



LUKS
Linux Unified Key Setup

Instalando o Debian em disco criptografado com LUKS



Debian Day
Brasil 2023

Thiago Andrade - 17 Ago 23



30
years
debian

SUMÁRIO

O que é LUKS

Por que utilizar LUKS?

Instalação do Debian 12 com LUKS - prática

Criando partições e criptografando o disco - prática

Conclusão

SUMÁRIO

O que é LUKS

Por que utilizar LUKS?

Instalação do Debian 12 com LUKS - prática

Criando partições e criptografando o disco - prática

Conclusão

O QUE É LUKS (Linux Unified Key Setup)



- Especificação de criptografia de disco criada por Clemens Fruhwirth em 2004, originalmente destinada ao Kernel Linux.
- **Implementada pelo módulo de Kernel dm-crypt.**
- Administrada no Debian pelo conjunto de ferramentas do pacote cryptsetup



```
# apt install cryptsetup
```

O QUE É LUKS (Linux Unified Key Setup)



- LUKS é o padrão para criptografia de disco do Linux. Ao fornecer um formato padronizado em disco, não só facilita a compatibilidade entre as distribuições, mas também permite o gerenciamento seguro de várias passphrases de usuário.
- O LUKS armazena todas as informações de configuração necessárias no cabeçalho da partição, que permite aos usuários transportar ou migrar dados sem problemas.

SUMÁRIO

O que é LUKS

Por que utilizar LUKS?

Instalação do Debian 12 com LUKS - prática

Criando partições e criptografando o disco - prática

Conclusão

POR QUE UTILIZAR LUKS?



- Por ser software livre, estar empacotado no Debian e fazer parte do Instalador do Debian.
- Para dificultar que pessoas má intencionados leiam seus arquivos pessoais (casa / trabalho).
- Utiliza por padrão criptografia 'forte' aes-xts-plain64 com chave de 512 bits.
- Pode criptografar todo o disco, inclusive o swap, com exceção da partição que contêm o initrd (bootloader).

POR QUE UTILIZAR LUKS?



- Permite que os usuários incluam chaves ou passphrases de backup, o padrão LUKS2 suporta 32 slots de chave enquanto o LUKS1 suporta 8 slots.
- É compatível com LVM (Logical Volume Management) e RAID.
- É compatível com APPLE MACOS FILEVAULT2 e com WINDOWS BITLOCKER.

SUMÁRIO

O que é LUKS

Por que utilizar LUKS?

Instalação do Debian 12 com LUKS - prática

Criando partições e criptografando o disco - prática

Conclusão

INSTALAÇÃO DO DEBIAN 12 COM LUKS

© debian 12

Debian GNU/Linux installer menu (BIOS mode)

Graphical install

Install

Advanced options >

Accessible dark contrast installer menu >

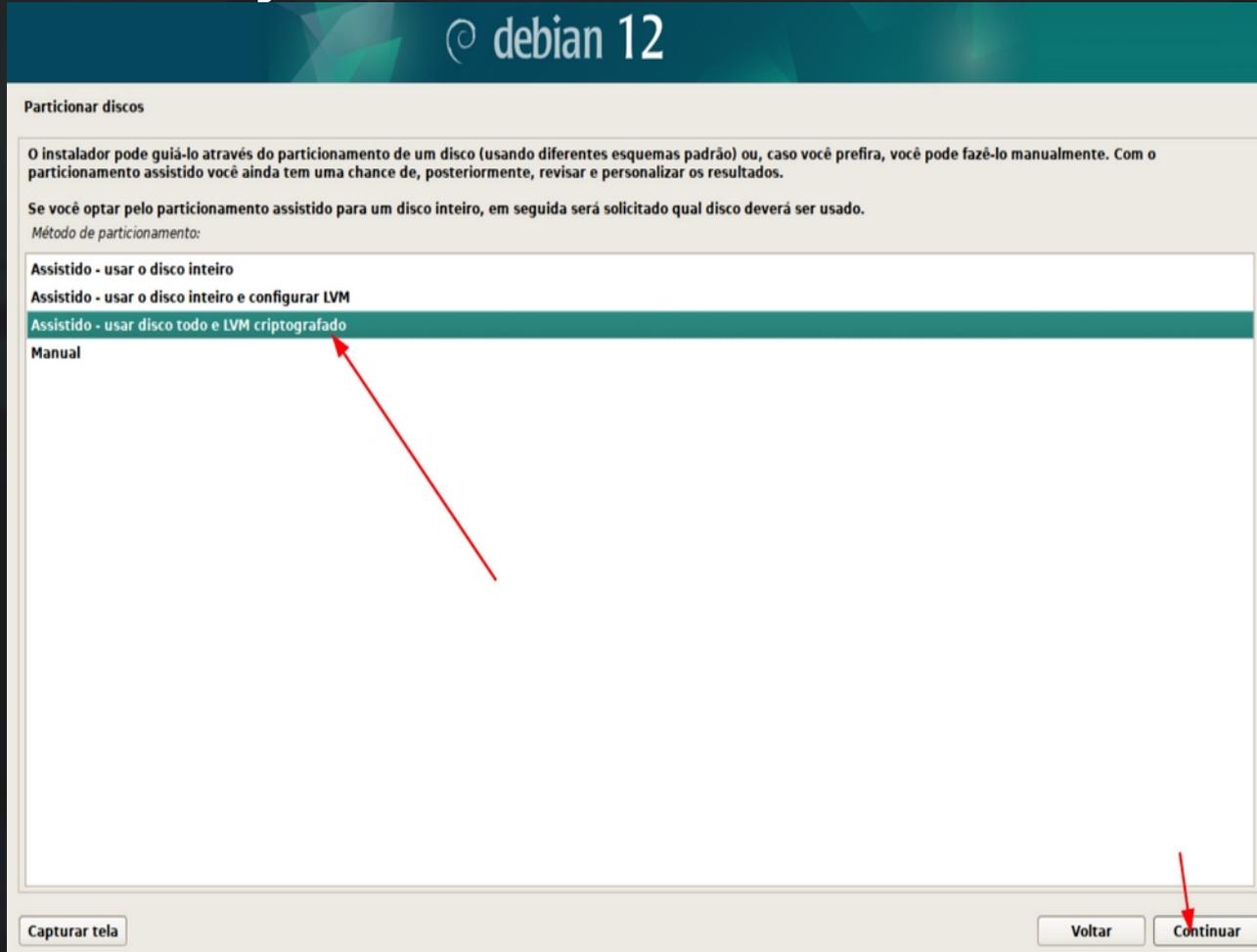
Help

Install with speech synthesis

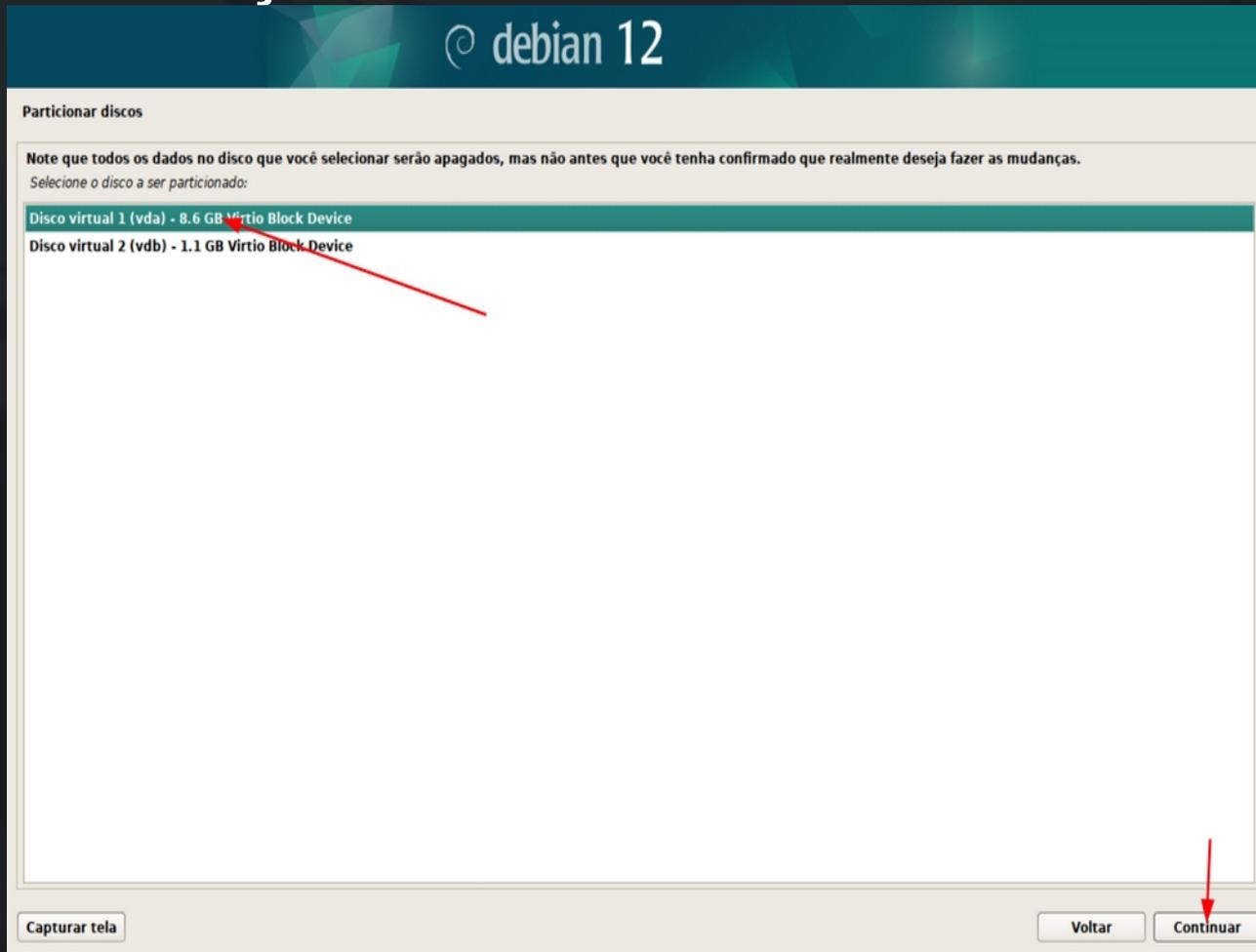
Press a key, otherwise speech synthesis will be started in 27 seconds...



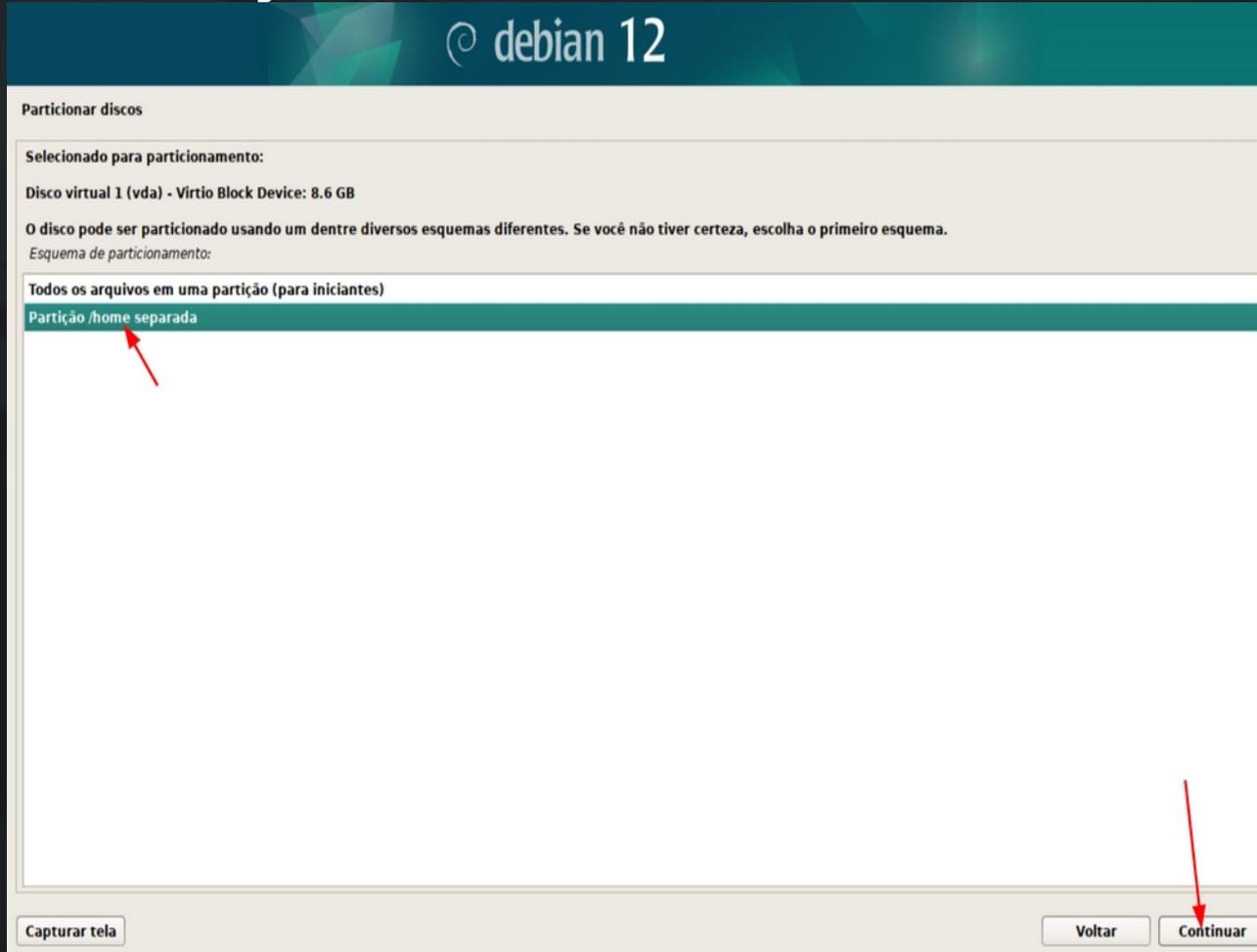
INSTALAÇÃO DO DEBIAN 12 COM LUKS



INSTALAÇÃO DO DEBIAN 12 COM LUKS



INSTALAÇÃO DO DEBIAN 12 COM LUKS



INSTALAÇÃO DO DEBIAN 12 COM LUKS

© debian 12

Particionar discos

Antes que o Gerenciador de Volumes Lógicos possa ser configurado, o esquema de particionamento atual precisa ser gravado em disco. Essas mudanças não poderão ser desfeitas.

Depois que o Gerenciador de Volumes Lógicos for configurado, nenhuma mudança adicional no esquema de particionamento dos discos que contém os volumes físicos será permitida durante a instalação. Por favor, decida se você está satisfeito com o esquema de particionamento atual antes de continuar.

As tabelas de partição dos dispositivos a seguir foram mudadas:
Disco virtual 1 (vda)

As seguintes partições serão formatadas:
partição #1 de Disco virtual 1 (vda) como ext2

Gravar as mudanças nos discos e configurar LVM?

Não

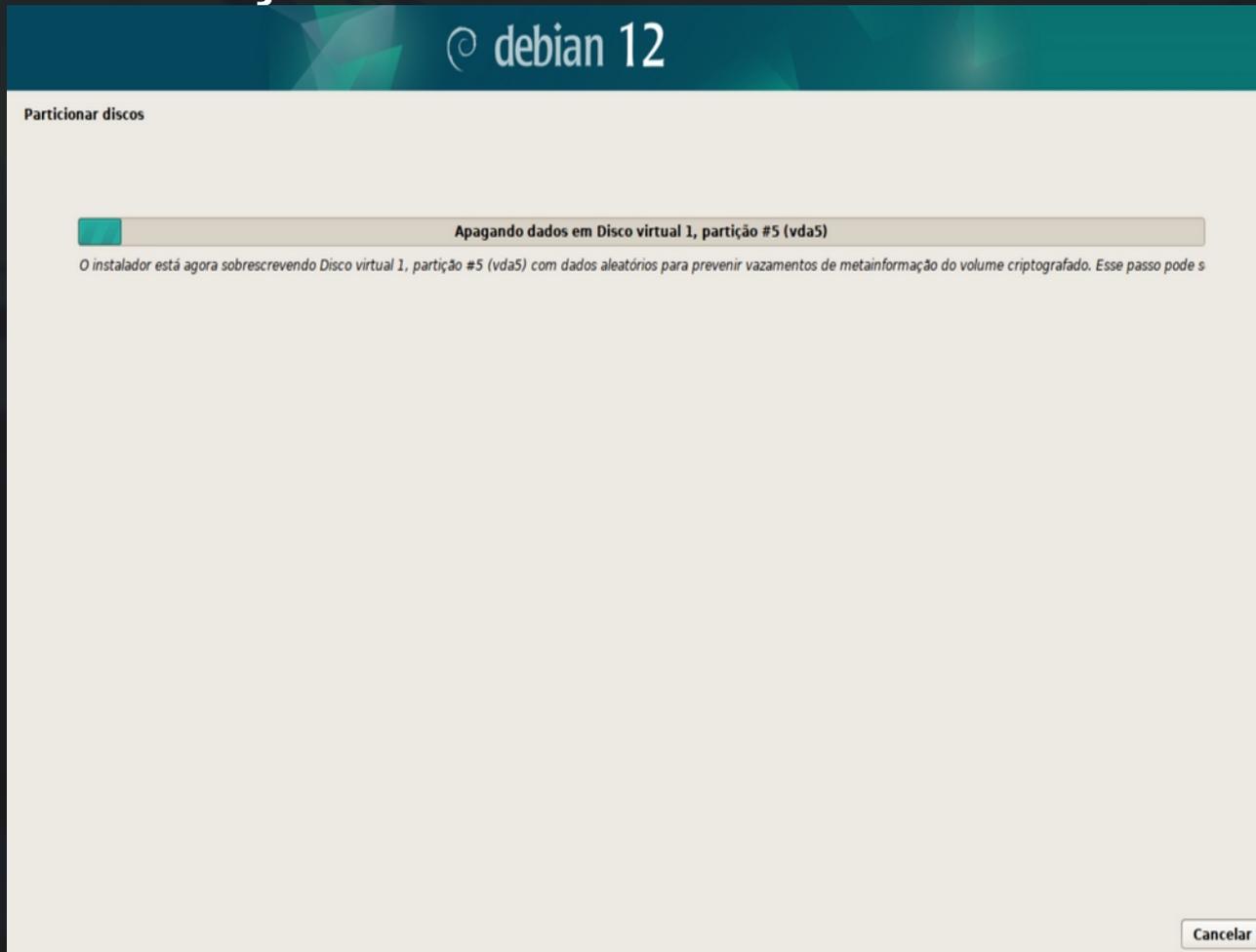
Sim

Capturar tela

Continuar



INSTALAÇÃO DO DEBIAN 12 COM LUKS



INSTALAÇÃO DO DEBIAN 12 COM LUKS

© debian 12

Particionar discos

Você precisa escolher uma frase secreta para criptografar Disco virtual 1, partição #5 (vda5).

A força geral da criptografia depende fortemente dessa frase secreta, portanto você deve tomar o cuidado de escolher uma frase secreta que não seja fácil de ser adivinhada. A mesma não deverá ser uma palavra ou uma sentença encontradas em dicionários ou mesmo uma frase que possa ser facilmente associada a você.

Uma boa frase secreta contém uma mistura de letras, números e sinais de pontuação. **É recomendado que frases secretas tenham um tamanho igual ou superior a 20 caracteres.**

Frase secreta criptográfica:

Mostrar a senha

Por favor, informe a mesma frase secreta novamente para verificar se você a digitou corretamente.

Informe a frase secreta novamente para verificação:

Mostrar a senha

Capturar tela

Voltar Continuar



INSTALAÇÃO DO DEBIAN 12 COM LUKS

© debian 12

Particionar discos

Você pode usar todo o grupo de volumes, ou apenas parte dele, no particionamento guiado. Se você usar apenas parte dele, ou adicionar mais discos depois, então você será capaz de aumentar os volumes lógicos posteriormente usando as ferramentas LVM, assim, usar uma pequena parte do grupo de volumes na hora da instalação pode oferecer mais flexibilidade.

O tamanho mínimo para a receita de particionamento selecionada é 3.5 GB (ou 43%). Por favor, note que os pacotes que você escolheu para instalar podem requerer mais espaço que isso. O tamanho máximo disponível é 8.1 GB.

Dica: "max" pode ser usado como um atalho para especificar o tamanho máximo, ou informe uma porcentagem (e.g. "20%") para usar essa porcentagem do tamanho máximo.
Quantidade do grupo de volumes para usar no particionamento guiado:

Capturar tela

Voltar Continuar



INSTALAÇÃO DO DEBIAN 12 COM LUKS

© debian 12

Particionar discos

Esta é uma visão geral de suas partições e pontos de montagem atualmente configurados. Selecione uma partição para modificar suas configurações (sistema de arquivos, ponto de montagem, etc), um espaço livre onde criar partições ou um dispositivo no qual inicializar uma tabela de partições.

Particionamento assistido

- Configurar RAID via software
- Configurar o Gerenciador de Volumes Lógicos
- Configurar volumes criptografados
- Configurar volumes iSCSI

▽ VG LVM debian-vg, LV home - 4.0 GB Linux device-mapper (linear)

>	#1	4.0 GB	f	ext4	/home
---	----	--------	---	------	-------

▽ VG LVM debian-vg, LV root - 3.0 GB Linux device-mapper (linear)

>	#1	3.0 GB	f	ext4	/
---	----	--------	---	------	---

▽ VG LVM debian-vg, LV swap_1 - 1.0 GB Linux device-mapper (linear)

>	#1	1.0 GB	f	swap	swap
---	----	--------	---	------	------

▽ Volume criptografado (vda5_crypt) - 8.1 GB Linux device-mapper (crypt)

>	#1	8.1 GB	K	lvm	
---	----	--------	---	-----	--

▽ Disco virtual 1 (vda) - 8.6 GB Virtio Block Device

>	#1	primária	510.7 MB	F	ext2	/boot
>	#5	lógica	8.1 GB	K	crypto	(vda5_crypt)

Disco virtual 2 (vdb) - 1.1 GB Virtio Block Device

Desfazer as mudanças nas partições

Finalizar o particionamento e escrever as mudanças no disco

Capturar tela Ajuda Voltar Continuar



INSTALAÇÃO DO DEBIAN 12 COM LUKS

© debian 12

Particionar discos

Se você continuar, as mudanças listadas abaixo serão escritas nos discos. Caso contrário, você poderá fazer mudanças adicionais manualmente.

As seguintes partições serão formatadas:
VG LVM debian-vg, LV home como ext4
VG LVM debian-vg, LV root como ext4
VG LVM debian-vg, LV swap_1 como swap

Escrever as mudanças nos discos?

Não

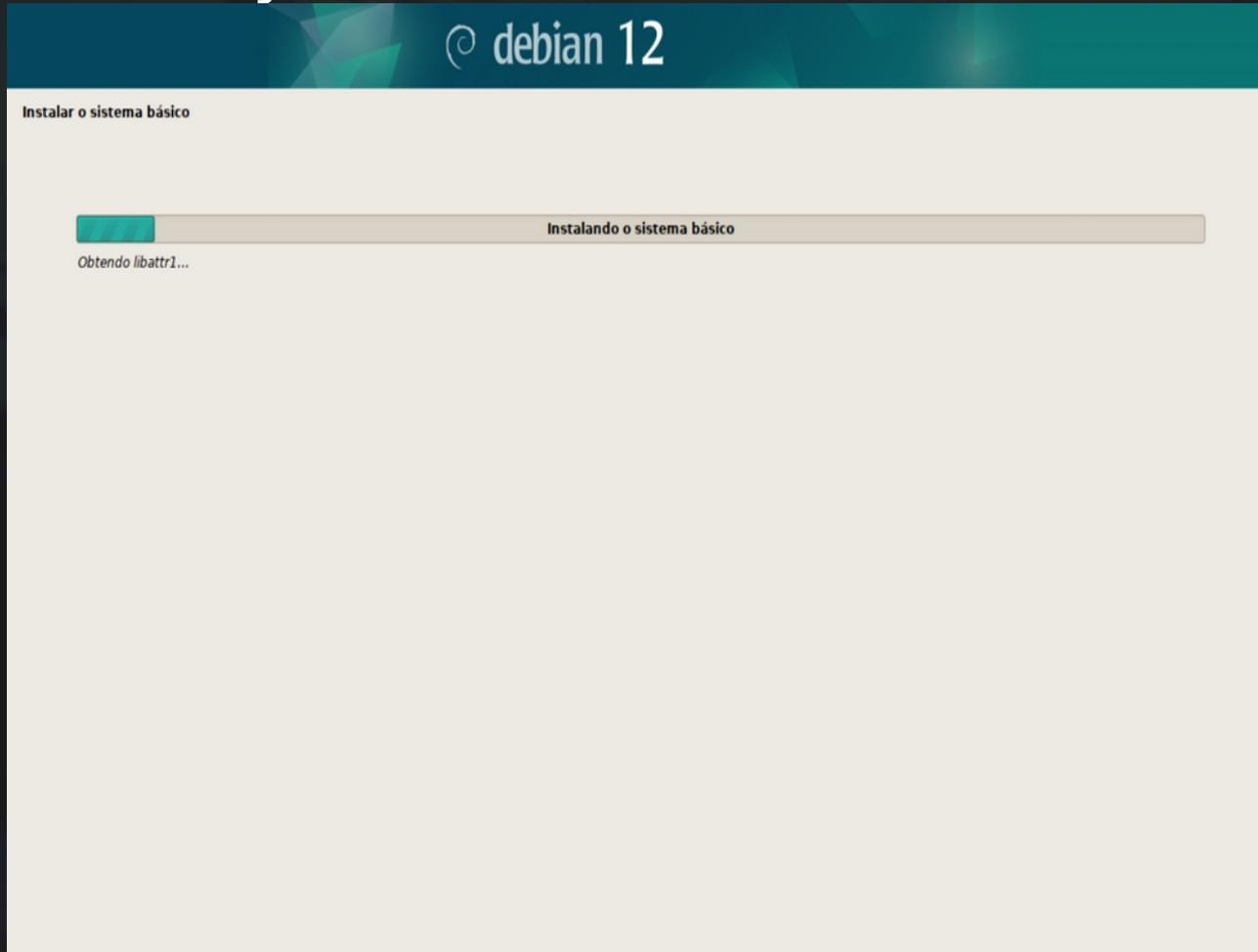
Sim

Capturar tela

Continuar



INSTALAÇÃO DO DEBIAN 12 COM LUKS



INSTALAÇÃO DO DEBIAN 12 COM LUKS

```
root@debian:~# lsblk
```

NAME	MAJ:MIN	RM	SIZE	RO	TYPE	MOUNTPOINTS
sr0	11:0	1	3.7G	0	rom	
vda	254:0	0	8G	0	disk	
├─vda1	254:1	0	487M	0	part	/boot
├─vda2	254:2	0	1K	0	part	
├─vda5	254:5	0	7.5G	0	part	
└─vda5_crypt	253:0	0	7.5G	0	crypt	
├─debian--vg-root	253:1	0	2.8G	0	lvm	/
├─debian--vg-swap_1	253:2	0	976M	0	lvm	[SWAP]
└─debian--vg-home	253:3	0	3.8G	0	lvm	/home
vdb	254:16	0	1G	0	disk	



SUMÁRIO

O que é LUKS

Por que utilizar LUKS?

Instalação do Debian 12 com LUKS - prática

Criando partições e criptografando o disco - prática

Conclusão

CRIANDO PARTIÇÕES E CRIPTOGRAFANDO O DISCO

Criação básica de partição com LUKS

```
apt install cryptsetup
lsblk
apt install hexyl
hexyl /dev/vdb | head
cryptsetup -v luksFormat /dev/vdb
hexyl /dev/vdb | head
cryptsetup open /dev/vdb pendrive-cripto
cryptsetup status pendrive-cripto
mkfs.ext4 /dev/mapper/pendrive-cripto
mkdir /mnt/pendrive
mount /dev/mapper/pendrive-cripto /mnt/pendrive/
touch lista
echo "arquivo de teste luks" >> lista
```

CRIANDO PARTIÇÕES E CRIPTOGRAFANDO O DISCO

Automatizar o processo de montagem

```
vi /etc/crypttab  
pendrive-cripto /dev/vdb none luks,discard  
  
vi /etc/fstab  
/dev/mapper/pendrive-cripto /mnt/pendrive ext4 defaults 0 0  
  
reboot
```

CRIANDO PARTIÇÕES E CRIPTOGRAFANDO O DISCO

Criando uma chave para montagem automática do bloco

```
dd if=/dev/urandom of=/root/key bs=4096 count=1
cryptsetup luksAddKey /dev/vdb /root/key
chmod 000 /root/key
vi /etc/crypttab
pendrive-cripto /dev/vdb /root/key luks,discard

reboot e verificar a partição montada
```

SUMÁRIO

O que é LUKS

Por que utilizar LUKS?

Instalação do Debian 12 com LUKS - prática

Criando partições e criptografando o disco - prática

Conclusão

CONCLUSÃO

- Instalar o Debian / Linux GNU com criptografia é simples e deve ser realizado sempre que possível.
- **A criptografia não substitui backup!**
- Fazer backup do HEADER da partição LUCKS é uma boa prática de segurança dos seus dados.

```
# cryptsetup luksHeaderBackup /dev/DEVICE --header-backup-file /path/to/backup
```

```
# cryptsetup luksHeaderRestore /dev/DEVICE --header-backup-file /path/to/backup
```

REFERÊNCIAS

- <https://gitlab.com/cryptsetup/cryptsetup/>
- https://gitlab.com/cryptsetup/LUKS2-docs/blob/main/luks2_doc_wip.pdf
- https://en.wikipedia.org/wiki/Linux_Unified_Key_Setup
- https://wiki.archlinux.org/title/dm-crypt/Device_encryption
Benchmark do disco criptografado
- <https://www.phoronix.com/review/ubuntu-1804-encrypt>

Palestra disponível em <https://andrade.wiki.br/palestras/>



Debian Day
Brasil 2023



Debian
Brasil



Andrade - Ago 23