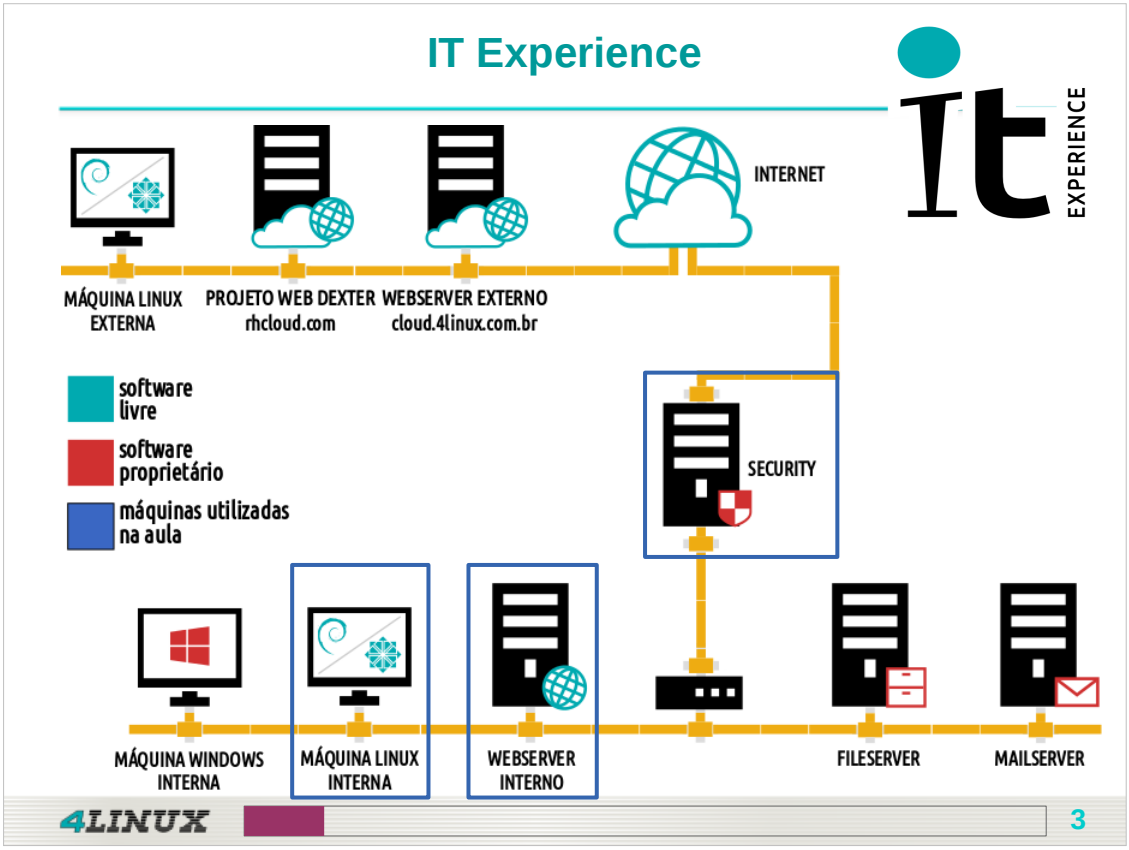
O gerenciamento de partições no Linux envolve tanto desempenho com segurança, quando manipulamos partições comuns e criptografadas. Neste cenário de infraestrutura, o Administrador tem acesso a diversas ferramentas para conversão de sistema de arquivos sem perdas de dados e configuração de mapeamentos manuas e automáticos de partições comuns e criptografadas.


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

Anotações:

Objetivos da Aula

Aula 12

- Migrar Filesystem sem perder dados;
- Gerenciar partições SWAP;
- Gerenciar montagens no boot;
- Gerenciar partições criptografadas;
- Configurar automount para partições.

Anotações:

Gerenciamento Avançado de Partições

Servidor: Webserver Interno

Migrar Filesystem: ext2 para ext3

- Desmonte a partição /backup:

```
1# umount /backup
```

- Vamos converter ext2 para ext3, sem perder os dados:

```
2# tune2fs -j /dev/sdb1
```

- Monte novamente a partição:

```
3# mount /dev/sdb1 /backup
```

Anotações:

Gerenciamento Avançado de Partições

Servidor: Webserver Interno

Migrar Filesystem: ext2 para ext3

- Visualize o tipo de filesystem com o comando mount:

```
1# mount
```

- Visualizar um arquivo para ver que não corrompeu:

```
2# cat /backup/etc/fstab
```

Anotações:

Gerenciamento Avançado de Partições

Servidor: Webserver Interno

Migrar Filesystem: ext3 para ext4

- Antes de iniciar a conversão, crie um arquivo na partição /srv:

```
1# echo "Dexter Courier" > /srv/index.html
```

- Desmonte a partição /srv:

```
2# umount /srv
```

- Agora vamos converter de ext3 para ext4, sem perder os dados:

```
3# tune2fs -O extents,uninit_bg,dir_index /dev/sdb2
```

Anotações:

Gerenciamento Avançado de Partições

Servidor: Webserver Interno

Migrar Filesystem: ext3 para ext4

- Cheque o sistema de arquivos do dispositivo:

```
1# e2fsck -pf /dev/sdb2
```

- Monte o sistema de arquivo:

```
2# mount /dev/sdb2 /srv
```

- Verifique o tipo de sistema de arquivos:

```
3# mount
```

- Visualize o arquivo index.html para ver que não corrompeu:

```
4# cat /srv/index.html
```

4LINUX 8

É possível utilizar diversos comandos no Linux para verificar se uma partição foi montada:

df -h

cat /etc/mtab

cat /proc/mounts

DICA LPI

Filesystems podem ser grandes aliados na prova, principalmente no tópico "migração de filesystems".

Lembre-se da migração mais comum de filesystems:

ext2 para ext3

Anotações:

Gerenciamento Avançado de Partições

Servidor: Webserver Interno

Gerenciar partições SWAP

- Vamos aproveitar a partição criada na aula anterior e aplicar o Swap à ela:

```
1# mkswap /dev/sdb3
```

- Ative essa nova partição de “swap”:

```
2# swapon /dev/sdb3
```

- Para visualizar as partições swaps ativas:

```
3# cat /proc/swaps
4# swapon -s
```

4LINUX 10

A SWAP é o tipo de partição utilizada para fornecer suporte a memória virtual ao GNU/Linux em adição a memória RAM instalada no sistema. Somente os dados na memória RAM são processados pelo processador, por ser mais rápida. Desta maneira quando você estiver executando um programa e a memória RAM começar a encher, o GNU/Linux moverá automaticamente os dados que não estão sendo utilizados para a partição Swap e libera a memória RAM para continuar carregando os dados necessários pelo programa. Quando os dados movidos para a partição Swap são solicitados, o GNU/Linux move os dados da partição Swap para a Memória. Por este motivo a partição Swap também é chamada de Área de Troca ou memória virtual. A velocidade em que os dados são movimentados da memória RAM para a partição é muito alta.

Gerenciamento Avançado de Partições

Servidor: Webserver Interno

Montagem automática no boot

- Para desabilitar a partição swap:

```
1# swapoff /dev/sdb3
```

- Para visualizar as partições swaps ativas:

```
2# swapon -s
```

- Dê um nome para a nova partição SWAP:

```
3# mkswap -L SWAP /dev/sdb3
```

O comando swapon tem a opção -p que habilita a prioridade:

-p, --priority <nº>

Quanto maior o número maior a prioridade que pode variar entre 0 e 32767.

Gerenciamento Avançado de Partições

Servidor: Webserver Interno

Montagem automática no boot

- Abra o arquivo /etc/fstab e adicione a linha do SWAP

```
1# vim /etc/fstab
....
LABEL=SWAP  none        swap    sw     0       0
```

- Desabilite a SWAP do novo dispositivo e teste a configuração

```
2# swapoff /dev/sdb3
3# mount -a
```

- Para visualizar as partições swaps ativas:

```
4# swapon -s
```

4LINUX 12

Relembrando …

As informações nas colunas do arquivo /etc/fstab são:

1° Coluna: Localização do “filesystem”

2° Coluna: Ponto de montagem;

3° Coluna: Tipo do filesystem:

4° Coluna: Opções de montagem:

5° Coluna: Aceita os valores 0 ou 1 e informa que, havendo um sistema de backup (dump) configurado, deverá ser feito o seu backup;

6° Coluna: Aceita os valores de 0 a 2 e informa que deverá ser realizada a checagem (pass) de integridade do sistema de arquivos. O valor zero desativa a funcionalidade, o valor 1 deve ser especificado apenas para o “/” e o valor 2 deve ser especificado para quaisquer outros sistemas de arquivo.

Gerenciamento Avançado de Partições

Servidor: Webserver Interno

Mostrar o uso de memória RAM:

- O comando “free” mostra o consumo de memória “RAM” e os detalhes sobre uso de memória virtual (SWAP):

```
1# free
```

- Execute o comando para obter mais detalhes:

```
2# free -m
```

- Você pode olhar os arquivos do /proc também:

```
3# less /proc/meminfo
4# less /proc/swaps
```

Gerenciamento Avançado de Partições

Gerenciar partições criptografadas na máquina Linux Interna:

- cryptsetup:
  - LuksOpen, LuksClose;
- cryptdisks_start;
- cryptdisks_stop;
- cryptdisks:
  - start, stop, restart.

Para manipular partições criptografas, vamos utilizar o LUKS (Linux Unified Key Setup) que fornece um padrão de formato de disco para partições criptografadas, e facilita a compatibilidade entre distribuições. Este padrão permite a múltiplos usuários/senhas, a revogação efetiva de senha e fornece segurança adicional contra ataques de baixa entropia.

Gerenciamento Avançado de Partições

Servidor: Máquina Linux Interna

Gerenciar partições criptografadas:

- Para ter suporte ao recurso de partições criptografadas é necessário instalar na máquina **Linux Interna**:

```
1# aptitude install cryptsetup -y
```

- Carregue os módulos através do comando modprobe:

```
2# modprobe dm_crypt
3# modprobe dm_mod
```

- Liste os módulos carregados através do comando lsmod:

```
4# lsmod | grep dm
```

4LINUX 15

Se vamos criptografar uma partição que já está montada e já contém dados, temos que fazer um Backup pois na construção do sistema de criptografia, os dados serão perdidos. Caso seja uma partição que ainda não contenha dados esse procedimento é mais tranquilo. Como exemplo utilize alguma partição sem nenhum sistema de arquivo aplicado.

Antes de podermos abrir uma partição encriptada precisamos inicializá-la. Este procedimento sera feito através do comando cryptsetup, que gerencia partições criptografas, permitindo operações de criação, remoção, redimensionamento e status.

Gerenciamento Avançado de Partições

Servidor: Máquina Linux Interna

Criar partições criptografadas:

- Utilize o comando cryptsetup na partição /dev/sdb1:

```
1# cryptsetup -y --cipher aes-cbc-essiv:sha256 --key-size 256
luksFormat /dev/sdb1


Are you sure? (Type uppercase yes): YES (Digite YES)
Enter LUKS passphrase: (Digite uma frase secreta)
Verify passphrase: (Repita a frase secreta)
```

- Nesse momento outros módulos de criptografia foram ativados:

```
2# lsmod | grep aes
```

4LINUX 16

Descrição dos parâmetros:

-y ou --verify-passphrase: Faz a checagem da senha digitada;

--cipher: Define qual é o modo de criptografia que o dispositivo vai usar;

--key-size: Define em bits o tamanho da chave de criptografia;

LuksFormat: Indica que o dispositivo vai utilizar o padrão LUKS. s de criação, remoção, redimensionamento e status.

Gerenciamento Avançado de Partições

Servidor: Máquina Linux Interna

Criar mapeamentos para partições LUKS:

- Agora que aplicamos o padrão LUKS na partição, podemos criar um mapeamento Device-Mapper através do opção luksOpen. Sera solicitada a frase secreta para continuar:

```
1# cryptsetup luksOpen /dev/sdb1 cryptfs
```

- Use o comando blkid para identificar dispositivos “crypt_LUKS”.

```
2# blkid | grep sdb1
```

Com a opção luksOpen nosso dispositivo /dev/sdb1 foi mapeado para /dev/mapper/cryptfs, e a partir de agora só pode ser acessado por por este caminho!

Gerenciamento Avançado de Partições

Servidor: Máquina Linux Interna

Aplicar sistema de arquivos e Montagem

- Antes de montar a partição criptografada é preciso aplicar um sistema de arquivos através do comando mkfs:

```
1# mkfs -t ext4 /dev/mapper/cryptfs
```

- Faça a montagem da partição através do comando mount:

```
2# mkdir /mnt/seguro
3# mount -t ext4 /dev/mapper/cryptfs /mnt/seguro
```

- Não esqueça de configurar uma nova entrada no /etc/fstab:

```
4# vim /etc/fstab
/dev/mapper/cryptfs /mnt/seguro ext4 defaults 0 2
```

4LINUX 18

Quando estamos manipulando partições criptografadas não basta apenas acrescentar a partição ao /etc/fstab, é preciso configurar mais um arquivo, o /etc/crypttab.

```
# vim /etc/crypttab
<target name>  <source device>  <key file>   <options>
cryptfs        /dev/sdc1        none         luks
```

Descrição dos parâmetros:

<target name>: Define o nome que a partição sera mapeada;
<source device>: Define o nome real da partição;
<key file>: Define a frase secreta, use none para nenhum;
<options>: Ativa o dispositivo com extensões LUKS.

Gerenciamento Avançado de Partições

Servidor: Máquina Linux Interna

Testando o funcionamento

- Para testar o funcionamento sem precisar reiniciar desmonte a partição:

```
1# umount /mnt/seguro
```

- E desative o dispositivo criptografado

```
2# cryptsetup luksClose cryptfs
```

- Inicie o script cryptdisks e sera solicitado a frase secreta.

```
3# /etc/init.d/cryptdisks start
```

Toda vez que o computador for iniciado ou este disco montando em outras maquinas, sera solicitada a frase secreta!

Gerenciamento Avançado de Partições

Servidor: Máquina Linux Interna

Montagem manual de partições criptografas

- Altere a opção “NO” para “YES” da diretiva “CRYPTDISKS_ENABLE” no arquivo /etc/default/cryptdisks:

```
1# vim /etc/default/cryptdisks
CRYPTDISKS_ENABLE=NO
```

- Um outro comando para ativar de forma manual é carregar o módulo dm_crypt no boot

```
2# echo dm_crypt >> /etc/modules
```

4LINUX 20

Como desativar as partições criptografadas durante o boot?

A ativação automática durante o boot em um servidor não é uma boa pratica de administração, pois acaba atrasando a inicialização do serviços. A solução é alterar a opção “NO” para “YES” da diretiva “CRYPTDISKS_ENABLE” no arquivo /etc/default/cryptdisks:

Para ativar de forma manual é só usar o comando cryptdisks_start e o nome mapeado da partição. Mas ainda não vai funcionar porque como desativamos o cryptdisks do boot, o modulo “dm_crypt” não sera carregado. Este módulo é responsável em fazer o mapeamento de dispositivos criptografados.

Gerenciamento Avançado de Partições

Servidor: Máquina Linux Interna

Como configurar automount

- Para começar instale o pacote autofs5

```
1# aptitude install autofs5 -y
```

- Para testar o automount comece criando uma configuração para o ponto de montagem /dexter/montagem:

```
2# vim /etc/auto.master
/mnt/montagem  /etc/auto.dexter     --timeout=10
```

4LINUX 21

Como configurar automount no sistema?

Esta pratica pode ser feita através do pacote autofs5, usado para controlar a operação dos "daemons" de auto montagem. Os "daemons" de auto montagem automaticamente montam sistemas de arquivos quando eles são usados e desmontados após um período de inatividade.

Ao instalar o autofs5 sera criado o arquivo /etc/auto.master que é consultado para configurar o automount e os pontos de montagem, gerenciados quando o script autofs é invocado, ou o programa de montagem quando executado de forma automática.

Gerenciamento Avançado de Partições

Servidor: Máquina Linux Interna

Como configurar automount

- Agora vamos criar o arquivo com as opções de montagem:

```
1# vim /etc/auto.dexter
dexter   -fstype=ext4,rw   :/dev/sdb1
```

- Para testar reinicie o serviço autofs.

```
2# /etc/init.d/autofs restart
```

- Para testar acesse o diretório /mnt/montagem/dexter e use o comando df para listar a partição montada de forma automática:

```
3# cd /mnt/montagem/dexter
4# df -Th
```

4LINUX 22

Descrição das opções do arquivo auto.master:

/mnt/montagem: Define em qual diretório sera executado o automout;
/etc/auto.dexter: Qual arquivo sera configurado as opções de montagem;
--timeout: Tempo de desmontagem automática. Executado quando nenhum processo ou usuário estiver usando o diretório.

Descrição das opções do arquivo auto.dexter:

dexter: Define qual diretório sera montado em /mnt/montagem de forma automática;
-fstype: Define as opção de montagem da partição;
/dev/sdb2: Define o dispositivo que sera montado.

Gerenciamento Avançado de Partições

Servidor: Máquina Linux Interna

Criar automount para partições criptografadas

- Comece criando uma configuração para o ponto de montagem /mnt/seguro:

```
1# vim /etc/auto.master
/mnt  /etc/auto.crypt      --timeout=10
```

- Agora vamos criar o arquivo com as opções de montagem:

```
2# vim /etc/auto.crypt
seguro   -fstype=ext4,rw   :/dev/mapper/cryptfs
```

Anotações:

Gerenciamento Avançado de Partições

Servidor: Máquina Linux Interna

Criar automount para partições criptografadas

- Comece criando uma configuração para o ponto de montagem /mnt/seguro:

```
1# vim /etc/fstab
###/dev/mapper/cryptfs    /mnt/seguro ext4
noauto,defaults 0  0
2# /etc/init.d/autofs restart
```

- Para testar acesse o diretório /mnt/seguro e use o comando df para listar a partição montada de forma automática:

```
3# cd /mnt/seguro
4# df -Th
```

Anotações:

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!

Anotações:

Curso 450

Linux Fundamentals in Cloud

Versão 2015_3.0