

D A T A
S Y S

Log management ELISA controlled by
Zabbix

Lukáš Malý



Lukáš Malý

IT consultant – security and
monitoring

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.

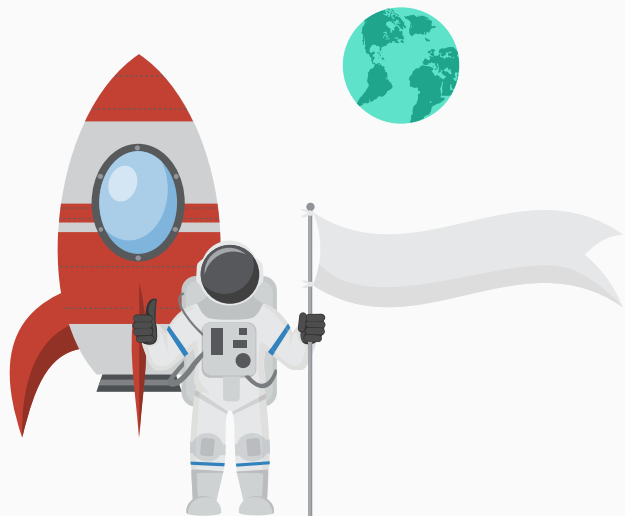


maly@datasys.cz

www.datasys.cz

www.logmanagement.cz

@SmEjDiL – [linkedin.com/in/smejdiL](https://www.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

85

Employees

10

Strategic areas

750

Turnover in 2015: CZK 750 million

50

Over 50 projects implemented in the
year 2015

4

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

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

Solution for Log Management and SIEM

Premium quality open source solutions Datasys ELISA and

top program McAfee SIEM

Video logs ObserveIT

Operation monitoring, SLA evaluation

Certified ZABBIX partner

Robust, straightforward, easy-to-customize system

Free license without functional restrictions

* SIEM – Security Information and Event Management

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

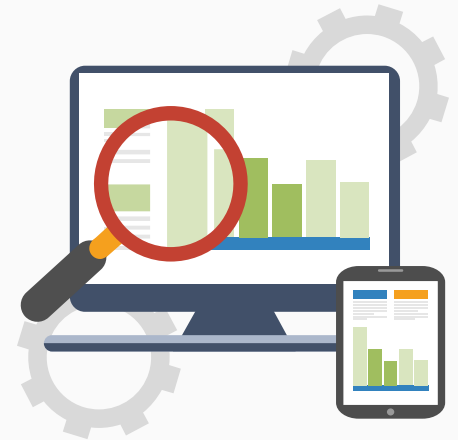
Log management and SIEM

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

The Central Operational and Security logs monitoring.
Fast Searching, Analyzing, Abnormality Detection and Reporting.

SEARCH DATA



- Linux Admins
- Network Admins
- Windows Admins
- ELISA Admins

CONFIGURATION

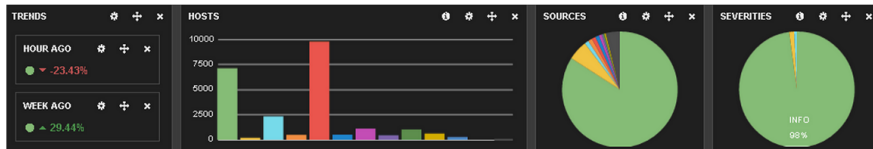


- Log Data Processing Rules
- User Accounts and Roles
- DB Indices Management
- Elasticsearch Configuration
- CentOS Configuration
- JasperReports@ server

HELP



About ELISA
Search Data
Log collecting
and Agent installation
NXlog/DSlog Configuration
Users' access permissions
DB Indices Management



Copyright 2014-2016 Dataysys

Elisa 3.3.0

DATA.....
SYS

E-mail: bezpecnost@dataysy.cz | Phone: +420 225 308 111

- ELISA is logmanagement
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 5 000 eps)

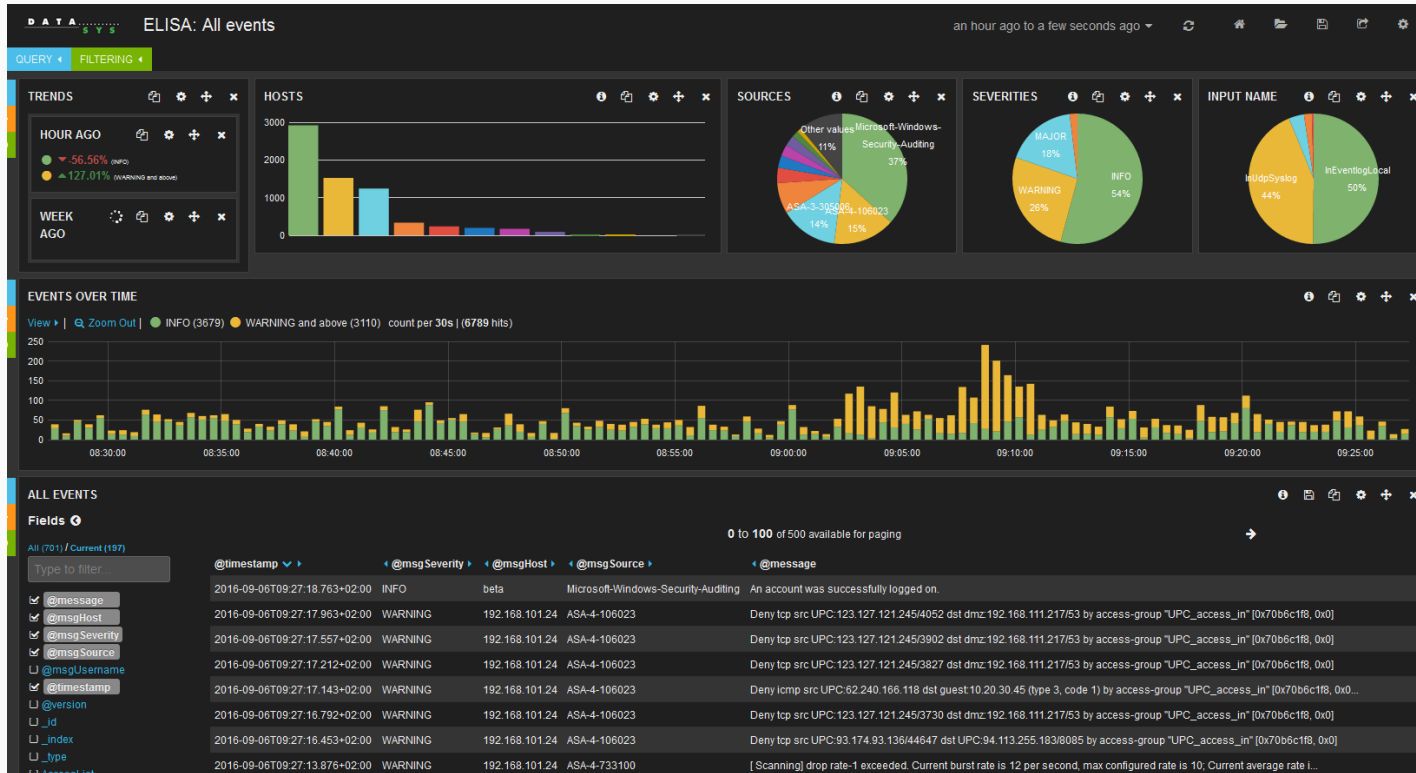
The main input channels of the ELISA

Input protocols

- binary ... (agents) protocol for transmission of structured events
- syslog (TCP, UDP or TLS/SSL)
- SNMP traps
- Microsoft Windows Eventing
- Netflow datagrams

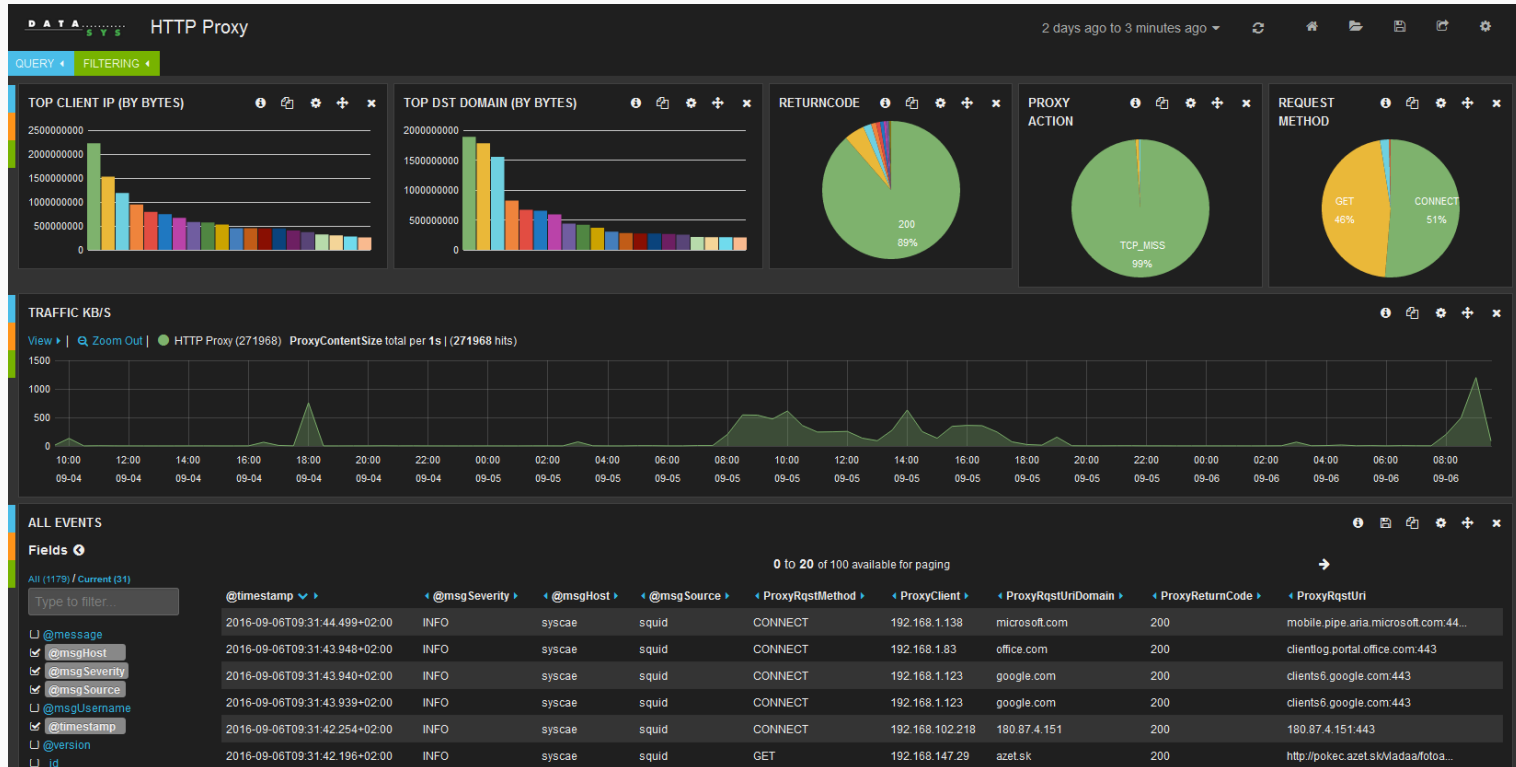
Enhanced Kibana as a frontend for data analysis

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

ZABBIX Monitoring Inventory Reports Configuration Administration Addons ELISA

Host groups **Templates** Hosts Maintenance Actions Discovery IT services

Templates

Group

<input type="checkbox"/> TEMPLATES ▲	APPLICATIONS	ITEMS	TRIGGERS	GRAPHS	SCREENS	DISCOVERY	WEB	LINKED TEMPLATES	LINKED TO
<input type="checkbox"/> Template-DS-Xlog_Alarm	Applications 1	Items 1	Triggers 5	Graphs	Screens	Discovery	Web		Template-DS-Xlog_Base_ALARM_ONLY, Template-DS-Xlog_Base_LINUX_LAN, DS-Xlog_Base_WINDOWS_LAN
<input type="checkbox"/> Template-DS-Xlog_Base_ALARM_ONLY	Applications 1	Items 1	Triggers 5	Graphs	Screens	Discovery	Web	Template-DS-Xlog_Alarm	siem-repozitory, zbx3
<input type="checkbox"/> Template-DS-Xlog_Base_LINUX_LAN	Applications 2	Items 10	Triggers 5	Graphs	Screens	Discovery	Web	Template-DS-Xlog_Alarm	ELISA server
<input type="checkbox"/> Template-DS-Xlog_Base_WINDOWS_LAN	Applications 2	Items 10	Triggers 5	Graphs	Screens	Discovery	Web	Template-DS-Xlog_Alarm	
<input type="checkbox"/> Template-DS-Xlog_ELISA_ESM-Correlation	Applications 1	Items 10	Triggers	Graphs	Screens	Discovery	Web		
<input type="checkbox"/> Template-DS-Xlog_ELISA_Proxy	Applications 1	Items 75	Triggers	Graphs	Screens	Discovery	Web		ELISA server
<input type="checkbox"/> Template-DS-Xlog_ELISA_Proxy-Correlation	Applications 1	Items 34	Triggers	Graphs	Screens	Discovery	Web		
<input type="checkbox"/> Template-DS-Xlog_ELISA_Proxy_AlarmToOpenNMS	Applications 1	Items 5	Triggers	Graphs	Screens	Discovery	Web		
<input type="checkbox"/> Template-DS-Xlog_ELISA_Server	Applications 1	Items 20	Triggers	Graphs	Screens	Discovery	Web		ELISA server
<input type="checkbox"/> Template-DS-Xlog_LINUX_Common	Applications 1	Items 15	Triggers	Graphs	Screens	Discovery	Web		ELISA server
<input type="checkbox"/> Template-DS-Xlog_LOTUS_KAV	Applications 1	Items 3	Triggers	Graphs	Screens	Discovery	Web		
<input type="checkbox"/> Template-DS-Xlog_MSSQL_AuditTrace	Applications 1	Items 10	Triggers	Graphs	Screens	Discovery	Web		

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, Snmpttrapd

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 – GeolP, Netflow

Zabbix integration with ELISA

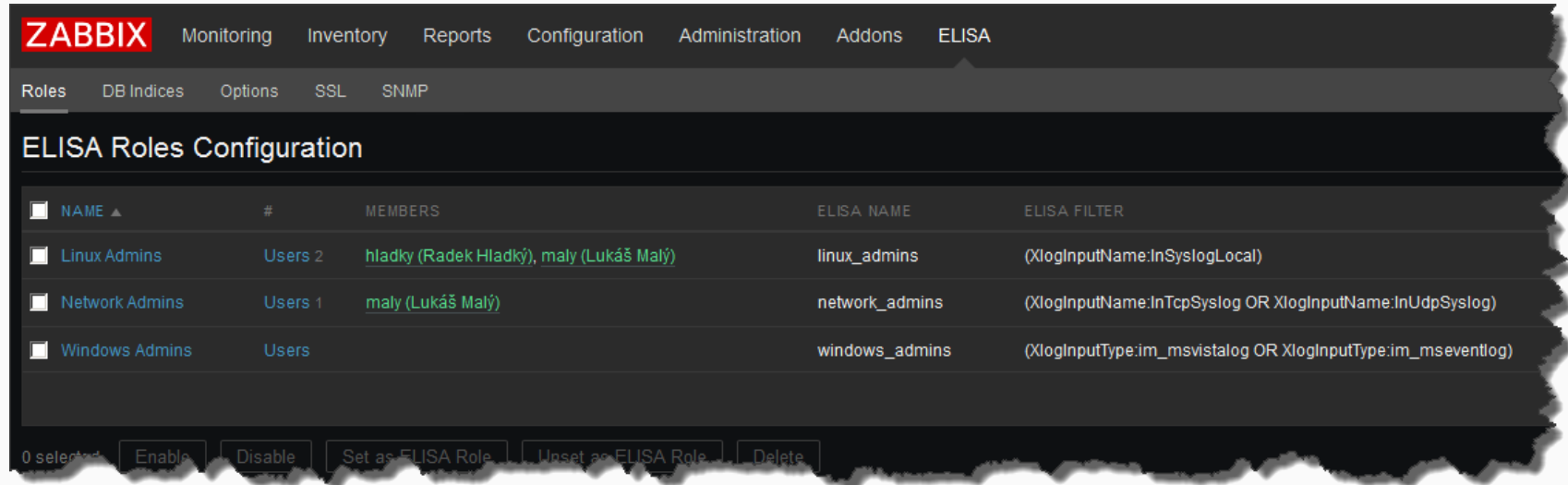
ELISA roles features

- 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.



The screenshot shows the Zabbix web interface with the 'ELISA' menu item selected. The 'ELISA Roles Configuration' page is displayed, showing a table of roles. The table has columns for 'NAME', '#', 'MEMBERS', 'ELISA NAME', and 'ELISA FILTER'. Three roles are listed: 'Linux Admins' (2 users: hladyk and maly), 'Network Admins' (1 user: maly), and 'Windows Admins' (Users). Below the table, there are buttons for '0 selected', 'Enable', 'Disable', 'Set as ELISA Role', 'Unset as ELISA Role', and 'Delete'.

NAME ▲	#	MEMBERS	ELISA NAME	ELISA FILTER
Linux Admins	Users 2	hladyk (Radek Hladký), maly (Lukáš Malý)	linux_admins	(XlogInputName:InSyslogLocal)
Network Admins	Users 1	maly (Lukáš Malý)	network_admins	(XlogInputName:InTcpSyslog OR XlogInputName:InUdpSyslog)
Windows Admins	Users		windows_admins	(XlogInputType:im_msvisualog OR XlogInputType:im_mseventlog)

Zabbix integration with ELISA

ELISA roles features

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

Frontend access **System default**

Enabled **Enabled**

ELISA Role

ELISA Name

ELISA Filter

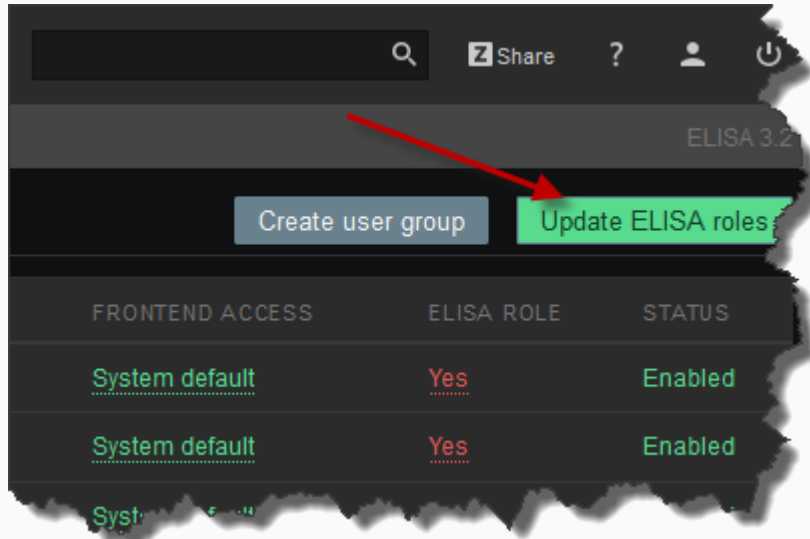
ELISA Access Type **Read-only Access** **Full Access**

Zabbix 3.0.2 © 2001–2016 Zabbix SIA

Zabbix integration with ELISA

ELISA roles features

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



Zabbix integration with ELISA

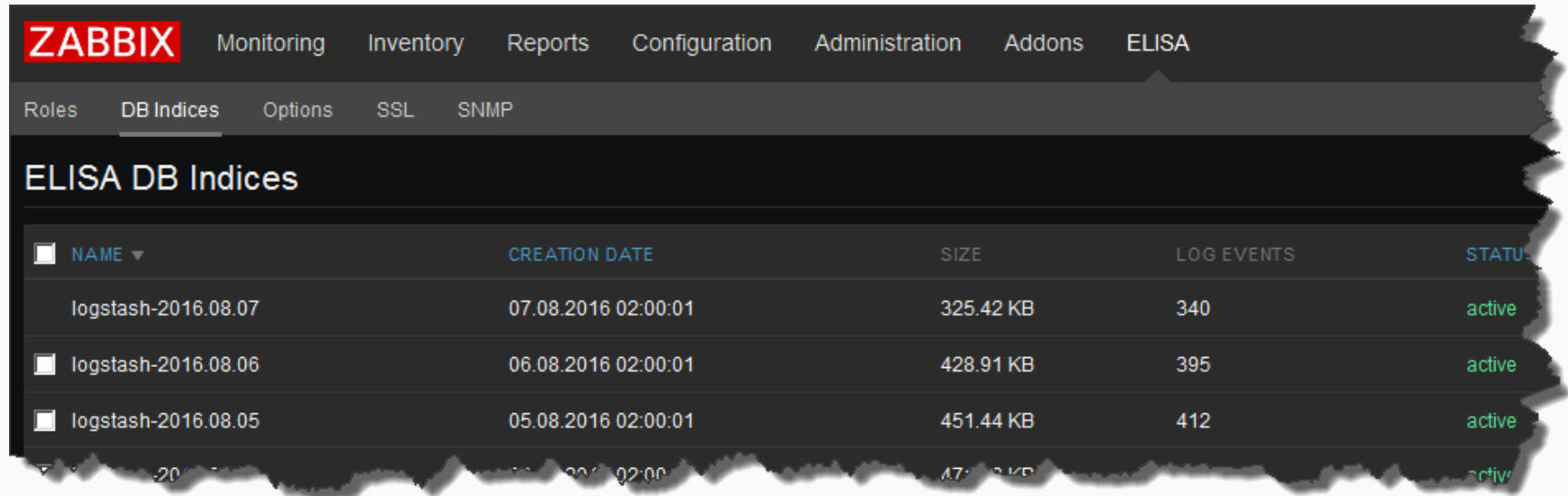
Use of Zabbix features

- 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.



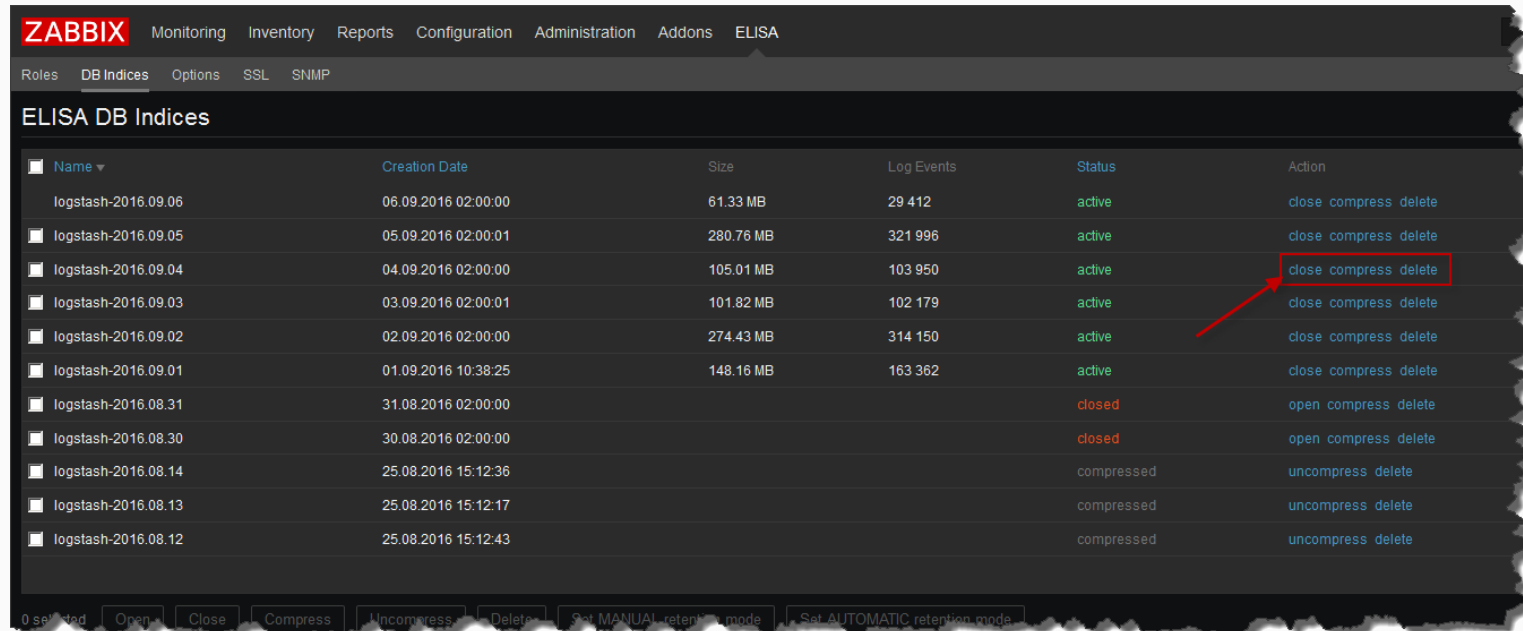
The screenshot shows the Zabbix Frontend interface with the 'ELISA' menu item selected. The 'DB Indices' sub-menu is active, displaying a table of Elasticsearch indices. The table has columns for Name, Creation Date, Size, Log Events, and Status. Three indices are listed, all with a status of 'active'.

NAME	CREATION DATE	SIZE	LOG EVENTS	STATUS
logstash-2016.08.07	07.08.2016 02:00:01	325.42 KB	340	active
logstash-2016.08.06	06.08.2016 02:00:01	428.91 KB	395	active
logstash-2016.08.05	05.08.2016 02:00:01	451.44 KB	412	active

Zabbix integration with ELISA

DB Indices features

- Elasticsearch indices are managed right in ZABBIX Frontend.



The screenshot shows the Zabbix web interface for managing ELISA DB Indices. The top navigation bar includes 'ZABBIX' and menu items: Monitoring, Inventory, Reports, Configuration, Administration, Addons, and ELISA. Below this, there are sub-menus: Roles, DB Indices (selected), Options, SSL, and SNMP. The main content area is titled 'ELISA DB Indices' and displays a table of indices. A red box highlights the 'close compress delete' actions for the index 'logstash-2016.09.04', with a red arrow pointing to it. At the bottom, there are buttons for '0 selected', 'Open', 'Close', 'Compress', 'Uncompress', 'Delete', and two buttons for setting retention modes: 'Set MANUAL retention mode' and 'Set AUTOMATIC retention mode'.

Name	Creation Date	Size	Log Events	Status	Action
logstash-2016.09.06	06.09.2016 02:00:00	61.33 MB	29 412	active	close compress delete
logstash-2016.09.05	05.09.2016 02:00:01	280.76 MB	321 996	active	close compress delete
logstash-2016.09.04	04.09.2016 02:00:00	105.01 MB	103 950	active	close compress delete
logstash-2016.09.03	03.09.2016 02:00:01	101.82 MB	102 179	active	close compress delete
logstash-2016.09.02	02.09.2016 02:00:00	274.43 MB	314 150	active	close compress delete
logstash-2016.09.01	01.09.2016 10:38:25	148.16 MB	163 362	active	close compress delete
logstash-2016.08.31	31.08.2016 02:00:00			closed	open compress delete
logstash-2016.08.30	30.08.2016 02:00:00			closed	open compress delete
logstash-2016.08.14	25.08.2016 15:12:36			compressed	uncompress delete
logstash-2016.08.13	25.08.2016 15:12:17			compressed	uncompress delete
logstash-2016.08.12	25.08.2016 15:12:43			compressed	uncompress delete

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.

Wizard	Name ▲	Triggers	Key	Interval	History	Trends	Type	Applications
...	Template-DS-Xlog_Alarm: Elisa Alarm	Triggers 5	zbx.elisa.alarm		10d		Zabbix trapper	App - Datasys ELISA - Alarms
	ELISA receiver (binary Xlog format)		xlog.config[AGENT,Output,OutTcpXlog]		10d	1500d	Zabbix trapper	Xlog Config - Linux Base
	JSON conversion support		xlog.config[AGENT,Extension,Json_Common]		10d	1500d	Zabbix trapper	Xlog Config - Linux Base
	Route events from internal Xlog agent log to ELISA		xlog.config[AGENT,Route,LogInternal2Collector]		10d	1500d	Zabbix trapper	Xlog Config - Linux Base
...	Template description - Xlog_Base_LINUX_LAN		xlog.comment[Base_LINUX_LAN]		10d		Zabbix trapper	
	Xlog deduplicator module [NorepeatFileXlog]		xlog.config[AGENT,Processor,NorepeatFileXlog]		10d	1500d	Zabbix trapper	Xlog Config - Linux Base
	Xlog internal log file processing		xlog.config[AGENT,Input,InFileXlog]		10d	1500d	Zabbix trapper	Xlog Config - Linux Base
	Xlog internal log file rotation		xlog.config[AGENT,Extension,InFileXlogRotation]		10d	1500d	Zabbix trapper	Xlog Config - Linux Base
	Xlog log file charset conversion		xlog.config[AGENT,Extension,CharconvAutoDetect]		10d	1500d	Zabbix trapper	Xlog Config - Linux Base
...	Xlog update scheduler		xlog.config[AGENT,Extension,ExecXlogUpdate]		10d		Zabbix trapper	Xlog Config - Linux Base

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.

```
Description #Processing rules for UniFi syslog events
#To filter out events, flag them using statements:
#if <CONDITION> set_var("dropEvent", 1);
Exec \
if ( $Message =~ /^(^(*),(*),(*))\s+([a-z+)]\s+(*)\ ) \
{ \
  $XlogParserLevel = 1; \
  $UniFiType = $1; \
  $UniFiMAC = $2; \
  $UniFiFirmwareVersion = $3; \
  $XlogDeviceType = "UniFi"; \
  $SourceName = $4; \
  $Message = $5; \
  $SourceName =~ s/[\d+]/;/; \
  if ( $Message =~ /(ath\d+)\s+STA\s+(((0-9A-Fa-f){2}):){5}[0-9A-Fa-f]{2}) \
  { \
    $XlogParserLevel = 2; \
    $UniFiDevice = $1; \
    $DeviceMAC = $2; \
  } \
} \
}
```

Enabled

Update Clone Delete Cancel

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.

<http://nxlog-ce.sourceforge.net/nxlog-docs/en/nxlog-reference-manual.pdf>

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"
```

The screenshot shows the Zabbix web interface. The top navigation bar includes 'ZABBIX', 'Monitoring', 'Inventory', 'Reports', 'Configuration', 'Administration', 'Addons', and 'ELISA'. Below this, there are sub-menus for 'Host groups', 'Templates', 'Hosts', 'Maintenance', 'Actions', 'Discovery', and 'IT services'. The main content area is titled 'Hosts' and shows the configuration for 'ELISA Server'. The 'Macros' tab is selected, and a red arrow points to it. The macro configuration table is highlighted with a red box and contains the following data:

MACRO	VALUE	
{XLOG.AGENT.ELISA_XLOG_AUT}	= 9c6199ba05e38bbb68ea130b4536bad6	Remove
{XLOG.AGENT.ELISA_XLOG_AUT}	= true	Remove
{XLOG.AGENT.ELISA_XLOG_INTI}	= 1 min	Remove

Below the table, there is an 'Add' link and buttons for 'Update', 'Clone', 'Full clone', 'Delete', and 'Cancel'.

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

Filesystem                Size  Used Avail Use% Mounted on
/dev/mapper/vg_elisa-lv_root 7.0G  2.8G  4.3G  40% /
/dev/mapper/vg_elisa-lv_var  8.5G  6.4G  2.1G  76% /var
/dev/mapper/vg_elisa-lv_tmp  3.0G   46M  3.0G   2% /tmp

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

[ELISA] : █
```

Thank you
for your attention

D A T A
S Y S