

X-tee: v5.5-st v6 osa eraldiseisvale serverile migreerimise juhend

Redaktsioon: 0.3

22.03.2017

Dokumendi id: UG-MIGR

Versioonide ajalugu

Kuupäev	Redaktsioon	Kirjeldus	Autor
15.02.2017	0.1	Esimene tulem	Kristo Heero
17.03.2017	0.2	Märkus sisemise TLS-sertifikaadi loomise kohta	Kristo Heero
22.03.2017	0.3	Mittesisulised formaadimuudatused PDF-väljundi tarbeks	Toomas Mölder

Sisukord

- [Litsents](#)
- [1 Sissejuhatus](#)
 - [1.1 Eesmärk](#)
 - [1.2 Viited](#)
- [2 Migreerimine](#)
 - [2.1 Uue v6 turvaserveri kasutusele võtmine](#)
 - [2.2 Vana v6 osa kasutusest maha võtmine v5.5 turvaserveris](#)

Litsents

This document is licensed under the Creative Commons Attribution-ShareAlike 3.0 Unported License. To view a copy of this license, visit <http://creativecommons.org/licenses/by-sa/3.0/>

1 Sissejuhatus

1.1 Eesmärk

Selle dokumendi eesmärk on anda konkreetset juhised, kuidas läbi viia versioon 5.5 turvaserverist versiooni 6 migreerimine eraldiseisvasse serverisse.

1.2 Viited

1. [IG-SS] Cybernetica AS. X-Road 6. Security Server Installation Guide. Document ID: IG-SS, http://x-road.eu/docs/x-road_v6_security_server_installation_guide.pdf.
2. [UG-SS] Cybernetica AS. X-Road 6. Security Server User Guide. Document ID: UG-SS, http://x-road.eu/docs/x-road_v6_security_server_user_guide.pdf.

2 Migreerimine

2.1 Uue v6 turvaserveri kasutusele võtmine

1. Paigalda uus v6 turvaserver, kuid ära vii läbi turvaserveri esialgset initsialiseerimist (vt [IG-SS]).
2. Vaheta uues v6 turvaserveris andmebaaside *serverconf* ja *messagelog* paroolid samaks, mis olid vastavalt vanas turvaserveris (vt v5.5 turvaserveri failis `/etc/xroad/db.properties` olevate parameetrite *serverconf.hibernate.connection.password* ja *messagelog.hibernate.connection.password* väärtusi).

2.1 Muuda failis `/etc/xroad/db.properties` olevate parameetrite *serverconf.hibernate.connection.password* ja *messagelog.hibernate.connection.password* väärtused samaks, mis olid vanas turvaserveris.

2.2 Muuda paroolid ka andmebaasis. Käsurea terminalis:

```
sudo su - postgres
psql -U postgres
ALTER USER serverconf WITH PASSWORD 'SIIA-VANA-SERVERCONF-PAROOL';
ALTER USER messagelog WITH PASSWORD 'SIIA-VANA-MESSAGELOG-PAROOL';
\q
```

2.3 Taaskäivita teenus *xroad-proxy*. Käsurea terminalis:

```
sudo restart xroad-proxy
```

3. Veendu, et v5.5 turvaserverisse on paigaldatud viimane versioon X-tee tarkvarast. Käsurea terminalis:

```
sudo apt-get update
sudo apt-get dist-upgrade
```

4. Varunda v5.5 turvaserveris v6 turvaserveri konfiguratsioon (vt peatükki "Back up and Restore" [UG-SS]).

5. Taasta uus v6 turvaserver käsurealt kasutades eelnevalt vanast turvaserverist varundatud konfiguratsiooni (vt peatükki "Back up and Restore" [UG-SS]).

6. Redigeeri uues v6 turvaserveris konfiguratsioonifaili `/etc/xroad/conf.d/local.ini` järgmiselt:

6.1 Eemalda sektsioonist *[proxy]* järgmised parameetrid:

- `client-http-port`
- `client-https-port`
- `verify-client-cert`
- `log-both-messages`

6.2 Eemalda täielikult sektsioonid *[client-mediator]* ja *[monitoringagent]*.

6.3 Eemalda sektsioonist *[proxy-ui]* järgmised parameetrid:

- `clients-importer-command`
- `tls-key-importer-command`
- `tls-key-exporter-command`

6.4 Taaskäivita *xroad-proxy* ja *xroad-jetty* teenused. Käsurea terminalis:

```
sudo restart xroad-proxy
sudo restart xroad-jetty
```

7. Kustuta järgmised üleliigsed konfiguratsioonifailid:

- `/etc/xroad/conf.d/client-mediator.ini`
- `/etc/xroad/conf.d/conf-importer.ini`
- `/etc/xroad/conf.d/clientmediator-logback.xml`
- `/etc/xroad/conf.d/confimporter-logback.xml`
- `/etc/xroad/conf.d/monitoragent-logback.xml`
- `/etc/xroad/services/xtee55-clientmediator.conf`
- `/etc/xroad/services/xtee55-confimporter.conf`
- `/etc/xroad/services/xtee55-monitor.conf`

8. Veendu, et uues v6 turvaserveris jäi riistvaralise krüptoseadme tugi tööle (näiteks uue võtme genereerimine õnnestub) (vt peatükki "Installing the Support for Hardware Tokens" [IG-SS] ja peatükki "Security Tokens, Keys, and Certificates" [UG-SS]). Vajadusel teosta vajalikud tegevused vastavalt kasutuses oleva riistvaralise krüptoseadme juhendile.

9. Genereeri uues v6 turvaserveris uus sisemine TLS-sertifikaat (vt peatükki "Changing the Internal TLS Key and Certificate" [\[UG-SS\]](#)) ja vajadusel impordi uus TLS-sertifikaat ka vastavatesse infosüsteemidesse.

Märkus: kui v6 turvaserveri versioon on 6.8.6, siis kasutajaliideses esineva vea tõttu ei ole võimalik seal uut sisemist TLS-sertifikaati luua. Samas saab selle genereerida aga käsurea terminalis, millele järgnevalt tuleb taaskäivitada ka *xroad-proxy* teenus. Käsurea terminalis (esimene käsk ühel real):

```
sudo -u xroad /usr/share/xroad/scripts/generate_certificate.sh \  
-n internal -f -S -p  
sudo restart xroad-proxy
```

10. Teavita X-tee keskust, et vana v6 turvaserveri IP-aadress asendataks uue v6 turvaserveri IP-aadressiga. Pärast aadressivahetust keskserveris levib muudatus globaalse konfiguratsiooniga kõigile turvaserveritele ning edaspidi päringuid vanasse v6 turvaserverisse enam ei suunata (kui turvaserver pakkus teenust).

2.2 Vana v6 osa kasutusest maha võtmine v5.5 turvaserveris

Kui v6 päringuvahendus on edukalt üle läinud uuele v6 turvaserverile, siis on vaja v6 osa vanast v5.5 turvaserverist kasutusest maha võtta.

1. Deaktiveeri v6 päringuvahendaja. Käsurea terminalis:

```
deactivate_v6_xroad.sh
```

2. Arhiveeri sõnumilogi andmebaas (vt. peatükki "Message Log" [\[UG-SS\]](#)).

2.1 Konfigureeri sõnumilogi kirjade arhiveerimise intervall väiksemaks, (puudumisel) lisades konfiguratsioonifaili `/etc/xroad/conf.d/local.ini` sektsiooni `[message-log]` ning selle alla parameetri `archive-interval` väärtuse, mis kutsub arhiveerimist välja näiteks iga 30 sekundi järel:

```
archive-interval=0/30 * * * * ? *
```

- 2.2 Pärast konfiguratsiooni muutmist taaskäivita teenus *xroad-proxy*. Käsurea terminalis:

```
sudo restart xroad-proxy
```

2.3 Oota, kuni kõik sõnumilogi kirjed on andmebaasist arhiveeritud. Selle veendumiseks kontrolli sõnumilogi andmebaasist, kas arhiveerimata sõnumilogi kirjade arv on 0. Käsurea terminalis (vajaliku andmebaasi parooli leiad failis `/etc/xroad/db.properties` olevalt parameetrilt `messagelog.hibernate.connection.password`):

```
psql -h 127.0.0.1 -U messagelog messagelog
select count(*) from logrecord where discriminator='m' and not archived;
\q
```

2.4 Arhiveeri kõik loodud arhiivifailid (*mlog-*.zip*) kaustast `/var/lib/xroad/` (kui seda pole konfigureeritud juba automaatselt tegema).

3. Seiska kõik mitte X-tee v5 süsteemi teenused. Käsurea terminalis:

```
sudo stop xroad-confclient
sudo stop xroad-proxy
sudo stop xroad-signer
sudo stop xroad-monitor
sudo stop xroad-jetty
sudo stop xtee55-clientmediator
sudo stop xtee55-monitor
```

4. Keela mitte X-tee v5 süsteemi teenuste käivitamine ka arvuti taaskäivitusel. Käsurea terminalis:

```
echo manual > /etc/init/xroad-confclient.override
echo manual > /etc/init/xroad-proxy.override
echo manual > /etc/init/xroad-signer.override
echo manual > /etc/init/xroad-monitor.override
echo manual > /etc/init/xroad-jetty.override
echo manual > /etc/init/xtee55-clientmediator.override
echo manual > /etc/init/xtee55-monitor.override
```

5. Arhiveeri auditilogi fail `/var/log/xroad/audit.log`.