U.PORTO

FACULDADE DE CIÊNCIAS
UNIVERSIDADE DO PORTO

[dcc]

LOGGING

ADMINISTRAÇÃO DE SISTEMAS

2021/2022

ROLANDO MARTINS

Referências dos slides

- O conteúdo destes slides é baseado no livro da disciplina: “Unix and Linux System Administration Handbook (4ªEd)” por Evi Nemeth, Garth Snyder, Trent R. Hein e Ben Whaley, Prentice Hall, ISBN: 0-13-148005-7
- Os slides de Admin. Sistemas do Prof Manuel Eduardo Correia também são usados.
- As imagens usadas têm a atribuição aos autores ou são de uso livre.

Objetivos

- Manter o registo de dados relativamente às operações do sistema
- Deteção/inspeção de falhas
- Pedidos de entidades policiais
- Políticas de segurança da entidade

Exemplo log centralizado

```
Dec 18 15:12:42 av18.cs.colorado.edu sbatchd[495]: sbatchd/main:
ls_info() failed: LIM is down; try later; trying …
Dec 18 15:14:28 proxy-1.cs.colorado.edu pop-proxy[27283]: Connection from
128.138.198.84
Dec 18 15:14:30 mroe.cs.colorado.edu pingem[271]:
malteseoffice.cs.colorado.edu has not answered 42 times
Dec 18 15:15:05 schwarz.cs.colorado.edu vmunix: Multiple softerrors: Seen
100 Corrected Softerrors from SIMM J0201
Dec 18 15:15:16 coyote.cs.colorado.edu PAM_unix[17405]: (sshd) session
closed for user trent
Dec 18 15:15:48 proxy-1.cs.colorado.edu pop-proxy[27285]: Connection from
12.2.209.183
Dec 18 15:15:50 av18.cs.colorado.edu last message repeated 100 times
```

Locais dos Diretórios

`/var/log`

`/var/adm`

- Não usado

- Mas podem ser definidas pelas aplicações:

`/var/log/samba`

File	Program	Where	Freq	Systems	Contents
acpid	acpid	F	64k	RZ	Power-related events
auth.log	sudo, etc.b	S	M	U	Authorizations
apache2/*	httpd (v2)	F	D	ZU	Apache HTTP server logs (v2)
apt*	APT	F	M	U	Aptitude package installations
boot.log	rc scripts	F	M	R	Output from system startup scripts
boot.msg	kernel	H	–	Z	Dump of kernel message buffer
cron, cron/log	cron	S	W	RAH	cron executions and errors
cups/*	CUPS	F	W	ZRU	Printing-related messages (CUPS)
daemon.log	various	S	W	U	All daemon facility messages
debug	various	S	D	U	Debugging output
dmesg	kernel	H	–	RU	Dump of kernel message buffer
dpkg.log	dpkg	F	M	U	Package management log
httpd/*	httpd	F	D	R	Apache HTTP server logs (in /etc)
kern.log	kernel	S	W	U	All kern facility messages
lastlog	login	H	–	RZ	Last login time per user (binary)
mail*	mail-related	S	W	all	All mail facility messages
messages	various	S	W	RZUS	The main system log file
samba/*	smbd, etc.	F	W	–	Samba (Windows/CIFS file-sharing)
secure	sshd, etc.	S	M	R	Private authorization messages
syslog*	various	S	W	SUH	The main system log file
warn	various	S	W	Z	All warning/error-level messages
wtmp	login	H	M	all	Login records (binary)
Xorg.n.log	Xorg	F	W	RS	X Windows server errors
dnf.log	dnf	F	M	R	Package management log

Exemplos de logs e programas

Where:

S = Syslog, H = Hardwired,
F = Configuration file

Freq:

D=Daily, W=Weekly,
M=Monthly,
N[u] = Size-based, in kB or MB

Systems:

U=Ubuntu, Z=SUSE, R=Red Hat and CentOS, S=Solaris,
H=HP-UX, A=AIX

(ver tabela completa no livro)

rsyslog

- "Rocket-fast SYStem for LOG processing"
- Em Linux o sistema usado por defeito

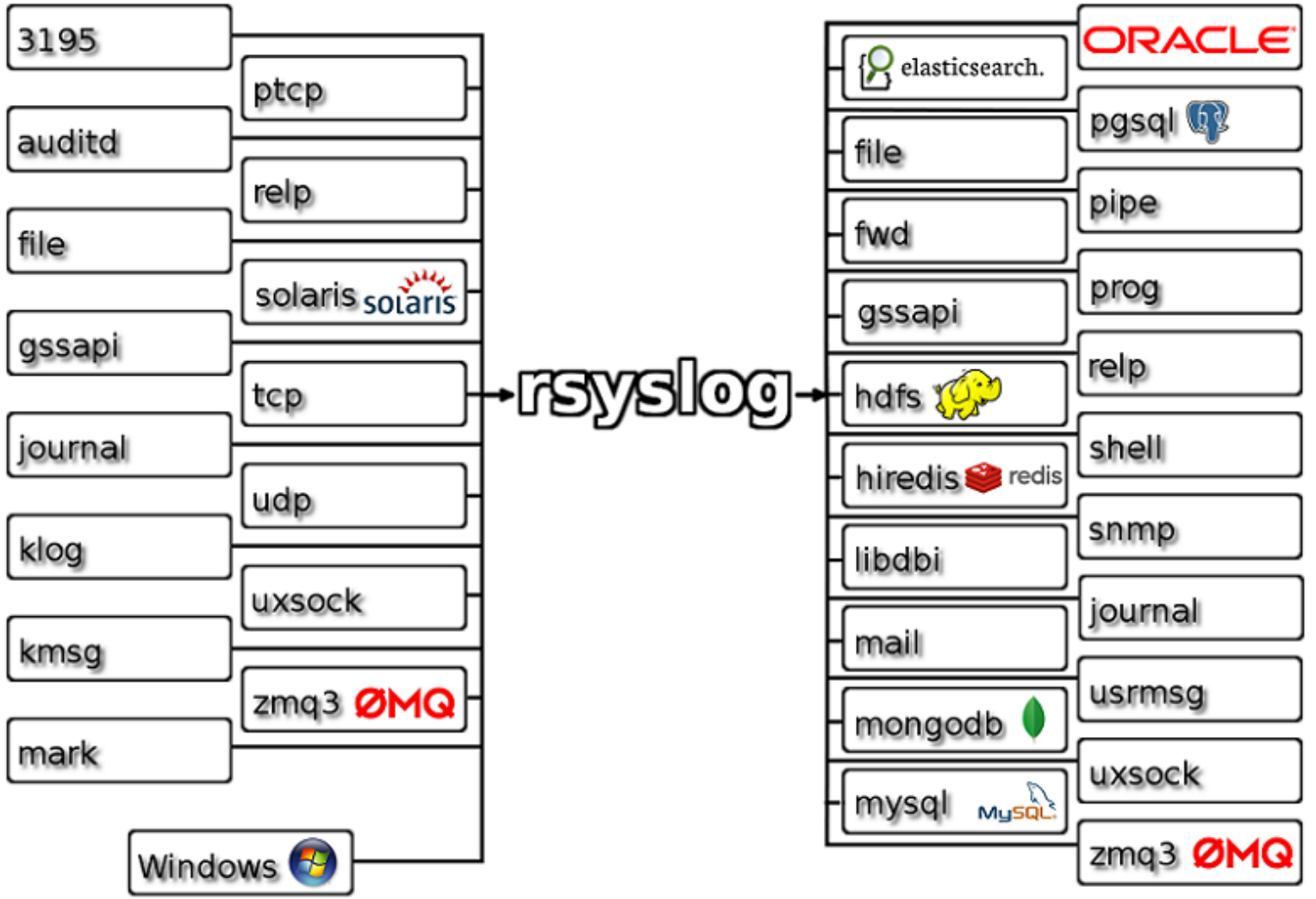


Imagem de rsyslog

(r)syslog

- Em Linux o sistema usado por defeito
- Configuração em:

`/etc/rsyslog.conf`

`/etc/rsyslog.d`

  - Fedora usa o rsyslog
  - Ubuntu também

(r)syslog

- Composto por:
  - Daemon (serviço): `rsyslogd`
  - Bibliotecas: `syslog`
  - Linha de comando: `logger`

- `/dev/log`: link simbólico para `/run/systemd/journal/dev-log`
  - Socket para escrita no log
- Protocolo definido por RFC5424

Objetivos rsyslog

- Receber mensagem de log e guardá-las nos locais “apropriados”
- Configuração estipula esses locais
- Formato:

  seletor ação
- Onde o seletor tem o formato:

  subsistema.nível
- Exemplo:

```
cron.info                /var/log/cron
```

subsistema. (facilities)

Facility	Programs that use it
*	All facilities except “mark”
auth	Security and authorization-related commands
authpriv	Sensitive/private authorization messages
cron	The cron daemon
daemon	System daemons
kern	The kernel
local0-7	Eight flavors of local message
lpr	The line printer spooling system
mail	sendmail and other mail-related software
mark	Time stamps generated at regular intervals
news	The Usenet news system (obsolete)
syslog	syslogd internal messages
user	User processes (the default if not specified)
uucp	UUCP subsystem

.níveis (levels)

- Níveis seguintes são de maior para menor severidade

Level	Approximate meaning
`emerg`	Panic situations
`alert`	Urgent situations
`crit`	Critical conditions
`err`	Other error conditions
`warning`	Warning messages
`notice`	Things that might merit investigation
`info`	Informational messages
`debug`	For debugging only
`none`	No logging

- Incluir num nível implica "receber" os níveis acima
- Nível none exclui o subsistema do logging

Exemplos

- = apenas do nível indicado
- ! exceto este nível

Selector	Meaning
mail.info	Mail-related messages of info priority and higher
mail.=info	Only messages at info priority
mail.info;mail.!err	Only priorities info, notice, and warning; not err and above
mail.debug;mail.!=warning	All priorities except warning

Ações

Action	Meaning
filename	Appends the message to a file on the local machine
@hostname	Forwards the message to the syslogd on hostname
@ipaddress	Forwards the message to the syslogd on host ipaddress
|fifoname	Writes the message to the named pipe fifoname
user1,user2,...	Writes the message to the screens of users if they are logged in
*	Writes the message to all users who are currently logged in

rsyslog “extras”

- Envio para:
  - Bases de dados
  - SNMP
- Formato do tempo
- Filtros extra baseados em
  - Propriedades (hostname, tag, mensagem, etc.)
  - Expressões
- Possibilidade de definir templates para as ações
- Ver man rsyslog.conf

journalctl

Ver How To Use Journalctl to View and Manipulate Systemd Logs, por Justin Ellingwood

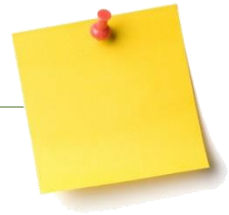
- Sistema de journaling do system
- Consegue cooperar com rsyslog (caso dos sistemas Fedora)
- Ferramenta
  - `journalctl`
- Exemplos:
  - `journalctl -b` #último boot com -r apresenta pelo mais recente
  - `journalctl --since yesterday`
  - `journalctl --unit NetworkManager`
  - `journalctl -k` # mensagens do kernel
  - `journalctl -p err` # mensagens por prioridade

AuditD

- Userspace daemon responsável por registar eventos para auditoria do sistema
  - Usado pelo SELinux
- Desenvolvido pela RedHat, sistema de log de eventos ligados à segurança do sistema
- Ver man de `ausearch`, `aureport`, `auditctl`, `augenrules`
- Relativamente ao SELinux ver `audit2why`, `audit2allow`
  - Permite explicar mensagens do SELinux guardadas pelo audit e criar módulos para permitir o que foi negado

Ver CentOS SELinux e RedHat audit2allow

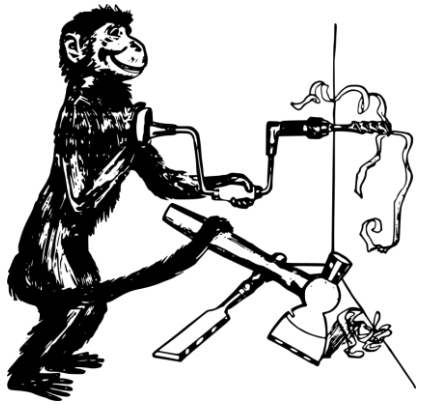
Notas



- Os timestamps são os locais
  - Quando se envia para máquina remota serão os dessa máquina ➔ sincronização pode ser necessária
- Muitos logs se não estiverem bem distribuídos por ficheiros podem "poluir" os mesmos logs
  - Ter em conta se se centralizar os logs
- Kernel logging
  - Suporte no rsyslogd ou journal
  - Arranque ter um sistema para escrever o log
    - Guardar num buffer, escrito quando sistema arranca

Ferramentas

- logrotate
  - Rotação dos logs, comprimindo-os
  - Configuração flexível
- Parsing e "monitorização" dos logs
  - SEC - simple event correlator
  - LogWatch
  - Logtail-v3
  - Simple Log Watch (swatch)
  - Logcheck



Resumo

- Logging
- rsyslog e configuração
- journalctl
- auditd
- Ferramentas extra

[dcc]

U.PORTO

FACULDADE DE CIÊNCIAS
UNIVERSIDADE DO PORTO

QUESTÕES/ COMENTÁRIOS