Estonian Information Technology College

System monitoring

Operating systems I800

Edmund Laugasson
edmund.laugasson@itcollege.ee

There has been used materials from Margus Ernits, Katrin Loodus when creating current slides.

System monitoring

- Running services must be monitored
  - If the service is not working properly, then the first thing you should investigate are the service log files
  - For monitoring services log files there are often used specialized applications (which may be a self-monitoring system components or self-written parser programs)
  - Services log files will provide an opportunity to assess the service (data / users / associations) growth in the long term. This information can help you decide whether there is a need for additional hardware / software.

Types of logs

- Services write its activity log
- There can be distinguish the application and error log
  - Application log – is intended to record application / service activities
  - Error log – is intended to record application / service errors
- sysadmin is interested in error logs particularly
- apps administrator is interested in the application log particularly

The ways log files are written

- The application can write log files (application log and error log) or use the log lines of syslog service to write down
- *Log level* will determine the log file writing depth
  - Application log for debugging is often denser than in the later phases of the application life cycle
- Usually you can configure the log file location and log level setting

Syslog

- Application can write own log files or use the *rsyslog* service
- There can be different programs – syslog-ng, metalog etc
- Syslog configuration in Ubuntu:
  - /etc/rsyslog.d/50-default.conf
  - /etc/rsyslog.conf
- Syslog can send log messages to another syslog servers and centralize the collection and research of log files

Syslog’i settings

- every syslog format line has
  - Facility *(area)*
  - Priority or *severity*
- Based on facility and priority there can be configured in settings file what and where to log file there will be saved
  - **[facility-level].[severity-level] [destination]**
- Facility determines the type of service (Kern, mail, lpr, etc.)
- Severity indicates the priority of the message (whether it is a critical notification or information)

Priority levels (RFC5424)

- 0 *Emergency (emerg)* – system down!
- 1 *Alerts (alert)* – the system requires immediate action
- 2 *Critical (crit)* – critical situation
- 3 *Errors (err)* – error situation
- 4 *Warnings (warn)* - warning
- 5 *Notification (notice)* – ordinary important message
- 6 *Information (info)* – ordinary information
- 7 *Debug (debug)* – program debug information

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

- kern.* -/var/log/kern.log
  - all kernel messages will be saved into kern.log file
- mail.* -/var/log/mail.log
  - all mail service messages will be saved into mail.log file
- Messages with different criticality can be stored in different files
  - mail.info -/var/log/mail.info
  - mail.warn -/var/log/mail.warn
  - mail.err /var/log/mail.err

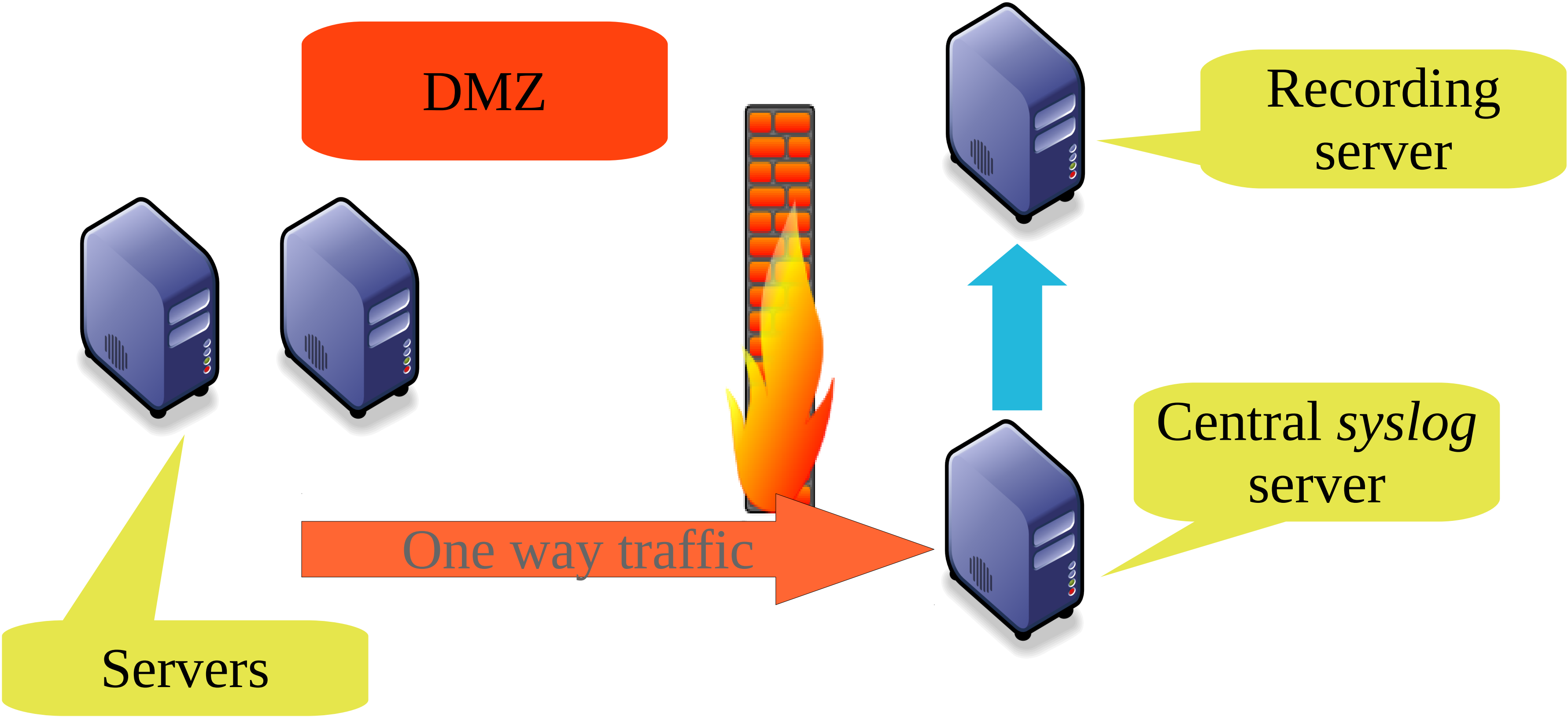
/etc/rsyslog.d/50-default.conf

- The log can be sent also to another machine, e.g. to the central log server
- *.*   @@logserver:port
  - will send all messages (*.*) to the *logserver*
- *kern.*   -/var/log/kern.log*
  - the minus (-) shows that there is no need to log every message (allows to reduce the load of hard disk but there is no guarantee that messages will be stored on the disk), see source1, source2

Centralizing the log files

- Sometimes it is useful to process the log file data in one or more central server
- In this case the syslog server is tuned to send log messages to another server
- Useful as the processing and archive can be handled in one place
- Allows you to reduce the risk of the log file deletion after cracker has breaked in
- Enables to obtain the information about the cause of failure in case of machine malfunctioning

Syslog server



DMZ – demilitarized zone, https://en.wikipedia.org/wiki/DMZ_(computing)

Centralizing

- Often, the log lines are sent to the central server, and at the same time are also stored in the local disk
- To save local disk is needed because the central server may not always be available (network loss or any other error)

Syslog problems

- It is an old protocol, where must be added
  - Rows encryption when transferring them to other servers
  - TCP (syslog-ng can handle it nicely)
  - Sometimes it is necessary to verify the authenticity and integrity of the message (protocol stable version is weak in that case)

Syslog and MS Windows

- MS Windows allows to send log messages to another system, using different tools for that (SCOM, NTsyslog, winlogd, in old times MOM), here is one example of NTsyslog
- However, it can be important to the existence of a single log monitoring system
- for MS Windows systems there has been many syslog service programs created
  - there is also popular the free software SNARE program
    - many features
    - free

The need

- Poor is the case when the system administrator will be informed about system failure by user or boss
  - A user may assume that the system is down and system administrator is dealing with that but this may not be the reality.
  - If users are accustomed to report systems malfunction, the blockage of information channels may occur (all users are calling and saying that the web server is down)
- In addition of failures also the time of restoring system normal state should be recorded
  - part of SLA (*Service Level Agreement*) monitoring

Volume monitoring

- By analyzing log files there can be found trends about service usage
- For example, you can analyze Web server usage and server load
- This allows you to plan hardware procurement needs and monitor existing stocks
- Volumes management allows predict the IT assets need for the future

Monitoring

- Computer systems are running with issues
  - There is no 100% error-free computer system
- Information about errors can be retrieved in several ways
  - user will call
  - systemm will announce about discovered failure
    - system may also announce about upcoming failure
- SLA is necessary but someone has to monitor compliance with it. Othewise the SLA agreement makes no sense.

Monitoring

- IT systems monitoring consists
  - System work monitoring in real-time
  - The system critical functionality is monitored
    - Since it is necessary to respond to the failure of the system
  - The system resource usage is observed
    - Since it is necessary to predict the growth and the need for resources for the future of the IT systems
- Monitoring system will change after adding each service or unit of hardware and software
    - The system changes require tracking change

Monitoring

- Tracking can take place
  - Actively - monitoring program will make a critical service requests to test the critical functionality of the service
    - Functionality, service latency, status
  - Passively - monitoring program monitors server log files, services and other indirect parameters
    - disk volume, processor use, I/O, fault code occurrence in log files

Active monitoring services

- In case of active monitoring of a service, there should be paid attention to the following aspects:
  - Functionality to be monitored
  - Query interval
    - The monitoring system should not overload the system
    - The interval should not be so rare that there is not enough accurate measurement of SLA parameters
    - The interval should depend on the calendar and clock
  - Latency
    - In addition to business functions there can be also tracked the system response speed, as it may be required by a service contract

Passive monitoring services

- OS parameters and log files are monitored
  - Free disk space
  - Error codes, patterns in the log files
  - I/O, CPU, RAM parameters

Monitoring services

- When creating and configuring monitoring system there should be considered:
  - In case of error, the administrator should not be overloaded with various messages
  - The system must take into account the dependencies
  - The system must allow to configure scheduled maintenance time during which the posts are not critical
  - It is worth to pay attention for testing of the monitoring systems to make sure that in case of alarm the messages are delivered to the operators

Informing

- There are used different ways
  - SMS
  - e-mail
  - sound signal (rather disturbing)
  - actively displays information in different colors
- Different alarms are set to a different activity
  - For example, during non-working hours could be different notification service than used during business hours
- One event may not produce the notification (occurrence of several events in a short period of time)
- Notification must be tested to ensure its operation!

Software for monitoring

- A variety of monitoring software packages are available
- When selecting there should be watched
  - monitoring functionality
    - What type of services, servers, network devices will be able to follow?
    - Can easily expand yourself?
  - Reporting functionality
    - How the system administrator will be informed?
  - Management
    - Whether the software is centrally managed and configured?
  - Compatibility with other devices and systems

Software for monitoring

- Nagios https://en.wikipedia.org/wiki/Nagios
  - alternatives http://alternativeto.net/software/nagios/
- Zabbix https://en.wikipedia.org/wiki/Zabbix
- SCOM, MOM https://en.wikipedia.org/wiki/System_Center_Operations_Manager
- Munin https://en.wikipedia.org/wiki/Munin_(software)
- Cacti https://en.wikipedia.org/wiki/Cacti_(software)
- Zenoss https://en.wikipedia.org/wiki/Zenoss_Core
- Xymon https://en.wikipedia.org/wiki/Xymon
- see also https://en.wikipedia.org/wiki/Comparison_of_network_monitoring_systems

Monitoring operating system

- top, htop, ps – processes, memory, swap monitoring;
- pmap single process information
- free – memory and swap
- df – free disk space
- du - estimate file space usage
- iostat – I/O monitoring
- vmstat – memory, processor, swapping and interrupts monitoring
- netstat, iptraf, iptraf-ng – network monitoring
- uptime – monitoring working time (SLA)
- w – monitoring users

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

Monitoring services

- MySQL
  - mysqladmin extended
  - mysqladmin processlist
  - mtop http://mtop.sourceforge.net/
  - for securing GreenSQL, see also alternatives http://alternativeto.net/software/greensql/
- IPS/IDS/NSM
  - Suricata https://en.wikipedia.org/wiki/Suricata_(software)
  - Snort https://en.wikipedia.org/wiki/Snort_(software)
  - Sguil https://en.wikipedia.org/wiki/Sguil
  - etc
- different tools (sh atop, iftop, apachetop, powertop, latencytop)
  - ENG https://www.serverdensity.com/monitor/linux/how-to/ , https://en.wikipedia.org/wiki/Comparison_of_S.M.A.R.T._tools
  - EST https://wiki.itcollege.ee/index.php/J%C3%B5udluse_j%C3%A4lgimine_ja_probleemilahendus_k%C3%A4surea_utiliitide_abil

Nagios

- Nagios are common in open source monitoring program for service, servers and network devices to monitor the availability
  - monitoring services (SMTP, HTTP, SSH, FTP, ICMP jne)
  - monitoring host resources (HDD, CPU load etc)
  - plugin architecture
  - availability is scalable
  - has a large and active community
  - GPL licence
- sysadmin’s proverb:
  - Nagios does not believe in tears
    - EST http://sysadminnid.tumblr.com/

More tools for system monitoring

- 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/

References

- EST https://wiki.itcollege.ee/index.php/Log_failid_Ubuntus
- EST https://wiki.itcollege.ee/index.php/Logwatch
- EST https://wiki.itcollege.ee/index.php/Syslog
- https://help.ubuntu.com/community/LinuxLogFiles
- http://xmodulo.com/configure-syslog-server-linux.html
- EST https://wiki.itcollege.ee/index.php/Keskse_logihalduse_s%C3%BCsteem_Splunk_baasil
- http://wiki.rsyslog.com/index.php/Configuration_Samples
- Syslog standard last changes http://tools.ietf.org/wg/syslog/
- Comparison of network monitoring software
  - http://en.wikipedia.org/wiki/Comparison_of_network_monitoring_systems
- One list of network monitoring tools
  - http://www.slac.stanford.edu/xorg/nmtf/nmtf-tools.html
- Popular monitoring software 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

References

- https://en.wikipedia.org/wiki/Intrusion_detection_system
- https://en.wikipedia.org/wiki/Host-based_intrusion_detection_system_comparison
- https://www.serverdensity.com/monitor/linux/how-to/

Questions?

Thank you for your attention!