Logid?!

T.Hanga
RIA

Täitsa algusesse...

Meil on:

- operatsioonisüsteemide logid
- Rakenduste logid (ehk ikka on...)
- Muude “asjade” logid (võrguseadmed jms.)

Nad on igal pool masinates laiali...

Ja neid on palju...

Rakendustest ja nende logidest ja seirest...

- Pekske oma arendajaid, et rakendused peavad lisaks oodatud ärifunktsioonidele ka:
  - LOGIMA ja soovitatavalt mõistlikult.
  - SUUTMA SUHELDA seiresüsteemiga
- Nõudke lisaks sellele, et rakendus oleks võimeline logima nii failisüsteemi kui syslogi serverisse.
- Ja kui keegi pakub teile lahenduseks hardcodetud väärtustega lahendusi, siis ... =“#%#!!

Need nõuded peab esitama ja neid peab kaitsma IT ja neist EI TOHI taganeda.

Vahepala asemel...

Murphy seadus on korduvalt tõestanud, et tavaliselt on sul logifaile siis hädasti vaja kui sa oled neist parasjagu ilma jäänud... no ja põhjused on erinevad eks igaüks teab:

- Logrotate on saanud “veidi” optimistlik
- Keegi on “aidanud” logidel kaduda
- Ketas sai täis või läks katki...

Jne.

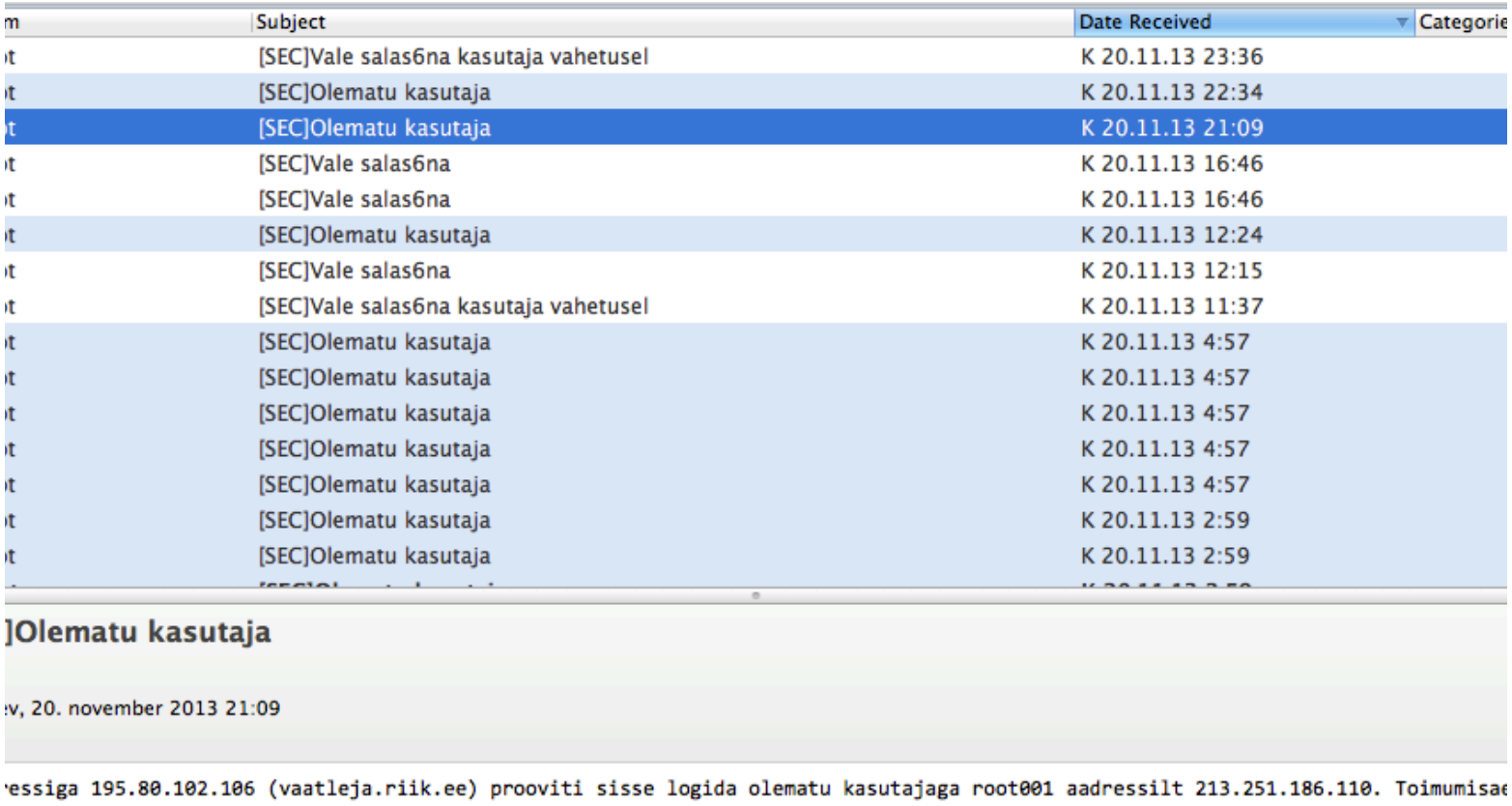
Alustame siis keskele kogumist...

Selleks on vaja:

- keskele üht syslogi oskavat serverit
  - rsyslog või syslog-ng
  - kommertsid.
- Klientide poolele midagi, mille abil saaks logifailid kokkku kraapida ja ära saata:
  - Linuxitel on sisseehitatud võimekus syslogi näol olemas
  - Enamustel kaasaegsetel võrguseadmetel samuti.
  - Windowsid on veidi probleemsemad aga lahenduvad ka:
    - Tasuta agentidega (nt. snare, syslogagent)
    - Kommertstükkidega kaasa tulevate agentidega

Sniik piik – seci rakendamine plussid syslogi serveril

..ja otsesed kasud reaalajas vaadates enda postkasti



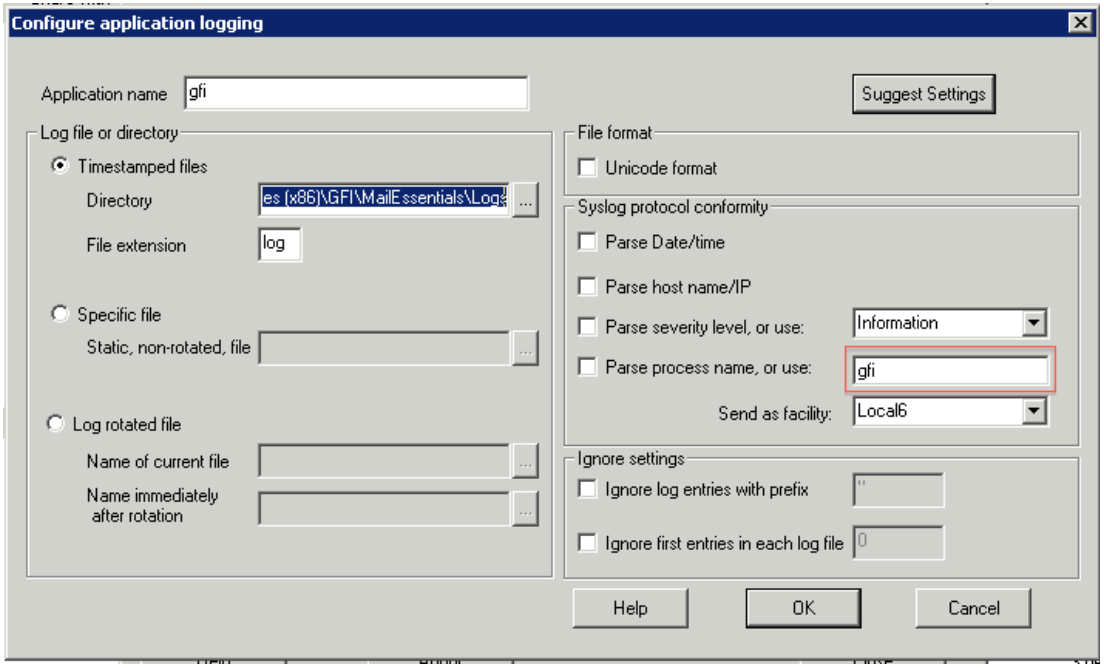
m	Subject	Date Received	Categorie
t	[SEC]Vale salas6na kasutaja vahetusel	K 20.11.13 23:36	
t	[SEC]Olematu kasutaja	K 20.11.13 22:34	
t	[SEC]Olematu kasutaja	K 20.11.13 21:09	
t	[SEC]Vale salas6na	K 20.11.13 16:46	
t	[SEC]Vale salas6na	K 20.11.13 16:46	
t	[SEC]Olematu kasutaja	K 20.11.13 12:24	
t	[SEC]Vale salas6na	K 20.11.13 12:15	
t	[SEC]Vale salas6na kasutaja vahetusel	K 20.11.13 11:37	
t	[SEC]Olematu kasutaja	K 20.11.13 4:57	
t	[SEC]Olematu kasutaja	K 20.11.13 4:57	
t	[SEC]Olematu kasutaja	K 20.11.13 4:57	
t	[SEC]Olematu kasutaja	K 20.11.13 4:57	
t	[SEC]Olematu kasutaja	K 20.11.13 4:57	
t	[SEC]Olematu kasutaja	K 20.11.13 2:59	
t	[SEC]Olematu kasutaja	K 20.11.13 2:59	

]Olematu kasutaja

v, 20. november 2013 21:09

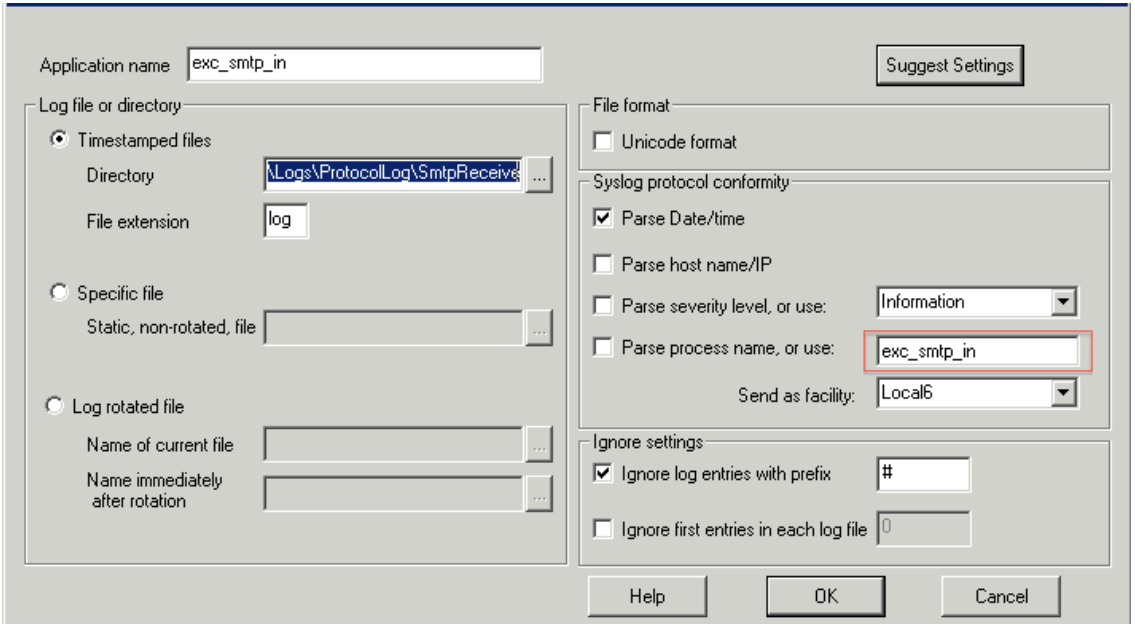
essiga 195.80.102.106 (vaatleja.riik.ee) prooviti sisse logida olematu kasutajaga root001 aadressilt 213.251.186.110. Toimumisae

Sniik piik – exchange ja syslogi agent gfi kallal




```
root@logi:/srv/syslog-prod/hosts/exc1.ria.ee/20131121# tail local6|grep gfi
Nov 21 08:06:02 exc1.ria.ee gfi[info] "11.21.13 08:06:02","IP Whitelist","help@ria.ee","anneli.touart@ria.ee","Kohaletoimeta
Nov 21 08:06:15 exc1.ria.ee gfi[info] "11.21.13 08:06:13","IP Whitelist","help@ria.ee","anneli.touart@ria.ee","Kohaletoimeta
Nov 21 08:06:30 exc1.ria.ee gfi[info] "11.21.13 08:06:29","Whitelist","nagios@aso.ee","rait.prits@ria.ee","Host UP alert for
Nov 21 08:06:30 exc1.ria.ee gfi[info] "11.21.13 08:06:29","Whitelist","nagios@aso.ee","arvi.pihus@ria.ee","Host UP alert for
```

Sniik piik – exchange ja syslogi agent smtp logi kallal




```
root@logi:/srv/syslog-prod/hosts/exc1.ria.ee/20131121# cat local6|grep exc_smtp_in|head
Nov 21 02:04:33 exc1.ria.ee exc_smtp_in[info] #Software: Microsoft Exchange Server
Nov 21 02:04:33 exc1.ria.ee exc_smtp_in[info] SMTP,08D09F157372FD11,0,192.168.2.20:25,10.0.6.220:43146,+,,
Nov 21 02:04:33 exc1.ria.ee exc_smtp_in[info] SMTP,08D09F157372FD11,1,192.168.2.20:25,10.0.6.220:43146,*,SMTPSubmit SMTPAcceptAnySend
Nov 21 02:04:33 exc1.ria.ee exc_smtp_in[info] SMTP,08D09F157372FD11,2,192.168.2.20:25,10.0.6.220:43146,>,220 RIA SMTP Server Ready,
Nov 21 02:04:33 exc1.ria.ee exc_smtp_in[info] SMTP,08D09F157372FD11,3,192.168.2.20:25,10.0.6.220:43146,<,EHLO smtp1a.aso.ee,
Nov 21 02:04:33 exc1.ria.ee exc_smtp_in[info] SMTP,08D09F157372FD11,4,192.168.2.20:25,10.0.6.220:43146,>,250-mail.ria.ee Hello [10.0.
Nov 21 02:04:33 exc1.ria.ee exc_smtp_in[info] SMTP,08D09F157372FD11,5,192.168.2.20:25,10.0.6.220:43146,>,250-SIZE 20971520,
Nov 21 02:04:33 exc1.ria.ee exc_smtp_in[info] SMTP,08D09F157372FD11,6,192.168.2.20:25,10.0.6.220:43146,>,250-PIPELINING,
Nov 21 02:04:33 exc1.ria.ee exc_smtp_in[info] SMTP,08D09F157372FD11,7,192.168.2.20:25,10.0.6.220:43146,>,250-DSN,
Nov 21 02:04:33 exc1.ria.ee exc_smtp_in[info] SMTP,08D09F157372FD11,8,192.168.2.20:25,10.0.6.220:43146,>,250-ENHANCEDSTATUSCODES,
```

Mõtleme kohe logide turvalisusele äkki?

- Krüptoaheldamine.
  - Aheldamist saab teha tasuta ja kohe suvalisele logifailile suvalisel pythoni sõbralikul op süsteemil, kasutades RIA üldotstarbelist logiaheldajat.
  - Kindlasti oskavad seda teha ka kommertstükid
- Ajatembeldamine.
  - Saab kasutada GT lahendust (RIA kasutab).
  - Saab kasutada muid lahendusi.

Näited - /etc/slog/slogd.conf sisu.

```
[securelog]

# Prefix for the output files.
securelog_prefix = /srv/syslog-prod/programs/auth/slog/auth.log


# Comma-separated list of sources.
# Reconfigure these sample sources!
sources = auth

# Output file size in KiB when new file creation is started (default: 4096)
max_filesize = 1024000

# Linking hash algorithm. Supported values are sha256, sha384, sha512
# (default: sha256)
hash_algorithm = sha256

# Source descriptions. Please note that only sources listed in configuration
# value sources (in section securelog) are used.

[source_auth]
# Name of the file to watch.
filename = /srv/syslog-prod/programs/auth/auth.log
```

Näited – GT tembelduse integratsioon aheldaja koodi.

```
global rotate_switch



if file_size >= self.__max_filesize or rotate_switch == 1:

    try:
        self.log_debug("Trying to sign the file:", file_name)
         process = subprocess.call(["gtime", "-s", "-f", file_name, "-o", file_name_timestamp, "-S", "http://gtg.tt.kit/gt-signingservice"])
    except:
        self.log_debug("Some Kind of Very Nasty Exception caught: nothing signed")
```

Näited – aheldatud failid ja sisu.

```
-rw------- 1 root root     3531 Nov 14 00:00 auth.log.6718045.20131113_000005_timestamp
-rw------- 1 root root 16362350 Nov 15 00:00 auth.log.6795777.20131114_000004
-rw------- 1 root root     3459 Nov 15 00:00 auth.log.6795777.20131114_000004_timestamp
-rw------- 1 root root 16576683 Nov 16 00:00 auth.log.6873289.20131115_000016
-rw------- 1 root root     3459 Nov 16 00:00 auth.log.6873289.20131115_000016_timestamp
-rw------- 1 root root 16271192 Nov 17 00:00 auth.log.6951938.20131116_000007
-rw------- 1 root root     3567 Nov 17 00:00 auth.log.6951938.20131116_000007_timestamp
-rw------- 1 root root 16157080 Nov 18 00:00 auth.log.7029080.20131117_000006
-rw------- 1 root root     3459 Nov 18 00:00 auth.log.7029080.20131117_000006_timestamp
-rw------- 1 root root 15768409 Nov 19 00:00 auth.log.7105625.20131118_000006
-rw------- 1 root root     3459 Nov 19 00:00 auth.log.7105625.20131118_000006_timestamp
-rw------- 1 root root 15012338 Nov 20 00:00 auth.log.7180959.20131119_000010
-rw------- 1 root root     3531 Nov 20 00:00 auth.log.7180959.20131119_000010_timestamp
-rw------- 1 root root 15193774 Nov 21 00:00 auth.log.7252894.20131120_000009
-rw------- 1 root root     3495 Nov 21 00:00 auth.log.7252894.20131120_000009_timestamp
```

```
root@logi:/srv/syslog-prod/programs/auth/slog# tail auth.log.7252894.20131120_000009
7325756 sha256 9e40d0c4ba316c7bb5180d25a976735dc7eb9c383355a3605055bdce29c46d5a msg 10.0.9.243 manaja.tt.kit Nov 20 23:59:33 pam_unix(sshd:se
7325757 sha256 813657684a9e2a00cf736f83d72a475911ec6c60ce874ba74be202aa0fcf0c1f msg 10.0.9.243 manaja.tt.kit Nov 20 23:59:33 Received disconn
7325758 sha256 b258c3255512b02e4299ff474cda3e2705c475e10f18baeae5a91ce02043efd9 msg 10.0.9.243 manaja.tt.kit Nov 20 23:59:33 pam_unix(sshd:se
7325759 sha256 38da99006f412dea29fd8884f8cf495dd286cb12483ed3df56d64ca496194b69 msg 10.0.9.243 manaja.tt.kit Nov 20 23:59:33 Accepted publick
7325760 sha256 2c11fb2c8a4ccb4097c8b1bb9bd0cdaec0da9d86a680af56a0cb3e84c8f9e245 msg 10.0.9.243 manaja.tt.kit Nov 20 23:59:33 pam_unix(sshd:se
7325761 sha256 9f7421ead86a66b9b4a043efe7c531c2b7d898dd6b0b6aac8707f802c207fb34 msg 10.0.9.243 manaja.tt.kit Nov 20 23:59:34 Received disconn
7325762 sha256 222d348f1358d921a315c735a9ad04ee1304aba16dcab8e40b39187a1fb42849 msg 10.0.9.243 manaja.tt.kit Nov 20 23:59:34 pam_unix(sshd:se
7325763 sha256 20f7485be500e6553096bdc48b3da5b4f62dd6d61bc99882f5939f2e0c0c11fb msg 10.0.9.3 rtm2.tt.kit Nov 20 23:59:37  _zabbix : TTY=unkno
7325764 sha256 052c29f2d7bed123b461b2c3b71b4e66c2eb285b74c59527ba8e01ee7321d981 msg 10.0.9.2 rtm1.tt.kit Nov 20 23:59:50  _zabbix : TTY=unkno
7325765 sha256 16b3459b196c8f4e67d30b330419cddf7d4125c9dfaff37a5dffdbd69e34cde8 msg 10.0.6.93 val1b.avalik.kit Nov 21 00:00:01 Accepted publ
```

Näited – kontrollime ahelat ka? No ikka :)

```
dwalin@logi:~$ /opt/dwalin/slog/slogverify.py -l /opt/dwalin/auth.log.7325765.20131121_000008

=== Analyzing file /opt/dwalin/auth.log.7325765.20131121_000008 ===
First record in this file has sequence number of 7325765
Last record in this file has sequence number of 7332595
```

```
dwalin@logi:~$ /opt/dwalin/slog/slogverify.py -l /opt/dwalin/auth.log.7325765.20131121_000008_mod

=== Analyzing file /opt/dwalin/auth.log.7325765.20131121_000008_mod ===
First record in this file has sequence number of 7325765
Error on line 11: Invalid linking info, log line probably tampered
Last record in this file has sequence number of 7332482
```

Aga võrdleme GT templit ja ahelat? Vabalt!

```
root@logi:/opt/dwalin# gtime -v -f auth.log.988734.20130418_000009 -i auth.log.988734.20130418_000009_timestamp
GT_PUBLIC_KEY_SIGNATURE_PRESENT: The PKI signature is present in the timesignature.
GT_DOCUMENT_HASH_CHECKED: The timesignature was checked against the document hash.
Timesignature looks fine, signed by "GT : GT : Riigi Infosüsteemi Amet" at 2013-04-19 00:00:03 EEST.
```

Lingid ja märksõnad

- Sec - http://simple-evcorr.sourceforge.net/
- GT - http://www.guardtime.com/
- Slog – https://www.ria.ee/public/slog.zip

- Linuxile
  - Rsyslog, Syslog-ng
- Windowsile
  - Snare (http://www.intersectalliance.com/projects/SnareWindows/)
  - Syslogagent (http://www.syslogserver.com/syslogagent.html)

Side lõpp :)