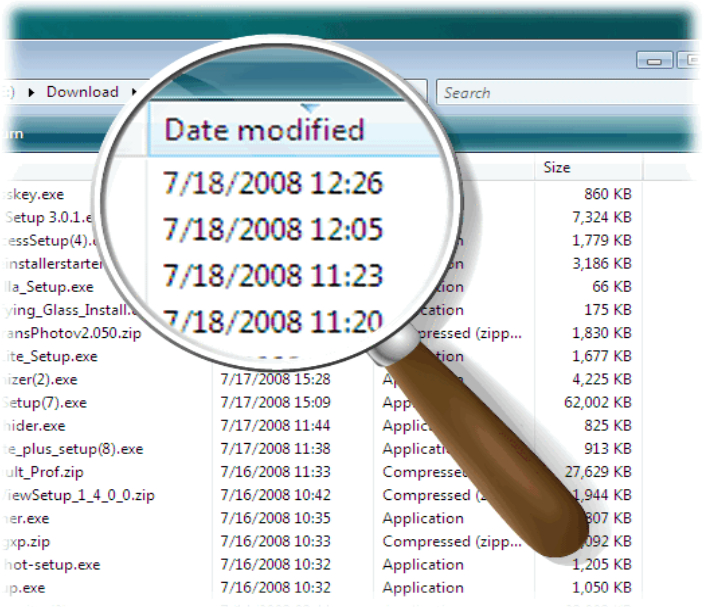
Gestión de Logs



Carlos Vicente
Servicios de Red
Universidad de Oregon

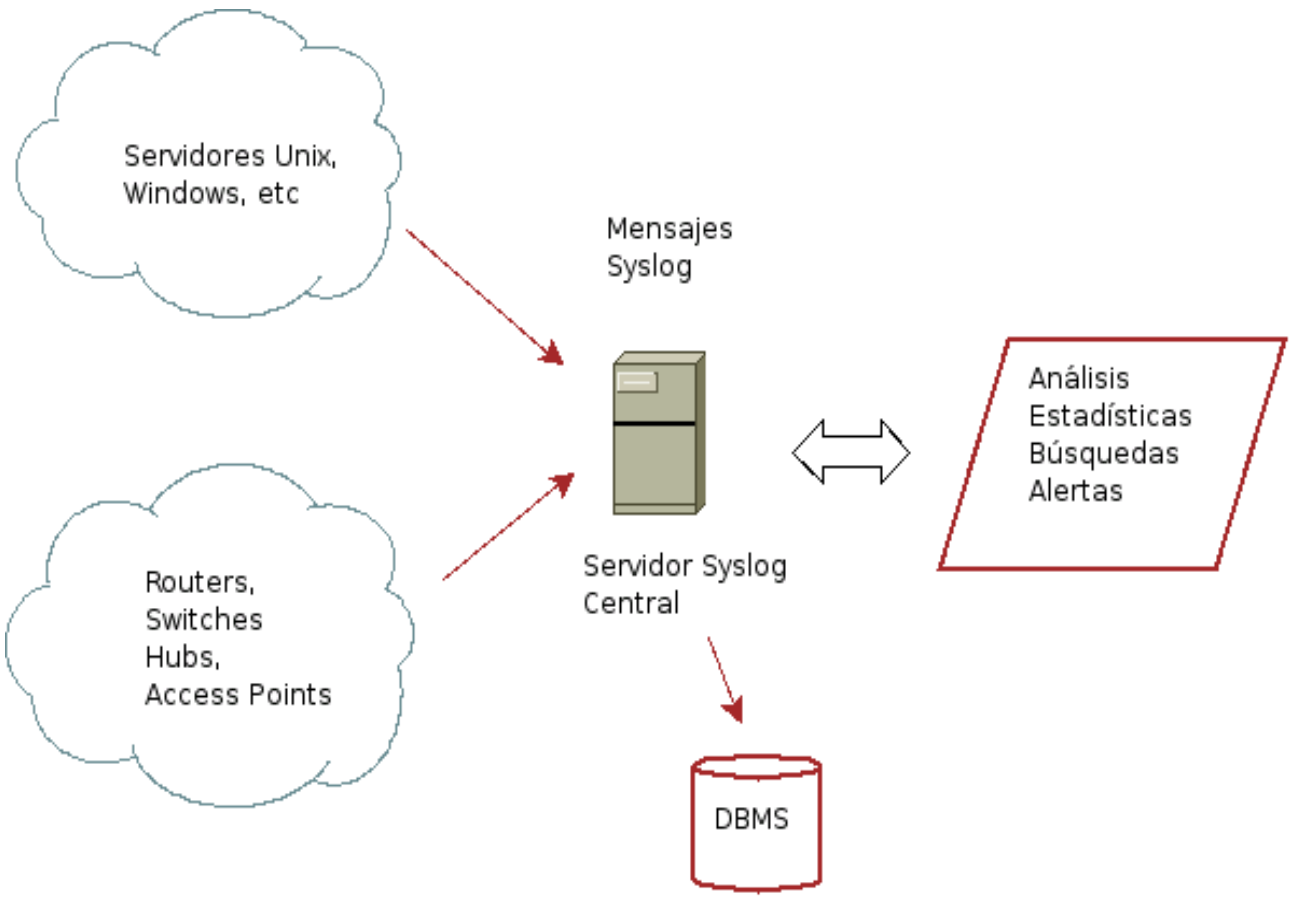
Contenido

- Introducción
- syslog
- syslog-ng
- php-syslogng
- tenshi

Introducción

- Los *logs* son la principal fuente de información acerca de la actividad de la red y los sistemas
- Esenciales para:
  - Detección de ataques e intrusos
  - Detección de problemas de hardware/software
  - Análisis forense de sistemas
- La clave de la monitorización pasiva es la centralización de los mensajes

Servidor Log Central



Syslog

- Syslog provee un servicio estándar y distribuido de mensajes
- Por qué estándar:
  - Una interfaz API para aplicaciones (y el sistema operativo)
  - Define niveles de severidad y agrupaciones de mensajes por tipo
- Por qué distribuido
  - Cliente/Servidor
  - Local o remoto

Niveles Syslog

```
LOG_EMERG      Sistema en estado inútil
LOG_ALERT      Se requiere acción inmediata
LOG_CRIT       Condiciones críticas
LOG_ERR        Condiciones de Error
LOG_WARNING    Condiciones de precaución
LOG_NOTICE     Condición normal, pero significativa
LOG_INFO       Mensaje informativo
LOG_DEBUG      Mensaje de depuración
```

Grupos Syslog (Facilities)

```
LOG_AUTH              Mensajes de seguridad/autenticación (descontinuado)
LOG_AUTHPRIV          Mensajes de seguridad/autenticación (privado)
LOG_CRON              Servicio CRON
LOG_DAEMON            Daemons del sistema
LOG_FTP               Daemon FTP
LOG_KERN              Mensajes del Kernel
LOG_LOCAL[0-7]       Reservados para uso local
LOG_LPR               Sub-sistema de impresión
LOG_MAIL              Sub-sistema de correo
LOG_NEWS              Sub-sistema de noticias USENET
LOG_SYSLOG            Mensajes generados internamente por Syslogd
LOG_USER (default)   Mensajes de nivel de usuario genéricos
LOG_UUCP              Sub-sistema UUCP
```

Configuración de cliente syslog

- /etc/syslog.conf
  - <facility>.<nivel>[,...] <path/to/logfile>|<@remote server>
  - Comodines:
    - * = todos
    - none = ninguno

```
*.info,mail.none                    /var/log/messages
mail.*                              /var/log/maillog
*.*                                 @192.168.0.10
```

syslog-ng

- ng = *nueva generación*
- Tiene varias ventajas sobre el syslog tradicional
  - Transporte UDP y TCP
  - Filtrado basado en el contenido de los mensajes
  - Soporte para cifrado
  - Puede ejecutarse bajo un entorno *chroot*
- Usar syslog-ng en el servidor central

Configuración syslog-ng

- /etc/syslog-ng.conf
- Consta de
  - Opciones globales
  - Fuentes (Sources)
  - Destinos (Destinations)
  - Filtros (Filters)
- Fuentes, Filtros y Destinos se conectan con comandos 'log'

Opciones globales en syslog-ng

```
options {
    create_dirs (yes);       # Crear subdirectorios
    dir_perm(0755);          # Permisos para los directorios creados
    use_dns(yes);
    dns_cache(yes);          # Hacer caching de DNS
    keep_hostname(yes);      # Usar el nombre de host en el mensaje
    use_fqdn(yes);           # Usar nombre DNS completo
    perm(0644);              # Permisos para los archivos creados
    sync(0);                 # Número de líneas en búfer antes de escribir
};
```

Fuentes en syslog-ng

- Determinan de dónde se sacan los mensajes.
  - Los métodos de obtención se llaman *Sourcedrivers:*
    - file, unix-dgram, unix-stream, udp, tcp

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

Destinos en syslog-ng

- Determinan dónde se van a enviar los mensajes
  - Los mismos métodos que en la fuente + usertty

```
destination allbyhostfile { file("/log/hosts/$HOST/$FACILITY.$PRIORITY"
        owner(root) group(root) perm(0644) dir_perm(0755) create_dirs(yes));
};

destination ciscofile { file("/log/cisco"
        owner(root) group(root) perm(0644) dir_perm(0755) create_dirs(yes));
};
```

Filtros en syslog-ng

- Sirven para clasificar los mensajes basados en su contenido. Aceptan operadores booleanos (AND, OR, NOT) y las siguientes funciones:
  - facility, level, program, host, match

```
filter ciscofilter { facility(local3) and not host(server1); };
```

Configuración syslog-ng

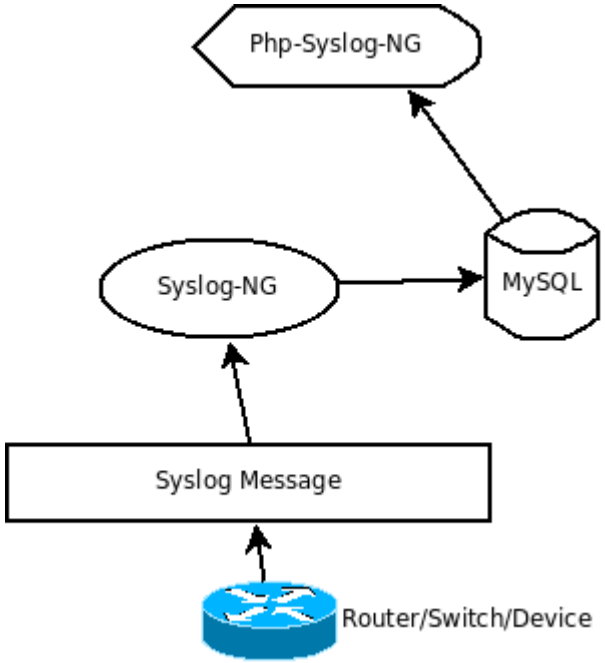
- El comando log combina los elementos descritos anteriormente para generar una acción

```
log {source(s_udp); filter(ciscofilter); destination(ciscofile); flags(final); };
```

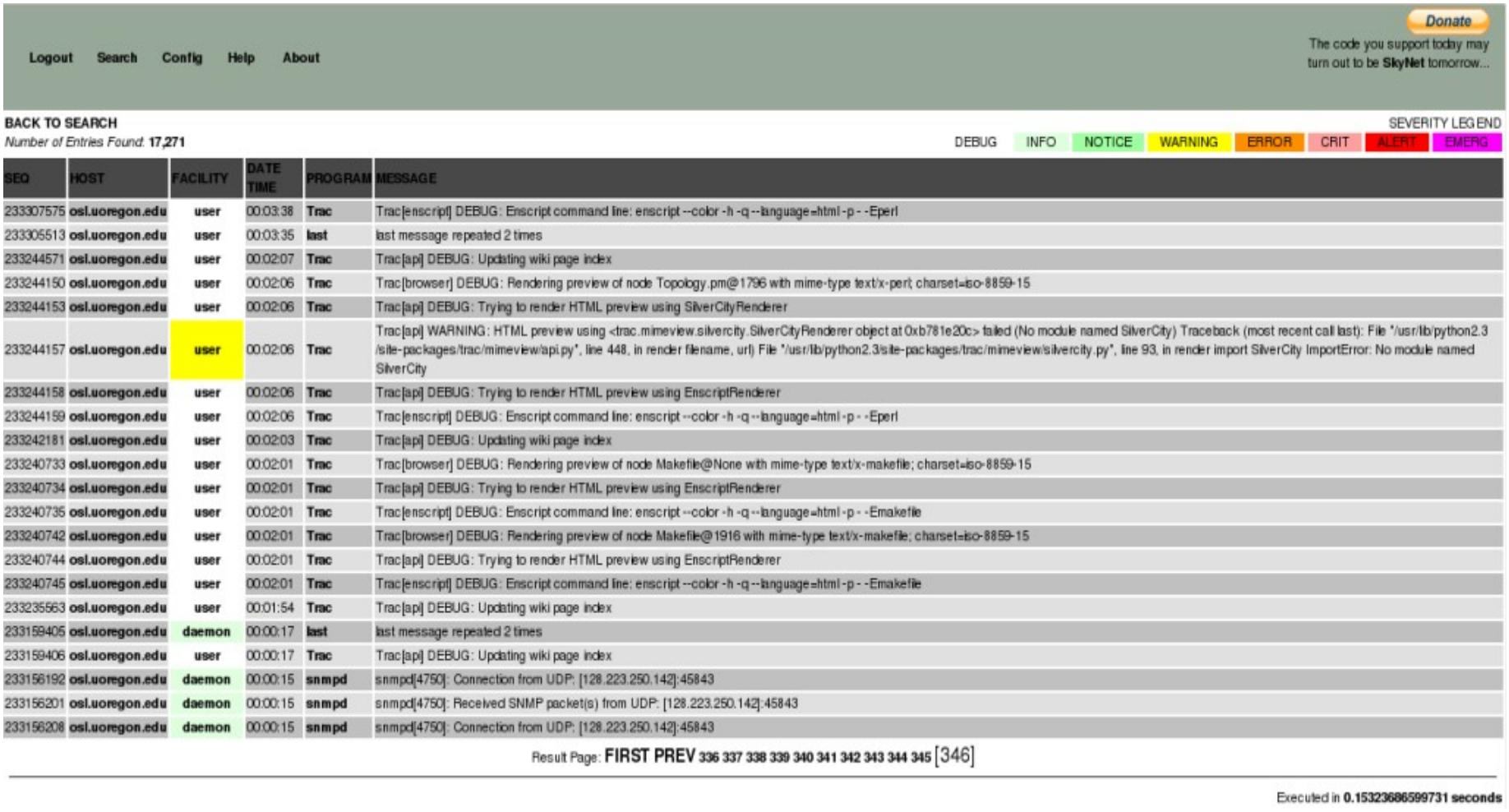
MySQL y php-syslog-ng

- Una herramienta muy útil para un servidor central de syslog-ng
  - Inserta cada mensaje en una simple tabla MySQL
  - Permite hacer búsquedas basadas en diversos criterios
    - Nodo de origen
    - Rango de tiempo
    - Prioridad
  - Interfaz web

php-syslog-ng



php-syslog-ng



Logout Search Config Help About

Donate

The code you support today may turn out to be **SkyNet** tomorrow...

BACK TO SEARCH

Number of Entries Found: **17,271**

SEVERITY LEGEND: DEBUG INFO NOTICE WARNING ERROR CRIT ALERT EMERG

SEQ	HOST	FACILITY	DATE TIME	PROGRAM	MESSAGE
233307575	osl.uoregon.edu	user	00:03:38	Trac	Trac[enscript] DEBUG: Enscript command line: enscript --color -h -q --language=html -p - --Eperl
233305513	osl.uoregon.edu	user	00:03:35	last	last message repeated 2 times
233244571	osl.uoregon.edu	user	00:02:07	Trac	Trac[api] DEBUG: Updating wiki page index
233244150	osl.uoregon.edu	user	00:02:06	Trac	Trac[browser] DEBUG: Rendering preview of node Topology.pm@1796 with mime-type text/x-perl; charset=iso-8859-15
233244153	osl.uoregon.edu	user	00:02:06	Trac	Trac[api] DEBUG: Trying to render HTML preview using SilverCityRenderer
233244157	osl.uoregon.edu	user	00:02:06	Trac	Trac[api] WARNING: HTML preview using <trac.mimeview.silvercity.SilverCityRenderer object at 0xb781e20c> failed (No module named SilverCity) Traceback (most recent call last): File "/usr/lib/python2.3/site-packages/trac/mimeview/api.py", line 448, in render filename, url) File "/usr/lib/python2.3/site-packages/trac/mimeview/silvercity.py", line 93, in render import SilverCity ImportError: No module named SilverCity
233244158	osl.uoregon.edu	user	00:02:06	Trac	Trac[api] DEBUG: Trying to render HTML preview using EnscriptRenderer
233244159	osl.uoregon.edu	user	00:02:06	Trac	Trac[enscript] DEBUG: Enscript command line: enscript --color -h -q --language=html -p - --Eperl
233242181	osl.uoregon.edu	user	00:02:03	Trac	Trac[api] DEBUG: Updating wiki page index
233240733	osl.uoregon.edu	user	00:02:01	Trac	Trac[browser] DEBUG: Rendering preview of node Makefile@None with mime-type text/x-makefile; charset=iso-8859-15
233240734	osl.uoregon.edu	user	00:02:01	Trac	Trac[api] DEBUG: Trying to render HTML preview using EnscriptRenderer
233240735	osl.uoregon.edu	user	00:02:01	Trac	Trac[enscript] DEBUG: Enscript command line: enscript --color -h -q --language=html -p - --Emakefile
233240742	osl.uoregon.edu	user	00:02:01	Trac	Trac[browser] DEBUG: Rendering preview of node Makefile@1916 with mime-type text/x-makefile; charset=iso-8859-15
233240744	osl.uoregon.edu	user	00:02:01	Trac	Trac[api] DEBUG: Trying to render HTML preview using EnscriptRenderer
233240745	osl.uoregon.edu	user	00:02:01	Trac	Trac[enscript] DEBUG: Enscript command line: enscript --color -h -q --language=html -p - --Emakefile
233235563	osl.uoregon.edu	user	00:01:54	Trac	Trac[api] DEBUG: Updating wiki page index
233159405	osl.uoregon.edu	daemon	00:00:17	last	last message repeated 2 times
233159406	osl.uoregon.edu	user	00:00:17	Trac	Trac[api] DEBUG: Updating wiki page index
233156192	osl.uoregon.edu	daemon	00:00:15	snmpd	snmpd[4750]: Connection from UDP: [128.223.250.142]:45843
233156201	osl.uoregon.edu	daemon	00:00:15	snmpd	snmpd[4750]: Received SNMP packet(s) from UDP: [128.223.250.142]:45843
233156208	osl.uoregon.edu	daemon	00:00:15	snmpd	snmpd[4750]: Connection from UDP: [128.223.250.142]:45843

Result Page: **FIRST PREV** 336 337 338 339 340 341 342 343 344 345 [346]

Executed in **0.15323686599731 seconds**

tenshi

- Monitor de archivos de log simple y flexible
- Los mensajes son clasificados en colas, utilizando expresiones regulares
- Cada cola puede configurarse con e-mail de destino y horario de notificación

configuración de tenshi

```
set uid tenshi
set gid tenshi

set logfile /log/dhcp

set sleep 5
set limit 800
set pager_limit 2
set mask ___
set mailserver localhost
set subject tenshi report
set hidepid on

set queue dhcpd tenshi@localhost sysadmin@noc.localdomain [*/10 * * * *]

group ^dhcpd:
dhcpd ^dhcpd: .+no free leases
dhcpd ^dhcpd: .+wrong network
group_end
```

Ejercicio Tenshi

- Configurar Tenshi para enviar un reporte cada 5 minutos de los intentos fallidos de login de *root*
  - Pista:
    - Observar /var/log/auth.log
    - Intentar logins de *root* con passwords inválidos

Consideraciones de Seguridad

- Restringir el tráfico syslog en el servidor central
  - Sólo permitir que sus equipos envíen logs
  - Por ejemplo, usar iptables:

```
# iptables -A INPUT -s 192.168.1.0/24 -p udp --dport 514 -j ACCEPT
# iptables -A INPUT -s 0/0 -p udp --dport 514 -j REJECT
```

Enlaces

- php-syslog-ng: http://code.google.com/p/php-syslog-ng/
- Splunk: http://www.splunk.com
- Tenshi: http://dev.inversepath.com/trac/tenshi
- Security Event Correlator: http://www.estpak.ee/~risto/sec
- Swatch: http://swatch.sourceforge.net/