Ubuntu kiszolgáló kézikönyve

Ubuntu kiszolgáló kézikönyve

Kivonat

Üdvözöljük az Ubuntu kiszolgáló kézikönyvében! Itt megismerheti a különféle kiszolgálóalkalmazások Ubuntu rendszerre telepítésének, és az Ön igényeinek megfelelő beállításuk módját. Ez a leírás lépésről lépésre, feladatközpontúan mutatja be a rendszer beállítását és személyre szabását.

Köszönetnyilvánítás és licenc

A honlap tartalmának karbantartója az Ubuntu dokumentációs csapat (https://wiki.ubuntu.com/DocumentationTeam). A csapat résztvevőinek listája az alábbi oldalon[1] olvasható.

[3] https://launchpad.net/~ubuntu-core-doc

[1] ../../libs/C/contributors.xml

[2] /usr/share/ubuntu-docs/libs/C/ccbysa.xml

Tartalom

A táblázatok listája

1. fejezet - Bevezetés

Üdvözöljük az Ubuntu kiszolgáló kézikönyvében!

Itt a különböző kiszolgálóalkalmazások telepítésével és konfigurálásával kapcsolatos információkat talál. Ez az útmutató lépésről lépésre, feladatközpontúan mutatja be a rendszer beállítását és személyre szabását.

This guide assumes you have a basic understanding of your Ubuntu system. Some installation details are covered in 2. fejezet - Telepítés [3], but if you need detailed instructions installing Ubuntu please refer to the Ubuntu Installation Guide[1].

A kézikönyv HTML változata elérhető az Ubuntu dokumentációs webhelyen[2]. A HTML fájlok elérhetők az ubuntu-serverguide csomagban is. A csomagok telepítésével kapcsolatban lásd: 3. fejezet - Csomagkezelés [17].

Ha telepíti az ubuntu-serverguide csomagot, akkor ezt a dokumentációt a konzolból is elérheti:

```
w3m /usr/share/ubuntu-serverguide/html/C/index.html
```

Lokalizált verzió használatakor a C helyére saját nyelvi kódját írja (például hu).

[1] https://help.ubuntu.com/10.04 LTS/installation-guide/

[2] http://help.ubuntu.com

1. Támogatás

Az Ubuntu kiszolgáló változatához számos különböző módon kaphat támogatást, elérhető kereskedelmi és közösségi támogatás is. Az elsődleges kereskedelmi támogatást (és a fejlesztés támogatását) a Canonical Ltd. biztosítja. Elfogadható áron kínálnak támogatási szerződéseket asztali gépenkénti vagy kiszolgálónkénti alapon. További információkért lásd a Canonical Services[3] oldalát.

Eltökélt magánszemélyek és cégek, akik szeretnék az Ubuntut a lehető legjobb disztribúcióvá tenni, közösségi támogatást biztosítanak. A támogatás több levelezőlistán, IRC-csatornákon, fórumokon, blogokon, wikikben stb. érhető el. Az elérhető információk nagy mennyisége sokkoló lehet, de egy jó keresőkifejezés általában választ ad kérdéseire. További információkért lásd az Ubuntu Support[4] oldalt.

[3] http://www.canonical.com/services/support

[4] http://www.ubuntu.com/support

2. fejezet - Telepítés

This chapter provides a quick overview of installing Ubuntu 10.04 LTS Server Edition. For more detailed instructions, please refer to the Ubuntu Installation Guide[1].

[1] https://help.ubuntu.com/10.04 LTS/installation-guide/

1. Felkészülés a telepítésre

Ez a szakasz a telepítés előtt megfontolandó különböző szempontokat ismerteti.

1.1. Rendszerkövetelmények

Az Ubuntu 10.04 LTS kiszolgáló változata két fő architektúrát támogat, ezek az Intel x86 és az AMD64. Az alábbi táblázat felsorolja az ajánlott hardver specifikációit. Igényeitől függően kevesebb is elég lehet. Azonban a legtöbb felhasználó esetén ezen javaslatok figyelmen kívül hagyása jelentős frusztrációt okozhat.

2.1. táblázat - Ajánlott minimális követelmények

Telepítés típusa	RAM	Merevlemezhely	
		Minden szolgáltatást telepítve	Alaprendszer
Kiszolgáló	128 megabájt	500 megabájt	1 gigabájt

A kiszolgáló változat az összes kiszolgálóalkalmazás számára egy közös alapot biztosít. Minimalista felépítése biztosítja a kívánt szolgáltatások, például fájl/nyomtatószolgáltatások, webkiszolgálás, e-mail kiszolgálás stb. környezetét.

Az UEC követelményei némileg eltérnek. Az előtét követelményeiért lásd az 3.2.1. szakasz - Előtét előfeltételei [276], az UEC csomópont követelményeiért pedig a 3.2.2. szakasz - Csomópont előfeltételei [277] szakaszt.

1.2. Különbségek a kiszolgáló és az asztali rendszer között

Van néhány különbség az Ubuntu kiszolgáló változata és az Ubuntu asztali változata között. Meg kell jegyezni, hogy mindkét változat ugyanazokat az apt tárolókat használja. Ez a kiszolgáló alkalmazások telepítését egyformán egyszerűvé teszi az asztali változatra és a kiszolgáló változatra is.

A két változat közti különbségek: az X ablakkezelő környezet hiánya a kiszolgáló változatban, a telepítési folyamat, és az eltérő kernelbeállítások.

1.2.1. Kernelkülönbségek:

- A kiszolgáló változat a Deadline I/O ütemezőt használja az asztali kiadásban használt CFQ ütemező helyett.
- A preemption ki van kapcsolva a kiszolgáló változatban.
- Az időzítő megszakítása 100 Hz a kiszolgáló változatban, és 250 Hz az asztali változatban.

Az Ubuntu 64 bites változatának 64 bites processzorokon való futtatásakor a memóriacímtér mérete nem jelent akadályt.

A kernel összes beállítását a `/boot/config-2.6.32-server` fájlban találja. Az elérhető beállításokkal kapcsolatban a Linux Kernel in a Nutshell[2] című könyv hasznos információforrás.

1.3. Mentés

- Az Ubuntu kiszolgáló verziójának telepítése előtt győződjön meg, hogy a rendszerén található összes adat mentésre került. A mentési lehetőségeket lásd: 18. fejezet - Biztonsági mentés [246].

  Ha nem először telepít operációs rendszert a számítógépre, akkor szükség lehet a lemez újraparticionálására az Ubuntunak szánt hely felszabadításához.

  A lemez particionálásakor fel kell készülnie a lemezen található összes adat elvesztésére, amennyiben hibát követ el, vagy a particionálás során valami rosszul sül el. A telepítéshez használt programok meglehetősen megbízhatók, a legtöbb évek óta használatban van, de visszavonhatatlan műveleteket is végrehajtanak.

[2] http://www.kroah.com/lkn/

2. Telepítés CD-ről

Az Ubuntu kiszolgáló változatának telepítésének alapvető lépései azonosak bármely operációs rendszer CD-ről telepítésének lépéseivel. Az asztali változattal ellentétben a kiszolgáló változat nem tartalmaz grafikus telepítőprogramot. Ehelyett a kiszolgáló változat konzolos menüalapú telepítőt használ.

- Első lépésként töltse le és írja ki a megfelelő ISO-fájlt az Ubuntu weboldaláról[3].
- Indítsa el a rendszert a CD-ROM meghajtóról.
- Az indítómenü bekéri a nyelvét. A telepítési folyamat ezután a billentyűzetkiosztásra kérdez rá.
- A fő indítómenüből elérhető néhány további beállítás az Ubuntu kiszolgáló változatának telepítéséhez. Választhatja alapszintű Ubuntu kiszolgáló telepítését, vagy telepítheti az Ubuntu kiszolgálót egy Ubuntu Enterprise Cloud részeként. Az UEC-vel kapcsolatos további információkért lásd: 3. szakasz - UEC [276]. Ezen szakasz a továbbiakban az alapszintű Ubuntu kiszolgáló telepítését ismerteti.
- A telepítő felderíti a hardverkonfigurációt, és DHCP segítségével beállítja a hálózatot. Ha nem szeretne DHCP-t használni, akkor a következő képernyőn válassza a „Vissza” lehetőséget, ekkor lehetősége lesz a „Hálózat kézi beállítására”.
- A telepítő ezután bekéri a rendszer gépnevét és időzónáját.
- Ezután számos lehetősége lesz a merevlemez-kiosztás konfigurálására. A speciális lemezbeállításokat lásd: 4. szakasz - Speciális telepítés [10].
- Az Ubuntu alaprendszer ezután telepítésre kerül.
- Egy új felhasználó kerül beállításra, ez a felhasználó a sudo segédprogram használatával tehet szert rendszergazdai jogosultságra.
- A felhasználó beállítása után a telepítő megkéri a `home` könyvtár titkosítására.
- A telepítési folyamat következő lépése a rendszer frissítési módjának eldöntése. Három lehetőség van:
  - Nincsenek automatikus frissítések: ebben az esetben a rendszergazdának be kell jelentkeznie a gépre, és saját kezűleg kell telepítenie a frissítéseket.
  - Biztonsági frissítések automatikus telepítése: ez telepíti az unattended-upgrades csomagot, amely a biztonsági frissítéseket rendszergazdai beavatkozás nélkül telepíti. További részletekért lásd: 5. szakasz - Automatikus frissítések [25].
  - A rendszer felügyelete a Landscape-pel: A Landscape a Canonical kereskedelmi szolgáltatása ubuntus gépek felügyeletéhez. Részletekért lásd a Landscape[4] oldalát.
- Ezután lehetősége van számos csomagfeladat telepítésére. Részletekért lásd: 2.1. szakasz - Csomagfeladatok [7]. Lehetőség van az aptitude elindítására is telepítendő csomagok kiválasztásához. További információkért lásd: 4. szakasz - Aptitude [23].
- Végül az újraindítás előtti utolsó lépés az óra beállítása az UTC-re.

Ha a telepítés során bármikor nem elégedett az alapértelmezett beállítással, a „Vissza” funkció használatával bármikor visszaléphet egy részletes telepítőmenübe, amely lehetővé teszi az alapértelmezett beállítások módosítását.

A telepítési folyamat során szükség lehet a telepítőrendszer által biztosított súgóképernyők megjelenítésére. Ehhez nyomja meg az F1 billentyűt.

Once again, for detailed instructions see the Ubuntu Installation Guide[5].

2.1. Csomagfeladatok

A kiszolgáló változat telepítése során lehetősége van további csomagok telepítésére a CD-ről. A csomagok az általuk biztosított szolgáltatás szerint vannak csoportosítva.

- Számítási felhő: Walrus tárolószolgáltatás
- Számítási felhő: minden egyben fürt
- Számítási felhő: fürtvezérlő
- Számítási felhő: csomópontvezérlő
- Számítási felhő: tárolóvezérlő
- Számítási felhő: felső szintű felhővezérlő
- DNS-kiszolgáló: a BIND DNS-kiszolgáló és dokumentációja.
- LAMP-kiszolgáló: előregyártott Linux/Apache/MySQL/PHP kiszolgáló
- Levelezőkiszolgáló: ez a feladat általános célú levelezőkiszolgáló rendszerhez hasznos csomagokat telepít.
- OpenSSH kiszolgáló: OpenSSH kiszolgálóhoz szükséges csomagok.
- PostgreSQL adatbázis: ez a feladat a PostgreSQL adatbázis-kezelő kliens- és kiszolgálócsomagjait telepíti.
- Nyomtatókiszolgáló: ez a feladat nyomtatókiszolgálóvá változtatja a rendszert.
- Samba fájlkiszolgáló: Ez a feladat Samba fájlkiszolgálóvá változtatja rendszerét, ez ideális Windows és Linux rendszereket egyaránt tartalmazó hálózatokra.
- Tomcat kiszolgáló: Az Apache Tomcatet és a szükséges függőségeket telepíti: Java, gcj stb.
- Virtuálisgép-kiszolgáló: ez a KVM virtuális gépek futtatásához szükséges csomagokat telepíti.
- Csomagok kézi kiválasztása: elindítja az aptitude csomagkezelőt, lehetővé téve a csomagok egyedi kiválasztását.

A csomagcsoportok telepítése a tasksel segédprogram használatával történik. Az Ubuntu (vagy Debian) és más GNU/Linux disztribúciók között az egyik fontos különbség az, hogy a csomagok telepítésükkor ésszerű alapértelmezések használatára vannak beállítva, és ezek néha további szükséges információkat kérnek. Hasonlóan feladatok telepítésekor a csomagok nem csak telepítésre kerülnek, de teljesen integrált szolgáltatás biztosítására is be vannak állítva.

[5] https://help.ubuntu.com/10.04 LTS/installation-guide/

A számítási felhő feladatokkal kapcsolatos további információkért lásd: 3. szakasz - UEC [276].

A telepítési folyamat befejeződése után az elérhető feladatok listáját a következő parancs kiadásával érheti el:

```
tasksel --list-tasks
```

A kimenet más Ubuntu-alapú disztribúciók, például a Kubuntu és az Edubuntu feladatait is felsorolja. A tasksel parancsot önállóan is futtathatja, ekkor a különböző elérhető feladatokat tartalmazó menüt jeleníti meg.

A --task-packages kapcsoló használatával megjelenítheti az egyes feladatok által telepített csomagok listáját. A DNS-kiszolgáló feladat által telepített csomagok listájáért adja ki a következőt:

```
tasksel --task-packages dns-server
```

A parancs kimenete a következő kell legyen:

```
bind9-doc
bind9utils
bind9
```

Ha a telepítési folyamat során nem telepítette valamelyik feladatot, és később szükségessé válik, csak a telepítő CD-re van szüksége. Egy új LAMP-kiszolgálót például a következő parancs segítségével alakíthat egyben DNS-kiszolgálóvá:

```
sudo tasksel install dns-server
```

3. Frissítés

Számos lehetőség van az egyik Ubuntu kiadásról a másikra frissítésre. Ez a szakasz az ajánlott frissítési módszert mutatja be.

3.1. do-release-upgrade

A kiszolgáló változat frissítésének ajánlott módja a do-release-upgrade segédprogram használata. Ez az update-manager-core csomag része, nincsenek grafikus függőségei, és alapértelmezésben telepítve van.

A Debian-alapú rendszerek frissíthetők az apt-get dist-upgrade parancs kiadásával is. Ezzel együtt a do-release-upgrade használata javasolt, mivel ez képes kezelni a kiadások között néha előforduló konfigurációváltozásokat.

Újabb kiadásra frissítéshez adja ki a következő parancsot:

```
do-release-upgrade
```

A do-release-upgrade használható az Ubuntu fejlesztői verziójára frissítésre is. Ehhez használja a -d kapcsolót:

```
do-release-upgrade -d
```

A fejlesztői kiadásra való frissítés nem ajánlott éles környezetben.

4. Speciális telepítés

4.1. Szoftveres RAID

A RAID több merevlemez egy lemezként való viselkedésének beállítására szolgál, ezzel csökkentve a merevlemez meghibásodásakor bekövetkező katasztrofális adatvesztés valószínűségét. Léteznek szoftveres (ekkor az operációs rendszer tud a lemezekről és aktívan karbantartja azokat) vagy hardveres (ekkor egy speciális vezérlő tartja karban a lemezeket, és elfedi azokat a rendszer elől, amely csak egy lemezt érzékel) RAID megvalósítások is.

A Linux (és Ubuntu) aktuális verzióiban található RAID szoftver az mdadm meghajtón alapul, és nagyon jól, sok úgynevezett „hardveres”RAID vezérlőnél is jobban működik. Ez a szakasz végigvezeti az Ubuntu kiszolgáló változatának két fizikai merevlemezen lévő két RAID1 partíció (egy a / és egy a swap számára) használatával történő telepítésén.

4.1.1. Particionálás

Kövesse a telepítési lépéseket, amíg el nem jut a Lemezek particionálása lépésig, ekkor:

1. Válassza a Kézi particionálási módot.
2. Válassza ki az első merevlemezt, és egyezzen bele az Új, üres partíciós tábla létrehozásába az eszközön.

   Ismételje meg ezt a lépést a RAID-tömb részévé tenni kívánt összes meghajtóra.
3. Válassza ki az üres helyet az első meghajtón, majd válassza az Új partíció létrehozása lehetőséget.
4. Ezután válassza ki a partíció méretét. Ez a partíció lesz a swap partíció, a méretére vonatkozó általános szabály, hogy a RAM méretének kétszerese kell legyen. Adja meg a partíció méretét, és válassza ki az Elsődleges, majd az Eleje lehetőséget.
5. Válassza ki a fenti Felhasználás: sort. Ennek értéke alapértelmezésben az Ext4 naplózó fájlrendszer, módosítsa ezt RAID fizikai kötetre, majd válassza a Partíció beállítása kész lehetőséget.
6. A / kötethez válassza ki újra az üres helyet az első meghajtón, majd az Új partíció létrehozása lehetőséget.
7. Használja fel a maradék szabad helyet a meghajtón, és válassza a Folytatás, majd az Elsődleges lehetőségeket.
8. A swap partícióhoz hasonlóan válassza ki a fenti Felhasználás: sort, módosítsa ezt RAID fizikai kötetre. Válassza ki az Indítási jelző: sort, és módosítsa be értékre, majd válassza a Partíció beállítása kész lehetőséget.
9. Ismételje meg a harmadik-nyolcadik lépéseket a másik lemezre és partíciókra.

4.1.2. RAID konfigurálása

A particionálás elkészültével a tömb készen áll a konfigurálásra:

1. A „Lemezek particionálása” oldalra visszalépve válassza a fenti Szoftveres RAID beállítása lehetőséget.
2. Válassza az Igen lehetőséget a módosítások lemezre írásához.
3. Válassza a Többlemezes eszköz létrehozása lehetőséget.
4. Ebben a példában a RAID1-et használjuk, de ha más összeállítást használ, akkor válassza ki az annak megfelelő típust (RAID0 RAID1 RAID5).

A RAID5 használatához legalább három meghajtó szükséges. A RAID0 vagy RAID1 használatához két meghajtó is elég.

5. Adja meg az aktív eszközök számát (2), vagy a tömbhöz használandó merevlemezeinek számát. Nyomja meg a Folytatás gombot.
6. Ezután adja meg a tartalékeszközök számát – alapértelmezésben 0, majd nyomja meg a Folytatás gombot.
7. Válassza ki a használandó partíciókat. Ezek általában sda1, sdb1, sdc1 stb. lehetnek. A számok jellemzően egyeznek, a különböző betűk pedig a különböző merevlemezeknek felelnek meg.

   A swap partícióhoz válassza az sda1 és sdb1 partíciókat. Nyomja meg a Folytatás gombot.
8. Ismételje meg a harmadik-hetedik lépéseket a / partícióhoz, az sda2 és sdb2 kiválasztásával.
9. Nyomja meg a Befejezés gombot.

4.1.3. Formázás

Most látnia kell a merevlemezek és RAID-eszközök listáját. A következő lépés a RAID-eszközök formázása és csatolási pontjuk beállítása. A RAID-eszközöket helyi merevlemeznek tekintve formázza és csatolja azokat.

1. Válassza az 1. lehetőséget az RAID1 0. eszköz partíció alatt.
2. Válassza a Felhasználás: sort, majd a lapozóterület, végül a Partíció beállítása kész lehetőséget.
3. Ezután válassza az 1. lehetőséget az RAID1 1. eszköz partíció alatt.
4. Válassza a Felhasználás: sort, majd az Ext4 naplózó fájlrendszer lehetőséget.
5. Ezután válassza a Csatolási pont, majd a / - a gyökér fájlrendszer lehetőséget. Módosítsa szükség szerint a további beállításokat, majd válassza a Partíció beállítása kész lehetőséget.
6. Végül válassza a Particionálás befejezése és a változtatások lemezre írása lehetőséget.

Ha a gyökér partíciót RAID-tömbre helyezi, akkor a telepítő megkérdezi, hogy szeretné-e leromlott állapotban is elindítani a rendszert. További részletekért lásd: 4.1.4. szakasz - Leromlott RAID [11].

A telepítési folyamat ezután normális módon folytatódik.

4.1.4. Leromlott RAID

Egy számítógép életében egyszer bekövetkezhet lemezhiba. Ha ez megtörténik, a szoftveres RAID használatakor az operációs rendszer a tömböt a leromlott néven ismert állapotba helyezi.

Ha a tömb az adatsérülés esélye miatt leromlottá vált, az Ubuntu kiszolgáló változata alapértelmezésben harminc másodperc után elindítja az initramfst. Az initramfs elindulása után tizenöt másodperc áll rendelkezésére eldönteni, hogy folytatja-e a rendszerindítást, vagy megpróbálja saját kezűleg helyreállítani. Az initramfs parancssorának elindítása helyzettől függően lehet kívánatos vagy nem kívánatos, különösen ha a gép távoli helyen van. A leromlott tömbön lévő rendszer indítása több módon is konfigurálható:

- A dpkg-reconfigure segédprogrammal beállítható az alapértelmezett viselkedés, és a folyamat során a tömbbel kapcsolatos további beállításokra is rákérdez, mint például a monitorozás, e-mail riasztások stb. Az mdadm újrakonfigurálásához adja ki a következőt:

  ```
  sudo dpkg-reconfigure mdadm
  ```

- A dpkg-reconfigure mdadm folyamat az `/etc/initramfs-tools/conf.d/mdadm` konfigurációs fájlt módosítja. A fájl előnye, hogy képes előzetesen beállítani a rendszer viselkedését, és saját kezűleg is szerkesztheti:

  ```
  BOOT_DEGRADED=true
  ```

  

  A konfigurációs fájl kernelparaméterek használatával felülbírálható.

- A kernelparaméterek használata lehetővé teszi a rendszernek a leromlott tömb elindítását is:
  - A kiszolgáló indulásakor nyomja meg a Shift billentyűt a Grub menü megnyitásához.
  - Nyomja meg az e billentyűt a kernel parancs paramétereinek szerkesztéséhez.
  - Nyomja meg a le nyilat a kernel sor kiemeléséhez.
  - A sor végére írja be a bootdegraded=true szöveget.
  - Nyomja meg a Ctrl+x billentyűkombinációt a rendszer elindításához.

Miután a rendszer elindult, megjavíthatja a tömböt (részletekért lásd: 4.1.5. szakasz - RAID karbantartása [12]), vagy súlyos hardverhiba esetén átmásolhatja a fontos adatokat másik gépre.

4.1.5. RAID karbantartása

Az mdadm segédprogrammal megjeleníthető a tömb állapota, lemezek adhatók a tömbhöz és távolíthatók el stb:

- Tömb állapotának megjelenítéséhez adja ki a következőt:

  ```
  sudo mdadm -D /dev/md0
  ```

  A -D hatására az mdadm részletes információkat jelenít meg a `/dev/md0` eszközről. A `/dev/md0` helyére a kívánt RAID-eszközt írja.

- Tömb egy lemezének állapotának megjelenítéséhez:

```
sudo mdadm -E /dev/sda1
```

A kimenet nagyon hasonló az mdadm -D parancséhoz, a `/dev/sda1` helyére a megfelelő eszközt írja.

- Ha egy lemez meghibásodik, és el kell távolítani a tömbből, adja ki a következőt:

```
sudo mdadm --remove /dev/md0 /dev/sda1
```

A `/dev/md0` és `/dev/sda1` helyére a megfelelő RAID-eszközt és lemezt írja.

- Hasonlóképpen új lemez hozzáadásához:

```
sudo mdadm --add /dev/md0 /dev/sda1
```

Néha a lemezek akkor is hibás állapotba kerülnek, ha fizikailag nincs semmi baj a lemezzel. Általában megéri a meghajtót eltávolítani a tömbből, és újra hozzáadni. Ennek hatására a lemez újraszinkronizálódik a tömbbel. Ha a meghajtó nem szinkronizál a tömbbel, az nagy valószínűséggel hardverhibát jelez.

A `/proc/mdstat` fájl is hasznos információkat tartalmaz a rendszer RAID-eszközeiről:

```
cat /proc/mdstat
Personalities : [linear] [multipath] [raid0] [raid1] [raid6] [raid5] [raid4] [raid10]
md0 : active raid1 sda1[0] sdb1[1]
      10016384 blocks [2/2] [UU]

unused devices: <none>
```

A következő parancs segítségével a szinkronizálódó meghajtó állapota figyelhető:

```
watch -n1 cat /proc/mdstat
```

A watch parancs leállításához nyomja meg a Ctrl+c billentyűkombinációt.

Ha egy hibás meghajtót cserélnie kell, akkor a csere és szinkronizálás után telepíteni kell a grubot. A grub új meghajtóra való telepítéséhez adja ki a következőt:

```
sudo grub-install /dev/md0
```

A `/dev/md0` helyére a megfelelő tömbeszköz nevét írja.

4.1.6. Információforrások

A RAID-tömbök témája a RAID beállítási lehetőségeinek tömege miatt nagyon összetett. A következő hivatkozásokon találhat további információkat:

- Ubuntu wiki cikkek a RAID-ről[6].
- Software RAID HOWTO[7]

- Managing RAID on Linux[8]

4.2. Logikaikötet-kezelő (LVM)

A logikaikötet-kezelő, vagy LVM lehetővé teszi a rendszergazdák számára logikai kötetek létrehozását egy vagy több fizikai merevlemezből. Az LVM kötetek létrehozhatók szoftveres RAID partíciókon és önálló lemezeken található szabványos partíciókból. A kötetek kiterjeszthetők, ezzel növelve a rendszer rugalmasságát az igények változása esetén.

4.2.1. Áttekintés

Az LVM hatékonyságának és rugalmasságának ára a bonyolultság nagyobb foka. Az LVM telepítési folyamatában való elmélyedés előtt meg kell ismerkednie néhány kifejezéssel:

- Kötetcsoport (VG): egy vagy több logikai kötet (LV) együttese.
- Logikai kötet (LV): hasonló a normál partíciókhoz. Több fizikai kötet (PV) alkothat egy LV-t, efölött helyezkedik el a tényleges EXT3, XFS, JFS stb fájlrendszer.
- Fizikai kötet (PV): a fizikai merevlemez vagy szoftveres RAID partíció. A kötetcsoport további PV-k hozzáadásával bővíthető.

4.2.2. Telepítés

Ez a szakasz példaként az Ubuntu kiszolgáló változatának telepítését mutatja be, ahol a `/srv` egy LVM kötetre van csatolva. A kiinduló telepítés során csak egy fizikai kötet (PV) lesz a kötetcsoport (VG) része. A telepítés után a VG kiterjesztésének bemutatása érdekében egy újabb PV lesz hozzáadva.

Számos lehetőség van az LVM telepítésére: Irányított - LVM beállítása a teljes lemezre, amely lehetővé tesz az elérhető hely egy részének LVM-hez rendelését, Irányított - titkosított LVM beállítása a teljes lemezre vagy Kézi is beállíthatja a partíciókat és az LVM-et. Jelenleg az LVM-et és normál partíciókat is használó rendszer beállítására telepítéskor csak a kézi megközelítés használható.

1. Kövesse a telepítési lépéseket, amíg el nem jut a Lemezek particionálása lépésig, ekkor:
2. A Lemezek particionálása képernyőn válassza a Kézi lehetőséget.
3. Válassza ki a merevlemezt, a következő képernyőn pedig válaszoljon igennel az Új, üres partíciós tábla létrehozása az eszközön kérdésre.
4. Ezután tetszőleges fájlrendszerrel hozza létre a normál /boot, swap, és / partíciókat.
5. Az LVM /srv számára hozzon létre egy új logikai partíciót. Ezután módosítsa a Felhasználás: mező értékét LVM fizikai kötetre, majd válassza a Partíció beállítása kész lehetőséget.
6. Most válassza a fenti A Logikaikötet-kezelő (LVM) beállítása lehetőséget, és nyomja meg az Igen gombot a változtatások lemezre írásához.
7. A következő képernyő LVM beállítási művelet: menüjében válassza a Kötetcsoport létrehozása lehetőséget. Adja meg a VG nevét, például vg01, vagy valami ennél beszédesebbet. A név megadása után válassza ki az LVM-hez konfigurált partíciót, és nyomja meg a Folytatás gombot.

8. Az LVM beállítási művelet: képernyőn válassza a Logikai kötet létrehozása lehetőséget. Válassza ki az újonnan létrehozott kötetcsoportot, és adja meg az új LV nevét, például srv, mert ez a tervezett csatolási pont. Válassza ki a méretet, ez lehet a teljes partíció, mivel később mindig bővíthető. Nyomja meg a Befejezés gombot, és visszakerül a fő Lemezek particionálása képernyőre.
9. Ezután vegyen fel egy fájlrendszert az új LVM-be. Válassza ki a partíciót az LVM VG vg01, LV srv (illetve a megadott név alatt), majd válassza a Felhasználás lehetőséget. Hozzon létre egy fájlrendszert a szokásos módon, ennek csatolási pontja legyen a /srv. Ha kész, válassza a Partíció beállítása kész lehetőséget.
10. Végül válassza a Particionálás befejezése és a változtatások lemezre írása lehetőséget. Erősítse meg a változtatásokat, és folytassa a telepítést.

Az LVM-mel kapcsolatos információk megjelenítésére hasznos segédprogramok szolgálnak:

- vgdisplay: a kötetcsoportokról jelenít meg információkat.
- lvdisplay: a logikai kötetekről jelenít meg információkat.
- pvdisplay: a fizikai kötetekről jelenít meg információkat.

4.2.3. Kötetcsoportok kiterjesztése

Továbbra is az srv-t használva példa LVM kötetként, ez a szakasz bemutatja egy második merevlemez hozzáadását, fizikai kötet (PV) létrehozását, a kötetcsoporthoz (VG) adását, az `srv` logikai kötet kiterjesztését, és végül a fájlrendszer kiterjesztését. Ez a példa feltételezi, hogy egy második merevlemez lett a rendszerhez adva. Ez a merevlemez a példában `/dev/sdb` néven szerepel. FIGYELEM: a lenti parancsok kiadása előtt győződjön meg róla, hogy nincs `/dev/sdb` nevű merevlemez a rendszerben. Ha nem üres lemezre adja ki a parancsokat, adatvesztés történhet. A példa a teljes lemezt felhasználja fizikai kötetként (választhatja partíciók létrehozását, és azok különböző fizikai kötetekként való használatát is).

1. Első lépésben hozza létre a fizikai kötetet a következő parancs kiadásával:

   ```
   sudo pvcreate /dev/sdb
   ```

2. Most terjessze ki a kötetcsoportot (VG):

   ```
   sudo vgextend vg01 /dev/sdb
   ```

3. A vgdisplay segítségével állapíthatja meg a szabad fizikai extentek (PE) számát - ezt a Free PE / size (a lefoglalható méret) sor tartalmazza. A példa 511 PE méretet feltételez (ez megfelel 2 GB-nak 4 MB-os PE méret mellett), és a teljes elérhető szabad helyet felhasználja. Ehelyett használja a saját PE és/vagy szabad hely értékeit.

   A logikai kötet (VG) most több módon is kiterjeszthető, ez a példa csak a PE használatát mutatja be:

```
sudo lvextend /dev/vg01/srv -l +511
```

A -l kapcsoló lehetővé teszi az LV kiterjesztését PE megadásával. A -L kapcsoló lehetővé teszi az LV kiterjesztését mega, giga, tera stb bájtok megadásával.

4. Noha az ext3 vagy ext4 fájlrendszer kiterjesztésére annak leválasztása nélkül is lehetőség van, érdemes inkább mindig leválasztani és ellenőrizni a fájlrendszert. Logikai kötet csökkentése esetén ugyanis a leválasztás kötelező, ezért ajánlott elkerülni a leválasztás nélküli módosítás megszokását.

   A következő parancsok ext3 vagy ext4 fájlrendszerhez használhatók. Más fájlrendszer használata esetén más segédprogramokat kell használni.

```
sudo umount /srv
sudo e2fsck -f /dev/vg01/srv
```

   Az e2fsck -f kapcsolója kikényszeríti az ellenőrzést akkor is, ha a fájlrendszer tisztának tűnik.

5. Végül méretezze át a fájlrendszert:

```
sudo resize2fs /dev/vg01/srv
```

6. Most csatolja a partíciót, és ellenőrizze a méretét.

```
mount /dev/vg01/srv /srv && df -h /srv
```

4.2.4. Információforrások

- Lásd az Ubuntu wiki LVM cikkeit[9].
- További információkért lásd az LVM HOWTO-t[10].
- Szintén remek információforrás az O'Reilly linuxdevcenter.com oldalán megjelent Managing Disk Space with LVM[11] cikk.
- Az fdisk-kel kapcsolatos további információkért lásd az fdisk kézikönyvoldalát[12].

3. fejezet - Csomagkezelés

Az Ubuntu átfogó, a szoftverek telepítésére, frissítésére, konfigurálására és eltávolítására használható csomagkezelő rendszert tartalmaz. A több, mint 24 000, Ubuntu rendszerhez készült szoftvercsomagot tartalmazó rendszerezett tárolók elérésének biztosításán túl a csomagkezelő rendszer tartalmaz függőségfeloldó képességeket, és képes szoftverfrissítések keresésére is.

Számos eszköz áll rendelkezésre az Ubuntu csomagkezelő rendszerének használatára, a rendszergazdák által gond nélkül automatizálható egyszerű parancssori segédprogramoktól az új Ubuntu felhasználóknak készült, könnyen kezelhető grafikus felületekig.

1. Bevezetés

Az Ubuntu csomagkezelő rendszere a Debian GNU/Linux disztribúció által használt rendszerből származik. A csomagfájlok minden szükséges fájlt, metaadatot és utasítást tartalmaznak, amely egy adott funkcionalitás vagy szoftveralkalmazás megvalósításához szükséges a számítógépen.

A Debian csomagfájljai általában a „.deb” kiterjesztéssel rendelkeznek, és általában tárolókban találhatók, amelyek különböző adathordozókon vagy online megtalálható csomagok gyűjteményei. A csomagok általában előre lefordított, bináris formában vannak, így a telepítés gyors, és nem igényli szoftverek fordítását.

Számos összetett csomag használja a függőségek fogalmát. A függőségek az elsődleges csomag megfelelő működéséhez szükséges további csomagokat jelentik. A Festival nevű beszédszintetizátor csomagja a libasound2 csomagtól függ, amely az ALSA nevű, hanglejátszáshoz szükséges programkönyvtárat tartalmazza. A Festival megfelelő működéséhez ezt és minden függőségét telepíteni kell. Az Ubuntu szoftverkezelő eszközei ezt automatikusan elvégzik.

2. A dpkg

A dpkg egy Debian alapú rendszerekhez készült csomagkezelő. Képes csomagok telepítésére, eltávolítására és összeállítására, de más csomagkezelő rendszerekkel szemben nem képes csomagok és függőségeik automatikus letöltésére és telepítésére. Ez a szakasz bemutatja a dpkg használatát helyileg telepített csomagok kezelésére:

- A rendszerre telepített összes csomag felsorolásához adja ki a következő parancsot:

```
dpkg -l
```

- A rendszeren lévő csomagok mennyiségétől függően ez egy hosszú listát eredményezhet. A kimenetet átvezetve a grep parancson kideríthető, hogy egy adott csomag telepítve van-e:

```
dpkg -l | grep apache2
```

  Az apache2 helyére tetszőleges csomagnevet, csomagnévrészletet vagy más reguláris kifejezést írhat.

- Egy csomag (ebben az esetben az ufw) által telepített fájlok felsorolásához adja ki a következőt:

```
dpkg -L ufw
```

- Ha nem biztos benne, melyik csomag telepített egy adott fájlt, a dpkg -S segíthet. Például:

```
dpkg -S /etc/host.conf
base-files: /etc/host.conf
```

  A kimenet szerint az `/etc/host.conf` a base-files csomag része.

  Számos fájl automatikusan kerül előállításra a csomag telepítési folyamata során, így noha a fájlrendszeren vannak, a dpkg -S nem tudja, melyik csomaghoz tartoznak.

- Helyi .deb csomagfájlt a következő parancs kiadásával telepíthet:

```
sudo dpkg -i zip_2.32-1_i386.deb
```

  A `zip_2.32-1_i386.deb` helyére a helyi .deb fájl tényleges fájlnevét írja.

- Csomag eltávolításához adja ki:

```
sudo dpkg -r zip
```

  A csomagok eltávolítása a dpkg használatával általában NEM ajánlott. A rendszer konzisztens állapotának biztosítása érdekében jobb megoldás a függőségek kezelésére képes csomagkezelő használata. A dpkg -r használatával eltávolíthatja például a zip csomagot, de az ettől függő csomagok továbbra is telepítve maradnak, és lehetséges hogy nem fognak megfelelően működni.

A dpkg további kapcsolóival kapcsolatban nézze meg a kézikönyvet: man dpkg.

3. Apt-Get

Az apt-get egy hatékony, az Advanced Packaging Tool (APT) kezelésére szolgáló parancssori eszköz. Segítségével új szoftvercsomagok telepíthetők, a meglévő szoftvercsomagok mellett a csomaglistaindex, sőt akár az egész Ubuntu rendszer is frissíthető.

Egyszerű parancssori eszközként az apt-get számos előnyt biztosít a rendszergazdák számára az Ubuntuban elérhető más csomagkezelő rendszerekhez képest. Ezek közé tartozik a könnyed használhatóság terminálkapcsolaton (SSH) keresztül, vagy a rendszeradminisztrációs parancsfájlokban való használhatóság, amelyek viszont a cron ütemezőeszközzel automatizálhatók.

Az apt-get segédprogram gyakori felhasználási módjaira néhány példa:

- Csomag telepítése: A csomagok telepítése az apt-get eszközzel meglehetősen egyszerű. Az nmap nevű hálózatfelderítő eszköz telepítéséhez például adja ki a következő parancsot:

  ```
  sudo apt-get install nmap
  ```

- Csomag eltávolítása: Csomag vagy csomagok eltávolítása hasonlóan egyszerű. Az előző példában telepített nmap csomag eltávolításához adja ki a következő parancsot:

  ```
  sudo apt-get remove nmap
  ```

  

  Több csomag: szóközökkel elválasztva több telepítendő vagy eltávolítandó csomagot is megadhat.

  Az apt-get remove parancs --purge kapcsolója eltávolítja a csomag beállítófájljait is. Ez egyaránt lehet hasznos vagy nemkívánatos, ezért óvatosan használja.

- A csomagindex frissítése: Az APT csomagindex alapvetően az `/etc/apt/sources.list` fájlban megadott tárolókban elérhető csomagok adatbázisa. Adja ki a következő parancsot a helyi csomagindex frissítéséhez a tárolók legfrissebb változásaival:

  ```
  sudo apt-get update
  ```

- Csomagok frissítése: Az idő múlásával a számítógépre telepített csomagok (például biztonsági frissítésekkel) frissített verziói válhatnak elérhetővé a csomagtárolókban. A rendszer frissítéséhez először frissítse a csomagindexet a fenti módon, majd adja ki a következő parancsot:

  ```
  sudo apt-get upgrade
  ```

  Az új Ubuntu kiadásokra frissítéssel kapcsolatos információkért lásd a 3. szakasz - Frissítés [9] szakaszt.

Az apt-get parancs műveletei, például csomagok telepítése és eltávolítása, a /var/log/dpkg.log naplófájlban kerülnek naplózásra.

Az APT használatával kapcsolatos további információkért lásd az átfogó Debian APT felhasználói kézikönyvet[1] vagy adja ki a következő parancsot:

```
apt-get help
```

[1] http://www.debian.org/doc/user-manuals#apt-howto

4. Aptitude

Az Aptitude egy menüvezérlésű szöveges felület az Advanced Packaging Tool (APT) rendszerhez. Számos gyakori csomagkezelési feladat, mint például a telepítés, eltávolítás és frissítés, az Aptitude-ban egybillentyűs (jellemzően kisbetűs) parancsokkal hajtható végre.

Az Aptitude a parancsbillentyűk megfelelő működésének biztosítása érdekében a nem grafikus terminálkörnyezetekben a leghasználhatóbb. Az Aptitude normál felhasználóként való indításához adja ki a következő parancsot a terminálban:

```
sudo aptitude
```

Az Aptitude indulásakor a képernyő tetején egy menüsor, alatta pedig két panel jelenik meg. A felső panel a csomagkategóriákat tartalmazza, mint például az Új csomagok és a Nem telepített csomagok. Az alsó panel a csomagokkal és csomagkategóriákkal kapcsolatos információkat tartalmaz.

Az Aptitude használata viszonylag egyértelmű, a felhasználói felület pedig egyszerűvé teszi a gyakori feladatok végrehajtását. A következő példák gyakori csomagkezelési műveletek az Aptitude használatával történő végrehajtását mutatják be:

- Csomagok telepítése: Csomag telepítéséhez keresse meg azt a Nem telepített csomagok kategóriában, például a nyílbillentyűk és az Enter használatával, és jelölje ki a telepítendő csomagot. A csomag kijelölése után nyomja meg a + billentyűt, ekkor a csomag színe zöldre változik, jelezve a telepítésre történt kiválasztását. Ezután nyomja meg a g billentyűt a csomagműveletek listájának megjelenítéséhez. Nyomja meg újra a g billentyűt, és a program bekéri a rendszergazdai jelszót a telepítés befejezéséhez. Az Enter megnyomása után megadhatja jelszavát. Végül nyomja meg még egyszer a g billentyűt, és a program rákérdez a csomag letöltésére. Nyomja meg az Enter billentyűt a Folytatás üzenet megjelenésekor, ekkor megtörténik a csomagok letöltése és telepítése.
- Csomagok eltávolítása: Csomag eltávolításához keresse meg azt a Telepített csomagok kategóriában, például a nyílbillentyűk és az Enter használatával, és jelölje ki az eltávolítandó csomagot. A csomag kijelölése után nyomja meg a - billentyűt, ekkor a csomag színe rózsaszínre változik, jelezve az eltávolításra történt kiválasztását. Ezután nyomja meg a g billentyűt a csomagműveletek listájának megjelenítéséhez. Nyomja meg újra a g billentyűt, és a program bekéri a rendszergazdai jelszót a telepítés befejezéséhez. Az Enter megnyomása után megadhatja jelszavát. Végül nyomja meg még egyszer a g billentyűt, és a program rákérdez a csomag letöltésére. Nyomja meg az Enter billentyűt a Folytatás üzenet megjelenésekor, ekkor megtörténik a csomagok eltávolítása.
- Csomagindex frissítése: A csomagindex frissítéséhez nyomja meg az u billentyűt, és a program bekéri a rendszergazdai jelszót a frissítés befejezéséhez. Az Enter megnyomása után megadhatja jelszavát. Végül nyomja meg még egyszer az Enter billentyűt az OK üzenet megjelenésekor a folyamatot befejező letöltési ablakban.
- Csomagok frissítése: Csomagok frissítéséhez hajtsa végre a csomagindex frissítését a fent részletezett módon, majd nyomja meg az U billentyűt az összes frissítés kijelöléséhez. Ezután

nyomja meg a g billentyűt, és megkapja a csomagműveletek összefoglalását. Ezután nyomja meg a g billentyűt a csomagműveletek listájának megjelenítéséhez. Nyomja meg újra a g billentyűt, és a program bekéri a rendszergazdai jelszót a telepítés befejezéséhez. Az Enter megnyomása után megadhatja jelszavát. Végül nyomja meg még egyszer a g billentyűt, és a program rákérdez a csomagok letöltésére. Nyomja meg az Enter billentyűt a Folytatás üzenet megjelenésekor, ekkor megtörténik a csomagok frissítése.

A csomaglisták megjelenítésekor a felső ablaktábla csomaglistájának első oszlopa leírja a csomag aktuális állapotát, és a következő jelöléseket használja a csomag állapotának leírására:

- i: Telepített csomag
- c: A csomag nincs telepítve, de a csomag beállításai a rendszeren maradtak.
- p: A csomag a beállításaival együtt törölve a rendszerről
- v: Virtuális csomag
- B: Törött csomag
- u: A csomag fájljai kibontva, de még nincs konfigurálva
- C: Félig konfigurált - a konfigurálás meghiúsult, és javítást igényel
- H: Félig telepített - az eltávolítás meghiúsult, és javítást igényel

Az Aptitude-ból való kilépéshez nyomja meg a q billentyűt, és erősítse meg, hogy ki szeretne lépni. Az Aptitude menüjéből számos más funkció is elérhető az F10 billentyű megnyomásával.

5. Automatikus frissítések

A frissített csomagok automatikus telepítésére az unattended-upgrades csomag használható, ez beállítható az összes csomag frissítésére, vagy csak a biztonsági frissítések telepítésére is. Első lépésként telepítse a csomagot a következő parancs kiadásával:

```
sudo apt-get install unattended-upgrades
```

Az unattended-upgrades beállításához szerkessze az `/etc/apt/apt.conf.d/50unattended-upgrades` fájlt, és módosítsa igényeinek megfelelően a következőket:

```
Unattended-Upgrade::Allowed-Origins {
        "Ubuntu lucid-security";
//      "Ubuntu lucid-updates";
};
```

Bizonyos csomagok feketelistára tehetők, így automatikus frissítésük letiltható. Egy csomag feketelistára tételéhez vegye fel azt az alábbi listába:

```
Unattended-Upgrade::Package-Blacklist {
//      "vim";
//      "libc6";
//      "libc6-dev";
//      "libc6-i686";
};
```

A dupla „//” megjegyzésként szolgál, így a „//” után következő szöveg nem lesz kiértékelve.

Az automatikus frissítések engedélyezéséhez szerkessze az `/etc/apt/apt.conf.d/10periodic` fájlt, és adja meg az apt megfelelő beállításait:

```
APT::Periodic::Update-Package-Lists "1";
APT::Periodic::Download-Upgradeable-Packages "1";
APT::Periodic::AutocleanInterval "7";
APT::Periodic::Unattended-Upgrade "1";
```

A fenti beállítások minden nap frissítik a csomaglistát, letöltik és telepítik az elérhető frissítéseket. A helyi letöltési archívum minden héten kiürítésre kerül.

Az apt Periodic beállítási lehetőségeiről az `/etc/cron.daily/apt` parancsfájl fejlécében is olvashat.

Az unattended-upgrades futásának eredményei a `/var/log/unattended-upgrades` fájlban kerülnek naplózásra.

5.1. Értesítések

Az Unattended-Upgrade::Mail beállítása az `/etc/apt/apt.conf.d/50unattended-upgrades` fájlban lehetővé teszi e-mail küldését a rendszergazdának a frissítést igénylő, vagy problémás csomagokról.

Szintén hasznos csomag az apticron. Az apticron beállít egy cron feladatot, amely e-mailt küld a rendszergazdának a rendszeren lévő, frissítést igénylő csomagokról, valamint azok változásairól.

Az apticron csomag telepítéséhez adja ki a következő parancsot:

```
sudo apt-get install apticron
```

A csomag telepítése után szerkessze az `/etc/apticron/apticron.conf` fájlt az e-mail cím és más beállítások megadása érdekében:

```
EMAIL="root@példa.hu"
```

6. Beállítás

Az Advanced Packaging Tool (APT) rendszer tárolóinak beállításai az /etc/apt/sources.list konfigurációs fájlban vannak. Alább látható egy példafájl, a tárolóhivatkozások hozzáadásával vagy eltávolításával kapcsolatos információkkal együtt.

Itt[2] találhat egy tipikus `/etc/apt/sources.list` fájlt bemutató egyszerű példafájlt.

A fájl szerkesztésével engedélyezheti vagy letilthatja a tárolókat. Ha például le szeretné tiltani az Ubuntu CD-ROM használatát a csomagműveletekhez, akkor tegye megjegyzésbe a CD-ROM-nak megfelelő sort, amely a fájl tetején található:

```
# ne kérje többé a CD-ROM-ot
# deb cdrom:[Ubuntu 10.04_Lucid_Lynx - Release i386 (20100429.1)]/ lucid main restricted
```

6.1. Kiegészítő tárolók

Az Ubuntuhoz elérhető hivatalosan támogatott csomagtárolókon kívül további, közösség által támogatott tárolók is léteznek, amelyek több ezer telepíthető csomagot tartalmaznak. A két legnépszerűbb a Universe és Multiverse tároló. Ezeket a tárolókat az Ubuntu hivatalosan nem támogatja, de mivel a közösség tartja ezeket karban, általában biztonságosan használható csomagokat tartalmaznak.

A Multiverse tárolóban lévő csomagok gyakran olyan licencelési problémákkal bírnak, amelyek megakadályozzák a szabad operációs rendszerrel együtt történő terjesztésüket, és egyes országokban illegálisak lehetnek.

Ne feledje, hogy sem a Universe, sem a Multiverse tároló nem tartalmaz hivatalosan támogatott csomagokat. Ez azt jelenti, hogy ezekhez a csomagokhoz nem biztos, hogy érkeznek biztonsági frissítések.

Számos más csomagforrás is elérhető, ezek néha csak egy csomagot tartalmaznak, mint például egy adott alkalmazás fejlesztője által biztosított csomagforrások esetén. Az ilyen nem szabványos csomagforrások használatakor óvatosnak és körültekintőnek kell lenni. Telepítés előtt vizsgálja meg a forrást és a csomagokat, mivel egyes csomagforrások és csomagjaik bizonyos szempontokból instabillá vagy működésképtelenné tehetik rendszerét.

Alapértelmezésben a Universe és Multiverse tárolók engedélyezve vannak. Ha le szeretné tiltani ezeket, szerkessze az `/etc/apt/sources.list` fájlt, és tegye megjegyzésbe a következőket:

```
deb http://archive.ubuntu.com/ubuntu lucid universe multiverse
deb-src http://archive.ubuntu.com/ubuntu lucid universe multiverse
```

[2] ../sample/sources.list

```
deb http://us.archive.ubuntu.com/ubuntu/ lucid universe
deb-src http://us.archive.ubuntu.com/ubuntu/ lucid universe
deb http://us.archive.ubuntu.com/ubuntu/ lucid-updates universe
deb-src http://us.archive.ubuntu.com/ubuntu/ lucid-updates universe

deb http://us.archive.ubuntu.com/ubuntu/ lucid multiverse
deb-src http://us.archive.ubuntu.com/ubuntu/ lucid multiverse
deb http://us.archive.ubuntu.com/ubuntu/ lucid-updates multiverse
deb-src http://us.archive.ubuntu.com/ubuntu/ lucid-updates multiverse

deb http://security.ubuntu.com/ubuntu lucid-security universe
deb-src http://security.ubuntu.com/ubuntu lucid-security universe
deb http://security.ubuntu.com/ubuntu lucid-security multiverse
deb-src http://security.ubuntu.com/ubuntu lucid-security multiverse
```

7. Hivatkozások

Az ezen szakaszban bemutatott ismeretek zöme megtalálható a man oldalakon, amelyek közül sok online is elérhető.

- Az InstallingSoftware[3] Ubuntu wiki oldal további információkat tartalmaz.
- A dpkg-val kapcsolatos további részletekért lásd a dpkg kézikönyvoldalát[4].
- Az APT HOWTO[5] és az apt-get kézikönyvoldala[6] az apt-get használatával kapcsolatos hasznos információkat tartalmaznak.
- Az aptitude további lehetőségeivel kapcsolatban lásd az aptitude kézikönyvoldalát[7].
- Az Ubuntu wiki Adding Repositories HOWTO[8] oldala a tárolók hozzáadásával kapcsolatban tartalmaz további részleteket.

4. fejezet - Hálózatkezelés

A hálózatok legalább két eszközből, például számítógépes rendszerekből, nyomtatókból és kapcsolódó berendezésekből állnak, amelyek az összekapcsolt eszközök közötti információmegosztás és -terjesztés érdekében fizikai kábelezéssel vagy vezeték nélküli kapcsolatokkal vannak összekötve.

Ez a szakasz általános és konkrét információkat tartalmaz a hálózatkezelésről, beleértve a hálózati fogalmak áttekintését, és a népszerű hálózati protokollok részletes ismertetését.

1. Hálózat beállítása

Az Ubuntu számos grafikus eszközt tartalmaz a hálózati eszközök beállításához. Ezt a leírást kiszolgálók rendszergazdáinak szántuk, ezért a hálózat parancssorból való kezelésére koncentrál.

1.1. Ethernet csatolók

Az Ethernet csatolókat a rendszer az ethX névmegállapodás alapján azonosítja, amelyben az X egy számot jelöl. Az első Ethernet csatolót általában eth0, a másodikat eth1, a továbbiakat pedig ehhez hasonlóan egyre nagyobb értékek jelölik.

1.1.1. Ethernet csatolók azonosítása

Az elérhető Ethernet csatolók gyors azonosítására az ifconfig parancsot használhatja, a következő módon:

```
ifconfig -a | grep eth
eth0      Link encap:Ethernet  HWaddr 00:15:c5:4a:16:5a
```

A rendszeren elérhető összes hálózati csatoló azonosítására használható az lshw parancs is. Az alábbi példában az lshw egyetlen Ethernet csatolót jelenít meg eth0 néven, a buszinformációkkal, meghajtóprogram részleteivel és az összes támogatott képességgel együtt.

```
sudo lshw -class network
  *-network
       description: Ethernet interface
       product: BCM4401-B0 100Base-TX
       vendor: Broadcom Corporation
       physical id: 0
       bus info: pci@0000:03:00.0
       logical name: eth0
       version: 02
       serial: 00:15:c5:4a:16:5a
       size: 10MB/s
       capacity: 100MB/s
       width: 32 bits
       clock: 33MHz
       capabilities: (snipped for brevity)
       configuration: (snipped for brevity)
       resources: irq:17 memory:ef9fe000-ef9fffff
```

1.1.2. Ethernet csatolók logikai nevei

A csatolók logikai nevei az `/etc/udev/rules.d/70-persistent-net.rules` fájlban vannak megadva. Ha szeretné befolyásolni, hogy melyik csatoló melyik logikai nevet kapja, akkor keresse meg a csatoló fizikai MAC-címének megfelelő sort, és módosítsa az NAME=ethX kulcs értékét a kívánt logikai névre. A változtatások véglegesítéséhez indítsa újra a rendszert.

```
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*", ATTR{address}=="00:15:c5:4a:16:5a", ATTR{dev_id}=="
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*", ATTR{address}=="00:15:c5:4a:16:5b", ATTR{dev_id}=="
```

1.1.3. Ethernet csatolók beállításai

Az ethtool program az Ethernet-kártyák beállításainak, például az automatikus egyeztetés, portsebesség, duplex mód és Wake-on-LAN megjelenítésére és módosítására szolgál. Alapértelmezésben nincs telepítve, de a tárolókból elérhető:

```
sudo apt-get install ethtool
```

A következő példa bemutatja egy Ethernet csatoló támogatott szolgáltatásainak és megadott beállításainak megjelenítését:

```
sudo ethtool eth0
Settings for eth0:
        Supported ports: [ TP ]
        Supported link modes:   10baseT/Half 10baseT/Full
                                100baseT/Half 100baseT/Full
                                1000baseT/Half 1000baseT/Full
        Supports auto-negotiation: Yes
        Advertised link modes:  10baseT/Half 10baseT/Full
                                100baseT/Half 100baseT/Full
                                1000baseT/Half 1000baseT/Full
        Advertised auto-negotiation: Yes
        Speed: 1000Mb/s
        Duplex: Full
        Port: Twisted Pair
        PHYAD: 1
        Transceiver: internal
        Auto-negotiation: on
        Supports Wake-on: g
        Wake-on: d
        Current message level: 0x000000ff (255)
        Link detected: yes
```

Az ethtool paranccsal végzett módosítások ideiglenesek, és újraindításkor elvesznek. Ha meg szeretné őrizni a beállításokat, egyszerűen vegye fel a kívánt ethtool parancsot az `/etc/network/interfaces` csatolókonfigurációs fájl pre-up utasításába.

A következő példa bemutatja, hogy az eth0 nevű csatoló hogyan állítható be véglegesen 1000 Mb/s portsebességű, full duplex módú működésre.

```
auto eth0
iface eth0 inet static
pre-up /usr/sbin/ethtool -s eth0 speed 1000 duplex full
```

Noha a fenti példában a csatoló a statikus módszer használatára van beállítva, más módszerekkel, például DHCP-vel is működik. A példa csak a pre-up utasítás megfelelő elhelyezését mutatja be a csatolókonfiguráció többi részéhez képest.

1.2. IP-címzés

A következő szakasz leírja a rendszer helyi hálózaton és az interneten való kommunikációjához szükséges IP-címének és alapértelmezett átjárójának beállítási módját.

1.2.1. Ideiglenes IP-cím kiosztása

Ideiglenes hálózati beállításokhoz használhatja a hagyományos ip, ifconfig és route parancsokat, amelyek más GNU/Linux operációs rendszerekben is megtalálhatók. Ezek a parancsok azonnal életbe lépő beállítások megadását teszik lehetővé, de azok nem állandóak, és újraindítás után elvesznek.

IP-cím ideiglenes beállítására az ifconfig parancsot használhatja a következő módon. Módosítsa az IP-címet és alhálózati maszkot a helyi hálózatnak megfelelően.

```
sudo ifconfig eth0 10.0.0.100 netmask 255.255.255.0
```

Az eth0 IP-címének ellenőrzésére az ifconfig parancsot használhatja a következő módon.

```
ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:15:c5:4a:16:5a
          inet addr:10.0.0.100  Bcast:10.0.0.255  Mask:255.255.255.0
          inet6 addr: fe80::215:c5ff:fe4a:165a/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:466475604 errors:0 dropped:0 overruns:0 frame:0
          TX packets:403172654 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2574778386 (2.5 GB)  TX bytes:1618367329 (1.6 GB)
          Interrupt:16
```

Alapértelmezett átjáró beállítására a route parancsot használhatja a következő módon. Módosítsa az alapértelmezett átjáró címét a helyi hálózatnak megfelelően.

```
sudo route add default gw 10.0.0.1 eth0
```

Az alapértelmezett átjáró beállításainak ellenőrzésére a route parancsot használhatja a következő módon.

```
route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
10.0.0.0        0.0.0.0         255.255.255.0   U     1      0        0 eth0
0.0.0.0         10.0.0.1        0.0.0.0         UG    0      0        0 eth0
```

Ha az ideiglenes hálózathoz DNS-re is szüksége van, akkor a DNS-kiszolgáló IP-címét az `/etc/resolv.conf` fájlba veheti fel. Az alábbi példa bemutatja, hogyan vehet fel két DNS-kiszolgálót az `/etc/resolv.conf` fájlba, amelyet a helyi kiszolgálóknak megfelelően kell módosítani. A DNS-kliens beállításának részletesebb leírása a következő szakaszban található.

```
nameserver 8.8.8.8
nameserver 8.8.4.4
```

Ha már nincs szüksége ezekre a beállításokra, és egy csatoló összes IP-beállítását törölni szeretné, akkor használja az ip parancsot a flush kapcsolóval, a következő módon:

```
ip addr flush eth0
```

Az IP-beállítások törlése az ip paranccsal nem törli az `/etc/resolv.conf` fájl tartalmát. Azokat a bejegyzéseket saját kezűleg kell eltávolítania vagy módosítania.

1.2.2. Dinamikus IP-címkiosztás (DHCP-kliens)

A kiszolgálójának dinamikus címkiosztáshoz DHCP használatára való beállításához vegye fel a dhcp módszert az inet címcsalád utasításához az `/etc/network/interfaces` fájlban. Az alábbi példa feltételezi, hogy az eth0 nevű első csatolót állítja be.

```
auto eth0
iface eth0 inet dhcp
```

A fentihez hasonló csatolóbeállítás felvétele után a csatolót az ifup paranccsal saját kezűleg engedélyezheti, amely a DHCP folyamatot a dhclient segítségével indítja el.

```
sudo ifup eth0
```

A csatoló kézi letiltásához az ifdown parancs használható, amely kezdeményezni fogja a DHCP-elengedési eljárást, és leállítja a csatolót.

```
sudo ifdown eth0
```

1.2.3. Statikus IP-címkiosztás

A rendszerének statikus IP-címkiosztás használatára való beállításához vegye fel a static módszert a megfelelő csatoló inet címcsalád utasításához az `/etc/network/interfaces` fájlban. Az alábbi példa feltételezi, hogy az eth0 nevű első csatolót állítja be. Módosítsa a address, netmask, és gateway értékeket a hálózatnak megfelelően.

```
auto eth0
iface eth0 inet static
address 10.0.0.100
```

```
netmask 255.255.255.0
gateway 10.0.0.1
```

A fentihez hasonló csatolóbeállítás felvétele után a csatolót az ifup paranccsal saját kezűleg engedélyezheti.

```
sudo ifup eth0
```

A csatoló saját kezű kikapcsolásához az ifdown parancsot használhatja.

```
sudo ifdown eth0
```

1.2.4. Visszacsatolási felület

A visszacsatolási felületet a rendszer lo néven azonosítja, és alapértelmezésben a 127.0.0.1 IP-címmel rendelkezik. Az ifconfig paranccsal jeleníthető meg.

```
ifconfig lo
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:2718 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2718 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:183308 (183.3 KB)  TX bytes:183308 (183.3 KB)
```

Alapértelmezésben az `/etc/network/interfaces` fájlnak két, a visszacsatolási felület konfigurálásáért felelős sort kell tartalmaznia. Ajánlott az alapértelmezett beállítások megtartása, hacsak nincs valami külön célja a módosításukkal. Alább látható a két alapértelmezett sor.

```
auto lo
iface lo inet loopback
```

1.3. Névfeloldás

A névfeloldás az IP-alapú hálózatoknál az IP-címek gépnevekre leképezésének folyamata, amely egyszerűbbé teszi a hálózati erőforrások azonosítását. A következő szakasz elmagyarázza, hogyan állíthatja be megfelelően a rendszert a névfeloldás használatára DNS és statikus gépnév-rekordok használatával.

1.3.1. DNS-kliens beállítása

A rendszere a névfeloldáshoz DNS használatára való beállításához vegye fel a hálózatának megfelelő DNS-kiszolgálók IP-címeit az `/etc/resolv.conf` fájlba. Felvehet opcionális DNS-utótaglistákat, amelyek a hálózata tartományneveire illeszkednek.

Alább látható az `/etc/resolv.conf` példakonfigurációja a példa.hu tartományban lévő és két nyilvános DNS-kiszolgálót használó kiszolgálóhoz.

```
search példa.hu
nameserver 8.8.8.8
nameserver 8.8.4.4
```

A search beállítás használható több tartománynévvel is, így a DNS-lekérdezések a felvételi sorrendjükben kerülnek összefűzésre. Tegyük fel, hogy a hálózaton több altartományban szeretne keresni, a szülőtartomány a példa.hu, a két altartomány pedig a kereskedelem.példa.hu és dev.példa.hu.

Ha több tartományban is szeretne keresni, akkor a konfiguráció a következőképpen nézhet ki:

```
search példa.hu, kereskedelem.példa.hu, dev.példa.hu
nameserver 8.8.8.8
nameserver 8.8.4.4
```

Ha a kiszolgáló1 nevű gépet próbálja pingelni, akkor a rendszer a következő sorrendben kérdezi le automatikusan a DNS-től a teljes képzésű tartománynevet (FQDN):

1. kiszolgáló1.példa.hu
2. kiszolgáló1.kereskedelem.példa.hu
3. kiszolgáló1.dev.példa.hu

Ha nincs találat, akkor a DNS-kiszolgáló a notfound eredményt adja vissza, és a DNS-lekérdezés meghiúsul.

1.3.2. Statikus gépnevek

A statikus gépnevek helyileg definiált gépnév-IP leképezések az `/etc/hosts` fájlban. A `hosts` fájl bejegyzései alapértelmezésben elsőbbséget élveznek a DNS-sel szemben. Ez azt jelenti, hogy amikor a rendszer megpróbál feloldani egy gépnevet, és az illeszkedik az `/etc/hosts` egyik bejegyzésére, akkor nem fogja megpróbálni a rekordot megkeresni a DNS-ben. Egyes esetekben, különösen ha nincs szükség internet-hozzáférésre, akkor a korlátozott számú erőforrással kommunikáló kiszolgálók könnyedén beállíthatók a DNS helyett statikus gépnevek használatára.

Az alábbi példában egy olyan `hosts` fájl látható, amelyben több helyi kiszolgálót egyszerű gépnevek, álnevek és az azoknak megfelelő teljes képzésű tartománynevek (FQDN-ek) azonosítanak.

```
127.0.0.1 localhost
127.0.1.1 ubuntu-server
10.0.0.11 kiszolgáló1 vpn kiszolgáló1.példa.hu
10.0.0.12 kiszolgáló2 mail kiszolgáló2.példa.hu
10.0.0.13 kiszolgáló3 www kiszolgáló3.példa.hu
10.0.0.14 kiszolgáló4 file kiszolgáló4.példa.hu
```

A fenti példában figyelje meg, hogy minden kiszolgáló a név és FQDN mellett álnevet is kapott. A kiszolgáló1 a vpn álnevet kapta, a kiszolgáló2 a mail, a kiszolgáló3 a www végül a kiszolgáló4 a file álnéven is elérhető.

1.3.3. Névszolgáltatás-váltás beállítása

A rendszer által a gépnevek IP-címekké feloldásához használt módszer kiválasztási sorrendjét a Névszolgáltatás-váltás (NSS) `/etc/nsswitch.conf` nevű beállítófájlja vezérli. Ahogy az előző szakaszban említettük, a rendszer `/etc/hosts` fájljában megadott statikus gépnevek elsőbbséget élveznek a DNS használatával feloldott nevekkel szemben. A következő példa bemutatja a gépnévkikeresés sorrendjéért felelős sorokat az `/etc/nsswitch.conf` fájlban.

```
hosts:          files mdns4_minimal [NOTFOUND=return] dns mdns4
```

- A files elsőként megpróbálja feloldani az `/etc/hosts` fájlban lévő statikus gépneveket.
- Az mdns4_minimal multicast DNS segítségével próbálja meg feloldani a nevet.
- A [NOTFOUND=return] azt jelenti, hogy az előző mdns4_minimal folyamattól kapott notfound válasz véglegesnek tekintendő, és a rendszer nem próbálkozik tovább választ kapni.
- A dns az öröklött unicast DNS lekérdezést jelképezi.
- Az mdns4 multicast DNS lekérdezést jelent.

A fent említett névfeloldási módszerek módosításához egyszerűen átírhatja a hosts: karakterláncot az Önnek megfelelőre. Ha például az örökölt unicast DNS-t szeretné inkább használni a multicast DNS helyett, akkor a következőképpen módosítsa az `/etc/nsswitch.conf` fájlban lévő karakterláncot:

```
hosts:          files dns [NOTFOUND=return] mdns4_minimal mdns4
```

1.4. Híd

Több csatoló összekötése híddal már speciálisabb konfigurációnak számít, de sok esetben nagyon hasznos. Az egyik ilyen eset, ha beállít egy több hálózati csatolót összekötő hidat, majd tűzfal segítségével szűri a forgalmat két hálózatszakasz között. A másik eset lehet a híd használata egy egyetlen csatolóval rendelkező gépen virtuális gépek közvetlen internet-hozzáférésének biztosításához. Az alábbi példa az utóbbi esetet mutatja be.

A híd beállítása előtt telepítenie kell a bridge-utils csomagot. Ehhez adja ki a következő parancsot:

```
sudo apt-get install bridge-utils
```

Ezután állítsa be a hidat az `/etc/network/interfaces` fájl szerkesztésével:

```
auto lo
iface lo inet loopback
```

```
auto br0
iface br0 inet static
        address 192.168.0.10
        network 192.168.0.0
        netmask 255.255.255.0
        broadcast 192.168.0.255
        gateway 192.168.0.1
        bridge_ports eth0
        bridge_fd 9
        bridge_hello 2
        bridge_maxage 12
        bridge_stp off
```

Adja meg a fizikai csatolónak és hálózatnak megfelelő értékeket.

Most indítsa újra a hálózatkezelést a híd csatoló bekapcsolásához:

```
sudo /etc/init.d/networking restart
```

Az új hídcsatolónak ezután működnie kell. A brctl segítségével hasznos információkat kaphat a híd állapotáról, vezérelheti hogy mely csatolók képezik a híd részét stb. További információkért lásd a man brctl kézikönyvoldalt.

1.5. Információforrások

- Az Ubuntu wiki Network oldala[1] hivatkozásokat tartalmaz a speciális hálózatbeállításokkal kapcsolatos cikkekre.
- Az interfaces kézikönyvoldal[2] tartalmazza az `/etc/network/interfaces` fájl beállítási lehetőségeivel kapcsolatos részleteket.
- A dhclient kézikönyvoldala[3] tartalmazza a DHCP-kliens további beállítási lehetőségeivel kapcsolatos részleteket.
- A DNS-kliensek beállításával kapcsolatos további információkért lásd a resolver kézikönyvoldalát[4]. Az O'Reilly Linux Network Administrator's Guide[5] kiadványának 6. fejezete is hasznos információforrás a resolverrel és a névszolgáltatás beállítási információival kapcsolatban.
- A hidakkal kapcsolatos további információkért lásd a brctl kézikönyvoldalát[6] és a Linux Foundation Net:Bridge[7] oldalát.

2. TCP/IP

A TCP/IP a hetvenes évek végén a DARPA által különböző számítógéptípusok és számítógépes hálózatok közötti kommunikáció eszközeként kifejlesztett protokollok általános halmaza. A TCP/IP az internetet hajtó erő, így a Föld legnépszerűbb hálózati protokolljainak halmaza.

2.1. A TCP/IP bemutatása

A TCP/IP két protokollkomponense a számítógépek hálózatkezelésének különböző területeit kezeli. Az Internet Protocol (IP) egy kapcsolat nélküli protokoll, amely csak a hálózati csomagok irányításával foglakozik, a hálózatkezelési információk alapegységeként az IP datagramot használva. Az IP datagram egy fejlécből és az azt követő üzenetből áll. A Transmission Control Protocol (TCP) lehetővé teszi a hálózat gépei számára adatfolyamok kicserélésére használható kapcsolatok létrehozását. A TCP garantálja az adatok kézbesítését a kapcsolatok között, és hogy az egyik hálózati kiszolgálóra ugyanabban a sorrendben érkezik, mint amelyben a másik elküldte.

2.2. TCP/IP beállítása

A TCP/IP protokoll beállítása számos elemből áll, amelyeket a megfelelő konfigurációs fájlok szerkesztésével, vagy a DHCP-kiszolgálóhoz hasonló, a hálózati klienseknek megfelelő hálózati beállítások automatikus biztosítására beállítható megoldások telepítésével kell elvégezni. Ezeket a konfigurációs értékeket megfelelően kell beállítani az ubuntus rendszer megfelelő hálózati működtetésének megkönnyítése érdekében.

A TCP/IP általános konfigurációs elemei, és azok céljai a következők:

- IP-cím Az IP-cím egy egyedi azonosító karakterlánc, amelyet négy, pontokkal elválasztott, 0 és 255 közötti decimális szám fejez ki, a négy szám mindegyike a cím 8 bitjét képviseli, így a teljes cím 32 bites. Ezt pontozott formátumnak nevezzük.
- Hálózati maszk Az alhálózati maszk (vagy egyszerűen hálózati maszk) egy helyi bitmaszk, vagy jelzők halmaza, amely elválasztja egymástól az IP-címek hálózatra és alhálózatra vonatkozó részeit. Egy C osztályú hálózatban például a szabványos hálózati maszk a 255.255.255.0, amely az IP-cím első három bájtját maszkolja, és az IP-cím utolsó bájtját tartja fenn az alhálózat gépeinek megadására.
- Hálózati cím A hálózati cím az IP-cím hálózati részét alkotó bájtokat képviseli. A 12.128.1.2 című gép egy A osztályú hálózaton például a 12.0.0.0 hálózati címet használja, ahol a 12 képviseli az IP-cím első bájtját (a hálózati rész) és a nullák a maradék három bájton a gépek azonosítására használható értékeket. A 192.168.1.100 privát IP-címet használó gép viszont a 192.168.1.0 hálózati címet használja, amely megadja a 192.168.1 C osztályú hálózat első három bájtját, valamint egy darab nullát a hálózaton elhelyezhető összes gép számára.
- Üzenetszórási cím Az üzenetszórási cím lehetővé teszi hálózati adatok egyidejű elküldését egy adott gép helyett a hálózat összes gépének. A szabványos általános üzenetszórási cím az IP-hálózatokon a 255.255.255.255, de ez az üzenetszórási cím nem használható szórt üzenetek

küldésére az internet minden gépére, mert a routerek blokkolják. A ténylegesen használható üzenetszórási címek egy adott alhálózatra illeszkednek. A privát C osztályú 192.168.1.0 hálózaton például az üzenetszórási cím a 192.168.1.255. A szórt üzeneteket általában hálózati protokollok állítják elő, mint például az ARP vagy a RIP.

- Átjárócím Az átjárócím az az IP-cím, amelyen keresztül egy adott hálózat vagy gép elérhető. Ha egy hálózati gép kommunikálni próbál egy másik hálózati géppel, és az a gép nem ugyanabban a hálózatban van, akkor egy átjárót kell használni. Sok esetben az átjárócím ugyanazon hálózat routerének címe, amely a forgalmat továbbítja más hálózatokra vagy gépekre, például internetes gépekre. Az átjárócím értékének helyesnek kell lennie, különben a rendszer nem lesz képes az azonos hálózatban lévő gépeken kívül más gépekhez csatlakozni.
- Névkiszolgáló címe A névkiszolgáló címe azon DNS-rendszerek IP-címeit képviseli, amelyek a gépneveket IP-címekké oldják fel. A névkiszolgálócímeknek három szintjük van: az elsődleges, a másodlagos és a harmadlagos névkiszolgáló. Ahhoz, hogy a rendszer képes legyen hálózati gépnevek feloldására az azoknak megfelelő IP-címekké, olyan érvényes névkiszolgálócímeket kell megadnia a rendszere TCP/IP beállításaiban, amelyek használatára jogosult. Sok esetben ezeket a címeket az Ön internetszolgáltatója biztosítja, de sok ingyenesen és nyilvánosan elérhető névkiszolgáló is használható, mint például a 4.2.2.1 és 4.2.2.6 közti 3. szintű (Verizon) kiszolgálók.

Az IP-címet, hálózati maszkot, hálózati címet, üzenetszórási címet és az átjáró címét általában az `/etc/network/interfaces` fájl megfelelő direktívái adják meg. A névkiszolgálók címeit általában az `/etc/resolv.conf` fájl nameserver direktívái adják meg. További információkért nézze meg az `interfaces` vagy a `resolv.conf` kézikönyvoldalát, a következő parancsok kiadásával:

Az `interfaces` fájl kézikönyvoldalának eléréséhez adja ki a következő parancsot:

```
man interfaces
```

A `resolv.conf` fájl kézikönyvoldalának eléréséhez adja ki a következő parancsot:

```
man resolv.conf
```

2.3. IP-útválasztás

Az IP-útválasztás a TCP/IP hálózatokon útvonalak megadásának és felfedezésének eszköze, amelyeken az adatok küldhetők. Az útválasztás útválasztási táblák halmazának segítségével irányítja az adatcsomagok továbbítását forrásuktól a céljukig, gyakran több köztes, útválasztó néven ismert hálózati csomóponton keresztül. Az útválasztásnak két elsődleges módja van: a statikus útválasztás és a dinamikus útválasztás.

A statikus útválasztás az IP-útvonalak kézi felvételét jelenti a rendszer útválasztási táblájába, és általában az útválasztási tábla a route paranccsal való manipulálásával végzik. A statikus útválasztás számos előnnyel rendelkezik a dinamikussal szemben, mint például a megvalósítás egyszerűsége kisebb hálózatokon, kiszámíthatóság (az útválasztási tábla mindig előre kerül kiszámításra, így az

útvonal minden használatkor pontosan ugyanaz), és alacsony túlterhelést okoz más útválasztókon és hálózati kapcsolatokon a dinamikus útválasztási protokoll hiánya miatt. Ugyanakkor a statikus útválasztásnak hátrányai is vannak. A statikus útválasztás például kis hálózatokra van korlátozva, és nem méreteződik jól. A statikus útválasztás egyáltalán nem képes az útvonalon előforduló hálózati kiesésekhez és hibákhoz alkalmazkodni annak rögzített természete miatt.

A dinamikus útválasztás a forrás és cél közötti több lehetséges IP-útvonalakkal rendelkező nagy hálózatoktól függ, és speciális útválasztási protokollokat használ, mint például a RIP, amelyek az útválasztási táblák automatikus módosításait kezelik, ezzel lehetővé téve a dinamikus útválasztást. A dinamikus útválasztásnak több előnye van a statikussal szemben, mint például a magasabb rendű skálázhatóság, és a hálózati útvonalak mentén fellépő meghibásodásokhoz és kiesésekhez való alkalmazkodás képessége. Ezen kívül az útválasztási táblák kevesebb kézi beállítást igényelnek, mivel az útválasztók egymástól értesülnek a többiek létezéséről és az elérhető útvonalakról. Ez a jellemzője megszünteti az útválasztási táblákba emberi hiba miatt bekerülő hibák lehetőségét is. A dinamikus útválasztás ugyanakkor nem tökéletes, és hátrányai is vannak, mint például a megnövekedett összetettség és hálózati túlterhelés az útválasztók kommunikációja miatt, amely nem érinti közvetlenül a felhasználókat, de fogyasztja a hálózati sávszélességet.

2.4. TCP és UDP

A TCP egy kapcsolatalapú protokoll, amely hibajavítást és az adatok garantált kézbesítését kínálja az adatátvitel vezérlésének segítségével. Az adatátvitel vezérlése meghatározza, hogy az adatfolyam küldését mikor kell megállítani, és a korábban elküldött adatcsomagokat újraküldeni az ütközésekhez hasonló problémák miatt, így biztosítva az adatok teljes és pontos kézbesítését. A TCP ezen kívül fontos információk, például adatbázis-tranzakciók cseréjére is használatos.

A UDP ezzel szemben egy kapcsolat nélküli protokoll, amely ritkán foglalkozik fontos adatok átvitelével, mert hiányzik belőle az adatátvitel vezérlése vagy bármi más, a megbízható adatkézbesítést szolgáló módszer. Az UDP-t széles körben használják például hang- és videoszórásnál, ahol a hibajavítás és adatátvitel-vezérlés hiánya miatt sokkal gyorsabb, ugyanakkor néhány csomag elvesztése általában nem katasztrofális.

2.5. ICMP

Az ICMP az IP kiterjesztése, és az RFC 792 definiálja, és a vezérlő-, hiba-, és információs üzeneteket tartalmazó hálózati csomagokat támogatja. Az ICMP-t olyan hálózati alkalmazások használják, mint a ping segédprogram, amely képes meghatározni egy hálózati gép vagy eszköz elérhetőségét. Az ICMP által visszaadott, hálózati gépek vagy eszközök (például útválasztók) esetében hasznos hibaüzenetek például a Cél nem érhető el vagy az Időtúllépés.

2.6. Démonok

A démonok speciális rendszeralkalmazások, amelyek általában folyamatosan futnak a háttérben, és az általuk más alkalmazásoknak biztosított szolgáltatásokra vonatkozó kéréseket várnak, Sok démon

hálózatközpontú, azaz egy Ubuntu rendszeren a háttérben futó démonok nagy része hálózatokkal kapcsolatos szolgáltatásokat biztosít. Ilyen hálózati démon például a HTTP démon (httpd), amely webkiszolgáló funkciókat; a biztonságos parancsértelmező (sshd), amely távoli bejelentkezési és fájlátviteli szolgáltatásokat, és az IMAP démon (imapd), amely e-mail szolgáltatásokat biztosít.

2.7. Információforrások

- A TCP[8] és IP[9] kézikönyvoldalai sok hasznos információt biztosítanak.
- Hasznos olvasmány a TCP/IP Tutorial and Technical Overview[10] IBM Redbook is.
- Szintén hasznos lehet az O'Reilly TCP/IP Network Administration[11] című könyve.

3. DHCP

A DHCP egy hálózati szolgáltatás, amely lehetővé teszi a számítógépekhez beállítások társítását egy kiszolgálóról, az egyes hálózati gépek kézi beállítása helyett. A DHCP-kliensnek beállított számítógépeknek nincs kontrolljuk a DHCP-kiszolgálótól kapott beállítások felett, és a beállítás a számítógép felhasználója számára észrevétlen.

A DHCP-kiszolgáló által a DHCP-klienseknek leggyakrabban biztosított beállítások:

- IP-cím és hálózati maszk
- DNS
- WINS

Ugyanakkor a DHCP-kiszolgáló képes olyan beállításokat is biztosítani, mint:

- Gépnév
- Tartománynév
- Alapértelmezett átjáró
- Időkiszolgáló
- Nyomtatókiszolgáló

A DHCP használatának előnye, hogy a hálózat változásait – például a DNS-kiszolgáló címének megváltozását – csak a DHCP-kiszolgálón kell lekövetni, a hálózat összes gépének beállítása automatikusan frissítésre kerül, amint a DHCP-kliensük lekérdezi a DHCP-kiszolgálót. További előny, hogy egyszerűbb az új számítógépek integrálása a hálózatba, mivel nincs szükség IP-cím elérhetőségének ellenőrzésére. Az IP-címfoglalási konfliktusok is ritkábbak.

A DHCP-kiszolgáló két módszerrel képes beállítások biztosítására:

MAC-cím
: Ez a módszer a DHCP a hálózatra kapcsolt minden egyes hálózati kártya egyedi hardvercímének azonosítására való használatát, majd állandó beállítások folyamatos biztosítását jelenti minden alkalommal, amikor a DHCP-kliens az adott hálózati eszköz használatával kéréssel fordul a DHCP-kiszolgálóhoz.

Címtároló
: Ez a módszer IP-címek egy tárolójának (néha tartománynak vagy hatókörnek is nevezik) megadásával jár, amelyből a DHCP-kliensek dinamikusan és érkezési sorrendben megkapják beállításaikat. Ha egy DHCP-kliens már nincs a hálózaton egy megadott ideig, akkor a beállítások lejárnak és visszakerülnek a címtárolóba, ezzel elérhetővé válnak más DHCP-kliensek számára.

Az Ubuntu egyaránt tartalmaz DHCP-kiszolgálót és -klienst is. A kiszolgáló a dhcpd. Az Ubuntu által biztosított kliens a dhclient, és minden automatikus beállítást igénylő gépre fel kell telepíteni. Mindkét program telepítése és beállítása egyszerű, és a rendszer indulásakor automatikusan elindulnak.

3.1. Telepítés

Adja ki a következő parancsot a dhcpd telepítéséhez:

```
sudo apt-get install dhcp3-server
```

Valószínűleg szüksége lesz az alapértelmezett beállítások megváltoztatására az /etc/dhcp3/dhcpd.conf szerkesztésével, a konkrét igényekhez és konfigurációhoz illesztése érdekében.

Szerkesztenie kell az /etc/default/dhcp3-server fájlt is, a dhcpd által figyelendő csatolók megadásához. Alapértelmezésben az eth0 csatolón figyel.

MEGJEGYZÉS: a dhcpd üzenetei bekerülnek a rendszernaplóba. A diagnosztikai üzeneteket a syslogban keresse.

3.2. Beállítás

A telepítést záró hibaüzenet kissé zavarba ejtő lehet, de az alábbi lépések segítik a szolgáltatás beállítását:

Általában véletlen IP-címek kiosztására van szükség. Ez a következő beállításokkal érhető el:

```
# Sample /etc/dhcpd.conf
# (add your comments here)
default-lease-time 600;
max-lease-time 7200;
option subnet-mask 255.255.255.0;
option broadcast-address 192.168.1.255;
option routers 192.168.1.254;
option domain-name-servers 192.168.1.1, 192.168.1.2;
option domain-name "sajáttartomány.példa";

subnet 192.168.1.0 netmask 255.255.255.0 {
range 192.168.1.10 192.168.1.100;
range 192.168.1.150 192.168.1.200;
}
```

Ennek eredményeként a DHCP-kiszolgáló a kliensnek a 192.168.1.10-192.168.1.100 vagy 192.168.1.150-192.168.1.200 tartományból fog IP-címet adni. Az IP-címet 600 másodpercre kölcsönzi ki, ha a kliens nem kér más időtartamot. Ellenkező esetben a maximálisan engedélyezett kölcsönzés 7200 másodperc lesz. A kiszolgáló közli a klienssel azt is, hogy alhálózati maszkként a 255.255.255.0, üzenetszórási címként a 192.168.1.255, az útválasztó/átjáró címeként a 192.168.1.254, DNS-kiszolgálókként pedig a 192.168.1.1 és 192.168.1.2 használható.

Ha WINS-kiszolgálót kell megadnia Windows kliensei számára, akkor meg kell adnia a netbios-name-servers beállítást, például:

```
option netbios-name-servers 192.168.1.1;
```

A dhcpd beállítások a DHCP mini-hogyanból származnak, amely itt megtalálható[12].

[12] http://www.tldp.org/HOWTO/DHCP/index.html

3.3. Hivatkozások

- A dhcp3-server Ubuntu wiki[13] oldal további információkat tartalmaz.
- For more `/etc/dhcp3/dchpd.conf` options see the dhcpd.conf man page[14].
- Nézze meg a DHCP FAQ[15] oldalt is.

4. Időszinkronizálás NTP-vel

Ez az oldal a számítógép idejének pontosan tartására szolgáló módszereket írja le. Ez kiszolgálók esetén hasznos, de asztali gépek esetén nem feltétlenül szükséges (vagy kívánatos).

Az NTP az idő hálózaton keresztüli szinkronizálására szolgáló TCP/IP protokoll. Alapvetően arról van szó, hogy a kliens lekéri az aktuális időt a kiszolgálótól, és azt a saját órájának beállítására használja.

Ezen egyszerű leírás mögött hatalmas összetettség található - az NTP-kiszolgálók több rétegbe vannak szervezve, az első rétegbeli NTP-kiszolgálók atomórákhoz kapcsolódnak (gyakran GPS-en keresztül), a második és harmadik rétegbeli kiszolgálók pedig az interneten érkező tényleges kérések terhelését osztják el. A kliensszoftver is sokkal bonyolultabb, mint gondolná - ki kell szűrnie a kommunikációs késleltetéseket, és úgy kell módosítania az időt, hogy az ne zavarja az összes többi folyamatot a kiszolgálón.

Az Ubuntu két lehetőséget kínál az idő automatikus beállításához: az ntpdate és ntpd programokat.

4.1. ntpdate

Az Ubuntu alapértelmezésben tartalmazza az ntpdate programot, amely minden rendszerindításkor lefut, és beállítja az órát az Ubuntu NTP kiszolgálójának megfelelően. Ugyanakkor a kiszolgálók órái az egyes újraindítások között jelentős csúszást gyűjthetnek össze, emiatt hasznos az időt alkalmanként is pontosítani. Ennek legegyszerűbb módja a cron beállítása az ntpdate napi futtatására. Kedvenc szerkesztőjével rendszergazdai jogokkal hozzon létre egy `/etc/cron.daily/ntpdate` nevű fájlt a következő tartalommal:

```
ntpdate ntp.ubuntu.com
```

Az `/etc/cron.daily/ntpdate` fájlnak végrehajthatónak is kell lennie.

```
sudo chmod 755 /etc/cron.daily/ntpdate
```

4.2. ntpd

Az ntpdate egy egyszerű eszköz - naponta csak egyszer képes az idő módosítására, egy nagy javítással. Az ntpd nevű NTP-démon sokkal finomabb. Kiszámítja a rendszeróra elcsúszását, és folyamatosan módosítja, így nem lesznek nagy javítások, amelyek például inkonzisztens naplókat eredményezhetnének. Ennek ára csak némi processzorteljesítmény és memória, de egy modern kiszolgálón ezek elhanyagolhatók.

Az ntpd telepítéséhez adja ki a következő parancsot:

```
sudo apt-get install ntp
```

4.3. Időkiszolgálók módosítása

Mind a két fenti esetben a rendszer alapértelmezésben az Ubuntu NTP-kiszolgálóját fogja használni az `ntp.ubuntu.com` címen. Ez nem probléma, de a pontosság és hibatűrés javítása érdekében szüksége lehet több kiszolgáló és/vagy földrajzilag Önhöz közelebb található kiszolgálók használatára. Az ntpdate esetén ehhez módosítsa az `/etc/cron.daily/ntpdate` tartalmát a következőre:

```
ntpdate ntp.ubuntu.com pool.ntp.org
```

Az ntpd esetén pedig vegyen fel további kiszolgálósorokat az `/etc/ntp.conf` fájlba:

```
server ntp.ubuntu.com
server pool.ntp.org
```

A fenti példákban észrevehette a `pool.ntp.org` sort. Ez azért remek választás, mert körbeforgó DNS segítségével választ NTP-kiszolgálót egy tárolóból, így elosztva a terhelést több különböző kiszolgáló között. Sőt, különböző területek szerint csoportosított tárolók is elérhetők, Magyarországról például a `pool.ntp.org` helyett használható a `hu.pool.ntp.org`. További részletekért keresse fel a http://www.pool.ntp.org/ oldalt.

A weben keresve is találhat Önhöz közeli NTP-kiszolgálókat, és ezeket is felveheti beállításai közé. Egy kiszolgáló működésének teszteléséhez adja ki a következő parancsot: `sudo ntpdate ntp.kiszolgáló.név`.

4.4. Hivatkozások

- További információkért lásd az Ubuntu Time[16] wiki oldalt.
- NTP-támogatás[17]
- Az NTP FAQ és HOWTO[18]

5. fejezet - Távoli adminisztráció

Linuxos kiszolgálóját számos módszerrel adminisztrálhatja távolról. Ez a szakasz az egyik legnépszerűbb megoldást, az SSH-t, valamint az eBox nevű webalapú adminisztrációs keretrendszert mutatja be.

1. OpenSSH kiszolgáló

1.1. Bevezetés

Az Ubuntu kiszolgáló kézikönyvének ezen szakasza hálózatba kapcsolt számítógépek távoli felügyeletére, és az ezek közti adatátvitelre használható hatékony eszközök OpenSSH néven ismert gyűjteményét mutatja be. Megismeri az OpenSSH kiszolgálóalkalmazáshoz rendelkezésre álló konfigurációs lehetőségek egy részét, valamint azok módosításának módját Ubuntu rendszeren.

Az OpenSSH a számítógépek távoli felügyeletére és fájlok számítógépek közti átvitelére szolgáló eszközök Secure Shell (SSH) protokollcsaládjának szabadon elérhető verziója. Az ezen funkciók megvalósítására hagyományosan használt eszközök, mint például a telnet vagy az rcp, nem biztonságosak, mert a felhasználó jelszavát egyszerű szövegként viszik át. Az OpenSSH egy kiszolgálódémont és klienseszközöket biztosít a biztonságos, titkosított távoli felügyelet és fájlátviteli műveletek megkönnyítésére, hatékonyan helyettesítve a hagyományos eszközöket.

Az OpenSSH kiszolgálókomponense, az sshd folyamatosan figyeli a klienskapcsolatokat a klienseszközöktől. Kapcsolódási kérés érkezésekor az sshd a kapcsolódó klienseszköztől függően létrehozza a megfelelő kapcsolatot. Ha például a távoli számítógép az ssh kliensalkalmazással kapcsolódik, akkor az OpenSSH kiszolgáló hitelesítés után létrehoz egy távoli felügyeleti munkamenetet. Ha a távoli felhasználó az OpenSSH kiszolgálóhoz az scp használatával csatlakozik, akkor az OpenSSH kiszolgálódémon a hitelesítés után fájlok biztonságos másolását kezdeményezi a kiszolgáló és a kliens között. Az OpenSSH számos hitelesítési módszert használhat, többek közt egyszerű szöveges jelszót, nyilvános kulcsot és Kerberos jegyeket.

1.2. Telepítés

Az OpenSSH kliens- és kiszolgálóalkalmazások telepítése egyszerű. Az OpenSSH kliensalkalmazások Ubuntu rendszerére telepítéséhez adja ki a következő parancsot:

```
sudo apt-get install openssh-client
```

Az OpenSSH kiszolgálóalkalmazás és a kapcsolódó támogató fájlok telepítéséhez adja ki a következő parancsot:

```
sudo apt-get install openssh-server
```

Az openssh-server csomag kiválasztható telepítésre a kiszolgálóváltozat telepítési folyamata során is.

1.3. Beállítás

Az OpenSSH kiszolgálóalkalmazás, az sshd alapértelmezett viselkedését az `/etc/ssh/sshd_config` fájl szerkesztésével konfigurálhatja. A fájlban használt konfigurációs direktívákkal kapcsolatos információkért nézze meg a megfelelő kézikönyvoldalt a következő parancs kiadásával:

```
man sshd_config
```

Az sshd konfigurációs fájljában számos direktíva található, amelyek például a kommunikációs beállításokat és hitelesítési módokat vezérlik. Az alábbiakban néhány példát láthat az `/etc/ssh/sshd_config` fájl szerkesztésével módosítható konfigurációs direktívákra.

A konfigurációs fájl szerkesztése előtt készítsen másolatot az eredeti fájlról, és tegye írásvédetté, így referenciaként megmaradnak az eredeti beállítások, és szükség esetén újra felhasználhatja azokat.

A következő parancsok kiadásával másolja le az `/etc/ssh/sshd_config` fájlt, és tegye írásvédetté:

```
sudo cp /etc/ssh/sshd_config /etc/ssh/sshd_config.original
sudo chmod a-w /etc/ssh/sshd_config.original
```

Az alábbi példák bemutatnak néhány módosítható konfigurációs direktívát:

- Módosítsa a Port direktívát a következőre az OpenSSH beállításához a 2222-es TCP port figyelésére az alapértelmezett 22-es TCP port helyett:

  Port 2222

- Ahhoz, hogy az sshd engedélyezze a nyilvános kulcs alapú bejelentkezést, vegye fel vagy módosítsa a következő sort:

  PubkeyAuthentication yes

  az `/etc/ssh/sshd_config` fájlba, ha pedig már tartalmazza, győződjön meg róla, hogy a sor nincs megjegyzésben.

- Az OpenSSH kiszolgáló megjelenítheti egy fájl, például az `/etc/issue.net` fájl tartalmát bejelentkezés előtti bannerként, ehhez vegye fel vagy módosítsa a következő sort:

  Banner /etc/issue.net

  az `/etc/ssh/sshd_config` fájlba.

Az `/etc/ssh/sshd_config` fájl módosításának befejezése után mentse a fájlt, és a következő parancs kiadásával indítsa újra az sshd kiszolgálót a módosítások életbe léptetéséhez:

```
sudo /etc/init.d/ssh restart
```

Az sshd kiszolgáló viselkedését számos konfigurációs direktíva segítségével igazíthatja igényeihez. Ne feledje azonban, hogy amennyiben a kiszolgáló elérésének egyetlen módja az ssh, és hibát vét az sshd az `/etc/ssh/sshd_config` fájllal végzett beállításakor, akkor az újraindítással kizárhatja magát a kiszolgálóról, vagy az sshd kiszolgáló visszautasíthatja az

elindulást a helytelen konfigurációs direktíva miatt. Legyen tehát különösen óvatos ezen fájl távoli kiszolgálón történő szerkesztésekor.

1.4. SSH-kulcsok

Az SSH-kulcsok lehetővé teszik két gép között a jelszó nélküli azonosítást. Az SSH-kulcsos hitelesítés két kulcsot használ: a személyes és a nyilvános kulcsot.

A kulcsok előállításához adja ki a következő parancsot:

```
ssh-keygen -t dsa
```

Ez előállítja a kulcsokat, a DSA hitelesítési azonosság használatával. A folyamat során a program bekér egy jelszót. A kulcs létrehozására vonatkozó kérdésnél egyszerűen nyomja meg az Enter billentyűt.

Alapértelmezésben a nyilvános kulcs a `~/.ssh/id_dsa.pub` fájlba kerül, míg a `~/.ssh/id_dsa` a személyes kulcsot tárolja. Ezután másolja az `id_dsa.pub` fájlt a távoli kiszolgálóra, és a következő parancs kiadásával fűzze a `~/.ssh/authorized_keys` fájl végéhez:

```
ssh-copy-id felhasználónév@távoligép
```

Végül ellenőrizze újra az `authorized_keys` fájl jogosultságait, csak a bejelentkezett felhasználónak lehet rá olvasási és írási jogosultsága. Ha a jogosultságok nem megfelelőek, módosítsa azokat a következő parancs kiadásával:

```
chmod 600 .ssh/authorized_keys
```

Ezután képesnek kell lennie az SSH használatával a jelszavak bekérése nélkül bejelentkezni a kiszolgálóra.

1.5. Hivatkozások

- Az Ubuntu wiki SSH[1] oldala.
- Az OpenSSH weboldala[2]
- Wikioldal az OpenSSH haladó használatáról[3]

2. eBox

Az eBox egy kiszolgálóalkalmazások felügyeletére használt webes keretrendszer. Az eBox moduláris felépítése lehetővé teszi a segítségével konfigurálni kívánt szolgáltatások kiválogatását.

2.1. Telepítés

A különböző eBox modulok külön csomagokba vannak osztva, lehetővé téve kizárólag a szükségesek telepítését. Az elérhető csomagok megjelenítésének egyik módja a következő parancs kiadása:

```
apt-cache rdepends ebox | uniq
```

Az alapértelmezett modulokat tartalmazó eBox csomag telepítéséhez adja ki a következőt:

```
sudo apt-get install ebox
```

A telepítés során meg kell adnia az ebox felhasználó jelszavát. Az eBox telepítése után a webes felület a https://kiszolgáló/ebox címen lesz elérhető.

2.2. Beállítás

Az eBox használata során fontos megjegyeznie, hogy a legtöbb modul konfigurálásakor az új beállítások alkalmazásához meg kell nyomni a Change gombot. A Change gomb megnyomása után a legtöbb, de nem minden modult menteni kell. Az új beállítások alkalmazásához kattintson a „Save changes” hivatkozásra a jobb felső sarokban.

A mentést igénylő módosítások elvégzése esetén a hivatkozás zöldről vörösre változik.

2.3. eBox modulok

Alapértelmezésben egyik eBox modul sincs engedélyezve, és új modul telepítésekor az nem lesz automatikusan engedélyezve.

Letiltott modul engedélyezéséhez kattintson a bal oldali menü Module status hivatkozására. Ezután ellenőrizze az engedélyezni kívánt modulokat, és kattintson a „Save” hivatkozásra.

2.3.1. Alapértelmezett modulok

Ez a szakasz röviden összefoglalja az alapértelmezett eBox modulokat.

- System: az általános eBox elemek konfigurálását lehetővé tevő beállításokat tartalmaz.
  - General: lehetővé teszi a nyelv és a portszám beállítását, valamint a jelszóváltoztatást.
  - Disk Usage: a lemezhasználatot részletező grafikont jelenít meg.

  - Backup: segítségével az eBox konfigurációs információiról készíthető biztonsági mentés, és a Full Backup lehetőség engedélyezésével a Configuration beállítás által nem tartalmazott összes eBox információ, mint például a naplófájlok is menthetők.
  - Halt/Reboot: leállítja vagy újraindítja a rendszert.
  - Bug Report: létrehoz egy hibajelentésekhez hasznos információkat tartalmazó fájlt.
- Logs: lehetővé teszi az eBox naplóinak lekérdezését, függően a beállított törlési időtől.
- Events: ez a modul képes riasztásokat küldeni rss, jabber és naplófájlok közvetítésével.
  - Elérhető események:
    - Free Storage Space: riasztást küld, ha a szabad lemezhely a beállított százalékos arány (alapértelmezésben 10%) alá esik.
    - Naplófigyelő: riasztást küld, ha egy beállított naplózó naplózott valamit.
    - RAID: ez figyeli a RAID rendszert, és riasztásokat küld az esetleges problémák felmerülésekor.
    - Service: riasztásokat küld, ha egy szolgáltatás rövid időn belül többször is újraindul.
    - State: értesítést küld az eBox állapotáról, akár fut, akár nem.
  - Kézbesítők:
    - Log: ez a kézbesítő eseményüzeneteket küld az eBox `/var/log/ebox/ebox.log` nevű naplófájljába.
    - Jabber: ezt a kézbesítőt az engedélyezése előtt be kell állítania a „Configure” ikonra kattintással.
    - RSS: Ezen kézbesítő beállítása után feliratkozhat az eseményértesítések elérésére szolgáló hírforrásra.

2.4. További modulok

A további elérhető eBox modulok leírásai:

- Network: lehetővé teszi a kiszolgáló hálózati beállításainak módosítását az eBoxon belül.
- Firewall: lehetővé teszi az eBox-ot futtató kiszolgáló tűzfalbeállításainak módosítása.
- UsersandGroups: ez a modul az OpenLDAP LDAP-címtárakban található felhasználókat és csoportokat kezeli.
- DHCP: felületet biztosít DHCP kiszolgáló beállítására.
- DNS: lehetővé teszi a BIND9 DNS-kiszolgáló beállításainak módosítását.
- Objects: lehetővé teszi az eBox hálózati objektumainak konfigurálását, aminek segítségével név rendelhető IP-címhez vagy IP-címek csoportjához.
- Services: konfigurációs információkat jelenít meg a hálózat felé elérhető szolgáltatásokról.
- Squid: a Squid proxy kiszolgáló beállításainak módosítása.
- CA: hitelesítésszolgáltató beállítása a kiszolgálóhoz.
- NTP: a Hálózati időprotokoll (NTP) beállításainak módosítása.

- Printers: lehetővé teszi a nyomtatók beállítását.
- Samba: lehetővé teszi a Samba beállításainak módosítását.
- OpenVPN: az OpenVPN virtuális magánhálózat beállításainak módosítása.

2.5. Információforrások

- Az Ubuntu wiki eBox[4] oldala további részleteket tartalmaz.
- További információkért lásd az eBox honlapját[5].

6. fejezet - Hálózati hitelesítés

Ez a szakasz a különböző hálózati hitelesítési protokollokat ismerteti.

1. OpenLDAP kiszolgáló

Az LDAP jelentése: könnyűsúlyú címtár-hozzáférési protokoll - ez az X.500 protokoll egyszerűsített változata. Ebben a szakaszban a címtár hitelesítésre lesz felhasználva. Ezzel együtt az LDAP számos módon használható: hitelesítés, megosztott könyvtár (levelezőklienseknek), címtár stb.

Az LDAP röviden azzal jellemezhető, hogy minden információ egy faszerkezetben található. Az OpenLDAP segítségével önállóan megállapíthatja a címtár faszerkezetét (a címtárinformációs fát, DIT). Egy egyszerű fával kezdünk, amely két csomópontot tartalmaz a gyökér alatt:

- A „People” csomópont, amelyben a felhasználók találhatók
- A „Groups” csomópont, amelyben a csoportjai lesznek tárolva

Mielőtt elkezdi, meg kell határoznia az LDAP címtár gyökerét. Alapértelmezésben a fát a teljes képzésű tartománynév (FQDN) határozza meg. Ha a tartomány a példa.hu (ezt fogjuk használni a példában), akkor a gyökércsomópont dc=példa,dc=hu.

1.1. Telepítés

Első lépésként telepítse az slapd nevű OpenLDAP kiszolgálódémont és az LDAP-kezelő segédprogramokat tartalmazó ldap-utils csomagot:

```
sudo apt-get install slapd ldap-utils
```

Alapértelmezésben a slapd a slapd démon futtatásához szükséges minimális beállításokkal van konfigurálva.

A következő szakaszok példái megegyeznek a kiszolgáló tartománynevével. Ha például a gép teljes képzésű tartományneve (FQDN) ldap.példa.hu, akkor az alapértelmezett utótag dc=példa,dc=hu lesz.

1.2. Az LDAP feltöltése

Az OpenLDAP önálló adatbázist használ, amely tartalmazza a cn=config könyvtárinformációs fát (DIT). A cn=config DIT segítségével dinamikusan kerül beállításra a slapd démon, lehetővé téve a sémadefiníciók, indexek, ACL-ek stb. a szolgáltatás leállítása nélküli módosítását.

A háttér cn=config címtár csak minimális beállításokkal rendelkezik, és az előtét feltöltése érdekében további beállításokat kell végezni. Az előtét egy „klasszikus” sémával lesz feltöltve, amely kompatibilis címtáralkalmazásokkal és a Unix Posix fiókokkal. A Posix fiókok lehetővé teszik a hitelesítést számos alkalmazás, például webes alkalmazások, levéltovábbító (MTA) alkalmazások stb. felé.

A külső alkalmazások számára az LDAP segítségével történő hitelesítéshez mindet külön be kell állítani. A részletekért nézze meg az adott alkalmazások dokumentációját.

Ne feledje el az alábbi példákban a dc=példa,dc=hu kifejezést az Ön LDAP konfigurációjának megfelelően módosítani.

Első lépésként néhány sémafájlt kell betölteni. Adja ki a következő parancsot:

```
sudo ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/ldap/schema/cosine.ldif
sudo ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/ldap/schema/nis.ldif
sudo ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/ldap/schema/inetorgperson.ldif
```

Ezután másolja az alábbi példa LDIF-fájlt a rendszerére `backend.példa.hu.ldif` néven:

```
# Dinamikus backend modulok betöltése
dn: cn=module,cn=config
objectClass: olcModuleList
cn: module
olcModulepath: /usr/lib/ldap
olcModuleload: back_hdb

# Adatbázis-beállítások
dn: olcDatabase=hdb,cn=config
objectClass: olcDatabaseConfig
objectClass: olcHdbConfig
olcDatabase: {1}hdb
olcSuffix: dc=példa,dc=hu
olcDbDirectory: /var/lib/ldap
olcRootDN: cn=admin,dc=példa,dc=hu
olcRootPW: titok
olcDbConfig: set_cachesize 0 2097152 0
olcDbConfig: set_lk_max_objects 1500
olcDbConfig: set_lk_max_locks 1500
olcDbConfig: set_lk_max_lockers 1500
olcDbIndex: objectClass eq
olcLastMod: TRUE
olcDbCheckpoint: 512 30
olcAccess: to attrs=userPassword by dn="cn=admin,dc=példa,dc=hu" write by anonymous auth by self wr
olcAccess: to attrs=shadowLastChange by self write by * read
olcAccess: to dn.base="" by * read
olcAccess: to * by dn="cn=admin,dc=példa,dc=hu" write by * read
```

A olcRootPW: titok sorban adja meg az admin jelszavát.

Most adja az LDIF-fájlt a címtárhoz:

```
sudo ldapadd -Y EXTERNAL -H ldapi:/// -f backend.példa.hu.ldif
```

Az előtét címtár készen áll a feltöltésre. Hozzon létre egy `frontend.példa.hu.ldif` nevű fájlt a következő tartalommal:

```
# A tartomány felső szintű objektumának létrehozása
dn: dc=példa,dc=hu
objectClass: top
```

```
objectClass: dcObject
objectclass: organization
o: Példaszervezet
dc: Example
description: LDAP példa

# Admin felhasználó.
dn: cn=admin,dc=példa,dc=hu
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP adminisztrátor
userPassword: titok

dn: ou=people,dc=példa,dc=hu
objectClass: organizationalUnit
ou: people

dn: ou=groups,dc=példa,dc=hu
objectClass: organizationalUnit
ou: groups

dn: uid=john,ou=people,dc=példa,dc=hu
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: john
sn: Doe
givenName: John
cn: John Doe
displayName: John Doe
uidNumber: 1000
gidNumber: 10000
userPassword: jelszó
gecos: John Doe
loginShell: /bin/bash
homeDirectory: /home/john
shadowExpire: -1
shadowFlag: 0
shadowWarning: 7
shadowMin: 8
shadowMax: 999999
shadowLastChange: 10877
mail: john.doe@példa.hu
postalCode: 31000
l: Toulouse
o: Example
mobile: +33 (0)6 xx xx xx xx
homePhone: +33 (0)5 xx xx xx xx
title: Rendszeradminisztrátor
postalAddress:
initials: JD
```

```
dn: cn=example,ou=groups,dc=példa,dc=hu
objectClass: posixGroup
cn: example
gidNumber: 10000
```

Ebben a példában a címtárszerkezet, egy felhasználó és egy csoport került beállításra. Más példákban találkozhat az objectClass: top hozzáadásával minden bejegyzéshez, de mivel ez az alapértelmezett viselkedés, így nem szükséges mindig felvenni.

Vegye fel a bejegyzéseket az LDAP-címtárba:

```
sudo ldapadd -x -D cn=admin,dc=példa,dc=hu -W -f frontend.példa.hu.ldif
```

Az ldapsearch segédprogrammal ellenőrizhető, hogy a tartalom megfelelően lett-e felvéve. Hajtsa végre a következő keresést az LDAP-címtárban:

```
ldapsearch -xLLL -b "dc=példa,dc=hu" uid=john sn givenName cn
```

```
dn: uid=john,ou=people,dc=példa,dc=hu
cn: John Doe
sn: Doe
givenName: John
```

Rövid magyarázat:

- -x: nem használja a SASL hitelesítési módszert, amely alapértelmezett.
- -LLL: az LDIF sémainformációk kiírásának kikapcsolása.

1.3. További beállítások

A cn=config fa az ldap-utils csomag segédprogramjaival manipulálható. Például:

- Az ldapsearch segítségével nézze meg a fát, megadva a telepítéskor vagy újrakonfiguráláskor beállított admin jelszót:

```
sudo ldapsearch -LLL -Y EXTERNAL -H ldapi:/// -b cn=config dn
```

```
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
dn: cn=config

dn: cn=module{0},cn=config

dn: cn=schema,cn=config
```

```
dn: cn={0}core,cn=schema,cn=config

dn: cn={1}cosine,cn=schema,cn=config

dn: cn={2}nis,cn=schema,cn=config

dn: cn={3}inetorgperson,cn=schema,cn=config

dn: olcDatabase={-1}frontend,cn=config

dn: olcDatabase={0}config,cn=config

dn: olcDatabase={1}hdb,cn=config
```

A fenti kimenet a cn=config háttéradatbázis aktuális beállításaiból áll. A tényleges kimenet eltérhet.

- A cn=config fa módosításához például felvehet egy új attribútumot az indexlistába az ldapmodify segítségével:

```
sudo ldapmodify -Y EXTERNAL -H ldapi:///
```

```
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
dn: olcDatabase={1}hdb,cn=config
add: olcDbIndex
olcDbIndex: uidNumber eq

modifying entry "olcDatabase={1}hdb,cn=config"
```

A módosítások befejezése után nyomja meg a Ctrl+D billentyűkombinációt a kilépéshez a segédprogramból.

- Az ldapmodify képes a változtatásokat fájlból is beolvasni. Hozzon létre egy `uid_index.ldif` nevű fájlt a következő tartalommal:

```
dn: olcDatabase={1}hdb,cn=config
add: olcDbIndex
olcDbIndex: uid eq,pres,sub
```

Ezután indítsa el az ldapmodify programot:

```
sudo ldapmodify -Y EXTERNAL -H ldapi:/// -f uid_index.ldif
```

```
SASL/EXTERNAL authentication started
```

```
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
modifying entry "olcDatabase={1}hdb,cn=config"
```

A fájlt használó módszer nagy változtatások esetén hasznos.

- Adding additional schemas to slapd requires the schema to be converted to LDIF format. The `/etc/ldap/schema` directory contains some schema files already converted to LDIF format as demonstrated in the previous section. Fortunately, the slapd program can be used to automate the conversion. The following example will add the dyngoup.schema:

  1. Első lépésként hozza létre a `schema_convert.conf` konverziós fájlt a következő tartalommal:

     ```
     include /etc/ldap/schema/core.schema
     include /etc/ldap/schema/collective.schema
     include /etc/ldap/schema/corba.schema
     include /etc/ldap/schema/cosine.schema
     include /etc/ldap/schema/duaconf.schema
     include /etc/ldap/schema/dyngroup.schema
     include /etc/ldap/schema/inetorgperson.schema
     include /etc/ldap/schema/java.schema
     include /etc/ldap/schema/misc.schema
     include /etc/ldap/schema/nis.schema
     include /etc/ldap/schema/openldap.schema
     include /etc/ldap/schema/ppolicy.schema
     ```

  2. Ezután hozzon létre egy átmeneti könyvtárat a kimenet tárolásához:

     ```
     mkdir /tmp/ldif_output
     ```

  3. Most a slapcat segítségével konvertálja a sémafájlokat LDIF formátumúra:

     ```
     slapcat -f schema_convert.conf -F /tmp/ldif_output -n0 -s "cn={5}dyngroup,cn=schema,cn=config
     ```

     Módosítsa a konfigurációs fájl nevét és az átmeneti könyvtár nevét, ha a sajátja eltér. Érdemes lehet megtartani az `ldif_output` könyvtárat, amennyiben további sémákat szeretne felvenni a jövőben.

  4. Szerkessze a `/tmp/cn\=dyngroup.ldif` fájlt, módosítsa a következő attribútumokat:

     ```
     dn: cn=dyngroup,cn=schema,cn=config
     ...
     cn: dyngroup
     ```

     Távolítsa el a következő sorokat a fájl aljáról:

     ```
     structuralObjectClass: olcSchemaConfig
     entryUUID: 10dae0ea-0760-102d-80d3-f9366b7f7757
     creatorsName: cn=config
     ```

```
createTimestamp: 20080826021140Z
entryCSN: 20080826021140.791425Z#000000#000#000000
modifiersName: cn=config
modifyTimestamp: 20080826021140Z
```

Az attribútumértékek eltérők lesznek, győződjön meg róla, hogy eltávolította az attribútumokat.

5. Végül az ldapadd segédprogrammal vegye fel az új sémát a címtárba:

```
sudo ldapadd -Y EXTERNAL -H ldapi:/// -f /tmp/cn\=dyngroup.ldif
```

Ezután létre kell jönnie egy dn: cn={4}dyngroup,cn=schema,cn=config bejegyzésnek a cn=config fában.

1.4. LDAP-replikáció

Az LDAP sok esetben gyorsan a hálózat kritikus szolgáltatásává válik. Egyre több szolgáltatás fogja hitelesítésre, jogosultságkezelésre, beállításokhoz stb. használni az LDAP-t. Ilyenkor hasznos lehet replikáció használatával beüzemelni egy redundáns rendszert.

A replikáció a Syncrepl alrendszer segítségével valósul meg. A Syncrepl fogyasztó-termelő modell használatával teszi lehetővé a címtár szinkronizálását. A termelő a címtár frissítéseit elküldi a fogyasztóknak.

1.4.1. Termelő beállítása

Az alábbi példa a single-master konfigurációt mutatja be. Ebben a konfigurációban egy OpenLDAP-kiszolgáló van beállítva termelőként, egy pedig fogyasztóként.

1. Első lépésként állítsa be a termelő kiszolgálót. Másolja a következőket egy `provider_sync.ldif` nevű fájlba:

```
# Indexek hozzáadása a frontend adatbázisához.
dn: olcDatabase={1}hdb,cn=config
changetype: modify
add: olcDbIndex
olcDbIndex: entryCSN eq
-
add: olcDbIndex
olcDbIndex: entryUUID eq

# A syncprov és accesslog modulok betöltése.
dn: cn=module{0},cn=config
changetype: modify
add: olcModuleLoad
olcModuleLoad: syncprov
-
add: olcModuleLoad
```

```
olcModuleLoad: accesslog

# Accesslog adatbázis meghatározása
dn: olcDatabase={2}hdb,cn=config
objectClass: olcDatabaseConfig
objectClass: olcHdbConfig
olcDatabase: {2}hdb
olcDbDirectory: /var/lib/ldap/accesslog
olcSuffix: cn=accesslog
olcRootDN: cn=admin,dc=példa,dc=hu
olcDbIndex: default eq
olcDbIndex: entryCSN,objectClass,reqEnd,reqResult,reqStart

# Accesslog adatbázis syncprov.
dn: olcOverlay=syncprov,olcDatabase={2}hdb,cn=config
changetype: add
objectClass: olcOverlayConfig
objectClass: olcSyncProvConfig
olcOverlay: syncprov
olcSpNoPresent: TRUE
olcSpReloadHint: TRUE

# syncrepl termelő az elsődleges adatbázishoz
dn: olcOverlay=syncprov,olcDatabase={1}hdb,cn=config
changetype: add
objectClass: olcOverlayConfig
objectClass: olcSyncProvConfig
olcOverlay: syncprov
olcSpNoPresent: TRUE

# az accesslog overlay meghatározásai az elsődleges adatbázishoz
dn: olcOverlay=accesslog,olcDatabase={1}hdb,cn=config
objectClass: olcOverlayConfig
objectClass: olcAccessLogConfig
olcOverlay: accesslog
olcAccessLogDB: cn=accesslog
olcAccessLogOps: writes
olcAccessLogSuccess: TRUE
# az accesslog adatbázis vizsgálata minden nap, és a 7 napnál régebbi bejegyzések törlése
olcAccessLogPurge: 07+00:00 01+00:00
```

2. Az slapd AppArmor profilját módosítani kell az accesslog adatbázis helyének megadásához. Szerkessze az `/etc/apparmor.d/usr.sbin.slapd` fájlt, és vegye fel a következőt:

```
  /var/lib/ldap/accesslog/ r,
  /var/lib/ldap/accesslog/** rwk,
```

Ezután hozza létre a könyvtárat, töltse újra az apparmor profilt, és másolja át a `DB_CONFIG` fájlt:

```
sudo -u openldap mkdir /var/lib/ldap/accesslog
sudo -u openldap cp /var/lib/ldap/DB_CONFIG /var/lib/ldap/accesslog/
```

```
sudo /etc/init.d/apparmor reload
```

A fenti sudo parancsok -u openldap kapcsolóval való használata hatására később nem kell az új könyvtár jogosultságait módosítania.

3. Szerkessze a fájlt, és módosítsa az olcRootDN értékét a címtárának megfelelően:

```
olcRootDN: cn=admin,dc=példa,dc=hu
```

4. Ezután vegye fel az LDIF-fájlt az ldapadd segédprogram használatával:

```
sudo ldapadd -Y EXTERNAL -H ldapi:/// -f provider_sync.ldif
```

5. Indítsa újra a slapd démont:

```
sudo /etc/init.d/slapd restart
```

A termelő kiszolgáló beállítása ezzel kész, ideje beállítani a fogyasztó kiszolgálót.

1.4.2. A fogyasztó beállítása

1. A fogyasztó kiszolgálót állítsa be ugyanúgy, mint a termelőt, a Syncrepl beállítási lépéseket kivéve.

   Vegye fel a kiegészítő sémafájlt:

```
sudo ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/ldap/schema/cosine.ldif
sudo ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/ldap/schema/nis.ldif
sudo ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/ldap/schema/inetorgperson.ldif
```

   Hozza létre vagy másolja át a termelő kiszolgálóról a `backend.példa.hu.ldif` fájlt.

```
# Dinamikus backend modulok betöltése
dn: cn=module,cn=config
objectClass: olcModuleList
cn: module
olcModulepath: /usr/lib/ldap
olcModuleload: back_hdb

# Adatbázis-beállítások
dn: olcDatabase=hdb,cn=config
objectClass: olcDatabaseConfig
objectClass: olcHdbConfig
olcDatabase: {1}hdb
olcSuffix: dc=példa,dc=hu
olcDbDirectory: /var/lib/ldap
olcRootDN: cn=admin,dc=példa,dc=hu
olcRootPW: titok
olcDbConfig: set_cachesize 0 2097152 0
olcDbConfig: set_lk_max_objects 1500
```

```
olcDbConfig: set_lk_max_locks 1500
olcDbConfig: set_lk_max_lockers 1500
olcDbIndex: objectClass eq
olcLastMod: TRUE
olcDbCheckpoint: 512 30
olcAccess: to attrs=userPassword by dn="cn=admin,dc=példa,dc=hu" write by anonymous auth by sel
olcAccess: to attrs=shadowLastChange by self write by * read
olcAccess: to dn.base="" by * read
olcAccess: to * by dn="cn=admin,dc=példa,dc=hu" write by * read
```

Vegye fel az LDIF-fájlt:

```
sudo ldapadd -Y EXTERNAL -H ldapi:/// -f backend.példa.hu.ldif
```

2. Tegye ugyanezt a fenti `frontend.példa.hu.ldif` fájllal, és vegye fel:

```
sudo ldapadd -x -D cn=admin,dc=példa,dc=hu -W -f frontend.példa.hu.ldif
```

A két kiszolgáló most a Syncrepl beállításoktól eltekintve azonos beállításokkal rendelkezik.

3. Most hozza létre a `consumer_sync.ldif` fájlt a következő tartalommal:

```
# A syncprov modul betöltése.
dn: cn=module{0},cn=config
changetype: modify
add: olcModuleLoad
olcModuleLoad: syncprov

# a syncrepl-hez kapcsolódó utasítások
dn: olcDatabase={1}hdb,cn=config
changetype: modify
add: olcDbIndex
olcDbIndex: entryUUID eq
-
add: olcSyncRepl
olcSyncRepl: rid=0 provider=ldap://ldap01.példa.hu bindmethod=simple binddn="cn=admin,dc=példa,
 credentials=titok searchbase="dc=példa,dc=hu" logbase="cn=accesslog"
 logfilter="(&(objectClass=auditWriteObject)(reqResult=0))" schemachecking=on
 type=refreshAndPersist retry="60 +" syncdata=accesslog
-
add: olcUpdateRef
olcUpdateRef: ldap://ldap01.példa.hu
```

Módosítsa a következő attribútumokat:

- A `ldap01.pelda.hu` helyett használja saját kiszolgálója gépnevét.
- binddn
- credentials
- searchbase
- olcUpdateRef:

4. Vegye fel az LDIF-fájlt a konfigurációs fába:

```
sudo ldapadd -c -Y EXTERNAL -H ldapi:/// -f consumer_sync.ldif
```

Az előtét-adatbázisnak most már szinkronizálódnia kell a kiszolgálók között. Igény esetén további kiszolgálókat a fenti lépések alkalmazásával vehet fel.

A slapd démon alapértelmezésben a `/var/log/syslog` fájlba küldi a naplóinformációkat. Ha probléma lépne fel, ebben a fájlban találhat a hibák elhárításával kapcsolatos információkat. Ne feledjen el meggyőződni arról, hogy minden kiszolgáló ismerje saját teljes képzésű tartománynevét (FQDN). Ez az `/etc/hosts` fájlban állítható be egy ehhez hasonló sorral:

```
127.0.0.1 ldap01.példa.hu ldap01
```

.

1.5. ACL beállítása

A hitelesítés a jelszó mező elérését igényli, ennek alapértelmezésben nem szabad elérhetőnek lennie. Ahhoz, hogy a felhasználók megváltoztathassák saját jelszavukat a passwd vagy egyéb segédprogramokkal, a shadowLastChange mezőnek is elérhetőnek kell lennie, miután a felhasználó hitelesítette magát.

To view the Access Control List (ACL), use the ldapsearch utility:

```
ldapsearch -xLLL -b cn=config -D cn=admin,cn=config -W olcDatabase=hdb olcAccess
```

```
Enter LDAP Password:
dn: olcDatabase={1}hdb,cn=config
olcAccess: {0}to attrs=userPassword,shadowLastChange by dn="cn=admin,dc=exampl
 e,dc=com" write by anonymous auth by self write by * none
olcAccess: {1}to dn.base="" by * read
olcAccess: {2}to * by dn="cn=admin,dc=example,dc=com" write by * read
```

1.6. TLS és SSL

Az OpenLDAP kiszolgálóra való bejelentkezés legjobb módja a titkosított munkamenet használata. Ez elvégezhető TLS vagy SSL használatával is.

A folyamat első lépése egy tanúsítvány beszerzése vagy létrehozása. Mivel a slapd a gnutls programkönyvtár használatával lett fordítva, a certtool segédprogrammal hozzuk létre a tanúsítványokat.

1. A következő parancs kiadásával telepítse a gnutls-bin csomagot:

```
sudo apt-get install gnutls-bin
```

2. Ezután hozzon létre egy személyes kulcsot a hitelesítésszolgáltató (CA) számára:

```
sudo sh -c "certtool --generate-privkey > /etc/ssl/private/cakey.pem"
```

3. Hozzon létre egy `/etc/ssl/ca.info` nevű információs fájlt a CA tanúsítvány önaláírásához a következő tartalommal:

```
cn = Példacég
ca
cert_signing_key
```

4. Ezután hozza létre az önaláírt CA tanúsítványt:

```
sudo certtool --generate-self-signed --load-privkey /etc/ssl/private/cakey.pem \ --template /et
```

5. Hozzon létre személyes kulcsot a kiszolgáló számára:

```
sudo sh -c "certtool --generate-privkey > /etc/ssl/private/ldap01_slapd_key.pem"
```

A fájlnévbe az ldap01 helyett a saját kiszolgálójának gépnevét írja. A tanúsítvány és kulcs az azokat használó gép és szolgáltatás után való elnevezése segít a fájlnevek és elérési utak rendben tartásában.

6. Hozza létre az `/etc/ssl/ldap01.info` nevű információs fájlt a következő tartalommal a kiszolgáló tanúsítványának aláírásához a CA-val:

```
organization = Példacég
cn = ldap01.példa.hu
tls_www_server
encryption_key
signing_key
```

7. Hozza létre a kiszolgáló tanúsítványát:

```
sudo certtool --generate-certificate --load-privkey /etc/ssl/private/x01-test_slapd_key.pem \ -
```

Miután a tanúsítvány, a kulcs és a CA is telepítve lett, az ldapmodify parancs segítségével vegye fel az új beállításokat:

```
sudo ldapmodify -Y EXTERNAL -H ldapi:///
```

```
Enter LDAP Password:
dn: cn=config
add: olcTLSCACertificateFile
olcTLSCACertificateFile: /etc/ssl/certs/cacert.pem
-
add: olcTLSCertificateFile
```

```
olcTLSCertificateFile: /etc/ssl/certs/ldap01_slapd_cert.pem
-
add: olcTLSCertificateKeyFile
olcTLSCertificateKeyFile: /etc/ssl/private/ldap01_slapd_key.pem

modifying entry "cn=config"
```

Módosítsa az `ldap01_slapd_cert.pem`, `ldap01_slapd_key.pem` és `cacert.pem` neveket, ha szükséges.

Ezután szerkessze az `/etc/default/slapd` fájlt, vegye ki megjegyzésből a SLAPD_SERVICES beállítást:

```
SLAPD_SERVICES="ldap:/// ldapi:/// ldaps:///"
```

Most az openldap felhasználónak hozzá kell férnie a tanúsítványhoz:

```
sudo adduser openldap ssl-cert
sudo chgrp ssl-cert /etc/ssl/private/ldap01_slapd_key.pem
sudo chmod g+r /etc/ssl/private/ldap01_slapd_key.pem
```

Ha az `/etc/ssl/private` és `/etc/ssl/private/server.key` fájlok jogosultságai eltérnek, akkor ennek megfelelően módosítsa a fenti parancsokat.

Végül indítsa újra az slapd démont:

```
sudo /etc/init.d/slapd restart
```

Az slapd démonnak ezután már figyelnie kell az LDAPS kapcsolatokra, és képesnek kell lennie a STARTTLS használatára a hitelesítéshez.

Ha azt tapasztalja, hogy a kiszolgáló nem indul el, akkor nézze meg a /var/log/syslog fájlt. Ha a következőhöz hasonló hibákat lát: main: TLS init def ctx failed: -1, akkor valószínűleg a beállítások hibásak. Ellenőrizze, hogy a tanúsítványt a fájlokban megadott hitelesítésszolgáltató írta alá, és hogy az ssl-cert csoportnak van olvasási joga a személyes kulcsra.

1.6.1. TLS replikáció

Ha beállította a kiszolgálók között a Syncrepl használatát, akkor bölcs lépés titkosítani a replikációs forgalmat TLS használatával. A replikáció beállításával kapcsolatos részletekért lásd: 1.4. szakasz - LDAP-replikáció [62].

Feltételezzük, hogy a fenti utasításokat követte, és létrehozott egy CA tanúsítványt és kiszolgálótanúsítványt a termelő kiszolgálón. Tegye a következőket a fogyasztó kiszolgáló tanúsítványának és kulcsának létrehozásához.

1. Hozza létre a fogyasztó kiszolgáló új kulcsát:

```
mkdir ldap02-ssl
cd ldap02-ssl
certtool --generate-privkey > ldap02_slapd_key.pem
```

Az új könyvtár létrehozása nem nélkülözhetetlen, de segít a fájlokat rendben tartani, és a fogyasztó kiszolgálóra másolás is egyszerűbb.

2. Ezután hozzon létre egy `ldap02.info` nevű információs fájlt a fogyasztó kiszolgálóhoz, módosítsa az attribútumokat a helységnek és kiszolgálónak megfelelően:

```
country = HU
state = Pest
locality = Budapest
organization = Példacég
cn = ldap02.példa.hu
tls_www_client
encryption_key
signing_key
```

3. Hozza létre a tanúsítványt:

```
sudo certtool --generate-certificate --load-privkey ldap02_slapd_key.pem \ --load-ca-certificat
```

4. Másolja a `cacert.pem` fájlt a könyvtárba:

```
cp /etc/ssl/certs/cacert.pem .
```

5. Már csak az `ldap02-ssl` könyvtárat kell átmásolni a fogyasztó kiszolgálóra, majd az `ldap02_slapd_cert.pem` és `cacert.pem` fájlokat kell az `/etc/ssl/certs`, illetve az `ldap02_slapd_key.pem` fájlt az `/etc/ssl/private` könyvtárba másolni.

6. Miután a fájlok a helyükre kerültek, módosítsa a cn=config fát a következő parancs kiadásával:

```
sudo ldapmodify -Y EXTERNAL -H ldapi:///
```

```
Enter LDAP Password:
dn: cn=config
add: olcTLSCACertificateFile
olcTLSCACertificateFile: /etc/ssl/certs/cacert.pem
-
add: olcTLSCertificateFile
olcTLSCertificateFile: /etc/ssl/certs/ldap02_slapd_cert.pem
-
add: olcTLSCertificateKeyFile
olcTLSCertificateKeyFile: /etc/ssl/private/ldap02_slapd_key.pem

modifying entry "cn=config"
```

7. A termelőhöz hasonlóan szerkesztheti az `/etc/default/slapd` fájlt, és felveheti az ldaps:/// paramétert a SLAPD_SERVICES beállításhoz.

Most, hogy a TLS mindkét kiszolgálón be van állítva, módosítsa újra a fogyasztó kiszolgáló cn=config fáját a következő parancs kiadásával:

```
sudo ldapmodify -Y EXTERNAL -H ldapi:///
```

```
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0

dn: olcDatabase={1}hdb,cn=config
replace: olcSyncrepl
olcSyncrepl: {0}rid=0 provider=ldap://ldap01.példa.hu bindmethod=simple binddn="cn=ad
 min,dc=példa,dc=hu" credentials=titok searchbase="dc=példa,dc=hu" logbas
 e="cn=accesslog" logfilter="(&(objectClass=auditWriteObject)(reqResult=0))" s
 chemachecking=on type=refreshAndPersist retry="60 +" syncdata=accesslog starttls=yes

modifying entry "olcDatabase={1}hdb,cn=config"
```

Ha az LDAP kiszolgáló gépneve nem egyezik a tanúsítványban lévő teljes képzésű tartománynévvel (FQDN), akkor szükség lehet az `/etc/ldap/ldap.conf` fájl szerkesztésére, és a következő TLS-beállítások felvételére:

```
TLS_CERT /etc/ssl/certs/ldap02_slapd_cert.pem
TLS_KEY /etc/ssl/private/ldap02_slapd_key.pem
TLS_CACERT /etc/ssl/certs/cacert.pem
```

Végül indítsa újra az slapd démont az összes kiszolgálón:

```
sudo /etc/init.d/slapd restart
```

1.7. LDAP hitelesítés

Ha az LDAP-kiszolgáló már működik, az auth-client-config és libnss-ldap csomagok leegyszerűsítik az Ubuntu kliens beállítását LDAP használatával való hitelesítésre. A csomagok telepítéséhez adja ki a következő parancsot:

```
sudo apt-get install libnss-ldap
```

A telepítés során egy párbeszédablak bekéri az LDAP-kiszolgáló kapcsolatinformációit.

Ha elrontotta az információk megadását, újra elindíthatja a párbeszédablakot:

```
sudo dpkg-reconfigure ldap-auth-config
```

A párbeszédablakban megadott adatok az `/etc/ldap.conf` fájlba kerülnek. Ha a kiszolgáló a menüben nem szereplő beállításokat igényel, akkor ezen fájl szerkesztésével megadhatja azokat.

Ezután a libnss-ldap beállítható az auth-client-config LDAP-profil engedélyezésére a következő parancs kiadásával:

```
sudo auth-client-config -t nss -p lac_ldap
```

- -t: csak az `/etc/nsswitch.conf` fájlt módosítja.
- -p: az engedélyezendő/letiltandó stb. profil neve.
- lac_ldap: az auth-client-config profil, amely az ldap-auth-config csomag része.

A pam-auth-update segédprogram segítségével állítsa be a rendszert az LDAP használatára hitelesítésre:

```
sudo pam-auth-update
```

A pam-auth-update menüből válassza ki az LDAP-t, és az egyéb szükséges hitelesítési mechanizmusokat.

Most már képesnek kell lennie az LDAP-címtárban tárolt felhasználóhitelesítési adatokkal való bejelentkezésre.

Ha az LDAP címtárat Samba felhasználók tárolására fogja használni, akkor be kell állítania a kiszolgálót az LDAP használatával való hitelesítésre. A részletekért lásd: 2. szakasz - Samba és LDAP [75].

1.8. Felhasználó- és csoportkezelés

Az ldap-utils csomag több segédprogramot is tartalmaz a címtár karbantartásához, de a használatát megnehezítheti a szükséges kapcsolók hosszú sora. Az ldapscripts csomag az LDAP felhasználók és csoportok egyszerű kezeléséhez tartalmaz konfigurálható parancsfájlokat.

A csomag telepítéséhez adja ki a következő parancsot:

```
sudo apt-get install ldapscripts
```

Ezután szerkessze az `/etc/ldapscripts/ldapscripts.conf` konfigurációs fájlt, vegye ki megjegyzésből és módosítsa a következőket a környezetének megfelelően:

```
SERVER=localhost
BINDDN='cn=admin,dc=példa,dc=hu'
BINDPWDFILE="/etc/ldapscripts/ldapscripts.passwd"
```

```
SUFFIX='dc=példa,dc=hu'
GSUFFIX='ou=Csoportok'
USUFFIX='ou=Emberek'
MSUFFIX='ou=Számítógépek'
GIDSTART=10000
UIDSTART=10000
MIDSTART=10000
```

Ezután hozza létre az `ldapscripts.passwd` fájlt a címtár hitelesített elérésének lehetővé tételéhez:

```
sudo sh -c "echo -n 'titok' > /etc/ldapscripts/ldapscripts.passwd"
sudo chmod 400 /etc/ldapscripts/ldapscripts.passwd
```

A „titok” helyére az LDAP admin felhasználójának tényleges jelszavát írja.

Az ldapscripts ezzel készen áll a címtára karbantartásának segítésére. Alább látható néhány példa a parancsfájlok használatára:

- Új felhasználó létrehozása:

  ```
  sudo ldapadduser geza példa
  ```

  Ez létrehoz egy felhasználót geza felhasználónévvel és példa elsődleges csoporttal.

- Felhasználó jelszavának módosítása:

  ```
  sudo ldapsetpasswd geza
  Changing password for user uid=geza,ou=Emberek,dc=példa,dc=hu
  New Password:
  New Password (verify):
  ```

- Felhasználó törlése:

  ```
  sudo ldapdeleteuser geza
  ```

- Csoport hozzáadása:

  ```
  sudo ldapaddgroup qa
  ```

- Csoport törlése:

  ```
  sudo ldapdeletegroup qa
  ```

- Felhasználó csoporthoz adása:

  ```
  sudo ldapaddusertogroup geza qa
  ```

  Ezután a qa csoport memberUid attribútumának értéke geza lesz.

- Felhasználó eltávolítása csoportból:

```
sudo ldapdeleteuserfromgroup geza qa
```

A memberUid attribútum ezzel eltávolításra került a qa csoportból.

- Az ldapmodifyuser parancsfájl lehetővé teszi felhasználó attribútumainak felvételét, eltávolítását vagy cseréjét. A parancsfájl az ldapmodify segédprogram szintaxisát használja, például:

```
sudo ldapmodifyuser geza
# About to modify the following entry :
dn: uid=geza,ou=Emberek,dc=példa,dc=hu
objectClass: account
objectClass: posixAccount
cn: geza
uid: geza
uidNumber: 1001
gidNumber: 1001
homeDirectory: /home/geza
loginShell: /bin/bash
gecos: geza
description: Felhasználói fiók
userPassword:: e1NTSEF9eXFsTFcyWlhwWkF1eGUybVdFWHZKRzJVMjFTSG9vcHk=

# Enter your modifications here, end with CTRL-D.
dn: uid=geza,ou=Emberek,dc=példa,dc=hu
replace: gecos
gecos: Hoffmann Géza
```

A felhasználó gecos attribútumának értéke ezután „Hoffmann Géza” lesz.

- Az ldapscripts másik nagyszerű szolgáltatása a sablonrendszer. A sablonok lehetővé teszik a felhasználó, csoport és gép objektumok attribútumainak személyre szabását. A user sablon engedélyezéséhez szerkessze az `/etc/ldapscripts/ldapscripts.conf` fájlt, és módosítsa:

```
UTEMPLATE="/etc/ldapscripts/ldapadduser.template"
```

Az `/etc/ldapscripts` könyvtárban minta sablonok találhatók. Másolja vagy nevezze át az `ldapadduser.template.sample` fájlt `/etc/ldapscripts/ldapadduser.template` névre:

```
sudo cp /etc/ldapscripts/ldapadduser.template.sample /etc/ldapscripts/ldapadduser.template
```

Szerkessze az új sablont a kívánt attribútumok felvételéhez. A következők az új felhasználókat az inetOrgPerson objectClass elemeként hozzák létre:

```
dn: uid=<user>,<usuffix>,<suffix>
objectClass: inetOrgPerson
objectClass: posixAccount
cn: <user>
sn: <ask>
```

```
uid: <user>
uidNumber: <uid>
gidNumber: <gid>
homeDirectory: <home>
loginShell: <shell>
gecos: <user>
description: Felhasználói fiók
title: Alkalmazott
```

Figyelje meg a cn értékeként használt <ask> szöveget. Az <ask> segítségével az ldapadduser beállítható az attribútumérték bekérésére a felhasználó létrehozása során.

További hasznos parancsfájlok is találhatók a csomagban, a teljes lista a következő parancs kiadásával érhető el: dpkg -L ldapscripts | grep bin

1.9. Információforrások

- Az Ubuntu wiki OpenLDAP[1] oldala további részleteket tartalmaz.
- További információkért lásd az OpenLDAP honlapját[2]
- Noha nem teljesen friss, az O'Reilly LDAP System Administration[3] könyve a mélyebb LDAP információk hasznos forrása
- A Packt Mastering OpenLDAP[4] egy remek referencia, amely az OpenLDAP újabb verzióit mutatja be.
- Az auth-client-config alkalmazással kapcsolatos további információkért lásd a kézikönyvoldalát: man auth-client-config.
- Az ldapscripts csomaggal kapcsolatos további részletekért lásd a kézikönyvoldalakat: man ldapscripts, man ldapadduser, man ldapaddgroup stb.

2. Samba és LDAP

Ez a fejezet a Samba beállításáról szól LDAP használatára a felhasználó-, csoport-, és gépi fiókinformációkhoz és hitelesítésre. Feltételezzük, hogy már van egy működő OpenLDAP címtára telepítve, és a kiszolgáló be van állítva annak használatára hitelesítéshez. Az OpenLDAP beállításával kapcsolatos információkért lásd a 1. szakasz - OpenLDAP kiszolgáló [56] és 1.7. szakasz - LDAP hitelesítés [70] szakaszokat. A Samba telepítésével és beállításával kapcsolatos információkért lásd: 17. fejezet - Windows hálózat [223]

2.1. Telepítés

Három csomag szükséges a Samba-LDAP integrációhoz: a samba, samba-doc és smbldap-tools csomagok. A csomagok telepítéséhez adja ki a következő parancsot:

```
sudo apt-get install samba samba-doc smbldap-tools
```

Szigorúan véve az smbldap-tools csomag nem szükséges, de ha nincs másik csomagja vagy egyéni parancsfájlja, akkor szükség van rá a felhasználók, csoportok és számítógépes fiókok kezeléséhez.

2.2. OpenLDAP beállítása

Ahhoz, hogy a Samba az OpenLDAP-t használja passdb háttérprogramként, a címtár felhasználóobjektumainak további attribútumokkal kell rendelkezniük. Ez a szakasz feltételezi, hogy a Sambát Windows NT tartományvezérlőként szeretné beállítani, és bemutatja a szükséges LDAP-objektumok és -attribútumok felvételét.

- A Samba-attribútumok a `samba.schema` fájlban vannak megadva, amely a samba-doc csomag része. A sémafájlt ki kell bontani, és át kell másolni az `/etc/ldap/schema` alá. Adja ki a következő parancsot:

  ```
  sudo cp /usr/share/doc/samba-doc/examples/LDAP/samba.schema.gz /etc/ldap/schema/
  sudo gzip -d /etc/ldap/schema/samba.schema.gz
  ```

- A samba sémát fel kell venni a cn=config fába. Az új séma slapd démonba felvételének eljárását a 1.3. szakasz - További beállítások [59] szakasz ismerteti.

  1. Első lépésként hozzon létre egy `schema_convert.conf` vagy hasonló beszédes nevű konfigurációs fájlt, a következő tartalommal:

     ```
     include /etc/ldap/schema/core.schema
     include /etc/ldap/schema/collective.schema
     include /etc/ldap/schema/corba.schema
     include /etc/ldap/schema/cosine.schema
     include /etc/ldap/schema/duaconf.schema
     include /etc/ldap/schema/dyngroup.schema
     include /etc/ldap/schema/inetorgperson.schema
     ```

```
include /etc/ldap/schema/java.schema
include /etc/ldap/schema/misc.schema
include /etc/ldap/schema/nis.schema
include /etc/ldap/schema/openldap.schema
include /etc/ldap/schema/ppolicy.schema
include /etc/ldap/schema/samba.schema
```

2. Ezután hozzon létre egy átmeneti könyvtárat a kimenet tárolásához:

```
mkdir /tmp/ldif_output
```

3. Most az slapcat használatával konvertálja a sémafájlokat:

```
slapcat -f schema_convert.conf -F /tmp/ldif_output -n0 -s "cn={12}samba,cn=schema,cn=config"
```

   Módosítsa a fenti fájl- és útvonalneveket a sajátjainak megfelelően.

4. Szerkessze az előállított `/tmp/cn\=samba.ldif` fájlt, módosítsa a következő attribútumokat:

```
dn: cn=samba,cn=schema,cn=config
...
cn: samba
```

   Távolítsa el a következő sorokat a fájl aljáról:

```
structuralObjectClass: olcSchemaConfig
entryUUID: b53b75ca-083f-102d-9fff-2f64fd123c95
creatorsName: cn=config
createTimestamp: 20080827045234Z
entryCSN: 20080827045234.341425Z#000000#000#000000
modifiersName: cn=config
modifyTimestamp: 20080827045234Z
```

   Az attribútumértékek eltérők lesznek, győződjön meg róla, hogy eltávolította az attribútumokat.

5. Végül az ldapadd segédprogrammal vegye fel az új sémát a címtárba:

```
ldapadd -x -D cn=admin,cn=config -W -f /tmp/cn\=samba.ldif
```

Ekkor létre kellett jönnie egy dn: cn={X}misc,cn=schema,cn=config elemnek, amelyben az X a soron következő sémabejegyzés a cn=config fában.

- Másolja a következőket egy `samba_indexes.ldif` nevű fájlba:

```
dn: olcDatabase={1}hdb,cn=config
changetype: modify
add: olcDbIndex
olcDbIndex: uidNumber eq
olcDbIndex: gidNumber eq
```

```
olcDbIndex: loginShell eq
olcDbIndex: uid eq,pres,sub
olcDbIndex: memberUid eq,pres,sub
olcDbIndex: uniqueMember eq,pres
olcDbIndex: sambaSID eq
olcDbIndex: sambaPrimaryGroupSID eq
olcDbIndex: sambaGroupType eq
olcDbIndex: sambaSIDList eq
olcDbIndex: sambaDomainName eq
olcDbIndex: default sub
```

Az ldapmodify segédprogrammal töltse be az új indexeket:

```
ldapmodify -x -D cn=admin,cn=config -W -f samba_indexes.ldif
```

Ha minden jól ment, az ldapsearch segítségével láthatja az új indexeket:

```
ldapsearch -xLLL -D cn=admin,cn=config -x -b cn=config -W olcDatabase={1}hdb
```

- Ezután állítsa be az smbldap-tools csomagot a környezetének megfelelően. A csomag tartalmaz egy beállító parancsfájlt, amely kérdéseket tesz fel a szükséges beállításokról. A futtatásához adja ki a következőt:

```
sudo gzip -d /usr/share/doc/smbldap-tools/configure.pl.gz
sudo perl /usr/share/doc/smbldap-tools/configure.pl
```

A kérdések megválaszolása után létre kell jönnie egy `/etc/smbldap-tools/smbldap.conf` és egy `/etc/smbldap-tools/smbldap_bind.conf` nevű fájlnak. Ezeket a fájlokat a beállító parancsfájl állítja elő, így ha a parancsfájl futtatásakor eltéveszt valamit, egyszerűbb lehet a fájl közvetlen szerkesztése.

- Az smbldap-populate parancsfájl felveszi a Samba által igényelt felhasználókat, csoportokat és LDAP-objektumokat. A parancs végrehajtása előtt jó ötlet LDIF-formátumú biztonsági mentést készíteni az slapcat segítségével:

```
sudo slapcat -l backup.ldif
```

- A naprakész biztonsági mentés elkészülte után hajtsa végre az smbldap-populate parancsot:

```
sudo smbldap-populate
```

A sudo smbldap-populate -e samba.ldif végrehajtásával létrehozhat egy, az új Samba-objektumokat tartalmazó LDIF-fájlt. Ez lehetővé teszi a változtatások áttekintését, így meggyőződhet arról, hogy minden rendben ment.

Az LDAP-címtár most rendelkezik a szükséges tartományinformációkkal a Samba-felhasználók hitelesítéséhez.

2.3. Samba beállítása

A Samba több módon is beállítható. Az egyes gyakoribb beállításokkal kapcsolatban nézze meg a 17. fejezet - Windows hálózat [223] szakaszt. A Samba LDAP használatára való beállításához szerkessze az `/etc/samba/smb.conf` nevű elsődleges Samba konfigurációs fájlt, és vegye ki megjegyzésből a passdb backend beállítást, valamint vegye fel a következőket:

```
#   passdb backend = tdbsam

# LDAP Settings
   passdb backend = ldapsam:ldap://gépnév
   ldap suffix = dc=példa,dc=hu
   ldap user suffix = ou=Emberek
   ldap group suffix = ou=Csoportok
   ldap machine suffix = ou=Számítógépek
   ldap idmap suffix = ou=Idmap
   ldap admin dn = cn=admin,dc=példa,dc=hu
   ldap ssl = start tls
   ldap passwd sync = yes
...
   add machine script = sudo /usr/sbin/smbldap-useradd -t 0 -w "%u"
```

Az új beállítások életbe léptetéséhez indítsa újra a samba démont:

```
sudo /etc/init.d/samba restart
```

A Sambának ismernie kell az LDAP admin jelszót. Adja ki a következő parancsot:

```
sudo smbpasswd -w titok
```

A titok helyére az LDAP admin jelszót írja.

Ha vannak felhasználók az LDAP-ban, és szeretné hogy azok a Samba használatával jelentkezzenek be, akkor meg kell adnia néhány Samba attribútumot a `samba.schema` fájlban. A meglévő felhasználókhoz a Samba attribútumokat az smbpasswd segédprogrammal adja hozzá, a felhasználónév helyére a meglévő felhasználó nevét írva:

```
sudo smbpasswd -a felhasználónév
```

Ezután a program bekéri a felhasználó jelszavát.

Új felhasználó, csoport és gépi fiókok felvételéhez használja az smbldap-tools csomag segédprogramjait. Néhány példa:

- Adja ki a következőt új felhasználó felvételéhez az LDAP-ba Samba attribútumokkal, a felhasználónév helyére a meglévő felhasználó nevét írva:

```
sudo smbldap-useradd -a -P felhasználónév
```

A -a kapcsoló felveszi a Samba attribútumokat, a -P kapcsoló pedig meghívja az smbldap-passwd segédprogramot a felhasználó létrehozása után, lehetővé téve a felhasználó jelszavának megadását.

- Adja ki a következőt felhasználó eltávolításához a címtárból:

```
sudo smbldap-userdel felhasználónév
```

Az smbldap-userdel segédprogram rendelkezik egy -r kapcsolóval is a felhasználó saját könyvtárának eltávolításához.

- Csoport hozzáadásához használja az smbldap-groupadd segédprogramot, a csoportnév helyett a megfelelő csoport megadásával:

```
sudo smbldap-groupadd -a csoportnév
```

Az smbldap-useradd segédprogramhoz hasonlóan a -a kapcsoló felveszi a Samba attribútumokat.

- Felhasználó csoporthoz adásához használja az smbldap-groupmod parancsot:

```
sudo smbldap-groupmod -m felhasználónév csoportnév
```

A felhasználónév helyére egy valódi felhasználó nevét írja. A -m kapcsolóval egyszerre több felhasználót is megadhat vesszőkkel elválasztott formátumban felsorolva őket.

- Az smbldap-groupmod felhasználó csoporból történő eltávolítására is használható:

```
sudo smbldap-groupmod -x felhasználónév csoportnév
```

- Ezen kívül az smbldap-useradd segédprogrammal gépi Samba fiókokat is felvehet:

```
sudo smbldap-useradd -t 0 -w felhasználónév
```

A felhasználónév helyére a munkaállomás gépnevét írja. A -t 0 kapcsoló a gépi fiókot késleltetés nélkül hozza létre, míg a -w kapcsoló a felhasználót gépi fiókként határozza meg. Ne feledje, hogy az `/etc/samba/smb.conf` add machine script beállítása megváltozott az smbldap-useradd használatára.

Az smbldap-tools csomag további hasznos segédprogramokat és lehetőségeket tartalmaz. Az egyes segédprogramok kézikönyvoldalai további részleteket tartalmaznak.

2.4. Információforrások

- Az LDAP és a Samba kapcsolata több helyen is dokumentálva van a Samba HOWTO Collection[5] részeként.
- Konkrétan lásd a passdb szakaszt[6]

- Szintén hasznos információk találhatók a Samba OpenLDAP HOWTO[7] oldalon.
- Az smbldap-tools csomaggal kapcsolatos további információk a kézikönyvoldalakon találhatók: man smbldap-useradd, man smbldap-groupadd, man smbldap-populate stb.
- Az Ubuntu wiki[8] is számos cikket tartalmaz a témáról.

3. Kerberos

A Kerberos egy megbízható harmadik fél elvére épülő hálózati hitelesítési rendszer. A másik két fél a felhasználó, és az a szolgáltatás, amelyhez a felhasználó be szeretne jelentkezni. Nem minden szolgáltatás és alkalmazás képes Kerberos használatára, de azok számára amelyek igen, a hálózatot egy lépéssel közelebb viszi a Single Sign On (SSO) típusú működéshez.

Ez a szakasz a Kerberos kiszolgáló telepítését és beállítását ismerteti, valamint néhány példa klienskonfigurációt.

3.1. Áttekintés

Ha még nem használt Kerberost, akkor néhány fogalommal meg kell ismerkednie a Kerberos kiszolgáló beállítása előtt. A legtöbb kifejezés más környezetekből ismerős dolgokhoz kapcsolódik:

- Résztvevő: minden felhasználót, számítógépet és kiszolgálók által biztosított szolgáltatást Kerberos résztvevőként kell meghatározni.
- Példányok: szolgáltatás-résztvevők és speciális adminisztratív résztvevők megnevezése.
- Tartományok: a Kerberos rendszer által biztosított egyedi felügyeleti tartomány. Általában a DNS-tartomány nagybetűssé alakítva (PÉLDA.HU).
- A kulcsszolgáltató (KDC) három részből áll, az összes résztvevő adatbázisa, a hitelesítési kiszolgáló és a jegymegadási kiszolgáló. Minden tartományhoz legalább egy KDC kell tartozzon.
- Jegybiztosító jegy: a hitelesítési kiszolgáló (AS) által kiadott jegybiztosító jegy (TGT) a felhasználó jelszavában van titkosítva, amelyet csak a felhasználó és a KDC ismer.
- A jegykiadó szolgáltatás (TGS) kérésre szolgáltatásjegyeket ad ki a klienseknek.
- A jegyek megerősítik a két résztvevő személyazonosságát. Az egyik résztvevő a felhasználó, a másik pedig a felhasználó által kért szolgáltatás. A jegyek létrehozzák a hitelesített munkamenet során a biztonságos kommunikációhoz használt titkosított kulcsot.
- Kulcstáblafájlok: ezek a KDC résztvevő-adatbázisából kinyert fájlok egy szolgáltatás vagy gép titkosítási kulcsát tartalmazzák.

Összefoglalva egy tartománynak legalább egy, de a redundancia érdekében inkább két, résztvevők adatbázisát tartalmazó KDC-vel kell rendelkeznie. Ha egy felhasználó résztvevő bejelentkezik egy Kerberos hitelesítésre beállított munkaállomásra, akkor a KDC kiad egy jegybiztosító jegyet (TGT). Ha a felhasználó által megadott hitelesítési adatok megfelelők, akkor a felhasználó hitelesítve lesz és jegyeket kérhet a Kerberost támogató szolgáltatásokhoz a jegykiadó szolgáltatástól (TGS). A szolgáltatásjegyek lehetővé teszik a felhasználó bejelentkezését a szolgáltatáshoz a felhasználónév és jelszó ismételt megadása nélkül.

3.2. Kerberos kiszolgáló

3.2.1. Telepítés

A Kerberos kiszolgáló telepítése előtt szükség van egy megfelelően beállított DNS-kiszolgálóra a tartományban. Mivel a Kerberos tartomány megállapodás szerint megegyezik a tartománynévvel, ez a szakasz az 2.3. szakasz - Elsődleges mester [97] szakaszban beállított példa.hu tartományt használja.

A Kerberos ezen kívül időérzékeny protokoll is. Emiatt ha a helyi rendszeridő a kliensgép és a kiszolgáló között (alapértelmezésben) 5 percnél többel tér el, akkor a munkaállomás nem lesz képes hitelesítésre. A probléma megszüntetése érdekében minden kiszolgálónak a Hálózati időprotokoll (NTP) segítségével kell szinkronizálnia idejét. Az NTP beállításáról lásd: 4. szakasz - Időszinkronizálás NTP-vel [46].

A Kerberos tartomány telepítésének első lépése a krb5-kdc és krb5-admin-server csomagok telepítése. Adja ki a következő parancsot:

```
sudo apt-get install krb5-kdc krb5-admin-server
```

A telepítés végén a program bekéri a tartomány Kerberos és Admin kiszolgálóinak nevét, ezek lehetnek önállóak vagy ugyanaz a kiszolgáló is.

Ezután hozza létre az új tartományt a kdb5_newrealm segédprogrammal:

```
sudo krb5_newrealm
```

3.2.2. Beállítás

A telepítés során feltett kérdések segítségével az `/etc/krb5.conf` fájl kerül beállításra. Ha módosítania kell a kulcsszolgáltató (KDC) beállításait, akkor szerkessze ezt a fájlt, és indítsa újra a krb5-kdc démont.

1. Miután a KDC működik, egy admin felhasználóra van szükség. Ajánlott a normál felhasználónevétől eltérő felhasználót használni. Ezt a kadmin.local segítségével teheti meg; adja ki a következő parancsot:

```
sudo kadmin.local
Authenticating as principal root/admin@PÉLDA.HU with password.
kadmin.local: addprinc geza/admin
WARNING: no policy specified for geza/admin@PÉLDA.HU; defaulting to no policy
Enter password for principal "geza/admin@PÉLDA.HU":
Re-enter password for principal "geza/admin@PÉLDA.HU":
Principal "geza/admin@PÉLDA.HU" created.
kadmin.local: quit
```

A fenti példában geza a résztvevő, az /admin egy példány, a @PÉLDA.HU pedig a tartományt jelzi. A mindennapos résztvevő geza@PÉLDA.HU, és csak normál felhasználói jogai vannak.

A PÉLDA.HU és a geza helyére a saját tartományának és admin felhasználójának nevét írja.

2. Ezután az új admin felhasználónak megfelelő hozzáférés-vezérlési (ACL) jogosultságokra van szüksége. A jogosultságokat az `/etc/krb5kdc/kadm5.acl` fájlban lehet megadni:

```
geza/admin@PÉLDA.HU        *
```

Ez a bejegyzés képessé teszi geza/admin felhasználót tetszőleges művelet végrehajtására a tartomány összes résztvevőjén.

3. Ezután indítsa újra a krb5-admin-server démont az új ACL életbe léptetéséhez:

```
sudo /etc/init.d/krb5-admin-server restart
```

4. Az új felhasználó résztvevő a kinit segédprogram használatával tesztelhető:

```
kinit geza/admin
geza/admin@PÉLDA.HU's Password:
```

A jelszó megadása után a klist segédprogrammal jeleníthetők meg a jegybiztosító jeggyel (TGT) kapcsolatos információk:

```
klist
Credentials cache: FILE:/tmp/krb5cc_1000
        Principal: geza/admin@PÉLDA.HU

  Issued           Expires          Principal
Jul 13 17:53:34  Jul 14 03:53:34  krbtgt/PÉLDA.HU@PÉLDA.HU
```

Szükség lehet egy bejegyzés felvételére az `/etc/hosts` fájlba a KDC-hez. Például:

```
192.168.0.1   kdc01.példa.hu       kdc01
```

A 192.168.0.1 helyére a KDC IP-címét írja.

5. A tartományhoz tartozó KDC kliensek általi lekéréséhez néhány DNS SRV rekord szükséges. Vegye fel a következőket az `/etc/named/db.példa.hu` fájlba:

```
_kerberos._udp.PÉLDA.HU.      IN SRV 1  0 88  kdc01.példa.hu.
_kerberos._tcp.PÉLDA.HU.      IN SRV 1  0 88  kdc01.példa.hu.
_kerberos._udp.PÉLDA.HU.      IN SRV 10 0 88  kdc02.példa.hu.
_kerberos._tcp.PÉLDA.HU.      IN SRV 10 0 88  kdc02.példa.hu.
_kerberos-adm._tcp.PÉLDA.HU. IN SRV 1  0 749 kdc01.példa.hu.
_kpasswd._udp.PÉLDA.HU.       IN SRV 1  0 464 kdc01.példa.hu.
```

A PÉLDA.HU, kdc01 és kdc02 helyére a tartomány, az elsődleges KDC és a másodlagos KDC nevét írja.

A DNS beállításával kapcsolatos részletes utasításokért lásd: 7. fejezet - Tartománynév-szolgáltatás (DNS) [94].

Az új Kerberos tartomány ezzel felkészült a kliensek hitelesítésére.

3.3. Másodlagos KDC

Miután beüzemelt egy kulcsszolgáltatót a hálózatán, hasznos lehet beállítani egy másodlagos KDC-t is, ha az első elérhetetlenné válna.

1. Első lépésként telepítse a csomagokat, majd a Kerberos és admin kiszolgálók neveinek bekérésekor adja meg az elsődleges KDC nevét:

```
sudo apt-get install krb5-kdc krb5-admin-server
```

2. A csomagok telepítése után hozza létre a másodlagos KDC kiszolgáló résztvevőjét. Adja ki a következő parancsot:

```
kadmin -q "addprinc -randkey host/kdc02.példa.hu"
```

Ezután a további kadmin parancsok kiadásakor a rendszer bekéri a felhasználónév/admin@PÉLDA.HU résztvevő jelszavát.

3. Másolja le a kulcstábla fájlt:

```
kadmin -q "ktadd -k keytab.kdc02 host/kdc02.példa.hu"
```

4. Meg kell jelennie egy `keytab.kdc02` fájlnak az aktuális könyvtárban. Mozgassa ezt a fájlt az `/etc/krb5.keytab` helyre:

```
sudo mv keytab.kdc02 /etc/krb5.keytab
```

Ha a `keytab.kdc02` fájl útvonala eltér, módosítsa értelemszerűen.

A klist segédprogrammal ki is írathatja a kulcstáblafájlt, ami hibakereséskor lehet hasznos:

```
sudo klist -k /etc/krb5.keytab
```

5. Ezen kívül lennie kell egy `kpropd.acl` fájlnak minden KDC-n, amely felsorolja a tartományban lévő összes KDC-t. Az elsődleges és másodlagos KDC-n is hozza létre az `/etc/krb5kdc/kpropd.acl` fájt:

```
host/kdc01.példa.hu@PÉLDA.HU
host/kdc02.példa.hu@PÉLDA.HU
```

6. Hozzon létre egy üres adatbázist a másodlagos KDC-n:

```
sudo kdb5_util -s create
```

7. Ezután indítsa el a kpropd démont, amely a kprop segédprogramtól érkező kapcsolatokat figyeli. A kprop a kiíratási fájlok átvitelére használatos:

```
sudo kpropd -S
```

8. Az elsődleges KDC-n egy terminálból hozzon létre egy kiíratási fájlt az elsődleges adatbázisból:

```
sudo kdb5_util dump /var/lib/krb5kdc/dump
```

9. Másolja ki az elsődleges KDC kulcstábla fájlját, és másolja át az `/etc/krb5.keytab` fájlba:

```
kadmin -q "ktadd -k keytab.kdc01 host/kdc01.példa.hu"
sudo mv keytab.kdc01 /etc/kr5b.keytab
```

A kulcstábla lemásolása előtt győződjön meg róla, hogy a kdc01.példa.hu bejegyzéshez tartozik host.

10. A kprop segédprogrammal vigye át az adatbázist a másodlagos KDC-re:

```
sudo kprop -r PÉLDA.HU -f /var/lib/krb5kdc/dump kdc02.példa.hu
```

Ha a másolás sikeres, egy SUCCEEDED üzenet jelenik meg. Ha hibaüzenetet lát, akkor további információkért nézze meg a `/var/log/syslog` fájlt.

Hasznos lehet létrehozni egy cron feladatot a másodlagos KDC adatbázisának rendszeres frissítéséhez. A következő például óránként átmásolja az adatbázist:

```
# m h  dom mon dow   command
0 * * * * /usr/sbin/kdb5_util dump /var/lib/krb5kdc/dump && /usr/sbin/kprop -r PÉLDA.HU -f /var
```

11. A másodlagos KDC-n hozzon létre egy stash fájlt a Kerberos elsődleges kulcsának tárolásához:

```
sudo kdb5_util stash
```

12. Végül indítsa el a krb5-kdc démont a másodlagos KDC-n:

```
sudo /etc/init.d/krb5-kdc start
```

A másodlagos KDC-nek ezután képesnek kell lennie jegyek kiadására a tartományhoz. Ez ellenőrizhető az elsődleges KDC krb5-kdc démonjának leállításával, majd egy jegy kérésével a kinit használatával. Ha minden jól megy, meg kell kapnia a jegyet a másodlagos KDC-től.

3.4. Kerberos Linux kliens

Ez a szakasz egy Linux rendszer Kerberos kliensként való beállítását ismerteti. Ez lehetővé teszi a Kerberost támogató szolgáltatások elérését, miután a felhasználó sikeresen bejelentkezett a rendszerbe.

3.4.1. Telepítés

Egy Kerberos tartományba való bejelentkezéshez a krb5-user és libpam-krb5 csomagok szükségesek, valamint van néhány nem kötelező, de az életet megkönnyítő csomag is. A telepítésükhöz adja ki a következőt:

```
sudo apt-get install krb5-user libpam-krb5 libpam-ccreds auth-client-config
```

Az auth-client-config csomag lehetővé teszi a PAM egyszerű beállítását több forrásból való bejelentkezéshez, a libpam-ccreds pedig gyorsítótárazza a bejelentkezési személyes adatokat, ezzel lehetővé téve a bejelentkezést akkor is, ha a kulcsszolgáltató (KDC) nem érhető el. Ez a csomag hasznos laptopok használatakor is, amelyeknek képeseknek kell lenniük Kerberos használatával való bejelentkezésre a céges hálózaton, de a hálózatról leválasztva is elérhetőnek kell maradniuk.

3.4.2. Beállítás

A kliens beállításához adja ki a következő parancsot:

```
sudo dpkg-reconfigure krb5-config
```

A beállítófelület bekéri a Kerberos tartomány nevét. Ha nincs beállítva DNS a Kerberos SRV rekordjaival, akkor a menü bekéri a kulcsszolgáltató (KDC) és tartományadminisztrációs kiszolgáló gépnevét.

A dpkg-reconfigure a tartomány `/etc/krb5.conf` fájljába vesz fel bejegyzéseket. A következőhöz hasonló bejegyzéseket kell látnia:

```
[libdefaults]
        default_realm = PÉLDA.HU
...
[realms]
        PÉLDA.HU = }
                kdc = 192.168.0.1
                admin_server = 192.168.0.1
        }
```

A beállításokat tesztelheti egy jegy kérésével a kinit segítségével. Például:

```
kinit geza@PÉLDA.HU
Password for geza@PÉLDA.HU:
```

A jegy megadása után a részletei a klist segítségével jeleníthetők meg:

```
klist
Ticket cache: FILE:/tmp/krb5cc_1000
Default principal: geza@PÉLDA.HU

Valid starting     Expires            Service principal
07/24/08 05:18:56  07/24/08 15:18:56  krbtgt/PÉLDA.HU@PÉLDA.HU
        renew until 07/25/08 05:18:57


Kerberos 4 ticket cache: /tmp/tkt1000
klist: You have no tickets cached
```

Ezután az auth-client-config segítségével állítsa be a libpam-krb5 modult jegy kérésére a bejelentkezés során:

```
sudo auth-client-config -a -p kerberos_example
```

A sikeres bejelentkezés után meg kell kapnia a jegyet.

3.5. Információforrások

- A Kerberossal kapcsolatos további információkért lásd a MIT Kerberos[9] oldalát.
- Az Ubuntu wiki Kerberos[10] oldala további részleteket tartalmaz.
- Az O'Reilly Kerberos: The Definitive Guide[11] című könyve remek referencia a Kerberos telepítésekor.
- A Freenode[12] #ubuntu-server IRC csatornáján is kérhet segítséget, ha a Kerberossal kapcsolatos kérdései vannak.

4. Kerberos és LDAP

A Kerberos résztvevő-adatbázis replikálása két kiszolgáló között bonyolult lehet, és egy újabb felhasználó-adatbázist ad a hálózatához. Szerencsére a MIT Kerberos beállítható LDAP címtár használatára résztvevő-adatbázisként. Ez a szakasz bemutatja az elsődleges és másodlagos Kerberos kiszolgáló beállítását OpenLDAP használatára résztvevő-adatbázisként.

4.1. OpenLDAP beállítása

Első lépésként a szükséges sémát kell betölteni egy OpenLDAP kiszolgálóra, amely rendelkezik hálózati kapcsolattal az elsődleges és másodlagos KDC-khez. A szakasz további része feltételezi, hogy az LDAP replikáció is be van állítva legalább két kiszolgáló között. Az OpenLDAP beállításával kapcsolatos információkért lásd: 1. szakasz - OpenLDAP kiszolgáló [56].

Szükség van még az OpenLDAP beállítására TLS és SSL kapcsolatokhoz, a KDC és az LDAP-kiszolgáló közötti forgalom titkosításához. A részletekért lásd: 1.6. szakasz - TLS és SSL [66].

- A séma LDAP-ba töltéséhez az LDAP-kiszolgálón telepítse a krb5-kdc-ldap csomagot. Adja ki a következő parancsot:

```
sudo apt-get install krb5-kdc-ldap
```

- Ezután bontsa ki a `kerberos.schema.gz` fájlt:

```
sudo gzip -d /usr/share/doc/krb5-kdc-ldap/kerberos.schema.gz
sudo cp /usr/share/doc/krb5-kdc-ldap/kerberos.schema /etc/ldap/schema/
```

- A kerberos sémát fel kell venni a cn=config fába. Az új séma slapd-be való felvételének módját a 1.3. szakasz - További beállítások [59] szakasz ismerteti.

1. Első lépésként hozzon létre egy `schema_convert.conf` vagy hasonló beszédes nevű konfigurációs fájlt, a következő tartalommal:

```
include /etc/ldap/schema/core.schema
include /etc/ldap/schema/collective.schema
include /etc/ldap/schema/corba.schema
include /etc/ldap/schema/cosine.schema
include /etc/ldap/schema/duaconf.schema
include /etc/ldap/schema/dyngroup.schema
include /etc/ldap/schema/inetorgperson.schema
include /etc/ldap/schema/java.schema
include /etc/ldap/schema/misc.schema
include /etc/ldap/schema/nis.schema
include /etc/ldap/schema/openldap.schema
include /etc/ldap/schema/ppolicy.schema
include /etc/ldap/schema/kerberos.schema
```

2. Hozzon létre egy ideiglenes könyvtárat az LDIF-fájlok tárolásához:

```
mkdir /tmp/ldif_output
```

3. Most az slapcat használatával konvertálja a sémafájlokat:

```
slapcat -f schema_convert.conf -F /tmp/ldif_output -n0 -s "cn={12}kerberos,cn=schema,cn=confi
```

Módosítsa a fenti fájl- és útvonalneveket a sajátjainak megfelelően.

4. Szerkessze a kapott `/tmp/cn\=kerberos.ldif` fájlt, és módosítsa a következő attribútumokat:

```
dn: cn=kerberos,cn=schema,cn=config
...
cn: kerberos
```

Távolítsa el a következő sorokat a fájl végéről:

```
structuralObjectClass: olcSchemaConfig
entryUUID: 18ccd010-746b-102d-9fbe-3760cca765dc
creatorsName: cn=config
createTimestamp: 20090111203515Z
entryCSN: 20090111203515.326445Z#000000#000#000000
modifiersName: cn=config
modifyTimestamp: 20090111203515Z
```

Az attribútumértékek eltérők lesznek, győződjön meg róla, hogy eltávolította az attribútumokat.

5. Töltse be az új sémát az ldapadd használatával:

```
ldapadd -x -D cn=admin,cn=config -W -f /tmp/cn\=kerberos.ldif
```

6. Vegyen fel indexet a krb5principalname attribútumhoz:

```
ldapmodify -x -D cn=admin,cn=config -W
Enter LDAP Password:
dn: olcDatabase={1}hdb,cn=config
add: olcDbIndex
olcDbIndex: krbPrincipalName eq,pres,sub

modifying entry "olcDatabase={1}hdb,cn=config"
```

7. Végül frissítse a hozzáférés-vezérlési listákat (ACL):

```
ldapmodify -x -D cn=admin,cn=config -W
Enter LDAP Password:
dn: olcDatabase={1}hdb,cn=config
replace: olcAccess
olcAccess: to attrs=userPassword,shadowLastChange,krbPrincipalKey by dn="cn=admin,dc=példa
,dc=hu" write by anonymous auth by self write by * none
```

```
-
add: olcAccess
olcAccess: to dn.base="" by * read
-
add: olcAccess
olcAccess: to * by dn="cn=admin,dc=példa,dc=hu" write by * read

modifying entry "olcDatabase={1}hdb,cn=config"
```

Ennyi az egész, az LDAP-címtár ezzel készen áll a Kerberos résztvevő-adatbázisként való használatra.

4.2. Elsődleges KDC beállítása

Az OpenLDAP beállítása után ideje beállítani a KDC-t is.

- Első lépésként telepítse a szükséges csomagokat, adja ki a következő parancsot:

```
sudo apt-get install krb5-kdc krb5-admin-server krb5-kdc-ldap
```

- Szerkessze az `/etc/krb5.conf` fájlt, az alábbi beállítások megfelelő szakaszokhoz adásával:

```
[libdefaults]
        default_realm = PÉLDA.HU

...

[realms]
        PÉLDA.HU = {
                kdc = kdc01.példa.hu
                kdc = kdc02.példa.hu
                admin_server = kdc01.példa.hu
                admin_server = kdc02.példa.hu
                default_domain = példa.hu
                database_module = openldap_ldapconf
        }

...

[domain_realm]
        .példa.hu = PÉLDA.HU


...

[dbdefaults]
        ldap_kerberos_container_dn = dc=példa,dc=hu

[dbmodules]
        openldap_ldapconf = {
```

```
                db_library = kldap
                ldap_kdc_dn = "cn=admin,dc=példa,dc=hu"

                # this object needs to have read rights on
                # the realm container, principal container and realm sub-trees
                ldap_kadmind_dn = "cn=admin,dc=példa,dc=hu"

                # this object needs to have read and write rights on
                # the realm container, principal container and realm sub-trees
                ldap_service_password_file = /etc/krb5kdc/service.keyfile
                ldap_servers = ldaps://ldap01.példa.hu ldaps://ldap02.példa.hu
                ldap_conns_per_server = 5
        }
```

A példa.hu, dc=példa,dc=hu, cn=admin,dc=példa,dc=hu és az ldap01.példa.hu helyére a hálózatának megfelelő tartományt, LDAP-objektumot és LDAP-kiszolgálót írja.

- Ezután a kdb5_ldap_util segédprogrammal hozza létre a tartományt:

```
sudo kdb5_ldap_util -D cn=admin,dc=példa,dc=hu create -subtrees dc=példa,dc=hu -r PÉLDA.HU -s -H
```

- Hozzon létre egy stash fájlt az LDAP-kiszolgálóhoz kapcsolódásra használt jelszóval. Ezt a jelszót az `/etc/krb5.conf` fájl ldap_kdc_dn és ldap_kadmin_dn beállításai használják:

```
sudo kdb5_ldap_util -D cn=admin,dc=példa,dc=hu stashsrvpw -f /etc/krb5kdc/service.keyfile cn=admi
```

- Másolja át a CA-tanúsítványt az LDAP-kiszolgálóról:

```
scp ldap01:/etc/ssl/certs/cacert.pem .
sudo cp cacert.pem /etc/ssl/certs
```

Módosítsa az `/etc/ldap/ldap.conf` fájlt a tanúsítvány használatához:

```
TLS_CACERT /etc/ssl/certs/cacert.pem
```

A tanúsítványt a másodlagos KDC-re is át kell másolni, az LDAP-kiszolgálókhoz LDAPS használatával való kapcsolódás engedélyezéséhez.

Most már felvehet Kerberos résztvevőket az LDAP-adatbázisba, ezek minden más, replikációra beállított LDAP-kiszolgálóra át lesznek másolva. Adja ki a következő parancsot résztvevő hozzáadásához a kadmin.local segédprogrammal:

```
sudo kadmin.local
Authenticating as principal root/admin@PÉLDA.HU with password.
kadmin.local:  addprinc -x dn="uid=geza,ou=emberek,dc=példa,dc=hu" geza
WARNING: no policy specified for geza@PÉLDA.HU; defaulting to no policy
Enter password for principal "geza@PÉLDA.HU":
Re-enter password for principal "geza@PÉLDA.HU":
Principal "geza@PÉLDA.HU" created.
```

Ezután a uid=geza,ou=emberek,dc=példa,dc=hu felhasználóobjektumhoz meg kell jelenniük a krbPrincipalName, krbPrincipalKey, krbLastPwdChange és krbExtraData attribútumoknak. A kinit és klist segédprogramokkal tesztelheti, hogy a felhasználó valóban kap-e jegyet.

Ha a felhasználóobjektum már létezik, akkor a -x dn="..." kapcsoló szükséges a Kerberos attribútumok hozzáadásához. Ellenkező esetben egy új résztvevőobjektum jön létre a tartomány részfájában.

4.3. Másodlagos KDC beállítása

A másodlagos KDC beállítása az LDAP-háttérprogram használatára hasonlóan történik a normál Kerberos adatbázist használó beállításához.

- Első lépésként telepítse a szükséges csomagokat, adja ki a következő parancsot:

```
sudo apt-get install krb5-kdc krb5-admin-server krb5-kdc-ldap
```

- Ezután szerkessze az `/etc/krb5.conf` fájlt az LDAP-háttérprogram használata érdekében:

```
[libdefaults]
        default_realm = PÉLDA.HU

...

[realms]
        PÉLDA.HU = {
                kdc = kdc01.példa.hu
                kdc = kdc02.példa.hu
                admin_server = kdc01.példa.hu
                admin_server = kdc02.példa.hu
                default_domain = példa.hu
                database_module = openldap_ldapconf
        }

...

[domain_realm]
        .példa.hu = PÉLDA.HU


...

[dbdefaults]
        ldap_kerberos_container_dn = dc=példa,dc=hu

[dbmodules]
        openldap_ldapconf = {
                db_library = kldap
                ldap_kdc_dn = "cn=admin,dc=példa,dc=hu"
```

```
                # this object needs to have read rights on
                # the realm container, principal container and realm sub-trees
                ldap_kadmind_dn = "cn=admin,dc=példa,dc=hu"

                # this object needs to have read and write rights on
                # the realm container, principal container and realm sub-trees
                ldap_service_password_file = /etc/krb5kdc/service.keyfile
                ldap_servers = ldaps://ldap01.példa.hu ldaps://ldap02.példa.hu
                ldap_conns_per_server = 5
        }
```

- Hozzon létre stash fájlt az LDAP-hoz kapcsolódásra használt jelszóról:

```
sudo kdb5_ldap_util -D cn=admin,dc=példa,dc=hu stashsrvpw -f /etc/krb5kdc/service.keyfile cn=admi
```

- Ezután az elsődleges KDC-n másolja át az `/etc/krb5kdc/.k5.PÉLDA.HU` elsődleges kulcs stash fájlt a másodlagos KDC-re. Ne feledje a fájlt titkosított kapcsolaton vagy fizikai adathordozón átmásolni.

```
sudo scp /etc/krb5kdc/.k5.PÉLDA.HU geza@kdc02.példa.hu:~
sudo mv .k5.PÉLDA.HU /etc/krb5kdc/
```

A PÉLDA.HU helyére a tényleges tartományt írja.

- Végül indítsa el a krb5-kdc démont:

```
sudo /etc/init.d/krb5-kdc start
```

Ezzel a hálózatán működő redundáns KDC-kkel és a redundáns LDAP-kiszolgálókkal képes lesz a felhasználók hitelesítésére akkor is, ha az egyik LDAP-kiszolgáló, az egyik Kerberos-kiszolgáló, vagy egy LDAP-kiszolgáló és egy Kerberos-kiszolgáló is elérhetetlenné válik.

4.4. Információforrások

- A Kerberos Admin Guide[13] további részleteket tartalmaz.
- A kdb5_ldap_util segédprogrammal kapcsolatos további információkért lásd az 5.6-os fejezetet[14] és a kdb5_ldap_util kézikönyvoldalát[15].
- Szintén hasznos lehet elolvasni a krb5.conf kézikönyvoldalát[16].
- Ezeken kívül nézze még meg a Kerberos és LDAP[17] Ubuntu wiki oldalt.

7. fejezet - Tartománynév-szolgáltatás (DNS)

A Tartománynév-szolgáltatás (DNS) egy internetes szolgáltatás, amely az IP-címeket és a teljes képzésű tartományneveket (FQDN) megfelelteti egymásnak. Ilyen módon a DNS megszünteti az IP-címek megjegyzésének szükségességét. A DNS-t futtató kiszolgálókat névkiszolgálóknak nevezzük. Az Ubuntu a BIND-et (Berkley Internet Naming Daemon) tartalmazza, ez Linuxon a névkiszolgáló működtetésére leggyakrabban használt program.

1. Telepítés

Adja ki a következő parancsot a dns telepítéséhez:

```
sudo apt-get install bind9
```

A DNS problémák teszteléséhez és megoldásához nagyon hasznos a dnsutils csomag. A dnsutils telepítéséhez adja ki a következő parancsot:

```
sudo apt-get install dnsutils
```

2. Beállítás

A BIND9 számos módon beállítható. A leggyakoribb konfigurációk a gyorsítótárazó névkiszolgáló, elsődleges mester és másodlagos mester.

- Gyorsítótárazó névkiszolgálóként használva a BIND9 megkeresi a lekérdezésekre a választ, és megjegyzi azt a tartomány következő lekéréséhez.
- Elsődleges mesterként a BIND9 beolvassa a zóna adatait a gépen lévő fájlból, és az adott zónára irányadó lesz.
- Másodlagos mester konfigurációban a BIND9 a zónaadatokat másik, az adott zónában mérvadó névkiszolgálótól kapja.

2.1. Áttekintés

A DNS-konfigurációs fájlok az `/etc/bind` könyvtárban találhatók. Az elsődleges konfigurációs fájl az `/etc/bind/named.conf`.

Az include sor megadja a DNS-beállításokat tartalmazó fájl nevét. Az `/etc/bind/named.conf.options` fájl directory sora adja meg a DNS-nek, hogy hol keresse a fájlokat. A BIND által használt összes fájlt ehhez a könyvtárhoz képest keresi.

Az `/etc/bind/db.root` nevű fájl írja le a világszintű gyökér-névkiszolgálókat. A kiszolgálók idővel változnak, emiatt az `/etc/bind/db.root` fájlt rendszeresen karban kell tartani. Ezt általában a bind9 csomag frissítései végzik. A zone szakasz egy mesterkiszolgálót definiál, és ez a file beállításban említett fájlban kerül tárolásra.

Ugyanaz a kiszolgáló beállítható gyorsítótárazó névkiszolgálónak, elsődleges és másodlagos mesternek is. Egy kiszolgáló lehet az egyik zóna esetén a mérvadó adatforrásrekord (SOA), míg másik zóna számára másodlagos szolgáltatást biztosíthat. Ezalatt pedig a helyi hálózat gépei számára gyorsítótárazási szolgáltatásokat nyújthat.

2.2. Gyorsítótárazó névkiszolgáló

Az alapértelmezett konfiguráció egy gyorsítótárazó kiszolgáló beállításait tartalmazza. Egyedül az internetszolgáltató DNS-kiszolgálóinak IP-címeit kell hozzáadnia. Vegye ki megjegyzésből és szerkessze a következőket az `/etc/bind/named.conf.options` fájlban:

```
forwarders {
                1.2.3.4;
                5.6.7.8;
          };
```

Az 1.2.3.4 és 5.6.7.8 helyére a tényleges névkiszolgálók IP-címeit írja.

Most indítsa újra a DNS-kiszolgálót az új beállítások engedélyezéséhez. Adja ki a következő parancsot:

```
sudo /etc/init.d/bind9 restart
```

A gyorsítótárazó DNS-kiszolgáló tesztelésével kapcsolatos információkért lásd a 3.1.2. szakasz - dig [101] szakaszt.

2.3. Elsődleges mester

Ebben a szakaszban a BIND9 elsődleges mesterként kerül beállításra a példa.hu tartományhoz. A példa.hu helyére a saját teljes képzésű tartománynevét (FQDN) írja.

2.3.1. Közvetlen zóna fájl

A BIND9 elsődleges mesterkiszolgálóvá tétele érdekében egy DNS-zóna BIND9-hez adásának első lépése az `/etc/bind/named.conf.local` fájl szerkesztése:

```
zone "példa.hu" {
 type master;
        file "/etc/bind/db.példa.hu";
};
```

Egy meglévő zónafájlt sablonként használva hozza létre az `/etc/bind/db.példa.hu` fájlt:

```
sudo cp /etc/bind/db.local /etc/bind/db.példa.hu
```

Szerkessze az új `/etc/bind/db.példa.hu` zónafájlt, és módosítsa a localhost. előtagot a kiszolgáló FQDN-jére, meghagyva a záró pontot a végén. A 127.0.0.1 helyére a névkiszolgáló IP-címét írja, a root.localhost helyére pedig egy érvényes e-mail címet, azonban a megszokott „@” szimbólum helyett használjon pontot, és a záró pontot itt is hagyja meg.

Hozzon létre egy A rekordot az ns.példa.hu számára. Ebben a példában a névkiszolgáló:

```
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     ns.példa.hu. root.példa.hu. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      ns.példa.hu.
@       IN      A       127.0.0.1
```

```
@       IN      AAAA    ::1
ns      IN      A       192.168.1.10
```

A Serial értékét minden alkalommal növelnie kell, amikor módosítja a zónafájlt. Ha több változtatást hajt végre a BIND9 újraindítása előtt, akkor elég csak egyszer növelni a Serial értékét.

Most már felveheti a DNS-rekordokat a zónafájl aljára. Részletekért lásd a 4.1. szakasz - Gyakori rekordtípusok [105] szakaszt.

Sok rendszergazda a zóna sorozatszámaként az utolsó szerkesztés dátumát szereti használni, például: 2010010100, amely ééééhhnnss formátumban van és az ss a sorozatszám.

Miután módosította a zónafájlt, a módosítások életbe léptetéséhez újra kell indítani a BIND9-et:

```
sudo /etc/init.d/bind9 restart
```

2.3.2. Fordított zónafájl

A zóna és a nevek IP-címekké feloldásának beállítása után szükség van egy fordított zónára is. A fordított zóna segítségével a DNS fel tudja oldani a címet névvé.

Szerkessze az /etc/bind/named.conf.local fájlt, és vegye fel a következőket:

```
zone "1.168.192.in-addr.arpa" {
        type master;
        notify no;
        file "/etc/bind/db.192";
};
```

Az 1.168.192 helyére az Ön által használt hálózat első három oktetjét írja. Ennek megfelelően nevezze el az `/etc/bind/db.192` zónafájlt. A névnek meg kell egyeznie a hálózat első oktetjével.

Most hozza létre az `/etc/bind/db.192` fájlt:

```
sudo cp /etc/bind/db.127 /etc/bind/db.192
```

Szerkessze az `/etc/bind/db.192` fájlt, és módosítsa ugyanazokat a beállításokat, mint az `/etc/bind/db.példa.hu` esetén:

```
;
; BIND reverse data file for local loopback interface
;
$TTL    604800
@       IN      SOA     ns.példa.hu. root.példa.hu. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
```

```
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      ns.
10      IN      PTR     ns.példa.hu.
```

A fordított zóna Serial értékét is növelni kell minden módosítás után. Az `/etc/bind/db.példa.hu` fájlban beállított minden A rekordhoz létre kell hoznia egy PTR rekordot az `/etc/bind/db.192` fájlban.

A fordított zóna létrehozása után indítsa újra a BIND9 démont:

```
sudo /etc/init.d/bind9 restart
```

2.4. Másodlagos mester

Az elsődleges mester beállítása után egy másodlagos mestert is be kell állítani a tartomány elérhetőségének fenntartása érdekében, amennyiben az elsődleges mester elérhetetlenné válna.

Első lépésként az elsődleges mester kiszolgálón engedélyezni kell a zónaátvitelt. Vegye fel az allow-transfer beállítást a példa közvetlen és fordított zónadefiníciókba az `/etc/bind/named.conf.local` fájlban:

```
zone "példa.hu" {
        type master;
 file "/etc/bind/db.példa.hu";
        allow-transfer { 192.168.1.11; };
};

zone "1.168.192.in-addr.arpa" {
        type master;
        notify no;
        file "/etc/bind/db.192";
 allow-transfer { 192.168.1.11; };
};
```

A 192.168.1.11 helyére a másodlagos névkiszolgáló IP-címét írja.

Ezután a másodlagos mesteren telepítse a bind9 csomagot. Szerkessze az `/etc/bind/named.conf.local` fájlt, és vegye fel a következő deklarációkat a közvetlen és fordított zónákhoz:

```
zone "példa.hu" {
 type slave;
        file "/var/cache/bind/db.példa.hu";
        masters { 192.168.1.10; };
};
```

```
zone "1.168.192.in-addr.arpa" {
 type slave;
        file "/var/cache/bind/db.192";
        masters { 192.168.1.10; };
};
```

A 192.168.1.10 helyére az elsődleges névkiszolgáló IP-címét írja.

Indítsa újra a BIND9 démont a másodlagos mesteren:

```
sudo /etc/init.d/bind9 restart
```

A `/var/log/syslog` fájlban valami ehhez hasonlót kell látnia:

```
slave zone "példa.hu" (IN) loaded (serial 6)
slave zone "100.18.172.in-addr.arpa" (IN) loaded (serial 3)
```

Megjegyzés: a zóna csak akkor kerül átvitelre, ha a Serial érték nagyobb az elsődleges mesteren, mint a másodlagoson.

A nem mérvadó zónafájlok alapértelmezett könyvtára a `/var/cache/bind/`. Az AppArmor engedélyezi az írást ebbe a könyvtárba a named számára. Az AppArmorral kapcsolatos további információkért lásd az 4. szakasz - AppArmor [121] szakaszt.

3. Hibaelhárítás

Ez a szakasz a DNS-sel és a BIND9-cel kapcsolatban fellépő problémák okának meghatározását segítő módszereket ismerteti.

3.1. Tesztelés

3.1.1. resolv.conf

A BIND9 tesztelésének első lépése a névkiszolgáló IP-címének felvétele egy gépnévfeloldóba. Be kell állítani az elsődleges névkiszolgálót, valamint még egy gépet az alapos ellenőrzés érdekében. Szerkessze az `/etc/resolv.conf` fájlt, és vegye fel a következőket:

```
nameserver 192.168.1.10
nameserver 192.168.1.11
```

Vegye fel a másodlagos névkiszolgáló IP-címét is arra az esetre, ha az elsődleges elérhetetlenné válna.

3.1.2. dig

Ha telepítette a dnsutils csomagot, akkor a dig nevű DNS-kikereső segédprogrammal tesztelheti a rendszert:

- A BIND9 telepítése után használja a dig programot a visszacsatolási felületen, és győződjön meg róla, hogy az figyel az 53-as porton. Adja ki a következő parancsot:

  ```
  dig -x 127.0.0.1
  ```

  A parancs kimenetében a következőhöz hasonló sorokat kell látnia:

  ```
  ;; Query time: 1 msec
  ;; SERVER: 192.168.1.10#53(192.168.1.10)
  ```

- Ha a BIND9-et gyorsítótárazó névkiszolgálóként állította be, akkor használja a „dig” programot egy külső tartományra a lekérdezési idő ellenőrzése érdekében:

  ```
  dig ubuntu.com
  ```

  Figyelje meg a lekérdezési időt a parancs kimenetének vége felé:

  ```
  ;; Query time: 49 msec
  ```

  A dig második kiadása után ennek javulnia kell:

  ```
  ;; Query time: 1 msec
  ```

3.1.3. ping

A DNS alkalmazások általi névfeloldásra való használatának bemutatása érdekében küldjön a ping segédprogrammal egy ICMP echo kérést. Adja ki a következő parancsot:

```
ping példa.hu
```

Ez teszteli, hogy a névkiszolgáló fel tudja-e oldani a ns.példa.hu nevet IP-címmé. A parancs kimenetének ehhez kell hasonlítania:

```
PING ns.példa.hu (192.168.1.10) 56(84) bytes of data.
64 bytes from 192.168.1.10: icmp_seq=1 ttl=64 time=0.800 ms
64 bytes from 192.168.1.10: icmp_seq=2 ttl=64 time=0.813 ms
```

3.1.4. named-checkzone

A zónafájlok tesztelésére jó módszer a bind9 csomaggal telepített named-checkzone segédprogram használata. Ez a segédprogram lehetővé teszi a beállítások helyességének ellenőrzését a BIND9 újraindítása és a változtatások életbe lépése előtt.

- A példa közvetlen zóna teszteléséhez adja ki a következő parancsot:

  ```
  named-checkzone példa.hu /etc/bind/db.példa.hu
  ```

  Ha minden megfelelően van beállítva, akkor a következőhöz hasonló kimenetet kell látnia:

  ```
  zone példa.hu/IN: loaded serial 6
  OK
  ```

- A fordított zóna teszteléséhez adja ki a következőt:

  ```
  named-checkzone példa.hu /etc/bind/db.192
  ```

  A kimenetnek ehhez hasonlónak kell lennie:

  ```
  zone példa.hu/IN: loaded serial 3
  OK
  ```

A zónafájl Serial értéke valószínűleg el fog térni.

3.2. Naplózás

A BIND9 rengeteg naplózási beállítással rendelkezik. Két fő beállítás van: a channel beállítás megadja, hogy a naplók hova kerüljenek, a category beállítás pedig a naplózandó információkat.

Ha nincs beállítva a naplózás, akkor az alapértelmezés a következő:

```
logging {
     category default { default_syslog; default_debug; };
     category unmatched { null; };
};
```

Ez a szakasz a BIND9 beállítását ismerteti a DNS-lekérdezésekkel kapcsolatos hibakeresési üzenetek külön fájlba küldésére.

- Első lépésként be kell állítani egy csatornát az üzenetek célfájljának megadásához. Szerkessze az `/etc/bind/named.conf.local` fájlt, és vegye fel a következőt:

```
logging {
    channel query.log {
        file "/var/log/query.log";
        severity debug 3;
    };
};
```

- Ezután állítson be egy kategóriát az összes DNS-lekérdezés elküldéséhez a lekérdezésfájlba:

```
logging {
    channel query.log {
        file "/var/log/query.log";
        severity debug 3;
    };
    category queries { query.log; };
};
```

Megjegyzés: a debug beállítás 1 és 3 közti értékeket vehet fel. Ha nincs megadva a szint, akkor az alapértelmezés az 1.

- Mivel a named démon a bind felhasználó nevében fut, ezért létre kell hozni a `/var/log/query.log` fájlt és jogosultságait módosítani kell:

```
sudo touch /var/log/query.log
sudo chown bind /var/log/query.log
```

- Mielőtt a named démon írhatna az új fájlba, az AppArmor profilt frissíteni kell. Első lépésként szerkessze az `/etc/apparmor.d/usr.sbin.named` fájlt, és vegye fel a következőt:

```
/var/log/query.log w,
```

Töltse újra a profilt:

```
cat /etc/apparmor.d/usr.sbin.named | sudo apparmor_parser -r
```

Az AppArmorral kapcsolatos további információkért lásd az 4. szakasz - AppArmor [121] szakaszt.

- Most indítsa újra a BIND9 démont a változtatások életbe léptetéséhez:

```
sudo /etc/init.d/bind9 restart
```

Látnia kell, hogy a `/var/log/query.log` fájl megtelik információkkal. Ez csak egy egyszerű példa a BIND9 naplózási lehetőségeinek bemutatására. A speciális beállításokért lásd a 4.2. szakasz - További információk [105] szakaszt.

4. Hivatkozások

4.1. Gyakori rekordtípusok

Ez a szakasz a leggyakrabban használt DNS-rekordtípusokat ismerteti.

- A rekord: ez a rekord egy IP-címet képez le gépnévre.

```
www      IN    A      192.168.1.12
```

- CNAME rekord: meglévő A rekord álnevének létrehozására szolgál. Másik CNAME rekordra mutató CNAME rekord nem hozható létre.

```
web     IN    CNAME  www
```

- MX rekord: az e-mailek céljának megadására szolgál. Nem mutathat CNAME rekordra, csak A rekordra.

```
        IN    MX  1   mail.példa.hu.
mail    IN    A       192.168.1.13
```

- NS rekord: egy zóna másolatait biztosító kiszolgálókra mutat. Nem mutathat CNAME rekordra, csak A rekordra. Ez határozza meg az elsődleges és másodlagos kiszolgálókat.

```
        IN    NS     ns.példa.hu.
 IN    NS     ns2.példa.hu.
ns      IN    A      192.168.1.10
ns2 IN    A      192.168.1.11
```

4.2. További információk

- A DNS HOWTO[1] további, a BIND9 konfigurálásához használható beállításokat ismertet.
- A DNS és BIND9 mélyebb megismeréséhez lásd a Bind9.net[2] oldalt.
- A DNS and BIND[3] egy népszerű könyv, és már az ötödik kiadásnál jár.
- A BIND9 problémák felvetésére, és az Ubuntu kiszolgáló közösség életébe való bekapcsolódásra remek hely a freenode[4] #ubuntu-server IRC-csatornája.
- Az Ubuntu wiki BIND9 Server HOWTO[5] oldalát is érdemes megnézni.

8. fejezet - Biztonság

A biztonságot mindig, minden számítógépes rendszer telepítésekor, üzembe állításakor és használatakor figyelembe kell venni. Noha az Ubuntu friss telepítése elég biztonságos az interneten való azonnali használathoz, fontos tisztában lenni a rendszer biztonsági helyzetével az üzembe helyezés utáni használat függvényében.

Ez a szakasz a biztonsággal kapcsolatos témákat mutatja be, amennyiben azok az Ubuntu 10.04 LTS kiszolgálókra szánt változatát érintik, és körvonalazza azokat az egyszerű intézkedéseket, amelyekkel kiszolgálója és hálózata tetszőleges számú lehetséges biztonsági fenyegetéstől megvédhető.

1. Felhasználókezelés

A felhasználókezelés a biztonságos rendszer karbantartásának kritikus része. A nem megfelelő felhasználó- és jogosultságkezelés gyakran a rendszerek feltörését eredményezi. Emiatt fontos megértenie, hogyan védheti meg rendszerét egyszerű és hatékony felhasználóifiók-kezelési eljárásokkal.

1.1. Hol van a root?

Az Ubuntu fejlesztői tudatos döntést hoztak, amikor alapértelmezésben letiltották a root fiókot minden Ubuntu telepítésen. Ez nem azt jelenti, hogy a root fiók törlésre került, vagy hogy ne lenne elérhető. Egyszerűen csak olyan jelszót kapott, amelyhez egyetlen lehetséges titkosított érték sem tartozik, így közvetlenül nem lehet bejelentkezni rá.

Ehelyett a felhasználókat a rendszergazdai feladatok végrehajtásához a sudo nevű eszköz használatára bátorítjuk. A sudo lehetővé teszi a felhatalmazott felhasználó számára jogosultságainak saját jelszavának használatával történő, a root fiókhoz tartozó jelszó ismerete nélküli ideiglenes megemelését. Ez az egyszerű, de mégis hatékony módszer biztosítja az összes felhasználói művelet elszámoltathatóságát, és lehetővé teszi a rendszergazdának a felhasználók által az adott jogokkal végezhető műveletek részletes felügyeletét.

- Ha valamilyen okból engedélyezni szeretné a root fiókot, egyszerűen csak adjon neki jelszót:

  ```
  sudo passwd
  ```

  A sudo bekéri a jelszavát, majd új jelszó megadására kéri a root felhasználó számára:

  ```
  [sudo] password for felhasználónév: (adja meg saját jelszavát)
  Enter new UNIX password: (adja meg a root új jelszavát)
  Retype new UNIX password: (ismételje meg a root új jelszavát)
  passwd: password updated successfully
  ```

- A root fiók letiltásához adja ki a következő parancsot:

  ```
  sudo passwd -l root
  ```

- További információkért nézze meg a Sudo kézikönyvoldalát:

  ```
  man sudo
  ```

Alapértelmezésben az Ubuntu telepítő által létrehozott első felhasználó az „admin” csoport tagja, amely felhatalmazott sudo felhasználóként felvételre kerül az `/etc/sudoers` fájlba. Ha másik fióknak is teljes rendszergazdai hozzáférést szeretne biztosítani a sudo használatával, akkor egyszerűen adja hozzá az admin csoporthoz.

1.2. Felhasználók hozzáadása és törlése

A helyi felhasználók és csoportok kezelése egyszerű és alig különbözik a más GNU/Linux operációs rendszereken megszokottól. Az Ubuntu és más Debian alapú disztribúciók a fiókok kezeléséhez az „adduser” csomag használatát ajánlják.

- Felhasználói fiók hozzáadásához használja a következő parancsot, és kövesse a megjelenő utasításokat a fiók jelszavának és azonosítható jellemzőinek (például teljes név, telefonszám, stb.) megadásához.

```
sudo adduser felhasználónév
```

- Felhasználói fiók és elsődleges csoportjának törléséhez adja ki a következő parancsot:

```
sudo deluser felhasználónév
```

  A fiók törlése nem törli a hozzá tartozó saját könyvtárat. Ez a rendszergazdára van bízva, aki saját kezűleg törölheti a könyvtárat, vagy megtarthatja a helyi adatmegőrzési irányelveknek megfelelően.

  Ne feledje, hogy az előző tulajdonossal azonos felhasználói- és csoportazonosítóval felvett új felhasználó hozzá fog férni ehhez a könyvtárhoz, ha nem tette meg a szükséges óvintézkedéseket.

  Hasznos lehet módosítani ezeket a felhasználói- és csoportazonosítókat valami megfelelőbbre, például a root fiókéra, sőt akár áthelyezni a könyvtárat a jövőbeli konfliktusok elkerülése érdekében:

```
sudo chown -R root:root /home/felhasználónév/
sudo mkdir /home/archivált_felhasználók/
sudo mv /home/felhasználónév /home/archivált_felhasználók/
```

- Felhasználói fiók ideiglenes zárolásához vagy feloldásához adja ki a következő parancsokat:

```
sudo passwd -l felhasználónév
sudo passwd -u felhasználónév
```

- Személyre szabott csoport hozzáadásához vagy törléséhez adja ki a következő parancsokat:

```
sudo addgroup csoportnév
sudo delgroup csoportnév
```

- Felhasználó csoporthoz adásához adja ki a következő parancsot:

```
sudo adduser felhasználónév csoportnév
```

1.3. Felhasználói profil biztonsága

Új felhasználó létrehozásakor az adduser segédprogram egy vadonatúj saját könyvtárat hoz létre `/home/felhasználónév` néven. Az alapértelmezett profil az `/etc/skel` könyvtár tartalma alapján jön létre, ez a könyvtár tartalmazza a profil minden alapértelmezését.

Ha a kiszolgálójának több felhasználója lesz, oda kell figyelnie a felhasználók saját könyvtárainak jogosultságaira az adatok bizalmasságának biztosítása érdekében. Ubuntu alatt alapértelmezésben a felhasználók saját könyvtárai mindenki számára olvasási és végrehajtási jogot biztosítanak. Ez azt jelenti, hogy minden felhasználó tallózhatja és elérheti más felhasználók saját könyvtárait. Ez nem biztos, hogy minden környezetben megfelelő.

- A meglévő felhasználók saját könyvtárainak jogosultságainak ellenőrzéséhez adja ki a következő parancsot:

  ```
  ls -ld /home/felhasználónév
  ```

  A következő kimenet jelzi, hogy a `/home/felhasználónév` könyvtár mindenki számára olvasható:

  ```
  drwxr-xr-x  2 felhasználónév felhasználónév     4096 2007-10-02 20:03 felhasználónév
  ```

- A mindenki számára biztosított olvasási jogosultság eltávolításához adja ki a következő parancsot:

  ```
  sudo chmod 0750 /home/felhasználónév
  ```

  

  Egyesek megkülönböztetés nélkül használják a rekurzív kapcsolót (-R), ami minden gyermekmappát és fájlt módosít, noha ez nem csak szükségtelen, de más nemkívánatos eredményekre is vezethet. A szülőkönyvtár önmagában elégséges a szülőkönyvtár tartalmának jogosultság nélküli elérésének megakadályozásához.

  A probléma sokkal hatékonyabb megoldása lehet az adduser globális alapértelmezett jogosultságainak módosítása a felhasználók saját könyvtárának létrehozásakor. Egyszerűen szerkessze az `/etc/adduser.conf` fájlt, és a `DIR_MODE` változót módosítsa úgy, hogy az összes új saját könyvtár a megfelelő jogosultságokat kapja.

  ```
  DIR_MODE=0750
  ```

- A könyvtárjogosultságok az előbbi eljárások egyikével való javítása után ellenőrizze az eredményeket a következő parancs kiadásával:

  ```
  ls -ld /home/felhasználónév
  ```

  Az alábbi kimenet jelzi, hogy a mindenki által olvasható jogosultság eltávolításra került:

  ```
  drwxr-x---   2 felhasználónév felhasználónév    4096 2007-10-02 20:03 felhasználónév
  ```

1.4. Jelszóházirend

A biztonsági helyzet egyik legfontosabb szempontja az erős jelszóházirend. Számos sikeres betöréshez nyers erőt és szótári támadást használtak gyenge jelszavak ellen. Ha a helyi jelszórendszert érintő bármilyen távoli hozzáférést tervez kínálni, akkor győződjön meg róla, hogy megfelelően kezeli a minimális jelszó-bonyolultsági követelményeket, a maximális jelszó-élettartamot, és a hitelesítési rendszer gyakori auditálását.

1.4.1. Minimális jelszóhossz

Alapértelmezésben az Ubuntu 4 karakteres minimális jelszóhosszt vár, valamint néhány minimális entrópia-ellenőrzést is végez. Ezeket az értékeket az `/etc/pam.d/common-password` fájl vezérli, amelyet alább részletezünk.

```
password   required   pam_unix.so nullok obscure min=4 max=8 md5
```

Ha a minimális hosszt 6 karakterre szeretné növelni, módosítsa a megfelelő változót min=6 értékre. A módosított sor a következő lesz:

```
password   required   pam_unix.so nullok obscure min=6 max=8 md5
```

A `max=8` változó nem a jelszó maximális hosszát képviseli. Azt jelenti, hogy a 8 karakternél hosszabb jelszavak összetettségi követelményei nem kerülnek ellenőrzésre. A jelszó entrópiájával kapcsolatos további segítségért telepítse a libpam-cracklib csomagot.

1.4.2. Jelszavak lejárata

Felhasználói fiókok létrehozásakor elő kell írnia a minimális és maximális jelszókort, így a jelszavak lejáratakor azok megváltoztatására kényszerítve a felhasználókat.

- A felhasználói fiók aktuális állapotát a következő parancs kiadásával jelenítheti meg:

  ```
  sudo chage -l felhasználónév
  ```

  Az alábbi kimenet érdekes tényeket közöl a felhasználói fiókról, nevezetesen azt, hogy nem érvényes rá semmilyen házirend:

  ```
  Last password change                                    : Jan 20, 2008
  Password expires                                        : never
  Password inactive                                       : never
  Account expires                                         : never
  Minimum number of days between password change          : 0
  Maximum number of days between password change          : 99999
  Number of days of warning before password expires       : 7
  ```

- Ezen értékek bármelyikének beállításához adja ki a következő parancsot, és kövesse a megjelenő utasításokat:

```
sudo chage felhasználónév
```

A következő példa bemutatja, hogyan módosíthatja saját kezűleg a pontos lejárati dátumot (-E) 2008. 01. 31.-re, a minimális jelszó-élettartamot (-m) 5 napra, a maximális jelszó-élettartamot (-M) 90 napra, és a figyelmeztetési időtartamot (-W) a jelszó lejártát megelőző 14 napra.

```
sudo chage –E 01/31/2008 –m 5 –M 90 –I 30 –W 14 felhasználónév
```

- A módosítások ellenőrzéséhez használja a korábban említett parancsot:

```
sudo chage –l felhasználónév
```

Az alábbi kimenet bemutatja a fiókhoz létrehozott új házirendet:

```
Last password change                                    : Jan 20, 2008
Password expires                                        : Apr 19, 2008
Password inactive                                       : May 19, 2008
Account expires                                         : Jan 31, 2008
Minimum number of days between password change          : 5
Maximum number of days between password change          : 90
Number of days of warning before password expires       : 14
```

1.5. Más biztonsági szempontok

Számos alkalmazás alternatív hitelesítési módszereket használ, amelyek egyszerűen elnézhetők még tapasztalt rendszergazdák számára is. Emiatt fontos megérteni és felügyelni a felhasználók hitelesítésének, és a kiszolgáló szolgáltatásainak és alkalmazásainak elérési módját.

1.5.1. SSH hozzáférés letiltott felhasználók által

A felhasználói fiók egyszerű letiltása/zárolása nem akadályozza meg a felhasználót a kiszolgálóra való távoli bejelentkezésben, ha korábban beállítottak nyilvános kulcsú RSA hitelesítést. Emiatt továbbra is képesek lesznek a kiszolgáló parancssoros elérésére, jelszó használata nélkül. Ne feledje el megkeresni a felhasználók saját mappáiban az ilyen típusú hitelesített SSH hozzáférést biztosító fájlokat, mint például a `/home/felhasználónév/.ssh/authorized_keys`.

Törölje, vagy nevezze át a `.ssh/` könyvtárat a felhasználó saját mappájában a jövőbeli SSH hitelesítési képesség megszüntetéséhez.

Ne feledje el ellenőrizni a letiltott felhasználó létrehozott SSH kapcsolatait, mert lehetséges hogy vannak létező bejövő vagy kimenő kapcsolatai. Ha talál ilyet, lője ki.

Korlátozza az SSH hozzáférést azokra a felhasználói fiókokra, akiknek tényleg szükségük van rá. Létrehozhat például egy „sshlogin” nevű csoportot, és felveheti a csoportnevet az `/etc/ssh/sshd_config` fájlban található `AllowGroups` változó értékeként.

```
AllowGroups sshlogin
```

Ezután vegye fel az engedélyezett SSH-felhasználókat az „sshlogin” csoportba, és indítsa újra az SSH szolgáltatást.

```
sudo adduser felhasználónév sshlogin
sudo /etc/init.d/ssh restart
```

1.5.2. Hitelesítés külső felhasználó-adatbázisból

A legtöbb vállalati hálózat központosított hitelesítést és hozzáférés-felügyeletet igényel az összes rendszer-erőforráshoz. Ha a kiszolgálóját a felhasználók külső adatbázisokból való hitelesítésére állította be, akkor tiltsa le a felhasználói fiókokat a külső adatbázisból és helyileg is, ezzel lehetetlenné téve a tartalék helyi hitelesítést.

2. Konzolos biztonság

A kiszolgáló védelmében emelt minden biztonsági akadályhoz hasonlóan meglehetősen nehéz a környezethez fizikai hozzáféréssel rendelkező személyek által okozott olyan váratlan károk ellen védekezni, mint például a merevlemezek ellopása, tápellátás vagy szolgáltatások megszakítása stb. Emiatt a konzolos biztonságot csak az átfogó fizikai biztonsági stratégia részeként kell kezelni. Egy bezárt „külső ajtóval” is el lehet rettenteni az átlagos bűnözőket, de legalábbis le lehet lassítani az eltökéltebbeket, emiatt a konzol biztonságával kapcsolatos alapvető óvintézkedések megtétele továbbra is javasolt.

Az alábbi utasítások segítenek megvédeni kiszolgálóját az olyan problémáktól, amelyek egyébként nagyon súlyos következményekkel járnának.

2.1. A Ctrl+Alt+Delete letiltása

Első és legfontosabb, hogy bárki, aki fizikai hozzáféréssel rendelkezik a billentyűzethez, a Ctrl+Alt+Delete billentyűkombináció lenyomásával bejelentkezés nélkül újraindíthatja a kiszolgálót. Persze ki is húzhatja a konnektorból, de éles kiszolgálón ezen billentyűkombináció használatát is le kell tiltani. Ez a támadót sokkal drasztikusabb lépésekre kényszeríti a kiszolgáló újraindításához, ugyanakkor megakadályozza a véletlen újraindítást is.

- A Ctrl+Alt+Delete billentyűkombináció lenyomására végrehajtott újraindítási művelet letiltásához a következő sort kell megjegyzésbe tenni az `/etc/init/control-alt-delete.conf` fájlban:

```
#exec shutdown -r now "Control-Alt-Delete pressed"
```

3. Tűzfal

3.1. Bevezetés

A Linux kernel tartalmazza a Netfilter alrendszert, amely a kiszolgálóra irányuló vagy azon átmenő hálózati forgalom sorsának befolyásolására vagy eldöntésére használható. Minden modern linuxos tűzfalmegoldás ezt a rendszert használja csomagszűrésre.

A kernel csomagszűrő rendszere kevéssé lenne használható a kezelésére szolgáló, felhasználói térből használható felület nélkül. Amikor egy csomag eléri a kiszolgálóját, átkerül a Netfilter alrendszernek elfogadásra, módosításra vagy elutasításra, a felhasználói térből az iptables segítségével megadott szabályok alapján. Így ha jól ismeri, akkor egyedül az iptablesre van szükség a tűzfal kezelésére, de számos előtétprogram érhető el a feladat egyszerűsítésére.

3.2. ufw - Uncomplicated Firewall

Az Ubuntu alapértelmezett tűzfalbeállító eszköze az ufw. Az iptables beállításának megkönnyítésére tervezett ufw felhasználóbarát módon teszi lehetővé IPv4 vagy IPv6 kiszolgálóalapú tűzfal létrehozását.

Alapértelmezésben az ufw le van tiltva. Az ufw kézikönyvoldala szerint:

„Az ufw-t nem teljes körű tűzfalszolgáltatások biztosítására tervezték a parancsfelületen keresztül, ehelyett lehetővé teszi egyszerű szabályok könnyű felvételét vagy eltávolítását.”

Az alábbiakban az ufw használatára láthat néhány példát:

- Első lépésként be kell kapcsolni az ufw-t. Adja ki a következő parancsot:

```
sudo ufw enable
```

- Port megnyitása (ebben a példában az SSH-hoz):

```
sudo ufw allow 22
```

- A szabályok számozott formátumban is felvehetők:

```
sudo ufw insert 1 allow 80
```

- Hasonlóképpen a nyitott port bezárásához:

```
sudo ufw deny 22
```

- Szabály eltávolításához használja a delete parancsot a szabály előtt:

```
sudo ufw delete deny 22
```

- Lehetőség van adott kiszolgálókról vagy hálózatokról engedélyezni a hozzáférést egy porthoz. A következő példa lehetővé teszi az SSH hozzáférést a 192.168.0.2 IP-című kiszolgálóról bármely IP-címhez ezen a kiszolgálón:

```
sudo ufw allow proto tcp from 192.168.0.2 to any port 22
```

  A 192.168.0.2 helyett a 192.168.0.0/24 használatával engedélyezhető az SSH hozzáférés a teljes alhálózatból.

- Az ufw parancs a --dry-run kapcsoló hatására kiírja az eredményül kapott szabályokat, de nem alkalmazza azokat. A következő példa bemutatja, hogy a HTTP port kinyitásához mi kerülne alkalmazásra:

```
sudo ufw --dry-run allow http
```

```
*filter
:ufw-user-input - [0:0]
:ufw-user-output - [0:0]
:ufw-user-forward - [0:0]
:ufw-user-limit - [0:0]
:ufw-user-limit-accept - [0:0]
### RULES ###

### tuple ### allow tcp 80 0.0.0.0/0 any 0.0.0.0/0
-A ufw-user-input -p tcp --dport 80 -j ACCEPT

### END RULES ###
-A ufw-user-input -j RETURN
-A ufw-user-output -j RETURN
-A ufw-user-forward -j RETURN
-A ufw-user-limit -m limit --limit 3/minute -j LOG --log-prefix "[UFW LIMIT]: "
-A ufw-user-limit -j REJECT
-A ufw-user-limit-accept -j ACCEPT
COMMIT
Rules updated
```

- Az ufw letiltható:

```
sudo ufw disable
```

- A tűzfal állapotának megjelenítéséhez adja ki a következőt:

```
sudo ufw status
```

- Részletesebb állapotinformációkért adja ki:

```
sudo ufw status verbose
```

- A számozott formátum megjelenítéséhez:

```
sudo ufw status numbered
```

Ha a kinyitni vagy bezárni kívánt port az `/etc/services` fájlban van meghatározva, akkor a szám helyett a portnevet is használhatja. A fenti példákban cserélje a 22-t az ssh-ra.

Ez az ufw használatának rövid bemutatása. További információkért nézze meg az ufw kézikönyvoldalát.

3.2.1. Az ufw alkalmazásintegrációja

A portokat megnyitó alkalmazások tartalmazhatnak egy ufw profilt, amely részletezi az alkalmazás megfelelő működéséhez szükséges portokat. Ezek a profilok az `/etc/ufw/applications.d` könyvtárban vannak, és az alapértelmezett portok módosításakor szerkeszthetők.

- A profilokat telepített alkalmazások felsorolásához adja ki a következő parancsot:

```
sudo ufw app list
```

- Az alkalmazásprofil használata a port forgalmának engedélyezéséhez hasonló módon, a következő parancs kiadásával érhető el:

```
sudo ufw allow Samba
```

- A bővített parancs is elérhető:

```
ufw allow from 192.168.0.0/24 to any app Samba
```

  A Samba és 192.168.0.0/24 helyett a használandó alkalmazásprofil nevét, és a hálózatának IP-tartományát adja meg.

  

  A protocol megadása nem szükséges az alkalmazáshoz, mivel ezt az információt a profil már tartalmazza. Ne feledje, hogy az alkalmazás neve helyettesíti a port számát.

- Egy alkalmazáshoz megadott portok, protokollok stb. részleteinek megjelenítéséhez adja ki a következőt:

```
sudo ufw app info Samba
```

Nem minden, hálózati port megnyitását igénylő alkalmazás tartalmaz ufw profilt, de ha készített profilt egy ilyen alkalmazáshoz, és szeretné azt a csomagban látni, akkor küldjön egy hibajelentést a csomaghoz a Launchpadra[1].

3.3. IP-maszkolás

Az IP-maszkolás célja, hogy a privát, nem közvetíthető IP-címekkel rendelkező gépek elérjék az internetet a maszkolást végző gépen keresztül. A magánhálózatból az internetre irányuló

[1] https://launchpad.net/

forgalmat úgy kell módosítani, hogy visszairányítható legyen a kérést küldő gépre. Ehhez a kernelnek módosítania kell minden csomag forrás IP-címét, hogy a válaszok hozzá legyenek visszairányítva, a kérést küldő gép IP-címe helyett, különben a válaszok nem érkeznének meg. A Linux a kapcsolatkövetést (conntrack) használja a gépek és a hozzájuk tartozó kapcsolatok nyilvántartására, és a visszaküldött csomagok ennek megfelelő átirányítására. A hálózatát elhagyó forgalom így „maszkolva” lesz, mintha az Ubuntu átjárógépről indult volna. Ezt a folyamatot a Microsoft dokumentációi internetkapcsolat megosztásának hívják.

3.3.1. ufw maszkolás

Az IP-maszkolás egyéni ufw szabályok használatával érhető el. Ez azért lehetséges, mert az ufw jelenlegi háttérprogramja az iptables-restore, amelynek szabályfájljai az `/etc/ufw/*.rules` alatt találhatók. Ezek a fájlok kiválóan alkalmasak az ufw nélkül használt örökölt iptables szabályok, valamint az inkább hálózati átjárókra és hidakra jellemző szabályok felvételére.

A szabályok két különböző fájlba vannak osztva: az ufw parancssori szabályok előtt, és az ufw parancssori szabályok után végrehajtandó szabályok.

- Első lépésként a csomagtovábbítást kell engedélyezni az ufw-ben. Két beállítófájlt kell módosítani, az `/etc/default/ufw` fájlban módosítsa DEFAULT_FORWARD_POLICY értékét „ACCEPT”-re:

  ```
  DEFAULT_FORWARD_POLICY="ACCEPT"
  ```

  Ezután szerkessze az `/etc/ufw/sysctl.conf` fájlt, és vegye ki megjegyzésből a következőt:

  ```
  net/ipv4/ip_forward=1
  ```

  Hasonlóképp, az IPv6 továbbításhoz vegye ki megjegyzésből a következőt:

  ```
  net/ipv6/conf/default/forwarding=1
  ```

- Ezután szabályokat kell az `/etc/ufw/before.rules` fájlba felvenni. Az alapértelmezett szabályok csak a filter táblát állítják be, a maszkolás engedélyezéséhez a nat táblát kell beállítani. A fejlécben lévő megjegyzések után vegye fel a következőket a fájl tetejére:

  ```
  # nat tábla szabályai
  *nat
  :POSTROUTING ACCEPT [0:0]

  # Forgalom továbbítása az eth1-ről az eth0-n keresztül.
  -A POSTROUTING -s 192.168.0.0/24 -o eth0 -j MASQUERADE

  # Ne törölje a „COMMIT” sort, különben ezen NAT-tábla szabályok nem kerülnek feldolgozásra
  COMMIT
  ```

A megjegyzések nem kötelezőek, de általában véve jó ötlet dokumentálni a beállításokat. Az `/etc/ufw` könyvtár rules fájljainak módosításakor ne felejtse el a módosított táblák utolsó soraként a következőt megadni:

```
# Ne törölje a „COMMIT” sort, különben ezen szabályok nem kerülnek feldolgozásra
COMMIT
```

Minden táblához tartoznia kell egy COMMIT utasításnak. Ebben a példában csak a nat és a filter táblák jelennek meg, de szerkesztheti a raw és mangle táblákat is.

A fenti példában látható eth0, eth1 és 192.168.0.0/24 helyett használja a hálózatának megfelelő csatolókat és IP-tartományt.

- Végül kapcsolja ki, majd be az ufw-t a módosítások alkalmazásához:

```
sudo ufw disable && sudo ufw enable
```

Az IP-maszkolás ezután engedélyezett. Felvehet további FORWARD szabályokat is az `/etc/ufw/before.rules` fájlba. Ezeket a további szabályokat javasolt az ufw-before-forward lánchoz adni.

3.3.2. iptables maszkolás

A maszkolás bekapcsolására az iptables is használható.

- Az ufw-hez hasonlóan az első lépés az IPv4 csomagtovábbítás engedélyezése az `/etc/sysctl.conf` szerkesztésével, és a következő sor megjegyzésből kivételével:

```
net.ipv4.ip_forward=1
```

Ha az IPv6 továbbítást is engedélyezni akarja, a következőt is vegye ki megjegyzésből:

```
net.ipv6.conf.default.forwarding=1
```

- Ezután adja ki a sysctl parancsot a beállítófájl új beállításainak életbe léptetéséhez:

```
sudo sysctl –p
```

- Az IP-maszkolás ezután elérhető egyetlen iptables szabállyal is, amely enyhén különbözhet a hálózati beállításoktól függően:

```
sudo iptables –t nat –A POSTROUTING –s 192.168.0.0/16 –o ppp0 –j MASQUERADE
```

A fenti parancs feltételezi, hogy a magán címtere a 192.168.0.0/16, és az internettel kommunikáló eszköze a ppp0. A szintaxis lebontva a következőkből áll:

- -t nat -- a szabály a nat táblába kerül
- -A POSTROUTING -- a szabályt a POSTROUTING lánchoz kell fűzni (-A)

- -s 192.168.0.0/16 -- a szabály a megadott címtérből induló forgalomra érvényes
- -o ppp0 -- a szabály a megadott hálózati eszközön való áthaladásra ütemezett forgalomra érvényes
- -j MASQUERADE -- a szabályra illeszkedő forgalomnak át kell „ugrania” (-j) a MASQUERADE célra a fent leírt manipuláció végrehajtásához

- A szűrőtábla (az alapértelmezett tábla, ahol a legtöbb vagy minden csomagszűrés történik) minden láncának alapértelmezett irányelve az ACCEPT, de ha átjáróeszközt kiegészítő tűzfalat készít, akkor szükség lehet a DROP vagy REJECT irányelv beállítására, ebben az esetben a maszkolt forgalmat át kell engedni a FORWARD láncon a fenti szabály működéséhez:

  ```
  sudo iptables –A FORWARD –s 192.168.0.0/16 –o ppp0 –j ACCEPT
  sudo iptables –A FORWARD –d 192.168.0.0/16 –m state ––state ESTABLISHED,RELATED –i ppp0 –j ACCEPT
  ```

  A fenti parancsok az összes kapcsolatot engedélyezik a helyi hálózatról az internetre, és lehetővé teszik az ezekhez a kapcsolatokhoz tartozó összes forgalom visszaküldését a kezdeményező gépre.
- Ha a maszkolást újraindítás után szeretné engedélyezni, akkor módosítsa az `/etc/rc.local` fájlt, és vegye fel bármelyik fenti parancsot. Például felveheti az első parancsot a szűrés kikapcsolásához:

  ```
  iptables –t nat –A POSTROUTING –s 192.168.0.0/16 –o ppp0 –j MASQUERADE
  ```

3.4. Naplók

A tűzfalnaplók alapvető fontosságúak a támadások felismerésében, a tűzfalszabályok hibáinak elhárításában, és a hálózatán tapasztalható szokatlan aktivitás felfedezésében. A tűzfalszabályok közé naplózási szabályokat is fel kell vennie a naplók előállításához, a naplózási szabályoknak pedig meg kell előzniük az alkalmazandó befejező szabályokat (a csomag sorsát eldöntő céllal rendelkező szabály, például ACCEPT, DROP vagy REJECT).

Ha az ufw-t használja, akkor a következő parancs kiadásával is bekapcsolhatja a naplózást:

```
sudo ufw logging on
```

A naplózás kikapcsolásához az ufw-ben egyszerűen cserélje a fenti parancsban az on értéket off-ra.

Ha az ufw helyett az iptables-t használja, akkor adja ki a következőt:

```
sudo iptables –A INPUT –m state ––state NEW –p tcp ––dport 80 –j LOG ––log-prefix "NEW_HTTP_CONN: "
```

Ezután a helyi gépről a 80-as portra irányuló kérés a dmesgben a következőhöz hasonló naplóbejegyzést hoz létre:

```
[4304885.870000] NEW_HTTP_CONN: IN=lo OUT= MAC=00:00:00:00:00:00:00:00:00:00:00:00:08:00 SRC=127.0.
```

A fenti naplósor megjelenik a `/var/log/messages`, `/var/log/syslog` és `/var/log/kern.log` fájlokban is. Ez a viselkedés az `/etc/syslog.conf` megfelelő szerkesztésével, vagy az ulogd

telepítésével és beállításával, valamint a LOG helyett az ULOG cél használatával módosítható. Az ulogd démon egy felhasználói térben futó kiszolgáló, amely a kerneltől a kifejezetten tűzfalakra vonatkozó naplózási utasításokat figyeli, és képes tetszőleges fájlba, vagy akár PostgreSQL vagy MySQL adatbázisba is naplózni. A tűzfalnaplók feldolgozása egyszerűsíthető olyan naplóelemző eszközök használatával, mint az fwanalog, fwlogwatch vagy lire.

3.5. Egyéb eszközök

Számos eszköz érhető el, amelyek az iptables mély ismerete nélkül is segítik a teljes tűzfal felépítésében. Grafikus felületen:

- A Firestarter[2] meglehetősen népszerű és egyszerűen használható.
- Az fwbuilder[3] nagyon hatékony, és ismerős lehet az olyan kereskedelmi tűzfal-segédprogramokhoz szokott rendszergazdáknak, mint a Checkpoint FireWall-1.

Ha parancssori eszközt használna egyszerű szöveges beállítófájlokkal:

- A Shorewall[4] egy nagyon hatékony megoldás, amely segítségével bármely hálózathoz fejlett tűzfal állítható be.
- Az ipkungfu[5] egy nulla beállítással is azonnal működő tűzfalat biztosít, és egyszerű, jól dokumentált beállítófájlok szerkesztésével teszi lehetővé fejlettebb tűzfalak könnyű beállítását.
- A firefliert[6] asztali tűzfalkezelő alkalmazásnak tervezték. Egy kiszolgálóból (fireflier-server) és tetszőleges grafikus kliensekből (GTK vagy QT) áll, és sok népszerű interaktív windowsos tűzfalalkalmazáshoz hasonlóan működik.

3.6. Hivatkozások

- Az Ubuntu Firewall[7] wikioldal az ufw fejlesztéséről tartalmaz információkat.
- Ezen kívül az ufw kézikönyvoldala is nagyon hasznos információkat tartalmaz: man ufw.
- Az iptables használatával kapcsolatos további információkért lásd a packet-filtering-HOWTO[8] dokumentumot.
- A nat-HOWTO[9] a maszkolással kapcsolatban tartalmaz további részleteket.
- Az IPTables HowTo[10] az Ubuntu wikiben hasznos olvasmány.

4. AppArmor

Az AppArmor a névalapú kötelező hozzáférés-vezérlés megvalósítása Linux biztonsági modulként. Az AppArmor az egyes programokat felsorolt fájlok és a posix 1003.1e vázlat szerinti képességek halmazához köti.

Az AppArmor alapértelmezésben telepítésre és betöltésre kerül. Az alkalmazásokra profilokat használ az alkalmazás által igényelt fájlok és jogosultságok meghatározásához. Néhány csomag saját profilt telepít, valamint további profilok találhatók az apparmor-profiles csomagban.

Az apparmor-profiles csomag telepítéséhez adja ki a következő parancsot:

```
sudo apt-get install apparmor-profiles
```

Az AppArmor profiloknak két végrehajtási módjuk van:

- Panaszkodás/tanulás: a profilsértések engedélyezettek, és naplózásra kerülnek. Új profilok teszteléséhez és fejlesztéséhez hasznos.
- Kényszerített/korlátozott: kikényszeríti a profilházirendet, és naplózza a megsértését.

4.1. Az AppArmor használata

Az apparmor-utils csomag parancssori segédprogramokat tartalmaz, amelyekkel módosíthatja az AppArmor végrehajtási módot, meghatározhatja egy profil állapotát, új profilokat hozhat létre stb.

- Az apparmor_status segítségével megjeleníthető az AppArmor profilok aktuális állapota.

  ```
  sudo apparmor_status
  ```

- Az aa-complain a profilt panaszkodás módba kapcsolja.

  ```
  sudo aa-complain /útvonal/végrehajtható
  ```

- Az aa-enforce a profilt kényszerített módba kapcsolja.

  ```
  sudo aa-enforce /útvonal/végrehajtható
  ```

- Az AppArmor profilok az `/etc/apparmor.d` könyvtárban találhatók. Használatával az összes profil módja kezelhető.

  Adja ki a következő parancsot az összes profil panaszkodás módba kapcsolásához:

  ```
  sudo aa-complain /etc/apparmor.d/*
  ```

  Minden profil kényszerített módba kapcsolásához:

  ```
  sudo aa-enforce /etc/apparmor.d/*
  ```

- Az apparmor_parser segítségével a profil betölthető a kernelbe. A -r kapcsoló segítségével használható a pillanatnyilag betöltött profil újratöltésére is. Profil betöltése:

```
cat /etc/apparmor.d/profil.név | sudo apparmor_parser -a
```

  Profil újratöltése:

```
cat /etc/apparmor.d/profil.név | sudo apparmor_parser -r
```

- Az `/etc/init.d/apparmor` segítségével az össze profil újratölthető:

```
sudo /etc/init.d/apparmor reload
```

- Az `/etc/apparmor.d/disable` könyvtár az apparmor_parser -R kapcsolójával együtt a profil letiltására használható.

```
sudo ln -s /etc/apparmor.d/profil.név /etc/apparmor.d/disable/
sudo apparmor_parser -R /etc/apparmor.d/profil.név
```

  Letiltott profil újraengedélyezéséhez távolítsa el a profilra mutató szimbolikus linket az `/etc/apparmor.d/disable/` könyvtárból. Ezután töltse be a profilt a -a kapcsoló használatával.

```
sudo rm /etc/apparmor.d/disable/profil.név
cat /etc/apparmor.d/profil.név | sudo apparmor_parser -a
```

- Az AppArmor letiltható, és a kernelmodul eltávolítható a következő parancs kiadásával:

```
sudo /etc/init.d/apparmor stop
sudo update-rc.d -f apparmor remove
```

- Az AppArmor újraengedélyezéséhez adja ki a következőt:

```
sudo /etc/init.d/apparmor start
sudo update-rc.d apparmor defaults
```

A profil.név helyet a kezelni kívánt profil nevét adja meg. Az `/útvonal/végrehajtható` helyett a tényleges végrehajtható fájl elérési útját adja meg. A ping parancshoz például a `/bin/ping` értéket használja.

4.2. Profilok

Az AppArmor profilok egyszerű szöveges fájlok az `/etc/apparmor.d/` könyvtárban. A fájlok neve az általuk leírt végrehajtható fájl teljes elérési útvonala, a „/” helyett a „.” elválasztóval. Az `/etc/apparmor.d/bin.ping` például a `/bin/ping` parancs AppArmor profilja.

A profilokban használt szabályoknak két fő típusuk van:

- Útvonalbejegyzések: ezek részletezik az alkalmazás által a fájlrendszerben elérhető fájlokat.

- Képességbejegyzések: ezek meghatározzák a korlátozott folyamat által használható jogosultságokat.

Vegyük például az `/etc/apparmor.d/bin.ping` fájlt:

```
#include <tunables/global>
/bin/ping flags=(complain) {
  #include <abstractions/base>
  #include <abstractions/consoles>
  #include <abstractions/nameservice>

  capability net_raw,
  capability setuid,
  network inet raw,

  /bin/ping mixr,
  /etc/modules.conf r,
}
```

- #include <tunables/global>: más fájlokban található utasítások felvétele. Ez lehetővé teszi a több alkalmazásra vonatkozó utasítások közös fájlba helyezését.
- /bin/ping flags=(complain): a profil által leírt program elérési útja, valamint a complain (panaszkodás) mód beállítása.
- capability net_raw,: lehetővé teszi az alkalmazás számára a CAP_NET_RAW Posix.1e képesség elérését.
- /bin/ping mixr,: engedélyezi az alkalmazásnak a fájl olvasását és végrehajtását.

A profilt a szerkesztés befejezése után újra kell tölteni. Részletekért lásd 4.1. szakasz - Az AppArmor használata [121] szakaszt.

4.2.1. Profil létrehozása

- Készítsen teszttervet: Gondolkodjon róla, hogy az alkalmazást hogyan kell megvizsgálni. A teszttervet kis tesztesetekre kell felosztani. Minden tesztesetnek rendelkeznie kell rövid leírással, és a követendő lépések listájával.

  Néhány általános teszteset:

  - A program elindítása.
  - A program leállítása.
  - A program újratöltése.
  - Az init parancsfájl által támogatott összes parancs tesztelése.
- Az új profil előállítása: Az aa-genprof használatával állítsa elő az új profilt. Adja ki a következő parancsot:

  `sudo aa-genprof végrehajtható`

Például:

```
sudo aa-genprof slapd
```

- A profil felvételéhez az apparmor-profiles csomagba, küldjön hibajelentést a Launchpadra az AppArmor[11] csomaghoz:
  - Vigye fel a teszttervet és teszteseteket.
  - Mellékelje az új profilt a hibajelentéshez.

4.2.2. Profilok frissítése

Amikor a program hibásan viselkedik, akkor auditálási üzenetek kerülnek a naplófájlokba. Az aa-logprof program segítségével kiszűrhetők a naplófájlokból az AppArmor auditálási üzenetei, majd áttekintésük után a profilok frissíthetők. Adja ki a következő parancsot:

```
sudo aa-logprof
```

4.3. Hivatkozások

- Speciális beállítási lehetőségekért lásd az AppArmor Administration Guide[12] dokumentumot.
- Az AppArmor más Ubuntu kiadásokon történő használatával kapcsolatban lásd az AppArmor közösségi wikioldalát[13].
- Az OpenSUSE AppArmor[14] oldala az AppArmor egy újabb bemutatását tartalmazza.
- Az AppArmor problémák felvetésére, és az Ubuntu kiszolgáló közösség életébe való bekapcsolódásra remek hely a freenode[15] #ubuntu-server IRC-csatornája.

5. Tanúsítványok

Napjainkban a titkosítás egyik legnépszerűbb formája a nyilvános kulcsú titkosítás. A nyilvános kulcsú titkosítás egy nyilvános kulcsot és egy személyes kulcsot használ. A rendszer működésének alapja az információk titkosítása a nyilvános kulccsal. Az információk ezután csak a személyes kulccsal fejthetők vissza.

A nyilvános kulcsú titkosítás általánosan elterjedt alkalmazások forgalmának titkosítására SSL vagy TLS kapcsolat segítségével. Az Apache beállítható például a HTTPS, az SSL feletti HTTP biztosítására. Ez lehetővé teszi az olyan protokollon folyó forgalom titkosítását, amely maga nem biztosít titkosítást.

A tanúsítvány egy nyilvános kulcs és a kiszolgálóval, valamint az azért felelős szervezettel kapcsolatos egyéb információk terjesztésére használt módszer. A tanúsítványokat digitálisan aláírhatják a hitelesítésszolgáltatók (CA). A CA egy megbízható harmadik fél, aki meggyőződött a tanúsítványban szereplő információk pontosságáról.

5.1. Tanúsítványok típusai

Biztonságos kiszolgáló nyilvános kulcsú titkosítás használatára való beállításához a legtöbb esetben el kell küldenie a hitelesítési kérést (a nyilvános kulccsal együtt), a cég azonosságának bizonyítékát, valamint a CA díjazását. A CA ellenőrzi a hitelesítési kérést és az azonosságot, majd visszaküldi a biztonságos kiszolgálóhoz használható tanúsítványt. Ennek alternatívájaként létrehozhat önaláírású tanúsítványt is.

Ne feledje, hogy az önaláírású tanúsítványokat nem szabad éles környezetben használni.

A HTTPS példát folytatva a CA által aláírt tanúsítvány két fontos képességet biztosít az önaláírású tanúsítványokkal szemben:

- A böngészők (általában) automatikusan felismerik a tanúsítványt, és lehetővé teszik a biztonságos kapcsolat létrehozását a felhasználó megkérdezése nélkül.
- Amikor egy CA aláírt tanúsítványt ad ki, garantálja a böngésző számára weboldalakat biztosító szervezet azonosságát.

A legtöbb SSL-t támogató webböngésző és számítógép rendelkezik a CA-k listájával, amelyek tanúsítványait automatikusan elfogadja. Ha a böngésző olyan tanúsítványt észlelt, amely jóváhagyó CA-ja nincs a listában, akkor a böngésző megkérdezi a felhasználót a kapcsolat elfogadásáról vagy visszautasításáról. Más alkalmazások hibaüzenetet adhatnak önaláírású tanúsítvány használatakor.

A CA-tól tanúsítvány beszerzésének folyamata viszonylag egyszerű. A teendők listája röviden:

1. Hozzon létre egy személyes és nyilvános titkosításikulcs-párt.
2. Hozzon létre egy tanúsítványigénylést a nyilvános kulcs alapján. A tanúsítványigénylés a kiszolgálóról és az azt működtető cégről tartalmaz információkat.

3. Küldje el a tanúsítványigénylést a személyazonosságát igazoló dokumentumokkal egy CA-nak. Nem tehetünk javaslatokat, hogy melyiket válassza. Döntését korábbi tapasztalataira, vagy barátai és kollégái tapasztalataira, vagy pusztán pénzügyi tényezőkre is alapozhatja.

   Miután kiválasztotta a CA-t, kövesse az általuk adott utasításokat a tanúsítvány megszerzéséhez.
4. Miután a CA meggyőződött arról, hogy Ön valóban az, akinek mondja magát, elküldi a digitális tanúsítványt.
5. Telepítse a tanúsítványt a biztonságos kiszolgálóra, és állítsa be a megfelelő alkalmazásokat annak használatára.

5.2. Tanúsítvány-aláírási kérés (CSR) előállítása

Akár egy CA-tól szerzi be a tanúsítványt, akár önaláírt tanúsítványt akar használni, az első lépés a kulcs előállítása.

Ha a tanúsítványt szolgáltatásdémonok fogják használni, mint például az Apache, Postfix, Dovecot stb., akkor a jelmondat nélküli kulcs sok esetben megfelelő. A jelmondat hiánya lehetővé teszi a szolgáltatások emberi beavatkozás nélküli elindítását, ez általában a démonok elvárt indítási módja.

Ez a szakasz ismerteti egy jelmondattal rendelkező, és egy azzal nem rendelkező kulcs előállítását. A jelmondat nélküli kulcs ezután szolgáltatásdémonok által használt tanúsítvány előállításához lesz felhasználva.

A biztonságos szolgáltatás jelmondat nélküli futtatása kényelmes, mert nem igényli a jelmondat megadását a szolgáltatás minden egyes elindításakor. Ugyanakkor nem biztonságos, és a kulcs veszélybe kerülése a kiszolgáló veszélybe kerülését is jelenti.

A tanúsítvány-aláírási kéréshez használandó kulcsok előállításához adja ki a következő parancsot:

```
openssl genrsa -des3 -out server.key 1024
```

```
Generating RSA private key, 1024 bit long modulus
.....................++++++
.................++++++
unable to write 'random state'
e is 65537 (0x10001)
Enter pass phrase for server.key:
```

Ezután adja meg a jelmondatot. A nagyobb biztonság érdekében legalább nyolc karakterből kell állnia. A -des3 megadásakor a minimális hossz négy karakter. Tartalmaznia kell számokat és/vagy írásjeleket, és nem lehet szótári szó. Ne feledje, hogy a jelmondat megkülönbözteti a kis- és nagybetűket.

Ellenőrzési célból írja be újra a jelmondatot. A sikeres ismételt megadás után elkészül a kiszolgálókulcs, és a `server.key` fájlba kerül mentésre.

Hozza létre a nem biztonságos, jelmondat nélküli kulcsot, és keverje meg a kulcsneveket:

```
openssl rsa -in server.key -out server.key.insecure
mv server.key server.key.secure
mv server.key.insecure server.key
```

A nem biztonságos kulcs neve most `server.key`, és segítségével előállíthatja a jelmondat nélküli CSR-t.

A CSR előállításához adja ki a következő parancsot:

```
openssl req -new -key server.key -out server.csr
```

A parancs bekéri a jelmondatot. A helyes jelmondat megadása után bekéri a cégnevet, az oldal címét, e-mail azonosítót stb. A részletes adatok megadása után elkészül a CSR, és a `server.csr` fájlba kerül mentésre.

Ezután ezt a CSR fájlt elküldheti feldolgozásra egy CA-nak. A CA a CSR fájlt fogja használni, és kiadja a tanúsítványt. Másrészt, ezen CSR segítségével létrehozhat önaláírású tanúsítványt is.

5.3. Önaláírású tanúsítvány létrehozása

Az önaláírású tanúsítvány létrehozásához adja ki a következő parancsot:

```
openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.crt
```

A fenti parancs bekéri a jelmondatot. A helyes jelmondat megadása után létrejön a tanúsítvány, és a `server.crt` fájlba kerül mentésre.

Ha kiszolgálóját éles környezetben szeretné használni, akkor egy CA által aláírt tanúsítványra lesz szüksége. Az önaláírású tanúsítványok használata nem javasolt.

5.4. A tanúsítvány telepítése

A következő parancsok kiadásával telepítheti a `server.key` kulcsfájlt és a `server.crt` tanúsítványfájlt, vagy a CA által kiadott tanúsítványfájlt:

```
sudo cp server.crt /etc/ssl/certs
sudo cp server.key /etc/ssl/private
```

Ezután egyszerűen állítsa be a nyilvános kulcsú titkosítást használni képes alkalmazásokat a tanúsítvány és kulcs fájlok használatára. Segítségükkel az Apache például a HTTPS, a Dovecot IMAPS és POP3S szolgáltatásokat nyújthatja.

5.5. Hitelesítésszolgáltató

Ha hálózatán a szolgáltatások néhány önaláírású tanúsítványnál többet igényelnek, érdemes lehet saját belső hitelesítésszolgáltatót (CA) készíteni. A saját CA által aláírt tanúsítványok használata lehetővé

teszi, hogy a tanúsítványokat használó különböző szolgáltatások megbízzanak az azonos CA által kibocsátott tanúsítványokat használó szolgáltatásokban.

1. Első lépésként hozza létre a CA tanúsítványát tartalmazó könyvtárakat és a kapcsolódó fájlokat:

```
sudo mkdir /etc/ssl/CA
sudo mkdir /etc/ssl/newcerts
```

2. A CA működéséhez néhány további fájl is szükséges, egy a CA által utoljára használt sorozatszám tárolására, mivel minden tanúsítványnak egyedi sorozatszámot kell használnia, és egy másik a kibocsátott tanúsítványok rögzítésére:

```
sudo sh -c "echo '01' > /etc/ssl/CA/serial"
sudo touch /etc/ssl/CA/index.txt
```

3. A harmadik fájl a CA beállítófájlja. Noha nem feltétlenül szükséges, több tanúsítvány kibocsátásakor nagyon kényelmes. Szerkessze az `/etc/ssl/openssl.cnf` fájlt, és a [CA_default] szakaszban módosítsa a következőket:

```
dir             = /etc/ssl/             # Where everything is kept
database        = $dir/CA/index.txt     # database index file.
certificate     = $dir/certs/cacert.pem # The CA certificate
serial          = $dir/CA/serial        # The current serial number
private_key     = $dir/private/cakey.pem# The private key
```

4. Ezután hozza létre az önaláírt gyökértanúsítványt:

```
openssl req -new -x509 -extensions v3_ca -keyout cakey.pem -out cacert.pem -days 3650
```

   A program bekéri a tanúsítvány részleteit.

5. Ezután telepítse a gyökértanúsítványt és a kulcsot:

```
sudo mv cakey.pem /etc/ssl/private/
sudo mv cacert.pem /etc/ssl/certs/
```

6. Most már készen áll tanúsítványok aláírására. Első lépésként egy tanúsítvány-aláírási kérésre (CSR) lesz szükség, a részletekért lásd: 5.2. szakasz - Tanúsítvány-aláírási kérés (CSR) előállítása [126]. A CSR beszerzése után adja ki a következő parancsot a CA által aláírt tanúsítvány kiadásához:

```
sudo openssl ca -in server.csr -config /etc/ssl/openssl.cnf
```

   A CA kulcs jelszavának megadása után a program megkéri a tanúsítvány aláírására, majd az új tanúsítvány véglegesítésére. Ezután nagyobb mennyiségű információ jelenik meg a tanúsítvány létrehozásával kapcsolatban.

7. There should now be a new file, `/etc/ssl/newcerts/01.pem`, containing the same output. Copy and paste everything between the -----BEGIN CERTIFICATE----- and ----END

CERTIFICATE----- lines to a file named after the hostname of the server where the certificate will be installed. For example `mail.example.com.crt`, is a nice descriptive name.

Az ezt követő tanúsítványok neve `02.pem`, `03.pem` stb. lesz.

A `levelezes.pelda.hu.crt` helyett használjon saját beszédes nevet.

8. Végül másolja át az új tanúsítványt az azt igénylő gépre, és állítsa be a megfelelő alkalmazásokat annak használatára. A tanúsítványok telepítésének alapértelmezett helye az `/etc/ssl/certs`. Ez túlbonyolított fájljogosultságok használata nélkül több szolgáltatás számára is lehetővé teszi ugyanazon tanúsítvány használatát.

   A CA tanúsítvány használatára beállítható alkalmazásokhoz át kell másolnia az `/etc/ssl/certs/cacert.pem` fájlt az egyes kiszolgálók `/etc/ssl/certs/` könyvtárába.

5.6. Hivatkozások

- A titkosítás használatával kapcsolatos részletesebb utasításokért lásd a tlpd.org SSL Certificates HOWTO[16] leírását.
- A PKI oldal[17] tartalmazza a hitelesítésszolgáltatók listáját.
- A Wikipédia HTTPS[18] oldala további információkat tartalmaz a HTTPS-ről.
- Az OpenSSL-lel kapcsolatos további információkért lásd az OpenSSL honlapját[19].
- Az O'Reilly Network Security with OpenSSL[20] könyve is remek referencia.

6. eCryptfs

Az eCryptfs egy POSIX-kompatibilis vállalati szintű titkosított fájlrendszer Linuxra. A fájlrendszer réteg fölött elhelyezkedő eCryptfs az alapul szolgáló fájlrendszertől, partíciótípustól, stb. függetlenül védi a fájlokat.

A telepítés során lehetőség van a `/home` partíció titkosítására. Ez automatikusan beállít mindent a partíció titkosításához és csatolásához.

Ez a szakasz példaként a `/srv` beállítását mutatja be az eCryptfssel való titkosításra.

6.1. Az eCryptfs használata

Első lépésként telepítse a szükséges csomagokat. Adja ki a következő parancsot:

```
sudo apt-get install ecryptfs-utils
```

Csatolja a titkosítandó partíciót:

```
sudo mount -t ecryptfs /srv /srv
```

Ezután a program bekér néhány részletet az adatok eCryptfssel való titkosításához.

Annak teszteléséhez, hogy a `/srv` alatti fájlok tényleg titkosítva vannak, másolja az `/etc/default` mappát a `/srv` alá:

```
sudo cp -r /etc/default /srv
```

Válassza le az `/srv` kötetet, és próbáljon megnézni egy fájlt:

```
sudo umount /srv
cat /srv/default/cron
```

A `/srv` újracsatolása az ecryptfs használatával újra láthatóvá teszi az adatokat.

6.2. Titkosított partíciók automatikus csatolása

Számos lehetőség van az eCryptfssel titkosított fájlrendszerek automatikus csatolására. Ez a példa egy csatolási beállításokat tartalmazó `/root/.ecryptfsrc` fájlt, valamint egy USB-kulcson található jelszófájlt fog használni.

Kezdésként hozza létre a `/root/.ecryptfsrc` fájlt a következő tartalommal:

```
key=passphrase:passphrase_passwd_file=/mnt/usb/jelszófájl.txt
ecryptfs_sig=5826dd62cf81c615
```

```
ecryptfs_cipher=aes
ecryptfs_key_bytes=16
ecryptfs_passthrough=n
ecryptfs_enable_filename_crypto=n
```

Módosítsa az ecryptfs_sig értékét a `/root/.ecryptfs/sig-cache.txt` fájlban lévő aláírásra.

Ezután hozza létre a `/mnt/usb/jelszófájl.txt` jelszófájlt:

```
passphrase_passwd=[titok]
```

Most vegye fel a szükséges sorokat az `/etc/fstab` fájlba:

```
/dev/sdb1       /mnt/usb        ext3    ro      0 0
/srv /srv ecryptfs defaults 0 0
```

Győződjön meg róla, hogy az USB-kulcs a titkosított partíció előtt kerül csatolásra.

Végül indítsa újra a számítógépet, ekkor a `/srv` csatolásra kerül az eCryptfs használatával.

6.3. Egyéb segédprogramok

Az ecryptfs-utils csomag több más hasznos segédprogramot tartalmaz:

- ecryptfs-setup-private: létrehoz egy `~/Private` könyvtárat a titkosított információk tárolására. Ezt a segédprogramot nem csak rendszergazdák futtathatják, így a rendszer más felhasználói előtt titokban tarthatják adataikat.
- ecryptfs-mount-private és ecryptfs-umount-private: csatolja és leválasztja a felhasználó `~/Private` könyvtárát.
- ecryptfs-add-passphrase: új jelmondatot vesz fel a kernel kulcstartójára.
- ecryptfs-manager: kezeli az eCryptfs objektumokat, például a kulcsokat.
- ecryptfs-stat: lehetővé teszi egy fájl ecryptfs metainformációinak megjelenítését.

6.4. Hivatkozások

- Az eCryptfssel kapcsolatos további információkért lásd a Launchpad projektoldalt[21].
- A Linux Journal[22] egyik cikke bemutatja az eCryptfst.
- Az ecryptfs további lehetőségeiért lásd az ecryptfs kézikönyvoldalát[23].
- Az Ubuntu wiki eCryptfs[24] oldala szintén tartalmaz további részleteket.

9. fejezet - Monitorozás

1. Áttekintés

Az alapvető kiszolgálók és szolgáltatások monitorozása a rendszeradminisztráció fontos része. A legtöbb hálózati szolgáltatásnak a teljesítményét, rendelkezésreállását vagy mindkettőt szokás monitorozni. Ez a szakasz a rendelkezésreállás monitorozására használható Nagios, és a teljesítmény monitorozására használt Munin telepítését és beállítását ismerteti.

A szakasz példái két kiszolgálót (kiszolgáló01 és kiszolgáló02) használnak. A kiszolgáló01 a Nagios segítségével fogja a rajta és a kiszolgáló02-n futó szolgáltatásokat monitorozni. A kiszolgáló01 a munin csomagot is használni fogja a hálózattal kapcsolatos információk gyűjtésére. A munin-node csomag segítségével a kiszolgáló02 az információk a kiszolgáló01-nek való visszaküldésére lesz beállítva.

Reményeink szerint ezen egyszerű példák alapján képes lesz a hálózatának további kiszolgálói és szolgáltatásai monitorozására.

2. Nagios

2.1. Telepítés

Az első lépés a kiszolgáló01 gépen a nagios csomag telepítése. Adja ki a következő parancsot:

```
sudo apt-get install nagios3 nagios-nrpe-plugin
```

A rendszer bekéri a nagiosadmin felhasználó jelszavát. A felhasználó hitelesítési adatai az `/etc/nagios3/htpasswd.users` fájlban találhatók. A nagiosadmin jelszavának módosításához, vagy további felhasználók a Nagios CGI parancsfájlokhoz adásához használja az apache2-utils csomag részét képező htpasswd segédprogramot.

A nagiosadmin felhasználó jelszavának módosításához például adja ki a következő parancsot:

```
sudo htpasswd /etc/nagios3/htpasswd.users nagiosadmin
```

Felhasználó felvételéhez:

```
sudo htpasswd /etc/nagios3/htpasswd.users geza
```

A második lépés a kiszolgáló02 kiszolgálón a nagios-nrpe-server csomag telepítése. A kiszolgáló02-n adja ki a következő parancsot:

```
sudo apt-get install nagios-nrpe-server
```

Az NRPE lehetővé teszi távoli gépek helyi ellenőrzéseinek futtatását. Ezt, illetve egyéb ellenőrzéseket más Nagios bővítményeken keresztül is végre lehet hajtani.

2.2. Konfiguráció áttekintése

Számos könyvtár tartalmaz Nagios konfigurációs és ellenőrzőfájlokat.

- `/etc/nagios3`: a nagios démon, CGI fájlok, gépek stb. működésére vonatkozó beállítófájlokat tartalmaz.
- `/etc/nagios-plugins`: a szolgáltatás-ellenőrzések konfigurációs fájljait tartalmazza.
- `/etc/nagios`: a távoli gépen a nagios-nrpe-server konfigurációs fájljait tartalmazza.
- `/usr/lib/nagios/plugins/`: az ellenőrző binárisok tárolási helye. Az ellenőrzés minden kapcsolójának megjelenítéséhez használja a -h kapcsolót.

  Például: /usr/lib/nagios/plugins/check_dhcp -h

A Nagios rengeteg ellenőrzés végrehajtására állítható be bármely kiszolgálón. Ebben a példában a Nagios a lemezterület, DNS és egy MySQL-gépcsoport ellenőrzésére lesz beállítva. A DNS-

ellenőrzés a kiszolgáló02 gépen történik, a MySQL-gépcsoportnak pedig a kiszolgáló01 és a kiszolgáló02 is tagja.

Az Apache beállításával kapcsolatban lásd: 1. szakasz - HTTPD – Apache2 webkiszolgáló [141], a DNS-sel kapcsolatban: 7. fejezet - Tartománynév-szolgáltatás (DNS) [94], a MySQL-lel kapcsolatban: 1. szakasz - MySQL [160].

Ezen kívül van néhány kifejezés, amelyek megismerése egyszerűbbé teszi a Nagios beállításának megértését:

- Gép: a megfigyelt kiszolgáló, munkaállomás, hálózati eszköz stb.
- Gépcsoport: hasonló gépek csoportja. Csoportosítható például az összes webkiszolgáló, fájlkiszolgáló stb.
- Szolgáltatás: a gépen monitorozott szolgáltatás, például: HTTP, DNS, NFS stb.
- Szolgáltatáscsoport: lehetővé teszi több szolgáltatás csoportosítását. Ez például több HTTP csoportosításakor hasznos.
- Kapcsolattartó: esemény bekövetkezésekor értesítendő személy. A Nagios beállítható e-mailek, SMS-üzenetek stb. küldésére.

Alapértelmezésben a Nagios a HTTP, lemezhely, SSH, aktuális felhasználók, folyamatok és a localhost terhelésének ellenőrzésére van beállítva. A Nagios pingeléssel ellenőrzi az átjárót.

A nagy Nagios telepítések beállítása meglehetősen bonyolult lehet. Általában legjobb kicsiben kezdeni, egy vagy két géppel, igényeinek megfelelően beállítani ezeket, majd bővíteni.

2.3. Beállítás

- 1. Első lépésként hozzon létre egy gépkonfigurációs fájlt a kiszolgáló02 számára. Adja ki a következő parancsot:

```
sudo cp /etc/nagios3/conf.d/localhost_nagios2.cfg /etc/nagios3/conf.d/kiszolgáló02.cfg
```

A fenti és alábbi példaparancsokban a kiszolgáló01, kiszolgáló02, 172.18.100.100 és 172.18.100.101 helyére saját kiszolgálóinak gépneveit és IP-címeit írja.

2. Ezután szerkessze az `/etc/nagios3/conf.d/kiszolgáló02.cfg` fájlt:

```
define host{
        use                     generic-host            ; Name of host template to use
        host_name               kiszolgáló02
        alias                   Kiszolgáló 02
        address                 172.18.100.101
}

# check DNS service.
define service {
        use                             generic-service
```

```
        host_name                       server02
        service_description             DNS
        check_command                   check_dns!172.18.100.101
}
```

3. Indítsa újra a nagios démont az új beállítások életbe léptetéséhez:

```
sudo /etc/init.d/nagios3 restart
```

- 1. Ezután vegyen fel egy szolgáltatásdefiníciót a MySQL ellenőrzéshez a következők hozzáadásával az `/etc/nagios3/conf.d/services_nagios2.cfg` fájlhoz:

```
# check MySQL servers.
define service {
        hostgroup_name                  mysql-servers
        service_description             MySQL
        check_command                   check_mysql_cmdlinecred!nagios!secret!$HOSTADDRESS
        use                             generic-service
        notification_interval           0 ; set > 0 if you want to be renotified
}
```

2. Most definiálni kell a mysql-servers gépcsoportot. Szerkessze az `/etc/nagios3/conf.d/hostgroups_nagios2.cfg` fájlt, és adja hozzá a következőket:

```
# MySQL hostgroup.
define hostgroup {
        hostgroup_name  mysql-servers
                alias           MySQL-kiszolgálók
                members         localhost, kiszolgáló02
        }
```

3. A Nagios ellenőrzésnek hitelesítenie kell magát a MySQL felé. Adja ki a következő parancsot a nagios felhasználó létrehozásához a MySQL adatbázisban:

```
mysql -u root -p -e "create user nagios identified by 'secret';"
```

A nagios felhasználót létre kell hozni a mysql-servers gépcsoport minden gépén.

4. Indítsa újra a nagiost a MySQL kiszolgálók ellenőrzésének megkezdéséhez.

```
sudo /etc/init.d/nagios3 restart
```

- 1. Végül állítsa be az NRPE-t a lemezterület ellenőrzésére a kiszolgáló02 gépen.

A kiszolgáló01 gépen adja hozzá a szolgáltatás-ellenőrzést az `/etc/nagios3/conf.d/kiszolgáló02.cfg` fájlhoz:

```
# NRPE disk check.
define service {
```

```
        use                             generic-service
        host_name                       kiszolgáló02
        service_description             nrpe-disk
        check_command                   check_nrpe_1arg!check_all_disks!172.18.100.101
}
```

2. Ezután a kiszolgáló02 gépen szerkessze az `/etc/nagios/nrpe.cfg` fájlt, és módosítsa:

   ```
   allowed_hosts=172.18.100.100
   ```

   A lentebbi parancsdefiníciós területhez adja hozzá a következőt:

   ```
   command[check_all_disks]=/usr/lib/nagios/plugins/check_disk -w 20% -c 10% -e
   ```

3. Végül indítsa újra a nagios-nrpe-server démont:

   ```
   sudo /etc/init.d/nagios-nrpe-server restart
   ```

4. A kiszolgáló01 gépen újra kell indítani a nagiost:

   ```
   sudo /etc/init.d/nagios3 restart
   ```

Ezután látnia kell a gép- és szolgáltatás-ellenőrzéseket a Nagios CGI-fájljaiban. Ezek eléréséhez nyissa meg a böngészőben a http://kiszolgáló01/nagios3 címet. Ez bekéri a nagiosadmin felhasználó nevét és jelszavát.

2.4. Hivatkozások

Ez a szakasz csak karcolta a Nagios szolgáltatásainak felszínét. A nagios-plugins-extra és nagios-snmp-plugins csomagok sok további szolgáltatás-ellenőrzést is tartalmaznak.

- További információkért lásd a Nagios[1] weboldalát.
- Ezen belül is az online dokumentációs[2] oldalt.
- A Nagiosról és hálózatmonitorozásról számos könyv[3] is készült.
- Az Ubuntu wiki Nagios[4] oldala is tartalmaz további részleteket.

3. Munin

3.1. Telepítés

A Munin a kiszolgáló01 gépre telepítése előtt az apache2 telepítése is szükséges. Az alapértelmezett beállítások megfelelők munin kiszolgáló futtatásához. További információkért lásd: 1. szakasz - HTTPD – Apache2 webkiszolgáló [141].

Első lépésként telepítse a kiszolgáló01 gépre a munin csomagot. Adja ki a következő parancsot:

```
sudo apt-get install munin
```

A kiszolgáló02 gépre telepítse a munin-node csomagot:

```
sudo apt-get install munin-node
```

3.2. Beállítás

A kiszolgáló01 gépen szerkessze az `/etc/munin/munin.conf` fájlt, és vegye fel a kiszolgáló02 IP-címét:

```
## Elsőként a „normál” gép.
[kiszolgáló02]
       address 172.18.100.101
```

A kiszolgáló02 és 172.18.100.101 helyére a kiszolgáló tényleges gépnevét és IP-címét írja.

Ezután állítsa be a munin-node csomagot a kiszolgáló02 gépen. Szerkessze az `/etc/munin/munin-node.conf` fájlt, és engedélyezze a kiszolgáló01 általi elérést:

```
allow ^172\.18\.100\.100$
```

A ^172\.18\.100\.100$ helyére a munin kiszolgálója tényleges IP-címét írja.

Indítsa újra a munin-node démont a kiszolgáló02 gépen az új beállítások életbe léptetéséhez:

```
sudo /etc/init.d/munin-node restart
```

Végül egy böngészőben nyissa meg a http://kiszolgáló01/munin címet, ekkor a lemezt, hálózatot, folyamatokat és rendszert monitorozó szabványos munin-bővítmények információit megjelenítő grafikonokra mutató hivatkozásokat kell látnia.

Mivel ez egy új telepítés, ezért eltelhet egy kis idő, amíg a grafikonok valami tényleg hasznosat kezdenek ábrázolni.

3.3. További bővítmények

A munin-plugins-extra csomag teljesítmény-ellenőrzéseket tartalmaz további szolgáltatásokhoz, mint például a DNS, DHCP, Samba stb. A csomag telepítéséhez adja ki a következő parancsot:

```
sudo apt-get install munin-plugins-extra
```

Ne feledje a csomagot egyaránt telepíteni a kiszolgáló és a csomópont gépekre is.

3.4. Hivatkozások

- További részletekért lásd a Munin[5] weboldalát.
- A Munin dokumentációs oldala[6] a további bővítményekkel, bővítmények írásával kapcsolatos információkat tartalmaz.
- Az Open Source Press német nyelvű könyve: Munin Graphisches Netzwerk- und System-Monitoring[7].
- További hasznos erőforrás az Ubuntu wiki Munin[8] oldala.

10. fejezet - Webkiszolgálók

A webkiszolgáló program képes HTTP kéréseket fogadni a webböngészőként ismert kliensektől, és kiszolgálni a HTTP kéréseket tetszőleges adattartalommal, amelyek rendszerint weboldalak, például HTML-dokumentumok és hivatkozott objektumok (képek stb.).

1. HTTPD – Apache2 webkiszolgáló

Az Apache a Linux rendszereken legszélesebb körben használt webkiszolgáló. A webkiszolgálók a kliensszámítógépek által kért weboldalak kiszolgálását végzik. A kliensek általában webböngésző alkalmazások, mint például a Firefox, Opera, vagy Mozilla használatával kérik le és jelenítik meg a weboldalakat.

A felhasználók az URL megadásával irányíthatják a böngészőt a webkiszolgálóra, a teljes képzésű tartománynév (FQDN) és a kért erőforrás útvonalának segítségével. Az Ubuntu weboldalának[1] megnyitásához a felhasználónak csak az FQDN-t kell megadnia. A kereskedelmi támogatással[2] kapcsolatos információk megjelenítéséhez a felhasználónak az FQDN mellett egy útvonalat is meg kell adnia.

A weboldalak átvitelére használt legáltalánosabb protokoll a HTTP. Ezen kívül további protokollok is támogatottak, például a HTTPS és az FTP.

Az Apache webkiszolgálót gyakran a MySQL adatbázismotorral, a PHP parancsnyelvvel és más népszerű parancsnyelvekkel, mint a Python és Perl együtt használják. Ezt az összeállítást LAMP-nak (Linux, Apache, MySQL és Perl/Python/PHP) nevezik, és hatékony és megbízható környezetet biztosít webalkalmazások fejlesztéséhez és telepítéséhez.

1.1. Telepítés

Az Apache2 webkiszolgáló elérhető Ubuntu Linux alatt. Az Apache2 telepítéséhez:

- A terminálban adja ki a következő parancsot:

```
sudo apt-get install apache2
```

1.2. Beállítás

Az Apache2 beállítása egyszerű szöveges beállítófájlokban elhelyezett direktívákkal történik. A beállítások a következő fájlokba és könyvtárakba vannak szétosztva:

- apache2.conf: az elsődleges Apache2 beállítófájl. Az Apache2 globális beállításait tartalmazza.
- conf.d: az Apache2-re globálisan érvényes beállítófájlokat tartalmazza. Az Apache2-t tartalom kiszolgálására használó egyéb csomagok ebbe a könyvtárba fájlokat vagy szimbolikus linkeket helyezhetnek el.
- envvars: az Apache2 környezeti változói ebben a fájlban kerülnek beállításra.
- httpd.conf: történetileg az elsődleges Apache2 beállítófájl, amelyet a httpd démonról neveztek el. Ez a fájl felhasználóspecifikus beállításokat tartalmazhat, amelyek globálisan befolyásolják az Apache2-t.

[1] http://www.ubuntu.com

[2] http://www.ubuntu.com/support/paid

- mods-available: ez a könyvtár a modulok betöltésére és beállítására szolgáló beállítófájlokat tartalmaz. Nem minden modulhoz tartoznak beállítófájlok.
- mods-enabled: szimbolikus linkeket tartalmaz az `/etc/apache2/mods-available` fájljaira. A modul beállítófájljára mutató szimbolikus link létrehozása után az adott modul bekapcsolásra kerül az apache2 következő újraindításakor.
- ports.conf: az Apache2 által figyelt TCP portokat meghatározó direktívákat tartalmazza.
- sites-available: ez a könyvtár az Apache2 virtuális kiszolgálóinak beállítófájljait tartalmazza. A virtuális kiszolgálók lehetővé teszik az Apache2 beállítását több, eltérő beállításokkal rendelkező webhely kiszolgálására.
- sites-enabled: a mods-enabled mintájára a `sites-enabled` szimbolikus linkeket tartalmaz az `/etc/apache2/sites-available` könyvtárra. Miután a sites-available egyik fájljára létrejön a szimbolikus link, az Apache2 újraindítása után az adott webhely engedélyezésre kerül.

Ezeken kívül további beállítófájlok is felvehetők az Include direktíva használatával, ebben helyettesítő karakterek is használhatók több beállítófájl felvételére. A beállítófájlok bármelyikébe bármely direktíva elhelyezhető. Az elsődleges beállítófájl módosításai csak az Apache2 elindításakor vagy újraindításakor lépnek életbe.

A kiszolgáló beolvassa a MIME-dokumentumtípusokat tartalmazó fájlt is, ennek nevét a TypesConfig direktíva adja meg és alapértelmezésben az `/etc/mime.types`.

1.2.1. Alapbeállítások

Ez a szakasz ismerteti az Apache2 kiszolgáló alapvető beállítási lehetőségeit. További részletekért lásd az Apache2 dokumentációját[3].

- Az Apache2 virtuális kiszolgálókra szabott alapértelmezett beállításokat tartalmaz. Ez azt jelenti, hogy egyetlen alapértelmezett virtuális kiszolgálóval van beállítva (a VirtualHost direktíva használatával). Ez módosítva vagy változatlanul hagyva is használható egyetlen oldal kiszolgálására, vagy ha több webhelye van, akkor használható további virtuális kiszolgálók sablonjaként. Ha nem módosítja, akkor az alapértelmezett virtuális kiszolgáló fog alapértelmezett webhelyként szolgálni, illetve a webhely felhasználói azt fogják látni, hogy az általuk megadott URL nem illeszkedik egyik webhely ServerName direktívájára sem. Az alapértelmezett virtuális kiszolgáló módosításához szerkessze az `/etc/apache2/sites-available/default` fájlt.

  

  Egy adott virtuális kiszolgálóra beállított direktívák csak az adott virtuális kiszolgálóra érvényesek. Ha egy direktíva meg van adva kiszolgálószinten, de a virtuális kiszolgáló beállításai közt nincs, akkor az alapértelmezett beállítás kerül felhasználásra. Megadhat például egy webmesteri e-mail címet, ekkor elhagyhatja ennek megadását az egyes virtuális kiszolgálókhoz.

  Ha új virtuális kiszolgálót vagy webhelyet szeretne beállítani, másolja ezt a fájlt ugyanebbe a könyvtárba tetszőleges néven. Például:

[3] http://httpd.apache.org/docs/2.2/

```
sudo cp /etc/apache2/sites-available/default /etc/apache2/sites-available/újoldal
```

Szerkessze az új fájlt az új webhely beállításához az alább leírt direktívák segítségével.

- A ServerAdmin direktíva megadja a kiszolgáló rendszergazdájaként közzétenni kívánt e-mail címet. Az alapértelmezett érték a webmaster@localhost. Ezt egy Önnek kézbesített e-mail címre kell cserélnie (ha Ön a kiszolgáló rendszergazdája). Ha a weboldalon probléma lép fel, az Apache2 megjelenít egy hibaüzenetet, amely ezt a címet adja meg a hiba bejelentéséhez. Ez a direktíva az /etc/apache2/sites-available alatti beállítófájljában található meg.
- A Listen direktíva megadja azt a portot és opcionálisan IP-címet, amelyen az Apache2-nek figyelnie kell a kéréseket. Ha az IP-cím nincs megadva, akkor az Apache2 a géphez rendelt minden IP-címen figyelni fog. A Listen direktíva alapértelmezett értéke a 80. Ha ezt 127.0.0.1:80 értékre állítja, az Apache2 csak a visszacsatolási felületen fog figyelni, és nem lesz elérhető az interneten, vagy 81-re állítva a figyelt port módosítható, vagy a normál működéshez hagyja változatlanul. Ez a direktíva az `/etc/apache2/ports.conf` fájlban található.
- A ServerName direktíva elhagyható és megadja, hogy a webhely mely FQDN-re válaszoljon. Az alapértelmezett virtuális kiszolgálóhoz nincs megadva a ServerName direktíva, így minden kérésre válaszol, amely nem illeszkedik egy másik virtuális kiszolgálón beállított ServerName direktívára. Ha például most szerezte meg az ubunturocks.com tartománynevet, és az Ubuntu kiszolgálóján szeretné üzemeltetni, akkor a ServerName direktíva értékének a virtuális kiszolgáló beállítófájljában ubunturocks.com kell lennie. Vegye fel ezt a direktívát a korábban létrehozott virtuális kiszolgáló beállítófájljába (`/etc/apache2/sites-available/újoldal`).

  Hasznos lehet úgy beállítani az oldalt, hogy a www.ubunturocks.com névre is válaszoljon, mivel sok felhasználó feltételezi, hogy a www előtag szükséges. Erre a célra a ServerAlias direktíva használható. A ServerAlias direktívában helyettesítő karaktereket is használhat.

  A következő beállítás hatására például a webhely minden .ubunturocks.com végű tartománykérésre válaszolni fog.

  ```
  ServerAlias *.ubunturocks.com
  ```

- A DocumentRoot direktíva megadja, hogy az Apache2 hol keresse a webhelyet felépítő fájlokat. Az alapértelmezett érték a /var/www. Itt nincs beállítva semmilyen webhely, de az `/etc/apache2/apache2.conf` fájl RedirectMatch direktívájának engedélyezésével a kérések át lesznek irányítva a /var/www/apache2-default helyre, ahol az alapértelmezett Apache2 webhely várja. Módosítsa ezt az értéket a webhely virtuális kiszolgálójának beállítófájljában, és ha még nem létezik, hozza létre azt a könyvtárat.

Az /etc/apache2/sites-available könyvtárat nem dolgozza fel az Apache2. Az /etc/apache2/sites-enabled alatti szimbolikus linkek mutatnak az „elérhető” oldalakra.

Engedélyezze az új VirtualHostot az a2ensite segédprogram használatával, és indítsa újra az Apache2-t:

```
sudo a2ensite újoldal
sudo /etc/init.d/apache2 restart
```

Ne felejtsen el az újoldal helyett beszédesebb nevet adni a VirtualHostnak. Ennek egy módja, hogy a fájlt a virtuális kiszolgáló ServerName direktívája alapján nevezi el.

Hasonlóképpen az a2dissite segédprogrammal tilthatja le a webhelyeket. Ez a több virtuális kiszolgálót érintő beállítási hibák elhárításakor lehet hasznos.

```
sudo a2dissite újoldal
sudo /etc/init.d/apache2 restart
```

1.2.2. Alapértelmezett beállítások

Ez a szakasz ismerteti az Apache2 kiszolgáló alapértelmezett beállításait. Virtuális kiszolgáló felvételekor például az ahhoz megadott beállítások élveznek elsőbbséget. A virtuális kiszolgáló beállításaiban meg nem adott direktívák esetén az alapértelmezett értékek kerülnek felhasználásra.

- A DirectoryIndex direktíva jelöli a kiszolgáló által alapértelmezésben kiszolgált oldalt, amikor a felhasználó a könyvtár indexét kéri le a könyvtárnév végén megadott / jellel.

  Ha például a felhasználó lekéri a http://www.példa.hu/példa_könyvtár/ címet, akkor vagy a DirectoryIndex oldalt kapja (ha az létezik), vagy ha meg van adva az Indexes beállítás, akkor a kiszolgáló által generált könyvtártartalmat, egyébként pedig a „hozzáférés megtagadva” oldalt. A kiszolgáló megpróbálja megkeresni a DirectoryIndex direktívában megadott fájlokat, és visszaadja az elsőként megtaláltat. Ha nem találja egyiket sem, és a könyvtárhoz meg van adva az Options Indexes direktíva, akkor a kiszolgáló HTML formátumba előállítja és visszaadja a könyvtár által tartalmazott könyvtárak és fájlok listáját. Az `/etc/apache2/mods-available/dir.conf` fájlban található alapértelmezett érték az „index.html index.cgi index.pl index.php index.xhtml index.htm”. Ha az Apache2 a lekért könyvtárban talál ilyen nevű fájlokat, akkor megjeleníti az elsőt.
- Az ErrorDocument direktíva lehetővé teszi az Apache2-nek adott hibaesemények ellenőrzését. Ha például a felhasználó nem létező erőforrást kér, 404-es hiba történik, és az Apache2 alapértelmezett beállításai szerint a `/usr/share/apache2/error/HTTP_NOT_FOUND.html.var` fájl jelenik meg. Ez a fájl nincs a kiszolgáló DocumentRoot-jában, de egy Alias direktíva az `/etc/apache2/apache2.conf` fájlban átirányítja az /error könyvtárra vonatkozó kéréseket a `/usr/share/apache2/error/` könyvtárba.

  Az alapértelmezett ErrorDocument direktívák listájának megjelenítéséhez adja ki a következő parancsot:

  ```
  grep ErrorDocument /etc/apache2/apache2.conf
  ```
- Alapértelmezésben a kiszolgáló az átviteli naplót a `/var/log/apache2/access.log` fájlba írja. Ezt webhelyenként megváltoztathatja a virtuális kiszolgáló beállítófájljaiban a CustomLog direktíva segítségével, vagy az `/etc/apache2/apache2.conf` fájlban megadott alapértelmezett használatához ki is hagyhatja. Az ErrorLog direktíva használatával megadhatja azt a fájlt,

amelybe a hibák naplózásra kerülnek, az alapértelmezett érték a `/var/log/apache2/error.log`. Ezek az Apache2 kiszolgálóval kapcsolatos hibák elhárításának megkönnyítése érdekében az átviteli naplóktól külön tárolódnak. Megadhatja a LogLevel (az alapértelmezett érték a „warn”) és a LogFormat (az alapértelmezett érték az `/etc/apache2/apache2.conf` fájlban található) direktívákat is.

- Egyes beállítások a könyvtárak és nem a kiszolgálók szintjén adhatók meg. Az egyik ilyen direktíva az Options. A Directory kifejezések XML-szerű címkék között vannak, például:

```
<Directory /var/www/újoldal>
...
</Directory>
```

A Directory kifejezésen belüli Options direktíva (többek közt) a következő, szóközökkel elválasztott értékeket fogadja el:

- ExecCGI - Lehetővé teszi a CGI parancsfájlok futtatását. A CGI parancsfájlok nem kerülnek végrehajtásra, ha ez a beállítás nincs megadva.

A legtöbb fájlt nem szabad úgy végrehajtani, mint a CGI parancsfájlokat. Ez nagyon veszélyes lenne. A CGI parancsfájlokat a DocumentRoot direktívában megadott könyvtártól külön, és nem az alatt kell tartani, valamint csak ezt a könyvtárat szabad megadni az ExecCGI direktívában. Ez az alapértelmezés, és a CGI parancsfájlok alapértelmezett helye a `/usr/lib/cgi-bin`.

- Includes - Engedélyezi a kiszolgálóoldali beágyazásokat. A kiszolgálóoldali beágyazások lehetővé teszik a HTML fájloknak más fájlok beágyazását. Ez egy ritkán használt beállítás. További információkért lásd az Apache2 SSI HOWTO[4] leírást.
- IncludesNOEXEC - Engedélyezi a kiszolgálóoldali beágyazásokat, de letiltja az #exec és #include parancsokat a CGI parancsfájlokban.
- Indexes - Megjeleníti a könyvtár tartalmának formázott tartalmát, ha a kért könyvtárban nincs DirectoryIndex fájl (például index.html).

Biztonsági okból ezt általában nem szabad beállítani, a DocumentRoot könyvtárra pedig egyáltalán nem. Ezt a beállítást óvatosan engedélyezze könyvtárszinten, és csak akkor, ha biztosan azt szeretné, hogy a felhasználók lássák a könyvtár teljes tartalmát.

- Multiview - Tartalomegyeztetéses többszörös nézetek támogatása; ez a beállítás biztonsági okból alapértelmezésben ki van kapcsolva. Lásd az Apache2 dokumentációját erről a beállításról[5].
- SymLinksIfOwnerMatch - Csak akkor követi a szimbolikus linket, ha a célfájl vagy -könyvtár tulajdonosa megegyezik a link tulajdonosával.

1.2.3. A httpd beállításai

Ez a szakasz a httpd démon néhány alapvető beállítási lehetőségét ismerteti.

LockFile - A LockFile direktíva megadja a zárolási fájl útvonalát, ha a kiszolgálót a USE_FCNTL_SERIALIZED_ACCEPT vagy USE_FLOCK_SERIALIZED_ACCEPT egyikével

fordították. Ezt a helyi lemezen kell tárolni. Az alapértelmezett értéket meg kell hagyni, kivéve ha a naplókönyvtár egy NFS-megosztáson van. Ebben az esetben az alapértelmezett értéket meg kell változtatni a helyi lemezen lévő helyre, mégpedig egy csak a rendszergazda által olvasható könyvtárra.

PidFile - A PidFile direktíva megadja azt a fájlt, amelybe a kiszolgáló a folyamatazonosítóját (pid) rögzíti. Ezt a fájlt csak a rendszergazda olvashatja. a legtöbb esetben az alapértelmezett érték használandó.

User - A User direktíva beállítja a kiszolgáló által a kérések megválaszolására használt felhasználói azonosítót. Ez a beállítás megadja a kiszolgáló hozzáférési jogosultságát. Az ezen felhasználó által elérhető fájlok a webhely látogatói számára is elérhetők lesznek. Az alapértelmezett érték a www-data.

Hacsak nem tudja pontosan, mit csinál, ne állítsa a User direktíva értékét root-ra. A root használata User-ként hatalmas biztonsági lyukakat nyit a webkiszolgálóra.

A Group direktíva hasonló a User direktívához. A Group beállítja azt a csoportot, amely tagjaként a kiszolgáló megválaszolja a kéréseket. Az alapértelmezett csoport is a www-data.

1.2.4. Apache2 modulok

Az Apache2 egy moduláris kiszolgáló. Ez azt jelenti, hogy a kiszolgáló magja csak a legalapvetőbb szolgáltatásokat tartalmazza. A bővített szolgáltatások az Apache2-be tölthető modulokban érhetők el. Alapértelmezésben a kiszolgáló fordításkor tartalmaz egy alapértelmezett modulkészletet. Ha a kiszolgálót dinamikusan betöltött modulok használatára fordítják, akkor a modulok külön is lefordíthatók, és a LoadModule direktíva segítségével bármikor felvehetők. Ellenkező esetben az Apache2-t újra kell fordítani a modulok hozzáadásához vagy eltávolításához.

Az Ubuntu a dinamikus modulbetöltés támogatásával fordítja az Apache2-t. Az <IfModule> blokkban megadott konfigurációs direktívák engedélyezése egy adott modul jelenlétéhez köthető.

További Apache2 modulokat is telepíthet és használhat webkiszolgálóján. A következő parancs futtatásával például a MySQL hitelesítés modul telepíthető:

```
sudo apt-get install libapache2-mod-auth-mysql
```

További modulokért lásd az `/etc/apache2/mods-available` könyvtárat.

Modulok engedélyezéséhez használja az a2enmod segédprogramot:

```
sudo a2enmod auth_mysql
sudo /etc/init.d/apache2 restart
```

Hasonlóképpen az a2dismod segítségével letilthatók a modulok:

```
sudo a2dismod auth_mysql
sudo /etc/init.d/apache2 restart
```

1.3. A HTTPS beállítása

A mod_ssl modul fontos szolgáltatással bővíti az Apache2 kiszolgálót: a kommunikáció titkosításának lehetőségével. Amikor a böngésző SSL használatával kommunikál, a https:// előtag jelenik meg a böngésző címsorában, az URI elején.

A mod_ssl modul az apache2-common csomagban érhető el. A mod_ssl modul engedélyezéséhez adja ki a következő parancsot a terminálban:

```
sudo a2enmod ssl
```

Az alapértelmezett HTTPS beállítófájl az `/etc/apache2/sites-available/default-ssl`. Az Apache2 számára a HTTPS biztosításához egy tanúsítvány- és egy kulcsfájl is szükséges. Az alapértelmezett HTTPS beállítás az ssl-cert csomag által előállított tanúsítványt és kulcsot használja. Ezek tesztelési célra megfelelnek, de az automatikusan előállított tanúsítványt és kulcsot le kell cserélni a weboldalra vagy a kiszolgálóra kiadottakkal. A kulcs előállításával és tanúsítvány beszerzésével kapcsolatos információkért lásd a 5. szakasz - Tanúsítványok [125] szakaszt.

Adja ki a következőt az Apache2 beállításához a HTTPS használatára:

```
sudo a2ensite default-ssl
```

Az `/etc/ssl/certs` és `/etc/ssl/private` könyvtárak az alapértelmezett helyek. Ha a tanúsítványt és a kulcsot másik könyvtárba másolja, ne felejtse ennek megfelelően módosítani az SSLCertificateFile és SSLCertificateKeyFile direktívák értékeit.

Miután beállította az Apache2-t a HTTPS használatára, indítsa újra a szolgáltatást az új beállítások engedélyezéséhez:

```
sudo /etc/init.d/apache2 restart
```

A tanúsítvány beszerzésének módjától függően szükség lehet egy jelmondat megadására az Apache2 indításakor.

A biztonságos kiszolgálóoldalakat a https://webhely_címe/url/ böngészőcímsorba írásával érheti el.

1.4. Hivatkozások

- Az Apache2 dokumentációja[6] részletes információkat tartalmaz az Apache2 konfigurációs direktíváiról. A hivatalos Apache2 dokumentáció elérhető az apache2-doc csomagban is.
- Az SSL-lel kapcsolatos információkért lásd a Mod SSL dokumentációs[7] oldalát.
- Az O'Reilly Apache Cookbook[8] című könyve is hasznos információforrás bizonyos Apache2 beállítások elvégzéséhez.

- Az Ubuntuval kapcsolatos Apache2 kérdéseket felteheti a #ubuntu-server IRC-csatornán a freenode.net[9] hálózaton.
- A PHP és MySQL szokásos integrálása esetén az Ubuntu wiki Apache MySQL PHP[10] oldala szintén hasznos olvasmány.

2. PHP5 - parancsnyelv

A PHP egy általános célú parancsnyelv, amelyet webes fejlesztésekhez terveztek. A PHP parancsfájlok beágyazhatók HTML-be. Ez a szakasz ismerteti a PHP5 telepítését és beállítását Ubuntu rendszerekre Apache2 és MySQL mellé.

Ez a szakasz feltételezi, hogy telepítette és beállította az Apache2 webkiszolgálót és a MySQL adatbázis-kiszolgálót. Az Apache2 és MySQL telepítésével és beállításával kapcsolatban nézze meg ezen dokumentum Apache2 és MySQL szakaszait.

2.1. Telepítés

A PHP5 elérhető Ubuntu Linux alatt.

- A PHP5 telepítéséhez adja ki a következő parancsot a terminálban:

  ```
  sudo apt-get install php5 libapache2-mod-php5
  ```

  PHP5 parancsfájlokat a parancssorból is futtathat. A PHP5 parancsfájlok parancssori futtatásához telepítenie kell a php5-cli csomagot. A php5-cli telepítéséhez adja ki a következő parancsot a terminálban:

  ```
  sudo apt-get install php5-cli
  ```

  PHP5 parancsfájlokat a PHP5 Apache modul telepítése nélkül is végrehajthatja. Ehhez a php5-cgi csomagot kell telepítenie. A php5-cgi csomag telepítéséhez adja ki a következő parancsot a terminálban:

  ```
  sudo apt-get install php5-cgi
  ```

  A MySQL és a PHP5 együttes használatához telepítenie kell a php5-mysql csomagot. A php5-mysql telepítéséhez adja ki a következő parancsot a terminálban:

  ```
  sudo apt-get install php5-mysql
  ```

  Hasonlóképpen a PostgreSQL és a PHP5 együttes használatához telepítenie kell a php5-pgsql csomagot. A php5-pgsql telepítéséhez adja ki a következő parancsot a terminálban:

  ```
  sudo apt-get install php5-pgsql
  ```

2.2. Beállítás

A PHP5 telepítése után a webböngészőből futtathat PHP5 parancsfájlokat. Ha telepítette a php5-cli csomagot, akkor a PHP5 parancsfájlokat a parancssorból is futtathatja.

Alapértelmezésben az Apache2 webkiszolgáló a PHP5 parancsfájlok futtatására van beállítva. Más szóval, a PHP5 modul a telepítésekor automatikusan engedélyezésre kerül az Apache2 webkiszolgálón. Ellenőrizze, hogy az `/etc/apache2/mods-enabled/php5.conf` és `/etc/apache2/mods-enabled/php5.load` fájlok léteznek-e. Ha nem, akkor az a2enmod paranccsal engedélyezheti a modult.

A PHP5-tel kapcsolatos csomagok telepítése és a PHP5 Apache2 modul engedélyezése után újra kell indítania az Apache2 webkiszolgálót a PHP5 parancsfájlok futtatásához. A webkiszolgáló újraindításához adja ki a következő parancsot a terminálban:

```
sudo /etc/init.d/apache2 restart
```

2.3. Tesztelés

A telepítés teszteléséhez futtathatja a következő PHP5 phpinfo parancsfájlt:

```
<?php
  phpinfo();
?>
```

Az előző sorokat elmentheti egy `phpinfo.php` nevű fájlba, és elhelyezheti az Apache2 webkiszolgáló DocumentRoot könyvtára alatt. Ezután a böngészőben a `http://gépnév/phpinfo.php` helyet megnyitva a PHP5 különböző konfigurációs paraméterei jelennek meg.

2.4. Hivatkozások

- Részletesebb információkért lásd a php.net[11] dokumentációit.
- Rengeteg könyv szól a PHP-ről. Két jó O'Reilly könyv: Learning PHP 5[12] és a PHP Cook Book[13].
- További információkért nézze meg az Ubuntu wiki Apache MySQL PHP[14] oldalt.

3. Squid - Proxy kiszolgáló

A Squid egy teljes körű szolgáltatásokat nyújtó webes proxy gyorsítótár-kiszolgáló, amely proxy és gyorsítótár-szolgáltatásokat biztosít a HTTP, FTP és más népszerű hálózati protokollokhoz. A Squid képes SSL kérések gyorsítótárazására és proxyzására, DNS-kikeresések gyorsítótárazására és transzparens gyorsítótárazásra. A Squid gyorsítótárazási protokollok széles körét támogatja, például az ICP, HTCP, CARP és WCCP protokollokat.

A Squid proxy gyorsítótár-kiszolgáló kitűnő megoldás rengeteg proxyzási és gyorsítótárazási kiszolgálóigényre, és a telephelyi irodától a vállalati hálózatokig remekül skálázódik, miközben átfogó és részletes hozzáférés-felügyeleti mechanizmusokat, valamint a kritikus paraméterek SNMP feletti figyelését is biztosítja. A dedikált Squid proxy vagy gyorsítótár-kiszolgálóként használandó számítógép kiválasztásakor gondoskodjon róla, hogy a rendszer nagy mennyiségű fizikai memóriát tartalmazzon, mivel a Squid a jobb teljesítmény érdekében memóriabeli gyorsítótárat tart fenn.

3.1. Telepítés

A Squid kiszolgáló telepítéséhez adja ki a következő parancsot a terminálban:

```
sudo apt-get install squid
```

3.2. Beállítás

A Squid beállítása az `/etc/squid/squid.conf` beállítófájl által tartalmazott direktívák szerkesztésével történik. A következő példák bemutatnak néhány olyan direktívát, amelyeket a Squid kiszolgáló viselkedésének befolyásolása érdekében módosíthat. A Squid beállításainak mélyebb megismeréséhez lásd a Hivatkozások szakaszt.

A beállítófájl szerkesztése előtt készítsen másolatot az eredetiről, és tegye írásvédetté, így referenciaként megőrizheti az eredeti beállításokat, és szükség esetén visszaállíthatja azokat.

Készítsen másolatot az `/etc/squid/squid.conf` fájlról, és tegye írásvédetté a terminálban kiadott következő parancsokkal:

```
sudo cp /etc/squid/squid.conf /etc/squid/squid.conf.original
sudo chmod a-w /etc/squid/squid.conf.original
```

- A http_port direktívát módosítsa a következőképpen a Squid kiszolgáló beállításához az alapértelmezett 3128-as helyett a 8888-as TCP port figyelésére:

```
http_port 8888
```

- Módosítsa a visible_hostname direktíva értékét a Squid kiszolgáló nevének megadásához. A névnek nem kötelező megegyezni a gépnévvel. Ebben a példában a név a weezie lesz.

```
visible_hostname weezie
```

- A Squid hozzáférés-vezérlésének segítségével beállíthatja, hogy a Squid által proxyzott internetes szolgáltatások csak bizonyos IP-című felhasználók számára legyenek elérhetők. A következő példa a 192.168.42.0/24 alhálózat felhasználóinak biztosít hozzáférést:

  Adja a következőket az `/etc/squid/squid.conf` fájl ACL szakaszának végéhez:

  ```
  acl fortytwo_network src 192.168.42.0/24
  ```

  Ezután vegye fel a következőket az `/etc/squid/squid.conf` fájl http_access szakasza fölé:

  ```
  http_access allow fortytwo_network
  ```

- A Squid kitűnő hozzáférés-vezérlési szolgáltatásainak köszönhetően beállíthatja, hogy a Squid által proxyzott internetes szolgáltatások csak a normál hivatali órákban legyenek elérhetők. A következő példa egy olyan vállalkozás alkalmazottainak hozzáférését mutatja be, amely hétfőtől péntekig 9 és 17 óra között működik, és a 10.1.42.0/42 alhálózatot használja:

  Adja a következőket az `/etc/squid/squid.conf` fájl ACL szakaszának végéhez:

  ```
  acl biz_network src 10.1.42.0/24
  acl biz_hours time M T W T F 9:00-17:00
  ```

  Ezután vegye fel a következőket az `/etc/squid/squid.conf` fájl http_access szakasza fölé:

  ```
  http_access allow biz_network biz_hours
  ```

Az `/etc/squid/squid.conf` fájl módosítása után mentse a fájlt, és a módosítások életbe léptetéséhez indítsa újra a squid kiszolgálót a következő parancs kiadásával:

```
sudo /etc/init.d/squid restart
```

3.3. Hivatkozások

A Squid weboldala[15]

Az Ubuntu wiki Squid[16] oldala.

[15] http://www.squid-cache.org/

[16] https://help.ubuntu.com/community/Squid

4. Ruby on Rails

A Ruby on Rails egy nyílt forrású webes keretrendszer adatbázis-alapú webalkalmazások fejlesztéséhez. A programozó fenntartható termelékenységére van optimalizálva, mivel lehetővé teszi, hogy a programozó kódoláskor a konvenciókat részesítse előnyben a konfigurációval szemben.

4.1. Telepítés

A Rails telepítése előtt telepíteni kell az Apache és MySQL kiszolgálókat. Az Apache csomag telepítésével kapcsolatban nézze meg a 1. szakasz - HTTPD – Apache2 webkiszolgáló [141] szakaszt, a MySQL telepítésével kapcsolatos információkért pedig a 1. szakasz - MySQL [160] szakaszt.

Az Apache és MySQL csomagok telepítése után készen áll a Ruby on Rails csomag telepítésére.

A Ruby alapcsomagok és a Ruby on Rails telepítéséhez adja ki a következő parancsot a terminálban:

```
sudo apt-get install rails
```

4.2. Beállítás

Módosítsa az `/etc/apache2/sites-available/default` beállítófájlt a tartományok beállításához.

Első lépésként a DocumentRoot direktívát módosítsa:

```
DocumentRoot /a/rails/alkalmazás/útvonala/public
```

Ezután módosítsa a <Directory "/a/rails/alkalmazás/útvonala/public"> direktívát:

```
<Directory "/a/rails/alkalmazás/útvonala/public">
        Options Indexes FollowSymLinks MultiViews ExecCGI
        AllowOverride All
        Order allow,deny
        allow from all
        AddHandler cgi-script .cgi
</Directory>
```

Engedélyezze az Apache mod_rewrite modulját is. A mod_rewrite modul engedélyezéséhez adja ki a következő parancsot a terminálban:

```
sudo a2enmod rewrite
```

Végül módosítsa az `/a/rails/alkalmazás/útvonala/public` és `/a/rails/alkalmazás/útvonala/tmp` könyvtárak tulajdonosát az Apache folyamat futtatására használt felhasználóra:

```
sudo chown -R www-data:www-data /a/rails/alkalmazás/útvonala/public
```

```
sudo chown -R www-data:www-data /a/rails/alkalmazás/útvonala/tmp
```

Ennyi volt! A kiszolgálója ezzel készen áll a Ruby on Rails alkalmazások futtatására.

4.3. Hivatkozások

- További információkért lásd a Ruby on Rails[17] weboldalát.
- Ezen kívül az Agile Development with Rails[18] könyv is nagyszerű információforrás.
- További információkért nézze meg az Ubuntu wiki Ruby on Rails[19] oldalt.

5. Apache Tomcat

Az Apache Tomcat egy webes tároló, amely lehetővé teszi Java Servletek és JSP (Java Server Pages) webalkalmazások kiszolgálását.

Az Ubuntu Tomcat 6.0 csomagjai a Tomcat futtatásának két módját támogatják. Telepítheti klasszikus, önálló rendszerszintű példányként, amely rendszerindításkor indul és a tomcat6 felhasználó nevében fut. Azonban telepíthet privát példányokat is, amelyek a saját felhasználójának jogaival futnak, és amelyeket Önnek kell elindítania és leállítania. Ez utóbbi fejlesztői kiszolgálókon hasznos, ahol több felhasználónak is képesnek kell lennie a tesztelésre a saját Tomcat példányán.

5.1. Rendszerszintű telepítés

A Tomcat kiszolgáló telepítéséhez adja ki a következő parancsot a terminálban:

```
sudo apt-get install tomcat6
```

Ezzel telepítésre került egy Tomcat kiszolgáló, amely csak egy alapértelmezett ROOT webalkalmazást tartalmaz. Ez alapértelmezésben egy minimális „It works” oldalt jelenít meg.

5.2. Beállítás

A Tomcat beállítófájljai az `/etc/tomcat6` könyvtárban találhatók. Itt csak néhány általános beállítási lehetőség kerül ismertetésre, további információkért lásd a Tomcat 6.0 dokumentációját[20].

5.2.1. Alapértelmezett portok megváltoztatása

Alapértelmezésben a Tomcat 6.0 egy HTTP kapcsolatkezelőt futtat a 8080-as porton, és egy AJP kapcsolatkezelőt a 8009-es porton. A rendszeren futó más kiszolgálókkal való ütközés elkerülése érdekében szükség lehet ezen portok megváltoztatására. Ezt az `/etc/tomcat6/server.xml` fájl következő sorainak megváltoztatásával érheti el:

```
<Connector port="8080" protocol="HTTP/1.1"
               connectionTimeout="20000"
               redirectPort="8443" />
...
<Connector port="8009" protocol="AJP/1.3" redirectPort="8443" />
```

5.2.2. A használt JVM megváltoztatása

Alapértelmezésben a Tomcat az OpenJDK-6 használatával fut, ezután a Sun JVM-jét próbálja, majd az egyéb JVM-eket. Ha több JVM van telepítve, az `/etc/default/tomcat6` JAVA_HOME változójának beállításával megadható a használni kívánt JVM:

[20] http://tomcat.apache.org/tomcat-6.0-doc/index.html

```
JAVA_HOME=/usr/lib/jvm/java-6-sun
```

5.2.3. Felhasználók és szerepek deklarálása

A felhasználónevek, jelszavak és szerepek (csoportok) központilag adhatók meg a Servlet tárolókban. A Tomcat 6.0-ban ezt az `/etc/tomcat6/tomcat-users.xml` fájlban teheti meg:

```
<role rolename="admin"/>
<user username="tomcat" password="t1t0k" roles="admin"/>
```

5.3. Szabványos Tomcat webalkalmazások használata

A Tomcat alapértelmezésben tartalmaz dokumentációs, adminisztrációs vagy bemutató célokra használható webalkalmazásokat.

5.3.1. Tomcat dokumentáció

A tomcat6-docs csomag a Tomcat 6.0 webalkalmazásként csomagolt dokumentációját tartalmazza, amelyet alapértelmezésben a http://azönkiszolgálója:8080/docs címen érhet el. A következő parancs kiadásával telepítheti:

```
sudo apt-get install tomcat6-docs
```

5.3.2. Tomcat adminisztrációs webalkalmazások

A tomcat6-admin csomag két webalkalmazást tartalmaz, amelyek a Tomcat kiszolgáló webes felületről történő adminisztrálására szolgálnak. Ezeket a következő parancs kiadásával telepítheti:

```
sudo apt-get install tomcat6-admin
```

Az első a manager webalkalmazás, amelyet alapértelmezésben a http://azönkiszolgálója:8080/manager/html címen érhet el. Elsősorban a kiszolgáló állapotának lekérésére és webalkalmazások újraindítására használható.

A manager alkalmazás elérése alapértelmezésben korlátozott: az eléréséhez meg kell adnia egy „manager” szerepű felhasználót az `/etc/tomcat6/tomcat-users.xml` fájlban.

A második a host-manager webalkalmazás, amelyet alapértelmezésben a http://azönkiszolgálója:8080/host-manager/html címen érhet el. Ez virtuális kiszolgálók dinamikus létrehozására használható.

A host-manager alkalmazás elérése alapértelmezésben szintén korlátozott: az eléréséhez meg kell adnia egy „admin” szerepű felhasználót az `/etc/tomcat6/tomcat-users.xml` fájlban.

Biztonsági okokból a tomcat6 felhasználó alapértelmezésben nem írhat az `/etc/tomcat6` könyvtárba. Ezen adminisztrációs webalkalmazások néhány szolgáltatása (alkalmazástelepítés, virtuális kiszolgálók létrehozása) írási hozzáférést igényel a könyvtárhoz. Ha ezeket a szolgáltatásokat

használni kívánja, akkor adja ki a következő parancsokat a megfelelő hozzáférés biztosításához a tomcat6 csoport felhasználóinak:

```
sudo chgrp -R tomcat6 /etc/tomcat6
sudo chmod -R g+w /etc/tomcat6
```

5.3.3. Példa Tomcat webalkalmazások

A tomcat6-examples csomag két webalkalmazást tartalmaz, amelyek servletek és JSP szolgáltatások tesztelésére vagy bemutatására használhatók, ezek alapértelmezésben a http://azönkiszolgálója:8080/examples címen érhetők el. A következő parancs kiadásával telepíthetők:

```
sudo apt-get install tomcat6-examples
```

5.4. Privát példányok használata

A Tomcatet sokszor fejlesztési és tesztelési célokra használják, ekkor egy rendszerszintű példány használata nem elégíti ki egy adott rendszer több felhasználójának igényeit. Az Ubuntu Tomcat 6.0 csomagjai a felhasználószintű példányok telepítését segítő eszközöket tartalmaznak, lehetővé téve a rendszer minden felhasználójának önálló privát példányok futtatását (rendszergazdai jog nélkül), ugyanúgy a rendszerre telepített programkönyvtárakat használva.

Lehetőség van a rendszerszintű példány és a privát példányok párhuzamos használatára is, amennyiben nem azonos TCP-portokat használnak.

5.4.1. Privát példányok támogatásának telepítése

A következő parancs kiadásával telepíthető minden, ami a privát példányok futtatásához szükséges:

```
sudo apt-get install tomcat6-user
```

5.4.2. Privát példány létrehozása

A következő parancs kiadásával hozhat létre privát példánykönyvtárat:

```
tomcat6-instance-create privátpéldány
```

Ez létrehozza az új `privátpéldány` könyvtárat, az összes szükséges alkönyvtárral és parancsfájllal. Az általános programkönyvtárakat például telepítheti a `lib/` könyvtárba, a webalkalmazásokat pedig a `webapps` alkönyvtárba. Alapértelmezésben nem kerülnek telepítésre webalkalmazások.

5.4.3. A privát példány beállítása

A privát példány szokásos Tomcat beállítófájljait a `conf/` alkönyvtárban találja meg. Mindenképpen szerkesztenie kell például a `conf/server.xml` fájlt a privát Tomcat példány által használt portok módosításához, így elkerülve az ütközést az egyéb, esetlegesen futó példányokkal.

5.4.4. A privát példány indítása/leállítása

A privát példányt a következő parancs kiadásával indíthatja el (feltételezve, hogy a példány a `privátpéldány` könyvtárban van):

```
privátpéldány/bin/startup.sh
```

Keressen hibákat a `logs/` alkönyvtárban. Ha a java.net.BindException: Address already in use<null>:8080 hibát látja, akkor a port már foglalt, és meg kell változtatnia.

A következő parancs kiadásával leállíthatja a példányt (feltételezve, hogy a példány a `privátpéldány` könyvtárban van):

```
privátpéldány/bin/shutdown.sh
```

5.5. Hivatkozások

- További információkért nézze meg az Apache Tomcat[21] weboldalát.
- A Tomcat: The Definitive Guide[22] egy kiváló könyv webalkalmazások építéséhez a Tomcattel.
- További könyvekért nézze meg a Tomcat Books[23] oldalt.
- Nézze meg az Ubuntu wiki Apache Tomcat[24] oldalát is.

11. fejezet - Adatbázisok

Az Ubuntu két népszerű adatbázis-kiszolgálót biztosít, ezek:

- MySQL™
- PostgreSQL

Mindkettő elérhető a main tárolóból. Ez a szakasz ezen adatbázis-kiszolgálók telepítését és beállítását ismerteti.

1. MySQL

A MySQL egy gyors, többszálú, többfelhasználós és megbízható SQL adatbázis-kiszolgáló. Küldetéskritikus, nagy terhelésű éles rendszerekre, valamint tömegesen telepített szoftverekbe való beágyazásra szánták.

1.1. Telepítés

A MySQL telepítéséhez adja ki a következő parancsot:

```
sudo apt-get install mysql-server
```

A telepítési folyamat során a program bekéri a MySQL root felhasználó jelszavát.

A telepítés után a MySQL kiszolgáló automatikusan elindul. A következő parancs kiadásával meggyőződhet róla, hogy a MySQL kiszolgáló megfelelően fut-e:

```
sudo netstat -tap | grep mysql
```

A parancs futtatásakor a következő sort, vagy valami hasonlót kell látnia:

```
tcp        0      0 localhost:mysql         *:*                     LISTEN      2556/mysqld
```

Ha a kiszolgáló nem fut, a következő parancs kiadásával elindíthatja:

```
sudo /etc/init.d/mysql restart
```

1.2. Beállítás

Az `/etc/mysql/my.cnf` fájl szerkesztésével módosíthatja az alapvető beállításokat – naplófájl, portszám stb. Például, a MySQL beállításához hálózati gépekről érkező kapcsolatok figyelésére módosítsa a bind-address direktívát a kiszolgáló IP-címére:

```
bind-address            = 192.168.0.5
```

A 192.168.0.5 helyére a megfelelő címet írja.

Az `/etc/mysql/my.cnf` módosítása után újra kell indítani a mysql démont:

```
sudo /etc/init.d/mysql restart
```

A MySQL root jelszavának módosításához adja ki a következőt:

```
sudo dpkg-reconfigure mysql-server-5.1
```

A mysql démon leáll, és a program bekéri az új jelszót.

1.3. Információforrások

- További információkért lásd a MySQL honlapját[1].
- A MySQL kézikönyv szintén elérhető a mysql-doc-5.0 csomagban. A csomag telepítéséhez adja ki a következő parancsot:

  ```
  sudo apt-get install mysql-doc-5.0
  ```

  A dokumentáció HTML-formátumban van, megjelenítéséhez nyissa meg a file:///usr/share/doc/mysql-doc-5.0/refman-5.0-en.html-chapter/index.html helyet a böngészőjében.
- Általános SQL információkért lásd Rafe Colburn Using SQL Special Edition[2] című könyvét.
- Az Ubuntu wiki Apache MySQL PHP[3] oldala is hasznos információkat tartalmaz.

2. PostgreSQL

A PostgreSQL egy objektumrelációs adatbázisrendszer, amely rendelkezik a hagyományos kereskedelmi adatbázisrendszerek szolgáltatásaival, és a következő generációs adatbázis-kezelő rendszerekben megtalálható fejlesztésekkel is.

2.1. Telepítés

A PostgreSQL telepítéséhez adja ki a következő parancsot:

```
sudo apt-get install postgresql
```

A telepítés befejeződésekor állítsa be a PostgreSQL kiszolgálót az igényeinek megfelelően, bár az alapértelmezett konfiguráció is használható.

2.2. Beállítás

Alapértelmezésben a TCP/IP kapcsolat le van tiltva. A PostgreSQL több klienshitelesítési módszert támogat. Alapértelmezésben az IDENT hitelesítési módszer van használatban a postgres és helyi felhasználókhoz. További információkért nézze meg a PostgreSQL Administrator's Guide[4] oldalt.

A következő szakasz feltételezi, hogy a TCP/IP módszert szeretné engedélyezni, és az MD5 módszert szeretné használni a kliensek hitelesítésére. A PostgreSQL konfigurációs fájljai az `/etc/postgresql/<verzió>/main` könyvtárban találhatók. A PostgreSQL 8.4 esetén például ez az `/etc/postgresql/8.4/main` könyvtár.

Az ident hitelesítés beállításához az `/etc/postgresql/8.4/main/pg_ident.conf` fájlba kell bejegyzéseket felvennie.

A TCP/IP kapcsolatok engedélyezéséhez szerkessze az `/etc/postgresql/8.4/main/postgresql.conf` fájlt.

Keresse meg a #listen_addresses = 'localhost' sort, és módosítsa:

```
listen_addresses = 'localhost'
```

Más számítógépek csatlakozását a PostgreSQL kiszolgálójához a „localhost” a kiszolgáló IP-címére cserélésével engedélyezheti.

A többi paramétert is szerkesztheti, ezekkel kapcsolatos információkat a konfigurációs fájlban vagy a PostgreSQL dokumentációban találhat.

Miután a csatlakozás már lehetséges a PostgreSQL kiszolgálóhoz, a következő lépés a postgres felhasználó jelszavának beállítása. Adja ki a következő parancsot az alapértelmezett PostgreSQL sablonadatbázishoz való csatlakozáshoz:

[4] http://www.postgresql.org/docs/8.4/static/admin.html

```
sudo -u postgres psql template1
```

A fenti parancs a postgres felhasználó nevében csatlakozik a template1 PostgreSQL adatbázishoz. Miután csatlakozott a PostgreSQL kiszolgálóhoz, az SQL parancsértelmezőbe kerül. A psql parancsértelmezőben futtathatja a következő SQL parancsot a postgres felhasználó jelszavának beállításához.

```
ALTER USER postgres with encrypted password 'az_ön_jelszava';
```

A jelszó beállítása után szerkessze az `/etc/postgresql/8.4/main/pg_hba.conf` fájlt az MD5 hitelesítés használatához a postgres felhasználóval:

```
local   all         postgres                          md5
```

Végül indítsa újra a PostgreSQL démont az új beállítások életbe léptetéséhez. Adja ki a következő parancsot a PostgreSQL újraindításához:

```
sudo /etc/init.d/postgresql-8.4 restart
```

A fenti konfiguráció semmi esetre sem teljes. További paraméterek beállításához nézze meg a PostgreSQL Administrator's Guide[5] oldalt.

2.3. Információforrások

- A fent említett Administrator's Guide[6] kiváló információforrás. Ez elérhető a postgresql-doc-8.4 csomagban is. A csomag telepítéséhez adja ki a következő parancsot:

  ```
  sudo apt-get install postgresql-doc-8.4
  ```

  Az útmutató megjelenítéséhez nyissa meg a file:///usr/share/doc/postgresql-doc-8.4/html/index.html helyet a böngészőjében.
- Általános SQL információkért lásd Rafe Colburn Using SQL Special Edition[7] című könyvét.
- További részletekért nézze meg az Ubuntu wiki PostgreSQL[8] oldalát.

12. fejezet - LAMP alkalmazások

1. Áttekintés

A LAMP-telepítések (Linux + Apache + MySQL + PHP) az Ubuntu kiszolgálók népszerű felhasználási módjának számítanak. Rengeteg nyílt forrású alkalmazás készült a LAMP alkalmazáscsomag felhasználásával. Néhány népszerű LAMP-alkalmazás: wikik, tartalomkezelő rendszerek (CMS), és menedzsment-szoftverek, mint a phpMyAdmin.

A LAMP egyik előnye a jelentős rugalmassága a különböző adatbázisok, webkiszolgálók és parancsnyelvek irányában. A MySQL népszerű helyettesítői a PostgreSQL és SQLite. A PHP helyett gyakran a Python, Perl és Ruby nyelveket használják.

A legtöbb LAMP alkalmazás telepítésének hagyományos módja:

- Az alkalmazás forrásfájljait tartalmazó archívum letöltése.
- Az archívum kibontása, általában a webkiszolgáló által elérhető könyvtárba.
- A források kibontási helyének függvényében egy webkiszolgáló beállítása a fájlok szolgáltatására.
- Az alkalmazás beállítása az adatbázishoz való kapcsolódásra.
- Egy parancsfájl futtatása, vagy az alkalmazás egy oldalának megnyitása az alkalmazás által igényelt adatbázis telepítéséhez.
- A fenti, vagy azokhoz hasonló lépések végrehajtása után készen áll az alkalmazás használatának megkezdésére.

Ezen megközelítés használatának hátránya, hogy az alkalmazás fájljai a fájlrendszerben nem szabványos módon kerülnek elhelyezésre, ez megnehezíti az alkalmazás telepítési helyének meghatározását. A másik nagy hátrány az alkalmazás frissítése. Új verzió kiadásakor az alkalmazás telepítéséhez szükséges eljárást kell alkalmazni a frissítés telepítéséhez.

Szerencsére számos LAMP alkalmazás elérhető Ubuntu csomagban, és a nem LAMP alkalmazásokkal azonos módon telepíthetők. Az alkalmazástól függően azonban szükség lehet néhány extra konfigurációs és telepítési lépésre.

Ez a szakasz a MoinMoin és MediaWiki wikialkalmazások, valamint a phpMyAdmin MySQL-menedzselő alkalmazás telepítését és konfigurálását mutatja be.

A wiki egy olyan weboldal, amely egyszerűen teszi lehetővé felhasználói számára a tartalom hozzáadását, eltávolítását és az elérhető tartalom módosítását. Az együttműködés és használat egyszerűsége a wikit hatékony eszközzé teszi a tömeges együttműködő szerkesztéshez. A wiki kifejezést az együttműködő szoftverekre is használjuk.

2. Moin Moin

A MoinMoin egy Python nyelven megvalósított, a PikiPiki wikirendszerre épülő és GNU GPL alatt elérhető wikirendszer.

2.1. Telepítés

A MoinMoin telepítéséhez adja ki a következő parancsot:

```
sudo apt-get install python-moinmoin
```

Az apache2 webkiszolgálót is telepítenie kell. Az apache2 webkiszolgáló telepítéséhez lásd a 1. szakasz - HTTPD – Apache2 webkiszolgáló [141] szakasz 1.1. szakasz - Telepítés [141] alszakaszát.

2.2. Beállítás

Az első wiki alkalmazásának beállításához futtassa a következő parancsokat. Tegyük fel, hogy egy sajátwiki nevű wikit hoz létre:

```
cd /usr/share/moin
sudo mkdir sajátwiki
sudo cp -R data sajátwiki
sudo cp -R underlay sajátwiki
sudo cp server/moin.cgi sajátwiki
sudo chown -R www-data.www-data sajátwiki
sudo chmod -R ug+rwX sajátwiki
sudo chmod -R o-rwx sajátwiki
```

Most állítsa be a MoinMoint az új sajátwiki nevű wiki megtalálásához. A MoinMoin beállításához nyissa meg az `/etc/moin/mywiki.py` fájlt, és módosítsa a következő sort:

```
data_dir = '/org/sajátwiki/data'
```

erre:

```
data_dir = '/usr/share/moin/sajátwiki/data'
```

A data_dir beállítás alatt vegye fel a data_underlay_dir beállítást:

```
data_underlay_dir='/usr/share/moin/sajátwiki/underlay'
```

Ha az `/etc/moin/mywiki.py` fájl nem létezik, akkor készítsen egy másolatot az `/etc/moin/moinmaster.py` fájlról `/etc/moin/mywiki.py` néven, ezután végezze el a fenti módosítást.

Ha a wikit saját_wikim_neve formában nevezte el, akkor szúrja be a „("saját_wikim_neve", r".*")” sort az `/etc/moin/farmconfig.py` fájlba a „("sajátwiki", r".*")” sor után.

Miután beállította a MoinMoint az első sajátwiki nevű wiki alkalmazás felismerésére, be kell állítania az apache2-t is, és fel kell készítenie a wiki alkalmazáshoz.

A következő sorokat kell felvennie az `/etc/apache2/sites-available/default` fájlba a „<VirtualHost *>” címkén belülre:

```
### moin
  ScriptAlias /sajátwiki "/usr/share/moin/sajátwiki/moin.cgi"
  alias /moin_static184 "/usr/share/moin/htdocs"
  <Directory /usr/share/moin/htdocs>
  Order allow,deny
  allow from all
  </Directory>
### end moin
```

A fenti sorban módosítsa a moin_static184 értéket a telepített moinmoin verziónak megfelelően.

Az apache2 webkiszolgáló beállítása és a wiki alkalmazás használatára való felkészítése után újra kell indítania azt. Adja ki a következő parancsot az apache2 webkiszolgáló újraindításához:

```
sudo /etc/init.d/apache2 restart
```

2.3. Ellenőrzés

A wiki alkalmazás működését a következő URL megnyitásával ellenőrizheti:

```
http://localhost/sajátwiki
```

Futtathatja a teszt parancsot is a következő URL megnyitásával:

```
http://localhost/sajátwiki?action=test
```

További részletekért lásd a MoinMoin[1] weboldalát.

2.4. Hivatkozások

- További információkért lásd a MoinMoin[2] weboldalát.
- Nézze meg az Ubuntu wiki MoinMoin[3] oldalát is.

[1] http://moinmo.in/

3. MediaWiki

A MediaWiki egy PHP nyelven írt webes wikiszoftver. A MySQL vagy PostgreSQL adatbázis-kezelő rendszerek használatára is képes.

3.1. Telepítés

A MediaWiki telepítése előtt telepítenie kell az Apache2 webkiszolgálót, a PHP5 parancsnyelvet, és egy adatbázis-kezelő rendszert. A MySQL és a PostgreSQL a legelterjedtebbek, válassza ki az igényeinek megfelelőt. A telepítési utasításokért nézze meg a megfelelő szakaszokat.

A MediaWiki telepítéséhez adja ki a következő parancsot:

```
sudo apt-get install mediawiki php5-gd
```

További MediaWiki funkciók eléréséhez telepítse a mediawiki-extensions csomagot.

3.2. Beállítás

A MediaWiki `mediawiki.conf` nevű Apache konfigurációs fájlja az `/etc/apache2/conf.d/` könyvtárban található. A következő sort kell kivennie megjegyzésből a MediaWiki alkalmazás eléréséhez:

```
# Alias /mediawiki /var/lib/mediawiki
```

A fenti sor megjegyzésből való kivétele után indítsa újra az Apache kiszolgálót. Ezután a MediaWiki a következő URL megnyitásával érhető el:

```
http://localhost/mediawiki/config/index.php
```

Olvassa el az ezen oldalon megjelenő „Checking environment...” szakaszt. Ennek elolvasásával számos problémát megoldhat.

A konfigurálás végén át kell másolnia a `LocalSettings.php` fájlt az `/etc/mediawiki` könyvtárba:

```
sudo mv /var/lib/mediawiki/config/LocalSettings.php /etc/mediawiki/
```

Szükség lehet az `/etc/mediawiki/LocalSettings.php` szerkesztésére, és a következő megváltoztatására:

```
ini_set( 'memory_limit', '64M' );
```

3.3. Kiterjesztések

A kiterjesztések új szolgáltatásokat biztosítanak a MediaWiki alkalmazáshoz. A kiterjesztések lehetővé teszik a wiki adminisztrátorai és végfelhasználói számára a MediaWiki igényeik szerinti személyre szabását.

A MediaWiki kiterjesztései letölthetők archívumfájlként, vagy a Subversion tárolóból. Másolja ezeket a `/var/lib/mediawiki/extensions` könyvtárba. A következő sort fel kell vennie az `/etc/mediawiki/LocalSettings.php` fájl végére:

```
require_once "$IP/extensions/Kiterjesztésnév/Kiterjesztésnév.php";
```

3.4. Hivatkozások

- További részletekért lásd a MediaWiki[4] weboldalát.
- A MediaWiki Administrators' Tutorial Guide[5] rengeteg információt tartalmaz az új MediaWiki adminisztrátorok számára.
- Az Ubuntu wiki MediaWiki[6] oldala is értékes információforrás.

4. phpMyAdmin

A phpMyAdmin egy kifejezetten MySQL kiszolgálók adminisztrálására írt LAMP alkalmazás. A PHP nyelven írt, és webböngészőből elérhető phpMyAdmin minden adatbázis-adminisztrációs feladathoz biztosít grafikus felületet.

4.1. Telepítés

A phpMyAdmin telepítése előtt el kell tudnia érni a MySQL adatbázist vagy ugyanazon a gépen, amelyre a phpMyAdmin telepítve van, vagy a hálózatról elérhető gépről. További információkért lásd: 1. szakasz - MySQL [160]. Adja ki a következő parancsot:

```
sudo apt-get install phpmyadmin
```

Válassza ki, melyik webkiszolgálót szeretné a phpMyAdmin számára beállítani. Ez a szakasz a továbbiakban az Apache2 webkiszolgálót használja.

Nyissa meg a böngészőben a http://kiszolgálónév/phpmyadmin oldalt, a kiszolgálónév helyére a tényleges gépnevet írja. A bejelentkező oldalon a username mezőben adja meg a root, vagy bármely beállított MySQL felhasználó nevét, és adja meg a MySQL felhasználó jelszavát.

Ha bejelentkezett, már megváltoztathatja a root jelszavát, felhasználókat hozhat létre, adatbázisokat és táblákat hozhat létre vagy törölhet stb.

4.2. Beállítás

A phpMyAdmin konfigurációs fájljai az `/etc/phpmyadmin` könyvtárban találhatók. Az elsődleges konfigurációs fájl az `/etc/phpmyadmin/config.inc.php`. Ez a fájl a phpMyAdminra globálisan érvényes beállításokat tartalmazza.

A phpMyAdmin másik kiszolgálón található MySQL adatbázis adminisztrálására való használatához módosítsa a következőket az `/etc/phpmyadmin/config.inc.php` fájlban:

```
$cfg['Servers'][$i]['host'] = 'db_kiszolgáló';
```

A db_kiszolgáló helyére a tényleges távoli adatbázis-kiszolgáló nevét vagy IP-címét írja. Ne feledjen jogosultságot adni a phpMyAdmin gépnek a távoli adatbázis eléréséhez.

A beállítások módosítása után jelentkezzen ki a phpMyAdminból, a következő belépéskor el kell tudnia érni az új kiszolgálót.

A `config.header.inc.php` és `config.footer.inc.php` fájlok a phpMyAdmin HTML fejlécének és láblécének megadására használhatók.

Szintén fontos konfigurációs fájl az `/etc/phpmyadmin/apache.conf`, erre a fájlra mutat az `/etc/apache2/conf.d/phpmyadmin.conf` szimbolikus link, és a phpMyAdmin oldal kiszolgálására használt

Apache2 beállítására szolgál. A fájl többek közt a PHP betöltésére és könyvtárjogosultságokhoz használt direktívákat tartalmaz. Az Apache2 konfigurálásával kapcsolatos további információkért lásd: 1. szakasz - HTTPD – Apache2 webkiszolgáló [141].

4.3. Hivatkozások

- A csomag tartalmazza a phpMyAdmin dokumentációját, amely elérhető a phpMyAdmin logó alatti phpMyAdmin Documentation hivatkozás (bekeretezett kérdőjel) megnyitásával. A hivatalos dokumentáció elérhető a phpMyAdmin[7] weboldalán is.
- A Mastering phpMyAdmin[8] című könyv is remek információforrás.
- Szintén értékes információforrás az Ubuntu wiki phpMyAdmin[9] oldala.

13. fejezet - Fájlkiszolgálók

Ha egy hálózaton több számítógépe is van, fel fog merülni az igény fájlok megosztására közöttük. Ebben a szakaszban az FTP, NFS és CUPS telepítését és beállítását ismertetjük.

1. FTP-kiszolgáló

A fájlátviteli protokoll (FTP) egy TCP protokoll fájlok számítógépek közti fel- és letöltésére. Az FTP kliens/szerver modell alapján működik. A kiszolgáló összetevőt FTP démonnak hívják. Folyamatosan figyeli a távoli kliensek FTP-kéréseit. Kérés fogadásakor kezeli a bejelentkezést, és létrehozza a kapcsolatot. A munkamenet időtartama alatt végrehajtja az FTP kliens által küldött parancsokat.

Az FTP-kiszolgáló elérése kétféleképp kezelhető:

- Névtelenül
- Hitelesítve

Névtelen módban a távoli kliensek az „anonymous” vagy „ftp” nevű alapértelmezett felhasználói fiók használatával, és jelszóként egy e-mail cím küldésével érhetik el az FTP-kiszolgálót. Hitelesített módban a felhasználónak rendelkeznie kell fiókkal és jelszóval. Az FTP kiszolgáló könyvtárainak és fájljainak elérése a bejelentkezéshez használt fiók jogosultságaitól függ. Általánosságban az FTP-démon elrejti az FTP-kiszolgáló gyökérkönyvtárát, és az FTP home könyvtárára változtatja. Ez elrejti a fájlrendszer többi részét a távoli munkamenetek elől.

1.1. vsftpd – FTP-kiszolgáló telepítése

A vsftpd az Ubuntuban elérhető egyik FTP-démon. Egyszerű telepíteni, beállítani és karbantartani. A vsftpd telepítéséhez adja ki a következő parancsot:

```
sudo apt-get install vsftpd
```

1.2. Névtelen FTP beállítása

Alapértelmezésben a vsftpd csak a névtelen letöltés engedélyezésére van beállítva. A telepítés során létrejön egy ftp felhasználó, a saját könyvtára pedig a `/home/ftp`. Ez az alapértelmezett FTP könyvtár.

Ha meg szeretné változtatni ezt a helyet, akkor egyszerűen hozza létre a könyvtárat (például: `/srv/ftp`), és módosítsa az ftp felhasználó saját könyvtárát.

```
sudo mkdir /srv/ftp
sudo usermod -d /srv/ftp ftp
```

A módosítás után indítsa újra a vsftpd démont:

```
sudo /etc/init.d/vsftpd restart
```

Végül másoljon át minden, a névtelen FTP-n megosztani kívánt fájlt és könyvtárat az `/srv/ftp` könyvtárba.

1.3. Felhasználókat hitelesítő FTP konfigurálása

A vsftpd beállításához a rendszer felhasználóinak hitelesítésére, és fájlok feltöltésének engedélyezéséhez szerkessze az `/etc/vsftpd.conf` fájlt:

```
local_enable=YES
write_enable=YES
```

Indítsa újra a vsftpd démont:

```
sudo /etc/init.d/vsftpd restart
```

Miután a rendszer felhasználói bejelentkeznek az FTP-re, a saját könyvtáraikba fognak belépni, és onnan tölthetnek le illetve fel, hozhatnak létre könyvtárakat stb.

Ehhez hasonlóan alapértelmezésben a névtelen felhasználók nem tölthetnek fel fájlokat az FTP-kiszolgálóra. Ezen beállítás módosításához vegye ki a következő sort megjegyzésből, és indítsa újra a vsftpd démont:

```
anon_upload_enable=YES
```

A névtelen FTP-feltöltés engedélyezése hatalmas biztonsági kockázat. A legjobb megoldás a névtelen feltöltés letiltva hagyása az internetről közvetlenül elérhető kiszolgálókon.

A konfigurációs fájl számos paramétert tartalmaz. Az egyes paraméterek leírása megtalálható a konfigurációs fájlban. Emellett a fájl kézikönyvoldalán (man 5 vsftpd.conf) is megtalálhatja ezek leírását.

1.4. FTP biztonságossá tétele

Az `/etc/vsftpd.conf` tartalmaz a vsftpd biztonságosabbá tételét segítő beállításokat is. A felhasználók például saját könyvtárukra korlátozhatók a következő kivételével a megjegyzésből:

```
chroot_local_user=YES
```

Korlátozhatja felhasználók adott csoportját is a saját könyvtárukra:

```
chroot_list_enable=YES
chroot_list_file=/etc/vsftpd.chroot_list
```

A fenti beállítások megjegyzésből való kivétele után hozzon létre egy `/etc/vsftpd.chroot_list` nevű fájlt, amely tartalmazza a felhasználók listáját, soronként egy felhasználót. Ezután indítsa újra a vsftpd démont:

```
sudo /etc/init.d/vsftpd restart
```

Az `/etc/ftpusers` fájl azon felhasználók listáját tartalmazza, akiknek `nem engedélyezett` az FTP elérése. Az alapértelmezett lista a root, daemon, nobody stb. felhasználókat tartalmazza. További felhasználók FTP-használatának megtiltásához egyszerűen vegye fel őket erre a listára.

Az FTP titkosítható is az FTPS segítségével. Az FTPS az SSL fölötti FTP rövidítése és nem azonos az SFTP-vel. Az SFTP egy FTP-szerű munkamenet titkosított SSH kapcsolat fölött. A fő különbség, hogy az SFTP felhasználóknak szükségük van egy parancsértelmező fiókra a rendszeren, és nem a nologin parancsértelmezőt használják. Nem biztos, hogy egyes környezetekben – például közös webkiszolgálók esetén – ideális minden felhasználónak parancsértelmezőt adni.

Az FTPS beállításához szerkessze az `/etc/vsftpd.conf` fájlt, és vegye fel a végére a következőt:

```
ssl_enable=Yes
```

Vegye észre a tanúsítvánnyal és kulccsal kapcsolatos beállításokat is:

```
rsa_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
rsa_private_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
```

Ezek a beállítások alapértelmezésben az ssl-cert csomag által biztosított tanúsítványra és kulcsra vannak állítva. Éles környezetben ezeket az adott géphez generált tanúsítvánnyal és kulccsal kell helyettesíteni. A tanúsítványokkal kapcsolatos további információkért lásd a 5. szakasz - Tanúsítványok [125] szakaszt.

Most indítsa újra a vsftpd démont, és a nem névtelen felhasználók az FTPS használatára lesznek kényszerítve:

```
sudo /etc/init.d/vsftpd restart
```

Ahhoz, hogy a `/usr/sbin/nologin` parancsértelmezővel rendelkező felhasználók elérhessék az FTP-t, szerkessze az `/etc/shells` fájlt, és vegye fel a nologin parancsértelmezőt:

```
# /etc/shells: valid login shells
/bin/csh
/bin/sh
/usr/bin/es
/usr/bin/ksh
/bin/ksh
/usr/bin/rc
/usr/bin/tcsh
/bin/tcsh
/usr/bin/esh
/bin/dash
/bin/bash
/bin/rbash
```

```
/usr/bin/screen
/usr/sbin/nologin
```

Erre azért van szükség, mert a vsftpd alapértelmezésben a PAM-ot használja hitelesítésre, és az `/etc/pam.d/vsftpd` konfigurációs fájl tartalmazza a következőt:

```
auth    required        pam_shells.so
```

A shells PAM modul korlátozza a parancsértelmezők elérését az `/etc/shells` fájlban felsoroltakra.

A legtöbb népszerű FTP-kliens beállítható az FTPS használatával történő csatlakozásra. Az lftp parancssori FTP-kliens is képes az FTPS használatára.

1.5. Hivatkozások

- További információkért lásd a vsftpd weboldalát[1].
- Az `/etc/vsftpd.conf` részletes beállításaiért lásd a vsftpd.conf kézikönyvoldalát[2].
- A FTPS vs. SFTP: What to Choose[3] cikk hasznos információkat tartalmaz az FTPS és az SFTP különbségeiről.
- További információkért nézze meg az Ubuntu wiki vsftpd[4] oldalát.

2. Hálózati fájlrendszer (NFS)

Az NFS lehetővé teszi könyvtárak és fájlok megosztását másokkal a hálózaton. Az NFS használatával a felhasználók és programok majdnem úgy érhetik el a távoli rendszereken lévő fájlokat, mintha azok helyiek lennének.

Az NFS által nyújtható legfontosabb előnyök közül néhány:

- A helyi munkaállomások kevesebb lemezhelyet használnak, mivel az általánosan használt adatok egyetlen gépen tárolhatók, mégis mindenki számára elérhetők maradnak a hálózaton.
- A felhasználóknak nem kell minden hálózati gépen saját könyvtárral rendelkezniük. A saját könyvtárak létrehozhatók az NFS-kiszolgálón, és elérhetővé tehetők a hálózaton.
- A tárolóeszközök, például CD-ROM és USB-meghajtók más gépek által is használhatók a hálózaton keresztül. Ez csökkentheti a hálózaton szükséges cserélhető adathordozós meghajtók számát.

2.1. Telepítés

Adja ki a következő parancsot az NFS-kiszolgáló telepítéséhez:

```
sudo apt-get install nfs-kernel-server
```

2.2. Beállítás

Az exportálandó könyvtárakat az `/etc/exports` fájlba felvéve konfigurálhatja. Például:

```
/ubuntu  *(ro,sync,no_root_squash)
/home    *(rw,sync,no_root_squash)
```

A * helyére gépnév-formátumok valamelyikét írhatja. A gépnév-deklarációt tegye a lehető legpontosabbá, hogy az NFS-csatolást ne érhesse el a szükségesnél több gép.

Az NFS-kiszolgáló elindításához adja ki a következő parancsot:

```
sudo /etc/init.d/nfs-kernel-server start
```

2.3. NFS-kliens beállítása

A mount parancs segítségével csatolhatja a másik gépen lévő megosztott NFS könyvtárat. Adjon ki egy ehhez hasonló parancsot:

```
sudo mount példa.hu:/ubuntu /local/ubuntu
```

A `/local/ubuntu` csatolási pontnak léteznie kell. Az `/local/ubuntu` könyvtárban nem lehetnek fájlok vagy alkönyvtárak.

Az NFS-megosztás csatolásának másik módja egy sor hozzáadása az `/etc/fstab` fájlhoz. A sornak tartalmaznia kell az NFS-kiszolgáló gépnevét, a kiszolgálón exportált könyvtárat és a helyi gép azon könyvtárát, amelybe az NFS-megosztást csatolni szeretné.

Az `/etc/fstab` fájlba írandó sor általános szintaxisa a következő:

```
példa.hu:/ubuntu /local/ubuntu nfs rsize=8192,wsize=8192,timeo=14,intr
```

Ha problémába ütközik egy NFS-megosztás csatolásakor, akkor győződjön meg róla, hogy az nfs-common csomag telepítve van a kliensen. Az nfs-common telepítéséhez adja ki a következő parancsot:

```
sudo apt-get install nfs-common
```

2.4. Hivatkozások

Linux NFS faq[5]

Ubuntu wiki NFS Howto[6]

[5] http://nfs.sourceforge.net/

[6] https://help.ubuntu.com/community/NFSv4Howto

3. CUPS nyomtatókiszolgáló

Az Ubuntun a nyomtatást és a nyomtatási szolgáltatásokat elsődlegesen a Common UNIX Printing System (CUPS) működteti. Ez a nyomtatórendszer egy szabadon elérhető, hordozható nyomtatási réteg, amely a legtöbb Linux disztribúció új nyomtatási szabványa lett.

A CUPS kezeli a nyomtatási feladatokat és sorokat, valamint hálózati nyomtatást biztosít a szabványos internetes nyomtatási protokoll (IPP) használatával. Támogatást nyújt nyomtatók széles körének a pontmátrixos nyomtatóktól a lézerekig, és köztük sok máshoz is. A CUPS támogatja a PostScript nyomtatóleírást (PPD) és a hálózati nyomtatók automatikus felismerését, valamint tartalmaz egy egyszerű webes konfigurációs és adminisztrációs eszközt.

3.1. Telepítés

A CUPS telepítéséhez használja a sudo apt-get parancsot. Adja ki a következő parancsot:

```
sudo apt-get install cups
```

A felhasználói jelszó megadása után a csomagok letöltődnek és telepítésre kerülnek. A telepítés befejeződésekor a CUPS-kiszolgáló automatikusan elindul.

Hibakeresési céllal a `/var/log/cups/error_log` könyvtárban megtalálja a CUPS-kiszolgáló hibanaplóit. Ha a hibanapló nem tartalmaz elég információt a tapasztalt hibák elhárításához, akkor a CUPS napló részletessége növelhető a konfigurációs fájl (lásd alább) LogLevel direktívájának „debug” vagy akár a mindent naplózó „debug2” értékre állításával az alapértelmezett „info” helyett. Ha ezt elvégzi, ne feledje el a hiba elhárítása után visszaállítani a naplózási szintet a naplófájl túl nagyra hízása elkerüléséhez.

3.2. Beállítás

A CUPS-kiszolgáló viselkedése az `/etc/cups/cupsd.conf` fájl direktívái segítségével konfigurálható. A CUPS konfigurációs fájlja az Apache HTTP-kiszolgáló elsődleges konfigurációs fájljának szintaxisát követi, így az Apache konfigurációs fájlok szerkesztését ismerőknek nem fog meglepetést okozni. Itt bemutatunk néhány olyan beállítást, amelyek megváltoztatására szüksége lehet.

A konfigurációs fájl szerkesztése előtt készítsen róla másolatot és tegye írásvédetté, így referenciaként megmaradnak az eredeti beállítások, és szükség esetén újra felhasználhatja azokat.

A következő parancsok kiadásával másolja le az `/etc/cups/cupsd.conf` fájlt és tegye írásvédetté:

```
sudo cp /etc/cups/cupsd.conf /etc/cups/cupsd.conf.original
sudo chmod a-w /etc/cups/cupsd.conf.original
```

- ServerAdmin: a CUPS-kiszolgáló kijelölt adminisztrátorának e-mail címének megadásához szerkessze az `/etc/cups/cupsd.conf` fájlt, és vegye fel vagy szerkessze a ServerAdmin sort. Ha például a CUPS-kiszolgáló adminisztrátorának címe geza@példa.hu, akkor a ServerAdmin sor így fog kinézni:

```
ServerAdmin geza@példa.hu
```

- Listen: alapértelmezésben az Ubuntu CUPS-kiszolgálója csak a visszacsatolási felületen figyel, a 127.0.0.1 címen. Ahhoz, hogy a CUPS-kiszolgáló a tényleges hálózati csatoló IP-címén figyeljen, meg kell adnia a gépnevet, IP-címet vagy egy IP-cím/port párt a Listen direktívában. Ha például a CUPS-kiszolgáló a helyi hálózaton a 192.168.10.250 címen található, és elérhetővé szeretné tenni más rendszerek számára az adott alhálózaton, akkor az `/etc/cups/cupsd.conf` fájlt a következőképpen kell szerkesztenie, a Listen direktíva felvételével:

```
Listen 127.0.0.1:631           # meglévő loopback Listen direktíva
Listen /var/run/cups/cups.sock # meglévő socket Listen direktíva
Listen 192.168.10.250:631      # Listen direktíva a LAN csatolón, a 631-es (IPP) porton
```

  A fenti példában megjegyzésbe teheti vagy eltávolíthatja a visszacsatolási címre (127.0.0.1) hivatkozást, ha azt szeretné, hogy a cupsd ne figyeljen a helyi kérésekre, csak a helyi hálózat (LAN) Ethernet csatolóin érkezőkre. Egy adott gépnévhez tartozó összes csatoló (beleértve a visszacsatolásit is) figyeléséhez a következőhöz hasonló Listen bejegyzést kell létrehozni:

```
Listen példa:631  # A példa nevű gép összes csatolójának figyelése
```

  A Listen direktíva ki is hagyható, helyette használható a Port:

```
Port 631  # A 631-es port figyelése minden csatolón
```

A CUPS-kiszolgáló konfigurációs direktíváival kapcsolatos további példákért nézze meg a megfelelő kézikönyvoldalt, a következő parancs kiadásával:

```
man cupsd.conf
```

Az `/etc/cups/cupsd.conf` konfigurációs fájl minden módosításakor újra kell indítani a CUPS-kiszolgálót a következő parancs kiadásával:

```
sudo /etc/init.d/cups restart
```

3.3. Webes felület

A CUPS webes felület használatával is beállítható és monitorozható, ez alapértelmezésben a http://localhost:631/admin címen érhető el. A webes felületen az összes nyomtatókezelési feladat elvégezhető.

Az adminisztrációs feladatok webes felületen való végrehajtásához engedélyeznie kell a root fiókot a kiszolgálón, vagy az lpadmin csoport tagjaként kell bejelentkeznie. Biztonsági okokból a CUPS nem engedélyezi jelszóval nem rendelkező felhasználók bejelentkezését.

Felhasználó az lpadmin csoporthoz adásához adja ki a következő parancsot:

```
sudo usermod –aG lpadmin felhasználónév
```

További dokumentációk a webes felület Documentation/Help lapján érhetők el.

3.4. Hivatkozások

A CUPS weboldala[7]

Az Ubuntu wiki CUPS oldala[8]

[7] http://www.cups.org/

[8] https://help.ubuntu.com/community/cups

14. fejezet - E-mail szolgáltatások

Egy e-mail továbbítása a hálózaton vagy az interneten keresztül a feladótól a címzetthez számos rendszer együttműködését igényli. A folyamat megfelelő működéséhez ezen rendszerek mindegyikét megfelelően kell beállítani. A feladó egy levelezőklienst (MUA) használ a levél átküldéséhez legalább egy levéltovábbító ügynökön (MTA), amelyek közül az utolsó átadja egy levélkézbesítő ügynöknek (MDA) a címzett postafiókjába való kézbesítésre, amelyből a címzett levelezőkliense egy POP3- vagy IMAP-kiszolgáló segítségével lekéri.

1. Postfix

A Postfix az Ubuntu alapértelmezett levéltovábbító ügynöke (MTA). Célja, hogy gyors, egyszerűen adminisztrálható és biztonságos legyen. Kompatibilis a sendmail MTA-val. Ez a szakasz ismerteti a postfix telepítését és konfigurálását. Ismerteti még a(z e-mailek biztonságos küldéséhez) biztonságos kapcsolatot használó SMTP-kiszolgálóként való beállításának módját.

Ez a leírás nem ismerteti a Postfix virtuális tartományok beállítását, a virtuális tartományokkal és egyéb speciális lehetőségekkel kapcsolatban lásd a 1.7.3. szakasz - Hivatkozások [188] szakaszt.

1.1. Telepítés

A postfix telepítéséhez adja ki a következő parancsot:

```
sudo apt-get install postfix
```

Nyomja meg az Entert, ha a telepítő kérdéseket tesz fel, a beállításokat a következő lépésben, részletesebben végezzük el.

1.2. Alapszintű konfiguráció

A postfix konfigurálásához adja ki a következő parancsot:

```
sudo dpkg-reconfigure postfix
```

Megjelenik a felhasználói felület. Az egyes képernyőkön válassza az alábbi értékeket:

- Internetes hely
- mail.példa.hu
- geza
- mail.példa.hu, localhost.localdomain, localhost
- Nem
- 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128 192.168.0.0/24
- 0
- +
- mind

A mail.példa.hu helyére azt a tartományt írja, amelynek leveleit fogadja, a 192.168.0.0/24 helyére a levelezőkiszolgáló tényleges IP-címét és címosztályát, a geza helyére pedig a megfelelő felhasználónevet írja.

Ezután ki kell választani a használandó postafiók-formátumot. A Postfix alapértelmezésben az mbox formátumot használja. A konfigurációs fájl közvetlen szerkesztése helyett használhatja a postconf parancsot a postfix minden paraméterének beállítására. A konfigurációs paramétereket az `/etc/`

`postfix/main.cf` fájl tárolja. Ha később egy adott paramétert újra szeretne konfigurálni, akkor futtathatja a parancsot, vagy saját kezűleg is módosíthatja a fájlban.

A postafiók-formátum átállításához Maildir formátummá:

```
sudo postconf -e 'home_mailbox = Maildir/'
```

Ez az új leveleket a /home/felhasználónév/Maildir könyvtárba fogja helyezni, ezért a levélkézbesítő ügynököt (MDA) ugyanezen útvonal használatára kell beállítani.

1.3. SMTP hitelesítés

Az SMTP-AUTH lehetővé teszi a kliensek számára egy hitelesítési mechanizmus (SASL) segítségével történő azonosítást. A hitelesítési folyamat titkosítására a TLS-t kell használni. A hitelesítés után az SMTP-kiszolgáló engedélyezi a kliensnek a levelek továbbítását.

1. Állítsa be a Postfixet SMTP-AUTH-ra SASL (Dovecot SASL) használatával:

```
sudo postconf -e 'smtpd_sasl_type = dovecot'
sudo postconf -e 'smtpd_sasl_path = private/auth-client'
sudo postconf -e 'smtpd_sasl_local_domain ='
sudo postconf -e 'smtpd_sasl_security_options = noanonymous'
sudo postconf -e 'broken_sasl_auth_clients = yes'
sudo postconf -e 'smtpd_sasl_auth_enable = yes'
sudo postconf -e 'smtpd_recipient_restrictions = permit_sasl_authenticated,permit_mynetworks,re
sudo postconf -e 'inet_interfaces = all'
```

Az smtpd_sasl_path beállításba lévő útvonal a Postfix sorkönyvtárához képest értendő.

2. Ezután szerezzen be egy digitális tanúsítványt a TLS-hez. Részletekért lásd: 5. szakasz - Tanúsítványok [125]. Ez a példa is egy hitelesítésszolgáltatót (CA) használ. A CA-tanúsítvány előállításával kapcsolatos információkért lásd: 5.5. szakasz - Hitelesítésszolgáltató [127].

A digitális tanúsítványt beszerezheti egy hitelesítésszolgáltatótól. A webes kliensekkel ellentétben az SMTP-kliensek ritkán panaszkodnak az „önaláírt tanúsítványok” miatt, ezért saját kezűleg is létrehozhatja a tanúsítványt. További részletekért lásd: 5.3. szakasz - Önaláírású tanúsítvány létrehozása [127].

3. Ha megvan a tanúsítvány, állítsa be a Postfixet a TLS titkosítás biztosítására a bejövő és kimenő levelekhez:

```
sudo postconf -e 'smtpd_tls_auth_only = no'
sudo postconf -e 'smtp_use_tls = yes'
sudo postconf -e 'smtpd_use_tls = yes'
sudo postconf -e 'smtp_tls_note_starttls_offer = yes'
sudo postconf -e 'smtpd_tls_key_file = /etc/ssl/private/server.key'
sudo postconf -e 'smtpd_tls_cert_file = /etc/ssl/certs/server.crt'
```

```
sudo postconf -e 'smtpd_tls_loglevel = 1'
sudo postconf -e 'smtpd_tls_received_header = yes'
sudo postconf -e 'smtpd_tls_session_cache_timeout = 3600s'
sudo postconf -e 'tls_random_source = dev:/dev/urandom'
sudo postconf -e 'myhostname = mail.példa.hu'
```

4. Ha saját hitelesítésszolgáltatót használ a tanúsítvány aláírására, akkor adja ki a következőt:

   sudo postconf -e 'smtpd_tls_CAfile = /etc/ssl/certs/cacert.pem'

   A tanúsítványokkal kapcsolatos további részletekért lásd: 5. szakasz - Tanúsítványok [125].

A parancsok futtatása után a Postfix beállítása az SMTP-AUTH használatára kész, és létrejött egy önaláírt tanúsítvány a TLS titkosításhoz.

Ezután az `/etc/postfix/main.cf` fájlnak valahogy így[1] kell kinéznie.

A Postfix kiinduló beállítása kész. Futtassa a következő parancsot a postfix démon újraindításához:

```
sudo /etc/init.d/postfix restart
```

A Postfix támogatja az RFC2554[2] által meghatározott SMTP-AUTH-ot. Ennek alapja a SASL[3]. Az SMTP-AUTH használatához ennek ellenére szükség van a SASL hitelesítés beállítására.

1.4. SASL beállítása

A Postfix két SASL-megvalósítást támogat, ezek a Cyrus SASL és Dovecot SASL. A Dovecot SASL engedélyezéséhez telepíteni kell a dovecot-common csomagot. Adja ki a következő parancsot:

```
sudo apt-get install dovecot-common
```

Az `/etc/dovecot/dovecot.conf` fájlt kell szerkesztenie. Az auth default szakaszban vegye ki megjegyzésből a socket listen beállítást, és módosítsa a következőt:

```
socket listen {
  #master {
    # Master socket provides access to userdb information. It's typically
    # used to give Dovecot's local delivery agent access to userdb so it
    # can find mailbox locations.
    #path = /var/run/dovecot/auth-master
    #mode = 0600
    # Default user/group is the one who started dovecot-auth (root)
    #user =
    #group =
  #}
```

[1] ../sample/postfix_configuration

[2] ftp://ftp.isi.edu/in-notes/rfc2554.txt

[3] ftp://ftp.isi.edu/in-notes/rfc2222.txt

```
    client {
      # The client socket is generally safe to export to everyone. Typical use
      # is to export it to your SMTP server so it can do SMTP AUTH lookups
      # using it.
      path = /var/spool/postfix/private/auth-client
      mode = 0660
      user = postfix
      group = postfix
    }
  }
```

Ahhoz hogy az Outlook kliensek SMTPAUTH-ot használhassanak, az /etc/dovecot/dovecot.conf auth default szakaszához adja hozzá a „login” lehetőséget:

```
  mechanisms = plain login
```

A Dovecot beállítása után indítsa újra azt:

```
sudo /etc/init.d/dovecot restart
```

1.5. Postfix-Dovecot

A másik lehetőség a Postfix SMTP-AUTH használatára való beállításának a dovecot-postfix csomag. Ez a csomag telepíti a Dovecotot, és beállítja a Postfixet ennek használatára a SASL-hitelesítésre és levélkézbesítő ügynökként (MDA) is. A csomag beállítja a Dovecotot IMAP, IMAPS, POP3 és POP3S használatához is.

Az IMAP, IMAPS, POP3 vagy POP3S futtatása a felhasználási módtól függően lehet szükséges vagy fölösleges a levelezőkiszolgálón. Levélátjáró, spam/vírusszűrő stb. esetén egyszerűbb lehet a fenti parancsok használata a Postfix beállítására SMTPAUTH használatához.

A csomag telepítéséhez adja ki a következő parancsot:

```
sudo apt-get install dovecot-postfix
```

Ezzel rendelkezésére áll egy működő levelezőkiszolgáló, de még van néhány beállítás, amelyek módosítása szükséges lehet. A csomag például az ssl-cert csomag tanúsítványát és kulcsát használja. Éles környezetben az adott géphez generált tanúsítványt és kulcsot kell használni. További részletekért lásd: 5. szakasz - Tanúsítványok [125].

Miután előállította a tanúsítványt és kulcsot a géphez, módosítsa a következő beállításokat az `/etc/postfix/main.cf` fájlban:

```
smtpd_tls_cert_file = /etc/ssl/certs/ssl-mail.pem
smtpd_tls_key_file = /etc/ssl/private/ssl-mail.key
```

Majd indítsa újra a Postfixet:

```
sudo /etc/init.d/postfix restart
```

1.6. Tesztelés

Az SMTP-AUTH beállítása kész, ideje kipróbálni a működését.

Az SMTP-AUTH és a TLS megfelelő működésének ellenőrzéséhez adja ki a következő parancsot:

```
telnet mail.példa.hu 25
```

Miután létrejött a kapcsolat a postfix levelezőkiszolgálóhoz, írja be a következőt:

```
ehlo mail.példa.hu
```

Ha egyebek mellett az alábbi sorokat látja, akkor minden megfelelően működik. A kilépéshez írja be a quit parancsot.

```
250-STARTTLS
250-AUTH LOGIN PLAIN
250-AUTH=LOGIN PLAIN
250 8BITMIME
```

1.7. Hibaelhárítás

Ez a szakasz néhány általános módszert ismertet a hibák okainak meghatározására.

1.7.1. Menekülés a chrootból

Az Ubuntu postfix csomagja biztonsági okból alapértelmezésben egy chroot környezetbe települ. Ez hibaelhárításkor növeli az összetettséget.

A chroot-beli működés kikapcsolásához keresse meg a következő sort az `/etc/postfix/master.cf` konfigurációs fájlban:

```
smtp      inet  n       -       -       -       -       smtpd
```

és módosítsa a következőképpen:

```
smtp      inet  n       -       n       -       -       smtpd
```

Az új beállítások használatához újra kell indítani a Postfixet. Adja ki a következő parancsot:

```
sudo /etc/init.d/postfix restart
```

1.7.2. Naplófájlok

A Postfix minden naplóüzenetet a `/var/log/mail.log` fájlba küld. Azonban a hiba- és figyelmeztető üzenetek néha elveszhetnek a normál naplókimenetben, ezért a `/var/log/mail.err` és `/var/log/mail.warn` fájlokba is naplózásra kerülnek.

A naplókba bevitt üzenetek valós idejű megjelenítéséhez használhatja a tail -f parancsot:

```
tail -f /var/log/mail.err
```

A naplóban rögzített részletek mennyisége növelhető. Alább látható néhány beállítás a fent ismertetett területek naplózási szintjének növeléséhez.

- A TLS aktivitás naplózásának növeléséhez állítsa az smtpd_tls_loglevel beállítást 1 és 4 közötti értékre.

```
sudo postconf -e 'smtpd_tls_loglevel = 4'
```

- Ha nem tud egy adott tartományba levelet küldeni, vagy onnan fogadni, akkor felveheti a tartományt a debug_peer_list paraméterbe.

```
sudo postconf -e 'debug_peer_list = problem.domain'
```

- Bármely Postfix démon folyamat részletességét növelheti az `/etc/postfix/master.cf` szerkesztésével, és a -v bejegyzéshez fűzésével. Szerkessze például az smtp bejegyzést:

```
smtp      unix  -       -       -       -       -       smtp -v
```

Fontos megjegyezni, hogy a fenti naplózási módosítások végrehajtása után azok életbe léptetéséhez újra kell indítani a Postfix folyamatot: sudo /etc/init.d/postfix reload

- A SASL-problémák elhárításakor naplózott információk mennyiségének növeléséhez megadhatja a következő beállításokat az `/etc/dovecot/dovecot.conf` fájlban:

```
auth_debug=yes
auth_debug_passwords=yes
```

A Postfixhoz hasonlóan a Dovecot beállításainak módosításakor azt is újra kell indítani: sudo /etc/init.d/dovecot reload.

A fenti beállítások némelyike jelentősen növeli a naplófájlokba küldött információk mennyiségét. Ne feledje el a hiba megszüntetése után visszaállítani a naplózási szintet a normálisra, illetve az új beállítások életbe léptetéséhez újraindítani a démont.

1.7.3. Hivatkozások

Egy Postfix kiszolgáló adminisztrálása nagyon bonyolult feladat lehet. Előbb-utóbb eljuthat arra a pontra, amikor az Ubuntu közösség segítségét kell kérnie.

A Postfix problémák felvetésére, és az Ubuntu kiszolgáló közösség életébe való bekapcsolódásra remek hely a freenode[4] #ubuntu-server IRC-csatornája. A webes fórumok[5] egyikén is felteheti kérdéseit.

A Postfix mélyebb megismeréséhez az Ubuntu fejlesztői a The Book of Postfix[6] című könyvet ajánlják.

Végül a Postfix[7] weboldala is remek dokumentációkkal rendelkezik a rendelkezésre álló konfigurációs lehetőségekkel kapcsolatban.

Az Ubuntu wiki Postifx[8] oldala is tartalmaz további információkat.

[4] http://freenode.net

[5] http://www.ubuntu.com/support/community/webforums

[6] http://www.postfix-book.com/

[7] http://www.postfix.org/documentation.html

[8] https://help.ubuntu.com/community/Postfix

2. Exim4

Az Exim4 egy másik levéltovábbító ügynök (MTA), amelyet az University of Cambridge fejlesztett ki az internetre kapcsolt Unix rendszereken való használatra. Az Exim telepíthető a sendmail helyett, noha az exim konfigurációja meglehetősen eltér a sendmail konfigurációjától.

2.1. Telepítés

Az exim4 telepítéséhez adja ki a következő parancsot:

```
sudo apt-get install exim4
```

2.2. Beállítás

Az Exim4 beállításához futtassa a következő parancsot:

```
sudo dpkg-reconfigure exim4-config
```

Megjelenik a felhasználói felület, amely számos paraméter konfigurálását teszi lehetővé. Az Exim4 konfigurációs lehetőségei például több fájlba vannak szétosztva. Ha ezeket inkább egy fájlban szeretné látni, ezen a felületen beállíthatja.

A felületen beállítható összes paraméter az `/etc/exim4/update-exim4.conf.conf` fájlban található. Ha módosítani szeretné a beállításokat, akkor újrafuttathatja a beállítóvarázslót, vagy saját kezűleg szerkesztheti a fájlt kedvenc szerkesztőjével. A konfigurálás után a következő parancs futtatásával állíthatja elő az elsődleges konfigurációs fájlt:

```
sudo update-exim4.conf
```

Az elsődleges konfigurációs fájl a `/var/lib/exim4/config.autogenerated` fájlba kerül előállításra és tárolásra.

A `/var/lib/exim4/config.autogenerated` elsődleges konfigurációs fájlt soha ne szerkessze saját kezűleg. Ez az update-exim4.conf minden futtatásakor automatikusan frissítésre kerül.

A következő paranccsal indíthatja el az Exim4 démont.

```
sudo /etc/init.d/exim4 start
```

2.3. SMTP hitelesítés

Ez a szakasz az Exim4 beállítását ismerteti SMTP-AUTH használatára TLS és SASL titkosítással.

Az első lépés a TLS-sel használandó tanúsítvány előállítása. Adja ki a következő parancsot:

```
sudo /usr/share/doc/exim4-base/examples/exim-gencert
```

Ezután be kell állítani az Exim4-et a TLS használatára az `/etc/exim4/conf.d/main/03_exim4-config_tlsoptions` fájl szerkesztésével. Vegye fel a következőt:

```
MAIN_TLS_ENABLE = yes
```

Következő lépésként be kell állítania az Exim4-et a saslauthd használatára hitelesítéshez. Szerkessze az `/etc/exim4/conf.d/auth/30_exim4-config_examples` fájlt, és vegye ki megjegyzésből a plain_saslauthd_server és login_saslauthd_server szakaszokat:

```
 plain_saslauthd_server:
   driver = plaintext
   public_name = PLAIN
   server_condition = ${if saslauthd{{$auth2}{$auth3}}{1}{0}}
   server_set_id = $auth2
   server_prompts = :
   .ifndef AUTH_SERVER_ALLOW_NOTLS_PASSWORDS
   server_advertise_condition = ${if eq{$tls_cipher}{}{}{*}}
   .endif
#
 login_saslauthd_server:
   driver = plaintext
   public_name = LOGIN
   server_prompts = "Username:: : Password::"
   # don't send system passwords over unencrypted connections
   server_condition = ${if saslauthd{{$auth1}{$auth2}}{1}{0}}
   server_set_id = $auth1
   .ifndef AUTH_SERVER_ALLOW_NOTLS_PASSWORDS
   server_advertise_condition = ${if eq{$tls_cipher}{}{}{*}}
   .endif
```

Végül frissítse az Exim4 beállításait, és indítsa újra a szolgáltatást:

```
sudo update-exim4.conf
sudo /etc/init.d/exim4 restart
```

2.4. SASL beállítása

Ez a szakasz a saslauthd az Exim4 számára hitelesítés biztosítására való beállításával kapcsolatos részleteket tartalmaz.

Az első lépés a sasl2-bin csomag telepítése. Adja ki a következő parancsot:

```
sudo apt-get install sasl2-bin
```

A saslauthd beállításához szerkessze az /etc/default/saslauthd konfigurációs fájlt, és módosítsa a START=no sort:

```
START=yes
```

Ezután a Debian-exim felhasználót a sasl csoport részévé kell tenni ahhoz, hogy az Exim4 használni tudja a saslauthd szolgáltatást:

```
sudo adduser Debian-exim sasl
```

Majd indítsa el a saslauthd szolgáltatást:

```
sudo /etc/init.d/saslauthd start
```

Az Exim4 beállítása TLS és SASL hitelesítést támogató SMTP-AUTH használatára ezzel kész.

2.5. Hivatkozások

- További információkért lásd az exim.org[9] oldalt.
- Elérhető egy Exim4 könyv[10] is.
- Másik hasznos információforrás az Ubuntu wiki Exim4[11] oldala.

3. Dovecot kiszolgáló

A Dovecot egy levélkézbesítő ügynök (MDA), amelyet a biztonságot szem előtt tartva írtak. Támogatja a népszerű postafiók-formátumokat, az mboxot és a Maildirt. Ez a szakasz ismerteti az IMAP vagy POP3 kiszolgálóként való beállítását.

3.1. Telepítés

A dovecot telepítéséhez adja ki a következő parancsot:

```
sudo apt-get install dovecot-imapd dovecot-pop3d
```

3.2. Beállítás

A dovecot beállításához szerkesztheti az `/etc/dovecot/dovecot.conf` fájlt. Kiválaszthatja a használandó protokollt, ez a pop3, pop3s (biztonságos pop3), imap és imaps (biztonságos imap) lehet. Ezen protokollok leírása meghaladja jelen útmutató lehetőségeit, ezekkel kapcsolatos információkért lásd a POP3[12] és IMAP[13] wikipédia cikkeket.

Az IMAPS és POP3S biztonságosabb az egyszerű IMAP és POP3 protokollnál, mivel SSL-titkosítást használnak a kapcsolódáshoz. A protokoll kiválasztása után módosítsa a következő sort az `/etc/dovecot/dovecot.conf` fájlban:

```
protocols = pop3 pop3s imap imaps
```

Ezután válassza ki a használni kívánt postafiókot. A Dovecot a maildir és mbox formátumokat támogatja. Mindkettőnek megvannak a maga előnyei, ezeket a Dovecot weboldalán[14] ismerheti meg.

A postafióktípus kiválasztása után szerkessze az `/etc/dovecot/dovecot.conf` fájlt, és módosítsa a következő sort:

```
mail_location = maildir:~/Maildir # (for maildir)
vagy
mail_location = mbox:~/mail:INBOX=/var/spool/mail/%u # (for mbox)
```

Állítsa be levéltovábbító ügynökét (MTA) a bejövő levelek ilyen típusú postafiókba továbbítására, ha az eltér a beállítottól.

A Dovecot beállítása után indítsa újra a dovecot démont a beállítások teszteléséhez:

```
sudo /etc/init.d/dovecot restart
```

[12] http://en.wikipedia.org/wiki/POP3

[13] http://en.wikipedia.org/wiki/Internet_Message_Access_Protocol

[14] http://wiki.dovecot.org/MailboxFormat

Ha engedélyezte az imap vagy pop3 egyikét, akkor megpróbálhat bejelentkezni a telnet localhost pop3 vagy telnet localhost imap2 parancsot egyikével. Ha a következőhöz hasonlót lát, akkor a telepítés sikeres volt:

```
bhuvan@rainbow:~$ telnet localhost pop3
Trying 127.0.0.1...
Connected to localhost.localdomain.
Escape character is '^]'.
+OK Dovecot ready.
```

3.3. Dovecot SSL beállítása

A dovecot SSL használatára való beállításához szerkesztheti az `/etc/dovecot/dovecot.conf` fájlt, és módosíthatja a következő sorokat:

```
ssl_cert_file = /etc/ssl/certs/ssl-cert-snakeoil.pem
ssl_key_file = /etc/ssl/private/ssl-cert-snakeoil.key
ssl_disable = no
disable_plaintext_auth = no
```

A digitális tanúsítványt beszerezheti egy hitelesítésszolgáltatótól, vagy előállíthatja saját kezűleg. Az utóbbi e-mailek esetén megfelelő, mivel az SMTP-kliensek ritkán panaszkodnak az „önaláírt tanúsítványok” miatt, ezért saját kezűleg is létrehozhatja a tanúsítványt. Az önaláírt SSL-tanúsítvány előállításával kapcsolatos további részletekért lásd: 5.3. szakasz - Önaláírású tanúsítvány létrehozása [127]. A tanúsítvány létrehozása után kap egy kulcsfájlt és egy tanúsítványfájlt. Másolja ezeket az `/etc/dovecot/dovecot.conf` konfigurációs fájlban megadott helyre.

3.4. Tűzfalbeállítások e-mail kiszolgálóhoz

A levelezőkiszolgáló másik számítógépről való eléréséhez engedélyeznie kell tűzfalán a kiszolgálóra irányuló kapcsolatokat a megfelelő portokon.

- IMAP - 143
- IMAPS - 993
- POP3 - 110
- POP3S - 995

3.5. Hivatkozások

- További információkért lásd a Dovecot weboldalát[15].
- Az Ubuntu wiki Dovecot[16] oldala is tartalmaz további részleteket.

4. Mailman

A Mailman egy nyílt forrású program levelezőlisták és hírlevelek kezelésére. Számos nyílt forrású levelezőlista (beleértve az összes Ubuntu levelezőlistát[17]) a Mailmant használja levelezőlista-szoftverként. Hatékony és egyszerű telepíteni és karbantartani.

4.1. Telepítés

A Mailman webes felületet biztosít az adminisztrátoroknak és felhasználóknak, az e-mailek küldésére és fogadására pedig külső levelezőkiszolgálót használ. Tökéletesen működik a következő levelezőkiszolgálókkal:

- Postfix
- Exim
- Sendmail
- Qmail

Ez a szakasz bemutatja a Mailman telepítését és beállítását az Apache webkiszolgálóval és a Postfix vagy Exim levelezőkiszolgálóval. Ha a Mailmant másik levelezőkiszolgálóval szeretné telepíteni, akkor nézze meg a Hivatkozások szakaszt.

Csak egy levelezőkiszolgálót kell telepítenie, és a Postfix az Ubuntu alapértelmezett levéltovábbító ügynöke.

4.1.1. Apache2

Az Apache2 telepítésével kapcsolatos részletekért lásd a HTTPD telepítése[18] szakaszt.

4.1.2. Postfix

A Postfix telepítésével és beállításával kapcsolatos részletekért lásd: 1. szakasz - Postfix [183].

4.1.3. Exim4

Az Exim4 telepítésével kapcsolatban lásd: 2. szakasz - Exim4 [190].

Az exim4 telepítése után a konfigurációs fájlok az `/etc/exim4` könyvtárba kerülnek. Az Ubuntuban alapértelmezésben az exim4 konfigurációs beállításai több fájlba vannak szétosztva. Ezt a viselkedést a következő változó módosításával változtathatja meg az `/etc/exim4/update-exim4.conf` fájlban:

- dc_use_split_config='true'

4.1.4. Mailman

A Mailman telepítéséhez futtassa a következő parancsot:

[17] http://lists.ubuntu.com

[18] ./web-servers.xml#http-installation

```
sudo apt-get install mailman
```

Ez átmásolja a telepítőfájlokat a /var/lib/mailman, a CGI parancsfájlokat pedig a /usr/lib/cgi-bin/mailman könyvtárba, és létrehozza a list felhasználót és list csoportot. A mailman folyamatot ez a felhasználó fogja birtokolni.

4.2. Beállítás

Ez a szakasz feltételezi, hogy sikeresen telepítette a mailman, apache2 és a postfix vagy exim4 csomagokat. Már csak be kell állítani ezeket.

4.2.1. Apache2

A Mailman tartalmaz egy példa Apache2 konfigurációs fájlt, amely az `/etc/mailman/apache.conf` alatt található. Ahhoz, hogy az Apache használatba vegye ezt a konfigurációs fájlt, át kell másolni az `/etc/apache2/sites-available` könyvtárba:

```
sudo cp /etc/mailman/apache.conf /etc/apache2/sites-available/mailman.conf
```

Ez egy új Apache2 VirtualHost-ot állít be a Mailman adminisztrációs oldalához. Most engedélyezze az új beállításokat, és indítsa újra az Apache2-t:

```
sudo a2ensite mailman.conf
sudo /etc/init.d/apache2 restart
```

A Mailman az Apache2 használatával jeleníti meg CGI-parancsfájljait. A Mailman CGI-parancsfájlok a /usr/lib/cgi-bin/mailman könyvtárban találhatók. A Mailman URL-címe így http://gépnév/cgi-bin/mailman/ lesz. Ezt az `/etc/apache2/sites-available/mailman.conf` fájlban változtathatja meg.

4.2.2. Postfix

A Postfix integrációhoz a lists.példa.hu tartományt társítjuk a levelezőlistákhoz. A lists.példa.hu helyett a saját tartományát használja.

A szükséges beállítások `/etc/postfix/main.cf` fájlhoz adására használhatja a postconf parancsot:

```
sudo postconf -e 'relay_domains = lists.példa.hu'
sudo postconf -e 'transport_maps = hash:/etc/postfix/transport'
sudo postconf -e 'mailman_destination_recipient_limit = 1'
```

Ellenőrizze, hogy az `/etc/postfix/master.cf` fájlban megvan a következő átvitel:

```
mailman   unix  -       n       n       -       -       pipe
  flags=FR user=list argv=/usr/lib/mailman/bin/postfix-to-mailman.py
  ${nexthop} ${user}
```

Ez meghívja a postfix-to-mailman.py parancsfájlt, amikor a lista levelet kap.

Az átvitelleképezéssel társítsa a lists.példa.hu tartományt a Mailman átvitelhez. Szerkessze az `/etc/postfix/transport` fájlt:

```
lists.példa.hu      mailman:
```

A következő parancs kiadásával építtesse fel a Postfix-szel az átvitelleképezést:

```
sudo postmap -v /etc/postfix/transport
```

Végül indítsa újra a Postfixet az új beállítások életbe léptetéséhez:

```
sudo /etc/init.d/postfix restart
```

4.2.3. Exim4

Az Exim4 telepítése után a következő parancs kiadásával indíthatja el az Exim kiszolgálót:

```
sudo /etc/init.d/exim4 start
```

A Mailman és az Exim4 együttműködéséhez be kell állítania az Exim4-et. Ahogy korábban említettük, az Exim4 több különböző típusú konfigurációs fájlt használ. Részletekért lásd az Exim[19] weboldalát. A Mailman futtatásához új konfigurációs fájlt kell felvenni a következő típusokhoz:

- Elsődleges
- Átvitel
- Útválasztó

Az Exim ezen mini konfigurációs fájlok rendezésével előállít egy elsődleges konfigurációs fájlt. Emiatt a konfigurációs fájlok sorrendje nagyon fontos.

4.2.4. Elsődleges

Az elsődleges típusba tartozó összes konfigurációs fájl az `/etc/exim4/conf.d/main/` könyvtárban található. Az alábbi tartalmat egy `04_exim4-config_mailman` nevű új fájlba vegye fel:

```
# start
# Home dir for your Mailman installation -- aka Mailman's prefix
# directory.
# On Ubuntu this should be "/var/lib/mailman"
# This is normally the same as ~mailman
MM_HOME=/var/lib/mailman
#
```

[19] http://www.exim.org

```
# User and group for Mailman, should match your --with-mail-gid
# switch to Mailman's configure script.  Value is normally "mailman"
MM_UID=list
MM_GID=list
#
# Domains that your lists are in - colon separated list
# you may wish to add these into local_domains as well
domainlist mm_domains=hostname.com
#
# -=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
#
# These values are derived from the ones above and should not need
# editing unless you have munged your mailman installation
#
# The path of the Mailman mail wrapper script
MM_WRAP=MM_HOME/mail/mailman
#
# The path of the list config file (used as a required file when
# verifying list addresses)
MM_LISTCHK=MM_HOME/lists/${lc::$local_part}/config.pck
# end
```

4.2.5. Átvitel

Az átvitel típusba tartozó összes konfigurációs fájl az `/etc/exim4/conf.d/transport/` könyvtárban található. Az alábbi tartalmat egy `40_exim4-config_mailman` nevű új fájlba vegye fel:

```
  mailman_transport:
   driver = pipe
   command = MM_WRAP \
               '${if def:local_part_suffix \
                     {${sg{$local_part_suffix}{-(\\w+)(\\+.*)?}{\$1}}} \
                     {post}}' \
               $local_part
    current_directory = MM_HOME
    home_directory = MM_HOME
    user = MM_UID
    group = MM_GID
```

4.2.6. Útválasztó

Az útválasztó típusba tartozó összes konfigurációs fájl az `/etc/exim4/conf.d/router/` könyvtárban található. Az alábbi tartalmat egy `101_exim4-config_mailman` nevű új fájlba vegye fel:

```
  mailman_router:
   driver = accept
   require_files = MM_HOME/lists/$local_part/config.pck
   local_part_suffix_optional
   local_part_suffix = -bounces : -bounces+* : \
                       -confirm+* : -join : -leave : \
                       -owner : -request : -admin
```

```
transport = mailman_transport
```

Az elsődleges és az átvitel típusú konfigurációs fájlok sorrendje tetszőleges lehet. Az útválasztó konfigurációs fájlok sorrendjének azonosnak kell lennie. Ennek a fájlnak a 200_exim4-config_primary fájl előtt kell megjelennie. Ez a két konfigurációs fájl azonos típusú információkat tartalmaz. Az első fájlnak elsőbbsége van. További részletekért lásd a hivatkozások szakaszt.

4.2.7. Mailman

A mailman telepítése után a következő paranccsal futtathatja:

```
sudo /etc/init.d/mailman start
```

A mailman telepítése után létre kell hoznia az alapértelmezett levelezőlistát. Ehhez adja ki a következő parancsot:

```
sudo /usr/sbin/newlist mailman
```

```
Enter the email address of the person running the list: bhuvan at ubuntu.com
Initial mailman password:
To finish creating your mailing list, you must edit your /etc/aliases (or
equivalent) file by adding the following lines, and possibly running the
`newaliases' program:

## mailman mailing list
mailman:              "|/var/lib/mailman/mail/mailman post mailman"
mailman-admin:        "|/var/lib/mailman/mail/mailman admin mailman"
mailman-bounces:      "|/var/lib/mailman/mail/mailman bounces mailman"
mailman-confirm:      "|/var/lib/mailman/mail/mailman confirm mailman"
mailman-join:         "|/var/lib/mailman/mail/mailman join mailman"
mailman-leave:        "|/var/lib/mailman/mail/mailman leave mailman"
mailman-owner:        "|/var/lib/mailman/mail/mailman owner mailman"
mailman-request:      "|/var/lib/mailman/mail/mailman request mailman"
mailman-subscribe:    "|/var/lib/mailman/mail/mailman subscribe mailman"
mailman-unsubscribe:  "|/var/lib/mailman/mail/mailman unsubscribe mailman"

Hit enter to notify mailman owner...

#
```

A Postfix vagy az Exim4 be lett állítva a Mailman e-mailjeinek felismerésére. Emiatt nem kötelező új bejegyzéseket létrehozni az `/etc/aliases` fájlban. Ha módosította a konfigurációs fájlokat, akkor ne feledje újraindítani a szolgáltatást a következő szakaszra lépés előtt.

Az Exim4 nem a fenti álneveket használja a levelek Mailmanhez továbbítására, mivel a felderítéses megközelítést használja. Az álnevek a lista létrehozásakor történő elnyomásához felveheti az MTA=None sort a Mailman `/etc/mailman/mm_cfg.py` konfigurációs fájljába.

4.3. Adminisztráció

Feltételezzük, hogy alapértelmezett telepítést használ. A Mailman CGI-parancsfájlok az /usr/lib/cgi-bin/mailman/ könyvtárban találhatók. A Mailman webalapú adminisztrációt biztosít. Ezen oldal eléréséhez nyissa meg a következő oldalt a böngészőjében:

http://gépnév/cgi-bin/mailman/admin

Ezen a képernyőn megjelenik az alapértelmezett, mailman nevű levelezőlista. A levelezőlista nevére kattintva bekéri jelszavát. A helyes jelszó megadása után képes lesz a levelezőlista minden beállításának módosítására. A parancssori segédprogram (/usr/sbin/newlist) segítségével, vagy ennek alternatívájaként a webes felületen is létrehozhat új levelezőlistát.

4.4. Felhasználók

A Mailman a felhasználók számára webes felületet biztosít. Ezen oldal eléréséhez nyissa meg a következő oldalt a böngészőjében:

http://gépnév/cgi-bin/mailman/listinfo

Ezen a képernyőn megjelenik az alapértelmezett, mailman nevű levelezőlista. A levelezőlista nevére kattintva megjeleníti a feliratkozási űrlapot. Megadhatja e-mail címét, nevét (nem kötelező) és jelszavát a feliratkozáshoz. Ezután egy meghívó levelet fog kapni. A feliratkozáshoz kövesse az e-mail utasításait.

4.5. Hivatkozások

GNU Mailman – telepítési kézikönyv[20]

HOWTO - Using Exim 4 and Mailman 2.1 together[21]

Nézze meg az Ubuntu wiki Mailman[22] oldalát is.

[20] http://www.list.org/mailman-install/index.html
[21] http://www.exim.org/howto/mailman21.html
[22] https://help.ubuntu.com/community/Mailman

5. Levélszűrés

Manapság az e-mailekkel kapcsolatos legnagyobb problémák egyike a nemkívánatos tömeges levélszemét. Ezek a spam néven is ismert üzenetek vírusokat és egyéb rosszindulatú programokat tartalmazhatnak. Egyes jelentések szerint ezek az üzenetek teszik ki az internet e-mail forgalmának zömét.

This section will cover integrating Amavisd-new, Spamassassin, and ClamAV with the Postfix Mail Transport Agent (MTA). Postfix can also check email validity by passing it through external content filters. These filters can sometimes determine if a message is spam without needing to process it with more resource intensive applications. Two common filters are dkim-filter and python-policyd-spf.

- Az Amavisd-new egy átalakítóprogram, amely képes tetszőleges számú tartalomszűrő programot meghívni levélszemét-felismerési, víruskeresési stb. céllal.
- A Spamassassin számos mechanizmust használ az e-mailek szűrésére az üzenet tartalma alapján.
- A ClamAV egy nyílt forrású víruskereső alkalmazás.
- dkim-filter implements a Sendmail Mail Filter (Milter) for the DomainKeys Identified Mail (DKIM) standard.
- A python-policyd-spf engedélyezi a SPF-ellenőrzéseket a Postfix-szel.

A részek így illeszkednek:

- A Postfix fogadja az e-mailt.
- The message is passed through any external filters dkim-filter and python-policyd-spf in this case.
- Ezután az Amavisd-new feldolgozza az üzenetet.
- A ClamAV megvizsgálja az üzenetet. Ha az üzenet vírust tartalmaz, akkor a Postfix visszautasítja az üzenetet.
- A tiszta üzeneteket a Spamassassin elemzi, és eldönti hogy az levélszemét-e. A Spamassassin X-Header sorokat ad az üzenethez, lehetővé téve az Amavisd-new számára azok további manipulálását.

Ha például egy üzenet levélszemét-pontszáma ötven felett van, akkor az üzenet automatikusan kidobható a sorból, a címzett tudta nélkül. Másik lehetőség a megjelölt üzenetek kezelésére azok átadása a levelezőkliensnek, lehetővé téve a felhasználónak az üzenet ízlésének megfelelő kezelését.

5.1. Telepítés

A Postfix telepítésével és beállításával kapcsolatos utasításokért lásd: 1. szakasz - Postfix [183].

A további alkalmazások telepítéséhez adja ki a következő parancsokat:

```
sudo apt-get install amavisd-new spamassassin clamav-daemon
sudo apt-get install dkim-filter python-policyd-spf
```

A jobb levélszemét-felismerés érdekében telepíthető néhány, a Spamassassinba integrálódó csomag:

```
sudo apt-get install pyzor razor
```

A fő szűrőalkalmazások mellett tömörítő segédprogramok is szükségesek egyes e-mail mellékletek feldolgozásához.

```
sudo apt-get install arj cabextract cpio lha nomarch pax rar unrar unzip zip
```

Ha néhány csomag nem található, akkor az `/etc/apt/sources.list` fájlban ellenőrizze, hogy a multiverse tároló engedélyezve van-e.

Ha módosította a fájlt, a telepítés újrapróbálása előtt futtassa a sudo apt-get update parancsot.

5.2. Beállítás

Most beállíthatja a csomagokat az együttműködésre és az e-mailek szűrésére.

5.2.1. ClamAV

A ClamAV alapértelmezett viselkedése megfelel igényeinknek. A ClamAV további beállítási lehetőségeivel kapcsolatban nézze meg az `/etc/clamav` alatti konfigurációs fájlokat.

Vegye fel a clamav felhasználót az amavis csoportba ahhoz, hogy az Amavisd-new megfelelő hozzáféréssel rendelkezzen a fájlok vizsgálatához:

```
sudo adduser clamav amavis
```

5.2.2. Spamassassin

A Spamassassin automatikusan felismeri az elhagyható összetevőket, és használatba veszi a jelenlévőket. Ez azt jelenti, hogy nincs szükség a pyzor és razor konfigurálására.

A Spamassassin démon aktiválásához szerkessze az `/etc/default/spamassassin` fájlt. Módosítsa az ENABLED=0 értéket:

```
ENABLED=1
```

Most indítsa el a démont:

```
sudo /etc/init.d/spamassassin start
```

5.2.3. Amavisd-new

Első lépésként engedélyezze a levélszemét- és víruskeresést az Amavisd-new programban az `/etc/amavis/conf.d/15-content_filter_mode` szerkesztésével:

```
use strict;

# You can modify this file to re-enable SPAM checking through spamassassin
# and to re-enable antivirus checking.

#
# Default antivirus checking mode
# Uncomment the two lines below to enable it
#

@bypass_virus_checks_maps = (
   \%bypass_virus_checks, \@bypass_virus_checks_acl, \$bypass_virus_checks_re);


#
# Default SPAM checking mode
# Uncomment the two lines below to enable it
#

@bypass_spam_checks_maps = (
   \%bypass_spam_checks, \@bypass_spam_checks_acl, \$bypass_spam_checks_re);

1;  # insure a defined return
```

A levélszemét visszaküldése rossz ötlet, mivel a visszatérési cím gyakran hamis. Szerkessze az `/etc/amavis/conf.d/20-debian_defaults` fájlt, és állítsa a $final_spam_destiny változót D_BOUNCE helyett D_DISCARD értékűre a következőképpen:

```
$final_spam_destiny       = D_DISCARD;
```

Ezen kívül szüksége lehet az alábbi beállítások módosítására több üzenet megjelöléséhez levélszemétként:

```
$sa_tag_level_deflt = -999; # add spam info headers if at, or above that level
$sa_tag2_level_deflt = 6.0; # add 'spam detected' headers at that level
$sa_kill_level_deflt = 21.0; # triggers spam evasive actions
$sa_dsn_cutoff_level = 4; # spam level beyond which a DSN is not sent
```

Ha a kiszolgáló gépneve eltér a tartomány MX rekordjától, akkor szükség lehet a $myhostname beállítás módosítására. Ha a kiszolgáló több tartomány leveleit is fogadja, akkor a @local_domains_acl beállítást kell módosítani. Szerkessze az `/etc/amavis/conf.d/50-user` fájlt:

```
$myhostname = 'mail.példa.hu';
@local_domains_acl = ( "példa.hu", "példa.org" );
```

A beállítások módosítása után az Amavisd-new démont újra kell indítani:

```
sudo /etc/init.d/amavis restart
```

5.2.3.1. DKIM fehérlista

Az Amavisd-new beállítható azon címek automatikus fehérlistázására, amelyek érvényes tartománykulcsú tartományokból jönnek. Ezek az előre beállított tartományok az `/etc/amavis/conf.d/40-policy_banks` fájlban találhatók.

Egy tartomány fehérlistája több módon is beállítható:

- 'példa.hu' => 'WHITELIST',: minden címet fehérlistára tesz a „példa.hu” tartományból.
- '.példa.hu' => 'WHITELIST',: minden címet fehérlistára tesz a „példa.hu” altartományaiból, amelyek aláírása érvényes.
- '.példa.hu/@példa.hu' => 'WHITELIST',: fehérlistára teszi a „példa.hu” altartományait, amelyek a példa.hu szülőtartomány aláírását használják.
- './@példa.hu' => 'WHITELIST',: a „példa.hu” tartományból érvényes aláírással rendelkező címeket fehérlistázza. Ezt általában az üzeneteiket aláíró tagokkal rendelkező listákhoz használják.

Egy tartománynak több fehérlista-beállítása is lehet. A fájl szerkesztése után indítsa újra az amaisd-new démont:

```
sudo /etc/init.d/amavis restart
```

Ebben a kontextusban a fehérlistához adott tartományok üzenetein nem lesz vírus- vagy levélszemétszűrés végrehajtva. Ez lehet egyes tartományok esetén a kívánatos vagy a nem kívánatos viselkedés.

5.2.4. Postfix

A Postfix integrációhoz adja ki a következő parancsot:

```
sudo postconf -e 'content_filter = smtp-amavis:[127.0.0.1]:10024'
```

Ezután szerkessze az `/etc/postfix/master.cf` fájlt, és adja a következőket a fájl végéhez:

```
smtp-amavis     unix    -       -       -       -       2       smtp
        -o smtp_data_done_timeout=1200
        -o smtp_send_xforward_command=yes
        -o disable_dns_lookups=yes
        -o max_use=20

127.0.0.1:10025 inet    n       -       -       -       -       smtpd
        -o content_filter=
        -o local_recipient_maps=
        -o relay_recipient_maps=
        -o smtpd_restriction_classes=
        -o smtpd_delay_reject=no
        -o smtpd_client_restrictions=permit_mynetworks,reject
        -o smtpd_helo_restrictions=
```

```
        -o smtpd_sender_restrictions=
        -o smtpd_recipient_restrictions=permit_mynetworks,reject
        -o smtpd_data_restrictions=reject_unauth_pipelining
        -o smtpd_end_of_data_restrictions=
        -o mynetworks=127.0.0.0/8
        -o smtpd_error_sleep_time=0
        -o smtpd_soft_error_limit=1001
        -o smtpd_hard_error_limit=1000
        -o smtpd_client_connection_count_limit=0
        -o smtpd_client_connection_rate_limit=0
        -o receive_override_options=no_header_body_checks,no_unknown_recipient_checks
```

A következő két sort is vegye fel közvetlenül a "pickup" átviteli szolgáltatás alá:

```
         -o content_filter=
         -o receive_override_options=no_header_body_checks
```

Ez megakadályozza a levélszemétről küldött értesítő üzenetek levélszeméttéé nyilvánítását.

Most indítsa újra a Postfix démont:

```
sudo /etc/init.d/postfix restart
```

A levélszemét- és vírusfelismeréses tartalomszűrés ezzel engedélyezve lett.

5.3. Tesztelés

Első lépésként ellenőrizze, hogy az Amavisd-new SMTP figyel-e:

```
telnet localhost 10024
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
220 [127.0.0.1] ESMTP amavisd-new service ready
^]
```

A tartalomszűrőn átmenő üzenetek fejlécében a következőt kell látnia:

```
X-Spam-Level:
X-Virus-Scanned: Debian amavisd-new at példa.hu
X-Spam-Status: No, hits=-2.3 tagged_above=-1000.0 required=5.0 tests=AWL, BAYES_00
X-Spam-Level:
```

A kimenet változhat, de a fontos részt az X-Virus-Scanned és X-Spam-Status sorok képezik.

5.4. Hibaelhárítás

A hibák okainak meghatározásához a legjobb módszer a naplók ellenőrzése.

- A Postfix naplózásával kapcsolatos információkért lásd a 1.7. szakasz - Hibaelhárítás [187] szakaszt.
- Az Amavisd-new a Syslogot használja az üzenetek `/var/log/mail.log` fájlba küldésére. A részletesség szintje növelhető a $log_level beállítás `/etc/amavis/conf.d/50-user` fájlhoz adásával, és az érték 1 és 5 közé állításával.

```
$log_level = 2;
```

A Spamassassin naplókimenetének részletessége az Amavisd-new naplókimenetének részletességével együtt nő.

- A ClamAV naplókimenetének részletessége az `/etc/clamav/clamd.conf` szerkesztésével, és a következő beállítás megadásával növelhető:

```
LogVerbose true
```

Alapértelmezésben a ClamAV a `/var/log/clamav/clamav.log` fájlba küldi a naplóüzeneteit.

Az alkalmazások naplózási beállításainak módosítása után ne felejtse el újraindítani a szolgáltatást az új beállítások életbe léptetéséhez. Ha a hiba elhárítása sikerült, állítsa vissza a naplózási szintet az eredetire.

5.5. Hivatkozások

A levélszűréssel kapcsolatos további információért lásd:

- Amavisd-new dokumentáció[23]
- ClamAV dokumentáció[24] és ClamAV wiki[25]
- Spamassassin wiki[26]
- A Pyzor honlapja[27]
- A Razor honlapja[28]
- DKIM.org[29]
- Postfix Amavis New[30]

A freenode[31] #ubuntu-server IRC-csatornáján is nyugodtan felteheti kérdéseit.

[31] http://freenode.net

15. fejezet - Csevegőalkalmazások

1. Áttekintés

Ez a szakasz az ircd-irc2 IRC-kiszolgáló telepítését és beállítását ismerteti. Szintén szó lesz a Jabber azonnaliüzenő-kiszolgáló telepítéséről és beállításáról is.

2. IRC-kiszolgáló

Az Ubuntu tárolói számos IRC-kiszolgálót tartalmaznak. Ez a szakasz az eredeti, ircd-irc2 nevű IRC-kiszolgáló telepítését és beállítását ismerteti.

2.1. Telepítés

Az ircd-irc2 telepítéséhez adja ki a következő parancsot:

```
sudo apt-get install ircd-irc2
```

A konfigurációs fájlok az `/etc/ircd` könyvtárban találhatók, a dokumentáció pedig az `/usr/share/doc/ircd-irc2` könyvtárban.

2.2. Beállítás

Az IRC beállítása az `/etc/ircd/ircd.conf` fájlban végezhető el. Az IRC gépnév ebben a fájlban állítható be a következő sor szerkesztésével:

```
M:irc.localhost::Debian ircd default configuration::000A
```

Ne feledjen DNS-álneveket megadni az IRC-gépnévhez. Ha például az IRC-gépnévként az irc.livecipher.com címet adja meg, győződjön meg róla, hogy a névkiszolgálója képes az irc.livecipher.com feloldására. Az IRC-gépnév nem lehet azonos a gépnévvel.

Az IRC-admin adatai a következő sor szerkesztésével állíthatók be:

```
A:Organization, IRC dept.:Daemon <ircd@example.irc.org>:Client Server::IRCnet:
```

Külön sorokat kell felvennie a figyelendő IRC-portok listájának megadásához, az operátor hitelesítési adatainak megadásához, a klienshitelesítés konfigurálásához stb. A részletekért nézze meg az `/usr/share/doc/ircd-irc2/ircd.conf.example.gz` példa konfigurációs fájlt.

Az IRC-kliensben a felhasználó kiszolgálóhoz csatlakozásakor megjelenítendő IRC-fejléc az `/etc/ircd/ircd.motd` fájlban állítható be.

A konfigurációs fájl szükséges módosításainak végrehajtása után indítsa újra az IRC-kiszolgálót a következő paranccsal:

```
sudo /etc/init.d/ircd-irc2 restart
```

2.3. Hivatkozások

Érdeklődésére tarthatnak még számot az Ubuntu tárolókban elérhető további IRC-kiszolgálók, többek között az ircd-ircu és az ircd-hybrid.

- Az IRC-kiszolgálóval kapcsolatos további részletekért nézze meg az IRCD FAQ[1] oldalt.
- Az Ubuntu wiki IRCD[2] oldala is tartalmaz további információkat.

3. Jabber azonnaliüzenő-kiszolgáló

A Jabber egy népszerű azonnali üzenő protokoll, amely az azonnali üzenetküldés egyik nyílt szabványára, az XMPP-re épül, és számos népszerű alkalmazás használja. Ez a szakasz ismerteti egy Jabberd 2 kiszolgáló telepítését a helyi hálózatra. Ez a konfiguráció módosítható üzenetküldési szolgáltatás biztosítására az interneten elérhető felhasználók számára.

3.1. Telepítés

A jabberd2 csomag telepítéséhez adja ki a következő parancsot:

```
sudo apt-get install jabberd2
```

3.2. Beállítás

Számos XML konfigurációs fájl kerül felhasználásra a jabberd2 beállításához Berkely DB felhasználóhitelesítés használatára. Ez a hitelesítés egy nagyon egyszerű formája. A jabberd2 azonban beállítható LDAP, MySQL, Postgresql stb. használatára is a felhasználóhitelesítéshez.

Első lépésként szerkessze az `/etc/jabberd2/sm.xml` fájlt, módosítsa a következőt:

```
<id>jabber.példa.hu</id>
```

A jabber.példa.hu értéket helyettesítse a kiszolgáló gépnevével, vagy más azonosítójával.

Most a <storage> szakaszban módosítsa a <driver> értékét a következőre:

```
<driver>db</driver>
```

Szerkessze az `/etc/jabberd2/c2s.xml` fájlt, és módosítsa a <local> szakaszt:

```
<id>jabber.példa.hu</id>
```

Az <authreg> szakaszban módosítsa a <module> szakaszt a következőre:

```
<module>db</module>
```

Végül indítsa újra a jabberd2 démont az új beállítások életbe léptetéséhez:

```
sudo /etc/init.d/jabberd2 restart
```

Most már képesnek kell lennie a kiszolgálóhoz csatlakozásra egy Jabber-kliens, mint például a Pidgin használatával.

A Berkeley DB felhasználói adatokhoz való használatának előnye, hogy a konfigurálás után nincs szükség további karbantartásra. Ha a felhasználói fiókok és hitelesítési adatok fölött szorosabb ellenőrzésre van szüksége, akkor másik felhasználóhitelesítési módszer használata javasolt.

3.3. Hivatkozások

- A Jabberd2 weboldala[3] további információkat tartalmaz a Jabberd2 beállításával kapcsolatban.
- További hitelesítési beállításokért lásd a Jabberd2 Install Guide[4] oldalt.
- Az Ubuntu wiki Setting Up Jabber Server[5] oldala is tartalmaz további részleteket.

16. fejezet - Verziókezelő rendszerek

A verziókezelés az információk változásainak kezelése. Régóta kritikus eszköz programozók számára, akik jellemzően a szoftverek apró változtatásaival töltik idejüket, hogy aztán másnap visszavonják azokat. Azonban a verziókezelő rendszerek hasznossága messzire túlnyúlik a szoftverfejlesztői világ határain. A verziókezelésnek mindenütt létjogosultsága van, ahol a számítógépekkel gyakran változó információkat kezelnek.

1. Bazaar

A Bazaar egy új verziókövető rendszer, amelyet az Ubuntu mögött álló Canonical támogat. A Subversion és CVS rendszerekkel szemben a Bazaar támogatja az elosztott verziókezelést, lehetővé téve a hatékonyabb együttműködést. A Bazaart kifejezetten a nyílt forrású projektekben való közösségi részvétel szintjének maximalizálására tervezték.

1.1. Telepítés

A Bazaar telepítéséhez adja ki a következő parancsot:

```
sudo apt-get install bzr
```

1.2. Beállítás

A bemutatkozáshoz a bzr-nek, használja a whoami parancsot, a következőképpen:

```
$ bzr whoami 'Kovács János <kovacs.janos@gmail.com>'
```

1.3. A Bazaar megismerése

A Bazaar csomag alapértelmezésben a dokumentációt is tartalmazza az /usr/share/doc/bzr/html alatt. Ez az ismertető megfelelő kiindulópont. A bzr parancs is tartalmaz beépített súgót:

```
$ bzr help
```

Az izé parancs megismeréséhez például adja ki a következőt:

```
$ bzr help izé
```

1.4. Launchpad-integráció

Noha önálló rendszerként is nagyon hasznos, a Bazaar opcionális integrációval rendelkezik a Launchpadhoz[1], a Canonical és a szélesebb nyílt forrású közösség által az Ubuntu kezelésére és fejlesztésére használt kollaboratív fejlesztői rendszerhez. A Bazaar és a Launchpad nyílt forrású projekteken való együttműködésre történő együttes használatával kapcsolatos információkért nézze meg a http://bazaar-vcs.org/LaunchpadIntegration[2] oldalt.

[1] https://launchpad.net/

[2] http://bazaar-vcs.org/LaunchpadIntegration/

2. Subversion

A Subversion egy nyílt forrású verziókezelő rendszer. A Subversion segítségével forrásfájlok és dokumentumok előzményeit rögzítheti. Használatával a fájlok és könyvtárak időbeli változásait kezelheti. A fájlokat tartalmazó fa a központi tárolóban található. A tároló hasonlít egy átlagos fájlkiszolgálóra, kivéve hogy a fájlok és könyvtárak minden módosítását feljegyzi.

2.1. Telepítés

A Subversion tároló HTTP feletti eléréséhez telepítenie kell egy webkiszolgálót. Az Apache2 jól működik a Subversionnel. Az Apache2 telepítésével és beállításával kapcsolatos információkért nézze meg az Apache2 szakasz HTTP alszakaszát. A Subversion tároló HTTPS feletti eléréséhez digitális tanúsítványt kell telepítenie és beállítania az Apache2 webkiszolgálóra. A digitális tanúsítvány telepítésével és beállításával kapcsolatban nézze meg az Apache2 szakasz HTTPS alszakaszát.

A Subversion telepítéséhez adja ki a következő parancsot:

```
sudo apt-get install subversion libapache2-svn
```

2.2. A kiszolgáló beállítása

Ez a lépés feltételezi, hogy a fenti csomagokat telepítette a rendszerre. Ez a szakasz ismerteti a Subversion tároló létrehozásának, és a projekt elérésének módját.

2.2.1. Subversion tároló létrehozása

A Subversion tároló a következő parancs kiadásával hozható létre:

```
svnadmin create /tároló/útvonala/projekt
```

2.2.2. Fájlok importálása

A tároló létrehozása után fájlokat importálhat a tárolóba. A fájlokat tartalmazó könyvtár importálásához adja ki a következő parancsot:

```
svn import /importálandó/könyvtár/útvonala file:///tároló/útvonala/projekt
```

2.3. Hozzáférési módok

A Subversion tárolók számos különböző módon érhetők el - helyi lemezen vagy hálózati protokollok használatával. A tároló helye azonban mindig URL. Az alábbi táblázat leírja a különböző URL sémák leképezését az elérhető hozzáférési módszerekre.

16.1. táblázat - Hozzáférési módok

Séma	Hozzáférési mód
file://	közvetlen tárolóelérés (helyi lemezen)
http://	A Subversiont ismerő Apache2 webkiszolgáló elérése WebDAV protokollon keresztül
https://	Ugyanaz, mint a http://, de SSL titkosítással
svn://	svnserve kiszolgáló egyedi protokollon való elérése
svn+ssh://	Ugyanaz, mint az svn://, de SSH alagúton keresztül

Ez a szakasz ismerteti a Subversion beállításának módját az összes fenti hozzáférési módhoz. Itt csak az alapok kerülnek bemutatásra. A részletesebb használati utasításokat az svn könyvben[3] találja.

2.3.1. Közvetlen tároló-hozzáférés (file://)

Mind közül ez a legegyszerűbb hozzáférési módszer. Nem igényli Subversion kiszolgálófolyamatok futását. Ez a módszer a Subversion ugyanazon gépről való elérésére használható. A terminálba kiadott parancs szintaxisa a következő:

```
svn co file:///tároló/útvonala/projekt
```

vagy

```
svn co file://localhost/tárolók/útvonala/projekt
```

Ha nem adja meg a gépnevet, három osztásjelet (///) kell használni - kettő a protokollhoz (ebben az esetben file), egy pedig az útvonal kezdő osztásjele. Ha megadja a gépnevet, két osztásjelet (//) kell használni.

A tároló jogosultságai a fájlrendszer jogosultságaitól függenek. Ha a felhasználó rendelkezik írási/olvasási jogosultságokkal, lekérheti a fájlokat a tárolóból, és véglegesítheti is azokat.

2.3.2. Hozzáférés WebDAV protokollon (http://)

A Subversion tároló WebDAV protokollon keresztüli eléréséhez az Apache2 webkiszolgáló beállításait kell módosítani. Vegye fel a következő részletet a <VirtualHost> és </VirtualHost> elemek között az `/etc/apache2/sites-available/default`, vagy másik VirtualHost fájlba:

```
<Location /svn>
 DAV svn
```

[3] http://svnbook.red-bean.com/

```
  SVNPath /home/svn
  AuthType Basic
  AuthName "A tároló neve"
  AuthUserFile /etc/subversion/passwd
  Require valid-user
</Location>
```

A fenti beállítófájl-részlet feltételezi, hogy a Subversion tárolók a `/home/svn/` könyvtár alatt jöttek létre az svnadmin paranccsal. Ezután a http://gépnév/svn/tároló_neve URL-címen érhetők el.

A tárolót a HTTP felhasználónak kell birtokolnia a fájlok HTTP feletti importálásához vagy véglegesítéséhez a Subversion tárolóba. Ubuntu rendszereken a HTTP felhasználó általában a www-data. A tároló fájljai tulajdonosának módosításához adja ki a következő parancsot:

```
sudo chown -R www-data:www-data /tárolók/útvonala
```

A tároló tulajdonosának www-data-ra módosítása után nem lesz képes fájlok importálására vagy véglegesítésére a tárolóba az svn import file:/// parancs futtatásával a www-data-tól eltérő felhasználóval.

Ezután létre kell hoznia az `/etc/subversion/passwd` fájlt, amely majd a felhasználóhitelesítési adatokat tartalmazza. A fájl létrehozásához adja ki a következő parancsot (ez létrehozza a fájlt, és hozzáadja az első felhasználót):

```
sudo htpasswd -c /etc/subversion/passwd felhasználó_neve
```

További felhasználók felvételéhez hagyja el a „-c” kapcsolót, mivel ennek megadásakor a parancs helyettesíti a régi fájlt. Ehelyett a következő alakot használja:

```
sudo htpasswd /etc/subversion/password felhasználó_neve
```

Ez a parancs bekéri a jelszót. A jelszó megadása után a felhasználó felvételre kerül. Ezután a tároló elérhető a következő parancs futtatásával:

```
svn co http://kiszolgálónév/svn
```

A jelszó egyszerű szövegként kerül átvitelre. Ha a jelszó ellopása miatt aggódik, ajánlott SSL titkosítás használata. Ezt a következő szakasz részletezi.

2.3.3. Elérés WebDAV protokollon SSL titkosítással (https://)

A Subversion tároló WebDAV protokollon keresztüli elérése SSL titkosítással (https://) hasonló a http:// eléréshez, kivéve hogy digitális tanúsítványt kell telepítenie és beállítania az Apache2 webkiszolgálójához. Az SSL és a Subversion együttes használatához adja a fenti Apache2 beállításokat az `/etc/apache2/sites-available/default-ssl` fájlhoz. További információkért az Apache2 beállításáról az SSL használatára lásd 1.3. szakasz - A HTTPS beállítása [147] szakaszt.

Telepíthet egy aláíró hatóság által kibocsátott digitális tanúsítványt. Ennek alternatívájaként a saját aláírású tanúsítványt is telepítheti.

Ez a lépés feltételezi, hogy telepített és beállított egy digitális tanúsítványt az Apache2 webkiszolgálójához. Ezután a Subversion tároló eléréséhez nézze meg a fenti szakaszt. A hozzáférési módszerek a protokoll kivételével azonosak. A Subversion tároló eléréséhez a https:// protokollt kell használnia.

2.3.4. Elérés egyedi protokollon keresztül (svn://)

A Subversion tároló létrehozása után beállíthatja a hozzáférés-felügyeletet a `/tároló/útvonala/projekt/conf/svnserve.conf` fájl szerkesztésével. A hitelesítés beállításához például a beállítófájl következő sorait kell kivenni megjegyzésből:

```
# [general]
# password-db = passwd
```

A fenti sorok aktiválása után a passwd fájlban tarthatja karban a felhasználók listáját. Ugyanabban a könyvtárban szerkessze a `passwd` fájlt, és vegye fel az új felhasználót. A szintaxis a következő:

```
felhasználónév = jelszó
```

További részletekért nézze meg a fájlt.

Ezután a Subversion elérhető az egyéni svn:// protokollon, ugyanarról vagy másik gépről. Az SVN kiszolgáló az svnserve parancs kiadásával futtatható. A szintaxis a következő:

```
$ svnserve -d --foreground -r /tárolók/útvonala
# -d -- démon mód
# --foreground -- futtatás előtérben (hibakereséshez hasznos)
# -r -- kiszolgálandó könyvtár gyökere

A használattal kapcsolatos részletekért adja ki a következőt:
$ svnserve --help
```

A parancs futtatása után a Subversion elkezdi az alapértelmezett portot (3690) figyelni. A projekttároló eléréséhez futtassa a következő parancsot:

```
svn co svn://gépnév/projekt projekt --username felhasználó_neve
```

A kiszolgáló a beállításainak megfelelően bekéri a jelszót. A hitelesítés után lekéri a fájlokat a Subversion tárolóból. A projekt tárolójának és helyi másolatának szinkronizálásához futtassa az update részparancsot. A parancs szintaxisa a következő:

```
cd projekt_könyvtár ; svn update
```

Az egyes Subversion részparancsok használatával kapcsolatos további részletekért nézze meg a kézikönyvet. A co (checkout) paranccsal kapcsolatos információkért például adja ki a következő parancsot:

```
svn co help
```

2.3.5. Hozzáférés egyéni protokollon SSL titkosítással (svn+ssh://)

A beállítás és a kiszolgálófolyamat ugyanaz, mint az svn:// módszer esetén. Részletekért lásd a fenti szakaszt. Ez a lépés feltételezi, hogy követte a fenti szakaszt, és elindította a Subversion kiszolgálót az svnserve paranccsal.

Feltételezzük továbbá, hogy az SSH kiszolgáló fut a gépen, és engedélyezi a bejövő kapcsolatokat. Ennek ellenőrzéséhez próbáljon bejelentkezni a gépre SSH-val. Ha sikerül, minden rendben. Ellenkező esetben ezt a problémát meg kell oldani a folytatás előtt.

Az svn+ssh:// protokollt a Subversion tárolók SSL-lel titkosított eléréséhez használják. Az adatátvitel ezzel a módszerrel kerül titkosításra. A projekt tárolójának eléréséhez (példaként egy lekérés művelettel) a következő parancsszintaxist kell használnia:

```
svn co svn+ssh://gépnév/var/svn/tárolók/projekt
```

Ezzel a hozzáférési módszerrel a Subversion tároló eléréséhez a teljes útvonalat kell használnia (/tárolók/útvonala/projekt).

A kiszolgáló a beállításainak megfelelően bekéri a jelszót. Ekkor az SSH-n keresztüli belépéshez használt jelszót kell megadnia. A hitelesítés után lekéri a fájlokat a Subversion tárolóból.

3. CVS kiszolgáló

A CVS egy verziókövető rendszer. Segítségével forrásfájlok előzményei rögzíthetők.

3.1. Telepítés

A CVS telepítéséhez adja ki a következő parancsot:

```
sudo apt-get install cvs
```

A cvs telepítése után telepítenie kell az xinetd csomagot a CVS kiszolgáló indításához/leállításához. Az xinetd telepítéséhez adja ki a következő parancsot:

```
sudo apt-get install xinetd
```

3.2. Beállítás

A CVS telepítése után a tároló automatikusan előkészítésre kerül. Alapértelmezésben a tároló a /var/lib/cvs könyvtárba kerül. Ezt az útvonalat a következő parancs kiadásával módosíthatja:

```
cvs -d /az/új/cvs/tároló init
```

A kiindulási könyvtár beállítása után beállítható az xinetd a CVS kiszolgáló indítására. A következő sorokat átmásolhatja az `/etc/xinetd.d/cvspserver` fájlba.

```
service cvspserver
{
     port = 2401
     socket_type = stream
     protocol = tcp
     user = root
     wait = no
     type = UNLISTED
     server = /usr/bin/cvs
     server_args = -f --allow-root /var/lib/cvs pserver
     disable = no
}
```

Ne feledje el a tárolót szerkeszteni, ha módosította az alapértelmezett tárolókönyvtárat (/var/lib/cvs).

Az xinetd beállítása után elindítható a CVS kiszolgáló a következő parancs kiadásával:

```
sudo /etc/init.d/xinetd restart
```

A CVS kiszolgáló futását a következő parancs kiadásával ellenőrizheti:

```
sudo netstat -tap | grep cvs
```

A parancs futtatásakor a következő sort, vagy valami hasonlót kell látnia:

```
tcp        0      0 *:cvspserver            *:* LISTEN
```

Innentől felvehet felhasználókat, új projekteket és felügyelheti a CVS kiszolgálót.

A CVS lehetővé teszi a felhasználók felvételét az azt kiszolgáló operációs rendszertől függetlenül. A legegyszerűbb módszer valószínűleg a Linux felhasználóinak használata a CVS-hez, noha ennek vannak lehetséges biztonsági kockázatai. A részletekért nézze meg a CVS kézikönyvét.

3.3. Projektek felvétele

Ez a szakasz ismerteti, hogyan vehet fel új projektet a CVS tárolóba. Hozza létre a könyvtárat, és adja hozzá a kívánt dokumentációkat és forrásfájlokat. Ezután adja ki a következő parancsot a projekt felvételéhez a CVS tárolóba:

```
cd könyvtár/projekt
cvs -d :pserver:felhasználónév@gépnév.com:/var/lib/cvs import -m "A projekt importálása a CVS tárol
```

A CVSROOT környezeti változóban megadhatja a CVS gyökérkönyvtárának helyét. A CVSROOT környezeti változó exportálása után elkerülheti a cvs parancs -d kapcsolójának használatát.

Az új_projekt egy szállítói címke, a start pedig egy kiadáscímke. Ebben a környezetben nincs jelentőségük, de mivel a CVS megköveteli ezeket, jelen kell lenniük.

Új projekt hozzáadásakor a CVS felhasználónak írási jogokkal kell rendelkeznie a CVS tárolóhoz (/var/lib/cvs). Alapértelmezésben az src csoportnak van hozzáférése a CVS tárolóhoz. Először tehát ehhez a csoporthoz adja hozzá a felhasználókat, akik így kezelhetik a CVS tárolóban lévő projekteket.

4. Hivatkozások

A Bazaar honlapja[4]

Launchpad[5]

A Subversion honlapja[6]

Subversion könyv[7]

CVS kézikönyv[8]

Az Ubuntu wiki Easy Bazaar oldala[9]

Az Ubuntu wiki Subversion oldala[10]

[4] http://bazaar-vcs.org/
[5] https://launchpad.net/
[6] http://subversion.tigris.org/
[7] http://svnbook.red-bean.com/
[8] http://ximbiot.com/cvs/manual/cvs-1.11.21/cvs_toc.html
[9] https://help.ubuntu.com/community/EasyBazaar
[10] https://help.ubuntu.com/community/Subversion

17. fejezet - Windows hálózat

A számítógépes hálózatok gyakran vegyes rendszerekből állnak, és noha egy csak Ubuntu asztali és kiszolgáló gépekből álló hálózat működtetése bizonyára jó móka, számos hálózatnak együttműködő Ubuntu és Microsoft®Windows® rendszerekből kell állnia. Az Ubuntu kiszolgáló kézikönyv ezen szakasza bemutatja azokat az alapelveket és eszközöket, amelyekkel beállíthatja Ubuntu kiszolgálóját hálózati erőforrások windowsos számítógépekkel való megosztására.

1. Bevezetés

Az Ubuntu rendszer sikeres összekapcsolása Windows kliensekkel a Windows környezetekben általános szolgáltatások biztosítását és integrálását jelenti. Az ilyen szolgáltatások az adatok és információk megosztását segítik a hálózatban lévő számítógépekről és felhasználókról, és három fő szolgáltatáskategóriába sorolhatók:

- Fájl- és nyomtatómegosztási szolgáltatások. A Server Message Block (SMB) protokollt használja a fájlok, mappák, kötetek és nyomtatók hálózaton belüli megosztásának megkönnyítésére.
- Címtárszolgáltatások. Alapvető információk megosztása a hálózat számítógépeiről és felhasználóiról a Lightweight Directory Access Protocol (LDAP) és a Microsoft Active Directory® technológiák használatával.
- Hitelesítés és hozzáférés. Számítógép vagy felhasználó azonosítójának létrehozása a hálózaton és azon információk meghatározása olyan alapelvek és technológiák használatával, mint a fájlhozzáférések, csoportházirendek és a Kerberos hitelesítési szolgáltatás, amelyek elérésére a számítógépnek vagy felhasználónak joga van.

Szerencsére az Ubuntu rendszer képes az összes ilyen szolgáltatás biztosítására Windows kliensek számára, és hálózati erőforrások megosztására azokkal. Az Ubuntu rendszer által tartalmazott egyik kulcsfontosságú szoftver windowsos hálózatkezeléshez az SMB kiszolgálóalkalmazások és eszközök Samba nevű csomagja.

Az Ubuntu kiszolgálókézikönyv ezen szakasza bemutatja a Samba felhasználásának néhány általános módját, valamint a szükséges csomagok telepítését és beállítását. A Sambával kapcsolatos további részleges dokumentációk és információk a Samba weboldalán[1] érhetők el.

[1] http://www.samba.org

2. Samba fájlkiszolgáló

Az Ubuntu és Windows számítógépek összekapcsolásának egyik legáltalánosabb módja a Samba beállítása fájlkiszolgálóként. Ez a szakasz bemutatja a Samba kiszolgáló beállítását fájlok megosztására Windows kliensekkel.

A kiszolgáló úgy lesz beállítva a fájlok megosztására a hálózat bármely kliensével, hogy nem kér jelszót. Ha a környezete szigorúbb hozzáférés-felügyeletet igényel, olvassa el a 4. szakasz - Samba fájl- és nyomtatókiszolgáló biztonságossá tétele [230] részt.

2.1. Telepítés

Az első lépés a samba csomag telepítése. Egy terminálban adja ki a következő parancsot:

```
sudo apt-get install samba
```

Ezzel ez kész is, most már készen áll a Samba beállítására fájlok megosztására.

2.2. Beállítás

A fő Samba beállítófájl az `/etc/samba/smb.conf`. Az alapértelmezett beállítófájl jelentős mennyiségű megjegyzést tartalmaz, a különféle beállítási lehetőségek dokumentálása érdekében.

Az alapértelmezett beállítófájl nem tartalmaz minden elérhető lehetőséget. További részletekért olvassa el az `smb.conf` man oldalát vagy a Samba HOWTO Collection[2] gyűjteményt.

1. Első lépésként szerkessze a következő kulcs/érték párokat az `/etc/samba/smb.conf` fájl [global] szakaszában:

   ```
   workgroup = EXAMPLE
   ...
   security = user
   ```

   A security paraméter a [global] szakaszban lejjebb van és megjegyzésben látható. Az EXAMPLE értékét is módosítsa a környezetének megfelelően.

2. Hozzon létre egy új szakaszt a megosztandó könyvtárnak a fájl alján, vagy az egyik példát vegye ki a megjegyzésből:

   ```
   [share]
       comment = Ubuntu fájlkiszolgáló megosztás
       path = /srv/samba/megosztas
       browsable = yes
       guest ok = yes
       read only = no
       create mask = 0755
   ```

- comment: a megosztás rövid leírása. Módosítsa igényeinek megfelelően.
- path: a megosztandó könyvtár útvonala.

  Ez a példa a `/srv/samba/megosztas` könyvtárat használja, mert a Filesystem Hierarchy Standard (FHS) szerint a telephely-specifikus adatokat az /srv[3] alól kell kiszolgálni. Technikailag a Samba megosztások bárhol elhelyezhetők a fájlrendszeren, amíg a jogosultságok megfelelők, de a szabványok követése ajánlott.
- browsable: lehetővé teszi a Windows klienseknek a megosztás tallózását a Windows Explorer használatával.
- guest ok: jelszó megadása nélkül teszi lehetővé a klienseknek a csatlakozást a megosztáshoz.
- read only: megadja, hogy a megosztás írásvédett-e, vagy van rá írási jog is. Az írási jog akkor él, ha az érték no, mint a fenti példában. Ha az érték yes, akkor a megosztás csak olvasható.
- create mask: megadja az új fájlok által létrehozásukkor kapott jogosultságokat.

3. A Samba beállítása után létre kell hozni a könyvtárat, és jogosultságait módosítani kell. Adja ki a következő parancsot:

```
sudo mkdir -p /srv/samba/megosztas
sudo chown nobody.nogroup /srv/samba/megosztas/
```

A -p kapcsoló megadásával az mkdir a teljes könyvtárfát létrehozza, ha az nem létezik. Módosítsa a megosztás nevét a környezete igényei szerint.

4. Végül indítsa újra a samba szolgáltatásokat az új beállítások életbe léptetéséhez:

```
sudo /etc/init.d/samba restart
```

Még egyszer: a fenti beállítások a helyi hálózat bármely kliensének teljes hozzáférést adnak. Biztonságosabb beállításokért olvassa el a 4. szakasz - Samba fájl- és nyomtatókiszolgáló biztonságossá tétele [230] részt.

Ezután a windowsos kliensekről képes lesz az Ubuntu fájlkiszolgáló tallózására és a megosztott könyvtár megjelenítésére. A beállítások ellenőrzéséhez próbáljon létrehozni egy könyvtárat Windows alól.

További megosztások létrehozásához egyszerűen csak új [dir] szakaszokat kell létrehoznia az `/etc/samba/smb.conf` fájlban, majd újra kell indítani a Samba szolgáltatást. Csak arról győződjön meg, hogy a megosztandó könyvtár tényleg létezik és a jogosultságai megfelelők.

2.3. Információforrások

- Összetettebb Samba beállításokért lásd a Samba HOWTO Collection[4] oldalt
- A kézikönyv nyomtatott formában[5] is elérhető.
- Az O'Reilly kiadó Using Samba[6] könyve szintén jó referencia.

- Az Ubuntu wiki Samba[7] oldala is jó kiindulópont.

3. Samba nyomtatókiszolgáló

A Samba másik gyakori felhasználási módja a helyileg vagy hálózati Ubuntu kiszolgálóra telepített nyomtatók megosztása. A 2. szakasz - Samba fájlkiszolgáló [225] mintájára ez a szakasz is úgy állítja be a Sambát, hogy a helyi hálózat bármely kliense felhasználónév és jelszó megadása nélkül használhassa a telepített nyomtatókat.

Biztonságosabb beállításokért lásd a 4. szakasz - Samba fájl- és nyomtatókiszolgáló biztonságossá tétele [230] részt.

3.1. Telepítés

A Samba telepítése és beállítása előtt jó, ha már rendelkezik egy működő CUPS telepítéssel. Részletekért lásd a 3. szakasz - CUPS nyomtatókiszolgáló [179] részt.

A samba csomag telepítéséhez adja ki a következő parancsot:

```
sudo apt-get install samba
```

3.2. Beállítás

A samba telepítése után szerkessze az `/etc/samba/smb.conf` fájlt. Módosítsa a workgroup attribútumot a hálózatának megfelelően, majd módosítsa a security értékét share-re:

```
workgroup = EXAMPLE
...
security = user
```

A [printers] szakaszban módosítsa a guest ok beállítást yes értékűre:

```
browsable = yes
guest ok = yes
```

Az `smb.conf` szerkesztése után indítsa újra a Sambát:

```
sudo /etc/init.d/samba restart
```

Az alapértelmezett Samba konfiguráció automatikusan megosztja az összes telepített nyomtatót. Egyszerűen csak telepítse a nyomtatót helyileg a Windows klienseken.

3.3. Információforrások

- Összetettebb Samba beállításokért lásd a Samba HOWTO Collection[8] oldalt
- A kézikönyv nyomtatott formában[9] is elérhető.
- Az O'Reilly kiadó Using Samba[10] könyve szintén jó referencia.

- A CUPS beállításával kapcsolatos további információkért lásd a CUPS weboldalát[11].
- Az Ubuntu wiki Samba[12] oldala is jó kiindulópont.

4. Samba fájl- és nyomtatókiszolgáló biztonságossá tétele

4.1. Samba biztonsági módjai

A Common Internet Filesystem (CIFS) hálózati protokollban két biztonsági szint érhető el: felhasználói szintű és megosztás szintű. A Samba biztonsági mód megvalósítása nagyobb rugalmasságot tesz lehetővé, a felhasználói szintű biztonság megvalósításához négy, a megosztás szintű biztonsághoz pedig egy módszer biztosításával:

- security = user: Felhasználónév és jelszó megadását követeli meg a kliensektől a megosztásokhoz csatlakozáshoz. A Samba felhasználói fiókok nem azonosak a rendszer felhasználói fiókjaival, de a libpam-smbpass csomag használatával szinkronizálhatók a rendszer felhasználói és jelszavai a Samba felhasználói adatbázissal.
- security = domain: Ez a mód lehetővé teszi, hogy a Samba kiszolgáló a windowsos kliensek számára elsődleges tartományvezérlőként (PDC), tartalék tartományvezérlőként (BDC), vagy tartománytag-kiszolgálóként (DMS) jelenjen meg. További információkért lásd: 5. szakasz - A Samba mint tartományvezérlő [235].
- security = ADS: Lehetővé teszi a Samba kiszolgálónak a csatlakozást Active Directory tartományokhoz natív tagként. Részletekért lásd: 6. szakasz - A Samba Active Directory integrációja [239].
- security = server: Ez a mód abból az időből maradt, amikor a Samba még nem tudott tag kiszolgálóvá válni, és bizonyos biztonsági problémák miatt nem szabad használni. További részletekért lásd a Samba guide Server Security[13] szakaszát.
- security = share: Lehetővé teszi a klienseknek a megosztásokhoz való csatlakozást felhasználónév és jelszó megadása nélkül.

A kiválasztandó biztonsági mód a környezettől, valamint a Samba kiszolgálóval ellátandó feladattól függ.

4.2. Security = User

Ebben a szakaszban bemutatjuk a 2. szakasz - Samba fájlkiszolgáló [225] és 3. szakasz - Samba nyomtatókiszolgáló [228] részben beállított Samba fájl- és nyomtatókiszolgáló újrakonfigurálását hitelesítés megkövetelésére.

Első lépésként telepítse a libpam-smbpass csomagot, amely a rendszer felhasználóit szinkronizálja a Samba felhasználói adatbázissal:

```
sudo apt-get install libpam-smbpass
```

Ha a telepítéskor kiválasztotta a Samba Server feladatot, akkor a libpam-smbpass csomag már telepítve van.

Szerkessze az `/etc/samba/smb.conf` fájlt, és módosítsa a [share] szakaszt:

```
guest ok = no
```

Végül indítsa újra a Sambát az új beállítások életbe léptetéséhez:

```
sudo /etc/init.d/samba restart
```

Ezután a megosztott könyvtárakhoz vagy nyomtatókhoz csatlakozáskor a rendszer felhasználói nevet és jelszót fog kérni.

Ha a megosztáshoz hálózati meghajtót rendelt, bejelölheti a „Reconnect at Logon” jelölőnégyzetet, amely csak egyszer követeli meg a felhasználónév és jelszó megadását, legalábbis a jelszó megváltozásáig.

4.3. Megosztás biztonsága

Számos lehetőség van minden egyes megosztott könyvtár biztonságának növelésére. A [share] példa felhasználásával ez a szakasz néhány általános lehetőséget mutat be.

4.3.1. Csoportok

A csoportok számítógépek vagy felhasználók halmazát adják meg, amelyeknek azonos hozzáférési szintjük van bizonyos hálózati erőforrásokhoz és az ilyen erőforrásokra vonatkozó hozzáférés adott részletességi szintjét biztosítják. Ha például a qa nevű csoport a freda, danika és rob felhasználókat tartalmazza, egy support nevű csoport pedig a danika, jeremy és vincent felhasználókat, akkor a qa csoportnak hozzáférést biztosító hálózati erőforrások lehetővé teszik freda, danika és rob hozzáférését, de jeremy vagy vincent nem érheti el ezeket. Mivel a danika nevű felhasználó egyaránt tagja a qa és support csoportoknak, képes lesz elérni a mindkét csoportnak hozzáférést engedő erőforrásokat, míg a többi felhasználó csak az ő csoportjukat engedélyező erőforrásokhoz férhet hozzá.

Alapértelmezésben a Samba a helyi rendszeren, az `/etc/group` fájlban megadott csoportokban próbálja elhelyezni a felhasználót. További információkért a felhasználók csoportokhoz adásáról és azokból eltávolításáról lásd a 1.2. szakasz - Felhasználók hozzáadása és törlése [108] részt.

A csoportok megadásakor az `/etc/samba/smb.conf` Samba konfigurációs fájlban a csoportnevet „@” szimbólummal kezdve jelölheti. Ha például a sysadmin nevű csoportot szeretné létrehozni az `/etc/samba/smb.conf` valamely szakaszában, akkor a csoportnevet a @sysadmin formában kell megadni.

4.3.2. Fájljogosultságok

A fájljogosultságok megadják, hogy az adott fájlra, könyvtárra vagy fájlcsoportra egy adott számítógép vagy felhasználó pontosan milyen jogosultságokkal rendelkezik. Az ilyen jogosultságok megadhatók az `/etc/samba/smb.conf` fájl szerkesztésével és adott fájlmegosztás konkrét jogosultságainak megadásával.

Ha például létrehozott egy megosztas nevű Samba megosztást és csak olvasási jogosultságokat szeretne adni a qa csoport felhasználóinak, de engedélyezni akarja a sysadmin csoport és a vincent

nevű felhasználó számára az írást, akkor ezt az `/etc/samba/smb.conf` fájl szerkesztésével és a [megosztas] bejegyzés alá a következő értékek beírásával teheti meg:

```
read list = @qa
write list = @sysadmin, vincent
```

Egy másik lehetséges Samba jogosultság az adminisztrációs jog egy adott megosztott erőforrásra. Az adminisztrációs jogosultsággal rendelkező felhasználók az erőforráson belül minden információt írhatnak, olvashatnak vagy módosíthatnak, amire adminisztrációs jogosultsággal rendelkeznek.

Ha például a melissa nevű felhasználónak adminisztrációs jogosultságot adna a share példához, az `/etc/samba/smb.conf` fájlt megnyitva a következő sort kellene a [share] bejegyzéshez adni:

```
admin users = melissa
```

Az `/etc/samba/smb.conf` szerkesztése után indítsa újra a Sambát a módosítások életbe léptetéséhez:

```
sudo /etc/init.d/samba restart
```

A read list és write list működéséhez a Samba biztonsági módot nem szabad security = share-re állítani

A Samba beállítása után a csoportok hozzáférésének korlátozására a megosztott könyvtárhoz, a fájlrendszer jogosultságait is frissíteni kell.

A hagyományos Linux fájljogosultságok nem képezhetők le jól a Windows NT hozzáférés-vezérlési listákra (ACL-ek). Szerencsére a POSIX ACL-ek elérhetők az Ubuntu kiszolgálókon, így részletesebb felügyeletet biztosítanak. Az ACL-ek engedélyezéséhez például a `/srv` alatti EXT3 fájlrendszeren szerkessze az `/etc/fstab` fájlt és vegye fel az acl beállítást:

```
UUID=66bcdd2e-8861-4fb0-b7e4-e61c569fe17d /srv  ext3    noatime,relatime,acl 0       1
```

Ezután csatolja újra a partíciót:

```
sudo mount -v -o remount /srv
```

A fenti példa feltételezi, hogy a `/srv` külön partíción van. Ha az `/srv`, vagy ahol a megosztás van, a `/` partíció része, a rendszer újraindítása szükséges.

A fenti Samba beállításoknak való megfeleléshez a sysadmin csoport olvasási, írási és végrehajtási jogosultságokat kap a `/srv/samba/share` könyvtárra, a qa csoport olvasási és végrehajtási jogosultságokat, a fájlok pedig a melissa nevű felhasználó tulajdonába kerülnek. Adja ki a következőket egy terminálba:

```
sudo chown -R melissa /srv/samba/share/
sudo chgrp -R sysadmin /srv/samba/share/
sudo setfacl -R -m g:qa:rx /srv/samba/share/
```

A fenti setfacl parancs végrehajtási jogosultságokat ad minden fájlra a `/srv/samba/share` könyvtárban, amit nem biztos hogy szeretne.

Most egy windowsos kliensről nézve új fájljogosultságok megjelenését fogja észlelni. A POSIX ACL-ekkel kapcsolatban lásd az acl és setfacl kézikönyvoldalakat.

4.4. Samba AppArmor profil

Az Ubuntu tartalmazza az AppArmor biztonsági modult, amely kötelező hozzáférés-vezérlést biztosít. A Samba alapértelmezett AppArmor profilját a beállításaihoz kell igazítania. Az AppArmor használatával kapcsolatos további részletekért lásd a 4. szakasz - AppArmor [121] részt.

Az apparmor-profiles csomag részeként elérhetők alapértelmezett AppArmor profilok az `/usr/sbin/smbd` és `/usr/sbin/nmbd` fájlokhoz, a Samba démon binárisaihoz. A csomag telepítéséhez adja ki a következő parancsot:

```
sudo apt-get install apparmor-profiles
```

Ez a csomag számos más binárishoz is tartalmaz profilokat.

Alapértelmezésben az smbd és nmbd profiljai a complain módban vannak, lehetővé téve a Samba működését a profil módosítása nélkül, csupán a hibák naplózása mellett. Az smbd profil enforce módba váltásához, és a Samba elvárt módon való működéséhez a profilt úgy kell beállítani, hogy tükrözze a megosztott könyvtárakat.

Szerkessze az `/etc/apparmor.d/usr.sbin.smbd` fájlt, és vegye fel a [share] megosztásra vonatkozó információkat a fájlkiszolgálós példából:

```
  /srv/samba/share/ r,
  /srv/samba/share/** rwkix,
```

Most állítsa a profilt enforce módba és töltse újra:

```
sudo aa-enforce /usr/sbin/smbd
cat /etc/apparmor.d/usr.sbin.smbd | sudo apparmor_parser -r
```

Ezután a megszokott módon képes lesz a megosztott könyvtárbeli fájlok olvasására, írására és végrehajtására, az smbd bináris pedig csak a beállított fájlokhoz és könyvtárakhoz férhet hozzá. Ne felejtsen el minden olyan könyvtárhoz felvenni egy bejegyzést, amelynek megosztására a Sambát beállította. A hibák a `/var/log/syslog` fájlba kerülnek naplózásra.

4.5. Információforrások

- Összetettebb Samba beállításokért lásd a Samba HOWTO Collection[14] oldalt
- A kézikönyv nyomtatott formában[15] is elérhető.
- Az O'Reilly Using Samba[16] könyve szintén jó referencia.
- A Samba HOWTO Collection 18. fejezete[17] a biztonságról szól.
- A Sambával és az ACL-ekkel kapcsolatos további információkért lásd a Samba ACL-ek oldalát[18].
- Az Ubuntu wiki Samba[19] oldala is jó kiindulópont.

5. A Samba mint tartományvezérlő

Noha a Samba kiszolgáló nem képes Active Directory elsődleges tartományvezérlőként (PDC) működni, beállítható a Windows NT4-stílusú tartományvezérlőként való megjelenésre. Ennek a beállításnak nagy előnye a felhasználó- és géphitelesítési adatok központosítása. A Samba képes a felhasználói információk tárolására több háttérprogramot is használni.

5.1. Elsődleges tartományvezérlő

Ez a szakasz lefedi a Samba beállítását elsődleges tartományvezérlőként (PDC), az alapértelmezett smbpasswd háttérprogram használatával.

1. A felhasználói fiókok szinkronizálásához első lépésként telepítse a Sambát és a libpam-smbpass csomagot a következő parancs kiadásával:

   ```
   sudo apt-get install samba libpam-smbpass
   ```

2. Ezután állítsa be a Sambát az `/etc/samba/smb.conf` fájl szerkesztésével. A security mód user legyen, a workgroup pedig kapcsolódjon az aktuális szervezethez:

   ```
   workgroup = EXAMPLE
   ...
   security = user
   ```

3. A megjegyzésbe tett „Domains” szakaszba vegye fel vagy vegye ki megjegyzésből a következőt:

   ```
   domain logons = yes
   logon path = \\%N\%U\profile
   logon drive = H:
   logon home = \\%N\%U
   logon script = logon.cmd
   add machine script = sudo /usr/sbin/useradd -N -g machines -c Machine -d /var/lib/samba -s /
   ```

   - domain logons: a netlogon szolgáltatást biztosítja, ennek segítségével a Samba tartományvezérlőként viselkedhet.
   - logon path: a felhasználó Windows profilját a saját mappájába helyezi. Lehetőség van egy [profiles] megosztás beállítására, amely minden profilt egy könyvtárba helyez.
   - logon drive: megadja a saját könyvtár helyi útvonalát.
   - logon home: megadja a saját könyvtár helyét.
   - logon script: megadja a felhasználó bejelentkezése után helyileg futtatandó parancsfájlt. A parancsfájlt a [netlogon] megosztásba kell tenni.
   - add machine script: ez a parancsfájl fogja automatikusan létrehozni a tartományhoz csatlakozáshoz szükséges Machine Trust Account-ot.

     Ebben a példában létre kell hozni a machines csoportot az addgroup segédprogrammal, részletekért lásd a 1.2. szakasz - Felhasználók hozzáadása és törlése [108] szakaszt.

Ha nem szeretne központi profilt használni, akkor hagyja a logon home és logon path beállításokat megjegyzésben.

4. Vegye ki megjegyzésből a [homes] megosztást a logon home leképezéséhez:

```
[homes]
   comment = Saját könyvtárak
   browseable = no
   read only = no
   create mask = 0700
   directory mask = 0700
   valid users = %S
```

5. Tartományvezérlőként való beállításkor egy [netlogon] megosztást is be kell állítani. Ehhez vegye ki megjegyzésből a következőt:

```
[netlogon]
   comment = Hálózati bejelentkezési szolgáltatás
   path = /srv/samba/netlogon
   guest ok = yes
   read only = yes
   share modes = no
```

A netlogon megosztás eredeti útvonala a `/home/samba/netlogon`, de a Filesystem Hierarchy Standard (FHS) szerint az /srv[20] a rendszer által biztosított telephely-specifikus adatok megfelelő helye.

6. Most hozza létre a `netlogon` könyvtárat és egy (egyelőre) üres `logon.cmd` parancsfájlt:

```
sudo mkdir -p /srv/samba/netlogon
sudo touch /srv/samba/netlogon/logon.cmd
```

A kliens környezetének személyre szabásához tetszőleges Windows bejelentkezési parancsfájl-parancsokat megadhat a `logon.cmd` fájlban.

7. Mivel a root alapértelmezésben le van tiltva, egy munkaállomás tartományhoz csatlakoztatásához egy rendszercsoportot meg kell feleltetni a Windows Domain Admins csoportnak. A net segédprogram segítségével adja ki a következő parancsot:

```
sudo net groupmap add ntgroup="Domain Admins" unixgroup=sysadmin rid=512 type=d
```

A sysadmin helyett tetszőleges másik csoportot is megadhat. Ezen kívül a tartományhoz csatlakozó felhasználónak a rendszer admin csoportja mellett a sysadmin csoportban is tagnak kell lennie. Az admin csoportbeli tagság lehetővé teszi a sudo használatát.

8. Végül indítsa újra a Sambát az új tartományvezérlő engedélyezéséhez:

```
sudo /etc/init.d/samba restart
```

9. Ezután ugyanúgy képesnek kell lennie windowsos kliensek csatlakoztatására a tartományba, mintha Windows kiszolgálón futó NT4 tartományba léptetné be azokat.

5.2. Tartalék tartományvezérlő

Ha a hálózaton van elsődleges tartományvezérlő (PDC), ajánlatos tartalék tartományvezérlőt (BDC) is tartani. Ez lehetővé teszi a kliensek hitelesítését akkor is, ha a PDC elérhetetlenné válik.

A Samba BDC-ként való beállításakor szükség van a fiókinformációk szinkronizálására a PDC-vel. Ez többféleképpen is megvalósítható: scp, rsync vagy LDAP használatával passdb háttérprogramként.

Az LDAP használata a legrobusztusabb, mivel mindkét tartományvezérlő valós időben képes ugyanazokat az információkat használni. Azonban egy LDAP kiszolgáló beállítása fölöslegesen bonyolult lehet kevés felhasználói és számítógépes fiók esetén. Részletekért lásd a 2. szakasz - Samba és LDAP [75] részt.

1. Első lépésként telepítse a samba és libpam-smbpass csomagokat. Egy terminálból adja ki a következőt:

```
sudo apt-get install samba libpam-smbpass
```

2. Szerkessze az `/etc/samba/smb.conf` fájlt, és a [global] szakaszban vegye ki megjegyzésből a következőt:

```
workgroup = EXAMPLE
...
security = user
```

3. A megjegyzésben lévő Domains alatt vegye fel a következőket:

```
domain logons = yes
domain master = no
```

4. Győződjön meg róla, hogy a felhasználónak joga van írni a `/var/lib/samba` könyvtár fájljait. Például az admin csoport tagjai számára az scp használatának engedélyezéséhez adja ki a következőt:

```
sudo chgrp -R admin /var/lib/samba
```

5. Ezután szinkronizálja a felhasználói fiókokat a `/var/lib/samba` könyvtárat az scp segítségével átmásolva a PDC-re:

```
sudo scp -r felhasználónév@pdc:/var/lib/samba /var/lib
```

A felhasználónevet helyettesítse a felhasználónévvel, a pdc-t pedig a tényleges PDC gépnevével vagy IP-címével.

6. Végül indítsa újra a sambat:

```
sudo /etc/init.d/samba restart
```

A tartalék tartományvezérlő működését a PDC Samba démonjának leállításával, majd a tartományba csatlakozott valamely windowsos kliensre való bejelentkezés megpróbálásával tesztelheti.

Szintén szem előtt kell tartani, hogy amennyiben a logon home beállításban egy, a PDC-n levő könyvtárat adott meg, a PDC elérhetetlenné válásakor a felhasználók saját meghajtója is elérhetetlenné válik. Emiatt a legjobb megoldás egy harmadik, a PDC-től és a BDC-től is eltérő fájlkiszolgálón található logon home beállítása.

5.3. Információforrások

- Összetettebb Samba beállításokért lásd a Samba HOWTO Collection[21] oldalt
- A kézikönyv nyomtatott formában[22] is elérhető.
- Az O'Reilly Using Samba[23] könyve szintén jó referencia.
- A Samba HOWTO Collection 4. fejezete[24] részletezi az elsődleges tartományvezérlő beállítását.
- A Samba HOWTO Collection 5. fejezete[25] részletezi a tartalék tartományvezérlő beállítását.
- Az Ubuntu wiki Samba[26] oldala is jó kiindulópont.

6. A Samba Active Directory integrációja

6.1. Samba megosztás elérése

A Samba másik felhasználási módja a meglévő Windows hálózatba való integrálás. Egy Active Directory tartomány részeként a Samba fájlkiszolgálást és nyomtatószolgáltatásokat biztosíthat az AD-felhasználóknak.

Az AD-tartományba csatlakozás legegyszerűbb módja a Likewise-open használata. Részletes utasításokért lásd a 7. szakasz - Likewise Open [242] szakaszt.

A tartomány részeként adja ki a következő parancsot:

```
sudo apt-get install samba smbfs smbclient
```

Mivel a likewise-open és a samba csomagok külön `secrets.tdb` fájlokat használnak, egy szimbolikus linket kell létrehozni a `/var/lib/samba` könyvtárban:

```
sudo mv /var/lib/samba/secrets.tdb /var/lib/samba/secrets.tdb.orig
sudo ln -s /etc/samba/secrets.tdb /var/lib/samba
```

Ezután szerkessze az `/etc/samba/smb.conf` fájlt:

```
workgroup = PÉLDA
...
security = ads
realm = PÉLDA.HU
...
idmap backend = lwopen
idmap uid = 50-9999999999
idmap gid = 50-9999999999
```

Indítsa újra a sambát az új beállítások életbe léptetéséhez:

```
sudo /etc/init.d/samba restart
```

Ezután elérheti a Samba megosztásokat windowsos kliensekről. Ugyanakkor győződjön meg róla, hogy a megfelelő AD-felhasználóknak vagy csoportoknak hozzáférést adott a megosztott könyvtárhoz. További részletekért lásd a 4. szakasz - Samba fájl- és nyomtatókiszolgáló biztonságossá tétele [230] szakaszt.

6.2. Windowsos megosztás elérése

Miután a Samba kiszolgáló az Active Directory tartomány része lett, elérheti a Windows kiszolgálók megosztásait:

- Windows fájlmegosztás csatolásához adja ki a következő parancsot a terminálban:

```
mount.cifs //fs01.példa.hu/megosztás csatolási_pont
```

  Olyan számítógépeken lévő megosztások is elérhetők, amelyek nem részei AD-tartománynak, de a felhasználónevet és jelszót meg kell adni:

- A megosztás a rendszerindítás alatti csatolásához helyezzen el egy bejegyzést az `/etc/fstab` fájlba, például:

```
//192.168.0.5/megosztás /mnt/windows cifs auto,username=geza,password=titok,rw 0       0
```

- Windowsos kiszolgálóról az smbclient segédprogrammal is másolhat fájlokat. Windowsos megosztás fájljainak kiíratása:

```
smbclient //fs01.példa.hu/megosztás -k -c "ls"
```

- Adja ki a következőt fájl másolásához a megosztásról:

```
smbclient //fs01.példa.hu/megosztás -k -c "get fájl.txt"
```

  Ez a `fájl.txt` fájlt az aktuális könyvtárba másolja.

- Fájl hozzáadása a megosztáshoz:

```
smbclient //fs01.példa.hu/megosztás -k -c "put /etc/hosts hosts"
```

  Ez az `/etc/hosts` fájlt átmásolja a `//fs01.példa.hu/megosztás/hosts` fájlba.

- A fentiekben használt -c kapcsoló lehetővé teszi az smbclient parancsainak egyszerre történő kiadását. Ez parancsfájlokhoz és kisebb fájlműveletekhez alkalmas. Az FTP-szerű smb: \> prompt eléréséhez, amelyben normál fájl- és könyvtárparancsokat használhat, adja ki a következő parancsot:

```
smbclient //fs01.példa.hu/megosztás -k
```

Helyettesítse az fs01.példa.hu/megosztás, //192.168.0.5/megosztás, username=geza,password=titok és a fájl.txt minden előfordulását a kiszolgáló IP-címével, gépnevével, megosztásnevével, a fájlnévvel, és a megosztási jogokkal rendelkező tényleges felhasználónévvel és jelszóval.

6.3. Információforrások

Az smbclient további kapcsolóival kapcsolatban lásd a kézikönyvoldalát: man smbclient, amely online[27] is elérhető.

[27] http://manpages.ubuntu.com/manpages/lucid/en/man1/smbclient.1.html

A mount.cifs kézikönyvoldala[28] szintén hasznos információkat tartalmaz.

Az Ubuntu wiki Samba[29] oldala is jó kiindulópont.

[28] http://manpages.ubuntu.com/manpages/lucid/en/man8/mount.cifs.8.html

[29] https://help.ubuntu.com/community/Samba

7. Likewise Open

A Likewise Open egyszerűsíti a linuxos számítógép Active Directory tartományba hitelesítéséhez szükséges beállításokat. A winbind-alapú likewise-open csomag fájdalommentessé teszi az Ubuntu hitelesítés integrálását meglévő Windows hálózatba.

7.1. Telepítés

A Likewise Open használata a likewise-open parancssoros segédprogram, és a likewise-open-gui segítségével lehetséges. Ez a fejezet a parancssoros segédprogramot írja le.

A likewise-open csomag telepítéséhez adja ki a következő parancsot:

```
sudo apt-get install likewise-open
```

7.2. Csatlakozás tartományhoz

A likewise-open elsődleges végrehajtható fájlja a `/usr/bin/domainjoin-cli`, amely a számítógép tartományba léptetésére használatos. A tartományhoz csatlakozás előtt győződjön meg róla, hogy rendelkezik:

- Hozzáféréssel a tartományhoz csatlakozásra jogosult Active Directory felhasználói azonosítóhoz.
- A tartomány teljes képzésű tartománynevével (FQDN), amelyhez csatlakozni akar. Ha az AD-tartomány neve nem hasonlít az érvényes tartományokéra, mint a példa.hu, akkor valószínűleg a tartománynév.local formában van.
- A tartományhoz megfelelően beállított DNS. Éles AD-környezetben ez a helyzet. A megfelelő Microsoft DNS esetén a munkaállomások képesek meghatározni az Active Directory tartomány elérhetőségét.

  Ha a hálózatán nincs Windows DNS kiszolgáló, akkor lásd a 7.5. szakasz - Microsoft DNS [244] szakaszt.

A tartományhoz csatlakozáshoz adja ki terminálból:

```
sudo domainjoin-cli join példa.hu Rendszergazda
```

Helyettesítse a példa.hu-t a tartománynévvel, a Rendszergazdát pedig a megfelelő felhasználónévvel.

Ezután a rendszer bekéri a felhasználói jelszót. Ha minden jól megy, akkor a SUCCESS üzenet jelenik meg a terminálban.

A tartományhoz csatlakozás után újra kell indítani a számítógépet a hitelesítés megpróbálása előtt a tartományban.

Miután sikeresen csatlakoztatta az Ubuntu gépet az Active Directory tartományhoz, bejelentkezhet bármely érvényes AD-felhasználónév használatával. A bejelentkezéshez a felhasználónevet „tartománynév\felhasználónév” formában kell megadni. A tartományba csatlakoztatott kiszolgálóra ssh kapcsolat nyitásához például adja ki:

```
ssh 'példa\geza'@gépnév
```

Asztali rendszer beállítása esetén a felhasználónevet a grafikus bejelentkezéskor is a tartomány\ előtaggal kell megadni.

Vegye fel a következőt az `/etc/samba/lwiauthd.conf` fájlba a likewise-open beállításához alapértelmezett tartomány használatára:

```
winbind use default domain = yes
```

Ezután indítsa újra a likewise-open démonokat:

```
sudo /etc/init.d/likewise-open restart
```

Az alapértelmezett tartomány használatának beállítása után a tartomány\ előtag nem szükséges, a felhasználók csupán a felhasználónevük használatával is bejelentkezhetnek.

A tartomány elhagyására a domainjoin-cli segédprogram is használható. Adja ki a következőt egy terminálban:

```
sudo domainjoin-cli leave
```

7.3. Egyéb segédprogramok

A likewise-open csomag tartalmaz néhány további segédprogramot is, amelyek az Active Directory környezettel kapcsolatos információk gyűjtéséhez lehetnek hasznosak. Ezek segítségével a gép csatlakoztatható a tartományba, és azonosak a samba-common és winbind csomagokban található segédprogramokkal.

- lwinet: Információkat ad a hálózatról és a tartományról.
- lwimsg: Lehetővé teszi az együttműködést a likewise-winbindd démonnal.
- lwiinfo: Információkat jelenít meg a tartomány különböző részeiről.

További részletekért nézze meg az egyes segédprogramok kézikönyvoldalait.

7.4. Hibaelhárítás

- Ha a kliensnek gondot okoz a tartományhoz csatlakozás, akkor ellenőrizze, hogy az `/etc/resolv.conf` fájlban a Microsoft DNS van elsőként felsorolva. Például:

```
nameserver 192.168.0.1
```

- A tartományhoz csatlakozással kapcsolatos részletesebb információkért használja a domainjoin-cli segédprogram --loglevel verbose vagy --advanced kapcsolóit:

```
sudo domainjoin-cli --loglevel verbose join példa.hu Rendszergazda
```

- Ha egy Active Directory felhasználónak problémát okoz a bejelentkezés, akkor részletekért nézze meg a `/var/log/auth.log` fájlt.
- Az Ubuntu asztali verzióját tartalmazó munkaállomás tartományba csatlakoztatásakor szükség lehet az `/etc/nsswitch.conf` fájl szerkesztésére, ha az AD tartomány a .local szintaxist használja. A tartományhoz csatlakozás érdekében a hosts fájl "mdns4" bejegyzését törölni kell. Például:

```
hosts: files mdns4_minimal [NOTFOUND=return] dns mdns4
```

A fentit módosítsa erre:

```
hosts: files dns [NOTFOUND=return]
```

Indítsa újra a hálózatkezelést a következő megadásával:

```
sudo /etc/init.d/networking restart
```

Ezután képes lesz csatlakozni az Active Directory tartományhoz.

7.5. Microsoft DNS

Az alábbi utasítások a DNS Windows Server 2003 kiszolgálón futó Active Directory tartományvezérlőre telepítését írják le, de más verziók esetén is hasonlóak:

- Válassza ki a Start → Felügyeleti eszközök → Kiszolgáló kezelése menüpontot. Ez megnyitja a Kiszolgálókezelő segédprogramot.
  1. Válassza a Szerepkör hozzáadása és eltávolítása lehetőséget
  2. Nyomja meg a Tovább gombot
  3. Válassza a „DNS-kiszolgáló” lehetőséget
  4. Nyomja meg a Tovább gombot
  5. Nyomja meg újra a Tovább gombot a folytatáshoz
  6. Válassza ki a „Címkeresési zóna létrehozása” lehetőséget, ha nincs kiválasztva
  7. Nyomja meg a Tovább gombot
  8. Jelölje ki az „Ez a kiszolgáló kezeli a zónát” lehetőséget, és nyomja meg a Tovább gombot
  9. Adja meg a tartománynevet, és nyomja meg a Tovább gombot
  10. Válassza a „Csak a biztonságos frissítések engedélyezése” lehetőséget, és nyomja meg a Tovább gombot

11. Adja meg a kérelmek továbbításához használandó DNS kiszolgálók IP-címeit, vagy válassza a „Nem, ne továbbítsa a kérelmeket” lehetőséget, és nyomja meg a Tovább gombot.
12. Kattintson a Befejezés gombra
13. Kattintson a Befejezés gombra

A DNS ezzel telepítésre került, a további beállításai a Microsoft Management Console DNS moduljával végezhetők el.

- Ezután állítsa be a kiszolgálót a DNS-lekérdezésekhez:
  1. Nyomja meg a Start gombot
  2. Vezérlőpult
  3. Hálózati kapcsolatok
  4. Kattintson a jobb egérgombbal a „Helyi kapcsolat” elemen
  5. Kattintson a Tulajdonságok elemre
  6. Kattintson duplán a „TCP/IP protokoll” elemre
  7. Adja meg a kiszolgáló IP-címét, mint „Elsődleges DNS-kiszolgáló”
  8. Kattintson az OK gombra
  9. A beállítások mentéséhez kattintson újra az OK gombra

7.6. Hivatkozások

További információkért lásd a Likewise[30] honlapját.

A domainjoin-cli további beállításaiért lásd a man domainjoin-cli kézikönyvoldalt.

Lásd még az Ubuntu wiki LikewiseOpen[31] oldalát.

[30] http://www.likewisesoftware.com/

[31] https://help.ubuntu.com/community/LikewiseOpen

18. fejezet - Biztonsági mentés

Számos lehetőség van egy Ubuntu telepítés biztonsági mentésére. A biztonsági mentésekkel kapcsolatos legfontosabb teendő egy mentési terv elkészítése, amely tartalmazza, hogy mit kell menteni, hova kell menteni és hogyan lehet visszaállítani.

A következő szakaszok ezen feladatok elvégzésének különböző módjait írják le.

1. Shell-parancsfájlok

Egy rendszer biztonsági mentésének legegyszerűbb módja shell-parancsfájlok használata. Egy parancsfájllal például beállíthatók a használandó könyvtárak, és ezek átadhatók paraméterként a tar segédprogramnak, amely létrehoz egy archívumfájlt. Az archívumfájl másik helyre helyezhető vagy másolható át. Az archívum létrehozható távoli fájlrendszeren, például NFS csatoláson is.

A tar segédprogram egy archívumfájlt hoz létre több fájlból vagy könyvtárból. A tar képes az archívum méretének csökkentése érdekében a fájlok átküldésére egy tömörítő segédprogramon.

1.1. Egyszerű shell-parancsfájl

Az alábbi shell-parancsfájl a tar segítségével hoz létre egy archívumfájlt egy csatolt távoli NFS fájlrendszeren. Az archívumfájl neve további parancssori segédprogramok használatával kerül megállapításra.

```
#!/bin/sh
###################################
#
# NFS-csatolásra biztonsági mentést készítő parancsfájl.
#
###################################

# Mit kell menteni.
backup_files="/home /var/spool/mail /etc /root /boot /opt"

# Hová kell menteni.
dest="/mnt/backup"

# Archívumfájl nevének létrehozása.
day=$(date +%A)
hostname=$(hostname -s)
archive_file="$hostname-$day.tgz"

# Kezdési állapotüzenet kiírása.
echo "$backup_files mentése ide: $dest/$archive_file"
date
echo

# A fájlok mentése a tar segítségével.
tar czf $dest/$archive_file $backup_files

# Befejezési állapotüzenet kiírása.
echo
echo "A mentés kész"
date

# A fájlok részletes felsorolása a $dest könyvtárban a fájlméretek ellenőrzéséhez.
ls -lh $dest
```

- $backup_files: ez a változó felsorolja a menteni kívánt könyvtárakat. A listát igényeinek megfelelően szabja személyre.
- $day: ez a változó tárolja a hét napjait. Ennek használatával a hét minden napjához létrejön egy archívumfájl, így hét napi archiválási előzménnyel fogunk rendelkezni. Ezt számos más módon is el lehet érni, beleértve a date segédprogram használatát.
- $hostname: ez a változó a rendszer rövid gépnevét tárolja. A gépnév az archívum fájlnevében való használatával elérhető, hogy több rendszer napi archívumfájljai ugyanabba a könyvtárba kerülhessenek.
- $archive_file: az archívumfájl teljes neve.
- $dest: az archívumfájl célja. A könyvtárat a mentési parancsfájl végrehajtása előtt létre kell hozni és ebben az esetben csatolni is kell. Az NFS használatával kapcsolatos részletekért lásd a 2. szakasz - Hálózati fájlrendszer (NFS) [177] szakaszt.
- állapotüzenetek: a konzolra az echo segédprogrammal kiírt elhagyható üzenetek.
- tar czf $dest/$archive_file $backup_files: az archívumfájl létrehozására használt tar parancs.
  - c: létrehozza az archívumot.
  - z: az archívumot tömöríti a gzip segédprogrammal.
  - f: archívumfájl használata. Enélkül a tar kimenete a szabványos kimenetre kerül elküldésre.
- ls -lh $dest: ez az elhagyható utasítás hosszú (-l) és közérthető (-h) formátumban kiírja a célkönyvtár tartalmát. Ez az archívumfájl méretének gyors ellenőrzésére használható. Ez az ellenőrzés ugyanakkor nem helyettesíti az archívumfájl tesztelését.

Ez egy egyszerű példa biztonsági mentési parancsfájl. A biztonsági mentést készítő parancsfájl rengeteg beállítást tartalmazhat. A shell parancsfájlok írásával kapcsolatos mélyebb információkat tartalmazó erőforrásokat a 1.4. szakasz - Hivatkozások [250] szakaszban találhat.

1.2. Parancsfájl végrehajtása

1.2.1. Végrehajtás terminálból

A fenti biztonsági mentést készítő parancsfájl végrehajtásának legegyszerűbb módja a tartalom beillesztése egy fájlba, és elmentése például `backup.sh` néven. Ezután kiadható a következő parancs:

```
sudo bash backup.sh
```

Ezzel tesztelhető a parancsfájl megfelelő és elvárt módon való működése.

1.2.2. Végrehajtás cron segítségével

A cron segédprogram használatával automatizálható a parancsfájl végrehajtása. A cron démon lehetővé teszi a parancsfájlok vagy parancsok adott időben történő futtatását.

A cron a `crontab` fájl bejegyzéseivel konfigurálható. A `crontab` fájlok mezőkre vannak osztva:

```
# m h dom mon dow   command
```

- m: a parancs végrehajtásának perce, 0 és 59 között.
- h: a parancs végrehajtásának órája, 0 és 23 között.
- dom: a hónap napja, amikor a parancs végrehajtásra kerül.
- mon: a parancs végrehajtásának hónapja 1 és 12 között.
- dow: a hét napja, amikor a parancs végrehajtásra kerül, 0 és 7 között. A vasárnap megadható 0-ként és 7-ként is, mindkét érték érvényes.
- command: a végrehajtandó parancs.

A `crontab` fájl bejegyzéseinek hozzáadásához vagy módosításához használja a crontab -e parancsot. A `crontab` fájl tartalma megjeleníthető a crontab -l parancs használatával.

A fenti backup.sh parancsfájl a cron segítségével történő végrehajtásához adja ki a következő parancsot:

```
sudo crontab -e
```

A crontab -e parancs sudo-val történő használata a root felhasználó crontab fájlját szerkeszti. Erre akkor van szükség, ha csak a root felhasználó által elérhető könyvtárakról is készít biztonsági mentést.

Vegye fel a következő bejegyzést a `crontab` fájlba:

```
# m h dom mon dow   command
0 0 * * * bash /usr/local/bin/backup.sh
```

A backup.sh parancsfájl minden délben végrehajtásra kerül.

A bejegyzés megfelelő végrehajtása érdekében a backup.sh parancsfájlt át kell másolni a `/usr/local/bin/` könyvtárba.

A crontab beállításaival kapcsolatos további, mélyebb információkért lásd a 1.4. szakasz - Hivatkozások [250] szakaszt.

1.3. Visszaállítás az archívumból

Az archívumot létrehozása után fontos tesztelni is. Az archívum tesztelhető az általa tartalmazott fájlok listáztatásával, de a legjobb teszt egy fájl visszaállítása az archívumból.

- Az archívum tartalmának kiíratásához adja ki a következő parancsot:

```
tar -tzvf /mnt/backup/host-Monday.tgz
```

- Az archívum egy fájljának visszaállításához egy másik könyvtárba:

```
tar -xzvf /mnt/backup/host-Monday.tgz -C /tmp etc/hosts
```

A tar -C kapcsolója átirányítja a kibontott fájlokat a megadott könyvtárba. A fenti példa az `/etc/hosts` fájlt a `/tmp/etc/hosts` helyre bontja ki. A tar újra létrehozza a fájlt tartalmazó könyvtárszerkezetet.

Figyelje meg, hogy a helyreállítandó fájl útvonalának elejéről lemaradt a / jel.

- Az archívum összes fájljának helyreállításához adja ki a következő parancsot:

```
cd /
sudo tar -xzvf /mnt/backup/host-Monday.tgz
```

Ez felülírja a fájlrendszeren éppen megtalálható fájlokat.

1.4. Hivatkozások

- A shell-parancsfájlok írásával kapcsolatos további információkért lásd az Advanced Bash-Scripting Guide[1] leírást.
- A Teach Yourself Shell Programming in 24 Hours[2] című könyv online elérhető, és remek információforrás a shell parancsfájlok írásához.
- A CronHowto wikioldal[3] a cron speciális lehetőségeivel kapcsolatos részleteket tartalmaz.
- A tar további lehetőségeivel kapcsolatban lásd a GNU tar kézikönyvét[4].
- A Wikipedia Backup Rotation Scheme[5] cikke a további mentésforgatási sémákról tartalmaz információkat.
- A parancsfájl a tar segédprogramot használja az archívum létrehozásához, de számos más parancssori segédprogram is használható, például:
  - cpio[6]: fájlok archívumokba másolására és azokból kibontására használható.
  - dd[7]: a coreutils csomag része, alacsony szintű segédprogram adatok egyik formátumból a másikba másolására.
  - rsnapshot[8]: teljes fájlrendszerek másolatainak készítésére használatos fájlrendszer-pillanatkép segédprogram.

2. Archívumforgatás

A 1. szakasz - Shell-parancsfájlok [247] szakaszban található shell-parancsfájl csak hét különböző archívum létrehozását teszi lehetővé. Ha a kiszolgáló adatai nem változnak gyakran, akkor ez elég lehet. Ha azonban a kiszolgáló nagy adatmennyiséget kezel, sokkal robusztusabb forgatási sémát kell használni.

2.1. NFS archívumok forgatása

Ebben a szakaszban a shell-parancsfájlt kibővítjük, és nagyapa-apa-fiú forgatási sémát (havi-heti-napi) valósítunk meg:

- A forgatás napi mentést készít vasárnaptól péntekig.
- Szombaton heti mentés készül, havonta négy heti mentést biztosítva.
- A havi mentés a hónap első napján készül, kéthavi mentést forgatva a hónap párossága vagy páratlansága alapján.

Az új parancsfájl a következő:

```
#!/bin/bash
###################################
#
# NFS-csatolásra biztonsági mentést készítő parancsfájl
# nagyapa-apa-fiú forgatással.
#
###################################

# Mit kell menteni.
backup_files="/home /var/spool/mail /etc /root /boot /opt"

# Hová kell menteni.
dest="/mnt/backup"

# Változók beállítása az archívum fájlnevéhez.
day=$(date +%A)
hostname=$(hostname -s)

# A hónap hetének (1-4) meghatározása.
day_num=$(date +%d)
if (( $day_num <= 7 )); then
        week_file="$hostname-week1.tgz"
elif (( $day_num > 7 && $day_num <= 14 )); then
        week_file="$hostname-week2.tgz"
elif (( $day_num > 14 && $day_num <= 21 )); then
        week_file="$hostname-week3.tgz"
elif (( $day_num > 21 && $day_num < 32 )); then
        week_file="$hostname-week4.tgz"
fi
```

```
# A hónap páros vagy páratlan.
month_num=$(date +%m)
month=$(expr $month_num % 2)
if [ $month -eq 0 ]; then
        month_file="$hostname-month2.tgz"
else
        month_file="$hostname-month1.tgz"
fi

# Archívumfájl nevének létrehozása.
if [ $day_num == 1 ]; then
 archive_file=$month_file
elif [ $day != "Saturday" ]; then
        archive_file="$hostname-$day.tgz"
else
 archive_file=$week_file
fi

# Kezdési állapotüzenet kiírása.
echo "$backup_files mentése ide: $dest/$archive_file"
date
echo

# A fájlok mentése a tar segítségével.
tar czf $dest/$archive_file $backup_files

# Befejezési állapotüzenet kiírása.
echo
echo "A mentés kész"
date

# A fájlok részletes felsorolása a $dest könyvtárban a fájlméretek ellenőrzéséhez.
ls -lh $dest/
```

A parancsfájl a 1.2. szakasz - Parancsfájl végrehajtása [248] szakaszban leírt módon hajtható végre.

A biztonsági mentés adathordozóit a katasztrófák eshetősége miatt ajánlott a géptől fizikailag messze tárolni. A példában a mentés adathordozója egy NFS-megosztást biztosító másik kiszolgáló. Az NFS-kiszolgáló mozgatása semmi esetre sem lenne praktikus. A kapcsolat sebességétől függően egy lehetőség az archívumfájl átmásolása WAN kapcsolaton egy másik helyen lévő kiszolgálóra.

Másik lehetőség az archívumfájl külső merevlemezre másolása, amely elszállítható. Mivel a külső merevlemezek ára folyamatosan csökken, költséghatékony lehet két meghajtó használata minden archívumszinthez. Ez lehetővé teszi, hogy az egyik külső meghajtó a mentendő kiszolgálóhoz legyen csatlakoztatva, míg a másik egy biztonságos távoli helyen van.

2.2. Szalagos meghajtók

A kiszolgálóhoz csatlakoztatott szalagos meghajtó is használható NFS-megosztás helyett. A szalagos meghajtó használata egyszerűsíti az archívumforgatást, valamint az adathordozó távoli helyre szállítását is.

Szalagos meghajtó használatakor a parancsfájl fájlnévre vonatkozó részei nem szükségesek, mivel a dátum közvetlenül kerül elküldésre a szalagos eszköznek. Csak néhány, a szalagot kezelő parancsra van szükség, ehhez a cpio csomag által tartalmazott mt nevű mágnesszalag-vezérlő segédprogramot használjuk.

A szalagos meghajtó használatához módosított shell-parancsfájl:

```
#!/bin/bash
###################################
#
# Szalagra biztonsági mentést készítő parancsfájl
#
###################################

# Mit kell menteni.
backup_files="/home /var/spool/mail /etc /root /boot /opt"

# Hová kell menteni.
dest="/dev/st0"

# Kezdési állapotüzenet kiírása.
echo "$backup_files mentése ide: $dest/$archive_file"
date
echo

# A szalag biztosan legyen visszatekerve.
mt -f $dest rewind

# A fájlok mentése a tar segítségével.
tar czf $dest $backup_files

# Visszatekerés és a szalag kiadása.
mt -f $dest rewoffl

# Befejezési állapotüzenet kiírása.
echo
echo "A mentés kész"
date
```

Az alapértelmezett eszköznév SCSI szalagos meghajtó esetén a `/dev/st0`. Ehelyett a rendszerének megfelelő eszközútvonalat használja.

A szalagos meghajtóról való helyreállítás alapvetően ugyanaz, mint a fájlból történő. Egyszerűen tekerje vissza a szalagot, és a fájlútvonal helyett használja az eszközútvonalat. Az `/etc/hosts` fájl visszaállítása például a `/tmp/etc/hosts` helyre:

```
mt -f /dev/st0 rewind
tar -xzf /dev/st0 -C /tmp etc/hosts
```

3. Bacula

A Bacula egy biztonságimentés-készítő program, amely lehetővé teszi az adatok mentését, visszaállítását és ellenőrzését a hálózatán. Léteznek Bacula kliensek Linux, Windows és Mac OSX rendszerekre is, ezzel keresztplatformos hálózati megoldássá emelve azt.

3.1. Áttekintés

A Bacula több, a mentendő fájlok és a mentési hely kezelésére szolgáló összetevőből és szolgáltatásból áll:

- Bacula Director: ez a szolgáltatás vezérli az összes mentési, visszaállítási, ellenőrzési és archiválási műveletet.
- Bacula Console: ez az alkalmazás lehetővé teszi a kommunikációt a Directorral. A konzolnak három változata van:
  - Szövegalapú parancssori verzió.
  - Gnome-alapú GTK+ felület.
  - wxWidgets grafikus felület.
- Bacula File: ez ismert Bacula Client programként is. Ezt az alkalmazást a mentendő gépekre kell telepíteni, és a Director által kért adatokért felelős.
- Bacula Storage: az adatok fizikai adathordozóra mentését és visszaállítását végrehajtó programok.
- Bacula Catalog: az összes mentett fájl fájlindexeinek és kötetadatbázisainak karbantartásáért felelős, lehetővé téve az összes archivált fájl gyors megkeresését és visszaállítását. A Catalog három különböző adatbázis-kezelőt támogat, ezek a MySQL, PostgreSQL és SQLite.
- Bacula Monitor: lehetővé teszi a Director, a File démonok és a Storage démonok megfigyelését. A Monitor jelenleg csak GTK+ felületű alkalmazásként érhető el.

Ezek a szolgáltatások és alkalmazások több kiszolgálón és kliensen is futhatnak, vagy telepíthetők egy gépre is, ha csak egy lemezt vagy kötetet kell menteni.

3.2. Telepítés

A különböző Bacula összetevőket több csomag tartalmazza. A Bacula telepítéséhez adja ki a következő parancsot:

```
sudo apt-get install bacula
```

Alapértelmezésben a bacula csomag egy MySQL adatbázist használ a Cataloghoz. Ha inkább a SQLite vagy PostgreSQL egyikét szeretné használni, akkor telepítse a bacula-director-sqlite3 vagy bacula-director-pgsql csomagot.

A telepítési folyamat bekéri az adatbázis adminisztrátorának és a bacula adatbázis tulajdonosának hitelesítési adatait. Az adatbázis adminisztrátorának rendelkeznie kell az adatbázis létrehozásához szükséges jogosultságokkal, további információkért lásd a 1. szakasz - MySQL [160] szakaszt.

3.3. Beállítás

A Bacula konfigurációs fájljai a „{}” zárójelekkel határolt direktívákból álló erőforrások alapján vannak formázva. Minden Bacula-összetevőhöz tartozik egy önálló fájl az `/etc/bacula` könyvtárban.

A különböző Bacula-összetevőknek fel kell hatalmazniuk magukat egymás felé. Erre szolgál a password direktíva. A Storage erőforrás jelszavának például az `/etc/bacula/bacula-dir.conf` fájlban meg kell egyeznie a Director erőforrás jelszavával az `/etc/bacula/bacula-sd.conf` fájlban.

Alapértelmezésben a Client1 nevű háttérfeladat alapértelmezésben be van állítva a Bacula Catalog archiválására. Ha a kiszolgálóval több kliens mentését tervezi, akkor a feladat nevét valamivel jellegzetesebbre kell módosítania. A név módosításához szerkessze az `/etc/bacula/bacula-dir.conf` fájlt:

```
#
# Az elsődleges éjszakai mentési feladat definiálása
#   Ez a feladat alapértelmezésben a lemezre ment
Job {
  Name = "BackupServer"
  JobDefs = "DefaultJob"
  Write Bootstrap = "/var/lib/bacula/Client1.bsr"
}
```

A fenti példa a feladat nevét BackupServerre változtatta, a gépnévnek megfelelően. A „BackupServer” helyett saját gépének nevét használja, vagy más leíró nevet.

A Console segítségével lekérdezhetők a feladatok a Directortól, de a Console nem root felhasználóval való használatához a felhasználónak a bacula csoportban kell lennie. Adja ki a következő parancsot felhasználó felvételéhez a bacula csoportba:

```
sudo adduser felhasználónév bacula
```

A felhasználónév helyére a tényleges felhasználónevet írja. Ha az aktuális felhasználót adja hozzá, akkor ki, majd újra be kell jelentkeznie az új jogosultságok életbe lépéséhez.

3.4. Helyi gép mentése

Ez a szakasz leírja, hogyan mentheti egyetlen gép megadott könyvtárait helyi szalagos meghajtóra.

- Elsőként a tároló eszközt kell beállítani. Szerkessze az `/etc/bacula/bacula-sd.conf` fájlt, és vegye fel a következőket:

```
Device {
  Name = "Tape Drive"
  Device Type = tape
  Media Type = DDS-4
  Archive Device = /dev/st0
```

```
  Hardware end of medium = No;
  AutomaticMount = yes;               # az eszköz beolvasása a megnyitásakor
  AlwaysOpen = Yes;
  RemovableMedia = yes;
  RandomAccess = no;
  Alert Command = "sh -c 'tapeinfo -f %c | grep TapeAlert'"
}
```

A példa egy DDS-4 szalagos meghajtóhoz készült. Módosítsa a Media Type és Archive Device sorokat a hardverének megfelelően.

A fájl további példáinak egyikét is kiveheti megjegyzésből.

- Az `/etc/bacula/bacula-sd.conf` fájl szerkesztése után újra kell indítani a Storage démont:

```
sudo /etc/init.d/bacula-sd restart
```

- Most vegyen fel egy Storage erőforrást az `/etc/bacula/bacula-dir.conf` fájlba az új eszköz használatához:

```
# A "TapeDrive" tárolóeszköz meghatározása
Storage {
  Name = TapeDrive
  # Ne használja a "localhost" értéket
  Address = backupserver              # Itt teljes képzésű nevet használjon
  SDPort = 9103
  Password = "Cv70F6pf1t6pBopT4vQOnigDrR0v3LT3Cgkiyj"
  Device = "Tape Drive"
  Media Type = tape
}
```

Az Address direktívának a kiszolgáló teljes képzésű tartománynevét kell tartalmaznia. A backupserver helyére a tényleges gépnevet írja.

Győződjön meg róla, hogy a Password direktíva az `/etc/bacula/bacula-sd.conf` fájlban lévővel azonos jelszót tartalmaz.

- A következők hozzáadásával hozzon létre egy új FileSet erőforrást, amely meghatározza a mentendő könyvtárakat:

```
# LocalhostBacup FileSet.
FileSet {
  Name = "LocalhostFiles"
  Include {
    Options {
      signature = MD5
      compression=GZIP
    }
    File = /etc
    File = /home
  }
```

```
}
```

Ez a FileSet az `/etc` és `/home` könyvtárakat menti. Az Options erőforrás direktívái megadják, hogy a FileSet hozzon létre minden mentett fájlhoz MD5 aláírást, és a fájlokat GZIP használatával tömörítse.

- Ezután hozzon létre egy új Schedule erőforrást a mentési feladathoz:

```
# LocalhostBackup ütemezés – napi.
Schedule {
  Name = "LocalhostDaily"
  Run = Full daily at 00:01
}
```

A feladat minden nap éjfél és dél után egy perccel fut le. Számos további ütemezési beállítás is elérhető.

- Végül hozza létre a Job erőforrást:

```
# Helyi gép mentése.
Job {
  Name = "LocalhostBackup"
  JobDefs = "DefaultJob"
  Enabled = yes
  Level = Full
  FileSet = "LocalhostFiles"
  Schedule = "LocalhostDaily"
  Storage = TapeDrive
  Write Bootstrap = "/var/lib/bacula/LocalhostBackup.bsr"
}
```

A feladat minden nap teljes mentést végez a szalagos meghajtóra.

- Minden felhasznált szalaghoz szükség van egy címkére. Ha az aktuális szalagnak nincs címkéje, akkor a Bacula e-mailben értesíti erről. Adja ki a következő parancsot szalag felcímkézéséhez a Console használatával:

```
bconsole
```

- A Bacula Console parancssorában adja ki a következőt:

```
label
```

- Ez rákérdez a Storage erőforrásra:

```
Automatically selected Catalog: MyCatalog
Using Catalog "MyCatalog"
The defined Storage resources are:
     1: File
```

```
     2: TapeDrive
Select Storage resource (1-2):2
```

- Adja meg az új Volume nevet:

```
Enter new Volume name: Vasárnap
Defined Pools:
     1: Default
     2: Scratch
```

  A Vasárnap helyére a kívánt címkét írja.

- Most válassza ki a Pool-t:

```
Select the Pool (1-2): 1
Connecting to Storage daemon TapeDrive at backupserver:9103 ...
Sending label command for Volume "Sunday" Slot 0 ...
```

Gratulálunk, ezzel elkészült a Bacula beállításával a helyi gép biztonsági mentésére a géphez kapcsolt szalagos meghajtóra.

3.5. Információforrások

- A Bacula további konfigurációs beállításaival kapcsolatban nézze meg a Bacula User's Manual[9] oldalt.
- A Bacula honlapja[10] beszámol a Bacula legfrissebb híreiről és fejlesztéseiről.
- Nézze meg az Ubuntu wiki Bacula[11] oldalát is.

19. fejezet - Virtualizáció

A virtualizációt számos különböző környezetben és helyzetben vezetik be. Fejlesztőként a virtualizáció olyan elzárt környezetet biztosít, amelyben tetszőleges fejlesztést végezhet az elsődleges munkakörnyezet tönkretételének veszélye nélkül. Rendszergazdaként a virtualizációval a szolgáltatások egyszerűbben elkülöníthetők, és igény szerint átrendezhetők.

Az Ubuntu által alapértelmezésben támogatott virtualizációs technológia a KVM, amely kihasználja az Intel és AMD hardverekbe épített virtualizációs kiterjesztéseket. A virtualizációs kiterjesztések nélküli hardverekhez népszerű megoldások a Xen és Qemu.

1. libvirt

A libvirt programkönyvtárat többféle virtualizációs technológia összekapcsolására használják. A libvirt megismerésének megkezdése előtt győződjön meg róla, hogy hardvere támogatja a KVM-hez szükséges virtualizációs kiterjesztéseket. Adja ki a következő parancsot:

```
kvm-ok
```

Megjelenik egy üzenet, amely közli hogy a CPU támogatja vagy nem támogatja a hardveres virtualizációt.

A legtöbb olyan számítógépen, amelynek processzora támogatja a virtualizációt, a virtualizáció bekapcsolásához engedélyezni kell egy BIOS beállítást.

1.1. Virtuális hálózatkezelés

A külső hálózat elérését a virtuális gépeknek több különböző módon is biztosítani lehet. Az alapértelmezett virtuálishálózat-beállítás a usermode hálózatkezelés, amely a SLIRP protokollt használja, és a forgalmat a gazda csatolóján keresztül kell a külső hálózatra NAT-olni.

A virtuális gépek szolgáltatásainak külső gépek általi eléréséhez be kell állítani egy hidat. Ez lehetővé teszi a virtuális csatolóknak a külső hálózat elérését a fizikai csatolón keresztül, így a hálózat többi része felé normál kiszolgálóként jelennek meg. A híd beállításával kapcsolatos további információkért lásd a 1.4. szakasz - Híd [37] szakaszt.

1.2. Telepítés

A szükséges csomagok telepítéséhez adja ki a következő parancsot:

```
sudo apt-get install kvm libvirt-bin
```

A libvirt-bin telepítése után a virtuális gépek kezelésére használt felhasználót fel kell venni a libvirtd csoportba. Ezzel a felhasználó hozzáférést kap a speciális hálózatkezelési beállításokhoz.

Adja ki a következő parancsot:

```
sudo adduser $USER libvirtd
```

Ha a kiválasztott felhasználó a jelenlegi felhasználó, akkor ki, majd újra be kell lépnie az új csoporttagság életbe lépéséhez.

Ezután készen áll egy vendég operációs rendszer telepítésére. Az operációs rendszer virtuális gépekre telepítésének folyamata megegyezik a közvetlenül a hardverre történő telepítés folyamatával. A telepítést vagy automatizálnia kell, vagy billentyűzetet és monitort kell csatlakoztatnia a fizikai géphez.

A virtuális gépek esetén a grafikus felhasználói felület megfelel a fizikai billentyűzet és egér használatának. A grafikus felület telepítése helyett a virt-viewer alkalmazás használható a virtuális gép konzoljára csatlakozáshoz VNC használatával. További információkért lásd a 1.6. szakasz - Virtuálisgép-megjelenítő [264] szakaszt.

There are several ways to automate the Ubuntu installation process, for example using preseeds, kickstart, etc. Refer to the Ubuntu Installation Guide[1] for details.

Az ubuntus virtuális gép telepítésének még egy módja az ubuntu-vm-builder használata. Az ubuntu-vm-builder lehetővé teszi speciális partíciók beállítását, egyéni telepítés utáni parancsfájlok futtatását stb. Részletekért lásd a 2. szakasz - JeOS és vmbuilder [266] szakaszt.

1.3. virt-install

A virt-install a python-virtinst csomag része. A telepítéséhez adja ki a következő parancsot:

```
sudo apt-get install python-virtinst
```

A virt-install használatakor számos lehetőség érhető el. Például:

```
sudo virt-install -n web_fejleszt -r 256 -f web_fejleszt.img \ -s 4 -c jeos.iso --accelerate \ --co
```

- -n web_fejleszt: ebben a példában a virtuális gép neve web_fejleszt lesz.
- -r 256: megadja a virtuális gép által használandó memória méretét.
- -f web_fejleszt.img: jelzi a virtuális gép útvonalát, ez fájl, partíció vagy logikai kötet lehet. Ebben a példában ez egy `web_fejleszt.img` nevű fájl.
- -s 4: a virtuális lemez mérete.
- -c jeos.iso: virtuális CD-ROM-ként használandó fájl. A fájl lehet ISO fájl, vagy a kiszolgáló fizikai CD-ROM eszközének útvonala.
- --accelerate: engedélyezi a kernel gyorsítási technológiáit.
- --vnc: a vendég virtuális konzoljának exportálása VNC segítségével.
- --noautoconsole: nem csatlakozik automatikusan a virtuális gép konzoljára.
- -v: teljesen virtualizált vendéget hoz létre.

A virt-install elindítása után csatlakozhat a virtuális gép konzoljára, ezt helyileg grafikus felületen, vagy távolról a virt-viewer segédprogrammal teheti meg.

1.4. virt-clone

A virt-clone alkalmazás virtuális gépek egymásra másolására használható. Például:

[1] https://help.ubuntu.com/10.04 LTS/installation-guide/

```
sudo virt-clone -o web_fejleszt -n adatbaz_fejleszt -f /útvonal/adatbaz_fejleszt.img --connect=qemu
```

- -o: az eredeti virtuális gép.
- -n: az új virtuális gép neve.
- -f: az új virtuális gép által használható fájl, logikai kötet vagy partíció útvonala.
- --connect: megadja a hypervisort, amelyhez csatlakozni kell.

A virt-clone problémáinak elhárításához használhatja a -d vagy --debug kapcsolókat is.

A web_fejleszt és adatbaz_fejleszt helyett a megfelelő virtuális gépek neveit adja meg.

1.5. Virtuális gépek kezelése

1.5.1. virsh

Számos segédprogram érhető el a virtuális gépek és a libvirt kezeléséhez. A virsh segédprogram a parancssorból használható. Néhány példa:

- A futó virtuális gépek felsorolása:

```
virsh -c qemu:///system list
```

- Virtuális gép elindítása

```
virsh -c qemu:///system start web_fejleszt
```

- Hasonlóképpen, a virtuális gép elindítása rendszerindításkor:

```
virsh -c qemu:///system autostart web_fejleszt
```

- Virtuális gép újraindítása:

```
virsh -c qemu:///system reboot web_fejleszt
```

- A virtuális gépek állapota a későbbi visszaállítás érdekében fájlba menthető. A következő elmenti a virtuális gép állapotát, a dátumnak megfelelően elnevezett fájlba:

```
virsh -c qemu:///system save web_fejleszt web_fejleszt-022708.state
```

  A virtuális gép elmentése után nem fog tovább futni.

- A mentett virtuális gép visszaállítható:

```
virsh -c qemu:///system restore web_fejleszt-022708.state
```

- Virtuális gép leállítása:

```
virsh -c qemu:///system shutdown web_fejleszt
```

- A virtuális gépbe CD-ROM eszköz csatolható:

```
virsh -c qemu:///system attach-disk web_fejleszt /dev/cdrom /media/cdrom
```

A fenti példákban a web_fejleszt helyett használja a megfelelő virtuális gép nevét, a `web_fejleszt-022708.state` helyett pedig egy jellemző fájlnevet.

1.5.2. Virtuálisgép-kezelő

A virt-manager csomag tartalmaz egy helyi és távoli virtuális gépek kezelésére szolgáló grafikus alkalmazást. A virt-manager telepítéséhez adja ki a következő parancsot:

```
sudo apt-get install virt-manager
```

Mivel a virt-manager működéséhez grafikus felület szükséges, a telepítése az éles kiszolgáló helyett egy munkaállomásra vagy tesztgépre javasolt. A helyi libvirt szolgáltatáshoz csatlakozáshoz adja ki a következő parancsot:

```
virt-manager -c qemu:///system
```

Másik gépen futó libvirt szolgáltatáshoz a következő parancs kiadásával csatlakozhat:

```
virt-manager -c qemu+ssh://virtcsp.tartomány.hu/system
```

A fenti példa feltételezi, hogy a felügyelő rendszer és a virtcsp.tartomány.hu közötti SSH kapcsolat már be van állítva és SSH-kulcsokat használ a hitelesítésre. Az SSH-kulcsok amiatt szükségesek, mert a libvirt a jelszókérést egy másik folyamatnak küldi el. Az SSH beállításával kapcsolatos információkért lásd az 1. szakasz - OpenSSH kiszolgáló [49] szakaszt.

1.6. Virtuálisgép-megjelenítő

A virt-viewer alkalmazás lehetővé teszi a csatlakozást a virtuális gép konzoljára. A virt-viewer nem igényel grafikus felületet a virtuális géppel való együttműködéshez.

A virt-viewer telepítéséhez adja ki a következő parancsot:

```
sudo apt-get install virt-viewer
```

A virtuális gép telepítése és elindítása után a konzoljához a következő parancs kiadásával csatlakozhat:

```
virt-viewer -c qemu:///system web_fejleszt
```

A virt-managerhez hasonlóan a virt-viewer is képes távoli kiszolgálókhoz csatlakozni kulcshitelesítést használó SSH kapcsolaton:

```
virt-viewer -c qemu+ssh://virtcsp.tartomány.hu/system web_fejleszt
```

Ne feledje a web_fejleszt helyett a megfelelő virtuális gép nevét behelyettesíteni.

A hidat használó hálózati csatoló esetén beállíthat SSH hozzáférést a virtuális gépre. További részletekért lásd az 1. szakasz - OpenSSH kiszolgáló [49] és 1.4. szakasz - Híd [37] szakaszokat.

1.7. Információforrások

- További részletekért lásd a KVM[2] honlapját.
- A libvirttel kapcsolatos további információkért lásd a libvirt honlapját[3].
- A virtuálisgép-kezelő[4] weboldala a virt-manager fejlesztéséről tartalmaz további információkat.
- Az Ubuntu virtualizációs technológiáiról a freenode[5] #ubuntu-virt IRC-csatornáján is beszélgethet.
- Az Ubuntu wiki KVM[6] oldala szintén hasznos olvasmány.

2. JeOS és vmbuilder

2.1. Bevezetés

2.1.1. Mi az a JeOS

Az JeOS az Ubuntu kiszolgáló operációs rendszer egy hatékony változata, amelyet kifejezetten virtuális eszközökhöz állítottak össze. Nem érhető el letölthető ISO-ként, csak:

- A kiszolgáló változat telepítésekor (az első képernyőn az F4 megnyomása után kiválaszthatja a „Minimális telepítés” lehetőséget, ez azonos a JeOS csomagkészletével).
- Felépíthető az Ubuntu vmbuilder eszközével, amelyet itt ismertetünk.

A JeOS az Ubuntu kiszolgáló változatának specializált telepítése, amely a virtualizált környezetben való futáshoz minimálisan szükséges elemeket tartalmazó kernelt használ.

Az Ubuntu JeOS a VMware legújabb virtualizációs termékeinek kulcsfontosságú teljesítménynövelő technikáinak kihasználására készült. A csökkentett méret és az optimalizált teljesítmény kombinációja biztosítja, hogy az Ubuntu JeOS változata a kiszolgáló-erőforrások különösen hatékony felhasználását nyújtsa nagy virtuális telepítéseken.

A szükségtelen meghajtóprogramok nélkül, és csak a minimálisan szükséges csomagokkal, a független szoftvergyártók teljesen az igényeikre szabhatják támogató operációs rendszerüket. Nyugodtak lehetnek afelől, hogy a frissítések, érkezzenek biztonsági vagy szolgáltatásbővítési okból, az adott környezetben szükséges minimumra korlátozódnak. Cserébe a JeOS alapokra épített virtuális eszközöket telepítő felhasználóknak kevesebb frissítést kell kezelniük, emiatt a teljes kiszolgálóhoz képest csökken a rendszerek karbantartási igénye.

2.1.2. Mi az a vmbuilder

A vmbuilder szükségtelenné teszi a JeOS ISO letöltését. A vmbuilder letölti a szükséges csomagokat, és percek alatt felépíti az igényeinek megfelelő virtuális gépet. A vmbuilder egy parancsfájl, amely automatizálja a használatra kész linuxos virtuális gép elkészítésének folyamatát. A jelenleg támogatott hypervisorok a KVM és a Xen.

Parancssori kapcsolók segítségével további csomagokat vehet fel vagy meglévőeket távolíthat el, kiválaszthatja a használni kívánt Ubuntu verziót vagy tükröt stb. Sok memóriával rendelkező új gépen, a `/dev/shm` alatti tmpdir vagy tmpfs, valamint helyi tükör használatával akár egy perc alatt is összeállíthat egy virtuális gépet.

Az ubuntu-vm-builder parancsfájl minden hírverés nélkül az Ubuntu 8.04 LTS-ben mutatkozott be először, mint a fejlesztőket segítő gányolás, amely megkönnyíti a kód tesztelését virtuális gépben a rendszeres újrakezdés nélkül. Ahogy egyes ubuntus rendszergazdák észrevették a jelenlétét, néhányan fejleszteni kezdték, és olyan sok helyzet kezelésére tették alkalmassá, hogy a fejlesztője Pythonban újraírta az Intrepidhez, néhány új fejlesztési céllal:

- Más disztribúciók számára is használható legyen.
- Bővítmények kezeljék a virtualizációs interakciókat, így más virtuális környezetek támogatása könnyen hozzáadható.
- A parancssoros felület mellett egy könnyen karbantartható webes felület is rendelkezésre álljon.

Az általános elvek és parancsok azonban ugyanazok maradtak.

2.2. Kiinduló telepítés

Feltételezzük, hogy a használt gépre helyileg telepítette és beállította a libvirt és KVM szoftvereket. Ezzel kapcsolatos részletekért lásd:

- 1. szakasz - libvirt [261]
- A KVM[7] wiki oldalát.

Feltételezzük még, hogy ismeri egy szöveges alapú szövegszerkesztő, például a nano vagy a vi használatát. Ha még nem használta ezeket, akkor nézze meg az ismertetésüket a PowerUsersTextEditors[8] wiki oldalon. Ezt az ismertetőt KVM-alapokra készítettük, de az alapelv más virtualizációs technológiák esetén is ugyanez.

2.2.1. A vmbuilder telepítése

Telepítse a python-vm-builder csomagot. Adja ki a következő parancsot:

```
sudo apt-get install python-vm-builder
```

Ha a Hardy kiadást használja, a leírás zömét a csomag ubuntu-vm-builder nevű régebbi verzióján is végrehajthatja, az eszköz szintaxisa alig változott.

2.3. A virtuális gép megadása

A virtuális gép megadása az Ubuntu vmbuilder segítségével nagyon egyszerű, de az alábbiakat figyelembe kell venni:

- Ha a virtuális eszköz továbbadására készül, ne feltételezze, hogy a végfelhasználó tudni fogja, hogyan igazíthatja a lemezméretet az igényeihez, emiatt vagy készítsen nagy virtuális lemezt, vagy dokumentálja alaposan a hely megnövelésének módját. Jó megközelítés lehet az adatok külső tárolón történő elhelyezése is.
- Mivel memóriát sokkal egyszerűbb foglalni a virtuális géphez, a memória méretét az eszköz működéséhez biztonságos minimumra kell állítani.

A vmbuilder parancsnak két fő paramétere van: a virtualizációs technológia (hypervisor) és a cél disztribúció. A további paraméterekből igen sok van és a következő parancs kiadásával kérhetők le:

[8] https://help.ubuntu.com/community/PowerUsersTextEditors

```
vmbuilder --help
```

2.3.1. Alapvető paraméterek

Mivel ez a példa a KVM-re és az Ubuntu 10.04 LTS (Lucid Lynx) kiadására épül, valamint ugyanez a virtuális gép többször is újjá lesz építve, a vmbuilder hívásához a következő paramétereket kell használni:

```
sudo vmbuilder kvm ubuntu --suite lucid --flavour virtual --arch i386 -o --libvirt qemu:///system
```

A --suite kapcsoló megadja az Ubuntu kiadást, a --flavour megadja, hogy a virtuális kernelt kell használni (ezt kell JeOS lemezkép készítéséhez használni), a --arch megadja, hogy 32 bites gépet használ, a -o felülírja a virtuális gép korábbi változatát, a --libvirt hatására pedig a helyi virtualizációs környezet felveszi a virtuális gépet az elérhető gépek listájába.

Megjegyzés:

- A vmbuildert az általa végrehajtott műveletek természetéből fakadóan rendszergazdai jogosultságokkal kell futtatni, emiatt szükséges a sudo.
- Ha a virtuális gépnek 3 GB-nál több memóriát kell használnia, akkor készítsen 64 bites gépet (--arch amd64).
- Az Ubuntu 8.10-ig a virtuális kernel csak 32 bitre készült el, így ha Hardy alatt szeretne 64 bites gépet készíteni, akkor a --flavour server kapcsolót kell megadnia.

2.3.2. A JeOS telepítési paraméterei

2.3.2.1. A JeOS hálózatkezelése

2.3.2.1.1. Rögzített IP-cím társítása

Mivel a virtuális eszközt számos, nagyon különböző hálózatba lehet telepíteni, nehéz megállapítani a tényleges hálózat pontos típusát. A beállítás megkönnyítése érdekében hasznos lehet a hálózati hardverek szállítóinak megközelítését alkalmazni, vagyis az eszközhöz kiinduló, egy privát osztályú hálózatba tartozó rögzített IP-címet rendelni, amelyet majd a dokumentációban ismertet. Erre általában a 192.168.0.0/255 tartománybeli címek megfelelőek.

Ehhez a következő paramétereket használhatja:

- --ip CÍM: IP-cím pontozott formátumban (alapértelmezésben dhcp, ha nincs megadva)
- --mask ÉRTÉK: IP-maszk pontozott formátumban (alapértelmezésben: 255.255.255.0)
- --net ÉRTÉK: IP-hálózat címe (alapértelmezésben: X.X.X.0)
- --bcast ÉRTÉK: IP broadcast (alapértelmezett: X.X.X.255)
- --gw CÍM: Átjáró címe (alapértelmezett: X.X.X.1)
- --dns CÍM: Névkiszolgáló címe (alapértelmezett: X.X.X.1)

Egyelőre feltételezzük, hogy az alapértelmezett értékek megfelelőek, így az eredményül kapott hívás a következő lesz:

```
sudo vmbuilder kvm ubuntu --suite lucid --flavour virtual --arch i386 -o --libvirt qemu:///system -
```

2.3.2.1.2. A libvirt sablon módosítása híd használatához

Mivel az eszközt valószínűleg távoli gépeknek is el kell majd érniük, a libvirtet úgy kell beállítani, hogy az eszköz a hálózatkezeléshez hidat használjon. Ehhez a vmbuilder sablon mechanizmusát kell használni, az alapértelmezett módosítására.

A munkakönyvtárban létre kell hozni a sablonhierarchiát, és át kell másolni az alapértelmezett sablont:

```
mkdir -p VMBuilder/plugins/libvirt/templates
cp /etc/vmbuilder/libvirt/* VMBuilder/plugins/libvirt/templates/
```

Ezután szerkeszthető a `VMBuilder/plugins/libvirt/templates/libvirtxml.tmpl`, és a következő rész módosítható:

```
<interface type='network'>
  <source network='default'/>
</interface>
```

Erre:

```
<interface type='bridge'>
  <source bridge='br0'/>
</interface>
```

2.3.2.2. Particionálás

A virtuális eszköz particionálásakor figyelembe kell venni, hogy az mire lesz használva. Mivel a legtöbb eszköz az adatokat külön tárolja, az önálló `/var` használatának van értelme.

Ennek megadásához a vmbuilder a --part kapcsolót biztosítja:

```
--part ÚTVONAL
  Lehetővé teszi partíciós tábla megadását az ÚTVONALON lévő partíciós fájlban.
  A fájl minden sorának a következőket kell megadnia:
  (elsőként a root partíciót):
      csatolási-pont méret
  ahol a méret megabájtban értendő. Legfeljebb 4 virtuális lemeze lehet, az új lemez a
  „---” tartalmú sortól kezdődik. Például:
      root 1000
      /opt 1000
      swap 256
```

```
---
/var 2000
/log 1500
```

Ebben az esetben egy `vmbuilder.partition` nevű fájlt kell létrehozni, a következő tartalommal:

```
root 8000
swap 4000
---
/var 20000
```

Ne feledje, hogy mivel virtuális lemezképekről van szó, az itt feltüntetett tényleges méretek a kötetek maximális méretei.

A parancssor most így néz ki:

```
sudo vmbuilder kvm ubuntu --suite lucid --flavour virtual --arch i386 \ -o --libvirt qemu:///system
```

A parancsban használt „\” lehetővé teszi a hosszú parancsok következő sorba törését.

2.3.2.3. Felhasználó és jelszó

A virtuális eszköz beállításához meg kell adni az alapértelmezett felhasználót és jelszót, amely elég általános ahhoz, hogy a saját dokumentációjába bekerülhessen. A dokumentumban később ismertetésre kerül egy olyan parancsfájl megadása, amely a felhasználó az eszközre történő első tényleges bejelentkezésekor lefut, és többek között a jelszó megváltoztatását kéri, így javítva a biztonságot. Ez a példa a „felhasználó” felhasználónevet és a „alapértelmezett” jelszót használja.

Ehhez a következő paraméterek szükségesek:

- --user FELHASZNÁLÓNÉV: A felvenni kívánt felhasználó neve. Alapértelmezés: ubuntu.
- --name TELJESNÉV: A felvenni kívánt felhasználó teljes neve. Alapértelmezés: Ubuntu.
- --pass JELSZÓ: A felvenni kívánt felhasználó jelszava. Alapértelmezés: ubuntu.

A kapott parancssor:

```
sudo vmbuilder kvm ubuntu --suite lucid --flavour virtual --arch i386 \ -o --libvirt qemu:///system
```

2.3.3. Szükséges csomagok telepítése

Ez a példa egy olyan csomag (Limesurvey) telepítését mutatja be, amely MySQL adatbázist használ, és webes felülettel rendelkezik. Emiatt a következők telepítése szükséges az operációs rendszerre:

- Apache
- PHP
- MySQL

- OpenSSH kiszolgáló
- Limesurvey (csomagban elérhető példaprogram)

Ez a vmbuilder --addpkg kapcsolójának többszöri megadásával végezhető el:

```
--addpkg CSOMAG
  A CSOMAG telepítése a vendégre (többször is megadható)
```

A vmbuilder működési módja miatt nem támogatottak azok a csomagok, amelyeknek a telepítés utáni szakaszban kérdéseket kell feltenniük a felhasználónak. Ezeket a csomagokat akkor kell telepíteni, amikor lehetőség van a kérdések megválaszolására. Ez a Limesurvey esetén is így van, emiatt a felhasználó bejelentkezésekor kell telepíteni.

Az olyan csomagok telepíthetők, amelyek egyszerű debconf kérdéseket tesznek fel, mint például a jelszó beállítását kérő mysql-server, de a felhasználó első bejelentkezésekor újra kell konfigurálni.

Ha egyes telepítendő csomagok nem érhetők el a main tárolóból, akkor a további tárolókat a --comp és --ppa kapcsolókkal kell engedélyezni:

```
--components KOMP1,KOMP2,...,KOMPN
           Felvenni kívánt disztribúciókomponensek vesszőkkel elválasztott listája (például main,un
           „main”
--ppa=PPA  A PPA hozzáadása a virtuális gép sources.list fájljához.
```

A Limesurvey jelenleg nem része az archívumnak, így a PPA címét kell megadni, hogy felvételre kerüljön a virtuális gép `/etc/apt/source.list` fájljába. A parancssor a következőkkel bővül:

```
--addpkg apache2 --addpkg apache2-mpm-prefork --addpkg apache2-utils --addpkg apache2.2-common \ --
```

2.3.3.1. OpenSSH

Egy másik kényelmes segédprogram, amelyet érdemes az eszközre telepíteni az OpenSSH, mivel lehetővé teszi a távoli rendszergazdai hozzáférést az eszközhöz. Azonban előre telepített OpenSSH-val nyilvánosan elérhetővé tenni bármilyen eszközt hatalmas biztonsági kockázat, mivel ezek a kiszolgálók ugyanazt a titkos kulcsot fogják használni, így pillanatok alatt feltörhetők. A felhasználói jelszóhoz hasonlóan ebben az esetben is egy parancsfájlt kell használni, amely a felhasználó első bejelentkezésekor telepíti az OpenSSH-t, így az egyes eszközökhöz előállított kulcsok egyediek lesznek. Ehhez egy --firstboot parancsfájlt kell megadni, mivel nem igényel felhasználói közreműködést.

2.3.4. Sebességszempontok

2.3.4.1. Csomag-gyorsítótárazás

Amikor a vmbuilder létrehozza a rendszert, minden csomagot le kell töltenie az egyik hivatalos tárolóból, ami az internetkapcsolat sebességétől, és a tükör terhelésétől függően jelentősen

befolyásolhatja a rendszer összeállítási idejét. Ennek csökkentése érdekében ajánlott helyi tárolót létrehozni (az apt-mirror segítségével), vagy az apt-proxy-hoz hasonló gyorsítótárazó proxyt használni. Ez utóbbi lehetőséget sokkal egyszerűbb megvalósítani, és kevesebb lemezterületet is igényel, ezért ezt mutatjuk be. A telepítéséhez adja ki a következő parancsot:

```
sudo apt-get install apt-proxy
```

Ezután az üres proxy használatra kész a http://tükörcíme:9999 címen, az ubuntu tároló pedig a /ubuntu alatt található. A vmbuilder a --mirror kapcsoló hatására fogja használatba venni:

```
--mirror=URL  Az URL címen található Ubuntu tükör használata az alapértelmezett
              helyett (http://archive.ubuntu.com/ubuntu hivatalos
              architektúrákhoz, és http://ports.ubuntu.com/ubuntu-ports
              egyébként)
```

A parancssor a következővel bővül:

```
--mirror http://tükörcíme:9999/ubuntu
```

Az itt megadott tükör címe kerül felhasználásra az újonnan létrehozott vendég `/etc/apt/sources.list` fájljában, így itt a vendég által feloldható címet érdemes használni, vagy betervezni a cím későbbi törlését, például egy --firstboot parancsfájlban.

2.3.4.2. Helyi tükör telepítése

Nagyobb környezetben hasznos lehet az Ubuntu tárolók helyi tükrének elkészítése. Az apt-mirror csomag biztosítja a tükrözést elvégző parancsfájlt. Minden támogatott kiadáshoz és architektúrához biztosítson 20 GB szabad helyet.

Alapértelmezésben az apt-mirror az `/etc/apt/mirror.list` beállítófájlt használja. Telepítéskor csak a helyi gép architektúráját replikálja. Ha más architektúrákat is támogatni szeretne a tükrön, egyszerűen kettőzze meg a „deb” kezdetű sorokat, és cserélje a deb kulcsszót a /deb-{arch} kulcsszóra, ahol az arch az i386, amd64 stb egyike lehet. Egy amd64 gépen az i386 archívumok tükrözéséhez a következő szükséges:

```
deb  http://archive.ubuntu.com/ubuntu lucid main restricted universe multiverse
/deb-i386  http://archive.ubuntu.com/ubuntu lucid main restricted universe multiverse

deb  http://archive.ubuntu.com/ubuntu lucid-updates main restricted universe multiverse
/deb-i386  http://archive.ubuntu.com/ubuntu lucid-updates main restricted universe multiverse

deb http://archive.ubuntu.com/ubuntu/ lucid-backports main restricted universe multiverse
/deb-i386  http://archive.ubuntu.com/ubuntu lucid-backports main restricted universe multiverse

deb http://security.ubuntu.com/ubuntu lucid-security main restricted universe multiverse
/deb-i386  http://security.ubuntu.com/ubuntu lucid-security main restricted universe multiverse
```

```
deb http://archive.ubuntu.com/ubuntu lucid main/debian-installer restricted/debian-installer univer
/deb-i386 http://archive.ubuntu.com/ubuntu lucid main/debian-installer restricted/debian-installer
```

Ne feledje, hogy a forráscsomagok nem kerülnek tükrözésre, mivel ezeket a binárisokhoz képest ritkán használják és sokkal több helyet foglalnak, de egyszerűen felvehetők.

Miután a tükör befejezte a replikálást (ez sokáig tarthat), be kell állítania az Apache-ot a tükör fájljainak (alapértelmezésben a `/var/spool/apt-mirror` alatt) közzétételére. Az Apache-csal kapcsolatos további információkért lásd a 1. szakasz - HTTPD – Apache2 webkiszolgáló [141] szakaszt.

2.3.5. Telepítés RAM lemezre

Könnyű elképzelni, hogy a memóriába írás SOKKAL gyorsabb a lemezre írásnál. Ha rendelkezik elég szabad memóriával, a vmbuilder beállítása RAM lemezre írásra jelentősen gyorsítja a folyamatot. Ezt a --tmpfs kapcsolóval lehet megadni:

```
--tmpfs OPTS  tmpfs használata munkakönyvtárként a méret megadásával, vagy
              a „-” megadásakor a tmpfs alapértelmezését használja (suid,dev,size=1G).
```

Emiatt a --tmpfs - hozzáadása jó választás, ha rendelkezésre áll legalább 1 GB szabad memória.

2.4. Az alkalmazás csomagolása

Két lehetőség van:

- A javasolt módszer a Debian csomag készítése. Mivel ennek bemutatása kívül esik ezen dokumentáció célján, információkért lásd az Ubuntu csomagolási útmutatót[9]. Ebben az esetben hasznos tárolót készíteni a csomaghoz, a frissítések egyszerű elérhetővé tételéhez. Ezzel kapcsolatos információkért lásd a Debian Administration[10] cikkét.
- Az alkalmazás telepítése saját kezűleg a `/opt` alá, az FHS irányelvek[11] által javasolt módon.

Ebben az esetben példaként a Limesurvey webalkalmazást használjuk, amelyhez virtuális eszközt biztosítunk. Korábban már volt róla szó, hogy a csomagolt verzió elérhető egy PPA-ban.

2.5. A telepítés befejezése

2.5.1. Első indítás

Ahogyan arról korábban szó volt, a gép első indulásakor kell telepíteni az openssh-server csomagot, hogy a hozzá generált kulcs minden géphez egyedi legyen. Ehhez egy `boot.sh` nevű parancsfájlt kell írni, a következőképpen:

```
# Ez a parancsfájl a virtuális gép első indulásakor fog lefutni.
# Rendszergazdai jogokkal fut.
```

```
apt-get update
apt-get install -qqy --force-yes openssh-server
```

Ezután a parancssort a --firstboot boot.sh kapcsolóval kell bővíteni.

2.5.2. Első bejelentkezés

A Mysql és a Limesurvey telepítésekor felhasználói együttműködésre van szükség, ezek beállítására egy login.sh nevű bejelentkezési parancsfájl használatával a felhasználó első bejelentkezésekor kerül sor. A parancsfájllal a felhasználó megadhatja a:

- Saját jelszavát
- A használni kívánt billentyűzetkiosztást és más területi beállításokat

A `login.sh` a következőképp fog kinézni:

```
# Ez a parancsfájl a felhasználó első bejelentkezésekor fut le.

echo "Az eszköz beállítása hamarosan befejeződik."
echo "Ehhez meg kell válaszolnia néhány kérdést, "
echo "kezdve a felhasználói jelszavának megváltoztatásával."

passwd

# a billentyűzet-kiosztás megváltoztatása
sudo dpkg-reconfigure console-setup

# a mysql kiszolgáló root jelszavának megadása
sudo dpkg-reconfigure mysql-server-5.0

#a limesurvey telepítése
sudo apt-get install -qqy --force-yes limesurvey

echo "Az eszköz beállítva. A használatához nyissa meg a böngészőben a"
echo "http://kiszolgáló-IP/limesurvey/admin címet"
```

Ezután hozzá kell adni a --firstlogin login.sh kapcsolót a parancssorhoz.

2.6. Hasznos bővítések

2.6.1. Automatikus frissítések beállítása

Az eszköz rendszeres automatikus frissítéséhez az unattended-upgrades csomagot kell telepíteni, így a parancssor a következővel bővíthető:

```
--addpkg unattended-upgrades
```

Mivel az alkalmazás csomagja egy PPA-ban van, a folyamat nem csak a rendszert, de az alkalmazást is frissíteni fogja, ha a PPA-ban lévő verzió frissül.

2.6.2. ACPI események kezelése

A virtuális gépnek küldött újraindítási és leállítási események kezelése érdekében ajánlott az acpid csomag telepítése. Ehhez a következő kapcsoló szükséges:

```
--addpkg acpid
```

2.7. Végső parancs

Az összes fenti kapcsolót tartalmazó parancs a következő:

```
sudo vmbuilder kvm ubuntu --suite lucid --flavour virtual --arch i386 -o \
        --libvirt qemu:///system --ip 192.168.0.100 --part vmbuilder.partition --user user \
        --name user --pass default --addpkg apache2 --addpkg apache2-mpm-prefork \
        --addpkg apache2-utils --addpkg apache2.2-common --addpkg dbconfig-common \
        --addpkg libapache2-mod-php5 --addpkg mysql-client --addpkg php5-cli \
        --addpkg php5-gd --addpkg php5-ldap --addpkg php5-mysql --addpkg wwwconfig-common \
        --addpkg mysql-server --addpkg unattended-upgrades --addpkg acpid --ppa nijaba \
        --mirror http://mirroraddress:9999/ubuntu --tmpfs - --firstboot boot.sh \
        --firstlogin login.sh es
```

2.8. Információforrások

Ha többet szeretne tudni, kérdései vagy javaslatai vannak, keresse meg az Ubuntu kiszolgáló csapatát:

- IRC: #ubuntu-server a freenode hálózaton
- Levelezőlista: ubuntu-server kukac lists.ubuntu.com[12]
- Nézze meg a Ubuntu wiki JeOSVMBuilder[13] oldalát is.

3. UEC

3.1. Áttekintés

Ez az ismertető bemutatja az UEC telepítését az Ubuntu 10.04 LTS kiszolgáló változatának CD-jéről, és felépít egy alapszintű hálózati topológiát, amelyben egyetlen rendszer szolgál „mindent egy helyen” vezérlőként, és legalább egy csomópont csatlakozik hozzá.

Ebből az ismertetőből megtanulhatja egy alapszintű UEC telepítését, konfigurálását, regisztrálását és számos művelet végrehajtását rajta, amely eredménye egy egy vezérlős „előtétből” és egy legalább egy csomópontból álló, virtuálisgép-példányokat futtató csomópontokból álló számítási felhő.

3.2. Előfeltételek

A minimális számítási felhő infrastruktúra telepítéséhez legalább két dedikált rendszerre van szükség:

- Egy előtétre.
- Legalább egy csomópontra.

Az alábbiak inkább javaslatok, mint kőbe vésett követelmények. A következő javaslatokat a dokumentáció írásakor szerzett tapasztalataink alapján tesszük.

3.2.1. Előtét előfeltételei

Az alábbi táblázat alapján állítsa össze azt a rendszert, amely a következők egyikét fogja futtatni:

- Felhővezérlő (CLC)
- Fürtvezérlő (CC)
- Walrus (az S3-szerű tárolószolgáltatás)
- Tárolóvezérlő (SC)

19.1. táblázat - UEC előtét előfeltételei

Hardver	Minimális	Javasolt	Megjegyzés
CPU	1 GHz	2 x 2 GHz	A mindent egy helyen előtét esetén hasznos, ha az legalább egy kétmagos processzorral rendelkezik.
Memória	512 MB	2 GB	A Java-alapú webes felületnek jól fog jönni a rengeteg elérhető memória.
Lemez	5400 RPM IDE	7200 RPM SATA	A lassabb lemezek is megfelelők, de a

Hardver	Minimális	Javasolt	Megjegyzés
			példányok indítási ideje sokkal hosszabb lesz.
Lemezhely	40 GB	200 GB	40 GB csak egy lemezképhez, gyorsítótárhoz stb. elég. Az Eucalyptus nem tűri jól a lemezhely elfogyását.
Hálózatkezelés	100 Mbps	1000 Mbps	A gépek lemezképei több száz MB méretűek, és a hálózaton kell azokat átmásolni a csomópontokra.

3.2.2. Csomópont előfeltételei

A többi rendszert csomópontnak nevezzük, amelyeken a következők futnak:

- a csomópontvezérlő (NC)

19.2. táblázat - UEC csomópont előfeltételei

Hardver	Minimális	Javasolt	Megjegyzés
CPU	VT kiterjesztések	VT, 64 bit, több mag	A 64 bites gépek képesek i386 és amd64 példányok futtatására is. Az Eucalyptus alapértelmezésben CPU-magonként csak egy virtuális gépet futtat a csomópontokon.
Memória	1 GB	4 GB	A több memória több és nagyobb vendégeket jelent.
Lemez	5400 RPM IDE	7200 RPM SATA vagy SCSI	Az Eucalyptus csomópontok intenzíven használják a lemezt, az I/O várakozás lesz valószínűleg a teljesítményben a szűk keresztmetszet.

Hardver	Minimális	Javasolt	Megjegyzés
Lemezhely	40 GB	100 GB	A lemezképek gyorsítótárazva lesznek helyileg, az Eucalyptus nem tűri jól a lemezhely elfogyását.
Hálózatkezelés	100 Mbps	1000 Mbps	A gépek lemezképei több száz MB méretűek, és a hálózaton kell azokat átmásolni a csomópontokra.

3.3. A felhő/fürt/tároló/Walrus előtét-kiszolgáló telepítése

1. Töltse le az Ubuntu 10.04 LTS kiszolgáló ISO-fájlját, és írja CD-re.
2. A rendszer indításakor válassza Az Ubuntu Enterprise Cloud telepítése lehetőséget.
3. Amikor a telepítő megkérdezi, hogy Fürtöt vagy Csomópontot szeretne telepíteni, válassza a Fürt lehetőséget.
4. A telepítés során két további, a fürttel kapcsolatos kérdést kell megválaszolnia:
   - Mi a fürt neve?
     - például: fürt1.
   - Nyilvános IP-címek tartománya a helyi hálózaton, amelyeket a számítási felhő a példányok számára lefoglalhat.
     - például: 192.168.1.200-192.168.1.249.

3.4. A csomópontvezérlők telepítése

A csomópontvezérlők telepítése ennél is egyszerűbb. Csak arról kell meggyőződnie, hogy csatlakozik ahhoz a hálózathoz, amelyen a felhő/fürtvezérlő már fut.

1. Indítsa el a gépet ugyanarról az ISO-ról a csomópontokon.
2. A rendszer indításakor válassza Az Ubuntu Enterprise Cloud telepítése lehetőséget.
3. Válassza Az Ubuntu Enterprise Cloud telepítése lehetőséget.
4. Ennek észlelnie kell a fürtöt, és ki kell választania a Csomópont telepítést.
5. Erősítse meg a particionálási sémát.
6. A telepítés további részének megszakítás nélkül kell folytatódnia. Várja meg a telepítés befejeződését, és indítsa újra a csomópontot.

3.5. A csomópontok regisztrálása

A csomópontok fizikai rendszerek az UEC-n belül, amelyek a számítási felhő virtuálisgép-példányait ténylegesen futtatják.

Ha már legalább egy Ubuntu kiszolgáló csomópont telepítve van, és futtatja az eucalyptus-nc szolgáltatást, akkor jelentkezzen be a Felhővezérlőre (CLC), és adja ki a következőt:

```
sudo euca_conf --no-rsync --discover-nodes
```

Ez feltérképezi a hálózaton az eucalyptus-nc szolgáltatást futtató rendszereket, és a rendszergazda megerősítheti az egyes csomópontok regisztrációját azok IP-címe alapján.

Ha a program jelszavakat kér, vagy scp hibákat kap, akkor nézze meg a kulcsszinkronizációs utasításokat az UEC/NodeInstallation[14] oldalon.

3.6. Hitelesítési adatok beszerzése

A felhővezérlő telepítése és elindítása után a felhő felhasználóinak szükségük lesz a hitelesítési adataik lekérésére. Ez történhet webböngészőben, vagy parancssorban.

3.6.1. Webböngészőből

1. A webböngészőben (távolról, vagy az Ubuntu kiszolgálón) nyissa meg a következő URL-címet:

   ```
   https://<felhő-vezérlő-ip-címe>:8443/
   ```

   

   Ehhez használjon biztonságos kapcsolatot, győződjön meg róla, hogy az URL-címben „https”-t és nem „http”-t ad meg. A biztonsági tanúsítvány megbízhatatlanságával kapcsolatban figyelmeztetést fog kapni. Fel kell vennie egy kivételt az oldal megjelenítéséhez, ellenkező esetben nem lesz képes az Eucalyptus konfigurációs oldalának megnézésére.
2. Használja az „admin” felhasználónevet és az „admin” jelszót az első bejelentkezéshez (a rendszer meg fogja kérni a jelszava megváltoztatására).
3. Kövesse a képernyőn megjelenő utasításokat a rendszergazdai jelszó és e-mail cím frissítéséhez.
4. Az első konfigurációs folyamat végén kattintson a képernyő bal felső részén található „credentials” lapra.
5. Kattintson a „Download Credentials” gombra a tanúsítványai lekéréséhez.
6. Mentse ezeket a `~/.euca` könyvtárba.
7. Bontsa ki a letöltött zip fájlt egy biztonságos helyre (`~/.euca`).

   ```
   unzip -d ~/.euca mycreds.zip
   ```

3.6.2. Parancssorból

- Ennek alternatívájaként a felhővezérlő parancssorában használhatja a következőt is:

  ```
  mkdir -p ~/.euca
  ```

```
chmod 700 ~/.euca
cd ~/.euca
sudo euca_conf --get-credentials mycreds.zip
unzip mycreds.zip
cd -
```

3.6.3. Hitelesítési adatok kibontása és használata

Ezután be kell állítania az EC2 API és AMI eszközöket a kiszolgálón az X.509 tanúsítványok segítségével.

1. Vegye fel az előző csomag által tartalmazott "eucarc" fájlt az Eucalyptus környezet beállításához:

```
. ~/.euca/eucarc
```

2. Ezt a parancsot felveheti a `~/.bashrc` fájlba is, így az Eucalyptus környezet automatikusan beállításra kerül minden bejelentkezésekor. Az Eucalyptus ezeket a hitelesítési adatokat rendszergazdainak tekinti, amelyek globális jogosultságokat biztosítanak tulajdonosuknak a felhőben. Emiatt ezeket a többi emelt jogosultságú hozzáféréshez hasonlóan kell védeni (azaz a normál felhasználók nem láthatják őket).

```
echo "[ -r ~/.euca/eucarc ] && . ~/.euca/eucarc" >> ~/.bashrc
```

3. Telepítse a szükséges felhőfelhasználói eszközöket:

```
sudo apt-get install euca2ools
```

4. A megfelelő működés ellenőrzéséhez kérje le a helyi fürt elérhetőségi adatait:

```
. ~/.euca/eucarc
euca-describe-availability-zones verbose
AVAILABILITYZONE   sajátfelhőm               192.168.1.1
AVAILABILITYZONE   |- vm types               free / max   cpu   ram  disk
AVAILABILITYZONE   |- m1.small               0004 / 0004   1    128     2
AVAILABILITYZONE   |- c1.medium              0004 / 0004   1    256     5
AVAILABILITYZONE   |- m1.large               0002 / 0002   2    512    10
AVAILABILITYZONE   |- m1.xlarge              0002 / 0002   2   1024    20
AVAILABILITYZONE   |- c1.xlarge              0001 / 0001   4   2048    20
```

A fenti parancs kimenete eltérhet.

3.7. Lemezkép futtatása

Számos módon példányosíthat egy lemezképet az UEC-ben:

- A parancssor használatával.
- Az UEC-kompatibilis felügyeleti eszközök egyikével, mint például a Landscape.
- Az ElasticFox[15] Firefox kiterjesztés használatával.

Itt a parancssoros eljárást írjuk le:

1. Mielőtt a lemezkép példányait futtatná, létre kell hoznia egy kulcspárt (SSH-kulcsot), amelynek segítségével bejelentkezhet rendszergazdaként a futó példányra. Ez a kulcs elmentésre kerül, így ezt csak egyszer kell végrehajtania.

   Adja ki a következő parancsot:

   ```
   if [ ! -e ~/.euca/kulcs.priv ]; then
       touch ~/.euca/kulcs.priv
       chmod 0600 ~/.euca/kulcs.priv
       euca-add-keypair mykey > ~/.euca/kulcs.priv
   fi
   ```

   

   A kulcsnak tetszőleges nevet adhat (ebben a példában kulcs), de ne felejtse el a nevet. Ha mégis elfelejti, bármikor futtathatja az euca-describe-keypairs parancsot a rendszeren tárolt létrehozott kulcsok listájának lekéréséhez.
2. Engedélyeznie kell a 22-es port elérését is a példányokon:

   ```
   euca-describe-groups
   euca-authorize default -P tcp -p 22 -s 0.0.0.0/0
   ```
3. Ezután létrehozhatja a regisztrált lemezkép példányait:

   ```
   euca-run-instances $EMI -k kulcs -t c1.medium
   ```

   

   Ha az image_id-ra vonatkozó hibaüzenetet kap, akkor az Images lap megnyitásával jelenítheti meg, vagy a Store lap „How to Run” pontjára kattintva elérheti a példa parancsot.
4. A példány első futtatásakor a rendszer gyorsítótárakat állít fel a lemezképhez, amelyből létre fog jönni. Ez az első alkalommal gyakran sokáig tart, mivel a virtuális gépek lemezképei elég nagyok.

   A példány állapotának monitorozásához adja ki a következőt:

   ```
   watch -n5 euca-describe-instances
   ```

   A kimenetében információkat kell látnia a példányról, beleértve annak állapotát. Az első alkalommal végzett gyorsítótárazáskor a példány állapota pending lesz.
5. A példány teljes elindulásakor a fenti állapot megváltozik és running lesz. Keresse meg a példányhoz társított IP-címet a kimenetben, és kapcsolódjon hozzá:

   ```
   IPADDR=$(euca-describe-instances | grep $EMI | grep running | tail -n1 | awk '{print $4}')
   ssh -i ~/.euca/kulcs.priv ubuntu@$IPADDR
   ```
6. Miután befejezte a munkát a példányon, lépjen ki az SSH-kapcsolatból, és állítsa le a példányt:

```
INSTANCEID=$(euca-describe-instances | grep $EMI | grep running | tail -n1 | awk '{print $2}')
euca-terminate-instances $INSTANCEID
```

3.8. Lemezkép telepítése a Store-ból

Az alábbi módszer messze a legegyszerűbb megoldás lemezképek telepítésére. Ugyanakkor a gyakorlott felhasználók érdeklődésére számot tarthat a saját lemezképek csomagolása[16] wiki oldal.

A lemezképek UEC-hez adásának legegyszerűbb módja annak telepítése az Image Store-ból az UEC webes felületén.

1. Nyissa meg a webes felületet a következő URL-címen (használjon https-t http helyett):

   ```
   https://<felhő-vezérlő-ip-címe>:8443/
   ```

2. Adja meg bejelentkezési nevét és jelszavát (ha szükséges, lehet hogy korábbról még be van jelentkezve).
3. Kattintson a Store lapra.
4. Válogasson az elérhető lemezképek között.
5. A kívánt lemezkép esetén kattintson az install lehetőségre.

A lemezkép letöltése és telepítése után a lemezkép gombja alatt megjelenő „How to run?” hivatkozásra kattintva megjelenítheti a lemezkép példányosításához (elindításához) szükséges parancsot. A lemezkép megjelenik az Image lapon látható listában is.

3.9. További információk

Hogyan használható a tárolóvezérlő[17]?

Eucalyptus szolgáltatások vezérlése:

- sudo service eucalyptus [start|stop|restart] (a CLC/CC/SC/Walrus oldalon)
- sudo service eucalyptus-nc [start|stop|restart] (a csomópont oldalon)

Néhány fontos fájl helye:

- Naplófájlok:
  - /var/log/eucalyptus
- Konfigurációs fájlok:
  - /etc/eucalyptus
- Adatbázis:

[16] https://help.ubuntu.com/community/UEC/BundlingImages
[17] https://help.ubuntu.com/community/UEC/StorageController

- /var/lib/eucalyptus/db
- Kulcsok:
  - /var/lib/eucalyptus
  - /var/lib/eucalyptus/.ssh

A klienseszközök futtatása előtt ne feledje el felvenni a `~/.euca/eucarc` fájlt.

3.10. Hivatkozások

- A példányok betöltésével kapcsolatos információkért nézze meg az Eucalyptus wikioldalát[18].
- Eucalyptus projektoldal (fórumok, dokumentáció, letöltések)[19].
- Eucalyptus a Launchpadon (hibák, kód)[20].
- Eucalyptus hibaelhárítás (1.5)[21].
- Regisztrálja számítási felhőjét a RightScale-nél[22].
- Segítséget kérhet a Freenode[23] #ubuntu-virt, #eucalyptus és #ubuntu-server szobáiban is.

3.11. Szójegyzék

Az Ubuntu Enterprise Cloud dokumentációja olyan terminológiát használ, amely egyes olvasók számára ismeretlen lehet. Ez az oldal az ilyen kifejezések és rövidítések gyűjteményét tartalmazza.

- Cloud – Fizikai gépek egyesített halmaza, amely dinamikusan létrehozott és visszatöltött virtuális gépek segítségével biztosít számítási erőforrásokat.
- Felhővezérlő (CLC) -A webes felhasználói felületet (https kiszolgáló a 8443-as porton) biztosító Eucalyptus összetevő, amely megvalósítja az Amazon EC2 API-t. Az UEC telepítésben csak egy felhővezérlőnek kell lennie. Ezt a szolgáltatást az Ubuntu eucalyptus-cloud csomagja biztosítja.
- Fürt – A fürtvezérlőhöz társított csomópontok gyűjteménye. Az UEC telepítésben több fürt is lehet. A fürtök néha csomópontok fizikailag elválasztott halmazai (például első emelet, második emelet, stb.).
- Fürtvezérlő (CC) – A csomópont-erőforrások gyűjteményeit kezelő Eucalyptus összetevő. Ezt a szolgáltatást az Ubuntu eucalyptus-cc csomagja biztosítja.
- EBS – Rugalmas blokktároló (Elastic Block Storage).
- EC2 – Rugalmas számítási felhő (Elastic Compute Cloud). Az Amazon idő- és gigabájtalapon elszámolt nyilvános számításifelhő-ajánlata.
- EKI – Eucalyptus kernel-lemezkép (Eucalyptus Kernel Image).
- EMI – Eucalyptus gép-lemezkép (Eucalyptus Machine Image).
- ERI – Eucalyptus RAM-lemezkép (Eucalyptus Ramdisk Image).
- Eucalyptus – Elastic Utility Computing Architecture for Linking Your Programs To Useful Systems. Nyílt forrású projekt, amely eredetileg a University of California at Santa Barbara berkeiből indult, ma pedig az Eucalyptus Systems, egy Canonical Partner támogatja.

- Előtét – A magas szintű Eucalyptus összetevők (felhő, walrus, tárolóvezérlő, fürtvezérlő) legalább egyikét kiszolgáló fizikai gép.
- Csomópont – A csomópont egy csomópontvezérlőt futtató, virtuális gépek futtatására képes fizikai gép. Ubuntu alatt ez általában azt jelenti, hogy a CPU VT-kiterjesztésekkel rendelkezik és képes a KVM hipervizor futtatására.
- Csomópontvezérlő (NC) – A felhőt alkotó virtuális gépeket kiszolgáló csomópontokon futó Eucalyptus összetevő. Ezt a szolgáltatást az Ubuntu eucalyptus-nc csomagja biztosítja.
- S3 – Egyszerű tárolószolgáltatás (Simple Storage Service). Az Amazon gigabájtalapon elszámolt állandó tárolási megoldása az EC2-höz.
- Tárolóvezérlő (SC) – A dinamikus blokkos tárolószolgáltatásokat (EBS) kezelő Eucalyptus-összetevő. Az Eucalyptus telepítésben minden fürt saját tárolóvezérlővel rendelkezhet. Ezt az összetevőt az eucalyptus-sc csomag biztosítja.
- UEC – Ubuntu Enterprise Cloud. Az Ubuntu Eucalyptus alapú számításifelhő-megoldása.
- VM – Virtuális gép.
- VT – Virtualizációs technológia. Egyes modern processzorok szolgáltatása, amely lehetővé teszi a virtuális gépek gyorsabb kiszolgálását.
- Walrus – A virtuálisgép-lemezképek és felhasználói adatok tárolására használt, Amazon S3 API-t megvalósító Eucalyptus összetevő, amely az S3 bucket put/get absztrakciókat használja.

4. OpenNebula

Az OpenNebula lehetővé teszi a virtuális gépek dinamikus elhelyezését és áthelyezését a fizikai erőforrások tárolójában. Ez lehetővé teszi a virtuális gépek üzemeltetését tetszőleges elérhető helyről.

Ez a szakasz az OpenNebula fürt beállítását ismerteti három gép használatával: egy előtét kiszolgáló és két számítási csomópont a virtuális gépek futtatására. A számítási csomópontokhoz be kell állítani hidat is, hogy a virtuális gépek elérhessék a helyi hálózatot. Részletekért lásd a 1.4. szakasz - Híd [37] szakaszt.

4.1. Telepítés

Első lépésként az előtét gépen adja ki a következő parancsot:

```
sudo apt-get install opennebula
```

A számítási csomópontokon pedig a következő parancsot:

```
sudo apt-get install opennebula-node
```

Az SSH kulcsok másolásához az oneadmin felhasználónak rendelkeznie kell jelszóval. Minden gépen adja ki a következő parancsot:

```
sudo passwd oneadmin
```

Ezután másolja az oneadmin felhasználó SSH kulcsát a számítási csomópontok és az előtét `authorized_keys` fájljába:

```
sudo scp /var/lib/one/.ssh/id_rsa.pub oneadmin@csomópont01:/var/lib/one/.ssh/authorized_keys
sudo scp /var/lib/one/.ssh/id_rsa.pub oneadmin@csomópont02:/var/lib/one/.ssh/authorized_keys
sudo sh -c "cat /var/lib/one/.ssh/id_rsa.pub >> /var/lib/one/.ssh/authorized_keys"
```

A számítási csomópontok SSH kulcsát fel kell venni az `/etc/ssh/ssh_known_hosts` fájlba az előtét-kiszolgálón. Ehhez jelentkezzen be ssh használatával minden számítási csomópontra a oneadmin-tól eltérő felhasználóként. Ezután lépjen ki az SSH munkamenetből, és adja ki a következő parancsot az SSH kulcs átmásolásához a `~/.ssh/known_hosts` fájlból az `/etc/ssh/ssh_known_hosts` fájlba:

```
sudo sh -c "ssh-keygen -f .ssh/known_hosts -F csomópont01 1>> /etc/ssh/ssh_known_hosts"
sudo sh -c "ssh-keygen -f .ssh/known_hosts -F csomópont02 1>> /etc/ssh/ssh_known_hosts"
```

A csomópont01 és csomópont02 helyett a megfelelő gépneveket adja meg.

Ez lehetővé teszi a oneadmin számára az scp jelszó vagy kézi beavatkozás nélküli használatát lemezképek számítási csomópontokra telepítéséhez.

Az előtéten hozzon létre egy könyvtárat a virtuális gépek lemezképeinek tárolásához, és adjon hozzáférést a oneadmin felhasználónak a könyvtárhoz:

```
sudo mkdir /var/lib/one/images
sudo chown oneadmin /var/lib/one/images/
```

Végül másoljon egy virtuálisgép-lemezképet a `/var/lib/one/images` könyvtárba. A vmbuilder segítségével létrehozhat egy Ubuntu virtuális gépet, részletekért nézze meg a 2. szakasz - JeOS és vmbuilder [266] szakaszt.

4.2. Beállítás

Az OpenNebula fürt készen áll a beállításra, és a virtuális gépek befogadására.

Adja ki a következő parancsot:

```
onehost create node01 im_kvm vmm_kvm tm_ssh
onehost create node02 im_kvm vmm_kvm tm_ssh
```

Ezután hozzon létre egy virtuálishálózat-sablon fájlt `vnet01.template` néven:

```
NAME            = "LAN"
TYPE            = RANGED
BRIDGE          = br0
NETWORK_SIZE    = C
NETWORK_ADDRESS = 192.168.0.0
```

A 192.168.0.0 helyett ne feledje el a helyi hálózatot beírni.

Az onevnet segédprogram segítségével vegye fel a virtuális hálózatot az OpenNebula-ba:

```
onevnet create vnet01.template
```

Hozzon létre egy virtuálisgép-sablon fájlt `vm01.template` néven:

```
NAME   = vm01
CPU    = 0.5
MEMORY = 512

OS      = [ BOOT   = hd ]

DISK   = [
  source   = "/var/lib/one/images/vm01.qcow2",
  target   = "hda",
  readonly = "no" ]
```

```
NIC    = [ NETWORK="LAN" ]

GRAPHICS = [type="vnc",listen="127.0.0.1",port="-1"]
```

Indítsa el a virtuális gépet a onevm segítségével:

```
onevm submit vm01.template
```

A onevm list segítségével információkat jeleníthet meg a virtuális gépekről. A onevm show vm01 parancs további részleteket jelenít meg az adott virtuális gépről.

4.3. Hivatkozások

- További információkért nézze meg az OpenNebula weboldalát[24].
- Segítséget találhat a Freenode[25] #ubuntu-virt és #ubuntu-server IRC csatornáin is.
- Az Ubuntu wiki OpenNebula[26] oldala további részleteket tartalmaz.

20. fejezet - Fürtözés

1. DRBD

Az Elosztott replikált blokkeszköz (DRBD) több gép között tükrözi a blokkeszközöket. A replikáció transzparens a gazda rendszer többi alkalmazása számára. Bármely blokkeszköz - merevlemezek, partíciók, RAID-eszközök, logikai kötetek stb. - tükrözhető.

A drbd használatának megkezdéséhez telepítse a szükséges csomagokat. Adja ki a következő parancsot:

```
sudo apt-get install drbd8-utils
```

Ha virtuális gép részeként a virtuális kernelt használja, akkor saját kezűleg kell lefordítani a drbd modult. A virtuális gépen belül egyszerűbb lehet a linux-server csomagot telepíteni.

Ez a szakasz a drbd beállítását ismerteti egy önálló, ext3 fájlrendszert használó `/srv` partíció replikálására két gép között. A partícióméret nem különösebben fontos, de mindkét partíciónak azonos méretűnek kell lennie.

1.1. Beállítás

A két gépet ebben a példában drbd01 és drbd02 névvel jelöljük. Ezeken működnie kell a névfeloldásnak a DNS-en vagy az `/etc/hosts` fájlon keresztül. A részletekért lásd: 7. fejezet - Tartománynév-szolgáltatás (DNS) [94].

- A drbd beállításához az első gépen szerkessze az `/etc/drbd.conf` fájlt:

```
global { usage-count no; }
common { syncer { rate 100M; } }
resource r0 {
        protocol C;
        startup {
                wfc-timeout  15;
                degr-wfc-timeout 60;
        }
        net {
                cram-hmac-alg sha1;
                shared-secret "secret";
        }
        on drbd01 {
                device /dev/drbd0;
                disk /dev/sdb1;
                address 192.168.0.1:7788;
                meta-disk internal;
        }
        on drbd02 {
                device /dev/drbd0;
                disk /dev/sdb1;
                address 192.168.0.2:7788;
```

```
                meta-disk internal;
        }
}
```

Az `/etc/drbd.conf` számos más beállítást is tartalmaz, de ehhez a példához az alapértelmezett értékek is megfelelnek.

- Másolja az `/etc/drbd.conf` fájlt a második gépre:

```
scp /etc/drbd.conf drbd02:~
```

- A drbd02 gépen mozgassa a fájlt az `/etc` könyvtárba:

```
sudo mv drbd.conf /etc/
```

- Mindkét gépen indítsa el a drbd démont:

```
sudo /etc/init.d/drbd start
```

- Most a drbdadm segédprogram segítségével készítse elő a metaadat-tárolót. Mindkét kiszolgálón adja ki a következő parancsot:

```
sudo drbdadm create-md r0
```

- Az elsődlegesnek szánt gépen (például a drbd01-en) adja ki a következő parancsot:

```
sudo drbdadm -- --overwrite-data-of-peer primary all
```

- A fenti parancs kiadása után megkezdődik az adatok szinkronizálása a másodlagos kiszolgálóval. A folyamat megfigyeléséhez adja ki a következő parancsot a drbd02 gépen:

```
watch -n1 cat /proc/drbd
```

A kimenet megfigyelésének befejezéséhez nyomja meg a Ctrl+c kombinációt.

- Végül hozzon létre fájlrendszert a `/dev/drbd0` eszközön, és csatolja:

```
sudo mkfs.ext3 /dev/drbd0
sudo mount /dev/drbd0 /srv
```

1.2. Tesztelés

Az adatok a két gép közötti tényleges szinkronizálásának teszteléséhez másoljon át néhány fájlt az elsődleges (drbd01) gépen a `/srv` könyvtárba:

```
sudo cp -r /etc/default /srv
```

Ezután válassza le a `/srv` partíciót:

```
sudo umount /srv
```

Fokozza le az elsődleges kiszolgálót másodlagos szerepbe:

```
sudo drbdadm secondary r0
```

Most a másodlagos kiszolgálón léptesse elő azt elsődleges szerepbe:

```
sudo drbdadm primary r0
```

Végül csatolja a partíciót:

```
sudo mount /dev/drbd0 /srv
```

Az ls segítségével látnia kell a korábbi elsődleges drbd01 gépről átmásolt `/srv/default` könyvtárat.

1.3. Hivatkozások

- A DRBD-vel kapcsolatos további információkért lásd a DRBD weboldalát[1].
- A drbd.conf kézikönyvoldala[2] tartalmazza az itt nem tárgyalt beállítási lehetőségekkel kapcsolatos részleteket.
- Nézze meg a drbdadm kézikönyvoldalát[3] is.
- Az Ubuntu wiki DRBD[4] oldala szintén tartalmaz további információkat.

21. fejezet - VPN

A virtuális magánhálózatnak (VPN) a legalább két hálózat közötti titkosított kapcsolatot nevezik. A VPN szoftveres létrehozására számos módszer áll rendelkezésre, a hardvereszközök mellett. Ez a szakasz ismerteti az OpenVPN telepítését és beállítását egy két kiszolgáló közti VPN létrehozására.

1. OpenVPN

Az OpenVPN a nyilvános kulcsinfrastruktúrát (PKI) használja a VPN-forgalom csomópontok közti titkosítására. Az OpenVPN-t használó VPN beüzemelésére egyszerű megoldást ad a klienseknek a VPN-kiszolgáló híd csatolóján keresztüli összekapcsolása. Ez a leírás feltételezi, hogy egy VPN-csomópont, ebben az esetben a kiszolgáló, rendelkezik beállított híd csatolóval. A híd beállításával kapcsolatban lásd a 1.4. szakasz - Híd [37] szakaszt.

1.1. Telepítés

Az openvpn csomag telepítéséhez adja ki a következő parancsot:

```
sudo apt-get install openvpn
```

1.1.1. Kiszolgálótanúsítványok

Az openvpn csomag telepítése után létre kell hozni a VPN kiszolgáló tanúsítványait.

Első lépésként másolja az `easy-rsa` könyvtárat az `/etc/openvpn` alá. Ez biztosítja, hogy a parancsfájlok módosításai a csomag frissítésekor sem vesznek el. Szüksége lesz az `easy-rsa` könyvtár jogosultságainak módosítására is a fájlok létrehozásának engedélyezéséhez az aktuális felhasználónak. Adja ki a következő parancsot:

```
sudo mkdir /etc/openvpn/easy-rsa/
sudo cp -r /usr/share/doc/openvpn/examples/easy-rsa/2.0/* /etc/openvpn/easy-rsa/
sudo chown -R $USER /etc/openvpn/easy-rsa/
```

Ezután szerkessze az `/etc/openvpn/easy-rsa/vars` fájlt, igazítsa az alábbiakat a környezetéhez:

```
export KEY_COUNTRY="HU"
export KEY_PROVINCE="Budapest"
export KEY_CITY="Budapest"
export KEY_ORG="Példacég"
export KEY_EMAIL="geza@példa.hu"
```

A kiszolgáló tanúsítványának létrehozásához adja ki a következő parancsot:

```
cd /etc/openvpn/easy-rsa/
source vars
./clean-all
./build-dh
./pkitool --initca
./pkitool --server server
cd keys
openvpn --genkey --secret ta.key
sudo cp server.crt server.key ca.crt dh1024.pem ta.key /etc/openvpn/
```

1.1.2. Klienstanúsítványok

A VPN-kliensnek is szüksége lesz tanúsítványra a kiszolgáló felé történő hitelesítéshez. A tanúsítvány létrehozásához adja ki a következő parancsot:

```
cd /etc/openvpn/easy-rsa/
source vars
./pkitool gépnév
```

A gépnév helyett a VPN-hez csatlakozó gép tényleges gépnevét adja meg.

Másolja a következő fájlokat a kliensre:

- /etc/openvpn/ca.crt
- /etc/openvpn/easy-rsa/keys/gépnév.crt
- /etc/openvpn/easy-rsa/keys/gépnév.key
- /etc/openvpn/ta.key

Ne felejtse el a fenti fájlnevekben átírni a kliensgép gépnevét.

A tanúsítvány- és kulcsfájlok átmásolására érdemes biztonságos módszert használni. Az scp segédprogram jó választás lehet, de a fájlok cserélhető adathordozóra, majd a kliensre másolása is megfelelő.

1.2. Beállítás

1.2.1. A kiszolgáló beállítása

Ezután állítsa be az openvpn kiszolgálót az `/etc/openvpn/server.conf` létrehozásával a példafájlból. Adja ki a következő parancsot:

```
sudo cp /usr/share/doc/openvpn/examples/sample-config-files/server.conf.gz /etc/openvpn/
sudo gzip -d /etc/openvpn/server.conf.gz
```

Szerkessze az `/etc/openvpn/server.conf` fájlt, és módosítsa a beállításokat az alábbiak szerint:

```
local 172.18.100.101
dev tap0
up "/etc/openvpn/up.sh br0"
down "/etc/openvpn/down.sh br0"
;server 10.8.0.0 255.255.255.0
server-bridge 172.18.100.101 255.255.255.0 172.18.100.105 172.18.100.200
push "route 172.18.100.1 255.255.255.0"
push "dhcp-option DNS 172.18.100.20"
push "dhcp-option DOMAIN példa.hu"
```

```
tls-auth ta.key 0 # This file is secret
user nobody
group nogroup
```

- local: a híd csatoló IP-címe.
- server-bridge: akkor szükséges, ha a rendszer hidat használ. A 172.18.100.101 255.255.255.0 rész a híd csatolót és a maszkot jelenti. A 172.18.100.105 172.18.100.200 IP-címtartomány a kliensekhez rendelendő IP-címek tartománya.
- push: a kliensek hálózatkezelési beállításai.
- user és group: adja meg, hogy az openvpn démon mely felhasználó és csoport nevében fut.

Minden fenti IP-címet és tartománynevet cseréljen le a hálózatának megfelelőre.

Ezután hozzon létre néhány segédparancsfájlt a tap csatoló hozzáadásához a hídhoz. Hozza létre az `/etc/openvpn/up.sh` fájlt:

```
#!/bin/sh

BR=$1
DEV=$2
MTU=$3
/sbin/ifconfig $DEV mtu $MTU promisc up
/usr/sbin/brctl addif $BR $DEV
```

És az `/etc/openvpn/down.sh` fájlt is:

```
#!/bin/sh

BR=$1
DEV=$2

/usr/sbin/brctl delif $BR $DEV
/sbin/ifconfig $DEV down
```

Ezután tegye mindkettőt végrehajthatóvá:

```
sudo chmod 755 /etc/openvpn/down.sh
sudo chmod 755 /etc/openvpn/up.sh
```

A kiszolgáló beállítása után indítsa újra az openvpnt a következő megadásával:

```
sudo /etc/init.d/openvpn restart
```

1.2.2. A kliens beállítása

Első lépésként telepítse az openvpn csomagot a kliensen:

```
sudo apt-get install openvpn
```

A kiszolgáló beállítása és a klienstanúsítványok az `/etc/openvpn/` könyvtárba történő átmásolása után példafájl átmásolásával hozzon létre egy kliensbeállító fájlt. A kliensgépen adja ki a következő parancsot:

```
sudo cp /usr/share/doc/openvpn/examples/sample-config-files/client.conf /etc/openvpn
```

Ezután szerkessze az `/etc/openvpn/client.conf` fájlt, és módosítsa a beállításokat az alábbiak szerint:

```
dev tap
remote vpn.példa.hu 1194
cert gépnév.crt
key gépnév.key
tls-auth ta.key 1
```

A vpn.példa.hu helyett adja meg a VPN-kiszolgáló gépnevét, a gépnév.* helyett pedig a tényleges tanúsítvány- és kulcsfájl neveit.

Végül indítsa újra az openvpnt:

```
sudo /etc/init.d/openvpn restart
```

Ezután a VPN használatával képes lesz csatlakozni a távoli helyi hálózatra.

1.3. Hivatkozások

- További információkért lásd az OpenVPN[1] weboldalát.
- Ezen kívül a Pakt OpenVPN: Building and Integrating Virtual Private Networks[2] című könyve is hasznos információforrás.
- További információkért nézze meg az Ubuntu wiki OpenVPN[3] oldalát.

22. fejezet - További hasznos alkalmazások

Az Ubuntu kiszolgáló csapata számos hasznos alkalmazást fejleszt, és több más alkalmazás is jól illeszkedik az Ubuntu kiszolgáló változatába, amelyek azonban kevésbé ismertek. Ez a szakasz bemutat néhány hasznos alkalmazást, amelyek egy vagy több Ubuntu kiszolgáló adminisztrációját sokkal egyszerűbbé tehetik.

1. pam_motd

Ubuntu kiszolgálókra bejelentkezéskor valószínűleg észrevette az informatív Nap üzenetét (MOTD). Ezek az információk több csomag használatával kerülnek beszerzésre és jelennek meg:

- A landscape-common biztosítja a landscape-client alapvető programkönyvtárait, amelyekkel a webes Landscape alkalmazás használatával felügyelhetők a rendszerek. A csomag tartalmazza a /usr/bin/landscape-sysinfo segédprogramot, a MOTD-ban megjelenő információk ennek segítségével kerülnek összegyűjtésre.
- Az update-notifier-common segítségével a MOTD automatikusan, a pam_motd használatával frissül.

Az pam_motd a nevük elején található számok sorrendjében végrehajtja az `/etc/update-motd.d` parancsfájljait. A parancsfájlok kimenete a számozott sorrendet fenntartva a `/var/run/motd/` fájlba, majd az `/etc/motd.tail` fájllal kerülnek összefűzésre.

Saját dinamikus információkat is adhat a MOTD-hez. Helyi időjárási információk hozzáadásához például:

- Első lépésként telepítse a weather-util csomagot:

  ```
  sudo apt-get install weather-util
  ```

- A weather segédprogram a National Oceanic and Atmospheric Administration METAR adatait, és a National Weather Service előrejelzéseit használja. A helyi információk eléréséhez szüksége lesz a 4 karakteres ICAO helyazonosítóra (például: LHBP Budapest esetén). Ez a National Weather Service[1] weboldalán határozható meg.

  Noha a National Weather Service az Egyesült Államok kormányzati ügynöksége, az időjárás-jelentő állomások világszerte megtalálhatók. Ugyanakkor nem biztos, hogy a helyi időjárási információk az Egyesült Államokon kívüli összes állomás esetén elérhetők.

- Hozzon létre egy egyszerű, `/usr/local/bin/local-weather` parancsfájlt, amely a weather programot és a helyi ICAO kódot használja:

  ```
  #!/bin/sh
  #
  #
  # Kiírja a helyi időjárást a MOTD számára.
  #
  #

  # Helyettesítse az LHBP-t a helyi időjárási állomás kódjával.
  # A helyi állomások itt találhatók: http://www.weather.gov/tg/siteloc.shtml

  echo
  weather -i LHBP
  echo
  ```

- Tegye végrehajthatóvá a parancsfájlt:

```
sudo chmod 755 /usr/local/bin/local-weather
```

- Ezután hozzon létre egy szimbolikus linket `/etc/update-motd.d/98-local-weather` néven:

```
sudo ln -s /usr/local/bin/local-weather /etc/update-motd.d/98-local-weather
```

- Végül lépjen ki a kiszolgálóról, majd újra be az új MOTD megjelenítéséhez.

Ezután néhány hasznos, és a helyi időjárással kapcsolatos kevésbé hasznos információval üdvözli a rendszer. Reméljük, a local-weather példával sikerült bemutatnunk az pam_motd rugalmasságát.

2. etckeeper

Az etckeeper lehetővé teszi az `/etc` könyvtár tartalmának egyszerű tárolását verziókezelő rendszerek (VCS) tárolóiban. Beépül az apt rendszerbe az `/etc` könyvtár csomagok telepítésekor vagy frissítésekor történő módosításainak automatikus véglegesítéséhez. Az `/etc` verziókezelés alá helyezése bevett ipari gyakorlat, és az etckeeper célja a folyamatot a lehető legegyszerűbbé tenni.

A következő parancs kiadásával telepítse az etckeeper csomagot:

```
sudo apt-get install etckeeper
```

Az elsődleges beállítófájl, az `/etc/etckeeper/etckeeper.conf` viszonylag egyszerű. A legfontosabb beállítás a használandó verziókezelő. Alapértelmezésben az etckeeper a bzr használatára van beállítva. A tároló a csomag telepítésekor automatikusan inicializálásra (és feltöltésre) kerül. Ez a következő parancs kiadásával érhető el:

```
sudo etckeeper uninit
```

Alapértelmezésben az etckeeper alapértelmezésben az /etc nem véglegesített változtatásait naponta véglegesíti. Ez letiltható az AVOID_DAILY_AUTOCOMMITS beállítási lehetőséggel. Ezen kívül automatikusan véglegesíti a változtatásokat a csomagok telepítése előtt és után. A módosítások pontosabb követése érdekében ajánlott a saját módosításokat saját kezűleg, egy véglegesítési üzenet kíséretében is véglegesíteni:

```
sudo etckeeper commit „..A beállítások módosításának oka..”
```

A verziókezelő rendszer parancsaival naplóinformációkat jeleníthet meg az `/etc` könyvtár fájljairól:

```
sudo bzr log /etc/passwd
```

A csomagkezelő rendszerrel való integráció bemutatásához telepítse a postfix csomagot:

```
sudo apt-get install postfix
```

A telepítés befejezése után a postfix összes beállítófájlja véglegesítésre kerül a tárolóba:

```
Committing to: /etc/
added aliases.db
modified group
modified group-
modified gshadow
modified gshadow-
modified passwd
modified passwd-
added postfix
```

```
added resolvconf
added rsyslog.d
modified shadow
modified shadow-
added init.d/postfix
added network/if-down.d/postfix
added network/if-up.d/postfix
added postfix/dynamicmaps.cf
added postfix/main.cf
added postfix/master.cf
added postfix/post-install
added postfix/postfix-files
added postfix/postfix-script
added postfix/sasl
added ppp/ip-down.d
added ppp/ip-down.d/postfix
added ppp/ip-up.d/postfix
added rc0.d/K20postfix
added rc1.d/K20postfix
added rc2.d/S20postfix
added rc3.d/S20postfix
added rc4.d/S20postfix
added rc5.d/S20postfix
added rc6.d/K20postfix
added resolvconf/update-libc.d
added resolvconf/update-libc.d/postfix
added rsyslog.d/postfix.conf
added ufw/applications.d/postfix
Committed revision 2.
```

A kézi módosítások követését az etckeeper által a következő példa mutatja be. Vegyen fel egy új kiszolgálót az `/etc/hosts` fájlba. A bzr segítségével láthatja a módosított fájlokat:

```
sudo bzr status /etc/
modified:
  hosts
```

Most véglegesítse a változtatásokat:

```
sudo etckeeper commit "új kiszolgáló"
```

További információkért a bzr rendszerről lásd a 1. szakasz - Bazaar [214] szakaszt.

3. Byobu

Bármely rendszergazda számára a leghasznosabb alkalmazások egyike a screen. Ez a program lehetővé teszi több parancsértelmező futtatását ugyanabban a terminálban. A speciálisabb screen szolgáltatások felhasználóbarátabbá tétele, és a rendszerrel kapcsolatos hasznos információk biztosítása érdekében jött létre a byobu csomag.

A byobu végrehajtásakor az F9 billentyű megnyomásakor megjelenik a Beállítások menü. Ez lehetővé teszi:

- A Súgó menü megjelenítését
- A Byobu háttérszínének megváltoztatását
- A Byobu előtérszínének megváltoztatását
- Állapotértesítések átváltását
- A billentyűtársítás-csoport módosítását
- Az escape szekvencia módosítását
- Új ablakok létrehozását
- Az alapértelmezett ablakok kezelését
- A Byobu jelenleg nem indul bejelentkezéskor (bekapcsolás)

A billentyűtársítások közé az escape szekvencia, új ablak, ablakváltás stb. tartozik. Két billentyűtársítás-csoport, az f-billentyűk és a screen-escape-keys közül választhat. Ha az eredeti billentyűtársításokat szeretné használni, válassza a nincs csoportot.

Az Ubuntu byobu egy menüt biztosít, amely megjeleníti az Ubuntu kiadást, processzorinformációkat, memóriainformációkat, és az időt és dátumot. A hatása hasonló az asztali menükhöz.

A „A Byobu jelenleg nem indul bejelentkezéskor (bekapcsolás)” lehetőség hatására a byobu minden megnyitott terminálban elindul. A byobu változtatásai felhasználói szintűek, és nem befolyásolják a rendszer többi felhasználóját.

A byobu használatakor az egyik eltérés a visszagörgetési módban van. Ha az egyik Ubuntu profilt használja, akkor az F7 megnyomásával léphet be a visszagörgetési módba. A visszagörgetési mód lehetővé teszi a korábbi kimenetben való navigálást vi-szerű parancsokkal. A mozgási parancsok rövid listája a következő:

- h - A kurzor egy karakterrel balra mozgatása
- j - A kurzor egy sorral lefelé mozgatása
- k - A kurzor egy sorral felfelé mozgatása
- l - A kurzor egy karakterrel jobbra mozgatása
- 0 - A jelenlegi sor elejére lépés
- $ - A jelenlegi sor végére lépés
- G - A megadott sorra lépés (alapértelmezésben a puffer végére)

- / - Keresés előre
- ? - Keresés vissza
- n - A következő találatra lépés, előre vagy hátra

4. Hivatkozások

- Az update-motd további elérhető beállításaival kapcsolatban lásd az update-motd kézikönyvoldalát[2].
- A nap Debian csomagja oldal weather[3] cikke további részletekkel szolgál a weather segédprogramról.
- Az etckeeper használatával kapcsolatos további információkért lásd az etckeeper[4] honlapját.
- És az Ubuntu wiki etckeeper[5] oldalát.
- A bzr rendszerrel kapcsolatos legfrissebb híreket és információkat a bzr[6] weboldalán találja.
- A screen használatával kapcsolatos további információkért lásd a screen weboldalát[7].
- És az Ubuntu wiki screen[8] oldalát.
- A byobu projektoldala[9] is hasznos információforrás.

A. függelék - Függelék

1. Az Ubuntu kiszolgáló verziójában talált hibák jelentése

Noha az Ubuntu projekt igyekszik szoftvereit a lehető legkevesebb hibával kiadni, így is előfordulnak hibák. Segítheti ezek javítását az Ön által találtak bejelentésével a projektnek. Az Ubuntu projekt a Launchpadet[1] használja a hibajelentések követésére. Az Ubuntu kiszolgálóváltozatával kapcsolatos hibák jelentéséhez létre kell hoznia egy fiókot[2].

1.1. Hibák jelentése az ubuntu-bug segítségével

A hibák jelentésének előnyben részesített módja az ubuntu-bug parancs használata. Az ubuntu-bug eszköz a bejelentett probléma felismeréséhez hasznos információkat gyűjt a rendszerről, amelyeket a Launchpaden bejelentett hiba tartalmazni fog. Az Ubuntu hibajelentéseit konkrét szoftvercsomagokhoz kell bejelenteni, így meg kell adni a hibás csomag nevét az ubuntu-bug programnak:

```
ubuntu-bug CSOMAGNÉV
```

Ha például az openssh-server csomagban talált hibát szeretné bejelenteni, adja ki a következőt:

```
ubuntu-bug openssh-server
```

Az ubuntu-bug programnak megadhat bináris vagy forrás csomagot is. Az openssh-server példánál maradva a hibajelentést az openssh-server forráscsomagja, az openssh felé is bejelentheti:

```
ubuntu-bug openssh
```

Az Ubuntu csomagjaival kapcsolatban lásd a 3. fejezet - Csomagkezelés [17] szakaszt.

Az ubuntu-bug parancs információkat gyűjt a kérdéses rendszerről, beleértve lehetőség szerint a megadott csomagra jellemző információkat is, majd megkérdezi, mit szeretne tenni a begyűjtött információkkal:

```
ubuntu-bug postgresql

*** Információgyűjtés a hibáról

Az összegyűjtött információkat elküldheti a fejlesztőknek, hogy javíthassanak
az alkalmazáson. A küldés eltarthat pár percig.
..........

*** Elküldi a hibajelentést a fejlesztőknek?
```

[1] https://launchpad.net/
[2] https://launchpad.net/

```
A hibajelentés elküldése után kérjük, töltse ki a kérdőívet az
automatikusan megnyíló webböngészőben.

Mit szeretne tenni? A lehetőségek:
  H: Hibajelentés küldése (4.9 KiB)
  B: Hibajelentés megtekintése
  K: Hibajelentés megtartása későbbi küldésre, vagy más helyre másolásra
  G: Mégse
Válasszon (H/B/K/G):
```

A lehetőségek:

- Hibajelentés küldése Ezen lehetőség kiválasztásakor az összegyűjtött információk elküldésre kerülnek a Launchpadre a hibajelentés elküldésének részeként. Lehetőséget kap a hiba előfordulásához vezető körülmények leírására.

  ```
  *** A hibával kapcsolatos információk feltöltése

  Az összegyűjtött információk elküldése a hibakövető rendszernek.
  Ez eltarthat pár percig.
  90%

  *** A folytatáshoz meg kell nyitnia a következő URL-címet:

    https://bugs.launchpad.net/ubuntu/+source/postgresql-8.4/+filebug/kc6eSnTLnLxF8u0t3e56EukFeqJ?

  Elindíthatja most a böngészőt, vagy átmásolhatja ezt az URL-címet egy másik számítógépen
   lévő böngészőbe.

  Lehetőségek:
    1: Böngésző indítása most
    G: Mégse
  Válasszon (1/G):
  ```

  Ha a böngésző elindítását választja, akkor alapértelmezésben a w3m nevű szöveges böngésző használatával fejezheti be a hibajelentés elküldését. Ennek alternatívájaként a megadott URL-címet átmásolhatja egy éppen futó böngészőbe is.

- Hibajelentés megtekintése Ezen lehetőség kiválasztásával megjelenítheti az összegyűjtött adatokat a terminálban.

  ```
  Package: postgresql 8.4.2-2
  PackageArchitecture: all
  Tags: lucid
  ProblemType: Bug
  ProcEnviron:
    LANG=en_US.UTF-8
    SHELL=/bin/bash
  Uname: Linux 2.6.32-16-server x86_64
  Dependencies:
  ```

```
  adduser 3.112ubuntu1
  base-files 5.0.0ubuntu10
  base-passwd 3.5.22
  coreutils 7.4-2ubuntu2
...
```

A jelentés megtekintése után visszajut ugyanabba a menübe, amely újra megkérdezi, hogy mit szeretne tenni a jelentéssel.

- Hibajelentés megtartása Ezen lehetőség hatására az összegyűjtött információk egy fájlba lesznek írva. Ez a fájl később felhasználható hibajelentések beküldéséhez, vagy átvihető más Ubuntu rendszerekre jelentések készítéséhez. A jelentésfájl beküldéséhez egyszerűen adja meg azt az ubuntu-bug parancs paramétereként:

```
Mit szeretne tenni? A lehetőségek:
  H: Hibajelentés küldése (4.9 KiB)
  B: Hibajelentés megtekintése
  K: Hibajelentés megtartása későbbi küldésre, vagy más helyre másolásra
  G: MégseVálasszon (H/B/K/G): kHibajelentésfájl: /tmp/apport.postgresql.v4MQas.apport

ubuntu-bug /tmp/apport.postgresql.v4MQas.apport

*** Elküldi a hibajelentést a fejlesztőknek?
...
```

- Mégse A Mégse kiválasztásával az összegyűjtött információk eldobásra kerülnek.

1.2. Alkalmazás-összeomlások jelentése

Az ubuntu-bug segédprogramot tartalmazó apport csomag beállítható az alkalmazások összeomlásakor való aktiválásra. Ez alapértelmezésben le van tiltva, mivel egy összeomlás elkapása az összeomlott alkalmazás memóriahasználatától függően erőforrás-igényes lehet, mivel az apport elkapja és feldolgozza a veremkiíratást.

Az apport beállítása az összeomló alkalmazásokról való információgyűjtésre több lépésből áll. Első lépésként a gdb-t kell telepíteni; ez alapértelmezésben nincs telepítve az Ubuntu kiszolgáló változatára.

```
sudo apt-get install gdb
```

Az Ubuntu csomagkezelésével kapcsolatban lásd a 3. fejezet - Csomagkezelés [17] szakaszt.

A gdb telepítése után nyissa meg az `/etc/default/apport` fájlt a szövegszerkesztőben, és módosítsa az enabled beállítás értékét 1-re a következőképpen:

```
# set this to 0 to disable apport, or to 1 to enable it
# you can temporarily override this with
# sudo service apport start force_start=1
```

```
enabled=1

# set maximum core dump file size (default: 209715200 bytes == 200 MB)
maxsize=209715200
```

Az `/etc/default/apport` szerkesztésének befejezése után indítsa el az apport szolgáltatást:

```
sudo start apport
```

Ha egy alkalmazás összeomlik, az apport-cli parancs segítségével megkeresheti a meglévő mentett összeomlás-jelentés információit:

```
apport-cli

*** dash váratlanul befejeződött (2010-04-09 23:34:18).

Ha éppen semmi bizalmasat sem végzett (jelszavak vagy egyéb
magánjellegű információk bevitele), a hiba bejelentésével segíthet
a fejlesztőknek annak javításában.

Mit szeretne tenni? A lehetőségek:
  H: Hiba jelentése…
  K: Mégse, és ezentúl a programverzió összeomlásainak figyelmen kívül hagyása
  G: Mégse
Válasszon (H/K/G):
```

A Hiba jelentése lehetőség kiválasztása az ubuntu-bug használatához hasonló lépéseken vezeti végig. Jelentős különbség, hogy az összeomlás-jelentés privátként lesz megjelölve a Launchpadre beküldéskor, azaz csak a hibavadászok korlátozott csoportja fogja látni. Ezek a vadászok személyes jellegű információkat fognak keresni a hiba nyilvánossá tétele előtt, és eltávolítják azokat.

1.3. Információforrások

- Lásd a Reporting Bugs[3] Ubuntu wiki oldalt.
- Az Apport[4] oldala is hasznos információkat tartalmaz, noha ezek egy része a grafikus felület használatára vonatkozik.