IVXV kogumisteenuse haldusjuhend

Juhend

Versioon 1.8.1

16.12.2022

62 lk

Dok IVXV-JSH-1.8.1

Sisukord

PEATÜKK 1

Annotatsioon

Käesolev juhend käsitleb tööd elektroonilise hääletamise raamistiku IVXV kogumisteenuse tarkvaraga süsteemiülema vaatepunktist ning kirjeldab tarkvara kõiki võimalusi kogu e-hääletusprotsessi ulatuses. Süsteemiülemalt eeldatakse e-hääletuse põhiterminoloogia tundmist.

PEATÜKK 2

Ülevaade

2.1 Kogumisteenuse ülevaade

IVXV kogumisteenus on elektroonilise hääletuse käigus hääletajate teenindamiseks ja häälte kogumiseks mõeldud tarkvara.

Kogumisteenus koosneb mikroteenustest ja nende haldamiseks mõeldud haldusteenusest. Haldusteenuse kasutamine on käsureapõhine. Osade funktsioonide kasutamist on laiendatud veebipõhise liidesega, mida on kirjeldatud dokumendis `IVXV kogumisteenuse haldusliidese kasutusjuhend`.

Tähelepanu: Kogumisteenus paigaldatakse ja seadistatakse eraldi iga hääletuse läbiviimiseks. Ühe kogumisteenusega on korraga võimalik teenindada ainult ühte hääletust.

2.2 Lisamaterjalid

Käesolevas dokumendis kasutatakse mõisteid ja definitsioone, mis on kirjeldatud dokumendis `IVXV-ÜK-0.95 Elektroonilise hääletamise üldraamistik ja selle kasutamine Eesti riiklikel valimistel`:

- E-hääletamise etapid;
- Süsteemi osapooled ja komponendid.

2.3 Kogumisteenuse kasutajate rollid

Kogumisteenuses on kasutusel järgnevad rollid:

1. **Kogumisteenuse haldur** tegeleb kogumisteenuse tehnilise haldamisega;
2. **Valimiste haldur** tegeleb valimiste seadistuste kehtestamisega;
3. **Vaataja** pääseb ligi haldusteenuse kaudu väljastatavatele seisundi- ja statistikaandmetele;

Rollide täpsem kirjeldus asub dokumendis `Elektroonilise hääletamise infosüsteemi IVXV seadistuste koostamise juhend`.

2.4 Süsteemi komponendid

Kogumisteenus

Haldusteenus on kogumisteenuse haldamise teenus. Haldusteenuse kaudu juhitakse ja jälgitakse kogumisteenust alates paigaldusest kuni mahavõtmiseni. Vaata lähemalt lõigus *Haldusteenus*.

Logikoguja on kogumisteenuse sisemine logiserver, mis kogub ja säilitab kõigi kogumisteenuste alamteenuste logisid. Logikogujasse kogutud logid antakse valimiste lõppedes üle korraldajale.

Sisemine varundus on kogumisteenuse varundusteenus, mis varundab kõigi alamteenuste andmeid ja teeb need lihtsa liidese (failisüsteemi kataloog) kaudu kättesaadavaks välisele varundusteenusele.

Alamteenused on kogumisteenuse eri lõikude eest vastutavad teenused.

Tugiteenused

Logiseire on kogumisteenuse logide analüüsiks ja jälgimiseks mõeldud seireprogramm.

Tehniline seire on kogumisteenuse tehnilise toimimise jälgimiseks mõeldud seireprogramm.

Väline varundus on kogumisteenuse sisemisest varunduse poolt varundatud andmete säilitamiseks mõeldud väline varundusteenus.

Välised teenused

Välised teenused on läbiviidavatele valimistele kehtestatud nõuetest sõltuvad teenused, millega kogumisteenus on võimeline liidestuma. Väliste teenuste hulka kuuluvad Registreerimisteenus, Ajatempliteenus, Mobiil-ID teenus, Smart-ID teenus, OCSP teenus vms.

2.5 Ülevaade toimingutest

- Hääletamiseelsel etapil:
  - Kirjeldatakse kogumisteenuse poolt kasutatavad *välised teenused*;
  - Valmistatakse ette kogumisteenuse *tugiteenused*;
  - Koostatakse kogumisteenuse seadistused (usaldusjuur, tehnilised seadistused ja valimiste seadistused);
  - Genereeritakse teenuse toimimiseks vajalikud krüptovõtmed ja sertifikaadid;
  - Valmistatakse ette kogumisteenuse käitamiseks vajalik taristu;
  - Paigaldatakse haldusteenus;
  - Rakendatakse seadistused haldusteenusele, mille põhjal haldusteenus paigaldab ja seadistab kogumisteenuse alamteenused.
- Hääletamisetapil
  - Jälgitakse teenuse toimimist;
  - Luuakse e-valimiskastist varukoopiaid.
- Töötlusetapil
  - Eksporditakse kogumisteenusesse kogutud andmed:
    1. konsolideeritud e-valimiskast kogutud häältega.
- Lugemisetapil
  - Lugemisetapil kogumisteenust ei kasutata;

PEATÜKK 3

Haldusteenus

Haldusteenus on kogumisteenuse haldamiseks mõeldud lahendus. Haldusteenus paigaldatakse eraldiseisvasse masinasse ja selle kaudu toimub kogumisteenuse juhtimine paigaldusest kuni seiskamiseni.

Haldusteenuse funktsioonid on:

1. Kogumisteenuse alamteenuste haldamine:
    1. Seadistuste ja valimisnimekirjade laadimine;
    2. Alamteenuste paigaldus selleks ettevalmistatud masinatesse;
    3. Alamteenustele seadistuste ja nimekirjade rakendamine;
    4. Valijate nimekirjade uuenduste hankimine Valimiste Infosüsteemist;
2. E-valimiskasti koostamine töötlemiseks;
3. Valimiste üldstatistika jälgimine;
4. Valijate statistika allalaadimine;
5. E-valimiskasti ja logide korrapärane varundamine;
6. Kogumisteenuse seisundi seire;

Haldusteenus suhtleb hallatavate teenustega üle SSH[1]-kanali. Suhtluse algatab alati haldusteenus. Usaldus teenusmasinate vastu luuakse süsteemihalduri abiga pärast teenuseid majutavate masinate paigaldamist.

Teenust majutava masina paigaldamise järel loob haldur haldusteenusele ligipääsu teenusmasina juurkontole, et haldusteenusel oleks võimalik teenuse tarkvara paigaldada. Pärast viimase teenuse paigaldamist teenuseid majutavasse masinasse eemaldab haldusteenus ligipääsu juurkontole.

[1] https://en.wikipedia.org/wiki/Secure_Shell

3.1 Haldusteenuse koosseis

Haldusteenuse kasutajaliides koosneb kahest osast:

1. Haldamise põhifunktsionaalsus on teostatud *käsureautiliitide* abil;
2. Graafiline kasutajaliides on veebipõhine liides, mille funktsionaalsuse tagavad käsureautiliidid.

   Vaata ka:

   Graafilise kasutajaliidese kasutusjuhend asub dokumendis `IVXV kogumisteenuse haldusliidese kasutusjuhend`.

Lisaks töötavad deemonprotsessid:

1. Veebiserver graafilise kasutajaliidese jaoks;
2. Haldusdeemon veebiserveri poolt vahendatud päringute käivitamiseks;
3. Agentdeemon teenuste seisundi jälgimiseks.

PEATÜKK 4

Süsteemi algseadistamine

Süsteemi algseadistamine tähendab süsteemi paigaldamist ning seadistamist läbiviidavate valimiste tarbeks.

4.1 Nõuded kasutatavale platvormile

Kogumisteenus töötab platvormil `Ubuntu 20.04 LTS (Focal Fossa).`

4.2 Väliste teenuste kaardistamine

Kogumisteenuse poolt toetatavate ja läbiviidavas hääletamises kasutatavate väliste teenuste (Mobiil-ID, Smart-ID, OCSP jms) kaardistamise käigus koostatakse nimekiri välistest teenustest ja nendega andmevahetuseks vajalikest andmetest (võrguaadress, port jms).

Väliste teenuste andmed on sisendiks kogumisteenuse tehnilise seadistuse koostamisel (*Kogumisteenuse seadistuste koostamine*).

Väliste teenuste kaardistamise tulemusena on kogumisteenuse osutajal olemas nimekiri kogumisteenuse poolt kasutatavatest välistest teenustest koos teenuste kasutamiseks vajalike parameetritega.

4.3 Tugiteenuste ettevalmistamine

Kogumisteenuse tugiteenusteks on:

1. Tehnilise seire teenus;
2. Logiseire teenus;
3. Varundusteenus.

Tehnilise seire ettevalmistamine

Tähtis: Kogumisteenuse osutaja peab kogumisteenuse töötamiseks eraldatud riistvara jälgimiseks läbi viima riistvara tehnilist seiret.

Tehnilise seire teenus on Zabbix[2] tarkvaral põhinev seire- ja teavitussüsteem. Zabbix serveri paigaldab ja seadistab kogumisteenuse osutaja iseseisvalt.

Tehnilisse seiresse võib hõlmata ka kogumisteenuse tarkvaralisi komponente nagu kirjeldatud lõigus „*Klastri seisundi monitoorimine Zabbixiga*“.

Seire toimimiseks on tarvis määrata seire eest vastutavad isikud ning tagada nende vahetu teavitamine seireprogrammi poolt avastatud kõrvalekalletest.

Lisaks standardsele tehnilisele seirele (teenusmasinate protsessori-/kettakasutus jms.) viib kogumisteenuse haldusteenus läbi alamteenuste seiret ja teavitab tehnilise seire serverit avastatud kõrvalekalletest.

Tehnilise seire ettevalmistamise tulemusena on kogumisteenuse osutajal olemas tehnilise seire server, kuhu on paigaldatud seiretarkvara ning kus on kirjeldatud tehnilise seire eest vastutavad isikud ja nende teavitamise meetodid.

Logiseire ettevalmistamine

Logiseire teenus koosneb rsyslog logiserverist koos analüüsi- ja visualiseerimistarkvaraga (Log Monitor, Grafana[3]).

Logiseire ettevalmistamine ja integreerimine kogumisteenusega on kirjeldatud dokumendis `IVXV tegevuslogi seirelahendus`.

Logiseire ettevalmistamise tulemusena on kogumisteenuse osutajal olemas logiseire server, kuhu on paigaldatud logiseire tarkvara ning kus on kirjeldatud logiseire andmetele ligipääsevad isikud.

[2] http://www.zabbix.com/
[3] https://grafana.com/

Varunduse ettevalmistamine

Varundusteenus on kogumisteenuse osutaja poolt paigaldatud ja seadistatud varundusserver, mis vastutab kogumisteenuse sisemises varundusserveris koostatud varukoopiate säilimise eest.

Varunduse ettevalmistamise tulemusena on kogumisteenuse osutajal olemas varundusserver, mis on suuteline kogumisteenuse varundusliidese kaudu andmeid varundama.

4.4 Kogumisteenuse seadistuste koostamine

Kogumisteenuse seadistused koosnevad kolmest eraldiseisvast osast:

1. **Usaldusjuure seadistus** sisaldab andmed seadistuste (kaasa arvatud usaldusjuure enda) allkirjade kontrollimiseks ja nimekirja kogumisteenuse haldurite volitustest.
2. **Kogumisteenuse tehniline seadistus** määrab kogumisteenuse tehnilised parameetrid, hääletuse läbiviimiseks kasutatavad teenused, samuti ka kogumisteenuse koosseisu kuulvad alamteenused.
3. **Valimiste seadistus** määrab ühe valimise seadistuse.

Seadistuste koostamine on kirjeldatud dokumendis IVXV-JSK-* „Elektroonilise hääletamise infosüsteemi IVXV seadistuste koostamise juhend“. Kogumisteenusele rakendatavad seadistused peavad olema pakendatud ASiC-E konteinerisse ja olema signeeritud volitatud kasutaja poolt.

Kogumisteenuse seadistuste koostamise tulemusena on kogumisteenuse osutajal olemas kogumisteenuse seadistamiseks vajalikud seadistuspakid. Kõik seadistused on signeeritud isiku(te) poolt, kelle volitused on kirjeldatud usaldusjuure seadistustes või kelle volitused on määratud eraldiseisvate korralduste abil.

4.5 Kogumisteenuse taristu paigaldamine

Kogumisteenuse taristu eraldatakse teenuse osutamiseks vastavalt koostatud seadistustele (*Kogumisteenuse seadistuste koostamine*).

Igas teenusmasinas:

1. peab olema seadistatud hostinimi (fail `/etc/hostname`);
2. peab olema paigaldatud SSH teenus (tarkvarapakk `openssh-server`);
3. peab olema paigaldatud tehnilise seire teenuse agent (tarkvarapakk `zabbix-agent`);
4. peab olema tagatud õige kellaaeg (näiteks õige kellaaja teenuse `ntp` abil).

5. peab olema seadistatud nimelahendus, mis võimaldab kõikide teenusmasinate aadresse lahendada;
6. peab olema seadistatud Eesti lokaat koos UTF-8 kooditabeli toega `et_EE.UTF-8` (kas tarkvarapakk `locales` koos nimetatud lokaadi seadistamisega või tarkvarapakk `locales-all`, mis paigaldab kõik toetatud lokaadid).

Märkus: Iga teenusmasina poolt kasutatav nimelahendus peab tagama, et suhtluseks kasutatavate hostide nimed lahenduvad korrektselt.

Vältima peab olukordi, kus hostinimi lahendub mitmeks aadressiks või teistele hostidele kättesaamatuks aadressiks.

Järgnev näide kirjeldab võimalikku olukorda failis `/etc/hosts`, kus opsüsteemi paigalduse järel on hostinimi `ivxv123` määratud kahele liidesele. Sellise seadistuse puhul võib tekkida olukord, kus aadressile `ivxv123` ühendusi vastu võtma seadistatud teenus hakkab kuulama kohalikul liidesel `127.0.0.1` ja pole avaliku liidese `192.168.10.1` kaudu teistele teenustele kättesaadav.

```
# /etc/hosts
127.0.0.1     ivxv123
192.168.10.1  ivxv123
```

Kogumisteenuse taristu jaoks eraldatud hostidest tuleb koostada nimekiri, kus on kirjas hosti asukohaks olev alamvõrk, hosti nimi, IP-aadress, SSH-serveri avalik võti ja hostile plaanitud teenused.

Kogumisteenuse taristu nimekirja näide:

```
Valimiste infrastruktuuri andmed

  Alamvõrk: zone1

     IP-aadress: 172.16.238.10
     Hostinimi: admin
     SSH-serveri avalik võti:
       ecdsa-sha2-nistp256 AAAAE2VjZHNhLX...SgtbbE= root@admin

     IP-aadress: 172.16.238.41
     Hostinimi: ivxv1
     SSH-serveri avalik võti:
       ecdsa-sha2-nistp256 AAAAE2VjZHNhLX...mN8ul0= root@ivxv1

  Alamvõrk: zone2

     IP-aadress: 172.16.100.63
     Hostinimi: ivxv2
     SSH-serveri avalik võti:
       ecdsa-sha2-nistp256 AAAE2VjZHNhLXN...rtWT7A= root@ivxv2
```

Kogumisteenuse taristusse kuuluvad hostid tuleb lisada tehnilisse seiresse.

Kogumisteenuse taristu paigaldamise tulemusena on kogumisteenuse osutajal olemas dokumenteeritud platvorm kogumisteenuse paigaldamiseks ettenähtud konfiguratsiooniga. Kõik taristusse kuuluvad (virtuaal)masinad on tehnilise seire teenuse poolt kättesaadavad ja nende seisundis pole tuvastatud probleeme.

4.6 Võrgupääsude loomine

Kogumistenuse paigaldamiseks ja seadistamiseks on vajalik seadustustele vastavate võrgupääsude olemasolu.

Süsteemiülemad ja kasutajad

1. Kogumisteenuse süsteemiülemate arvutitest haldusteenusesse (protokoll SSH, port 22);
2. Haldusteenuse kasutajate arvutitest haldusteenusesse (protokoll HTTPS, port 443);
3. Kogumisteenuse süsteemiülemate arvutitest logiseire teenusesse (protokoll SSH, port 22);
4. Logiseire kasutajate arvutitest logiseire teenusesse (protokoll HTTPS, port 443).

Teenuste omavaheline suhtlus

1. Haldusteenusest kõikidesse mikroteenustesse (protokoll SSH, port 22);
2. Haldusteenusest logiseire teenusesse (protokoll SSH, port 22);
3. Kõigist mikroteenuste hostidest kõikidesse logikogumisteenustesse (protokoll RELP, port 20514);
4. Kõigist mikroteenuste hostidest kõikidesse välistesse logikogumisteenustesse (sh, ka logiseire teenusesse) (protokoll RELP, port 20514);
5. Kõigist mikroteenuste hostidest logiseire teenusesse (protokoll SSH, port 22);
6. Kõigist logikogumisteenuste hostidest logiseire teenusesse (protokoll SSH, port 22);
7. Vahendusteenusest teistesse mikroteenustesse peale talletusteenuse (protokoll TLS, port vastavalt tehnilisele seadistusele);
8. Nimekirjateenusest talletusteenustesse (protokoll TLS, port vastavalt tehnilisele seadistusele);
9. Hääletamisteenusest talletusteenustesse (protokoll TLS, port vastavalt tehnilisele seadistusele);
10. Kontrolliteenusest talletusteenustesse (protokoll TLS, port vastavalt tehnilisele seadistusele);
11. Talletusteenusest teistesse talletusteenustesse (protokoll TLS, port vastavalt tehnilisele seadistusele);

12. Mobiil-ID tugiteenusest välisesse Mobiil-ID teenusesse (protokoll HTTP(S), port vastavalt tehnilisele seadistusele);
13. Smart-ID tugiteenusest välisesse Smart-ID teenusesse (protokoll HTTP(S), port vastavalt tehnilisele seadistusele);
14. Hääletamisteenusest välisesse kvalifitseerimisteenusesse (protokoll HTTP(S), port vastavalt tehnilisele seadistusele);
15. Varundusteenusest haldusteenusesse (protokoll SSH, port 22);
16. Varundusteenusest logikogumisteenustesse (protokoll SSH, port 22);
17. Varundusteenusest talletusteenustesse (protokoll SSH, port 22);

Hääletaja

1. Hääletaja kasutatavast seadmest vahendusteenusesse (protokoll TLS, port vastavalt tehnilisele seadistusele, eeldatavalt 443).

4.7 Haldusteenuse paigaldamine

Haldusteenuse paigaldamine toimub haldusteenuse hostil.

Haldusteenuse paigaldamiseks tuleb kopeerida **kõik** kogumisteenuse tarkvarapakid haldusteenuse masina kataloogi `/etc/ivxv/debs/`. Nendest pakkidest paigaldatakse haldusteenus, samuti kasutab haldusteenus neid pakke alamteenuste paigaldamiseks.

Haldusteenuse sõltuvuste paigaldamine:

```
root@admin # apt-get install --yes --quiet adduser openssh-server␣
↪openssl rsync rsyslog rsyslog-relp sudo tzdata locales libc6␣
↪python3-bottle python3-dateutil python3-debian python3-docopt␣
↪python3-fasteners python3-jinja2 python3-jsonschema python3-
↪openssl python3-pkg-resources python3-yaml python3:any apache2␣
↪cron fonts-font-awesome javascript-common language-pack-et␣
↪libapache2-mod-wsgi-py3 libjs-bootstrap libjs-jquery libjs-jquery-
↪datatables libjs-jquery-datatables-extensions python3-gdbm␣
↪python3-requests ssl-cert
Reading package lists...
Building dependency tree...
Reading state information...
adduser is already the newest version (3.118ubuntu2).
cron is already the newest version (3.0pl1-136ubuntu1).
fonts-font-awesome is already the newest version (5.0.10+really4.7.
↪0~dfsg-1).
javascript-common is already the newest version (11).
libapache2-mod-wsgi-py3 is already the newest version (4.6.8-
↪1ubuntu3).
libjs-jquery is already the newest version (3.3.1~dfsg-3).
```

(jätkub järgmisel leheküljel)

(jätk eelmisele leheküljele)

```
libjs-jquery on määratud käsitsi paigaldatuks.
...
Paki apache2-data (2.4.41-4ubuntu3.8) paikasättimine ...
Paki openssl (1.1.1f-1ubuntu2.10) paikasättimine ...
Paki rsync (3.1.3-8ubuntu0.1) paikasättimine ...
invoke-rc.d: WARNING: No init system and policy-rc.d missing!␣
↪Defaulting to block.
Paki apache2-utils (2.4.41-4ubuntu3.8) paikasättimine ...
Paki apache2 (2.4.41-4ubuntu3.8) paikasättimine ...
invoke-rc.d: WARNING: No init system and policy-rc.d missing!␣
↪Defaulting to block.
invoke-rc.d: WARNING: No init system and policy-rc.d missing!␣
↪Defaulting to block.
Processing triggers for systemd (245.4-4ubuntu3.13) ...
```

Haldusteenuse paigaldamine:

```
root@admin # dpkg -i /etc/ivxv/debs/ivxv-common_1.7.8_all.deb /etc/
↪ivxv/debs/ivxv-admin_1.7.8_amd64.deb
Selecting previously unselected package ivxv-common.
(Andmebaasi lugemine ... 13710 files and directories currently␣
↪installed.)
Preparing to unpack .../debs/ivxv-common_1.7.8_all.deb ...
Unpacking ivxv-common (1.7.8) ...
Selecting previously unselected package ivxv-admin.
Preparing to unpack .../ivxv-admin_1.7.8_amd64.deb ...
Unpacking ivxv-admin (1.7.8) ...
Paki ivxv-common (1.7.8) paikasättimine ...
# Adding user group 'ivxv'
Adding group `ivxv' (GID 109) ...
...
  systemctl restart apache2
# Starting Apache web server
# Restarting rsyslog log server
Created symlink /etc/systemd/system/multi-user.target.wants/ivxv-
↪admin.service → /lib/systemd/system/ivxv-admin.service.
Created symlink /etc/systemd/system/multi-user.target.wants/ivxv-
↪admin-agent.service → /lib/systemd/system/ivxv-admin-agent.
↪service.
/usr/lib/python3/dist-packages/schematics/validate.py:121:␣
↪SyntaxWarning: "is" with a literal. Did you mean "=="?
  if not kwargs or kwargs.pop('context', 0) is 0:
Processing triggers for rsyslog (8.2001.0-1ubuntu1.1) ...
invoke-rc.d: WARNING: No init system and policy-rc.d missing!␣
↪Defaulting to block.
```

Tähtis: Haldusteenuse edasine kasutamine toimub haldusteenuse konto alt. Selleks tuleb halduril luua SSH-ligipääs haldusteenuse kontole `ivxv-admin`. Soovitav on au-

tentimine teha ID-kaardi põhiseks (vaata *SSH kasutajate autentimine ID-kaardi abil*).

Haldusteenuse paigaldamise tulemusena on kogumisteenuse osutajal teenuse haldamiseks vajalik liides.

Haldusteenuse seadistamine

Osad haldusteenuse protsessid käivitatakse korrapärase intervalliga cron teenuse abil. Nende protsesside puhul väljastatakse võimalik tõrkeinfo standardväljunditesse ja cron edastab selle e-posti teel käivitaja konto aadressile. Seetõttu tuleb haldusteenuse masinasse paigaldada meiliserver ja seadistada see nii, et kõigile masinas asuvatele kontodele (nt. `root@localhost`) saadetavad sõnumid edastatakse teenuse halduritele.

Kogumisteenuse taristu hõlmamine haldusesse

Haldusteenus kasutab kogumisteenuse haldamiseks SSH protokolli. Selleks, et haldusteenusel oleks võimalik teisi teenushoste usaldada, tuleb haldusteenusesse lisada hallatavate teenushostide SSH-serveri võtmed.

Näide hosti `ivxv1` SSH-võtmete lisamisest haldusteenuse usaldatavate hostide hulka:

```
ivxv-admin@admin $ ssh-keyscan ivxv1 >> ~/.ssh/known_hosts
# ivxv1:22 SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.2
# ivxv1:22 SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.2
# ivxv1:22 SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.2
```

Selleks, et haldusteenusel oleks võimalik teenushostidesse tarkvara paigaldada, tuleb haldusteenuse kontole `ivxv-admin` luua SSH-ligipääs teenushostide juurkasutaja kontole.

Märkus: Haldusteenus vajab juurkasutaja ligipääsu alamteenuse tarkvara paigaldamiseks. Pärast edukat paigaldamist ühel hostil eemaldab haldusteenus ligipääsu selle hosti juurkasutaja kontole.

Haldusteenuse konto SSH-võtmepaari avalik võti asub kasutaja `ivxv-admin` kodukataloogi all failis `.ssh/id_ed25519.pub` ja see on genereeritud haldusteenuse paigaldamise käigus. Vajadusel võib haldur selle võtme asendada (kuid see peab toimuma enne, kui võti on üle kantud hallatavatesse teenusmasinatesse).

Teenusmasinas tuleb haldusteenuse konto SSH avalik võti panna faili `/root/.ssh/authorized_keys`. See fail peab kuuluma juurkasutajale ja olema loetav ainult juurkasutaja poolt (faili pääsuõigused `0600`).

Kogumisteenuse taristu haldusesse hõlmamise tulemusena on haldusteenusel usal-

dusväärne ligipääs kogumisteenuse taristusse kuuluvatele teenusmasinate juurkasutaja kontodele.

Logiseire lahenduse ühendamine haldusteenusega

Logiseire lahenduse kasutamise korral peab haldusteenusel olema ligipääs logiseire lahendusele, et sealt kogutud statistikat alla laadida ja vajadusel värskendada logiseire poolt analüüsitavaid logisid.

Selleks, et haldusteenusel oleks usaldus logiseire teenuse vastu, tuleb haldusteenusesse lisada logiseire teenuse hosti (käesolevas näites nimega `logmonitor`) SSH-serveri võtmed:

```
ivxv-admin@admin $ ssh-keyscan -t ecdsa logmonitor >> ~/.ssh/known_
↪hosts
```

Selleks, et haldusteenus pääseks logiseire kontole ligi, tuleb haldusteenuse konto SSH avalik võti panna logiseire konto `logmon` volitatud võtmete faili `~logmon/.ssh/authorized_keys`. See fail peab kuuluma logimonitori kasutajale ja olema loetav ainult selle kasutaja poolt (faili pääsuõigused `0600`).

Logiseire lahenduse haldusteenusega ühendamise tulemusena on tegevuslogi seirelahendus haldusteenusele kättesaadav ning haldusteenusel on võimalik seirelahendusest statistikaandmeid laadida ning seirelahenduse andmehoidlasse ajakohaseid logiandmeid üle kanda.

Haldusteenuse veebiliidese vaikimisi TLS-sertifikaadi asendamine

Haldusteenuse paigalduse käigus genereeritakse kasutajaliidese veebiserveri TLS-sertifikaat koos krüptovõtmega ja tugeva Diffie-Hellman grupifailiga (vaata https://weakdh.org/). Vajadusel on halduril võimalik need asendada.

Failide asukohad:

- Veebiserveri TLS-sertifikaadi võti: `/etc/ssl/private/ivxv-admin-default.key`
- Veebiserveri TLS-sertifikaat: `/etc/ssl/certs/ivxv-admin-default.crt`
- Diffie-Hellmani grupifail: `/etc/ssl/dhparams.pem`

Asendatud failide rakendamiseks tuleb veebiserver taaskäivitada käsuga **`service apache2 restart`** ja veenduda, et veebiliides töötab.

Haldusteenuse veebiliidese vaikimisi TLS-sertifikaadi asendamise tulemusena kasutab haldusteenuse veebiliides turvalist sertifikaati.

Haldusteenuse vaikimisi autentimissertifikaadi asendamine

Haldusteenuse paigalduse käigus genereeritakse haldusteenuse autentimissertifikaat koos krüptovõtmega (haldusteenus kasutab seda Valimiste Infosüsteemiga infovahetusel autentimiseks). Vajadusel on halduril võimalik need asendada.

Failide asukohad:

- Autentimissertifikaadi võti: `/etc/ssl/private/ivxv-admin-client.key`
- Autentimissertifikaat: `/etc/ssl/certs/ivxv-admin-client.crt`

Haldusteenuse vaikimisi autentimissertifikaadi asendamise tulemusena kasutab haldusteenus Valimiste Infosüsteemi autentimiseks turvalist sertifikaati.

Autentimissertifikaadi testimine:

```
$ openssl s_client -connect vis-address:443 \
  -cert /etc/ssl/certs/ivxv-admin-client.crt \
  -key /etc/ssl/private/ivxv-admin-client.key
```

4.8 Haldusteenuse lähtestamine

Haldusteenuse lähtestamine toimub käsuga *ivxv-collector-init*. Selle käigus puhastatakse haldusteenuse andmekataloogid ja lähtestatakse andmebaas.

4.9 Seadistuste ja valimisnimekirjade rakendamine kogumisteenusele

---

Märkus: Käesolevas lõigus ja alamlõikudes tähendab „seadistuspakk“ nii seadistusi sisaldavat faili kui valimisnimekirja faili, mis on signeeritud volitatud isiku poolt.

Kogumisteenusele tuleb rakendada järgmised seadistuspakid:

1. Usaldusjuur – laaditakse alati esimesena;
2. Kogumisteenuse tehniline seadistus – laaditakse enne valimiste seadistust;
3. Valimiste seadistus – laaditakse enne nimekirju;
4. Valikute nimekiri;
5. Ringkondade nimekiri;
6. Valijate algnimekiri.

Ettevalmistatud seadistuspakkide rakendamiseks tuleb läbi viia järgmised tegevused:

1. Ülekandmine haldusteenuse masinasse;

2. Laadimine haldusteenusesse;
3. Rakendamine alamteenustele.

Vihje: Seadistuspakkide ettevalmistamine on kirjeldatud lõigus „*Kogumisteenuse seadistuste koostamine*“.

Tähelepanu: Usaldusjuure seadistuse laadimisega kaasneb alati ka kogumisteenuse haldusteenuse andmebaasi lähtestamine!

Seadistuste ja valimisnimekirjade kogumisteenusele rakendamise tulemusena on kogumisteenus seadistatud ettenähtud perioodil osutama nõuetekohast häälte kogumise teenust.

Seadistuspaki ülekandmine haldusteenuse masinasse

Seadistuspaki ülekandmine haldusteenuse masinasse toimub üle SCP[4] protokolli. Seadistuspakk peab olema kättesaadav haldusteenuse kasutajakontole `ivxv-admin`.

Näide:

```
$ scp seadistus.asice ivxv-admin@admin:
seadistus.asice               100%   15KB  79.5KB/s   00:00
```

Märkus: Kogumisteenus osutaja võib seadistuspakkide ülekandmiseks kasutada ka muid meetodeid, näiteks irdmeediat.

Seadistuspaki ülekandmise tulemusena on seadistuspakk haldusteenuse poolt ligipääsetaval andmekandjal.

Seadistuspaki laadimine haldusteenusesse

Seadistuspakk laaditakse haldusteenusesse käsuga *ivxv-cmd-load*. Selle käigus kontrollib haldusteenus seadistuspaki signeerinud isiku volitusi ja valideerib seadistuste sisu ning kooskõlalisust. Laadimise tulemusena on seadistuspakk valmis rakendamiseks hallatavatele teenustele.

Näide: Usaldusjuure laadimine haldusteenusesse:

[4] https://en.wikipedia.org/wiki/Secure_copy

```
ivxv-admin@admin $ ivxv-cmd-load trust /output/voting/HA-SETUP/
↪config/HA-SETUP.trust.asice
command_file:INFO: Loading command file '/output/voting/HA-SETUP/
↪config/HA-SETUP.trust.asice' (trust root configuration)
command_file:INFO: Validating trust root configuration
command_file:INFO: Files in trust root configuration package are␣
↪valid
INFO: Config file is signed by: ORAV,IVAN,30809010001 2021-12-
↪28T11:38:37Z
INFO: User ORAV,IVAN,30809010001 with role 'admin' is authorized to␣
↪execute 'trust' commands
INFO: Using signature 'ORAV,IVAN,30809010001 2021-12-28T11:38:37Z'␣
↪as config file version
INFO: Config file version is 'ORAV,IVAN,30809010001 2021-12-
↪28T11:38:37Z'
INFO: Loading command 'trust root configuration' from file '/output/
↪voting/HA-SETUP/config/HA-SETUP.trust.asice'
command_file:INFO: Loading command file '/output/voting/HA-SETUP/
↪config/HA-SETUP.trust.asice' (trust root configuration)
command_file:INFO: Validating trust root configuration
command_file:INFO: Files in trust root configuration package are␣
↪valid
INFO: Resetting collector management database
db:INFO: Initializing management database '/var/lib/ivxv/db/ivxv-
↪management.db'
Removing crontab (if exist)
no crontab for ivxv-admin
INFO: Trust root configuration file loaded successfully
INFO: Resetting user permissions
INFO: Trust root configuration file is registered in management␣
↪service
```

Seadistuspaki haldusteenusesse laadimise tulemusena on haldusteenus valmis rakendama seadistuspakki alamteenustele. Seadistuspaki versiooni kuvatakse haldusteenuse olekuandmetes.

Vaata ka:

- *Korralduste valideerimine*

Seadistuste rakendamine alamteenustele

Haldusteenusesse laaditud seadistuspakid rakendatakse hallatavatele teenustele käsuga *ivxv-config-apply*. Rakendamine on võimalik tehniliste seadistuse laadimise järel, kuna tehnilise seadistusega tekivad haldusteenusesse andmed hallatavate teenuste kohta.

Seadistuste rakendamise käigus haldusteenus:

- Paigaldab seadistatava teenuse tarkvara (tehnilise seadistuse laadimisel, kui po-

le eelnevalt paigaldatud);

- Kannab seadistuspaki üle hallatava teenuse hosti failisüsteemi;
- Valimiste seadistuse laadimisel lubab ja käivitab seadistatava teenuse.

Märkus: Seadistuste rakendamise järjekord on kirjeldatud utiliidi ivxv-config-apply abiteabe lõigus (vaata *ivxv-config-apply*).

Näide: Haldusteenusesse laaditud seadistuste rakendamine hallatavatele teenusele:

```
ivxv-admin@admin $ ivxv-config-apply
INFO: Technical config is signed by ÕIGE,VALIK,44444444444 2017-06-
↪07T12:05:44Z
INFO: Service choices@choices1.ivxv.ee: Applying technical config
SERVICE choices@choices1.ivxv.ee: Installing service to host "ivxv1"
SERVICE choices@choices1.ivxv.ee: Querying state of the service␣
↪software package "ivxv-choices"
SERVICE choices@choices1.ivxv.ee: Copying software package files to␣
↪service host
SERVICE choices@choices1.ivxv.ee: Checking state of dpkg database␣
↪in service host
SERVICE choices@choices1.ivxv.ee: Installing dependencies for␣
↪package "ivxv-common"
Reading package lists...
Building dependency tree...
Reading state information...
...
SERVICE voting@voting3.ivxv.ee: Set trust config file permissions␣
↪in service host
SERVICE voting@voting3.ivxv.ee: Trust root config successfully␣
↪applied to service
SERVICE voting@voting3.ivxv.ee: Applying technical config to service
SERVICE voting@voting3.ivxv.ee: Copying technical config to service␣
↪host
SERVICE voting@voting3.ivxv.ee: Set technical config file␣
↪permissions in service host
SERVICE voting@voting3.ivxv.ee: Technical config successfully␣
↪applied to service
SERVICE voting@voting3.ivxv.ee: Registering technical config␣
↪version "ÕIGE,VALIK,44444444444 2017-06-07T12:05:44Z" in␣
↪management database
SERVICE voting@voting3.ivxv.ee: Registering service state as
↪"INSTALLED" in management database
INFO: Service voting@voting3.ivxv.ee: technical config config␣
↪applied successfully
INFO: 15 configuration packages successfully applied
```

Seadistuste alamteenustele rakendamise tulemusena on hallatavad teenused seadistatud ja nende seisund on haldusteenusest jälgitav.

Vaata ka:

- *Korralduste laadimine ja rakendamine*

Kogumisteenuse krüptovõtmete rakendamine

Teenuste krüptovõtmete ja TLS-sertifikaatide rakendamine toimub käsuga *ivxv-secret-load*.

Vihje: Teenuse krüptovõtmete seisundit on võimalik väljastada käsuga **`ivxv-status --service=<service-id>`** (vaata *ivxv-status*)

Võtme laadimine teenusele:

```
$ ivxv-secret-load --service=<teenuse-id> tls-key tls.key
```

Sertifikaadi laadimine teenusele:

```
$ ivxv-secret-load --service=<teenuse-id> tls-cert tls.pem
```

Tähtis: Igale teenuse isendile tuleb rakendada selle isendi jaoks genereeritud võti ja sertifikaat!

Hääletamisteenuse ajatemplipäringute signeerimisvõtme rakendamine toimub käsuga *ivxv-secret-load*:

```
$ ivxv-secret-load tsp-regkey tspreg.key
```

Märkus: Hääletamisteenuse ajatemplipäringute signeerimisvõti on vaja rakendada vaid juhul, kui ajatempliteenust kasutatakse registreerimisteenuseks (valimiste seadistuses on `qualification/protocol` välja väärtuseks `tspreg`).

Mobiil-ID/Smart-ID identsustõendi võtme rakendamine toimub käsuga *ivxv-secret-load*:

```
$ ivxv-secret-load mid-token-key mobid-shared-secret.key
```

Märkus: Mobiil-ID/Smart-ID identsustõendi võti on vaja rakendada vaid juhul, kui Mobiil-ID/Smart-ID tugiteenus on kasutusel (valimiste seadistuses on olemas plokk `auth.ticket`).

Kogumisteenuse krüptovõtmete rakendamise tulemusena on hallatavate teenuste suhtluskanalid varustatud kanali turvamiseks vajalike krüptovõtmetega, samuti on tee-

nustel olemas krüptovõtmed muude oluliste operatsioonide jaoks.

4.10 Algseadistamise tulemuse kontrollimine

Algseadistamise tegevuste tulemusena on kogumisteenus eeldatavalt valmis hääletuse läbiviimiseks. Tulemust on võimalik kontrollida kogumisteenuse oleku jälgimisega, mis on kirjeldatud süsteemi haldustoimingute lõigus (*Kogumisteenuse oleku jälgimine*).

Hääletuse läbiviimiseks seadistatud kogumisteenuse olek on „Seadistatud“ (CONFIGURED). Oleku „Paigaldatud“ puhul tuleb kontrollida mikroteenuste seisundit ja seisundi taustainfot.

PEATÜKK 5

Süsteemi haldustoimingud

5.1 Kogumisteenuse oleku jälgimine

Kogumisteenuse olekuandmed registreeritakse haldusteenuse andmebaasis. Oleku kuvamiseks on utiliit *ivxv-status*.

Olekus kuvatakse järgmisi andmeid:

- Valimise ID, faas, algus- ja lõpuaeg;
- Haldusteenusesse laaditud konfiguratsioon:
  - Seadistuspakkide versioonid;
  - Valikute nimekirja ja ringkondade nimekirja versioonid;
  - Valijate nimekirjade versioonid ja olekud;
- Teenuste nimekiri koos rakendatud seadistuste versioonidega, teenuse seisundi ja selle viimase tuvastamise ajaga;
- Väliste teenuste seisundid;
- Haldusteenuse andmehoidla statistika.

Sõltuvalt kogumisteenuse seisundist võib oleku kuvamise utiliit jätta mõned andmeblokid kuvamata (kui need pole jooksva seisundi puhul olulised). Täieliku andmestiku väljastamiseks vaata utiliidi *ivxv-status* abiteavet.

Mikroteenuste oleku jälgimise ning oleku ja võimaliku veainfo registreerimisega haldusteenuse andmebaasis tegeleb haldusteenuse *agentdeemon*.

Valijate muudatusnimekirjade hankimine Valimiste Infosüsteemist toimub utiliidiga *ivxv-voter-list-download*, mis käivitatakse teenuse *cron* poolt veerandtunnise intervalliga.

Kogumisteenuse haldusteenuse sündmuste logi kuvamiseks on utiliit *ivxv-eventlog-dump*.

Tähtis: Haldusteenus tagab kogumisteenuse alamteenuste olekuandmetes vajaliku teabe teenuse töökorda seadmiseks. See võib olla järgmine:

1. Teave puuduvate seadistuste kohta (seadistusfailid, võtmed jms). Seda kuvatakse kuni teenus on varustatud kõigi käivitamiseks vajalike seadistustega.
2. Veateade - alamteenuse haldusvahendite (seadistuste kontrollivahend, teenuse haldusvahend) veaväljund mittetöötava teenuse kohta.

5.2 Korralduste valideerimine

Korraldusfailide valideerimine võimaldab veenduda korralduste vastavuses vormistusnõuetele ning tuvastada vigased või mittekooskõlalised korraldused.

Valideerimine toimub käsuga *ivxv-config-validate*.

Valimise seadistuse valideerimise näide:

```
$ ivxv-config-validate --election=valimise-seadistus-TEST2017.asice
```

Korralduste kooskõlalisuse valideerimine

Kooskõla valideerimine viiakse läbi kahel juhul:

1. Kui valideerimise käsule antakse korraga valideerimiseks mitu korraldust;
2. Korralduse laadimisel juhul, kui laaditava korraldusega kooskõla nõudev oluline korraldus juba haldusteenusesse laaditud.

Korralduste kooskõla valideerimise kontrollid:

1. Korraga valimiste seadistust ja/või nimekirju (valikute, ringkondade või valijate) valideerides kontrollitakse valimiste identifikaatori kooskõla.
2. Korraga mitut valijate nimekirja valideerides viiakse läbi järgnevad kontrollid:
   - Nimekirjade korrektne järjestus;
   - Muudatusnimekirjas kontrollitakse:
     1. Valija topeltlisamist ja -eemaldamist;
     2. Valija eemaldamist pärast tema lisamist sama muudatusnimekirjaga.
     3. Valija eemaldamist ringkonnast, kuhu teda pole lisatud;
3. Korraga ringkondade ja valikute nimekirja valideerides viiakse läbi järgnevad kontrollid:
   - Igas valimisringkonnas peab olema kirjeldatud vähemalt üks valik;

    - Iga valik peab olema seotud olemasoleva valimisringkonnaga.
4. Korraga ringkondade nimekirja ja valijate nimekirju valideerides viiakse läbi järgnevad kontrollid:
    - Igas valimisjaoskonnas peab olema vähemalt üks valija;
    - Iga valimisnimekirja kantud isik peab olema seotud olemasoleva ringkonnaga;
5. Valijate nimekirja(de) ja ringkondade nimekirja valideerimisel kontrollitakse valijale määratud ringkonna olemasolu ringkondade nimekirjas.

Kui valimiste seadistuses on määratud välisriigis asuvale valijale määratav ringkonna haldusüksuse EHAK-kood (parameeter `voterforeignehak`), peab valikute, valijate ja ringkondade nimekirjade vastavuse valideerimisel olema kaasatud ka valimiste seadistus ja seadistuste valideerimisel tehakse täiendavad kontrollid:

1. Valijate nimekirja ja ringkondade nimekirja kooskõla valideerides kontrollitakse, et ringkondade nimekirjas on parameetriga määratud haldusüksuses olemas valijale määratud ringkond.

5.3 Korralduste laadimine ja rakendamine

Kogumisteenuse korraldused koostatakse signeeritud korralduspakkidena, millega kirjeldatakse kasutaja identifikaator (*Common Name* ehk CN väli ID-kaardilt) ja rollide nimekiri.

Sõltuvalt korraldusest tuleb rakendamiseks kasutada ühte või kahte käsku. Haldusteenust puudutavad korralduste rakendamiseks piisab nende laadimisest haldusteenusesse. Alamteenuseid puudutavad korraldused (näiteks seadistuspakid) tuleb pärast haldusteenusesse laadimist rakendada ka hallatavatele teenustele.

Korralduste laadimine haldusteenusesse toimub käsuga *ivxv-cmd-load*. Laadimise käigus viiakse läbi ka *korralduse valideerimine*, vigane või mittekooskõlaline korraldus jäetakse laadimata.

Valikute nimekirja korralduse rakendamise näide:

```
ivxv-admin@admin $ ivxv-cmd-load choices /output/voting/HA-SETUP/
↪config/choices.asice
INFO: Config file is signed by: NÕID,VÄIKE,33333333333 2021-12-
↪28T11:49:03Z
INFO: User NÕID,VÄIKE,33333333333 with role 'election-conf-manager'␣
↪is authorized to execute 'choices' commands
INFO: Using signature 'NÕID,VÄIKE,33333333333 2021-12-28T11:49:03Z'␣
↪as config file version
INFO: Config file version is 'NÕID,VÄIKE,33333333333 2021-12-
↪28T11:49:03Z'
INFO: Loading command 'choices list' from file '/output/voting/HA-
↪SETUP/config/choices.asice'
command_file:INFO: Loading command file '/output/voting/HA-SETUP/
↪config/choices.asice' (choices list)
```

(jätkub järgmisel leheküljel)

(jätk eelmisele leheküljele)

```
command_file:INFO: Validating choices list
command_file:INFO: Files in choices list package are valid
INFO: Choices list file loaded successfully
INFO: Choices list file is registered in management service
```

Vaata ka:

- Käsu *ivxv-cmd-load* abiteave;
- Korralduste rollide kirjeldus ja korralduste koostamise juhend asuvad dokumendis `IVXV seadistuste koostamise juhend`.

5.4 Teenuse isendi seisundi tuvastamine

Mikroteenuse isendi seisundi tuvastamiseks on utiliit *ivxv-service*, millega on võimalik teenuse seisundit vahetult küsida (utiliit *ivxv-status* kuvab andmebaasis puhverdatavat seisundit).

Teenuse seisundi päringu näide:

```
ivxv-admin@admin $ ivxv-service ping voting@voting2.ivxv.ee
INFO: Pinging service voting@voting2.ivxv.ee
SERVICE voting@voting2.ivxv.ee: Registering background info: Ping␣
↪error: * ivxv-voting@voting@voting2.ivxv.ee.service - IVXV voting␣
↪service
SERVICE voting@voting2.ivxv.ee: ERROR: Pinging service failed
ERROR: Failed to query service voting@voting2.ivxv.ee status
```

5.5 Teenuse (taas)käivitamine

Mikroteenuste käivitamiseks ja taaskäivitamiseks on utiliit *ivxv-service*.

Teenuse taaskäivitamise näide:

```
ivxv-admin@admin $ ivxv-service restart voting@voting2.ivxv.ee
INFO: Restarting service voting@voting2.ivxv.ee
SERVICE voting@voting2.ivxv.ee: Restarting service
SERVICE voting@voting2.ivxv.ee: Registering service state as
↪'CONFIGURED' in management database (last state: 'FAILURE')
SERVICE voting@voting2.ivxv.ee: Service restarted successfully
INFO: Service voting@voting2.ivxv.ee restarted
```

Märkus: Protseduuri nimetamine käivitamiseks või taaskäivitamiseks sõltub teenuse protsessi seisundist. Tehniliselt on tegemist sarnaste protseduuridega, kus esmalt

veendutakse, et teenus seisab (vajadusel jäetakse see seisma) ja siis püütakse käivitatada hetkel kehtivate seadistustega.

5.6 Teenuse seiskamine

Mikroteenuste seiskamiseks on utiliit *ivxv-service*.

Teenuse seiskamise näide:

```
ivxv-admin@admin $ ivxv-service stop voting@voting2.ivxv.ee
INFO: Stopping service voting@voting2.ivxv.ee
SERVICE voting@voting2.ivxv.ee: Stopping service
SERVICE voting@voting2.ivxv.ee: Service stopped successfully
INFO: Service voting@voting2.ivxv.ee stopped
```

5.7 Teenuse isendi asendamine

Teenuse isendi asendamine koosneb ühe mikroteenuse isendi eemaldamisest (vt. *Teenuse isendi eemaldamine*) ja teise sama funktsiooniga mikroteenuse isendi lisamisest (vt. *Teenuse isendi lisamine*).

5.8 Teenuse isendi lisamine

Teenuse isendi lisamiseks tuleb vajadusel teenust hostiv server ette valmistada (vt. *Kogumisteenuse taristu paigaldamine*) ning rakendada uus tehniline seadistus, mis sisaldab lisatavat teenuse isendit.

Tähtis: Lisatava isendi identifikaator ei tohi kattuda ühegi teise, ka minevikus eemaldatud isendi identifikaatoriga.

5.9 Teenuse isendi eemaldamine

Teenuse isendi eemaldamiseks tuleb:

1. Teenuse isend seisma jätta (vt. *Teenuse seiskamine*);
2. Keelata teenuse isendi uuesti käivitamine (vt. allpool);
3. Rakendada uus tehniline seadistus, mis eemaldatavat isendit enam ei sisalda.

Tähtis: Teenuse isendi eemaldamisel kogumisteenuse koosseisust on oluline eemaldatava isendi täielik elimineerimine.

Teenuste isendid kasutavad üksteisele usalduse tõestamiseks kindla sertifitseerimiskeskuse (CA) poolt välja antud sertifikaate, kuid ei kasuta sama meetodit eemaldatud isendi usalduse tühistamiseks (vastava protseduuri rakendamise liigse keerukuse tõttu).

Seetõttu on oluline veenduda, et kogumisteenusest eemaldatud teenuse isend on enne uue seadistuse rakendamist täielikult süsteemist eemaldatud. Vastasel juhul tekib oht, et eemaldatav isend jätkab tegutsemist ja häirib kogumisteenuse tööd.

Teenuse isendi käivitamise keelamiseks teenuse eemaldamisel tuleb eemaldada vastava teenuse tarkvarapakk teenuse hostist:

- Nimekirjateenuse paki eemaldamine:

```
$ apt purge ivxv-choices
```

- Mobiil-ID tugiteenuse paki eemaldamine:

```
$ apt purge ivxv-mid
```

- Smart-ID tugiteenuse paki eemaldamine:

```
$ apt purge ivxv-smartid
```

- Vahendusteenuse paki eemaldamine:

```
$ apt purge haproxy
```

- Talletusteenuse paki eemaldamine:

```
$ apt purge etcd-server
```

- Kontrolliteenuse paki eemaldamine:

```
$ apt purge ivxv-verification
```

- Hääletamisteenuse paki eemaldamine:

```
$ apt purge ivxv-voting
```

5.10 Kasutajate haldus

Kasutajate algsed kirjeldused määratakse usaldusjuure seadistuses, hilisem haldus toimub vastavate korralduste abil.

Kasutajate halduse korraldused rakendatakse käsuga *ivxv-cmd-load* (vaata *Korralduste laadimine ja rakendamine*).

Kasutajaõiguste määramise korralduse rakendamise näide:

```
ivxv-admin@admin $ ivxv-cmd-load user /output/voting/HA-SETUP/
↪config/user-NÕID,VÄIKE,33333333333-election-conf-manager.asice
INFO: Config file is signed by: ORAV,IVAN,30809010001 2021-12-
↪28T11:46:31Z
INFO: User ORAV,IVAN,30809010001 with role 'admin' is authorized to␣
↪execute 'user' commands
INFO: Using signature 'ORAV,IVAN,30809010001 2021-12-28T11:46:31Z'␣
↪as config file version
INFO: Config file version is 'ORAV,IVAN,30809010001 2021-12-
↪28T11:46:31Z'
INFO: Loading command 'user permissions configuration' from file '/
↪output/voting/HA-SETUP/config/user-NÕID,VÄIKE,33333333333-
↪election-conf-manager.asice'
command_file:INFO: Loading command file '/output/voting/HA-SETUP/
↪config/user-NÕID,VÄIKE,33333333333-election-conf-manager.asice'␣
↪(user permissions configuration)
command_file:INFO: Validating user permissions configuration
command_file:INFO: Files in user permissions configuration package␣
↪are valid
INFO: User permissions configuration file loaded successfully
INFO: Resetting user 'NÕID,VÄIKE,33333333333' permissions
```

Tähelepanu: Juba lisatud kasutajate eemaldamine süsteemist pole võimalik. Kasutaja eemaldamise asemel tuleb kasutaja rolliks määrata „õigusteta kasutaja“.

Vaata ka:

- Kasutajate rollide kirjeldus ja volituste korralduste koostamise juhend asuvad dokumendis `IVXV seadistuste koostamise juhend`.
- Korralduste rakendamine on kirjeldatud lõigus *Korralduste laadimine ja rakendamine*.

5.11 Tarkvarauuenduste rakendamine

Tarkvarauuendused jagunevad kogumisteenuse vaatepunktist kaheks: operatsioonisüsteemi uuendused ja kogumisteenuse uuendused.

Operatsioonisüsteemi tarkvarapakkide uute versioonide paigaldamine pole kogumisteenuse dokumentatsioonis käsitletud. Süsteemiülem peab tagama ajakohaste turvauuenduste rakendamise kogumisteenuses kasutatavate operatsioonisüsteemidele;

Kogumisteenuse tarkvarapakkide uute versioonide paigaldamine toimub järgnevalt:

1. Uuenenud tarkvarapakid kopeeritakse haldusteenuse kataloogi `/etc/ivxv/debs` (soovitavalt juurkasutaja õigustes);
2. Haldusteenuse tarkvara uuendatakse juurkasutaja õigustes käsuga **`dpkg -i /etc/ivxv/debs/ivxv-common_1.0_all.deb /etv/ivxv/debs/ivxv-admin_1.0_amd64.deb`** (tegelik versiooninumber erineb käesolevas näites kasutatud versioonist);
3. Hallatavate teenuste tarkvara uuendamine toimub haldusteenuse kasutaja `ivxv-admin` õigustes käsuga *ivxv-update-packages*.

5.12 Varundamine

Varundamine hõlmab kolme liiki andmeid:

1. Haldusteenuse seadistused;
2. Kogumisteenuse e-valimiskast;
3. Kogutud logid.

Varukoopia loomine toimub haldusteenuse masinas utiliidi *ivxv-backup* abil, varukoopiad talletatakse varundusserveri kataloogis `/var/backups/ivxv`.

Haldusteenus seadistuste varundamine

Haldusteenuse seadistustest varundatakse järgmised andmed:

1. `etc/` - haldusteenusesse laadiditud tarkvarapakid ja hetkel kehtivad seadistusfailid;
2. `admin-ui-permissions/` - haldusteenuse kasutajaliidese pääsuõigused;
3. `commands/` - kõik haldusteenusese laaditud korraldusfailid.

Haldusteenuse varundamist viiakse läbi haldusteenuses, varundatavad andmed kopeeritakse varundusserverisse.

Vihje: Haldusteenuse andmete tõhusamaks varundamiseks ja taasteks on soovitav kasutada haldusteenuse virtuaalmasina dünaamilist tõmmist (*snapshot dump*).

Haldusteenuse seadistuste varukoopiast taastamise protseduuri pole kogumisteenuses ette nähtud.

Haldusteenuse seadistusete varukoopia loomise näide:

```
$ ivxv-backup management-conf
```

Kogumisteenuse e-valimiskasti varundamine

Kogumisteenuse e-valimiskasti varundamine toimub talletusteenuses kogutud häältest e-valimiskasti loomisega ja selle kopeerimisega varundusteenusesse. Varundatud andmete taastamine toimub hääletuse järel e-valimiskasti väljastamise käigus, kus talletusteenuses olevatest häältest ja varukoopiatesse salvestatud häältest pannakse kokku töötlemisele minev e-valimiskast.

E-valimiskasti varundamist viib läbi haldusteenus. Varukoopia loomine toimub talletusteenuses ja see kopeeritakse varundusserverisse.

Varukoopia on sama vorminguga, nagu kogumisteenuse poolt väljastatav e-valimiskast (ZIP64).

Varundamise andmemahtu saab arvutada järgmise meetodiga: `häälte arv * 12, 1 kB * pakkimistegur`.

Näiteks saja tuhande hääle suurus, kus pakkimistegur on 0,4 = 472 MB.

E-valimiskasti varukoopia loomise näide:

```
$ ivxv-backup ballot-box
```

Logide varundamine

Logikogumisteenustes kogutud logifailide varundamine toimub logifailide `/var/log/ivxv-YYYY-MM-DD.log` kopeerimisega varundusserverisse. Logide varundamist viib läbi haldusteenus.

Logide varukoopiast taastamise protseduuri pole kogumisteenuses ette nähtud.

Logikogumisteenusesse kogutud logist varukoopia loomise näide:

```
$ ivxv-backup log
```

5.13 Konsolideeritud e-valimiskasti koostamine

Konsolideeritud e-valimiskast koostatakse talletusteenusesse kogutud häältest ja varundusteenusesse varundatud e-valimiskastidest. Konsolideerimise protsess koosneb järgmistest sammudest:

1. Talletusteenusesse kogutud hääled varundatakse varundusteenusesse. Selle tulemusena on varundusteenusesse salvestatud kõik kogutud e-valimiskastid;
2. Varundusteenuses koostatakse konsolideeritud e-valimiskast;
3. Konsolideeritud e-valimiskast kopeeritakse haldusteenusesse.

Konsolideeritud e-valimiskasti koostamise näide:

```
ivxv-admin@admin $ ivxv-export-votes /output/voting/HA-SETUP/
↪exported-votes.zip
INFO: Creating backup copy from current ballot box
SERVICE backup@backup.ivxv.ee: Copying list of known SSH hosts to␣
↪service host
# Preparing ballot box backup file in voting service voting@voting1.
↪ivxv.ee
# Creating ballot box backup file ballot-box-20211228_1155.zip
Exporting votes: 0
Exporting votes: 1
Exporting votes: 2
Exporting votes: 3
Exporting votes: 4
Exporting votes: 5
Exporting votes: 6
Exporting votes: 7
Exporting votes: 8
# Copying backup file ballot-box-20211228_1155.zip to backup service
# Removing backup file ballot-box-20211228_1155.zip from voting␣
↪service
INFO: Copying ballot box to management service
SERVICE backup@backup.ivxv.ee: Copying ballot box from service host
INFO: Collected votes archive is written to '/output/voting/HA-
↪SETUP/exported-votes.zip'
```

5.14 Töötlemisrakenduse sisendi aluse koostamine

Töötlemisrakenduse sisendi alus on häälte töötlemiseks vajalike sisendfailide komplekt, mis genereeritakse kogumisteenuses salvestatud andmete põhjal. Komplekti koosseis on järgmine:

1. Ringkondade nimekiri;
2. Valijate nimekirjad;
3. E-valimiskast kogutud häältega;

4. Häälte registreerimispäringute valideerimisandmed;
5. Töötlemisrakenduse seadistused.

Väljund on ZIP-konteiner, mis sisaldab järgmisi faile:

1. Ringkondade nimekiri digitaalselt signeerituna `<election-id>.districts.json.asice`;
2. Valijate nimekirjade signeerimisvõtme avalik võti `voterfile.pub.key`;
3. Valijate nimekirjad `<changeset_no>.<election-id>.voters.utf`;
4. Valijate nimekirjade signatuurid `<changeset_no>.<election-id>.voters.sig`;
5. Valijate nimekirja vahelejätmise korraldused `<changeset_no>.<election-id>.voters-skip.yaml.asice`;
6. Registreerimispäringute verifitseerimise avalik võti `ts.key`;
7. Töötlemisrakenduse seadistuste mall e-valimiskasti verifitseerimiseks `<election-id>.processor.yaml`.

Töötlemisrakenduse sisendi alus koostatakse utiliidi *ivxv-generate-processor-input* abil. Näide:

```
ivxv-admin@admin $ ivxv-generate-processor-input /output/voting/HA-
↪SETUP/processor.cfg.zip
INFO: Generating processor application config
command_file:INFO: Loading command file '/etc/ivxv/election.bdoc'␣
↪(elections configuration)
INFO: Creating input file for processor application
INFO: Preparing container structure in directory '/tmp/tmp6jswwi8i'
INFO: Copying district list 'HA-SETUP.districts.json.bdoc'
INFO: Copying voter list signing key 'voterfile.pub.key'
INFO: Copying voter list #0 content '00.HA-SETUP.voters.utf'
INFO: Copying voter list #0 signature '00.HA-SETUP.voters.sig'
INFO: Copying voter list #1 content '01.HA-SETUP.voters.utf'
INFO: Copying voter list #1 signature '01.HA-SETUP.voters.sig'
...
INFO: Adding '02.HA-SETUP.voters.sig' to ZIP container
INFO: Adding '02.HA-SETUP.voters.utf' to ZIP container
INFO: Adding '03.HA-SETUP.voters.sig' to ZIP container
INFO: Adding '03.HA-SETUP.voters.utf' to ZIP container
INFO: Adding 'HA-SETUP.districts.json.bdoc' to ZIP container
INFO: Adding 'HA-SETUP.processor.yaml' to ZIP container
INFO: Adding 'ts.key' to ZIP container
INFO: Adding 'voterfile.pub.key' to ZIP container
INFO: Processor input is written to '/output/voting/HA-SETUP/
↪processor.cfg.zip'
```

5.15 Hääletamise statistika eksportimine

Häälestamise statistika koostatake hääletusteenuses ja see koosneb kahest osast: üldstatistika (hääletajate koguarv) ja detailstatistika. Üldstatistika kopeeritakse haldusteenusesse ja eksporditakse Valimiste Infosüsteemi 15 minutilise intervalliga. Detailstatistika koostatakse ja eksporditakse Valimiste Infosüsteemi käsitsi.

Häälestamise statistika importimine ja eksportimine toimub haldusteenuse masinas utiliidi *ivxv-voterstats* abil. Üldstatistika importimise ja eksportimise automaatika on teostatud cron-teenuse abil ja kirjeldatud failis `/etc/cron.d/ivxv-admin`.

5.16 Hääletamise seansside väljavõtte koostamine

Hääletamise ja hääle kontrollimise seansside väljavõte on CSV-vormingus ja see koostatakse logiseire teenuses.

Väljavõtet on võimalik koostada anonüümistatud kujul, kus kasutajate isikukoodid ja IP-aadressid on asendatud anonüümsete väärtustega.

Võimalik on valida, kas väljastada kõik hääletamise seansid või ainult hääle kontrollimisega seansid.

ivxv-voting-sessions

PEATÜKK 6

Krahhitaaste

Kogumisteenus on projekteeritud nii, et teenuse või selle osade krahhimise tagajärjel ei tekiks andmekadu või oleks see minimaalne.

6.1 Eeldused edukaks krahhitaasteks

Kõrgkäideldav seadistus

Peamine eeldus edukaks krahhitaasteks on kogumisteenuse paigaldamine kõrgkäideldava seadistusega, mis määrab vähemalt kolme talletusteenuse isendi kasutamise. Lisaks on krahhiolukorra kiiremaks lahendamiseks kasulik eraldada mikroteenustele ühe lisaisendite komplekti paigalduseks vajalik taristu.

Logikoguja kasutamine

Kogumisteenuse seadistus peab kirjeldama logikogumisteenuse, et mikroteenuste poolt toodetavad logisid oleks võimalik lihtsal moel kokku koguda. Soovitav on kasutada mitut logikogujat erinevas füüsilises lokatsioonis, et minimeerida logikirjete kaotsimineku võimalust.

Varundusteenuse kasutamine

Kogumisteenuse seadistus peab kirjeldama varundusteenuse ning automaatse varundamise ajad piisava sagedusega. Samuti on soovitav teha varukoopiad ka varundusteenusest.

Automaatne varundamine tagab e-valimiskasti koopia säilimise *talletusteenuse täieliku krahhi* korral.

Märkus: Varundusteenus on soovitav paigaldada teistest kogumisteenuse isenditest füüsiliselt eraldi, et võimalikud eriolukorrad (näiteks tulekahju) ei mõjutaks korraga nii varundusteenust kui teisi teenuseid.

Varundusteenus on projekteeritud kogumisteenuse andmetest automaatsete varukoopiate loomiseks ühte kohta ning nende kättesaadavaks tegemiseks operatsioonidele, mis varukoopiaid kasutavad (näiteks häälte kokkulugemine).

Märkus: Kogumisteenuse osutaja peaks kaaluma võimalust teha varundusteenusest täiendavaid varukoopiaid, et tagada varundatud andmete säilimine ka varundusteenuse krahhi korral.

Valmisolek krahhiks

Kogumisteenuse krahh mõjutab kõiki e-hääletamise komponente, erilist tähelepanu tuleb pöörata valijarakenduste ja kontrollrakenduste nimelahendusele ning TLS ühenduste usaldamiseks vajalikele sertifikaatidele.

Hääletamise edukaks läbiviimiseks tuleb tagada, et nimeserverid sisaldaks kogu hääletusperioodi vältel ajakohast infot hääletamissüsteemi sisendpunktide kohta - siis suudavad valijarakendused ja kontrollrakendused vastavalt muutuvatele oludele nimesid korrektselt lahendada.

1. Krahhimise tuvastamisel tuleb esimeste tegevuste hulgas eemaldada nimelahendusest krahhinud teenus, et rakendused enam selle poole pöörduda ei saaks.
2. Kui teenus(ed) pärast krahhi uuesti töökorda saadakse, tuleb viimase sammuna nimelahenduses panna uute teenuste aadressid lahenduma vastavalt rakendustes defineeritule.

Kui kogumisteenusesse lisatakse uusi mikroteenuseid (eeldatavalt pärast krahhimist), siis on tarvis tagada lisatud teenuste usaldusväärsus rakendustes.

Teenuse plaanimisel tuleb luua serdid/võtmed ka võimalike asendusteenuste jaoks (choices, mid, voting). Need võtmed tuleb pakendada valijarakendusse, et pärast krahhi poleks tarvis hakata uut rakendust levitama. Kui sertifikaadid luuakse ühe CA alt, siis piisab valijarakendusse vastava CA sertifikaadi pakendamisest. Kontrollrakendus-

te jaoks tuleb seadistustes alati näidata konkreetsed teenussertifikaadid, kuid kontrollrakenduste seadistuste muutmine ei eelda kontrollrakenduste uuesti levitamist.

6.2 Teenuste taastamine krahhist

Mikroteenuse isendi krahh ilma andmekaota

Mikroteenuse isendi krahh ilma andmekaota võib esineda teenuste puhul, mis ei tegele andmete säilitamisega (nimekirjateenus, hääletusteenus, kontrolliteenus või mobiil-id tugiteenus). Sellises olukorras piisab teenuse isendi taastamiseks kas teenuse taaskäivitamisest (kui see on võimalik) või teenuse isendi asendamisest uuega.

Vaata ka:

- *Teenuse (taas)käivitamine*
- *Teenuse isendi asendamine*

Logikogumisteenuse isendi krahh

Logikogumisteenuse krahh võib esineda nii logiandmete riknemisega kui ka ilma.

Ilma logiandmete riknemiseta krahh tähendab olukorda, kus rsyslog teenus seisab ja ei võta seetõtte teenustelt logikirjeid vastu ning salvestatud logifailid ei ole rikutud. Sellises olukorras piisab teenuse isendi töökorda seadmiseks selle taaskäivitamisest.

Logikogumisteenuse krahh koos logiandmete riknemisega nõuab teenuse isendi asendamist uuega.

Kui logiandmete riknemisega kaasneb alati logiandmete kadu, siis ilma riknemiseta krahhi puhul tuleb samuti selle võimalusega arvestada. Logisid edastatakse üle RELP-protokolli, mis on küllalt töökindel, kuid vaatamata sellele võib logiedastus katkeda olukorras, kus logi genereeriva teenuse hostil on rsyslogi isendit taaskäivitatud ajal, mil logikoguja rsyslog isend ei töötanud.

Vaata ka:

- *Teenuse (taas)käivitamine*
- *Teenuse isendi asendamine*
- RELP - The Reliable Event Logging Protocol[5]

[5] https://www.rsyslog.com/doc/relp.html

Varundusteenuse isendi krahh

Varundusteenuse isendi krahh tähendab varundusteenusesse varundatud andmete riknemist. Teenuse taastamiseks tuleb varundusteenus uuesti paigaldada ja varundatud andmed taastada. Andmete taastamine varundusserverisse võib toimuda ka pärast häälte kogumise lõppemist, kuid enne häälte kokkulugemist.

Märkus: Varundusprotseduuride käivitamist juhitakse haldusteenusest ja seetõttu pole varundusteenust võimalik käivitada ega seisma jätta.

Talletusteenuse isendi krahh

Talletusteenuse ühe isendi krahhimisel piisab isendi asendamisest uuega.

Talletusteenuseid saab lisada ja eemaldada ainult siis, kui klastris on vähemalt kvoorumi jagu töökorras talletusteenuse isendeid. Kvoorumi suurus on N/2+1 ümardatud alla, kus N on seadistatud isendite arv (näiteks kolme seadistatud isendi korral on kvoorumi suurus kaks).

Kui talletusteenuse isendeid jääb alles vähem kui kvoorumi jagu, siis tuleb teha kõigile isenditele uus paigaldus (vt. *Talletusteenuste täielik krahh*).

Talletusteenuse kvoorumist tingitud piirangud:

1. Talletusteenuse isendite arvu ei ole kunagi võimalik vähendada ühele;
2. Talletusteenuste isendite eemaldamisel peab arvestama kvoorumi säilimisega.
   Näide: kui on seadistatud 6 talletusteenuse isendit (kvoorum=4), siis sealt ei saa korraga eemaldada kolme isendit (jääks järgi kolm isendit, kvoorum=2), kuna seadistatud isendite hulk oleks siis väiksem kui algne kvoorum. Kõigepealt tuleb eemaldada üks (jääb järgi 5 isendit, kvoorum=3) isend ja alles pärast seda saab eemaldada ülejäänud kaks.

Vaata ka:

- *Teenuse (taas)käivitamine*
- *Teenuse isendi asendamine*

Talletusteenuste täielik krahh

Talletusteenuste täielikul asendamisel tuleb koostada uus tehniline seadistus, mis vastab järgmistele tingimustele:

- ei sisalda ühtegi vana talletusteenust;
- kõik uued talletusteenused on loetletud parameetri `storage.conf.bootstrap` nimekirjas.

Tähtis: Talletusteenuste täielikul asendamisel tuleb arvestada järgnevada:

- enne asendamist kogutud hääled säilivad varundusserveritesse tehtud varukoopiates;
- varukoopia loomise ja krahhi vahel kogutud hääled lähevad kaotsi;
- valikute, ringkondade ja valijate nimekirjad tuleb teenustele uuesti rakendada.

Kogumisteenuse täielik asendamine

Kui tekib vajadus kogumisteenuse täielikuks asendamiseks, siis tuleb kogumisteenusele teha uus paigaldus ilma andmete taastamiseta, mis on kiireim meetod teenuse uuesti töökorda seadmiseks.

Varasemalt kogutud häälte kaasamiseks häälte kokkulugemisele tuleb varundusserverisse taastada eelnevalt loodud varukoopiad.

Tähtis: Kogumisteenuse täielikul asendamisel tuleb arvestada, et enne asendamist kogutud hääled säilivad varundusserveritesse tehtud varukoopiates. Pärast varukoopia loomist kogutud hääled lähevad kaotsi.

PEATÜKK 7

Kogumisteenuse seadistused

7.1 Logimise seadistused

Kogumisteenuse logi hoitakse logi tekkimise asukohas ja dubleeritakse logiserveritesse. Logide kogumiseks ja edastamiseks kasutatakse vaikimisi *syslog*-teenust `rsyslog`.

Kogumisteenus toetab kahte liiki logiservereid, mis kirjeldatakse kogumisteenuse tehnilises seadistuses.

1. Kogumisteenuse logikogumisteenus on kogumisteenuse sisemine teenus ja seda võib süsteemis olla mitu isendit.
2. Tegevusmonitooringu server on kogumisteenuse jaoks väline teenus ja seda võib olla ainult üks isend.

Kogumisteenusele tehniliste seadistuse rakendamisel paigaldab haldusteenus logikogumisteenuse(d) enne teise teenuseid, et teenuste poolt toodetav logi saaks võimalikult varakult ka logikogumisteenusesse kogutud.

Märkus: Kogumisteenuse logiteated tekivad pärast valimiste seadistuse esmakordset laadimist, kuna teenused käivitatakse selle seadistuse laadimise järel.

Logi tootva teenuse logimise korraldus

Logi tootva teenuse logimise seadistuse genereerib haldusteenus vastavalt tehnilistele seadistustele.

1. Iga teenus logib kohalikku *syslog*-teenusesse;
2. Kõigi teenusmasinate *syslog*-teenused on seadistatud kogumisteenuse logi salvestama kohalikku failisüsteemi (`/var/log/ivxv-YYYY-MM-DD.log`);
3. Kõigi teenusmasinate (peale logikogumisteenuse) *syslog*-teenused on seadistatud edastama üle võrgu:
    1. Kõiki logikirjeid logikogumisteenusesse (protokoll: RELP);
    2. Kogumisteenuse logikirjeid tegevuslogi monitooringu serverisse (protokoll: RELP);

Logikogumisteenuse korraldus

Logikogumisteenuse seadistusfail tuleb teenuse tarkvarapakist (*ivxv-logcollector.conf*).

1. Logikogumisteenus võtab logikirjeid vastu RELP-protokolli kaudu;
2. Kogumisteenuse logikirjeid kirjutatakse JSON-vormingus faili `/var/log/ivxv-YYYY-MM-DD.log` (välja arvatud päringu- ja silumislogi);
3. Kogumisteenuse päringulogi kirjutatakse rsyslogi standardvormingus faili `/var/log/ivxv-request-YYYY-MM-DD.log`;
4. Kogumisteenuse silumislogi ja teiste oluliste teenuste (haproxy, etcd, rsyslog, sshd) logi kirjutatakse rsyslogi standardvormingus faili `/var/log/ivxv-debug-YYYY-MM-DD.log`.

7.2 Talletamisteenuse seadistused

Hetkel ainus talletamisteenuse teostus kasutab hajusat võti-väärtus andmebaasi `etcd`. Korraga käivitatakse mitu `etcd` isendit, mis saavutavad omavahel konsensuse talletatud andmete osas.

Talletusteenuse sujuvaks tööks võib olla vajalik osade `etcd` parameetrite häälestamine konkreetse evituskeskkonna jaoks. Selleks tuleb teenuse masinas luua fail `/etc/default/ivxv` ning sinna lisada järgmistes jaotistes kirjeldatud read. Pärast faili loomist või selle sisu muutmist tuleb uute väärtuste rakendamiseks talletusteenus taaskäivitada. Parameetri puudumise korral kasutatakse vaikeväärtust.

Seadistuste väärtuste valimisel on abiks `etcd` dokumentatsioon aadressil https://coreos.com/etcd/docs/latest/tuning.html.

Ajaparameetrid

`etcd` klaster valib ühe liikmetest juhiks, mis koordineerib kõiki andmemuudatusi. Lisaks pingib juht perioodiliselt kõiki ülejäänud klastri liikmeid aitamaks tuvastada olukorda, kus ühendus juhiga on katkenud: kui mõni klastri liikmetest pole piisavalt kaua ühtegi pingi saanud, algatab see uue juhi valimise.

Suurema võrgu- või kettalatentsuse tagajärjel võib juhi ping liialt viibida ning põhjustada uue juhi valimise. Tõrgete korral on juhivahetus süsteemi loomulik osa, ent töötava süsteemi puhul tarbetu koormus. Seetõttu tuleks seadistada juhi pingimise tihedust `ETCD_HEARTBEAT_INTERVAL` ning teiste liikmete ooteaega `ETCD_ELECTION_TIMEOUT` vastavalt evituskeskkonna latentsusele:

```
ETCD_HEARTBEAT_INTERVAL=100
ETCD_ELECTION_TIMEOUT=1000
```

Mõlemad väärtused on millisekundites ning vaikimisi vastavalt 100ms ja 1000ms.

Tähtis: Ühes klastris peavad kõigil talletamisteenuse isenditel olema samad ajaparameetrid. Vastasel korral võib esineda stabiilsusprobleeme erinevate pingi ootuste tõttu.

Hetkvõtete parameetrid

`etcd` peab logi kõigist andmemuudatustest. Vältimaks logi liiga suureks kasvamist tehakse andmebaasi seisust perioodiliselt hetkvõtteid ning eelnev logi kustutatakse. Kui talletamisteenus kasutab liiga palju mälu või kettaruumi, siis võib aidata tihedam hetkvõtete tegemine.

Uus hetkvõte tehakse iga `ETCD_SNAPSHOT_COUNT` andmemuudatuse järel, seega madalam väärtus toob kaasa tihedamad hetkvõtted ning väiksema logi suuruse:

```
ETCD_SNAPSHOT_COUNT=10000
```

Vaikimisi tehakse hetkvõte iga 10000 muudatuse järel.

PEATÜKK 8

Lisad

8.1 Utiliidid

Kogumisteenuse haldamise käsureautiliitide ülevaade ja abiteave.

.

Andmehoidla utiliidid

ivxv-create-data-dirs

`ivxv-create-data-dirs --help`:

```
Create IVXV Collector Management Service data directories.

NOTE: Directory owners and permissions are not set by this utility!

Usage: ivxv-create-data-dirs
```

ivxv-db-reset

`ivxv-db-reset --help`:

```
Reset IVXV Collector Management Service database.

Usage: ivxv-db-reset [--force]

Options:
    --force     Don't ask user confirmation
```

ivxv-db-dump

`ivxv-db-dump --help`:

```
Dump IVXV Collector Management Service database.

Usage: ivxv-db-dump [<key>] ...
```

Teenuse seisundi utiliidid

ivxv-status

`ivxv-status --help`:

```
Output IVXV Collector state.

Usage: ivxv-status [--json] [--service=<service-id> ...] [<filter> .
↪..]

Options:
    --json                  Output full data in JSON format.
                            Note: filters have no effect in JSON␣
↪output.
```

(jätkub järgmisel leheküljel)

(jätk eelmisele leheküljele)

```
    --service=<service-id>  Filter output by service ID.
                            Note: This filter conflicts other␣
↪section
                            filters than "smart" or "service".
    <filter>                Filter output by section. Possible␣
↪values are:
                              * collector - collector state;
                              * election - election data;
                              * config - versions of loaded config;
                              * list - versions of loades lists;
                              * service - service information;
                              * ext - external service information;
                              * storage - storage information;
                              * smart - output only relevant data;
                              * all - output all data;
                            [Default: smart].
```

ivxv-service

`ivxv-service --help`:

```
Manage IVXV services.

Usage: ivxv-service <action> <service-id> ...

Options:
    <action>    Management action: start, stop, restart, ping
```

Sündmuste logi utiliidid

ivxv-eventlog-dump

`ivxv-eventlog-dump --help`:

```
Dump IVXV Collector Management event log in human readable format.

Usage: ivxv-eventlog-dump
```

Kasutajate halduse utiliidid

ivxv-users-list

`ivxv-users-list --help`:

```
List IVXV Collector Management Service registered users.

Usage: ivxv-users-list
```

Seadistusutiliidid

ivxv-collector-init

`ivxv-collector-init --help`:

```
Initialize IVXV Collector.

Usage: ivxv-collector-init [--force]

Options:
    --force     Don't ask user confirmation
```

ivxv-cmd-load

`ivxv-cmd-load --help`:

```
Load command to IVXV Collector Management Service.

Usage: ivxv-cmd-load [--autoapply] [--show-version] <type> FILE

Options:
    <type>              Command type. Possible values are:
                        - election: election config
                        - technical: collector technical config
                        - trust: trust root config
                        - choices: choices list
                        - districts: districts list
                        - voters: voters list or voters list␣
↪skipping
                        - user: user account and role(s)
    --autoapply         Apply command file automatically (by Agent␣
↪Daemon).
    --show-version      Output config file version and exit.
```

ivxv-config-validate

`ivxv-config-validate --help`:

```
Validate IVXV collector config files.

Validate single config files. Also validate voting lists␣
↪consistency if
multiple lists are provided.

Usage:
    ivxv-config-validate [--plain] [--trust=<trust-file>]
        [--technical=<technical-file>] [--election=<election-file>]
        [--choices=<choices-file>] [--districts=<districts-file>]
        [--voters=<voters-file> ...]

Options:
    --plain     Validate plain config file (Default: BDOC container)
```

ivxv-config-apply

`ivxv-config-apply --help`:

```
Apply loaded IVXV Collector config to services.

Usage: ivxv-config-apply [--type=<type>] ... [<service-id>] ...

Options:
    --type=<type>    Config type. Possible values are:
                     - election: election config file
                     - technical: collector technical config file
                     - choices: choices list
                     - districts: districts list
                     - voters: voters list
```

Seadistuste rakendamine hallatavatele teenustele on võimalik siis, kui haldusteenusesse on laaditud kogumisteenuse tehnilised seadistused.

Seadistuste rakendamise järjekord:

1. Tehnilised seadistused koos usaldusjuure seadistustega.
    1. Teenuse tarkvara paigaldamine;
    2. Haldusteenuse ligipääsu loomine hallatava teenuse kontole;
    3. Teenuse logimisseadistuste rakendamine;
    4. Haldusteenuse ligipääsu eemaldamine teenuse hosti juurkasutaja kontole (ainult juhul, kui teenusmasinas pole rohkem seadistamata teenuseid);
    5. Usaldusjuure rakendamine teenusele;
    6. Tehniliste seadistuste rakendamine teenusele;

2. Valikute nimekiri;
3. Ringkondade nimekiri;
4. Valijate nimekirjad;

Logikogumisteenus erineb teistest hallatavatest teenustest:

1. Logikogumisteenus seadistatakse enne teisi teenuseid, et tagada võimalikult varajane logi kogumine.
2. Logikogumisteenustele ei rakendata muid seadistusi peale logikogumisteenuse seadistuste (usaldusjuure seadistusi, kogumisteenuse tehnilised seadistusi ja valimiste seadistusi logikogumisteenus ei vaja).

Valimisnimekirjade (valikute ja valijate nimekirjad) rakendamine tähendab nimekirja ülekandmist talletusteenusesse vastavat nimekirja teenindava teenuse kaudu.

Näiteks valikute nimekiri rakendatakse vaid ühele (juhuslikult valitud) nimekirjateenusele, mis kannab nimekirja talletusteenusesse. Talletusteenuse kaudu on nimekiri kättesaadav kõigile teistele nimekirjateenustele.

ivxv-voter-list-download

`ivxv-voter-list-download --help`:

```
Download next available voter list changeset from VIS to IVXV␣
↪Collector
Management Service.

Usage:
    ivxv-voter-list-download [--output-report=<filepath>] [--log-
↪level=<level>]

Options:
    --output-report=<filepath>  Write JSON report about HTTP␣
↪request to VIS.
    --log-level=<level>         Logging level [Default: INFO].
```

ivxv-secret-load

`ivxv-secret-load --help`:

```
Load secret data to IVXV services.

This utility loads file that contains secret data to services.

Supported secret types are:

    tls-cert - TLS certificate for service.
```

(jätkub järgmisel leheküljel)

(jätk eelmisele leheküljele)

```
        Certificate (and key) is used for securing
        communication between services and service instances.

    tls-key - TLS key for service.

        Key is used together with service certificate.

    tsp-regkey - PKIX TSP registration key for voting services.

        Key is used for signing Time Stamp Protocol requests.

        Key file must be in PEM format and must be not password␣
↪protected.

    mid-token-key - Mobile ID identity token for
                    choices, mobile-id and voting services.

        Key file must be 32 bytes long.

Usage: ivxv-secret-load [--service=<service-id>] <secret-type>
↪<keyfile>
```

ivxv-copy-log-to-logmon

`ivxv-copy-log-to-logmon --help`:

```
Copy IVXV log files from service hosts to Log Monitor.

This utility transports collected IVXV log files from IVXV services
(including Log Collector Service) to Log Monitor.

Usage: ivxv-copy-log-to-logmon [--log-level=<level>] [<hostname> ...
↪]

Options:
    <hostname>              Service host name.
    --log-level=<level>     Logging level [Default: INFO].
```

ivxv-update-packages

`ivxv-update-packages --help`:

```
Update service packages in IVXV service hosts.

This utility checks versions of software packages in service hosts
and installs new versions if required.

Usage: ivxv-update-packages [--force]

Options:
    --force     Update even package version does not require update
```

ivxv-backup-crontab

`ivxv-backup-crontab --help`:

```
Generate crontab for IVXV backup automation.

This utility must be called as editor by crontab utility:

    $ env VISUAL=ivxv-backup-crontab crontab -e

Usage: ivxv-backup-crontab <filename>
```

Andmete eksportimise ja varundamise utiliidid

ivxv-export-votes

`ivxv-export-votes --help`:

```
Export collected votes.

This utility copies current ballot box from voting service to backup
service and outputs ballot box content.

Usage: ivxv-export-votes [--consolidate] <output-file>

Options:
    --consolidate   Consolidate all collected votes
```

ivxv-backup

`ivxv-backup --help`:

```
Backup IVXV collector data.

Usage: ivxv-backup management-conf
       ivxv-backup ballot-box [<voting_service_id>]
       ivxv-backup log
```

ivxv-generate-processor-input

`ivxv-generate-processor-input --help`:

```
Generate input for processor application.

This utility generates ZIP container with data files
for processor application to validate ballot box:

    1. District list;
    2. Voter lists;
    3. Validation key for vote registration requests;
    4. Configuration for processor application.

Usage: ivxv-generate-processor-input <output-file>
```

ivxv-voterstats

`ivxv-voterstats --help`:

```
Import voter stats from voting service and export common stats to␣
↪VIS.

Usage: ivxv-voterstats <TYPE> [--action=<action>] [--file=<file>]
            [--service-id=<service_id>] [--log-level=<level>]

Options:
    <TYPE>                      Stats type "common" or "detail".
    --action=<action>           Limit actions for "common" stats␣
↪type.
                                Possible values are "import" and
↪"export".
                                [Default: all]
    --file=<file>               Path to stats file.
    --service-id=<service_id>   Voting service ID [Default: random].
    --log-level=<level>         Logging level [Default: INFO].
```

ivxv-voting-sessions

`ivxv-voting-sessions --help`:

```
Import list of voting sessions from Log Monitor.

Session data is in CSV format.

Usage: ivxv-voting-sessions (vote | verify) <output_file> [--
↪anonymize]
            [--log-level=<level>]

Options:
    <output_file>               Write sessions to file.
    --anonymize                 Anonymize session data
                                (IP addresses and ID codes).
    --log-level=<level>         Logging level [Default: INFO].
```

Deemonid

ivxv-agent-daemon

`ivxv-agent-daemon --help`:

```
IVXV Collector Management Service agent daemon.

Usage: ivxv-agent-daemon [--get-stats] [--register-status]

Options:
    --get-stats         Copy statistics from Log Monitor to
                        Management Service without daemonizing.
    --register-status   Register collector state (if not␣
↪registered).
```

Sisemised utiliidid

Tähelepanu: Sisemised utiliidid on kasutusel haldusdeemoni poolt alamteenuste haldamiseks ja neid ei ole reeglina tarvis eraldi käivitada.

ivxv-admin-helper

`ivxv-admin-helper --help`:

```
Usage:
    ivxv-admin-helper check-service-config <service-type> <service-
↪id>
        Check service configuration

    ivxv-admin-helper copy-logs-to-logmon <hostname> <logmonitor-
↪address>
        Copy IVXV service log files to Log Monitor

    ivxv-admin-helper restart-service <service-type> <service-id>
                                      <systemctl-service-id>
        Restart service
```

ivxv-admin-sudo

`ivxv-admin-sudo --help`:

```
Usage:
    ivxv-admin-sudo backup-ballot-box <voting-host> <service-id>
                                      <backup-filename>
        Backup ballot box (in backup service)

    ivxv-admin-sudo backup-log <log-host> <backup-timestamp>
        Backup log file (in backup service)

    ivxv-admin-sudo create-ssh-access <account-name>
        Create management service access to account in service host

    ivxv-admin-sudo init-host
        Initialize service host

    ivxv-admin-sudo init-service <service-id>
        Initialize service data directory.
        Value 'backup' is used for all backup services

    ivxv-admin-sudo install-pkg <package-filename>
        Install IVXV package with dependencies

    ivxv-admin-sudo prepare-ballot-box-backup <service-id> <backup-
↪filename>
        Prepare votes backup file in voting service

    ivxv-admin-sudo remove-admin-root-access
        Remove management service access to service host root␣
↪account

    ivxv-admin-sudo rsyslog-config-apply
        Apply rsyslog config file for IVXV logging
```

8.2 Seadistusfailid

Logikogumisteenuse seadistusfail

```
# IVXV Internet voting framework

# Rsyslog configuration file for log collector service
# /etc/rsyslog.d/ivxv-logcollector.conf

# Collect log messages over RELP protocol
module(load="imrelp")
input(type="imrelp" port="20514" maxDataSize="32k")

# write IVXV log to /var/log/ivxv.log (up to level INFO)
if ($programname startswith 'ivxv-') and ($syslogfacility-text ==
↪'local0') and
   ($syslogseverity <= '6') then
action(
    type="omfile"
    dynaFile="IVXV_DEFAULT_LOG_FILENAME"
    template="ivxv-json"
)

# write IVXV request log to /var/log/ivxv-request.log
if ($programname startswith 'ivxv-') and ($syslogfacility-text ==
↪'local1') then
action(
    type="omfile"
    dynaFile="IVXV_REQUEST_LOG_FILENAME"
)

# write IVXV debug log and log of related
# services (haproxy, etcd, rsyslog, sshd) to /var/log/ivxv-debug-
↪YYYY-MM-DD.log
if ($programname startswith 'ivxv-') or ($programname startswith
↪'rsyslog') or
   ($programname == 'haproxy') or ($programname == 'sshd') or (
↪$programname == 'etcd') then
action(
    type="omfile"
    dynaFile="IVXV_DEBUG_LOG_FILENAME"
)
```

8.3 Lisaseadistused

SSH kasutajate autentimine ID-kaardi abil

SSH-teenusesse on võimalik autentida ID-kaardi avaliku võtmega abil, kasutades selleks PKCS#11 toega SSH-klienti kitty.exe (http://kitty.9bis.net/).

Turvakaalutustel tuleks keelata haldusliidese SSH-teenusesse parooliga autentimine. Parooliga autentimise keelamiseks tuleb seadistusfailis `/etc/ssh/sshd_config` määrata parameetri `PasswordAuthentication` väärtuseks `no`:

```
# To disable tunneled clear text passwords, change to no here!
PasswordAuthentication no
```

Volitatud kasutajate faili asukoht (`/etc/ssh/kasutajad`) tuleb failis `/etc/ssh/sshd_config` määrata parameetriga `AuthorizedKeysFile`:

> AuthorizedKeysFile /etc/ssh/kasutajad

Tähtis: Seadistusfailis /etc/ssh/sshd_config tehtud muutuse rakendamiseks tuleb SSH teenus taaskäivitada:

```
# service ssh restart
[ ok ] Restarting OpenBSD Secure Shell server: sshd.
```

ID-kaardi isikutuvastamise sertifikaadiga autenditava kasutaja ülesseadmine käib järgmiselt:

1. Kasutajale konto loomine:

   ```
   # adduser --disabled-password kasutajanimi
   # usermod -a -G www-data kasutajanimi
   ```

2. Kasutaja ID-kaardi isikutuvastamise sertifikaadi salvestamine PEM-vormingus faili `usercert.cer` (ID-kaardi haldusvahendi abil);
3. Sertifikaadist kasutaja avaliku võtme eraldamine ja salvestamine faili `userpubkey.pem`:

   ```
   # openssl x509 -in usercert.cer -pubkey -noout > userpubkey.pem
   ```

4. Avaliku võtme teisendamine PKCS#8 vormingusse, kasutaja tunnusega varustamine ja salvestamine SSH volitatud kasutajate faili `/etc/ssh/kasutajad`:

   ```
   # KEY=$(ssh-keygen -i -m PKCS8 -f userpubkey.pem)
   # echo "$KEY kasutaja@eesti.ee" >> /etc/ssh/kasutajad
   ```

5. Kontrollimine, kas lisatud kirje on kujul `ssh-rsa PKCS8-võti` kasutajatunnus:

```
# tail -1 /etc/ssh/kasutajad
ssh-rsa AAAAB3NzaC1yc2EAAAAELGuiTwAAAIEAxZf/
↪TuSrGJEU1PlfkY9jJ33VOYVZ9Vao0Uiytlf8
7HJu/
↪78fCIB7m05J7ibpMhsZoZ4DElU7ve0VwbvdDS3srh1OhiQcUjpznTlx4rIM1vkHwadrHtmF+BN
DwbLbbdD5y3puGcLH+sLuwba6Vuc3aU0QuqzenYmY9pV7w9y0wc=␣
↪kasutaja@eesti.ee
```

8.4 Andmehoidla

Haldusteenuse andmeid hoitakse failisüsteemis ja andmebaasis. Failisüsteemis hoitakse andmeid, mis on pärit välistest süsteemidest ja on haldusteenusesse üle kantud faili kujul. Andmebaasis hoitakse andmeid, mis on genereeritud haldusteenuse töö käigus.

Failisüsteemis hoitavad andmed

- `/etc/ivxv/` – kogumisteenusele rakendatud ja hetkel kehtivad seadistus- ja nimekirjafailid;
- `/var/lib/ivxv/` – kogumisteenuse haldusteenuse andmefailid;
- `/var/lib/ivxv/admin-ui-data/` – haldusteenuse veebiliidese jaoks serveeritavad JSON-failid;
- `/var/lib/ivxv/admin-ui-data/status.json` – kogumisteenuse seisundi koondandmed;
- `/var/lib/ivxv/admin-ui-permissions/` – haldusteenuse veebiliidese kasutajaõigused (Apache veebiserveri jaoks);
- `/var/lib/ivxv/ballot-box/` – allalaaditava e-valimiskasti salvestamise kataloog;
- `/var/lib/ivxv/commands/` – kogumisteenuse juhtimiseks rakendatud korraldusfailide ajalugu;
- `/var/lib/ivxv/commands/<command-type>-<timestamp>.bdoc` – digitaalselt allkirjastatud korraldus ASiC-E vormingus.
- `/var/lib/ivxv/commands/<command-type>-<timestamp>.json` – korralduse olekufail JSON-vormingus.
- `/var/lib/ivxv/db/` – haldusteenuse andmebaasi kataloog;
- `/var/lib/ivxv/db/ivxv-management.db` – haldusteenuse andmebaasi fail;
- `/var/lib/ivxv/ivxv-management-events.log` – haldusteenuse sündmuste logi;
- `/var/lib/ivxv/service/` – muud teenusespetsiifilised failid (nt. registreerimisvõtmest eraldatud avalik võti);

- `/var/lib/ivxv/upload/` – kogumisteenusesse veebiliidese kaudu laaditud failid;

Andmebaasis hoitavad andmed

Andmevälja nimi ja kirjeldus:

- `collector/state` – kogumisteenuse olek;
- `config/election` – kogumisteenuses rakendatud valimiste seadistusele digiallkirja andnud volitatud kasutaja andmed kujul `<CN> <timestamp>`;
- `config/technical` – kogumisteenuses rakendatud tehnilisele seadistusele digiallkirja andnud volitatud kasutaja andmed kujul `<CN> <timestamp>`;
- `config/trust` – kogumisteenuses rakendatud usaldusjuure seadistusele digiallkirja andnud volitatud kasutaja andmed kujul `<CN> <timestamp>`;
- `election/election-id` – valimiste identifikaator;
- `election/electionstart` – valimiste algusaeg;
- `election/electionstop` – valimiste lõpuaeg;
- `election/servicestart` – kogumisteenuse käivitamise aeg;
- `election/servicestop` – kogumisteenuse seiskamise aeg;
- `host/<hostname>/state` – teenushosti seisund;
- `list/choices` – haldusteenusesse laaditud valikute nimekirjale digiallkirja andnud volitatud kasutaja andmed kujul `<CN> <timestamp>`;
- `list/choices-loaded` – nimekirjateenustesse laaditud valikute nimekirjale digiallkirja andnud volitatud kasutaja andmed kujul `<CN> <timestamp>`;
- `list/districts` – nimekirjateenustesse laaditud ringkondade nimekirjale digiallkirja andnud volitatud kasutaja andmed kujul `<CN> <timestamp>`;
- `list/districts-loaded` – nimekirjateenustesse laaditud ringkondade nimekirjale digiallkirja andnud volitatud kasutaja andmed kujul `<CN> <timestamp>`;
- `list/voters0000` – haldusteenusesse laaditud valijate algnimekirjale digiallkirja andnud volitatud kasutaja andmed kujul `<CN> <timestamp>`;
- `list/voters<list-number>` (`list-number >= 01`) – haldusteenusesse laaditud valijate muudatusnimekirja allalaadimise hetke ajatempel;
- `list/voters<list-number>-state` – nimekirjateenustesse laaditud valijate nimekirja olek.

  Võimalikud väärtused:

  1. `PENDING` - laaditud haldusteenusesse;
  2. `APPLIED` - rakendatud nimekirjateenusele;
  3. `INVALID` - nimekiri on märgitud vigaseks ja ootab halduri otsust vahelejätmise kohta (ainult muudatusnimekirja korral);
  4. `SKIPPED` - nimekiri on vahele jäetud (ainult muudatusnimekirja korral).
- `logmonitor/address` – seireteenuse aadress või võrgunimi;

- `logmonitor/last-data` – viimase seireteenusest statistikafaili hankimise aeg;
- `user/<idcode>` – haldusteenuse kasutaja nimi ja rollid kujul `<surname, name> <role>[,<role>]`;
- `service/<service-id>/service-type` – Teenuse liik;
- `service/<service-id>/technical-conf-version` – Teenusele rakendatud tehnilise seadistuse versioon;
- `service/<service-id>/election-conf-version` – Teenusele rakendatud valimiste seadistuse versioon;
- `service/<service-id>/network` – Teenusele alamvõrgu nimi;
- `service/<service-id>/state` – Teenuse olek;
- `service/<service-id>/ping-errors` – Teenuse elusoleku kontrollimise järjestikuste vigade arv;
- `service/<service-id>/last-data` – Teenuse viimase oleku hankimise aeg;
- `service/<service-id>/ip-address` – Teenuse IP-aadress;
- `service/<service-id>/bg_info` – Teenuse taustainfo stringina (näiteks elusoleku kontrolli käigus genereeritud veateade);
- `service/<service-id>/backup-times` – Varundusteenuse automaatvarunduse kellaajad;
- `service/<service-id>/mid-token-key` – Mobiil-ID/Smart-ID tugiteenuse identsustõendi võtmefaili kontrollsumma (SHA256);
- `service/<service-id>/tls-cert` – Teenuse TLS-sertifikaadi faili kontrollsumma (SHA256);
- `service/<service-id>/tls-key` – Teenuse TLS-sertifikaadi võtmefaili kontrollsumma (SHA256);
- `service/<service-id>/tspreg-key` – Hääletamisteensue ajatempliteenuse signeerimisvõtme faili kontrollsumma (SHA256);

Kasutatud tähised:

- `<command-type>` – korralduse liik:
  1. `trust` – usaldusjuure seadistused;
  2. `technical` kogumisteenuse seadistused;
  3. `election` valimiste seadistused;
- `<CN>` – ID-kaardi CN väli kujul `PEREKONNANIMI,EESNIMI,ISIKUKOOD`;
- `<config-type>` on seadistuse liik. Usaldusjuure seadistus on `trust`, valimiste seadistus on `election` ja kogumisteenuse tehniline seadistus on `tech`;
- `<hostname>` teenushosti nimi;
- `<list-number>` valimisnimekirja kahekohaline järjekorranumber, esimene nimekiri kannab numbrit 01.
- `<service-id>` teenuse identifikaator kogumisteenuse seadistustest;
- `<timestamp>` on ajatempel ISO-8601 vormingus.

8.5 Klastri seisundi monitoorimine Zabbixiga

Etcd klaster tagab süsteemi toimimise ka olukorras, kus mõni klastriliige kaotab töövõime (krahh, võrguühenduse kadumine jms.). Siiski on oluline selliseid sündmuseid monitoorida ning nende algpõhjus tuvastada. Etcd krahhimise tuvastamiseks tuleb talletusteenuste logidest (`ivxv-YYYY-MM-DD.log`) monitoorida `ivxv.ee/service/storage.EtcdTerminatedError` kirjet.

Täiendavalt saab etcd käsureakliendiga küsida klastri liikmete olekut. Kuna IVXV klastris on kõik klient-päringud autenditud, siis tuleb korraldus käivitada mõnes `ivxv-storage` teenuse masinas kasutajakonto `ivxv-storage` (või juurkasutaja) õigustes:

```
# ivxv-storage@ivxv1:~$ env ETCDCTL_API=3 etcdctl \
      --cacert /var/lib/ivxv/service/storage@storage1.ivxv.ee/ca.
↪pem \
      --cert /var/lib/ivxv/service/storage@storage1.ivxv.ee/tls.pem␣
↪\
      --key /var/lib/ivxv/service/storage@storage1.ivxv.ee/tls.key \
      --endpoints ivxv1:2379,ivxv2:2379,ivxv3:2379 \
      endpoint status

ivxv1:2379, 2d0df029f29770a4, 3.2.17, 25 kB, true, 12, 15
ivxv2:2379, d4a9ae16c8557764, 3.2.17, 25 kB, false, 12, 15
ivxv3:2379, e8914f4e0b89b80f, 3.2.17, 25 kB, false, 12, 15
```

Vastuses on veergude tähendused järgmised:

1. klastri liige;
2. klastri liikme identifikaator;
3. etcd versioon;
4. baasi suurus (max 8GB ehk 8589934592);
5. kas konkreetne klastri liige on hetkel juht;
6. RAFT ametiaeg (sisuliselt toimunud juhi-valimiste arv);
7. RAFT indeks - etcd kirjutamisoperatsioonide arv (sh. konfiguratsiooni muutused).

Monitooringule on oluline parameeter RAFT ametiaeg. Selle väärtuse muutumine tähendab juhivahetust, mis üldjuhul on seotud probleemidega klastri töös - olemasolev juht ei vasta piisavalt kiiresti klastri liikmete päringutele.

Käsurea seletus:

- `env ETCDCTL_API=3`: kasutame etcd API versiooni 3 (Ubuntu versioonis 20.04 LTS on `etcdctl` API vaikeversioon veel 2);
- `--cacert`: usaldame ainult servereid, mille sertifikaat on antud selle CA poolt;
- `--cert` ja `--key`: kasutame klient-autentimiseks ivxv1 talletusteenuse sertifikaati ja võtit;

- `--endpoints`: millistele serveritele päring saata. Siin võib kõigi kolme asemel ka ainult ühe loetleda: sellisel juhul on väljundis vaid üks rida. Kasulik nt kui Zabbix tahab igas talletusteenuses küsida ainult selle isendi kohta;
- `endpoint status`: küsime loetletud serverite olekut.

Väljundit on võimalik küsida ka masinloetavas JSON-vormingus (parameeter `-w json`):

```
ivxv-storage@ivxv1:~$ env ETCDCTL_API=3 etcdctl \
    --cacert /var/lib/ivxv/service/storage@storage1.ivxv.ee/
↪ca.pem \
    --cert /var/lib/ivxv/service/storage@storage1.ivxv.ee/
↪tls.pem \
    --key /var/lib/ivxv/service/storage@storage1.ivxv.ee/
↪tls.key \
    --endpoints ivxv1:2379,ivxv2:2379,ivxv3:2379 \
    endpoint status -w json

[{"Endpoint":"ivxv1:2379","Status":{"header":{"cluster_id
↪":1867986262344190226,"member_id":3246514969358332068,
↪"revision":1,"raft_term":12},"version":"3.2.17","dbSize
↪":24576,"leader":3246514969358332068,"raftIndex":15,
↪"raftTerm":12}},
{"Endpoint":"ivxv2:2379","Status":{"header":{"cluster_id
↪":1867986262344190226,"member_id":15323970619978381156,
↪"revision":1,"raft_term":12},"version":"3.2.17","dbSize
↪":24576,"leader":3246514969358332068,"raftIndex":15,
↪"raftTerm":12}},
{"Endpoint":"ivxv3:2379","Status":{"header":{"cluster_id
↪":1867986262344190226,"member_id":16758262885041944591,
↪"revision":1,"raft_term":12},"version":"3.2.17","dbSize
↪":24576,"leader":3246514969358332068,"raftIndex":15,
↪"raftTerm":12}}]
```