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.

DATA SYS

ELISA

Event **L**og
Interception
Storage and
Analysis

ELISA Security Manager

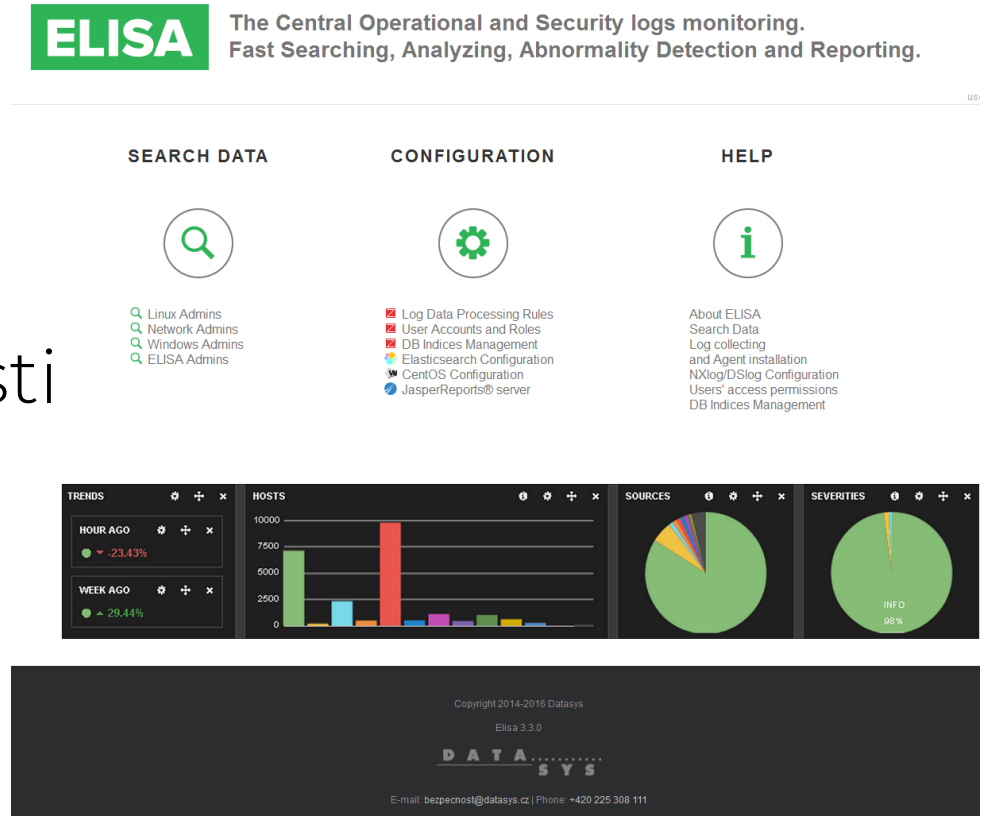
Robustní nástroj pro sběr a analýzu bezpečnostních událostí

- **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

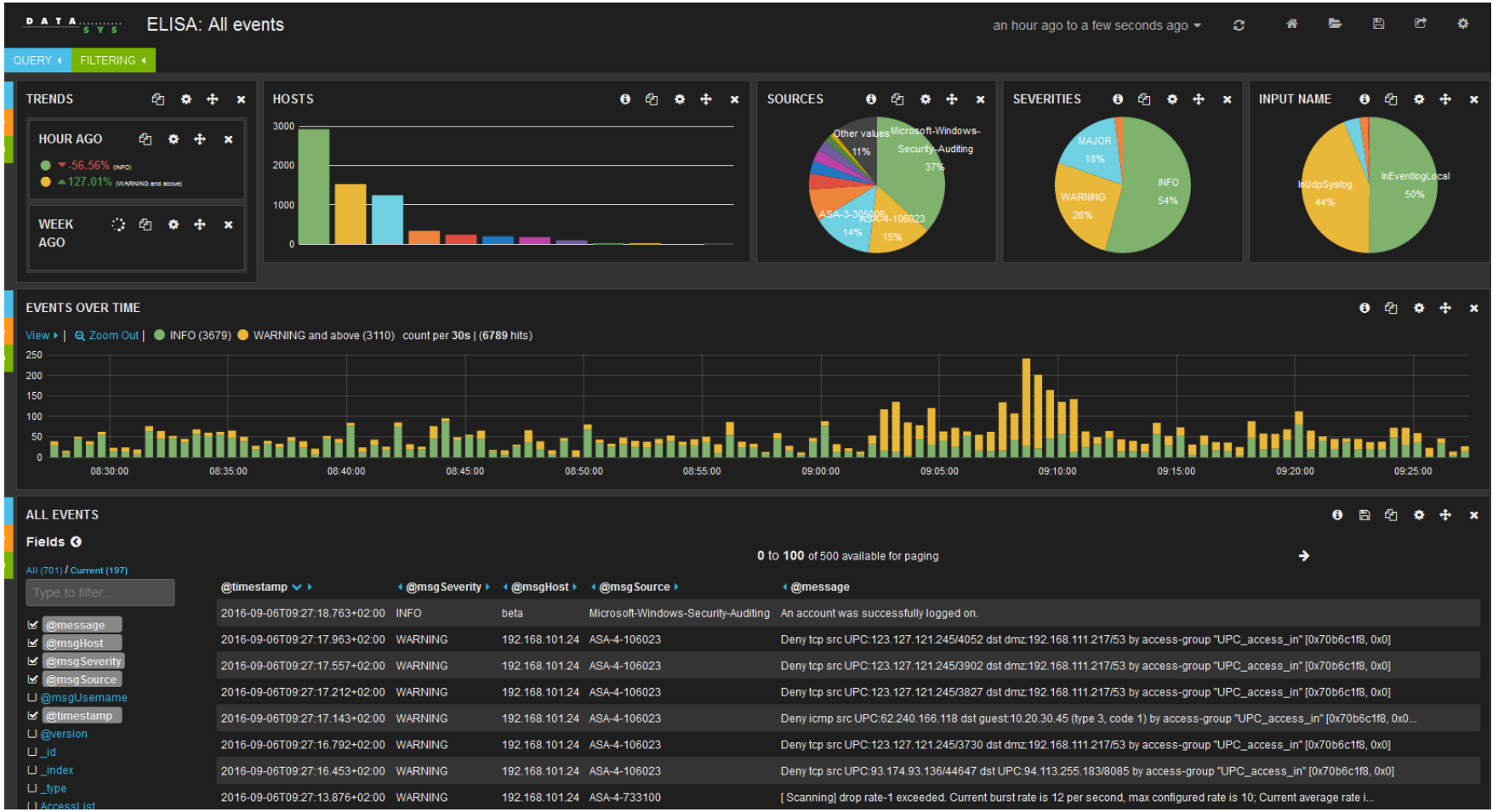
- Portál pro Kibana a Zabbix
- Používá Free Software
- Zachová strukturu původní události
- Webové rozhraní Kibana 3
- Vysoký výkon (až 5 000 eps)



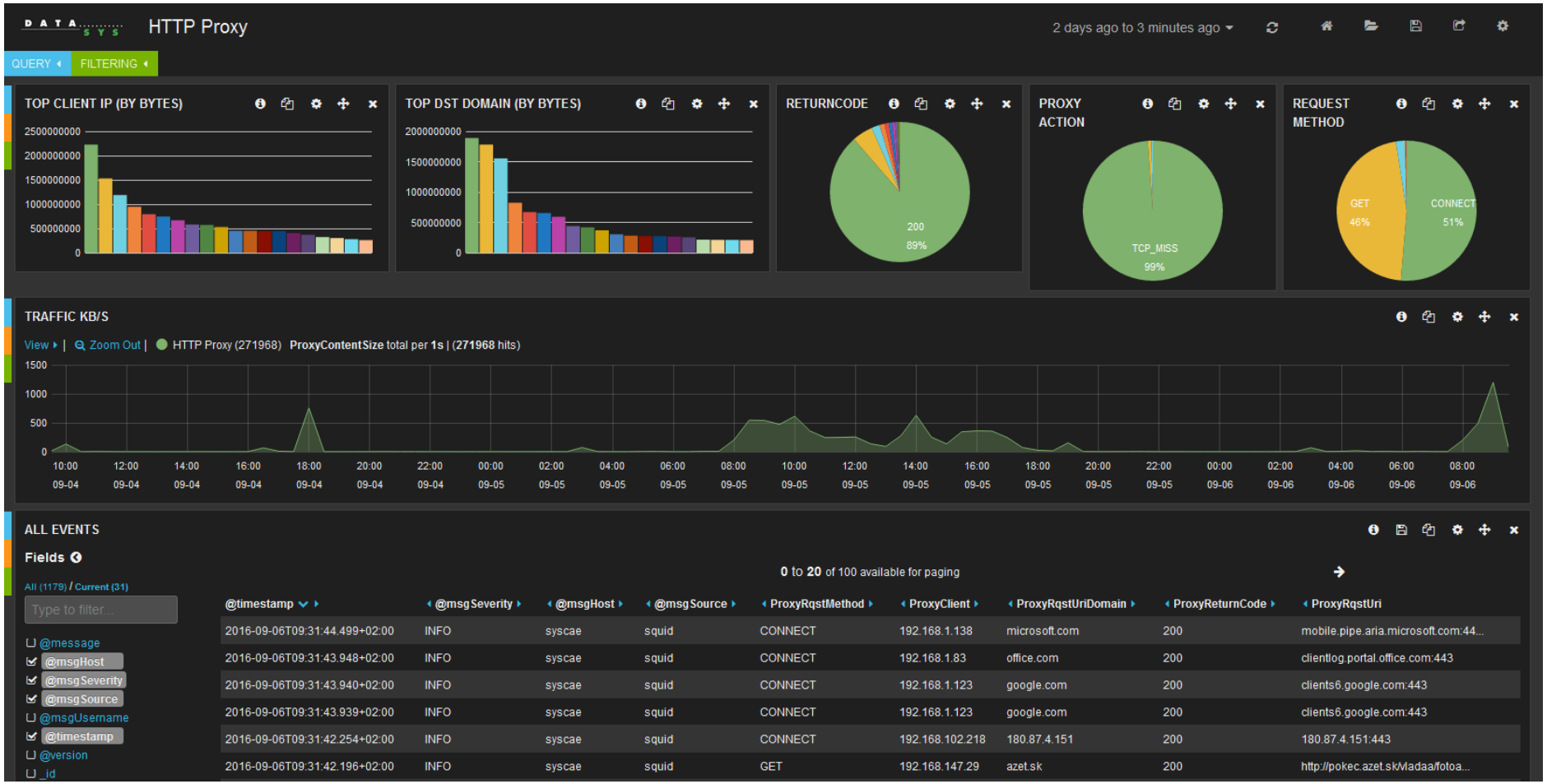
Hlavní vstupní kanály ELISA

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

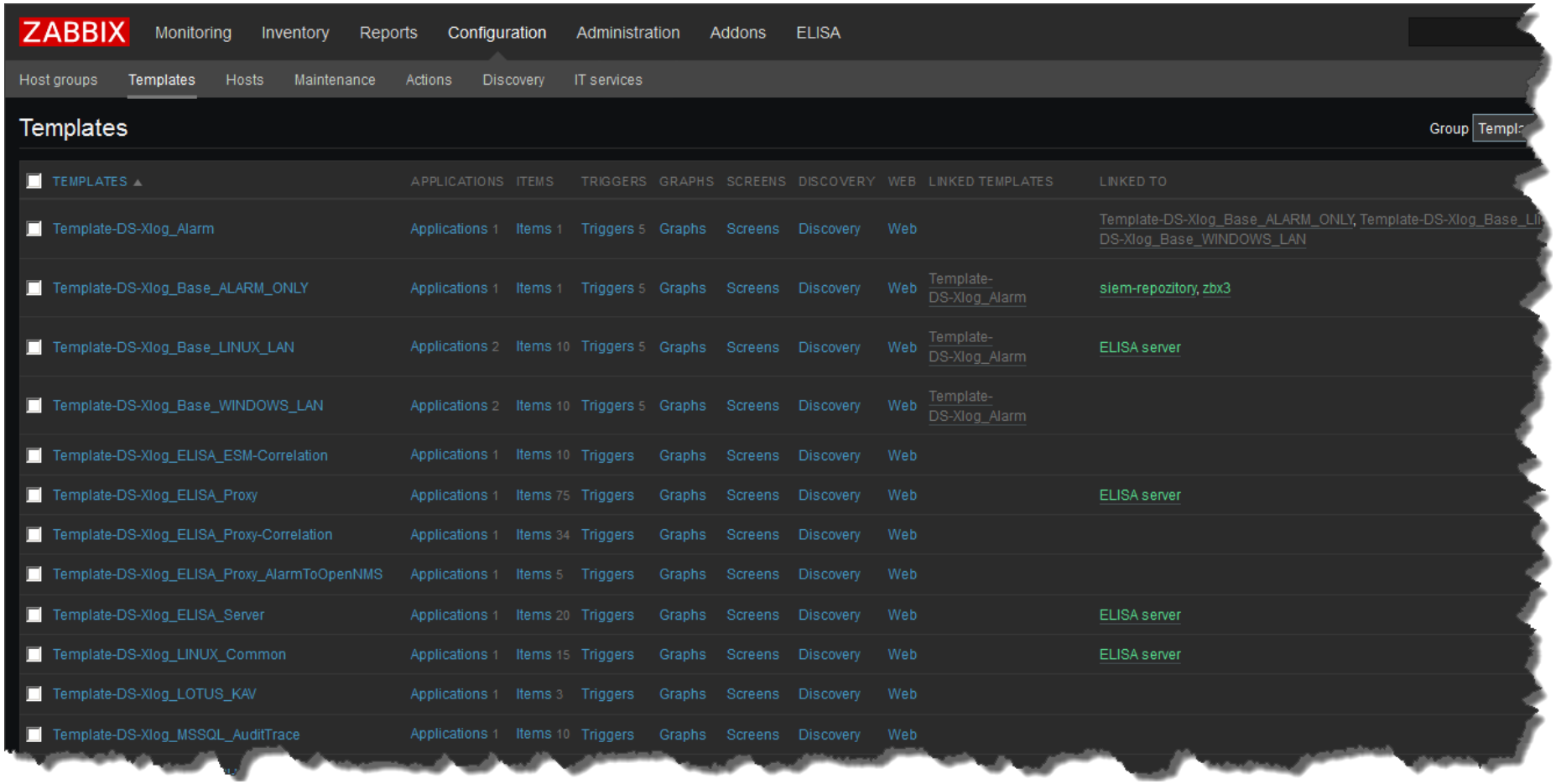
Vylepšená Kibana jako frontend pro analýzu dat



KIBANA JE FLEXIBILNÍ ROZHRANÍ



Pomocí ZABBIX šablon nastavujeme NXLog



Komponenty ELISA

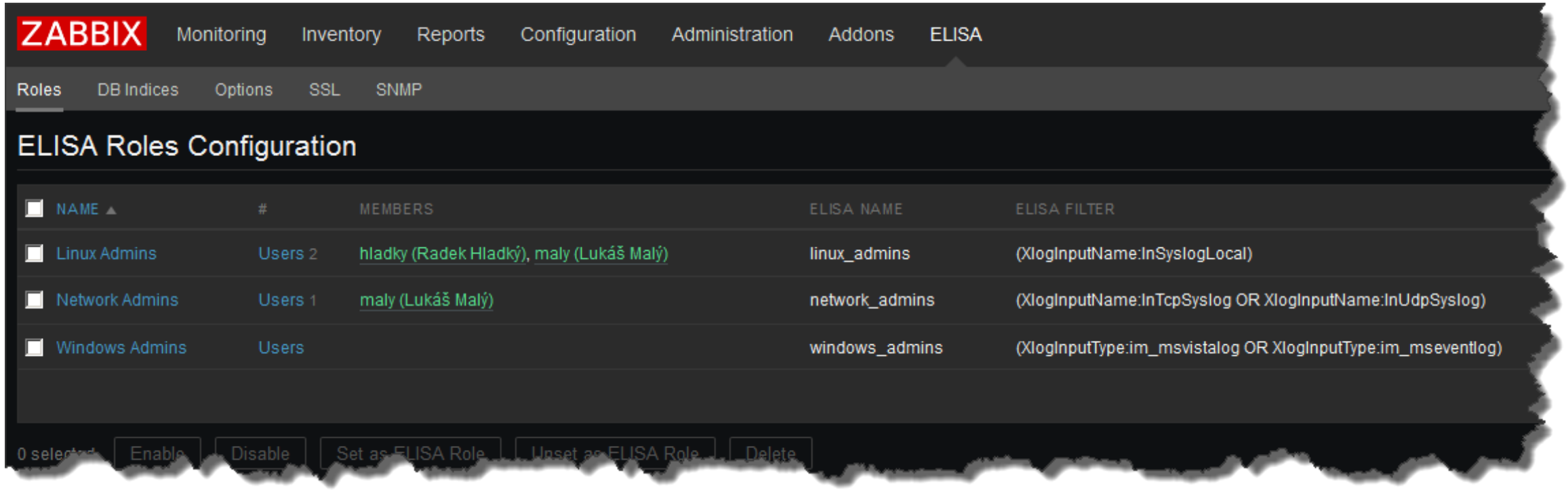
- Elasticsearch, Kibana
- NXLog (Enterprice edition)
- Zabbix, Xlog, HTTPd Apache s mod_authnz_external
- JasperReport Server s pluginem ElasticJasper
- Memcached

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

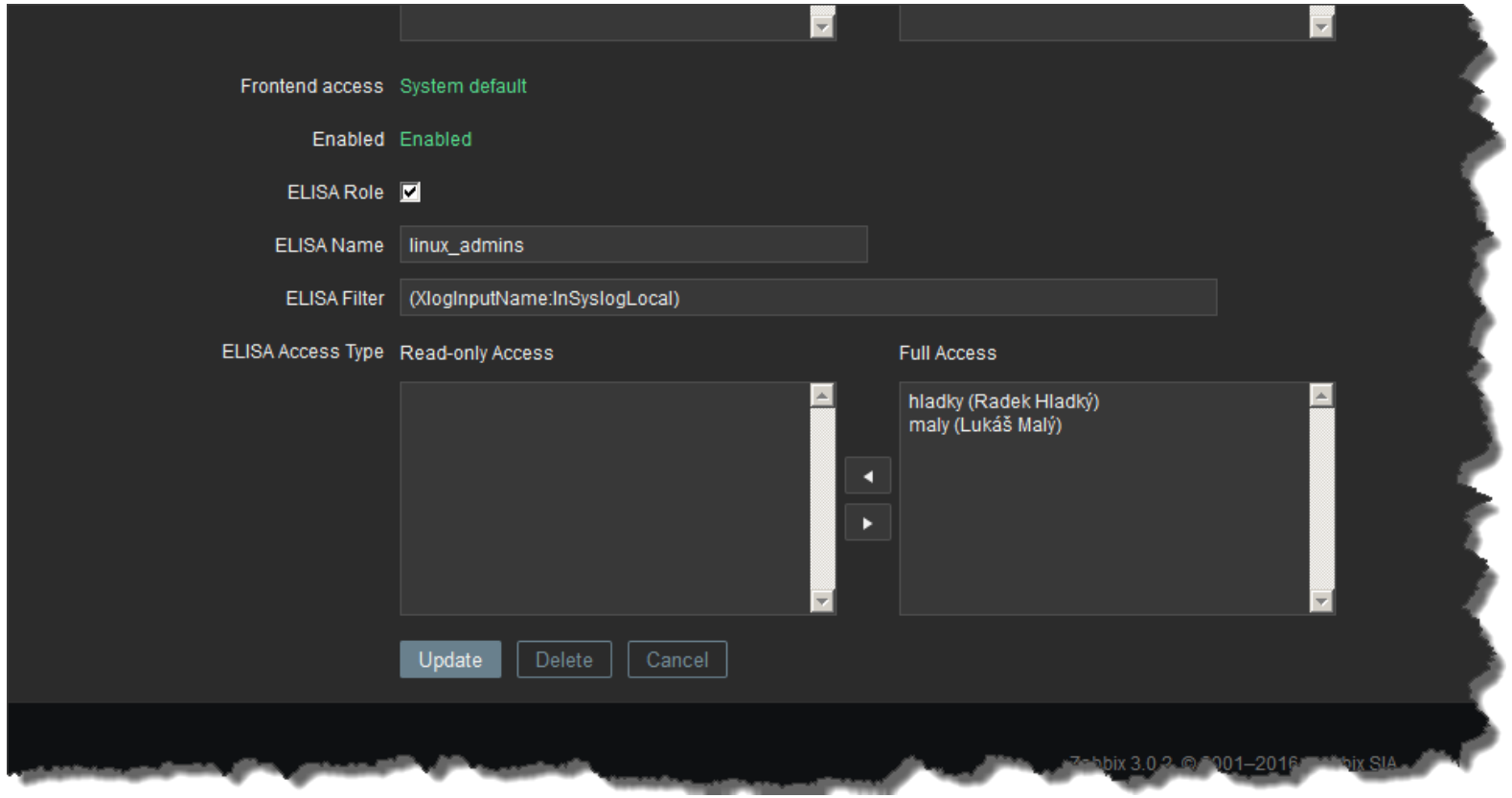
ELISA využívá funkcionalit ZABBIXu

- Ověřování uživatelů a řízení přístupu založené na rolích



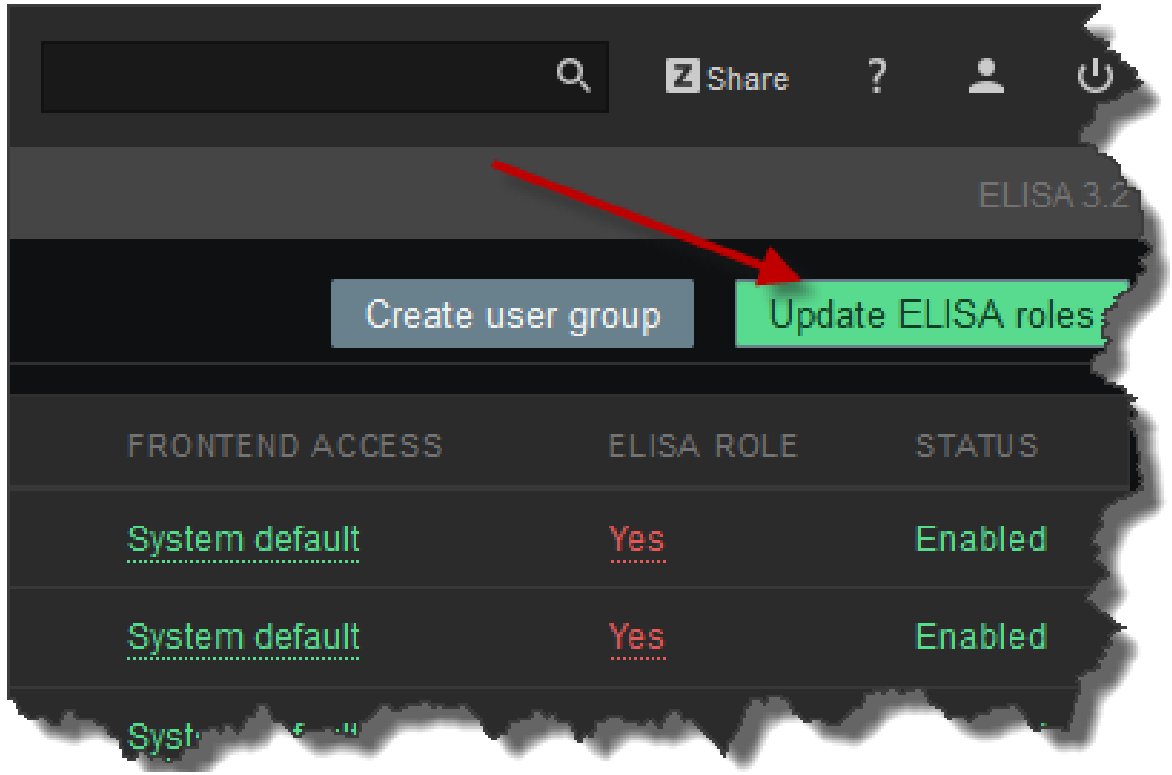
ELISA využívá funkcionalit ZABBIXu

- Ověřování uživatelů a řízení přístupu založené na rolích



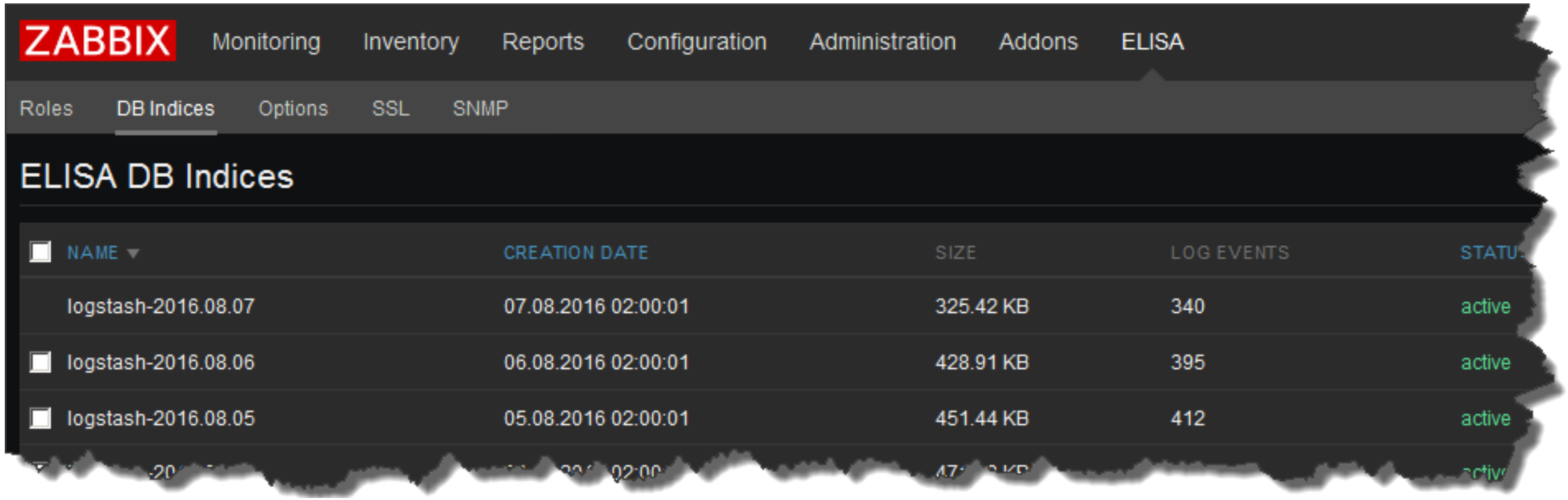
ELISA VYUŽÍVÁ FUNKCIONALIT ZABBIXU

- Ověřování uživatelů a řízení přístupu založené na rolích



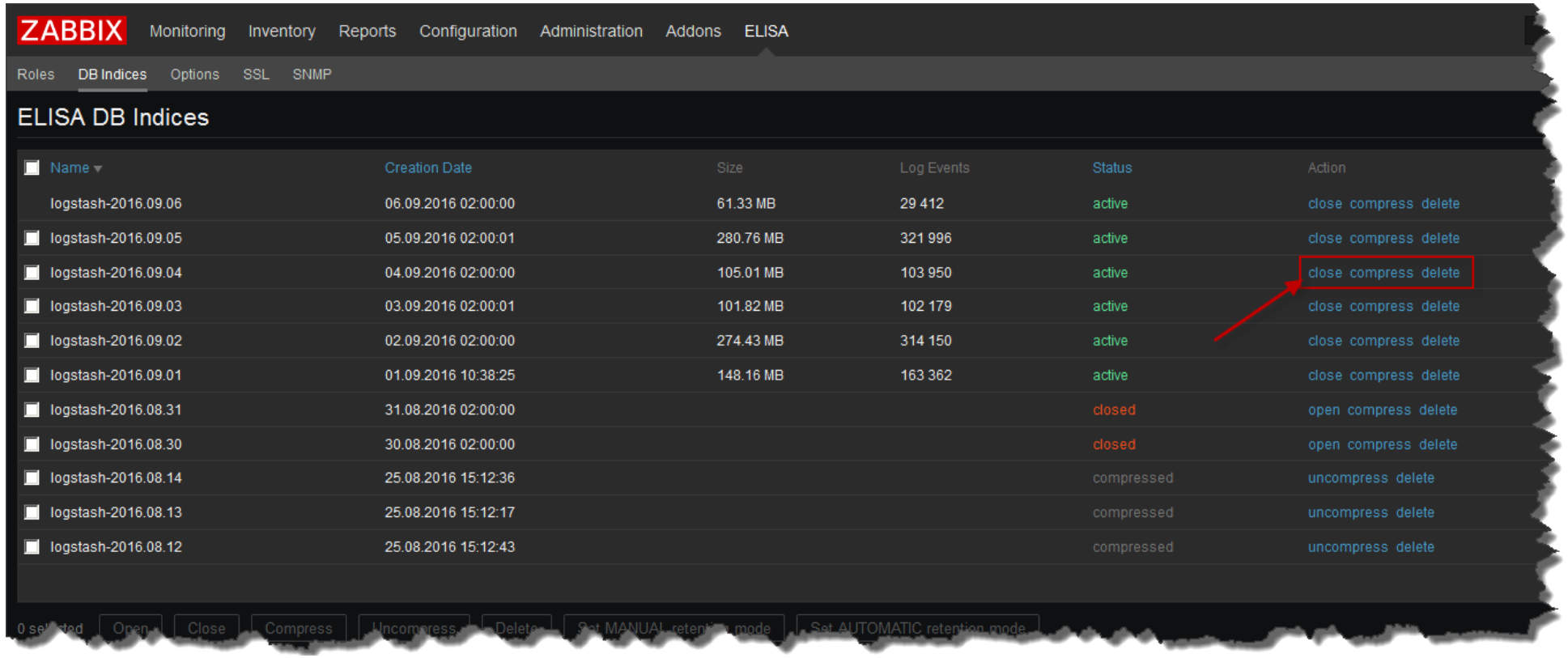
ZABBIX INTEGROVÁN DO ELISA

- ELK indexy jsou spravovány přímo v ZABBIX Frontend.



ZABBIX INTEGROVÁN DO ELISA

- ELK indexy jsou spravovány přímo v ZABBIX Frontend.



ZABBIX INTEGROVÁN DO ELISA

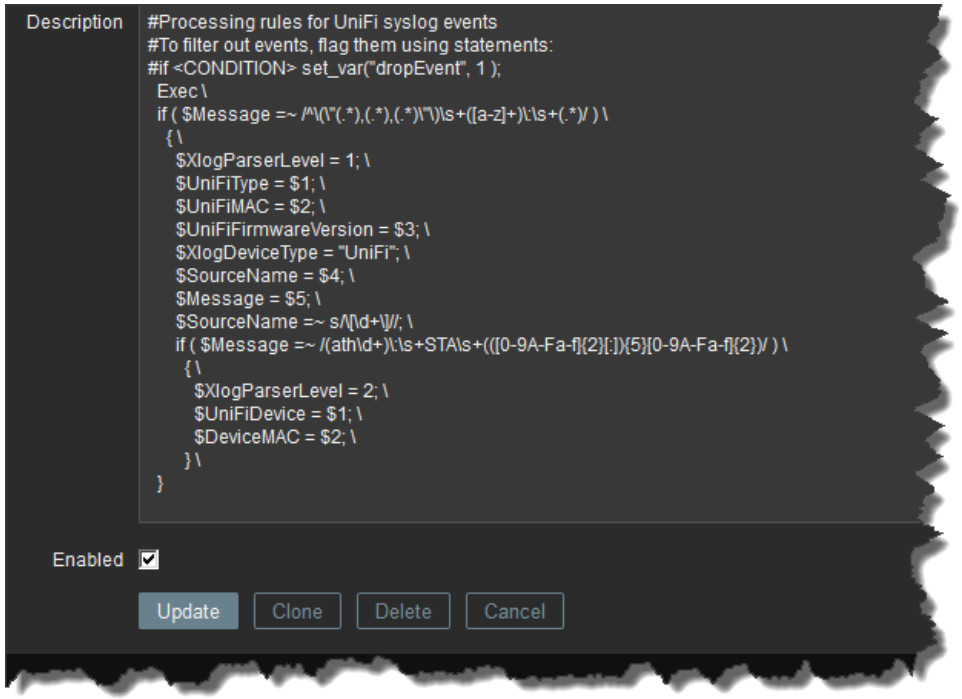
- K centrální správě konfigurace distribuovaného prostředí agentů NXLog se používají - ZABBIX Item type "trapper„.

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.



NXLOG MODULY

- xm_* - Extension Modules
- im_* - Input Modules
- pm_* - Processor Modules
- om_* - Output Modules

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

NXLOG MODULY

- im_ssl
- om_elasticsearch
- pm_buffer, pm_null
- xm_perl, xm_snmp, xm_kvp, xm_csv, xm_fileop, xm_exec,
- xm_charconv, xm_syslog, xm_json

https://nxlog.co/documentation/nxlog-user-guide#modules_list

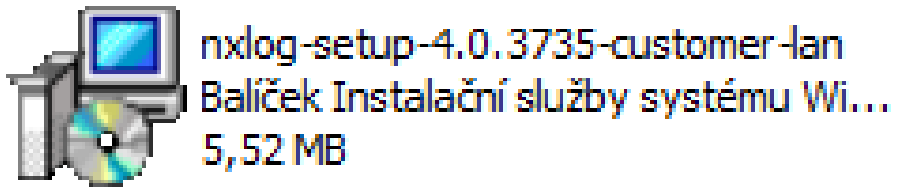
NXLOG.CONF

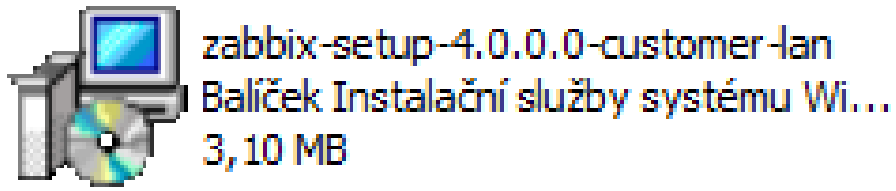
- Počet řádků konfiguračního souboru nxlog

```
[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





Autoregistrace agentů do ELISA

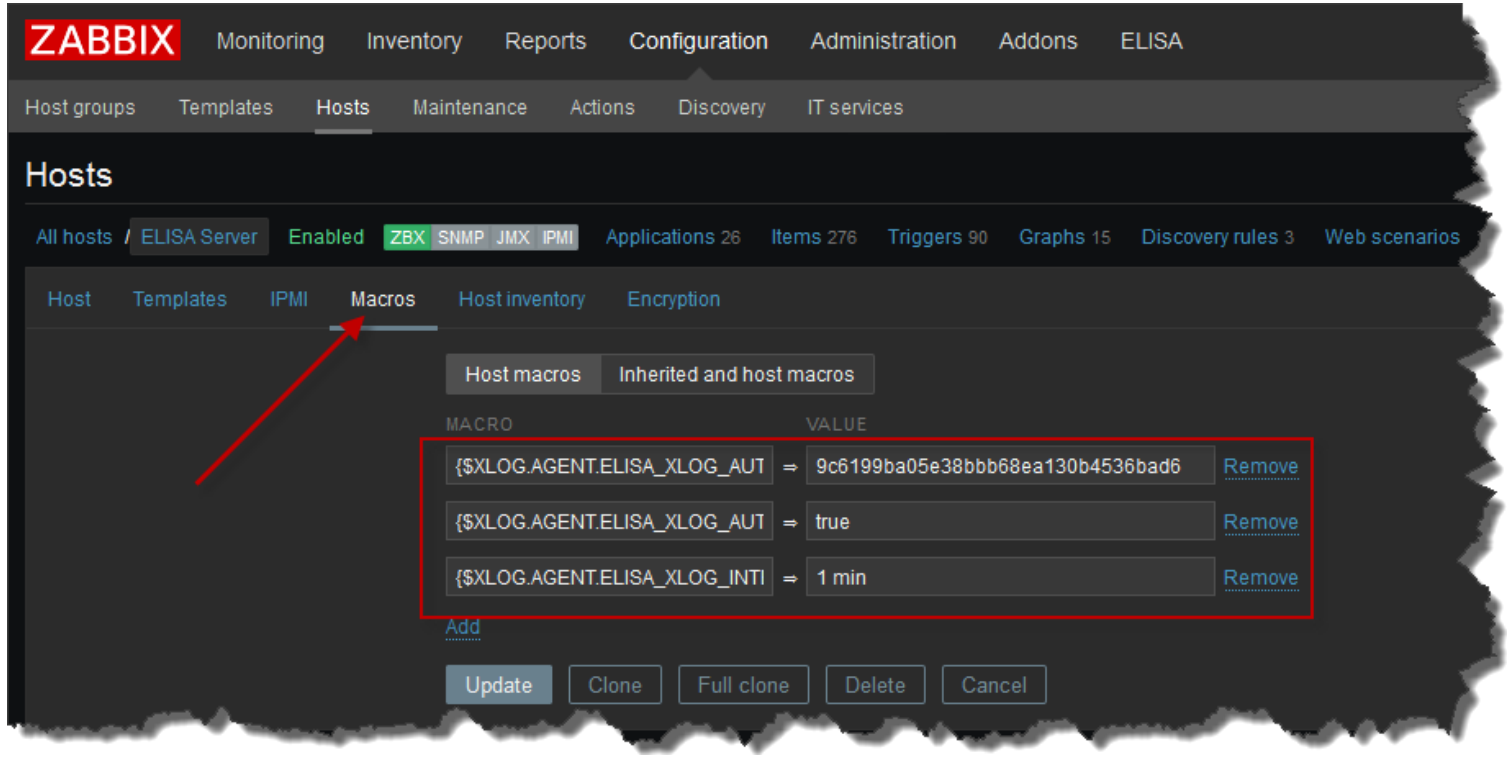
- Zabbix Agent – většina Linux distribucí, *BSD, AIX
- NXLog Agent - většina Linux distribucí, AIX

```
[root@elisa-dev-4 nxlog]# ls -1
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"



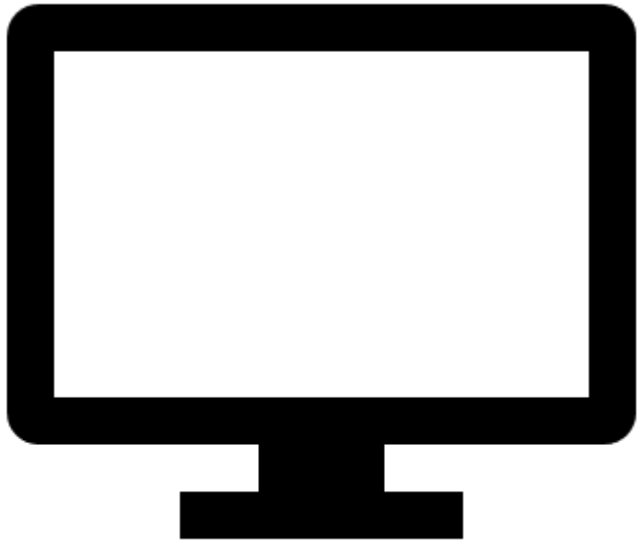
ELISA Proxy

- Zabbix Proxy

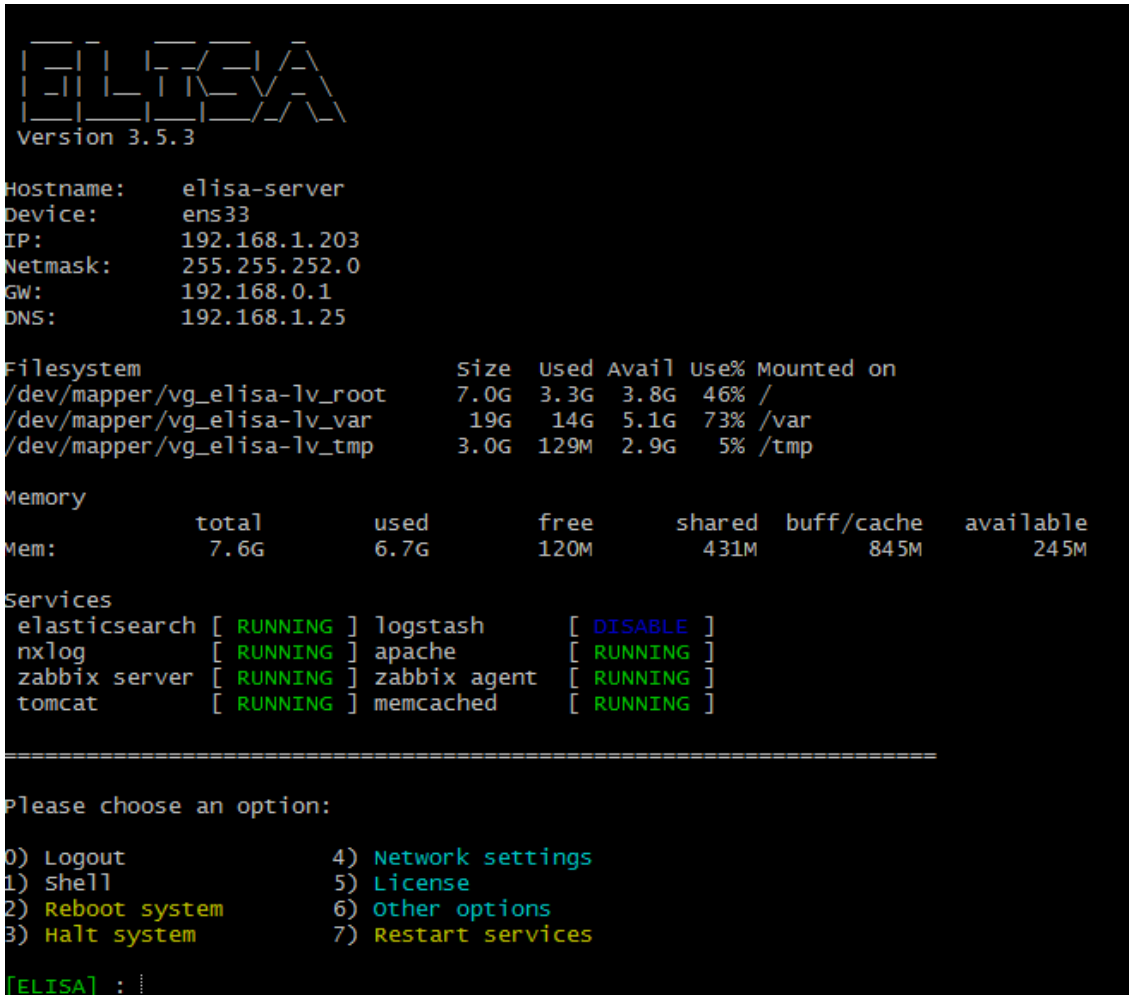
- ELISA Proxy

  - NXLog

  - XLog



ELISA APPLIANCE

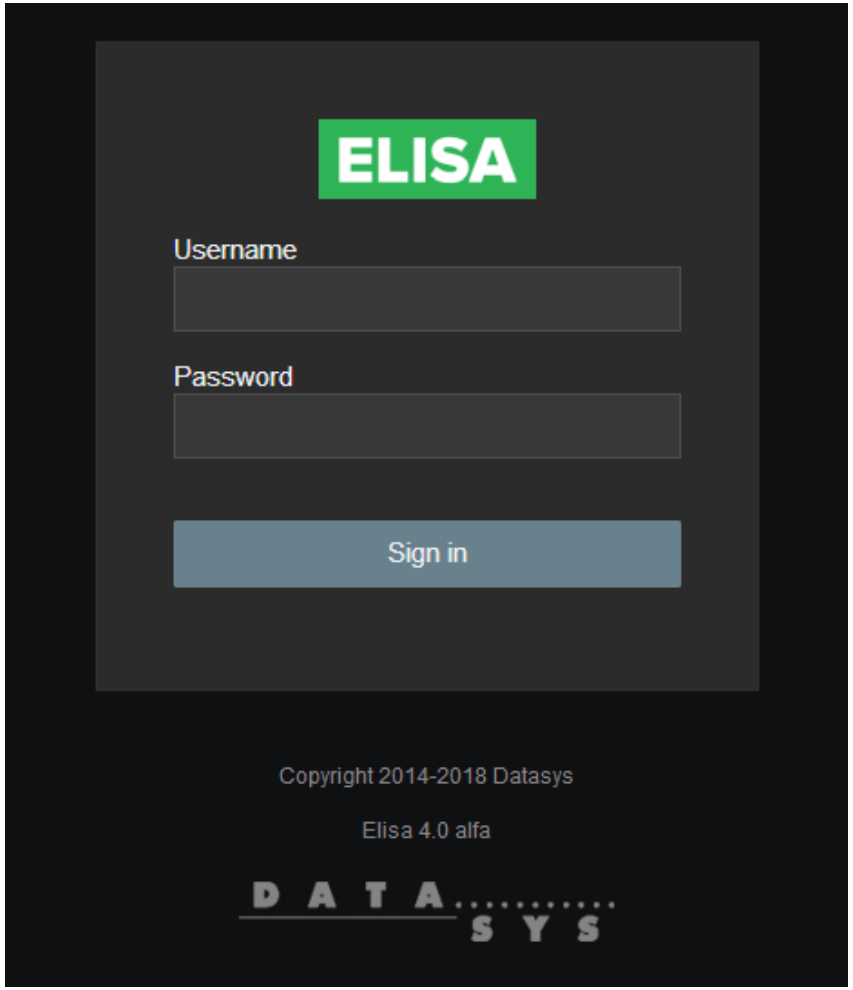


- ELISA menu, pro základní úkony v systému
- Změna IPv4
- Restart komponent

Novinky ELISA 4.0

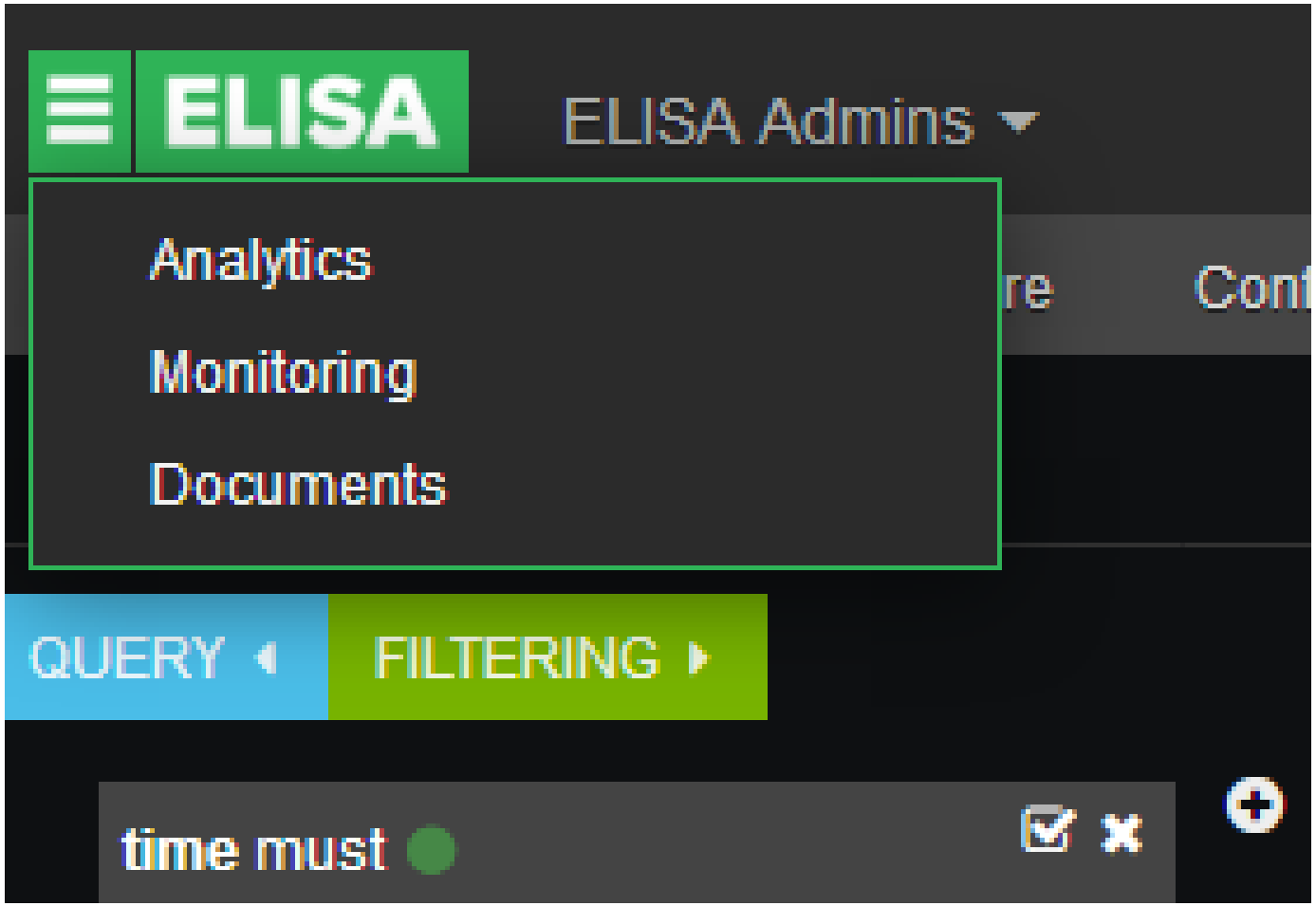
- Zabbix 4.0 LTS
- Elasticsearch 6.4
- NXLog 4.0
- Propojení dvou systémů do jedné Web konzole
- Integrace s OpenVAS a Flowmon APM

Novinky ELISA 4.0



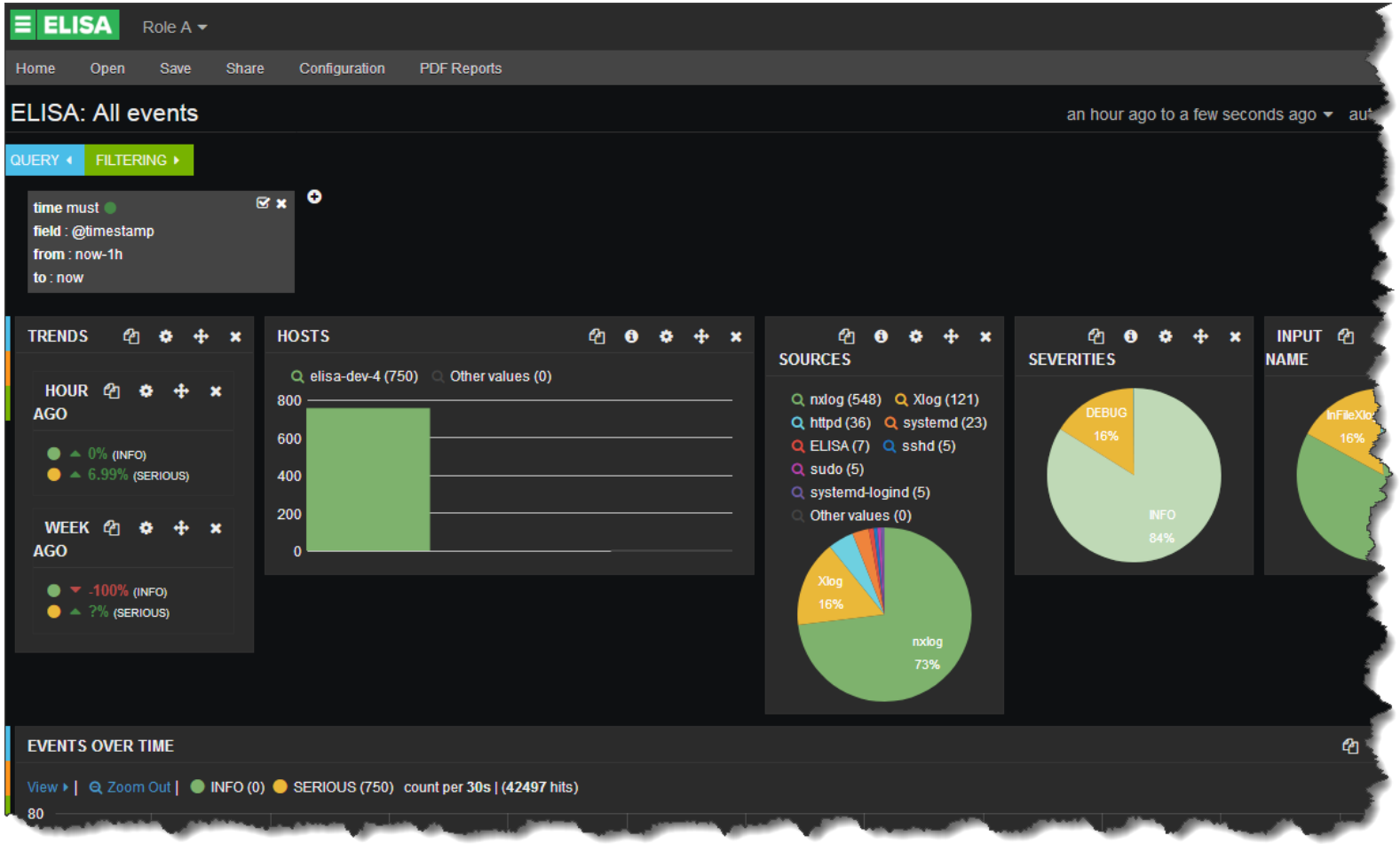
- Nové přihlášení do ELISA

Novinky ELISA 4.0



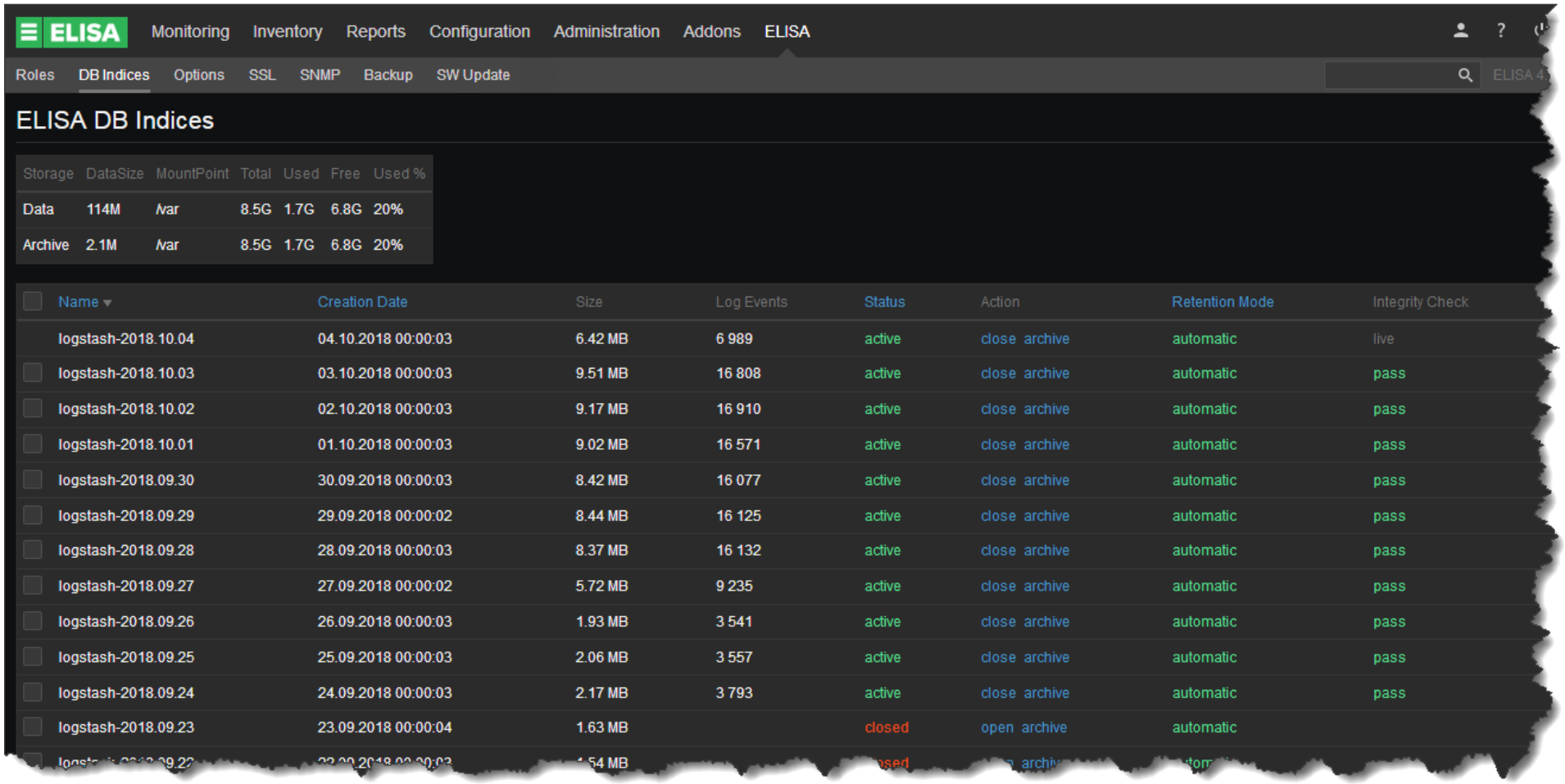
- Navigační lišta

Novinky ELISA 4.0



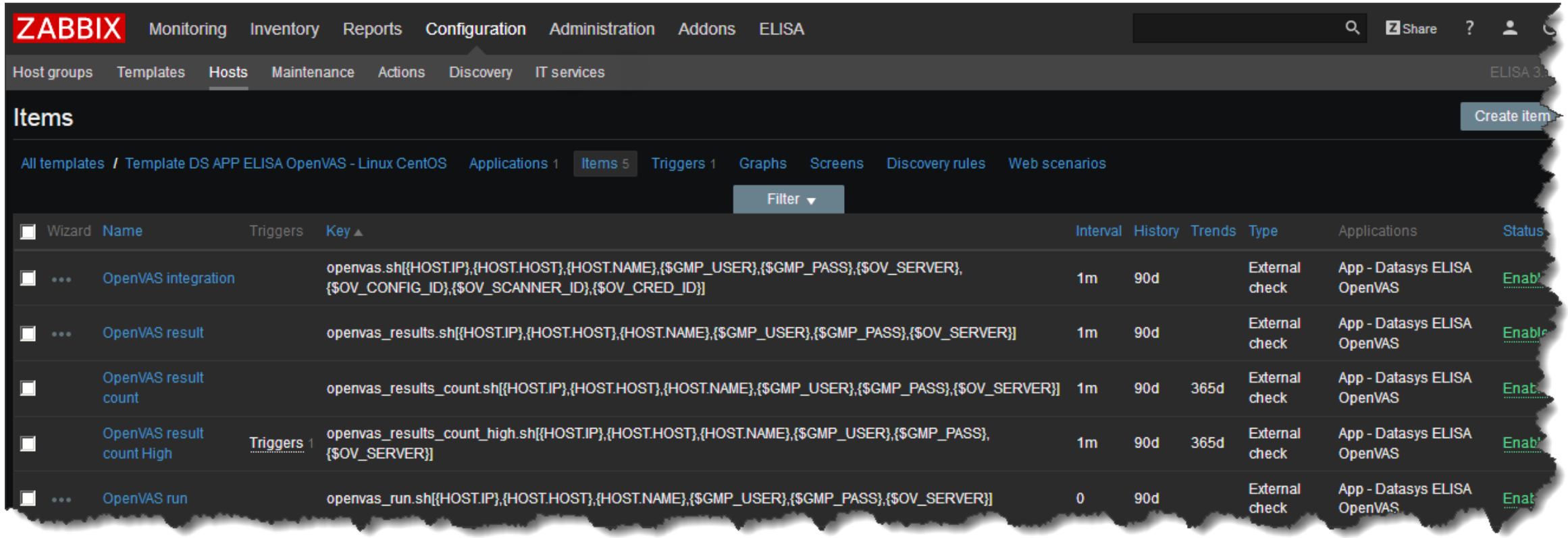
- Kibana 3

Novinky ELISA 4.0



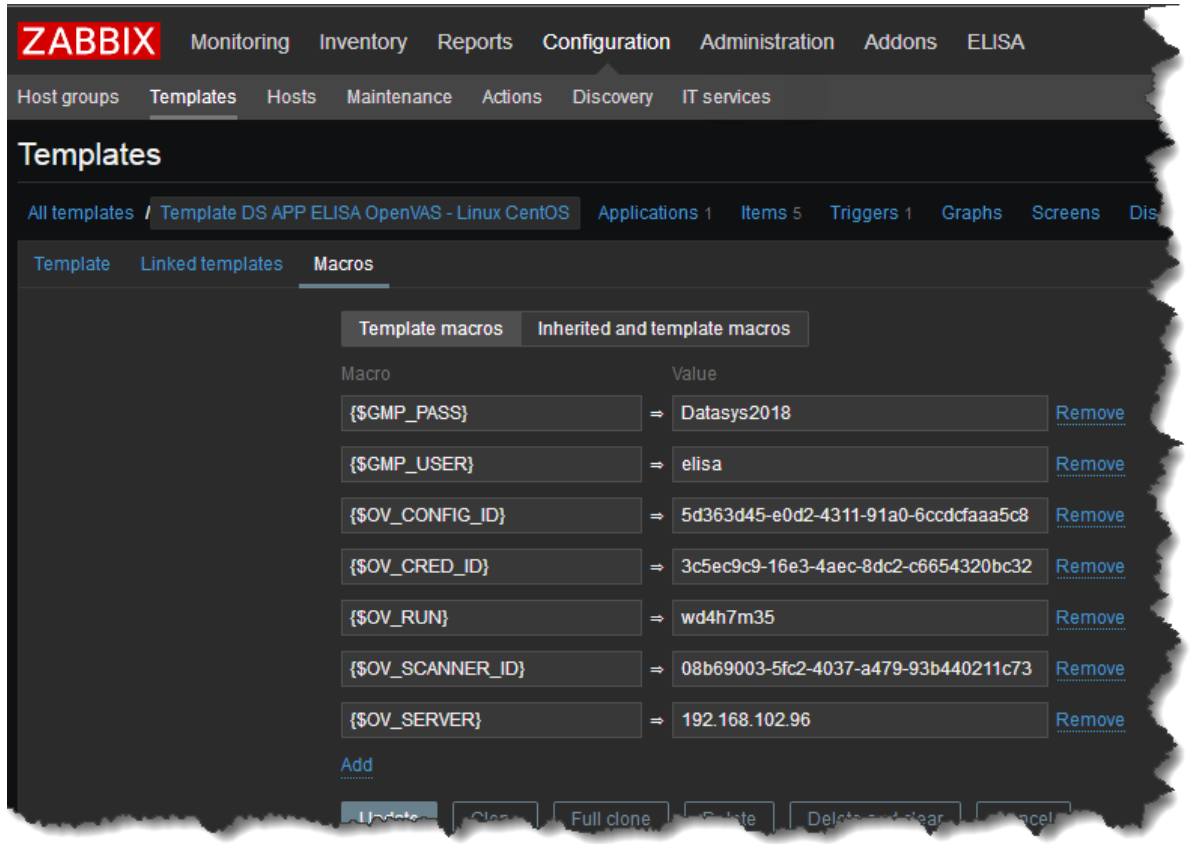
Novinky ELISA 4.0

- Integrace s Greenbone Security Manager (OpenVAS)



NOVINKY ELISA 4.0

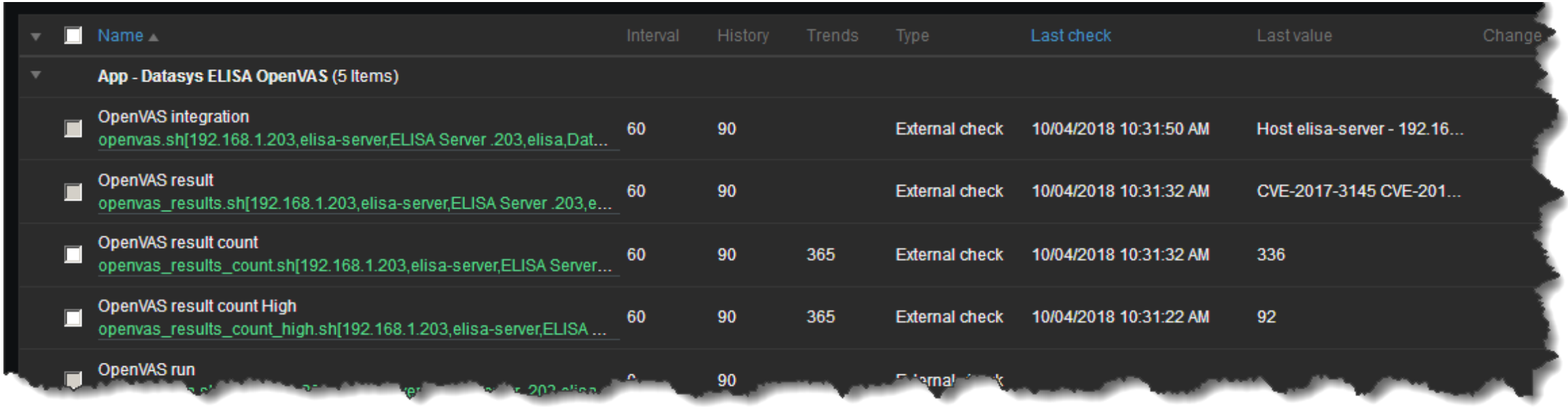
- Integrace s Greenbone Security Manager (OpenVAS)



Využití Zabbix Maker pro konfiguraci skenů

Novinky ELISA 4.0

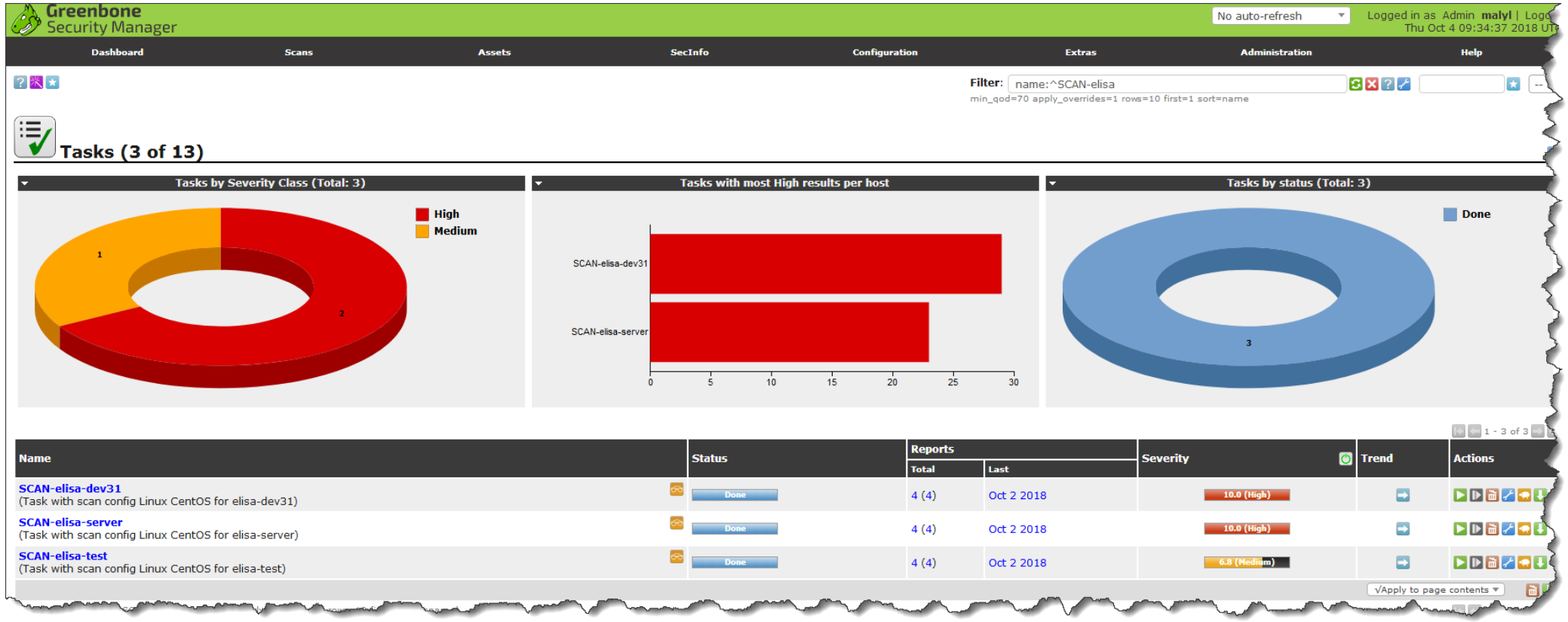
- Integrace s Greenbone Security Manager (OpenVAS)



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

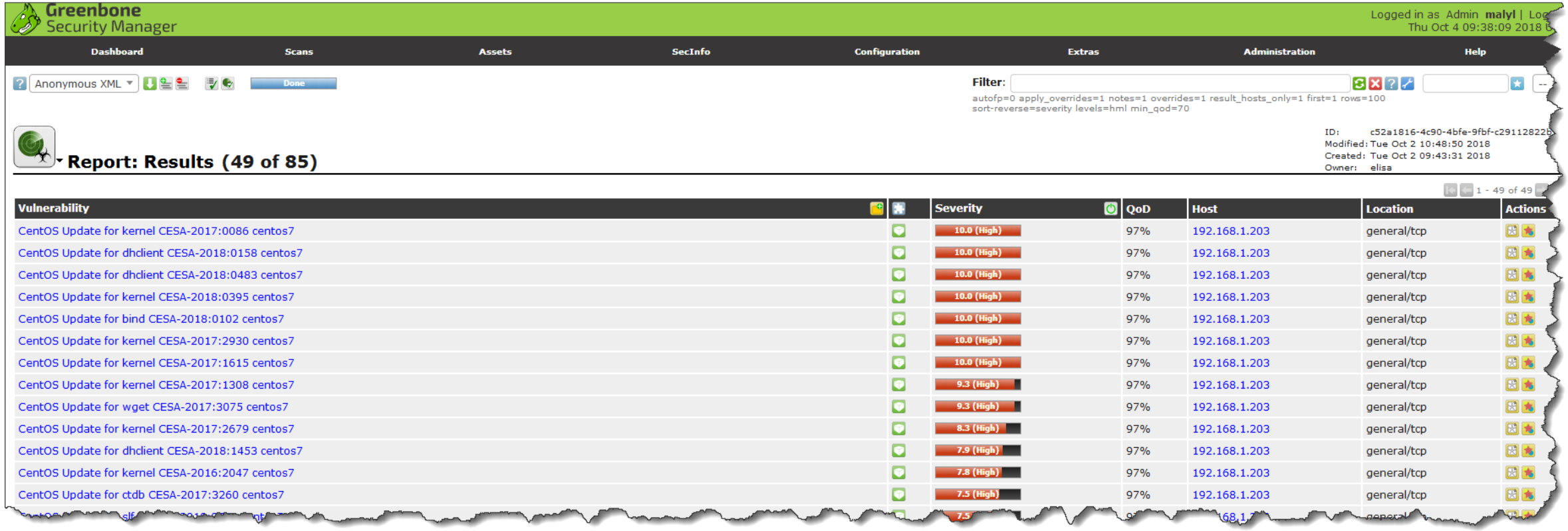
NOVINKY ELISA 4.0

- Integrace s Greenbone Security Manager (OpenVAS)



Novinky ELISA 4.0

- Integrace s Greenbone Security Manager (OpenVAS)



DĚKUJI
ZA POZORNOST

Lukáš MALÝ

Konzultant bezpečnost a monitoring

maly@datasys.cz
+420 225 308 640


DATA
SYS

POZNÁMKY

DATA SYS