

# Program incron ve službách administrátora

Lukáš Jelínek  
Jakubská 3  
Kutná Hora, Česká republika  
+420 606 362 315

lukas@aiken.cz

## ABSTRAKT

incron je nástroj (podobný standardnímu programu cron), který reaguje na události na souborech a spouští definované příkazy. Program incron má široké možnosti využití pro různé úkoly, které výrazně usnadní práci administrátora (notifikace, zálohování, správa verzí, obnova dat, úklid, automatické zpracování dat, statistiky, separace práv apod.).

## Klíčová slova

incron, inotify, Linux, soubor, událost, zálohování, oprávnění

## 1. ÚVOD

Program incron je nástroj, který prostřednictvím technologie inotify (které je součástí linuxového jádra) sleduje události na souborech a na základě těchto událostí spouští definované příkazy. Program pracuje s tabulkami pravidel – každý uživatel má svoji tabulku (spravovanou podobně jako u programu cron), dále může být libovolný počet systémových tabulek (akce se spouští s právy uživatele root). incron má rozsáhlé možnosti využití při správě serverů, desktopů i jiných počítačů.

## 2. O TECHNOLOGII INOTIFY

Technologie inotify je subsystém v jádře Linuxu, která umožňuje sledovat události na souborech v souborových systémech (v některých souborových systémech jen některé soubory nebo některé události). Tato technologie nahrazuje zastaralou technologii dnotify, která má řadu nevýhod.

Sledování pomocí technologie inotify funguje tak, že si běžící proces otevře speciální souborový deskriptor, přes který provádí veškeré manipulace se sledovacím mechanismem a na kterém může synchronním nebo asynchronním způsobem čekat na události. Informace o událostech proces získá čtením strukturovaných dat prostřednictvím souborového deskriptoru.

Jednotlivé sledované soubory mají přiřazeny speciální čísla (deskriptory) pro pozdější identifikaci – jak pro rozlišení událostí, tak pro manipulaci se sledovacím mechanismem. Události na souborech se řadí do fronty. Ve frontě může být uložen libovolný počet událostí do dosažení nastaveného limitu. Limitům podléhá také počet sledovaných souborů v rámci souborového deskriptoru inotify a počet souborových deskriptorů inotify.

## 3. HISTORIE PROGRAMU INCRON

Program incron vznikl na základě diskuse následující po zveřejnění informací o vydání první verze frameworku inotify-cxx, tedy sady objektů jazyka C++ pracujících s technologií inotify. Framework inotify-cxx se stal základem programu incron.

První verze programu incron byla vydána v září 2006 a obsahovala základní funkcionalitu pro spouštění příkazů na základě událostí na souborech. V dalších verzích postupně přibývaly další funkce, například systémové tabulky, hlášení

podporovaných typů událostí, konfigurace, možnost řízení přístupu k programu atd. Přidávání funkcionality bylo řízeno především požadavky uživatelů.

Program incron se postupně dostal do řady linuxových distribucí a stal se nástrojem volby k řešení široké škály problémů. Pro jednodušší ovládání vzniklo grafické uživatelské rozhraní jIncron napsané v jazyce Java.

Mezi nejdůležitější vlastnosti plánované pro budoucí verze programu incron patří zejména rekurzivní sledování (celé adresářové podstromy), možnost spouštění příkazů pod konkrétním uživatelem (v systémových tabulkách) nebo odesílání výstupu příkazů e-mailem.

## 4. FUNKCE PROGRAMU INCRON

Program incron implicitně běží jako démon, ale lze ho spustit i jako běžný program na popředí. Při spouštění načte konfiguraci (obejde se ale i bez ní) a zpracuje existující uživatelské a systémové tabulky. Veškeré tyto tabulky jsou za běhu dále monitorovány, při změně je program opět načte a aktualizuje stav sledování (aktuálně tak, že veškeré sledování zruší a vybuduje znovu; v budoucích verzích by se ale měly pouze promítnout provedené změny).

incron má pro každou tabulku jeden souborový deskriptor – sleduje události na všech těchto deskriptorech a při výskytu jedné či více událostí nejprve přesune všechny události z fronty v jádře do své vlastní fronty (aby při velkém počtu událostí nebylo nutné zvětšovat délku fronty v jádře a spotřebovávat tak cennou fyzickou paměť). Potom začne jednu událost po druhé zpracovávat a spouštět příkazy podle definovaných pravidel.

Příkazová řádka spouštěných příkazů se vyhodnocuje až v okamžiku spouštění, může totiž obsahovat i informace získané z události na souboru (např. typ události nebo název souboru). Během zpracování události spuštěným příkazem mohou dále přicházet stejné události, není-li to zakázáno (zákaz je zatím neatomický, nicméně v budoucích verzích se počítá s jeho atomicitou).

Příkazy definované v uživatelských tabulkách jsou samozřejmě spouštěny pod daným uživatelem, příkazy v systémových tabulkách se zatím vždy spouštějí pod uživatelem root (v budoucnosti bude možné uživatele určit).

S uživatelskými tabulkami se pracuje podobně jako u programu cron. Manipulační program incrontab umožňuje načtení tabulky z předem připraveného souboru nebo přímou editaci tabulky prostřednictvím editoru (určeného některým ze standardních způsobů, případně výchozím editorem vim). Systémové tabulky se spravují v běžných souborech.

## 5. VYUŽITÍ PROGRAMU INCRON

Program incron má širokou škálu využití v různých oblastech činností na počítači. Vzhledem ke svému charakteru a ke způsobu ovládání je určen především pro administrátory a pokročilé uživatele.

### 5.1 Notifikace

incron umožňuje notifikovat uživatele nebo správce o různých událostech na souborech – například změně konfiguračních souborů, uploadu do určitého adresáře, změně nebo smazání důležitých knihoven nebo systémových nástrojů (adresáře /lib, /sbin apod.), otevření nějakého souboru atd.

Notifikaci lze zajistit například e-mailovou cestou (kupř. pomocí příkazu sendmail nebo mutt) či přes XMPP/Jabber nebo nějaký jiný komunikační mechanismus. Stejně tak lze události zaznamenávat do souboru nebo do databáze. Notifikace může být doplňkovou operací k dalším zde uváděným činnostem.

### 5.2 Zálohování a správa verzí

Program incron lze využít k zálohování a k vytváření verzí souborů. Takto se dá postupovat třeba u konfiguračních souborů, ale i u dokumentů na souborovém serveru. Rozhodující událostí je zde uzavření souboru po otevření k zápisu.

K zálohování mohou posloužit běžné zálohovací nástroje nebo i obyčejné kopírování souboru (třeba s následným dalším zpracováním). Vytváření verzí se též nelší od situace, kdy se tyto verze vytvářejí ručně (např. v programech SVN, CVS, git, Bazaar a mnohých dalších).

### 5.3 Obnova dat

Administrátor systému může zajistit, aby při smazání důležitých souborů nebo jejich nechtěnému přepisu byly tyto nahrazeny původním souborem ze zálohy. Opět se to týká zejména klíčových konfiguračních souborů nebo základních nástrojů.

Obnovu dat (typicky zkopírováním odjinud nebo vytažením z archivu či repozitáře) lze realizovat například vytvořením nového souboru pod jiným názvem a následně přejmenováním na cílový soubor (aby byla zajištěna atomická kroka).

### 5.4 Úklid

Někdy může být žádoucí, aby bylo po nějakém programu (typicky běžícímu jako démon) náležitě uklizeno, a to i tehdy, když program skončí neobvyklým způsobem. I když takové ukončení programu není standardní věcí, lze případně problémy (mohou vznikat třeba při ladění) řešit i pomocí programu incron.

Pro incron se vytvoří v tabulce pravidlo, které bude sledovat uzavření spustitelného souboru s programem. Při výskytu takové události pak incron smaže příslušné soubory, případně s nimi naloží nějak jinak (např. něco odešle e-mailem nebo zazálohuje).

### 5.5 Automatické zpracování dat

U některých služeb lze pro příchozí data (poskytovaná uživateli) využít (třeba i veřejný) FTP server, na kterém mají uživatelé právo zápisu do určitého adresáře. incron může tento adresář monitorovat a při dokončení uploadu nového souboru provést potřebné zpracování dat.

Podobně ho lze využít i při sledování poštovních složek (např. realizovaných jako maildir) a příchozí poštu nějak dále

zpracovávat, zaznamenávat nebo o ní posílat notifikace (třeba přes Jabber). Lze to využít i pro realizaci e-mailových konferencí (takto například funguje konference pro incron, kde se jedná o spolupráci programů incron a SmartList).

### 5.6 Statistiky využití souborů

Administrátora může zajímat, jak uživatelé využívají různé programy nebo jiné soubory a zkoumat tyto údaje např. z časového hlediska. incron pak sleduje otevírání nebo zavírání souborů a zaznamenává je do souboru nebo databáze.

Lze to využít i ke zjišťování, kolikrát určitý program za svého běhu přistupuje k nějakému souboru a jakým způsobem s ním pracuje (například zda zapisuje přímo do souboru nebo vytváří nový soubor a přejmenovává ho).

### 5.7 Spouštění na žádost

Někdy může být potřeba umožnit spouštění nějakého příkazu/programu, aniž by měl uživatel možnost se do systému normálně přihlásit a pracovat v něm. Typicky má uživatel pouze FTP nebo SFTP přístup, případně třeba jen pomocí poštovního protokolu IMAP. Pak lze vazbou na vhodné soubory zajistit spouštění potřebných příkazů.

Realizace je možná například sledování operace zavření souboru (po čtení nebo zápisu) nebo vytvoření souboru v adresáři. Pomocí tohoto souboru lze také předávat příkazy nějaká data.

### 5.8 Separace práv

Program incron lze (stylem „spouštění na žádost“) využít k separaci práv spouštějícího uživatele a uživatele, pod kterým příkaz běží. Jedním z typických případů je potřeba spustit skript s právy jeho vlastníka. Běžně to z bezpečnostních důvodů nelze – skript nemůže využít SUID bit.

Protože příkazy z uživatelských tabulek programu incron běží vždy s právy daného uživatele, může tento uživatel připravit pravidla, která která umožní jiným uživatelům bezpečně spouštět skript s právy uživatele, který ho vytvořil (resp. který vlastní příslušnou tabulku).

Jinou takovou oblastí jsou webové aplikace požadující vykonání nějaké privilegované akce. V systémové tabulce programu incron se nadefinují (s maximálním ohledem na bezpečnost) příkazy, které bude aplikace spouštět. Pomocí vyvolání události na souboru se privilegovaná akce spustí, webová aplikace si může případně i počkat na výsledek (sdělený opět přes nějaký soubor nebo jinak).

### 5.9 Správa instalací

Přestože je vždy metodou první volby instalace programů z balíčků, někdy se nelze obejít ani bez dodatečné instalace např. pomocí make install. Protože při větším množství souborů v cílových adresářích (typicky v /usr/local/bin atd.) už není v silách člověka vše uhlídat, lze ke správě instalací využít incron.

Program incron může hlídat příslušné adresáře a zaznamenávat změny. Záznam změn může mít i charakter tvorby odinstalačního skriptu, takže pozdějším spuštěním takového skriptu lze uvést adresáře do původního stavu.

Výhodné může být i spojení programu incron se systémem správy verzí, kdy lze pro veškeré změny vytvářet verze a návratem ke konkrétní verzi pak uvést systém do požadovaného stavu.

## 6. PODĚKOVÁNÍ

Děkuji všem, kteří se podíleli na zlepšování a rozšiřování programu incron, zejména správcům distribučních balíčků a oznamovatelům nalezených chyb.

## 7. REFERENCE

- [1] Corbet, J. 2004. Watching filesystem events with inotify. LWN.net. <http://lwn.net/Articles/104343/>
- [2] Love, R. 2005. Kernel Korner - Intro to inotify. Linux Journal. <http://www.linuxjournal.com/article/8478>