Abordagem

- Finalidade do sistema log
- Modo de utilização
- Padrões
- Manutenção dos logs

Sistema de registro de eventos

- Kernel Log
- Syslog
- Logrotate
- Crontab
- Chamadas de Sistema

Sistema de registro de eventos

- Importante para depuração, acompanhameno e auditoria de sistemas.
- Dois sitemas separados: nível de kernel (kernel log) e nível de usuário (user space syslog).
- Dispor de padrões e formas simples para análise dos dados registrados.
- Manutenção e descarte dos conteúdos antigos de log.
- Execução automática da renovação dos arquivos.

Kernel Log

- Buffer de armazenamento para eventos gerados pelo kernel.
- Klogd deve receber mensagens do kernel para supostamente repassá-las a outro subsistema
- Kernel armazena mensagens em buffer /proc/kmsg
- Daemon de klog pode fazer coleta direta ao buffer ou então receber/executar chamadas de sistema.

Kernel Log

- Pode rodar como daemon ou como cliente do syslog
- /var/log/dmesg ou dmesg
- Klog traduz símbolos de System.map ou recebe informações dos próprios módulos
- /proc/sys/kernel/printk

Define níveis de mensagens a serem impressos no console

Níveis de criticidade

- O que fazem o comandos?

#> dmesg -n 1

ou

#> dmesg -n 4

Syslog

- **Padrão para sistema de log. Solução de problemas como formatação e troca de registros entre sistemas diferentes**
- **Principais sistemas de log: syslog, rsyslog, sysklog.**

Níveis de prioridade de logs do kernel

0 Situação de emergência (KERN_EMERG).
1 Um erro crucial ocorreu (KERN_ALERT).
2 Um erro crítico ocorreu (KERN_CRIT).
3 Um erro ocorreu (KERN_ERR).
4 Um alerta foi gerado (KERN_WARNING).
5 Algo deve ser verificado (KERN_NOTICE).
6 Verborrágico e informações detalhadas (KERN_INFO).
7 Mensagem de acompanhamento (KERN_DEBUG).

Syslog

- Arquivo de configuração em /etc/syslogd.conf e diretório de configuração /etc/syslog.d/
- Debian utiliza rsyslog como solução integrada
- Sistema em serviço por socket (protocolo bem definido há mais de 30 anos)
- Regras definidas por linha
- São pré definidos os recursos. Cada qual com 8 níveis de criticidade
- Sintaxe: ”recurso.nível ação”

Syslog

- Recursos

- * - auth - authpriv - cron - daemon - ftp - kern - local [0-7]
- lpr - mail - mark - news - syslog - user

Syslog

- Níveis

- emerg
- alert
- crit
- err
- warning
- notice
- info
- debug

Syslog

- Ações
- @ipaddress, username, arquivo, etc

- Seletores
- , . ; = != ! *

Syslog

- **Se um arquivo de syslog.conf contiver as seguintes linhas, quais serão os registros e seus respectivos destinos?**

auth,authpriv.*	/var/log/auth.log
daemon.*	/var/log/daemon.log
kern.debug;kern.!err	/var/log/kern.log
lpr.warning;daemon.!=alert	/var/log/lpr.log
mail.=info	@192.168.0.1

Exercitando

Determine a diferença entre os dois registros de log

mail,uucp.notice;uucp.!=alert /var/log/mail

mail,uucp.notice;uucp.!alert /var/log/mail

Problema no voulme

O que vai acontecer quando /var/log/kern.log crescer indefinidamente?

- Por exemplo, se esse arquivo atinigir 4 Gbytes de tamanho?
- Se esse arquivo estiver guardado por 3 anos no mesmo sistema sem ser renovado? Como idnetificar informações antigas?

Solução

- Automatização do processo de retenção e descarte dos arquivos

Solução:

LOGROTATE

Logrotate

- Rodízio de arquivos de registro do sistema
- Configuração em /etc/logrotate.conf e /etc/logrotate.d/
- Arquivos criados para cada um dos sistemas que utilizam o syslog
- Conjunto de regras para cada um dos arquivos

Logrotate

- **Opções**

prerotate
rotate n
sharedscripts
size=logsize
create mod user group
nocreate
prerotate
rotate n
sharedscripts
size=logsize
create mod user group
nocreate

Logrotate

- **Rotação definida pela frequência e quantidade**

rotate 15

daily

arquivo

arquivo.1

arquivo.2

arquivo.3

.

.

.

arquivo.15

Logrotate

- **Exemplo**

```
/var/log/ppp-connect-errors {
        weekly
        rotate 4
        missingok
        notifempty
       compress
        nocreate
}
var/log/wtmp {
   missingok
   monthly
   create 0664 root utmp
   rotate 1
}
```

Exercitando

- Considere a data atual de 15/05/2012.

Crie uma regra de logrotate que permita a você ainda manter em filesystem local, o registro de log do dia 20/04/2012 do arquivo /var/log/bazinga.log.

Faça com que a primeira rotação do arquivo não seja compactada

Por fim, elimine a necessidade de criar o arquivo caso o mesmo ainda não exista

Syslog: Interface

- Utilizar interface como logger, openlog( ) e closelog( )

EX:

#> logger -p local0.notice -t TAG "HOLA"

#> logger -p local0.notice -t TAG -f /etc/hosts

Crontab

- Agendador de tarefas: scripts em lote, execuções repetitivas, etc
- Arquivos de configuração /etc/cron.daily, /etc/cron.hourly, /etc/cron.monthly
- crontab -e | crontab -l
- min hora diames mes diasemana

Problema

- Sistema muito antigo
- Apesar de padronizada não requer autenticação e facilmente burlado por hackers
- Proposta de atualização pelo novo sistema “Journal” (ainda não muito popular)

Conclusão: Usando o syslog

- Preocupar-se com sincronismo e data do sistema
- Preocupar-se com o agendamento do rodízio (crontab) e com política de retenção
- Configuração adequada das ações/destinos
- Reiniciar daemons de syslog em qualqer alteração de data.
- Finalmente, utilizar alguma ferramenta para análise e coleta qualitativa do kernel