ZABBIX

ZABBIX JAKO ZÁKLAD PRO SIEM SYSTÉM

ČESKÝ ZABBIX ONLINE MEEETUP

1 Kdo jsem a co děláme?

Kdo jsem?

ZABBIX

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

DATA SYS

Co děláme?

- Datasys je rodinná, ryze česká a soukromá společnost, kterou v roce 1994 společně se svou manželkou založil Miloslav Novák.

- Zabýváme se komplexními implementačními a integračními IT službami, telekomunikací a vývojem na zakázku.

- Od 19. ledna 2010 jsme partnery Zabbix SIA.

2

ESM – ELISA Security Manager

Event Log Interception Storage and Analysis

https://logmanagement.cz

ČESKÝ ZABBIX ONLINE MEEETUP

Distribuce

- ELISA od 16.6.2020 spadá pod distributorskou síť Novicom

- Novicom – český výrobce pro síťovou správu, monitoring a bezpečnost

Přirovnání ELISA

ZABBIX

INTERNET
obsahuje množství informací.

Internetové vyhledávače
je sbírají a indexují.

Využíváte je pro
rychlé nalezení odpovědí **!!!**

INFORMAČNÍ SYSTÉMY
generují množství informací.

Log management nástroje
je sbírají a indexují.

Využíváte je pro
rychlé nalezení odpovědí **???**

Co zjistíte?

ZABBIX

Z JAKÝCH MÍST LIDÉ PŘISTUPUJÍ
NA FIREMNÍ WEB?

KDO PROVEDL ZMĚNU
V DATABÁZI?

KTEŘÍ UŽIVATELÉ STAHUJÍ NEJVÍCE
DAT Z INTERNETU?

KDO SMAZAL SOUBORY
NA SDÍLENÉM DISKU?

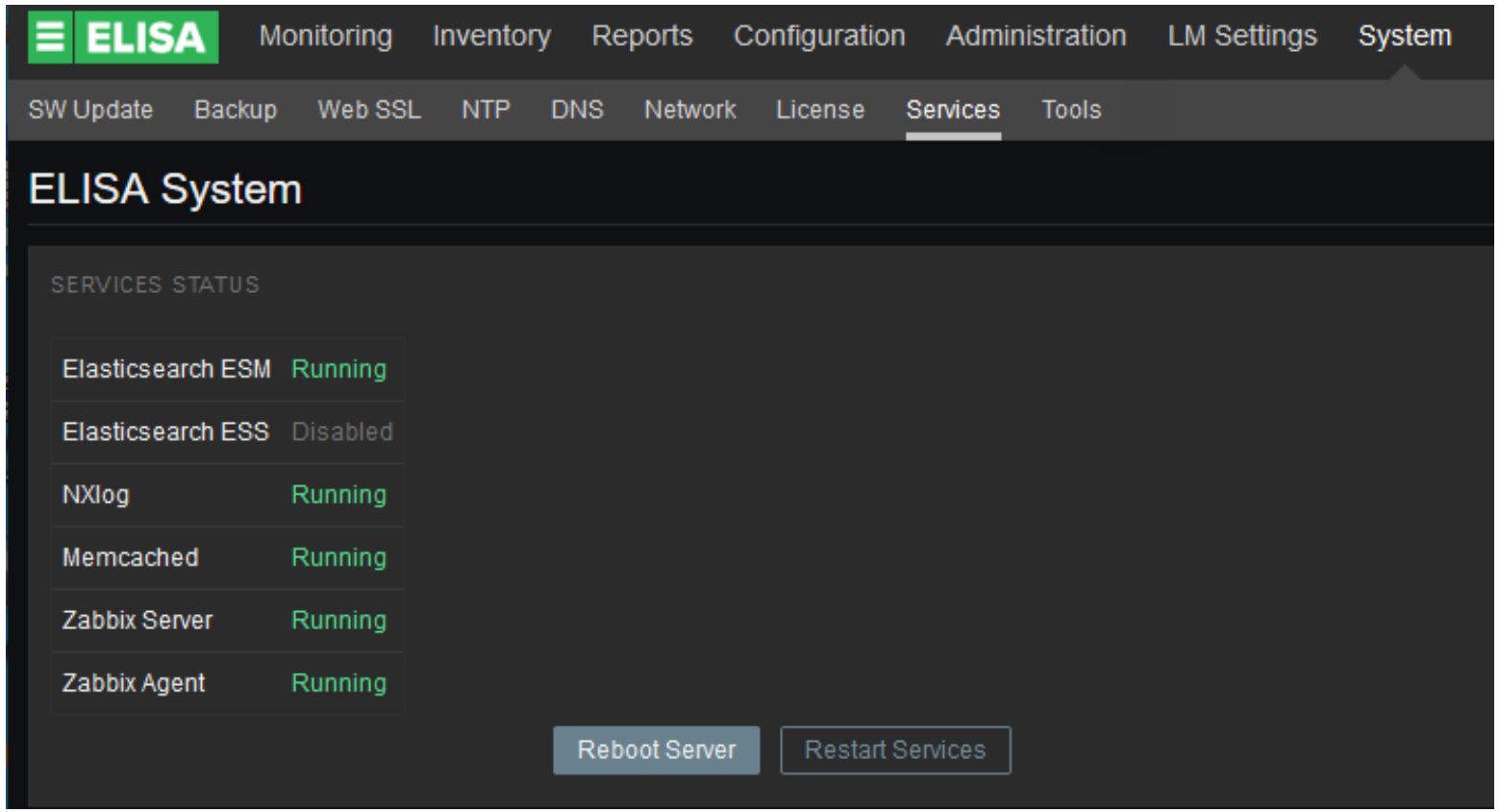
K JAKÝM CHYBÁM DOCHÁZÍ
V PODNIKOVÉM IS?

KDO SE SNAŽÍ UHÁDNOUT
PŘÍSTUPOVÉ HESLO?

3 ELISA a její komponenty

Komponenty

- Kibana a Zabbix WebGUI
- NXLog Enterprise Edition
- Elasticsearch
- Memcached
- Zabbix server
- Zabbix agent
- Apache + PHP



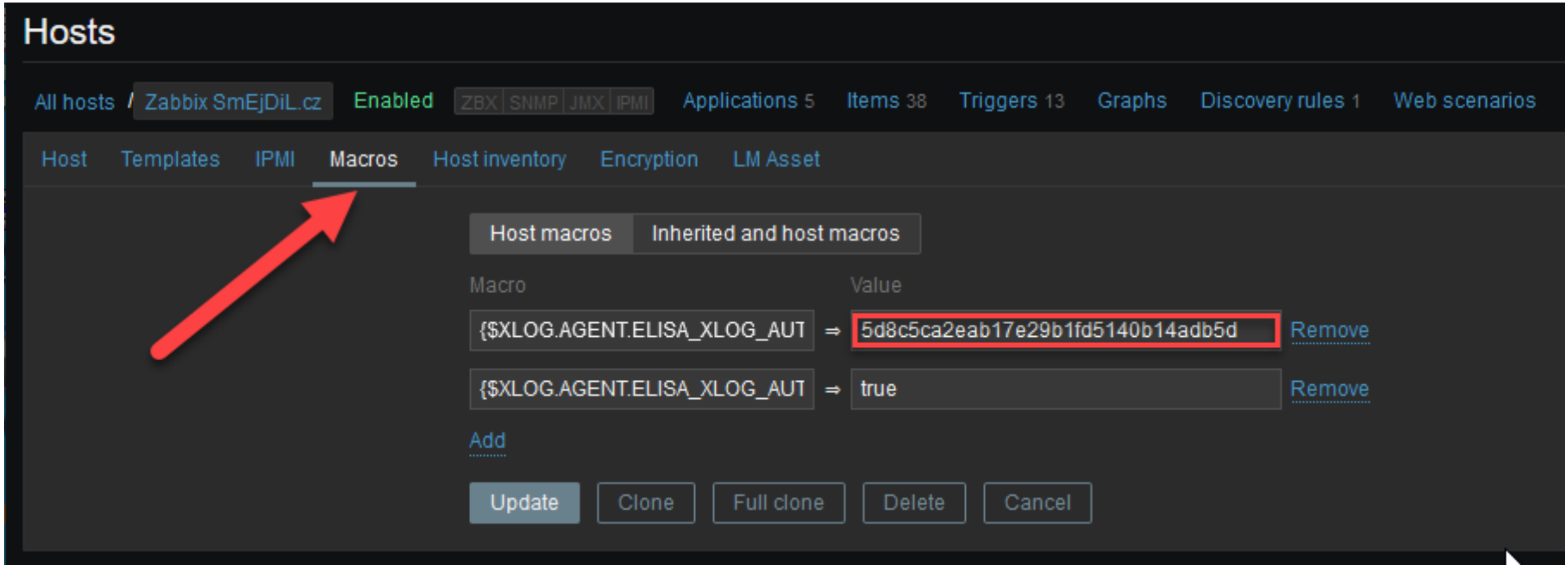
Hlavní vstupní kanály ELISA

ZABBIX

- binary ... (agent) protocol příjem událostí
- syslog (TCP, UDP a TLS/SSL)
- File
- ODBC
- SNMP traps
- Microsoft Windows Evenlog
- NetFlow - v1, v5, v7, v9, a IPFIX (v10)

NXLog agent

ZABBIX



- Autentizační makro je jedinečné pro každého hosta

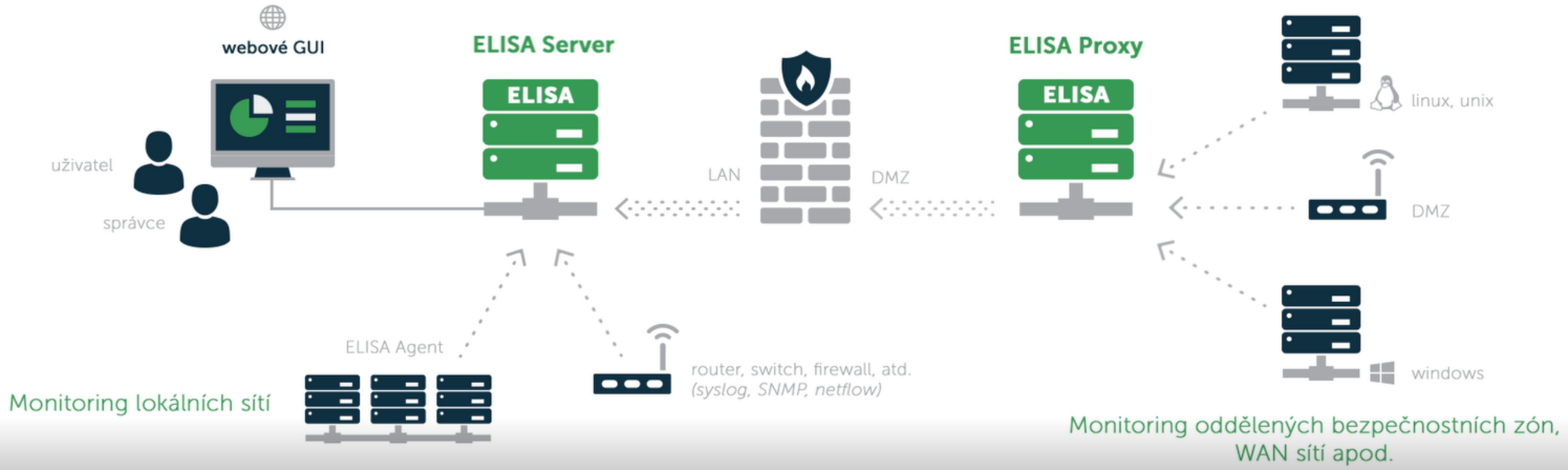
4 OD LOG MANAGEMENTU K NÁSTROJI TYPU SIEM

ESM – ELISA Security Manager

ZABBIX

ZÍSKÁTE CENTRÁLNÍ KONZOLI BEZPEČNOSTNÍHO DOHLEDU

Je to vcelku jednoduchá disciplína ☺



Klíčové vlastnosti

ZABBIX

DETEKCE BEZPEČNOSTNÍCH RIZIK

NÍZKÉ NÁKLADY

PŘEHLEDNÉ UŽIVATELSKÉ PROSTŘEDÍ

- Soulad se ZKB, GDPR, ISO, PCI
- Rychlé odezvy
- Snadno nastavitelné filtry
- Horizontální škálovatelnost

- Integrace s OpenVAS a GSM
- Integrace s Flowmon ADS
- Fyzické i virtuální appliance
- Vysoký výkon (až 10 000 EPS)

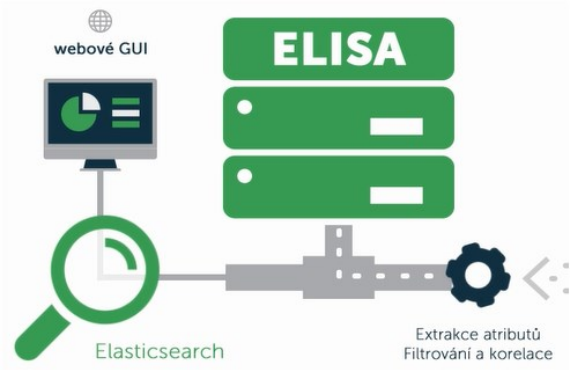
Klíčové vlastnosti

ZABBIX

OD LOG MANAGEMENTU K NÁSTROJI TYPU SIEM

- Automatizované vyhodnocování
- Korelace – nalézání vzájemných vztahů
- Zabudovaný „Change Auditor”
- Propracovanější alarmy a notifikace
- Centrální správa agentů
- Distribuovaný sběr logů

- Výpočet míry rizika
- Zjišťování zranitelností
- Normalizace logů a systematizace dat
- Agregace logů



Zdroje logů

ZABBIX

PODPORA PRAKTICKY VŠECH ZDROJŮ DAT …

Zabudovaný Zabbix

ZABBIX

K TOMU JEŠTĚ NĚCO NAVÍC! PROVOZNÍ MONITORING!

Nejpopulárnější nástroj! Nadupaný a svobodný!

5 Co vše v ELISA dělá Zabbix?

Co vše v ELISA dělá Zabbix?

ZABBIX

- Evidence hostů
- Konfigurace agentů pomocí šablon a maker
- Akce – notifikace
- Autentizace a uživatelské skupiny (Role)
- Mapování hodnot do LM
- Správa indexů Elasticsearch (open, close, archive)
- Import SNMP MIB
- Import Web SSL certifikátů (PEM, PFX/PKCS#12)
- NTP, DNS, Network

6 Evidence hostů

Evidence hostů

ZABBIX

ELISA | Monitoring | Inventory | Reports | Configuration | Administration | LM Settings | System

Host groups | Templates | Hosts | Maintenance | Actions | Event correlation | Discovery | Services

ELISA 4.6.1

Hosts

Group pfSense Firewall | Create host | Import

Filter

Name	Applications	Items	Triggers	Graphs	Discovery	Web	Interface	Templates	Status	Availability	Agent encryption	Info
acboom.pfsense.cz	Applications 3	Items 2	Triggers 5	Graphs	Discovery 1	Web	acboom.pfsense.cz: 10050	Template-DS-Xlog_Base_ALARM_ONLY (Template-DS-Xlog_Alarm)	Enabled	ZBX SNMP JMX IPMI	NONE	
auto-qualt.pfsense.cz	Applications 3	Items 2	Triggers 5	Graphs	Discovery 1	Web	85.13.68.25: 10050	Template-DS-Xlog_Base_ALARM_ONLY (Template-DS-Xlog_Alarm)	Enabled	ZBX SNMP JMX IPMI	NONE	
but.pfsense.cz	Applications 3	Items 2	Triggers 5	Graphs	Discovery 1	Web	89.203.163.210: 10050	Template-DS-Xlog_Base_ALARM_ONLY (Template-DS-Xlog_Alarm)	Enabled	ZBX SNMP JMX IPMI	NONE	
cistirna5.pfsense.cz	Applications 3	Items 2	Triggers 5	Graphs	Discovery 1	Web	84.246.163.16: 10050	Template-DS-Xlog_Base_ALARM_ONLY (Template-DS-Xlog_Alarm)	Enabled	ZBX SNMP JMX IPMI	NONE	
dalmacko.pfsense.cz	Applications 3	Items 4	Triggers 13	Graphs	Discovery 1	Web	85.132.128.17: 10050	Template-DS-Xlog_Base_ALARM_ONLY (Template-DS-Xlog_Alarm)	Enabled	ZBX SNMP JMX IPMI	NONE	
dentmode.pfsense.cz	Applications 3	Items 2	Triggers 5	Graphs	Discovery 1	Web	85.13.68.234: 10050	Template-DS-Xlog_Base_ALARM_ONLY (Template-DS-Xlog_Alarm)	Enabled	ZBX SNMP JMX IPMI	NONE	
gas-therm.pfsense.cz	Applications 3	Items 2	Triggers 5	Graphs	Discovery 1	Web	109.183.157.95: 10050	Template-DS-Xlog_Base_ALARM_ONLY (Template-DS-Xlog_Alarm)	Enabled	ZBX SNMP JMX IPMI	NONE	
home-dknl.pfsense.cz	Applications 3	Items 5	Triggers 17	Graphs	Discovery 1	Web	89.111.88.10: 10050	Template-DS-Xlog_Base_ALARM_ONLY (Template-DS-Xlog_Alarm)	Enabled	ZBX SNMP JMX IPMI	NONE	
karadzos.pfsense.cz	Applications 3	Items 2	Triggers 5	Graphs	Discovery 1	Web	62.168.63.253: 10050	Template-DS-Xlog_Base_ALARM_ONLY (Template-DS-Xlog_Alarm)	Enabled	ZBX SNMP JMX IPMI	NONE	
lte-apu.pfsense.cz	Applications 3	Items 3	Triggers 9	Graphs	Discovery 1	Web	62.141.29.28: 10050	Template-DS-Xlog_Base_ALARM_ONLY (Template-DS-Xlog_Alarm)	Enabled	ZBX SNMP JMX IPMI	NONE	
lukas.pfsense.cz	Applications 3	Items 2	Triggers 5	Graphs	Discovery 1	Web	85.163.24.30: 10050	Template-DS-Xlog_Base_ALARM_ONLY (Template-DS-Xlog_Alarm)	Enabled	ZBX SNMP JMX IPMI	NONE	
milcom-dknl.pfsense.cz	Applications 3	Items 2	Triggers 5	Graphs	Discovery 1	Web	45.82.232.242: 10050	Template-DS-Xlog_Base_ALARM_ONLY (Template-DS-Xlog_Alarm)	Enabled	ZBX SNMP JMX IPMI	NONE	
milcom-fve.pfsense.cz	Applications 3	Items 2	Triggers 5	Graphs	Discovery 1	Web	milcom-fve.pfsense.cz: 10050	Template-DS-Xlog_Base_ALARM_ONLY (Template-DS-Xlog_Alarm)	Enabled	ZBX SNMP JMX IPMI	NONE	
milcom-pha.pfsense.cz	Applications 3	Items 3	Triggers 9	Graphs	Discovery 1	Web	185.75.117.2: 10050	Template-DS-Xlog_Base_ALARM_ONLY (Template-DS-Xlog_Alarm)	Enabled	ZBX SNMP JMX IPMI	NONE	
milcom-tabor.pfsense.cz	Applications 3	Items 3	Triggers 9	Graphs	Discovery 1	Web	164.215.123.202: 10050	Template-DS-Xlog_Base_ALARM_ONLY (Template-DS-Xlog_Alarm)	Enabled	ZBX SNMP JMX IPMI	NONE	
office.pfsense.cz	Applications 3	Items 4	Triggers 13	Graphs	Discovery 1	Web	89.111.88.84: 10050	Template-DS-Xlog_Base_ALARM_ONLY (Template-DS-Xlog_Alarm)	Enabled	ZBX SNMP JMX IPMI	NONE	
skoda-zahrada.pfsense.cz	Applications 3	Items 2	Triggers 5	Graphs	Discovery 1	Web	31.30.62.51: 10050	Template-DS-Xlog_Base_ALARM_ONLY (Template-DS-Xlog_Alarm)	Enabled	ZBX SNMP JMX IPMI	NONE	
troch-cb.pfsense.cz	Applications 3	Items 2	Triggers 5	Graphs	Discovery 1	Web	92.62.231.158: 10050	Template-DS-Xlog_Base_ALARM_ONLY (Template-DS-Xlog_Alarm)	Enabled	ZBX SNMP JMX IPMI	NONE	
troch-jihlava.pfsense.cz	Applications 3	Items 3	Triggers 9	Graphs	Discovery 1	Web	213.226.231.42: 10050	Template-DS-Xlog_Base_ALARM_ONLY (Template-DS-Xlog_Alarm)	Enabled	ZBX SNMP JMX IPMI	NONE	
troch-trutnov.pfsense.cz	Applications 3	Items 2	Triggers 5	Graphs	Discovery 1	Web	troch-trutnov.pfsense.cz: 10050	Template-DS-Xlog_Base_ALARM_ONLY (Template-DS-Xlog_Alarm)	Enabled	ZBX SNMP JMX IPMI	NONE	
troch-zacler.pfsense.cz	Applications 3	Items 2	Triggers 5	Graphs	Discovery 1	Web	troch-zacler.pfsense.cz: 10050	Template-DS-Xlog_Base_ALARM_ONLY (Template-DS-Xlog_Alarm)	Enabled	ZBX SNMP JMX IPMI	NONE	
vitezna.pfsense.cz	Applications 3	Items 2	Triggers 5	Graphs	Discovery 1	Web	192.162.98.146: 10050	Template-DS-Xlog_Base_ALARM_ONLY (Template-DS-Xlog_Alarm)	Enabled	ZBX SNMP JMX IPMI	NONE	

Displaying 22 of 22 found

Host v Zabbixu je současně hostem ELISA.

Evidence hostů

ZABBIX

ELISA Monitoring Inventory Reports Configuration Administration LM Settings System

Host groups Templates Hosts Maintenance Actions Event correlation Discovery Services

Hosts

All hosts / home-dknl.pfsense.cz Enabled ZBX SNMP JMX IPMI Applications 3 Items 5 Triggers 17 Graphs Discovery rules 1 Web scenarios

Host Templates IPMI Macros Host inventory Encryption LM Asset

Asset Value

Name	Value	Action
Default	Low Normal High Critical	Host Template

Add

Log sources Inactivity Interval

Value	Origin
10h	Host Template

Log sources Monitoring

Source	Status
Log Source 'InUdpNetFlow' neposila data	Disabled Enabled
Log Source 'InUdpSnmpTrap' neposila data	Disabled Enabled
Log Source 'InUdpSyslog' neposila data	Disabled Enabled

Update Clone Full clone Delete Cancel

Rozšířená konfigurace hosta.

Hodnota Asset Value ovlivňuje risk skóre.

Pomocí custom LLD se objevují log source pro jednotlivé hosty.

Evidence hostů

- Na jednotlivých hostech můžeme nastavovat LM Asset

- Asset Value
- Log sources Inactivity Interval
- Log sources Monitoring

- Asset Value na hostech ovlivňují **výpočet skóre rizika**

7 Konfigurace pomocí šablon a maker

Konfigurace pomocí šablon a maker

ZABBIX

ELISA | Monitoring | Inventory | Reports | Configuration | Administration | LM Settings | System

Host groups | Templates | Hosts | Maintenance | Actions | Event correlation | Discovery | Services

ELISA 4.6.1

Templates

Group: Templates - Xlog | Create template | Import

Filter

Name: Win | Linked templates: type here to search | Select

Apply | Reset

Name	Applications	Items	Triggers	Graphs	Screens	Discovery	Web	Linked templates	Linked to
Template-DS-Xlog_Base_WINDOWS_LAN	Applications 6	Items 53	Triggers 5	Graphs	Screens	Discovery 1	Web	Template-DS-Xlog_Alarm, Template-DS-Xlog_WINDOWS_Common, Template-DS-Xlog_WINDOWS_HotFix_VBS	
Template-DS-Xlog_NXlogUpdate-WINDOWS	Applications 1	Items 2	Triggers	Graphs	Screens	Discovery	Web		
Template-DS-Xlog_WINDOWS_Common	Applications 1	Items 32	Triggers	Graphs	Screens	Discovery	Web	Template-DS-Xlog_VisualEditor_Agent	Template-DS-Xlog_Base_WINDOWS_LAN
Template-DS-Xlog_WINDOWS_DHCP	Applications 1	Items 3	Triggers	Graphs	Screens	Discovery	Web		
Template-DS-Xlog_WINDOWS_HotFix_VBS	Applications 1	Items 9	Triggers	Graphs	Screens	Discovery	Web		Template-DS-Xlog_Base_WINDOWS_LAN

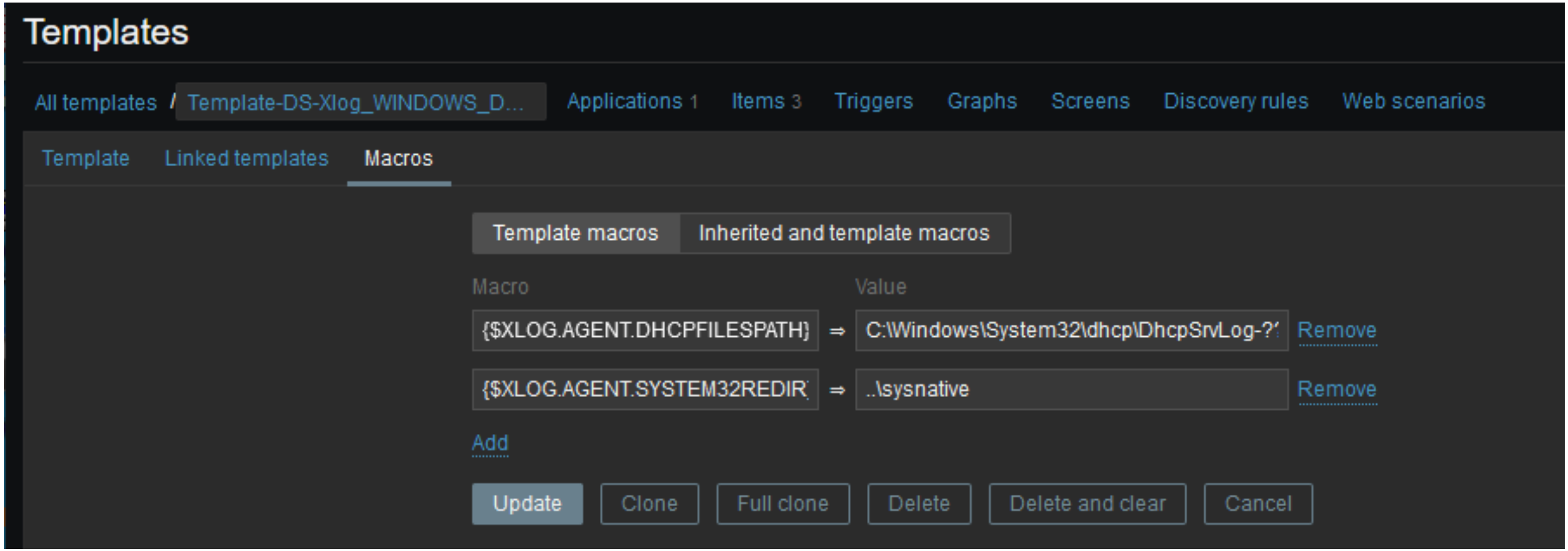
Displaying 5 of 5 found

0 selected | Export | Delete | Delete and clear

- Šablona pro sběr logu Windows DHCP serveru

Konfigurace pomocí šablon a maker

ZABBIX

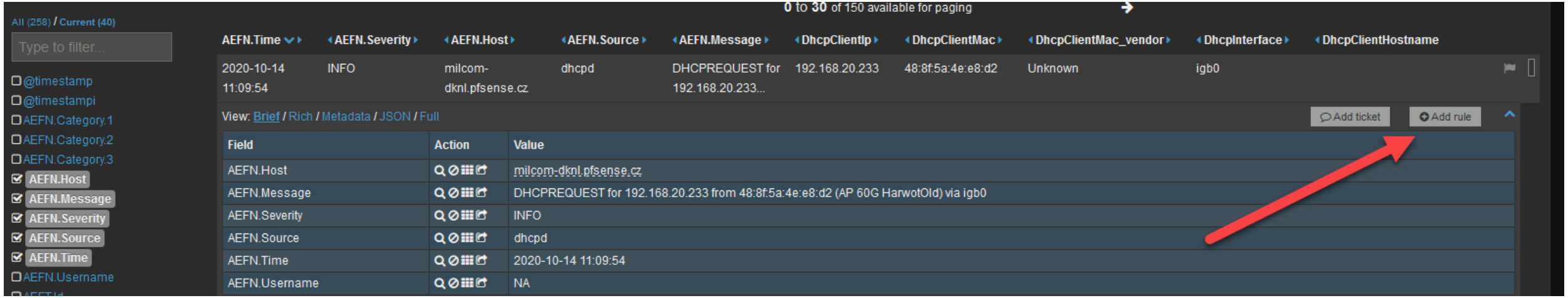


- Makro, kde je definována cesta k souboru

Konfigurace pomocí šablon a maker

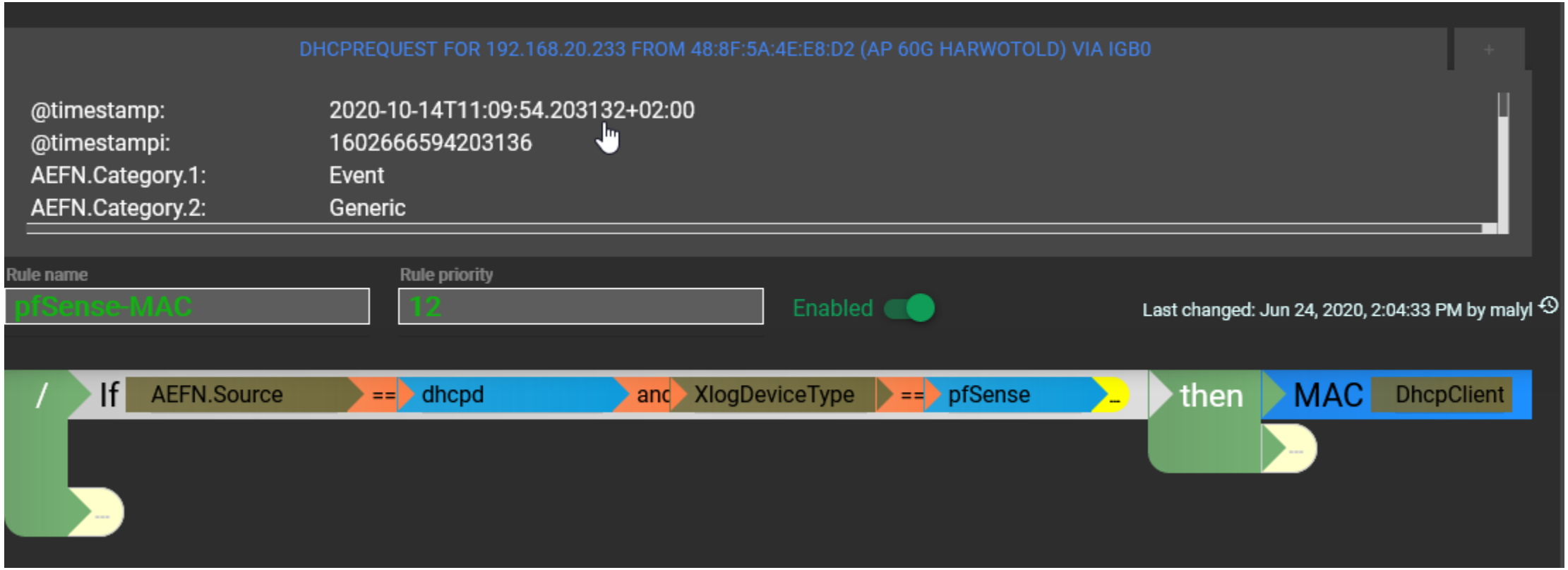
ZABBIX

- V ELISA lze realizovat i velmi jednoduchá pravidla
- Tvorba a úpravy pravidel se provádějí prostřednictvím webového rozhraní
- Pro snadnou uživatelskou tvorbu pravidel slouží **Visuální Editor** pravidel



Konfigurace pomocí šablon a maker

ZABBIX



- Načtením log zprávy do Visual Editoru můžete snadno a jednoduše vytvořit nové pravidlo

Konfigurace pomocí šablon a maker

ZABBIX

GENERATED CODE

```
Exec \
 if ($AEFN.Source  == "dhcpd"  and $XlogDeviceType  == "pfSense") {\
$AEFT.MAC.DhcpClientMac = $DhcpClientMac; \
$AEFT.True = 1; \
}\
```

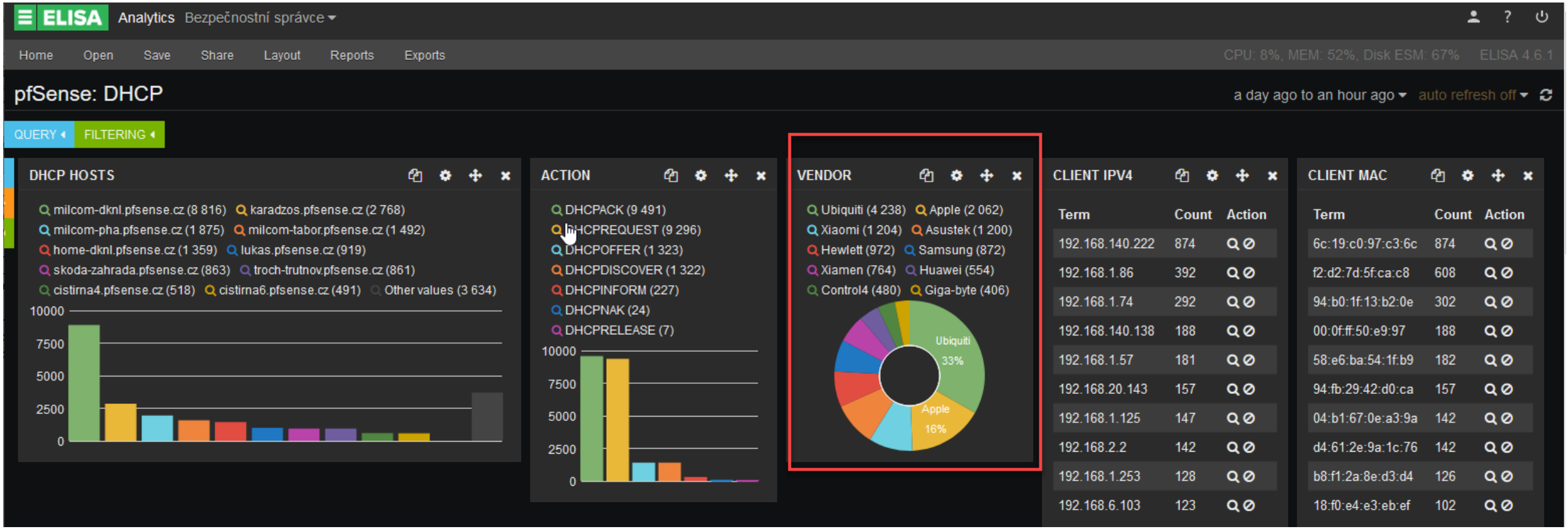
TEST REMOVE SAVE CANCEL

- Editor vygeneruje pravidlo
- Zkontroluje syntaxi NXLog
- Zapíše nové pravidlo do šablony

Name ▲	Applications	Items
Template-DS-Xlog_VisualEditor_Agent	Applications	Items 2
Template-DS-Xlog_VisualEditor_Proxy	Applications	Items 22
Template-DS-Xlog_VisualEditor_Server	Applications	Items 4

Konfigurace pomocí šablon a maker

ZABBIX

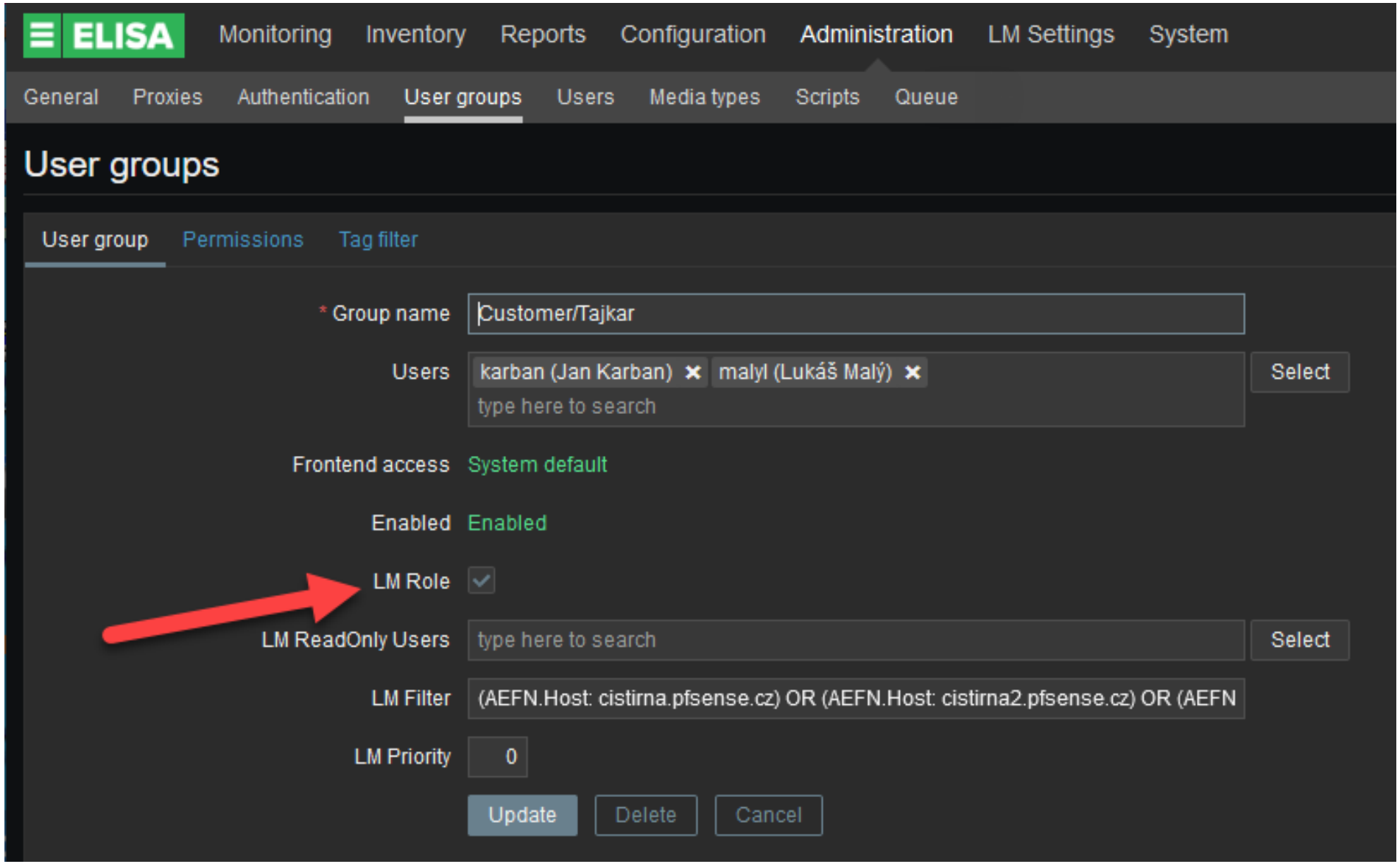


- Výsledkem je překlad MAC adres na výrobce
- Obohacení zpráv o nové informace

8 Autentizace a uživatelské skupiny

Autentizace a uživatelské skupiny (Role)

ZABBIX



Uživatelská skupina použita jako LM Role s nastaveným filtrem AEFN.Host.

Filtrováním v rolích omezíme přístup k datům, která uživatelé mohou vidět.

9 Mapování hodnot, dynamické mapování hodnot - CTI

Mapování hodnot

ZABBIX

- Value mapping – je použit i v ELISA
- Staticky se mapují hodnoty na výrazy

  0 ⇒ Down

  1 ⇒ Up

  6 ⇒ TCP

  17 ⇒ UDP
- Dynamické mapování
- **CTI - Cyber Threat Intelligence**

Mapování hodnot

ZABBIX

ELISA.EVENTLOG_LOGON_FAILURE_CODE	0xc000006a ⇒ Wrong Password 0xc000006f ⇒ Out Of Work Hours 0xc0000064 ⇒ User Not Exist 0xc0000070 ⇒ Workstation Restriction 0xc0000071 ⇒ Password Expired 0xc0000072 ⇒ Account Disabled 0xc0000133 ⇒ Clock Diff Too High 0xc000015b ⇒ Not Granted Requested Logon Type 0xc0000193 ⇒ Account Expiration 0xc0000224 ⇒ Required To Change Passwd 0xc0000234 ⇒ Account Locked
ELISA.EVENTLOG_LOGON_FAILURE_KERBEROS_CODE	0x12 ⇒ Credentials revoked 0x18 ⇒ Invalid credentials 0x25 ⇒ Clock difference too great
ELISA.NETFLOW_PROTOCOLS_CODE	0 ⇒ IP 1 ⇒ ICMP 2 ⇒ IGMP 3 ⇒ GGP 4 ⇒ IPv4 5 ⇒ ST 6 ⇒ TCP 7 ⇒ CBT 8 ⇒ EGP 9 ⇒ IGP 10 ⇒ BBN-RCC-MON 11 ⇒ NVP-II 12 ⇒ PUP 17 ⇒ UDP 18 ⇒ MUX

Mapování hodnot

ZABBIX

NetFlow: Traffic IPv6

QUERY FILTERING

time must
field : @timestamp
from : now-24h
to : now

HOSTS

home-dknl.pfsense.cz (69 830) office.pfsense.cz (24 624) Missing field (0) Other values (0)

80000
60000
40000
20000
0

PROTOCOLS

Term	Count	Action
UDP	79 691	
TCP	14 305	
IP	1	
Missing field	457	
Other values	0	

IP VERSION

Term	Count
6	94 454
Missing field	0
Other values	0

SRC ADDRESS

2a01:a040:2002:8040::2	28 261
2001:4860:4860::8844	19 200
2001:4860:4860::8888	19 163
2a01:a040:2002:8050::2	10 375
2a01:a040:2002:8041:a843:ffe5:b34f:ddae	1 491
2a01:a040:2002:8041:4c15:fe3b:b6f5:b9cb	1 220
2a01:a040:2002:8041:7969:5227:ae89:a4a	1 057
2a01:a040:2002:8041:29d7:9c71:ea38:97f6	1 017

SRC PORT

53	38 224
443	7 964
80	493
123	207
5222	93
5228	50
4327	6
45562	6

Dynamické mapování hodnot - CTI

ZABBIX

ELISA | Monitoring | Inventory | Reports | Configuration | Administration | LM Settings | System

DB Indices | Archive | Options | SNMP | Syslog | Forwarding | CTI | ELISA 4.6.1

Cyber Threat Intelligence

Create

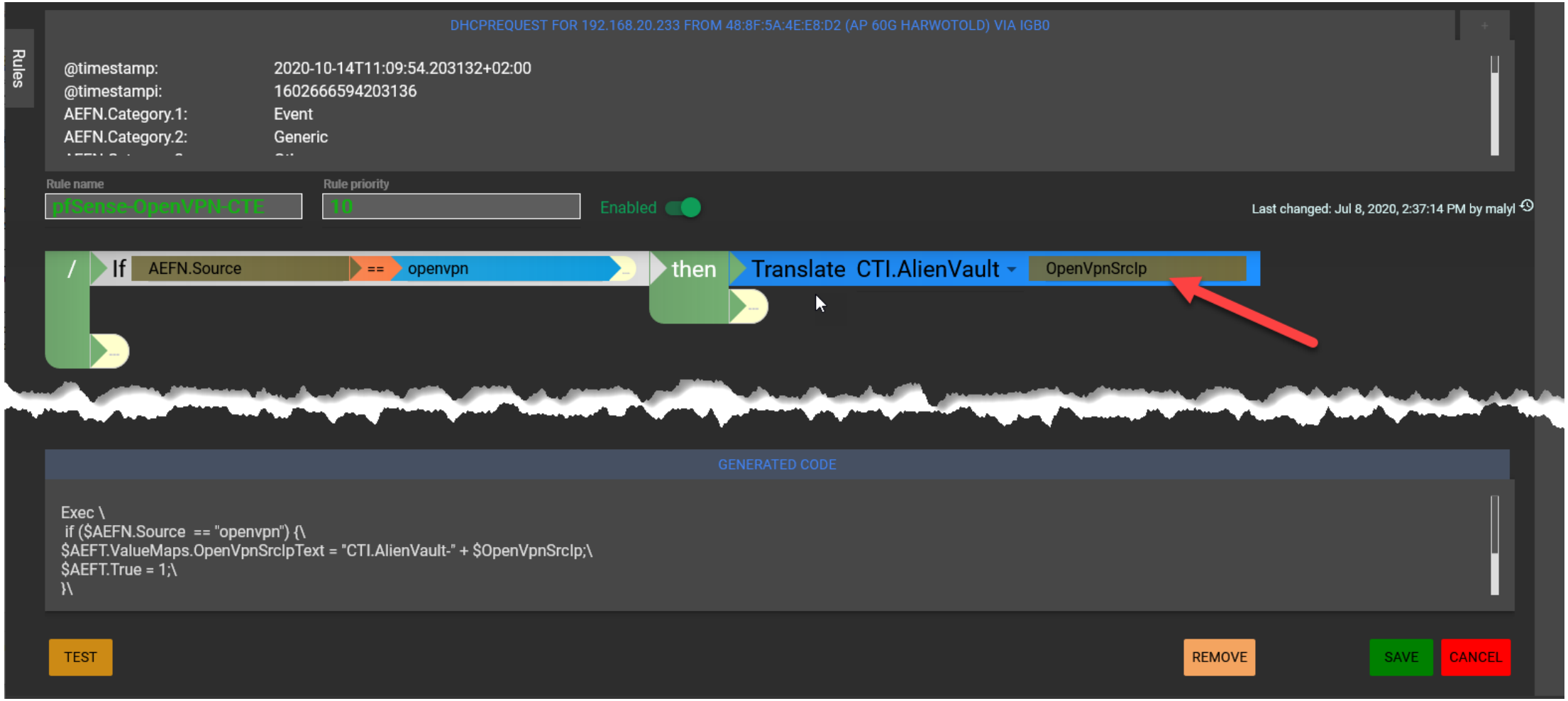
Type	Title	Url	Frequency	Status	Last run	Items	Action
Text	AlienVault	https://reputation.alienvault.com/reputation.data	1d	Enabled	2020-10-14 05:41:18	275629	delete
XML	Stix - Command and Control IP List - EXAMPLE	https://stixproject.github.io/documentation/idioms/c2-ip-list/command-and-control-ip-list.xml	1d	Disabled	Never	0	delete
Text	Talos	http://www.talosintelligence.com/documents/ip-blacklist	1d	Disabled	Never	0	delete

- Každý den si ELISA stáhne seznam nebezpečných IPv4 adres
- Které se načtou do systému

ELISA.CTI.AlienVault — Values stored in memcached ⇒ DO NOT EDIT !!!

Dynamické mapování hodnot - CTI

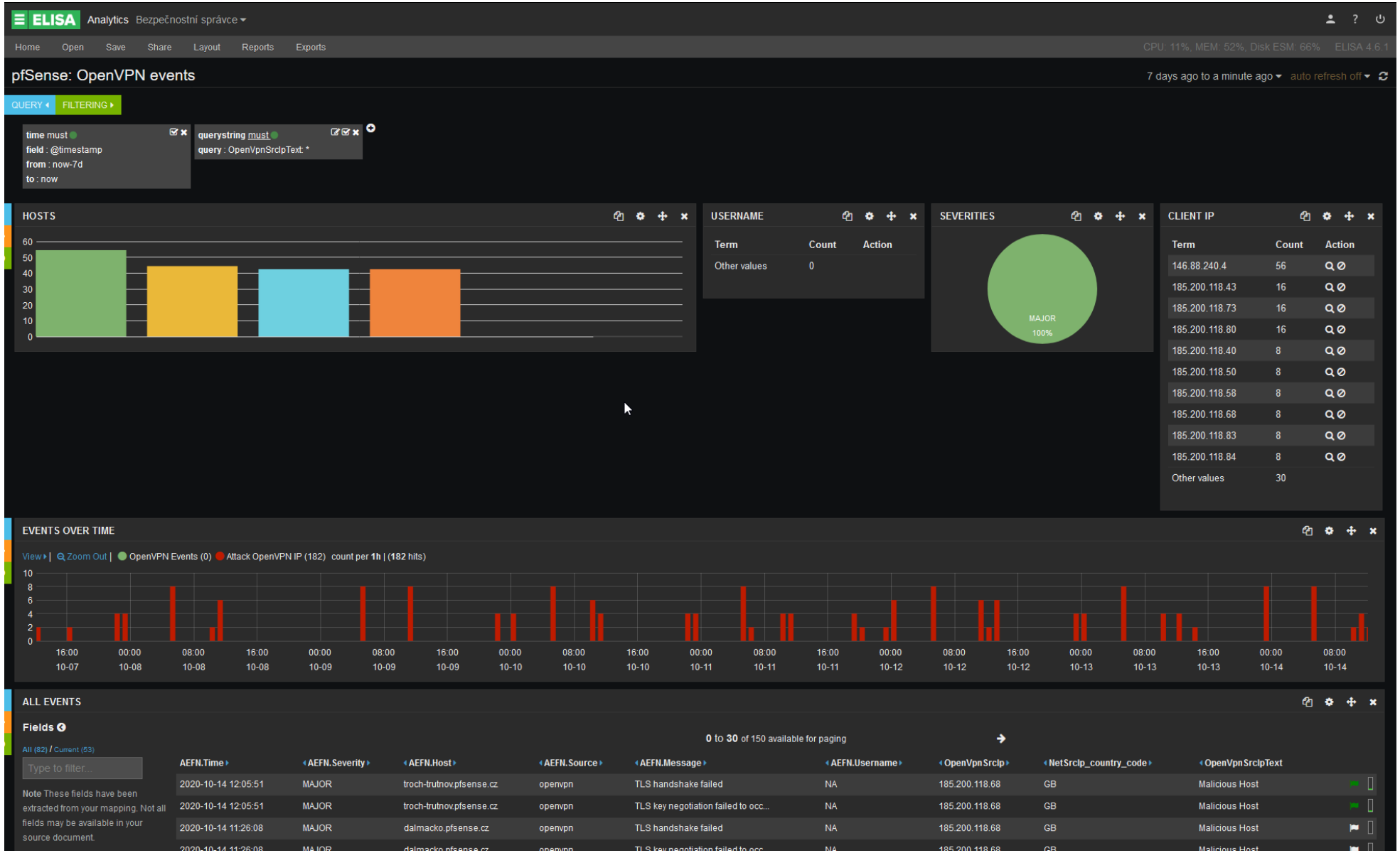
ZABBIX



- Kontrola IPv4 adres, ze kterých se realizuje připojení na OpenVPN

Dynamické mapování hodnot - CTI

ZABBIX

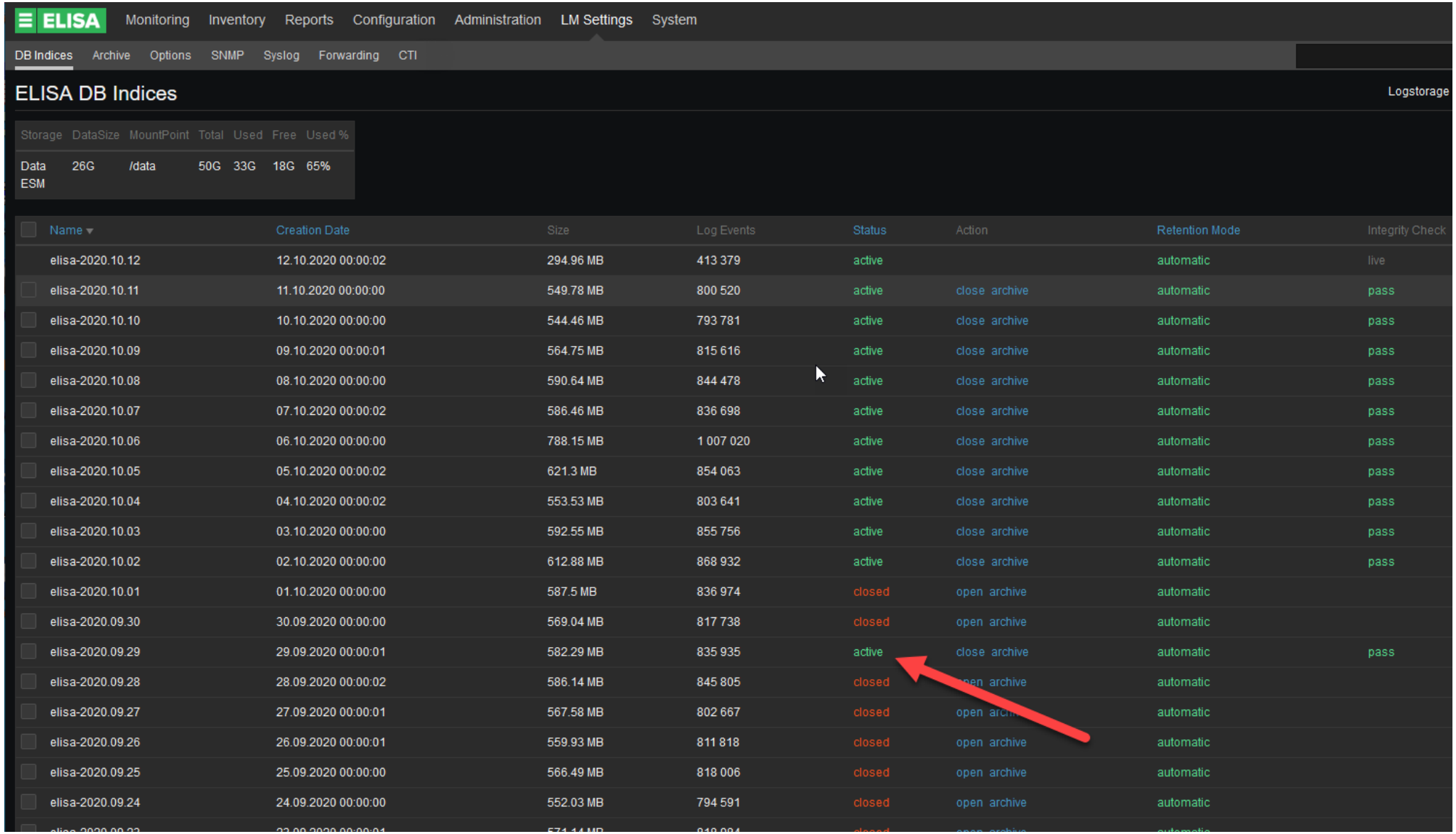


Přehled komunikace OpenVPN, která pochází z pofidérních IPv4 adres.

10 Správa indexů Elasticsearch

Správa indexů Elasticsearch

ZABBIX



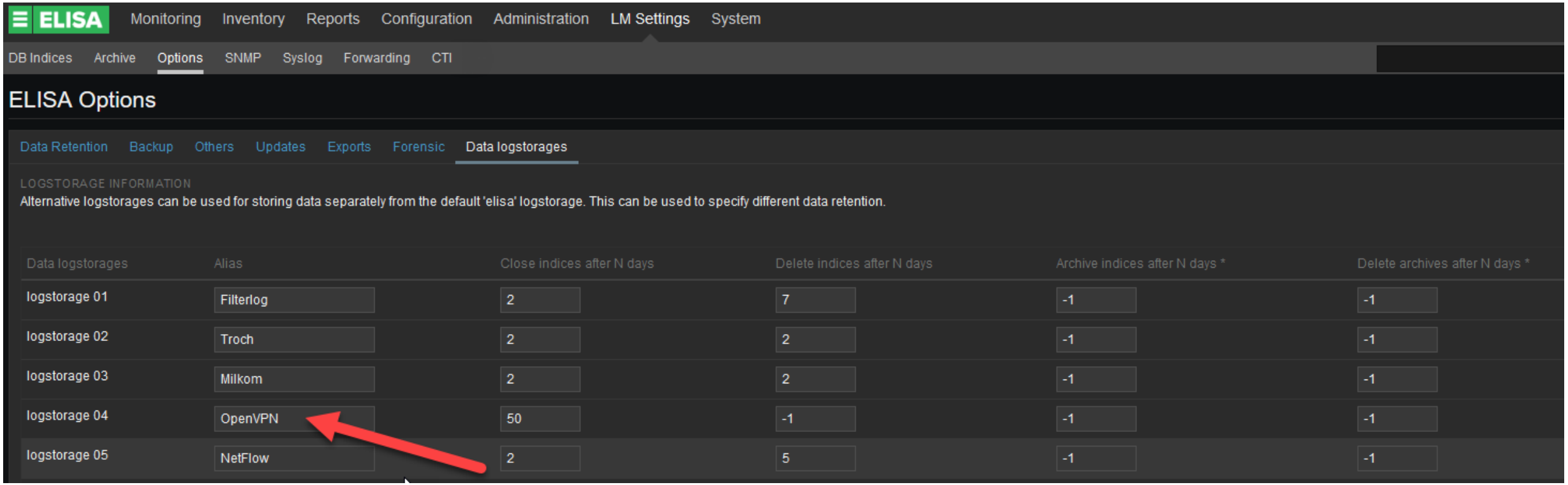
Hlavní index reprezentuje data za celý den.

Retenční mechanismus s indexy rotuje a zakládá nové indexy rámci dnů.

Správa indexů Elasticsearch

ZABBIX

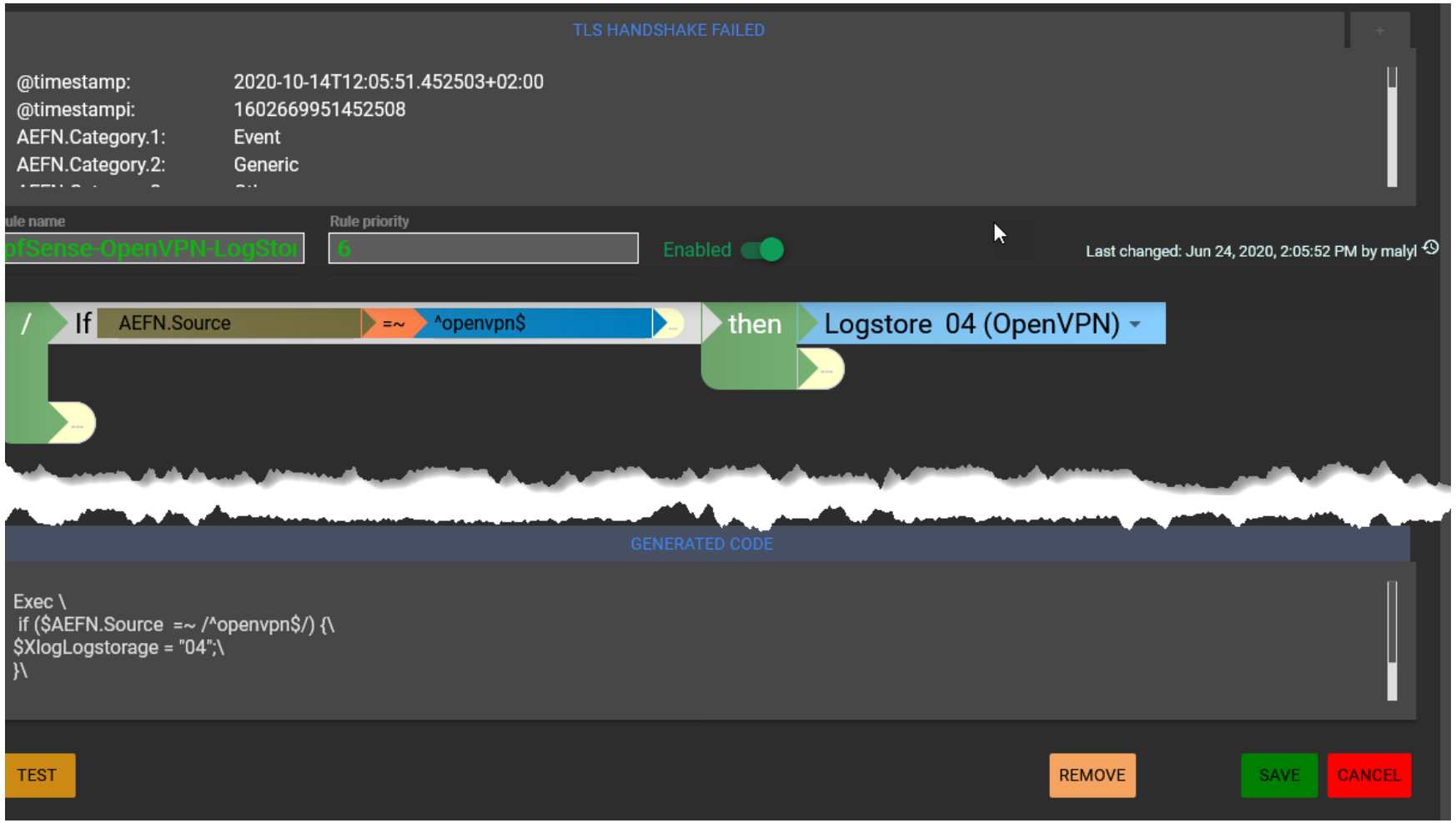
- Nastavením můžete definovat např. odlišné retence nebo jmenný alias indexu
- ELISA poskytuje 10 úložišť logů



Správa indexů Elasticsearch

ZABBIX

- Pomocí Visuálního Editoru vytvoříme snadno pravidlo pro uložení dat do Logstore 04



Data z logstore 04 (OpenVPN) zobrazují logy 50 dnů staré.

Má odlišnou retenci než hlavní index.

Tímto pravidlem se řídí chování úložiště ELISA.

Toto zajistí libovolné pravidlo.

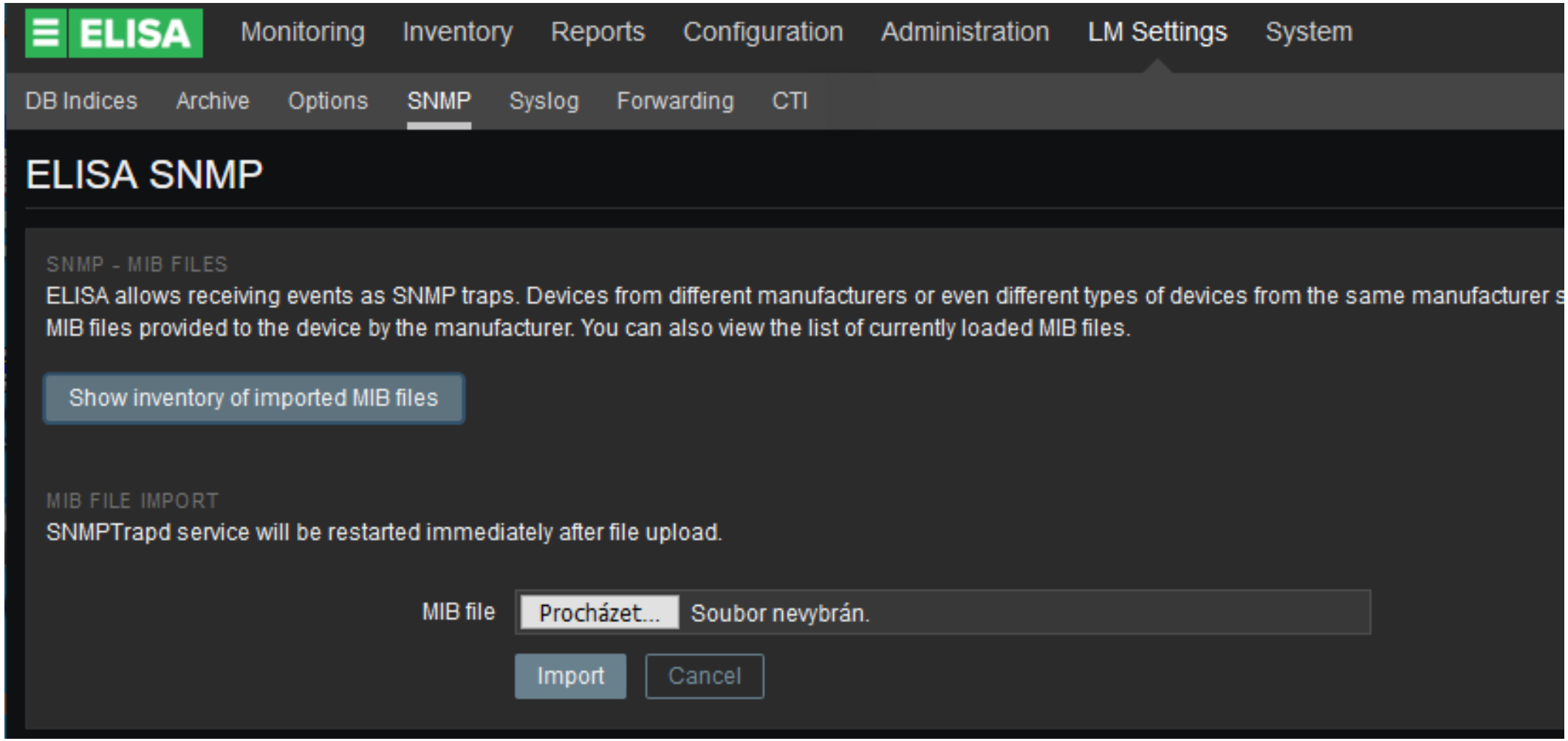
11

Import SNMP MIB, import Web SSL certifikátů, archivace a zálohování

Import SNMP MIB

ZABBIX

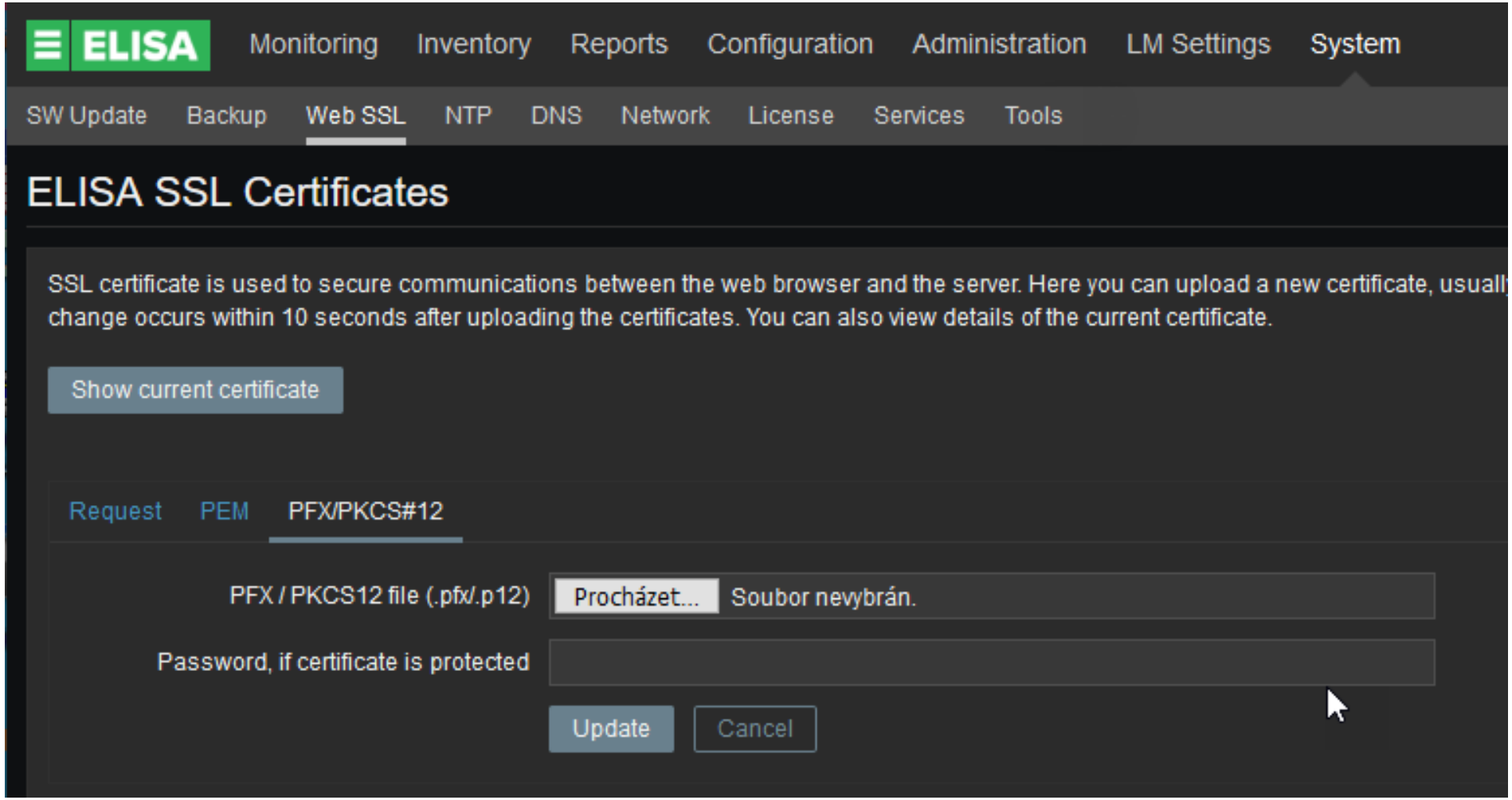
- Instalace MIB souborů se provádí z WebGUI



Import Web SSL certifikátů

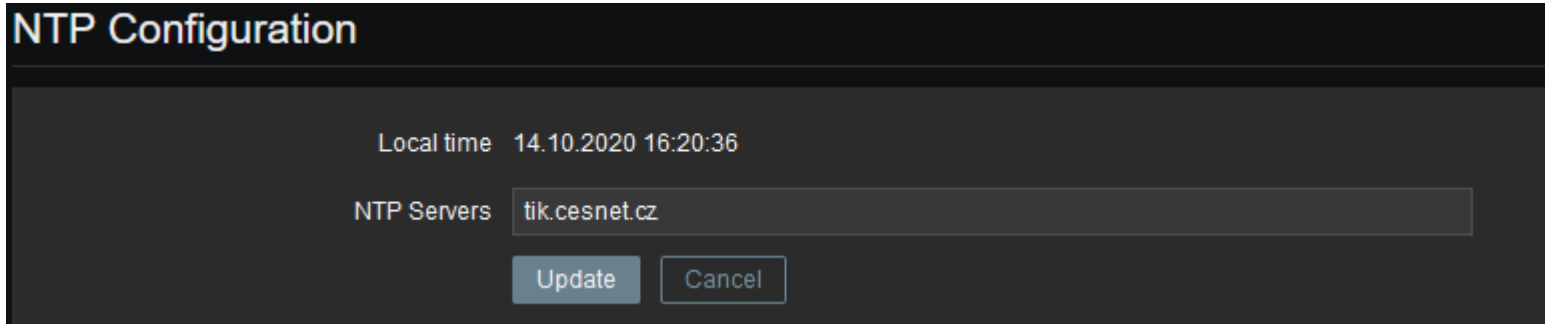
ZABBIX

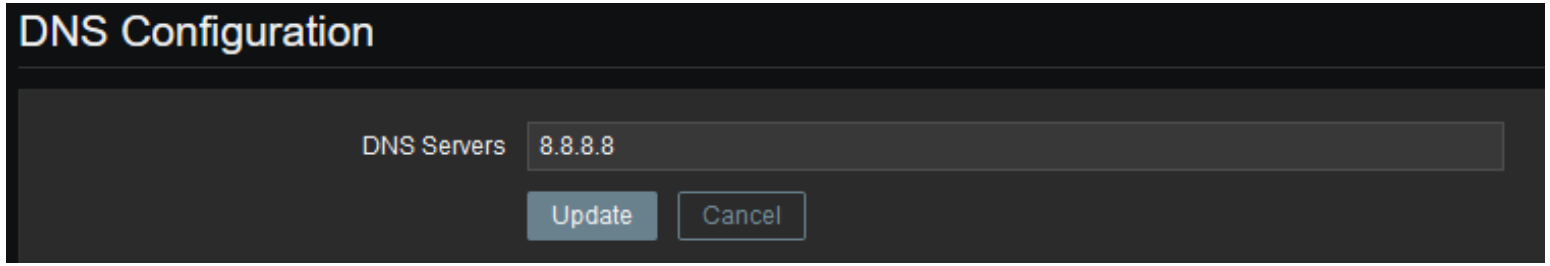
- Výměna SSL certifikátů se provádí z WebGUI



NTP, DNS, Network

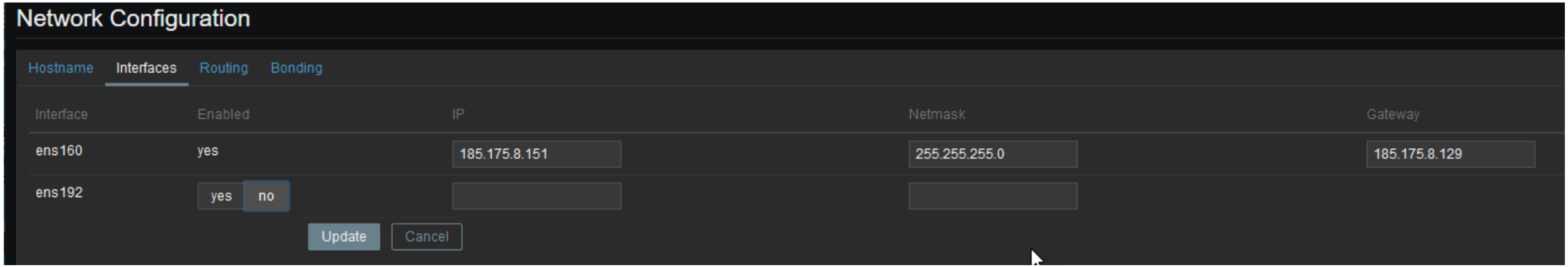
ZABBIX





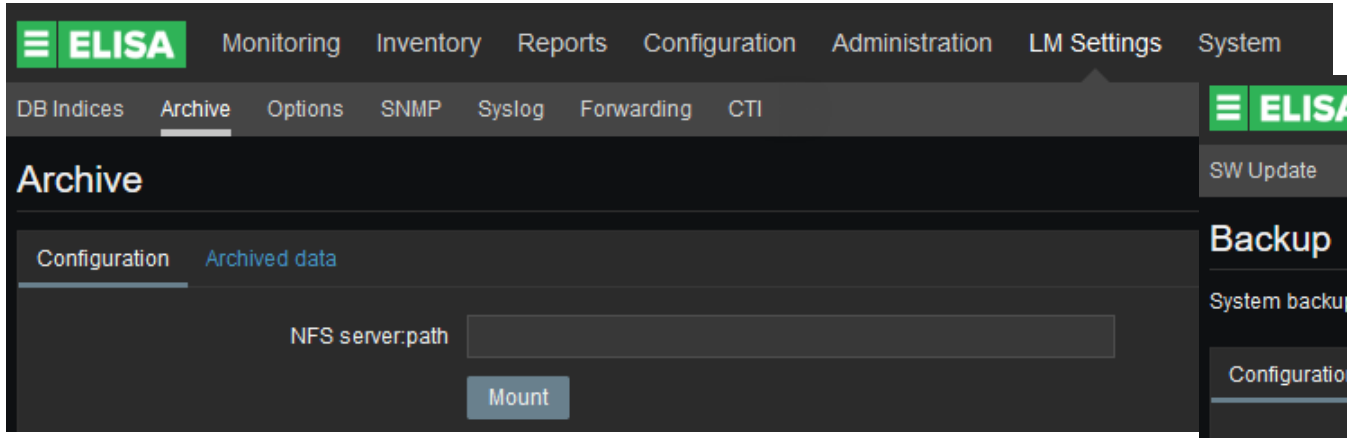
Nastavení systému z WebGUI

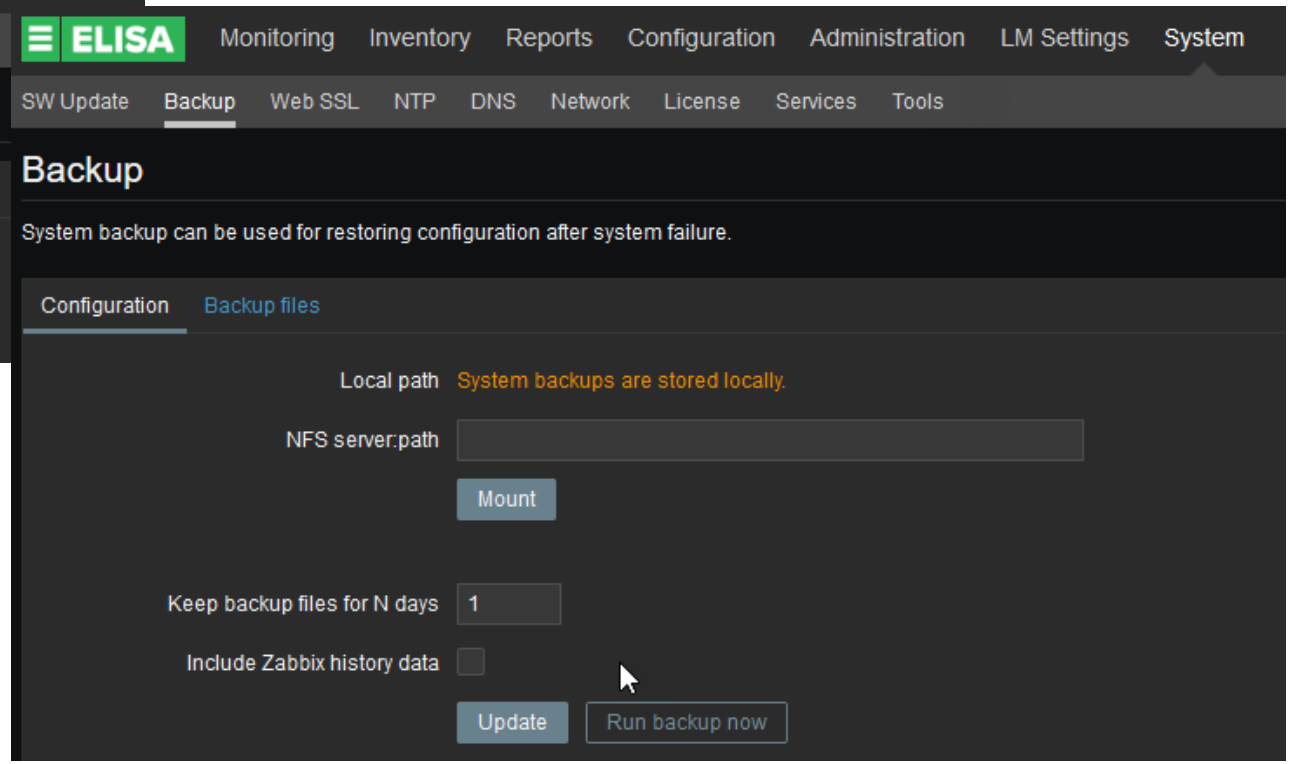
- NTP – (Chrony)
- DNS
- Network
- Backup
- Licence
- Services



Archivace a zálohování

- Archivace indexů je možná pomocí externího NFS úložiště, kam se indexy přesouvají





- Zálohy ELISA se též mohou ukládat na NFS

! Děkuji za pozornost

ČESKÝ

ZABBIX MEETUP ONLINE '20

Hlavní organizátor:

CoreIT

Spoluorganizátoři:

DATA SYS

ICZ

TOTALSERVICE

Q A OTÁZKY A ODPOVĚDI

- Všichni účastníci jsou ztlumeni, abychom eliminovali hluk
- Otázky prosím pište do sekce Q&A, ne do chatu
- Chat používejte pro diskuzi, networking nebo potlesk
- Pokud chcete vložit na sociální média nějaký příspěvek týkající se této akce, použijte hashtag: **#ZabbixMeetupOnline**

Kontakty

Telefon:	+420 225 308 250
Web:	https://www.datasys.cz/
Email:	monitoring@datasys.cz
	maly@datasys.cz
LinkedIn:	https://www.linkedin.com/company/datasys/
	https://www.linkedin.com/in/smejdil/
Twitter:	https://twitter.com/datasysDS
	https://twitter.com/smejdil
Tel. Lukáš Malý:	+420 775 890 041