Log management ELISA controlled by Zabbix

Lukáš Malý
Hi, Every One!

A Little About Me:
I work as an IT consultant at Datasys. Datasys company is involved in the development and implementation of log management ELISA, which integrates several well-known Open Source projects. I participate in the implementation of Zabbix.

maly@datasys.cz
www.datasys.cz
www.logmanagement.cz
@SmEjDIL – linkedin.com/in/smejdil
22 years of experience - comprehensive implementation and integration services in IT, telecommunications and customized development

Czech private company
Dynamism and innovation

Strategic vision
Real customers' needs
Long-term cooperation

Quality control
ISO 9001 - Quality Management
ISO / IEC 20000-1 - IT Service Management
ISO 27001 – Information Security Management System
ISO 14001 - Environmental Management
ISO 10006 – Quality Management in Projects
BS OHSAS 18001 – Occupational Health and Safety Management Systems
NBÚ (National Security Authority)
DATASYS in figures

- Employees: 85
- Strategic areas: 10
- Turnover in 2015: CZK 750 million
- Over 50 projects implemented in the year 2015
- 4 branch offices
Company's areas of interest

- Security and monitoring
- Microsoft And Virtualization
- Storage and Backup
- Networking
- Application development
- Documents
- Innovation
- USM
- ServiceDesk /HelpDesk
- Infrastructure
Security and monitoring

Cyber-security legislation
Risk analysis, we use a fully localised tool "verinice"
Security-related documentation, compliance with regulations

Solution for Log Management and SIEM
Premium quality open source solutions Datasys ELISA and top program McAfee SIEM
Video logs ObserveIT

* SIEM – Security Information and Event Management

Expert services of security specialists
Risk analysis, security-related documentation
Ensuring compliance with the legal requirements for cyber-security
References: Data boxes, Prague Castle Administration, Administration of State Material Reserves, Ministry of Foreign Affairs of the Czech Republic

Operation monitoring, SLA evaluation
Certified ZABBIX partner
Robust, straightforward, easy-to-customize system
Free license without functional restrictions
Security and monitoring - references

Monitoring system ZABBIX
- Czech Statistical Office
- Česká pošta (Czech Post)
- Český aeroholding (Czech Aeroholding)
- ČEZ (energy/utility operator and provider)
- Data box information system (Ministry of the Interior of the Czech Republic)
- Ministry of Foreign Affairs of the Czech Republic
- Administration of State Material Reserves

Log management and SIEM
- Artesa, saving and loan cooperative
- Česká pošta (Czech Post)
- Ministry of Regional Development
- Ministry of Foreign Affairs of the Czech Republic
ELISA is log management and security monitoring tool

**ELISA** is log management and security monitoring tool, Event Log Interception Storage and Analysis. Free software with support from the producer. Preserves the structure of the original event, uses several components. Extreme scalability and high availability. Attractive web user interface Kibana. High performance (up to 5000 eps).
The main input channels of the ELISA

Input protocols

- binary ... (agents) protocol for transmission of structured events
- syslog (TCP, UDP or TLS/SSL)
- SNMP traps
- Microsoft Windows Eventing
- Netflow datagrams
Enhanced Kibana as a frontend for data analysis

Kibana is used for viewing log data
Kibana is a very flexible interface
Dashboard can be modified and stored
Extended ZABBIX frontend for administration
Zabbix 'NXlog templates' for central management of agents
ELISA Open Source component

Used projects

- **Elasticsearch, Logstash, Kibana**
  Open source product of the 'Elastic' company.

- **NXLog (Community or Enterprise edition)**
  In concept NXLog is similar to syslog-ng or rsyslog but it is not limited to unix and syslog only. It supports different platforms, log sources and formats so nxlog can be an ideal choice to implement a centralized logging system.

- **Zabbix, Xlog, HTTPd Apache with mod_authnz_external.**
  Zabbix serves several major functions in ELISA. Datasys component Xlog uses Zabbix API.

- **JasperReport Server with plugin ElasticJasper, Snmptrapd**
  ELISA provides various opportunities to report information about stored events
Zabbix integration with ELISA

ELISA combines many features

- **ELISA utilizes ZABBIX features**
  - User authentication (internal or LDAP)
  - Role based access control (flexible log data access restrictions, RW or RO access to dashboards)
  - Notifications
  - Self-monitoring – ELK, NXlog

- **ELISA utilizes Elasticsearch features**
  - Robustness
  - Scalability
  - Dashboards – Kibana
  - Logstash – GeoIP, Netflow
ELISA heavily utilizes ZABBIX for user authentication and role based access control.
Zabbix integration with ELISA

ELISA roles features

- ELISA heavily utilizes ZABBIX for user authentication and role based access control.
Zabbix integration with ELISA

ELISA roles features

- ELISA heavily utilizes ZABBIX for user authentication and role based access control.
Zabbix integration with ELISA

ELISA roles features

- ELISA heavily utilizes ZABBIX for user authentication and role based access control.
Zabbix integration with ELISA

Use of Zabbix features

- ELISA heavily utilizes ZABBIX for user authentication and role based access control, notifications and self-monitoring.

- Elasticsearch indices are managed right in ZABBIX Frontend.
Zabbix integration with ELISA

DB Indices features

- Elasticsearch indices are managed right in ZABBIX Frontend.

---

**ELISA DB Indices**

<table>
<thead>
<tr>
<th>NAME</th>
<th>CREATION DATE</th>
<th>SIZE</th>
<th>LOG EVENTS</th>
<th>STATUS</th>
</tr>
</thead>
<tbody>
<tr>
<td>logstash-2016.08.07</td>
<td>07.08.2016 02:00:01</td>
<td>325.42 KB</td>
<td>340</td>
<td>active</td>
</tr>
<tr>
<td>logstash-2016.08.06</td>
<td>06.08.2016 02:00:01</td>
<td>428.91 KB</td>
<td>395</td>
<td>active</td>
</tr>
<tr>
<td>logstash-2016.08.05</td>
<td>05.08.2016 02:00:01</td>
<td>451.44 KB</td>
<td>412</td>
<td>active</td>
</tr>
</tbody>
</table>
## Zabbix integration with ELISA

**DB Indices features**

- Elasticsearch indices are managed right in ZABBIX Frontend.

### ELISA DB Indices

<table>
<thead>
<tr>
<th>Name</th>
<th>Creation Date</th>
<th>Size</th>
<th>Log Events</th>
<th>Status</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>legstash-2016.09.06</td>
<td>08.09.2016 02:00:00</td>
<td>61.33 MB</td>
<td>29412</td>
<td>active</td>
<td>close compress delete</td>
</tr>
<tr>
<td>legstash-2016.09.05</td>
<td>09.09.2016 02:00:00</td>
<td>280.78 MB</td>
<td>321996</td>
<td>active</td>
<td>close compress delete</td>
</tr>
<tr>
<td>legstash-2016.09.04</td>
<td>09.09.2016 02:00:00</td>
<td>105.05 MB</td>
<td>103950</td>
<td>active</td>
<td>close compress delete</td>
</tr>
<tr>
<td>legstash-2016.09.03</td>
<td>03.09.2016 02:00:00</td>
<td>101.82 MB</td>
<td>102179</td>
<td>active</td>
<td>close compress delete</td>
</tr>
<tr>
<td>legstash-2016.09.02</td>
<td>02.09.2016 02:00:00</td>
<td>274.42 MB</td>
<td>314150</td>
<td>active</td>
<td>close compress delete</td>
</tr>
<tr>
<td>legstash-2016.09.01</td>
<td>01.09.2016 19:38:25</td>
<td>148.18 MB</td>
<td>193392</td>
<td>active</td>
<td>close compress delete</td>
</tr>
<tr>
<td>legstash-2016.08.31</td>
<td>31.08.2016 02:00:00</td>
<td>closed</td>
<td></td>
<td></td>
<td>open compress delete</td>
</tr>
<tr>
<td>legstash-2016.08.30</td>
<td>30.08.2016 02:00:00</td>
<td>closed</td>
<td></td>
<td></td>
<td>open compress delete</td>
</tr>
<tr>
<td>legstash-2016.08.14</td>
<td>25.08.2016 15:12:35</td>
<td>compressed</td>
<td></td>
<td></td>
<td>uncompressed delete</td>
</tr>
<tr>
<td>legstash-2016.08.13</td>
<td>25.08.2016 15:12:17</td>
<td>compressed</td>
<td></td>
<td></td>
<td>uncompressed delete</td>
</tr>
<tr>
<td>legstash-2016.08.12</td>
<td>25.08.2016 15:12:43</td>
<td>compressed</td>
<td></td>
<td></td>
<td>uncompressed delete</td>
</tr>
</tbody>
</table>
Zabbix integration with ELISA

Use of Zabbix features

- ELISA heavily utilizes ZABBIX for user authentication and role based access control, notifications and self-monitoring.
- Elasticsearch indices are managed right in ZABBIX Frontend.
- ZABBIX "trapper" items and monitoring templates are used to centrally manage configuration of distributed environment of NXlog agents.
Zabbix integration with ELISA

ELISA configuration by Zabbix Templates-Xlog

- ZABBIX “trapper” items and monitoring templates are used to centrally manage configuration of distributed environment of NXlog agents.

<table>
<thead>
<tr>
<th>Wizard</th>
<th>Name</th>
<th>Triggers</th>
<th>Key</th>
<th>Interval</th>
<th>History</th>
<th>Trends</th>
<th>Type</th>
<th>Applications</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Zabbix trapper</td>
<td>App - Datsys ELISA - Alarms</td>
</tr>
<tr>
<td></td>
<td>ELISA receiver (binary Xlog format)</td>
<td>xlog.conf(AGENT,Output,OutTopXlog)</td>
<td>10d</td>
<td></td>
<td></td>
<td></td>
<td>Zabbix trapper</td>
<td>Xlog Config - Linux Base</td>
</tr>
<tr>
<td></td>
<td>JSON conversion support</td>
<td>xlog.conf(AGENT,Extension,Json_Common)</td>
<td>10d</td>
<td></td>
<td>1500d</td>
<td></td>
<td>Zabbix trapper</td>
<td>Xlog Config - Linux Base</td>
</tr>
<tr>
<td></td>
<td>Route events from internal Xlog agent log to ELISA</td>
<td>xlog.conf(AGENT,Route,LogInternal2Collector)</td>
<td>10d</td>
<td></td>
<td>1500d</td>
<td></td>
<td>Zabbix trapper</td>
<td>Xlog Config - Linux Base</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Zabbix trapper</td>
<td>Xlog Config - Linux Base</td>
</tr>
<tr>
<td></td>
<td>Template description - Xlog_Base_LINUX_LAN</td>
<td>xlog.comment(Base_LINUX_LAN)</td>
<td>10d</td>
<td></td>
<td>1500d</td>
<td></td>
<td>Zabbix trapper</td>
<td>Xlog Config - Linux Base</td>
</tr>
<tr>
<td></td>
<td>Xlog de-duplicator module [NorepeatFileXlog]</td>
<td>xlog.conf(AGENT,Processor,NorepeatFileXlog)</td>
<td>10d</td>
<td></td>
<td>1500d</td>
<td></td>
<td>Zabbix trapper</td>
<td>Xlog Config - Linux Base</td>
</tr>
<tr>
<td></td>
<td>Xlog internal log file processing</td>
<td>xlog.conf(AGENT,Input,InFileXlog)</td>
<td>10d</td>
<td></td>
<td>1500d</td>
<td></td>
<td>Zabbix trapper</td>
<td>Xlog Config - Linux Base</td>
</tr>
<tr>
<td></td>
<td>Xlog internal log file rotation</td>
<td>xlog.conf(AGENT,Extension,InFileXlogRotation)</td>
<td>10d</td>
<td></td>
<td>1500d</td>
<td></td>
<td>Zabbix trapper</td>
<td>Xlog Config - Linux Base</td>
</tr>
<tr>
<td></td>
<td>Xlog log file charset conversion</td>
<td>xlog.conf(AGENT,Extension,CharconvAutoDetect)</td>
<td>10d</td>
<td></td>
<td>1500d</td>
<td></td>
<td>Zabbix trapper</td>
<td>Xlog Config - Linux Base</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Zabbix trapper</td>
<td>Xlog Config - Linux Base</td>
</tr>
</tbody>
</table>

Template-DS-Xlog_Base_LINUX_LAN for Nxlog agent
Zabbix integration with ELISA

NXlog configuration in Templates-Xlog

- ZABBIX “trapper” items - The field 'Description' contains NXlog configuration directives.

```
xlog.config[AGENT,Input,InBinarySyslog,170,Rules-UniFi]
```
Zabbix integration with ELISA

NXlog configuration

- **ZABBIX “trapper” items** - The field 'Description' contains NXlog configuration directives.

**NXlog basic modules**

- **im_tcp** - This module accepts TCP connections on the address and port specified in the configuration. It can handle multiple simultaneous connections. The TCP transfer protocol provides more reliable log transmission than UDP. If security is a concern, consider using the **im_ssl** module instead.

- **im_udp** - This module accepts UDP datagrams on the address and port specified in the configuration. UDP is the transport protocol of the old BSD syslog standard as described in RFC 3164.

- **im_file** - This module can be used to read log messages from files.

- **om_file** - This module can be used to write log messages to a file.

- **xm_csv** - This module provides functions and procedures to process data formatted as comma separated values (CSV) and allows to convert to CSV and parse CSV into fields.

Zabbix integration with ELISA

Use of Zabbix features

- ELISA heavily utilizes ZABBIX for user authentication and role based access control, notifications and self-monitoring.

- Elasticsearch indices are managed right in ZABBIX Frontend.

- ZABBIX “trapper” items and monitoring templates are used to centrally manage configuration of distributed environment of NXlog agents.

- NXlog Agents are capable to securely auto-register as ZABBIX "hosts".
Zabbix integration with ELISA

Host configuration

- NXlog Agents are capable to securely auto-register as ZABBIX "hosts".

```
curl -k "https://elisa:10443/xlog/getRuleset.php?&hostname=elisa&label=AGENT&auth=DEFAULT&platform=LINUX_LAN"
```
ELISA Virtual Appliance
General Availability in November 2016

Version 3.3.0

Hostname: elisa-server
Device: ens160
IP: 192.168.1.203
Netmask: 255.255.252.0
GW: 192.168.0.1
DNS: 192.168.1.25

<table>
<thead>
<tr>
<th>Filesystem</th>
<th>Size</th>
<th>Used</th>
<th>Avail</th>
<th>Use%</th>
<th>Mounted on</th>
</tr>
</thead>
<tbody>
<tr>
<td>/dev/mapper/vg_elisa-lv_root</td>
<td>7.0G</td>
<td>2.8G</td>
<td>4.3G</td>
<td>40%</td>
<td>/</td>
</tr>
<tr>
<td>/dev/mapper/vg_elisa-lv_var</td>
<td>8.5G</td>
<td>6.4G</td>
<td>2.1G</td>
<td>76%</td>
<td>/var</td>
</tr>
<tr>
<td>/dev/mapper/vg_elisa-lv_tmp</td>
<td>3.0G</td>
<td>46M</td>
<td>3.0G</td>
<td>2%</td>
<td>/tmp</td>
</tr>
</tbody>
</table>

Services

- elasticsearch [RUNNING]
- logstash [RUNNING]
- nxlog [RUNNING]
- apache [RUNNING]
- zabbix server [RUNNING]
- zabbix agent [RUNNING]
- tomcat [RUNNING]
- memcached [RUNNING]

Please choose an option:

0) Logout
1) Shell
2) Reboot system
3) Halt system
4) Network settings
5) SSH and SSL keys
6) Change hostname
7) Restart services

[ELISA]:
Thank you for your attention