

EXEMPLO DE

IMPLANTAÇÃO E
INSTALAÇÃO



Kiraz Log Forensic

V1.17-R25-MINER

Topologia

L1-L2

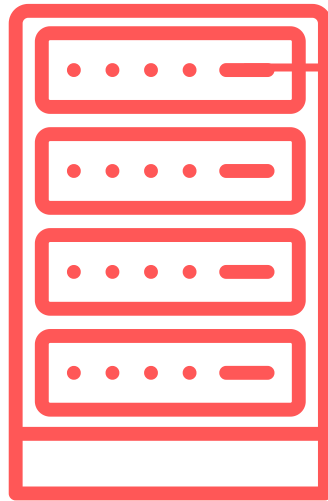
Na sua borda de rede você terá algo semelhante a isso:

Exemplo: ISP-1000

- 4 Núcleo
- 4GB RAM
- 50GB HD - Sistema
- 200GB HD - Logs

Importante: HD Logs deve ser adicionado na sua VM e não particionar sistema e guarda de logs em um único HD. Se seu server de VM tiver capacidade de receber HD externo como HD USB você pode atachar a sua VM.

KIRAZ - VM



R1



BGP



Operadora
Link



Kiraz Log Forense

V1.17-R25-MINER

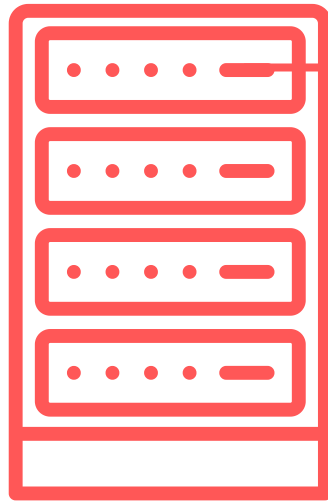
Topologia

L3

Roteamento e IPs vamos focar apenas no [R1 vs Kiraz]:

Vamos considerar nesse cenário que você tem um server de VM, podendo por exemplo ser um xenserver, ou proxmox, e que criamos uma vlan100 na eth2 do router interligando com a eth0 placa de rede do server VM onde estará a vlan100 para vincular ao Kiraz.

KIRAZ - VM



eth0/vlan100 - IP: 172.31.0.2/30

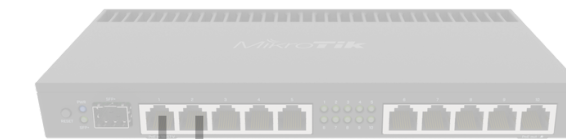
R1



eth2/vlan100 - IP: 172.31.0.1/30

Operadora
Link

BGP



Atenção: Certifique de ter internet sobre esse IP ou da sua escolha para poder continuar as próximas etapas.



Kiraz Log Forensense

V1.17-R25-MINER

Configurar pelo menos uma interface que este servidor possa usar para se comunicar com outras máquinas e que, de preferência, forneça acesso suficiente para atualizações.

NAME	TYPE	NOTES
[eth0	eth	-
desativado	autoconfiguration failed	
6a:89:ad:1e:3e:25 / Unknown Vendor / Unknown Model		

[Criar limite ▶]

Edit eth0 IPv4 configuration

Método IPv4: [Manual ▼]

Subnet: 172.31.0.0/30

Endereço: 172.31.0.2

Gateway: 172.31.0.1

Nomear de servidores: 8.8.8.8, 8.8.4.4

IP addresses, comma separated

Procurar em domínios:

Domains, comma separated

[Guardar]

[Cancelar]

Após digitar os IPs e dns ir em
Save (Guardar) e abaixo aparecerá **Done** (Feito).

[Continuar sem rede]
[Voltar]

Aplicação do IPv4



Configure a guided storage layout, or create a custom one:

☒ Use an entire disk

[/dev/xvda local disk 20.000G ▼]

Escolha o HD (disk) para o sistema.

☒ Set up this disk as an LVM group

☐ Encrypt the LVM group with LUKS

Passphrase:

Confirm passphrase:

☐ Also create a recovery key

The key will be stored as ~/recovery-key.txt in the live system
and will be copied to /var/log/installer/ in the target system.

☐ Custom storage layout

[Done]
[Back]

Configuração HD - Sistema



Configuração HD - Sistema

FILE SYSTEM SUMMARY

MOUNT POINT	SIZE	TYPE	DEVICE TYPE
[/	10.000G	new ext4	new LVM logical volume ▶]
[/boot	1.771G	new ext4	new partition of local disk ▶]

AVAILABLE DEVICES

DEVICE	TYPE	SIZE
[ubuntu-vg (new)	LVM volume group	18.222G ▶]
free space		8.222G ▶]

[Create software RAID (md) ▶]
[Create volume group (LVM) ▶]

USED DEVICES

DEVICE	TYPE	SIZE
[ubuntu-vg (new)	LVM volume group	18.222G ▶]
ubuntu-lv	new, to be formatted as ext4, mounted at /	10.000G ▶]

[/dev/xvda

	TYPE	SIZE
partition 1	new, BIOS grub spacer	1.000M ▶]
partition 2	new, to be formatted as ext4, mounted at /boot	1.771G ▶]
partition 3	new, PV of LVM volume group ubuntu-vg	18.225G ▶]

Agora precisamos entrar na ubuntu-lv e redimensionar o tamanho para o máximo dela.



FILE SYSTEM SUMMARY

MOUNT POINT	SIZE	TYPE	DEVICE TYPE
[/	10.000G	new ext4	new LVM logical volume ▶]
[/boot	1.771G	new ext4	new partition of local disk ▶]

AVAILABLE DEVICES

DEVICE	TYPE	SIZE
[ubuntu-vg (new)	LVM volume group	18.222G ▶]
free space		8.222G ▶

[Create software RAID (md) ▶]
[Create volume group (LVM) ▶]

USED DEVICES

DEVICE	TYPE	SIZE
[ubuntu-vg (new)	LVM volume group	18.222G ▶
ubuntu-lv	new, to be formatted as ext4, mounted at /	10.000G ▶

[/dev/xvda

partition	new, BIOS grub spacer	local disk	SIZE
1			20.000G ▶
2	new, to be formatted as ext4, mounted at /boot		1.000M ▶
3	new, PV of LVM volume group ubuntu-vg		1.771G ▶
			18.225G ▶

◀ (close)
Edit ▶
Delete ▶

Vamos em **edit** (Editar)



Configuração HD - Sistema

Configuração HD - Sistema

FILE SYSTEM SUMMARY

MOUNT POINT	SIZE	TYPE	DEVICE TYPE
[/	10.000G	new ext4	new LVM logical volume ▶]
[/boot	1.771G	new ext4	new partition of local disk ▶]

AVAILABLE DEVICES

DEVICE	TYPE	SIZE
[ubuntu-vg (new)	LVM volume group	18.222G ▶]
free space		8.222G ▶]

[Create so
[Create vo

USED DEVICE

DEVICE
[ubuntu-vg
ubuntu-lv

[/dev/xvda
partition
partition
partition

Editing logical volume ubuntu-lv of ubuntu-vg

Name: ubuntu-lv

Size (max 18.222G): 10.000G

Format: [ext4 ▼]

Mount: [/ ▼]

[Save]
[Cancel]

[Done]
[Reset]
[Back]

**E por fim vamos ir em
Save e depois em Done.**

**O exemplo acima o nosso HD sistema é
de 20Gb e ficou 50% “pra trás”. Agora
vamos digitar o Size (max) que aparece
ao lado do campo, no caso acima é
18.222G para sua instalação digitar o
max que aparecerá ao lado do campo.**



FILE SYSTEM SUMMARY

MOUNT POINT	SIZE	TYPE	DEVICE TYPE
[/	18.222G	new ext4	new LVM logical volume ▶]
[/boot	1.771G	new ext4	new partition of local disk ▶]

AVAILABLE DEVICES

No available devices

[Create software RAID (md) ▶]
[Create volume group (LVM) ▶]

USED DEVICES

DEVICE	TYPE	SIZE
[ubuntu-vg (new)	LVM volume group	18.222G ▶]
ubuntu-lv	new, to be formatted as ext4, mounted at /	18.222G ▶]
[/dev/xvda	local disk	20.000G ▶]
partition 1	new, BIOS grub spacer	1.000M ▶]
partition 2	new, to be formatted as ext4, mounted at /boot	1.771G ▶]
partition 3	new, PV of LVM volume group ubuntu-vg	18.225G ▶]

*Apenas fazer a conferencia e ir em **Done**.*

[Done]
[Reset]
[Back]

Configuração HD - Sistema



Configuração HD - Sistema

Selecting Continue below will begin the installation process and result in the loss of data on the disks selected to be formatted.

Are you sure you want to continue?

```
[ No ]
[ Continue ]
```

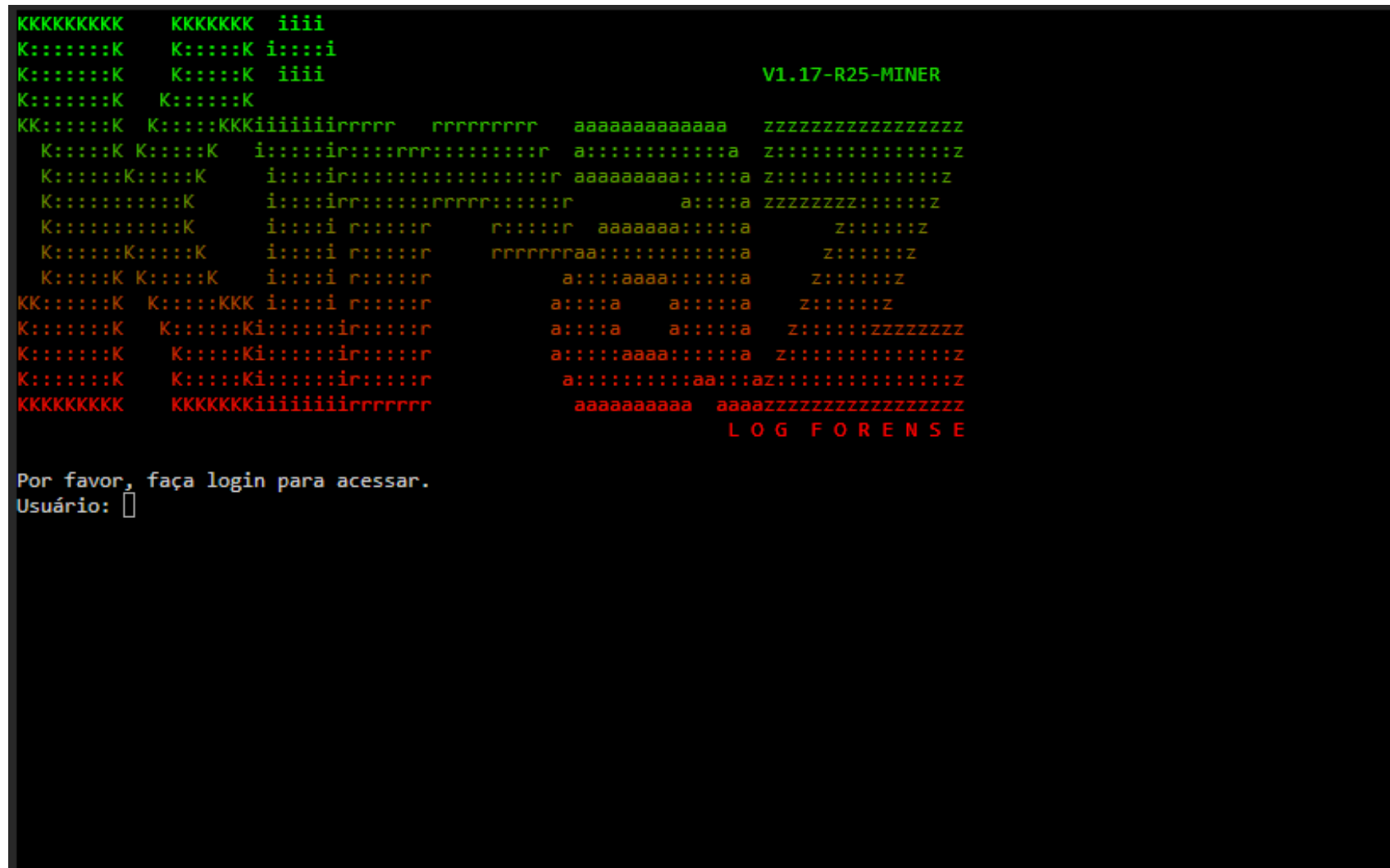
Agora ir em *Continue* para gravar as alterações em disco (disk).

A instalação daqui pra frente será toda automática.

Aguardar *Full Complete* no top da imagem e o “botão” *reboot* e estará finalizado.



Finalização



Após reiniciar você terá acesso via CLI Terminal, WCLI e WEB.

Solicite sua licença TRIAL ou definitiva pelo site www.kirazlogforense.com e nossa equipe entrará em contato para agendar seu treinamento.

