

# Log management ELISA

Konference **LinuxDays 2018**

DATA.....  
SYS

# KDO JSEM?



## Něco o mě ...

- Pracuji ve společnosti Datasys s.r.o. jako konzultant bezpečnosti a monitoringu.
- Podílím se na implementacích a vývoji log managementu ELISA.

**D A T A**.....  
**S Y S**

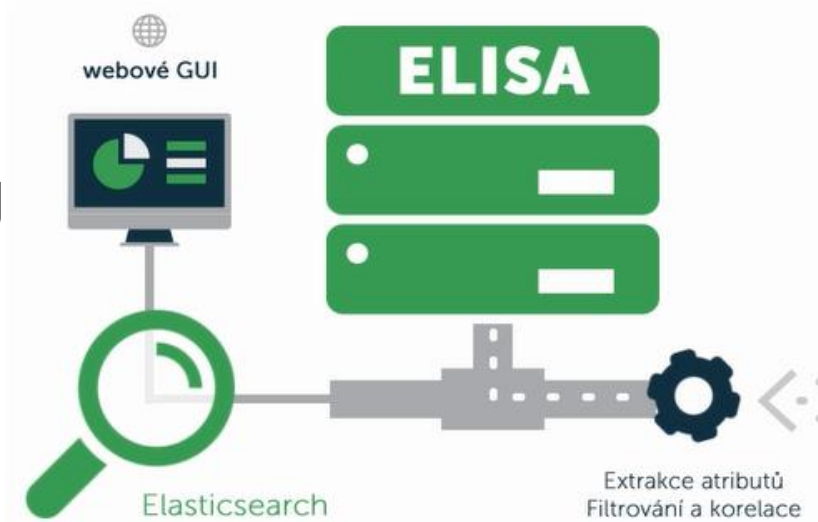
# **ELISA**

**E**vent **L**og  
**I**nterception  
**S**torage and  
**A**nalysis

# ELISA SECURITY MANAGER

Robustní nástroj pro sběr a analýzu bezpečnostních událostí

- **Získáte centrální konzoli bezpečnostního dohledu**
  - ❑ **Náš tip: Získejte i našeho bezpečnostního specialistu!**
- Podpora prakticky všech zdrojů dat
- Bezpečnostní i provozní monitoring
- Přehledné uživatelské rozhraní
- Škálovatelnost a nízké náklady



# ELISA

- Portál pro Kibana a Zabbix
- Používá Free Software
- Zachová strukturu původní události
- Webové rozhraní Kibana 3
- Vysoký výkon (až 5 000 eps)

**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

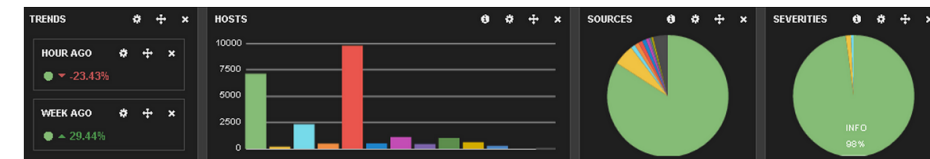


Log Data Processing Rules  
User Accounts and Roles  
DB Indices Management  
Elasticsearch Configuration  
CentOS Configuration  
JasperReports@ server

HELP



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

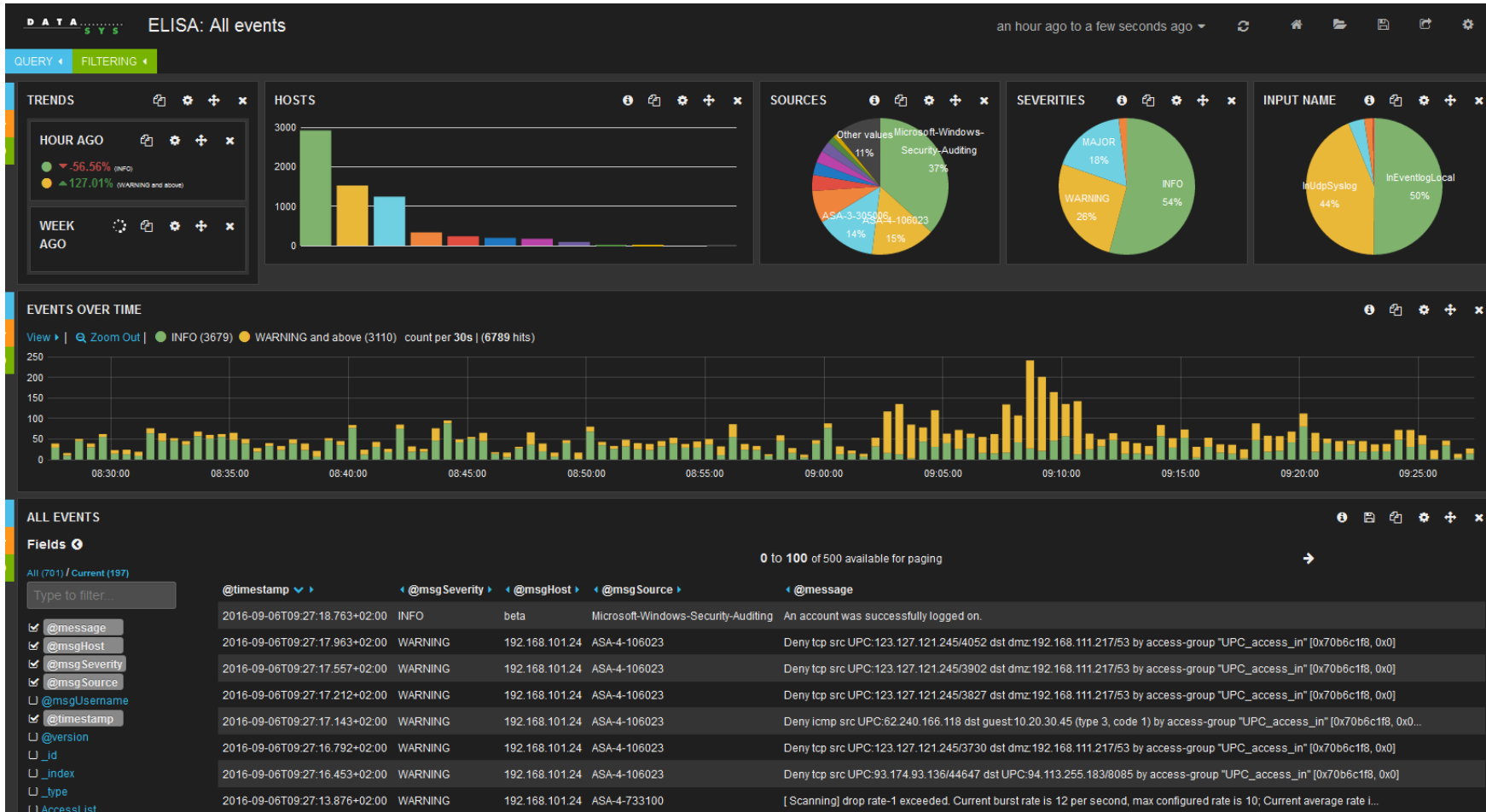


Copyright 2014-2016 Dalasys  
Elisa 3.3.0  
**DATA.....  
SYS**  
E-mail: [bezpecnost@dalasys.cz](mailto:bezpecnost@dalasys.cz) | Phone: +420 225 308 111

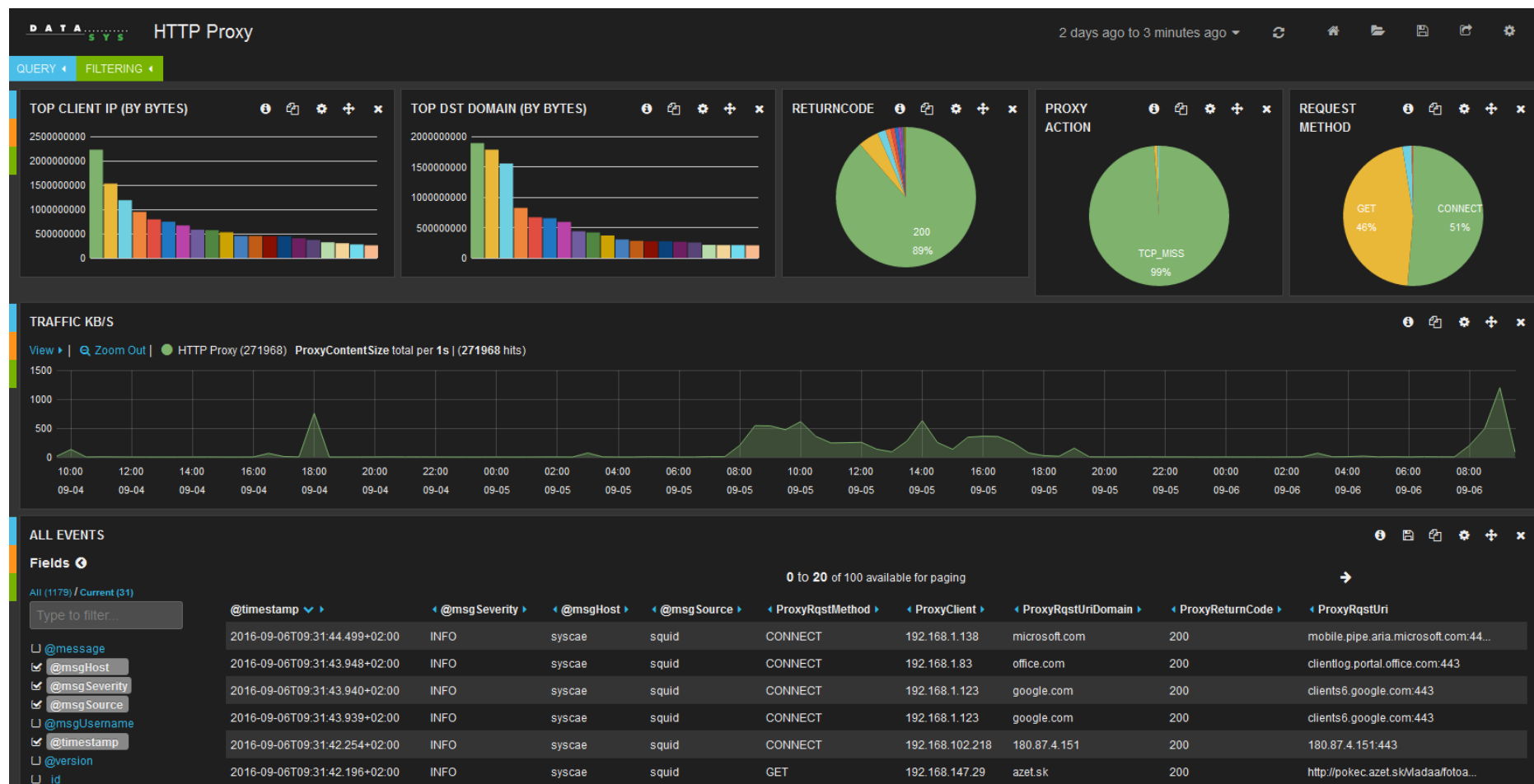
# HLAVNÍ VSTUPNÍ KANÁLY ELISA

- binary ... (agent) protocol příjem událostí
- syslog (TCP, UDP a TLS/SSL)
- SNMP traps
- Microsoft Windows Eventlog

# VYLEPŠENÁ KIBANA JAKO FRONTEND PRO ANALÝZU DAT



# KIBANA JE FLEXIBILNÍ ROZHRANÍ





# POMOCÍ ZABBIX ŠABLON NASTAVUJEME NXLOG

ZABBIX Monitoring Inventory Reports Configuration Administration Addons ELISA

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

### Templates

Group

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

# KOMPONENTY ELISA

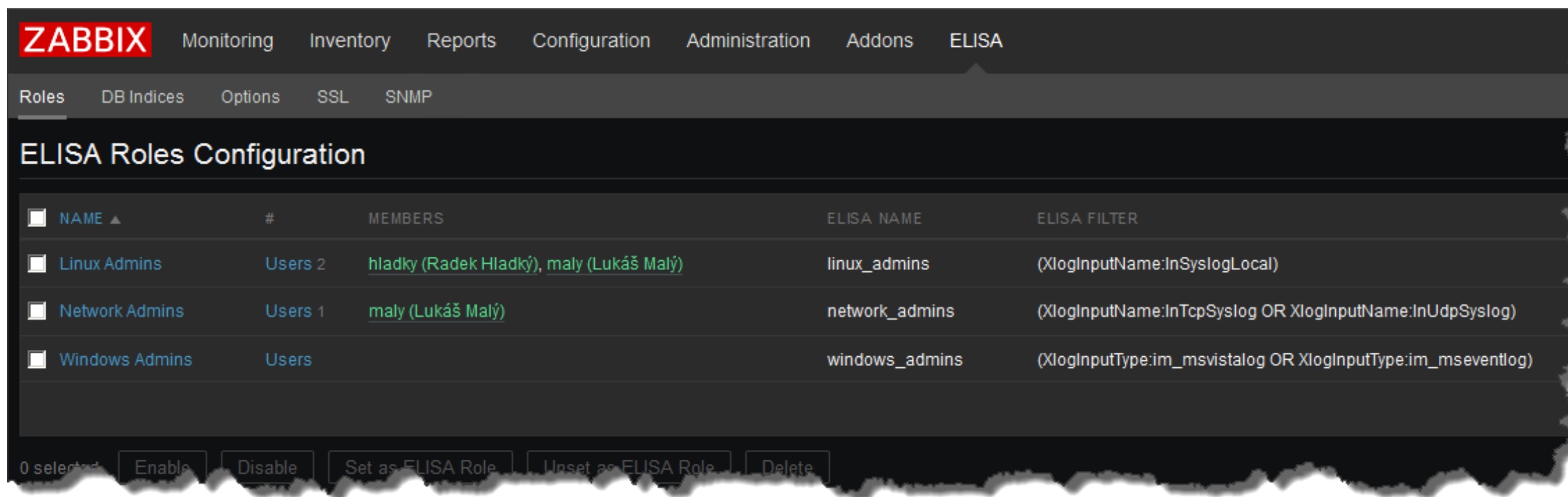
- Elasticsearch, Kibana
- NXLog (Enterprise edition)
- Zabbix, Xlog, HTTPd Apache s mod\_authnz\_external
- JasperReport Server s pluginem ElasticJasper
- Memcached

# ZABBIX INTEGROVÁN DO ELISA

- ELISA využívá funkce ZABBIX
- Autentizace (Interní nebo LDAP)
- Řízení přístupu založené na rolích – RO nebo RW
- Notifikace
- Self-monitoring – ELK, NXLog, Zabbix server, MariaDB

# ELISA VYUŽÍVÁ FUNKCIONALIT ZABBIXU

- Ověřování uživatelů a řízení přístupu založené na rolích

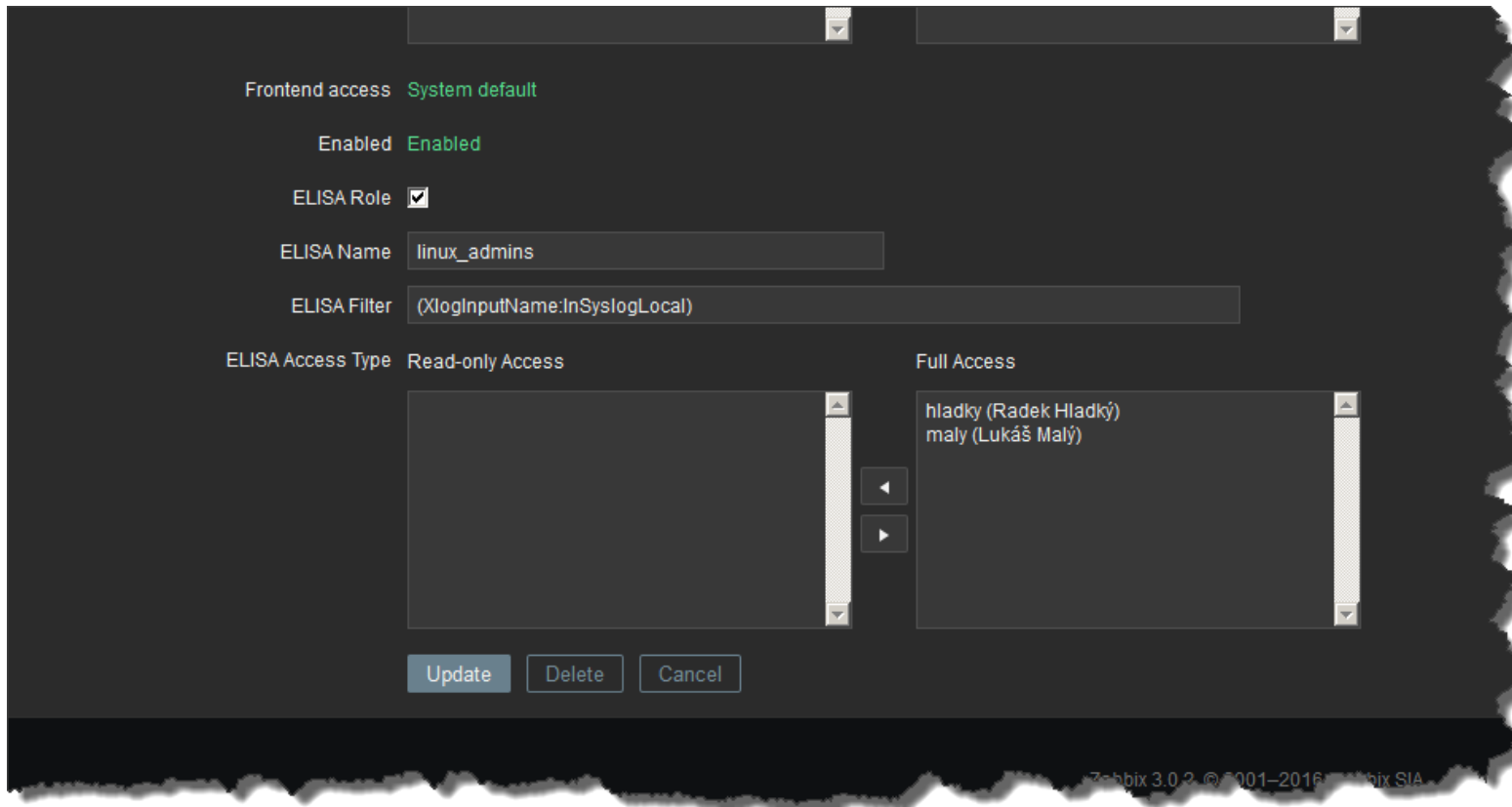


The screenshot shows the Zabbix web interface for ELISA Roles Configuration. The navigation menu includes Monitoring, Inventory, Reports, Configuration, Administration, Addons, and ELISA. The ELISA menu is expanded to show Roles, DB Indices, Options, SSL, and SNMP. The main content area displays a table of roles with columns for NAME, #, MEMBERS, ELISA\_NAME, and ELISA\_FILTER. Below the table are buttons for '0 selected', 'Enable', 'Disable', 'Set as ELISA Role', 'Unset as ELISA Role', and 'Delete'.

<input type="checkbox"/> NAME ▲	#	MEMBERS	ELISA_NAME	ELISA_FILTER
<input type="checkbox"/> Linux Admins	Users 2	<a href="#">hladky (Radek Hladký)</a> , <a href="#">maly (Lukáš Malý)</a>	linux_admins	(XlogInputName:InSyslogLocal)
<input type="checkbox"/> Network Admins	Users 1	<a href="#">maly (Lukáš Malý)</a>	network_admins	(XlogInputName:InTcpSyslog OR XlogInputName:InUdpSyslog)
<input type="checkbox"/> Windows Admins	Users		windows_admins	(XlogInputType:im_msvisialog OR XlogInputType:im_mseventlog)

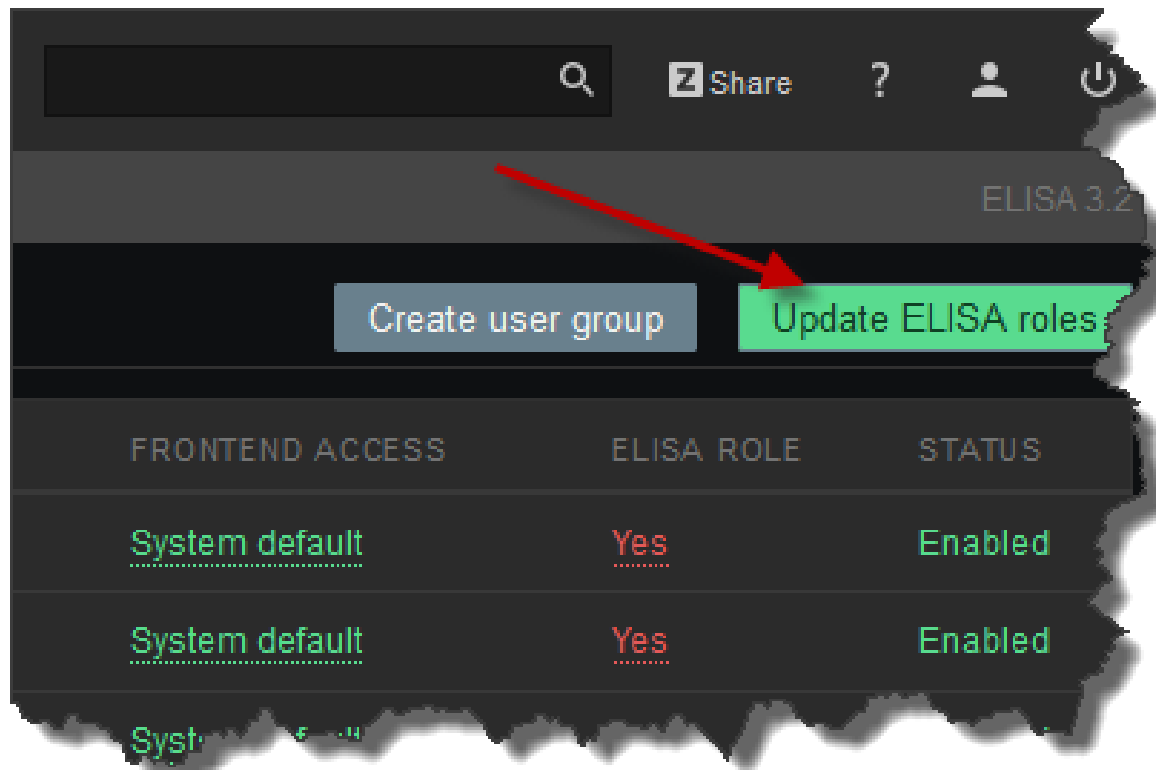
# ELISA VYUŽÍVÁ FUNKCIONALIT ZABBIXU

- Ověřování uživatelů a řízení přístupu založené na rolích



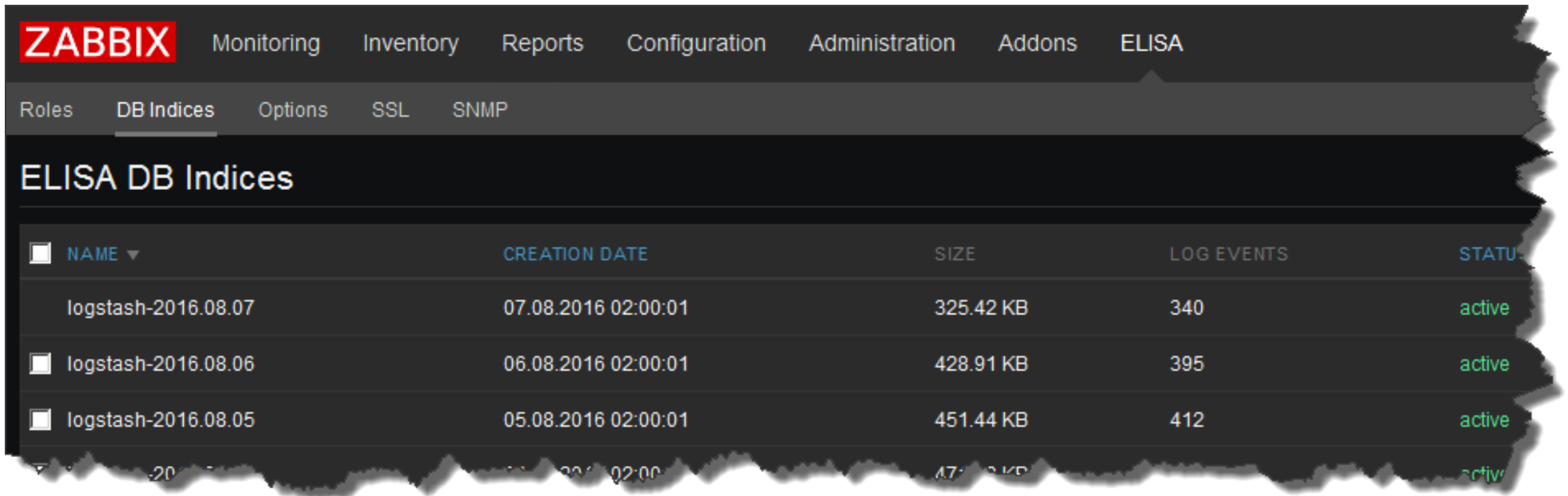
# ELISA VYUŽÍVÁ FUNKCIONALIT ZABBIXU

- Ověřování uživatelů a řízení přístupu založené na rolích



# ZABBIX INTEGROVÁN DO ELISA

- ELK indexy jsou spravovány přímo v 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 ELISA database indices. The table has columns for NAME, CREATION DATE, SIZE, LOG EVENTS, and STATUS. Three indices are visible, all with a status of 'active'.

<input type="checkbox"/> NAME ▾	CREATION DATE	SIZE	LOG EVENTS	STATUS
<input type="checkbox"/> logstash-2016.08.07	07.08.2016 02:00:01	325.42 KB	340	active
<input type="checkbox"/> logstash-2016.08.06	06.08.2016 02:00:01	428.91 KB	395	active
<input type="checkbox"/> logstash-2016.08.05	05.08.2016 02:00:01	451.44 KB	412	active

# ZABBIX INTEGROVÁN DO ELISA

- ELK indexy jsou spravovány přímo v ZABBIX Frontend.

The screenshot shows the ZABBIX Frontend interface with the 'ELISA DB Indices' table. The table has columns for Name, Creation Date, Size, Log Events, Status, and Action. The 'logstash-2016.09.04' row is highlighted with a red box around its 'close compress delete' actions, and a red arrow points to it.

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

0 selected | Open | Close | Compress | Uncompress | Delete | Set MANUAL retention mode | Set AUTOMATIC retention mode



# ZABBIX INTEGROVÁN DO ELISA

- K centrální správě konfigurace distribuovaného prostředí agentů NXLog se používají - ZABBIX Item type "trapper,,.

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

# ZABBIX INTEGROVÁN DO ELISA

- ZABBIX Item type "trapper," - používá formulář  
„Description“ obsahuje direktivy konfigurace NXLog.

```
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+)(.*)\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
```

# NXLOG MODULY

- xm\_\* - Extension Modules
- im\_\* - Input Modules
- pm\_\* - Processor Modules
- om\_\* - Output Modules

[https://nxlog.co/documentation/nxlog-user-guide#modules\\_list](https://nxlog.co/documentation/nxlog-user-guide#modules_list)

# NXLOG MODULY

- im\_tcp – zajišťuje připojení TCP na adrese a portu
- im\_udp - zajišťuje připojení UDP na adrese a portu
- im\_file – čtení ze souboru
- om\_file – zápis do souboru
- xm\_csv – zpracování CSV formátu dat

[https://nxlog.co/documentation/nxlog-user-guide#modules\\_list](https://nxlog.co/documentation/nxlog-user-guide#modules_list)

# NXLOG MODULY

- im\_ssl
- om\_elasticsearch
- pm\_buffer, pm\_null
- xm\_perl, xm\_snmp, xm\_kv, xm\_csv, xm\_fileop, xm\_exec,
- xm\_charconv, xm\_syslog, xm\_json

[https://nxlog.co/documentation/nxlog-user-guide#modules\\_list](https://nxlog.co/documentation/nxlog-user-guide#modules_list)

# NXLOG.CONF

- Počet řádků konfiguračního souboru nxlog

```
[root@elisa-dev-4 nxlog]# wc -l /var/log/nxlog/updates/elisa.rls  
3363 /var/log/nxlog/updates/elisa.rls  
[root@elisa-dev-4 nxlog]# |
```

# AUTOREGISTRACE AGENTŮ DO ELISA

- Zabbix Agent - Windows
- NXLog Agent - Windows



nxlog-setup-4.0.3735-customer-lan  
Baliček Instalační služby systému Wi...  
5,52 MB



zabbix-setup-4.0.0.0-customer-lan  
Baliček Instalační služby systému Wi...  
3,10 MB

# AUTOREGISTRACE AGENTŮ DO ELISA

- Zabbix Agent – většina Linux distribucí, \*BSD, AIX
- NXLog Agent - většina Linux distribucí, AIX

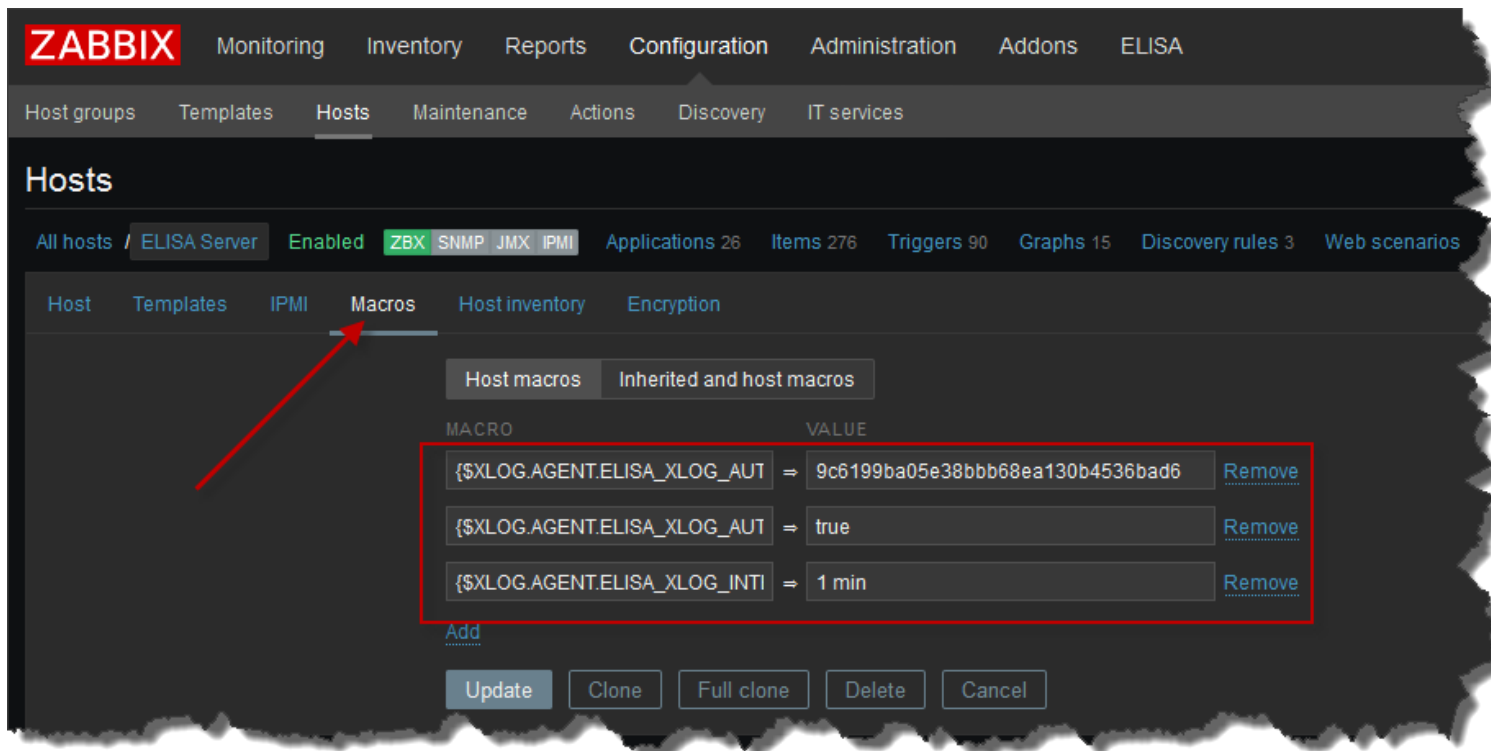
```
[root@elisa-dev-4 nxlog]# ls -l
nxlog-4.0.3735-1_rhel7.x86_64.rpm
nxlog-checkpoint-4.0.3735-1_rhel7.x86_64.rpm
nxlog-dbi-4.0.3735-1_rhel7.x86_64.rpm
nxlog-kafka-4.0.3735-1_rhel7.x86_64.rpm
nxlog-odbc-4.0.3735-1_rhel7.x86_64.rpm
nxlog-perl-4.0.3735-1_rhel7.x86_64.rpm
nxlog-python-4.0.3735-1_rhel7.x86_64.rpm
nxlog-ruby-4.0.3735-1_rhel7.x86_64.rpm
nxlog-wmi-4.0.3735-1_rhel7.x86_64.rpm
nxlog-wseventing-4.0.3735-1_rhel7.x86_64.rpm
nxlog-zmq-4.0.3735-1_rhel7.x86_64.rpm
[root@elisa-dev-4 nxlog]#
```



# AUTOREGISTRACE AGENTŮ DO ELISA

- NXLog agenti se bezpečně registrují do Zabbixu.

```
curl -k "https://elisa:10443/xlog/getRuleset.php?&hostname=elisa&label=AGENT&auth=DEFAULT&platform=LINUX_LAN"
```



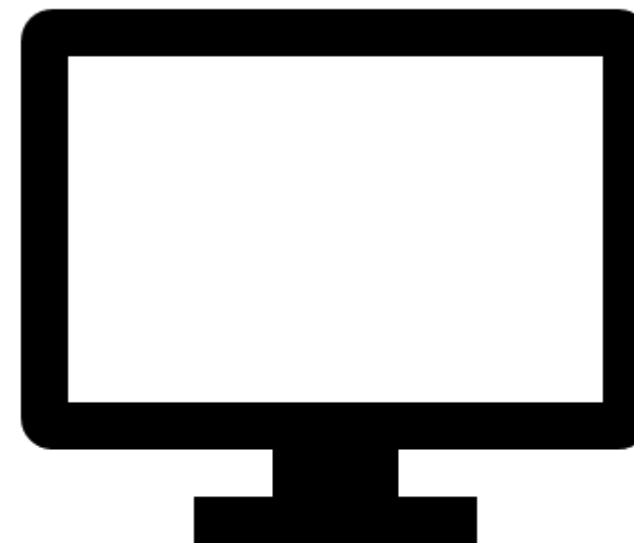
The screenshot shows the Zabbix web interface. The top navigation bar includes 'ZABBIX', 'Monitoring', 'Inventory', 'Reports', 'Configuration', 'Administration', 'Addons', and 'ELISA'. Below this, there are sub-navigation tabs for 'Host groups', 'Templates', 'Hosts', 'Maintenance', 'Actions', 'Discovery', and 'IT services'. The main content area is titled 'Hosts' and shows the configuration for the 'ELISA Server' host, which is 'Enabled'. The 'Macros' tab is selected, and a red arrow points to it. The 'Host macros' section is active, showing a table of macros:

MACRO	VALUE	
{XLOG.AGENT.ELISA_XLOG_AUT}	= 9c6199ba05e38bbb68ea130b4536bad6	<a href="#">Remove</a>
{XLOG.AGENT.ELISA_XLOG_AUT}	= true	<a href="#">Remove</a>
{XLOG.AGENT.ELISA_XLOG_INTI}	= 1 min	<a href="#">Remove</a>

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

## ELISA Proxy

- Zabbix Proxy
- ELISA Proxy
  - NXLog
  - XLog



# ELISA APPLIANCE

```
ELISA
Version 3.5.3

Hostname: elisa-server
Device: ens33
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  3.3G  3.8G  46% /
/dev/mapper/vg_elisa-lv_var   19G   14G  5.1G  73% /var
/dev/mapper/vg_elisa-lv_tmp   3.0G  129M  2.9G   5% /tmp

Memory
Mem: total used free shared buff/cache available
      7.6G  6.7G  120M  431M  845M  245M

Services
elasticsearch [ RUNNING ] logstash [ DISABLE ]
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) License
2) Reboot system         6) Other options
3) Halt system           7) Restart services

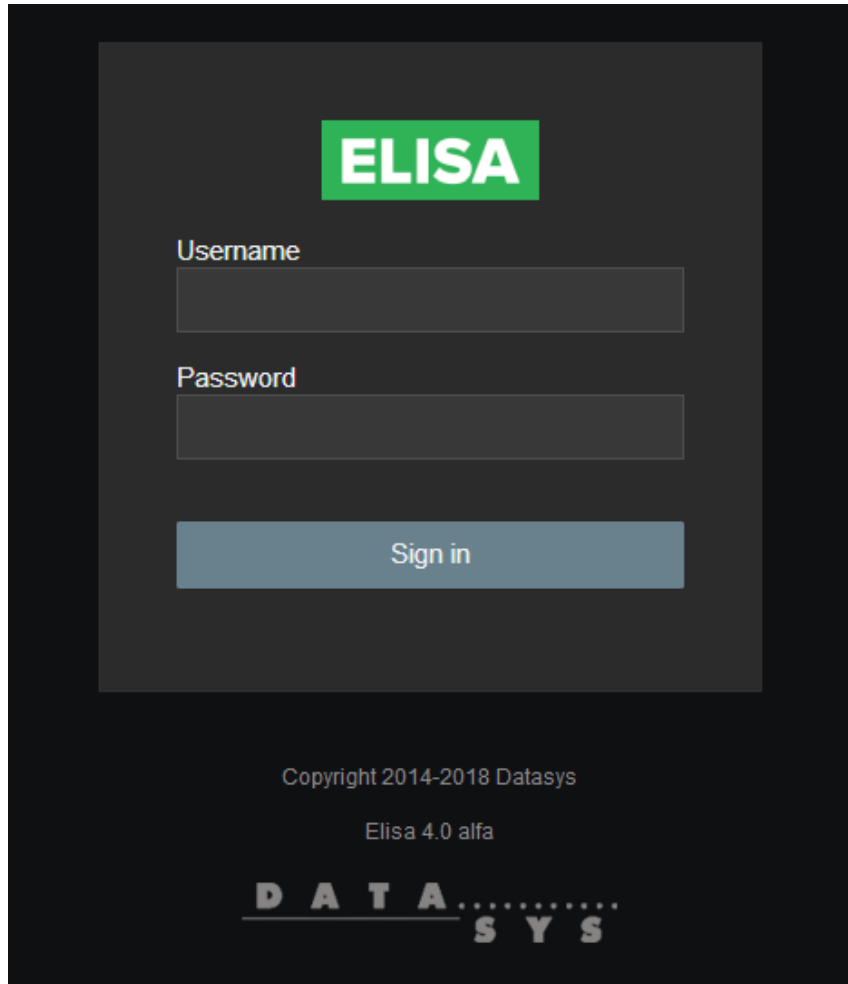
[ELISA] :
```

- ELISA menu, pro základní úkony v systému
- Změna IPv4
- Restart komponent

## NOVINKY ELISA 4.0

- Zabbix 4.0 LTS
- Elasticsearch 6.4
- NXLog 4.0
- Propojení dvou systémů do jedné Web konzole
- Integrace s OpenVAS a Flowmon APM

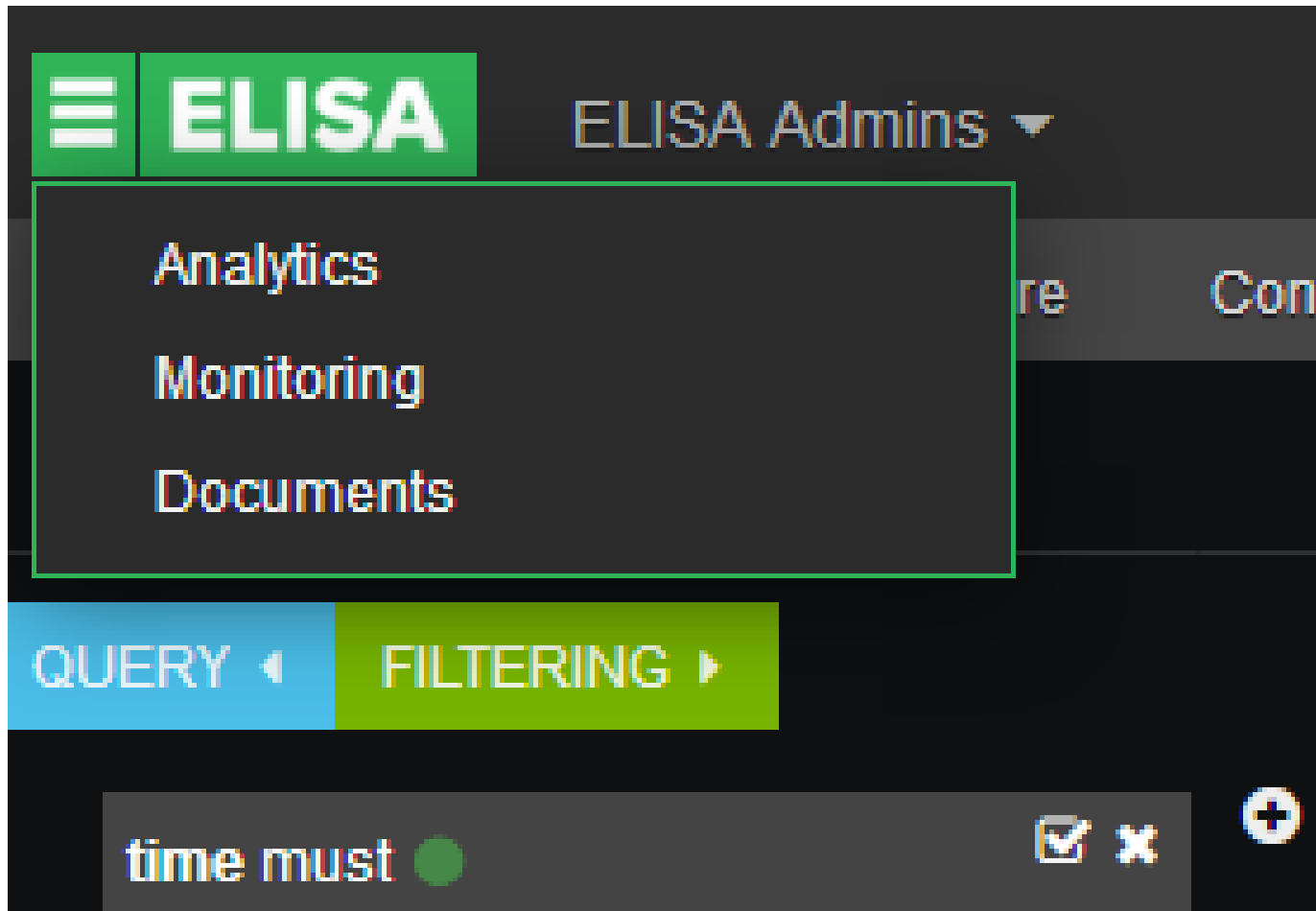
# NOVINKY ELISA 4.0



The screenshot shows a dark-themed login interface for ELISA. At the top, the word "ELISA" is displayed in white text on a green rectangular background. Below this, there are two input fields: "Username" and "Password", each with a light gray border. A "Sign in" button is positioned below the password field. At the bottom of the interface, the text "Copyright 2014-2018 Datasys" and "Elisa 4.0 alfa" is visible, along with the "DATA.....SYS" logo.

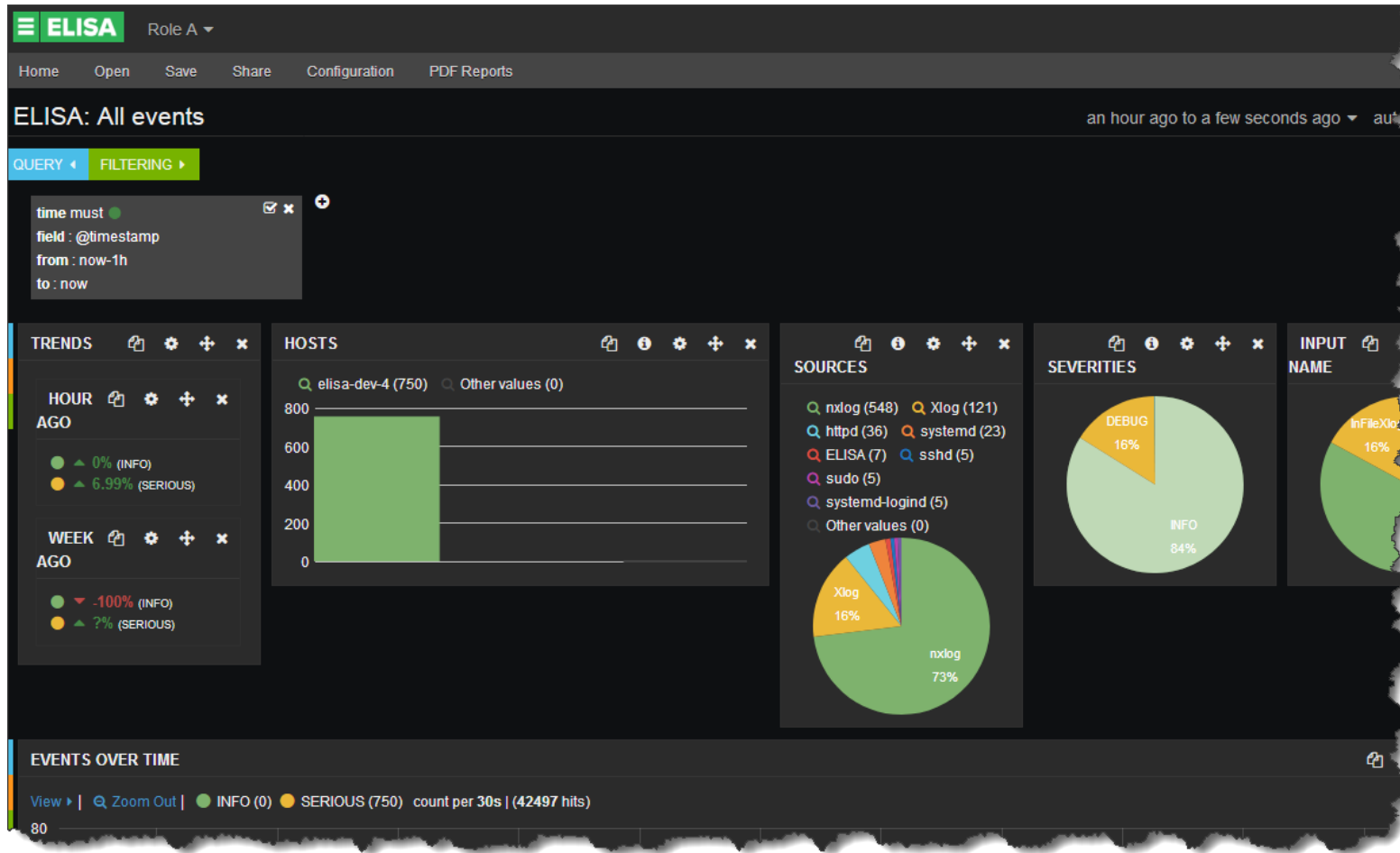
- Nové přihlášení do ELISA

# NOVINKY ELISA 4.0



- Navigační lišta

# NOVINKY ELISA 4.0



● Kibana 3

# NOVINKY ELISA 4.0

The screenshot displays the ELISA 4.0 web interface. At the top, there is a navigation menu with items: ELISA, Monitoring, Inventory, Reports, Configuration, Administration, Addons, and ELISA. Below this is a secondary menu with: Roles, DB Indices, Options, SSL, SNMP, Backup, and SW Update. A search bar on the right contains the text 'ELISA 4.0'. The main content area is titled 'ELISA DB Indices' and features a summary table and a detailed list of indices.

Storage	DataSize	MountPoint	Total	Used	Free	Used %
Data	114M	/var	8.5G	1.7G	6.8G	20%
Archive	2.1M	/var	8.5G	1.7G	6.8G	20%

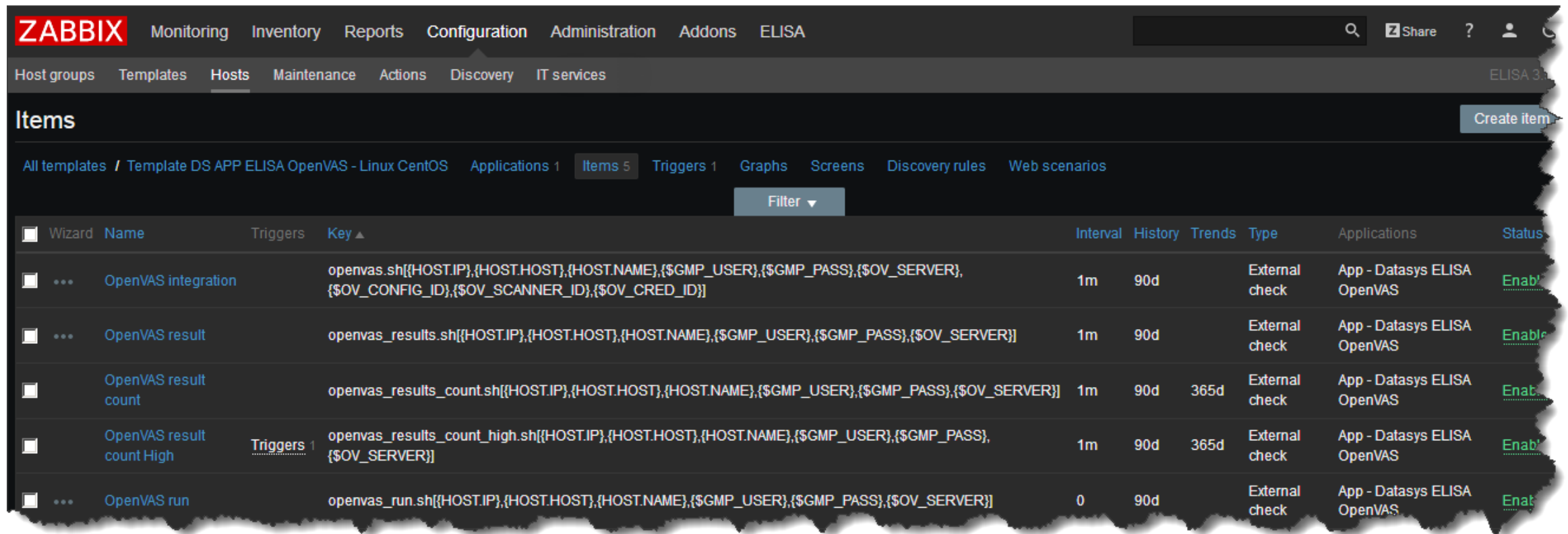
  

<input type="checkbox"/>	Name	Creation Date	Size	Log Events	Status	Action	Retention Mode	Integrity Check
<input type="checkbox"/>	logstash-2018.10.04	04.10.2018 00:00:03	6.42 MB	6 989	active	close archive	automatic	live
<input type="checkbox"/>	logstash-2018.10.03	03.10.2018 00:00:03	9.51 MB	16 808	active	close archive	automatic	pass
<input type="checkbox"/>	logstash-2018.10.02	02.10.2018 00:00:03	9.17 MB	16 910	active	close archive	automatic	pass
<input type="checkbox"/>	logstash-2018.10.01	01.10.2018 00:00:03	9.02 MB	16 571	active	close archive	automatic	pass
<input type="checkbox"/>	logstash-2018.09.30	30.09.2018 00:00:03	8.42 MB	16 077	active	close archive	automatic	pass
<input type="checkbox"/>	logstash-2018.09.29	29.09.2018 00:00:02	8.44 MB	16 125	active	close archive	automatic	pass
<input type="checkbox"/>	logstash-2018.09.28	28.09.2018 00:00:03	8.37 MB	16 132	active	close archive	automatic	pass
<input type="checkbox"/>	logstash-2018.09.27	27.09.2018 00:00:02	5.72 MB	9 235	active	close archive	automatic	pass
<input type="checkbox"/>	logstash-2018.09.26	26.09.2018 00:00:03	1.93 MB	3 541	active	close archive	automatic	pass
<input type="checkbox"/>	logstash-2018.09.25	25.09.2018 00:00:03	2.06 MB	3 557	active	close archive	automatic	pass
<input type="checkbox"/>	logstash-2018.09.24	24.09.2018 00:00:03	2.17 MB	3 793	active	close archive	automatic	pass
<input type="checkbox"/>	logstash-2018.09.23	23.09.2018 00:00:04	1.63 MB		closed	open archive	automatic	
<input type="checkbox"/>	logstash-2018.09.22	22.09.2018 00:00:03	1.54 MB		closed	open archive	automatic	



# NOVINKY ELISA 4.0

- Integrate s Greenbone Security Manager (OpenVAS)

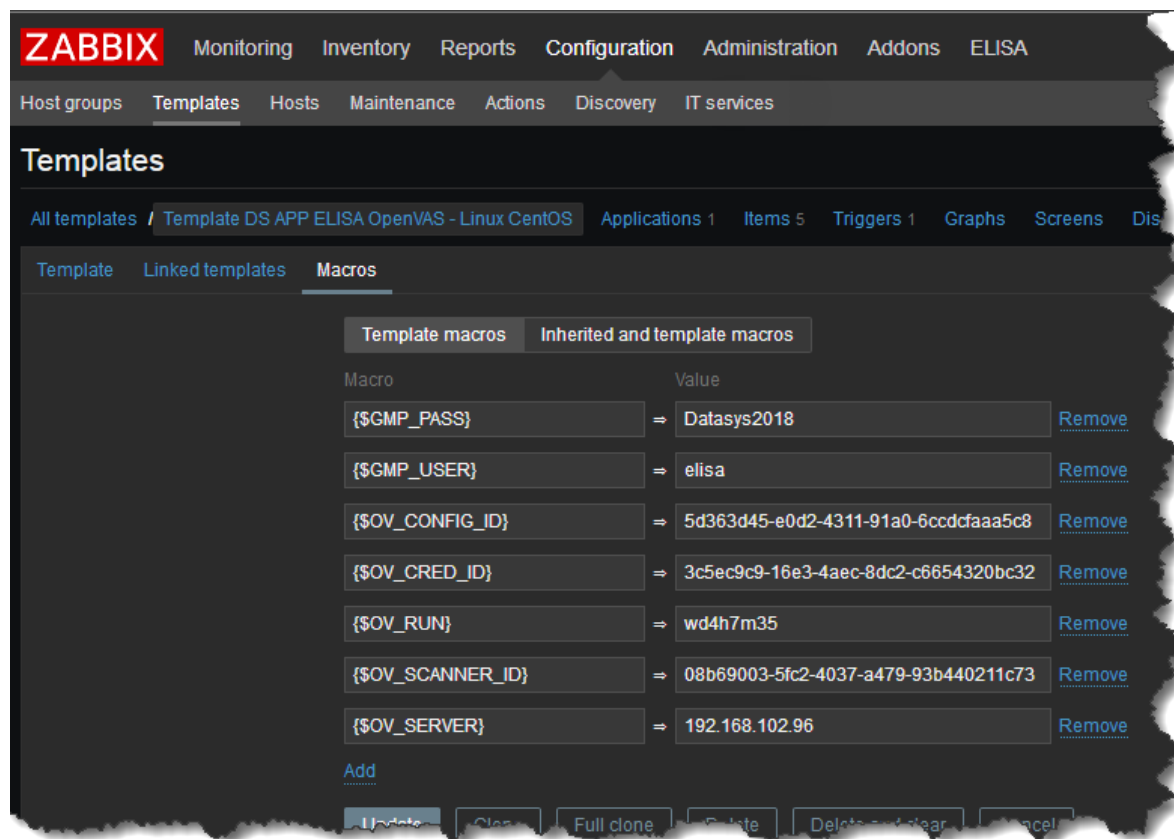


The screenshot displays the Zabbix web interface for the 'ELISA' application. The 'Items' section is active, showing a list of configuration items for OpenVAS integration. The interface includes a navigation menu at the top with options like Monitoring, Inventory, Reports, Configuration, Administration, Addons, and ELISA. Below the navigation, there are tabs for Host groups, Templates, Hosts, Maintenance, Actions, Discovery, and IT services. The main content area shows a list of items with columns for Name, Triggers, Key, Interval, History, Trends, Type, Applications, and Status. The items listed are:

Wizard	Name	Triggers	Key	Interval	History	Trends	Type	Applications	Status
<input type="checkbox"/>	OpenVAS integration		openvas.sh[{{HOST.IP}},{{HOST.HOST}},{{HOST.NAME}},{{GMP_USER}},{{GMP_PASS}},{{OV_SERVER}},{{OV_CONFIG_ID}},{{OV_SCANNER_ID}},{{OV_CRED_ID}}]	1m	90d		External check	App - Datasys ELISA OpenVAS	Enabled
<input type="checkbox"/>	OpenVAS result		openvas_results.sh[{{HOST.IP}},{{HOST.HOST}},{{HOST.NAME}},{{GMP_USER}},{{GMP_PASS}},{{OV_SERVER}}]	1m	90d		External check	App - Datasys ELISA OpenVAS	Enabled
<input type="checkbox"/>	OpenVAS result count		openvas_results_count.sh[{{HOST.IP}},{{HOST.HOST}},{{HOST.NAME}},{{GMP_USER}},{{GMP_PASS}},{{OV_SERVER}}]	1m	90d	365d	External check	App - Datasys ELISA OpenVAS	Enabled
<input type="checkbox"/>	OpenVAS result count High	Triggers 1	openvas_results_count_high.sh[{{HOST.IP}},{{HOST.HOST}},{{HOST.NAME}},{{GMP_USER}},{{GMP_PASS}},{{OV_SERVER}}]	1m	90d	365d	External check	App - Datasys ELISA OpenVAS	Enabled
<input type="checkbox"/>	OpenVAS run		openvas_run.sh[{{HOST.IP}},{{HOST.HOST}},{{HOST.NAME}},{{GMP_USER}},{{GMP_PASS}},{{OV_SERVER}}]	0	90d		External check	App - Datasys ELISA OpenVAS	Enabled

# NOVINKY ELISA 4.0

- Integrate s Greenbone Security Manager (OpenVAS)



The screenshot shows the Zabbix web interface. The top navigation bar includes 'ZABBIX' and menu items: 'Monitoring', 'Inventory', 'Reports', 'Configuration', 'Administration', 'Addons', and 'ELISA'. Below this, a secondary navigation bar has 'Host groups', 'Templates', 'Hosts', 'Maintenance', 'Actions', 'Discovery', and 'IT services'. The main content area is titled 'Templates' and shows a breadcrumb path: 'All templates / Template DS APP ELISA OpenVAS - Linux CentOS'. Underneath, there are tabs for 'Template', 'Linked templates', and 'Macros'. The 'Macros' tab is active, showing a table of 'Template macros' and 'Inherited and template macros'. The table has two columns: 'Macro' and 'Value'. Each row contains a macro name, its value, and a 'Remove' link.

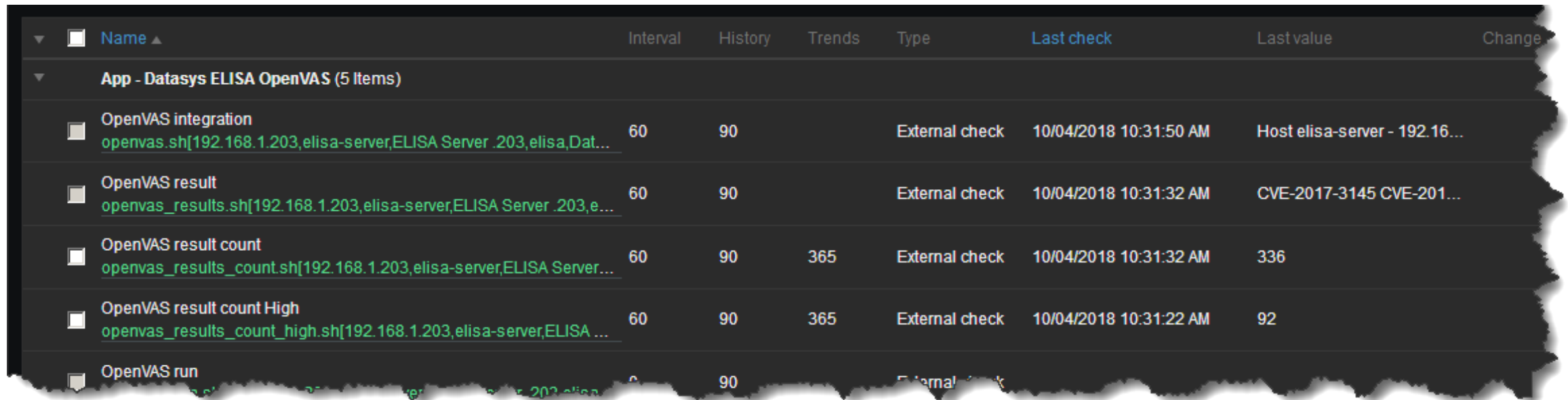
Macro	Value	
{GMP_PASS}	Datsys2018	<a href="#">Remove</a>
{GMP_USER}	elisa	<a href="#">Remove</a>
{SOV_CONFIG_ID}	5d363d45-e0d2-4311-91a0-6ccdcfaaa5c8	<a href="#">Remove</a>
{SOV_CRED_ID}	3c5ec9c9-16e3-4aec-8dc2-c6654320bc32	<a href="#">Remove</a>
{SOV_RUN}	wd4h7m35	<a href="#">Remove</a>
{SOV_SCANNER_ID}	08b69003-5fc2-4037-a479-93b440211c73	<a href="#">Remove</a>
{SOV_SERVER}	192.168.102.96	<a href="#">Remove</a>

At the bottom of the table, there is an 'Add' link and a row of buttons: 'Update', 'Clone', 'Full clone', 'Delete', 'Delete and clear', and 'Cancel'.

Využití Zabbix Maker pro konfiguraci skenů

# NOVINKY ELISA 4.0

- Integrate s Greenbone Security Manager (OpenVAS)



The screenshot displays a monitoring dashboard for 'App - Datasys ELISA OpenVAS' with 5 items. The table lists various checks with their intervals, history, trends, types, last check times, and last values.

Name	Interval	History	Trends	Type	Last check	Last value	Change
<b>App - Datasys ELISA OpenVAS (5 Items)</b>							
OpenVAS integration <a href="#">openvas.sh[192.168.1.203,elisa-server,ELISA Server .203,elisa,Dat...</a>	60	90		External check	10/04/2018 10:31:50 AM	Host elisa-server - 192.16...	
OpenVAS result <a href="#">openvas_results.sh[192.168.1.203,elisa-server,ELISA Server .203,e...</a>	60	90		External check	10/04/2018 10:31:32 AM	CVE-2017-3145 CVE-201...	
OpenVAS result count <a href="#">openvas_results_count.sh[192.168.1.203,elisa-server,ELISA Server...</a>	60	90	365	External check	10/04/2018 10:31:32 AM	336	
OpenVAS result count High <a href="#">openvas_results_count_high.sh[192.168.1.203,elisa-server,ELISA ...</a>	60	90	365	External check	10/04/2018 10:31:22 AM	92	
OpenVAS run <a href="#">openvas_run.sh[192.168.1.203,elisa-server,ELISA Server .203,elisa...</a>	60	90		External check	10/04/2018 10:31:22 AM		

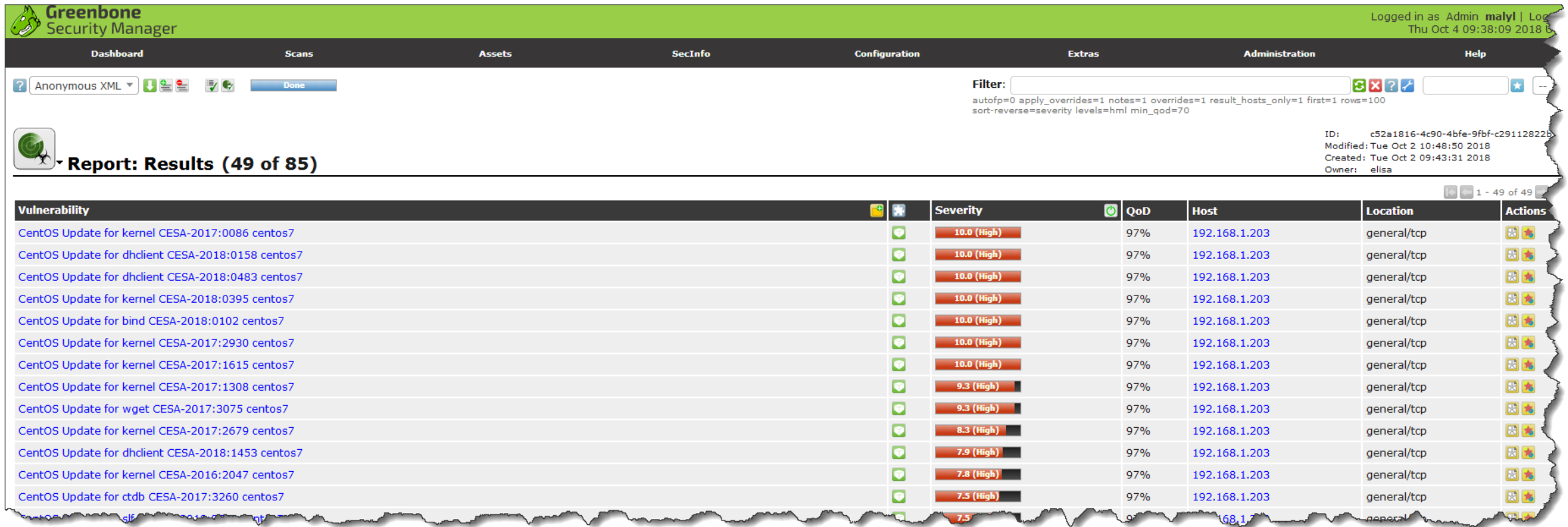
# NOVINKY ELISA 4.0

- Integrate s Greenbone Security Manager (OpenVAS)



# NOVINKY ELISA 4.0

- Integrate s Greenbone Security Manager (OpenVAS)



Greenbone Security Manager

Logged in as Admin malyi | Log out Thu Oct 4 09:38:09 2018

Dashboard Scans Assets SecInfo Configuration Extras Administration Help

Anonymous XML Done

Filter: autofp=0 apply\_overrides=1 notes=1 overrides=1 result\_hosts\_only=1 first=1 rows=100 sort-reverse=severity levels=hml min\_qod=70

Report: Results (49 of 85)

ID: c52a1816-4c90-4bfe-9fbf-c29112822b  
Modified: Tue Oct 2 10:48:50 2018  
Created: Tue Oct 2 09:43:31 2018  
Owner: elisa

Vulnerability	Severity	QoD	Host	Location	Actions
CentOS Update for kernel CESA-2017:0086 centos7	10.0 (High)	97%	192.168.1.203	general/tcp	
CentOS Update for dhclient CESA-2018:0158 centos7	10.0 (High)	97%	192.168.1.203	general/tcp	
CentOS Update for dhclient CESA-2018:0483 centos7	10.0 (High)	97%	192.168.1.203	general/tcp	
CentOS Update for kernel CESA-2018:0395 centos7	10.0 (High)	97%	192.168.1.203	general/tcp	
CentOS Update for bind CESA-2018:0102 centos7	10.0 (High)	97%	192.168.1.203	general/tcp	
CentOS Update for kernel CESA-2017:2930 centos7	10.0 (High)	97%	192.168.1.203	general/tcp	
CentOS Update for kernel CESA-2017:1615 centos7	10.0 (High)	97%	192.168.1.203	general/tcp	
CentOS Update for kernel CESA-2017:1308 centos7	9.3 (High)	97%	192.168.1.203	general/tcp	
CentOS Update for wget CESA-2017:3075 centos7	9.3 (High)	97%	192.168.1.203	general/tcp	
CentOS Update for kernel CESA-2017:2679 centos7	8.3 (High)	97%	192.168.1.203	general/tcp	
CentOS Update for dhclient CESA-2018:1453 centos7	7.9 (High)	97%	192.168.1.203	general/tcp	
CentOS Update for kernel CESA-2016:2047 centos7	7.8 (High)	97%	192.168.1.203	general/tcp	
CentOS Update for ctdb CESA-2017:3260 centos7	7.5 (High)	97%	192.168.1.203	general/tcp	

# DĚKUJI ZA POZORNOST

**Lukáš MALÝ**

*Konzultant bezpečnost a  
monitoring*

maly@datasys.cz  
+420 225 308 640



datasyscz



datasys



datasysds



+420 225 308 111



datasys@datasys.cz

**D A T A . . . . .**  
**S Y S**

# POZNÁMKY

