12. Turvaserveri paigaldamine

Õpikeskkond: Riigi Infosüsteemi Ameti juhendid
Kursus: X-tee turvaserveri administraatori õppematerjal
Raamat: 12. Turvaserveri paigaldamine
Printija: Jan Raik
Kuupäev: kolmapäev, 26. august 2020, 11.30

Sisukord

12.1. Sissejuhatus

Selles õppetükis antakse juhiseid X-tee turvaserveri paigaldamiseks. Samuti tutvustatakse turvaserveri süsteemiteenuseid ja kasutajarolle. Õppetüki lõpetamise järel oskad Sa ise X-tee turvaserverit paigaldada ning paigaldusel ilmnevaid vigu parandada.

Turvaserveri paigaldamiseks kulub Sul 30-40 minutit.

12.2. Nõuded turvaserveri taristule ja OS-ile

Turvaserveri tarkvara tarnitakse .deb-pakkidena, mis on kättesaadavad ametliku X-tee repositooriumi kaudu siit.

Turvaserver töötab 64-bitisel platvormil Ubuntu Server 18.04 Long-Term Support (LTS); miinimumnõuded on 3 GB RAM-mälu ja 3 GB vaba kettaruumi.

Tarkvara võib paigaldada nii tavalisele kui ka virtualiseeritud riistvarale. Viimast on testitud Xeni ja Oracle VirtualBoxi keskkondades.

Kui kasutad toodangukeskkonda, tutvu kindlasti jõudlustestidega ning allkirjastamisseadme piirangutega virtualiseeritud platvormil. USB-seadmetel on väiksem jõudlus ja need sobivad paremini mittevirtualiseeritud keskkonda. Lisateavet leiad siit.

RIA turvaserveri koormustestide tulemused

Ressursid

X-tee turvaserverite teste viiakse läbi kolmel jõudlustasemel. Iga testi puhul turvaserveri masinale on eraldatud **3GB** mälu ning Java protsesside jaoks on kasutatud vaikimisi mälu konfiguratsioonid. Igat testi taset kirjeldatakse protsessorite tuumade arvu järgi:

- Low-end: 2 CPU cores
- Mid-range: 4 CPU cores
- High-end: 8 CPU cores

NB! Low-end vastab täielikult turvaserveri miinimum nõuetele.
Täiendavalt teste viiakse läbi erinevate krüptoseadmetega:

- Soft token (tarkvaraline võti)
- Utimaco Se52
- Utimaco Se500
- SafeNet eToken PRO (v4.29, Aladdin)

Konfiguratsioon

Teste jooksutakse järgmises konfiguratsioonis:

- Kõik komponendid (koormaja, 2 turvaserverit, teenuse mock) töötasid virtuaalses keskkonnas. Selle tulemusena võib kohati märgata mitteloogilised jõudluse kõikuvused.
- Koormaja jaoks on kasutatud Gatling v2.2.2
- Teenuse mock: https://github.com/ria-ee/X-Road-tests/tree/master/common/xrd-mock-soapui
- Kõik komponendid paiknevad samas kohtvõrgus
- Kasutatud turvaserveri versioon 6.9.5
- Testide jooksul toimus sõnumite ajatembeldamine kord minutis, mis mõjutas samaaegselt töötavate päringute kiirust ning seoses sellega ka üldist päringute standardhälvet (Loe lisaks: https://github.com/vrk-kpa/xroad-joint-development/issues/152).
- Testide jooksul ei toimunud sõnumite logi arhiveerimist
- Tenuste monitooringu andmete salvestamine oli aktiivne testide ajal

- Utimaco HSM'ide testimisel mõlemad turvaserverid kasutasid sama Net HSM'i
- Safenet eToken'ite puhul igal turvaserveril oli oma USB token küljes
- Koormaja käivitab päringuid fikseeritud kasutajate arvu poolt (threadid). Kui üks kasutaja saab vastuse, siis see käivitab uue päringu ilma viivituseta.
- Teenuse mockis kuluv aeg on sõltuvalt koormusest keskmiselt **5-20 ms**.
- Testides on kasutatud "Intel(R) Xeon(R) CPU E5-2650L v2 @ 1.70GHz" protsessorid.

Teststsenaarium

- Iga testi viiakse läbi fikseeritud sõnumi suurusega (100KB keerulise XML struktuuriga SOAP keha)
- Teste viiakse läbi kõikide CPU tuumade ning krüptoseadmete kombinatsioonide jaoks.
- Testide eel käivitatakse soojendav test mille käigus esialgu käivitatakse päringuid: 20 kasutajate poolt 120 sekundi jooksul ja seejärel 1 kuni 20 kasutajat 12 sekundi jooksul iga kasutajate arvu jaoks.
- Testi käivitatakse järgmiselt: alustatakse 1 kasutajaga (thread) 120 sekundi jooksul. Siis suurendatakse kasutajate arvu ühe võrra ning saadetakse päringud veel 120 sekundi jooksul. Jätkatakse kuni 20 kasutajateni mis samuti saadavad päringuid 120 sekundi jooksul.
- Kuna virtuaalmasinate jõudlus pole piisavalt stabiilne, siis testid on käivitatud 3 korda järjest ning lõppraporti jaoks on valitud iga kasutajate arvu puhul kõige parema tulemuse.
- Sõnumi ajaks on loetud aeg alates päringu saatmisest koormaja poolt kuni vastuse saabumiseni koormajasse.

Low-end (2 Cores) tulemused

Soft Token

Users	Requests (per 120 sec)	Mean (ms)
1	954	96
5	3346	176
10	4377	271
15	4581	390
20	4865	491

Utimaco Se52

Users	Requests (per 120 sec)	Mean (ms)
1	884	105
5	2617	226
10	3410	348
15	3890	460
20	4137	581

Utimaco Se500

Users	Requests (per 120 sec)	Mean (ms)
1	1097	80
5	3124	189
10	3760	316
15	4264	419
20	4461	535

SafeNet eToken PRO

Users	Requests (per 120 sec)	Mean (ms)
1	126	926
5	527	1140
10	951	1264
15	1396	1288
20	1736	1387

Mid-range (4 Cores) tulemused

Soft Token

Users	Requests (per 120 sec)	Mean (ms)
1	922	100
5	3795	155
10	5880	201
15	7000	254
20	7828	304

Utimaco Se52

Users	Requests (per 120 sec)	Mean (ms)
1	896	103
5	2721	217
10	4107	289
15	5063	354
20	5622	424

Utimaco Se500

Users	Requests (per 120 sec)	Mean (ms)
1	1087	81
5	3386	174
10	4791	247
15	5504	324
20	6208	384

SafeNet eToken PRO

Users	Requests (per 120 sec)	Mean (ms)
1	127	917
5	541	1109
10	1044	1151
15	1505	1197
20	2066	1162

High-end (8 Cores) tulemused

Soft Token

Users	Requests (per 120 sec)	Mean (ms)
1	882	106
5	4706	126
10	8434	139
15	10882	161
20	11913	197

Utimaco Se52

Users	Requests (per 120 sec)	Mean (ms)
1	879	106
5	2787	212
10	4525	264
15	6170	288
20	7280	326

Utimaco Se500

Users	Requests (per 120 sec)	Mean (ms)
1	1071	82
5	3444	171
10	5700	208
15	7846	226
20	9200	257

SafeNet eToken PRO

Users	Requests (per 120 sec)	Mean (ms)
1	126	928
5	530	1134
10	1057	1136
15	1526	1182
20	1926	1248

Detailsemad RIA koormustestide tulemused tabeli kujul

Koormustestid_6.9.5.xlsx

***

Soome koormustesti tulemused

Soome poolt läbiviidud testid ei ole otseselt võrreldavad RIA poolt läbi viidud testidega, kuna turvaserverite jõudlus ei olnud samaväärne, samuti erines mock teenus. Soome testid annavad ülevaate turvaserverite jõudlusest ekstreem olukordades. „Logging on“ testide puhul säilitatakse

sõnumite logides sõnumite sisu.

Soome koormustestide tulemused failina

XROAD_692_Loadtest_results.pdf

***

X-tee 6.16.0-0 versiooni tulemused (12.09.2017 reliis)

Testid on läbi viidud samadel tingimustel nagu versiooni 6.9.5 puhul.

Low-end (2 Cores) tulemused

Soft Token

Users	Requests (per 120 sec)	Mean (ms)
1	847	112
5	3064	193
10	4232	281
15	4762	375
20	5010	477

Detailsemad RIA koormustestide tulemused tabeli kujul

Koormustestid_6.16.0-0.xlsx

***

X-tee 6.18.0 versiooni tulemused (21.06.2018 reliis)

Testid on läbi viidud samadel tingimustel nagu versiooni 6.9.5 puhul.

Low-end (2 Cores) tulemused

Soft Token

Users	Requests (per 120 sec)	Mean (ms)
1	917	103
5	3353	171
10	4395	270
15	5010	357
20	5046	474

Detailsemad RIA koormustestide tulemused tabeli kujul

Koormustestid_6.18.0.xlsx

***

X-tee 6.19.0 versiooni tulemused (17.01.2019 reliis)

Testid on läbi viidud samadel tingimustel nagu versiooni 6.9.5 puhul.

Low-end (2 Cores) tulemused

Soft Token

Users	Requests (per 120 sec)	Mean (ms)
1	863	110
5	3174	181
10	4223	281
15	4739	377
20	4935	485

Detailsemad RIA koormustestide tulemused tabeli kujul

Koormustestid_6.19.0.xlsx

12.3. Nõuded võrgule

Turvaserveril peab olema kaks IP-aadressi. Üks IP-aadress peaks olema sisevõrkude jaoks halduseks ja ühendusteks kohalike infosüsteemidega. Teine IP-aadress peaks olema kas avalik IP-aadress või juurdepääs NAT-i kaudu suhtlemiseks teiste turvaserveritega.

Luba ka lisateenuseid, mis on operatsioonisüsteemi toimimiseks ja haldamiseks olulised (nagu DNS, NTP ja SSH).

> **NB!** Järgnevates tabelites on antud soovitused tulemüüri reeglite seadistamiseks.
> **NB!** Suhtlus teiste turvaserveritega on soovitatav white-listida X-tee turvaserveritele (või nende vajalikule alamhulgale), mis on võimalik leida X-tee globaalsest konfiguratsioonist.

Sisenevate ühenduste pordid (välisvõrgust turvaserverini)

Port	Selgitus	Soovitus
TCP 5500	sõnumivahetus turvaserverite vahel	Avada ainult turvaserveritele, kes tarbivad Teie teenuseid.
TCP 5577	OCSP-vastuste päringud turvaserverite vahel	Avada ainult turvaserveritele, kes tarbivad Teie teenuseid.

Väljuvate ühenduste pordid (turvaserverist välisvõrku)

Port	Selgitus	Soovitus
TCP 5500	sõnumivahetus turvaserverite vahel	Avatud turvaserverite pihta, kuhu päringui tehakse
TCP 5577	OCSP-vastuste päringud turvaserverite vahel	Avatud turvaserverite pihta, kuhu päringui tehakse
TCP 4001	suhtlus keskserveriga	Peab olema avatud keskserverite suunal.
TCP 80	globaalse konfiguratsiooni allalaadimine	Peab olema avatud keskserverite suunal.
TCP 80,443	levinumad kehtivuskinnituse- ja ajatempliteenused	Peab olema avatud usaldusteenuse pakkuja(te)le.
UDP 123	NTP	Peab olema avatud kasutatavate ajaserverite suunal.
TCP/UDP 53	DNS	Peab olema avatud kasutatavate nimeserverite suunal.

Kohalik juurdepääs

Port	Selgitus	Soovitus

Port	Selgitus	Soovitus
TCP 4000	kasutajaliides	Soovitatavalt avada ainult eraldi sisemises alamvõrgus
TCP 80	ühendused infosüsteemidest	Piirangud vajaduspõhiselt ja sõltuvad infosüsteemi ülesehitusest.
TCP 80,443	ühendused infosüsteemidest	Erinevate klientide ja infosüsteemide puhul kasutada HTTPSi.

Enne kui alustad turvaserveri tarkvara paigaldamist, veendu, et vajalikud teenuspordid on avatud. Selleks vali sihtvõrgus masin (*host*), mis ei ole kaitstud tulemüüriga. Kasutades „netcat" vahendit, ava vajalik port:

```
netcat -l <port>
```

Kontrolli turvaserverist, kas port on nähtav ja lahti, kasutades „telnet" vahendit:

```
telnet host <port>
```

Korda seda sammu kõikide portide puhul.

12.6. X-tee turvaserveri tarkvara paigaldamine

X-tee turvaserveri tarkvara paigaldamiseks tee järgmist.

1. Lisa X-tee paki repositooriumi ja `nginx`-repositooriumi aadress faili `/etc/apt/sources.list.d/xroad.list`:

```
deb http://x-tee.ee/packages/live/xroad trusty main
deb http://ppa.launchpad.net/nginx/stable/ubuntu trusty main
deb http://ppa.launchpad.net/openjdk-r/ppa/ubuntu trusty main
```

2. Lisa usaldusvõtmete loendisse X-tee repositooriumi allkirjavõti:

```
curl http://x-tee.ee/packages/xroad_repo.gpg | sudo apt-key ad
d -
sudo apt-key adv --keyserver hkp://keyserver.ubuntu.com:80 --r
ecv-keys 00A6F0A3C300EE8C
sudo apt-key adv --keyserver hkp://keyserver.ubuntu.com:80 --r
ecv-keys EB9B1D8886F44E2A
```

3. Turvaserveri pakkide paigaldamiseks anna järgmised käsud:

```
sudo apt-get update
sudo apt-get install openjdk-8-jre-headless
sudo apt-get install xroad-securityserver-ee
```

12.7. Pärast X-tee turvaserveri tarkvara paigaldamist

Pakkide esmakordsel paigaldamisel küsib süsteem järgmist teavet:

1. Sellise kasutaja konto nimi, kellele antakse kasutajaliideses õigus kõiki toiminguid teha. See kasutaja peab olema sama, kes loodi enne turvaserveri paigaldust `adduser` käsuga.
2. Kasutajaliidese enda poolt allkirjastatud TLS-sertifikaadi omaniku DN („Subject DN“) ja selle alternatiivsed nimed („subjectAltName“). Sertifikaati kasutatakse kasutajaliidesega ühenduste turvamiseks. Vaikeväärtustena pakutakse operatsioonisüsteemist tuvastatud nime ja IP-aadresse.

   „Subject DN“ tuleb sisestada kujul:

   ```
   /CN=server.domain.tld
   ```

   Alternatiivseteks nimekujudeks peab sisestama kõik kasutusel olevad IP-aadressid ning nimekujud järgmises vormingus:

   ```
   IP:1.2.3.4,IP:4.3.2.1,
   DNS:servername,DNS:ser
   vername2.domain.tld
   ```

3. Infosüsteemide HTTPS-i juurdepääsupunkti turvamiseks kasutatud TLS-sertifikaadi omaniku DN. Vaikeväärtustena pakutakse süsteemist tuvastatud nime ja IP-aadresse.

   „Subject DN“ tuleb sisestada kujul:

   ```
   /CN=server.domain.tld
   ```

   Alternatiivseteks nimekujudeks peab sisestama kõik kasutusel olevad IP-aadressid ning nimekujud järgmises vormingus:

   ```
   IP:1.2.3.4,IP:4.3.2.1,
   DNS:servername,DNS:ser
   vername2.domain.tld
   ```

Metapakett `xroad-securityserver` paigaldab ka metateenuste mooduli `xroad-addon-metaservices`, sõnumilogi mooduli `xroad-addon-messagelog` ja WSDL validaatori mooduli `xroad-addon-wsdlvalidator`.

Vaata paigaldusprotsessi eespool kirjeldatud etappe tutvustavat videot.

12.8. Kasutajarollid ja kasutajate haldamine

Turvaserveris on toetatud järgmised kasutajarollid:

- **turvahaldur** (`xroad-security-officer`) vastutab turvapoliitika ja turvanõuete rakendamise eest, sh haldab võtmeseadeid, võtmeid ja sertifikaate;
- **registreerimishaldur** (`xroad-registration-officer`) vastutab turvaserveri klientide registreerimise ja eemaldamise eest;
- **teenusehaldur** (`xroad-service-administrator`) haldab teenuste andmeid ja juurdepääsuõigusi;
- **süsteemiadministraator** (`xroad-system-administrator`) vastutab turvaserveri paigaldamise, konfigureerimise ja tööshoidmise eest.

Ühel kasutajal võib olla mitu rolli ja ühes rollis võib olla mitu kasutajat. Rollidele vastavad süsteemigrupid, mis luuakse süsteemi paigaldamisel.

Juhul, kui kasutajaliidesesse sisse loginud kasutaja ei oma toimingu sooritamiseks õigust, on tegevuse käivitamise nupp peidetud (ning tegevust ei ole võimalik käivitada ka vastavate klahvikombinatsioonide/hiiretoimingute abil). Kasutaja näeb vaid temale lubatud andmeid ja saab teha lubatud toiminguid.

Kõik õigused antakse turvaserveri tarkvara paigaldamisel valitud kasutajanimele (**X-Road Superuser**).

Kasutajate haldamine toimub juurkasutaja õiguste käsureal.

Uue kasutaja lisamiseks sisesta käsk

```
sudo adduser username
```

Loodud kasutajale õiguste andmiseks lisa ta vastavatesse süsteemigruppidesse, näiteks

```
sudo adduser username
  xroad-security-officer
```

```
sudo adduser username
  xroad-registration-officer
```

```
sudo adduser username
  xroad-service-administrator
```

```
sudo adduser username
xroad-system-administrator
```

Kasutajaõiguse eemaldamiseks eemalda kasutaja vastavast süsteemigrupist, näiteks

```
sudo deluser username xroad-security-officer
```

Kasutaja eemaldamiseks sisesta

```
sudo deluser username
```

12.9. Paigaldusjärgne kontroll

X-tee teenused on olekus start/running, mida saab kontrollida käsureaga (järgneb näide väljundist):

```
sudo initctl list | gr
ep "^xroad-"
```

```
xroad-jetty start/runn
ing, process 19796
xroad-confclient star
t/running, process 195
63
xroad-signer start/run
ning, process 19393
xroad-proxy start/runn
ing, process 19580
```

Kontrolli, kas turvaserveri kasutajaliidest aadressil **https://SECURITYSERVER:4000/** saab veebibrauseris avada.

Sisselogimiseks kasutage paigaldamise ajal valitud kontonime. Kasutajaliidese käivitamisel võidakse veebibrauseris kuvada tõrketeade “502 Bad Gateway”.

12.10. Süsteemiteenused

Kõige olulisemad X-tee turvaserveri teenused (need, mida on vaja rakenduse toimimiseks) ja nende logid on järgmised (juhul, kui teil on vaja üksikteenust käivitada või taaskäivitada).

Teenus	Eesmärk	Logi
`xroad-confclient`	Globaalse konfiguratsiooni jagaja klientprotsess	`/var/log/xroad/configuration_client.log`
`xroad-jetty`	Kasutajaliidest käitav rakendusserver	`/var/log/xroad/jetty/`
`xroad-proxy`	Päringuvahendaja	`/var/log/xroad/proxy.log`
`xroad-signer`	Võtmeseadmete kontrollprotsess	`/var/log/xroad/signer.log`
`nginx`	Veebiserver, mis vahendab kasutajaliidese rakendusserveri ja päringuvahendaja teenust	`/var/log/nginx/`

Süsteemiteenuseid saab hallata süsteemi `upstart` abil.

Teenuse käivitamiseks tuleb anda juurkasutaja õigustes käsk

```
sudo service <service>
start
```

Teenuse peatamiseks sisesta

```
sudo service <service>
stop
```

Logide lugemiseks peab kasutaja omama juurkasutaja õiguseid või olema süsteemigrupis `xroad`. Logitakse süsteemi **Logback** abil. Logide konfiguratsioonifailid asuvad kaustas `/etc/xroad/conf.d/`.

Logimise vaikeseaded:

- logimise tase INFO,
- logifailide roteerimine toimub 100MB täitumisel.

12.11. Riistvaraliste võtmeseadmete paigaldamine

Riistvaraliste võtmeseadmete (kiipkaart, USB-seade, HSM) toe konfigureerimisel tee järgmist.

1. Paigalda riistvaraliste võtmeseadmete toe moodul järgmise käsu abil:

```
sudo apt-get install xroad-addon-hwtokens
```

2. Paigalda ja konfigureeri riistvaralise seadme jaoks PKCS#11 draiver vastavalt tootja juhistele.
3. Lisa PKCS#11 draiveri tee faili `/etc/xroad/devices.ini` (nagu on kirjeldatud failis toodud näites).
4. Pärast draiveri installimist ja konfigureerimist tuleb teenus `xroad-signer` taaskäivitada.

```
sudo service xroad-signer restart
```

12.12. Tõrgete haldamine

Õppetüki lõpuks anname juhiseid selle kohta, mida teha, kui paigaldusprotsessi käigus kuvatakse järgmised tõrketeated:

- “Cannot set LC_ALL to default locale”
- “PostgresSQL is not UTF8 compatible”
- “Could not create default cluster”
- “PostgresSQL is running on port 5432”

12.13. Cannot set LC_ALL to default locale

Kui lokaadi käsu käivitamisel kuvatakse tõrketeade locale: `Cannot set LC_ALL to default locale: No such file or directory`, pole konkreetse keele jaoks tuge paigaldatud.

Toe paigaldamiseks käivitage järgmine käsk (näites kasutatakse inglise keelt):

```
sudo apt-get install l
anguage-pack-en
```

Süsteemi lokaadifaile saab uuendada järgmiste käskudega (näites kasutatakse USA lokaati):

```
sudo locale-gen en_US.
UTF-8
```

```
sudo update-locale en_
US.UTF-8
```

Määra operatsioonisüsteemi lokaat. Lisa faili `/etc/environment` järgmine rida:

```
LC_ALL=en_US.UTF-8
```

Pärast süsteemi lokaadiseadete uuendamist on soovitatav operatsioonisüsteem taaskäivitada.

12.14. PostgresSQL is not UTF8 compatible

Kui turvaserveri paigaldamisel katkestatakse paigaldus tõrketeatega `postgreSQL is not UTF8 compatible`, on PostgreSQL paigaldatud vale lokaadiga.

Üks võimalik lahendus on eemaldada PostgreSQL-i paigalduse käigus loodud andmehoidla ning luua see uuesti õige kodeeringuga. NB! Kõik andmed andmebaasis kustutatakse!

```
sudo pg_dropcluster --
stop 9.3 main
LC_ALL="en_US.UTF-8" s
udo pg_createcluster -
-start 9.3 main
```

Katkenud paigalduse saab lõpule viia käsuga

```
sudo apt-get -f instal
l
```

12.15. Could not create default cluster

PostgresSQL-i paigaldamisel võidakse kuvada üks järgmistest tõrketeadetest:

- `Error: The locale requested by the environment is invalid.`
- `Error: could not create default cluster. Please create it manually with pg_createcluster 9.3 main –start.`

Sel juhul saab PostgreSQL andmeklastri luua järgmise käsuga:

```
LC_ALL="en_US.UTF-8" s
udo pg_createcluster -
-start 9.3 main
```

Katkenud paigalduse saab lõpule viia käsuga

```
sudo apt-get -f instal
l
```

12.16. PostgresSQL is running on port 5432

Paigaldamise ajalvõidakse kuvada ka järgmine tõrketeade: `Is postgres running on port 5432? Aborting installation! please fix issues and rerun with apt-get -f install.`

Selle tõrke kõrvaldamiseks tuleb kontrollida, kas andmeklastri paigaldamisel ilmnes mõni viga. Kui jah, siis järgi eespool toodud juhiseid.

Kui tõrget ei ilmnenud, pole turvaserveri paigalduse käigus paigaldatud PostgreSQL-i andmeklaster tõenäoliselt seadistatud kuulama porti 5432.

Kuulatavat porti saab kontrollida ja seadistada PostgreSQL-i konfiguratsioonifailis `/etc/postgresql/9.3/main/postgresql.conf`. Kuulatava pordi muutmisel tuleks teenus `postgresql` taaskäivitada.

Katkenud paigalduse saab lõpule viia käsuga

```
sudo apt-get -f instal
l
```

12.17. Muud tõrked

Probleemide jätkumisel kontrollige, kas viga võib olla

- OS-i süsteemilogis:

```
/var/log/syslog
```

- X-tee auditilogis:

```
/var/log/xroad/audit.log
```

- kasutajaliidest käitava rakendusserveri logis:

```
/var/log/xroad/jetty/jetty.log
```

12.18. Küsimused

Selle õppetüki läbimiseks loe tähelepanelikult järgmisi väiteid ja otsusta, kas need on tõesed või mitte.

A. `nginx` on veebiserver, mis vahendab `xroad-jetty` ja `xroad-proxy` teenuseid.
B. Süsteemiadministraator paigaldab, konfigureerib ja hoiab töös turvaserverit; turvahaldur vastutab muu hulgas võtmeseadete, võtmete ja sertifikaatide haldamise eest.

Õigeid vastuseid vaata siit (avanevad uues aknas).

12.19. Kokkuvõte

Turvaserver töötab 64-bitisel platvormil Ubuntu Server 14.04 Long-Term Support (LTS); miinimumnõuded on 2 GB RAM-mälu ja 3 GB vaba kettaruumi.

Turvaserveri tarkvara võib paigaldada nii tavalisele kui ka virtualiseeritud riistvarale.

Turvaserveril peaks olema kaks IP-aadressi: üks ühendusteks kohalike infosüsteemidega ja halduseks, teine avalik IP-aadress või juurdepääs NAT-i kaudu teiste turvaserveritega suhtlemiseks.

12.4. OS-i paigaldamine

Enne OS-i paigaldamist tee järgmist.

1. Leia järgmine teave:
   - väline IP-aadress (IP, alamvõrk, lüüs),
   - sisemine IP-aadress (IP, alamvõrk),
   - täielik domeeninimi (FQDN) ja
   - DNS-server.
2. Konfigureeri võrgujuurdepääs ja valmista ette DNS-kirje.
3. Vali esialgne kasutajanimi operatsioonisüsteemi ja turvaserveri haldusjuurdepääsuks.
4. Seejärel laadi alla uusim Ubuntu 14.04 64-bitine versioon ja valmistage ette paigaldusvahendid.

   > **NB!** Kasutada ainult ametlikku allikat OSi pakettide jaoks https://www.ubuntu.com/download/server ja https://launchpad.net/ubuntu/+archivemirrors

5. Operatsioonisüsteemi ja turvaserveri tarkvara alla laadimisel veendutakse paigalduspaketi õigsuses kasutades md5sum utiliidiga
6. Kontrolli, et serveri ketas vastab logi- ja arhiveerimisnõuetele.

Kogutud ja ette valmistatud andmetega on OS-i paigaldamine üsna lihtne.

12.5. Pärast OS-i paigaldamist

Pärast OS-i paigaldamist tee järgmist.

Konfigureeri sisevõrgu kasutajaliides faili `/etc/network/interfaces` muutmisega, lisades oma sisevõrgu IP konfiguratsiooni põhjal järgmised andmed:

```
auto eth1
iface eth1 inet static
address 1.2.3.4
netmask 255.255.255.0
```

Käivita teine võrguliides järgmise käsuga:

```
sudo ifup eth1
```

Lisa süsteemikasutaja, kellele antakse kasutajaliideses kõik rollid (kui see pole sama, keda kasutati paigalduse ajal). Lisa uus kasutaja käsuga

```
sudo adduser username
```

Määra operatsioonisüsteemi lokaat. Lisa faili `/etc/environment` järgmine rida:

```
LC_ALL=en_US.UTF-8
```

Paigaldus on õnnestunud, kui süsteemiteenused käivituvad ja kasutajaliides vastab.