4450 – Linux Fundamentals in Cloud

Laboratório: Gerenciamento Avançado de Partições

Pré-Requisito para o Laboratório 12:

- Você precisa estar logado com o usuário root;
- Para iniciar o Laboratório execute o startdexterlab-12;
- Os comandos abaixo devem ser executados antes de começar as tarefas e são fundamentais para que a correção automática funcione corretamente:

  # startdexterlab-12

  # history -c

Laboratório 12:

Execute as tarefas abaixo somente na máquina **Practice Lab Debian** do curso Linux Fundamentals in Cloud:

O servidor da empresa Dexter necessita proteger documentos de auditoria armazenados em /dexter/auditoria, mas o diretório onde os arquivos estão armazenados não possui uma partição criptografada. Para que esta infraestrutura tenha sucesso é preciso adicionar um novo disco criptografado no servidor, e fazer uma migração dos documentos da auditoria para o novo ponto de montagem criptografado. Use seus conhecimentos em gerenciamento avançado em partições executando as seguintes tarefas:

01 – Instale o **pacote cryptsetup e carregue os módulos** “dm_crypt” e “dm_mod ”:

```
# aptitude install cryptsetup
# modprobe dm_crypt
# modprobe dm_mod
```

02 – Adicione um novo disco (/dev/sdc) com 1 **partição encriptada** de 5GB**,** com **chave de 256 bits** e a frase secreta “curso-455”:

```
# fdisk -l /dev/sdc
# fdisk /dev/sdc
Command: n
Command action: p
Partition number: 1
First cylinder: ENTER
Last cylinder: +5G
Command: w

# partprobe
# cryptsetup -y --cipher aes-cbc-essiv:sha256 --key-size 256 luksFormart /dev/sdc1
Are you sure: YES
```

03 – Crie o **mapeamento** de nome “auditoria” para a partição encriptada:

```
# cryptsetup luksOpen /dev/sdc1 auditoria
```

04 – **Filtre** somente partição encriptada e verifique se a mesma apresenta o tipo "crypto_LUKS":

```
# blkid | grep sdc1 | grep crypto_LUKS
```

05 – **Configure o mapeamento** da partição criptografada para ser ativada no boot:

```
# echo "auditoria /dev/sdc1 none luks" >> /etc/crypttab
```

06 – **Desative e Ative de forma manual** a partição, para testar a frase secreta:

```
# cryptdisks_stop auditoria
# cryptdisks_start auditoria
```

07 – Aplique o **sistema de arquivos** ext4 na partição, crie o **ponto de montagem** /media/auditoria e **monte** a partição criptografada. Faça a cópia de todo o conteúdo do diretório /dexter/auditoria para /media/auditoria:

```
# mkfs -t ext4 /dev/mapper/auditoria
# mkdir /media/auditoria
# mount -t ext4 /dev/mapper/auditoria /media/auditoria
# cp -r /dexter/auditoria /media/auditoria
```

08 – Configure o sistema para que durante a inicialização **NÃO seja solicitada a frase secreta** para ativar a partição criptografada:

```
# sed -i 's/CRYPTDISKS_ENABLE=Yes/CRYPTDISKS_ENABLE=NO/g' /etc/default/cryptdisks
```

09 – Crie a **configuração de automount** para **/media/auditoria** com **15 segundos** como tempo de desmontagem automática, apontando a configuração para **/etc/auto.auditoria:**

```
# vim /etc/auto.master
/media/auditoria /etc/auto.auditoria –timeout=15
```

10 – **Configure as opções de montagem** em /etc/auto.auditoria para o automount da partição criptografada que está mapeada em **/dev/mapper/auditoria**:

```
# vim /etc/auto.auditoria
auditoria -fstype=ext4,rw :/dev/mapper/auditoria
```

- Após concluir o laboratório execute o comando `history -w;`
- Para executar a autocorreção use o comando `# dexterlab-12`
- Para refazer o laboratório execute o comando `# recoverylab-12`

Para cada tarefa correta será computado 1 ponto. Se não atingir a nota máxima, você pode repetir o laboratório e corrigir novamente.

Caso tenha alguma dificuldade não esqueça de postar sua dúvida no Fórum Socorro Monitor.