Vabariigi Valimiskomisjon

E-hääletamise süsteem
Operatsioonisüsteemi paigaldus

versioon 4.3

dokument: EHA-03-10-4.3
kuupäev: 19.01.2015

Redaktsioonide ajalugu

kuupäev	versioon	kirjeldus	autor
16.11.2006	1.0	algversioon	Uve Lokk
19.12.2006	1.1	parandatud, täiendatud peatükke „Cd-de loomine”, „Üldine”	Uve Lokk
28.12.2006	1.2	täiendatud peatükke „HES”, „HTS” ja „HLR”	Uve Lokk
04.01.2007	1.3	muudetud struktuuri, täpsustatud termineid	Uve Lokk
05.01.2007	1.3.1	muudetud peatükki „Töökeskkonnaks tarvilike ...”; tööserverite paigaldusse lisatud arvutivõrgu puudumise kontroll	Uve Lokk
19.01.2007	1.4	üldine vigade parandus, punktliigendus asendatud suuremas osas numberliigendusega	Uve Lokk
19.01.2007	1.4.1	pisitäpsustused, liigendusmuudatused	Uve Lokk
27.01.2007	1.5	lisatud üldteavet ja selgitusi	Uve Lokk
15.04.2009	2.0	suurem hulk muudatusi seoses operatsioonisüsteemi vahetusega (Debian 3.1 -> Debian 4.0)	Uve Lokk
21.04.2009	2.1	läbivad muudatused / täiendused / parandused	Uve Lokk
18.05.2009	2.2	kuna e-hääletamise tarkvaraplaat ei ole Debian'i repositooriumina kasutatav, on lisatud e-hääletamise tarkvara repositooriumi loomise protseduur	Uve Lokk
16.09.2009	2.3	läbivad parandused	Uve Lokk
18.09.2009	2.4	Muudetud peatükki "Töökeskkonnaks tarvilike DVD-plaatide loomine", teistes peatükkides ühtlustatud termineid	Uve Lokk
20.01.2011	3.0	suurem hulk muudatusi seoses operatsioonisüsteemi vahetusega (Debian 4.0 i386 -> Debian 5.0 amd64)	Uve Lokk
20.09.2013	4.0	suurem hulk muudatusi seoses operatsioonisüsteemi vahetusega (Debian 5.0 amd64 -> Debian 7 amd64); lisandus logiserver;	Uve Lokk

kuupäev	versioon	kirjeldus	autor
20.09.2013	4.1	lisatud peatükk e-hääletamise tarkvara kontrolliks ja valmendamiseks	Tarvi Martens
16.04.2014	4.2	serverite kettapinna partitsioneerimisel võetud kasutusele LVM; veidi täpsustusi	Uve Lokk
19.01.2015	4.3	täiendused, parandused; lisandusid uued rakenduspakid (samhain ja exim4)	Uve Lokk

Sisukord

Sissejuhatuseks

Käesoleva juhendi eesmärgiks on anda võimalikult detailne ülevaade sellest, kuidas saada füüsiline server e-hääletamiseks kõlbulikku seisu, täitmaks kas häältee-dastuse (HES), häältetalletuse (HTS), logitalletuse (LOG) või häältelugemise (HLR) funktsiooni. Kirja on pandud ka elementaarsena tunduvad asjad – teinekord kipuvad just need ununema.

Vast ainus oluline punkt, mis ühe veebiserveri paigaldusega kokku käib ent mida käesolev juhend ei kajasta, on veebiserveri võtmete protseduurid (võtmepaari loomine, sertifikaadipäring jne.). Viimased on kirjas dokumendis EHA-03-02-* - "E-hääletamise käsiraamat"

Töökeskkonnaks tarvilike DVD-plaatide loomine

1. Eesmärk: luua

1.1. operatsioonisüsteemi Debian 7 amd64 viimase väljalaske (edaspidi ‚OS') kontrollitud räsiga tõmmisfailidest paigaldus-DVD'd;

1.2. OS'i uuenduspakkidega andmekandja (uuendusplaat)

2. Eeldused:

2.1. OS'i 1. ja 2. DVD-tõmmisfailid või -valmisplaadid; kuna 3. DVD-tõmmisfaililt kasutatavate pakkide arv on tühine, laaditakse need protseduuride käigus alla ning lisatakse uuendusplaadile;

2.2. Cybernetica AS'i e-hääletamise tarkvara plaat;

2.3. DVD-kirjutajaga tööjaam;

2.4. võrguühendus

3. Paigaldus-DVD'd

3.1. laadi alla OSi 1, ja 2. DVD iso-faili ning SHA256-räsifail. Debian'i failiserveri aadress `ftp://cdimage.debian.org/cdimage/release/`.

3.2. kontrolli iso-failide räsisid. Viimased saab Debiani iso-failide primaarserverist (vt. ka eelmist punkti). Pärast räsifaili allalaadimist eemalda tööjaamalt DVD'de kirjutamise ajaks võrgukaabel, välistamaks allalaaditud iso-falide asendamist.

3.3. kirjuta iga iso-tõmmis tühjale dvd-plaadile. Näiteks Linux'is käsuga

```
$ growisofs -speed=4 -Z /dev/dvd=iso_faili_nimi
```

4. paigalda OS

4.1. Alglaadi tööjaam OS'i 1. DVD'lt

4.2. vali 'Advanced options' -> 'Expert install'

4.3. järgnevatest valikutest on olulised:

- Configure the package manager
  - peegelserveriks `ftp.ee.debian.org`
  - Use non-free software : <No>
  - Use contrib software: <Ei>
  - Services to use:
    - [*] security updates
    - [ ] release updates
- 'Select and install software' jäta vahele

4.4. Järgneb taaskäivitus

5. OSi häälestus

5.1. Lisa OS'i DVD 2. plaat ning e-hääletamise tarkvara repositoorium tarkvara paigaldusallikate nimekirja käsuga

```
$ apt-cdrom add
```

5.2. tühjenda puhverdatud pakkide kaust:

```
$ aptitude clean
```

5.3. uuenda pakiinfot:

```
$ aptitude update
```

5.4. paigalda tarkvarauuendused:

```
$ aptitude safe-upgrade
```

5.5. paigalda vajalikud rakenduspakid

```
$ aptitude -R install dvd+rw-tools exim4-daemon-light \
    irqbalance less lvm2 minicom mysqltuner ncftp ntpdate \
    openssh-server samhain wodim
```

5.6. Peata paigalduse käigus käivitatud võrguteenused:

```
$ service ssh stop
$ service exim4 stop
```

6. Uuendusplaadi loomine

6.1. loo kataloog `/home/plaat`

```
$ mkdir /home/plaat
```

6.2. paigalda evote-pakid, saamaks kätte Debian'i sõltuvuspakid

```
$ aptitude -R install evote-common
$ aptitude -R install evote-hes
$ aptitude purge evote-hes
$ aptitude -R install evote-hts
$ aptitude purge evote-hts
$ aptitude -R install ivote-monitor
$ aptitude purge ivote-monitor
$ aptitude -R install evote-hlr
$ aptitude purge evote-hlr
```

6.3. kontrolli kataloogis `/var/cache/apt/archives/` olevate pakkide kontrollsummat. Allpooltoodud failidest saab genereerida faili, mis võimaldab utiliidi `sha256sum` abil automaatset räsikontrolli. Näiteks security-pakkide Packages-failist eraldatatakse vaid read, mis algavad stringiga ‚Filename' või ‚SHA256', seejärel asendatakse väljundis olevad kaldkriipsud tühikutega; seejärel pannakse ühte ritta stringiga ‚SHA256' algava rea 2. väli (räsi) ning stringiga ‚Filename' algava rea 6. või 7. väli (failinimi), jättes nende vahele kaks tühikut.

```
$ cd
$ wget -O SecPackages.bz2 http://security.debian.org/dists/\
    wheezy/updates/main/binary-amd64/Packages.bz2
$ bunzip2 SecPackages.bz2

$ wget http://ftp.debian.org/debian/dists/wheezy/main/\
    binary-amd64/Packages.bz2
$ bunzip2 Packages.bz2

$ grep –e '^Filename:\|^SHA256:' SecPackages | \
    sed –e 's,/, ,g' | awk '/Filename:/ {filename=$7} \
    /SHA256:/ {sha=$2; print sha"  "filename}' \
    > kontroll.txt

$ grep –e '^Filename:\|^SHA256:' Packages | \
    sed –e 's,/, ,g' | awk '/Filename:/ {filename=$6} \
    /SHA256:/ {sha=$2; print sha"  "filename}' \
    >> kontroll.txt

$ cd /var/cache/apt/archives
$ ls *.deb | grep -f - /root/kontroll.txt | sha256sum -c -
```

6.4. kopeeri kõik allalaaditud deb-pakid kataloogi `/home/plaat`

```
$ cp /var/cache/apt/archives/*.deb /home/plaat/
```

6.5. sikuta võrgust alla Debian'i indices-fail.

```
$ cd /home
$ wget http://ftp.ee.debian.org/debian/indices/\
    override.wheezy.main.gz
$ gunzip override.wheezy.main.gz
```

6.6. paigalda pakk `dpkg-dev` (selles on käivitusfail dpkg-scanpackages)

```
$ aptitude -R install dpkg-dev
```

6.7. genereeri pakkide nimekiri

```
$ dpkg-scanpackages plaat/ override.wheezy.main 2>vead | \
    gzip > plaat/Packages.gz
```

6.8. loo plaadi tunnus

```
$ mkdir plaat/\.disk
$ echo –n 'Uuendusplaat' > plaat/\.disk/info
```

6.9. kirjuta dvd-plaat:

```
$ growisofs -Z /dev/dvd –R -J -l -speed=4 /home/plaat/
```

6.10. kontrolli, kas uuendusplaat on korrektne: lisa plaat repositooriumide nimekirja:

```
$ apt-cdrom add
```

6.11. märgista dvd-plaat: „Uuendusplaat"

E-hääletamise serveritarkvara kontroll ja valmendamine

Eesmärk: kontrollida tarkvaraarendaja poolt tarnitud e-hääletamise süsteemi terviklust ning selle vastavust Internetis avalikustatud versiooniga. Etapi tulemuseks on kontrollitud paigaldustarkvara sisaldav DVD-plaat.

7. Kontrolli tarkvaratootja poolt tarnitud digitaalselt allkirjastatud kontrollsummade faile; pärast digitaalallkirja kontrolli eralda konteinerite sisu edasiseks töötlemiseks.

8. Vii läbi protseduur „E-hääletamissüsteemi paigalduspakkide valmendamine" vastavalt dokumendi „Süsteemiülema juhend" jaotisele 2.2.

9. Lisa valmendatud .deb pakkidele fail `evote-analyzer_*.deb` ja `ivote-monitor_*.deb` tarkvaratootja poolt tarnitud CD-lt.

10. Loo ISO tõmmis ning kirjuta DVD plaat. Markeeri see. Kirjutamiseks sobib käsk

```
$ growisofs -speed=4 -Z /dev/dvd=iso_faili_nimi
```

11. Kontrolli, et loodud plaat oleks repositooriumina kasutatav:

```
$ apt-cdrom add
```

Üldine paigaldus

Etapi eesmärk on paigaldada tööserveritele operatsioonisüsteem ning seejärel häälestada see paigaldusskripti abil konkreetsele e-hääletamise funktsioonile vastavaks. Automaatsele häälestusele järgneb veel käsitsihäälestus, mis allpool samuti dokumenteeritud.

12. Eeldused:

12.1. OS'i 1. ja 2. DVD-plaat

12.2. uuendusplaat

12.3. emb-kumb - tarnitud või isetehtud - e-hääletamise tarkvara repositooriumidest

12.4. riistvaralise turvamooduli tarkvaraplaat

12.5. füüsilised serverid

13. kontrolli, et server ei oleks ühendatud arvutivõrku

14. käivita server OSi 1. DVD-ga

15. Vali 'Advanced Options' -> 'Expert Install'.

16. Choose language

16.1. Choose a language: 'English'

16.2. Choose a country, territory or area: 'other' -> 'Europe' -> 'Estonia'

16.3. Country to base default locale settings on: ’en_US.UTF-8’

16.4. Additional locales: ’et_EE.UTF-8’, ’et_EE’

16.5. System locale: ’en_US.UTF-8’

17. Configure the keyboard

17.1. Keymap to use: vali laotusele vastav

18. Detect and mount CD-ROM

18.1. Modules to load: ära muuda valikut

18.2. CD-ROM detected; 'Continue'

19. Load installer components from CD

19.1. Installer components to load: ära muuda valikut; 'Continue'

20. Detect network hardware

20.1. Juhul, kui tegemist on omandusliku koodiga püsivara nõudva võrgukaardiga (näiteks Broadcom), tuleb teha järgmist:

- võtta Debian 7 Wheezy'ga tööjaam, millel oleks võrguühendus;
- kontrollida, et OSi tarkvarapakkide repositooriumis oleks hääles-tatud ka omandusliku koodiga ("non-free") tarkvara kasutamine lubatud;
- kontrollida, et vajalik püsivarapakk ei oleks juba paigaldatud;
- kontrollida, et kaustas `/lib/firmware` vajalikku püsivarafaili juba olemas ei oleks;
- allalaadida püsivarapakk; näiteks

```
aptitude download pakinimi
```

- laadi alla (soovitavalt mõnest teisest tarkvarapeeglist kui see, kust pakk sai alla laaditud) omandusliku koodiga tarkvara-pakkide nimekiri;
- kontrolli viimase abil allalaaditud püsivarapaki kontrollsummat;

- paigalda pakk:
  ```
  dpkg -i pakinimi
  ```
- võta tühi mälupulk ning vorminda see;
- sisesta mälupulk arvuti USB-porti ning haagi see;
- kopeeri mälupulga juurkataloogi
  - püsivarafailid, kaustast `/lib/firmware`,
  - püsivarapakk;
- haagi mälupulk lahti ning eemalda USB-pordist;
- kasuta mälupulka nii nagu rakendusserveri OSi paigaldamise teated seda ette näevad

21. Configure the network

21.1. Waiting time (in seconds) for link detection: ära muuda

21.2. Primaarne võrguliides (küsitakse juhul, kui serveris on 2 või enam võrgukaarti): eth0

21.3. Auto-configure networking: 'No'

21.4. IP address: HES, HTS ja LOG: xxx.xxx.xxx.xxx; HLR: 10.0.0.2

21.5. Netmask: HES, HTS ja LOG: 255.255.xxx.xxx; HLR: 255.255.255.0

21.6. Gateway: HES, HTS ja LOG: xxx.xxx.xxx.xxx; HLR: väli jääb tühjaks)

21.7. Nimeserverid jäävad kõikidel serveritel määramata

21.8. Is this information correct?: (kui on, siis 'Yes')

21.9. Hostname: kas ‚hes', ‚hts', 'log' või ‚hlr'

21.10. Domain name: valimised.ee

22. Set up users and passwords

22.1. Enable shadow passwords: 'Yes'

22.2. Allow login as root: Yes

22.3. Root password: *********. Operaatorid lepivad kokku parooli, kumbki paneb selle kirja. Parooli sisestab Operaator1

22.4. Re-enter password to verify. Parooli sisestab kontrolliks Operaator2

22.5. Create a normal user account now: 'No'

23. Configure the clock

23.1. Set the clock using NTP?: 'No'

23.2. Select your time zone: 'Europe/Tallinn'

24. Detect disks

25. Partition disks

25.1. Partitioning method: Manual

25.2. Kustuta olemasolevad partitsioonid

25.3. Loo järgmised primaarpartitsioonid:

- /boot – 100 MB, failisüsteem ext4; nodev, nosuid, noexec
- ülejäänud kettapind kasuta LVMi füüsilise köite alana

25.4. Configure the Logical Volume Manager

- loo köitegrupp (Volume Group)
- loo järgnevad loogilised köited arvestusega, et köitegrupil jääks vähemalt 2GB kasutamata:

LV nimi	haakepunkt	suurus	failisüsteem	haakeparameetrid
juur	/	≥20G	ext4	
var	/var	≥20G	ext4	nodev
log	/var/log	50G	ext4	nodev,noexec
tmp	/tmp	10G	ext4	nodev
swap		1G	swap	

- **NB!: HLR'ile saaleala luua ei tohi!**

25.5. Finish partitioning and write changes to disk

- Write the changes to disks?: 'Yes'

26. Install the base system

26.1. Kernel to install: vali määratud versiooniga kernel

26.2. Drivers to include in the initrd: targeted

27. Jäta vahele etapid "Configure the package manager" ja "Select and install software"

28. Jätka etapiga "Install the GRUB boot loader on a hard disk"

28.1. Install the GRUB boot loader to the master boot record?: 'Yes'

28.2. Jäta GRUB'ile salasõna määramata

29. Finish the installation

29.1. Is the system clock set to UTC?: 'Yes'

29.2. Installation is complete ...: 'Continue'

30. Järgneb alglaadimine

31. Logi sisse

32. Vajadusel sünkroniseeri serveri kell, käsuga

```
$ date MMDDhhmmYYYY
```

33. Lisa tarkvaraplaadid paigaldusallikate nimekirja

33.1. Pane OSi 2. plaat, uuendusplaat ja e-hääletamise tarkvara repositoorium ükshaaval DVD-seadmesse ning iga plaadi puhul anna käsk

```
$ apt-cdrom add && eject
```

33.2. HLRile lisa sama käsuga ka HSM'i tarkvara plaat

34. Kontrolli, et kõik plaadid oleks paigaldusallikate nimekirjas failis `/etc/apt/sources.list`

35. Juhul, kui OSi paigaldamisel oli vaja kasutada omanduslikku püsivara, paigalda ka selle pakk samalt mälupulgalt, mida kasutati OSi paigaldamisel.

36. aseta DVD-seadmesse plaat, kus on skript `evote_post_ava.sh`, kopeeri see serverisse ning eemalda plaat

```
$ mount /dev/dvd /media/cdrom0
$ cp /media/cdrom0/debian/evote_post_ava.sh .
$ chmod 700 evote_post_ava.sh
$ umount /media/cdrom0
```

37. käivita järelhäälestusskript, kus $TÜÜP on serveritüüp (hes, hts, log või hlr)

```
$ HOME/evote_post_ava.sh $TÜÜP
```

38. Pane kasutajale ‚hes', ‚hts', ‚log' ja ‚hlr' määratud salasõna kirja ning hoolitse, et see oleks asjaga mitteseotud inimeste eest varjatud

39. Kopeeri serverisse järelhäälestusskript `evote_post_priv.sh` ning käivita see

```
$ HOME/evote_post_priv.sh $TÜÜP
```

HES

40. Kontrolli, et võrgukaardid oleks korrektselt häälestatud (kerneli moodulid, ip-aadressid). Vajadusel korrigeeri (näiteks mitme HESi puhul).

41. Paigalda pakk evote-analyzer

HTS

42. Kontrolli, et võrgukaardid oleks korrektselt häälestatud (kerneli moodulid, ip-aadressid). Vajadusel korrigeeri.

43. Kontrolli, et veebiserver 'kuulaks' vaid HESiga ühendatud võrguliidesel ning ip-aadressil 127.0.0.1 (häälestusfailiks `/etc/apache2/apache2.conf`, parameeter 'Listen')

44. Lisa failis `/etc/networking/if-pre-up.d/iptables` OUTPUT-ahelasse logiserveri suunas lubatud syslog-ühendused

LOG

45. Kontrolli, et netfilter'i reeglistikus (fail `/etc/network/if-pre-up.d/iptables`) lubataks HESist ja HTSist saadetav syslog