



IT KOLLEDŽ
TALLINNA TEHNIKAÜLIKOOL

Süsteemi jälgimine

Operatsioonisüsteemid ja nende haldamine ICA0001

Edmund Laugasson

edmund.laugasson@taltech.ee

https://wiki.itcollege.ee/index.php/User:Edmund#eesti_keeles

Käesoleva dokumendi paljundamine, edasiandmine ja/või muutmine on sätestatud tühega järgnevatest litsentsidest kasutaja valikul:

* GNU Vaba Dokumentatsiooni Litsentsi versioon 1.2 või uuem

* Creative Commons Autorile viitamine + Jagamine samadel tingimustel 4.0 litsents (CC BY-SA)



Süsteemide jälgimine

- Töötavaid teenuseid tuleb jälgida
 - Kui teenus ei tööta korrektselt, siis esimese asjana tuleks uurida teenuse logfaile
 - Teenuste logifailide jälgimiseks kasutatakse tihti spetsiaalseid rakendusi (võivad olla monitoorimise süsteemi osad või ise kirjutatud *parser* programmid)
 - Teenuste logi annab võimaluse hinnata teenuse mahtude (andmed/kasutajad/ühendused) kasvu pikemas perspektiivis. Selle info alusel saab otsustada, kas vajatakse lisa riistvara/tarkvara.

Logide tüübid

- Teenused kirjutavad oma tegevuse kohta logifaili
- Eristada võib rakenduse logi ja vealogi
 - **Application** log – rakenduse logi on ette nähtud rakenduse/teenuse tegevuste salvestamiseks
 - **Error** log – vealogi on ette nähtud rakenduse töös esinevate vigade salvestamiseks
- Süsteemide administreerija huvitub eelkõige vealogidest
- Rakenduste administreerija huvitub eelkõige rakenduse logis olevast infost

Logifailide kirjutamisviisid

- Rakendus võib kirjutada logifaile (*application log* ja *error log*) või kasutada *syslog* teenust logiridade kirjapanemiseks
- *Log Level* määrab ära rakenduse logifaili kirjutamise põhjalikuse
 - Rakenduse silumisel on logi tihti tihedam, kui hilisematel rakenduse elutsükli faasidel
- Reeglina saab konfigureerida logifailide asukohta ja *log level* määrangut

Syslog

- Rakendus võib kirjutada oma logfaile või kasutada *rsyslog* teenust logfailide kirjutamiseks
- Võivad olla ka muud – syslog-ng, metalog jne
- Syslog konfiguratsioon on Ubuntu puhul failides
 - */etc/rsyslog.d/50-default.conf*
 - */etc/rsyslog.conf*
- Syslog võimaldab saata logiteateid teistele syslog serveritele ja tsentraliseerida logifailide kogumist ja uurimist

Syslog'i seaded

- Igal syslog formaadis logreal on
 - **Valdkond** *facility*
 - **Tõsidusaste** *priority* või *severity*
- Valdkonna ja tõsidusastme alusel saab seadistuste failis määrata mida ja kuhu logifaili salvestatakse
 - **[facility-level].[severity-level] [destination]**
- Valdkond määrab teenuse liigi (kern, mail, lpr jne)
- Tõsidusaste näitab teate prioriteeti (kas on tegu kriitilise teate või infoga)

Tõsidusasted (RFC5424)

- 0 *Emergency (emerg)* – süsteem maas!
- 1 *Alerts (alert)* – süsteem nõuab kohest tegutsemist
- 2 *Critical (crit)* – kriitiline situatsioon
- 3 *Errors (err)* – veasituatsioon
- 4 *Warnings (warn)* - hoiatus
- 5 *Notification (notice)* – tavaline oluline teade
- 6 *Information (info)* - tavainfo
- 7 *Debug (debug)* – programmi silumise info

/etc/rsyslog.d/50-default.conf

- kern.* -/var/log/kern.log
 - kerneli kõik teated salvestatakse kern.log faili
- mail.* -/var/log/mail.log
 - Mail teenuse kõik teated salvestatakse mail.log faili
- Erineva kriitilisusega teateid võib salvestada erinevatesse failidesse
 - mail.info -/var/log/mail.info
 - mail.warn -/var/log/mail.warn
 - mail.err /var/log/mail.err

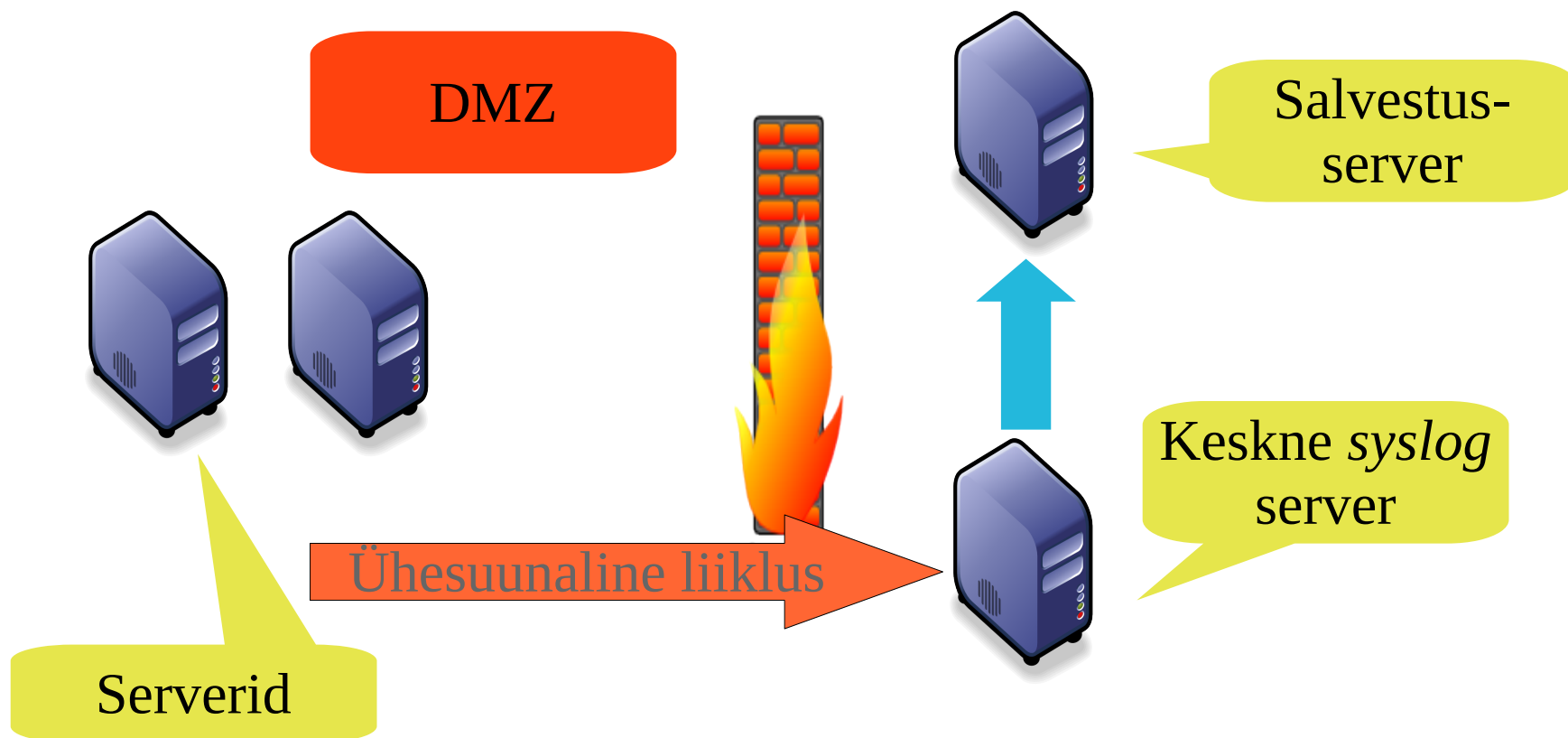
/etc/rsyslog.d/50-default.conf

- Logi saab saata ka teise masinasse, näiteks kesksesse log serverisse
- `*.* @logiserver:port`
 - Saadame kõik teated (`*.*`) serverisse *logiserver*
- `kern.* -/var/log/kern.log`
 - - märk näitab, et ei pea sünkroniseerima iga log teadet (võimaldab ketta koormust vähendada, kuid samas ei ole garantiid, et teated kettale jõuavad), vt [allikas1](#), [allikas2](#)

Logifailide tsentraliseerimine

- Vahele on kasulik töödelda log failide infot ühes või mitmes **keskses** serveris
- Sellisel puhul häälestatakse syslog server saatma logiteateid teise serverisse
- Kasulik, kuna saab töödelda ja arhiveerida ühes kohas
- Võimaldab vähendada ohtu, et kräkker kustutab peale pahategu oma mustad jäljed
- Võimaldab masina hävimisel saada infot, mis võis rikke põhjustada

Syslog server



Tsentraliseerimine

- Tihti saadetakse logiread kesksesse serverisse ja samal ajal salvestatakse ka kohalikule kettale
- Kohalikule kettale salvestamine on vajalik, kuna keskne server ei pruugi olla alati kättesaadav (võrgu kadumine või muu viga)

Syslog probleemid

- Tegu on vana protokolliga, kuhu tuleb lisada
 - Ridade krüpteerimine nende edastamisel teistele serveritel
 - TCP (syslog-ng saab sellega kenasti hakkama)
 - Vahel on vaja kontrollida sõnumi autentsust ja terviklikkust (protokolli stabiilne versioon on selle koha pealt nõrk)

Syslog ja Windows

- Windows võimaldab logiteateid saata teise süsteemi, kasutades erinevaid vahendeid ([SCOM](#), [NTsyslog](#), [winlogd](#), vanasti [MOM](#)), siin üks [NTsyslog näidis](#)
- Samas võib olla oluline ühtse logijälgimisüsteemi olemasolu
- Windows süsteemidele
[on tehtud palju syslog teenuse programme](#)
 - populaarne on ka vabavaraline [SNARE programm](#)
 - Võimalusterohke
 - Tasuta

Vajadus

- Halb on juhus, kus süsteemiadministraator saab rikkest teada kasutajalt või ülemuselt.
 - Kasutaja võib arvata, et süsteem on maas ja asjaga tegeletakse kuid see ei pruugi olla tegelikkus.
 - Kui kasutajad on harjunud süsteemide riketest teatama, siis võib rikke korral tekkida infokanalite ummistus (kõik helistavad ja ütlevad, et veebiserver on maas :)
- Lisaks riketele tuleks jäädvustada ka süsteemi normaalse töö taastamise ajamoment
 - SLA jälgimise üks osa.



Mahtude jälgimine

- Log faile analüüsidest saab leida teenuse kasutamise trende
- Näiteks saab analüüsida veebiserveri kasutust ja serveri koormust
- See võimaldab planeerida riistvarahanke vajadusi ja jälgida olemasolevat varu
- Mahtude haldus lubab ennustada IT varade vajadust tulevikus

Monitooring (seire) 1

- Arvutisüsteemid töötavad tõrgetega
 - Pole olemas 100% veakindlaid arvutisüsteeme
- Tõrgetest võib teada saada mitmel moel
 - Kasutaja helistab
 - Süsteem teavitab avastatud tõrkest
 - Süsteem teavitab, et tõrge võib toimuda
- SLA on vajalik, kuid keegi peab selle täitmist ka jälgima. Vastasel juhul pole SLA lepingul mõtet.

Monitooring (seire) 2

- IT süsteemide monitooring ehk seire
 - Süsteemi töö reaalajas jälgimine
 - Jälgitakse süsteemi kriitilist funktsionaalsust
 - Kuna on vaja reageerida süsteemi riketele
 - Jälgitakse süsteemi ressursikasutust
 - Kuna on vaja ennustada mahtude kasvu ja IT süsteemide ressurside tulevikuvajadust
- Monitoorimissüsteem muutub iga lisatud teenuse või riistvara- ja tarkvaraühiku puhul
 - Süsteemi muudatused nõuavad jälgimise muutmist

Monitooring

- Jälgimine võib toimuda
 - Aktiivselt – monitooringuprogramm teeb päringuid teenuse kriitilise funktsionaalsuse toimimise testimiseks
 - Funktsionaalsus, teenuse kosteaeg, staatus
 - Passiivselt – monitooringu programm jälgib serveri logifaile, teenuseid ja muid kaudseid parameetreid
 - Kettamaht, protsessori kasutus, IO, veakoodide esinemine logides

Teenuste aktiivne seire

- Teenuste aktiivsel monitoorimisel tuleb pöörata tähelepanu järgmistele aspektidele:
 - Funktsionaalsus, mida jälgitakse
 - Päringute intervall
 - Seire ei tohi süsteemi üle koormata
 - Intervall ei tohi olla nii harv, et SLA parameetrite mõõtmise pole piisavalt täpne
 - Intervall peaks sõltuma kalendrist ja kellast
 - Kosteaaeg (latency)
 - Lisaks äriefunktsioonidele võib jälgida ka süsteemi reageerimise kiirust, kuna seda võib nõuda teenusleping

Teenuste passiivne seire

- Jälgitakse OS parameetreid ja logifaile
 - Vaba kettaruum
 - Veakoodid/mustrid log failides
 - IO/CPU/RAM parameetrid

Teenuste seire

- Monitoorimise süsteemi loomisel ja seadistamisel tuleb arvestada:
 - Vea korral ei tohiks administraatorit erinevate teadetega üle koormata
 - Süsteem peab arvestama sõltuvustega
 - Süsteem peab võimaldama seadistada planeeritud hoolduse aega, mille jooksul teated pole kriitilised
 - Tasub testida seriesüsteeme veendumaks, et häire korral alarmeeritakse haldureid

Teavitamine

- Kasutatakse erinevaid vahendeid
 - SMS
 - e-post
 - helisignaal (suhteliselt häiriv)
 - ekraanidel aktiivselt info eri värvides
- Erinevatele häiretele seatakse vastavusse erinev tegevus
 - Näiteks töövälisel ajal võib teavitamise viis olla erinev teenuse tööajal kasutatavast
- Üks sündmus ei pruugi rakendada teavitust (mitme sündmuse esinemine lühikese aja jooksul)
- Teavituste toimimist tuleb testida!

Kasutatav tarkvara

- Erinevaid monitooringu tarkvarapakette on palju
- Valikul tuleks jälgida
 - Jälgimisfunktsionaalsust
 - Mis tüüpi teenuseid/servereid/võrguseadmeid suudab jälgida?
 - Kas saab ise lihtsalt laiendada?
 - Teavitusfunktsionaalsust
 - Kuidas süsteemiadministraatorit teavitatakse?
 - Haldust
 - Kas tarkvara on keskselt hallatav ja seadistatav?
 - Ühilduvust teiste seadmete ja süsteemidega

Tarkvara

- Nagios <https://wiki.itcollege.ee/index.php/Nagios>
 - vt ka <http://alternativeto.net/software/nagios/>
- Zabbix <https://wiki.itcollege.ee/index.php/Zabbix>
- SCOM, MOM
https://wiki.itcollege.ee/index.php/Microsoft_System_Center_Operations_Manager
- Munin <https://wiki.itcollege.ee/index.php/Munin>
- Cacti <https://wiki.itcollege.ee/index.php/Cacti>
- Zenoss <https://wiki.itcollege.ee/index.php/Zenoss>
- Xymon <https://en.wikipedia.org/wiki/Xymon>
- vt ka https://wiki.itcollege.ee/index.php/Visualiseerimise_materjalid

OS jälgimine

- **top, htop, ps** – protsessitabeli, mälu ja saaleala jälgimine; **pmap** üksiku protsessi info
- **free** – mälu ja saaleala
- **df** – vaba kettaruum
- **iostat** – I/O jälgimine
- **vmstat** – mälu, protsessori, saalimise ja katkestuste jälgimine
- **netstat, iptraf, iptraf-ng** – võrgu jälgimine
- **uptime** – tööaja jälgimine (SLA)
- **w** – kasutajate jälgimine

<http://www.cyberciti.biz/tips/top-linux-monitoring-tools.html>

Teenuste monitooring

- MySQL
 - [mysqladmin extended](#)
 - [mysqladmin processlist](#)
 - [mtop](#)
 - turvamiseks [GreenSQL](#)
- IPS/IDS/NSM
 - Suricata <https://wiki.itcollege.ee/index.php/Suricata>
 - Snort <https://wiki.itcollege.ee/index.php/Snort>
 - Sguil <https://wiki.itcollege.ee/index.php/Sguil>
 - [jne](#)
- erinevad vahendid (sh atop, iftop, apachetop, powertop, latencytop)
 - https://wiki.itcollege.ee/index.php/J%C3%B5udluse_j%C3%A4lgimine_ja_probleemilahendus_k%C3%A4surea_utiliitide_abil

Nagios

- Nagios on levinud vabavaraline monitooringu programm teenuste, serverite ja võrguseadmete käideldavuse jälgimiseks
 - Teenuste jälgimine (SMTP, HTTP, SSH, FTP, ICMP jne)
 - Host ressursside jälgimine (HDD, CPU Load jne)
 - Plugin arhitektuur
 - Käideldavus on skaleeritav
 - Toetajaskond on suur ja aktiivne
 - GPL litsents

Veel vahendeid süsteemi jälgimiseks

- SEM – *Security Event Management*
- SIEM - *Security Information and Event Management*
 - Trailbot <https://trailbot.io/>
 - OSSIM <https://sourceforge.net/projects/os-sim/>
 - AlienVault <https://www.alienvault.com/> (vt alternatiivid)
 - Security Onion <https://securityonion.net/>
 - OpenSmart <http://opensmart.sourceforge.net/>
 - TripWire <https://sourceforge.net/projects/tripwire/>
 - Rootkit Hunter <https://sourceforge.net/projects/rkhunter/>
 - Splunk <http://www.splunk.com/> (vt ka alternatiivid)
 - Unhide <https://sourceforge.net/projects/unhide/>

Viiteid

- https://wiki.itcollege.ee/index.php/Log_failid_Ubuntus
- <https://wiki.itcollege.ee/index.php/Logwatch>
- <https://wiki.itcollege.ee/index.php/Syslog>
- <https://help.ubuntu.com/community/LinuxLogFiles>
- <http://xmodulo.com/configure-syslog-server-linux.html>
- https://wiki.itcollege.ee/index.php/Keskse_logihalduse_s%C3%BCsteem_Splunk_baasil
- http://wiki.rsyslog.com/index.php/Configuration_Samples
- Syslog standardi viimased muutused
 - <http://tools.ietf.org/wg/syslog/>
- Monitooringutarkvara võrdlustabel
 - http://en.wikipedia.org/wiki/Comparison_of_network_monitoring_systems
- Monitooringutarkvara nimekiri
 - <http://www.slac.stanford.edu/xorg/nmtf/nmtf-tools.html>
- Populaarne monitooringutarkvara Nagios
 - <http://www.nagios.org/>

- syslog:
 - [arch wiki](#)
 - [gentoo wiki](#)
 - [Wikipedia](#)

System Center 2012 Management Pack
for UNIX and Linux Operating Systems
<http://www.microsoft.com/en-us/download/details.aspx?id=29696>

IDS

https://en.wikipedia.org/wiki/Intrusion_detection_system

Küsimused? Tänan tähelepanu eest!



IT KOLLEDŽ
TALLINNA TEHNIKAÜLIKOOL



TTÜ IT KOLLEDŽ

Raja 4C, 12616 Tallinn

tel +372 628 5800

info@itcollege.ee

<http://www.itcollege.ee/>



IT KOLLEDŽ
TALLINNA TEHNIKAÜLIKOO

Süsteemi jälgimine

Operatsioonisüsteemid ja nende haldamine ICA0001

Edmund Laugasson

edmund.laugasson@taltech.ee

https://wiki.itcollege.ee/index.php/User:Edmund#eesti_keeles

Käesoleva dokumendi paljundamine, edasiandmine ja/või muutmine on sätestatud ühega järgnevatest litsentsidest kasutaja valikul:
* GNU Vaba Dokumentatsiooni Litsentsi versioon 1.2 või uuem
* Creative Commons Autorile viitamine + Jagamine samadel tingimustel 4.0 litsents (CC BY-SA)

Küsimused? Tänan tähelepanu eest!



IT KOLLEDŽ
TALLINNA TEHNIKAÜLIKOO



TTÜ IT KOLLEDŽ
Raja 4C, 12616 Tallinn
tel +372 628 5800
info@itcollege.ee
<http://www.itcollege.ee/>