

Linuxos kiszolgálót mindenkinek! (4. rész)

A SuSE Linux mint kiszolgáló – kisvállalati és otthoni környezetben.

Sorozatunk előző részében beállítottuk a kiszolgáló első tényleges szolgáltatásait az ügyfelek számára, nevezetesen fájlkiszolgálót és DHCP-kiszolgálót létesítettünk, amelyekkel a helyi hálózat támasztotta igények egy részét ki tudjuk elégíteni. Most azt a szolgáltatást nézzük meg, ami a számítógépes hálózatok egyik úttörő szolgáltatása és az internetfelhasználók egyik legkedveltebb, leghatékonyabb információközlő eszköze: az elektronikus levelezést.

Az elektronikus levelezés működéséhez több különböző feladatot ellátó programnak, az úgynevezett ügynököknek (agent) az együttműködése szükséges. Az egyes ügynökök a levelezés folyamán különböző feladatokat látnak el: az MUA (Mail User Agent – Felhasználói levelezőügynök) feladata a levélnek a felhasználói oldalon történő összeállítás, szerkesztése. Ezek gyakorlatilag a felhasználó által használt levelezőprogramok, ilyen a Mozilla Mail, a Pine vagy az Evolution.

Az MDA (Mail Delivery Agent – Levélkézbesítő ügynök) feladata az adott kiszolgálón az őt címzettként megjelölt üzeneteknek a rajta lévő megfelelő postafiókba való eljuttatása.

Az LDA (Local Delivery Agent – Helyi kézbesítőügynök) feladata a helyi címzetteknek küldött leveleknek a megfelelő postaládába rendezése. Az LDA a rendszerek többségében megegyezik az MDA-val. Linuxos rendszer alatt ilyen ügynök például a procmail.

Utolsóként beszéljünk az MTA-ról (Mail Transfer Agent – Levéltovábbító ügynök), amelynek a leveleknek a megfelelő kiszolgálóhoz való eljuttatása a feladata. Linuxos rendszeren ilyen például a Postfix, a Sendmail vagy az Exim. Jelen cikkünk gerincét a Postfix beállításának az ismertetése alkotja, SuSE 9.0-s rendszer alatt.

A Postfix

A Postfix levélkiszolgáló telepítéséhez indítsuk el a YaST-ot, és a már jól megszokott módon pakoljuk fel a Postfix csomagot. Ha a csomagot telepítettük, a */etc/postfix* könyvtárban lesznek a kiszolgáló beállításait tartalmazó állományok, a */usr/sbin* könyvtárban találjuk meg a kiszolgáló futtatható állományát, valamint a */etc/init.d* könyvtárba kerülnek a kiszolgáló indításához és leállításához használatos parancsállományok.

Továbbá a telepítő létrehozza a */var/spool/postfix* könyvtárat, amelyben a kiszolgáló a feldolgozás alatt álló leveleket fogja



Az elektronikus levél útja

Elektronikus levelet minden esetben egy levelezőprogramban (MUA-ban) írunk meg. Amint elküldjük a levelet, egy MTA veszi át kezelésre és továbbításra, méghozzá azon a címen, amelyik a levelezőprogramunkban SMTP-kiszolgálóként be van állítva. Ezután a levél fejlécéből az MTA megkeresi a címzettet, illetve a címzettkiszolgálót. Miután azonosította a kiszolgálót, továbbítja neki a levelet. Elképzelhető, hogy a levélünk több kiszolgálón is keresztülhalad (a kiépítéstől függően), mire eléri a címzett gépet. Mivel az elektronikus levelek titkosítás nélkül haladnak keresztül a kiszolgálókon, a köztes kiszolgálókon elvileg lehetőségünk nyílik a levél elolvasására. Ennek kiküszöbölésére születtek meg a különböző titkosítási módszerek, amelyekkel a levél tartalma illetéktelenek számára hozzáférhetetlenné válik. A legkorszerűbb titkosítási eljárások az úgynevezett nyílt kulcsú titkosítási eljárások, amelyek egy kulcspárral üzemelnek, mégpedig olyan módon, hogy a küldő egy mindenki számára ismert kulccsal titkosítja a levelet, amit utána a saját titkos kulcsával csak a címzett tud visszafejteni. Ilyen kulcspárral történő aláírással érhető el az is, hogy a tőlünk származó leveleket elektronikusan aláírjuk, így egyértelműen megállapítható, hogy tőlünk érkeztek-e. Nagyon kell azonban ügyelnünk a titkos kulcsra, mert nyilvánosságra kerülése esetén mind az azonosítási rendszer, mind a titkosítás átjárható lesz. Miután a levél megérkezett a címzett kiszolgálóhoz, a kiszolgáló LDA ügynöke átveszi a levelet – az ő feladata a levélnek a megfelelő helyi postaládában való elhelyezése. Amint ez megtörtént, levelünket, s a címzett a saját levelezőprogramjával – a MUA-val – el is tudja olvasni ezzel az elektronikus üzenet célba is ért.

tárolni, így a várakozási sorban lévő és a visszautasított levelek is itt lesznek megtalálhatóak. Ez azért fontos, mert ha esetleg rossz beállítással futtatjuk a kiszolgálót, óriási mennyiségű felesleges levéllel töltheti fel a rendszert – e könyvtárak kiürítésével tudjuk a felesleges elemeket törölni, s ezzel megelőzhetjük a rendszer esetleges összeomlását.

A YaST a barátunk

Mint azt már megszokhattuk, a SuSE ismét kínál egy eszközt, amellyel kiszolgálónk alapbeállításait el tudjuk végezni. A YaST *Hálózati szolgáltatások* menüpontja alatt található *Levéltovábbító szerver* modult indítva lehetővé teszi számunkra az elsődleges levélkiszolgáló szabványos felületen történő beállítását.

A megjelenő *Kapcsolat típus* ablakban ki kell választanunk a hálózati kapcsolatunkat. Ha interneten keresztül is szeretnénk levelezni, tehát nem csak egyfajta vállalati levelezést szeretnénk megvalósítani, internetkapcsolatunk típusától függően válasszuk az *Állandó* vagy a *Betárcsázás* *kapcsolat*-ot. Amennyiben „betárcsázással” kapcsolódunk az internetre, a levelező a várakozási sorba érkező leveleket nem továbbítja önműködően, elindításukat a `sendmail -q` parancs révén kézzel tehetjük meg. Ilyen esetben természetesen írhatunk egy olyan parancsállományt, amely az internetes kapcsolat létrejöttekor lefuttatja a várakozási sor ürítésére szolgáló parancsot.

Amennyiben víruskereső szolgáltatást is szeretnénk kapcsolni a levélkiszolgálóhoz, azt a *Víruskeresés engedélyezése* bekapcsolásával tehetjük lehetővé. Ha az Amavis víruskereső nincs telepítve, a YaST ezt is elvégzi helyettünk.

A következő lépésben megadhatjuk a levelek továbbítására használni kívánt SMTP-kiszolgálót. A mező értékének adjuk a `localhost` értéket, amennyiben a jelenleg telepített kiszolgálót szeretnénk használni. Ha azonban egy másik kiszolgálóval szeretnénk a leveleket továbbítani, a teljes internetcímét adjuk meg.

Az *Álcázás* gombra kattintva lehetőségünk nyílik gépünk és felhasználóink alapértelmezett nevének és címének a felülírására. Ez akkor lehet hasznos, ha a rendszert internetes és belső hálózati (intranetes) környezetben egyaránt használjuk, valamint több címtartományt is kiszolgálunk, ezért különböző felhasználóinkhoz különböző címek tartoznak. Az első sorban a *Doménnév* a *'From'* (küldő) fejlécmező *száma* mezőben megadhatjuk a kiszolgálóhoz tartozó elsődleges címet, így amennyiben például a gépünk a *kiszulgo.tartomany.hu* címmel azonosítható és mi ebbe a mezőbe a *tartomany.hu* értéket írjuk, a *felhasznalo@kiszulgo.tartomany.hu* helyett a kimenő levelek feladója minden esetben a *felhasznalo@tartomany.hu* lesz.

A *Doménevek helyi kézbesítéshez* mezőben megadhatjuk, hogy a helyi levelek kézbesítésekor a felhasználó neve után milyen cím szerepeljen. Továbbá lehetőségünk van annak a beállítására is, hogy csak a helyi nevet akarjuk-e álcázni vagy egyéb címeket is felül akarunk-e írni. Ezenkívül azt is megtehetjük, hogy minden egyes felhasználónkhoz egyesével rendelünk hozzá elektronikus levélcímeket. Ehhez a *Hozzáadás* gombot szükséges használnunk, és a felhasználót ki kell választanunk a listából, valamint meg kell adni a hozzá tartozó elektronikus levélcímet. Ezzel az *Álcázás* menüpont beállítási lehetőségeinek a végére értünk – az *OK*-ra kattintva visszatérünk a *Kimenő levelek* ablakba. Az *Azonosítás* gombra kattintva lehetőségünk van elérési

jellemzők megadására a szolgáltatónk által rendelkezésünkre bocsátott SMTP-kiszolgálóhoz, ha a szolgáltató ezt a levelek elküldéséhez kéri. Amennyiben a saját gépünkön (`localhost`) lévő kiszolgálót használjuk, és előzőleg nem állítottunk be elérési korlátokat, ezeket a mezőket nyugodtan kihagyhatjuk.

A következő megjelenő ablak a *Bejövő levelek* ablaka; itt lehetőségünk nyílik beállítani, hogy a bejövő levelek melyik címzethez kerüljenek, továbbá azt is, hogy a helyi kiszolgálónk egy másik levélkiszolgálóról töltse le a nekünk szóló leveleket, éppen úgy, mint azt a levelezőprogramok is teszik. Az utóbbinak akkor van értelme, ha kapcsolt vonali internetszol-



gátatással rendelkezünk, ezért nincs rá lehetőség, hogy közvetlenül a kiszolgálónk címezzék azokat.

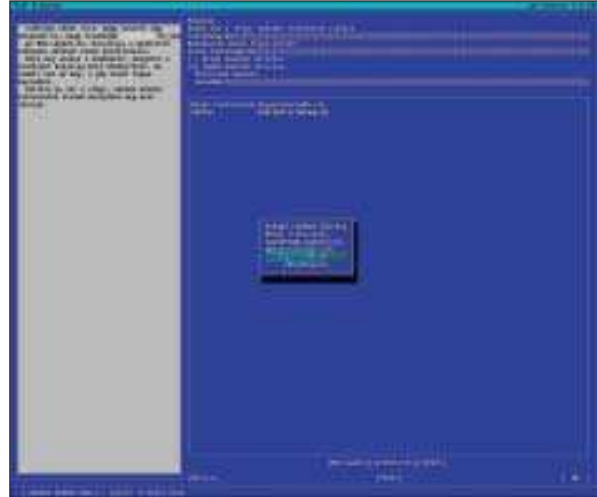
Nézzük először a levelek kézbesítésének a beállításait! A *root* leveleinek továbbítása az *alábbi felhasználónak* változó értékéként adjuk meg azt a felhasználót, akinek a rendszergazdához érkező leveleket továbbítani szeretnénk. Ez azért szükséges, mert a *root*-ot általában nem használjuk levelezési célokra, a rendszer felügyeletét végző embernek pedig valószínűleg egy külön felhasználót hoztunk létre, így neki továbbíthatjuk az olyan leveleket, amiket a rendszergazdának kell megkapnia, például a naplóállományokat, a riasztásokat.

Kézbesítési mód-ként válasszuk a *procmailen keresztül* lehetőséget, ami azért lesz hasznos, mert a *procmail* LDA-hoz tartozik egy központi és egy felhasználótól függő beállításállomány, amiben a levelek szűrését, csoportosítását központilag vagy külön-külön is szabályozni tudjuk. Bővebb tájékoztatással a *procmail* sűgőállománya szolgál. Az *Álnevek* gombra kattintva szerkeszthetjük a */etc/aliases* állományt, amely a helyi felhasználó-kézbesítési hely párokat tartalmazza. Itt lehet beállítani, hogy az adott felhasználónak érkező levelet a levelező hová továbbítsa. Ez lehet egy másik helyi felhasználó, de egy másik gépen lévő felhasználó is, emiatt itt akár egy elektronikus levélcímet is megadhatunk.

A *Virtuális doméne* gombra kattintva a */etc/postfix/virtual* állomány tartalmát szerkeszthetjük. Ennek hasonló a szerepe, mint a */etc/aliases* állománynak, de itt a bal olda-



1. kép A bejövő levelek beállítása a YaST-ban

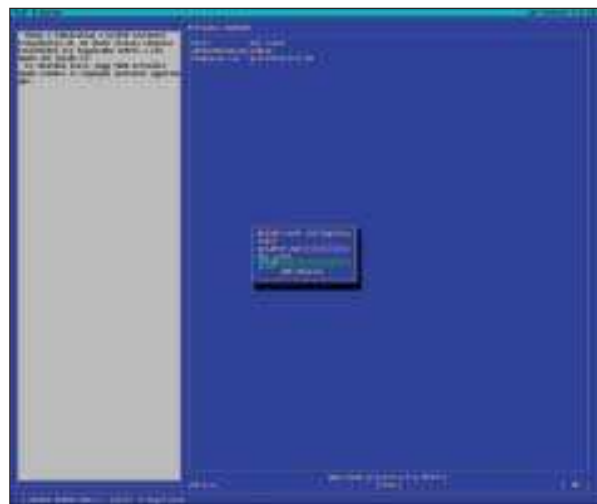


2. kép Álcázás és alapértelmezett címek beállítása a YaST-ban

lon megadhatunk felhasználót, tartományt vagy akár elektronikus levélcímet is. Például beállítható, hogy a *tartomany.hu* tartomány bármelyik felhasználójához érkező levelet egyvalaki kapja meg. Lássunk egy-két példát! Ha egy olyan bejegyzést készítünk, aminek a bal oldalán az *info@tartomany.hu* áll, míg a jobb oldalon a titkárnő, akkor a fenti elektronikus levélcímre érkező leveleket a titkárnő felhasználó fogja megkapni. Amennyiben olyan szabályt készítünk, hogy a *@tartomány2.hu: főnök*, akkor a *tartomány2.hu* tartományba érkező összes levelet a főnök felhasználó kapja meg. További útmutatást a `man virtual` paranccsal kaphatunk. Mind az *aliases*, mind pedig a *virtual* állományokat a fent leírt helyeken kézzel is szerkeszthetjük, de a szerkesztés után az adatbázist is frissíteni kell. Első esetben ezt a `newaliases`, az utóbbiban a `postmap /etc/postfix/virtual` paranccsal tehetjük meg. Utolsó beállításként nézzünk egy hasznos eszközt azok számára, akiknek különböző szolgáltatóknál vannak postaládái, ideiglenes kapcsolattal rendelkeznek, és így nincs lehetőségük közvetlen levélfogadásra a nap minden percében. A Linux ennek feloldására is kínál egy eszközt, a Fetchmail. Ezzel a programmal a megfelelő beállításállományban megadott értékekkel csatlakozik a gépünk a távoli kiszolgálóhoz és onnan a megfelelő levelezőprotokoll használatával letölti leveleinket a saját kiszolgálónkra, így olyan módon tudjuk kezelni őket, mintha közvetlenül a kiszolgálónkra érkeztek volna.

Egy ilyen beállítást ki is tudunk tölteni a *Bejövő levelek* oldalon, de ha a *Részletek* gombra kattintunk, a felbukkanó új ablakban egész listát vehetünk fel a különböző felhasználókhoz. A *Hozzáadás* gomb megnyomására felbukkanó ablakban meg kell adnunk a kiszolgáló nevét: ez a távoli postaládánkat tároló kiszolgáló címe lesz; a használni kívánt protokollt, ami általában vagy a POP3 vagy az IMAP, továbbá meg kell adnunk a távoli felhasználó nevét jelszavát, amivel hozzáférésünk lesz a rendszerhez; és végül be kell írunk a felhasználót, akinek a helyi gépen a leveleket le akarjuk tölteni.

Ha végeztünk a lista elkészítésével, az itt felvett jellemzők a `/etc/fetchmail.rc` állományban mentésre kerülnek, amelyben



3. kép Virtuális címek és kézbesítési helyük

a későbbiek során a listát kézzel is szerkeszteni tudjuk. Az állomány szerkesztésével lehetőségünk van SSL-kapcsolattal is ellátni a letöltést, így a jelszavak és az adatok titkosítva haladnak a távoli kiszolgáló és a miénk között – amennyiben ezt a távoli kiszolgáló számunkra lehetővé teszi. Ehhez a létrehozott bejegyzés végére be kell szúrni az `options ssl` tagot.

Ha ezzel is végeztünk, zárjuk be a varázslót, amely elkészíti nekünk a levélkiszolgáló alapbeállításait.

Nézzük meg a beállításokat közelebbről is!

Bár a varázsló ügyes megoldás a SuSE részéről, korántsem lehet minden apró lehetőséget kiaknázni vele, ezért lehet, hogy kézzel is bele kell nyúlnunk a beállításokba. Először nézzük a `/etc/postfix/main.cf` állományt. Megvizsgálunk pár beállítást, amit a kiszolgáló biztonsága érdekében mindenképpen el kell végeznünk. Az első ilyen a *mynetworks* – ennek a változónak az értéke azt mutatja meg, hogy az SMTP-kiszolgáló mely hálózatoknak nyújt levélküldési szolgáltatást. Ahhoz, hogy elkerülhessük a

reklámozók rajtunk keresztüli történő levélszemétküldését (spam), ezt a változót olyan módon kell beállítanunk, hogy csak a saját gépről (localhost), esetleg a belső hálózat IP-tartományából fogadjon el levelet küldésre. Például a `mynetworks=127.0.0.0/8 10.0.0.0/24` beállítás csak a saját gépről, valamint a 10.0.0.1 és 10.0.0.254 közötti gépekről fogad el levélküldési parancsot. Egyes ügyfeleket adhatunk meg IP-címmel, vagy hálózatokat címmel és hálózati maszkkal, egyszerű felsorolásként, szóközzel elválasztva. A `myorigin` változó tárolja a kiszolgáló elsődleges tartománynevét. A `mydestination` változóban tartományneveket sorolhatunk fel vesszővel elválasztva, ezeket fogja a kiszolgáló a beérkező leveleknél címzettként elfogadni. Amennyiben azt szeretnénk, hogy a levél beérkezése után a Postfix a feldolgozást adja át a `procmail`-nek, valamint a felhasználók szűrési szabályokat tudjanak írni, a `mailbox_command = procmail -a "$EXTENSION"` sornak mindenképpen szerepelnie kell a beállítások között. Amennyiben a rendszer terhelésének ellenőrzéséhez korlátozni szeretnénk a postaládák méretét, illetve meg kívánjuk adni az elküldhető levél legnagyobb méretét, ezt a `mailbox_size_limit` és a `message_size_limit` változók beállításával tehetjük meg. Mindkét változó egy számot vár értéként, ez a szám pedig a méret leírása bajtokban. Például az 1 MB-os postaládaméret beállításához a `mailbox_size_limit=1024000` értéket szokták megadni. A `/etc/postfix/virtual` állomány tárolja a virtuális tartományokhoz tartozó elektronikus levélcímeket és felhasználókat, ha ilyet a varázslón keresztül készített beállításban megadtunk. Amennyiben eddig nem tettük volna meg, a fent leírt szabályokat itt is meg tudjuk adni. Bal oldalon azt a címzettet vagy címtartományt szükséges beírni, ahová a levél érkezik, majd egy szóköz után azt a helyi felhasználót vagy elektronikus levélcímet kell megadnunk, ahová a szabálynak megfelelő levelek továbbítódnak. Így tudunk olyan elektronikus levélcímeket is létrehozni, amelyekhez nem tartozik valóságos felhasználó a rendszerben, hanem csak egy távoli postafiókba továbbítjuk a levelet. Ne felejtsük el azonban, hogy az állomány módosítása után a `postmap /etc/postfix/virtual` parancsot le kell futtatnunk – ha a `virtual` állomány a `/etc/postfix` könyvtárban helyezkedik el – ahhoz, hogy a változásokat a rendszer érvényre juttassa. A mindenkori adatbázis a `/etc/postfix/virtual.db` állományban található. A `/etc/postfix/access` állományban állíthatjuk be a szűrési feltételeket az elektronikus levelek feladójára, a teljes elektronikus levélcímre vagy az elektronikus levél feladójának tartományára. Ezzel egy egyszerű levélszemétszűrést állíthatunk be, ami mostanában már sajnos nem túl hatékony, mert a levélszemétküldők vagy állandóan változó címet használnak, vagy úgy választanak címet, hogy a feladót a saját tartományunkból érkezőként állítják be. A szűrési feltétel egy párosból áll, amely egy mintából és egy cselekvésből tevődik össze. Minta lehet egy elektronikus levélcím, például a `felhasznalo@kiszorgalo.tartomany.hu` – ekkor a teljes címet figyeljük, vagy a cím töredéke (`felhasznalo@`), amikor is a felhasználó nevű felhasználóktól érkező levelek kerülnek szűrésre, függetlenül attól, hogy a levél milyen tartományból érkezett. Végül, de nem utolsósorban a szűrési

feltétel lehet egy tartomány, tehát például a `kiszorgalo.tartomany.hu` vagy a `tartomany.hu`. Az utóbbi esetben természetesen az első példa is szűrt lesz, de emellett az összes olyan cím is, ami `tartomany.hu`-ra végződik. Cselekvés lehet a levél eldobása (DISCARD), a levél visszatartása (REJECT) vagy a levél elfogadása is (OK). Ezeken kívül beállítható még, hogy a beérkező levelet tartalomszűrésnek is alá vesszük, ehhez a FILTER kulcsszót kell megadni. Erről és többi beállításról bővebb leírást a `man access` parancs kiadásával kaphatunk.

A `virtual` tábla frissítéséhez hasonlóan az `access` táblát is frissíteni kell a `postmap` parancsral, pontosabban a `postmap /etc/postfix/access` parancsral. Ahhoz, hogy ezt a szűrést használni tudjuk, a `/etc/postfix/main.cf` beállításai között szerepelnie kell a `smtpd_sender_restrictions=hash:/etc/postfix/access` beállításnak.

Ezzel a legfontosabb beállításokat talán el is végeztük levelezőrendszerünkön, ami mostanra már működőképes. Ne felejtsük el a tűzfalunkon a megfelelő kapukat kinyitni, ha szükségesek, valamint figyeljünk oda arra is, hogy a YaST-on belül a *Futási szint szerkesztő*-ben szintén be kell állítani, hogy a megfelelő futási szinteken a Postfix önműködően elinduljon. Továbbá ne feledjük, hogyha a beállításokat elvégeztük, a `/etc/init.d/postfix restart` parancsral indítsuk újra a levélkiszolgálót, hogy az új beállítások érvénybe lépjenek.

Ha végeztünk a kiszolgáló beállításával és elindítottuk, akkor a biztonság kedvéért kövessük figyelemmel a `/var/log/mail`, `mail.err`, `mail.warn`, `mail.info` naplóállományokat, hogy a kiszolgálón felmerülő esetleges hibákat mielőbb orvosolni tudjuk. Nincs ugyanis kellemtlenebb dolog, mint egy rosszul beállított kiszolgáló miatt elkallódó levél. Írásom végére érve elmondhatjuk, hogy működő SMTP-kiszolgálót hoztunk létre. Sorozatom következő részében ezt kiegészítjük azzal, hogy a legnépszerűbb ügyfél-hozzáférési protokollokat telepítjük a rendszerre, foglalkozunk a POP3 és IMAP protokollokkal, illetve azok titkosított, úgynevezett SSL-változatával.



Illés Viktor (viktorei.hu)

23 éves, a BME műszaki informatikus szakának hallgatója, mellette weblapokkal, linuxos és windowsos rendszerekkel foglalkozik. Szabadidejét legszívesebben a szabadban tölti, teniszezik és kerékpározik.

Helyreigazítás

A 2003. decemberi számban megjelent cikkemben a rendszer hálózati csatlóinak ellenőrzésére az `IPCONFIG` parancsot neveztem meg – ez elírás, ugyanis a hálózati csatlókat linuxos rendszereken az `IFCONFIG` parancsral tudjuk listázni. Az `IPCONFIG` is működő parancs, de az egy másik kereskedelmi operációs rendszer hasonló célokra szolgáló utasítása.

A fenti elírás miatt minden kedves olvasó elnézését kérem.