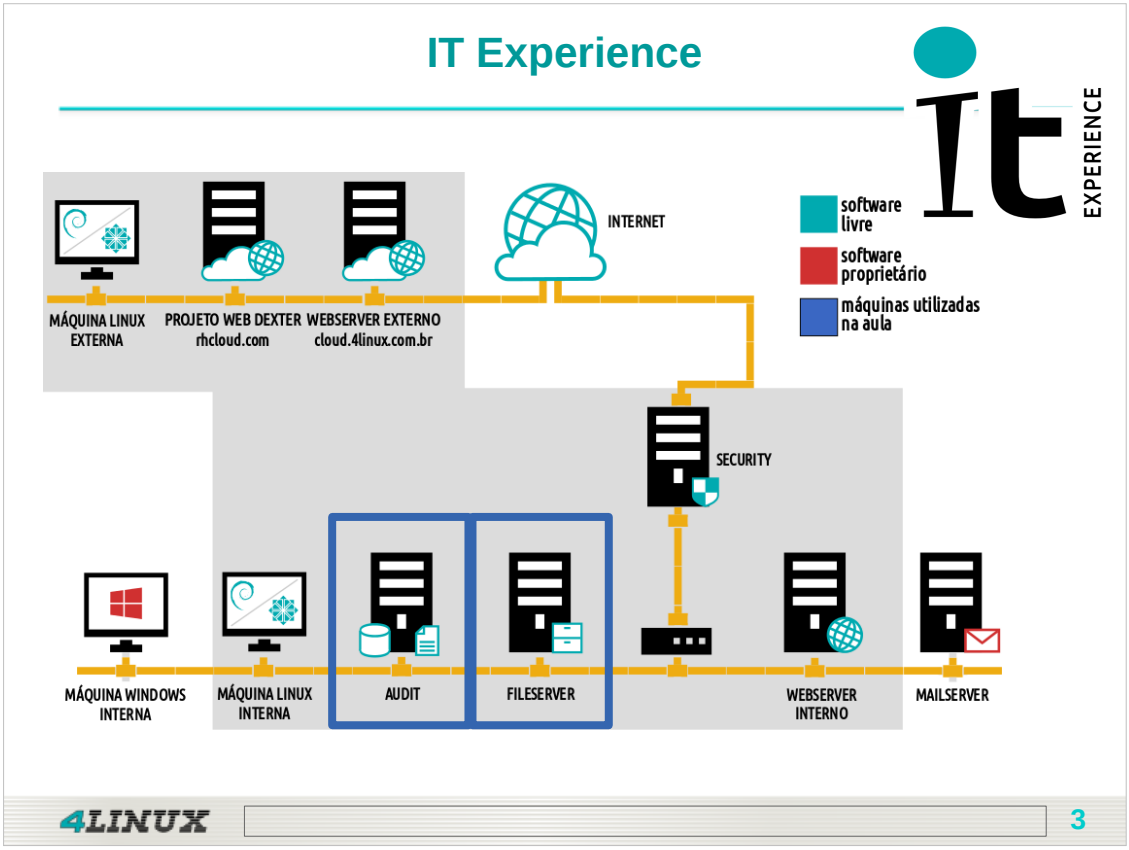
Curso 4451

Linux Security Administration in Cloud

Fundamentação

Manter o sistema com o horário correto é uma tarefa muito importante e que muitas vezes é negligenciada pelos administradores. Sem o horário ajustado corretamente, fica difícil agendar tarefas a serem executadas periodicamente, ou até mesmo fazer a leitura dos logs e determinar em que horário um determinado evento ocorreu.

Uma solução para essa questão é criar um servidor responsável pela manutenção de data e hora no sistema, ou utilizar um servidor já existente para atualizar as máquinas de sua rede neste capítulo exploraremos estas possibilidades conhecendo o protocolo NTP e os comandos **“date”** e **“hwclock”.**


IT Experience
IT EXPERIENCE
INTERNET
software livre
software proprietário
máquinas utilizadas na aula
MÁQUINA LINUX EXTERNA
PROJETO WEB DEXTER rhcloud.com
WEBSERVER EXTERNO cloud.4linux.com.br
SECURITY
MÁQUINA WINDOWS INTERNA
MÁQUINA LINUX INTERNA
AUDIT
FILESERVER
WEBSERVER INTERNO
MAILSERVER
4LINUX
3

Anotações:

Objetivos da Aula

Aula 08 (parte 1/2)

- Ajuste manual de horário:
  - Timezone, data e hora da BIOS e Sistema;
- Introdução ao protocolo NTP;
- Configurar cliente NTP;
- Instalar e configurar um servidor NTP.

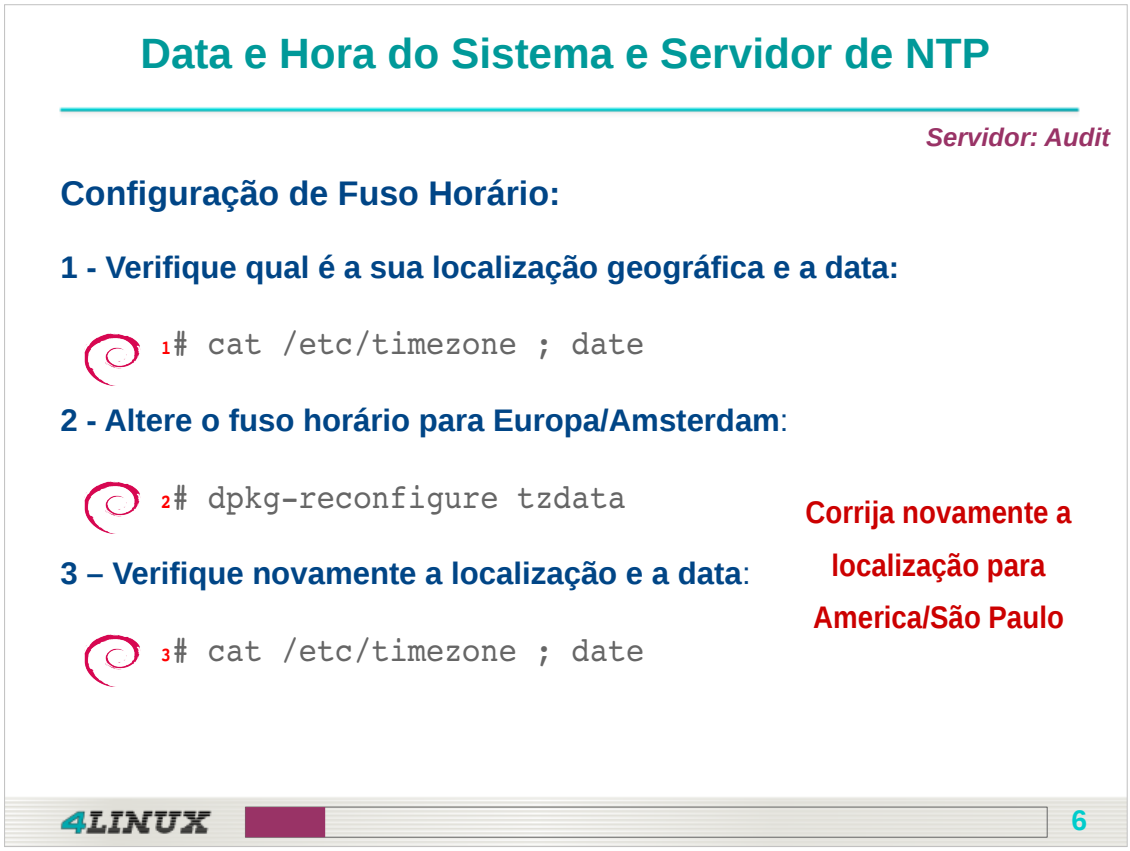
Anotações:

Objetivos da Aula

Aula 08 (parte 2/2)

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

Anotações:



Timezone

No que diz respeito a configuração de data e hora no sistema um ponto importante é a configuração da "timezone", ou seja, o fuso horário em que a máquina se encontra.

Essa configuração pode ser efetuada utilizando os comandos “dpkg-reconfigure tzdata" (específico do Debian) e "system-config-date" em distribuições como CentOS, Suse e Gentoo.

Data e Hora do Sistema e Servidor de NTP

Servidor: WebServerInterno

Configuração de Fuso Horário:

1 - Verifique qual é a sua localização geográfica no CentOS:

```
1# cat /etc/sysconfig/clock ; date
```

2 – Faça alteração de fuso horário através do arquivo /etc/localtime:

```
2# rm -rf /etc/localtime

3# cd /usr/share/zoneinfo/America

4# ln Los_angeles /etc/localtime
```

O arquivo **/etc/localtime** é responsável por definir o fuso horário do sistema.

4LINUX 7

DICA:

Se pretende prestar a LPI tome nota da função e localização dos arquivos **“localtime”** e dos arquivos de fuso horário disponíveis em “**/usr/share/zoneinfo/”** pois ambos podem ser cobrados em prova.

Data e Hora do Sistema e Servidor de NTP

Servidor: WebServerInterno

Configuração de Fuso Horário:

3 – Verifique se houve alteração na data:

```
1# date
```

4 – Faça a correção do fuso horário:

```
2# rm -rf /etc/localtime
3# cd /usr/share/zoneinfo/America
4# ln Sao_Paulo /etc/localtime
5# date
```

O comando **ln** possui a função de criar um link, um tipo de arquivo existente em sistemas UNIX que faz ligações entre arquivos.

Para alterar o fuso horário criamos um link físico (hard link) entre o arquivo de fuso horário e o arquivo **/etc/localtime**.

Outra opção para alteração de fuso horário é o comando **tzselect**

Anotações:

Data e Hora do Sistema e Servidor de NTP

Servidor: Audit

Configuração de Fuso Horário:

- E se pudéssemos verificar qualquer fuso horário do mundo? Sem alterar o horário do sistema?
  - Isso é possível através da varável TZ, capaz de exibir a time zone de um determinado país.

1 – Verifique o fuso horário em Berlim e, a seguir, em Moscou:

```
1# TZ=Europe/Berlin date
2# TZ=Europe/Moscow date
```


Anotações:

Data e Hora do Sistema e Servidor de NTP

Servidor: Audit

Configurar Data e Hora da Bios e Sistema:

O comando date permite verificar e/ou alterar data e hora no sistema:

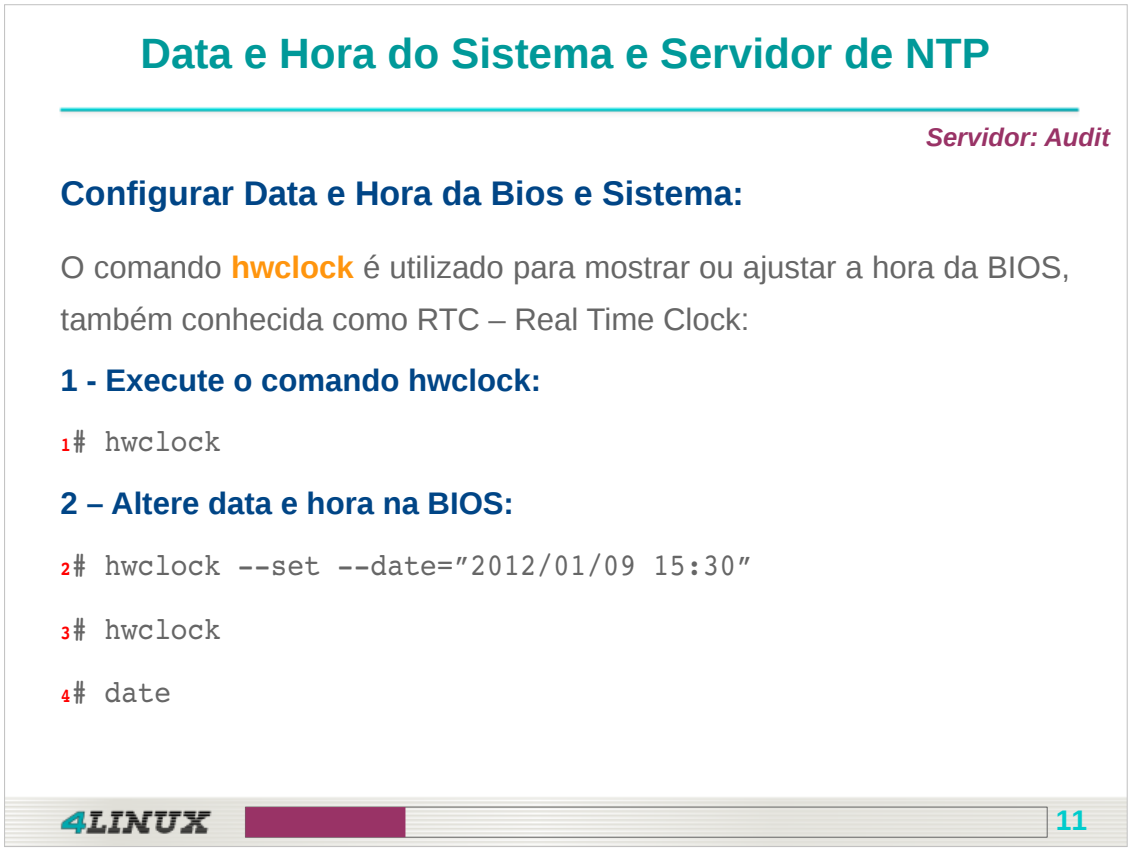
1 - Definindo data e hora no formato padrão (MMDDHHmmYYYY):

```
1# date 120520302014
2# date
```

2 - Definindo data e hora no formato string (MM/DD/YYYY HH:mm):

```
3# date -s "12/05/2014 20:30"
4# date
```


Anotações:



O comando hwclock

O comando “hwclock” é utilizado para mostrar ou ajustar a hora da BIOS da máquina sendo conhecido como RTC - Real Time Clock. Este é o relógio que fica continuamente em funcionamento mesmo que a máquina esteja desligada; de forma que o horário esteja atualizado da próxima vez que a máquina for religada.

Data e Hora do Sistema e Servidor de NTP

Servidor: Audit

Atualizar Data e Hora da Bios e Sistema:

O **hwclock** também pode ser utilizado para sincronização de data e hora entre a BIOS e o sistema.

1 – Ajuste o horário do sistema utilizando o horário da BIOS:

```
1# hwclock -s ou hwclock --hctosys
2# date
```

2 – Modifique a data do sistema e, a seguir, ajuste o horário da BIOS utilizando o horário do sistema:

```
3# hwclock -w ou hwclock --systohc
```


Anotações:

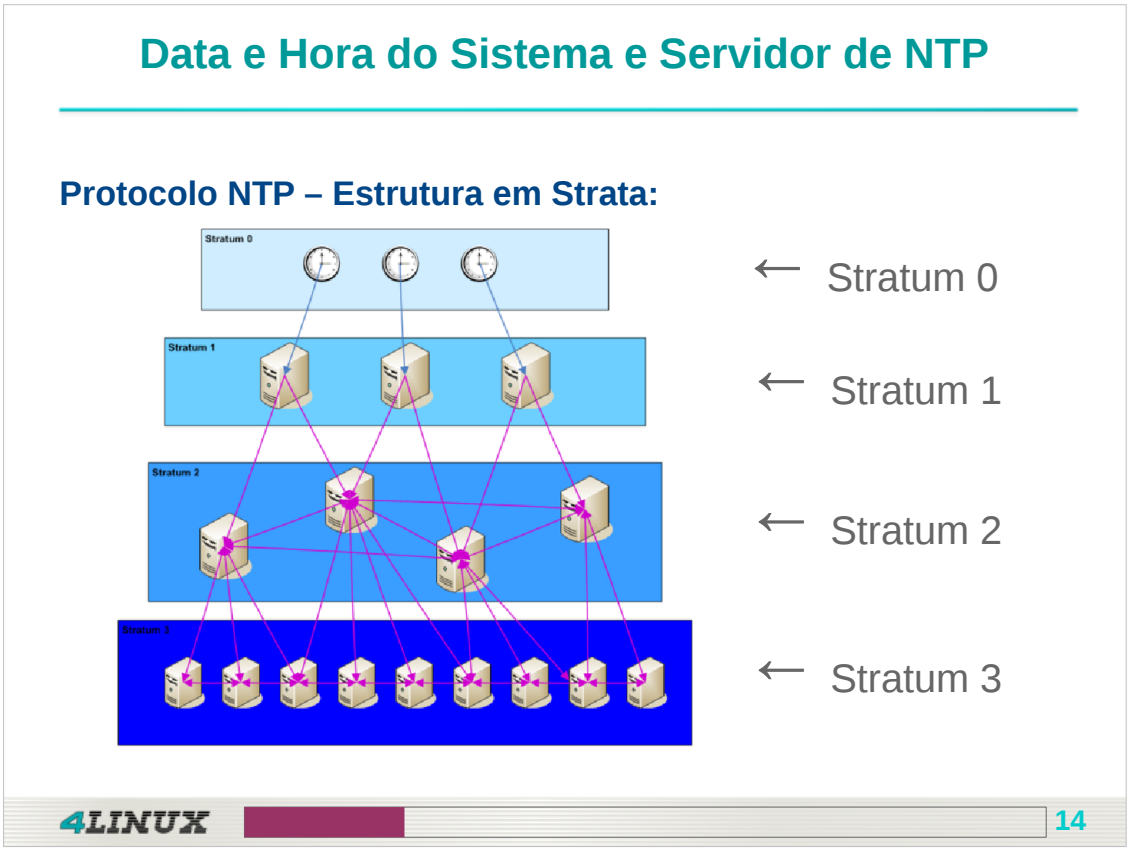
Data e Hora do Sistema e Servidor de NTP

Protocolo NTP – Network Time Protocol:

O protocolo de sincronização de horários "NTP" foi desenvolvido a fim de possibilitar que qualquer computador ligado à internet possa ajustar sua data e hora automaticamente, utilizando um servidor de “hora” preciso.

NTP - Network Time Protocol

O Serviço NTP utiliza a porta UDP 123 para realizar a sincronização de horários. Este serviço baseia-se no Protocolo NTP – (Network Time Protocol), criado em 1985, é com certeza um dos protocolos de internet mais antigos ainda em uso, seu funcionamento pode atingir uma precisão de aproximadamente 200µs(duzentos microssegundos).

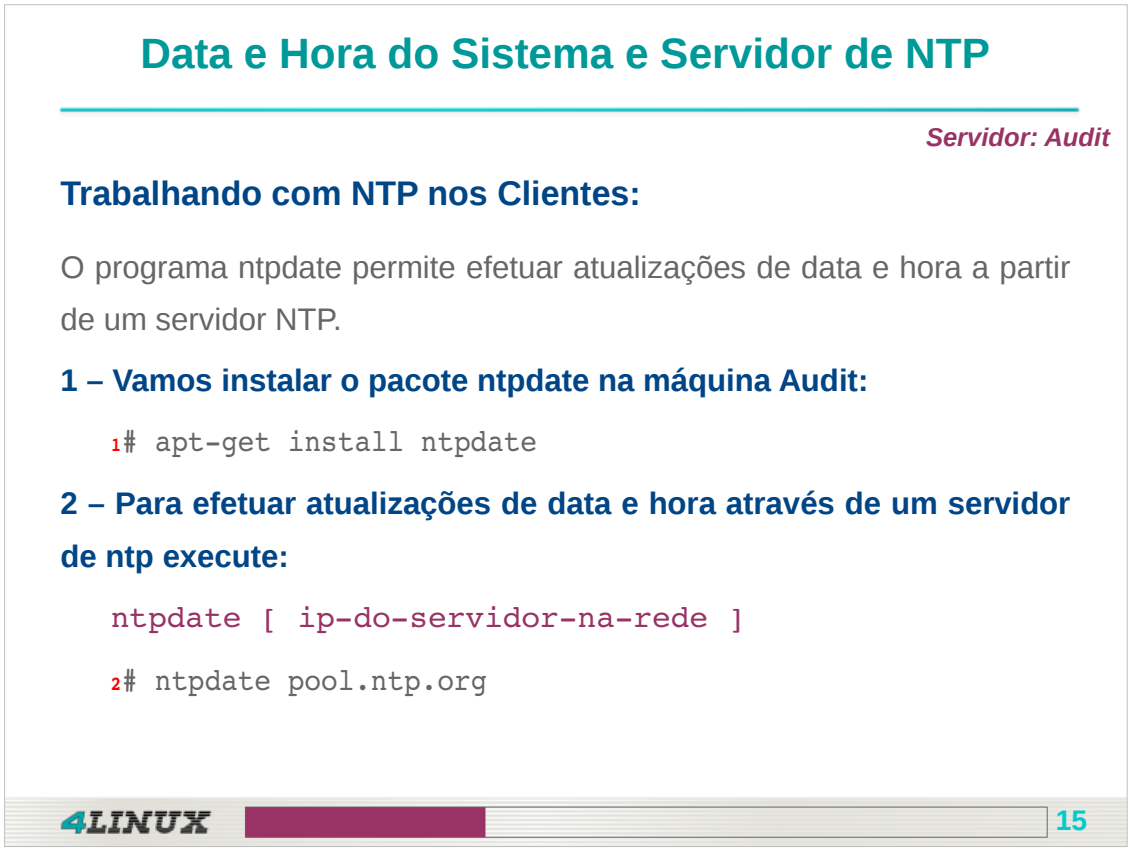


Organização em Strata

A hierarquia do NTP é dividida em vários níveis, o conjunto deles é denominado **"strata"** e cada um deles corresponde a um **"stratum"**.

A raiz desse sistema é o denominado **“stratum 0“** e que corresponde aos relógios nucleares espalhados pelo mundo, aos quais estão conectados os servidores de **"stratum 1"**, ou seja, são eles que fazem o processamento da informação recebida do ”stratum 0”.

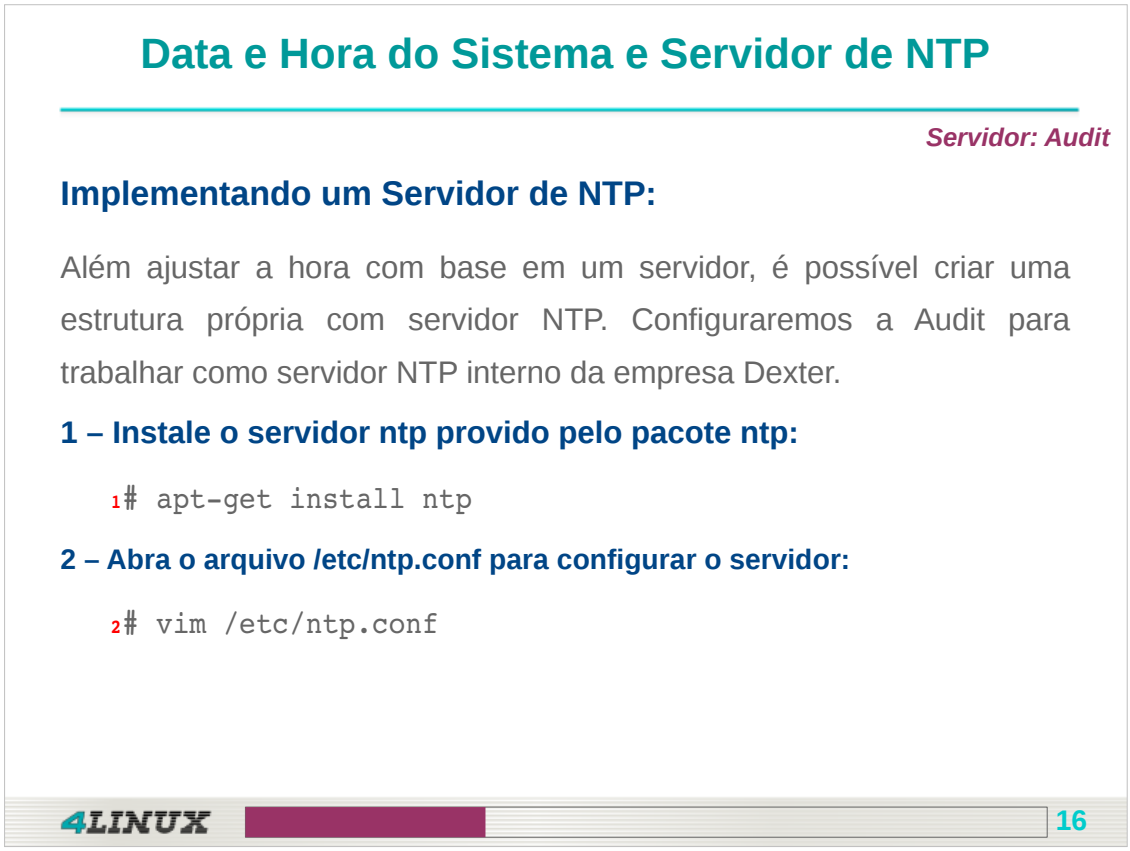
Uma representação esquemática dessa estrutura pode ser vista na figura acima.



Organização em Strata

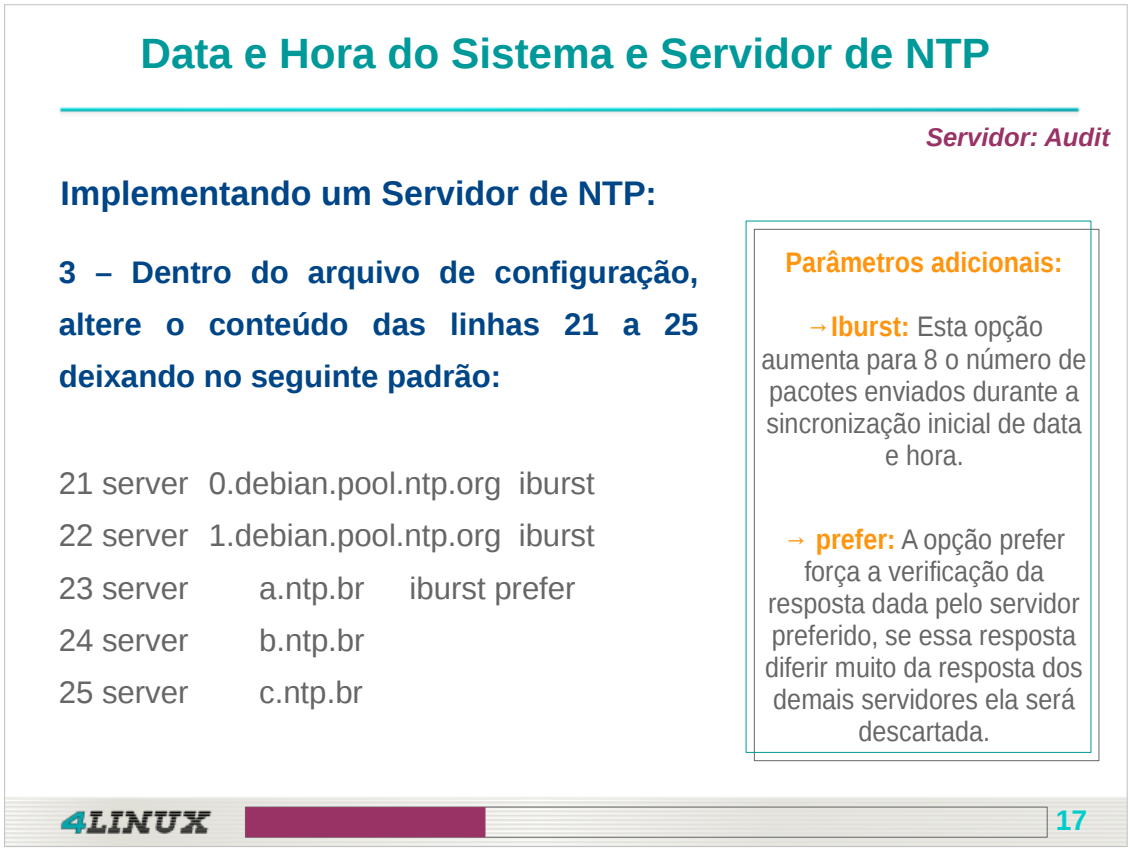
Conectados aos "stratum 1" há o sistema **"stratum 2"** os servidores deste sistema em geral estão conectados a mais de um servidor de “stratum 1” e determinam de fato qual é a hora padrão com base nos dados recebidos dos "stratum 1" utilizando o algoritmo do NTP.

Os "stratum 2" respondem ao **"stratum 3"** que responde ao **"stratum 4"** e assim por diante até atingir, no máximo, 16 níveis.



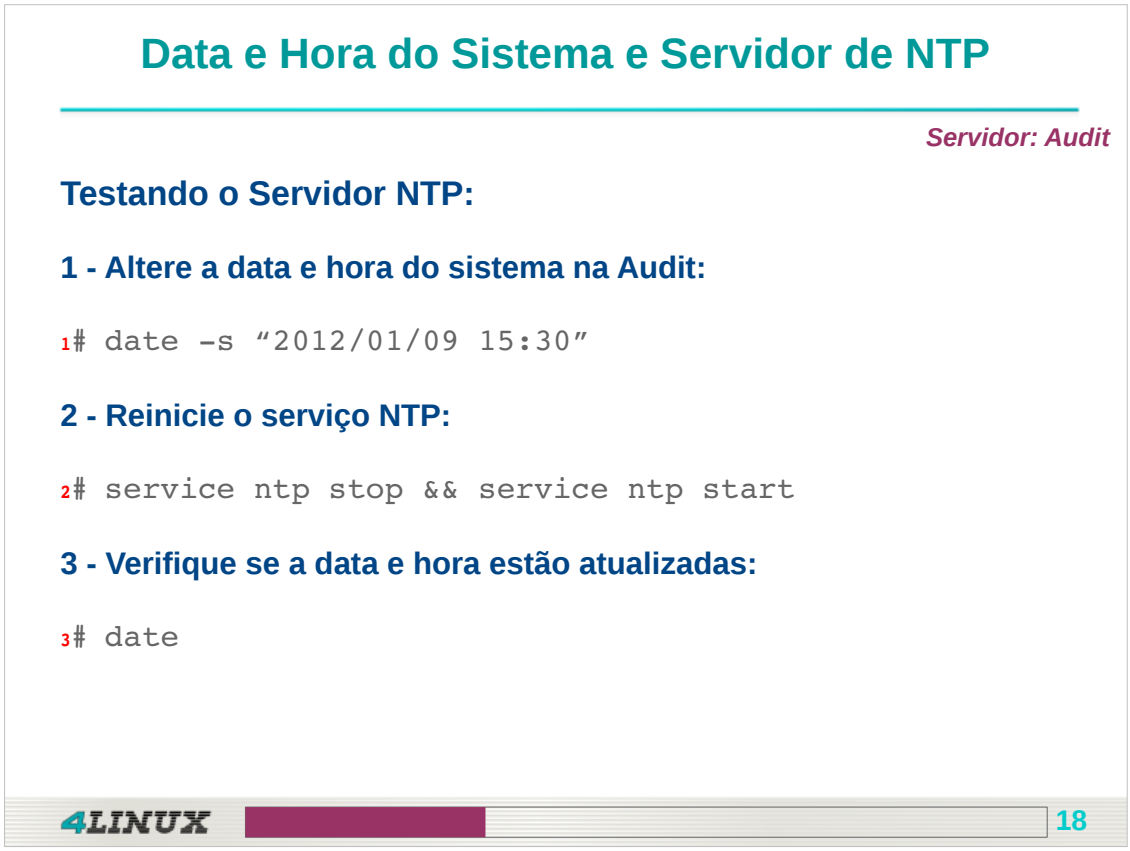
Com qual nível devo sincronizar?

A menos que estejamos montando um servidor para ser um "stratum 1", 2 ou 3, nunca devemos utilizar os servidores "stratum 1"ou 2 para sincronizarmos nossos servidores; mas sim acessar um "stratum 3". Dessa forma deixamos os níveis mais baixos para as máquinas que realmente precisam acessá-los.



Com qual nível devo sincronizar?

Ainda assim, nossa política de acesso aos "stratum 3"deve ser também bastante criteriosa. Se nossa rede possuí diversas máquinas, não há sentido em fazermos todas elas se sincronizarem em um "stratum 3", mas sim escolher uma de nossas máquinas para ser um “stratum 4” e nossos clientes realizarem a sincronização a partir dela.



Com qual nível devo sincronizar?

É sempre aconselhável utilizar mais de um servidor para que, caso ocorra algum erro em algum deles, o nosso sistema possa continuar com a configuração correta.

Data e Hora do Sistema e Servidor de NTP

Servidores: Debian/Ubuntu

Agora que nosso servidor NTP está pronto, vamos ajustar os servidores internos da Dexter para atualizar data e hora de forma interna:

1 – Instale o pacote nptdate no servidor FileServer:

```
1# apt-get install ntpdate
```

2 – Configure o arquivo default do ntpdate indicando o IP do servidor da audit como fonte de atualização de data e hora:

```
2# vim /etc/default/ntpdate
10 NTPSERVERS="192.168.200.20"
3# ntpdate 192.168.200.20
```

NOTA: Seja paciente, seu servidor NTP só irá fornecer a hora para os clientes quando ele estiver totalmente sincronizado com um Stratum acima dele.

Anotações:

Limitando as Consultas ao Servidor NTP

Servidor: Audit

Restrigindo Consultas ao Servidor Audit:

Para que um servidor NTP não sofra abusos em relação a consultas externas não autorizadas é possível definir quem poderá fazer consultas no servidor.

- Abra o arquivo **/etc/ntp.conf**:

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


Anotações:

Limitando as Consultas ao Servidor NTP

Servidor: Audit

- Adicione a seguinte informação a linha 42:

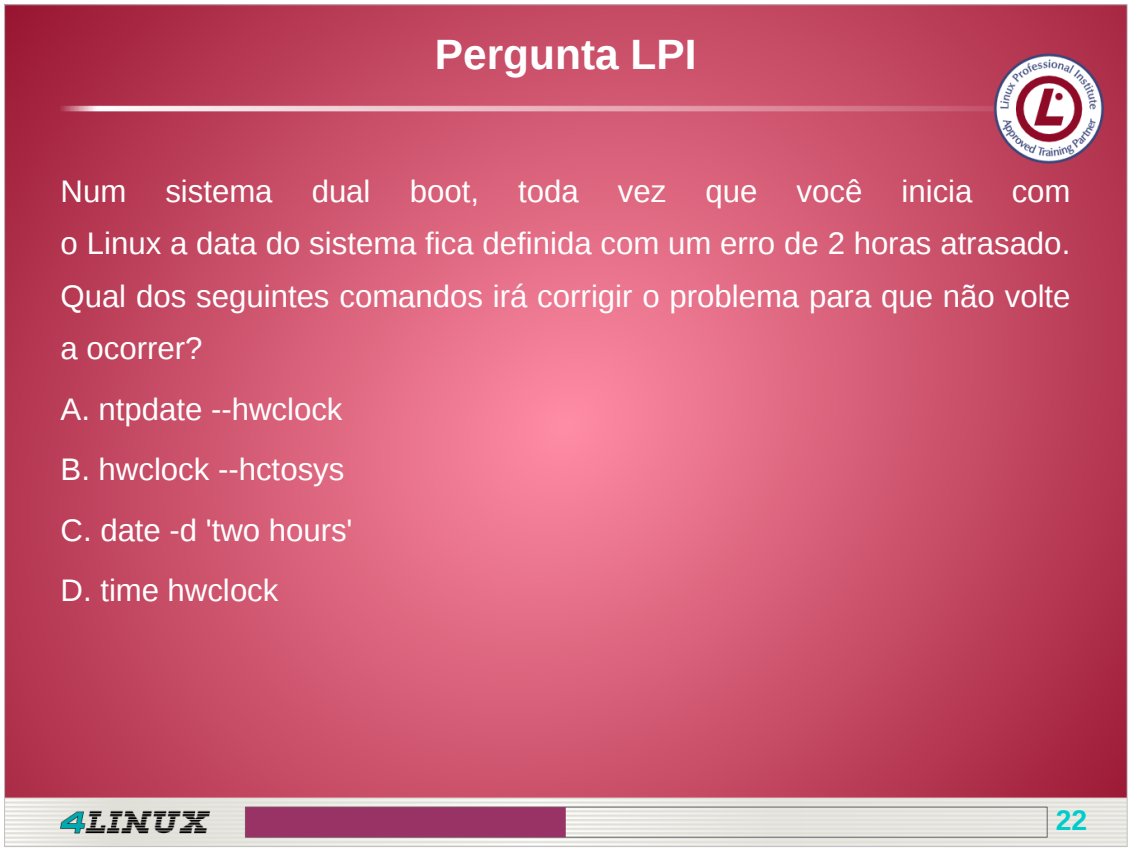
  restrict 192.168.200.0

  (Substitua o IP acima pelo IP da rede Dexter)

- Tente utilizar o comando ntpdate para atualizar a data através das máquinas da empresa Dexter.

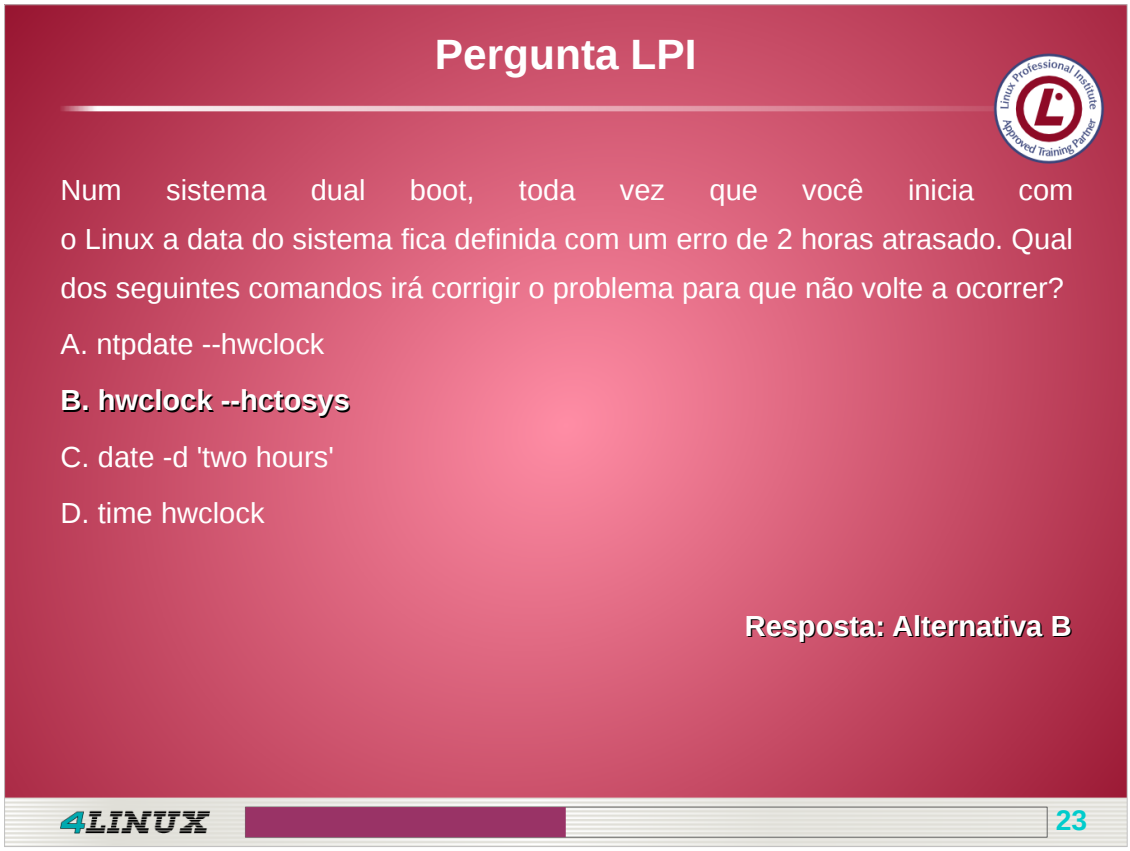
A partir de agora só a rede Dexter poderá obter data e hora!

Anotações:



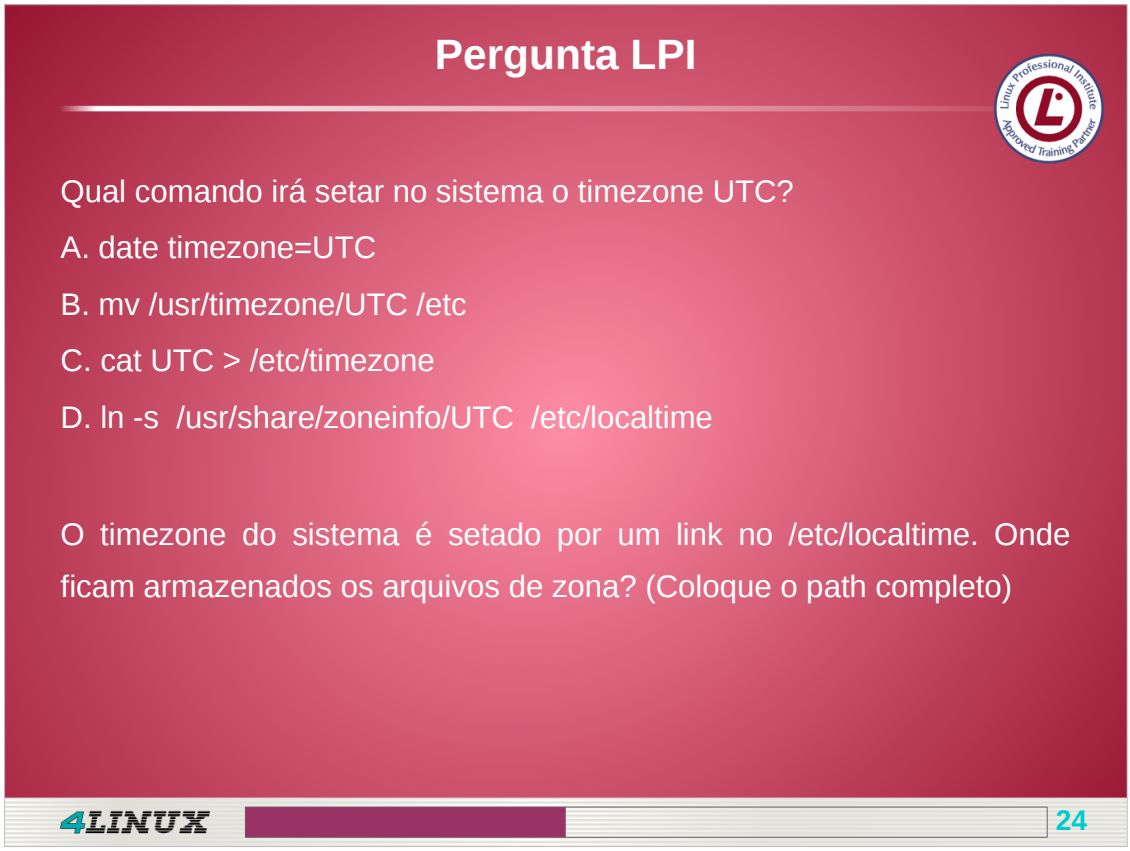
Alternativa B: RESPOSTA CORRETA!

Considerando que o problema descrito está relacionado a data do sistema e não da BIOS e admitindo que a BIOS esteja com a data corretamente configurada o comando **hwclock --hctosys** ou **hwclock -w** replicaria o horário da BIOS para o sistema resolvendo o problema.



Alternativa B: RESPOSTA CORRETA!

Considerando que o problema descrito está relacionado a data do sistema e não da BIOS e admitindo que a BIOS esteja com a data corretamente configurada o comando **hwclock --hctosys** ou **hwclock -w** replicaria o horário da BIOS para o sistema resolvendo o problema.

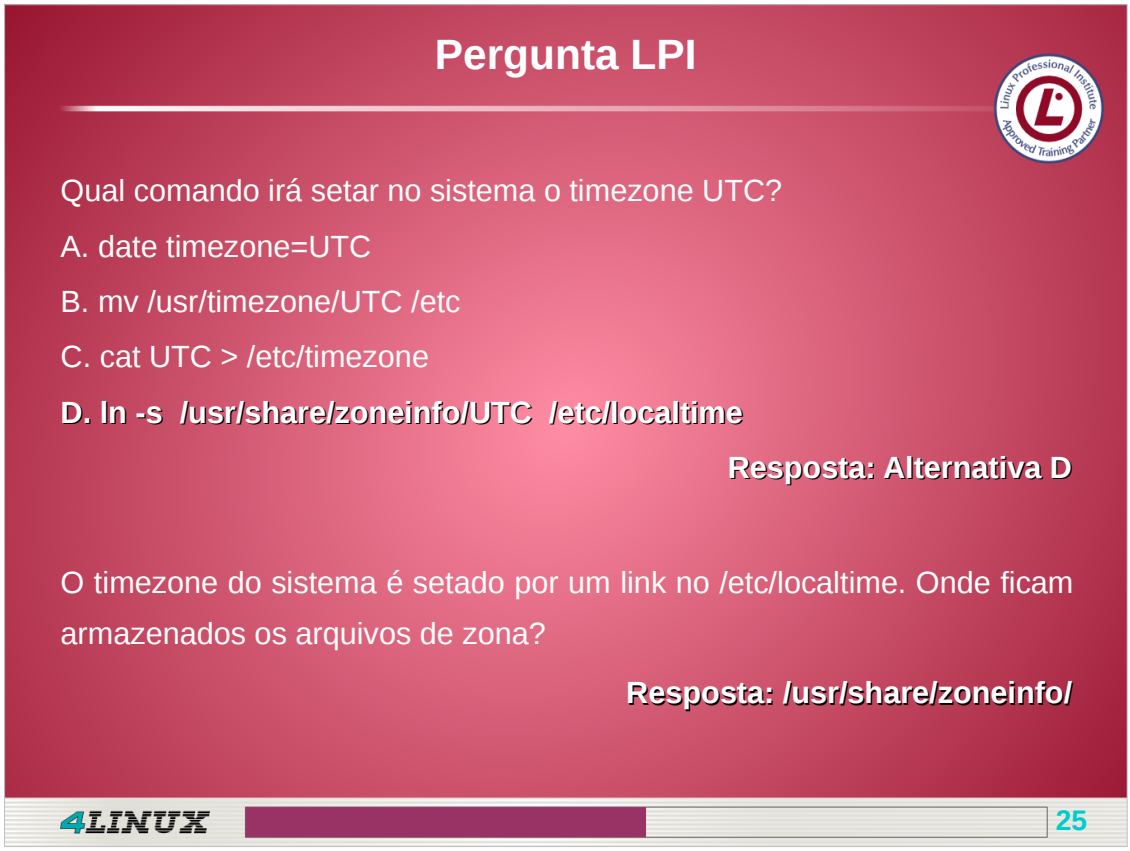


Alternativa D: RESPOSTA CORRETA!

O conteúdo do arquivo **/etc/localtime** é gerado a partir de um hard link (obtido pelo comando ln) ou através de um link simbólico (obtido pelo comando ln -s) criado entre o arquivo original e o arquivo alvo para criação do link, o arquivo localtime.

RESPOTA CORRETA: /usr/share/zoneinfo/

Assim como exemplificado na pergunta anterior e como comentado em aula, todos os arquivos de fuso horário de um sistema GNU/Linux estão alocados dentro do diretório /usr/share/zoneinfo/.



Alternativa D: RESPOSTA CORRETA!

O conteúdo do arquivo **/etc/localtime** é gerado a partir de um hard link (obtido pelo comando ln) ou através de um link simbólico (obtido pelo comando ln -s) criado entre o arquivo original e o arquivo alvo para criação do link, o arquivo localtime.

RESPOTA CORRETA: /usr/share/zoneinfo/

Assim como exemplificado na pergunta anterior e como comentado em aula, todos os arquivos de fuso horário de um sistema GNU/Linux estão alocados dentro do diretório /usr/share/zoneinfo/.

Gerenciamento de Logs com Rsyslog

Fundamentação

Um sistema GNU/Linux registra uma grande quantidade mensagens. Sejam estas referentes a erros, depuração, ou avisos, as mensagens geram os logs do sistema.

O objetivo deste capítulo é adquirir melhores praticas em relação a gerência destes arquivos e consulta de seu conteúdo.

Visualização de Logs do Sistema

Entendendo as Mensagens de Log:

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

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

O padrão **FHS** define que um sistema linux armazenará os seus logs no diretório /var/log

Arquivos de log não são arquivos de erros!

Arquivos de logs são utilizados essencialmente para análise e resolução de problemas, ou seja, verificação de falhas. Além disso provêm outras finalidades tão importantes quanto essas, como auditoria de servidores e extração de relatórios.

Visualização de Logs do Sistema

Servidor: Audit

Entendendo as Mensagens de Log:

- Mensagens de log podem assumir dois formatos: **texto puro** que são logs visualizados por comandos como tail,cat,head,tac,more,less...

```
1# cat /var/log/dmesg
```

- E o **formato binário** que são visualizados por comandos específicos:

```
2# last
3# lastlog
```


Logs em formato binário:

Sobre os comandos acima, o comando last visualiza o arquivo /var/log/wtmp enquanto o comando lastlog visualiza o conteúdo do arquivo de log /var/log/lastlog;

Visualização de Logs do Sistema

Principais Arquivos de Log:

cron→ Mensagens de funcionamento do servidor crond, ou seja, os logs sobre execução de tarefas agendadas;

dmesg→ Contém as mensagens de reconhecimento de hardware pelo kernel, geradas durante a inicialização da máquina;

messages → Considerado o principal arquivo de log do sistema, contém mensagens enviadas por aplicações e serviços.

Anotações:

Visualização de Logs do Sistema

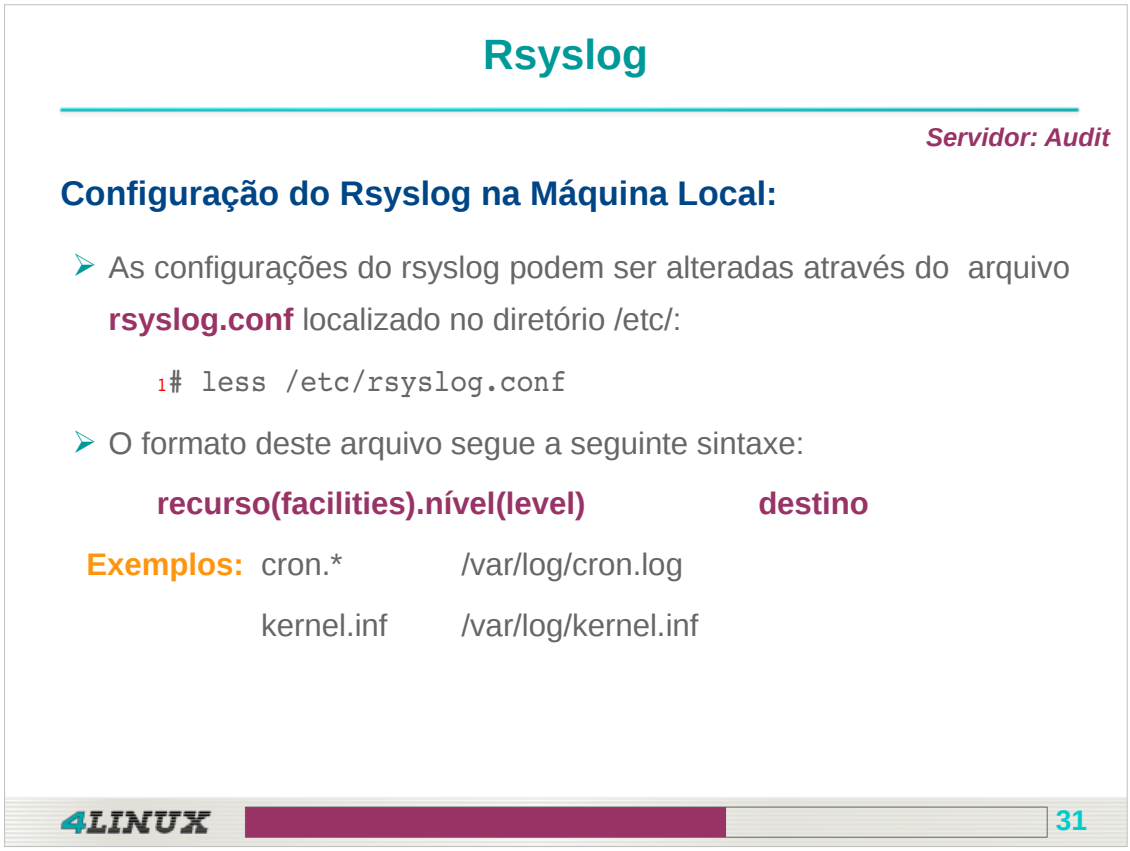
Principais Arquivos de Log:

lastlog → Contém informações sobre os últimos logins de usuário (date e hora);

wtmp→ Carrega informações sobre quem está logado e o que está fazendo no sistema;

auth.log → Log com informações referentes a autenticação e mudanças de usuários.

Anotações:



Configurando o Rsyslog

Uma vez que se tenha conhecimento da quantidade de mensagens geradas pelo sistema, é fácil entender a necessidade de se organizar veementemente essas informações, permitindo verificações futuras;

Fica a cargo do serviço rsyslog a responsabilidade de armazenar essas mensagens;

O rsyslog permitirá, entre muitas opções, armazenar essas mensagens em diferentes arquivos e organizá-las de acordo com nível e importância e origem.

Facilidades (Recursos) do Rsyslog

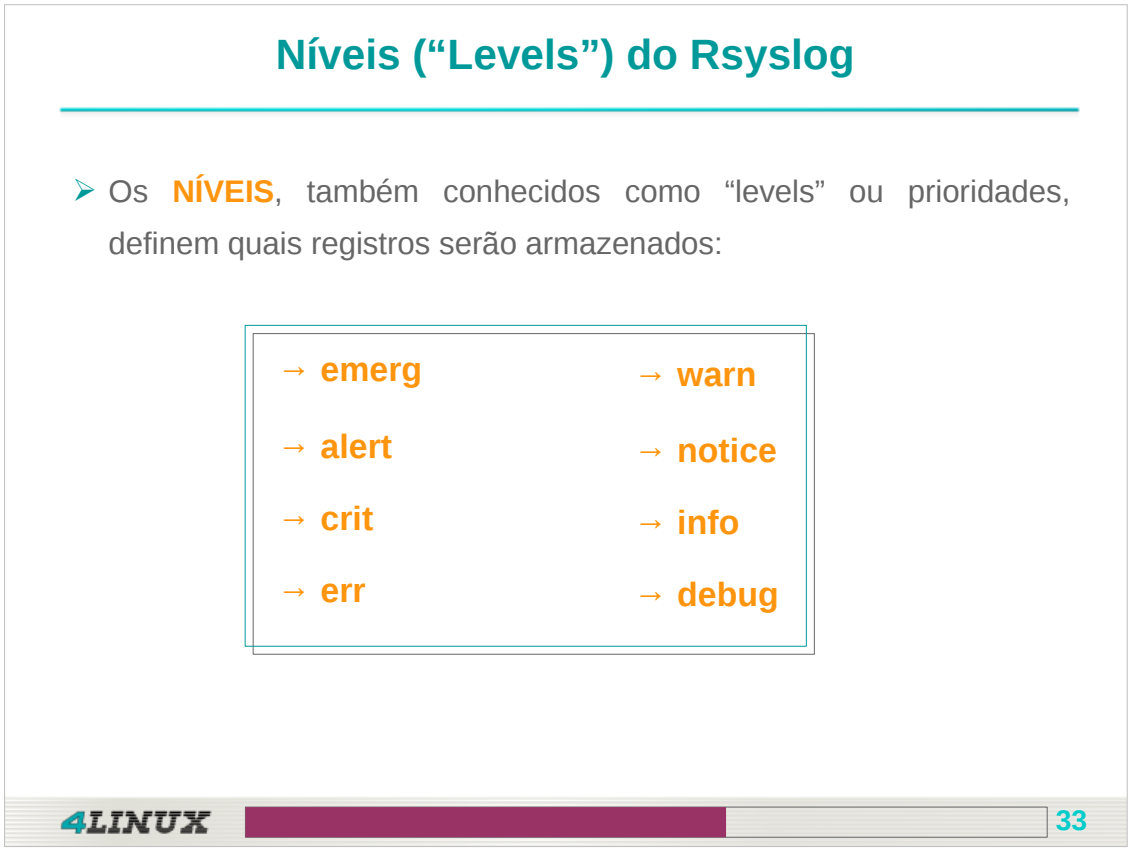
- As **FACILIDADES** representam os grupos de logs nos quais são enquadrados os registros do rsyslog;

- O **rsyslog** utiliza as seguintes facilidades:

→ auth	→ daemon	→ local[0-7]	→ news
→ authpriv	→ ftp	→ lpr	→ syslog
→ cron	→ kern	→ mail	→ user

Por que usamos Facilidades para categorizar os logs?

Ao definir em qual facilidade um log se enquadra estamos basicamente categorizando os tipos de logs por grupos de recursos como autenticação (auth), e-mail (mail) e etc.



E qual a importância dos níveis?

A depender da importância um registro, ele poderá ser ignorado pelo rsyslog com base em especificações feitas no arquivo de configuração, é ai que entram os níveis, eles servirão para priorizar ou não uma mensagem de acordo com o seu conteúdo.

Rsyslog

Servidor: Audit

- Ao configurar um arquivo de log o **destino** do log gerado pode variar conforme abaixo:

  /dev/tty → O destino é uma console;

  /var/log/arquivo.log → O destino do log é um arquivo de log;

  @host_destino → O destino é uma máquina remota;

  usuário → O destino é um usuário específico conectado a máquina.

Exemplos de uso prático dos destinos acima:

/dev/tty → mail.* /dev/tty5;

/var/log/arquivo.log → kern.emerg /var/log/messages;

@host_destino → *.* @192.168.20*.X

usuário → auth,authpriv.* root

Rsyslog

Servidor: Audit

Configurando o Rsyslog:

1 – Abra o arquivo de configuração do rsyslog:

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

2 – Descomente a linha referente aos logs do cron:

```
cron.*                  /var/log/cron.log
```

3 – Reinicie o rsyslog para que as alterações entrem em vigor e o crontab gere entradas no log:

```
2# service rsyslog restart
3# service cron restart
4# tailf /var/log/cron.log
```


Anotações:

Rsyslog

Servidor: Audit

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


Anotações:

Rsyslog

Servidor: Audit

Implementando um Servidor de Logs no Audit:

3 – Reinicie o serviço do Rsyslog:

```
1# service rsyslog restart
```

4- Verifique a porta 514 ativa:

```
2# netstat -nlu

3# netstat -nlu | grep 514
```


Anotações:

Rsyslog

Servidor: FileServer / WebServerInterno

Configuração do Servidor Cliente:

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

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

   *.*      @192.168.200.20
```

2 – Grave o arquivo e reinicie o serviço do Rsyslog:

```
2# service rsyslog restart
```


Anotações:

Rsyslog

Servidor: FileServer / WebServerInterno

Configuração do Servidor Cliente:

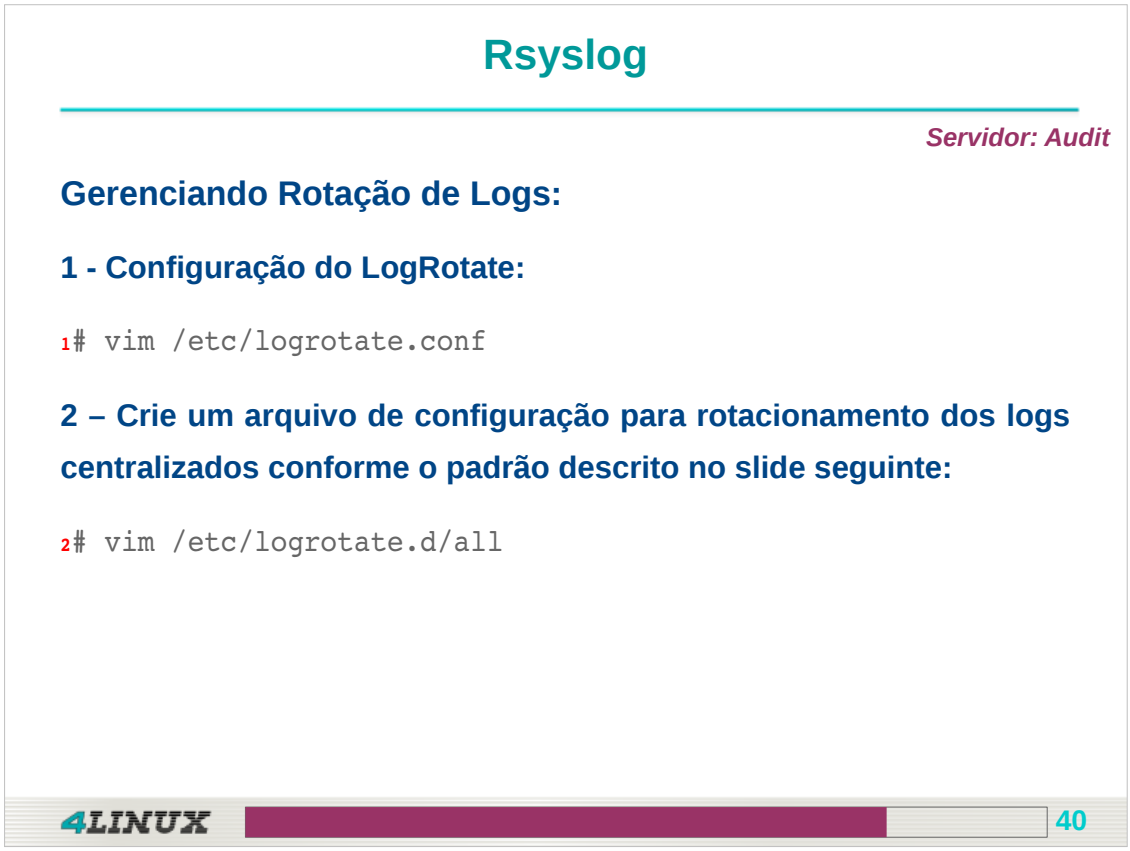
3 – Para testar use o comando logger na máquina cliente:

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

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

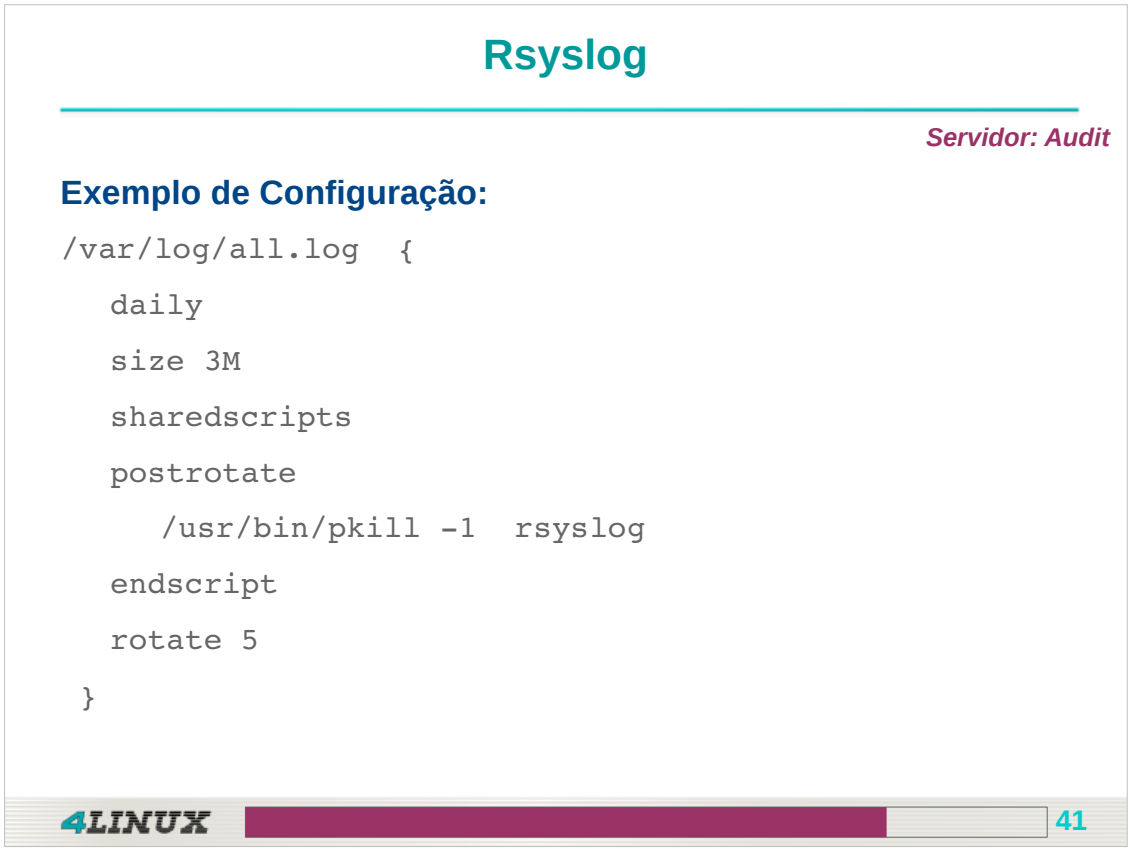
```
2# tail -f /var/log/all.log
```


Anotações:



Rotacionamento de Logs

Com o tempo, os logs podem ocupar muito do espaço disponível na partição. Por isso, devemos configurar corretamente a política de rotação dos logs, ou seja, durante quanto tempo os logs serão armazenados no seu computador.



Opções do Rotacionamento acima:

/var/log/all.log → Representa o arquivo que será rotacionado; diariamente até 5 vezes, caso o arquivo tenha pelo menos 3M.
daily → O sistema de logs será diário.
size 3M → Faz a rotação somente se o arquivo alcançar 3M.
sharedscripts → Marca o início do bloco de comandos.
postrotate → Executa os scripts após aplicar a rotação aos arquivos.
/usr/bin/pkill -1 rsyslog → Envia sinal 1 ao processo rsyslog.
endscript → Encerra o bloco de comandos.
rotate 5 → Aplica a rotação aos arquivos 5 vezes.

Rsyslog

Servidor: Audit

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
```


Anotações:

Rsyslog

Servidor: Audit

Testando o Logrotate:

4 – Verifique a rotação de LOG:

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

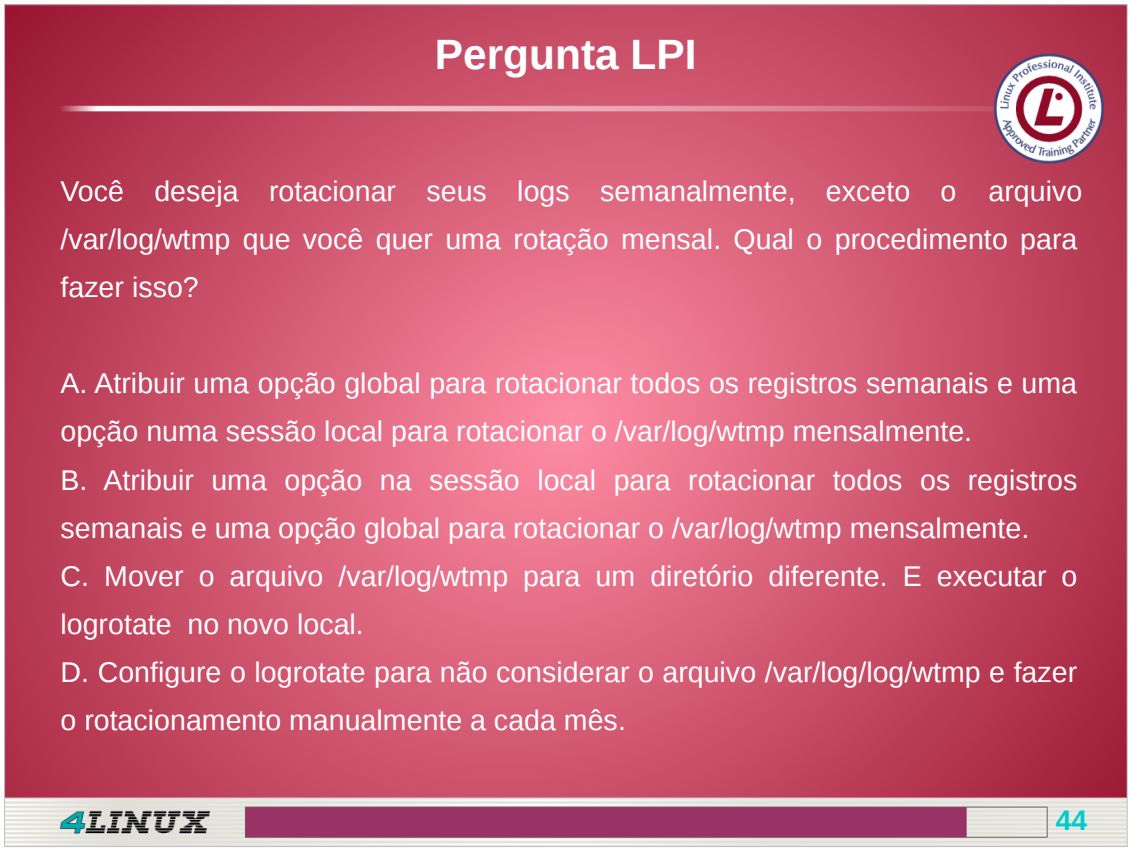
5 – Acrescente compressão de dados após a linha endscript:

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

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

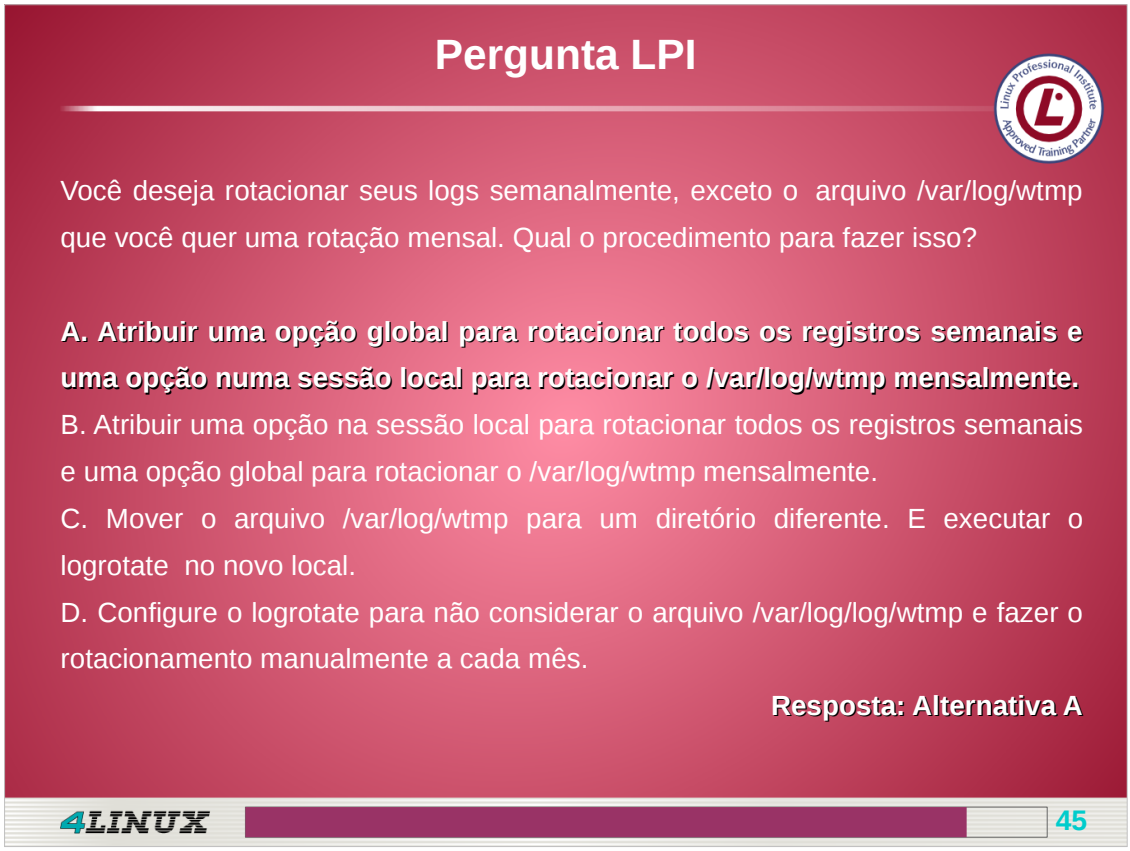
Opções do Rotacionamento acima:

compress → Define a compressão do arquivos rotacionados.



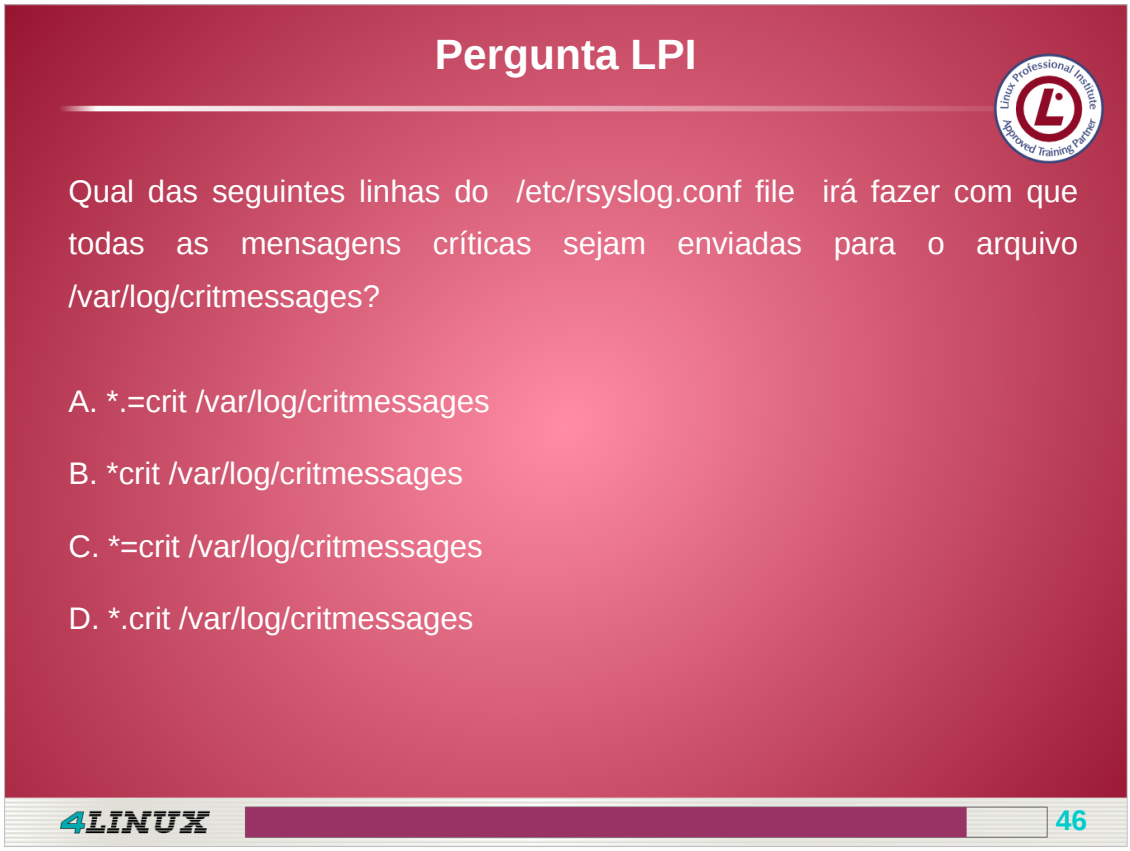
Alternativa A: RESPOSTA CORRETA!

O logrotate permite a criação de esquemas de rotacionamento em sessões diferentes dentro do arquivo /etc/logrotate.conf ou em arquivos alocados dentro do diretório /etc/logrotate.d/.



Alternativa A: RESPOSTA CORRETA!

O logrotate permite a criação de esquemas de rotacionamento em sessões diferentes dentro do arquivo /etc/logrotate.conf ou em arquivos alocados dentro do diretório /etc/logrotate.d/.

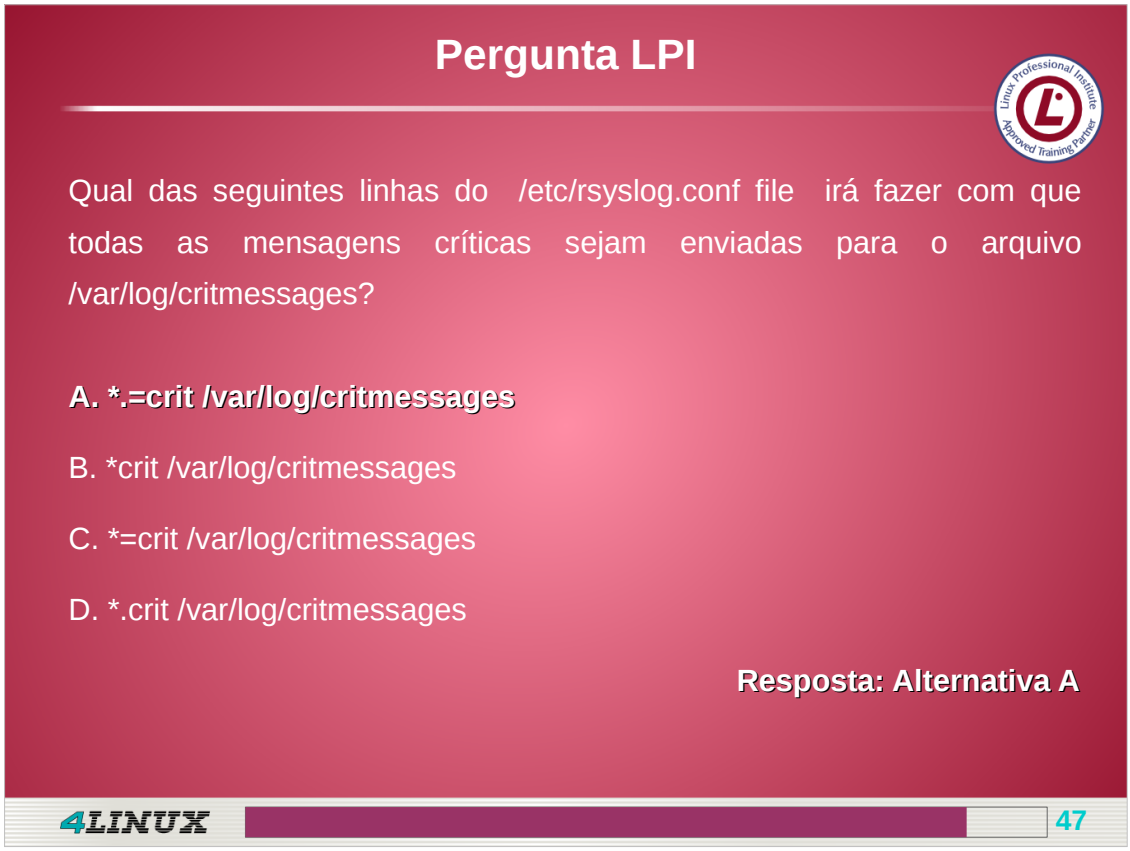


Alternativa A: RESPOSTA CORRETA!

Fique atento! Ao criar configurações no rsyslog deve-se levar em consideração o fato de que o envio de logs segue um modelo hierárquico

Ao definir o envio de logs com prioridade “crit” no formato de envio **'*.crit /var/log/critmessages'** automaticamente estaríamos enviando também qualquer prioridade **ACIMA** desta, ou seja: Mensagens de Prioridade alert e emerg também seriam enviadas.

Para enviar **APENAS** mensagens de prioridade crit o formato correto é **'*.=crit /var/log/critmessages'.**



Alternativa A: RESPOSTA CORRETA!

Fique atento! Ao criar configurações no rsyslog deve-se levar em consideração o fato de que o envio de logs segue um modelo hierárquico

Ao definir o envio de logs com prioridade “crit” no formato de envio **'*.crit /var/log/critmessages'** automaticamente estaríamos enviando também qualquer prioridade **ACIMA** desta, ou seja: Mensagens de Prioridade alert e emerg também seriam enviadas.

Para enviar **APENAS** mensagens de prioridade crit o formato correto é **'*.=crit /var/log/critmessages'.**

Próximos Passos

Para que você tenha um melhor aproveitamento do curso, participes das seguintes atividades disponíveis no Netclass:

- Executar as tarefas do **Practice Lab**;
- Resolver o **Desafio Appliance Lab** e postar o resultado no Fórum Temático;
- Responder as questões do **Teste de Conhecimento** sobre o conteúdo visto em aula.

Mãos à obra!