

Sem vložte zadání Vaší práce.



ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE  
FAKULTA INFORMAČNÍCH TECHNOLOGIÍ  
KATEDRA SOFTWAREVÉHO INŽENÝRSTVÍ



Bakalářská práce

# Flexibilní logování pro embedded Linuxové systémy

*David Vavříčka*

Vedoucí práce: Ing. Matěj Laitl

25. února 2016



---

## Poděkování

Doplňte, máte-li komu a za co děkovat. V opačném případě úplně odstráňte tento příkaz.



---

## Prohlášení

Prohlašuji, že jsem předloženou práci vypracoval(a) samostatně a že jsem uvedl(a) veškeré použité informační zdroje v souladu s Metodickým pokynem o etické přípravě vysokoškolských závěrečných prací.

Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorského zákona, ve znění pozdějších předpisů. V souladu s ust. § 46 odst. 6 tohoto zákona tímto uděluji nevýhradní oprávnění (licenci) k užití této mojí práce, a to včetně všech počítačových programů, jež jsou její součástí či přílohou, a veškeré jejich dokumentace (dále souhrnně jen „Dílo“), a to všem osobám, které si přejí Dílo užít. Tyto osoby jsou oprávněny Dílo užít jakýmkoli způsobem, který nesnižuje hodnotu Díla, a za jakýmkoli účelem (včetně užití k výdělečným účelům). Toto oprávnění je časově, teritoriálně i množstevně neomezené. Každá osoba, která využije výše uvedenou licenci, se však zavazuje udělit ke každému dílu, které vznikne (byť jen zčásti) na základě Díla, úpravou Díla, spojením Díla s jiným dílem, zařazením Díla do díla souborného či zpracováním Díla (včetně překladu), licenci alespoň ve výše uvedeném rozsahu a zároveň zpřístupnit zdrojový kód takového díla alespoň srovnatelným způsobem a ve srovnatelném rozsahu, jako je zpřístupněn zdrojový kód Díla.

V Praze dne 25. února 2016

.....

České vysoké učení technické v Praze  
Fakulta informačních technologií

© 2016 David Vavříčka. Všechna práva vyhrazena.

*Tato práce vznikla jako školní dílo na Českém vysokém učení technickém v Praze, Fakultě informačních technologií. Práce je chráněna právními předpisy a mezinárodními úmluvami o právu autorském a právech souvisejících s právem autorským. K jejímu užití, s výjimkou bezúplatných zákonných licencí, je nezbytný souhlas autora.*

### **Odkaz na tuto práci**

Vavříčka, David. *Flexibilní logování pro embedded Linuxové systémy*. Bakalářská práce. Praha: České vysoké učení technické v Praze, Fakulta informačních technologií, 2016.



---

## Abstrakt

Doplňte

**Klíčová slova** logování, vestavěné systémy, logovací démoni, Linux, Rsyslog

---

## Abstract

Sem doplňte ekvivalent abstraktu Vaší práce v angličtině.

**Keywords** logging, embedded systems, logging daemons, Linux, Rsyslog



---

# Obsah

<b>Úvod</b>	<b>1</b>
<b>1 Technické požadavky</b>	<b>3</b>
1.1 Základní technické požadavky . . . . .	3
1.2 Rozšířené technické požadavky . . . . .	4
<b>2 Analýza</b>	<b>5</b>
2.1 Set-top box O2 TV - EKT DID7006mTF . . . . .	5
2.2 Volba postupu řešení . . . . .	5
2.3 Srovnání logovacích démonů . . . . .	5
2.4 Vzdálená konfigurace . . . . .	7
<b>3 Realizace</b>	<b>9</b>
3.1 Nasazení Rsyslogu . . . . .	9
3.2 Shell API . . . . .	9
<b>4 Testování</b>	<b>11</b>
<b>Závěr</b>	<b>13</b>
<b>Literatura</b>	<b>15</b>
<b>A Seznam použitých zkratk</b>	<b>17</b>
<b>B Obsah příloženého CD</b>	<b>19</b>



---

## Seznam obrázků



---

# Úvod





# Technické požadavky

Cílem je upravit logovací řešení pro set-top box EKT DID7006mTF [1] tak, aby splňovalo technické požadavky popsané v této kapitole. Řešení musí fungovat a být otestováno na zmíněném modelu set-top boxu a pokud možno by mělo být přenositelné i na jiné typy set-top boxů. Požadavky jsou rozděleny na základní a rozšířené. Rozšířené požadavky není nutno implementovat. V takovém případě je ale nutné zdůvodnit proč.

## 1.1 Základní technické požadavky

### 1.1.1 Snížení objemu logů

Je žádoucí snížit objem zasílaných logů z důvodu přílišného zatížení sítě a serverových disků. Původní řešení všechny logy odesílalo na vzdálené servery. Nové řešení by mělo odesílat pouze důležité zprávy tedy zprávy s nízkou severitou.

TODO1 probrat s Matějem: (už konkrétně specifikovat zadání) jaké severity a facility filtrovat (případně jiné podmínky)

### 1.1.2 Vzdálená konfigurace

Je nutno umožnit na dálku dočasně zvýšit objem zasílaných logů na původní úroveň. Je také zapotřebí zajistit perzistenci konfigurace logování i po restartu zařízení.

TODO2 jak má konkrétně to API vypadat, co má umět

### 1.1.3 Rate-limiting odesílaných zpráv

Nové logovací řešení musí být schopné provádět rate-limiting odesílaných zpráv tak, aby nepřekročilo maximální vyhrazenou šířku pásma. Bude umožněno nastavit jak dlouhodobé tak krátkodobé limity.

TODO3 jaké by měly být ty limity jak jsou řešeny ty limity v současném řešení

### 1.2 Rozšířené technické požadavky

#### 1.2.1 Post-processing zpráv

Zadavatel má pouze částečnou kontrolu nad zprávami generovanými aplikacemi na set-top boxu, například nedokáže ve všech případech eliminovat dlouhé prefixy u zpráv. Je proto nutno takové prefixy rozpoznat a vhodně odfiltrovat před odesláním. Ze stejného důvodu mají některé zprávy nevhodně vyplněnou severitu a položku app-name. Jejich správné hodnoty jsou uloženy v textu zprávy, jejíž formát je konstantní. Řešení bude schopné tyto údaje z těla zprávy extrahovat a nahradit jimi původní metadata.

#### 1.2.2 Komprese zpráv

Bylo by vhodné zvážit pro a proti komprese zpráv. Vyplatí se ušetřená přenesená data oproti režiji spojené s kompresí a dekompresí zpráv?

---

# Analýza

## 2.1 Set-top box O2 TV - EKT DID7006mTF

Hardware specifikace

Nainstalovaný software

Gu

PKGBUILD

## 2.2 Volba postupu řešení

Prvně je nutno zvážit, zda problém řešit na straně serveru nebo set-top boxu. Vhodnou konfigurací logovacího démona na straně serveru, který by nepotřebné zprávy zavčas rozpoznal, zahodil a dále nezpracovával bychom splnili požadavek na snížení zátěže serverových disků. Přetížení sítě se takto vyřešit ale nedá a proto toto řešení zavrhuji. Je tedy nutno problém řešit na straně set-top boxu kde původní řešení je postaveno na busy-box syslogd. Nabízí se možnost upravit fungování tím způsobem, aby se logy s nízkou severitou už na set-top boxu zahazovaly a pouze v případě potřeby bylo umožněné na dálku změnit konfiguraci démona tak, aby se povolilo logování pro logy s nastavenou danou komponentou a severitou. To vše přes SHELL-ové API. Součástí zadání je ale i implementovat škrcení zpráv, aby nedocházelo k zahlcení linky. Takovou možnost prostý syslogd neposkytuje a je proto nutno zvážit napsání vlastního démona či nasazení jiného, vyspělejšího logovacího démona.

## 2.3 Srovnání logovacích démonů

Démon v UNIXovém světě je označení pro takový proces, který oproti běžným procesům neinteraguje přímo s uživatelem, ale běží na pozadí operačního systému a funguje samostatně. Účelem logovacího démona je sběr logů

od ostatních procesů, které následně v závislosti na jeho konfiguraci dokáže filtrovat a ukládat na disk či odesílat na požadovaný vzdálený server.

V této kapitole zmíním a popíši vybrané logovací démony a v závěru kapitoly je porovnám.

### **BusyBox Syslogd**

Tato logovací utilita se skládá ze dvou démonu, jmenovitě z Klogd, který má na starost logy linuxového kernelu, druhým démonem je pak syslogd, který spravuje všechny zbylé logy. Oba tyto démoni mají velice omezenou funkcionalitu. Dokáží logy lokálně ukládat, přeposílat je dále po síti, zahazovat duplikáty, rotovat logy v závislosti na velikosti a tím výčet jejich funkcionalit končí.

### **Syslog-ng**

Flexibilní logovací démon zaměřený na centralizované a zabezpečené logování. Má široké možnosti nastavení a poskytuje obrovské množství funkcionalit. Takže jeho vhodným nakonfigurováním se dají snadno splnit všechny vytyčené technické požadavky až na požadavek pro možnost vzdálené změny konfigurace. Je nutno ale zmínit, že pokročilé funkce jako například šifrování zpráv, bufferování nebo message-rate kontrola jsou dostupné pouze v komerční closed-source verzi.

### **Rsyslog**

Výčet funkcionalit Rsyslogu je ještě obsáhlejší než u Syslog-ng. Technické požadavky se s jeho použitím tedy také dají splnit všechny, kromě vzdálené změny konfigurace. Oproti Syslog-ng je Rsyslog kompletně zdarma a open-source. Navíc není jen logovacím démonem, ale i analyzérem logů. Dokáže logy podle obsahu zprávy měnit, třídit a jinak s nimi nakládat. Že je Rsyslog vyspělý a kvalitní program dokazuje fakt, že je defaultním logovacím démonem na spoustě linuxových distribucích, jmenovitě například v Ubuntu. Jeho slabiny shledávám v nedostatečné dokumentaci a ve specifických případech v neefektivním analyzování logů mající za následek (obzvláště na embedded zařízení s pomalým ARM procesorem) rychlostní deficit. Jeho vývoj obstarává z velké většiny pouze jeden člověk, jeho původní tvůrce Rainer Gerhards. A v jednom člověku není snadné dovést tak rozsáhlý projekt k dokonalosti.

### **Porovnání výše zmíněných logovacích utilit**

Pouhým nasazením jakéhokoli známého logovacího démonu není možné splnit všechny vytyčené technické požadavky. V případě ponechání původního BusyBox syslogd démonu by pro splnění technických požadavků bylo nutno doimplementovat tolik funkcionalit, že by to výrazně přesahovalo rozsah bakalářské

práce. Výhodněji se jeví nasadit pokročilý logovací démon jako je Syslog-ng či Rsyslog. Oba totiž poskytují námi požadované funkcionality. Syslog-ng však většinu z nich poskytuje pouze v placené closed-source verzi a proto jsem se rozhodl pro Rsyslog.

## 2.4 Vzdálená konfigurace

Rsyslog při svém zapnutí čte konfigurační soubor `rsyslog.conf`, který za jeho běhu není možné měnit. Je pro to nutné napsat SHELL-ové API, které umožní na dálku přenastavit tento konfigurační soubor a restartovat rsyslog



## Realizace

### 3.1 Nasazení Rsyslogu

build

konfigurace

### 3.2 Shell API





## **Testování**



---

## **Závěr**



---

## Literatura

- [1] *EKT DID7006*. Dostupné z: <http://exploredoc.com/doc/3174828/model-did7006-high-definition-ott-stb>



## Seznam použitých zkratk

**GUI** Graphical user interface

**XML** Extensible markup language





## Obsah přiloženého CD

	readme.txt.....	stručný popis obsahu CD
	exe .....	adresář se spustitelnou formou implementace
	src	
	impl.....	zdrojové kódy implementace
	thesis .....	zdrojová forma práce ve formátu L <sup>A</sup> T <sub>E</sub> X
	text .....	text práce
	thesis.pdf .....	text práce ve formátu PDF
	BP_Vavricka_David_2016.pdf .....	text práce ve formátu PDF