Administração de Sistemas I

Ficha de trabalho

5 de Dezembro de 2006

Resumo

Infra-estrutura de *logging* em redes heterogéneas.

1 Introdução

Pretende-se planear, com base no protocolo syslog, a infra-estrutura de logs de uma rede local com sistemas heterogéneos (Linux e Windows). Assuma a existência de várias máquinas Linux, de várias máquinas Windows (família NT) e de um servidor central de logs (Linux).

Serviço de tempo

Assuma a existência de um servidor de NTP contactável a partir da rede local que administra.
1 Indique como configuraria o serviço de tempo nos postos Linux.

2 Indique como configuraria o serviço de tempo nos postos Windows.

Servidor de Logs

Pretende-se que o servidor de logs utilize o *daemon* Syslog-NG.

Syslog-NG

3 Indique como re-escreveria as seguintes regras Syslog em Syslog-NG:

```
*.info;mail.none;authpriv.none;local1.none    /var/log/messages
*.info;mail.none;authpriv.none;local2.none    @192.168.1.100
```

4 Indique como criaria ficheiros de logs específicos para cada uma das máquinas clientes. O nome dos ficheiros a serem criados devem seguir o seguinte modelo - `/var/log/servidores/endereco_ip/ano_mes` - em que "endereço_ip" e "ano_mes" são directórios que contem o endereço IP do cliente e o ano/mês da mensagem de log.

5 Crie novas mensagens de log que incluam a *facility* e a *prioridade* das mensagens.

6 Crie um filtro que permita apenas fazer log de mensagens que contenham uma dada string.

7 Crie um script perl que permita enviar mensagens de teste para cada uma das prioridades de uma dada facility.

8 Crie um script perl que permita realizar testes de carga do servidor de logs a partir de vários postos.

9 Indique alguns métodos que poderia utlizar para melhorar a segurança do servidor: evitar mensagens de logging enviadas a partir de máquinas não autorizadas, ...

Postos Linux

10 Indique que regras precisaria criar para efectuar o log remoto de toda a informação.

Postos Windows

11 Analise e teste vários daemons syslog para Windows. Uma das caracteristicas importantes a analisar é capacidade de filtragem destes daemons.

12 Instale e configure um dos daemons analisados. Indique como procederia para efectuar o envio de mensagens de log das máquinas Windows para o servidor central.

Referências

- Loganalysis.Org
  `http://www.loganalysis.org/`
- Syslog-NG
  `http://www.balabit.com/products/syslog_ng/`