, akkor itt nem látható virtuális gép.

Egy gép hozzáadásához kattintson a *Hozzáadás* gombra. Megnyílik egy párbeszédablak, amelyben megadhatja a géppel kapcsolatos legfontosabb adatokat, mint például a *Kiszolgálónév*, a *Webes tartalom gyökere* (`DocumentRoot`) és az *Adminisztrátor e-mail címe*. A *Kiszolgáló névfeloldás* szolgál annak megadására, hogyan történjen a gép azonosítása (név vagy IP alapján). Adja meg a nevet vagy IP-címet a *Virtuális gép ID megváltoztatása* mezőben.

Kattintson a *Tovább* gombra a virtuálisgép-konfigurációs párbeszédablak második részére továbblépéshez.

A virtuálisgép-konfiguráció második részében adhatja meg, hogy kíván-e CGI-parancsfájlokat használni, és ha igen, ezek melyik könyvtárban találhatók. Szintén itt lehet bekapcsolni az SSL használatát. Ha így tesz, akkor meg kell adni a tanúsítvány elérési útját is. Az SSL-lel és a tanúsítványokkal kapcsolatos további részletek: 28.6.2. - Apache beállítása SSL-hez (488. oldal). A *Könyvtárindex* paraméterben adhatja meg, hogy mely fájlt jelenítse meg a kiszolgáló, ha a kliens csak egy könyvtárat adott meg (az alapértelmezett érték az index.html). Írja be a kívánt fájlneveket (szóközzel elválasztva), ha ezt módosítani kívánja. A *Nyilvános HTML engedélyezése* mezőben a felhasználók nyilvános könyvtárainak (`~felhasználó/public_html/`) tartalma tehető elérhetővé a kiszolgálón a `http://www.example.com/~felhasználó` címen.

FONTOS: Virtuális gépek létrehozása

Virtuális gépeket nem lehet összevissza felvenni. Név alapú virtuális gépek használata esetén minden egyes gépnévnek feloldhatónak kell lennie a hálózaton. IP alapú virtuális gépek használata esetén minden egyes IP-címhez csak egy gépnév rendelhető.

Összegzés

Ez a varázsló utolsó lépése. Itt adhatja meg, hogy hogyan és mikor induljon az Apache kiszolgáló: rendszerindításkor, vagy kézzel. Szintén itt jelenik meg az eddig elvégzett beállítások rövid összefoglalója. Ha meg van elégedve a beállításokkal, akkor kattintson

a *Befejezés* gombra a beállítások befejezéséhez. Ha módosítani kíván valamit, akkor kattintson a *Vissza* gombra egészen addig, amíg a kívánt párbeszédablakhoz nem ér. A *HTTP-kiszolgáló szakértői beállítások* gomb a „HTTP-kiszolgáló beállítások” szakasz (466. oldal) részben leírt párbeszédablakot nyitja meg.

28.2. ábra *HTTP-kiszolgáló varázsló: Összegzés*

HTTP-kiszolgáló beállítások

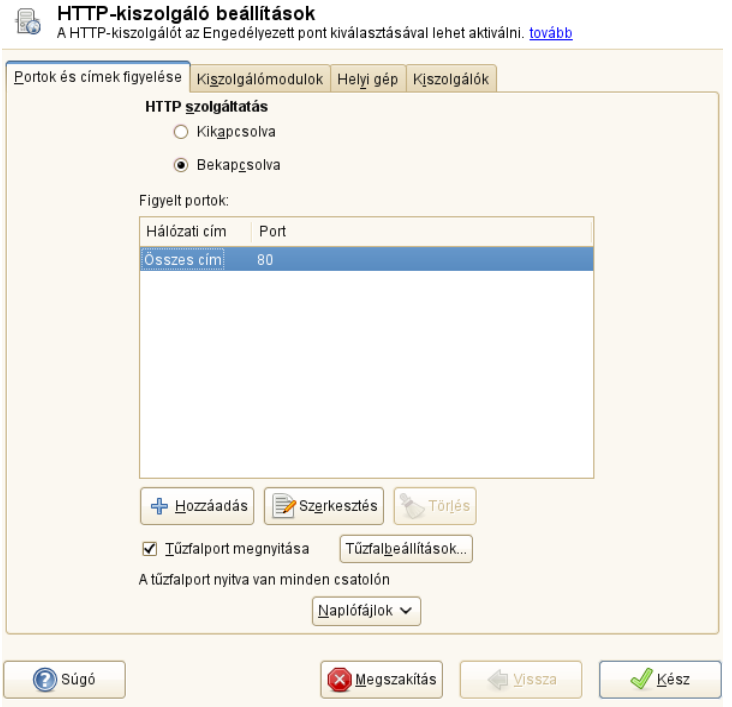
A *HTTP-kiszolgáló beállítások* párbeszédablakban a varázslónál még részletesebben adhatók meg a beállítások (a varázsló egyébként is csak akkor fut le, ha az első alkalommal állítja be a webkiszolgálót). Négy lapból áll, amelyeket az alábbiakban mutatunk be. Itt semmilyen beállítás nem lép azonnal érvényre – a módosításokat előbb meg kell erősíteni a *Befejezés* gombra kattintva. A *Megszakítás* gombra kattintás esetén kilép a konfigurációs modulból és elveti a változtatásokat.

Figyelt portok és címek

A *HTTP szolgáltatás* részben adja meg, hogy az Apache fusson-e (*Bekapcsolva*) vagy le legyen állítva (*Letiltva*). A *Figyelt portok* részben a *Hozzáadás*, *Szerkesztés*, és *Törlés* gombok használatával vegye fel a címeket és portokat, amelyeken a kiszolgálónak elérhetőnek kell lennie. Az alapértelmezés az összes csatolón a 80-as port figyelése. A *Tűzfal megnyitása a kiválasztott portokon* pontot mindig jelölje meg, különben a webkiszolgálót nem lehet majd elérni kívülről. A port zárva tartásának csak olyan teszthelyzetekben van értelme, ahol senkinek nem kell kívülről elérnie a webkiszolgálót. Ha egynél több hálózati csatoló van a gépben, akkor kattintson a *Tűzfalbeállítások* pontra és adja meg, mely csatoló(ko)n mely porto(k) legyen(ek) megnyitva.

A *Naplófájlok* részben tekintheti meg a hozzáférési naplót és a hibanaplót. Ez hasznos, ha tesztelni kívánja a beállításokat. A naplófájl egy külön ablakban nyílik meg, ahonnan újraindíthatja és újratöltheti a webkiszolgálót (ennek részletei: 28.3. - Az Apache elindítása és leállítása (469. oldal)). Ezek a parancsok azonnal életbe lépnek.

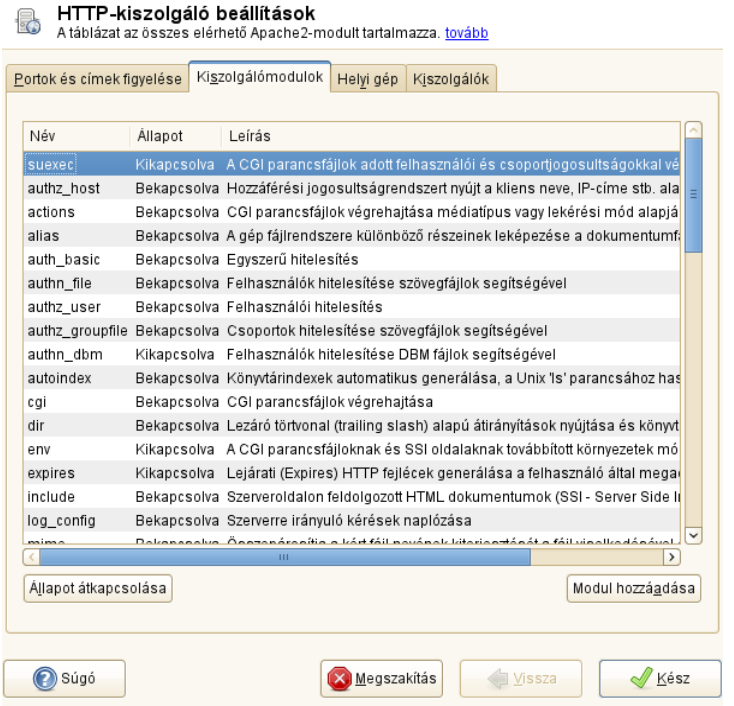
28.3. ábra *HTTP-kiszolgáló beállítások: Figyelt portok és címek*



Kiszolgálómodulok

Az Apache2-modulok (bekapcsolt vagy kikapcsolt) állapotának módosításához kattintson az *Állapot átkapcsolása* gombra. A *Modul hozzáadása* gombra kattintva vehet fel egy új, már telepített, de még fel nem sorolt modult. Tudjon meg többet a modulokról a 28.4. - Modulok telepítése, aktiválása és beállítása (471. oldal) című fejezetből.

28.4. ábra *HTTP-kiszolgáló beállítások: Kiszolgálómodulok*



Helyi gép vagy gépek

Ezek a párbeszédablakok megegyeznek a már leírtakkal. További információ: „Alapértelmezett gép” szakasz (462. oldal) és „Virtuális gépek” szakasz (465. oldal).

28.3 Az Apache elindítása és leállítása

Ha a YaST-tal állította be (lásd: 28.2.2. - Az Apache beállítása a YaST segítségével (461. oldal)), akkor az Apache a 3-as és 5-ös futási szinteken automatikusan elindul a rendszer indításakor, a 0, 1, 2. és 6. futási szinteken pedig le van állítva. Ez a viselkedés módosítható a YaST futásiszint-szerkesztőjével és a `chkconfig` parancssori eszközzel is.

Az Apache egy már futó rendszeren elindításához, leállításához vagy befolyásolásához használja az `/usr/sbin/rcapache2` init-parancsfájlt (az init parancsfájlok általános leírása a 14.2.2. - Init parancsfájlok (190. oldal) szakaszban olvasható). Az `rcapache2` parancsnak a következő paramétereket lehet megadni:

`status`
: Ellenőrzi, hogy az Apache el van-e indítva.

`start`
: Ha még nem lenne elindítva, akkor elindítja az Apache kiszolgálót.

`startssl`
: Ha még nem lenne elindítva, akkor elindítja az Apache kiszolgálót SSL-támogatással. További információ az SSL-támogatásról: 28.6. - Biztonságos webkiszolgáló beállítása SSL használatával (482. oldal).

`stop`
: Leállítja az Apache kiszolgálót (a szülőfolyamat leállításával).

`restart`
: Leállítja, majd újraindítja az Apache kiszolgálót. Ha még nem lett volna elindítva, akkor elindítja a webkiszolgálót.

`try-restart`
: Csak akkor állítja le és indítja újra az Apache kiszolgálót, ha az már el volt elindítva.

`reload` vagy `graceful`
: Leállítja a webkiszolgálót úgy, hogy az összes leágazott Apache-folyamatot értesíti, hogy leállás előtt még szolgálják ki a kéréseiket. Ahoz az egyes folyamatok elhalnak, újak indulnak helyettük, így végül az Apache teljesen „újraindul”.

TIPP

Éles környezetekben az `rcapache2 reload` az Apache újraindításának javasolt módja (például a konfiguráció módosítása után), mivel így az összes kliens ki lesz szolgálva és nem tapasztalják a kapcsolat megszakadását.

`restart-graceful`
: Elindít egy második webkiszolgálót, amely azonnal kiszolgálja az összes bejövő kérést. A webkiszolgáló előző példánya még a `GracefulShutdownTimeout` paraméternél megadott ideig kiszolgálja az összes meglévő kérést.

  Az `rcapache2 restart-graceful` hasznos lehet egy új verzióra frissítésnél, vagy ha olyan beállításokat módosított, amelyek mindenképpen teljes újraindítást igényelnek. E paraméter használatával minimálisra csökkenthető a kiszolgáló leállása.

  A `GracefulShutdownTimeout` paramétert be kell állítani, különben a `restart-graceful` egy szokásos újraindítást fog eredményezni. Nullára állítás esetén a kiszolgáló egészen addig vár, amíg az összes függőben lévő kérést ki nem szolgálja.

  Az ilyen "kellemes" (graceful) újraindítás azonban lehet, hogy nem sikerül, ha az eredeti Apache-példánynak nem sikerül felszabadítania az összes szükséges erőforrást. Ebben az esetben a parancs egy "kellemes" leállást fog eredményezni.

`stop-graceful`
: Leállítja a webkiszolgálót a `GracefulShutdownTimeout` paraméternél megadott idő után, annak érdekében, hogy a meglévő kéréseket még ki lehessen szolgálni.

  A `GracefulShutdownTimeout` paramétert be kell állítani, különben a `stop-graceful` egy szokásos újraindítást fog eredményezni. Nullára állítás esetén a kiszolgáló egészen addig vár, amíg az összes függőben lévő kérést ki nem szolgálja.

`configtest` vagy `extreme-configtest`
: A futó webkiszolgáló befolyásolása nélkül ellenőrzi a konfigurációs fájlok szintaxisának helyességét. Mivel ez az ellenőrzés megtörténik a kiszolgáló minden egyes indulásakor, újratöltésekor és újraindításakor, általában nincs szükség a teszt külön

futtatására (ha ugyanis konfigurációs hiba van, akkor a webkiszolgáló indítása, újratöltése vagy újraindítása nem fog sikerülni). Az `extreme-configtest` paraméter a webkiszolgálót a `nobody` felhasználó nevében elindítja és ténylegesen be is tölti, így több hiba észlelhető. Ügyeljen azonban arra, hogy bár a konfigurációt betölti a program, az SSL-beállításokat nem fogja tudni vizsgálni, mivel a `nobody` felhasználó nem jogosult elolvasni az SSL-tanúsítványokat.

`probe`
: Ellenőrzi, hogy van-e szükség újratöltésre (azt vizsgálja meg, hogy módosult-e a konfiguráció) és javaslatot tesz az `rcapache2` parancs után használandó paraméterre.

`server-status és full-server-status`
: Rövid ill. részletes állapotjelentést ír ki a kiszolgálóról. Használatához telepíteni kell a lynx vagy w3m csomagot, továbbá a mod_status modult is be kell kapcsolni. Ezenfelül az `/etc/sysconfig/apache2` fájlban az `APACHE_SERVER_FLAGS` sorban fel kell venni a `status` paramétert is.

TIPP: További jelzők

Ha további jelzőket ad meg az `rcapache2` parancsnak, akkor ezeket továbbítja a webkiszolgáló felé.

28.4 Modulok telepítése, aktiválása és beállítása

Az Apache szoftver modulárisan lett kialakítva: néhány alapfeladat kivételével mindent modulok végeznek. Ez egészen odáig megy, hogy még a HTTP-t is egy modul (http_core) dolgozza fel.

Az Apache-modulok befordíthatók a bináris Apache-fájlba összeszerkesztéskor, de betölthetők dinamikusan, futás közben is. A modulok dinamikus betöltéséről a 28.4.2. - Aktiválás és deaktiválás (472. oldal) rész szól.

Az Apache-modulok négyféle kategóriába tartozhatnak:

Alapmodulok
: Az alapmodulok alapértelmezés szerint be vannak fordítva az Apache-ba. A SUSE Linux Apache kiszolgálójába csak a (többi modul betöltéséhez szükséges) mod_so és a http_core van befordítva. Minden más megosztott objektumként érhető el: ahelyett, hogy a bináris kiszolgálófájlban lennének benne, futás közben tölthetők be.

Bővítőmodulok
: Általában a bővítésként megjelölt modulok benne találhatók az Apache-szoftvercsomagban, de nincsenek statikusan belefordítva a kiszolgálóba. openSUSE rendszereken ezek megosztott, az Apache-ba futás közben betölthető objektumokként érhetők el.

Külső modulok
: A külsőnek jelölt modulok nem részei a hivatalos Apache-disztribúciónak. A openSUSE számos ilyen modult tartalmaz, azonnal használható formában.

Többprocesszoros modulok (MPM)
: Az MPM-ek felelősek a webkiszolgálóhoz érkező kérések fogadásáért és kezeléséért, és ezek alkotják a webkiszolgáló szoftver magját.

28.4.1 Modulok telepítése

Ha az Apache telepítésének (a 28.1.2. - Telepítés (452. oldal) részben leírt) alapértelmezett módját követte, akkor telepítve lett az összes alap- és bővítőmodul, a Prefork többprocesszoros modul (MPM), valamint a mod_php5 és mod_python külső modulok.

További külső modulok telepítéséhez indítsa el a YaST-ot és válassza ki a *Szoftver* > *Szoftverkezelés* szakaszt. Válassza ki a *Szűrő* > *Keresés* menüpontot, és keresse ki az *apache*-t. Más egyéb csomagok mellett az eredménylistában megjelenik az összes rendelkezésre álló külső Apache-modul is.

28.4.2 Aktiválás és deaktiválás

A YaST segítségével kényelmesen aktiválhatja és deaktiválhatja a parancsnyelv-kezelő modulokat (PHP5, Perl, Python és Ruby) a „A HTTP-kiszolgáló varázsló” szakasz (461. oldal) részben leírt modulkonfiguráció lépéseit követve. Az összes többi modul be- és kikapcsolásának módját a „Kiszolgálómodulok” szakasz (468. oldal) rész írja le.

Ha inkább kézzel kívánja be- és kikapcsolni a modulokat, használja az `a2enmod` *`mod_foo`* vagy `a2dismod` *`mod_foo`*, parancsokat (ahol mod_foo a modul neve). Az `a2enmod -l` parancs kilistázza az összes éppen aktív modult.

FONTOS: Külső modulok konfigurációs fájlainak beágyazása

Ha kézzel aktivált külső modulokat, akkor ügyeljen rá, hogy a konfigurációs fájljaik be legyenek töltve az összes virtuálisgép-konfigurációba. A külső modulok konfigurációs fájljai az `/etc/apache2/conf.d/` könyvtárban találhatók, és alapértelmezés szerint nincsenek betöltve. Ha ugyanazokra a modulokra van szükség mindegyik virtuális gépben, akkor a beágyazásnál megadhatja a `*.conf` értéket erre a könyvtárra vonatkozóan. Ha nem, akkor ágyazza be az egyes fájlokat külön-külön. Példák az `/etc/apache2/vhost.d/vhost.template` sablonfájlban találhatók.

28.4.3 Alap- és bővítőmodulok

Az összes alap- és bővítőmodul részletesen le van írva az Apache dokumentációjában. Itt csak a legfontosabb modulok rövid leírását szerepeltetjük. Az egyes modulok részleteivel kapcsolatban tekintse meg a http://httpd.apache.org/docs/2.2/mod/ webhelyet.

mod_actions
: Módszereket kínál parancsfájlok végrehajtására, amikor egy meghatározott MIME-típusú (például `application/pdf`) vagy meghatározott kiterjesztésű (például `.rpm`) fájlt, vagy meghatározott kérési móddal (például `GET`) kérnek. Ez a modul alapértelmezés szerint be van kapcsolva.

mod_alias
: `Alias` (másodlagos név) és `Redirect` (átirányítás) direktívákat biztosít, amelyekkel egy adott URI egy adott könyvtárhoz rendelhető (`Alias`), vagy egy URL átirányítható egy másik helyre. Ez a modul alapértelmezés szerint be van kapcsolva.

mod_auth*
: A hitelesítési modulok különféle hitelesítési eljárásákat kínálnak: alapszintű hitelesítést a mod_auth_basic, vagy kivonat alapú hitelesítést a mod_auth_digest segítségével. Az Apache 2.2-ben a kivonat alapú hitelesítés egyelőre kísérletinek tekintendő.

A mod_auth_basic és mod_auth_digest kombinálható egy hitelesítésszolgáltató (mod_authn_*) modullal (például a mod_authn_file szövegfájl alapú hitelesítést biztosít) és egy engedélyezési (mod_authz_*) modullal (a mod_authz_user például a felhasználók engedélyeit szabályozza).

Ezzel kapcsolatban további információ a „Hitelesítési HOWTO”-ban olvasható (a `http://httpd.apache.org/docs/2.2/howto/auth.html` címen).

mod_autoindex
: Az autoindex könyvtárlistákat készít, ha nem található külön indexfájl (például `index.html`). Az indexek megjelenése állítható. Ez a modul alapértelmezés szerint be van kapcsolva. A könyvtárak tényleges kilistázása azonban le van tiltva az `Options` direktívával – írja felül ezt a beállítást a virtuálisgép-konfigurációban. A modul alapértelmezett konfigurációs fájlja az `/etc/apache2/mod_autoindex-defaults.conf`.

mod_cgi
: A mod_cgi szükséges CGI-parancsfájlok végrehajtásához. Ez a modul alapértelmezés szerint be van kapcsolva.

mod_deflate
: E modul használatával az Apache beállítható, hogy menet közben, még kiszolgálás előtt tömörítsen bizonyos fájltípusokat.

mod_dir
: A mod_dir biztosítja a `DirectoryIndex` direktívát, amellyel beállítható, hogy egy könyvtár lekérésekor mely fájlok kerüljenek automatikusan kiszolgálásra (az alapértelmezés az `index.html`). Szintén ez biztosít automatikus átirányítást a megfelelő URl-ra, ha a lekért könyvtár végén nem szerepel a lezáró törtvonal. Ez a modul alapértelmezés szerint be van kapcsolva.

mod_env
: A CGI-parancsfájloknak vagy SSI-oldalaknak átadott környezetet szabályozza. A httpd folyamatot meghívó parancsértelmezőben beállíthatók és kikapcsolhatók, illetve onnan átadhatók környezeti változók. Ez a modul alapértelmezés szerint be van kapcsolva.

mod_expires
: A mod_expires használatával szabályozható, hogy a proxy és böngésző gyorsítótárak milyen sűrűn frissítsék a dokumentumokat egy `Expires` fejléc küldésével. Ez a modul alapértelmezés szerint be van kapcsolva.

mod_include
: A mod_include lehetővé teszi kiszolgálóoldali beágyazások (Server Side Includes, SSI) használatát, amely egy alapszintű megoldás a HTML-oldalak dinamikus előállítására. Ez a modul alapértelmezés szerint be van kapcsolva.

mod_info
: Részletes áttekintést ír ki a kiszolgáló konfigurációjáról a http://localhost/server-info/ speciális címen. Biztonsági okokból ennek az URL-nek az elérését feltétlenül korlátozni kell. Alapértelmezés szerint egyedül a `localhost` jogosult elérni ezt az URL-t. A mod_info beállításai az `/etc/apache2/mod_info.conf` fájlban találhatók.

mod_log_config
: Ezzel a modullal lehet beállítani az Apache naplófájljainak a külalakját. Ez a modul alapértelmezés szerint be van kapcsolva.

mod_mime
: A fájlnevek kiterjesztése alapján a mime modul gondoskodik arról, hogy a fájlok a megfelelő (tehát például HTML dokumentumok esetében `text/html`) MIME-fejléccel legyenek elküldve . Ez a modul alapértelmezés szerint be van kapcsolva.

mod_negotiation
: A tartalom egyeztetéséhez szükséges. További információ a `http://httpd.apache.org/docs/2.2/content-negotiation.html` oldalon olvasható. Ez a modul alapértelmezés szerint be van kapcsolva.

mod_rewrite
: A mod_alias funkcióit biztosítja, de többféle lehetőséggel és nagyobb rugalmassággal. A mod_rewrite használatával többféle szabály, kérési fejlécek és még sokminden más alapján lehet átirányítani az URL-eket.

mod_setenvif
: A klienstől érkező kérés részletei, például a kliens által elküldött böngészőazonosító vagy a kliens IP-címe alapján állít be környezeti változókat. Ez a modul alapértelmezés szerint be van kapcsolva.

mod_speling
: A mod_speling megkísérli automatikusan korrigálni az URL-ek elgépeléseit, például a véletlen nagybetűket.

mod_ssl
: Titkosított kapcsolatot létesít a webkiszolgáló és a kliensek között. Részletek: 28.6. - Biztonságos webkiszolgáló beállítása SSL használatával (482. oldal). Ez a modul alapértelmezés szerint be van kapcsolva.

mod_status
: A kiszolgáló tevékenységével és teljesítményével kapcsolatos adatokat jelenít meg a http://localhost/server-status/ speciális címen. Biztonsági okokból ennek az URL-nek az elérését feltétlenül korlátozni kell. Alapértelmezés szerint egyedül a `localhost` jogosult elérni ezt az URL-t. A mod_status beállításai az `/etc/apache2/mod_status.conf` fájlban találhatók.

mod_suexec
: A mod_suexec lehetővé teszi a CGI-parancsfájlok egy másik felhasználó és csoport nevében történő futtatását. Ez a modul alapértelmezés szerint be van kapcsolva.

mod_userdir
: Lehetővé teszi a *~user/* alatti felhasználóspecifikus könyvtárak használatát. Az `UserDir` direktívát meg kell adni a konfigurációban. Ez a modul alapértelmezés szerint be van kapcsolva.

28.4.4 Többprocesszoros modulok (MPM)

A openSUSE kétféle többprocesszoros modul (MPM) használatát biztosítja az Apache-hoz.

Prefork MPM

A prefork MPM egy nem szálkezelő, előre elágaztatott .webkiszolgálót valósít meg. Ennek hatására a webkiszolgáló úgy viselkedik, mint az Apache 1.x verziója: elszigetel minden egyes kérést és úgy kezeli őket, hogy külön leszármazott folyamatot indít a kiszolgálásukra. Ily módon az esetleg problémát okozó kérések nincsenek hatással a többire és megakadályozzák a webkiszolgáló lefagyását.

Miközben azonban jobb stabilitást biztosít a folyamat alapú megközelítés révén, a prefork MPM jóval több rendszererőforrást használ el, mint párja, a worker MPM. UNIX alapú operációs rendszereken a prefork MPM számít az alapértelmezett MPM-nek.

FONTOS: A jelen dokumentumban tárgyalt MPM-ek

A jelen dokumentumban feltételezzük, hogy az Apache kiszolgálót a prefork MPM-mel használják.

Worker MPM

A worker MPM egy többszálú webkiszolgálót valósít meg. A szál a folyamatnak egy „egyszerűbb” fajtája. Ha szálakat használ folyamatok helyett, kevesebb erőforrást emészt fel a rendszer. Ahelyett, hogy leszármazott folyamatokat indítana, a worker MPM a kiszolgálófolyamatok szálait használva szolgálja ki a kéréseket. Az előre elágaztatott leszármazott folyamatok többszálúak. E megközelítés használatával az Apache jobb teljesítményt ér el, mivel kevesebb rendszer-erőforrást használ, mint a prefork MPM.

A legnagyobb hátrányok egyike azonban a worker MPM stabilitása: ha egy szállal baj történik, az a folyamat összes szálát befolyásolja. A legrosszabb esetben a teljes kiszolgáló összeomolhat. Különösen akkor, ha CGI-t használnak Apache alatt és nagy a terhelés, különféle belső kiszolgálóhibák jelentkezhetnek, mivel a szálak nem tudnak kommunikálni a rendszer erőforrásaival. Másik érv a worker MPM használata ellen, hogy nem minden Apache-modul képes szálkezelésre, és emiatt nem használható együtt a worker MPM-mel.

FIGYELEM: PHP-modulok használata az MPM-ekkel

Nem minden PHP-modul képes szálkezelésre. A worker MPM használata a mod_php modullal együtt határozottan ellenjavallt.

28.4.5 Külső modulok

Alább felsoroljuk a openSUSE összes külső modulját. A modul dokumentációja a jelzett könyvtárban található.

mod-apparmor
: Képessé teszi az Apache kiszolgálótt, hogy a mod_php5 és mod_perl modulok által kezelt CGI-parancsfájlokat a Novell AppArmor segítségével elszigetelje.

  Csomagnév: `apache2-mod_apparmor`
  További információ: *Novell AppArmor Administration Guide* (↑*Novell AppArmor Administration Guide*)

mod_mono
: A mod_mono használatával a kiszolgáló ASP.NET oldalak futtatására is képessé válik.

  Csomagnév: `apache2-mod_mono`
  Konfigurációs fájl: `/etc/apache2/conf.d/mod_mono.conf`

mod_perl
: A mod_perl használatával a Perl parancsfájlok egy beépített értelmezővel futtathatók. A kiszolgálóba épített állandó értelmező révén nincs szükség állandóan egy külső értelmező elindítására, és minden alkalommal a Perl indulásának kivárására.

  Csomagnév: `apache2-mod_perl`
  Konfigurációs fájl: `/etc/apache2/conf.d/mod_perl.conf`
  További információ: `/usr/share/doc/packages/apache2-mod_perl`

mod_php5
: A PHP egy kiszolgálóoldali, többplatformos, HTML-be ágyazott parancsnyelv.

  Csomagnév: `apache2-mod_php5`
  Konfigurációs fájl: `/etc/apache2/conf.d/php5.conf`
  További információ: `/usr/share/doc/packages/apache2-mod_php5`

mod_python
: A mod_python segítségével lényegesen jobb teljesítménnyel ágyazható be a Python az Apache HTTP kiszolgálóba, és rugalmasabban alakíthatók ki a webes alkalmazások.

  Csomagnév: `apache2-mod_python`
  További információ: `/usr/share/doc/packages/apache2-mod_python`

mod_tidy
: A mod_tidy minden egyes kimenő HTML-oldalt ellenőriz a TidyLib alapján. Ellenőrzési hiba esetén egy hibalistát tartalmazó oldal jelenik meg. Ellenkező esetben az eredeti HTML oldal kerül kiszolgálásra.

  Csomagnév: `apache2-mod_tidy`
  Konfigurációs fájl: `/etc/apache2/mod_tidy.conf`
  További információ: `/usr/share/doc/packages/apache2-mod_tidy`

28.4.6 Fordítás-összeszerkesztés

Képzett felhasználó ki is bővíthetik az Apache funkcionalitását egyedi modulok írásával. Apache-modulok fejlesztéséhez, illetve külső fejlesztésű modulok lefordításához szükség van az `apache2-devel` csomagra, valamint a megfelelő fejlesztőeszközökre. Az `apache2-devel` tartalmazza az `apxs2` eszközöket is, amelyekre szükség van,ha további modulokat akar készíteni az Apache-hoz.

Az `apxs2` teszi lehetővé a forráskódú modulok lefordítását és telepítését (beleértve a konfigurációs fájlok megfelelő módosításait is), az Apache-ba futási időben betölthető, ún. *dinamikus megosztott objektumok* (DSO-k) készítését.

Az `apxs2` bináris fájljai az `/usr/sbin` könyvtárban találhatók.

- Az `/usr/sbin/apxs2` segítségével bármely MPM alatt használható bővítőmodulok készíthetők. A telepítési helye az `/usr/lib/apache2`.
- Az `/usr/sbin/apxs2-prefork` segítségével a prefork MPM alatt használható bővítőmodulok készíthetők. A telepítési helye az `/usr/lib/apache2-prefork`.
- Az `/usr/sbin/apxs2-worker` segítségével a worker MPM alatt használható bővítőmodulok készíthetők. A telepítési helye az `/usr/lib/apache2-worker`.

A forráskódú modulok telepítéséhez és aktiválásához használja a következő parancsokat: `cd /modul/forrása; apxs2 -cia mod_foo.c` (A `-c` hatására lefordul a modul, az `-i` határása telepítésre kerül, az `-a` pedig aktiválja). Az `apxs2` egyéb paramétereit az `apxs2(1)` kézikönyvoldala írja le.

28.5 CGI-parancsfájlok használata

Az Apache Common Gateway Interface (CGI) csatolójával dinamikus tartalom is előállítható különféle programokkal vagy parancsfájlokkal, amelyeket általában CGI-parancsfájlok néven szokás emlegetni. CGI-parancsfájlok bármilyen programozási nyelven írhatók. Leggyakrabban a Perlhez és PHP-hoz hasonló parancsnyelveket használnak e célra.

Ahhoz, hogy az Apache kiszolgálja a CGI-parancsfájlok által előállított tartalmat, a mod_cgi modult aktiválni kell. Szükség van a mod_alias-ra is. Alapértelmezés szerint mindkét modul be van kapcsolva. A modulok aktiválásának részletei: 28.4.2. - Aktiválás és deaktiválás (472. oldal).

FIGYELEM: CGI-biztonság

A CGI-parancsfájlok végrehajtásának engedélyezése potenciális biztonsági rést jelent a kiszolgálón. További információ: 28.7. - Biztonsági problémák elkerülése (489. oldal).

28.5.1 Az Apache beállítása

openSUSE rendszereken a CGI-parancsfájlok végrehajtása kizárólag a `/srv/www/cgi-bin/` könyvtárból engedélyezett. Ez a hely viszont már be is van előre állítva a CGI-parancsfájlok futtatására. Ha virtuális gépeket használ (lásd „Virtuális gépek konfigurációja” szakasz (456. oldal)) és a parancsfájlokat a géphez tartozó könyvtárba kívánja helyezni, akkor ezt a könyvtárat előbb fel kell oldani és be kell állítani.

28.5 példa *Virtuális gépek beállítása CGI-hez*

```
ScriptAlias /cgi-bin/ "/srv/www/www.example.com/cgi-bin/"❶

<Directory "/srv/www/www.example.com/cgi-bin/">
 Options +ExecCGI❷
 AddHandler cgi-script .cgi .pl❸
 Order allow,deny❹
 Allow from all
</Directory>
```

❶ Azt jelzi az Apache számára, hogy a könyvtárban található minden fájlt tekintsen CGI-parancsfájlnak.

❷ Engedélyezi a CGI-parancsfájlok végrehajtását

❸ Azt jelzi a kiszolgáló számára, hogy a .pl és .cgi kiterjesztésű fájlokat tekintse CGI-parancsfájloknak. Módosítsa igényei szerint.

❹ Az `Order` és `Allow` direktívák szabályozzák az alapértelmezett hozzáférés állapotát, illetve az Allow és Deny direktívák kiértékelésének a sorrendjét. A jelen esetben a „deny” utasítások az „allow” utasítások előtt értékelődnek ki, és a hozzáférés mindenhonnan engedélyezett.

28.5.2 Egy példaparancsfájl futtatása

A CGI-programozás eltér annyiban a "szokásos" programozástól, hogy a CGI-programokat és -parancsfájlokat egy MIME-Type fejlécnek kell megelőznie, például egy ilyennek: `Content-type: text/html`. A kliens megkapja ezt a fejlécet, hogy tisztában legyen vele, milyen típusú tartalom is érkezik ezután. Másodszor, a parancsfájl kimenete valami olyan kell, hogy legyen, amit a kliens (jellemzően egy webböngésző) megért – vagyis elsősorban HTML, esetleg sima szöveg vagy például egy kép.

Az Apache csomag része egy egyszerű példaparancsfájl, az `/usr/share/doc/packages/apache2/test-cgi`. Ez néhány környezeti változó tartalmát írja ki egyszerű szövegként. Másolja át ezt a parancsfájlt akár az `/srv/www/cgi-bin/` könyvtárba, akár a virtuális gép parancsfájl-könyvtárába (`/srv/www/www.example.com/cgi-bin/`) és nevezze át `test.cgi` névre.

A webkiszolgáló által elérhető fájloknak a `root` felhasználó tulajdonában kell lenniük (további információ: 28.7. - Biztonsági problémák elkerülése (489. oldal)). Mivel a webkiszolgáló más felhasználó nevében fut, a CGI-parancsfájloknak mindenki által

olvashatónak és végrehajthatónak kell lenniük. Váltson át a CGI-könyvtárba, és adja ki a `chmod 755 test.cgi` parancsot a megfelelő jogosultságok biztosításához.

Most már beírhatja a böngészőbe a `http://localhost/cgi-bin/test.cgi` vagy a `http://www.example.com/cgi-bin/test.cgi` címet. Meg kell, hogy jelenjen a „CGI/1.0 test script report” oldal.

28.5.3 Hibaelhárítás

Ha nem jelenik meg a tesztprogram kimenete, csak egy hibaüzenet látszik, akkor ellenőrizze az alábbiakat:

CGI-hibaelhárítás

- Újratöltötte-e a kiszolgálót a konfiguráció módosítása után? Ellenőrizze ezt az `rcapache2 probe` paranccsal.
- Ha egyéni CGI-könyvtárat állított be, helyesek-e a beállítások? Ha nem biztos benne, próbálja ki a parancsfájlt az alapértelmezett CGI-könyvtárral (`/srv/www/cgi-bin/`) és érje el a `http://localhost/cgi-bin/test.cgi` címen.
- Rendben vannak-e a fájljogosultságok? Váltson át a CGI-könyvtárba, és adja ki az `ls -l test.cgi` parancsot. A kimenetnek így kell kezdődnie:

  ```
  -rwxr-xr-x  1 root root
  ```

- Győződjön meg róla, hogy a parancsfájl nem tartalmaz programozási hibákat. Ha a test.cgi-t használja, ez nem fordulhat elő, de ha saját programokat ír, mindig győződjön meg róla, hogy azok hibátlanul működnek.

28.6 Biztonságos webkiszolgáló beállítása SSL használatával

Amikor bizalmas adatok, például hitelkártyaszámok kerülnek továbbításra a webkiszolgáló és a kliens között, akkor felettébb kívánatos egy biztonságos, titkosított, hitelesített kapcsolat használata. A mod_ssl erős titkosítást biztosít és az SSL (Secure Sockets Layer), illetve TLS (Transport Layer Security) protokollok használatával védi a webki-

szolgáló és a kliens közötti HTTP-kommunikációt. Az SSL/TSL használata esetén a webkiszolgáló és a kliens között privát kapcsolat jön létre. Garantált az adatok integritása, és mind a kliens, mind a kiszolgáló képes ellenőrizni a másik hitelességét.

Ehhez a kiszolgáló, még mielőtt bármilyen URL-re válaszolna, egy SSL-tanúsítványt küld, benne a kiszolgáló érvényes azonosságával. Ezzel igazolja, hogy a kiszolgáló valóban a helyes végpontja a kommunikációnak. Ezenfelül a tanúsítvány használatával titkosított kapcsolat jön létre a kliens és a kiszolgáló között, így a nyílt szövegű adatok szabadon továbbíthatók a felfedés kockázata nélkül.

A mod_ssl does nem maga valósítja meg az SSL/TSL protokollokat, csupán közvetítőként működik közre az Apache és egy SSL-függvénytár között. A openSUSE rendszerben ez utóbbi az OpenSSL függvénytár. Az OpenSSL az Apache mellett automatikusan telepítésre kerül.

A mod_ssl használatának legészrevehetőbb jellemzője, hogy az URL-ek `https://`-sel kezdődnek, nem `http://`-vel.

28.6.1 SSL-tanúsítvány előállítása

Az SSL/TSL használatához a webkiszolgálón szükség van egy SSL-tanúsítványra. A tanúsítvány a webkiszolgáló és a kliens közötti hitelesítés során játszik szerepet, ennek alapján azonosíthatók az egyes felek egyértelműen. A tanúsítvány integritásának biztosítása érdekében azt egy olyan félnek kell aláírnia, amelyben minden felhasználó megbízik.

A létrehozható tanúsítványoknak három fajtája van: „üres” (dummy) tanúsítványok kizárólag teszteléshez, önállóan aláírt tanúsítványok azon felhasználók számára, akik megbíznak Önben, illetve az egy független, széles körben ismert és elfogadott tanúsítványhatóság (CA) által aláírt tanúsítványok.

A tanúsítványok előállítása két lépésből álló folyamat. Először egy saját kulcs készül a tanúsítványhatóság számára; utána a kiszolgálótanúsítvány ezzel a kulccsal lesz aláírva.

TIPP: További információk

Az SSL/TSL fogalmaival és meghatározásaival kapcsolatos további részletek a `http://httpd.apache.org/docs/2.2/ssl/ssl_intro.html` címen olvashatók.

„Üres” tanúsítvány előállítása

Az üres tanúsítványok előállítása igen egyszerű. Mindössze meg kell hívni az `/usr/bin/gensslcert` parancsfájlt. Ez létrehozza vagy felülírja az alábbi fájlokat:

- `/etc/apache2/ssl.crt/ca.crt`
- `/etc/apache2/ssl.crt/server.crt`
- `/etc/apache2/ssl.key/server.key`
- `/etc/apache2/ssl.csr/server.csr`

A `ca.crt` egy másolata bekerül az `/srv/www/htdocs/CA.crt` helyre is, letöltéshez.

FONTOS

Éles rendszeren nem szabad üres tanúsítványt használni. Kizárólag tesztelési célokat szolgál.

Önállóan aláírt tanúsítvány létrehozása

Ha egy intraneten vagy felhasználók meghatározott köre számára hoz létre biztonságos webkiszolgálót, akkor elegendő lehet, ha csak a saját tanúsítványhatóság (CA) által aláírt tanúsítványt használ.

Az önállóan aláírt tanúsítványok létrehozása egy interaktív, kilenclépéses folyamat. Váltson át az `/usr/share/doc/packages/apache2` könyvtárba, és futtassa le az alábbi parancsot: `./mkcert.sh make --no-print-directory /usr/bin/openssl /usr/sbin/ custom`. Ne próbálja meg ezt a parancsot más helyről futtatni. A program egy sor kérdést jelenít meg, amelyekre válaszolni kell.

28.1. eljárás *Önállóan aláírt tanúsítvány előállítása az mkcert.sh használatával*

1 Válassza ki a tanúsítványokhoz használt aláírási algoritmust

Érdemes az RSA-t (R, ez az alapértelmezés) választani, mert néhány régebbi böngészőnek gondjai vannak a DSA-val.

2 `RSA saját kulcs előállítása a CA számára (1024 bit)`

Nincs szükség egyéb beavatkozásra.

3 `X.509 tanúsítvány aláírási kérés előállítása a CA számára`

Itt kell létrehozni a CA megkülönböztetett nevét. Ehhez meg kell válaszolni néhány kérdést, például meg kell adni az ország és a szervezet nevét. Érvényes adatokat adjon meg, mert mindez később látszani fog a tanúsítványban. Nem muszáj minden kérdésre válaszolni. Ha valamelyik nem alkalmazható, vagy üresen kívánja hagyni, akkor adjon meg egy „.” karaktert válaszul. Az általános név (common name) a CA-nak magának a neve – célszerűen valami értelmes nevet adjon meg, például azt, hogy *`Futrimpex Kft.`* CA (ha például így hívják a céget).

4 `X.509 tanúsítvány előállítása a CA számára, saját maga által aláírva`

Válassza a 3-as (az alapértelmezett) tanúsítványverziót.

5 `RSA saját kulcs előállítása a kiszolgáló számára (1024 bit)`

Nincs szükség egyéb beavatkozásra.

6 `X.509 tanúsítvány aláírási kérés előállítása a kiszolgáló számára`

Itt hozza létre a kiszolgáló megkülönböztetett nevét. A kérdések szinte tökéletesen megegyeznek azokkal, amelyeket a CA megkülönböztetett nevénél megválaszolt. Az itt beírt adatok a webkiszolgálóra vonatkoznak, és nem kell feltétlenül megegyezniük a CA adataival (lehet például, hogy a kiszolgáló valahol másutt van fizikailag).

FONTOS: Általános név választása

Az itt megadott általános név a biztonságos kiszolgáló teljesen megadott állomásneve kell, hogy legyen (tehát például www.example.com). Ha nem ezt adja meg, akkor a böngésző a kiszolgáló elérésekor figyelmeztetést fog kiírni, hogy a tanúsítvány nem felel meg a kiszolgálónak.

7 `A saját CA által aláírt X.509 tanúsítvány előállítása`

Válassza a 3-as (az alapértelmezett) tanúsítványverziót.

8 `A CA saját RSA-kulcsának titkosítása egy jelszóval a biztonság érdekében`

Határozottan javasolt a CA saját kulcsát titkosítani egy jelszóval, ezért ebben a lépésben Y-nal válaszoljon és adjon meg egy jelszót.

9 `A kiszolgáló saját saját RSA-kulcsának titkosítása egy jelszóval a biztonság érdekében`

Ha a kiszolgáló kulcsát is titkosítja egy jelszóval, akkor ezt a jelszót minden egyes alkalommal meg kell majd adnia, amikor elindítja a webkiszolgálót. Ez megnehezíti a webkiszolgáló automatikus indítását a rendszer indításakor vagy a webkiszolgáló újraindításakor. Éppen ezért a szokásos válasz erre a kérdésre az N. Ne feledje ugyanakkor, hogy ha nincs jelszóval titkosíta, akkor ez a kulcs védtelen, ezért győződjön meg róla, hogy csak az arra jogosult személyek férhetnek hozzá a kulcshoz.

FONTOS: A kiszolgáló kulcsának titkosítása

Ha úgy döntött, hogy titkosítja jelszóval a kiszolgáló kulcsát, akkor növelje meg az `APACHE_TIMEOUT` értékét az `/etc/sysconfig/apache2` fájlban. Ellenkező esetben nem lesz elegendő ideje beírni a jelszót, mielőtt a kiszolgáló leállnasikertelen indításra hivatkozva.

A parancsfájl eredményoldalán megjelenik az előállított kulcsok és tanúsítványok listája. Szemben azzal, amit a parancsfájl állít, a fájlok nem a helyi `conf` könyvtárban jöttek létre, hanem a megfelelő helyen, az `/etc/apache2/` könyvtárban.

Az utolsó lépés a CA-tanúsítványfájl átmásolása az `/etc/apache2/ssl.crt/ca.crt` helyről egy olyan helyre, ahol a felhasználók elérhetik és felvehetik az ismert és megbízható CA-k közé webböngészőikben. Ellenkező esetben a böngésző panaszkodni fog, hogy a tanúsítványt egy ismeretlen hatóság állította ki. A tanúsítvány egy évig érvényes.

FONTOS: Önállóan aláírt tanúsítványok

Csak olyan webkiszolgálón használjon önállóan aláírt tanúsítványt, amelyet olyan emberek érnek el, akik megbíznak Önben és elfogadják tanúsítványhatóságnak. Egy nyilvános webáruházban például nem javasolt ilyen tanúsítványt használni.

Hivatalosan aláírt tanúsítvány beszerzése

Számos hivatalos tanúsítványhatóság létezik, amely vállalja a tanúsítványok aláírását. A tanúsítványt egy megbízható harmadik fél írja alá, ettől megbízható. A nyilvánosan működő webkiszolgálók általában ilyen, hivatalos tanúsítványt használnak.

A legismertett hivatalos CA-k a Thawte (`http://www.thawte.com/`) és a Verisign (`http://www.verisign.com`). Ezek és más CA-k be is vannak építve az összes böngészőbe, úgyhogy az általuk aláírt tanúsítványokat a böngészők automatikusan elfogadják.

Egy hivatalosan aláírt tanúsítvány kérésekor az ember nem a tanúsítványt küldi el a CA-nak. Helyette tanúsítvány-aláírási kérést (Certificate Signing Request, CSR) kell küldeni. Egy CSR létrehozásához az `/usr/share/ssl/misc/CA.sh –newreq` parancsfájlt kell meghívni.

A parancsfájl először bekér egy jelszót, amellyel titkosítani fogja a CSR-t. Ezután bekéri a megkülönböztetett nevet. Ehhez meg kell válaszolni néhány kérdést, például meg kell adni az ország és a szervezet nevét. Érvényes adatokat adjon meg, mert mindez később látszani fog a tanúsítványban és le is ellenőrzik. Nem muszáj minden kérdésre válaszolni. Ha valamelyik nem alkalmazható, vagy üresen kívánja hagyni, akkor adjon meg egy „.” karaktert válaszul. Az általános név (common name) a CA-nak magának a neve – célszerűen valami értelmes nevet adjon meg, például azt, hogy *`Futrimpex Kft.`* CA (ha például így hívják a céget). Utoljára egy ellenőrző jelszót és egy alternatív cégnevet kell megadni.

A CSR ugyanabba a könyvtárba kerül, mint amelyikből a parancsfájlt meghívta. A fájl neve `newreq.pem` lesz.

28.6.2 Apache beállítása SSL-hez

Az SSL- és TLS-kérések alapértelmezett portszáma a webkiszolgáló oldalán a 443-as. Egy „normál”, a 80-as porton figyelő Apache és egy, a 443-as porton figyelő SSL/TLS-es Apache között nincs ütközés. Valójában a HTTP és a HTTPS akár ugyanazon az Apache-példányon is futtatható. Általában különböző virtuális gépeket állítanak be a 80-as és a 443-as portokhoz a virtuális kiszolgálók elkülönítéséhez.

FONTOS: Tűzfal beállítása

Ne felejtse el kinyitni a 443-as portot a tűzfalon az SSL-es Apache számára. Ez elvégezhető a YaST-tal is, a 33.4.1. – Tűzfal beállítása a YaST segítségével (537. oldal) részben leírt módon.

Az SSL használatához azt be kell kapcsolni a globális kiszolgálókonfigurációban. Nyissa meg az `/etc/sysconfig/apache2` fájlt egy szövegszerkesztőben és keresse ki az `APACHE_MODULES` részt. Ha még nem szerepelne, vegye fel az „ssl”-t a modulok listájába (a mod_ssl is alapértelmezés szerint be van kapcsolva). Ezután keresse ki az `APACHE_SERVER_FLAGS` részt és ott is írja be, hogy „SSL”. Ha úgy döntött, hogy jelszóval védi a kiszolgálótanúsítványt, akkor növelje meg az `APACHE_TIMEOUT` kellő mértékben ahhoz, hogy legyen ideje beírni a jelszót az Apache indulásakor. Indítsa újra a kiszolgálót a módosítások érvényre juttatásához. Most nem elegendő az újratöltés.

A virtuálisgép-konfigurációs könyvtárban van egy sablonfájl (`/etc/apache2/vhosts.d/vhost-ssl.template`) SSL-specifikus direktívákkal, megjegyzésekkel bőségesen ellátva. A virtuális gépek általános beállításaival kapcsolatban forduljon a „Virtuális gépek konfigurációja” szakasz (456. oldal) részhez.

Első lépésként másolja át a sablontfájlt az `/etc/apache2/vhosts.d/`*`sajatSSL-host`*`.conf` fájlba és módosítsa igény szerint. Általában elegendő az alábbi értékeket módosítani:

- `DocumentRoot`
- `ServerName`

- `ServerAdmin`
- `ErrorLog`
- `TransferLog`

FONTOS: Név alapú virtuális gépek és SSL

Csupán egyetlen IP-címmel rendelkező kiszolgálón nem lehet több SSL-es virtuális gépet futtatni. Beállítani ugyan be lehet egy ilyen rendszert, de az ezt meglátogató felhasználók minden egyes alkalommal figyelmeztető üzenetet fognak kapni, hogy a tanúsítvány nem egyezik a kiszolgáló nevével. Minden egyes SSL-re felkészített tartománynak saját IP-címmel kell rendelkeznie ahhoz, hogy érvényes SSL-tanúsítvánnyal tudjon kommunikálni.

28.7 Biztonsági problémák elkerülése

A nyilvános interneten működő webkiszolgálók folyamatos felügyeletet igényelnek. Elkerülhetetlenül fellépnek biztonsági problémát, akár a szoftverből, akár a véletlen félrekonfigurálásból adódóan. Az alábbiakban néhány ötletet szeretnénk adni az elkerülésükhöz.

28.7.1 Naprakész szoftver

Amikor sérülékenységeket találnak az Apache szoftverben, a SUSE biztonsági tanácsot ad ki. Ebben leírja a sérülékenységek kijavításának módját, amelyet a lehető leghamarabb el kell végezni. A SUSE biztonsági bejelentések az alábbi címeken érhetők el:

- **Weblap:** `http://www.novell.com/linux/security/securitysupport.html`
- **Levelezőlista** `http://en.opensuse.org/Communicate#Mailinglists`
- **RSS-folyam** `http://www.novell.com/linux/security/suse_security.xml`

28.7.2 DocumentRoot-jogosultságok

Alapértelmezés szerint a openSUSE rendszerben a `DocumentRoot` könyvtár (`/srv/www/htdocs`) és a CGI-könyvtár (`/srv/www/cgi-bin`) a `root` felhasználóhoz és csoporthoz tartoznak. Ezeket a jogosultságokat nem célszerű megváltoztatni. Ha a könyvtárak bárki által írhatók lennének, akkor akármelyik felhasználó rakhatna beléjük fájlokat. Utána pedig előfordulhat, hogy az Apache végrehajtaná ezeket a fájlokat a `wwwrun` felhasználó jogosultságával, és így a felhasználónak a más szándék ellenére hozzáférést engedne a fájlrendszer erőforrásaihoz. Éppen ezért az `/srv/www` alkönyvtáraiba helyezze el a virtuális gépek `DocumentRoot` és CGI-könyvtárait, és gondoskodjon róla, hogy ezek a könyvtárak és fájlok a `root` felhasználóhoz és csoporthoz tartozzanak.

28.7.3 Fájlrendszer elérése

Alapértelmezés szerint a teljes fájlrendszer elérése le van tiltva az `/etc/apache2/httpd.conf` fájlban. Ezeket a direktívákat ne írja felül; engedélyezze külön-külön az Apache által elérni szükséges könyvtárakat (ennek részletei: „Virtuális gépek alapszintű beállításai” szakasz (460. oldal)). Ily módon garantálható, hogy semmilyen kritikus fájl (például jelszavakat tároló, vagy rendszerkonfigurációs fájl) nem érhető el kívülről.

28.7.4 CGI-parancsfájlok

A Perl, PHP, SSI és más programozási nyelveken írott interaktív parancsfájlok lényegében tetszés szerinti parancsokat végrehajthatnak, ezért általánosságban biztonsági kockázatot jelentenek. A kiszolgálón végrehajtott parancsfájlokat csak a kiszolgáló rendszergazdája által megbízhatónak tartott forrásokból szabad telepíteni – általában nem túl jó ötlet engedni a felhasználóknak, hogy mindenféle parancsfájlt végrehajthassanak. Szintén célszerű biztonsági szempontból megvizsgálni a parancsfájlokat.

A parancsfájlok felügyeletének megkönnyítése érdekében bevált gyakorlat korlátozni a CGI-parancsfájlok végrehajtását néhány könyvtárra és nem engedélyezni őket globálisan. Ennek beállítására a `ScriptAlias` és `Option ExecCGI` direktívák használhatók. A openSUSE alapértelmezett konfigurációja nem engedi a CGI-parancsfájlok végrehajtását tetszés szerinti helyről.

Minden CGI-parancsfájl ugyanazon felhasználó nevében fut, ezért a különböző parancsfájlok lehetséges, hogy megzavarják egymást. A mod_suEXEC modul lehetővé teszi a CGI-parancsfájlok egy másik felhasználó és csoport nevében történő futtatását.

28.7.5 Felhasználói könyvtárak

A felhasználói könyvtárak (a mod_userdir vagy a mod_rewrite segítségével történő) engedélyezésekor igen komolyan érdemes megfontolni, hogy ne használhassák a `.htaccess` fájlokat, amelyekkel felülírhatók a biztonsági beállítások. Legalábbis korlátozni kell azt, hogy a felhasználó milyen mértékben befolyásolhatja a beállításokat (az `AllowOverRide` direktívával). openSUSE rendszereken a `.htaccess` fájlok alapértelmezés szerint engedélyezve vannak ugyan, de a felhasználók nem jogosultak felülírni semmilyen `Option` direktívát a mod_userdir használatakor (lásd az `/etc/apache2/mod_userdir.conf` konfigurációs fájlt).

28.8 Hibaelhárítás

Ha az Apache nem indul el, a weboldalak nem érhetők el, vagy a felhasználók nem tudnak csatlakozni a webkiszolgálóhoz, akkor fontos a probléma okának mihamarabbi azonosítása. Alább bemutatunk néhány szokásos helyet, ahol érdemes kutatni hibák után, és néhány fontos ellenőrzendő dolgot.

Először is, az (28.3. - Az Apache elindítása és leállítása (469. oldal) részben leírt) `rcapache2` igen részletesen kiírja a hibákat (amennyiben ezt használják az Apache üzemeltetéséhez). Néha jó ötletnek tűnhet az `/usr/sbin/httpd2` bináris fájl használata a webkiszolgáló elindításához és leállításához. Ez mindenképpen kerülendő, használja helyette az `rcapache2` parancsfájlt. Az `rcapache2` még ötleteket is ad a konfigurációs hibák elkerüléséhez.

Másodszor, nem lehet eleget hangsúlyozni a naplófájlok fontosságát. Az Apache-naplófájlokat végzetes és nem végzetes hibák esetén egyaránt hasznos megvizsgálni az okok után kutatva. Amennyiben részletesebb adatokra van szükség a naplófájlokban, ez a `LogLevel` direktívával szabályozható. Alapértelmezés szerint a hibanaplófájl a `/var/log/apache2/error_log`.

TIPP: Egy egyszerű vizsgálat

Írassa ki az Apache naplóüzeneteit a `tail -F /var/log/apache2/my_error_log` paranccsal. Ezután adja ki az `rcapache2 restart` parancsot. Most próbáljon meg csatlakozni egy böngészővel és nézze meg a kimenetet.

Szokásos hiba nem kinyitni az Apache portjait a kiszolgáló tűzfalán. Ha az Apache beállítását a YaST-tal végezte, akkor egy külön opció szolgál pontosan ennek a végrehajtására (lásd: 28.2.2. - Az Apache beállítása a YaST segítségével (461. oldal)). Ha kézzel állította be az Apache webkiszolgálót, használja a YaST tűzfal modulját a HTTP és a HTTPS portok megnyitásához.

Ha a hiba okát a fentiek egyikével sem sikerült megtalálni, nézzen körül az Apache online hibaadatbázisában, a `http://httpd.apache.org/bug_report.html` címen. Végül az Apache felhasználói közösség elérhető egy levelezőlistán is (`http://httpd.apache.org/userslist.html`). A javasolt hírcsoport az `comp.infosystems.www.servers.unix`.

28.9 További információk

Az `apache2-doc` csomag tartalmazza az Apache teljes kézikönyvét különféle nyelveken, a helyi telepítéshez és referenciának. Alapértelmezés szerint nincs telepítve – a leggyorsabb módja a telepítésének a `zypper in apache2-doc` parancs kiadása. Telepítés után az Apache kézikönyv a `http://localhost/manual/` címen érhető el. Elérhető a weben is, a `http://httpd.apache.org/docs-2.2/` címen. A SUSE-val kapcsolatos beállítási javaslatok az `/usr/share/doc/packages/apache2/README.*` könyvtárban olvashatók.

28.9.1 Apache 2.2

Az Apache 2.2 új funkcióinak a listája: `http://httpd.apache.org/docs/2.2/new_features_2_2.html`. A 2.0-ról 2.2-es verzióra frissítéssel kapcsolatos információ: `http://httpd.apache.org/docs-2.2/upgrading.html`.

28.9.2 Apache-modulok

További információ a külső Apache-modulokkal (28.4.5. - Külső modulok (477. oldal)) kapcsolatban az alábbi helyeken található:

mod-apparmor
http://en.opensuse.org/AppArmor

mod_mono
http://www.mono-project.com/Mod_mono

mod_perl
http://perl.apache.org/

mod_php5
http://www.php.net/manual/en/install.unix.apache2.php

mod_python
http://www.modpython.org/

mod_tidy
http://mod-tidy.sourceforge.net/

28.9.3 Fejlesztés

További információ az Apache-modulok fejlesztésével, illetve az Apache webkiszolgáló projektben részvétellel kapcsolatban az alábbi helyeken található:

Apache fejlesztői információk
http://httpd.apache.org/dev/

Apache fejlesztői dokumentáció
http://httpd.apache.org/docs/2.2/developer/

Apache-modulok írása Perl és C nyelveken
http://www.modperl.com/

28.9.4 Egyéb források

Ha nehézségekbe ütközne a openSUSE rendszeren az Apache használatával, nézzen körül az openSUSE wiki-n a http://http://en.opensuse.org/Apache címen. Az Apache történetének leírása a http://httpd.apache.org/ABOUT_APACHE.html címen olvasható Itt azt is megismerheti, miért Apache névre hallgat a .kiszolgáló.

FTP-kiszolgáló beállítása a YaST segítségével

29

A YaST *FTP-kiszolgáló* moduljában beállítható, hogy a gépe FTP-kiszolgálóként működjön. A név nélküli (anonymous) és/vagy hiteleített felhasználók hozzákapcsolódhatnak a géphez, és letölthetnek -- illetve konfigurációtól függően fel is tölthetnek fájlokat az FTP-protokoll használatával. A YaST egyesített konfigurációs felületet nyújt a rendszeren telepített különféle FTP-kiszolgálódémonokhoz.

A YaST *FTP-kiszolgáló* konfigurációs modulja két különböző FTP-kiszolgálódémon beállítására használható: ezek a vsftpd ("Very Secure FTP Daemon") és a pure-ftpd. Csak telepített kiszolgálók állíthatók be. Az alap openSUSE adathordozó nem tartalmazza a pure-ftpd csomagot. Ha azonban ezt egy másik forrásból telepíti, akkor beállítható a YaST modul használatával.

A vsftpd és a pure-ftpd kiszolgálók egy kicsit másképp konfigurálhatók, különösen a *Szakértői beállítások* párbeszédablak különbözik. Ebben a fejezetben elmondjuk, hogyan kell beállítani a vsftpd-t, hogy az openSUSE alapértelmezett kiszolgálója legyen.

Ha a YaST FTP-kiszolgáló modulja nem áll rendelkezésre a rendszerben, akkor telepítse a `yast2-ftp-server` csomagot.

Az FTP-kiszolgáló beállításához YaST segítségével tegye a következőket:

1. Nyissa meg a YaST vezérlőközpontot és válassza a *Hálózati szolgáltatások* > *FTP-kiszolgáló* lehetőséget, vagy adja ki a `yast2 ftp-server` parancsot root felhasználóként.

2. Ha a rendszerben nincs telepítve semmilyen FTP-kiszolgáló, akkor a YaST FTP-kiszolgáló moduljának indításakor a gép megkérdezi, melyik kiszolgálót telepítse.

Válassza ki a kiszolgálót (az openSUSE esetében az vsftpd a szokásos), és hagyja jóvá a választást.

3 Az *Indítás* párbeszédablakban állítsa be az FTP-kiszolgáló indítását. További információkért lásd: 29.1. - Az FTP-kiszolgáló elindítása (496. oldal).

Az *Általános* párbeszédablakban állítsa be az FTP-könyvtárakat, az üdvözlő üzenetet, a fájl-létrehozási maszkokat és a többi paramétert. További információkért lásd: 29.2. - Általános FTP-beállítások (497. oldal).

A *Teljesítmény* párbeszédablakban adja meg azokat a paramétereket, amelyek befolyásolják az FTP-kiszolgáló letöltési tulajdonságait. További információkért lásd: 29.3. - FTP teljesítménybeállítások (498. oldal).

A *Hitelesítés* párbeszédablakban adja meg, hogy az FTP-kiszolgálót elérhessék-e a névtelen (anonymous) és/vagy hitelesített felhasználók. További információkért lásd: 29.4. - Hitelesítés (499. oldal).

A *Szakértői beállítások* párbeszédablakban állítsa be az FTP-kiszolgáló működési módját, az SSL-kapcsolatokat és adja meg a tűzfalbeállításokat is. További információkért lásd: 29.5. - Szakértői beállítások (499. oldal).

4 A beállítások mentéséhez nyomja meg az *Elfogadás* gombot.

29.1 Az FTP-kiszolgáló elindítása

Az *FTP indítása* párbeszédablakának *Szolgáltatásindítás* részében adható meg, hogy hogyan induljon el az FTP-kiszolgáló. Választhat aközött, hogy a kiszolgáló automatikusan elinduljon a rendszerindításkor, vagy kézzel kelljen elindítani. Ha az FTP-kiszolgáló csak az FTP kapcsolódási kérés után induljon, válassza az *xinetd-ben* lehetőséget.

Az FTP-kiszolgáló jelenlegi állapota az *FTP indítása* párbeszédablak *Ki- és bekapcsolás* részében látható. Az FTP-kiszolgáló elindítható az *Az FTP azonnali indítása* gombra kattintva. A kiszolgáló leállításához kattintson az *FTP azonnali leállítása* gombra. Ha módosította a kiszolgáló beállításait, akkor nyomja meg a *Beállítások mentése és az FTP azonnali újraindítása* gombot. A beállítások a konfigurációs modul elhagyásakor az *Elfogadás* gombra kattintva is elmenthetők.

Az *FTP indítása* párbeszédablak *Kiválasztott szolgáltatás* részében ellenőrizhető, hogy melyik FTP-kiszolgáló van használatban. Vagy a vsftpd, vagy a pure-ftpd. Ha mindkét kiszolgáló telepítve van, akkor váltani lehet közöttük. A pure-ftpd csomag nincs fent az alap openSUSE adathordozón, így ha azt szeretné használni, akkor egy másik forrásból kell telepítenie.

29.1. ábra *FTP-kiszolgáló beállítások — Indítás*

29.2 Általános FTP-beállítások

Az *FTP általános beállításai* párbeszédablak *Általános beállítások* részében megadható, hogy milyen *Üdvözlés* jelenjen meg az FTP-kiszolgálóra kapcsolódás után.

Ha megjelölte a *Chroot mindenkinek* lehetőséget, akkor a bejelentkezés után az összes helyi felhasználó bekerül a saját könyvtára chroot jail-jébe. Ennek azonban vannak biztonsági következményei, különösen, ha a felhasználóknak van feltöltési jogosultsága

vagy rendelkeznek parancsértelmező hozzáféréssel -- szóval ezt a beállítást óvatosan engedélyezze!

Ha megjelölte a *Részletes naplózás* beállítást, akkor a rendszer feljegyzi az összes FTP-kérést és választ.

A névtelen és/vagy hitelesített felhasználók által készített fájlok jogosultságai az umask használatával korlátozhatók. Az umask értékben beállított bitek minden újonnan létrehozott fájl esetén le lesznek tiltva. Állítsa be a névtelen felhasználók fájlkészítési maszkját az *Umask - névtelen*, a hitelesített felhasználókét az *Umask - hitelesített* menüpontban. A maszkokat oktális számként kell beírni, egy vezető nullával.

Az *FTP-könyvtárak* részben adhatók meg a névtelen és a hitelesített felhasználók által használt könyvtárak. A névtelen felhasználók alapértelmezett FTP-könyvtára az `/srv/ftp`. Figyeljen rá, hogy a vsftpd nem engedélyezi minden felhasználó számára ennek a könyvtárnak az írását. Ehelyett az `upload` alkönyvtár kínál írási lehetőségeket a névtelen felhasználóknak.

MEGJEGYZÉS

A pure-ftpd kiszolgáló megengedi a névtelen felhasználóknak az FTP-könyvtár írását. Mielőtt visszavált a vsftpd kiszolgálóra, győződjön meg róla, hogy megszüntette a pure-ftpd által használt könyvtár írási jogosultságát.

29.3 FTP teljesítménybeállítások

Az *FTP teljesítménybeállításai* részben adhatók meg az FTP-kiszolgáló terhelését befolyásoló paraméterek. A *Maximális tétlenségi idő* az a leghosszabb szünet (percben), amennyit egy távoli kliens tarthat két FTP-parancs között. Ha ennél tovább inaktív, akkor a rendszer kilépteti a távoli klienst. A *Maximális kliensek száma egyetlen IP-címről* beállítással határozható meg, hogy egyetlen IP-címről legfeljebb hány kliens csatlakozhat. A *Maximális kliensszám* határozza meg, hogy összesen maximum hány kliens csatlakozhat. Ha ennél több próbál kapcsolódni, akkor hibaüzenetet fog kapni.

A helyi hitelesített felhasználók maximális adatátviteli sebessége (KB/másodpercben) a *Hitelesített felhasználók maximális adatátviteli sebessége* beállítással, a névteleneké az *Anonymous felhasználók maximális adatátviteli sebessége* beállítással adható meg.

Az adatátviteli sebességnél az alapértelmezett érték 0, ami azt jelenti, hogy nincs korlátozva az adatátvitel sebessége.

29.4 Hitelesítés

A *Hitelesítés* párbeszédablak *Névtelen és helyi felhasználók engedélyezése/letiltása* részében állítható be, hogy mely felhasználók érhetik el az FTP-kiszolgálót. Megadható, hogy csak a névtelen felhasználók, csak a hitelesített felhasználók vagy mindkét kategória elérhesse a rendszert.

Ha engedélyezni kívánja, hogy a felhasználók fájlokat tölthessenek fel az FTP-kiszolgálóra, jelölje meg a *Hitelesítés* párbeszédablak *Feltöltés* részében található *Felöltés engedélyezése* lehetőséget. Itt engedélyezhető a feltöltés vagy a könyvtárak létrehozása még a névtelen felhasználóknak is, a megfelelő jelölőnégyzet kiválasztásával.

MEGJEGYZÉS

Ha vsftpd kiszolgálót használ és szeretné, hogy a névtelen felhasználóknak lehetősége legyen a fájlok feltöltésére és a könyvtárak létrehozására, akkor létre kell hozni egy minden felhasználó számára írási jogosultsággal bíró alkönyvtárat az anonymous FTP-könyvtárban.

29.5 Szakértői beállítások

Az FTP-kiszolgálók aktív vagy passzív módban is futhatnak. A kiszolgáló alapértelmezésben passzív módban fut. Az aktív módra váltáshoz vegye ki a jelölést a *Passzív mód engedélyezése* jelölőnégyzetéből a *Szakértői beállítások* párbeszédablakban. Módosíthatja a kiszolgáló által az adatfolyamokhoz használt portok tartományát is a *Legalacsonyabb portszám passzív módban* és *Legmagasabb portszám passzív módban* beállítások átírásával.

Ha titkosítani szeretné a kliensek és a kiszolgáló kommunikációját, akkor használhatja az FTPS-protokollt (FTP/SSH) is. Figyeljen azonban arra, hogy az FTPS eltér a sokkal elterjedtebb SFTP-től (SSH File Transport Protocol). Ha használni kívánja az FTPS-t, akkor adja meg az SSL-beállításokat a *Szakértői beállítások* párbeszédablakban.

Ha a rendszert tűzfal védi, akkor az FTP-kiszolgálóhoz csatlakozás engedélyezéséhez jelölje meg a *Tűzfalport megnyitása* lehetőséget.

29.6 További információk

A vsftpd kiszolgálóval kapcsolatban további információkat talál a `vsftpd` és a `vsftpd.conf` kézikönyvoldalain.

VI. rész - Mobilitás

30 Vezetéknélküli kommunikáció

Számos lehetőség áll rendelkezésre a Linux-rendszer és más számítógépek, mobiltelefonok vagy perifériák kommunikációjához. A WLAN (vezetéknélküli LAN) hálózati noteszgépekhez használható.

30.1 Vezetéknélküli LAN

A vezetéknélküli LAN-ok a mobil számítástechnika nélkülözhetetlen tényezőjévé váltak. Manapság a legtöbb noteszgép rendelkezik beépített WLAN-kártyával. A WLAN-kártyák vezetéknélküli kommunikációjához használt 802.11 szabványt az IEEE szervezet készítette elő. A szabvány eredetileg 2 MBit/s maximális átviteli sebességet biztosított. Időközben azonban az adatsebesség növelése érdekében többször is kiegészítésre került. A kiegészítések meghatározzák az olyan részleteket, mint például a moduláció, az átvitel kimenete és átviteli sebesség (lásd: 30.1 táblázat - A különböző WLAN-szabványok áttekintése (503. oldal)). Számos cég valósít meg hardvereszközöket egyedi, vagy még csak szabványvázlat formájában létező funkciókkal.

30.1. táblázat *A különböző WLAN-szabványok áttekintése*

Név	Sáv (GHz)	Maximális átviteli sebesség (MBit/s)	Megjegyzés
802.11 Legacy	2.4	2	Elavult; gyakorlatilag nincsenek ilyen végberendezések

Név	Sáv (GHz)	Maximális átviteli sebesség (MBit/s)	Megjegyzés
802.11a	5	54	Kevésbé érzékeny az interferenciákra
802.11b	2.4	11	Kevésbé általános
802.11g	2.4	54	Széles körben elterjedt, visszamenőlegesen kompatibilis a 11b-vel
802.11n vázlat	2.4 és/vagy 5	300	Közös

Az openSUSE nem támogatja a 802.11 Legacy kártyákat. A legtöbb 802.11a, 802.11b, 802.11g és 802.11n vázlat szabványnak megfelelő kártya támogatott. Az új kártyák általában a 802.11n szabványnak felelnek meg, de a 802.11g-t használók tábora is nagy.

30.1.1 Funkció

A vezetéknélküli hálózatok világában számos technikát és beállítást használnak a gyors, megbízható, biztonságos kapcsolatok érdekében. A különféle működési típusok különféle helyzetekhez a legalkalmasabbak. Nem egyszerű kiválasztani a legjobb hitelesítési módszert sem. A rendelkezésre álló titkosítási eljárásoknak vannak előnyei és hátrányai is.

A vezetéknélküli hálózatok alapvetően vezérelt és ad-hoc hálózatokként osztályozhatók. A vezérelt hálózatok rendelkeznek egy vezérlő eszközzel, ez a hozzáférési pont. Ebben a módban (infrastruktúra módnak is hívják) a hálózatban lévő WLAN-állomások minden kapcsolata átmegy a hozzáférési ponton, amely Ethernet csatlakozási pontként is működik. Az ad-hoc hálózatokban nincs hozzáférési pont. Az állomások közvetlenül egymással kommunikálnak, ezért egy ad-hoc hálózat álalában gyorsabb, mint egy felügyelt hálózat. A ad-hoc hálózatokban azonban az átviteli hatókör és a résztvevő állomások száma nagyon korlátozott. Ezenfelül nem támogatják a WPA-hitelesítést sem. Ezért általában hozzáférési pontot használnak. WLAN-kártya is használható hozzáférési pontként. Egyes kártyák támogatják ezt a működést.

Hitelesítés

Mivel a vezetéknélküli hálózatok lehallgatása és támadása egyszerűbb, mint a vezetékes hálózatoké, a különböző szabványok hitelesítési és titkosítási eljárásokat is tartalmaznak. Az IEEE 802.11 szabvány eredeti változatában ezek a WEP kifejezés alatt voltak leírva. Mivel azonban a WEP bizonyítottan nem biztonságos (lásd: „Biztonság” szakasz (512. oldal)), a (*Wi-Fi Alliance* név alatt egyesült) WLAN iparág egy új, WPA nevű kiterjesztést adott ki, amelynek célja a WEP gyengeségeinek kiküszöbölése. A későbbi IEEE 802.11i szabvány (WPA2-nek is hívják, mivel a WPA a 802.11i draft változatára épül) WPA-t és néhány másik hitelesítési és titkosítási szabványt foglal magában.

Annak biztosításához, hogy csak a jogosult állomások csatlakozhassanak, a vezérelt hálózatokban különböző hitelesítési mechanizmusok kerülnek alkalmazásra:

Megnyitva
: A nyílt rendszer nem igényel hitelesítést. Bármely állomás csatlakozhat a hálózatra. Mindamellett WEP titkosítás (lásd: „Titkosítás” szakasz (506. oldal)) használható.

Megosztott kulcs (az IEEE 802.11 szabványnak megfelelően)
: Ebben az eljárásban a hitelesítéshez a WEP-kulcsot használják. Ez az eljárás azonban nem javasolt, mivel a WEP-kulcs érzékenyebb a támadásokra. A támadónak elég csupán egy ideig figyelnie az állomás és a hozzáférési pont közötti kommunikációt. A hitelesítési folyamat során mindkét oldal ugyanazt az információt cseréli ki, egyszer titkosított és egyszer titkosítatlan formában. Így a kulcs a megfelelő eszközök segítségével újból előállítható. Mivel ez az eljárás a WEP-kulcsot használja hitelesítéshez és titkosításhoz, nem javítja a hálózat biztonságát. A megfelelő WEP-kulccsal rendelkező állomás hitelesítést, titkosítást és visszafejtést végezhet. A kulccsal nem rendelkező állomás nem tudja visszafejteni a kapott csomagokat. Következésképp nem tud kommunikálni, függetlenül attól, hogy tudta-e hitelesíteni magát.

WPA-PSK (az IEEE 802.1x szabványnak megfelelően)
: A WPA-PSK (a PSK az előre megosztott kulcsot (Pre-Shared Key) jelenti) a megosztott kulcsos eljáráshoz hasonlóan működik. Minden résztvevő állomás és a hozzáférési pont ugyanazt a kulcsot használja. A kulcs 256 bites és általában jelszóként kerül megadásra. Ez a rendszer nem igényel olyan bonyolult kulcskezelést, mint a WPA-EAP és privát használatra jobban megfelel. Ezért a WPA-PSK-t „Otthoni” WPA-nak (WPA Home) is nevezik.

WPA-EAP (az IEEE 802.1x szabványnak megfelelően)
: A WPA-EAP valójában nem hitelesítési rendszer, hanem hitelesítési információ átvitelére szolgáló protokoll. A WPA-EAP a vállalati vezetéknélküli hálózatokat védi. Magánhálózatokban nem nagyon használják. Emiatt a WPA-EAP-t „Vállalati" WPA-nak (WPA Enterprise) is szokás hívni.

  A WPA-EAP Radius kiszolgálót használ a felhasználók hitelesítéséhez. Az EAP háromféle módszert kínál a kiszolgálóhoz csatlakozásra és hitelesítésre: TLS (Transport Layer Security), TTLS (Tunneled Transport Layer Security) és PEAP (Protected Extensible Authentication Protocol). Nagyon röviden, ezek a lehetőségek a következőket jelentik:

  EAP-TLS
  : A TLS-hitelesítés lényege, hogy a kiszolgáló és a kliens kölcsönösen tanúsítványokat cserél. Először a kiszolgáló mutatja be a saját tanúsítványát a kliensnek, amelyik azt megvizsgálja. Ha tanúsítványt érvényesnek találja, akkor a kliens mutatja be tanúsítványát a kiszolgálónak. A TLS biztonságos rendszer, de a használatához szükség van a hálózatban egy működő tanúsítványkezelő infrastruktúrára. Ilyen infrastruktúra ritkán található magánhálózatokban.

  EAP-TTLS és PEAP
  : A TTLS és a PEAP kétszakaszos protokollok. Az első szakaszban egy biztonságos kapcsolat létesül és a másodikban történik meg a kliens hitelesítési adatainak a továbbítása. Sokkal kevesebb extra tanúsítványkezelést igényelnek, mint a TLS (vagy akár nincs is szükség rá).

Titkosítás

Többféle titkosítási eljárás áll rendelkezésre annak biztosításához, hogy jogosulatlan személyek ne olvashassák el a vezetéknélküli hálózatban forgalmazott csomagokat és ne férhessenek hozzá a hálózathoz:

WEP (az IEEE 802.11 definiálja)
: Ez a szabvány az RC4 titkosítási algoritmust használja, kezdetben 40 bites kulccsal, később 104 bitessel is. A hosszát gyakran 64 vagy 128 bitként adják meg, ha a 24 bites inicializálási vektort beleszámolják. A szabványnak van néhány gyenge pontja. A rendszer által előállított kulcsok elleni támadás sikeres lehet. Ennek ellenére jobb WEP-et használni, mint egyáltalán nem titkosítani a hálózatot.

Egyes gyártók a nem szabványos „Dinamikus WEP” megoldást valósították meg. Ez pontosan ugyanúgy működik, mint a WEP és pont ugyanazok a gyenge pontjai is, de egy kulcskezelő szolgáltatás időről-időre lecseréli a kulcsokat.

TKIP (WPA/IEEE 802.11i által megadott)
: A WPA szabványban megadott kulcskezelési protokoll ugyanazt a titkosítási algoritmust használja, mint a WEP, de kiküszöböli annak gyengeségeit. Mivel minden adatcsomaghoz új kulcs kerül előállításra, a kulcsok elleni támadás nem sikerülhet. A TKIP-t a WPA-PSK-val együtt használják.

CCMP (az IEEE 802.11i definiálja)
: A CCMP a kulcskezelést írja le. Ezt általában a WPA-EAP-vel együtt használják, de WPA-PSK-val is használható. A titkosítás az AES-nek megfelelően történik és ez erősebb, mint a WEP szabvány RC4 titkosítása.

30.1.2 Beállítás a YaST segítségével

A vezetéknélküli hálózati kártya beállításához válassza ki a *Hálózati eszközök* > *Hálózati beállítások* modult a YaST vezérlőközpontban. Megnyílik a Hálózati beállítások párbeszédablak, amelyben megadhatók az általános hálózati beállítások. Az általános hálózati beállításokkal kapcsolatos további információ a 20.4. - Hálózati kapcsolat beállítása a YaST segítségével (297. oldal) szakaszban olvasható. Minden egyéb, a rendszer által felderített hálózati kártya az *Áttekintés* lapon jelenik meg.

Válassza ki a vezetéknélküli kártyát a listából, majd kattintson a *Szerkesztés* gombra a Hálózati kártya beállítása párbeszédablak megnyitásához. A *Cím* lapon állítsa be, hogy dinamikus vagy statikus IP-címet kíván használni. Az *Általános* és *Harder* lap beállításait is módosíthatja, mint például az *Eszközaktiválás* vagy a *Tűzfalzóna* illetve megadhatja az illesztőprogram beállításait. A legtöbb esetben nincs szükség az előre beállított értékek módosítására.

Kattintson a *Tovább* gombra a vezetéknélküli hálózati kártya saját konfigurációs párbeszédablakára ugráshoz. Ha a NetworkManagert használja (további információ: 20.5. - NetworkManager (317. oldal)), akkor nincs szükség a vezetéknélküli eszköz beállításainak módosítására, mivel ezeket a NetworkManager beállítja igény szerint – lépjen tovább a *Tovább* és *Igen* gombokra kattintva a beállítás befejezéséhez. Ha a számítógépet csak egy meghatározott vezetéknélküli hálózatban használja, akkor adja meg a WLAN-működés legfontosabb beállításait itt.

30.1. ábra *YaST: vezetéknélküli hálózati kártya beállítása*

Működési mód

A WLAN-ba egy állomás háromféleképp illeszkedhet be. A megfelelő mód a hálózattól függ, amelyben a kommunikáció zajlik: *Ad-hoc* (hozzáférési pont nélküli egyenrangú hálózat), *Vezérelt* (hozzáférési pont által vezérelt hálózat) vagy *Master* (a hálózati kártya hozzáférési pontként kerül használatra). A WPA-PSK vagy WPA-EAP módok bármelyikének használatához a működési mód csak *Vezérelt* lehet.

Hálózat neve (ESSID)

A vezetéknélküli hálózat minden állomásának ugyanarra az ESSID-re van szüksége az egymással való kommunikációhoz. Ha semmi nincs megadva, akkor a kártya lehet, hogy automatikusan kiválaszt egy hozzáférési pontot, amely nem biztos, hogy megegyezik a használni kívánttal. A *Hálózat vizsgálata* pontra kattintva megjelenik a rendelkezésre álló vezetéknélküli hálózatok listájának megjelenítéséhez.

Hitelesítési mód

Válassza ki a hálózat kívánt hitelesítési módját: *Nincs titkosítás*, *WEP-Nyílt*, *WEP - Osztott kulcs*, *WPA-EAP* vagy *WPA-PSK*. Ha WPA-hitelesítést választ, akkor a hálózat nevét (ESSID) be kell állítani.

Kulcsbevitel típusa

A WEP és a WPA-PSK hitelesítési eljárások megkövetelik egy kulcs beírását. A kulcs beírható, mint egy *Titkosítási jelszó*, mint egy *ASCII* karaktersorozat vagy mint egy *Hexadecimális* karaktersorozat.

WEP-kulcsok

Adja meg itt az alapértelmezett kulcsot, vagy kattintson a *WEP kulcsok* pontra a szakértői kulcskonfigurációs párbeszédablakba belépéshez. Adja meg a kulcs hosszát: *128 bit* vagy *64 bit*. Az alapértelmezett beállítás a *128 bit*. A párbeszédablak alsó részén található listaterületen maximum négy különböző kulcs adható meg az állomás titkosításához. Az egyik alapértelmezett kulcsként való megadásához kattintson az *Alapértelmezettként beállít* gombra. Hacsak meg nem változtatja, akkor a YaST az elsőként megadott kulcsot használja alapértelmezettként. Az alapértelmezett kulcs törlése esetén egy másik kulcsot kell kézzel alapértelmezettként megjelölni. A meglévő listabejegyzések módosításához vagy új kulcsok létrehozásához kattintson a *Szerkesztés* gombra. Ebben az esetben egy előugró ablakban ki kell választani egy beviteli típust (*Jelszó*, *ASCII* vagy *Hexadecimális*). Ha a *Jelszó* lehetőséget választja, akkor adjon meg egy szót vagy karaktersorozatot, amelyből a kulcs a korábban megadott hossznak megfelelően létrehozásra kerül. Az *ASCII* 64 bites kulcs esetén 5, 128 bites kulcs esetén pedig 13 karakteres bemenet megadását kéri. A *Hexadecimális* lehetőség esetén 64 biteshez 10, 128 bites hexadecimális formátumú kulcshoz pedig 26 karaktert kell megadni.

WPA-PSK

WPA-PSK kulcs megadásához a *Jelszó* vagy *Hexadecimális* beviteli eljárást válassza. *Jelszó* módban a bemenet 8 - 63 karakter lehet. *Hexadecimális* módban 64 karaktert kell megadni.

Szakértői beállítások

Ez a gomb megnyit egy párbeszédablakot a WLAN-kapcsolat részletes beállításához. Általában nincs szükség az előre megadott beállítások módosítására.

Csatorna
: A csatornát, amelyet a WLAN-állomásnak használnia kell, csak *Ad-hoc*, illetve *Master* módban kell megadni. *Vezérelt* módban a kártya automatikusan megkeresi a hozzáférési ponthoz rendelkezésre álló csatornákat. *Ad-hoc* módban az állomás másik állomásokkal való kommunikációjához válassza ki a felkínált csatornák egyikét (11-14 csatorna, országtól függően). *Master* módban adja meg, hogy a kártyának mely csatornán kell hozzáférési pont funkciót biztosítania. Az alapértelmezett beállítás az *Automatikus*.

Bitsebesség
: A hálózat teljesítményétől függően elképzelhető, hogy az átvitelhez az egyik pontról a másikra be kíván állítani egy adott bitsebességet. Az alapértelmezett *Automatikus* beállításban a rendszer a lehető legnagyobb adatátviteli sebességet próbálja meg használni. Néhány WLAN-kártya nem támogatja a bitsebesség beállítását.

Hozzáférési pont
: Több hozzáférési ponttal rendelkező környezetben a MAC-cím megadásával az egyik előzetesen kiválasztható.

Energiagazdálkodás használata
: Ha úton van, akkor érdemes használni az energiagazdálkodási funkciókat az akkumulátoros üzemidő maximalizálása érdekében. Az energiagazdálkodási funkciók használata azonban befolyásolhatja a kapcsolat minőségét és ronthatja a hálózat késleltetését.

Kattintson a Tovább gombra a beállítások befejezéséhez. Ha WPA-EAP hitelesítést választott, akkor még egy beállítási lépésre van szükség, mielőtt az állomás készen áll a WLAN-on belüli használatra. Adja meg a hálózati rendszergazda által biztosított hitelesítési adatokat. TLS esetében az *Azonosító*, *Klienstanúsítvány*, *Klienskulcs* és *Kiszolgálótanúsítvány* értékeket kell megadni. A TTLS és a PEAP esetében az *Azonosító* és a *Jelszó* értékekre van szükség. A *Kiszolgálótanúsítvány* és az *Anonim azonosság* használata nem kötelező. A YaST az `/etc/cert` könyvtárban keresi a tanúsítványokat. Éppen ezért a kapott tanúsítványokat ebbe a könyvtárba mentse el, és állítsa `0600`-ra (tulajdonos olvasás-írás) a jogosultságokat. A *Részletek* gombra kattintva léphet be a WPA-EAP konfiguráció speciális hitelesítési párbeszédablakába.. Válassza ki a hitelesítési eljárást az EAP-TTLS vagy EAP-PEAP kommunikáció második szakaszához. Ha az előző ablakban a TTLS-t választotta, akkor válassza ki a `Mind`, `MD5`, `GTC`, `CHAP`, `PAP`, `MSCHAPv1` vagy `MSCHAPv2` lehetőséget. Ha a PEAP-t választotta, akkor a `Mind`, `MD5`, `GTC` és `MSCHAPv2` közül választhat. A *PEAP-verzió* beállítással lehet kényszerí-

teni egy bizonyos PEAP-implementáció használatát, ha az automatikusan meghatározott beállítások nem lennének megfelelők.

FONTOS: Biztonság a vezetéknélküli hálózatokban

A hálózati forgalom védelme érdekében feltétlenül használja valamelyik támogatott hitelesítési és titkosítási eljárást. A titkosítatlan WLAN-kapcsolatok lehetővé teszik a hálózati adatok lehallgatását. Még a gyenge titkosítás (WEP) is jobb, mint a semmi. További információ: „Titkosítás” szakasz (506. oldal) és „Biztonság” szakasz (512. oldal).

30.1.3 Segédprogramok

A `wireless-tools` csomag olyan segédprogramokat tartalmaz, amelyek lehetővé teszik a vezetéknélküli LAN-specifikus paraméterek megadását és statisztikák gyűjtését. További információkért lásd: `http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Tools.html`.

A kismet (`kismet` csomag) egy hálózatdiagnosztikai eszköz, amellyel a WLAN-csomagforgalom figyelhető. Ily módon a hálózatba való behatolási kísérletek is detektálhatók. További információ a `http://www.kismetwireless.net/` címen és a kézikönyvoldalon található.

30.1.4 Tippek és trükkök WLAN beállításához

Az alábbi tippek segíthetnek a WLAN sebességének, stabilitásának, valamint biztonsági tényezőinek beállításában.

Stabilitás és sebesség

A vezetéknélküli hálózat teljesítménye és megbízhatósága főként attól függ, hogy a résztvevő állomások tiszta jelet kapnak-e a többi állomástól. A különböző akadályok, mint például a falak, lényegesen gyengítik a jelet. Minél jobban csökken a jel erőssége, annál jobban lelassul az átvitel. A működés során a konzolon (`Csatlakozás minősége` mező) az iwconfig, a NetworkManager vagy a KNetworkManager segítsé-

gével ellenőrizze a jel erősségét. Ha problémája van a jel minőségével, akkor próbálja meg az eszközöket valahol másutt beállítani vagy állítson a hozzáférési pontok antennáinak pozícióján. Számos PCMCIA WLAN kártyához vételt javító kiegészítő antennák is kaphatók. A gyártó által megadott sebesség (például 54 MBit/s) egy névleges érték, amely az elméleti maximumot jelenti. Gyakorlatban a maximális adatátviteli sebesség nem több, mint a megadott érték fele.

Biztonság

Ha vezetéknélküli hálózatot kíván beállítani, akkor ne feledje el, hogy biztonsági intézkedések nélkül azt az átviteli hatókörben lévő személyek közül bárki könnyen elérheti. Ezért mindenképpen alkalmazzon valamilyen titkosítási eljárást. Minden WLAN-kártya és hozzáférési pont támogatja a WEP titkosítást. Bár nem teljesen biztonságos, némi akadályt azért jelent egy potenciális támadó számára. A WEP saját használatra általában megfelelő. A WPA-PSK jobb, de a régi hozzáférési pontok és WLAN funkcióval rendelkező útválasztók nem támogatják. Néhány eszközön a WPA firmware-frissítés után használható. Ezenfelül, bár a Linux támogatja a WPA-t a legtöbb hardverkomponensen, előfordulhat, hogy egyes illesztőprogramok nem biztosítanak WPA-támogatást. Ha nem áll rendelkezésre WPA, akkor a WEP még mindig jobb, mint ha egyáltalán nincs titkosítás. Speciális biztonsági követelményeket támasztó vállalatokban a vezetéknélküli hálózatok csak WPA-val használhatók.

30.1.5 Hibaelhárítás

Ha a WLAN-kártyát nem sikerült automatikusan felismerni, akkor ellenőrizze, hogy az openSUSE valóban támogatja-e. A támogatott WLAN hálózati kártyák listája a `http://en.opensuse.org/HCL/Network_Adapters_(Wireless)` címen érhető el. Ha a kártya nem támogatott, akkor még mindig lehetséges, hogy az Ndiswrapper segítségével használni tudja a windowsos illesztőprogramokat. Részletes információ: `http://en.opensuse.org/Ndiswrapper`.

Ha a WLAN-kártya nem válaszol, akkor ellenőrizze, hogy letöltötte-e a szükséges firmware-t. További információ az `/usr/share/doc/packages/wireless-tools/README.firmware` fájlban található.

Több hálózati eszköz

A modern noteszgépek általában hálózati kártyával és WLAN-kártyával is rendelkeznek. Ha mindkét eszközt DHCP (automatikus címkiosztás) használatára állította be, akkor probléma lehet a névfeloldással és az alapértelmezett ájáróval. Ez nyilvánvaló abból, ha az útválasztót tudja pingelni, de nem tud böngészni az interneten. A http://en.opensuse.org/SDB:Name_Resolution_Does_Not_Work_with_Several_Concurrent_DHCP_Clients címen található Támogatási adatbázisban van egy, a témakörrel kapcsolatos cikk.

Problémák a Prism2 kártyákkal

Számos illesztőprogram érhető el a Prism2 lapkákra épülő eszközökhöz. A különböző kártyák többé-kevésbé problémamentesen működnek a különböző illesztőprogramokkal. Ezen kártyákkal WPA csak a hostap illesztőprogram alkalmazása esetén használható. Ha egy ilyen kártya nem működik megfelelően vagy egyáltalán nem működik, illetve ha WPA-t kíván használni, olvassa el az `/usr/share/doc/packages/wireless-tools/README.prism2` fájl tartalmát.

30.1.6 További információk

Jean Tourrilhes (aki a *vezetéknélküli eszközöket* fejlesztette Linuxhoz) oldalain sok, a vezetéknélküli hálózatokkal kapcsolatos hasznos információ található. Lásd:http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Wireless.html

31 Tábla PC-k használata

Az openSUSE támogatja a tábla PC-ket, mind a soros Wacom-eszközöket használókat (mint például az IBM/Lenovo X41, az ACER TM C300/C301/C302 series, a Fujitsu Lifebook T series (T3010/T4010), a HP Compaq TC4200, Motion M1200/M1400), mind a FinePoint eszközzel felszerelteket (mint a Gateway Tablet PC-i), valamint a Fujitsu Siemens Computers P-sorozat gépeit is. Ismerje meg, hogyan telepítheti és állíthatja be tábla PC-jét, valamint bemutatunk néhány hasznos linuxos alkalmazást is, amelyek elfogadják a digitális tollakat bemenetként.

Miután telepítette a tábla PC-hez tartozó csomagokat és elvégezte a digitalizáló megfelelő beállítását, a toll (amelyet stylusnak is neveznek) segítségével a következő műveleteket végezheti el:

- Bejelentkezés a KDM-be vagy a GDM-be
- A képernyő zárolásának feloldása a KDE és a GNOME munkaasztalon.
- Egyéb műveletek, amelyek más bemeneti eszközökkel (mint az egér vagy a touch pad) is elvégezhetőek, például a kurzor mozgatása a képernyőn, alkalmazások indítása, ablakok bezárása, átméretezése és áthelyezése, ablak fókuszának módosítása, objektumok áthúzása
- Gesztusfelismerő használata az X Window System alkalmazásaiban
- Rajzolás a The GIMP eszközzel
- Jegyzetek vagy vázlatok készítése az olyan alkalmazásokkal mint a Jarnal vagy a Xournal, illetve nagymennyiségű szöveg szerkesztése a Dasher segítségével

MEGJEGYZÉS: A telepítéshez szükséges egy billentyűzet vagy egy egér

Az openSUSE telepítése során a toll nem használható bemeneti eszközként. Ha tábla PC-jén nincs beépített billentyűzet vagy touch pad, a rendszer telepítéséhez csatlakoztatnia kell egy külső billentyűzetet vagy egeret.

31.1 Tábla PC csomagok telepítése

A `Hordozható gép` telepítési minta tartalmazza a tábla PC-k használatához szükséges csomagokat – ha ezt választotta ki telepítéskor, akkor az alábbi csomagok már telepítve kell, hogy legyenek a rendszeren:

- `jarnal`: egy Java alapú jegyzetkészítő alkalmazás
- `xournal`: egy jegyzetek és ábrák készítésére használható alkalmazás
- `xstroke`: egy gesztusfelismerő program az X Window System-hez
- `xvkbd`: egy virtuális billentyűzet az X Window System-hez
- `cellwriter`: egy karakter alapú, kézírásfelismerő beviteli panel
- `x11-input-wacom`: az X bemeneti modul a Wacom táblákhoz
- `x11-input-wacom-tools`: konfiguráció, diagnosztika, és könyvtárak a Wacom táblákhoz
- `x11-input-fujitsu`: a Fujitsu P-sorozatú táblagépek X-beviteli modulja

Ha ezek a csomagok nem lennének telepítve, akkor telepítse a szükséges csomagokat kézzel a parancssorból, vagy válassza ki a YaST-ban a `Hordozható gép` telepítési mintát.

31.2 A tábla eszköz beállítása

A tábla PC csomagok telepítése után állítsa be a (belső vagy külső) tábla eszközt a SaX2 segítségével.

1. Indítsa el a SaX2-ot a parancssorból vagy nyomja meg az Alt + F2 gombot és írja be, hogy `sax2`.

2. Ha Wacom eszközt használ, akkor kattintson a *Tábla PC* pontra a *Tábla PC gyártója és típusa* megjelenítéséhez.

   Ha Fujitsu P-sorozatú gépet használ, akkor az *Érintőképernyő* pontra kattintson.

3. A jobb oldali listából válassza ki a *Tábla PC-k* gyártóját, majd jelölje meg a *Tábla PC aktiválása* pontot.

   Ha a gép nincs felsorolva, de biztos benne, hogy Wacom eszköz van benne, válassza ki a *Wacom ISDV4 tábla PC (soros)* pontot.

4. Váltson át az *Electronikus tollak* lapra, és győződjön meg róla, hogy az alábbi pontok ki vannak választva: *Toll hozzáadása* és *Radír hozzáadása*.

5. A módosítások mentéséhez kattintson az *OK* gombra.

Az X Window rendszer beállítása után indítsa újra az X kiszolgálót: jelentkezzen ki. Alternatív megoldásként lépjen ki a felhasználói felületről és futtassa le egy virtuális konzolban az `init 3 && init 5` parancsot.

A tábla eszköz beállítása után elkezdheti használni a tollat beviteli eszközként.

31.3 A virtuális billentyűzet használata

Ha be kíván jelentkezni a KDE vagy a GNOME munkaasztalra, vagy a képernyő zárolását szeretné feloldani, felhasználónevét és jelszavát a megszokott módszeren kívül a bejelentkezési mező alatt található xvkbd virtuális billentyűzet segítségével is megad-

hatja. A billentyűzet beállításához vagy a beépített súgó megnyitásához kattintson a bal alsó sarokban az *xvkbd* mezőre az xvkbd főmenü megnyitásához.

31.1. ábra *xvkbd Virtuális billentyűzet*

Ha használni kívánja az xvkbd-t a bejelentkezés után, indítsa azt el a főmenüből vagy az `xvkbd` parancs beírásával egy parancsértelmezőbe.

31.4 A képernyő elforgatása

A KRandRTray (KDE) vagy gnome-display-properties (GNOME) kisalkalmazásokkal menet közben forgathatja el és méretezheti át a képernyőt. Mind a KRandRTray, mind a gnome-display-properties az X kiszolgáló RANDR-bővítésének kisalkalmazásai.

Indítsa el a KRandRTray-t vagy gnome-display-properties-t a főmenüből, vagy ha egy parancsértelmezőből akarja indítani a kisalkalmazást, akkor írja be, hogy `krandrtray` ill. `gnome-display-properties`. A megfelelő kisalkalmazás elindítása után a kisalkalmazás ikonja általában megjelenik a rendszer tálcáján. Ha a gnome-display-properties ikonja nem jelenne meg automatikusan a rendszer tálcáján, akkor ellenőrizze, hogy a *Monitorfelbontás beállításai* párbeszédablakban a *Képernyők megjelenítése a panelen* funkció be van-e kapcsolva.

Ha el akarja forgatni a képernyőt a KRandRTray segítségével, akkor kattintson a jobb egérgombbal, majd válassza ki az előugró menü *Kijelző beállítása* pontját. A konfigurációs párbeszédablakban válassza ki a kívánt tájolást.

Ha el akarja forgatni a képernyőt a gnome-display-properties segítségével, akkor kattintson a jobb egérgombbal, majd válassza ki a kívánt tájolást. A képernyő azonnal el-

fordításra kerül az új irányba. A grafikai tábla tájolása is módosul, hogy a továbbiakban is helyesen értelmezze a toll mozgását.

Ha gondjai lennének a képernyő tájolásának beállításával, akkor további információt a 31.7. - Hibaelhárítás (522. oldal) rész tartalmaz.

31.5 A gesztusfelismerés használata

Az xstroke segítségével a gesztusokat a toll vagy egy egyéb mutatóeszköz segítségével bemeneti adatként használhatja fel az X Window rendszer alkalmazásaiban. Az xstroke ABC egy unistroke ABC, amely hasonlít a Graffiti* ABC-re. Aktivált állapotban az xstroke az éppen fókuszált ablakba küldi a bemeneti jelet.

1. Az xstroke-ot elindíthatja a főmenüből vagy az `xstroke` parancs beírásával egy parancsértelmezőbe. Ez hozzáad egy ceruza ikont a rendszertálcához.

2. Indítsa el azt az alkalmazást amelyikben a szöveget akarja bevinni a toll segítségével (például egy terminálablak, egy szövegszerkesztő, vagy az OpenOffice.org Writer).

3. A gesztusfelismerő mód aktiválásához kattintson egyszer a ceruza ikonra.

4. Mutasson be néhány gesztust a grafikus táblán a toll vagy valamely egyéb mutatóeszköz segítségével. Az xstroke rögzíti a gesztusokat és szöveggé alakítja át azokat, amely a fókusszal rendelkező alkalmazásablakban jelenik meg.

5. Ah egy másik ablakra szeretné átváltani a fókuszt, kattintson a kívánt ablakra a tollal és tartsa ott egy pillanatig (vagy használja az asztal vezérlőpultjában meghatározott gyorsbillentyűt).

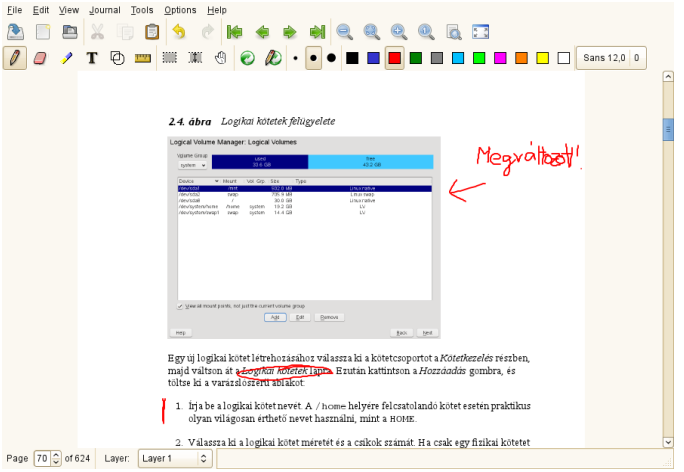
6. A gesztusfelismerő mód deaktiválásához kattintson ismét a ceruza ikonra.

31.6 Jegyzetek és ábrák készítése a Toll segítségével

Ha rajzolni szeretne a tollal, használhatja a professzionális grafikus szerkesztőket - mint a The GIMP - vagy kipróbálhatja a jegyzetkészítő alkalmazások - Xournal vagy Jarnal - egyikét. A Xournal és a Jarnal is lehetőséget ad jegyzetek és rajzok készítésére, illetve a toll segítségével PDF fájlokhoz is megjegyzéseket fűzhet. A Java alapú alkalmazás számos platformon elérhető, a Jarnal ezen túlmenően némi alapszintű együttműködést is lehetővé tesz. További információért lásd: `http://www.dklevine.com/general/software/tc1000/jarnal-net.htm`. A tartalom mentése során a Jarnal archív formátumban (*.jaj) tárolja az adatokat, amely tartalmaz egy SVG formátumban levő fájlt is.

A Jarnalt és a Xournalt is elindíthatja a főmenüből, csak írja be egy parancsértelmezőbe a `jarnal` vagy a `xournal` parancsot. Ha például megjegyzést kíván fűzni egy PDF fájlhoz a Xournalban, válassza a *Fájl > Feljegyzés PDF fájlhoz* menüpontot és nyissa meg a PDF fájlt a rendszerben. A PDF-hez kapcsolódó feljegyzés készítéséhez használja a tollat vagy egy más mutatóeszközt, majd mentse el a módosításokat a *Fájl > Nyomtatás PDF fájlba* menüpontra kattintva.

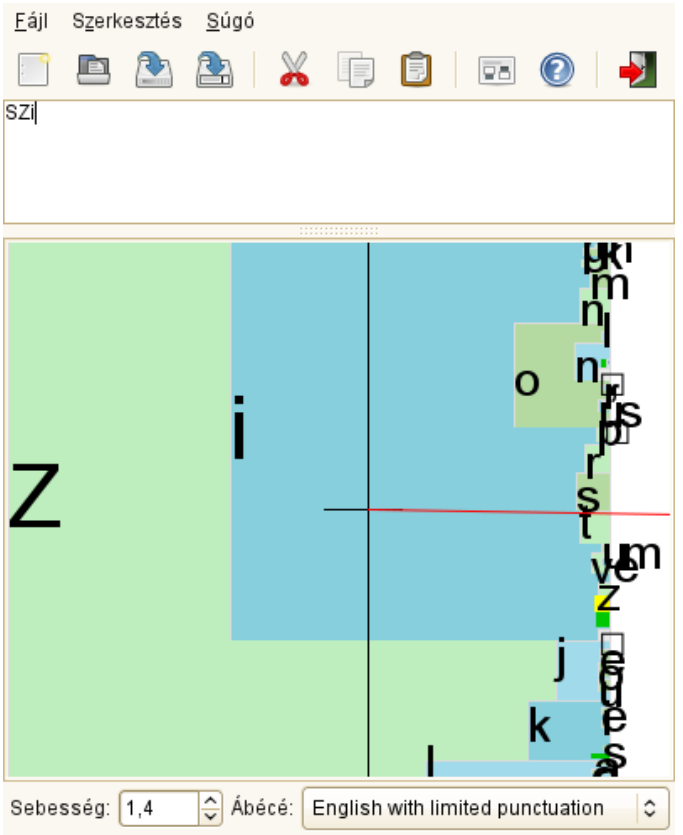
31.2. ábra *Feljegyzés készítése PDF fájlhoz a Xournal segítségével*



A Dasher szintén hasznos alkalmazás. Azokra az esetekre tervezték, mikor a billentyűvel végzett adatbevitel nem praktikus vagy nem elérhető. Némi gyakorlás után képes lesz nagyon gyorsan nagymennyiségű szöveget bevinni csak a toll segítségével is (vagy egy más beviteli eszközzel—, még egy szemkövetővel is működtethető).

A Dashert elindíthatja a főmenüből vagy a `dasher` parancs beírásával egy parancsértelmezőbe. Mozgassa el a tollat valamelyik irányban és az alkalmazás kinagyítja a jobb oldalon található betűket. A program a középen található célkereszteken áthaladó betűkből megalkotja vagy megpróbálja kitalálni a szöveget, amely aztán az ablak felső részében jelenik meg. Az írás elindításához vagy leállításához kattintson egyszer a tollal a kijelzőre. Az ablak alján módosíthatja a nagyítási/kicsinyítési sebességet.

31.3. ábra *Szövegszerkesztés a Dasher segítségével*



A Dasher-elgondolás számos nyelven működik. További információkat a Dasher honlapján talál részletes dokumentációkkal, demonstrációs és oktató szövegekkel együtt. Itt találhatja meg: http://www.inference.phy.cam.ac.uk/dasher/

31.7 Hibaelhárítás

A virtuális billentyűzet nem jelenik meg a bejelentkezési képernyőn

A virtuális billentyűzet néha nem jelenik meg a bejelentkezési képernyőn. A probléma megoldásához indítsa újra az X kiszolgálót a(z) Ctrl + Alt + <— megnyomásával, vagy nyomja mega tábla PC-n a megfelelő billentyűt (ha integrált billentyűzet nélküli modellt használ). Ha továbbra sem jelenik meg a virtuális billentyűzet, csatlakoztasson egy külső billentyűzetet számítógépéhez és jelentkezzen be annak segítségével.

A GNOME-ban nem módosul a grafikus táblák tájolása

A `xrandr` paranccsal módosíthatja a megjelenítés tájolását egy parancsértelmezőben. Az elérhető opciók megtekintéséhez írja be a következőt: `xrandr --help`. A grafikai tábla tájolásának egyidejű módosításához a parancsot a következőképpen kell módosítani:

- Normál tájoláshoz (0° elforgatás):

```
xrandr -o 0 && xsetwacom set "Mouse[7]" Rotate NONE
```

- 90°-os elforgatáshoz (óramutató járásával megegyező, álló):

```
xrandr -o 3 && xsetwacom set "Mouse[7]" Rotate CW
```

- 180° -os elforgatáshoz (fekvő):

```
xrandr -o 2 && xsetwacom set "Mouse[7]" Rotate HALF
```

- 270°-os elforgatáshoz (óramutató járásával ellentétes, álló):

```
xrandr -o 1 && xsetwacom set "Mouse[7]" Rotate CCW
```

Ne feledje, hogy a fenti parancsok nem függetlenek az `/etc/X11/xorg.conf` konfigurációs fájl tartalmától. Ha az eszközt a SaX2 segítségével állította be (lásd: 31.2. - A tábla eszköz beállítása (517. oldal)), akkor a parancsoknak az itt leírt módon működniük kell. Ha módosította a táblatoll bemeneti eszközhöz tartozó `Azonosító`

paramétert az `xorg.conf` fájlban, helyettesítse a `"Mouse[7]"` értékét az új `Azonosító`-val.

31.8 További információk

Az említett alkalmazások közül néhány nem tartalmaz beépített online súgót, de a telepített rendszerhez kapcsolódó beállításokról és használatról hasznos információkat találhat az interneten illetve a következő helyen: `/usr/share/doc/package/`*`packagename`*:

- Az Xournal kézikönyv itt található: `http://xournal.sourceforge.net/manual.html`
- A Jarnal dokumentáció itt található: `http://www.dklevine.com/general/software/tc1000/jarnal.htm#documentation`
- Az xstroke főoldal itt található: `http://davesource.com/Projects/xstroke/xstroke.txt`
- A HOWTO az X konfigurálásához a Linux Wacom weboldalon itt található: `http://linuxwacom.sourceforge.net/index.php/howto/x11`
- Egy kifejezetten informatív weboldal a Dasher projektről itt található: `http://www.inference.phy.cam.ac.uk/dasher/`
- További információk a CellWriterről: at `http://risujin.org/cellwriter/`
- A gnome-display-properties programmal kapcsolatos információ a `http://en.opensuse.org/GNOME/Multiscreen` címen olvasható.

Az ujjlenyomat-olvasó használata

32

Ha az ön rendszerében található ujjlenyomat-olvasó, a hagyományos felhasználóneves és jelszavas bejelentkezés mellett biometrikus azonosítást is használhat. Az ujjlenyomatuk regisztrálása után a felhasználók vagy az ujjuknak az olvasón történő végighúzásával vagy pedig egy jelszó beírásával jelentkezhetnek be. Az openSUSE a kereskedelmi forgalomban elérhető legtöbb ujjlenyomat-olvasót kezeli. A támogatott eszközök listája: `http://reactivated.net/fprint/wiki/Supported_devices`.

Ha a program a hardverellenőrzés során felismeri a laptopján (vagy ahhoz csatolva) az ujjlenyomat-olvasót, akkor a `libfprint`, `pam_fp`, és `yast2-fingerprint-reader` csomagok automatikusan telepítésre kerülnek.

Jelenleg felhasználónként csak egy ujjlenyomat regisztrálható. A felhasználó ujjlenyomatadatai a `/home/`*`login`*`/.fprint/` könyvtárban tárolódnak.

32.1 Támogatott alkalmazások és műveletek

A `pam_fp` PAM-modul a következő műveletekhez és alkalmazásokhoz kapcsolódóan támogatja az ujjlenyomat-azonosítást (nem minden alkalmazás kéri fel külön ujjának végighúzására az olvasón):

- Bejelentkezés a GDM/KDM-be vagy egy bejelentkezési parancsértelmezőbe
- A zárlat feloldása a GNOME/KDE asztal képernyőjén

- A YaST és a YaST modulok indítása
- Alkalmazás indítása a `root` engedéllyel: `sudo` vagy `gnomesu`
- Váltás egy másik felhasználói identitásra a következőkkel: `su` vagy `su –` *`felhasználónév`*

MEGJEGYZÉS: Ujjlenyomat-olvasó eszközök és titkosított saját könyvtárak

Ha ujjlenyomat-olvasó eszközt kíván használni, akkor nem használhat titkosított saját könyvtárakat (további információ: 5. fejezet - *Managing Users with YaST* (↑*Start-Up*)). Ha ugyanis így tesz, akkor a bejelentkezés nem fog sikerülni, mivel a bejelentkezéskor még nem működik a visszafejtés az aktív ujjlenyomat-olvasó eszköz mellett.

32.2 Ujjlenyomatok kezelése a YaST programmal

32.1. eljárás *Ujjlenyomatos azonosítás engedélyezése*

Csak akkor használhat biometriai hitelesítést, ha a PAM ennek megfelelően van beállítva. Általában ez automatikusan megtörténik a csomagok telepítése során, amikor a hardverellenőrzés során a rendszer támogatott ujjlenyomat-olvasót észlel. Ha mégsem így lenne, állítsa be az ujjlenyomat-kezelést a YaST az alábbi módon:

1. Indítsa el a YaST programot, majd válassz a *Hardver* > *Ujjlenyomat-olvasó* lehetőséget.
2. A konfigurációs párbeszédablakban aktiválja az *Ujjlenyomat-olvasó használata* lehetőséget, majd a módosítások mentéséhez és a párbeszédablak bezárásához kattintson a *Befejezés* gombra.

Mostantól ujjlenyomatot is regisztrálhat a különböző felhasználókhoz kapcsolódva.

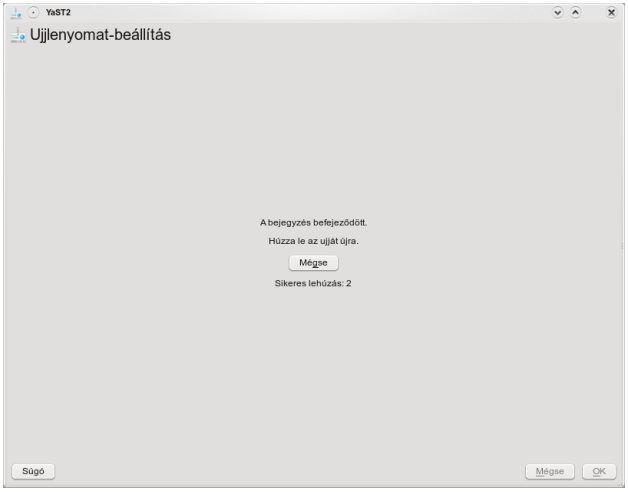
32.2. eljárás *Ujjlenyomat regisztrálása*

1. A YaST programban kattintson a *Biztonság és felhasználók* > *Felhasználók* pontra a *Felhasználók és csoportok* párbeszédablak megnyitásához. Megjelenik a rendszerben található felhasználók és csoportok egy listája.

2. Jelölje ki azt a felhasználót, akihez az ujjlenyomatot regisztrálni kívánja, majd kattintson a *Szerkesztés* pontra.

3. A *Bővítőmodulok* lapon jelölje ki az ujjlenyomat-bevitel lehetőséget, majd kattintson az *Indítás* pontra az *Ujjlenyomat-beállítás* párbeszédablak megnyitásához.

4. A YaST egy üzenet segítségével felkéri a felhasználót, hogy húzza végig az ujját az olvasón addig, amíg a rendszer összegyűjt három olvasható ujjlenyomatot.



5. Az ujjlenyomat sikeres leolvasása után kattintson az *Elfogad* pontra az *Ujjlenyomat-beállítás* párbeszédablak és a felhasználóhoz tartozó párbeszédablak bezárásához.

6. Ha a YaST vagy a YaST modulok indítását is ujjlenyomat-azonosításhoz kívánja kötni, a `root` számára is be kell állítania egy ujjlenyomatot.

Ehhez állítsa be a szűrőt a *Felhasználók és csoportok adminisztrációja* párbeszédablakban a következőre: *Rendszerfelhasználók*, jelölje ki a `root` bejegyzést és a fentebb leírtak alapján regisztrálja az ujjlenyomatot a `root` számára.

7 Miután regisztrálta az ujjlenyomatokat a kiválasztott felhasználók részére, az adminisztrációs párbeszédablak bezárásához és a módosítások mentéséhez kattintson a *Befejezés* gombra.

Amint a felhasználó ujjlenyomata sikeresen regisztrálásra került, a felhasználó eldöntheti, hogy ujjlenyomatos vagy jelszavas azonosítást szeretne kapcsolni azokhoz a műveletekhez és alkalmazásokhoz, amelyek itt kerültek felsorolásra: 32.1. - Támogatott alkalmazások és műveletek (525. oldal).

Jelenleg a YaST nem támogatja az ujjlenyomatok ellenőrzését vagy eltávolítását, de az eltávolításhoz egyszerűen csak törölje a `/home/login/.fprint` könyvtárat.

További technikai részletek a következő hivatkozás alatt találhatók: `http://reactivated.net/fprint/`.

VII. rész - Biztonság

33 Álcázás és tűzfalak

Hálózati környezetben üzemeltetett Linux-rendszereken használhatók azok a kernelfunkciók, amelyek lehetővé teszik a hálózati csomagok előfeldolgozását a belső és külső hálózati terület határozott szétválasztása érdekében. A Linux hálózati szűrő keretrendszer biztosítja egy hatékony tűzfal létrehozásának lehetőségét, amely a különböző hálózatokat szétválasztja. Az iptables – ez egy általános táblázatos struktúra a szabályhalmazok meghatározásához – segítségével precízen szabályozható, hogy a hálózati csatolóhoz milyen csomagok jussanak el. A SuSEfirewall2 és a megfelelő YaST-modul segítségével egyszerűen beállítható egy ilyen csomagszűrő.

33.1 Csomagszűrés az iptables segítségével

A netfilter és iptables komponens felelős a hálózati csomagok szűréséért és kezeléséért, valamint a hálózati címfordításért (network address translation, NAT). A szűrési feltételek és a hozzájuk tartozó tevékenységek láncokként tárolódnak és az érkező hálózati csomagok sorban, a lánc összes feltételének meg kell, hogy feleljenek. A feltételláncokat táblázatok tartalmazzák. A táblák és a szabályhalmazok az `iptables` parancs segítségével módosíthatók.

A Linux-kernel három táblázatot tart fenn, a csomagszűrő funkcióinak megfelelő kategóriáihoz:

szűrő
: Ez a táblázat tárolja a szűrőszabályok nagy részét, mivel szigorúbb értelemben ez valósítja meg a *csomagszűrési* mechanizmust, amely meghatározza, hogy a csomagok átengedésre (`ACCEPT`) vagy eldobásra (`DROP`) kerüljenek.

nat (címfordítás)
: Ez a táblázat a csomagok forrás -és célcímének módosításait határozza meg. E funkciók segítségével *álcázás* is megvalósítható, amely a NAT egy speciális esete egy magánhálózat és az internet összekapcsolásakor.

mangle (szétdarabolás)
: Az ebben a táblázatban tárolt szabályok lehetővé teszik az IP-csomagok fejléceiben tárolt értékek módosítását (mint például a szolgáltatás típusa).

A fent említett táblázatok előre meghatározott láncokat is tartalmaznak a csomagok ellenőrzéséhez:

PREROUTING
: Ez a lánc a bejövő csomagokra vonatkozik.

INPUT
: Ez a lánc a rendszer belső folyamataihoz címzett csomagokra vonatkozik.

FORWARD
: Ez a lánc a rendszeren keresztül csak továbbított csomagokra vonatkozik.

OUTPUT
: Ez a lánc a rendszertől származó csomagokra vonatkozik.

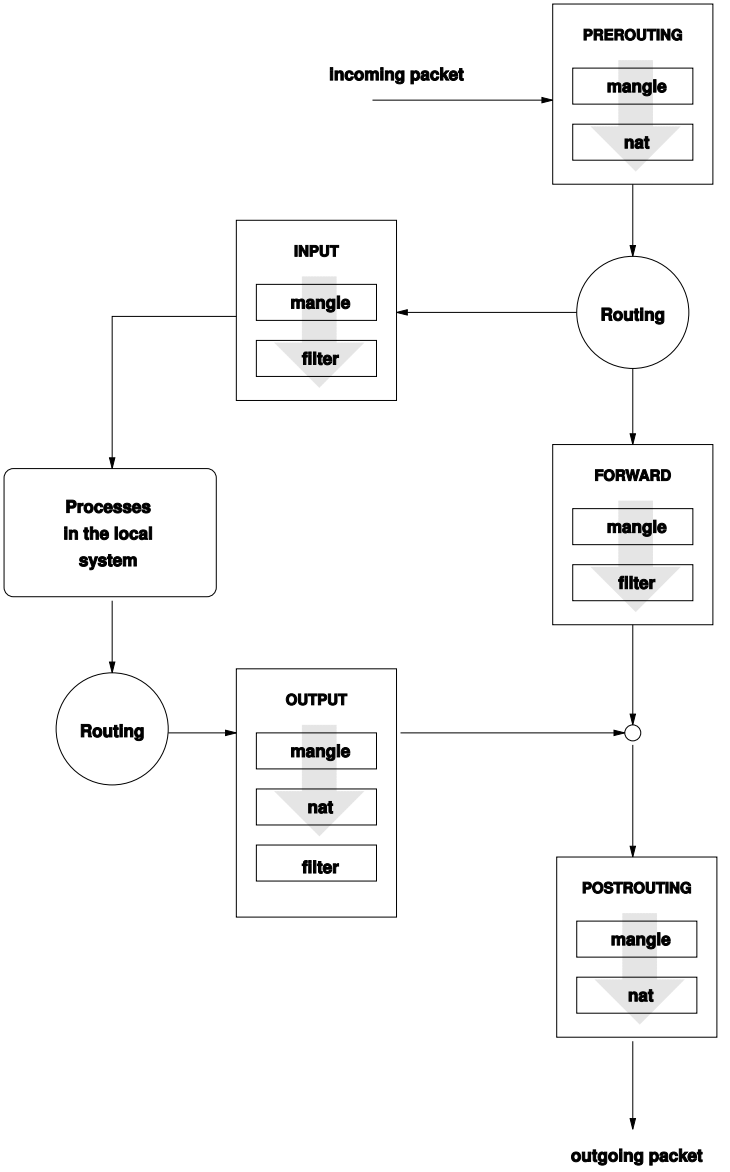
POSTROUTING
: Ez a lánc a kimenő csomagokra vonatkozik.

Az 33.1. ábra - iptables: A csomag lehetséges útjai (533. oldal) ábra bemutatja az utakat, amelyeken keresztül a hálózati csomag mozog egy adott rendszeren. Az egyszerűség kedvéért az ábra a táblázatokat a láncok részeként jeleníti meg, de valójában a láncok kerülnek a táblázatokon belül tárolásra.

Legegyszerűbb esetben a rendszerhez címzett bejövő csomag az `eth0` csatolón keresztül érkezik. A csomag először a `mangle` táblázat `PREROUTING` láncához, majd a `nat` táblázat `PREROUTING` láncához kerül. A csomag irányítására vonatkozó következő lépésben kiderül, hogy a csomag valódi célja a rendszer egy folyamata. A `mangle` és

`filter` táblázat `INPUT` láncainak átadás után a csomag végül eléri a célját, feltéve, hogy a `filter` táblázat szabályainak is megfelel.

33.1. ábra *iptables: A csomag lehetséges útjai*



33.2 Álcázás – alapok

Az álcázás a NAT (hálózati címfordítás) Linux-specifikus formája. Egy kis LAN (amelyben a gépek privát tartományból származó IP-címeket használnak – lásd: 20.1.2. - Hálózati maszkok és útválasztás (283. oldal)) internethez csatlakoztatásához használható (ahol viszont a hivatalos IP-címek használatosak. Ahhoz, hogy a helyi hálózat gépei csatlakozni tudjanak az internetre, a privát címeket hivatalosra kell átfordítani. Ezt az útválasztó végzi, amely a LAN és az internet közötti átjáróként működik. Az alapelv egyszerű: az útválasztó egynél több hálózati csatolóval rendelkezik, jellemzően egy hálózati kártyával és egy másik, internet-csatlakozást biztosító felülettel. Az utóbbi köti össze az útválasztót a külső világgal, a másik (vagy esetleg a többi) csatoló pedig a helyi hálózat gépeivel. A helyi hálózat gépei az útválasztó hálózati kártyájához (például `eth0`) csatlakoznak, és a nem helyi hálózaton belüli, hanem azon kívülre címzett csomagjaikat az alapértelmezett átjáróhoz (az útválasztóhoz) küldik.

FONTOS: Megfelelő hálózati maszk használata

A hálózat beállításakor győződjön meg róla, hogy a nyilvános (broadcast) cím és a hálózati maszk minden helyi gép esetén megegyezik. Ha nem, abból probléma származik, mivel a csomagok nem továbbíthatók megfelelően.

Mint már említettük, ha a LAN egyik gépe csomagot küld egy internetes címre, akkor az az alapértelmezett útválasztóhoz kerül. Az útválasztót azonban be kell állítani ahhoz, hogy továbbítani tudja az ilyen csomagokat. Biztonsági okokból az alapértelmezett telepítésben ez nem engedélyezett. Az engedélyezéshez állítsa az `/etc/sysconfig/sysctl` fájlban lévő `IP_FORWARD` változót `IP_FORWARD=yes` értékre.

A kapcsolat célgépe látja ugyan az útválasztót, de semmit nem tud meg a belső hálózat azon gépéről, amelyről a csomagok erednek. Ezért hívják ezt a technikát álcázásnak (masquerading). A címfordítás miatt minden válaszcsomag az útválasztóhoz érkezik. Az útválasztónak azonosítania kell a bejövő csomagokat és le kell fordítania a célcímeket, hogy a csomagok a helyi hálózat megfelelő gépéhez kerüljenek.

Mivel a bejövő forgalom irányítása az álcázási (címfordítási) táblázattól függ, kívülről nem lehet kapcsolatot kezdeményezni egy belső gép felé. Az ilyen kapcsolathoz ugyanis nincs bejegyzés a táblázatban (nincs hová továbbítani). A már létesített kapcsolatokhoz pedig egy állapotbejegyzés tartozik a táblázatban, és ezt a bejegyzést másik kapcsolat nem használhatja.

Ez viszont problémákat jelenthet számos alkalmazásprotokoll – például az ICQ, a cucme, az IRC (DCC, CTCP) és az FTP (PORT módban) – alkalmazása esetén. A webböngésző, a szabványos FTP program és számos más program az úgynevezett passzív (PASV) módot használja. A passzív mód használata sokkal kevesebb gondot jelent csomagszűrés és álcázás esetén.

33.3 Tűzfalak – alapok

A *tűzfal* valószínűleg a legszélesebb körben használt kifejezés azon mechanizmus leírására, amely egyszerre biztosítja és kezeli a hálózatok közötti kapcsolatot és szabályozza a közöttük haladó adatok folyamát. Precízen fogalmazva az itt leírt mechanizmus neve nem tűzfal, hanem *csomagszűrő*. A csomagszűrő meghatározott feltételeknek megfelelően szabályozza az adatfolyamot: engedélyez vagy tilt protokollok, portok és IP-címek alapján. Használatával blokkolhatók az olyan csomagok, amelyeknek – címük alapján – nem szabad elérniük a hálózatot. A webkiszolgáló nyilvános elérésének biztosításához például kifejezetten meg kell nyitni a megfelelő portot. A csomagszűrő azonban a cím- és portszűrési feltételeknek megfelelő (például a webkiszolgálónak küldött) csomagok tartalmát nem nézi meg. A csomagszűrő tehát akkor is átengedi a webkiszolgálóhoz érkező csomagokat, ha azok célja egyébként az, hogy feltörjék vagy megrongálják a webkiszolgálón futó CGI programot.

Egy lényegesen hatékonyabb, de sokkal bonyolultabb mechanizmus többfajta rendszer kombinációja, például az alkalmazásátjáróval vagy proxyval együttműködő csomagszűrés. Ebben az esetben a csomagszűrő visszautasítja a letiltott portokhoz címzett csomagokat. Csak az alkalmazásátjárónak küldött csomagok lesznek elfogadva. Ez az átjáró vagy proxy úgy tesz, mintha ő lenne a kiszolgáló valódi kliense. Ebben az esetben az ilyen proxy egy álcázó gépnek tekinthető az alkalmazás által használt protokollszinten. Egy példa ilyen proxyra a Squid, amely egy HTTP proxykiszolgáló. A Squid használatához a böngészőt be kell állítani a proxyn keresztüli kommunikációra. A kért HTTP-oldalak a proxy gyorsítótárából kerülnek kiszolgálásra, a gyorsítótárból hiányzó oldalakat pedig a proxy kéri le az internetről. Másik példa: a SUSE proxycsomagja (`proxy-suite`) az FTP-protokollhoz is biztosít proxyt.

Az alábbiakban az openSUSE rendszerhez mellékelt csomagszűrőre koncentrálunk. A csomagszűréssel és tűzfalkezeléssel kapcsolatos további információért olvassa el a `howto` csomagban lévő Tűzfal HOWTO-t. Ha a csomag telepítve van, akkor a HOWTO-t a következővel olvashatja el:

```
less /usr/share/doc/howto/en/txt/Firewall-HOWTO.gz
```

33.4 SuSEfirewall2

A SuSEfirewall2 egy parancsfájl, amely beolvassa az `/etc/sysconfig/SuSEfirewall2` fájlban beállított változókat az iptables szabályok előállításához. Három biztonsági zónát ad meg, de a következő példában csak az elsőt és másodikat vesszük figyelembe:

Külső zóna
: Mivel nem szabályozható, hogy mi történik a külső hálózaton, a gépet védeni kell tőle. A legtöbb esetben a külső hálózat az internet, de a gyakorlatban lehet egy másik nem biztonságos hálózat is, mint például a WLAN.

Belső zóna
: Ez a saját hálózatra utal, ami legtöbb esetben a helyi hálózat (LAN). Ha a hálózaton lévő gépek privát tartományba eső IP-címeket használnak (lásd: 20.1.2. - Hálózati maszkok és útválasztás (283. oldal)), akkor engedélyezze a hálózati címfordítást (NAT), hogy a belső hálózaton lévő gépek el tudják érni a külső hálózatot.

Demilitarizált zóna (DMZ)
: Az ebben a zónában lévő gépek a külső és belső hálózatról is elérhetők, de a belső hálózathoz nem tudnak hozzáférni. Ez a beállítás egy további védelmi vonalat húz a belső hálózat elé, mivel a DMZ-ben működő rendszerek el vannak szigetelve a belső hálózattól.

A szűrési szabályok által kifejezetten nem engedélyezett hálózati forgalmat az iptables blokkolja. A bejövő forgalommal rendelkező csatolókat tehát a három zóna egyikébe kell helyezni. Minden zónához meg kell adni az engedélyezett szolgáltatásokat és protokollokat. A szabályhalmaz csak a távoli gépektől eredő csomagokra érvényes. A helyileg létrehozott csomagokat a tűzfal nem fogja el.

A beállítás a YaST segítségével is végrehajtható (lásd: 33.4.1. - Tűzfal beállítása a YaST segítségével (537. oldal)). Ez kézzel is elvégezhető az `/etc/sysconfig/SuSEfirewall2` fájl módosításával. Az `/usr/share/doc/packages/SuSEfirewall2/EXAMPLES` fájlban számos példa tekinthető meg.

33.4.1 Tűzfal beállítása a YaST segítségével

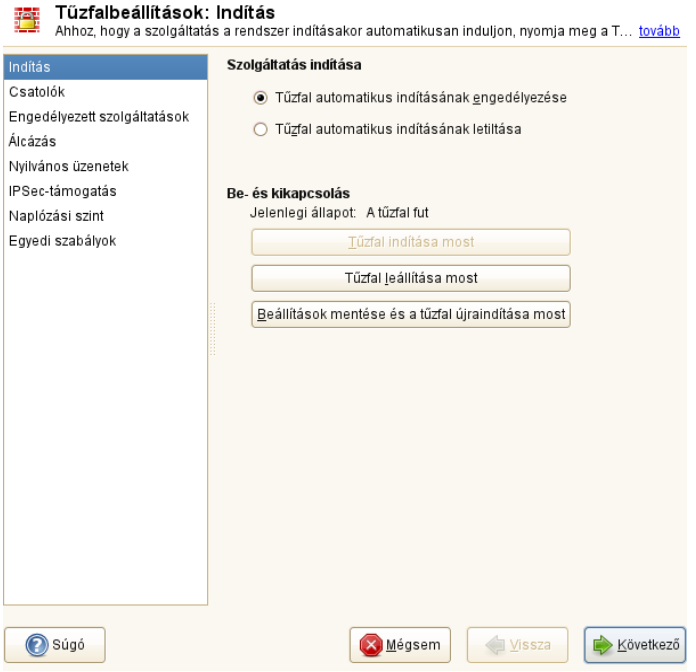
FONTOS: Automatikus tűzfalbeállítás

Telepítés után a YaST automatikusan elindít egy tűzfalat az összes beállított csatolón. Ha egy kiszolgálóprogram beállításra és aktiválásra kerül a rendszeren, akkor a YaST a kiszolgálókonfigurációs modulok *Portok megnyitása a tűzfal kiválasztott csatolóján* vagy *Tűzfal portjának megnyitása* részeiben megadott beállításokkal módosítja az automatikusan létrehozott tűzfalkonfigurációt. Néhány kiszolgálómodul-párbeszédablak rendelkezik egy *Tűzfalbeállítások* gombbal a további szolgáltatások és portok aktiválásához. A YaST tűzfalbeállítási moduljával aktiválható, letiltható vagy függetlenül újrakonfigurálható a tűzfal.

A grafikus konfiguráció YaST párbeszédablaka a YaST vezérlőközpontból érhető el. Válassza ki a *Biztonság és felhasználók* > *Tűzfal* menüpontot. A beállítások hét részre vannak osztva, amelyek közvetlenül a képernyő bal oldali fastruktúrájában érhetők el.

Indítás
: Ebben párbeszédablakban állítható be az indítási viselkedés. Az alapértelmezett telepítés végén a SuSEfirewall2 már fut a frissen telepített rendszeren. Itt indítható el és állítható le a tűzfal. Ha meg kívánja valósítani az új beállításokat a futó tűzfalon, akkor használja a *Beállítások mentése és a tűzfal újraindítása most* lehetőséget.

33.2. ábra *A YaST tűzfal beállítása*



Csatolók

Itt látható az összes ismert hálózati csatoló. Egy csatoló egy zónából eltávolításához válassza ki a csatolót, nyomja meg a *Módosítás* gombot, majd válassza ki a *____nincs_zóna____* menüpontot. Egy csatoló zónához adásához válassza ki a csatolót, nyomja meg a *Módosítás* gombot, majd válassza ki a kívánt zónát a listából. Az *Egyéni* menüpont segítségével egy saját beállításokkal rendelkező speciális csatoló is létrehozható.

Engedélyezett szolgáltatások

Itt lehet szolgáltatásokat biztosítani a rendszerről olyan zónákhoz, amelytől az védve van. A rendszer alapértelmezés szerint csak a külső zónáktól védett. Kifejezetten engedélyezni kell a szolgáltatásokat, amelyeket a külső gépeknek látniuk kell. Aktiválja a megfelelő szolgáltatást, miután az *Engedélyezett szolgáltatások a kiválasztott zónához* menüpontban kiválasztotta a kívánt zónát.

Álcázás
: Az álcázás segítségével a belső hálózat elrejthető a külső hálózatok (például az internet) elől. Lehetővé teszi ugyanakkor, hogy a belső hálózat átlátszó módon elérje a külső hálózatot. A külső hálózatról a belső hálózat felé érkező kérések blokkolásra kerülnek, a belső hálózat kérései kívülről nézve pedig úgy tűnnek, mintha az álcázó kiszolgálóról érkeznének. Ha egy belső gép speciális szolgáltatásait elérhetővé kell tenni a külső hálózat számára, akkor a megfelelő szolgáltatáshoz speciális átirányítási szabályok adhatók meg.

Nyilvános üzenetek
: Ebben a párbeszédablakban a nyilvános üzeneteket engedélyező UDP-portok kerülnek beállításra. A szükséges portszámokat vagy szolgáltatásokat hozzá kell adni a megfelelő zónához, szóközzel elválasztva. Lásd még: `/etc/services`.

  A letiltott nyilvános üzenetek naplózása is itt engedélyezhető. Ez azonban problémát jelenthet, mivel a Windows gépek nyilvános üzeneteket használnak ahhoz, hogy tudjanak egymásról, ami nagyon sok elutasított csomagot eredményez.

IPSec-támogatás
: Ebben a párbeszédablakban állítható be, hogy az IPsec-szolgáltatás engedélyezve legyen-e a külső hálózatból. A *Részletek* pontban állítható be, hogy mely csomagok megbízhatók.

Naplózási szint
: Kétféle típusú esemény naplózható: az engedélyezett és az elutasított csomagok. Az elutasított csomagok eldobásra (DROPPED) vagy visszautasításra (REJECTED) kerülnek. A *Minden naplózása*, *Csak a kritikus események naplózása* és a *Naplózás kikapcsolása* lehetőségek közül választhat.

Egyadi szabályok
: Itt állíthatók be azok a speciális tűzfalszabályok, amelyek engedélyezik a kapcsolatokat meghatározott speciális feltételek, például a forráshálózat, a használt protokoll, a célport, vagy a forrásport alapján. Ilyen szabályok megadhatók a külső, a belső és a demilitarizált zónára vonatkozóan.

A tűzfal beállításának befejezésekor a *Tovább* gombbal lépjen ki a párbeszédablakból. Ezután a tűzfalbeállítások zónaorientált összefoglalása jelenik meg. Ebben ellenőrizheti a beállításokat. Az összefoglalásban minden engedélyezett szolgáltatás, port és protokoll, valamint minden egyéni szabály megjelenik. A konfiguráció módosításához kattintson a *Vissza* gombra. A konfiguráció mentéséhez kattintson az *Elfogadás* gombra.

33.4.2 Kézi beállítás

Az alábbi bekezdésekben megpróbálunk részletes útmutatást adni a tűzfal sikeres beállításához. Minden konfigurációs elem meg van jelölve, hogy a tűzfalhoz vagy az álcázáshoz fontos-e. Ha lehetséges, adjon meg porttartományt (például `500:510`). A DMZ-vel (demilitarizált zóna) kapcsolatos szempontokról, amint azt a konfigurációs fájlnál említettük, itt nem lesz szó. Ezek jellemzően nagyobb szervezetek (vállalati hálózatok) összetettebb hálózati csatolóira alkalmazhatók és alkalmazandók, amelyek részletes beállításokat és a témával kapcsolatos alapos tudást igényelnek.

Először a YaST Rendszerszolgáltatások (futási szint) modulja segítségével engedélyezze a SuSEfirewall2-t az adott futási szinten (ez általában 3 vagy 5). Ekkor beállításra kerülnek az `/etc/init.d/rc?.d/` könyvtárakban a SuSEfirewall2_* parancsfájlok megfelelő szimbolikus láncai.

`FW_DEV_EXT` (tűzfal, álcázás)
: Az internetre csatlakoztatott eszköz. Modemes csatlakozás esetén a `ppp0`, ISDN kapcsolat esetén az `ippp0`, DSL kapcsolatok esetén a `dsl0` értéket adja meg. Az alapértelmezett útvonalnak megfelelő csatoló használatához `auto` értéket adjon meg.

`FW_DEV_INT` (tűzfal, álcázás)
: A belső, privát hálózatra csatlakoztatott eszköz (például az `eth0`). Hagyja üresen, ha nincs belső hálózat és a tűzfal csak azokat a gépeket védi, amelyen fut.

`FW_ROUTE` (tűzfal, álcázás)
: Ha szükség van az álcázási funkcióra, akkor állítsa `yes` értékre. A belső gépek nem láthatók kívülről, mivel magán hálózati címüket (például `192.168.x.x`) az internetes útválasztók figyelmen kívül hagyják.

  Álcázás nélküli tűzfal esetén akkor állítsa `yes` értékre, ha engedélyezni kívánja a hozzáférést a belső hálózathoz. A belső gépeknek ebben az esetben hivatalosan bejegyzett IP-címeket kell használniuk. Normális esetben *nem* szabad engedélyezni a belső hálózat kívülről történő korlátlan elérését.

`FW_MASQUERADE` (álcázás)
: Ha szükség van az álcázási funkcióra, akkor állítsa `yes` értékre. A belső gépek számára virtuálisan közvetlen kapcsolatot biztosít az internethez. Biztonságosabb,

ha a belső hálózat gépei és az internet között van proxykiszolgáló. A proxykiszolgáló által biztosított szolgáltatásokhoz nincs szükség álcázásra.

`FW_MASQ_NETS` (álcázás)
: Adja meg az álcázandó gépeket vagy hálózatokat, az egyedi bejegyzések között szóközt hagyva. Például:

```
FW_MASQ_NETS="192.168.0.0/24 192.168.10.1"
```

`FW_PROTECT_FROM_INT` (tűzfal)
: A tűzfalgép a belső hálózatból érkező támadások elleni védelme érdekében állítsa ezt `yes` értékre. A szolgáltatások csak akkor állnak a belső hálózat rendelkezésére, ha kifejezetten engedélyezve vannak. Lásd még: `FW_SERVICES_INT_TCP` és `FW_SERVICES_INT_UDP`.

`FW_SERVICES_EXT_TCP` (tűzfal)
: Adja meg az elérhetővé tenni kívánt TCP-portokat. Szokásos otthoni munkaállomás esetén, amelyik nem nyújt szolgáltatásokat, hagyja üresen.

`FW_SERVICES_EXT_UDP` (tűzfal)
: Hagyja üresen, hacsak nem futtat UDP-szolgáltatást és nem kívánja kívülről elérhetővé tenni. UDP-t használó szolgáltatások: DNS-kiszolgálók, IPSec, TFTP, DHCP és egyebek. Ebben az esetben adja meg a használandó UDP-portokat.

`FW_SERVICES_ACCEPT_EXT` (tűzfal)
: Az internet felől engedélyezett szolgáltatásokat sorolja fel. Ez egy általánosabb formája a `FW_SERVICES_EXT_TCP` és `FW_SERVICES_EXT_UDP` beállításoknak, de specifikusabb, mint a `FW_TRUSTED_NETS`. A jelölés a *`hálózat`*`,`*`protokoll`*`[,`*`célport`*`][,`*`forrásport`*`]` szóközzel elválasztott listája, tehát például `0/0,tcp,22`.

`FW_SERVICES_INT_TCP` (tűzfal)
: Ezzel a változóval lehet megadni a belső hálózat számára rendelkezésre álló szolgáltatásokat. A jelölés ugyanaz mint `FW_SERVICES_EXT_TCP` esetén, de a beállítások a *belső* hálózatra érvényesek. A változót csak akkor kell beállítani, ha a `FW_PROTECT_FROM_INT` értéke `yes`.

`FW_SERVICES_INT_UDP` (tűzfel)
: Lásd: `FW_SERVICES_INT_TCP`.

FW_SERVICES_ACCEPT_INT (firewall)
: A belső gépek felől engedélyezett szolgáltatásokat sorolja fel. Lásd: FW_SERVICES_ACCEPT_EXT.

FW_SERVICES_ACCEPT_RELATED_* (tűzfal)
: A SuSEfirewall2 egy kicsit másképp működik az olyan csomagokat illetően, amelyeket a netfilter RELATED-nek (kapcsolódónak) tekint.

  Például annak érdekében, hogy finomabban lehessen szűrni a Samba broadcast-csomagjait, a RELATED csomagokat már nem fogadja el a tűzfal feltétel nélkül. Az FW_SERVICES_ACCEPT_RELATED_-del kezdődő nevű új változók pontosan azért lettek bevezetve, hogy lehessen korlátozni a RELATED csomagokat meghatározott hálózatokra, protokollokra és portokra.

  Ez azt jelenti, hogy a kapcsolatkövető (conntrack) modulok hozzáadása az FW_LOAD_MODULES-hoz nem eredményezi a modulok által megjelölt csomagok automatikus elfogadását. Ezenfelül az FW_SERVICES_ACCEPT_RELATED_-del kezdődő nevű változókat is be kell állítani egy megfelelő értékre.

A tűzfal beállítása után tesztelje az eredményt. A tűzfalszabályhalmazok akkor jönnek létre, amikor a root felhasználó kiadja a SuSEfirewall2 start parancsot. Ezután próbálja ki például a telnet parancsot egy külső gépről, hogy a kapcsolat valóban le van-e tiltva. Majd tekintse meg a /var/log/messages könyvtárat, amelyben az alábbihoz hasonlót kell látnia:

```
Mar 15 13:21:38 linux kernel: SFW2-INext-DROP-DEFLT IN=eth0
OUT= MAC=00:80:c8:94:c3:e7:00:a0:c9:4d:27:56:08:00 SRC=192.168.10.0
DST=192.168.10.1 LEN=60 TOS=0x10 PREC=0x00 TTL=64 ID=15330 DF PROTO=TCP
SPT=48091 DPT=23 WINDOW=5840 RES=0x00 SYN URGP=0
OPT (020405B40402080A061AFEBC0000000001030300)
```

A tűzfal tesztelésére szolgáló csomag az nmap és a nessus. A megfelelő csomag telepítése után az nmap dokumentációja az /usr/share/doc/packages/nmap, a nessus dokumentációja pedig az /usr/share/doc/packages/nessus-core könyvtárban található.

33.5 További információk

A `SuSEfirewall2` csomaggal kapcsolatos legfrissebb információ és más dokumentáció az `/usr/share/doc/packages/SuSEfirewall2` könyvtárban található. A netfilter és iptables projekt honlapján (`http://www.netfilter.org`) , egy nagy dokumentumgyűjtemény található, több nyelven is.

SSH: Biztonságos hálózati műveletek

34

Ahogy egyre több számítógép működik hálózatos környezetekben, annál gyakrabban van szükség arra, hogy egy gépet távolról elérjünk. Ez általában azt jelenti, hogy a felhasználó hitelesítési célból elküld egy bejelentkezési név és jelszó karaktersorozatot. Ha ezek a karaktersorozatok nyílt szövegként kerülnek átvitelre, akkor mások lehallgathatják ezeket, és visszaélhetnek a felhasználói fiókokkal úgy, hogy a jogosult felhasználó még csak nem is tud róla. Azon kívül, hogy ezzel egy támadó a felhasználó minden fájljához hozzáférhet, az illegális fiókot a rendszergazda vagy `root` hozzáférés megszerzésére, vagy akár a más rendszerekbe behatolásra is fel lehet használni. A múltban a távoli kapcsolatokhoz a Telnet protokollt használták, ami sem titkosítással, sem egyéb biztonsági mechanizmusok útján nem adott védelmet a lehallgatás ellen. Más nem védett kommunikációs csatornák is léteznek, ilyen például a hagyományos FTP protokoll és néhány távoli másolóprogram.

Az SSH programcsomag a hitelesítési karaktersorozatok (általában egy bejelentkezési név és jelszó), valamint a gépek közötti egyéb adatcsere titkosításával biztosítja a szükséges védelmet. Az SSH használata esetén az adatfolyamot továbbra is rögzítheti egy harmadik fél, de a tartalom titkosítva van és a titkosítási kulcs ismerete nélkül nem fejthető vissza nyílt szöveggé. Így az SSH biztonságos kommunikációt tesz lehetővé nem biztonságos hálózatokon, például az interneten. Az openSUSE csomagban az OpenSSH csomag található meg.

34.1 Az OpenSSH csomag

Az openSUSE alapértelmezésben telepíti az OpenSSH csomagot. Ezután a telnet, rlogin, rsh, rcp és ftp programok alternatívájaként rendelkezésre áll az ssh, az scp és az sftp.

Az alapértelmezett konfigurációban egy openSUSE rendszer elérése csak OpenSSH segédprogramok használatával lehetséges és csak akkor, ha a tűzfal engedélyezi a hozzáférést.

34.2 Az ssh program

Az ssh programmal be lehet jelentkezi a távoli rendszerekre és azokat interaktívan lehet használni. Kiváltja mind a telnet, mind az rlogin programot. Az slogin program az ssh-ra mutató szimbolikus lánc. Az `ssh sun` parancs segítségével például jelentkezzen be a sun gépre. A gép bekéri a sun géphez tartozó jelszót.

A sikeres hitelesítés után használhatja a távoli parancssort vagy az interaktív alkalmazásokat – például a YaST-ot – is. Ha a helyi felhasználónév eltér a távoli gépen használttól, akkor az `ssh -l augustine sun` vagy `ssh augustine@sun` parancs segítségével másik névvel is bejelentkezhet.

Az ssh ezen felül lehetőséget ad arra is, hogy parancsokat futtassunk a távoli rendszeren ugyanúgy, mint az rsh esetében. Az alábbi példában adja ki az `uptime` parancsot a sun nevű gépen, és hozzon létre egy `tmp` nevű könyvtárat. A program kimenete megjelenik a helyi terminálon.

```
ssh otherplanet "uptime; mkdir tmp"
Password:
1:21pm  up  2:17,  9 users,  load average: 0.15, 0.04, 0.02
```

Az idézőjelek ahhoz szükségesek, hogy mindkét utasítást el lehessen küldeni egy paranccsal. Ennek hatására a második parancs is végrehajtásra kerül a sun gépen.

34.3 scp – Secure Copy (biztonságos másolás)

Az scp fájlokat másol két gép között. Ez az rcp biztonságos és titkosított megfelelője. Az `scp MyLetter.tex sun:` parancs például átmásolja a `MyLetter.tex` fájlt a jupiter gépről a sun gépre. Ha a felhasználói név a jupiter gépen különbözik a sun gépen használttól, akkor adja meg az utóbbit `felhasználónév@gépnév` formátumban. Az `-l` paraméter ennél a parancsnál mást jelent.

A megfelelő jelszó megadása után az scp elindítja az adatátvitelt és csillagokat ír egymás mellé egy sorba, ezzel mutatja a folyamat előrehaladását. Emellett jobb oldalon kiírja az átvitel várható idejét is. A kimenet a `-q` paraméter segítségével letiltható.

Az scp rekurzív másolási funkciót is biztosít a teljes könyvtárakhoz. Az `scp -r src/ sun:backup/` parancs az `src` könyvtár teljes tartalmát – az összes alkönyvtárat is beleértve – átmásolja a sun gépen lévő `backup` könyvtárba. Ha ez az alkönyvtár még nem létezik, akkor a rendszer automatikusan létrehozza.

A `-p` paraméter hatására az scp változatlanul hagyja a fájlok időbélyegét. A `-C` tömöríti az adatávitelt. Ez a lehető legkisebbre nyomja össze az átvinni kívánt adatkötetet, de jobban leterheli a processzort.

34.4 sftp – Secure File Transfer (biztonságos fájlátvitel)

Az sftp az scp helyett használható biztonságos fájlátvitelre. Az sftp munkamenet során számos, az ftp-ből már ismert parancs használható. Az sftp program jobb választás lehet, mint az scp, különösen ismeretlen fájlnevű adatok átvitelekor.

34.5 Az SSH démon (sshd) – kiszolgálóoldal

Az ssh és scp SSH kliensprogramok használatához futnia kell egy kiszolgálónak – az SSH démonnak – a háttérben, hogy figyelje a kapcsolatokat a `22-es TCP/IP porton`. A démon az első elindításkor három kulcspárt hoz létre. Minden kulcspár egy privát és egy nyilvános kulcsból áll. Éppen ezért hívják ezt az eljárást nyilvános kulcsúnak. Az SSH-n keresztüli kommunikáció biztonsága érdekében a saját kulcsfájlok elérhetőségét a rendszeradminisztrátorra kell korlátozni. A fájljogosultságok az alapértelmezett telepítésnek megfelelően kerülnek beállításra. A saját kulcsokat csak helyileg kéri az SSH démon, és azokat nem is szabad senki másnak odaadni. A nyilvános kulcsokat (ezek nevének kiterjesztése `.pub`) viszont meg kell kapnia a kapcsolatot kérő kliensnek. Ezek bárki számára olvashatók.

A kapcsolatot az SSH-kliens kezdeményezi. A várakozó SSH-démon és a kérő SSH-kliens kicseréli azonosítási adatait, hogy összehasonlítsák a használt protokollt és szoftververziót, illetve megakadályozzák a rossz porton történő kapcsolódást. Mivel az eredeti SSH-démon leszármazott folyamata válaszol a kérésre, egyszerre több SSH-kapcsolat is létesíthető.

Az SSH-kiszolgáló és -kliens közötti kommunikációhoz az OpenSSH az SSH protokoll 1-es és 2-es verzióját támogatja. Alapértelmezés szerint az SSH protokoll 2-es változata kerül alkalmazásra. A protokoll 1-es változatának használatához írja ezt felül a `-1` kapcsolóval. Ha frissítés után is az 1. változatot szeretné tovább használni, kövesse az `/usr/share/doc/packages/openssh/README.SuSE` fájl utasításait. Ez a dokumentum azt is leírja, hogy az SSH 1 környezet hogyan alakítható át pár lépés segítségével működő SSH 2 környezetté.

SSH 1-es verzió használata esetén a kiszolgáló elküldi a saját nyilvános kulcsát és egy kiszolgáló kulcsot, amelyet az SSH démon minden órában újból létrehoz. Ezekkel az SSH-kliens titkosítani tud egy szabadon választott munkamenet-kulcsot, amelyet átküld az SSH-kiszolgálónak. Az SSH-kliens azt is megmondja a kiszolgálónak, hogy mely titkosítási módszert (rejtjelezést) használja.

Az SSH 2-es verzió nem igényel kiszolgálókulcsot. Mindkét oldal a Diffie-Helman algoritmust használja a kulcsok cseréjéhez.

A saját kulcsra és a kiszolgálókulcsra feltétlenül szükség van a munkamenetkulcs visszafejtéséhez, azok nem származtathatók le a nyilvános részekből. Csak az érintett SSH-démon tudja visszafejteni a munkamenetkulcsot a saját kulcsai segítségével (lásd: `man /usr/share/doc/packages/openssh/RFC.nroff`). Ez a kezdeti kapcsolati fázis közelebbről is megfigyelhető az SSH-kliens `-v` hibakeresési lehetősége segítségével.

A kliens, ha már egyszer kapcsolatba lépett egy távoli géppel, a nyilvános kulcsokat a `~/.ssh/known_hosts` fájlban tárolja. Ez megakadályozza azokat a támadásokat, amikor idegen SSH-kiszolgáló megpróbálnak hamis neveket és IP-címeket használni. Az ilyen támadások felismerhetők a `~/.ssh/known_hosts` fájlban nem szereplő nyilvános kulcsról, vagy arról, hogy a kiszolgáló a megfelelő saját példány hiányában nem tudja visszafejteni a munkamenetkulcsot.

Az `/etc/ssh/` fájlban tárolt saját és nyilvános kulcsokról ajánlatos biztonsági másolatot készíteni egy megfelelően védett külső helyre. Így a kulcsmódosítások észrevehetők, és a régiek egy újratelepítés után ismét használhatók. Ez megkíméli a felhasználókat a

zavaró figyelmeztetésektől. Ha kiderül, hogy a figyelmeztetés dacára mégis egy megfelelő SSH-kiszolgálóról van szó, akkor a `~/.ssh/known_hosts` fájlból el kell távolítani a rendszerre vonatkozó meglévő bejegyzést.

34.6 SSH hitelesítési mechanizmusok

Ezután történik a tényleges hitelesítés, amely a legegyszerűbb formában egy jelszó megadásából áll. Az SSH célja egy biztonságos, egyszerűen használható szoftver bevezetése volt. Mivel az rsh-t és rlogin-t is kiváltja, az SSH-nak egy mindennapi használatra megfelelő hitelesítési eljárást is biztosítania kell. Az SSH ezt egy másik kulcspár segítségével hajtja végre, amelyet a felhasználó állít elő. Az SSH csomagban egy segédprogram szolgál erre: az ssh-keygen. Az `ssh-keygen -t rsa` vagy `ssh-keygen -t dsa` parancs beírása után létrejön a kulcspár. A rendszer ezután egy fájlnevet kér a a kulcsok tárolásához.

Erősítse meg az alapértelmezett beállítást és válaszoljon a jelszókérésre. Annak ellenére, hogy a szoftver üres jelszót kínál fel, az itt leírt eljáráshoz ajánlatos egy 10-30 karakteres szöveget megadni. Ne használjon rövid és egyszerű szavakat vagy kifejezéseket. Ismétléssel erősítse meg a jelszót. Ezt követően látni fogja, hogy az alkalmazás saját és a nyilvános kulcsokat eltárolja, alapértelmezésként az `id_rsa` és az `id_rsa.pub` fájlban.

Az `ssh-keygen -p -t rsa` vagy `ssh-keygen -p -t dsa` parancs segítségével változtassa meg a régi jelszót. Másolja át a nyilvános kulcskomponenseket (a példában `id_rsa.pub`) a távoli gépre és mentse el a `~/.ssh/authorized_keys` fájlba. A következő kapcsolatteremtéskor a jelszó segítségével hitelesítenie kell magát. Ha ez nem történik meg, akkor ellenőrizze a fájlok helyét és tartalmát.

Hosszú távon ez az eljárás nehézkesebb, mint a jelszó megadása minden alkalommal. Ezért az SSH csomag egy másik eszközt is biztosít, az ssh-agent programot, amely az X munkamenet időtartamára megtartja a saját kulcsokat. A teljes X munkamenet az ssh-agent leszármazott folyamataként kerül elindításra. Ennek legegyszerűbb módja, ha a `.xsession` fájl elején a `usessh` változót `yes` értékre állítja és bejelentkezik egy képernyőkezelőn keresztül (pl. KDM vagy XDM). Egy másik lehetőség az `ssh-agent startx` megadása.

Ezután a szokásos módon használhatja az ssh és az scp parancsot. Ha a fent leírt módon osztotta ki a nyilvános kulcsot, akkor a továbbiakban nem kell jelszót megadnia. Ne

felejtse el bezárni vagy jelszavas védelmi alkalmazással (ilyen pl. az xlock) zárolni az X munkamenetet.

Az SSH 2 protokoll miatt bevezetett minden fontos változás dokumentálva van az `/usr/share/doc/packages/openssh/README.SuSE` fájlban is.

34.7 X hitelesítési és továbbítási mechanizmusok

A korábban leírt biztonsággal kapcsolatos javításokon túl az SSH a távoli X alkalmazások használatát is leegyszerűsíti. Ha az `ssh` parancsot `-X` paraméterrel futtatja, akkor a DISPLAY változó automatikusan beállításra kerül a távoli gépen, és a meglévő SSH kapcsolaton keresztül minden X kimenet exportálásra kerül a távoli gépre. Az ezzel a módszerrel távolról elindított és helyileg megjelenített X alkalmazásokat ugyanakkor nem hallgathatják le jogosulatlan egyének.

A `-A` paraméter hozzáadásával az ssh-agent hitelesítési mechanizmus átkerül a következő gépre. Ezen a módon különböző gépekről dolgozhat jelszó megadása nélkül, de csak akkor, ha a nyilvános kulcsot eljuttatta a célgépekre is, és ott megfelelően elmentette.

Az alapértelmezett beállítások mindkét mechanizmust letiltják, de az `/etc/ssh/sshd_config` rendszerszintű konfigurációs fájl vagy a felhasználó `~/.ssh/config` fájlja segítségével ezek ideiglenesen aktiválhatók.

Az ssh segítségével a TCP/IP-kapcsolatok is átirányíthatók. Az alábbi példákban az SSH átirányítja az SMTP és POP3 portot:

```
ssh -L 25:sun:25 jupiter
```

E parancs segítségével a jupiter 25-ös portjára (SMTP) érkező kapcsolatok egy titkosított csatornán keresztül átirányításra kerülnek a sun SMTP portjára. Ez különösen azok számára hasznos, akik SMTP-AUTH vagy POP-before-SMTP funkció nélkül használnak SMTP-kiszolgálókat. Az e-mail üzenetek a hálózatra csatlakozó tetszés szerinti helyről továbbíthatók kézbesítésre a „saját” levelezőkiszolgálóra. Ehhez hasonlóan a jupiter POP3 kérései (110-es port) is továbbíthatók a sun POP3 portjára a következő parancs segítségével:

```
ssh -L 110:sun:110 jupiter
```

Mindkét parancsot `root` felhasználóként kell végrehajtani, mivel a kapcsolat kiváltságos helyi portokkal került kialakításra. Az e-maileket a normál felhasználók egy meglévő SSH-kapcsolaton keresztül küldik el és kapják meg. Ebben az esetben az SMTP és POP3 ügyfélprogramokban `localhost`-ot kell megadni kiszolgálóként. További információt a fent leírt programok kézikönyvoldalai, valamint az `/usr/share/doc/packages/openssh` könyvtárban található fájlok adnak.

35 X.509 tanúsítványok kezelése

Egyre több hitelesítési eljárás alapul titkosítási eljárásokon. Ezért fontos szerepet játszanak azok a digitális tanúsítványok, amelyek a titkosítási kulcsokat a tulajdonosaikhoz rendelik. Ilyen tanúsítványok nem csak a kommunikációban használatosak, de megtalálhatók például a vállalati beléptetőkártyákon is. A tanúsítványok készítését és felügyeletét általában hivatalos cégek látják el, amelyek ezt kereskedelmi szolgáltatás keretében végzik. Különböző esetekben azonban felmerülhet az igény, hogy saját maga vegye át ezt a feladatot, például, ha a cég nem akarja kívülállóknak kiadni a személyes adatokat.

A YaST két modult kínál erre a célra, amelyek alapszintű felügyeleti funkciókat biztosítanak a digitális X.509 tanúsítványokhoz. A következő részekben betekintést nyújtunk a digitális tanúsítványok alapjaiba, és elmagyarázzuk, hogyan tudja a YaST segítségével elkészíteni és felügyelni ilyen típusú tanúsítványait. További, részletes információ: `http://www.ietf.org/html.charters/pkix-charter.html`

35.1 A digitális tanúsítványok alapelvei

A digitális tanúsítványok titkosítási folyamatokat használnak azon adatok titkosításához, amelyeket védeni kell az illetéktelen hozzáféréstől. A felhasználó adatai egy másodlagos adatbejegyzéssel, vagy más néven *kulccsal* vannak titkosítva. A kulcs matematikai úton előállított adattal titkosítja a felhasználó adatait, így az eredeti tartalom nem ismerhető fel. Napjainkban általában az aszimmetrikus titkosítást alkalmazzák (*nyilvános kulcs alapú titkosítás*). A kulcsok mindig párban állnak:

Saját kulcs
: A saját kulcsot tulajdonosának biztonságos helyen kell tárolnia. Véletlen nyilvánosságra kerülése veszélyezteti a kulcspárt, és ezzel használhatatlanná teszi azt.

Nyilvános kulcs
: A nyilvános kulcsot a tulajdonosa nyilvánosságra hozza harmadik felek általi felhasználásra.

35.1.1 Kulcshitelesség

Mivel a nyilvános kulcs eljárás széles körben elterjedt, számos nyilvános kulcs elérhető. A rendszer sikeres használatához elengedhetetlen, hogy a nyilvános kulcs biztosan a kijelölt felhasználóé legyen. A felhasználók és a nyilvános kulcsok egymáshoz rendelését hitelesítő szervezetek igazolják a nyilvánoskulcs-tanúsítás által. A tanúsítványok tartalmazzák a tulajdonos nevét, a megfelelő nyilvános kulcsot és a kibocsátó elektronikus aláírását.

A hitelesítő szervezetek általában egy tanúsító infrastruktúrához tartoznak, amely a tanúsítványok kibocsátása, aláírása mellett egyéb tanúsítványfelügyeleti feladatokat is ellátnak, mint a tanúsítványok közzététele, visszavonás és megújítása. Az ilyen infrastruktúrát általában *nyilvános kulcsú infrastruktúrának* vagy *PKI*-nak nevezik. Közismert PKI-szabvány az *OpenPGP*, amelyben a felhasználók teszik közzé saját tanúsítványukat központi hitelesítés nélkül. Ezek a tanúsítványok akkor válnak hitelessé, ha a „bizalmi hálózathoz" (web of trust) tartozó külső hitelesítő aláírja őket.

A hierarchikusan szervezett *X.509 nyilvános kulcsú infrastruktúra* (PKIX) egy másik lehetséges modell, amelyet az *IETF* (internet Engineering Task Force) szervezet határozott meg. Ez a mintája majdnem minden nyilvánosan használt PKI-nek. Ebben a modellben a hitelesítés hierarchikus fastruktúrában történik a *tanúsítványhatóság* (CA) által. A fa gyökerét a gyökér CA jelenti, amely hitelesíti az összes alsóbb rendű CA-t. A legalsó szintű CA állítja ki a felhasználói tanúsítványokat. A felhasználói tanúsítvány akkor válik megbízhatóvá, ha végigkövethető a gyökér CA-ig.

Az ilyen PKI-megoldások biztonsága a tanúsítányok hitelességén áll vagy bukik. Annak érdekében, hogy a tanúsítványkibocsátás zavartalan legyen, a PKI-üzemeltető meghatároz egy *tanúsítványalkalmazási nyilatkozatot* (certificate practice statement - CPS), amelyben meghatározza a tanúsítványkezelés folyamatát. Ezzel biztosítható, hogy a PKI kizárólag megbízható tanúsítványokat állítson elő.

35.1.2 X.509 tanúsítványok

Egy X.509 tanúsítvány számos állandó mezővel és opcionális kiegészítésekkel rendelkező adatstruktúra. A fix mezők tartalmazzák a tulajdonos nevét, a nyilvános kulcsot és a kibocsátó CA adatait (nevét és aláírását). Biztonsági okokból a tanúsítványok csak meghatározott ideig érvényesek, tehát egy dátummező is található bennük. A CA a tanúsítvány érvényességét a megadott időszakra garantálja. A CPS általában kiköti, hogy a PKI (a kibocsátó CA) a lejárati határidő előtt készítsen és küldjön szét új tanúsítványt.

A kiegészítések bármiféle járulékos információt tartalmazhatnak. Az alkalmazásnak nem kell figyelembe vennie a kiegészítéseket, hacsak nincs *kritikusként* megjelölve. Ha egy alkalmazás egy kritikus kiegészítést nem ismer fel, el kell utasítania a tanúsítványt. Egyes kiegészítések a tanúsítvány használatát néhány alkalmazásra, például aláírásra vagy titkosításra korlátozhatják.

A Táblázat 35.1 bemutatja az X.509 tanúsítvány 3-as változatának mezőit.

35.1. táblázat *X.509v3 tanúsítvány*

Mező	Tartalom
Változat	A tanúsítvány verziója - például v3
Sorozatszám	Egyedi tanúsítványazonosító (egész szám)
Aláírás	A tanúsítvány aláírásához használt algoritmus azonosítója
Kiállító	A kiállító hatóság (CA) egyedi neve (DN)
Érvényesség	Az érvényesség időtartama
Tulajdonos	A tulajdonos egyedi neve (DN)
Tulajdonos nyilvános kulcsadatai	A tulajdonos nyilvános kulcsa és az algoritmus azonosítója
A kiállító egyedi azonosítója (Unique ID)	A kiállító CA egyedi azonosítója (elhagyható)

Mező	Tartalom
A tulajdonos egyedi azonosítója	A tulajdonos egyedi azonosítója (Unique ID) - opcionális
Kiegészítések	Egyéb opcionális információ, például „KeyUsage” (kulcshasználat) vagy „BasicConstraints” (Kikötések) stb.

35.1.3 X.509 tanúsítványok letiltása

Ha egy tanúsítvány az érvényességi időn belül megbízhatatlanná válik, azonnal le kell tiltani. Ez szükséges lehet például olyan esetben, amikor a saját kulcs nyilvánosságra került. A letiltás különösen akkor fontos, ha a saját kulcs a CA-hoz tartozik, és nem egy felhasználói tanúsítványhoz. Ebben az esetben az összes felhasználói tanúsítványt, amelyet a CA kiállított, azonnal le kell tiltani. Amennyiben egy tanúsítvány le lett tiltva, a PKI-nak (illetve a felelős CA-nak) azonnal értesítenie kell a használókat. Az ehhez használt eszköz a *tanúsítvány-visszavonási lista* (certificate revocation list - CRL).

Ezt a listát a CA készíti a CRL elosztási helyek (a CDP-k) számára megadott időnként. A CDP opcionális attribútumként felvehető egy tanúsítványba, így a használó ellenőrizheti a tanúsítvány hitelességét, valamint, hogy nem lett-e visszavonva. Egy lehetséges megoldás az ellenőrzésre az*online tanúsítványstátusz protokoll* (online certificate status protocol - OCSP). A CRL listák hitelességét a kibocsátó CA aláírása szavatolja. Az Táblázat 35.2 táblázat bemutatja az X.509 CRL legfontosabb részeit.

35.2. táblázat *X.509 visszavonási lista (CRL)*

Mező	Tartalom
Változat	A CRL verziója (pl. v2)
Aláírás	A CLR aláírásához használt algoritmus azonosítója (ID)
Kiállító	A CRL lista kibocsátójának (általában a CA-nak) egyedi neve (DN)

Mező	Tartalom
Frissítés ideje	A CRL közzétételének ideje (dátum és idő)
Következő frissítés	A következő CRL-frissítés ideje (dátum és idő)
A visszavont tanúsítványok listája	Minden bejegyzés tartalmazza a tanúsítvány sorozatszámát, a visszavonás idejét és az opcionális kiegészítéseket.
Kiegészítések	Egyéb CRL kiegészítések

35.1.4 A tanúsítványok és CRL-ek tárolása

A CA tanúsítványainak és CRL-listáinak nyilvánosan elérhetőknek kell lenniük egy *lerakatban*. Mivel a tanúsítványok és a CRL-ek nem hamisíthatók, az aláírásoknak köszönhetően a lerakatot nem szükséges különösen védeni. Ellenkezőleg, a lehető legegyszerűbb és leggyorsabb elérés biztosítása a cél. Ezért a tanúsítványok általában LDAP vagy HTTP kiszolgálókon keresztül érhetők el. Bővebb információ az LDAP-ról: 26. fejezet - *LDAP – címtárszolgáltatás* (397. oldal) a 28. fejezet - *Az Apache HTTP kiszolgáló* (451. oldal) fejezet a HTTP kiszolgálóról tartalmaz információkat.

35.1.5 Saját PKI

A YaST tartalmazza az alapvető eszközöket az X.509 tanúsítványok kezeléséhez. Ez főként a CA-k, alárendelt CA-k és tanúsítványaik létrehozását foglalja magába. Itt kell megjegyezni, hogy a PKI szolgálatásai messze túlmutatnak a tanúsítványok és CRL-ek előállításán és terjesztésén. Egy PKI üzemeltetéséhez komoly, átgondolt adminisztrációs infrastruktúra szükséges, amely lehetővé teszi a tanúsítványok és CRL-ek folyamatos frissítését. Ezt az infrastruktúrát a kereskedelmi PKI termékek biztosítják és részben automatizálják. A YaST biztosít eszközöket a CA-k és tanúsítványok létrehozásához és szétosztásához, de jelenleg nem képes ezeket a háttérinformációkat biztosítani. Kisméretű PKI felállításához használhatja a YaST modulokat. Azonban egy „hivatalos” vagy kereskedelmi PKI üzembe helyezéséhez fizetős termékek szükségesek.

35.2 YaST CA-felügyeleti modulok

A YaST két modult biztosít az alapvető CA-felügyeleti funkciók ellátására. A két modul legfontosabb felügyeleti funkcióit az alábbiakban mutatjuk be.

35.2.1 Gyökér CA létrehozása

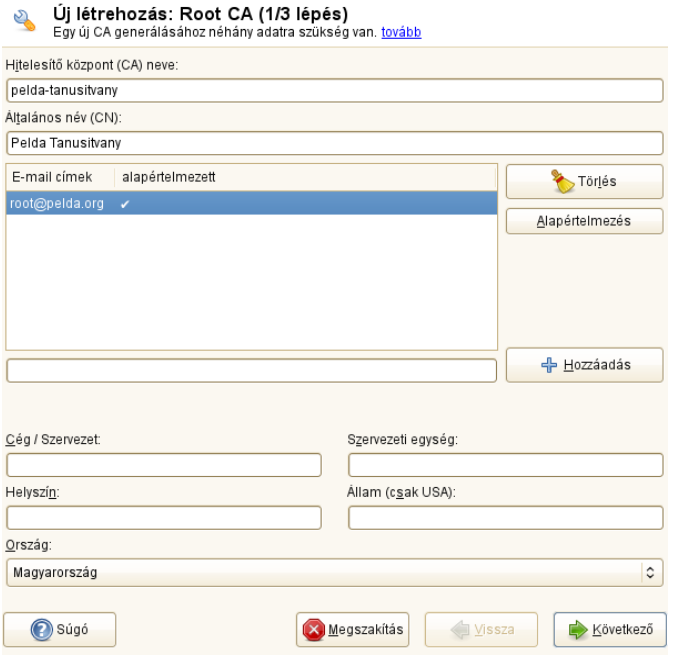
PKI készítéséhez az első lépés mindig a gyökér CA elkészítése. A következőket kell tennie:

1. Indítsa el a YaST-ot és lépjen be a *Felhasználók és biztonság* > *Hitelesítő központ (CA) kezelés* modulba.

2. Kattintson a *Gyökér CA létrehozása* gombra.

3. Az első párbeszédablakban adja meg a CA létrehozásához szükséges legfontosabb adatokat (35.1. ábra). A szövegmezők jelentése a következő:

35.1. ábra *YaST CA-modul – Alapadatok a gyökér CA készítéséhez*



Hitelesítő központ (CA) neve
: Adja meg a CA hivatalos nevét. Több más dolog mellett például a könyvtárnevek ebből a névből származnak, ezért kizárólag a súgóban meghatározott karakterek használhatók. Ez a név jelenik meg az összefoglalóban is, amikor a modul elindul.

Általános név
: Adja meg azt a nevet, amelyen hivatkozik a CA-ra.

E-mail címek
: Több elektronikus levélcím is megadható, amelyeket a CA felhasználói láthatnak. Ez hasznos lehet az érdeklődőknek.

Ország
: Adja meg az országot, ahol a CA üzemel.

Szervezet, *Szervezeti egység*, *Hely*, *Állam*
: Opcionális értékek.

4 Kattintson a *Tovább* gombra.

5 Adja meg a jelszót a második párbeszédablakban. Ez a jelszó mindig szükséges a CA használatakor – alárendelt CA és tanúsítvány készítéséhez. A szövegmezők jelentése a következő:

Kulcshossz
A *Kulcshossz* alapértelmezésként tartalmaz egy használható értéket, amelynek megváltoztatása nem feltétlenül szükséges, kivéve, ha egy alkalmazás nem tudja kezelni ezt a kulcsméretet. Minél nagyobb a szám, annál biztonságosabb a jelszó.

Érvényességi időtartam (napok)
Az *Érvényességi időtartam* CA esetén 3650 nap (körülbelül 10 év). Ez a hosszú időtartam érthető, hiszen egy CA lecserélése, törlése számos adminisztrációs ráfordítást igényel.

A *További opciók* pontot választva egy párbeszédablak jelenik meg, ahol az X.509 attribútumkiterjesztések adhatók meg (35.4. ábra - YaST CA modul – Speciális beállítások (566. oldal)). Ezek az értékek megfelelő alapbeállításokat tartalmaznak, és csak akkor változtassa meg, ha valóban tudja, mit csinál.

6 Kattintson a *Tovább* gombra. A YaST kiírja a jelenlegi beállításokat, és megerősítést vár. Kattintson a *Létrehozás* gombra. A gyökér CA elkészül, és megjelenik az áttekintő képernyőn.

TIPP

Általánosságban ajánlott tiltani felhasználói tanúsítványok kibocsátását a gyökér CA-n. Érdemes legalább egy alárendelt CA-t készíteni és azon létrehozni a felhasználói tanúsítványokat. Így a gyökér CA elkülönített, biztonságos környezetben üzemeltethető - például egy elkülönített, megbízható számítógépen. Ez nagyon megnehezíti a gyökér CA megtámadását.

35.2.2 Jelszó módosítása

Ha meg kell változtatni a CA jelszavát, kövesse az alábbi lépéseket:

1 Indítsa el a YaST-ot és nyissa meg a CA-modult.

2 Válassza ki a kívánt gyökér CA-t, majd kattintson a *Belépés a CA-ba* gombra.

3 Adja meg a jelszót, ha most először lép be a CA-ba. A YaST a *Leírás* lapon megjeleníti a CA kulcsadatait (lásd: 35.2. ábra).

4 Kattintson a *Szakértői* gombra és válassza ki a *Jelszócsere* pontot. Megjelenik egy párbeszédpanel.

5 Írja be a régi és új jelszavakat

6 A befejezéshez nyomja meg az *OK* gombot.

35.2.3 Alárendelt CA készítése és visszavonása

Az alárendelt CA ugyanúgy készül, mint a gyökér CA.

MEGJEGYZÉS

Az alárendelt CA érvényességi idejének teljes mértékben a „szülő” CA érvényességi idején belül kell lennie. Mivel az alárendelt CA mindig a „szülő” CA után készül, az alapértelmezett érték hibaüzenethez vezet. Ennek elkerülésére adjon meg helyes értéket érvényességi időnek.

A következőket kell tennie:

1 Indítsa el a YaST-ot és nyissa meg a CA-modult.

2 Válassza ki a kívánt gyökér CA-t, majd kattintson a *Belépés a CA-ba* gombra.

3 Adja meg a jelszót, ha most először lép be a CA-ba. A YaST a *Leírás* lapon megjeleníti a CA kulcsadatait (lásd: 35.2. ábra).

35.2. ábra *YaST CA modul – CA használata*

4 Kattintson a *Szakértői* gombra és válassza ki a *Hitelesítő alközpont (subCA) létrehozása* pontra. Ugyanaz a párbeszédablak jelenik meg, mint a gyökér CA létrehozásakor.

5 Folytassa tovább az itt leírtak alapján: 35.2.1. - Gyökér CA létrehozása (558. oldal).

Használhatja ugyanazt a jelszót az összes CA-hoz. Jelölje meg a *CA jelszó használata tanúsítvány jelszavaként* pontot, hogy az alárendelt CA-k jelszava ugyanaz legyen, mint a gyökér CA-é: így kevesebb jelszóval kell foglalkozni a CA-k kezelése során.

MEGJEGYZÉS: Érvényességi időtartam ellenőrzése

Ne feledje, hogy az érvényességi időtartam nem lehet hosszabb, mint a gyökér CA érvényességi időtartama.

6 Válassza ki a *Tanúsítványok* lapot. Kapcsolja ki a nem kívánt (vagy veszélyeztetett) alárendelt CA-kat a *Visszavonás* gombbal. A visszavonás azonban nem elég az alárendelt CA kikapcsolásához. A kikapcsolt alárendelt CA-t közzé kell tenni egy CRL-ben is. A CRL készítési folyamatának leírása: 35.2.6. - CRL készítése (566. oldal).

7 A befejezéshez nyomja meg az *OK* gombot.

35.2.4 Felhasználói tanúsítványok készítése és visszavonása

A kliens- és kiszolgálótanúsítványok készítése nagyon hasonlít a CA-k létrehozásához (35.2.1. - Gyökér CA létrehozása (558. oldal)). Ugyanazok az elvek érvényesek itt is. Az elektronikus levelek aláírására készült tanúsítványok esetén a küldő (a saját kulcs birtokosának) elektronikus levélcímét feltétlenül fel meg kell adni a tanúsítványban, hogy a megfelelő tanúsítvány a levelezőprogramban hozzárendelhető legyen. A titkosításhoz használt tanúsítvány hozzárendelésénél a fogadó (a nyilvános kulcs tulajdonosa) elektronikus levélcímét kell elhelyezni a tanúsítványban. Kiszolgáló- és klienstanúsítványok esetén meg kell adni a kiszolgáló nevét az *Általános név* mezőben. A tanúsítványok alapértelmezett érvényessége 365 nap.

A kiszolgáló- és klienstanúsítványok létrehozásának módja:

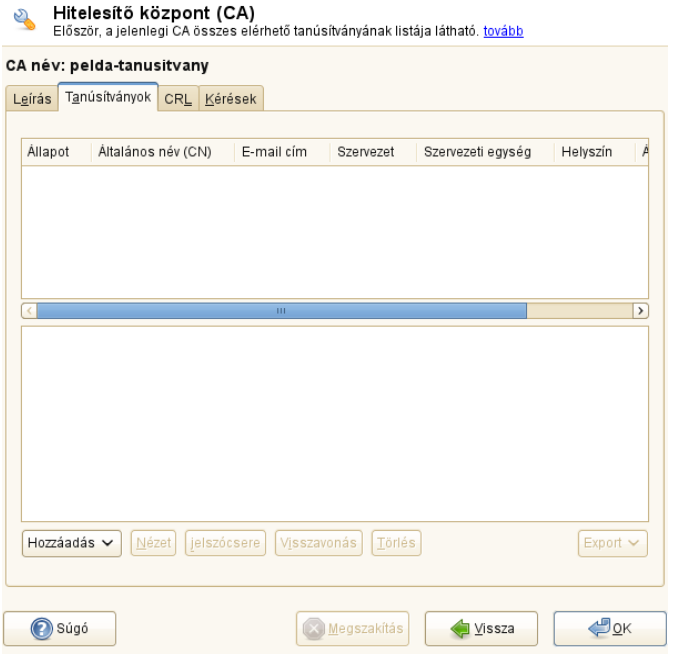
1 Indítsa el a YaST-ot és nyissa meg a CA-modult.

2 Válassza ki a kívánt gyökér CA-t, majd kattintson a *Belépés a CA-ba* gombra.

3 Adja meg a jelszót, ha most először lép be a CA-ba. A YaST a *Leírás* lapon megjeleníti a CA kulcsadatait.

4 Kattintson a *Tanúsítványok* lapra (lásd: 35.3. ábra).

35.3. ábra *A CA tanúsítványai*



5 Kattintson a *Hozzáadás* > *Kiszolgálótanúsítvány hozzáadása* pontra és készítse el a kiszolgálótanúsítványt.

6 Kattintson a *Hozzáadás* > *Kliens tanúsítvány hozzáadása* pontra és készítse el a klienstanúsítványt. Ne feledje el megadni az e-mail címeket.

7 A befejezéshez nyomja meg az *OK* gombot.

A veszélyeztetett vagy megbízhatatlanná vált tanúsítványok visszavonásának módja:

1 Indítsa el a YaST-ot és nyissa meg a CA-modult.

2 Válassza ki a kívánt gyökér CA-t, majd kattintson a *Belépés a CA-ba* gombra.

3 Adja meg a jelszót, ha most először lép be a CA-ba. A YaST a *Leírás* lapon megjeleníti a CA kulcsadatait.

4 Kattintson a *Tanúsítványok* lapra (lásd: 35.2.3. - Alárendelt CA készítése és visszavonása (561. oldal)).

5 Válassza ki a visszavonni kívánt tanúsítványt és kattintson a *Visszavonás* gombra.

6 Adja meg a tanúsítvány visszavonásának okát.

7 A befejezéshez nyomja meg az *OK* gombot.

MEGJEGYZÉS

A visszavonás önmagában nem elég a tanúsítvány deaktiválásához. A visszavont tanúsítványt közzé kell tenni egy CRL-ben is. A CRL-ek létrehozását a 35.2.6. - CRL készítése (566. oldal) rész írja le. A visszavont tanúsítványokat a CRL-ben közzététel után a *Törlés* gombbal lehet törölni.

35.2.5 Alapértelmezett adatok megváltoztatása

Az előző részben ismertettük, hogyan tud alárendelt CA-t, kliens- és kiszolgálótanúsítványokat készíteni. A speciális beállításokat az X.509 tanúsítványok kiterjesztései használják. Ezek a kiterjesztések előre definiált értékekekkel rendelkeznek minden tanúsítványtípusra, és normál körülmények között ezek módosítása nem szükséges. Néhány speciális alkalmazás azonban igényelheti ezek módosítását. Amennyiben ilyen alkalmazások részére gyakran készít tanúsítványokat, érdemes az alapértelmezett értékeket átállítani. Ellenkező esetben minden egyes tanúsítványnál külön kell módosítani ezeket.

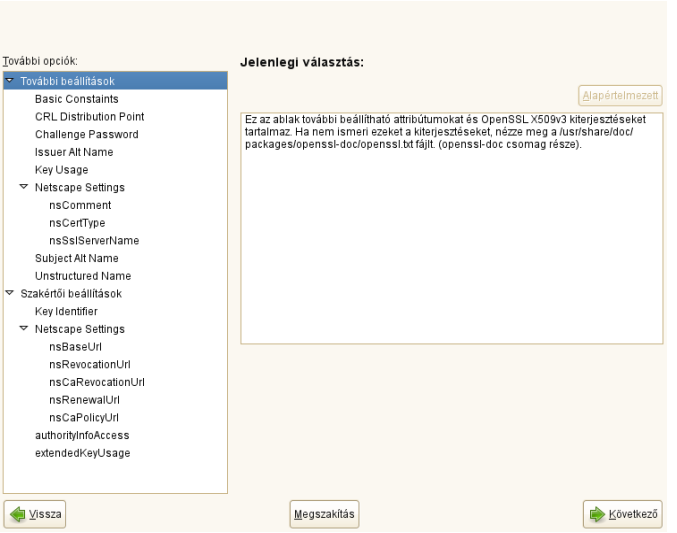
1 Indítsa el a YaST-ot és nyissa meg a CA-modult.

2 Lépjen be a megfelelő gyökér CA-ba (35.2.3. - Alárendelt CA készítése és visszavonása (561. oldal))

3 Kattintson a *Szakértői* > *Alapértelmezett szerkesztése* pontra.

4 Válassza ki a módosítani kívánt beállítások típusát. Ezek után megjelenik az alapértékeket tartalmazó párbeszédablak: 35.4. ábra - YaST CA modul – Speciális beállítások (566. oldal).

35.4. ábra *YaST CA modul – Speciális beállítások*



5 Módosítsa a megfelelő értéket a jobb oldalon, és állítsa be vagy törölje a *kritikus* értéket.

6 Kattintson a *Tovább* gombra. Megjelenik egy rövid összefoglalás.

7 A módosítások véglegesítéséhez kattintson a *Mentés* gombra.

MEGJEGYZÉS

Minden alapérték-módosítás csak a módosítás után készült objektumokra érvényes. A módosítás a már meglévő CA-kat és tanúsítványokat nem érinti.

35.2.6 CRL készítése

Nem elég a veszélyeztetett vagy megbízhatatlanná vált tanúsítványokat törölni, előbb vissza is kell vonni őket. Ennek leírása a 35.2.3. - Alárendelt CA készítése és visszavonása (561. oldal) (alárendelt CA-k), illetve a 35.2.4. - Felhasználói tanúsítványok készítése és visszavonása (563. oldal) (felhasználói tanúsítványok) részekben olvashatók. Ezek után a CRL-t el kell készíteni és közzé kell tenni.

A rendszer minden CA-hoz pontosan egy CRL-t tart nyilván. E CRL elkészítéséhez vagy frissítéséhez:

1. Indítsa el a YaST-ot és nyissa meg a CA-modult.
2. Lépjen be a megfelelő CA-ba (35.2.3. - Alárendelt CA készítése és visszavonása (561. oldal)).
3. Kattintson a *CRL* pontra. A következő párbeszédablakban a CA utolsó CRL-jéről készült összefoglalóját tekintheti meg.
4. Amennyiben visszavont alárendelt CA-kat vagy tanúsítványokat a lista készülte óta, hozzon létre egy új CRL-t a *CRL létrehozása* gombra kattintva.
5. Adja meg az új CRL érvényességi idejét (alapértelmezés 30 nap).
6. Kattintson az *OK* gombra a CRL elkészítéséhez és megjelenítéséhez. Ezek után közzé kell tenni a CRL-t.

TIPP

A CRL-t használó alkalmazások elutasítják azokat a tanúsítványokat, amelyek a CRL-ben szerepelnek. PKI-szolgáltatóként az Ön feladata, hogy mindig készítse el és tegye közzé a legújabb CRL listát, mielőtt a régi lejár (érvényességi ideje lejárta előtt). A YaST jelenleg nem rendelkezik a funkció automatizálására szolgáló megoldással.

35.2.7 CA objektumok exportálása LDAP-ba

A YaST LDAP-klienssel elő kell készíteni a végrehajtó számítógépet LDAP-exportra. Így futási időben elérhetővé válnak LDAP kiszolgálóinformációk, és ezek használhatók a párbeszédablakok automatikus kiegészítésére. Az LDAP export lehetséges egyéb esetben is, azonban az LDAP adatokat kézzel kell beírni. Mindig több jelszót is be kell írni (bővebb információ: 35.3 táblázat - LDAP exportálás közben szükséges jelszavak (568. oldal)).

35.3. táblázat *LDAP exportálás közben szükséges jelszavak*

Jelszó	Jelentés
LDAP jelszó	A jelszó hitelesíti a klienst, hogy képes legyen objektumok létrehozására az LDAP-címtárfában.
Tanúsítványjelszó	A jelszó hitelesíti a felhasználót, hogy ki tudja exportálni a tanúsítványt.
Új tanúsítványjelszó	PKCS12 formátum használatos LDAP export közben. Ez a formátum kikényszeríti egy új jelszó hozzárendelését az exportált tanúsítványhoz.

Tanúsítványok, CA-k,és CRL-ek exportálhatók LDAP protokollon keresztül.

CA exportálása LDAP-ba
: CA exportálásához adja meg a CA-t (35.2.3. - Alárendelt CA készítése és visszavonása (561. oldal)). Válassza ki a *Kiterjesztés* > *Exportálás LDAP-ba* pontot a következő párbeszédablakban, amely megnyitja az LDAP-adatok beírására szolgáló újabb párbeszédablakot. Ha a rendszer YaST-al lett beállítva, a mezők automatikusan kitöltődnek. Ellenkező esetben minden adatot kézzel kell megadni. Az LDAP-ban megadott bejegyzések egy külön fában, a „caCertificate” attribútummal lesznek megadva.

Tanúsítvány exportálása LDAP-ba
: Adja meg a CA-t, amely tartalmazza az exportálni kívánt alárendelt CA-t, majd válassza ki a *Tanúsítványok* lapot. Válassza ki az alárendelt CA-t a tanúsítványlistából, a párbeszédablak felső részében, majd válassza ki az *Exportálás* > *Exportálás LDAP-ba* pontot. Az LDAP-adatokat ugyanúgy kell megadni, mint a CA-knál. Ezután a tanúsítvány a megfelelő felhasználói objektummal együtt el lesz mentve az LDAP-címtárfában, kibővítve a „userCertificate” (PEM formátum) és „userPKCS12” (PKCS12 formátum) attribútumokkal.

CRL exportálása LDAP-ba
: Adja meg a CRL-t tartalmazó CA-t, amelyet exportálni kíván és válassza ki a *CRL* pontot. Ha szükséges, készítsen egy új CRL-t, majd kattintson az *Exportálás* gombra. A megjelenő párbeszédablakban láthatók az exportálási paraméterek. A CA CRL-je exportálható egyszer, de meghatározott időközönként rendszeresen is. Aktiválja az exportálást: válassza ki az *Exportálás LDAP-ba* pontot, majd adja meg

a megfelelő LDAP-adatokat. A rendszeres végrehajtáshoz jelölje meg a *Ismétlődő újrakészítés és exportálás* választógombot, és ha szükséges, módosítsa az időközt.

35.2.8 CA-objektumok exportálása fájlba

Ha beállított egy lerakatot a számítógépen a CA adminisztrálásához, akkor ezzel a funkcióval hozhatja létre a megfelelő CA-objektumokat a megfelelő helyeken, közvetlenül fájl formájában. Különböző formátumok használhatók, például PEM, DER vagy PKCS12. PEM formátum esetén kiválaszthatja, hogy el kívánja -e menteni a kulcsokat, illetve, hogy a kulcsok titkosítottak legyenek-e. PKCS12 formátum esetén lehetséges a tanúsítvány-útvonal exportálása is.

A tanúsítvány CA és CRL fájl formátumba történő exportálása ugyanúgy történik, mint az LDAP export (35.2.7. - CA objektumok exportálása LDAP-ba (567. oldal)), azzal a különbséggel, hogy az *Exportálás LDAP-ba* pont helyett az *Exportálás fájlba* pontot kell kiválasztani. Ezek után megjelenik a párbeszédablak, ahol kiválaszthatja a kimeneti formátumot, és beírhatja a jelszót és a fájl nevét. A tanúsítványok az *OK* gombra kattintás után a megfelelő helyre lesznek elmentve.

CRL-ek esetén kattintson az *Exportálás* gombra, válassza ki az *Exportálás fájlba* pontot, adja meg az exportálás formátumát (PEM vagy DER), majd adja meg az elérési útvonalat. Kattintson az *OK* gombra a megfelelő helyre mentéshez.

TIPP

Bármely tárolási helyet kiválaszthat a fájlrendszeren. Ez a parancs használható a CA objektumok hordozható adathordozóra, például USB-meghajtóra exportálásra is. A `/media` általában mindenféle egyéb meghajtót jelenthet (a merevlemez kivételével).

35.2.9 Általános kiszolgálótanúsítványok importálása

Ha rendelkezik egy exportált kiszolgálótanúsítvánnyal egy cserélhető adathordozón, amely a YaST segítségével készült egy elkülönített CA-felügyeleti gépen, importálhatja azt egy másik kiszolgálón, mint *általános kiszolgálótanúsítványt*. Ezt a telepítés során vagy később is megteheti a YaST használatával.

MEGJEGYZÉS

A tanúsítvány sikeres importálásához valamelyik PKCS12 formátumot kell használni.

Az általános kiszolgálótanúsítvány az `/etc/ssl/servercerts` könyvtárban tárolódik és bármely CA által támogatott szolgáltatáshoz használható. Ha a tanúsítvány lejár, hasonló módon könnyedén lecserélhető. Egyetlen további művelet szükséges: a tanúsítványt használó szolgáltatásokat újra kell indítani.

TIPP

Az *Importálás* kiválasztása után keresse ki a fájlrendszerből a forrásfájlt. Ez a megoldás alkalmazható a tanúsítvány cserélhető adathordozókról, például USB-meghajtókról történő importáláshoz is.

Egy általános kiszolgálótanúsítvány importálása:

1. Indítsa el a YaST-ot, majd nyissa meg az *Általános kiszolgálótanúsítvány* részt a *Biztonság és felhasználók* modulban.
2. Miután a YaST elindult, tekintse meg a jelenlegi tanúsítvány adatait a leírás mezőben.
3. Válassza ki az *Importálás* pontot, majd a tanúsítványfájlt.
4. Írja be a jelszót és kattintson a *Tovább* gombra. Az importált tanúsítvány a leírás mezőben jelenik meg.
5. Zárja be YaST-ot a *Befejezés* gombra kattintással.

36 Partíciók és fájlok titkosítása

Minden felhasználó rendelkezik bizalmas adatokkal, amelyekhez nem akarja, hogy mások hozzáférjenek. Minél jobban támaszkodik valaki a mobil számítástechnikai eszközökre, illetve minél sokszínűbb környezeteket és hálózatokat használ, annál óvatosabban kell kezelnie adatait. Ajánlatos a fájlok vagy a teljes partíciók titkosítása, ha másoknak is van a rendszerhez hálózati vagy fizikai hozzáférése. A noteszgépek vagy a cserélhető adathordozók (például a külső merevlemezek vagy az USB-meghajtók) ki vannak téve az ellopás vagy elvesztés veszélyének. Emiatt érdemes a bizalmas adatokat tartalmazó fájlokat titkosítani.

Számos módja van annak, hogy adatait titkosítással védje:

Merevlemez-partíciók titkosítása
: A YaST lehetővé teszi egy titkosított partíció létrehozását a telepítés során, vagy akár a már telepített rendszeren. A részleteket lásd: 36.1.1. - Titkosított partíció létrehozása a telepítés közben (573. oldal) és 36.1.2. - Titkosított partíció létrehozása működő rendszeren (574. oldal). Ez a lehetőség a cserélhető adathordozóknál – például külső merevlemezeknél – is használható a következő részben leírtak szerint: 36.1.4. - Cserélhető adathordozók tartalmának titkosítása (575. oldal).

Titkosított fájl létrehozása tárolóként
: Titkosított fájl bármikor létrehozható a merevlemezen vagy egy cserélhető adathordozón a YaST használatával. A titkosított fájl ezután más fájlok vagy mappák *tárolására* használható. További információért lásd: 36.1.3. - Titkosított tárolófájlok létrehozása (574. oldal).

Saját könyvtárak titkosítása
: Az openSUSE használatával titkosított saját könyvtárak készíthetők a felhasználóknak. Ha egy felhasználó bejelentkezik a rendszerbe, a rendszer felcsatolja a titkosított saját könyvtárat és annak tartalma elérhető lesz a felhasználó számára. További információkért lásd: 36.2. - Titkosított saját könyvtárak használata (575. oldal).

Egy-egy ASCII szövegtájl titkosítása
: Ha csak kevés olyan ASCII fájlja van, ami érzékeny vagy bizalmas adatokat tartalmaz, akkor azok egyenként is titkosíthatók és jelszóval védhetők a vi szerkesztő segítségével. További információkért lásd: 36.3. - ASCII szövegfájlok titkosítása a vi segítségével (576. oldal).

FIGYELEM: A titkosított adathordozó használata csak korlátozott védelmet jelent

Az ebben a részben leírt módszerek csak korlátozott védelmet nyújtanak. A működő rendszer nem védhető meg az illetéktelen használattól. Ha egy titkosított adathordozó sikeresen fel lett kapcsolva, akkor a szükséges jogosultságok birtokában mindenki hozzáférhet. Mégis érdemes titkosított adathordozókat használni, hátha elvész a számítógép vagy ellopják, illetve védelmet jelent az ellen, hogy jogosulatlan személyek elolvassák a bizalmas adatokat.

36.1 Titkosított fájlrendszer létrehozása YaST használatával

A YaST lehetővé teszi a fájlrendszer részeinek vagy partícióknak a titkosítását a telepítés során, vagy akár a már telepített rendszeren. Azonban egy már telepített rendszeren található partíció titkosítása bonyolultabb, mivel át kell méretezni és meg kell változtatni a meglévő partíciókat. Ilyenkor lehet, hogy kényelmesebb egy adott méretű titkosított fájlt létrehozni a fájlrendszer egyéb fájljainak vagy részeinek *tárolására*. Egy teljes partíció titkosításához azonban rá kell szánni erre egy külön partíciót – gondoljon erre, amikor a partíciók elrendezését kialakítja. A YaST által javasolt szokásos partíciókiosztás alapértelmezésben nem tartalmaz titkosított partíciót. Az ilyen partíciókat a particionálás során kézzel kell felvenni.

36.1.1 Titkosított partíció létrehozása a telepítés közben

FIGYELEM: Jelszó megadása

Győződjön meg róla, hogy jól megjegyezte a titkosított partíciók jelszavát. Jelszó nélkül titkosított adatok nem érhetők el és nem állíthatók vissza.

A particionálásra szolgáló YaST szakértői párbeszédablak tartalmazza a titkosított partíció létrehozásához szükséges összes lehetőséget. Egy új titkosított partíció készítése a következőképpen történik:

1. Indítsa el a YaST particionálót a YaST vezérlőközpontból a *Rendszer* > *Particionáló* menüpont használatával
2. Kattintson a *Létrehozás* gombra és válasszon ki egy elsődleges vagy logikai partíciót.
3. Adja meg a használni kívánt fájlrendszert, méretet és a partíció csatolási pontját.
4. Ha a titkosított fájlrendszert csak szükség esetén kell felcsatolni, akkor az *Fstab beállítások* részben jelölje meg az *Indítás során ne kerüljön csatolásra* négyzetet.
5. Jelölje meg a *Fájlrendszer titkosítása* négyzetet.
6. Kattintson az *OK* gombra. A rendszer be fogja kérni a jelszót a partíció titkosításához. A jelszó nem jelenik meg a képernyőn. A gépelési hibák kivédése érdekében adja meg a jelszót mégegyszer.
7. A feladat befejezéséhez nyomja meg az *OK* gombot. Az új titkosított partíció létrejött.

Az operációs rendszer induláskor, a partíció felcsatolása előtt bekéri a jelszót. Ha a partíció már fel van csatolva, akkor minden felhasználó elérheti.

Ha az indítás során nem kívánja felcsatolni a titkosított partíciót, akkor a jelszó kérésekor egyszerűen csak üsse le az Enter billentyűt. Ezután utasítsa el a jelszó újbóli beírásának lehetőségét is. A titkosított fájlrendszer ebben az esetben nem kerül felcsatolásra és az

operációs rendszer folytatja a rendszerindítást. úgy, hogy megakadályozza az adatok elérését.

Ha olyan gépre telepíti a rendszert, ahol már eredetileg is létezik több partíció, akkor a telepítés során dönthet úgy, hogy egy meglévő partíciót titkosít. Ebben az esetben kövesse a 36.1.2. - Titkosított partíció létrehozása működő rendszeren (574. oldal) részben található leírást és ne feledje, hogy a művelet megsemmisíti a meglévő titkosítandó partíción található összes adatot.

36.1.2 Titkosított partíció létrehozása működő rendszeren

FIGYELEM: Titkosítás aktiválása egy futó rendszeren

Titkosított partíciók futó rendszeren is létrehozhatók. Egy meglévő partíció titkosítása azonban megsemmisíti az azon található adatokat és a jelenlegi partíciók átméretezését és átszervezését igényli.

A futó rendszeren a YaST vezérlőpanelben válassza ki a *Rendszer* > *Particionálás* menüpontot. A folytatáshoz kattintson az *Igen* lehetőségre. A *Szakértői particionálóban* válassza ki a titkosítani kívánt partíciót és kattintson a *Szerkesztés* gombra. Az eljárás további része ugyanaz, mint a 36.1.1. - Titkosított partíció létrehozása a telepítés közben (573. oldal) részben.

36.1.3 Titkosított tárolófájlok létrehozása

A bizalmas adatok tárolásához teljes partíciók titkosítása helyett egy-egy fájlon belül is létrehozható egy titkosított fájlrendszer. Az ilyen tárolófájlok a YaST Szakértői partícionáló részében készíthetők. Nyomja meg a *Titkosított fájlok* gombot, majd adja meg a fájl elérési útját és kívánt méretét. Fogadja el a formázáshoz felajánlott beállításokat és a fájlrendszer típusát. Ezután adja meg a csatolási pontot és döntse el, hogy a titkosított fájlrendszert a rendszerindítás során kívánja-e felcsatolni. Ellenőrizze, hogy a *Fájlrendszer titkosítása* négyzet meg van-e jelölve.

A titkosított tárolófájlok előnye a titkosított partíciók használatával szemben, hogy a merevlemez átparticionálása nélkül is elkészíthetők. A hurokeszköz segítségével kerülnek felcsatolásra és ugyanúgy viselkednek, mint a normál partíciók.

36.1.4 Cserélhető adathordozók tartalmának titkosítása

A YaST ugyanúgy kezeli a cserélhető adathordozókat (például a külső merevlemezeket vagy az USB-meghajtókat), mint bármilyen más merevlemezt. Az ilyen adathordozón található tárolófájlok és partíciók is titkosíthatók a fent leírt módon. Az *Fstab beállítások* részben azonban az *Indítás során ne kerüljön csatolásra* lehetőséget kell megjelölni, hiszen a cserélhető adathordozókat általában csak akkor csatlakoztatják, amikor a rendszer már fut.

Ha a YaST használatával titkosította a cserélhető adathordozót, akkor a KDE és a GNOME automatikusan felismeri a titkosított partíciót és bekéri a jelszót az eszköz észlelésekor. Ha egy FAT formázású cserélhető adathordozót csatlakoztat KDE vagy GNOME használatakor, akkor a jelszót megadó felhasználó automatikusan az eszköz tulajdonosává válik, olvashatja és írhatja a fájlokat. A más (nem FAT) fájlrendszereket használó eszközök esetében kifejezetten be kell állítani a tulajdonjogot a felhasználókhoz (nem lehet `root`) ahhoz, hogy írni vagy olvasni tudják az eszközön található fájlokat.

36.2 Titkosított saját könyvtárak használata

Ahhoz, hogy a saját könyvtárakban található adatok védve legyenek egy lopás vagy a merevlemez eltávolítása esetén, a YaST felügyeleti modul használatával engedélyezze a saját könyvtárak titkosítását. Titkosított saját könyvtár új és meglévő felhasználóknak is készíthető. A már létező felhasználók saját könyvtárának titkosításához és visszafejtéséhez tudni kell a bejelentkezési jelszavukat. További útmutatás: 5. fejezet - *Managing Users with YaST* (↑*Start-Up*)

Titkosított saját partíciók készíthetők egy fájltárolóban is, a következő részben leírtak szerint: 36.1.3. - Titkosított tárolófájlok létrehozása (574. oldal) Minden titkosított saját könyvtár esetében két fájl jön létre a `/home` könyvtárban:

`LOGIN``.img`
: A könyvtárat tartalmazó képfájl

LOGIN.key
: A képfájl kulcsa, a felhasználó bejelentkezési jelszavával védve.

Bejelentkezéskor a saját könyvtár automatikusan visszafejtődik. Ezt belsőleg a pam_mount nevű pam modul intézi. Ha a saját könyvtárak titkosítását eredményező kiegészítő bejelentkezési módszerrel kell bővíteni a rendszert, akkor ezt a modult hozzá kell adni az /etc/pam.d/ könyvtárban található megfelelő konfigurációs fájlhoz. További információk: 19. fejezet - *Hitelesítés PAM használatával* (267. oldal), valamint lásd a pam_mount kézikönyvoldalát.

FIGYELEM: Biztonsági korlátozások

A felhasználó saját könyvtárának titkosítása nem jelent erős védelmet a többi felhasználóval szemben. Ha erős védelemre van szükség, akkor a rendszert fizikailag nem szabad megosztani.

A biztonság növeléséhez titkosítsa a swap partíciót, valamint a /tmp és a /var/tmp könyvtárakat, mivel tartalmazhatják a kritikus adatok ideiglenes képfájljait. A swap, a /tmp és a/var/tmp is titkosítható a YaST particionálóval a(z) 36.1.1. - Titkosított partíció létrehozása a telepítés közben (573. oldal) vagy 36.1.3. - Titkosított tárolófájlok létrehozása (574. oldal) részben leírtak szerint.

36.3 ASCII szövegfájlok titkosítása a vi segítségével

A titkosított partíciók használatának az a hátránya, hogy amíg a partíció fel van csatolva, addig legalább a root felhasználó hozzá tud férni az adatokhoz. Ez megakadályozható a vi titkosított módban használatával.

Készítsen a vi –x *fájlnév* paranccsal egy új fájlt. A vi bekér egy jelszót, amellyel titkosítja a fájl tartalmát. Amikor a fájlt legközelebb megnyitja vi-ban, ismét meg kell adni a megfelelő jelszót.

A még nagyobb biztonság érdekében a titkosított szövegfájl egy titkosított partíción is elhelyezhető. Ez különösen azért ajánlott, mivel a vi-ban használt titkosítási mechanizmus nem nevezhető erősnek.

Jogosultságok korlátozása az AppArmor segítségével

37

Számos biztonsági sérülékenység származik a *megbízható* programok hibáiból. Egy megbízható program olyan kiemelt jogosultságokkal fut, amelyet a támadó meg kíván szerezni. A program nem tudja megőrizni a bizalmat, mert a programhibát kihasználó támadó is hozzájut az adott kiemelt jogosultsághoz.

A Novell AppArmor egy alkalmazásbiztonsági megoldás, amelyik kifejezetten abból a célból készült, hogy a lehető legkevesebb jogosultságra korlátozza a gyanús programokat. Az AppArmor segítségével a rendszergazda megadhatja, hogy milyen határok között működhet a program. Ehhez egy úgynevezett biztonsági *profilt* készít az adott alkalmazáshoz – ebben azoknak a fájloknak a listája található, amelyekhez a program hozzáférhet és azok a műveletek, amelyeket a program végrehajthat.

A számítógépes rendszerek tényleges megerősítéséhez minimalizálni kell azon programok számát, amelyek a jogosultságokt állítására szolgálnak, majd ezek utána a lehető legjobban meg kell védeni a programokat. A Novell AppArmor használatakor csak azokhoz a programokhoz kell profilt készíteni, amlyek ki vannak téve a támadás veszélyének. Ez látványosan lecsökkenti a számítógép megerősítéséhez szükséges munka mennyiségét. Az AppArmor profilok irányelvek betartásával garantálja, hogy a programok annyit tehessenek, amennyire jogosultak, de semmivel ne többet.

A rendszergazdáknak csak a támadásoknak valóban kitett alkalmazásokkal kell törődniük, és ezekhez kell profilokat készíteniük. Egy rendszer megerősítése tehát az AppArmor profilhalmaz kidolgozását és karbantartását jelenti, valamint AppArmor jelentéskezelő alrendszere által naplózott irányelvértések és kivételek folyamatos figyelését.

Az AppArmor profilok készítése az alkalmazások korlátozásához igen világos, intuitív folyamat. Az AppArmor számos eszközt tartalmaz, amely segít a profilok létrehozásában.

Nincs szükség programozásra vagy parancsfájlok készítésére. A rendszergazda egyetlen feladata, hogy a megerősítendő alkalmazások mindegyikéhez meg kell határoznia egy irányelvet a legszigorúbb hozzáférési és végrehajtási jogosultságokkal.

Az alkalmazásprofilok frissítésére vagy módosítására csak akkor van szükség, ha a szoftverkonfiguráció vagy a tevékenységek igényelt köre megváltozik. Az AppArmor intuitív eszközöket kínál a profilok frissítéséhez és módosításához.

A felhasználók elvileg semmit nem kell, hogy észrevegyenek az AppArmor működéséből. A „színfalak mögött” fut és nem igényel semmilyen felhasználói beavatkozást. Az AppArmor érdemben nem befolyásolja a teljesítményt. Ha az alkalmazás valamely tevékenységét nem fedi le az AppArmor profil, vagy az alkalmazás valamely tevékenységét megakadályozza az AppArmor, akkor a rendszergazdának igazítania kell az alkalmazás profilján, hogy az erre a viselkedésre is kiterjedjen.

A jelen ismertetőben felvázoljuk, hogy melyek a legfontosabb feladatok, amelyeket az AppArmorral el kell végezni a rendszer hatékony megerősítése érdekében. További, részletes információ: *Novell AppArmor Administration Guide* (↑*Novell AppArmor Administration Guide*).

37.1 A Novell AppArmor telepítése

A Novell AppArmor alapértelmezés szerint az openSUSE mindenféle telepítése esetén települ, függetlenül attól, hogy milyen mintát választ ki. Az AppArmor teljes értékben működő példányának telepítéséhez az alábbi csomagokra van szükség:

- `apparmor-docs`
- `apparmor-parser`
- `apparmor-profiles`
- `apparmor-utils`
- `naplóz`
- `libapparmor1`
- `perl-libapparmor`
- `yast2-apparmor`

37.2 A Novell AppArmor be- és kikapcsolása

Az Novell AppArmor alapértelmezés szerint az openSUSE minden frissen telepített példányában be van kapcsolva. Az AppArmor állapota kétféleképpen kapcsolható át:

A YaST rendszerszolgáltatások (futási szint) modulban
: Az AppArmor be- és kikapcsolásához vegye fel (vagy távolítsa el) a rendszerindító parancsfájlját a rendszer indulásakor végrehajtott parancsfájlok közé (közül). Az állapot a rendszer következő indulásakor fog megváltozni.

A Novell AppArmor vezérlőpult használatával
: Egy működő rendszerben a Novell AppArmor állapota a YaST Novell AppArmor vezérlőpultban kapcsolható ki és be. Az itteni változtatások azonnal életbe lépnek. A vezérlőpult egy leállítási vagy indítási eseményt generál az AppArmor számára, valamint eltávolítja a rendszerindító parancsfájlját a rendszer indulásakor végrehajtott parancsfájlok közül (ill. felveszi oda).

Az AppArmor tartós lekapcsolása, a rendszerindító parancsfájljának a rendszer indulásakor végrehajtott parancsfájlok közül eltávolításával:

1. Indítsa el a YaST-ot.
2. Válassza ki a *Rendszer* > *Rendszerszolgáltatások (futási szint)* modult.
3. Válassza ki a *Szakértői mód* pontot.
4. Válassza ki a `boot.apparmor` elemet, majd a *Beállítás/Visszaállítás* > *Szolgáltatás tiltása* menüpontot.
5. Lépjen ki a YaST futásiszint-szerkesztőből a *Befejezés* gombbal.

Az AppArmor a rendszer következő indításánál már nem lesz inicializálva, és egészen addig inaktív marad, amíg újra nem engedélyezi. A szolgáltatás visszakapcsolása a YaST futásiszint-szerkesztőjével nagyon hasonlít a kikapcsolásra.

Egy működő rendszerben az AppArmor állapota az AppArmor vezérlőpulttal kapcsolható át. Ez a módosítás azonnal életbe lép, és a rendszer újraindítása után is érvényben marad. Az AppArmor állapotának átkapcsolása:

1 Indítsa el a YaST-ot.

2 Válassza ki a *Novell AppArmor* > *AppArmor vezérlőpult* modult.

3 Jelölje meg az *AppArmor bekapcsolása* pontot. Az AppArmor letiltásához törölje ezt a jelölést.

4 Lépjen ki az AppArmor vezérlőpultból a *Kész* gombra kattintva.

37.3 Az alkalmazásprofilok készítésének első lépései

A Novell AppArmor sikeres alkalmazása az alábbiak gondos elvégzéséből áll:

1 Határozza meg, mely alkalmazásokhoz kíván profilt készíteni. Erről további részletek: 37.3.1. - A profilírozandó alkalmazások kiválasztása (580. oldal).

2 Készítse el a szükséges profilokat. Ennek vázlatos leírása: 37.3.2. - Profilok készítése és módosítása (582. oldal). Ellenőrizze az eredményeket és ha szükséges, módosítsa a profilokat.

3 Figyelje, hogy mi történik a rendszeren: futtassa az AppArmor jelentéseit és reagáljon a biztonsági eseményekre. További információk:37.3.3. - Novell AppArmor eseményértesítések és jelentések beállítása (584. oldal).

4 Frissítse a profilokat, ha a környezet változik, vagy ha reagálni kell az AppArmor jelentéskészítő eszköze által naplózott biztonsági eseményekre. További információk:37.3.4. - Profilok frissítése (586. oldal).

37.3.1 A profilírozandó alkalmazások kiválasztása

Csak azokat a programokat kell védeni, amelyek az adott rendszerben támadásnak vannak kitéve, vagyis csak azokhoz az alkalmazásokhoz kell profilokat készíteni, amelyeket valóban használ is. A legesélyesebb programok meghatározásában segít az alábbi lista:

Hálózati ügynökök
: A nyitott hálózati portokat kezelő programok (kiszolgálók és kliensek egyaránt). A felhasználói kliensprogramok, például a levelezőkliensek vagy a webböngészők jogosultságait ki lehet használni. Ezek a programok jogosultak írni a felhasználó saját könyvtárát, ugyanakkor potenciálisan veszélyes távoli forrásokból érkező bemeneteket dolgoznak fel (például webhelyek, vagy e-mailben elküldött rosszindulatú kódok).

Webes alkalmazások
: A webböngészővel meghívható programok, például CGI Perl parancsfájlok, PHP-oldalak és egyéb, komplex webes alkalmazások.

Cron-nal futtatott feladatok
: Olyan programok, amelyeket a cron démon futtat rendszeresen, különféle forrásokból.

Ha meg akarja állapítani, hogy éppen mely portok futnak nyitott hálózati portokkal, és melyekhez lehet szükség profil készítésére, indítsa el `root` felhasználóként az `aa-unconfined` programot.

37.1 példa *Az aa-unconfined program kimenete*

```
19848 /usr/sbin/cupsd not confined
19887 /usr/sbin/sshd not confined
19947 /usr/lib/postfix/master not confined
29205 /usr/sbin/sshd confined by '/usr/sbin/sshd (enforce)'
```

A fenti példa minden `nem korlátozott`-nak jelölt folyamatát érdemes lehet egy egyéni profillal korlátozni. A `korlátozza` címkéjű programokat már védi az AppArmor.

TIPP: További információk

További információ a profilírozandó alkalmazások kiválasztásáról. 1.2. - Determining Programs to Immunize (1. fejezet - *Immunizing Programs*, ↑*Novell AppArmor Administration Guide*).

37.3.2 Profilok készítése és módosítása

Az openSUSE rendszeren futó Novell AppArmor egy sor előre elkészített profilt tartalmaz a legfontosabb alkalmazásokhoz. Ezenfelül az AppArmorral természetesen bármely alkalmazáshoz készíthetők saját profilok.

A profilok kezelésének két módja létezik. Az egyik a YaST Novell AppArmor modulok grafikus felületének, a másik az AppArmor csomag parancssori eszközeinek használata. Mindkét módszer lényegében hasonlóan működik.

Az aa-unconfined futtatása a leírt módon (37.3.1. - A profilírozandó alkalmazások kiválasztása (580. oldal)) azonosít egy sor alkalmazást, amelyekhez célszerű lehet profilt készíteni.

Az egyes alkalmazások profiljai az alábbi lépésekkel készíthetők el:

1. `Root` felhasználóként készíttessen az AppArmorral egy durva alkalmazásprofilt: futtassa le az `aa-genprof` *`program_neve`* parancsot.

   vagy

   A durva alapprofil a *YaST* > *Novell AppArmor* > *Profil hozzáadása varázsló* futtatásával és a profilírozandó alkalmazás teljes elérési útjának megadásával is elkészíthető.

   Elkészül az alapprofil, és az AppArmor tanulási módba vált. Ez azt jelenti, hogy naplózza a végrehajtott programok minden tevékenységét, de még nem korlátozza őket.

2. Használja az alkalmazás összes műveletét, hogy az AppArmor pontos képet kapjon róluk.

3. Elemeztesse az AppArmorral az előállított naplófájlokat (2. Lépés (582. oldal)): az aa-genprof programban írja be, hogy `S`.

   vagy

   A naplófájlok elemzésének másik módja a *Profil hozzáadása varázsló AppArmor események keresése a rendszernaplóban* pontjára kattintás, és a varázsló útmutatásának követése, amíg a profil el nem készül.

Az AppArmor megvizsgálja az alkalmazás futtatása során készített naplókat, és felszólít, hogy adja meg a hozzáférési jogokat minden egyes naplózott eseményhez. Vagy adja meg őket fájlonként, vagy használjon helyettesítő karaktereket.

4 Az alkalmazás bonyolultságától függően szükség lehet a 2. Lépés (582. oldal) és 3. Lépés (582. oldal) részek megismétlésére. Korlátozza az alkalmazást, hajtsa végre a korlátozott körülmények között, és vizsgálja meg az újonnan naplózott eseményeket. Az alkalmazás teljes funkciókörének korlátozásához lehet, hogy ezt az eljárást többször is meg kell ismételni.

5 Ha minden hozzáférési jogosultságot sikerült beállítani, kapcsolja a profilt kényszerítés módba. A profil ezután élesben működik és az AppArmor az imént létrehozott profil beállításainak megfelelően korlátozza az alkalmazást.

   Ha egy olyan alkalmazáson indította el az aa-genprof parancsot, amelynek már volt egy panasz módba állított meglévő profilja, akkor ez a profil tanulási módban marad egész addig, amíg ki nem lép a tanulási ciklusból. További információ a profilok módjának megváltoztatásáról: „aa-complain—Entering Complain or Learning Mode” szakasz (5. fejezet - *Building Profiles from the Command Line*, ↑*Novell AppArmor Administration Guide*) és „aa-enforce—Entering Enforce Mode” szakasz (5. fejezet - *Building Profiles from the Command Line*, ↑*Novell AppArmor Administration Guide*).

Próbálja ki a profil beállításait: hajtson végre minden szükséges műveletet az imént korlátozott alkalmazással. Normális esetben a korlátozott program simán fut és észre sem venni, hogy az AppArmor működik. Ha azonban rendellenességeket tapasztal az alkalmazás működése kapcsán, akkor ellenőrizze a rendszernaplókat és nézze meg, hogy nem túl szigorúan korlátozza-e az AppArmor az alkalmazást. A rendszeren használt naplózási mechanizmustól függően több helyen is lehet keresni AppArmor naplóbejegyzéseket:

`/var/log/audit/audit.log`

Ha az `audit` csomag telepítve van és fut is az auditd, akkor az AppArmor események így naplózódnak:

```
type=APPARMOR_DENIED msg=audit(1210347212.123:18):
operation="inode_permission" requested_mask="::w" denied_mask="::w"
fsuid=1000 name="/tmp/.X11-unix/X0" pid=9160 profile="/usr/bin/ksmserver
```

`/var/log/messages`
: Ha nem használja az auditd démont, akkor az AppArmor eseményei a normál rendszernaplóba (`/var/log/messages`) kerülnek. Egy jellemző bejegyzés például így nézhet ki:

```
May  9 17:39:56 neovirt klogd: type=1503 audit(1210347596.146:23):
operation="inode_permission" requested_mask="::w" denied_mask="::w"
fsuid=1000 name="/tmp/.X11-unix/X0" pid=9347 profile="/usr/bin/ksmserver"
```

`dmesg`
: Ha az auditd nem fut, akkor az AppArmor-események ellenőrizhetők a `dmesg` paranccsal is:

```
type=1503 audit(1210347596.146:23): operation="inode_permission"
requested_mask="::w" denied_mask="::w" fsuid=1000 name="/tmp/.X11-unix/X0"
 pid=9347 profile="/usr/bin/ksmserver"
```

A profil módosításához először vizsgálja meg az alkalmazással kapcsolatos naplóüzeneteket (lásd: 3. Lépés (582. oldal)). Amikor a program felszólítja, adja meg a hozzáférési jogokat vagy korlátozásokat.

TIPP: További információk

További információ a profilok készítéséről és módosításáról: 2. fejezet - *Profile Components and Syntax* (↑*Novell AppArmor Administration Guide*), 4. fejezet - *Building and Managing Profiles with YaST* (↑*Novell AppArmor Administration Guide*) és 5. fejezet - *Building Profiles from the Command Line* (↑*Novell AppArmor Administration Guide*).

37.3.3 Novell AppArmor eseményértesítések és jelentések beállítása

Állítsa be a Novell AppArmor eseményértesítési funkcióit, hogy reagálhasson a biztonsági eseményekre. Az eseményértesítés a Novell AppArmor hasznos szolgáltatása, amely értesítést küld egy megadott e-mail címre egy meghatározott súlyosságú Novell AppArmor esemény bekövetkezése esetén. Ez a funkció jelenleg a YaST felületen érhető el.

Az eseményértesítés beállításához a következőt kell tenni a YaST-ban:

1. Győződjön meg róla, hogy van a rendszeren megfelelően működő levélkiszolgáló, amelyik el tudja küldeni az eseményértesítéseket.

2. Indítsa el a YaST-ot. Ezután válassza ki a *Novell AppArmor* > *AppArmor vezérlőpult* modult.

3. A *Biztonsági esemény értesítés* képernyőn nyomja meg a *Beállítás* gombot.

4. Minden egyes rekordtípushoz (*Rövid*, *Összefoglaló*, és *Részletes*) állítsa be a jelentés gyakoriságát, adja meg az e-mail címet, ahová a jelentéseket küldi, és határozza meg a naplózandó események súlyosságát. Ha az ismeretlen eseményeket is bele kívánja venni az eseményjelentésekbe, akkor jelölje meg az *Ismeretlen súlyosságú események hozzáadása* pontot.

   MEGJEGYZÉS: A naplózandó események kiválasztása

   Ha nincs tisztában az AppArmor eseménykategorizálási rendszerével, akkor kérjen értesítést mindegyik biztonsági szint eseményeiről.

5. A beállítások alkalmazásához lépjen ki a párbeszédablakból az *OK* > *Kész* gombokkal.

A Novell AppArmor jelentéseinek használatával elolvashatók a fontos Novell AppArmor biztonsági események jelentései anélkül, hogy át kellene rágnia magát az aa-logprof eszközzel értelmezhető üzeneteken. A jelentés mérete csökkenthető, ha szűr dátumtartományra vagy egy adott program nevére.

Az AppArmor jelentések beállítása:

1. Indítsa el a YaST-ot. Válassza ki a *Novell AppArmor* > *AppArmor jelentések* modult.

2. Válassza ki a megvizsgálni vagy beállítani kívánt jelentés típusát: *Executive Security Summary*, *Alkalmazásaudit* vagy *Biztonsági esemény jelentés*.

3. Adja meg, hogy milyen sűrűn készüljön jelentés, továbbá e-mail címet, az exportálás formátumát, valamint a jelentések helyét: nyomja meg a *Szerkesztés* gombot és adja meg a kért adatokat.

4. Egy adott típusú jelentés futtatásához kattintson a *Futtatás most* gombra.

5 Az adott típusú archivált jelentések tallózásához kattintson az *Archívum megtekintése* pontra, majd adja meg a jelentés típusát.

vagy

Törölje a már nem szükséges jelentéseket, vagy készítsen újakat.

TIPP: További információk

További információ a Novell AppArmor eseményértesítés beállításáról: 7.2. - Configuring Security Event Notification (7. fejezet - *Managing Profiled Applications*, ↑*Novell AppArmor Administration Guide*). További információ a jelentések beállításáról: 7.3. - Configuring Reports (7. fejezet - *Managing Profiled Applications*, ↑*Novell AppArmor Administration Guide*).

37.3.4 Profilok frissítése

A szoftverek és a rendszer beállításai időről-időre megváltoznak. Ennek eredményeképpen időnként szükség lehet az AppArmor profil beállításainak hangolására. Az AppArmor megvizsgálja a rendszernaplót, hogy lát-e benne irányelvsértéseket vagy más AppArmor-eseményeket, és lehetővé teszi, hogy ezeknek megfelelően módosítsa a profilt. Az alkalmazások profildefiníción kívüli viselkedése szintén kezelhető a *Profil frissítése* varázslóval.

A profilhalmaz frissítése:

1 Indítsa el a YaST-ot.

2 Indítsa el a *Novell AppArmor* > *Profil frissítése* varázslóját.

3 A megjelenő ablakban módosítsa a naplózott erőforrások vagy végrehajtható fájlok hozzáférési vagy végrehajtási jogait.

4 A kérdések megválaszolása után lépjen ki a YaST-ból. A módosítások érvénybe lépnek a profilokon.

TIPP: További információk

További információ a profilok frissítésével kapcsolatban a rendszernaplók alapján: 4.5. - Updating Profiles from Log Entries (4. fejezet - *Building and Managing Profiles with YaST*, ↑*Novell AppArmor Administration Guide*).

38 Biztonság és megbízhatóság

A Linux- és UNIX-rendszerek egyik fő jellemzője, hogy egyszerre több felhasználót tudnak kezelni (többfelhasználósság) és lehetővé teszik, hogy ezek a felhasználók egyidejűleg több feladatot hajtsanak végre ugyanazon a számítógépen (többfeladatosság). Az operációs rendszer a hálózat szempontjából átlátszó. A felhasználók gyakran nem is tudják, hogy az általuk használt adatokat és alkalmazásokat helyileg vagy a hálózaton keresztül érik el.

A többfelhasználósság miatt a különböző felhasználók adatait külön kell tárolni. Garantálni kell a biztonságot és megbízhatóságot. Az adatok biztonsága már azelőtt is fontos probléma volt, hogy a számítógépeket hálózatokon keresztül összekapcsolták volna. Csakúgy, mint manapság, a legfontosabb szempont akkor is az volt, hogy az adatok akkor is rendelkezésre álljanak, ha az adathordozó – általában merevlemez – elveszett vagy másképp károsodott.

Ez a rész elsősorban a megbízhatósággal kapcsolatos témakörökre és a felhasználók személyiségi jogainak védelmére koncentrál, de nem hangsúlyozható eléggé, hogy egy átfogó biztonsági alapelvnek mindig tartalmaznia kell azokat az eljárásokat, amelyekkel garantálható, hogy rendszeresen frissített, működő és tesztelt biztonsági mentések legyenek kéznél. Enélkül nagyon nehéz az adatok visszanyerése – nemcsak hardverhiba esetén, hanem akkor is, ha az a gyanú merült fel, hogy valaki jogosulatlan hozzáférés birtokában belenyúlt a fájlokba.

38.1 Helyi és hálózati biztonság

Az adatok sokféleképp elérhetők:

- személyes kommunikáció révén olyan személyekkel, akik rendelkeznek a kívánt információval, vagy hozzáférnek egy számítógép adataihoz
- közvetlenül a számítógép konzoljáról (fizikai hozzáférés)
- soros vonalon keresztül
- hálózati kapcsolat segítségével

Ezen esetek mindegyikében a kérdéses erőforrások és adatok elérése előtt a felhasználót hitelesíteni kell. A webkiszolgálók kevésbé lehetnek korlátozók ebben a vonatkozásban, de továbbra sem kívánatos a személyes adatok nyilvánosságra hozatala.

A fenti lista első esete az, ahol a legtöbb felhasználói interakció történik; például, amikor kapcsolatba lép egy banki alkalmazottal, és bizonyítania kell, hogy Ön a bankszámla tulajdonosa. Ezután meg kell adnia egy aláírást, PIN-kódot vagy jelszót annak bizonyítására, hogy Ön valóban az, akinek állítja magát. Bizonyos esetekben lehet, hogy egyes adatok kicsalhatók egy tájékozott személytől azzal, hogy ügyesen előadva valami olyan szöveget, ami ismert információmorzsákat tartalmaz, elnyerik a bizalmát. Az áldozat lépésről-lépésre egyre több információt adhat ki, esetleg anélkül, hogy egyáltalán észrevenné azt. A hackerek ezt *social engineering* néven emlegetik. Ez ellen csak az emberek felvilágosításával, a nyelvhasználat és az információ tudatos kezelésével lehet védekezni. A számítógéprendszerekbe betörés előtt a támadók gyakran megpróbálják célba venni a recepciósokat, a vállalatnál dolgozó karbantartó személyzetet vagy akár a családtagokat. Az ilyen emberi kapcsolatokra épülő támadások sok esetben csak nagyon lassan derülnek ki.

A jogosulatlan adatelérésre vágyó személyek a hagyományos módszereket is kipróbálhatják, és megpróbálhatnak közvetlenül hozzáférni a hardvereszközökhöz. Éppen ezért a gépet mindenféle beavatkozás ellen érdemes védeni, hogy senki ne távolíthassa el, cserélhesse le vagy tehesse tönkre az alkatrészeit. Ez a biztonsági mentésekre, valamint a hálózati és tápkábelekre is vonatkozik. Biztonságossá kell tenni a rendszerindítási folyamatot is, mivel vannak olyan jól ismert billentyűkombinációk, amelyekkel furcsa eredmények érhetők el. Ez ellen a BIOS és a rendszertöltő jelszavának beállításával lehet védekezni.

Még mindig sok helyen használnak soros portokhoz csatlakozó soros terminálokat. A hálózati csatolókkal szemben ezeknek nincs szükségük hálózati protokollokra a gazdagéppel folytatott kommunikációhoz. Egy egyszerű kábelen vagy infravörös porton sima karakterek haladnak át az eszközök között. Az ilyen rendszerek leggyengébb pontja maga a kábel: egy erre csatlakoztatott régebbi nyomtatóval egyszerűen rögzíthető minden, amely a vezetékeken keresztülmegy. Ami egy nyomtató számára elérhető, az más módon is hozzáférhető, a támadásba fektetett erőfeszítéstől függően.

Egy fájl helyi gépen történő olvasásához más hozzáférési szabályokra van szükség, mint egy hálózati kapcsolat megnyitásához egy másik gépen futó kiszolgáló felé. Különbség van a helyi és a hálózati biztonság között. A határ ott húzódik, ahol a máshová küldendő adatokat csomagokba kell helyezni.

38.1.1 Helyi biztonsági beállítások

A helyi biztonság a gép helyének fizikai környezetével kezdődik. Olyan helyre telepítse a gépet, ahol a biztonság megfelel az elvárásoknak. A helyi biztonság fő célja a felhasználók elkülönítése, így a felhasználók nem szerezhetik meg a többiek jogosultságait és személyazonosságát. Ez egy általánosan betartandó szabály, de különösen igaz a `root` felhasználóra, aki a legfőbb jogokat gyakorolja a rendszeren. A `root` bármely helyi felhasználó azonosságát magára veheti jelszó megadása nélkül és elolvashatja bármelyik helyileg tárolt fájlt.

38.1.2 Jelszavak

A Linux-rendszereken a jelszavak természetesen nem nyílt szövegként kerülnek tárolásra és a beírt szöveges karaktersorozat sem egyszerűen csak össze van vetve az eltárolt mintával. Ha ez lenne a helyzet, akkor a rendszeren lévő minden fiók veszélybe kerülne, ha valaki hozzáférne a jelszófájlhoz. Ehelyett a jelszavak titkosítva tárolódnak, minden beíráskor újból titkosításra kerülnek, és a két titkosított karaktersorozat kerül összehasonlításra. Ez persze csak akkor nyújt nagyobb biztonságot, ha a titkosított jelszóból nem fejthető vissza az eredeti karaktersorozat.

Ez egy speciális algoritmussal érhető el, amelyet *csapóajtó (trapdoor) algoritmusnak* is hívnak, mivel csak egy irányba működik. A titkosított karaktersorozatot megszerző támadó hiába ismeri az algoritmust, nem tudja egyszerűen, az algoritmus alkalmazásával megszerezni a jelszót. Ehelyett az összes lehetséges karakterkombinációt ki kell próbálnia, amíg nem talál egy olyan kombinációt, ami titkosítva úgy néz ki, mint a jelszó.

Nyolc karakter hosszúságú jelszó esetén meglehetősen sok kombinációt kell kiszámoltatni.

A hetvenes években bizonyították, hogy ez a metódus a használt algoritmus viszonylagos lassúsága miatt sokkal biztonságosabb a többinél, mivel egy jelszó titkosítása eltart néhány másodpercig. Időközben azonban a PC-k teljesítménye eléggé megnövekedett ahhoz, hogy több százezer vagy millió titkosítást végezzenek másodpercenként. Éppen ezért ma már a normál felhasználók a titkosított jelszavakat sem láthatják (az `/etc/shadow` fájlt a normál felhasználók nem olvashatják). Ami még fontosabb, hogy a jelszavak ne legyenek egyszerűen kitalálhatók abban az esetben, ha a jelszófájl egy esetleges hiba miatt láthatóvá válik. Következésképpen nem túl hasznos például a „micimacko” jelszót „m@1c1m@ck0” értékre „lefordítani”.

A szó néhány betűjének hasonlóan kinéző számokkal való helyettesítése nem elég biztonságos. A szavak megfejtéséhez szótárakat használó jelszótörő-programok is alkalmaznak hasonló behelyettesítéseket. Jobb módszer egy olyan szó létrehozása, amelynek nincs általános jelentése; egy olyan szóé, ami csak az adott személy számára értelmes, például egy mondat szavainak vagy egy könyv címének első betűi, mint például Umberto Eco „A rózsa neve” című könyve. Ez az alábbi biztonságos jelszót adja: „U3Arn9”. Ezzel szemben a „borbarat” vagy „kati72” és hasonló jelszavakat egyszerűen kitalálhatja egy olyan személy, aki egy kicsit is ismeri a felhasználót.

38.1.3 A rendszerindítási folyamat

Állítsa be a rendszert úgy, hogy ne lehessen hajlékonylemezről vagy CD-ről elindítani: vagy azzal, hogy teljesen eltávolítja ezeket a meghajtókat, vagy azzal, hogy beállít egy BIOS-jelszót és megadja, hogy a rendszer csak merevlemezről indulhasson. A Linux-rendszert általában egy rendszertöltő indítja el, amely lehetőséget ad arra, hogy további paramétereket adjon át az elindított kernelnek. A `/boot/grub/menu.lst` fájlban (lásd: 15. fejezet - *A rendszertöltő* (201. oldal)) fájlban egy további jelszó beállításával akadályozza meg, hogy mások ilyen paramétereket adhassanak meg a rendszerindítás során. Ez kritikus fontosságú a rendszer biztonsága szempontjából. A kernel nemcsak hogy maga is `root` jogosultságokkal fut, de ő az első, aki a rendszerindítás során `root` jogosultságokat oszt ki.

38.1.4 Fájlengedélyek

Általános szabályként mindig a lehető legkorlátozottabb jogosultságokat kell használni az adott feladathoz. E-mail olvasásához vagy írásához például biztosan felesleges `root` jogosultság. Ha a levelezőprogramban hiba van, akkor ezt ki lehet használni egy olyan támadáshoz, amely pontosan azokkal a jogosultságokkal zajlik, mint amelyekkel a program rendelkezett induláskor. A fenti szabályt követve a lehető legkisebbre csökkenthető a potenciális kár.

Az openSUSE disztribúció fájljainak jogosultságát körültekintően kell megválasztani. A kiegészítő szoftvereket vagy egyéb fájlokat telepítő rendszeradminisztrátornak körültekintően kell eljárnia, különösen a jogosultságbitek beállításakor. A tapasztalt és a biztonságot szem előtt tartó rendszeradminisztrátorok mindig a `-l` paraméterrel használják az `ls` parancsot, és egy bővebb fájllistát jelenítenek meg, amelyben azonnal észlelhetők a nem megfelelő fájljogosultságok. Egy nem megfelelő fájlattribútum nemcsak azt jelenti, hogy a fájlok módosíthatók vagy törölhetők. Ezeket a módosított fájlokat a `root` felhasználó hajthatja végre, illetve konfigurációs fájlok esetén a programok az ilyen fájlokat `root` jogosultságokkal használhatják. Ez jelentősen növeli egy támadó esélyeit. Az ilyen támadásokat kakukktojásoknak (cuckoo eggs) hívják, mivel a programot (a tojást) egy másik felhasználó (madár) hajtja végre (költi ki) hasonlóan ahhoz, ahogy a kakukk másik madarat vesz rá, hogy költse ki a tojásait.

Az openSUSE rendszer a következő fájlokat tartalmazza az `/etc` könyvtárban: `permissions`, `permissions.easy`, `permissions.secure` és `permissions.paranoid`. Ezeknek a fájloknak az a célja, hogy speciális jogosultságokat határozzanak meg, például bárhonnan írható könyvtárakat, vagy fájlok esetében megadják a set user ID bitet (a set user ID bittel rendelkező programok nem az ezeket elindító felhasználó jogosultságaival futnak, hanem a fájl tulajdonosának – a legtöbb esetben a `root` felhasználónak a jogosultságaival). Az adminisztrátor az `/etc/permissions.local` fájl segítségével saját beállításokat adhat meg.

Annak meghatározásához, hogy az openSUSE konfigurációs programjai melyik fenti fájlokat használják a megfelelő jogosultságok beállításához, válassza ki a YaST szoftver *Biztonság és felhasználók* menüjének *Helyi biztonság* menüpontját. A témakörrel kapcsolatos további információt az `/etc/permissions` megjegyzései és a `chmod` kézikönyvoldala (`man chmod`) tartalmaz.

38.1.5 Puffertúlcsordulások és formátum-karaktersorozat hibák

Különleges körültekintéssel kell eljárni, amikor a programnak olyan adatokat kell feldolgoznia, amelyet a felhasználó módosíthat vagy módosíthatott, de ez inkább az alkalmazásprogramozó problémája, mint a normál felhasználóké. A programozónak vigyáznia kell arra, hogy az alkalmazás megfelelően értelmezze az adatokat, ne történhessen meg, hogy az adatok tárolásához túl kicsi memóriaterületekre ír. A programnak is következetes módon kell átadnia az adatokat az erre a célra meghatározott felületeken keresztül.

Puffertúlcsordulás akkor történhet, ha a memóriapuffer aktuális mérete a pufferbe íráskor nem kerül figyelembevételre. Ez olyan esetekben fordul elő, amikor a felhasználó által előállított adat több területet használ fel, mint amennyi a pufferben rendelkezésre áll. Ennek eredményeképp az adatok a pufferterület végén túlra íródnak, ami bizonyos körülmények között lehetővé teszi, hogy a program a felhasználói adatok egyszerű feldolgozása helyett a felhasználó (és nem a programozó) által befolyásolt programkódot hajtson végre. Az ilyen típusú hibáknak komoly következményei vannak, különösen akkor, ha a program speciális jogosultságokkal kerül végrehajtásra (lásd: 38.1.4. - Fájlengedélyek (593. oldal)).

A *formátum-karaktersorozat hibák* némileg eltérő módon működnek, de ez ismét egy olyan felhasználói bemenet, amely rossz irányba viszi a programot. A legtöbb esetben ezek a programozási hibák a speciális jogosultságokkal rendelkező programok – a setuid és setgid programok – esetén kerülnek kihasználásra. Ez szintén azt jelenti, hogy az adatok és a rendszer úgy védhetők az ilyen hibák ellen, hogy a megfelelő jogosultságokat megvonják a programokról. A legjobb módszer a lehető legalacsonyabb szintű jogosultságok alkalmazása (lásd: 38.1.4. - Fájlengedélyek (593. oldal)).

Mivel a puffeltúlcsordulások és a formátum-karaktersorozat hibák a felhasználói adatok kezelésével kapcsolatos hibák, nemcsak akkor használhatók ki, ha egy helyi fiók rendelkezik hozzáféréssel. A jelentett hibák nagy része egy hálózati kapcsolaton keresztül is kihasználható. Ennek megfelelően a puffertúlcsordulásokat és formátum-karatersorozat hibákat úgy kell osztályozni, hogy a helyi és a hálózati biztonság szempontjából is lényegesek.

38.1.6 Vírusok

Szemben azzal, amit néhányan mondanak, vannak Linuxon futó vírusok is. Az ismert vírusokat a szerzők *az elv igazolásaként* készítették, bizonyítva, hogy az alkalmazott technika valóban működik. Eddig e vírusok egyike sem *szabadult még el*.

A vírusok nem maradhatnak életben és nem terjedhetnek olyan gazdarendszer nélkül, amelyeken megtelepedhetnének. A mi esetünkben a gazdarendszer lehet egy program vagy a rendszer egy fontos tárolóterülete, mint például a master boot rekord, amelynek a vírus programkódja számára írhatónak kell lennie. A többfelhasználósság miatt a Linux az írási hozzáférést bizonyos fájlok esetén korlátozhatja. Ez különösen a rendszerfájlok esetén fontos. Ha a szokásos munkát `root` jogosultságokkal végzi, akkor megnöveli annak esélyét, hogy a rendszert vírus fertőzze meg. Ha ezzel szemben a fent említett lehető legalacsonyabb jogosultságok alapelvét követi, akkor a vírusfertőzés esélye kicsi.

Nem érdemes továbbá olyan internetes forrásból programot telepíteni, amelyet nem ismer igazán. Az openSUSE RPM csomagjai kriptográfiai aláírást tartalmaznak, így afféle digitális címkék formájában jelzik, hogy a csomagok a megfelelő gondossággal lettek elkészítve. A vírusok megjelenése tipikus jele annak, hogy az adminisztrátor vagy a felhasználó nem rendelkezik a szükséges biztonsági ismeretekkel és veszélyezteti a rendszert, amelyet a tervezés legelső lépésétől kezdve nagyon biztonságossá kell tenni.

A vírusokat nem szabad összekeverni a férgekkel (worm), amelyek teljes mértékben a hálózatok világához tartoznak. A férgek terjedéséhez nincs szükség gazdagépre.

38.1.7 Hálózati biztonság

A hálózati biztonság kialakítása fontos, hogy védettek legyünk a kívülről indított támadásokkal szemben. A felhasználó hitelesítéséhez felhasználónevet és jelszót bekérő szokásos bejelentkezési folyamat továbbra is helyi biztonsági kérdés. Abban a speciális esetben, amikor a bejelentkezés hálózaton keresztül történik, meg kell különböztetni a két biztonsági aspektust. A tényleges hitelesítésig történő dolgok a hálózati biztonság tárgykörébe tartoznak, ami pedig utána következik, az már a helyi biztonságéba.

38.1.8 X Window rendszer és X hitelesítés

Ahogy már az elején is szó volt róla, a hálózat átlátszósága a UNIX rendszer egyik központi jellemzője. A UNIX operációs rendszer ablakkezelő rendszere, az X igen látványosan képes ezt a funkciót kihasználni. X használata esetén teljesen normális dolog bejelentkezni egy távoli gépen és elindítani egy grafikus programot, amely azután adatokat küld át a hálózaton, amelyek megjelennek a saját gépünkön.

Amikor az X klienst távolról kell megjeleníteni egy X kiszolgáló segítségével, a kiszolgálónak meg kell védenie az általa kezelt erőforrást (azaz a megjelenítőt) a hitelesítés nélküli eléréstől. Konkrétabban: a kliensprogram számára meg kell adni bizonyos jogosultságokat. X Window rendszerrel ez kétféleképpen hajtható végre; a két módszer neve gép alapú hozzáférés-vezérlés és cookie alapú hozzáférés-vezérlés. Az előbbi annak a gépnek az IP-címére épül, amelyen a kliensnek futnia kell. Ezt az xhost program vezérli. Az xhost megadja egy legális kliens IP-címét az X kiszolgálóhoz tartozó kis adatbázisban. Az IP-cím alapú hitelesítés azonban nem túl biztonságos. Ha például egy második felhasználó is használja a kliensprogramot küldő gépet, akkor ez a felhasználó az X kiszolgálóhoz is hozzáférhet – ugyanúgy, mint az, aki ellopja az IP-címet. E hibák miatt ez a hitelesítési mód nem is kerül részletesebben leírásra itt, de a `man xhost` parancs használatával többet is megtudhat róla.

Cookie alapú hozzáférés-vezérlés esetén a rendszer létrehoz egy karaktersorozatot, amelyet csak az X kiszolgáló és a jogosult felhasználó ismer – ez olyan, mint valami azonosítókártya. Ez a cookie (a szó nem a szokásos sütikből ered, hanem a kínai szerencsesütikből, amelyek mindegyike egy mondást tartalmaz) a felhasználó saját könyvtárában található `.Xauthority` fájlban kerül tárolásra, és minden X kliens számára rendelkezésére áll, amely az ablak megjelenítéséhez az X kiszolgáló használatára vár. A felhasználó az xauth eszköz segítségével megjelenítheti a `.Xauthority fájlt`. Ha átnevezte a `.Xauthority` fájlt vagy véletlenül törölte a saját könyvtárból, akkor nem nyithatók meg új ablakok és X kliensek.

Az SSH (secure shell) segítségével a hálózati kapcsolat teljesen titkosítható és átlátszó módon továbbítható egy X kiszolgálóhoz anélkül, hogy a felhasználó észrevenné a titkosítási mechanizmust. Ezt X továbbításnak (X forwarding) is nevezik. Az X továbbítás a kiszolgálóoldalon egy X kiszolgáló szimulálásával, a távoli gépen pedig egy DISPLAY környezeti változó beállításával valósítható meg. Az SSH-val kapcsolatban további részletek: 34. fejezet - *SSH: Biztonságos hálózati műveletek* (545. oldal).

FIGYELEM

Ha azt a gépet, amelyre bejelentkezett, nem tekinti biztonságosnak, akkor ne használjon X továbbítást. Engedélyezett X továbbítással egy támadó az SSH-kapcsolaton keresztül hitelesítheti magát az X kiszolgálóra, és ha már behatolt, akkor figyelheti például a billentyűzetbemenetet.

38.1.9 Puffertúlcsordulások és formátum-karaktersorozat hibák

Amint már szó esett róla (38.1.5. - Puffertúlcsordulások és formátum-karaktersorozat hibák (594. oldal)), a puffertúlcsordulásokat és formátum-karaktersorozat hibákat a helyi és hálózati biztonságot is érintőként kell kezelni. Hasonlóan az ilyen hibák helyi változataihoz, a hálózati programok puffertúlcsodulásait sikeresen kihasználók általában `root` jogosultságokat igyekeznek szerezni. Még ha nem is ez a helyzet, egy támadó akkor is kihasználhatja a hibát arra, hogy megszerezze egy nem kiváltságos felhasználói fiók elérését a rendszeren esetleg előforduló egyéb gyenge pontok kiaknázására.

A hálózati kapcsolaton keresztül kihasználható puffertúlcsordulások és formátum-karaktersorozat hibák a távoli támadások leggyakoribb formái. Ezek kihasználásának módjai – az újonnan megtalált biztonsági lyukakat kihasználó programok – gyakran felkerülnek a biztonsági levelezési listákra. Ezek segítségével a gyenge pont a kód részleteinek ismerete nélkül is célba vehető. Az évek során a tapasztalat azt mutatta, hogy a hibákat kihasználó kódok elérhetősége szerepet játszott a még biztonságosabb operációs rendszerek kifejlesztésében, nyilvánvalóan azzal, hogy az operációs rendszerek készítői kényszerítve voltak a szoftvereikban található hibák kijavítására. Szabad szoftver esetén bárki hozzáférhet a forráskódhoz (az openSUSE programot az összes rendelkezésre álló forráskóddal együtt adják ki) és bárki, aki gyenge pontot és ezt kihasználó kódot talál, javítást küldhet a megfelelő hiba kijavításához.

38.1.10 DoS – szolgáltatás megbénítása (Denial of Service)

Az ilyen támadás célja egy kiszolgálóprogram vagy egy teljes kiszolgáló blokkolása, ami többféle módon érhető el: a kiszolgáló túlterhelése, illetve leterhelve tartása rossz csomagokkal; vagy egy távoli puffertúlcsordulás kihasználása. A DoS támadások

egyetlen célja legtöbbször a szolgáltatás kiiktatása. Ha egy adott szolgáltatás elérhetetlenné válik, akkor a kommunikáció sebezhető lesz a *köztes támadásokkal* (lehallgatás, TCP-kapcsolat eltérítése, hamisítás), valamint a DNS-hamisítással szembe.

38.1.11 Köztes támadások: lehallgatás, eltérítés, hamisítás

Általában minden olyan távoli támadást *köztes támadásnak* hívunk, amikor a támadó a kommunikáló gépek közé áll. Majdnem minden köztes támadásra jellemző, hogy az áldozat általában észre sem veszi, hogy valami történik. Számos különböző változat létezik, például a támadó elfoghat egy kapcsolatkérést és maga továbbíthatja a célgép számára. Ezután az áldozat tudtán kívül kapcsolatot teremt egy rossz géppel, mivel a másik végpont átveszi a legális célgép helyét.

A köztes támadás legegyszerűbb formáját *lehallgatásnak* (sniffing) hívják– a támadó „csak" figyeli az átmenő hálózati forgalmat. Összetettebb támadás, ha a „köztes" támadó egy már felépített kapcsolatot próbál meg átvenni (eltérítés). Ehhez a támadónak elemeznie kell egy ideig a csomagokat, hogy meg tudja jósolni a kapcsolathoz tartozó TCP-sorozatszámokat. Amikor a támadó végül átveszi a célgép szerepét, az áldozat észreveszi, mivel hibaüzenetet kap, amely jelzi, hogy a kapcsolat hiba miatt megszakadt. Az eltérítéssel szemben titkosítással nem védett protokollok, amelyek csak egy egyszerű hitelesítési eljárást hajtanak végre a kapcsolat létrehozásakor, leegyszerűsítik a támadók dolgát.

A *hamisítás* (spoofing) egy olyan támadás, amelyben a csomagok módosításra kerülnek, hogy hamis forrásadatokat (legtöbbször IP-címet) tartalmazzanak. A támadás aktívabb formái ilyen hamis csomagok küldésére épülnek – ilyet Linux-gépen csak az adminisztrátor (a `root`) tehet.

Az említett támadások nagy részét DoS támadással együtt hajtják végre. Ha egy támadó lehetőséget lát arra, hogy egy adott gépet váratlanul leterheljen – hacsak egy rövid időre is – akkor ez egyszerűbbé teszi számára egy aktív támadás végrehajtását, mivel a gép egy ideig nem tud beavatkozni a támadásba.

38.1.12 DNS-hamisítás

A DNS-hamisítás azt jelenti, hogy a támadó módosítja a DNS-kiszolgáló gyorsítótárát azáltal, hogy hamisított DNS-válaszcsomagokkal válaszol és megpróbálja rábírni a kiszolgálót bizonyos adatok küldésére a kiszoltálótól információt kérő áldozatnak. Számos kiszolgáló IP-címek vagy gépnevek alapján bizalmi kapcsolatokat tart fenn más gépekkel. A támadónak jól kell ismernie a gépek közötti bizalmi kapcsolat tényleges felépítését ahhoz, hogy magát megbízható gépnek álcázza. A támadó a szükséges információ megszerzéséhez általában elemez a kiszolgálótól kapott néhány csomagot. A támadónak gyakran egy jól időzített DoS támadást kell indítania a névkiszolgálón is. Védekezzen ez ellen úgy, hogy csak titkosított kapcsolatokat használ, amelyek képesek ellenőrizni a túloldali gépnek az azonosságát.

38.1.13 Férgek

A férgeket (worm) általában keverik a vírusokkal, pedig a kettő között világos különbség van. A vírusokkal ellentétben a férgeknek a működéshez nem kell megfertőzniük a gép valamely programját. Ehelyett arra specializálódtak, hogy a lehető leggyorsabban terjedjenek a hálózati struktúrákban. A régebben megjelent férgek, mint például a Ramen, a Lion vagy az Adore, a kiszolgálóprogramok – például bind8 vagy lprNG – jól ismert biztonsági réseit használják ki. A férgek elleni védekezés viszonylag könnyű. Mivel a biztonsági rés felfedezése és a féreg támadása között eltelik egy kis idő, jó esély van arra, hogy az érintett program frissített változata időben megjelenjen. Ez csak akkor hasznos, ha az adminisztrátor a kérdéses rendszeren valóban telepíti a biztonsági frissítéseket.

38.2 Néhány általános biztonsági tipp és trükk

A biztonság megfelelő kezelése érdekében figyelemmel kell kísérni az új fejlesztéseket és ismerni kell a legfrissebb biztonsági problémákat. A rendszer mindenfajta problémák elleni védelmének egyik lehetséges módja a biztonsági közlemények által javasolt frissítési csomagok lehető leggyorsabb telepítése. A SUSE biztonsági bejelentéseit a `opensuse-security-announce@opensuse.org` listán teszik közzé. A listán első kézből értesülhet a frissítési csomagokkal kapcsolatos tudnivalókról és a SUSE

biztonsági csoportjának tagjai is az aktív listatagok között vannak. A listára a http://en.opensuse.org/Communicate/Mailinglists oldalon lehet előfizetni.

A opensuse-security@opensuse.org levelezési lista kiváló hely bármilyen biztonsági kérdés felvetésére. Erre ugyanazon a weboldalon lehet feliratkozni.

A bugtraq@securityfocus.com a világ egyik legismertebb biztonsági listája. Ajánljuk a lista olvasását (naponta körülbelül 15-20 levél érkezik). További információ: http://www.securityfocus.com.

Az alábbi szabálylista az alapszintű biztonsági megfontolások kezeléséhez nyújt hasznos segítséget:

- A mindennapos feladatok lehető legkorlátozottabb jogosultsággal való elvégzését előíró szabálynak megfelelően a rendszeres feladatokat ne `root` felhasználóként hajtsa végre. Ez csökkenti a kakukktojások és vírusok saját hiba miatti érkezését.
- Ha lehetséges, akkor mindig titkosított kapcsolatot alkalmazzon egy távoli gép használatához. `telnet`, `ftp`, `rsh` és `rlogin` helyett mindig érdemes az `ssh`-t (secure shell) használni.
- Kerülje a csak IP-címekre épülő hitelesítési módszerek használatát.
- A hálózattal kapcsolatos legfontosabb csomagokból mindig telepítse a legfrissebb változatot és jelentkezzen fel a megfelelő levelezési listákra, hogy értesüljön a megfelelő programok (bind, sendmail, ssh stb.) új verzióiról. Ugyanez igaz a helyi biztonság szempontjából fontos szoftverekre is.
- A rendszer biztonsága szempontjából kritikus fontosságú fájlok jogosultságainak optimalizálása érdekében módosítsa az `/etc/permissions` fájlt. Ha eltávolította egy programról a setuid bitet, akkor elképzelhető, hogy nem tudja a kívánt módon végrehajtani a feladatát. Cserébe viszont a program nem jelent további biztonsági kockázatot. Hasonló megközelítés alkalmazható a mindenki számára írható könyvtárak és fájlok esetében is.
- A kiszolgáló működéséhez nem elegendhetetlenül szükséges hálózati szolgáltatásokat tiltsa le. Ez biztonságosabbá teszi a rendszert. A LISTEN socket állapottal rendelkező nyitott portok a `netstat` programmal kereshetők meg. Ami a paramétereket illeti, érdemes a `netstat -ap` vagy `netstat -anp` formában használni

a parancsot. A `-p` opció lehetővé teszi annak megtekintését, hogy melyik eljárás milyen néven foglal le portot.

Hasonlítsa össze a `netstat` eredményeit azzal, amelyet egy, a gépen kívülről kezdeményezett portelemzés eredményez. E feladatra megfelelő program az `nmap`, amely nem csak a gép portjait ellenőrzi, hanem ebből következtet is arra, hogy mely szolgáltatások várnak ezek mögött. A portelemzés azonban agresszív cselekedet is lehet, így ne hajtsa végre olyan gépen, ahol az adminisztrátor kifejezetten nem hagyta jóvá. Végül ne feledje el, hogy nem csak a TCP-portokat kell elemezni, hanem az UDP-portokat is (`-sS` és `-sU` paraméter).

- A rendszer fájlintegritásának megbízható módon történő megfigyeléséhez használja az openSUSE `AIDE` (Advanced Intrusion Detection Environment) programját. Titkosítsa az AIDE által létrehozott adatbázist a módosítás megakadályozásához. A gépen kívül, egy hálózatra nem csatlakoztatott adathordozón tartson fenn az adatbázisról egy biztonsági másolatot.

- Harmadik féltől származó szoftver telepítésekor megfelelő körültekintéssel járjon el. Előfordult már, hogy egy cracker egy trójai programot épített be a biztonsági szoftvercsomag tar archív állományába, de ezt szerencsére gyorsan észrevették. Ha kétségei vannak egy adott webhellyel kapcsolatban, ne telepítse az onnan letöltött bináris csomagokat.

  A SUSE RPM csomagjai gpg-aláírással vannak ellátva. A SUSE által az aláíráshoz használt kulcs:

  ```
  ID:9C800ACA 2000-10-19 SUSE Package Signing Key <build@suse.de>
  Key fingerprint = 79C1 79B2 E1C8 20C1 890F 9994 A84E DAE8 9C80 0ACA
  ```

  Az `rpm --checksig package.rpm` parancs megmutatja, hogy az eltávolított csomag aláírása és ellenőrzőösszege helyes-e. A kulcs a disztribúció első CD-jén és a legtöbb kulcskiszolgálón megtalálható.

- Rendszeres időközönként ellenőrizze a felhasználók és a rendszerfájlok biztonsági mentéseit. Gondoljon arra, hogyha nem ellenőrzi, hogy a mentés működik-e, akkor az lehet, hogy teljesen értéktelen.

- Ellenőrizze a naplófájlokat. Hacsak lehetséges, írjon egy kis parancsfájlt a gyanús bejegyzések megkereséséhez. Ez kétségkívül nem egyszerű feladat. A végén csak azt tudhatja, hogy mely bejegyzések szokatlanok és melyek nem.

- A `tcp_wrapper` segítségével korlátozhatja a gépen futó egyedi szolgáltatások elérését, így explicit módon vezérelheti, hogy melyik IP-címek csatlakozhatnak egy szolgáltatáshoz. A `tcp_wrapper`-rel kapcsolatos további információrt tekintse meg a tcpd és hosts_access kézikönyvoldalát (`man 8 tcpd`, `man hosts_access`).

- A SuSEfirewall segítségével javítható a `tcpd`által kínált biztonság (`tcp_wrapper`).

- A biztonsági intézkedéseket redundánsra tervezze: a kétszer megjelenő üzenet jobb, mintha nincs üzenet.

- Ha lemezre felfüggesztést használ, akkor érdemes megfontolni a felfüggesztés során kiírt rendszerkép titkosítását a `configure-suspend-encryption.sh` parancsfájllal. A program létrehozza a kulcsot, átmásolja az `/etc/suspend.key` fájlba, majd átírja az `/etc/suspend.conf` fájlt, hogy használjon titkosítást a felfüggesztés során kiírt adatoknál.

38.3 Központi biztonsági jelentési cím használata

Biztonsággal kapcsolatos problémák észlelése esetén (először ellenőrizze a rendelkezésre álló frissítési csomagokat) írjon egy e-mailt az alábbi címre: `security@suse.de`. Adja meg a probléma részletes leírását és az érintett csomag verziószámát. A SUSE mindent megtesz, hogy a lehető leggyorsabban válaszoljon. Az e-mail üzeneteket bátran titkosítsa pgp segítségével. A SUSE pgp kulcsa az alábbi:

```
ID:3D25D3D9 1999-03-06 SUSE Security Team <security@suse.de>
Key fingerprint = 73 5F 2E 99 DF DB 94 C4 8F 5A A3 AE AF 22 F2 D5
```

Ez a kulcs a `http://www.novell.com/linux/security/securitysupport.html` címről is letölthető.

39 Súgó és dokumentáció

Az openSUSE számos információs és dokumentációs forrást kínál, amelyek közül számos megtalálható a telepített rendszeren:

Dokumentáció az `/usr/share/doc` könyvtárban
: Ez a hagyományos súgókönyvtár számos különféle dokumentációs fájlt tartalmaz, valamint a rendszer kiadási megjegyzéseit. További, részletes információ: 39.1. - Dokumentációkönyvtár (604. oldal).

Kézikönyvoldalak (man) és info oldalak a parancsértelmező parancsairól
: Amikor a parancsértelmezőt használja, nincs szükség arra, hogy minden parancs minden paraméterét fejből tudja. A parancsértelmező hagyományosan kínál beépített segítséget a kézikönyvoldalak és az info oldalak formájában. További részletek a 39.2. - Kézikönyvoldalak (man) (606. oldal) és 39.3. - Információs oldalak (607. oldal) részekben olvashatók.

Asztali rendszerek súgóközpontjai
: A KDE és a GNOME súgóközpontjai (a KDE help center, illetve a Yelp) központi, jól kereshető elérést kínálnak a rendszer legfontosabb dokumentációs erőforrásaihoz. Ide tartoznak a telepített alkalmazások online súgói, a kézikönyvoldalak, az info oldalak, valamint a termék mellé kapott Novell/SUSE kézikönyvek.

Egyes alkalmazások saját súgócsomagjai
: Amennyiben új szoftvert telepít a YaST segítségével, a legtöbb esetben a szoftverdokumentáció is automatikusan telepítésre kerül, és rendszerint megjelenik az asztal segítségnyújtó rendszerében. Néhány más alkalmazás ellenben (például a The GIMP) más típusú online súgócsomagokat tartalmaz, amelyet a(z) YaST alkalmazástól függetlenül kell telepíteni és nem részei a súgócentrumnak.

39.1 Dokumentációkönyvtár

Hagyományosan a könyvtár, amelyben a telepített Linux-rendszeren a dokumentáció megtalálható, az `/usr/share/doc`. Ez a könyvtár általában a rendszeren telepített csomagokkal kapcsolatos információt, kiadási megjegyzéseket, kézikönyveket és sok más egyebet tartalmaz.

MEGJEGYZÉS: A tartalom függ a telepített csomagoktól

A Linux-világban számos kézikönyv és más dokumentáció szintén csomagok formájában érhető el, csakúgy, mint a programok. Az, hogy mennyi és milyen információ található az `/usr/share/docs` könyvtárban, a telepített(dokumentációs) csomagoktól is függ. Ha az itt említett alkönyvtárak hiányoznának, akkor ellenőrizze, hogy a megfelelő csomagok telepítve lettek-e a rendszeren, és ha nem, akkor telepítse őket a YaST-tal.

39.1.1 Novell/SUSE kézikönyvek

A könyvek HTML- és PDF-változatban is hozzáférhetők, különféle nyelveken. A `manual` alkönyvtárban a termékhez kapcsolódó Novell/SUSE kézikönyvek többsége elérhető HTML formátumban. A termékhez kapcsolódó dokumentációról a kézikönyvek előszavából kaphat áttekintést.

Ha egynél több nyelvet telepített, akkor az `/usr/share/doc/manual` könyvtárban lehet, hogy a kézikönyvek is több nyelven szerepelnek. A Novell/SUSE kézikönyvek HTML-változatai szintén megtalálhatók mindkét asztali környezet súgóközpontjaiban. Azzal kapcsolatban, hogy hol találja a könyvek PDF- és HTML-változatait a telepítési adathordozón, forduljon az openSUSE Kiadási megjegyzéseihez. Ezek a telepített rendszeren az `/usr/share/doc/release-notes/` fájlban, vagy online a `http://www.novell.com/documentation/` címen, a termékhez tartozó weboldalon találhatók.

39.1.2 Feladatleírások (HOWTO)

Ha a `howto` csomag telepítve van a rendszeren, akkor az `/usr/share/doc` alatt található egy `howto` alkönyvtár is, ahol további dokumentumok találhatók a Linux-szoftverek telepítésének és üzemeltetésének számos feladatáról.

39.1.3 Csomagdokumentáció

A `packages` könyvtárban találhatók azok a dokumentumok, amelyek a rendszeren telepített szoftvercsomagok részei. Minden csomaghoz létrejön egy `/usr/share/doc/packages/`*csomagnév* alkönyvtár. Ebben gyakran találhatók a csomaggal kapcsolatos README fájlok, néha példák, konfigurációs fájlok vagy kiegészítő parancsfájlok. Az alábbi listában az `/usr/share/doc/packages` könyvtárban jellemzően előforduló fájlok láthatók. A bejegyzések egyike sem kötelező azonban, és sok csomag csak néhányat tartalmaz közülük.

`AUTHORS`
: A fő fejlesztők listája.

`BUGS`
: Ismert hibák vagy hibás működés. Tartalmazhat egy hivatkozást egy Bugzilla weboldalra, ahol kereshet az összes hiba között.

`CHANGES , ChangeLog`
: Az egyes verziók közötti változások összefoglalása. Általában fejlesztők számára érdekes, mert nagyon részletes.

`COPYING , LICENSE`
: Licencadatok.

`FAQ`
: Levelezőlistákról vagy hírcsoportokból összegyűjtött kérdések és válaszok.

`INSTALL`
: A csomag telepítésének leírása. Mivel amikorra ezt a fájlt olvassa, a csomag már telepítve van, ennek a fájlnak a tartalma nyugodtan figyelmen kívül hagyható.

`README`, `README.*`
: Általános információ a szoftverről, például hogy mire szolgál és hogyan kell használni.

`TODO`
: Olyan funkciók, amelyek egyelőre még nincsenek megvalósítva, de a jövőben várhatóan meg lesznek.

`MANIFEST`
: A fájlok jegyzéke, rövid összefoglalóval.

`NEWS`
: Az adott verzió újdonságainak leírása.

39.2 Kézikönyvoldalak (man)

A kézikönyvoldalak (man) a Linux-rendszer nélkülözhetetlen részei. Elmagyarázzák a parancsok használatát, valamint információt adnak az összes rendelkezésre álló beállításról és paraméterről. A kézikönyvoldalak megjelenítéséhez írja be, hogy `man`, mögötte a parancs nevével, tehát például `man ls`.

A kézikönyvoldalak közvetlenül a parancsértelmezőben jelennek meg. A bennük való fel- és lefelé mozgáshoz használja a Page ↑ és Page ↓ billentyűket. A dokumentum elejére, vagy végére a Home és End billentyűkkel lehet ugrani. A megtekintési módból a Q megnyomásával léphet ki. A `man` parancsról magáról is kérhető információ: írja be, hogy `man man`. A kézikönyvoldalak kategóriákba vannak sorolva, ahogy az a következő helyen látható: 39.1 táblázat - Man oldalak – Kategóriák és leírások (607. oldal) (részlet a man program man oldalából).

39.1. táblázat *Man oldalak – Kategóriák és leírások*

Szám	Leírás
1	Végrehajtandó programok vagy parancsok
2	Rendszerhívások (a kernel által nyújtott szolgáltatások)
3	Könyvtárhívások (a programkönyvtárakon belüli funkciók)
4	Speciális fájlok (általában a `/dev` alatt találhatók)
5	Fájlformátumok és konvenciók (`/etc/fstab`)
6	Játékok
7	Vegyes (makrócsomagok és konvenciók), például man(7), groff(7)
8	Rendszeradminisztrációs parancsok (általában csak a `root` számára;)
9	Kernelrutinok (nem szabványos)

Minden kézikönyvoldal több részből áll, ezek címkéje *NAME*, *SYNOPSIS*, *DESCRIPTION*, *SEE ALSO*, *LICENSING* és *AUTHOR* . A parancs fajtájától függően további kiegészítő részek is lehetnek.

39.3 Információs oldalak

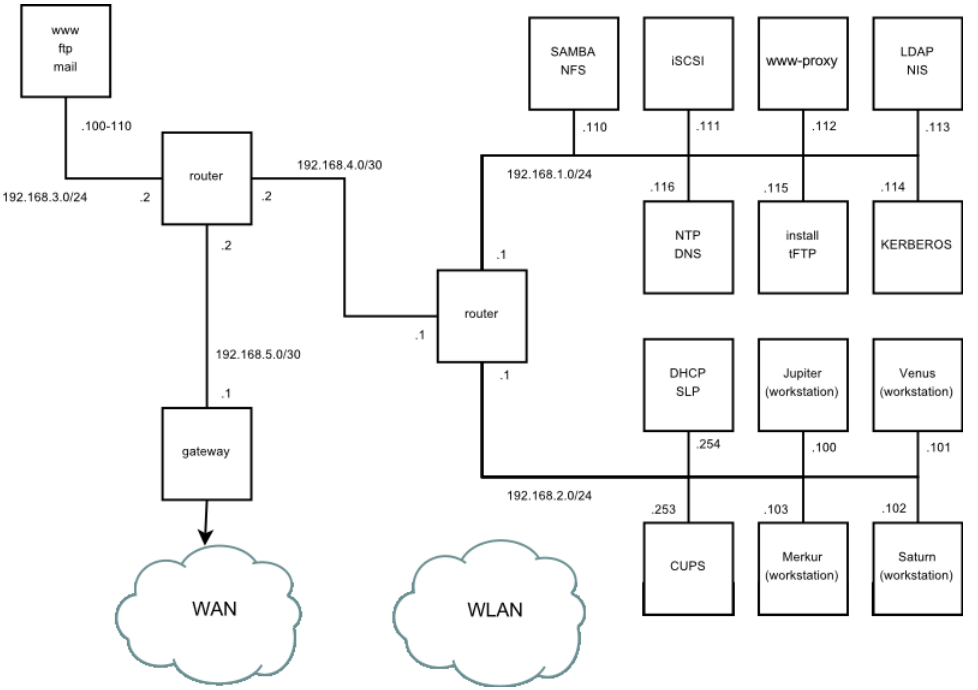
Az információs oldalak is fontos információforrásnak számítanak a rendszeren belül. Általában bővebb információt adnak, mint a kézikönyvoldalak. Egy adott parancs info oldalának megjelenítéséhez írja be, hogy `info`, utána a parancs nevével, tehát például `info ls`. Az info oldalakat és annak egyes részeit, az úgynevezett „csomópontokat” (node) közvetlenül a parancsértelmezőben tekintheti meg egy megjelenítő programmal. A Szóköz billentyűvel léphet előre és a <— billentyűvel visszafelé. Egy adott csomóponton belül tallózhat a Page ↑ és Page ↓ billentyűkkel is, de csak a Szóköz és <— viszi

át az előző ill. következő csomópontra. A megjelenítőből a Q megnyomásával léphet ki. Nem minden kézikönyvoldalhoz tartozik info oldal és fordítva.

A

Egy példahálózat

Ezt a példahálózatot használjuk az openSUSE összes hálózattal kapcsolatos dokumentációjában.



GNU licencek

B

Ez a függelék a GNU Általános közzétételi feltételeit és a GNU szabad dokumentációs licencet tartalmazza.

GNU General Public License (GPL)

http://www.gnu.org/licenses/old-licenses/gpl-2.0.html

Előszó

A legtöbb szoftver licencei azzal a szándékkal készültek, hogy minél kevesebb lehetőséget adjanak a szoftver megváltoztatására és terjesztésére. Ezzel szemben a GNU GPL célja, hogy garantálja a szabad szoftver másolásának és terjesztésének szabadságát, ezáltal biztosítva a szoftver szabad felhasználhatóságát minden felhasználó számára. A GPL szabályai vonatkoznak a Free Software Foundation legtöbb szoftverére, illetve minden olyan programra, melynek szerzője úgy dönt, hogy ezt használja a szerzői jog megjelölésekor. (A Free Software Foundation egyes szoftvereire a GNU LGPL érvényes.) Bárki használhatja a programjaiban a GPL-t a szerzői jogi megjegyzésnél.

A szabad szoftver megjelölés nem jelenti azt, hogy a szoftvernek nem lehet ára. A GPL licencek célja, hogy garantálja a szabad szoftver másolatainak szabad terjesztését (és e szolgáltatásért akár díj felszámítását), a forráskód elérhetőségét, hogy bárki szabadon módosíthassa a szoftvert, vagy felhasználhassa a részeit új szabad programokban; és hogy mások megismerhessék ezt a lehetőséget.

A szerző jogainak védelmében korlátozásokat kell hozni, amelyek megtiltják, hogy bárki megtagadhassa ezeket a jogokat másoktól, vagy ezekről való lemondásra kényszeritsen bárki mást. Ezek a megszorítások bizonyos felelősségeket jelentenek azok számára, akik a szoftver másolatait terjesztik vagy módosítják.

Ha valaki például ilyen program másolatait terjeszti, akár ingyen vagy bizonyos összeg fejében, a szoftverre vonatkozó minden jogot tovább kell adnia a fogadó feleknek. Biztosítani kell továbbá, hogy megkapják vagy legalábbis megkaphassák a forráskódot is. És persze ezeket a licencfeltételeket is el kell juttatni, hogy tisztában legyenek a jogaikkal.

A jogok védelme két lépésből áll: (1) a szoftver szerzői jogainak védelméből és (2) a jelen licenc biztosításából, amely jogalapot biztosít a szoftver másolására, terjesztésére és/vagy módosítására.

Az egyes szerzők és a magunk védelmében biztosítani akarjuk, hogy mindenki megértse: a jelen szabad szoftverre nincs jótállás. Ha a szoftvert módosították és továbbadták, akkor mindenkinek, aki a módosított változatot kapja, tudnia kell, hogy az nem az eredeti, így a mások által okozott hibáknak nem lehet hatása az eredeti szerző hírnevére.

Végül, a szabad szoftver létét állandóan fenyegetik a szoftverszabadalmak. El szeretnénk kerülni annak veszélyét, hogy a szabad program terjesztői szabadalmat jegyezhessenek be rá, ezáltal saját szellemi tulajdont képezővé tegyék a programot. Ennek megelőzéséhez tisztázni kívánjuk: szabadalom szabad szoftverrel kapcsolatban csak mindenki általi szabad használatra jegyezhető be, vagy egyáltalán nem jegyezhető be.

A másolásra, terjesztésre, módosításra vonatkozó pontos szabályok és feltételek:

A MÁSOLÁSRA, TERJESZTÉSRE ÉS MÓDOSÍTÁSRA VONATKOZÓ FELTÉTELEK ÉS KIKÖTÉSEK

0. Ez a licenc minden olyan programra vagy munkára vonatkozik, amelynek a szerzői jogi megjegyzésében a jog tulajdonosa a következő szöveget helyezte el: a GPL-ben foglaltak alapján terjeszthető. Az alábbiakban a Program kifejezés bármely ilyen programra vagy munkára vonatkozik, a Programon alapuló munka pedig magát a programot vagy egy szerzői joggal védett munkát jelenti: vagyis olyan munkát, amely tartalmazza a programot vagy annak egy részletét, módosítottan vagy módosítatlanul és/vagy más nyelvre fordítva. (Az alábbiakban a fordítás minden egyéb megkötés nélkül beletartozik a módosítás fogalmába.) Minden engedélyezés címzettje Ön.

A jelen licenc a másoláson, terjesztésen és módosításon kívül más tevékenységre nem vonatkozik, azok a hatályán kívül esnek. A Program futtatása nincs korlátozva, illetve a Program kimenetére is csak abban az esetben vonatkozik ez a szabályozás, ha az tartalmazza a Programon alapuló munka egy részletét (függetlenül attól, hogy ez a Program futtatásával jött-e létre). Ez tehát a Program működésétől függ.

1. A Program forráskódja módosítás nélkül másolható és bármely adathordozón terjeszthető, feltéve, hogy minden egyes példányon pontosan szerepel a megfelelő szerzői jogi megjegyzés, illetve a garanciavállalás elutasítása; érintetlenül kell hagyni minden erre a szabályozásra és a garancia teljes hiányára utaló szöveget és a jelen licencdokumentumot is el kell juttatni mindazokhoz, akik a Programot kapják.

Felszámítható díj a másolat fizikai továbbítása fejében, illetve ellenszolgáltatás fejében a Programhoz garanciális támogatás is biztosítható.

2. A Program vagy annak egy része módosítható, így a Programon alapuló munka jön létre. A módosítás ezután az 1. szakaszban adott feltételek szerint tovább terjeszthető, ha az alábbi feltételek is teljesülnek:

a) A módosított fájlokat el kell látni olyan megjegyzéssel, amely feltünteti a módosítást végző nevét és a módosítások dátumát.

b) Minden olyan munkát, amely részben vagy egészben tartalmazza a Programot vagy a Programon alapul, olyan szabályokkal kell kiadni vagy terjeszteni, hogy annak használati joga harmadik személy részére licencdíjmentesen hozzáférhető legyen, a jelen dokumentumban található feltételeknek megfelelően.

c) Ha a módosított Program interaktívan olvassa a parancsokat futás közben, akkor úgy kell elkészíteni, hogy a megszokott módon történő indításkor megjelenítsen egy üzenetet a megfelelő szerzői jogi megjegyzéssel és a garancia hiányára utaló közléssel (vagy éppen azzal az információval, hogy miként juthat valaki garanciához), illetve azzal az információval, hogy bárki terjesztheti a Programot a jelen feltételeknek megfelelően, és arra is utalást kell tenni, hogy a felhasználó miként tekintheti meg a licenc egy példányát. (Kivétel: ha a Program interaktív ugyan, de nem jelenít meg hasonló üzenetet, akkor a Programon alapuló munkának sem kell ezt tennie.)

Ezek a feltételek a módosított munkára, mint egészre vonatkoznak. Ha a munka azonosítható részei nem a Programon alapulnak és független munkákként elkülönülten azonosíthatók, akkor ez a szabályozás nem vonatkozik ezekre a részekre, ha azok külön munkaként kerülnek terjesztésre. Viszont, ha ugyanez a rész az egész részeként kerül terjesztésre, amely a Programon alapuló munka, akkor az egész terjesztése csak a jelen dokumentum alapján lehetséges, amely ebben az esetben a jogokat minden egyes felhasználó számára kiterjeszti az egészre tekintet nélkül arra, hogy melyik részt ki írta.

E szövegrésznek tehát nem az a célja, hogy mások jogait elvegye vagy korlátozza a kizárólag saját maga által írt munkákra; a cél az, hogy a jogok gyakorlása szabályozva legyen a Programon alapuló illetve a gyűjteményes munkák terjesztése esetében.

Ezenkívül más munkáknak, amelyek nem a Programon alapulnak, a Programmal (vagy a Programon alapuló munkával) közös adathordozón vagy adattárolón szerepeltetése nem jelenti a jelen szabályok érvényességét azokra is.

3. A Program (vagy a Programon alapuló munka a 2. szakasznak megfelelően) másolható és terjeszthető tárgykódú vagy végrehajtható kódú formájában az 1. és 2. szakaszban foglaltak szerint, amennyiben az alábbi feltételek is teljesülnek:

a) a teljes, gép által értelmezhető forráskód kíséri az anyagot, amelynek terjesztése az 1. és 2. szakaszban foglaltak szerint történik, jellemzően szoftverterjesztésre használt adathordozón; vagy,

b) legalább három évre szólóan írásban vállalja, hogy bármely külső személynek rendelkezésre áll a teljes gép által értelmezhető forráskód, a fizikai továbbítást fedező összegnél nem nagyobb díjért az 1. és 2. szakaszban foglaltak szerint szoftverterjesztésre használt adathordozón; vagy,

c) a megfelelő forráskód terjesztésére vonatkozóan megkapott tájékoztatás kíséri az anyagot. (Ez az alternatíva csak nem kereskedelmi terjesztés esetén alkalmazható abban az esetben, ha a terjesztő a Programhoz a tárgykódú vagy forráskódú formájában jutott hozzá az ajánlattal együtt a fenti b. cikkelynek megfelelően.)

Egy munka forráskódja a munkának azt a formáját jelenti, amelyben a módosításokat elsődlegesen végezni szokás. Egy végrehajtható program esetében a teljes forráskód a tartalmazott összes modul forráskódját jelenti, továbbá a kapcsolódó felületdefiníciós fájlokat és a fordítást vezérlő parancsfájlokat. Egy speciális kivételként a forráskódnak nem kell tartalmaznia normál esetben a végrehajtható kód futtatására szolgáló operációs rendszer főbb részeiként (kernel, fordítóprogram stb.) terjesztett részeit (forrás vagy bináris formában), kivéve, ha a komponens maga a végrehajtható állományt kíséri.

Ha a végrehajtható program vagy tárgykód terjesztése a forráskód hozzáférését egy megadott helyen biztosító írásban vállalja, akkor ez egyenértékű a forráskód terjesztésével, bár másoknak nem kell a forrást lemásolniuk a tárgykóddal együtt.

4. A Programot csak a jelen Licencben leírtaknak megfelelően szabad lemásolni, terjeszteni, módosítani és allicencbe adni. Az egyéb módon történő másolás, módosítás, terjesztés és allicencbe adás érvénytelen, és azonnal érvényteleníti a dokumentumban megadott jogosultságokat. Mindazonáltal azok, akik a Licencet megszegőtől kaptak példányokat vagy jogokat, tovább gyakorolhatják a Licenc által meghatározott jogaikat mindaddig, amíg teljesen megfelelnek a Licenc feltételeinek.

5. Önnek nem kötelező elfogadnia ezt a szabályozást, hiszen nem írta alá. Ezen kívül viszont semmi más nem ad jogokat a Program terjesztésére és módosítására. Ezeket a cselekedeteket a törvény bünteti, ha nem a jelen szerzői jogi szabályozás keretei között történnek. Mindezek miatt a Program

(vagy a Programon alapuló munka) terjesztése vagy módosítása a jelen dokumentum szabályainak, és azon belül a Program vagy a munka módosítására, másolására vagy terjesztésére vonatkozó összes feltételének elfogadását jelenti.

6. Minden alkalommal, amikor a Program (vagy az azon alapuló munka) továbbadása történik, a Programot megkapó személy automatikusan hozzájut az eredeti licenctulajdonostól származó licenchez, amely a jelen szabályok szerint biztosítja a jogot a Program másolására, terjesztésére és módosítására. Nem lehet semmilyen módon tovább korlátozni a fogadó félnek az itt megadott jogait. A Program továbbadója nem felelős harmadik személyekkel betartatni a jelen szabályokat.

7. Ha bírósági határozat, szabadalomsértés vélelme, vagy egyéb (nem kizárólag szabadalmakkal kapcsolatos) okból olyan feltételeknek kell megfelelnie (akár bírósági határozat, akár megállapodás, akár bármi más eredményeképp), amelyek ellentétesek a jelen feltételekkel, az nem menti fel a terjesztőt a jelen feltételek figyelembevétele alól. Ha a terjesztés nem lehetséges a jelen Licenc és az egyéb feltételek kötelezettségeinek együttes betartásával, akkor tilos a Program terjesztése. Ha például egy szabadalmi szerződés nem engedi meg egy program jogdíj nélküli továbbterjesztését azok számára, akik közvetve vagy közvetlenül megkapják, akkor az egyetlen módja, hogy eleget tegyen valaki mindkét feltételnek az, hogy eláll a Program terjesztésétől.

Ha ennek a szakasznak bármely része érvénytelen, vagy nem érvényesíthető valamely körülmény folytán, akkor a szakasz maradék részét kell alkalmazni, egyéb esetekben pedig a szakasz egésze alkalmazandó.

Ennek a szakasznak nem az a célja, hogy a szabadalmak vagy egyéb hasonló jogok megsértésére ösztönözzön bárkit is; mindössze meg szeretné védeni a szabad szoftver terjesztési rendszerének egységét, amelyet a szabad közreadást szabályozó feltételrendszerek teremtenek meg. Sok ember nagymértékben járult hozzá az e rendszer keretében terjesztett, különféle szoftverekhez, és számít a rendszer következetes alkalmazására; azt a szerző/adományozó dönti el, hogy a szoftverét más rendszer szerint is közzé kívánja-e tenni, és a licencet kapók ezt nem befolyásolhatják.

E szakasz célja, hogy pontosan tisztázza azt, ami elgondolásunk szerint a jelen licenc többi részének a következménye.

8. Ha a Program terjesztése és/vagy használata egyes országokban nem lehetséges akár szabadalmak, akár szerzői jogokkal védett felületek miatt, akkor a Program szerzői jogainak eredeti tulajdonosa, aki a Programot ezen szabályozás alapján adja közre, egy explicit földrajzi megkötést adhat a terjesztésre, és egyes országokat kizárhat. Ebben az esetben úgy tekintendő, hogy a jelen licenc ezt a megkötést is tartalmazza, ugyanúgy mintha csak a fő szövegében lenne leírva.

9. A Free Software Foundation időről időre kiadja a General Public License dokumentum felülvizsgált és/vagy újabb változatait. Ezek az újabb dokumentumok az előzőek szellemében készülnek, de részletekben különbözhetnek, hogy új problémákat vagy aggályokat is kezeljenek.

A dokumentum minden változata egy megkülönböztető verziószámmal ellátva jelenik meg. Ha a Program szerzői jogi megjegyzésében egy bizonyos vagy annál újabb verzió van megjelölve, akkor lehetőség van akár a megjelölt, vagy a Free Software Foundation által kiadott későbbi verzióban leírt feltételek követésére. Ha nincs ilyen megjelölt verzió, akkor lehetőség van a Free Software Foundation által valaha kibocsátott bármelyik dokumentum alkalmazására.

10. A Programot más szabad szoftverbe, amelynek szerzői jogi szabályozása különbözik, csak akkor építheti be, ha a szerzőtől erre engedélyt szerzett. Abban az esetben, ha a program szerzői jogainak tulajdonosa a Free Software Foundation, akkor a Free Software Foundation címére kell írni; néha kivételt teszünk. A döntés a következő két cél szem előtt tartásával fog történni: megmaradjon a szabad szoftveren alapuló munkák szabad állapota, valamint segítse elő a szoftver újrafelhasználását és megosztását.

GARANCIAVÁLLALÁS HIÁNYA

11. MIVEL A JELEN PROGRAM HASZNÁLATI JOGA DÍJMENTES, AZ ALKALMAZHATÓ JOGSZABÁLYOK ÁLTAL BIZTOSÍTOTT MAXIMÁLIS MÉRTÉKBEN VISSZAUTASÍTJUK A PROGRAMHOZ A GARANCIA BIZTOSÍTÁSÁT. AMENNYIBEN A SZERZŐI JOGOK TULAJDONOSAI ÍRÁSBAN MÁSKÉNT NEM NYILATKOZNAK, A PROGRAM A "JELEN ÁLLAPOTÁBAN" KERÜL KIADÁSRA, MINDENFÉLE GARANCIAVÁLLALÁS NÉLKÜL, LEGYEN AZ KIFEJEZETT VAGY BELEÉRTETT, BELEÉRTVE, DE NEM KIZÁRÓLAGOSAN A FORGALOMBA HOZHATÓSÁGRA VAGY ALKALMAZHATÓSÁGRA VONATKOZÓ GARANCIÁKAT. A PROGRAM MINŐSÉGÉBŐL ÉS MŰKÖDÉSÉBŐL FAKADÓ ÖSSZES KOCKÁZAT A FELHASZNÁLÓT TERHELI. HA A PROGRAM HIBÁSAN MŰKÖDIK, A FELHASZNÁLÓNAK MAGÁNAK KELL VÁLLALNIA A JAVÍTÁSHOZ SZÜKSÉGES MINDEN KÖLTSÉGET.

12. AMENNYIBEN A HATÁLYOS JOGSZABÁLYOK VAGY A SZERZŐI JOGOK TULAJDONOSAI ÍRÁSOS MEGÁLLAPODÁSBAN MÁSKÉNT NEM RENDELKEZNEK, SEM A PROGRAM SZERZŐJE, SEM MÁSOK, AKIK MÓDOSÍTOTTÁK ÉS/VAGY TERJESZTETTÉK A PROGRAMOT A FENTIEKNEK MEGFELELŐEN, NEM TEHETŐK FELELŐSSÉ A KÁROKÉRT, BELEÉRTVE MINDEN VÉLETLEN, VAGY KÖVETKEZMÉNYES KÁRT, AMELY A PROGRAM HASZNÁLATÁBÓL VAGY A HASZNÁLAT MEGAKADÁLYOZÁSÁBÓL SZÁRMAZIK (BELEÉRTVE, DE NEM KIZÁRÓLAGOSAN AZ ADATVESZTÉST ÉS A HELYTELEN ADATFELDOLGOZÁST, VALAMINT A MÁS PROGRAMOKKAL VALÓ HIBÁS EGYÜTTMŰKÖDÉST), MÉG AKKOR SEM, HA EZEN FELEK TUDATÁBAN VOLTAK, HOGY ILYEN KÁROK KELETKEZHETNEK.

FELTÉTELEK ÉS SZABÁLYOK VÉGE

Hogyan alkalmazhatók ezek a szabályok egy új programra?

Ha valaki egy új programot készít és szeretné, hogy az bárki számára a lehető leginkább hasznos legyen, akkor a legjobb módszer, hogy azt szabad szoftverré teszi, megengedve mindenkinek a szabad másolást és módosítást a jelen feltételeknek megfelelően.

Ehhez a következő megjegyzést kell csatolni a programhoz. A legbiztosabb ezt minden egyes forrásfájl elejére beírni, így közölve leghatásosabban a garancia visszautasítását; ezenkívül minden fájl kell, hogy tartalmazzon egy copyright sort és egy mutatót arra a helyre, ahol a teljes szöveg található.

Egy sor, amely megadja a program nevét és funkcióját Copyright (C) év; szerző neve;

```
Ez a program szabad szoftver; terjeszthető illetve módosítható a
Free Software Foundation által kiadott GNU General Public License
dokumentumában leírtak; akár a licenc 2-es, akár (tetszőleges) későbbi
változata szerint.


Ez a program abban a reményben kerül közreadásra, hogy hasznos lesz,
de minden egyéb GARANCIA NÉLKÜL, az ELADHATÓSÁGRA vagy VALAMELY CÉLRA
VALÓ ALKALMAZHATÓSÁGRA való származtatott garanciát is beleértve.
További részleteket a GNU General Public License tartalmaz.


A felhasználónak a programmal együtt meg kell kapnia a GNU General
Public License egy példányát; ha mégsem kapta meg, akkor
ezt a Free Software Foundationnak küldött levélben jelezze
(cím: Free Software Foundation Inc., 59 Temple Place, Suite 330,
Boston, MA 02111-1307, USA.)
```

A programhoz csatolni kell azt is, hogy miként lehet kapcsolatba lépni a szerzővel, elektronikus vagy hagyományos levél küldésével.

Ha a program interaktív, a következőhöz hasonló üzenettel lehet ezt megtenni a program indulásakor:

```
Gnomovision version 69, Copyright (C) év, a szerző neve.
A Gnomovision programhoz SEMMILYEN GARANCIA NEM JÁR; részletekért
írja be a 'show w' parancsot. Ez egy szabad szoftver, bizonyos
feltételek mellett terjeszthető, illetve módosítható; részletekért
írja be a 'show c' parancsot.
```

A show w és show c képzeletbeli parancsok, és a GPL megfelelő részeit kell megjeleníteniük. Természetesen a valódi parancsok a show w és show c parancstól különbözhetnek; lehetnek akár egérkattintások vagy menüpontok is, ami a programnak megfelel.

Ha szükséges, meg kell szerezni a munkáltatótól (ha a szerző programozóként dolgozik) vagy az iskolától a program szerzői jogairól való lemondás igazolását. Erre itt egy példa; változtassa meg a neveket:

```
A Fiktív Bt. ezennel lemond minden szerzői jogi érdekeltségéről
a „Gnomovision” programmal (amelyet több fázisban fordítanak le
a fordítóprogramok) kapcsolatban, amelyet H. Ekker János írt.


Aláírás: Tira Mihály, 1989. április 1. Tira Mihály ügyvezető
```

A GNU General Public License nem engedi meg, hogy a program része legyen szellemi tulajdont képező programoknak. Ha a program egy szubrutin-könyvtár, akkor megfontolhatja, hogy nem célszerűbb-e megengedni, hogy szellemi tulajdont képező alkalmazásokkal is összefűzhető legyen a programkönyvtár. Ha ezt szeretné, akkor a GPL helyett a GNU LGPL-t kell használni. GNU Lesser General Public License [http://www.fsf.org/licenses/lgpl.html].

GNU Free Documentation License (FDL)

1.2-es változat, 2002. november

Copyright (C) 2000,2001,2002 Free Software Foundation, Inc. 51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA

http://www.gnu.org/licenses/fdl.html

A jelen licencdokumentumot bárki szabadon lemásolhatja és a pontos másolatait terjesztheti, de a módosítása tilos.

ELŐSZÓ

Jelen Licenc célja egy tetszőleges kézikönyv, tankönyv, vagy más, ehhez hasonló felhasználható és hasznos dokumentum a szó szoros értelmében „szabaddá” tétele: annak érdekében, hogy mindenkinek biztosítsa a szöveg sokszorosításának és terjesztésének teljes szabadságát, módosításokkal, vagy anélkül, akár kereskedelmi, akár nem kereskedelmi területen. Másfelől, e Licenc megőrzi a szerző vagy kiadó munkájának elismeréséhez fűződő jogát, s egyúttal mentesíti őt a mások által beiktatott módosítások következményei alól.

A jelen Licenc egyfajta „copyleft” licencnek tekintendő: ez azt jelenti, hogy a dokumentumból származtatott munkák maguk is szabad minősítést kell, hogy kapjanak. Ez a dokumentum egyben a GNU General Public License kiegészítőjeként is szolgál, mely egy, a szabad szoftverekre vonatkozó etalon licenc.

A jelen Licenc a szabad szoftverek kézikönyveihez való használatra készült, hiszen a szabad szoftver egyben szabad dokumentációt is igényel: egy szabad programot olyan kézikönyvvel kell ellátni, amely ugyanazon szabadságokat biztosítja, mint maga a program. Mindazonáltal a jelen Licenc nem korlátozódik pusztán kézikönyvekre; feltételei tetszőleges tárgykörű írott dokumentumra alkalmazhatók, függetlenül attól, hogy az könyvformában valaha megjelent-e. Mindamellett e Licencet főként olyan munkákhoz ajánljuk, melyek elsődleges célja az útmutatás vagy a tájékoztatás.

ALKALMAZHATÓSÁG ÉS DEFINÍCIÓK

A jelen Licenc minden olyan kézikönyvre, vagy más jellegű, bármilyen adathordozón található munkára vonatkozik, amelyen megtalálható a szerzői jog tulajdonosa által feltüntetett figyelmeztetés, miszerint a dokumentum terjesztése jelen Licenc feltételei alapján lehetséges. Ez a figyelmeztetés nemzetközi, jogdíjmentes, korlátlan idejű licencet biztosít a mű benne meghatározott felhasználhatóságára vonatkozóan. Az alábbiakban használt „Dokumentum" kifejezés bármely ilyen jellegű kézikönyvre, vagy egyéb munkára vonatkozhat. A nyilvánosság bármely tagja potenciális licenctulajdonosnak tekinthető, és a továbbiakban az „Ön" megszólítást használjuk rá. Ön elfogadja a licenc feltételeit, amennyiben a művet a szerzői jogok alapján engedélyhez kötött módon lemásolja, módosítja vagy terjeszti.

A Dokumentum „Módosított Változata" bármely olyan munkára vonatkozik, amely tartalmazza a Dokumentumot, vagy annak elemeit akár szó szerint, akár módosításokkal, és/vagy más nyelvre lefordítva.

A „Másodlagos szakasz" egy egyedi névvel bíró függelék, esetleg a Dokumentum egy bevezető szakasza, amely kizárólag a kiadóknak, vagy az alkotóknak a Dokumentum átfogó tárgyköréhez (vagy kapcsolódó témákhoz) fűződő viszonyáról szól, és nem tartalmaz semmi olyat, ami közvetlenül ezen átfogó témakör alá eshet. (Vagyis ha a Dokumentum részben egy matematika-tankönyv, akkor a Másodlagos szakasz nem tartalmazhat matematikai tárgyú magyarázatokat). A fenti kapcsolat tárgya lehet a témakörrel, vagy a kapcsolódó témákkal való történelmi viszony, illetve az azokra vonatkozó jogi, kereskedelmi, filozófiai, etikai, vagy politikai felfogás.

A „Nem Változtatható szakaszok" olyan Másodlagos szakaszok, amelyek címe Nem Változtatható szakaszként van megjelölve abban a közleményben, amely szerint a Dokumentum a jelen Licenc hatálya alatt lett kiadva. Ha egy szakasz nem felel meg a Másodlagos szakasz fenti definíciójának, akkor Nem Változtatható sem lehet. Nem kötelező, hogy egy Dokumentumban legyen Nem Változtatható szakasz, így ha a Dokumentum nem jelöl meg egyetlen Nem Változtatható szakaszt sem, akkor nem tartalmaz ilyet.

A „Borítószövegek" olyan rövid szövegrészek, melyek Címlapszövegként, illetve Hátlapszövegként kerülnek felsorolásra a közleményben, amely szerint a Dokumentum a jelen Licenc hatálya alatt lett kiadva. A Címlapszöveg maximum 5, a Hátlapszöveg maximum 25 szóból állhat.

A Dokumentum „Átlátszó" példánya olyan géppel olvasható változatot jelent, amely a nyilvánosság számára hozzáférhető formátumban kerül terjesztésre, továbbá amelynek tartalma alkalmas a szokványos szövegszerkesztő-programokkal, illetve (pixelekből álló képek esetén) szokványos képmegjelenítő-programokkal, vagy (rajzok esetén) általánosan hozzáférhető rajzprogramok segítségével azonnali és közvetlen változtatásokra; továbbá olyan formátumban mely alkalmas a szövegszerkesztőkbe való bevitelre, vagy a szövegszerkesztők által kezelt formátumokra való automatikus átalakításra. Egy olyan, egyébként Átlátszó formátumban készült példány, melynek a jelölőnyelve vagy ennek hiánya úgy lett kialakítva, hogy megakadályozza, vagy eltántorítsa az olvasókat minden további módosítástól, nem tekinthető Átlátszónak. A nem „Átlátszó" példányok az „Átlátszatlan" megnevezést kapják.

Az Átlátszóság kritériumainak megfelelő formátumok között megtalálható például a jelölőnyelvet nem használó egyszerű ASCII, a Texinfo beviteli formátum, a LaTeX beviteli formátum, az SGML vagy az XML egy általánosan hozzáférhető DTD használatával, és a szabványnak megfelelő, emberi módosításra tervezett egyszerű HTML, PostScript vagy PDF. Átlátszó képformátumokra példa a PNG, XCF és a JPG. Az Átlátszatlan formátumok közé sorolhatóak a a szellemi tulajdont képező formátumok, amelyeket csak szellemi tulajdont képező szövegszerkesztőkkel lehet elolvasni, az olyan SGML vagy XML, amelyhez a szükséges DTD és/vagy egyéb feldolgozó eszközök nem általánosan hozzáférhetők, és az olyan gépileg generált HTML, PostScript vagy PDF formátum, amely kizárólag egyes szövegszerkesztők kimeneti formátumaként áll elő.

Egy nyomtatott könyv esetében a „Címlap" magát a címlapot, illetve bármely azt kiegészítő további oldalt jelöli, amely a jelen Licencben előírt címlaptartalom közzétételéhez szükséges. Az olyan formátumú munkáknál, amelyek nem rendelkeznek effajta címlappal, a „Címlap" a munka címének legjobban kiemelt változatához legközelebb eső, ám a szöveg törzsét megelőző szövegrészeket jelöli.

Egy „XYZ elnevezésű" szakasz a Dokumentum azon alegységét jelenti aminek címe pontosan XYZ, vagy zárójelek között tartalmazza XYZ-t, és az XYZ más nyelvre való fordítását követi. (Az XYZ itt egy alább megjelölt szakasznevet helyettesít, mint például „Köszönetnyilvánítás", „Ajánlások", „Jóváhagyás" vagy „Előzmények".) Egy ilyen szakasz „Címét Megőrizni" a Dokumentum módosítása során azt jelenti, hogy a szakasz „XYZ elnevezésű" marad ezen definíció szerint.

A Dokumentum tartalmazhatja Garanciák Kizárását azon figyelmeztetés mellett, amely kijelenti hogy a Dokumentumra a jelen Licenc érvényes. Ezen Garaciakizárások a jelen Licenc mellékleteinek tekintendők, azonban csak a garanciák kizárásainak tekintetében: minden egyéb állítás, melyet esetleg ezen Garanciakizárás tartalmaz, érvénytelen, és nincs hatással a jelen Licenc tartalmára.

SZÓ SZERINTI SOKSZOROSÍTÁS

Önnek lehetősége van a Dokumentum kereskedelmi, vagy nem kereskedelmi jellegű sokszorosítására és terjesztésére a felhasznált adathordozó típusától függetlenül, feltéve, hogy a jelen Licenc, a szerzői jogi figyelmeztetés, továbbá a Dokumentumot a jelen Licenc hatálya alá rendelő közlemény minden példányban egyaránt megjelenik, és hogy ezeken kívül semmilyen feltételt nem szab meg a szöveghez. Nem alkalmazhat olyan technikai eszközöket, amelyekkel megakadályozható vagy szabályozható az Ön által terjesztett példányok elolvasása vagy sokszorosítása. Mindazonáltal elfogadhat ellenszolgáltatást a másolatokért cserébe. Amennyiben az Ön által terjesztett példányok száma meghalad egy bizonyos mennyiséget, úgy a 3. szakasz feltételeinek is eleget kell tennie.

A fenti feltételeket betartva kölcsönözhet is példányokat, de akár nyilvánosan is közzéteheti a szöveget.

SOKSZOROSÍTÁS NAGYOBB MENNYISÉGBEN

Amennyiben 100-nál több nyomtatott példányt (vagy olyan adathordozón található példányokat, amelyeknek jellemzően van nyomtatott címlapjuk) tesz közzé a Dokumentumból, és a dokumentum Licence feltételül szabja a Borítószövegek meglétét, úgy minden egyes példányt köteles ellátni olyan borítólapokkal, amelyeken a következő Borítószövegek tisztán és olvashatóan fel vannak tüntetve: Címlapszövegek a címlapon, illetve Hátlapszövegek a hátlapon. Mindkét borítólapra egyértelműen és olvashatóan rá kell vezetnie a kiadó, vagyis jelen esetben az Ön nevét. A címlapon a Dokumentum teljes címének szerepelnie kell, és a cím minden szavának egyformán kiemeltnek és láthatónak kell lennie. Ezen felül, belátása szerint, további részleteket is hozzáadhat a borítólapokhoz. Amennyiben az esetleges módosítások kizárólag a borítólapokat érintik, és feltéve, hogy a Dokumentum címe változatlan marad, továbbá a borítólapok megfelelnek minden egyéb követelménynek, úgy a sokszorosítás ettől eltekintve szó szerinti sokszorosításnak minősül.

Abban az esetben, ha a borítólapok bármelyikén megkövetelt szövegrészek túl hosszúnak bizonyulnának az olvasható közzétételhez, úgy csak az elsőként felsoroltakat kell feltüntetnie (amennyi józan belátás szerint elfér) a tényleges borítón, a továbbiak pedig átkerülhetnek a következő oldalakra.

Amennyiben 100-nál több Átlátszatlan példányt tesz közzé, vagy terjeszt a Dokumentumból, úgy köteles vagy egy géppel olvasható Átlátszó példányt mellékelni minden egyes Átlátszatlan példányhoz, vagy leírni minden egyes Átlátszatlan példányban egy, a módosítatlan Átlátszó példányt tartalmazó olyan számítógép-hálózat elérhetőségét, amely elérhető az általános hálózati felhasználók számára, és onnan nyilvános szabványú hálózati protokollok segítségével a Dokumentum hozzáadott anyagok nélküli, teljes változata letölthető. Ha az utóbbi lehetőséget választja, köteles gondoskodni arról, hogy attól a naptól kezdve, amikor az utolsó Átlátszatlan példány is terjesztésre került (akár közvetlenül Ön által, akár kiskereskedelmi forgalomban), a fenti helyen közzétett Átlátszó példány még legalább egy évig hozzáférhető legyen a felhasználók számára.

Megkérjük, ámde nem kötelezzük Önt arra, hogy minden esetben, amikor nagyobb példányszámú terjesztésbe kezd, már jóval ezt megelőzően lépjen kapcsolatba a Dokumentum szerzőivel, annak érdekében, hogy megkaphassa tőlük a Dokumentum esetleges újabb változatát.

MÓDOSÍTÁSOK

Önnek lehetősége van a Dokumentum Módosított Változatának sokszorosítására és terjesztésére a 2. és 3. szakaszok fenti rendelkezései alapján, feltéve, hogy a Módosított Változatot kizárólag jelen Licenc feltételeivel összhangban teszi közzé, ahol a Módosított Változat a Dokumentum szerepét tölti be, ezáltal lehetőséget biztosítva annak terjesztésére és módosítására bárkinek, aki csak hozzájut egy példányához. Mindezen felül, a Módosított Változat az alábbi követelményeknek is meg kell, hogy feleljen:

A. A Címlapon (és ha van, a borítókon) tüntessen fel egy a Dokumentumétól, illetve bármely korábbi változatétól eltérő címet (amelyeknek, ha vannak, a Dokumentum Előzmények szakaszában kell szerepelniük). Egy korábbi változat címét csak akkor használhatja, ha annak szerzője engedélyezte azt.

B. A Címlapon szerzőkként sorolja fel a Módosított Változatban elvégzett változtatásokért felelős természetes vagy jogi személyeket, továbbá a Dokumentum fő szerzői közül legkevesebb ötöt (vagy mindet, ha ötnél kevesebben vannak) kivéve, ha ezen feltétel alól ők Önt felmentik.

C. A Címlapon a Módosított Változat közzétételéért felelős személyt tüntesse fel kiadóként.

D. A Dokumentum összes szerzői jogi figyelmeztetését hagyja érintetlenül.

E. Saját módosításaira vonatkozóan is tegyen közzé egy szerzői jogi megjegyzést, a többi ilyen jellegű figyelmeztetés mellett.

F. Rögtön a szerzői jogi figyelmeztetéseket követően tüntessen fel egy közleményt, az alábbi Függelék mintájára, amelyben engedélyezi a Módosított Változat felhasználását a jelen Licenc feltételeinek megfelelően.

G. A fenti közleményben hagyja érintetlenül a Nem Változtatható szakaszok és a szükséges Borítószövegek a jelen Dokumentum licencében előírt teljes listáját.

H. Mellékelje a jelen Licenc egy eredeti példányát.

I. Az „Előzmények" elnevezésű szakaszt, illetve annak címét szintén hagyja érintetlenül, emellett adjon hozzá egy új elemet, amely minimálisan tartalmazza a Módosított Változat címét, kiadási évét, továbbá az új szerzők, illetve a kiadó nevét, a Címlapon láthatókhoz hasonlóan. Amennyiben a Dokumentum nem tartalmaz semmiféle „Előzmények" elnevezésű szakaszt, úgy hozzon létre egyet, amely tartalmazza a Dokumentum címét, kiadási évét, továbbá a szerzők, illetve a kiadó nevét, a Címlapon láthatókhoz hasonlóan; majd ezt követően adjon hozzá egy új, a Módosított Változatra vonatkozó elemet, a fentiekkel összhangban.

J. Ne tegyen változtatásokat a Dokumentumban megadott Átlátszó példány nyilvános hálózati elérhetőségét (ha van ilyen) illetően, vagy hasonlóképp, a Dokumentum alapjául szolgáló korábbi változatok hálózati helyére vonatkozóan. Ezek az „Előzmények" szakaszban is szerepelhetnek. Csak abban az esetben hagyhatja el egyes korábbi változatok hálózati elérhetőségét, ha azok legkevesebb négy évvel a Dokumentum előtt készültek, vagy ha maga az alkotó engedélyezi azt.

K. Bármely „Köszönetnyilvánítás", vagy „Ajánlások" elnevezésű szakasz címét hagyja érintetlenül, továbbá gondoskodjon arról, hogy azok tartalma és hangvétele az egyes hozzájárulókat, és/vagy az ajánlásokat illetően változatlan maradjon.

L. A Dokumentum összes Nem Változtatható szakaszát hagyja érintetlenül, úgy címüket, mint tartalmukat illetően. A szakaszok számozása, vagy bármely azzal egyenértékű jelölés nem tartozik a szakaszcímek közé.

M. Töröljön minden „Hozzájárulás" elnevezésű szakaszt. Effajta szakaszok nem képezhetik részét a Módosított Változatnak.

N. Ne nevezzen át semmilyen létező szakaszt „Hozzájárulás" elnevezésűre, vagy olyasmire, amely címében a Nem Változtatható szakaszokkal ütközhet.

O. Tartson meg minden Garanciakizárást.

Ha a Módosított Változat új bevezető szakaszokat tartalmaz, vagy olyan függelékeket, melyek Másodlagos szakasznak minősülnek, ám nem tartalmaznak a Dokumentumból származó anyagot, abban az esetben, belátása szerint, e szakaszok némelyikét, vagy akár az összeset besorolhatja nem változtathatóként. Ehhez nem kell mást tennie, mint felsorolni a szóban forgó címeket a Módosított Változat licencének Nem Változtatható szakaszok listájában. E címeknek határozottan el kell különülnie minden egyéb szakaszcímtől.

„Hozzájárulás" elnevezésű szakaszt csak akkor adhat a Dokumentumhoz, ha az kizárólag a Módosított Változatra utaló megjegyzéseket tartalmaz – például mások recenzióira vonatkozóan, vagy hogy egy szervezet a szöveget egy szabvány mérvadó definíciójaként ismerte el.

Címlapszöveg gyanánt egy legfeljebb öt szóból álló szövegrészt adhat meg, a Hátlapszöveg esetén pedig 25 szót fűzhet a Módosított Változat Borítószövegeinek végéhez. Bármely természetes vagy jogi személy csak és kizárólag egy Címlapszöveg és egy Hátlapszöveg részt adhat (akár közvetítőn keresztül) a Dokumentumhoz. Ha a Dokumentum már rendelkezik Borítószöveggel ehhez a változathoz, mert korábban Ön adta hozzá, vagy az a szervezet, amelynek nevében Ön fellép, akkor nem adhat hozzá másik Borítószöveget; a régit mindazonáltal lecserélheti, abban az esetben, ha az azt hozzáadó korábbi kiadó egyértelműen engedélyezi.

A közös Dokumentum szerzői és kiadói ezzel a Licenccel nem járulnak hozzá nevük felhasználására, a Módosított Változat népszerűsítésére, és nem támogatják azt.

KOMBINÁLT DOKUMENTUMOK

Önnek lehetősége van a Dokumentum egyéb, e Licenc hatálya alatt kiadott dokumentumokkal való kombinálására a 4. szakasz módosított változatokra vonatkozó rendelkezései alapján, feltéve, hogy a kombináció módosítás nélkül tartalmazza az eredeti dokumentumok összes Nem Változtatható szakaszát, és hogy azok mind Nem Változtatható szakaszként kerülnek felsorolásra a kombinált munka licencében, és tartalmazzák a hozzájuk tartozó Garanciák Kizárásait is.

A kombinált munkának a jelen Licenc mindössze egy példányát kell tartalmaznia, az egymással átfedésben lévő Nem Változtatható szakaszok pedig kiválthatók egy összegzett példánnyal. Amennyiben több Nem Változtatható szakasz szerepelne ugyanazon címmel, ám eltérő tartalommal, úgy alakítsa át minden egyes szakasz címét olyan módon, hogy mögé írja zárójelben az eredeti szerző és kiadó nevét (ha ismeri) vagy egy egyedi sorszámot. Ha szükséges, a Nem Változtatható szakaszok címeivel is végezze el a fenti módosításokat a kombinált munka licencében.

A kombinált munkában az eredeti dokumentumok összes „Előzmények" elnevezésű szakaszát össze kell olvasztania, miáltal egy összefüggő „Előzmények" elnevezésű szakasz jön létre; hasonlóképp kell eljárnia a „Köszönetnyilvánítás", illetve az „Ajánlások" elnevezésű szakaszok tekintetében. Ugyanakkor minden „Hozzájárulás" elnevezésű szakaszt törölnie kell.

DOKUMENTUMGYŰJTEMÉNYEK

Önnek lehetősége van a Dokumentumból, illetve bármely egyéb, a jelen Licenc hatálya alatt kiadott dokumentumból gyűjteményt létrehozni, és az egyes dokumentumokban található licenceket egyetlen példánnyal kiváltani, feltéve, hogy a gyűjteményben szereplő összes dokumentum esetén minden más tekintetben követi a jelen Licenc feltételeit azok szó szerinti sokszorosítására vonatkozóan.

Tetszése szerint ki is emelhet egy meghatározott dokumentumot a gyűjteményből, továbbá terjesztheti azt jelen Licenc feltételei alapján, feltéve, hogy a szóban forgó dokumentumhoz mellékeli a jelen Licenc egy példányát, és minden egyéb tekintetben betartja jelen Licenc előírásait a dokumentum szó szerinti sokszorosítására vonatkozóan.

ÖSSZEFŰZÉS FÜGGETLEN MUNKÁKKAL

A Dokumentum és annak származékainak különálló, vagy független dokumentumokkal, illetve munkákkal való összefűzése egy közös tárolási, vagy terjesztési egységen „gyűjteménynek" nevezendő, amennyiben az összefűzés eredményeképpen érvényes szerzői jogi feltételek nem korlátozzák nagyobb mértékben az összefűzés felhasználóinak jogait, mint amennyire azt az egyes összetevők teszik. Amikor a Dokumentum része egy gyűjteménynek, akkor a jelen Licenc nem érvényes a gyűjtemény azon részeire, amelyek nem a Dokumentumból származtatott munkák.

Amennyiben a 3. szakasz Borítószövegekre vonatkozó rendelkezései alkalmazhatók a Dokumentum e példányaira, és a Dokumentum a teljes összegzésnek kevesebb, mint felét teszi ki, úgy a Dokumentum Borítószövegeit olyan módon is el lehet helyezni a borítókon, hogy azok csak magát a Dokumentumot fogják közre, vagy a borítóknak megfelelő elektronikus formában, amennyiben a Dokumentum elektronikus formában található. Minden más esetben a teljes összegzés borítólapjain kell feltüntetni a fenti szövegeket.

FORDÍTÁS

A fordítás egyfajta módosításnak tekinthető, így a Dokumentum lefordított példányai a 4. szakasz rendelkezései alapján terjeszthetők. A Nem Változtatható szakaszok lefordításához külön engedélyt kell kérni a szerzői jogtulajdonostól, mindazonáltal közzétehetők a lefordított változatok is úgy, ha az eredeti Nem Változtatható szakaszokat is belefoglalja a munkába. E Licenc lefordítására, valamint minden, a Dokumentumhoz tartozó Licencmellékletre, illetve az esetleges Garanciák Kizárásaira ugyanezek a feltételek érvényesek, vagyis a lefordított változatok csak akkor jelenhetnek meg, ha mellette ott vannak az eredeti, angol nyelvű Licenc, a mellékletek és kizárások szövegei is. Amennyiben eltérés mutatkozna az eredeti változatok, illetve a fordítás között, úgy a Licenc, a mellékletek és kizárások angol nyelvű eredetije tekintendő mérvadónak.

Ha a Dokumentum egy szakasza „Köszönetnyilvánítások", „Ajánlások" vagy „Előzmények" elnevezésű, akkor a Cím Megőrzésének (1. szakasz) feltétele (4. szakasz) általában a konkrét cím megváltoztatását jelenti.

MEGSZŰNÉS

A jelen Licencben egyértelműen kijelölt kereteken kívül tilos a Dokumentum bárminemű sokszorosítása, módosítása, továbblicencelése, vagy terjesztése. Minden ezzel szembeni sokszorosítási, módosítási, továbblicencelési, vagy terjesztési kísérlet a jelen Licencben meghatározott jogok automatikus megszűnését vonja maga után. Ugyanakkor azok a felek, akik Önön keresztül jutottak másolathoz vagy jogosultságokhoz, nem veszítik el azokat, amíg maradéktalanul betartják e Licenc előírásait.

JELEN LICENC JÖVŐBENI JAVÍTÁSAI

Megtörténhet, hogy a Free Software Foundation időről időre felülvizsgált és/vagy új verziókat bocsát ki a GNU Free Documentation License-ből. E verziók szellemisége hasonló lesz jelen változatéhoz, ám részleteikben eltérhetnek, új problémák, új aggályok felmerülése okán. Vö.: http://www.gnu.org/copyleft/.

A Licenc minden változata egyedi verziószámmal van ellátva. Ha a Dokumentum jelen Licenc egy konkrét, számozott verziójára „vagy bármely újabb verzióra” hivatkozik, úgy önnek a szóban forgó változat, vagy bármely újabb a Free Software Foundation által (nem vázlatként) kiadott verzió feltételeinek követésére lehetősége van. Ha a Dokumentum nem ad meg semmilyen verziószámot, úgy bármely, a Free Software Foundation által valaha (nem vázlatként) kiadott változat megfelel.

FÜGGELÉK: A Licenc alkalmazása saját dokumentumaira

Ha a jelen Licencet egy Ön által írt dokumentumban kívánja használni, akkor mellékelje hozzá a Licenc egy példányát, továbbá vezesse rá az alábbi szerzői jogi és licencközleményeket, rögtön a címlapot követően:

```
Copyright (C) ÉV AZ ÖN NEVE.
Engedélyt adunk Önnek a jelen dokumentum sokszorosítására,
terjesztésére és/vagy módosítására a Free Software Foundation
által kiadott GNU FDL 1.2-es, vagy bármely azt követő verziójának
feltételei alapján.
Nincs Nem Változtatható szakasz, nincs Címlapszöveg, nincs Hátlapszöveg.
A jelen licenc egy példányát a „GNU FDL” elnevezésű szakasz alatt találja.
```

Ha a szövegben vannak Nem Változtatható szakaszok, Címlapszövegek vagy Hátlapszövegek, akkor a „Nincs ... nincs Hátlapszöveg” részt cserélje az alábbira:

```
Nem Változtatható szakaszok: ITT SOROLJA FEL A CÍMEIKET,
Címlapszövegek: FELSOROLÁS, Hátlapszövegek: FELSOROLÁS.
```

Ha vannak Nem Változtatható szakaszok de nincsenek Címlapszövegek, vagy ezen három lehetőség egyéb kombinációinak esetén a fenti két változatból szerkessze meg a helyzetnek megfelelő szöveget.

Amennyiben a dokumentum nem egyértelmű programkódpéldákat is tartalmaz, úgy azt javasoljuk, hogy e példákat egy választása szerinti szabad szoftver licenc alatt közölje – mint például a GNU GPL –, hogy lehetővé tegye a kódok szabad szoftverekben való alkalmazását.