

Logování

Sbírání, uchovávání a používání zásadních informací

Aleš Padrta, Radomír Orkáč
CESNET, z. s. p. o.

- Úvodní slovo
- Definice logu
- Skladování logů
- Využívání logů
- Logy a CSIRT (bezpečnostní správci)
- Shrnutí
- Praktické ukázky

- Administrátoři
 - Provoz systémů
 - Funkčnost sítě
- Potřeba vědět
 - Co se děje \Rightarrow okamžitá reakce
 - Co se dělo \Rightarrow analýza proběhlých událostí
- Bezpečnostní aspekty
 - Analýza (průběhu) bezpečnostního incidentu
 - Identifikace původce BI
- Logy = potřebné informace

Co je to „log“?

- Český nejblíže „žurnál“
- Záznamy o činnosti systému
 - Operační systémy
 - Jednotlivé aplikace
 - Síťové prvky
 - IDS
- Časová značka
- Událost
 - Stav důležitých operací
 - Detekované chyby / problémy
 - Pokusy o nepovolené aktivity

Co je to „log“?

- Požadavky
 - Chronologická návaznost
 - Možnost vyhledávání
 - Čitelný pro lidi
- Formát
 - Obvykle textový soubor (*nix)
 - Databáze
 - ...

```
Apr  6 00:00:14 147.228.52.222 dhcpd: DHCPREQUEST for  
147.228.172.40 from 01:23:45:67:89:ab via eth0
```

```
Apr  6 00:00:15 147.228.52.222 dhcpd: DHCPACK on  
147.228.172.40 to 01:23:45:67:89:ab via eth0
```

- Dostatečně dlouhou dobu
 - Limitováno objemem dat
 - Časem klesá jejich hodnota
 - Kompromis
 - Dle důležitosti údajů
 - Cca 6 měsíců dostatečné
- Nutno zaručit
 - Dostupnost (logy jsou kdykoliv dostupné)
 - Důvěrnost (přístup jen vymezené skupině)
 - Integritu (logy nebyly změněny)

- Lokálně
 - V případě výpadku systému nedostupné
 - Možné narušení integrity
- Centrální log server
 - **Kopie** všech lokálních logů
 - Zlepšení dostupnosti
 - Lze analyzovat i vypnutý systém
 - Lepší zajištění integrity
 - Lze porovnat s lokálním logem
 - Centrální bod
 - Snadnější a přehlednější vyhledávání
 - Korelace dat z více systémů

- Vhodná struktura
 - Podle času
 - Např. každý měsíc vlastní adresář
 - Dle strojů (IP adres)
 - Snadnější analýza chování stroje
 - Dle služeb
 - Analýza služby
 - Např. logy více DHCP serverů jsou spojeny v jeden
- Nástroje
 - Syslog-ng (pravidla pro třídění a posílání logů)

- Pasivní ~ skladování informací
 - Analýza proběhlých událostí
 - Statistiky
 - Optimalizace
- Aktivní ~ průběžné sledování
 - Odhalení aktuálního problému / útoku
 - Možnost rychlé reakce
 - Obvykle (polo)automatické
 - Např. e-mail správci
 - Zpravidla pouze klíčové charakteristiky

- Logy = základní pomocník
 - Dodává potřebné informace
- Kdo a co dělá (dělal) v „naší“ síti?
 - Přístupy k systémům (a síti)
 - Jednoznačná identifikace viníka / oběti
 - IP – čas – uživatel (login)
 - Systémové a síťové aktivity
 - Odhalení či předejití problému
 - Dohled na vhodné používání
 - Ověření hlášených událostí

- Přístupové a klíčové služby
 - Kerberos
 - VPN
 - Radius
 - DHCP
 - DNS
 - ...
- Síťové aktivity
 - NetFlow (informace o všech spojeních mezi uzly)
 - IDS (informace o závadné komunikaci)

- Logy
 - Záznamy o činnosti systémů
 - Ponechat dostatečně dlouhou dobu
 - Bezpečně uchovávat
 - Aktivně/pasivně zpracovávat
- Bezpečnostní aspekty
 - Kdo používal naše prostředky
 - Co s nimi prováděl
- Log = přítel (bezpečnostního) administrátora

Praktické ukázky, nápady, postřehy

- Pokusy o přihlášení (Unix, GNU/Linux):
 - Prozrazené heslo
 - Odkud se uživatel hlásil a jak dlouho byl přihlášen

```
# last -f /var/log/wtmp
```

```
abc001 pts/0 :0.0 Sun Mar 29 12:11 still logged in
abc001 pts/0 :0.0 Sat Mar 28 09:56 - 13:09 (03:13)
reboot system boot 2.6.24 Sat Mar 28 09:52 - 17:33 (1+06:41)
```

```
# less /var/log/auth.log
```

```
.. sshd[7580]: Invalid user admin from 85.25.71.xxx
.. sshd[7580]: pam_unix(sshd:auth): check pass; user unknown
.. sshd[7580]: pam_unix(sshd:auth): authentication failure; .. ruser= rhost=85.25.71.xxx
.. sshd[7580]: Failed password for invalid user admin from 85.25.71.xxx port 53236 ssh2
```

```
# grep "Invalid user" /var/log/auth.log
```

```
Mar 24 20:19:49 nb sshd[7396]: Invalid user ben from 85.25.71.xxx
```

```
Mar 24 20:19:56 nb sshd[7404]: Invalid user ben from 85.25.71.xxx
```

Logwatch:

Authentication Failures:

root (219.153.xxx.xxx): 160 Time(s)

Invalid Users:

Unknown Account: 73 Time(s)

Sessions Opened:

ftp: 1 Time(s)

Users logging in through sshd:

ftp:

220.164.xxx.xxx (180.144.164.220.broad.sm.yn.dynamic.163data.com.cn): 1 time

----- Cron Begin -----

Commands Run:

User root:

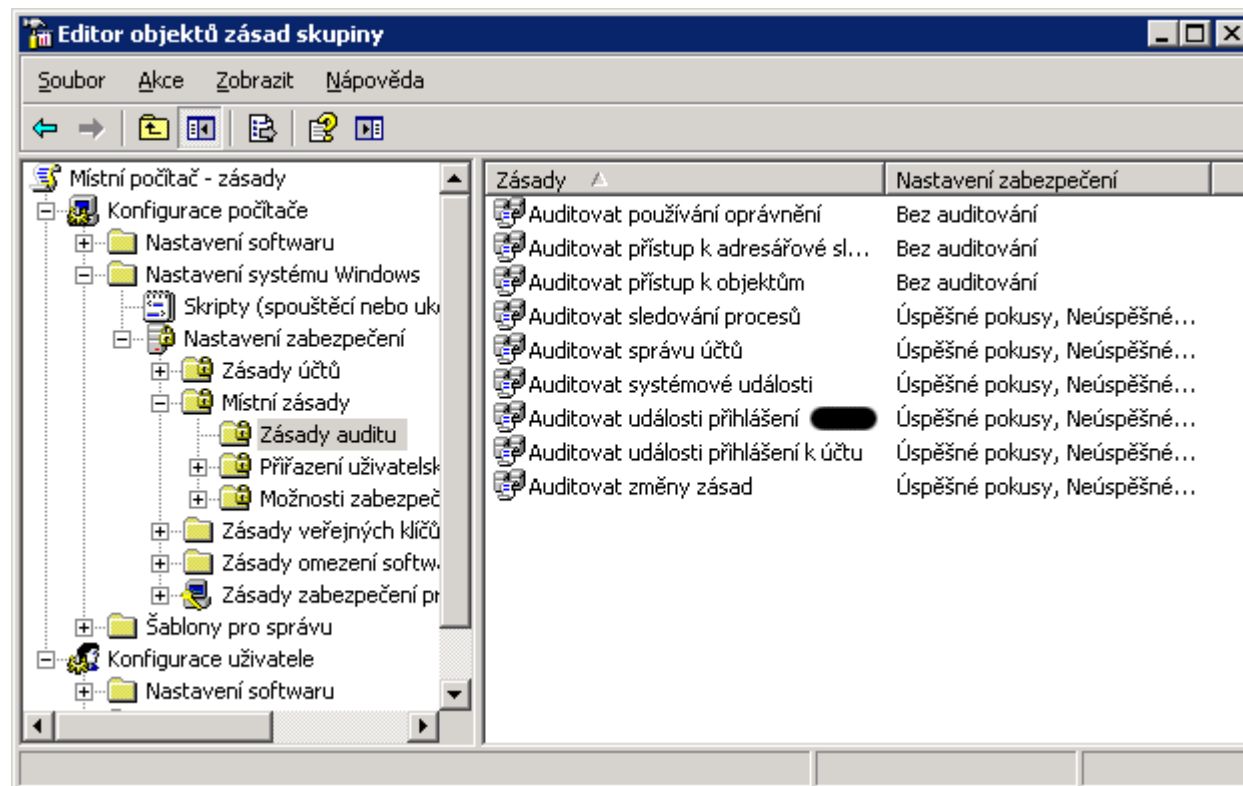
/usr/local/awstats/tools/awstats_updateall.pl now 2>&1 >> /dev/null: 24 Time(s)

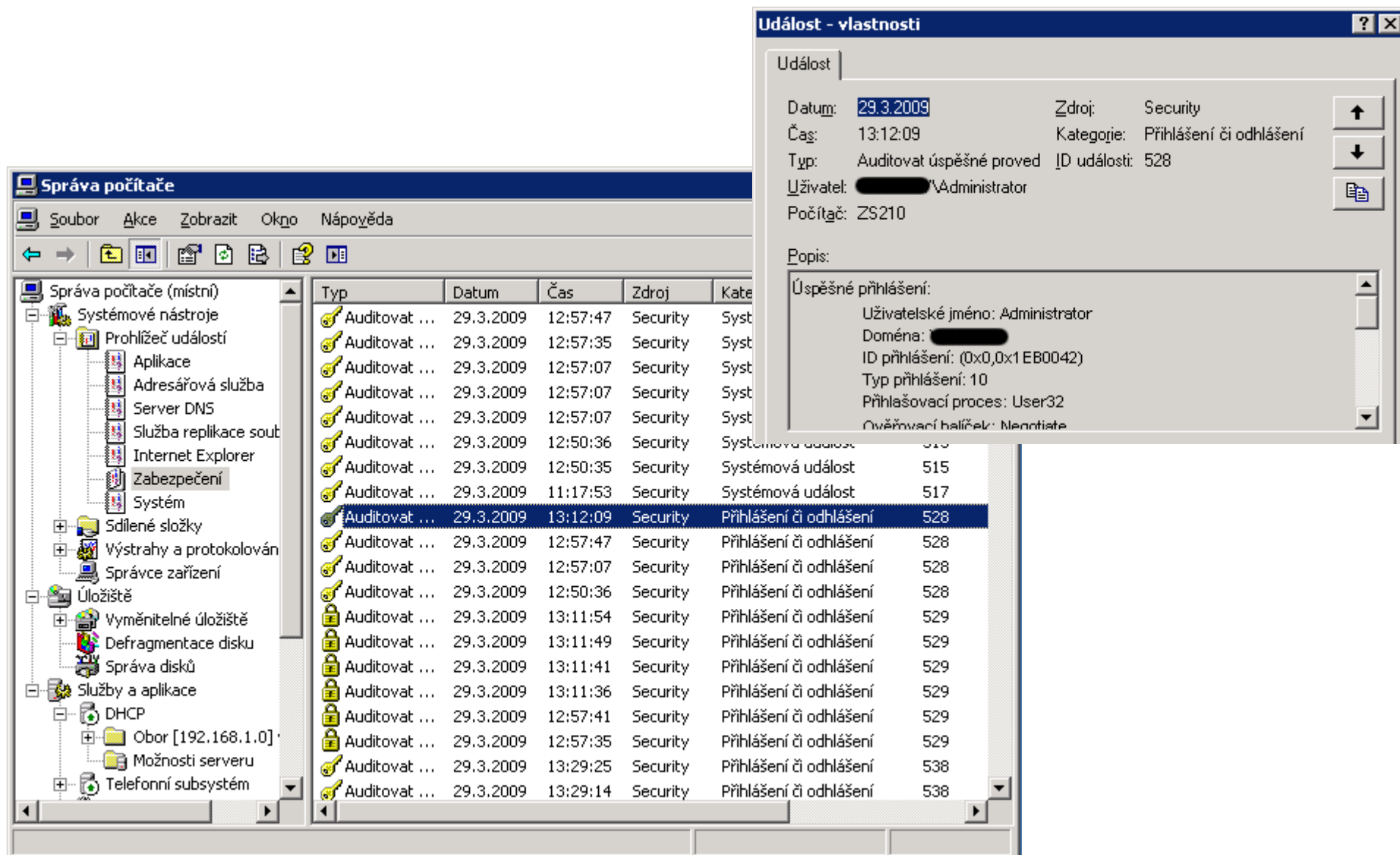
...

----- Cron End -----

- CustomLog /var/log/apache2/access.log combined
CustomLog "|/usr/bin/logger -t apache -i -p
local6.notice" combined
- netstat -natup | \
grep -v "Active\|Aktiv\|Proto" | \
awk '{print \$1"|" "\$4"|" "\$5"|" "\$6"|" "\$7}' | \
/usr/bin/logger -t netstat -i -p local6.notice
- tshark -i eth0 -o http.tcp.port:0-10000 -R
"http.request.method contains GET" -T fields -E
separator=';' -e ip.src -e ipv6.src -e http.host -e
http.request.uri

- Úspěšná/neúspěšná přihlášení (Windows):
 - Start -> Spustit -> gpedit.msc





The screenshot displays the Windows Event Viewer interface. The left pane shows the 'Správa počítače' (Computer Management) tree with 'Zabezpečení' (Security) selected. The main pane shows a list of security events. The selected event is expanded in a separate window titled 'Událost - vlastnosti' (Event - Properties).

Typ	Datum	Čas	Zdroj	Kategorie	ID události
Auditovat ...	29.3.2009	12:57:47	Security	Systémová událost	515
Auditovat ...	29.3.2009	12:57:35	Security	Systémová událost	515
Auditovat ...	29.3.2009	12:57:07	Security	Přihlášení či odhlášení	528
Auditovat ...	29.3.2009	12:57:07	Security	Přihlášení či odhlášení	528
Auditovat ...	29.3.2009	12:57:07	Security	Přihlášení či odhlášení	528
Auditovat ...	29.3.2009	12:57:07	Security	Přihlášení či odhlášení	528
Auditovat ...	29.3.2009	12:50:36	Security	Přihlášení či odhlášení	528
Auditovat ...	29.3.2009	12:50:35	Security	Přihlášení či odhlášení	528
Auditovat ...	29.3.2009	11:17:53	Security	Přihlášení či odhlášení	528
Auditovat ...	29.3.2009	13:12:09	Security	Přihlášení či odhlášení	528
Auditovat ...	29.3.2009	12:57:47	Security	Přihlášení či odhlášení	528
Auditovat ...	29.3.2009	12:57:07	Security	Přihlášení či odhlášení	528
Auditovat ...	29.3.2009	12:50:36	Security	Přihlášení či odhlášení	528
Auditovat ...	29.3.2009	13:11:54	Security	Přihlášení či odhlášení	529
Auditovat ...	29.3.2009	13:11:49	Security	Přihlášení či odhlášení	529
Auditovat ...	29.3.2009	13:11:41	Security	Přihlášení či odhlášení	529
Auditovat ...	29.3.2009	13:11:36	Security	Přihlášení či odhlášení	529
Auditovat ...	29.3.2009	12:57:41	Security	Přihlášení či odhlášení	529
Auditovat ...	29.3.2009	12:57:35	Security	Přihlášení či odhlášení	529
Auditovat ...	29.3.2009	13:29:25	Security	Přihlášení či odhlášení	538
Auditovat ...	29.3.2009	13:29:14	Security	Přihlášení či odhlášení	538

Událost - vlastnosti

Událost

Datum: 29.3.2009 Zdroj: Security

Čas: 13:12:09 Kategorie: Přihlášení či odhlášení

Typ: Auditovat úspěšné provedení ID události: 528

Uživatel: [redacted] \Administrator

Počítač: ZS210

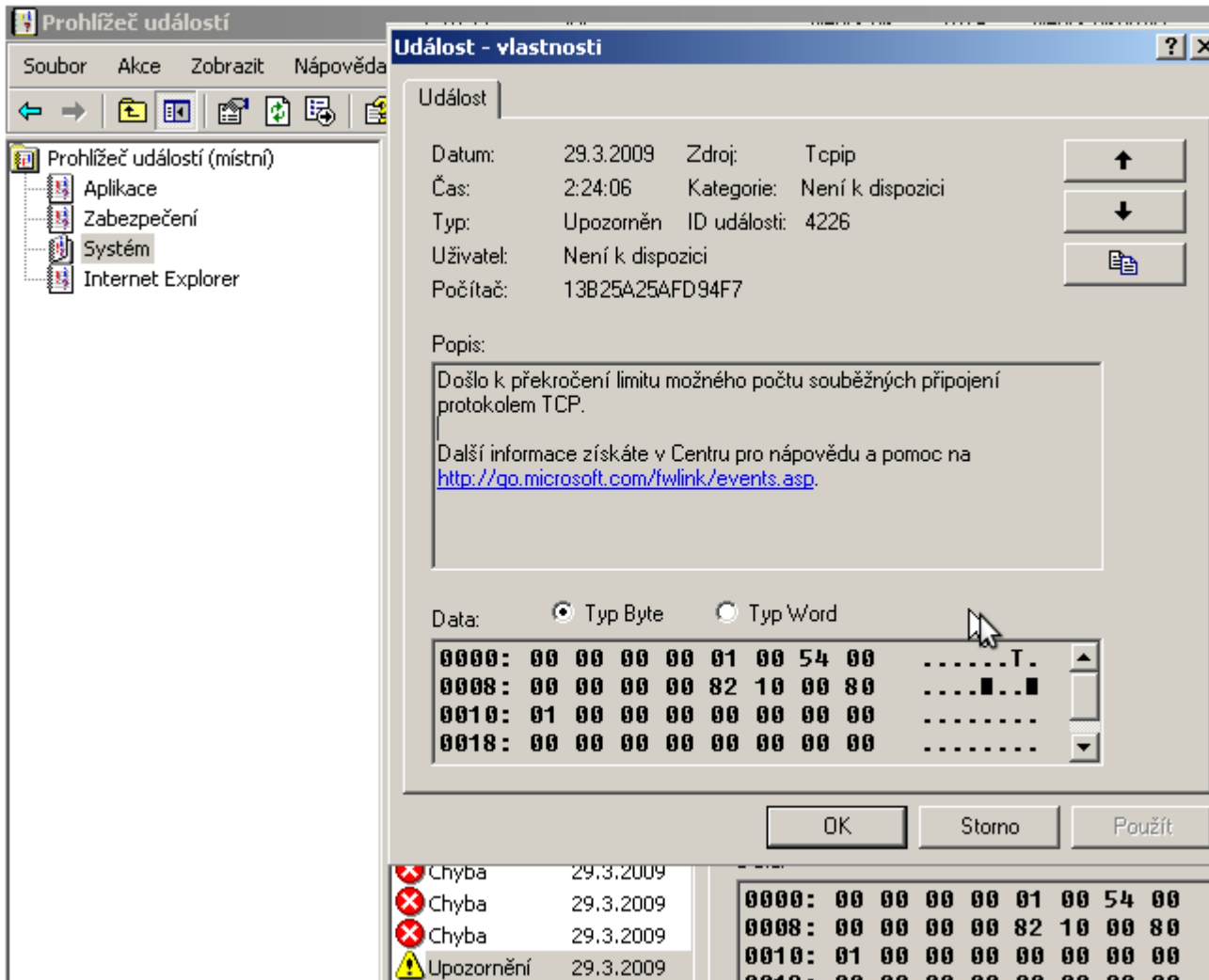
Popis:

Úspěšné přihlášení:

- Uživatelské jméno: Administrator
- Doména: [redacted]
- ID přihlášení: (0x0,0x1 EB0042)
- Typ přihlášení: 10
- Přihlašovací proces: User32
- Ověřovací balíček: Negotiate

Praktické ukázky

- pravděpodobná ochrana před extrémně rychlým šířením internetových červů nebo proti SYN útoku



The screenshot shows the Windows Event Viewer window titled "Prohlížeč událostí" (Event Viewer). The left pane shows the "Prohlížeč událostí (místní)" (Local Event Viewer) tree with categories like "Aplikace", "Zabezpečení", "Systém", and "Internet Explorer". The right pane shows the "Událost - vlastnosti" (Event Properties) dialog for a specific event.

Událost - vlastnosti

Událost

Datum: 29.3.2009 Zdroj: Tcpip
 Čas: 2:24:06 Kategorie: Není k dispozici
 Typ: Upozornění ID události: 4226
 Uživatel: Není k dispozici
 Počítač: 13B25A25AFD94F7

Popis:

Došlo k překročení limitu možného počtu souběžných připojení protokolem TCP.

Další informace získáte v Centru pro nápovědu a pomoc na <http://go.microsoft.com/fwlink/events.asp>.

Data: Typ Byte Typ Word

0000:	00	00	00	00	01	00	54	00T.
0008:	00	00	00	00	82	10	00	80■.■
0010:	01	00	00	00	00	00	00	00
0018:	00	00	00	00	00	00	00	00

Buttons: OK, Storno, Použít

Event Log Summary:

Chyba	29.3.2009	0000: 00 00 00 00 01 00 54 00
Chyba	29.3.2009	0008: 00 00 00 00 82 10 00 80
Chyba	29.3.2009	0010: 01 00 00 00 00 00 00 00
Upozornění	29.3.2009	0018: 00 00 00 00 00 00 00 00

- Zasílání informací o aktualizacích (GNU/Linux)
 - apticron, cron-apt, yum-updatesd

..

The following packages will be upgraded:

liblcms1

1 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.

Need to get 0B/103kB of archives.

After this operation, 4096B of additional disk space will be used.

Download complete and in download only mode

..

There are 2 package updates available. Please run the system updater.

Packages available for update:

device-mapper-multipath

kpartx

Thank You,
Your Computer

- Tiger UNIX security tool (Unix, GNU/Linux)
 - Sada shell skriptů a utilit
 - Pasivní ochrana
 - Zasílání varovných mailů

```
--WARN-- [root001w] Remote root login allowed in /etc/ssh/sshd_config
--WARN-- [pass014w] Login (abc75) is disabled, but has a valid shell.
--WARN-- [lin015w] The system has IP forwarding enabled
--WARN-- [path009w] /etc/profile does not export an initial setting for PATH.
--FAIL-- [netw020f] There is no /etc/ftpusers file.
--FAIL-- [boot02] File /boot/grub/menu.lst has world permissions. Should be 0600
```

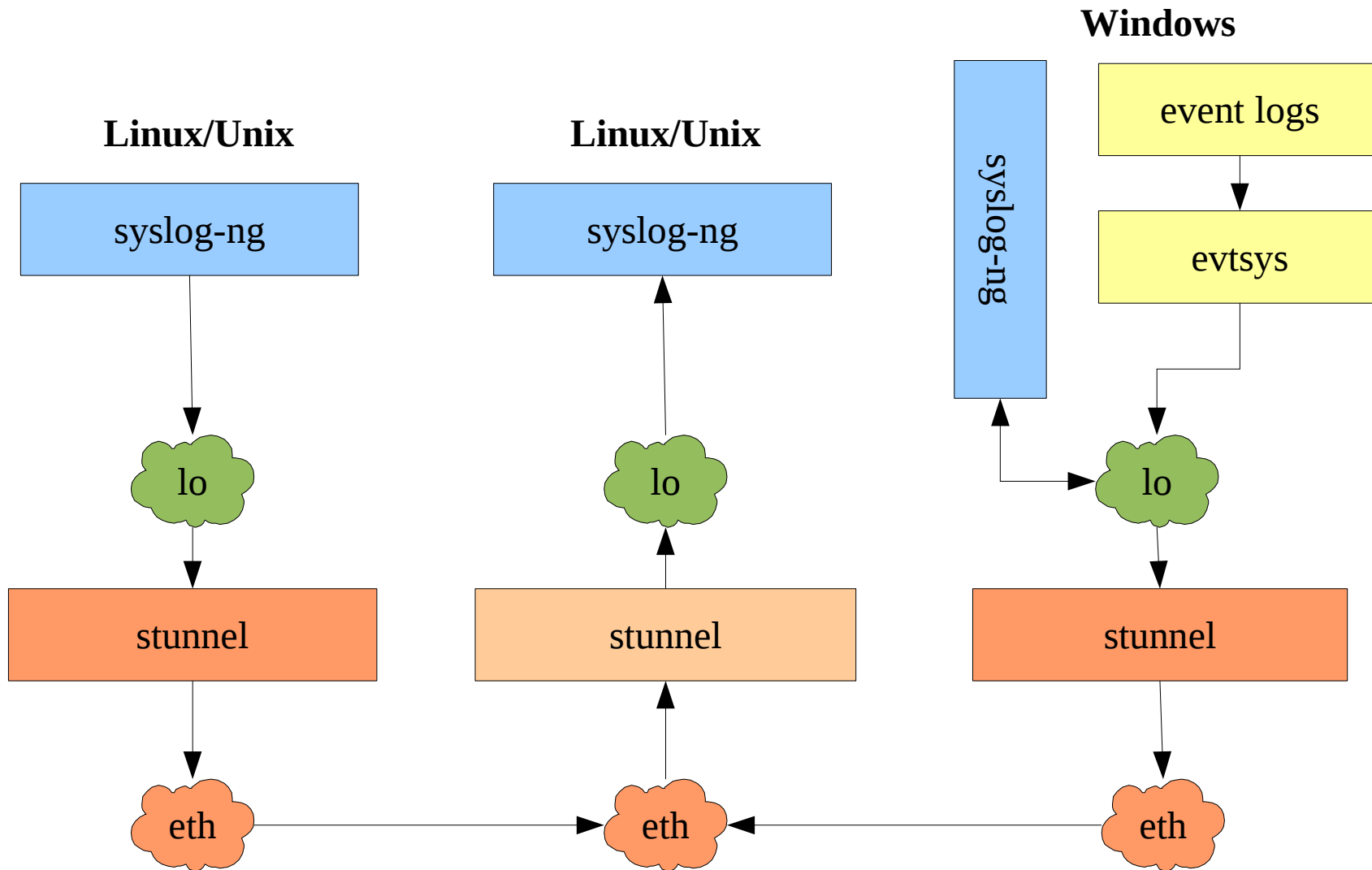
```
NEW: .. is listening on socket 5140 (TCP on every interface) is run by stunnel4
OLD: .. is listening on socket 8000 (TCP on every interface) is run by abc01.
```

- Snoopy
 - Zaznamenává spouštěné příkazy
 - Pracuje plně transparentně
 - Zachytává volání `execve()`
 - Informace předává přes `syslog`

```
May 6 1 13:24:48 vps snoopy[27626]: [ork01, uid:0 sid:27611]: dircolors -b
May 6 1 13:24:48 vps snoopy[27628]: [ork01, uid:0 sid:27611]: uname -s
May 6 1 13:24:48 vps snoopy[27630]: [ork01, uid:0 sid:27611]: uname -r
May 6 1 13:24:49 vps snoopy[27633]: [ork01, uid:0 sid:27611]: sed -ne /^# START
exclude/,/^# FINISH e
May 6 1 13:25:03 vps snoopy[27642]: [ork01, uid:0 sid:27611]: mc
```

- Syslog-ng (alternativa k syslogd)
 - Podpora komunikace přes TCP
 - Filtrování zpráv pomocí regulárních výrazů
- Stunnel
 - Přidává programům podporu komunikace přes SSL
- Cygwin
 - Portace *NIXových utilit do Windows
- Evtsys
 - Kopíruje Eventlog zprávy přes Syslog

Vzdálené logování



- Splunk
 - Indexování a analýza logů
 - Rychlé vyhledávání informací
 - Uživatelské rozhraní podobné Google
 - Výstrahy → email, SMS, trigger skripty
 - SplunkBase
 - databáze chyb (poznatky k chybám)
 - usnadňuje troubleshooting
 - Komerční produkt

Děkujeme za pozornost

Prostor pro případné otázky.