Recolha e Gestão de Logs

José Pedro Oliveira
(jpo@di.uminho.pt)

Grupo de Sistemas Distribuídos
Departamento de Informática
Escola de Engenharia
Universidade do Minho

Administração de Sistemas I
2006-2007

Conteúdo

1. Sincronização de tempo
   - Introdução
   - Unix
   - Windows
   - Referências

Introdução

Sincronização de tempo

- O protocolo NTP (Network Time Protocol) sincroniza relógios de conputadores e routers na Internet
- Fornece precisões de poucas dezenas de milisegundos em WANs, de submilisegundos em LANs e de submicrosegundos usando uma fonte precisa de tempo tal como um receptor GPS ou um oscilador de Cesium

Razões

- Detecção de intrusões e *logging*
- Monitorização, aquisição de valores e controlo de redes
- Jornais de base de dados distribuídas
- Transações RPC *at-most-once*
- Ordenação de transações em bases de dados distribuídas
- Serviços de *timestamping* criptográficos
- Gestão de chaves criptográficas e controlo de tempo de vida
- Sincronização de *streams* em multimédia distribuída

Standards

Normas

DATE - Date Protocol
Request for Comments: 868

NTP - Network Time Protocol
Versão 3: Request for Comments: 1305
Versão 4: draft

SNTP - Simple Network Time Protocol
Versão 4: Request for Comments: 2030

Protocolo

Protocolo UDP (porta 123)

Funcionamento

Alternativas

1. O cliente obtem informação horária de um ou mais servidores por *polling* e usa essa informação para calibrar o seu relógio
2. O cliente recebe informação horária difundida por *broadcast* por um servidor e usa essa informação para calibrar o seu relógio
3. O cliente recebe informação horária difundida por *multicast* por um servidor e usa essa informação para calibrar o seu relógio (NTP: endereço multicast reservado: 224.0.1.1)

Utilitários

Utilitários

- **ntpd**
  - *daemon* de sistema que mantem a informação horária em sincronismo com servidores de tempo padrão da Internet
- **ntpdate**
  - actualiza relógio com base em informação obtida ao fazer *polling* a servidores NTP
  - deve ser executado como root
- **ntpq**
  - utilitário de query
- **ntptrace**
  - permite descobrir hierarquia de servidores de tempo

Windows

Windows 9x (95, 98, Me)

Necessitam de software adicional

Windows NT 3.5x, 4.0

Serviço incluido no Resource Kit (timserv ou w32time (??)).

Windows 2000/XP/2003

Serviço de tempo - **Windows Time** - incluido no sistema operativo.

Diversos

`http://nettime.sourceforge.net/`
`http://home.att.net/~Tom.Horsley/ntptime.html`

Windows Time Service

Windows Time service

- Plataformas: Windows 2000, XP e 2003.
- Nome longo: **Windows Time**
- Nome curto: **W32Time**
- Registry: HKLM\System\CurrentControlSet\Services\W32Time

Arrancar/parar o serviço de tempo

- `net start w32time`
- `net start "windows time"`
- `net stop W32Time`
- `net stop "Windows Time"`

Windows Time Service

net time

- `net time /setsntp:ntp.di.uminho.pt`
- `net time /setsntp`
- `net time /querysntp`

Outras ferramentas

- `w32tm` - Windows Time Service Diagnostic Tool

Windows Time Service

C:\> net time /setsntp:ntp.di.uminho.pt

The command completed successfully.

C:\> net stop w32time

The Windows Time service is stopping.
The Windows Time service was stopped successfully.

C:\> net start w32time

The Windows Time service is starting.
The Windows Time service was started successfully.

Referências

Referências

- **Network Time Protocol**
  `http://www.ntp.org/`
- **NTP specification documents**
  `http://www.eecis.udel.edu/~mills/`
- **OpenNTPD**
  `http://www.openntpd.org/`
- **The Windows Time Service**

Conteúdo

2 Protocolo syslog
- Syslog
- Syslog-NG
- Syslog em Windows

Introdução

Syslog

- de-facto standard
- consiste num *daemon*, uma API e um protocolo RFC3164
- `http://www.infodrom.org/projects/sysklogd/`

Utiliza

- protocolo UDP (porta por omissão: 514)
- ficheiros de texto

Introdução

Ficheiro de configuração

- /etc/syslog.conf

Regras de logging

Regras de logging

As regras de logging são especificadas no ficheiro de configuração **syslog.conf**. Cada regra é composta por dois campos separados por um ou mais espaços (ou tabs):

1. **selector**
   - padrão de *facilities* e prioridades
2. **acção**
   - destino a dar às mensagens

Selectores

Selectores (filtros)

- par facility.priority
- operador: ‘,’
- operador: ‘;’

Facilities (1/2)

Número de classes de mensagens

- 12 + 8

Classes de mensagens

- **auth** - security/authorization messages
- **authpriv** - security/authorization messages (private)
- **cron** - clock daemon
- **daemon** - system daemons
- **ftp** - ftp daemon
- **kern** - kernel messages
- **lpr** - line printer subsystem

Facilities (2/2)

Classes de mensagens (cont.)

- **mail** - mail system
- **news** - network news subsystem
- **syslog** - messages generated internally by syslogd
- **user** - random user-level messages
- **uucp** - UUCP subsystem
- **local0 .. local7** - reserved for local use

Wildcards

- * - todas as classes de mensagens

Priorities (1/2)

Graus de prioridade: 8 (ordenados)

- **emerg** - system is unusable
- **alert** - action must be taken immediately
- **crit** - critical conditions
- **err** - error conditions
- **warning** - warning conditions
- **notice** - normal but significant condition
- **info** - informational
- **debug** - debug-level messages

Priorities (2/2)

Wildcards

- * - todas as prioridades
- **none** - nenhuma das prioridades

Nota

- A categoria e a prioridade de uma mensagem são especificadas pelo programa que a gera e não pelo syslog

Modificadores

Modificadores

= - restringe a uma prioridade especifica

! - exclue certas prioridades

Exemplos

- **mail.notice** - todas as prioridades >= notice
- **mail.=notice** - prioridade == notice
- **mail.!notice** - todas as prioridades < notice
- **mail.!=notice** - todas as prioridades com a excepção de notice

Destinos de mensagens

Destinos

- ficheiros
- pipes (|)
- ttys
- impressoras
- máquinas remotas (@)
- utilizadores (todas as consolas)

Exemplo de configuração

Exemplo de um ficheiro de configuração

```
# Log anything (except mail) of level info or higher.
# Don't log private authentication messages!
*.info;mail.none;authpriv.none        /var/log/messages

# The authpriv file has restricted access.
authpriv.*                            /var/log/secure

# Log all the mail messages in one place.
mail.*                                /var/log/maillog

# Save local0 messages in a different file
# Don't sync after every logging
local0.*                              -/var/log/dhcp.log
```

Problemas

Problemas

- fontes e destinos de mensagens
  - pouca diversidade (rede: udp/syslog(514))
- segurança
  - não possui mecanismos de autenticação
  - sujeito a ataques DOS e a falsificação de pacotes
- filtragem
  - não possui mecanismos de filtragem para além de facilities/priorities (por exemplo: string, endereço IP)
- permissões de ficheiros de log
  - não permite especificar permissões de ficheiros

Desempenho

Sync

- **-** - não fazer sync em cada mensagem
- degradação drástica de desempenho

Medidas de segurança

Controlo de acessos baseado em *hosts*

- **tcp_wrappers**
  - biblioteca *linkada* com o *daemon*
  - ficheiros: /etc/hosts.allow e /etc/hosts.deny
- **iptables (ipchains)**
  - controlo externo ao *daemon*
  - iptables -A INPUT -i eth0 -p udp -s 192.168.0.1 –dport syslog –sport syslog -j ACCEPT

Introdução

Syslog-NG

O daemon **syslog-ng** tenta preencher algumas lacunas do syslogd:

- criação de filtros sobre o conteudo das mensagens
- utilização do protocolo TCP

Homepage

`http://www.balabit.com/products/syslog_ng/`

Log de mensagens

A rota de uma mensagem é constituída por três partes:

1. uma fonte (*source*)
2. um destino (*destination*)
3. zero ou mais regras de filtragem (*filtering rules*)

Ficheiro de configuração

Ficheiro de configuração

`/etc/syslog-ng/syslog-ng.conf`

Formato

O ficheiro de configuração é constituído por:

- opções globais
- fontes de mensagens
- destino de mensagens
- filtros
- regras de logging

Opções globais

Sintaxe

```
options {
    opcao1(parametros);
    opcao2(parametros);
    ...
};
```

Opções globais

Quando especificadas permitem modificar o comportamento do syslog-ng.

Opções globais - exemplo

Exemplo de opções globais

```
options {
    sync (0);
    time_reopen (10);
    log_fifo_size (1000);
    long_hostnames (off);
    use_dns (no);
    use_fqdn (no);
    create_dirs (no);
    keep_hostname (yes);
};
```

Fontes de mensagens

Sintaxe

```
source <nomefonte> {
    driverfonte(parametros);
    driverfonte(parametros);
    ...  ;
};
```

Fontes de mensagens

- internal
- file <ficheiro>
- unix-dgram <ficheiro>
- unix-stream <ficheiro>
- udp <ip>,<porto>
- tcp <ip>,<porto>

Fontes de mensagens - exemplos

Exemplo - Sistema Linux

```
source s_sistema {
    file ("/proc/kmsg" log_prefix("kernel: "));
    unix-stream ("/dev/log");
    internal();
};
```

Exemplo - Rede

```
source s_rede {
    udp(ip(0.0.0.0) port(514));
};
```

Destinos de mensagens

Sintaxe

```
destination <nomedestino> {
    driverdestino(parametros);
    driverdestino(parametros);
    ...  ;
};
```

Destinos

- file <ficheiro>
- fifo, pipe <ficheiro>
- unix-dgram <ficheiro>
- unix-stream <ficheiro>
- udp <ip>,<porto>
- tcp <ip>,<porto>

Destinos de mensagens - exemplos

Exemplos de alguns destinos típicos

```
destination d_consola { file("/dev/console"); };
destination d_mensagens { file("/var/log/messages"); };
destination d_terminais { usertty("*"); };
```

Exemplo de um destino gerado com base em variáveis

```
destination d_servidores {
    file("/var/log/servidores/$YEAR$MONTH/$HOST"
        create_dirs(yes)
        owner(root) group(root) perm(0600)
        dir_owner(root) dir_group(root) dir_perm(0755)
    );
};
```

Destinos de mensagens - mais exemplos

Exemplo - personalizando formato das mensagens

```
destination d_logfile {
    file("/var/log/logfile"
        template("$YEAR-$MONTH-$DAY $HOUR:$MIN:$SEC $TZ
                  $HOST [$FACILITY:$LEVEL] $MSG\n")
        template_escape(no)
    );
};
```

Destinos de mensagens - mais exemplos

Exemplo - servidores remotos

```
destination d_logsrv1 { udp(192.168.1.1); };

destination d_logsrv2 { udp(192.168.1.2 port(514)); };

destination d_logsrv3 { tcp(192.168.1.3); };

destination d_logsrv4 { tcp(192.168.1.4 port(10514)); };
```

Filters

Sintaxe

```
filter <nomefiltro> {
    expressao;
};
```

Filtros

- facility
- level
- host
- program
- match
- filter
- netmask

Filtros - exemplos

Exemplo de alguns filtros

```
filter f_filtro1   { facility(kern); };

filter f_filtro2   { level(emerg); };

filter f_filtro3   {
    level(info..emerg) and
    not facility(mail,authpriv,cron);
};
```

Regras de logging

Sintaxe

```
log {
    source(s1); source(s2); ...
    filter(f1); filter(f2); ...
    destination(d1); destination(d2); ...
    flags(flag1[, flag2 ...]);
};
```

Flags

- final
- fallback
- catchall

Regras - exemplos

Exemplos de regras de logging

```
log {
    source(s_sistema);
    filter(f_filtro3);
    destination(d_mensagens);
};

log {
    source(s_sys);
    destination(d_logsrv1);
};
```

Introdução

Subsistema de logs em Windows NT

- Ficheiros binários
- Front-end gráfico - Event Viewer

Daemons Syslog

Daemons Syslog para plataformas Windows

- Kiwi
  - http://www.kiwisyslog.com/products.htm
- 3Com
  - http://support.3com.com/software/utilities_for_windows_32_bit.htm
- LogLady
  - http://www.kaska.demon.co.uk/loglady.htm
- sl4nt
  - http://www.netal.com/sl4nt.htm
- WinSyslog - Enhanced Syslog Server
  - http://www.winsyslog.com/en/

Eventlog to syslog forwarders

Forwarders

- EventReporter - NT Event Monitoring & Forwarding
  - http://www.eventreporter.com/en/
- evtsys - Eventlog to Syslog Utility
  - https://engineering.purdue.edu/ECN/Resources/Documents/UNIX/evtsys/
- ntsyslog - Windows NT/2000/XP syslog service
  - http://ntsyslog.sourceforge.net/
- Snare Agent for Windows
  - http://www.intersectalliance.com/projects/SnareWindows/

Utilitários

Utilitários

- Microsoft logevent (Windows 2000, XP (??))
  - `http://support.microsoft.com/default.aspx?scid=kb;en-us;315410&sd=tech`
- Microsoft eventcreate (Windows 2003)
  - `http://support.microsoft.com/default.aspx?scid=kb;en-us;315410&sd=tech`
- logger - An UNIX-like logger for Windows
  - `http://www.monitorware.com/en/logger/`
- Kiwi Logger
  - `http://www.kiwisyslog.com/products.htm`

Módulos Perl

- Win32::EventLog - Interface to Win32 EventLog functions
  - `http://search.cpan.org/dist/libwin32/`

Conteúdo

3 Utilitários

4 Rotação de logs

5 Análise de logs
- logwatch - system log analyzer and reporter
- swatch - the simple watcher of logfiles
- sec - simple event correlator

Introdução

Envio de mensagens para *daemons* Syslog

- **logger**
  - interface de linha de comando
  - permite enviar mensagens para o subsistema de logging a partir de scripts shell

logger

Sintaxe

```
logger [opções] [mensagem ...]
```

Algumas opções

-i - Inclui o pid do processo

-p pri - Envia mensagem com a prioridade especificada. Valor por omissão: **user.notice**

-t tag - Inclui em cada mensagem a etiqueta `tag`

Exemplo

```
$ logger -p local0.notice -t TESTE 'texto da mensagem'
```

Módulos Perl

Módulos de Perl

- **Sys::Syslog**
  - Interface Perl da API syslog
  - Módulo distribuido com o interpretador Perl
- **Unix::Syslog**
  - Interface Perl da API syslog
- **Net::Dev::Tools::Syslog**
  - Send, Listen Syslog messages, Parse syslog files
- **Net::Syslog**
  - Perl extension for sending syslog messages directly to a remote syslogd

Módulos Perl

Módulos de Perl

- **Log::Dispatch**
  - Permite entregar mensagens num ou mais destinos
- **Log::Log4perl**
  - Excelente API de logging baseada em Log4j (Java)

Perl: módulo Sys::Syslog

Interface

```
use Sys::Syslog;
use Sys::Syslog qw(:DEFAULT setlogsock);

setlogsock $sock_type;

openlog $ident, $logopt, $facility;
syslog $priority, $format, @args;
$oldmask = setlogmask $mask_priority;
closelog;
```

Exemplo de utilização Sys::Syslog

Exemplo

```
1  #!/usr/bin/perl -w
2  use strict;
3
4  use Sys::Syslog qw(:DEFAULT setlogsock);
5
6  my $program = $0;
7  my $options = 'pid|ndelay';
8  my $facility = 'user';
9  my $priority = 'info';
10
11 setlogsock('unix');
12 openlog($program, $options, $facility);
13 syslog($priority, 'Teste OK');
14 closelog();
```

Conteúdo

3 Utilitários

4 Rotação de logs

5 Análise de logs
- logwatch - system log analyzer and reporter
- swatch - the simple watcher of logfiles
- sec - simple event correlator

Introdução

Rotação de logs

- **logrotate** (Red Hat/Fedora)
  - rotates, compresses, and mails system logs

Conteúdo

3 Utilitários

4 Rotação de logs

5 Análise de logs
- logwatch - system log analyzer and reporter
- swatch - the simple watcher of logfiles
- sec - simple event correlator

Introdução

Análise de logs

Ferramentas que permitam gerar relatórios/alertas com base no conteúdo de ficheiros de logs.

logwatch - system log analyzer and reporter

logwatch

- Logwatch is a customizable log analysis system. Logwatch parses through your system's logs for a given period of time and creates a report analyzing areas that you specify, in as much detail as you require. Logwatch is easy to use and will work right out of the package on most systems.

Homepage

`http://www.logwatch.org/`

swatch - the simple watcher of logfiles

swatch

- SWATCH: The Simple WATCHer of Logfiles
- The Simple WATCHer is an automated monitoring tool that is capable of alerting system administrators of anything that matches the patterns described in the configuration file, whilst constantly searching logfiles using perl.

Homepage

`http://swatch.sourceforge.net/`

sec - free and platform independent event correlation tool

sec

SEC is a simple event correlation tool that reads lines from files, named pipes, or standard input, and matches the lines with regular expressions, Perl subroutines, and other patterns for recognizing input events. Events are then correlated according to the rules in configuration files, producing output events by executing user-specified shell commands, by writing messages to pipes or files, etc.

Referências

- Homepage
  `http://www.estpak.ee/~risto/sec/`
- Working with SEC - the Simple Event Correlator
  `http://sixshooter.v6.thrupoint.net/SEC-examples/article.html`

  `http://sixshooter.v6.thrupoint.net/SEC-examples/article-part2.html`

Conteúdo

6 Referências

Referências

Referências

- **LogAnalysis website**
  `http://www.loganalysis.org/`
- **Linux Server Security *(2nd edition)***
  Michael D. Bauer
  `http://www.oreilly.com/catalog/linuxss2/`
  - Capítulo 12 - System Log Management and Monitoring (disponível *online* em formato PDF)
- **Practical UNIX and Internet Security *(3rd edition)***
  Simson Garfinkel, Gene Spafford, Alan Schwartz
  `http://www.oreilly.com/catalog/puis3/`
  - Capítulo 21 - Auditing, Logging, and Forensics