SYSLOG-NG

Logovací systémy v OS Linux

Jan Pikl

Syslog-ng

- Nástroj pro správu logování pro Linux a další Unix-like systémy
- Moderní náhrada za syslogd
- Vlastnosti
  - Dobře konfigurovatelný
  - Široké možnosti filtrace log. zpráv
  - Posílání logů přes síť
  - Šifrování
  - Centralizovaná správa logování

Verze syslog-ng

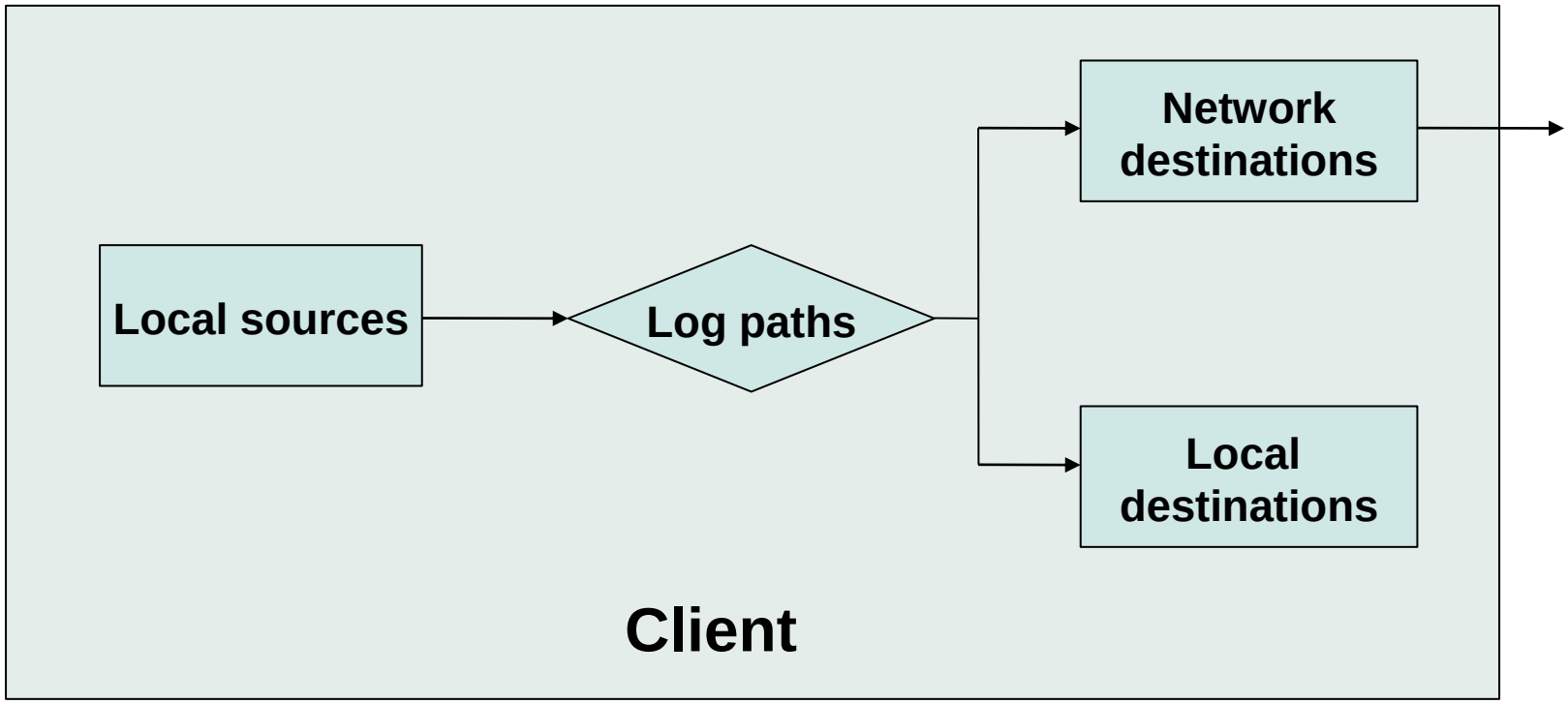
- Open Source Edition
  - Otevřený zdrojový kód, zdarma
  - V repozitáři většiny Linuxových distribucí
- Premium Edition
  - Closed source, placená verze
  - Více vlastností (disk-based buffering, logstore, …)
  - Oficiálně podporované platformy
    - Debian, Red Hat, CentOS, SLES, openSuse
    - FreeBSD, HP-UX, Solaris, …

Jak syslog-ng pracuje

- Syslog-ng beží v systému jako démon
  - Přijímá zprávy
    - Jádro OS, programy, síť, ...
  - Zpracovává zprávy
    - Filtrace, analýza, …
  - Ukládá / odesílá zprávy
- 3 způsoby konfigurace
  - Klient
  - Relay
  - Server

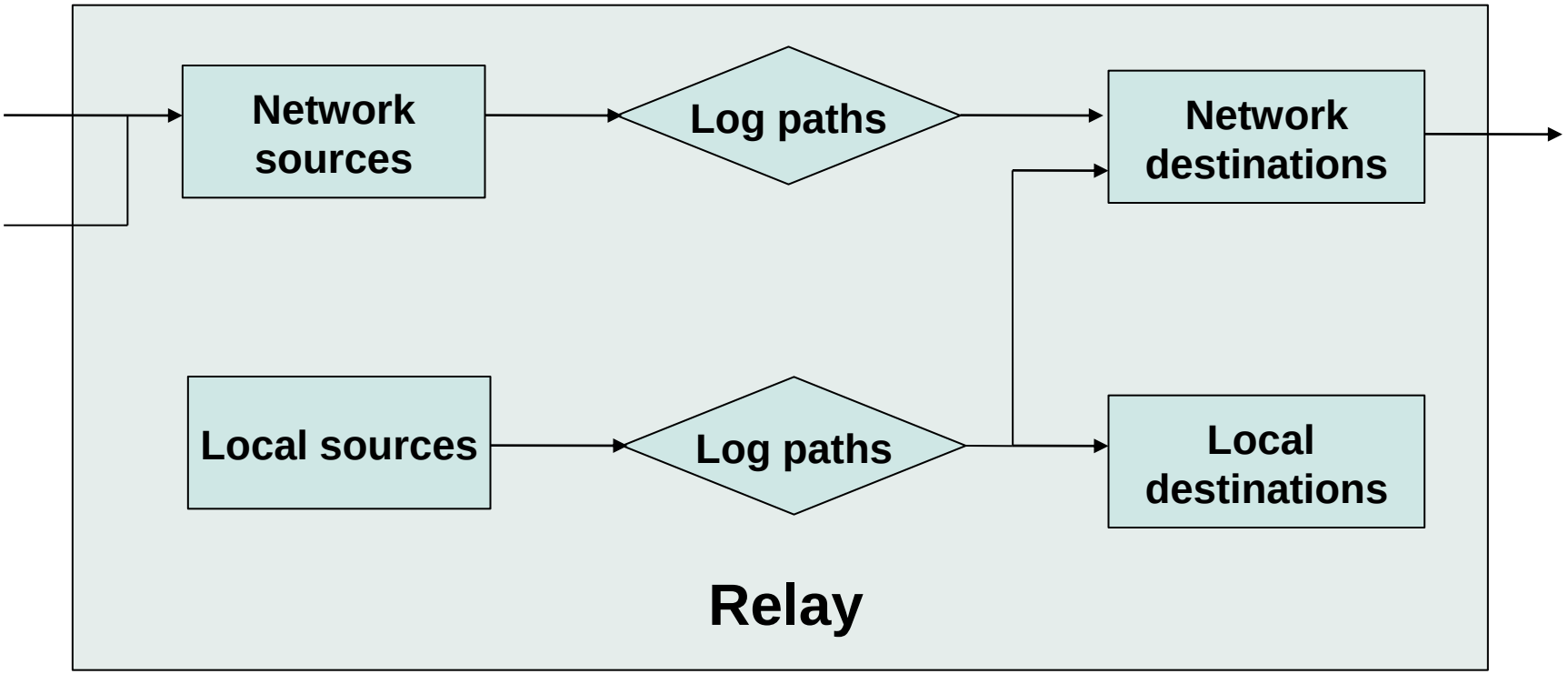
Klient

- Přijímá pouze lokální zprávy
- Zprávy ukládá lokálně / odesílá do sítě



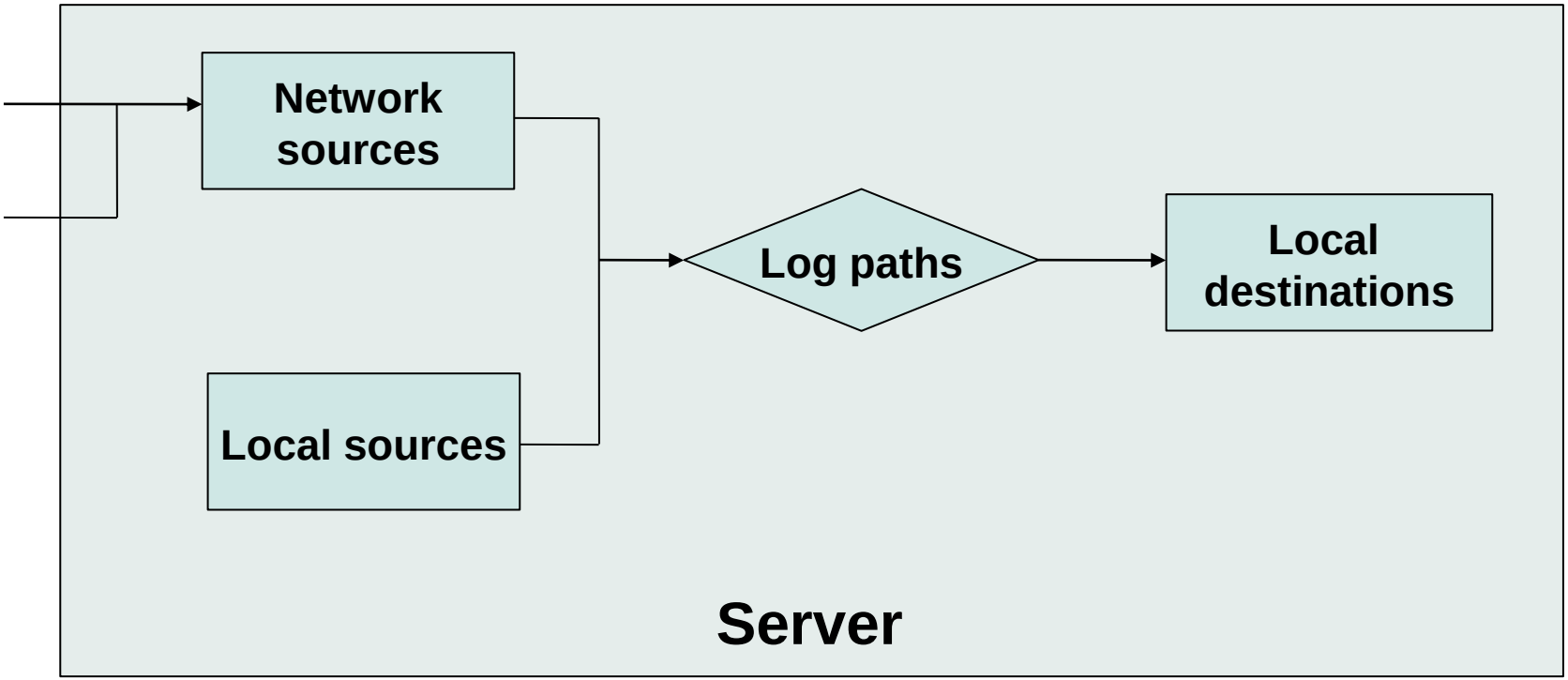
Relay

- Forwarduje příchozí zprávy
- Ukládá pouze lokální zprávy



Server

- Přijímá zprávy ze sítě
- Archivuje zprávy (soubory, logstore, databáze)



Zdroje zpráv

- Lokální
  - Jádro OS, soubory, aplikace
  - Unix sockety (např. /dev/log)
  - Pojmenované roury
- Síť
  - UDP
  - TCP
    - Nešifrovaná komunikace
    - Šifrovaná komunikace (TLS)

Destinace zpráv

- Lokální
  - Soubory
  - Unix sockety, pojmenované roury, aplikace
  - SQL databáze
  - Logstore
- Síť
  - UDP
  - TCP
    - Nešifrovaná komunikace
    - Šifrovaná komunikace (TLS)

SQL databáze

- Pouze v Premium Edition
- Ukládání zpráv do SQL databází
  - MySQL
  - PostgreSQL
  - Microsoft SQL
  - Oracle DB
- Definice sloupců tabulky
- Automatická tvorba tabulek
  - msgs_${YEAR}_${MONTH}_${DAY}

Logstore

- Pouze v Premium Edition
- Binární soubor
  - Rozdělen na oddíly (chunky)
    - Komprese
    - Šifrování (AES)
    - Časová značka
  - Kontrola integrity (SHA-1)
- Zabezpečená archivace logů
- Nástroj lgstool – lgstool cat file

Filtrace zpráv

- Filtrace dle
  - Priority (alert, warning, debug, ...)
  - Typu (kern, user, ftp, …)
  - Programu
  - Obsahu zprávy
  - ...
  - Hodnoty makra
- Možnost použití regulárních výrazů

Makra a šablony

- Makra
  - Proměnné obsahující část zprávy
  - Použití
    - Filtrace
    - Šablony
- Šablony
  - Změna obsahu zprávy
    - [$ISOTIME][$PROGRAM] - $MSG
  - Nastavení cesty k souborům
    - /var/log/$YEAR.$MONTH.$DAY/$PROGRAM.log

Analýza zpráv

- CSV parser
  - server.com:80 → $HOST, $PORT
  - Nastavení uživatelských maker
- Pattern DB
  - XML soubor
  - Databáze vzorů
    - @IPv4:addr@ port @NUMBER:port@
  - Klasifikace zpráv
  - Nastavení uživatelských maker
  - Mnohem rychlejší než regulární výrazy

Řízení toku

- Co nastane při přetížení ?
  - Výstupní buffer je zaplněný
  - Přijaté zprávy jsou zahazovány
- Možnost nastavení řízení toku
  - log_fech_limit – max. příchozích zpráv 1 spojení
  - max_connections – max. počet spojení
  - log_iw_size – velikost okénka zpráv zdroje
  - log_fifo_size – velikost výstupního bufferu
- Použití diskového bufferu

Diskový buffer

- Pouze v Premium Edition
- Ukládání neodeslaných zpráv na pevný disk
  - Při zaplněném výstupním bufferu
  - Při ztrátě spojení
- Odeslání uložených zpráv až když to je možné
- Perzistentní uložení zpráv
  - Zprávy se neztratí ani při restartu syslog-ng

Syslog-ng Windows agent

- Součást Premium Edition
- Speciální aplikace pro platformu Windows
  - Běží jako služba
  - Konfigurace v GUI
- Sbírá a shromažďuje log. zprávy
  - Události systému
  - Textové soubory
- Odesílá zprávy syslog-ng serveru
  - Podpora šifrování (TLS)

Děkuji za pozornost

Prostor pro vaše dotazy