24. Sõnumilogi arhiivimine

Õpikeskkond: Riigi Infosüsteemi Ameti juhendid
Kursus: X-tee turvaserveri administraatori õppematerjal
Raamat: 24. Sõnumilogi arhiivimine
Printija: Jan Raik
Kuupäev: kolmapäev, 26. august 2020, 11.39

Sisukord

24.1. Sissejuhatus

Selles õppetükis antakse juhised sõnumilogi arhiivimiseks. Pärast õppetüki läbimist oskad

- muuta sõnumilogi arhiivimiskonfiguratsiooni,
- otsida arhiivifaili ja edastada seda turvaserverist ja
- kasutada arhiivifaili jaoks kaugandmebaasi.

Õppetüki läbimiseks kulub sul 20-30 minutit.

Euroopa Liit
Euroopa
Regionaalarengu Fond

Eesti
tuleviku heaks

X-TEE

RIIGI INFOSÜSTEEMI AMET

24.2. Sõnumilogi arhiivimise olulisus

Sõnumilogi funktsiooniks on tõendada X-teel vahetatud tavaliste taotlus- või vastussõnumite vastuvõtmist.

Iga sõnumi jaoks toodab server täieliku allkirjastatud ja aegtembeldatud sõnumikonteineri (*Associated Signature Container, ASiC*) ja arhiivib selle kohalikku failisüsteemi. Arhiivifailid on spetsiaalse linikimisteabega failiga ZIP-konteinerid täiendavaks tervikluse kontrollimiseks.

Väga oluline on tuvastada sõnumilogi talletamise pikkuse nõue. Pea meeles, et sõnumilogi kasutatakse enda kaitseks, et tõendada, kas teavet on muudetud või mitte. Näiteks kui teave on seotud raamatupidamisandmetega, tuleb seaduse kohaselt neid talletada kuni 7 aastat. Selle nõude teave tuleb hankida äripoolelt.

Sõnumilogi arhiivimisprotseduuri väljatöötamine ja selle teostamine turvalises asukohas väljaspool turvaserverit on üliioluline.

24.3. Sõnumilogi konfiguratsiooni arhiivimiskonfiguratsiooni muutmine

Konfiguratsiooni parameetrid määratletakse INI-failis, milles iga jaotis sisaldab konkreetse turvaserveri komponendi parameetreid.

Sõnumilogi vaikekonfiguratsioon asub failis

```
/etc/xroad/conf.d/addo
ns/message-log.ini
```

Vaikeväärtuste alistamiseks loo või redigeeri faili

```
/etc/xroad/conf.d/loca
l.ini
```

Loo failis jaotis `[message-log]` (kui seda pole veel). Jaotise alguses loenda parameetrite väärtused, üks rea kohta. Näiteks parameetrite `archive-path` ja `archive-max-filesize` konfigureerimiseks tuleb lisada konfiguratsioonifail

```
[message-log]
archive-path=/my/arhci
ve/path/
archive-max-filesize=6
7108864
```

Võimalik on konfigureerida parameetrit `hash-algo-id`. See on algoritm, mida kasutatakse sõnumilogi räsiks. Võimalikud valikud on SHA-256, SHA-384 ja SHA-512. (Vaikimisi SHA-512)

24.4. Aegtembeldamise parameetrid

Võimalik on kasutada järgmisi aegtembeldamise parameetreid.

```
timestamp-immediately
```

Kui väärtuseks on Tõene, luuakse ajatempel sünkroonselt iga taotlus- või vastussõnumi jaoks. See on turvapoliitika, mis tagab ajatempli sõnumi logimise hetkel.

Paremaks käideldavuseks on vaikimisi väärtuseks seatud Väär.

```
timestamp-records-limit
```

Maksimaalne aegtembeldatavate kirjete arv ühes paketis

Selle väärtuse määramisel tuleb arvestada sõnumivahetuse jõudluse (sõnumit minutis) ja turvaserveri aegtembeldamise vahemikuga.

Ilma kindla põhjuseta ei tohi seda parameetrit muuta.

Vaikimisi 10000

```
acceptable-timestamp-failure-period
```

Aeg sekundites, kui pika aja jooksul võib aegtembeldamine nurjuda, enne kui sõnumivahetus turvaserverite vahel peatatakse

Kontrolli keelamiseks on väärtuseks seatud 0.

Vaikimisi 14400

24.5. Arhiivimisparameetrid

Kasutada saad ka järgmisi arhiivimisparameetreid.

`keep-records-for`

Aeg päevades aegtembeldatud ja arhiivitud kirjete hoidmiseks andmebaasis

Vaikimisi 30

`archive-max-filesize`

Arhiivitud failide maksimummaht baitides

Maksimumväärtuseni jõudmine käivitab failide rotatsiooni

Vaikimisi 33554432 baiti (32 MB)

`archive-interval`

Ajavahemik Cron-avaldisena aegtembeldatud kirjete arhiivimiseks

Vaikimisi 0 0 0/6 1/1 * ? * (käivita iga 6 tunni järel)

`archive-path`

Kataloog, kus arhiivitakse aegtembeldatud logikirjed

Vaikimisi `/var/lib/xroad`

`clean-interval`

Ajavahemik Cron-avaldisena arhiivitud kirjete puhastamiseks andmebaasist

Vaikimisi 0 0 0/12 1/1 * ? * (käivita iga 12 tunni järel)

`archive-transfer-command`

Käsk, mis käitatakse pärast (regulaarset) arhiivimistoimingut. See võimaldab konfigureerida välist skripti arhiivifailide automaatseks ülekandmiseks turvaserverist.

Vaikimisi ei tööta.

24.6. Arhiivifail

Kõvakettaruumi säästmiseks soovitatakse arhiivifailid turvaserverist regulaarselt üle kanda (käsitsi või automaatselt).

Arhiivifailid asuvad kataloogis, mille on määranud konfiguratsiooniparameeter `archive-path`. Failinimede vorminguks on mlog-X-Y-Z-.zip, kus

- X on esimese sõnumilogikirje ajatempel (UTC-aeg vormingus AAAAKKPPTTmmss),
- Y on viimase sõnumilogikirje ajatempel (kirjeid töödeldakse kronoloogilises järjestuses) ja
- Z on 10-märgiline tähtnumbriline juhuväärtus.

Arhiivifaili nime näide:

mlog-20150504152559-20150504152559-a7JS05XAJC.zip

24.7. Arhiivifailide ülekandmine turvaserverist

Sõnumilogi pakett pakub arhiivifailide ülekandmiseks abiskripti:

```
/usr/share/xroad/scripts/archive-http-transporter.sh
```

Skript kasutab HTTP/HTTPS protokolli (POST-i meetod, vormi nimi on fail) arhiivifailide edastamiseks arhiiviserversisse.

Skripti kasutamine:

-d, --dir, DIR	Arhiivikataloog Vaikimisi /var/lib/xroad
-r, --remove	Eemaldab transporditud failid arhiivikataloogist.
-k, --key, KEY	Privaatvõtme failinimi PEM-vormingus (TLS) Vaikimisi /etc/xroad/ssl/internal.key
-c, --cert, CERT	Kliendi serdifail PEM-vormingus (TLS) Vaikimisi /etc/xroad/ssl/internal.crt
--cacert, FILE CA	Serdifail partneri kinnitamiseks (TLS) Fail võib sisaldada mitmeid CA-sertifikaate. Sertifikaadid peavad olema PEM-vormingus.
-h, --help	Spikritekst

Arhiivifail on edukalt üle kantud, kui arhiiviserver tagastab HTTP-oleku koodi 200.

Edastamisskripti seadistamiseks alista konfiguratsiooniparameeter `archive-transfer-command` (loo või redigeeri faili `etc/xroad/conf.d/local.ini`). Näiteks:

```
[message-log]
archive-transfer-command=/usr/share/xroad/scripts/archive-http-transporter.sh -r http://my-archiving-server/cgi-bin/upload
```

Sõnumilogi pakett sisaldab testimiseks või arenduseks demo arhiiviserveri CGI-skripti

```
/usr/share/doc/xroad-addon-messagelog/archive-server/demo-upload.pl
```

24.8. Kaugandmebaasi kasutamine arhiivifaili jaoks

Sõnumilogi andmebaas võib asuda väljaspool turvaserverit. Allpool kirjeldatakse kaugandmebaasi skeemi konfigureerimist ja asustamist sõnumilogi jaoks. Eeldatakse, et juurdepääs andmebaasile turvaserverist on konfigureeritud.

1. Loo andmebaasi kasutaja kaugandmebaasi hosti juures.

```
postgres@db_host:~$ createuser -P messagelog_user
```

Sisalda parool uue rolli jaoks: `<messagelog_password>`

Sisesta see uuesti: `<messagelog_password>`

2. Loo sõnumilogi kasutaja andmebaas kaugandmebaasi hosti juures.

```
postgres@db_host:~$ createdb messagelog_dbname -O messagelog_user -E UTF-8
```

3. Kontrolli ühenduvust turvaserverist kaugandmebaasi.

```
user@security_server:~$ psql -h db_host -U messagelog_user
```

```
messagelog_dbname
```

Parool kasutaja `messagelog_user` jaoks: `<messagelog_password>`

psql (9.3.9)

SSL-ühendus (šiffer DHE-RSA-AES256-GCM-SHA384, bitte: 256)

Spikri leidmiseks tipi sõna „Spikker“.

```
messagelog_dbname=>
```

4. Peats uuesti konfigureerimiseks teenus `xroad-proxy`.

```
root@security_server:~ # service xroad-proxy stop
```

5. Konfigureeri andmebaasi ühenduse parameetrid krüptitud ühenduste saamiseks asukohas `/etc/xroad/db.properties`.

```
messagelog.hibernate.jdbc.use_streams_for_binary = true
messagelog.hibernate.dialect =
ee.ria.xroad.common.db.CustomPostgreSQLDialect
messagelog.hibernate.connection.driver_class =
org.postgresql.Driver
messagelog.hibernate.connection.url =
jdbc:postgresql://db_host:5432/messagelog_dbname?
ssl=true&sslfactory=org.postgresql.ssl.NonValidatingFactory
messagelog.hibernate.connection.username = messagelog_user
messagelog.hibernate.connection.password = messagelog_password
```

6. Andmebaasiskeemi asustamiseks installi uuesti pakett `messagelog addon` (see käivitab ka teenuse `xroad-proxy`).

```
root@security_server:~ # apt-get install --reinstall xroad-addon-messagelog
```

24.9. Küsimused

Selle õppetüki läbimiseks otsusta, millised järgmised väited on tõesed.

A. Sõnumilogi funktsiooniks on tõendada X-teel vahetatud tavaliste taotlus- või vastussõnumite vastuvõtmist.
B. Kui `timestamp-immediately` väärtuseks on seatud Tõene, luuakse ajatempel sünkroonselt iga taotlus- või vastussõnumi jaoks.
C. Arhiivifailid asuvad kataloogis, mille on määranud konfiguratsiooniparameeter `archive-path`.

Õigeid vastuseid vaata siit (avanevad uues aknas).