Syslog Server

Eddie Aronovich

School of CS

Tel-Aviv University

www.eu-egee.org

Table of context

- Motivation
- Possible attitudes
- Possible solutions & Implementations

How good is our memory ?

Count the number of ball passes between

the

WHITE

players only !

Motivation – why logging ?

- Human memory is a poor storage device
- Large systems are too complex
- Incidents are reported retroactively
- Law (or other authority) might enforce logging
- Logs show trends and anomalies

Project requirements

- **CE: "**The *gatekeeper* logfile (usually */var/log/globus-gatekeeper.log)* should be retained."

- **SE**: "*The gridftp* service should be configured to log input and output transfers (*-i –o* options) with verbose logging (*-l –L* options) and the logfiles (usually */var/log/globus-xferlog, /var/log/gsiwuftpd.log)* retained."

- **Batch system:** "should include the following data for each job –
  - **the batch system job identifier**
  - **the location (address/name) of the machine(s) used**
  - **the time the job was started**
  - **the time the job ended (or duration)**
  - **the command executed.**

  In cases where the batch system data is not available to the *jobmanager,* the batch system logfiles should be retained separately and include the information listed

- **GDB**: following data be retained by **all LCG-1 sites** for a **minimum period of 90days.**
  - ***Jobmanager* and/or *gatekeeper* logfiles (section 2.3 above).**
  - **Data transfer logs (section 2.4 above).**
  - **Batch system and process activity records (section 2.5 above).**

- **RB (WMS):** "*Security Group will make recommendations for audit data retention at the RB in the future."*

More at: LCG_Audit_Requirements

Why centralized logging ?

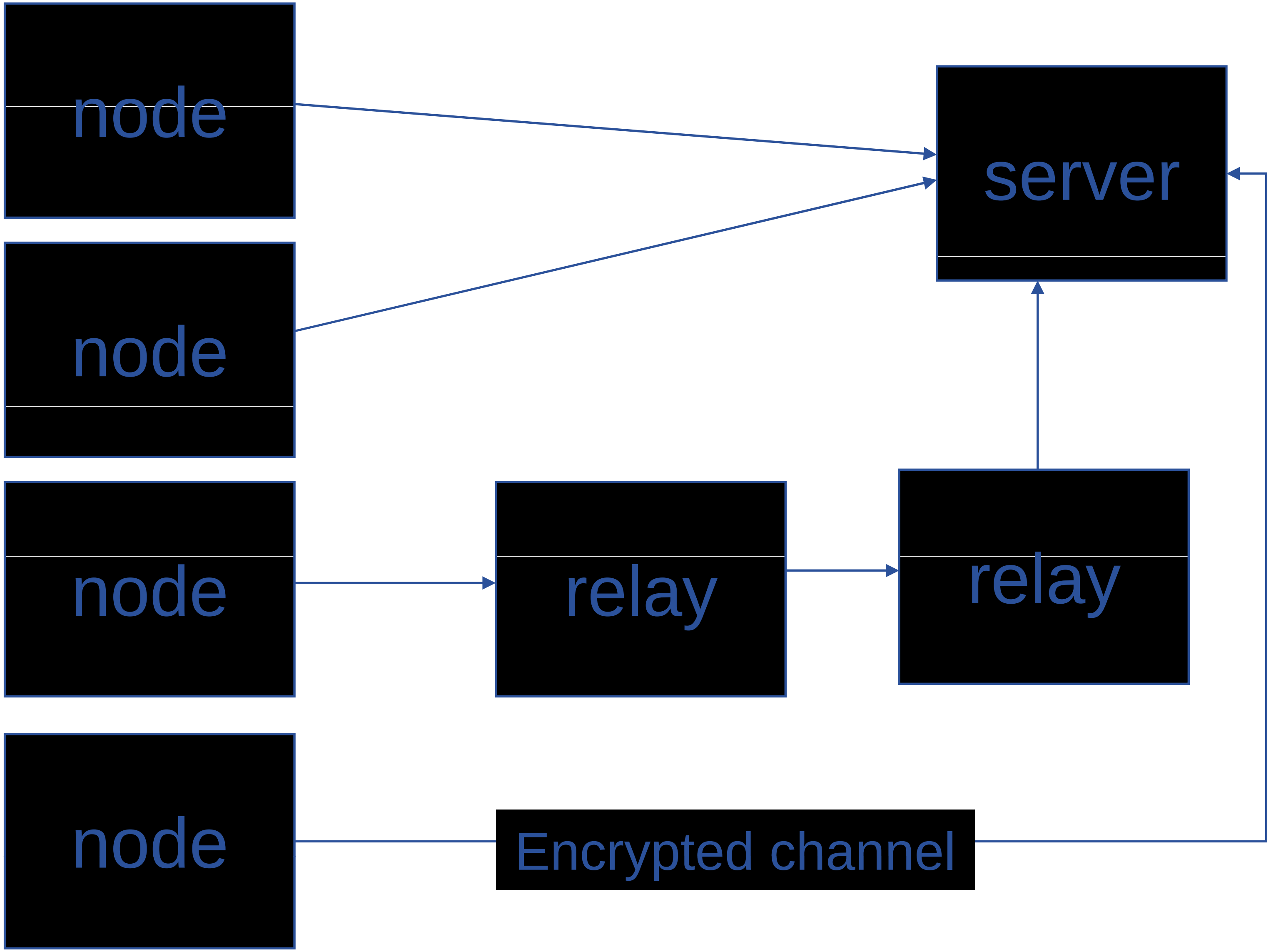
- Vulnerability of local logs
- Accessibility to information - Searching in one place is easier
- Most of us prefer to log all and search later
- Analyzing is easier (manual & automatically)
- Information from several sources gives better picture
- There are lot of logs (system, fw, ids, web servers, etc.)

RFC's

- RFC **3164 - The BSD** Syslog **Protocol** **(informational)**
- RFC **3195 - Reliable Delivery for** syslog (std track)

And other are in preparation mode…

Syslog mechanism



How is it implemented ?

- **Changes needed at server:**
  - Install syslog server
  - Configure the log mechanism output files (/etc/syslog.conf)
    - {selector}   {action}
    - *.*   /var/log/unified_log
    - kern.crit   on-duty-cell-alias

- **Changes needed at remote stations**
  - Change the logging destination (local copy is sometime needed) (/etc/syslog.conf)
    - {selector}   {action}
    - *.emerg   @loghost
    - kern.*   joe,eddiea
  - Only software that uses syslog functions will be redirected !

- **Changes needed in the applications**
  - Use syslog() sys-call function for logging
  - MW : “Middleware Security Audit Logging Guidelines”
  - Suggested configuration “Grid Log Retention Guidelines**”**

Logging tools

Central Syslogging

- Logconf - centralised configuration control
- Unix syslog daemon
- Syslog-ng

Log analyzer

- Logwatch
- swatch

Logrotate – very useful utility

More in Central loghost mini-Howto

Analyzing challenges

- **Most of process is pattern based**
- **Search & filtering are text based (active research area)**
- **Searching in DB is faster (but less flexible)**
- **XML trend is coming….(be aware)**
- **Large sets are difficult to analyze (use grid for that one ☺)**

Central syslog vulnerabilities

- **Inherits UDP vulnerabilities**
- **Overload (quantity and rate)**
- **Enter junk information**
- **Auto pilot might cause an auto crash !**
  - Check your logging system
  - Analyze your logs (anomalies, trends)

Remember the Demo ?

How many ball passes you counted ?

Thanks

Thanks to the OSCT & Romain for helpful remarks !