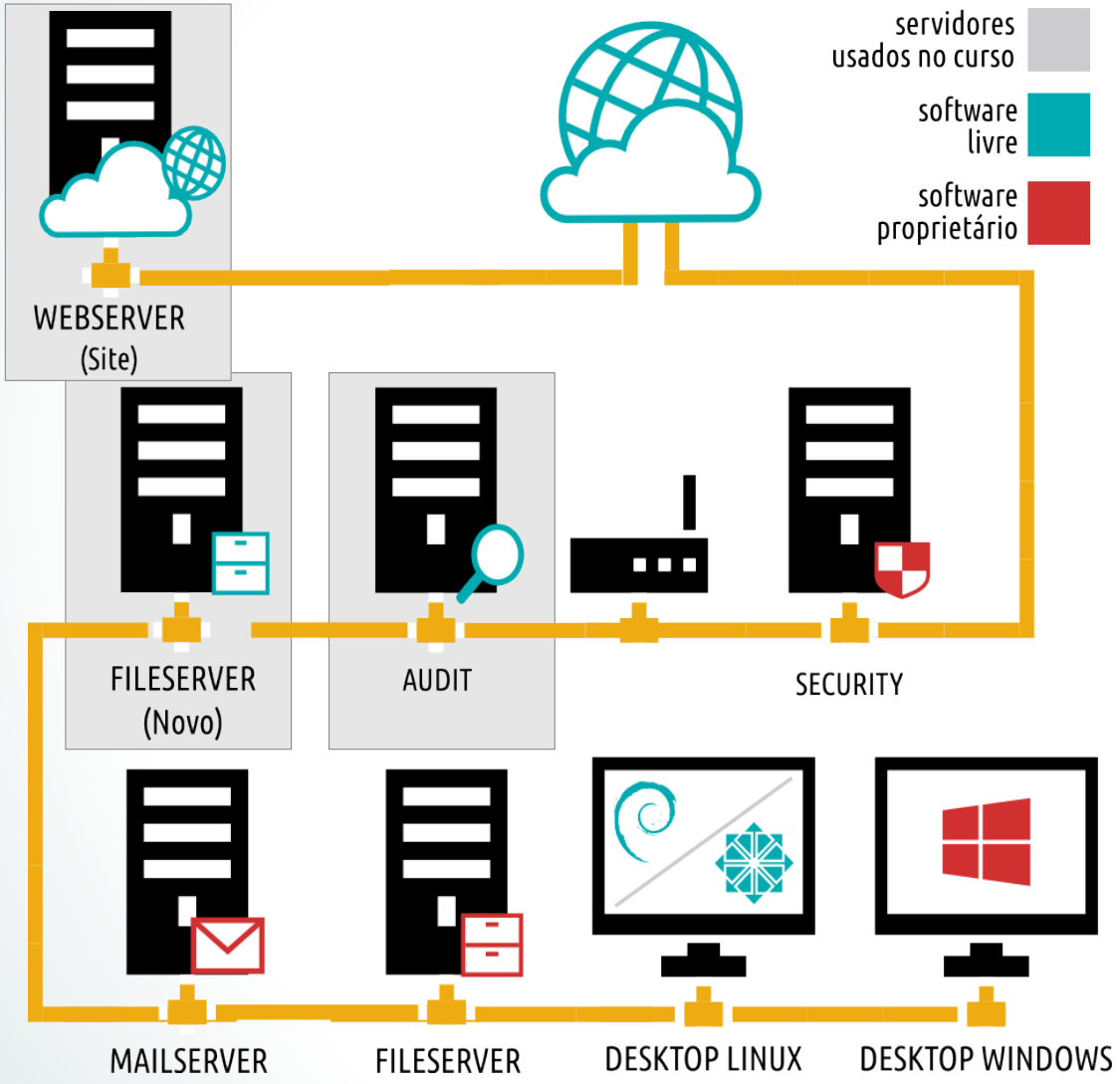

4LINUX
FREE SOFTWARE SOLUTIONS

Só na 4Linux você aprende MUITO MAIS!

Data e Hora do Sistema e Servidor de NTP

IT EXPERIENCE



Nesta Aula:

- Audit – Local

  Acesso pelo VirtualBox

  SO: Debian Linux

Rsyslog

Objetivos:

- Introdução ao Rsyslog;
- Configurar Rsyslog na máquina local;
- Configurar um servidor de Logs;
- Configuração de Logs no cliente;
- Gerenciar rotação de Logs.

Rsyslog

Introdução

- A norma NBR ISO/IEC 27002 recomenda no item 10.10.1 as seguintes características de um sistema de logs:

1. Identificação dos usuários;
2. Datas e horários de entrada e saída de terminais;
3. Hostname ou endereço IP, para serviços acessados via rede;
4. Registro das tentativas de acessos aceitos e rejeitados.

Rsyslog

Configuração do Rsyslog na maquina local

- As configurações do Rsyslog podem ser alteradas através do seguinte arquivo:

```
1# vim /etc/rsyslog.conf
```

Syntax: facilidade.nível destino

Exemplos:

cron.*	/var/log/cron.log
kernel.inf	/var/log/kernel.inf
.	/var/log/all.log

Rsyslog

Facilidades do Rsyslog

- auth
- authpriv
- cron
- daemon
- ftp
- kern
- lpr
- local0-7
- mail
- news
- security
- rsyslog
- user
- uucp

Rsyslog

Níveis do Rsyslog

- emerg
- alert
- crit
- err
- warning
- notice
- info
- debug
- none
- error
- panic
- warn

Rsyslog

Destino do Rsyslog

- **Arquivo**.

  Exemplo: cron.* /var/log/cron.log

- **Pipe (|)**.

  Exemplo: mail.* | /dev/tty12

- **Remoto (@).**

  Exemplo: *.* @192.168.20*.X

- **Usuário**.

  Exemplo: auth,authpriv.* root

Rsyslog

Implementando um Servidor de Logs no Audit:

1 – Acrescente o parâmetro “-r” no arquivo de configuração do rsyslog

```
1# vim /etc/default/rsyslog
```

```
RYSLOGD_OPTIONS = "-c5,-r"
```

2 – Descomente no arquivo rsyslog.conf as linhas mostradas abaixo:

```
2# vim /etc/rsyslog.conf
```

```
16    $ModLoad imudp
17    $UDPServerRun 514
123   *.*     /var/log/all.log
```

Rsyslog

Implementando um Servidor de Logs no Audit:

3 – Reinicie o serviço do Rsyslog

```
3# service rsyslog restart
```

4- Verifique a porta 514 ativa:

```
4# netstat -nlu

5# netstat -nlu | grep 514
```

Rsyslog

Configuração do Servidor Cliente

1 – Edite o arquivo de configuração do rsyslog adicionando ao final:

```
1# vim /etc/rsyslog.conf
```

. @192.168.20*.X

2 – Grave o arquivo e reinicie o serviço do Rsyslog

```
2# service rsyslog restart
```

Rsyslog

Configuração do Servidor Cliente

3 – Para testar use o comando logger na maquina cliente:

```
3# logger -p authpriv.err "Log remoto"
```

4 – No servidor da máquina Audit utilize o comando tail verificando o conteúdo do arquivo all.log:

```
4# tail -f /var/log/all.log
```

Rsyslog

Gerenciando Rotação de Logs

1 - Configuração do LogRotate:

```
1# vim /etc/logrotate.conf
```

2 – Crie um arquivo de configuração para rotacionamento dos logs centralizados conforme o padrão descrito no slide seguinte:

```
2# vim /etc/logrotate.d/all
```

Rsyslog

Exemplo de configuração:

```
/var/log/all.log  {
    daily
    size 3M
    sharedscripts
    postrotate
        /usr/bin/pkill -1  rsyslog
    endscript
    rotate 5
}
```

Rsyslog

Testando o Logrotate:

1 – Adicione conteúdo aos arquivos para aumentar o tamanho

```
1# cat /var/log/* >> /var/log/all.log
```

2 – Pare quando o valor for maior a 3MB

```
2# du -hs /var/log/all.log
```

3 – Execute o comando de Logrotate para ativar as regras

```
3# logrotate /etc/logrotate.conf
```

Rsyslog

Testando o Logrotate:

4 – Verifique a rotação de LOG:

```
1# ls -l /var/log/all*
2# du -hs /var/log/all*
```

5 – Acrescente compressão de dados após a linha endscript:

```
3# vim /etc/logrotate.d/all
```

compress

6 – Repita os passos 1 a 4 para comparar a diferença.

Pergunta LPI

Você deseja rotacionar seus logs semanalmente, exceto o arquivo /var/log/wtmp que você quer uma rotação mensal. Como você pode fazer isso?

A. Atribuir uma opção global para rotacionar todos os registros semanais e uma opção numa sessão local para rotacionar o /var/log/wtmp mensalmente.

B. Atribuir uma opção na sessão local para rotacional todos os registros semanais e uma opção global para rotacionar o /var/log/wtmp mensalmente.

C. Mover o arquivo /var/log/wtmp para um diretório diferente. Execute o logrotate no novo local.

D. Configure o logrotate para não considerar o arquivo /var/log/log/wtmp. Fazer manualmente a cada mês.

Pergunta LPI

Você deseja rotacionar seus logs semanalmente, exceto o arquivo /var/log/wtmp que você quer uma rotação mensal. Como você pode fazer isso?

A. Atribuir uma opção global para rotacionar todos os registros semanais e uma opção numa sessão local para rotacionar o /var/log/wtmp mensalmente.

B. Atribuir uma opção na sessão local para rotacional todos os registros semanais e uma opção global para rotacionar o /var/log/wtmp mensalmente.

C. Mover o arquivo /var/log/wtmp para um diretório diferente. Execute o logrotate no novo local.

D. Configure o logrotate para não considerar o arquivo /var/log/log/wtmp. Fazer manualmente a cada mês.

4LINUX
FREE SOFTWARE SOLUTIONS

Resposta: A

Pergunta LPI

Qual das seguintes linhas do /etc/syslog.conf file irá fazer com que todas as mensagens críticas sejam enviadas para o arquivo /var/log/critmessages?

A. *.=crit /var/log/critmessages

B. *crit /var/log/critmessages

C. *=crit /var/log/critmessages

D. *.crit /var/log/critmessages

Pergunta LPI

Qual das seguintes linhas do /etc/syslog.conf file irá fazer com que todas as mensagens críticas sejam enviadas para o arquivo /var/log/critmessages?

A. *.=crit /var/log/critmessages

B. *crit /var/log/critmessages

C. *=crit /var/log/critmessages

D. *.crit /var/log/critmessages

Resposta: A


4LINUX
FREE SOFTWARE SOLUTIONS