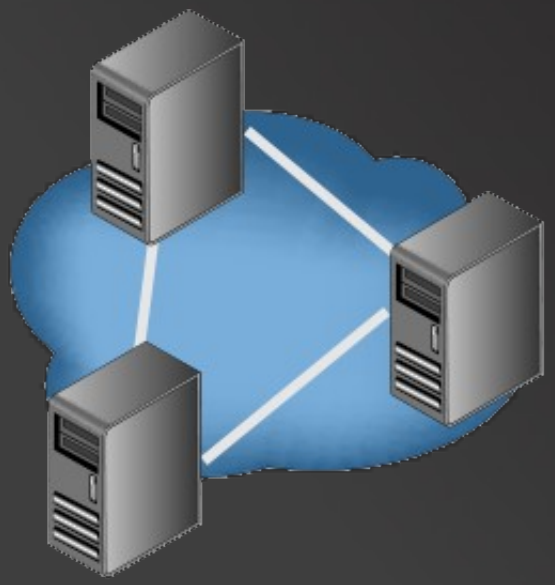
Linux Week 2008

Administración centralizada de logs en una red de servidores



Ing. Arturo Díaz Rosemberg

¿Qué?

- ¿Qué es un log?
  - Un log es un registro de un evento que es generado por algun proceso.
- ¿Para qué sirven?
  - Descubrir utilización y actividades en los equipos.
  - Obtener métricas de uso y tendencias.
  - Encontrar el origen de algun error o ataque.

¿Dónde?

- En el caso de un Linux se encuentran usualmente en el directorio /var/log

```
[arturodr@cefiro ~]$ ls /var/log/
acpid             cron.2     maillog.3   rpmpkgs.3          spooler.3
anaconda.log      cron.3     maillog.4   rpmpkgs.4          spooler.4
anaconda.syslog   cron.4     messages    samba              squid
anaconda.xlog     cups       messages.1  scrollkeeper.log   tallylog
audit             dmesg      messages.2  secure             vbox
boot.log          faillog    messages.3  secure.1           wtmp
boot.log.1        gdm        messages.4  secure.2           wtmp.1
boot.log.2        httpd      mysqld.log  secure.3           xferlog
boot.log.3        iperf      news        secure.4           Xorg.0.log
boot.log.4        iptraf     pm          setroubleshoot     Xorg.0.log.old
btmp              lastlog    ppp         snmpd.log          yum.log
conman            mail       prelink     snmpd.log.1        yum.log.1
conman.old        maillog    rpmpkgs     spooler
cron              maillog.1  rpmpkgs.1   spooler.1
cron.1            maillog.2  rpmpkgs.2   spooler.2
```

¿Cómo?

- Archivo o grupos de archivos
  - Por ejemplo:

```
-rw------- 1 root root 5.7K Mar 11 04:02 /var/log/maillog
-rw------- 1 root root  17K Mar  9 04:02 /var/log/maillog.1
-rw------- 1 root root  16K Mar  2 04:02 /var/log/maillog.2
-rw------- 1 root root 6.3K Feb 24 04:02 /var/log/maillog.3
-rw------- 1 root root 6.6K Feb 17 04:02 /var/log/maillog.4
```

Tipos de logs

- Facility

Numerical Code	Facility
0	kernel messages
1	user-level messages
2	mail system
3	system daemons
4	security/authorization messages (note 1)
5	messages generated internally by syslogd
6	line printer subsystem
7	network news subsystem
8	UUCP subsystem
9	clock daemon (note 2)
10	security/authorization messages (note 1)
11	FTP daemon
12	NTP subsystem
13	log audit (note 1)
14	log alert (note 1)
15	clock daemon (note 2)
16	local use 0 (local0)
17	local use 1 (local1)
18	local use 2 (local2)
19	local use 3 (local3)
20	local use 4 (local4)
21	local use 5 (local5)
22	local use 6 (local6)
23	local use 7 (local7)

Table 1. syslog Message Facilities

- Severity

Numerical Code	Severity
0	Emergency: system is unusable
1	Alert: action must be taken immediately
2	Critical: critical conditions
3	Error: error conditions
4	Warning: warning conditions
5	Notice: normal but significant condition
6	Informational: informational messages
7	Debug: debug-level messages

Table 2. syslog Message Severities

RFC3164

Algunos Problemas

- Los log guardan información importante, pero...
  - ¿Quién se encarga de la revision?
  - ¿Cada cuanto tiempo?

  - ¿Cuantos equipos?

Revisando logs de forma “tradicional”

- Revisando periodicamente los archivos
  - Por ejemplo:

```
$ less /var/log/messages
```

  - “En linea”

```
$ tail -f /var/log/messages
```

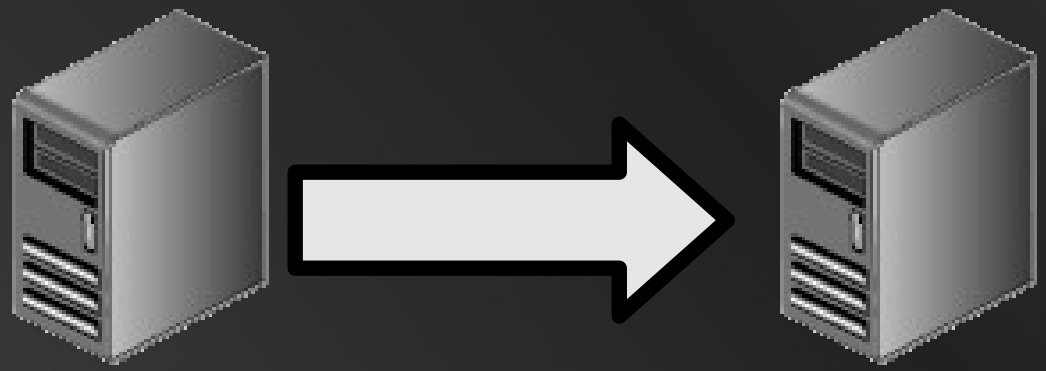
X nro de logs a revisar
X nro de equipos

Consolidación y correlación

- Consolidación:
  - Reunir los mensajes de los eventos de distintos dispositivos en un único punto.
- Correlación:
  - Relacionar logs de distintos dispositivos en busca del origen de un evento.

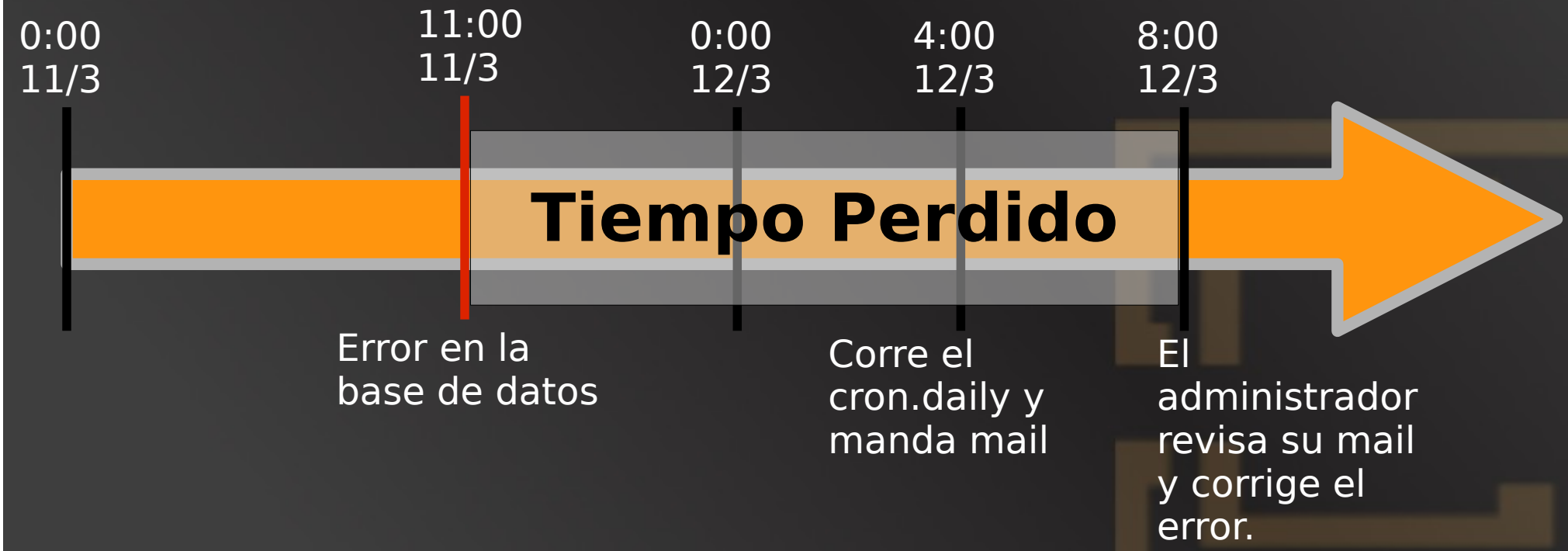
Centralizando logs

- El syslog permite exportar log a otro equipo mediante mensajes **UDP**



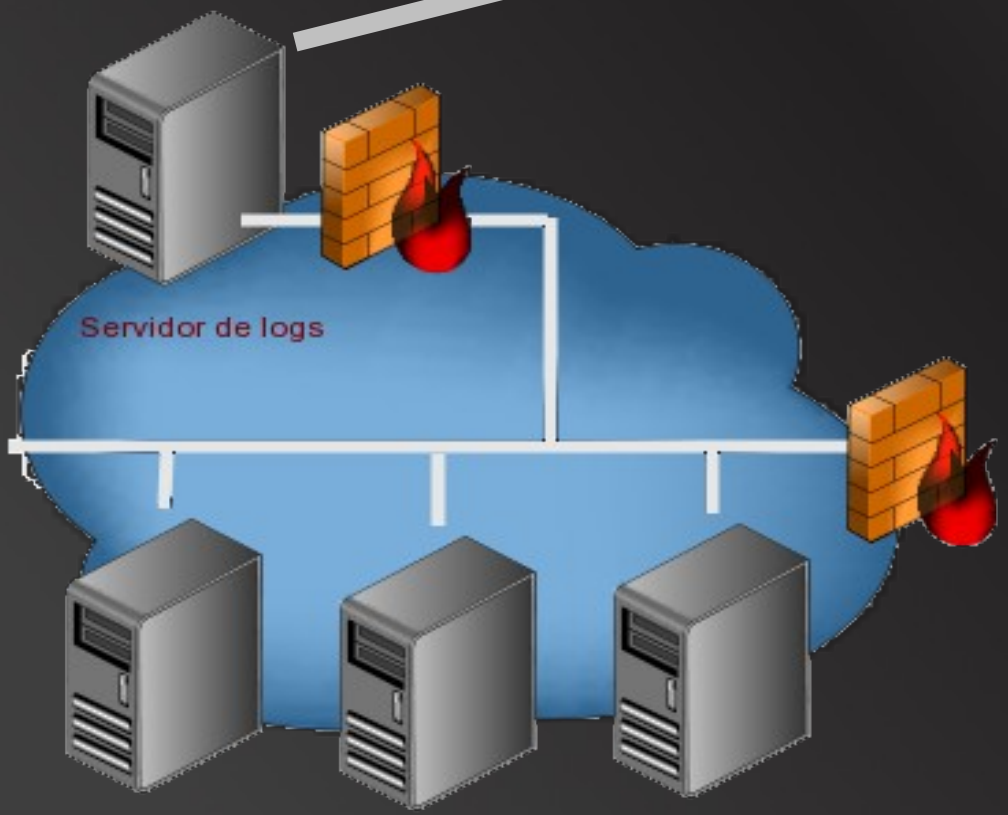
LogWatch

- Herramienta incluida por defecto en la mayoria de distribuciones.
- Con la configuracion basica corre una vez al dia y no revisa todos los logs.

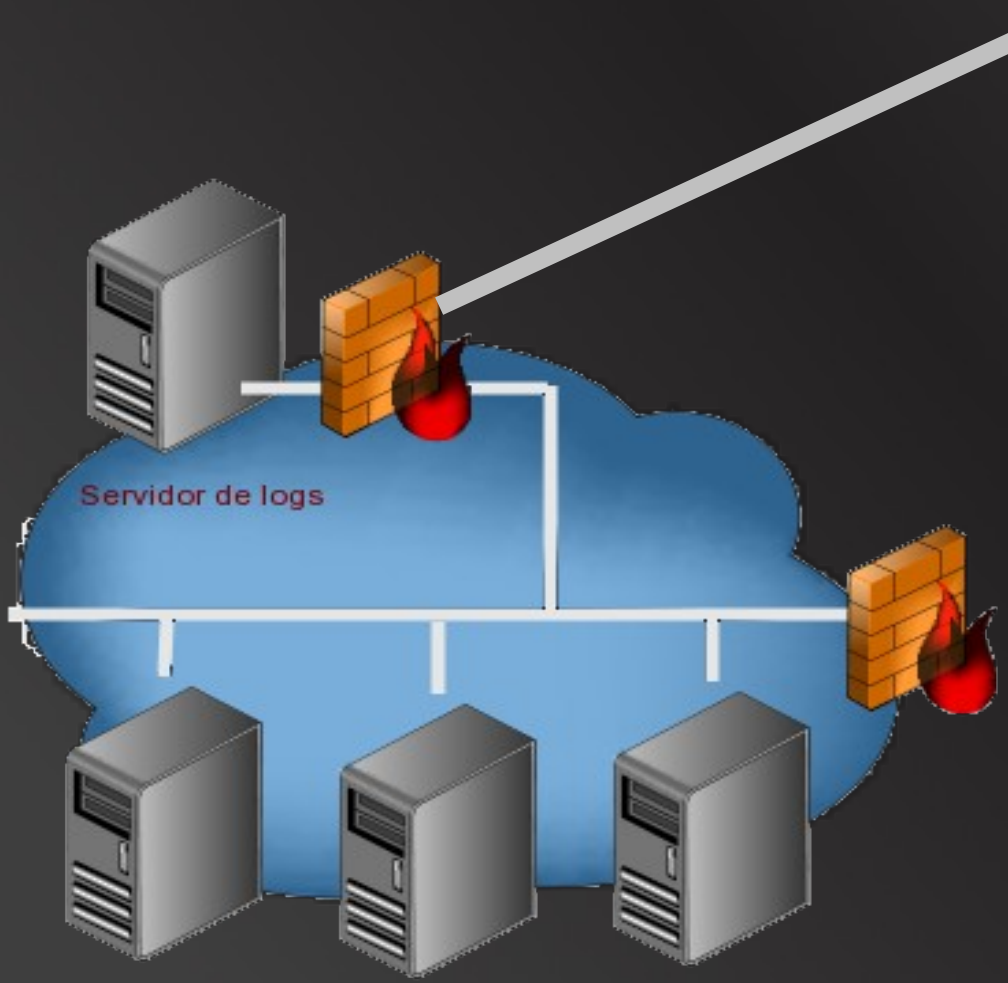


Solucion propuesta

- Utilizar un servidor dedicado a almacenar todos los logs de la red.



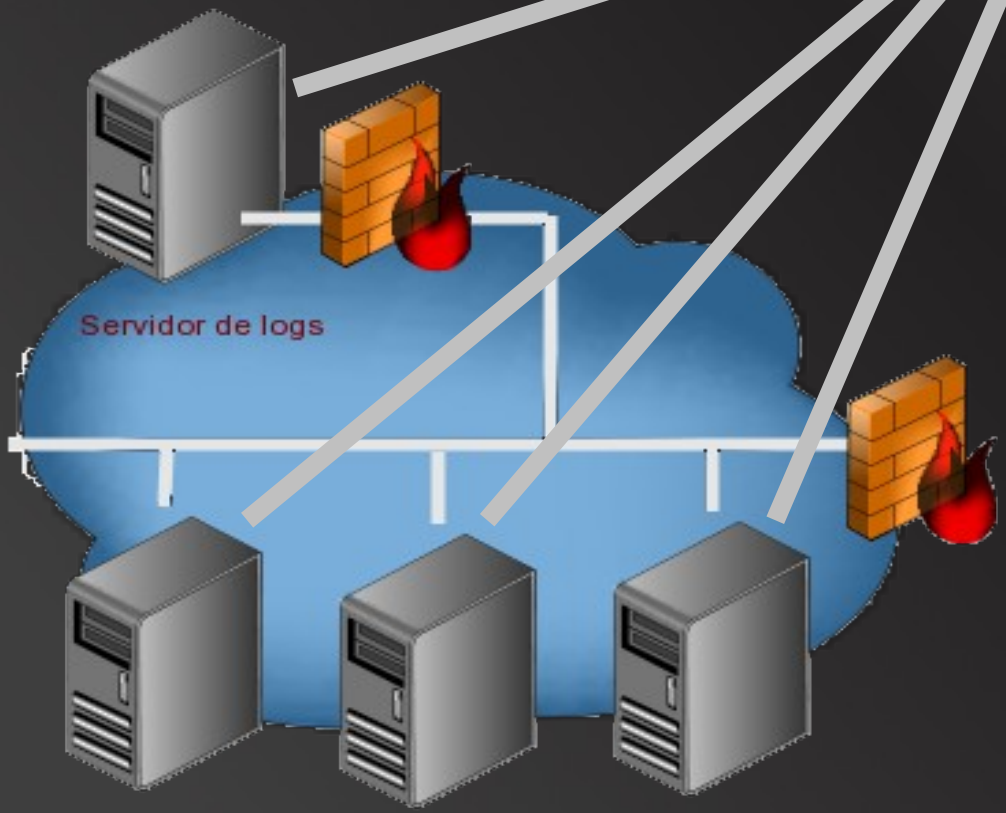
Solucion propuesta



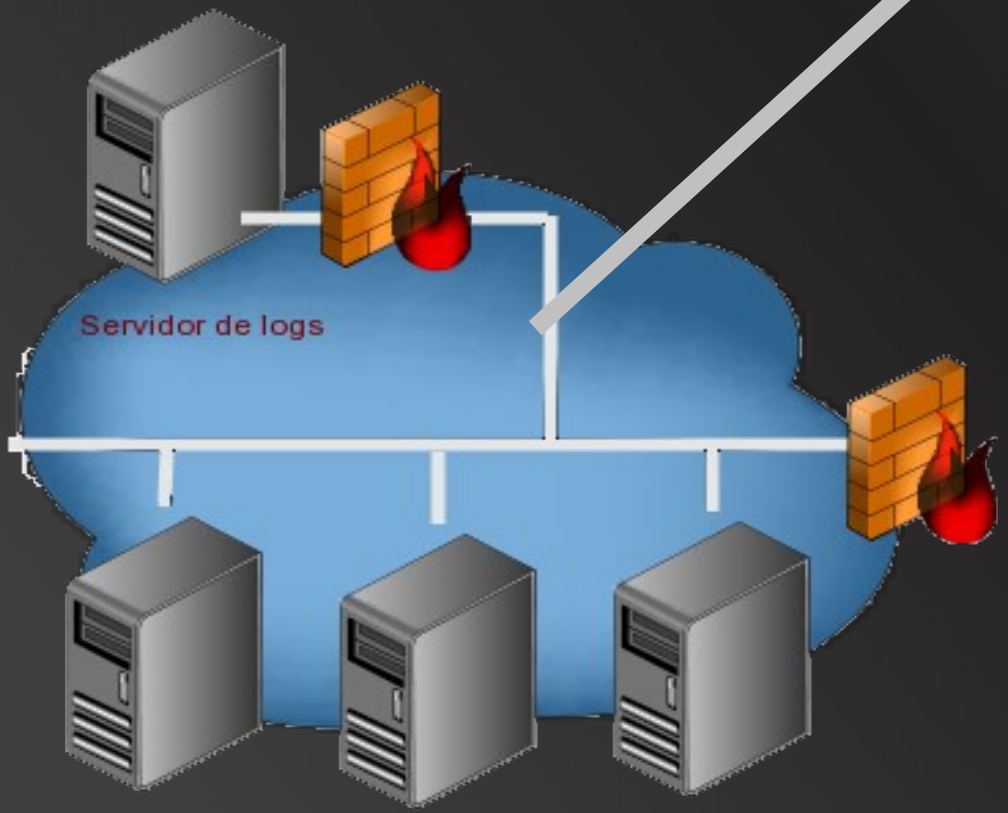
- Para mayor seguridad este equipo debe estar protegido por un firewall.

Solucion propuesta

- Los equipos deben estar sincronizados.

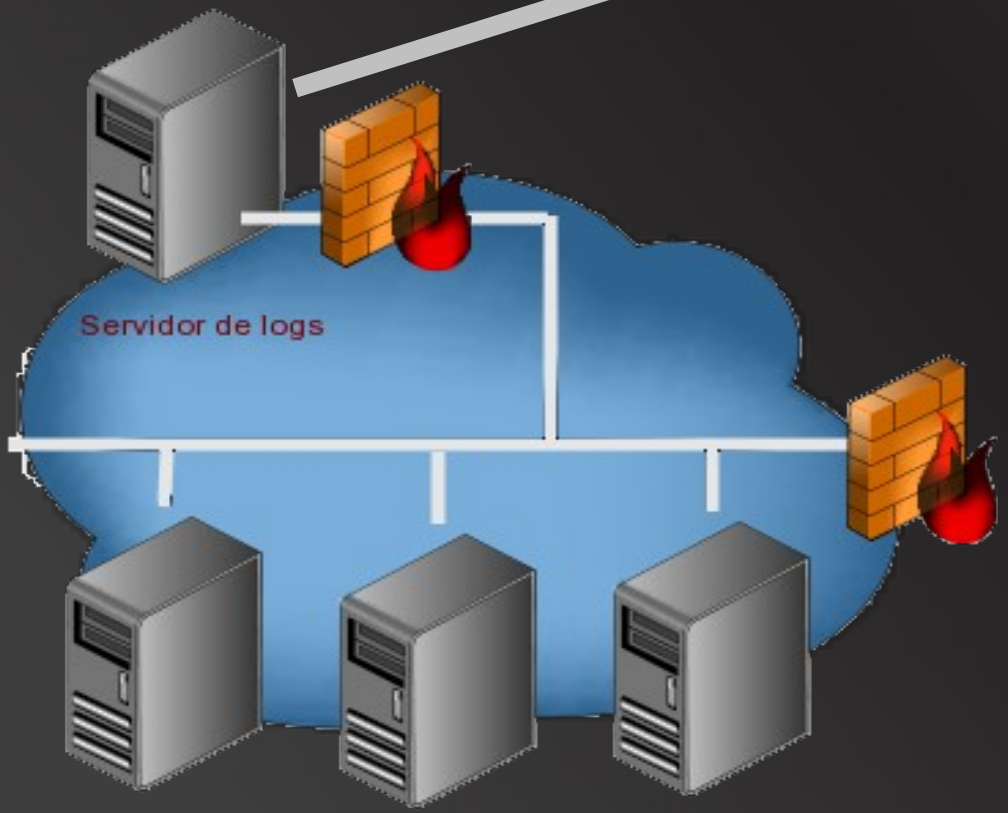


Solucion propuesta



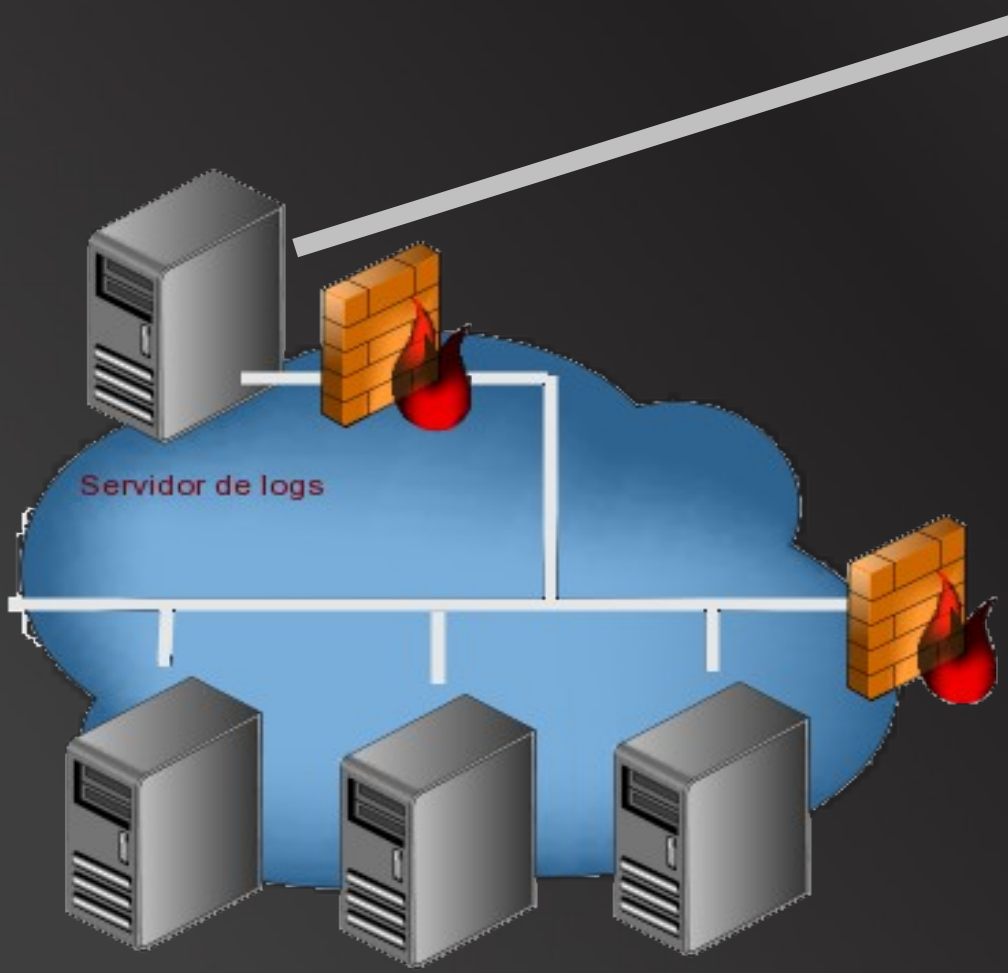
- Se pueden enviar los logs utilizando un tunel de SSH para el transporte.

Solucion propuesta



- Para un manejo mas facil de los log se recomienda almacenarlos en una base de datos

Solucion propuesta



- Se pueden utilizar interfaces web para mostrar los log y que su analisis sea mas sencillo
- Por ejemplo:
  - php-syslog-ng

Cosas a considerar

- No solo equipos con GNU/Linux generan logs
  - Routers, switches, APs..
- Equipos con Windows pueden generar log similares con Ntsyslog.
- Es conveniente decidir que logs se van a almacenar dependiendo del uso de cada equipo.

Referencias

- ”Linux Administration Handbook”, E. nemeth, G. Snyder, T. R. Hein
- RFC3164 - The BSD Syslog Protocol
- Log Consolidation with syslog - Donald Pitt http://www.giac.org/practical/gsec/Donald_Pitts_GSEC.pdf
- Administración centralizada de logs como un método de aproximación a la recolección de evidencia digital y detección temprana de fallos. - Andres Holguin Coral www.acis.org.co/memorias/JornadasSeguridad/IVJNSI/Andres
- Centralización de logs: Una experiencia real - Daniel Sánchez Dorado www.rediris.es/jt/jt2006/archivo/16Jueves/1600-1830/A/

Gracias

Arturo Diaz Rosemberg
adiazr@pucp.edu.pe