## IMPLANTAÇÃO E Instalação

## EXEMPLO DE



### Kiraz Log Forense

V1.17-R25-MINER

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



### KIRAZ - VM

Exemplo: ISP-1000

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

*Importante:* HD Logs deve ser adicionado na não VM е sua 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.



### Topologia L1-L2







### Edit ethO IPv4 configuration Método IPv4: 172.31.0.0/30 Subnet: 172.31.0.2 Endereço: 172.31.0.1 Gateway: 8.8.8.8, 8.8.4.4 Nomear de servidores: IP addresses, comma separated Procurar em domínios: [ Cancelar Após digitar os IPs e dns ir em (Guardar) e abaixo aparecerá Done (Feito). liraz Log Forense V1.17-R25-MINER



# Aplicação do IPv4





## **Configuração HD - Sistema**

### FILE SYSTEM SUMMARY

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

### AVAILABLE DEVICES

DEVICE ubuntu–vg (new) free space	TYPE LVM volume group	SIZE 18.222G 8.222G	► ] ►

Create	softwar	e RAID		
Create	volume	group	(LVM)	

### USED DEVICES

[	DEVICE ubuntu-vg ubuntu-lv	(ne	w) new,	to be form	natted	as (	ext4,	TYPE LVM volume mounted at	group /	SIZE 18.222G 10.000G
[	/dev/xvda partition partition	123	new, new,	BIOS grub to be form	spacer atted	as (	ext4,	local disk mounted at	∕boot	20.000G 1.000M 1.771G

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





Done Reset Back

# **Configuração HD - Sistema**



### Storage configuration

### FILE SYSTEM SUMMARY

MOUNT POINT		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) free space	LVM volume group	18.2220 8.2220

Create	softwar	e RAID		
Create	volume	group	(LVM)	

### USED DEVICES

[	DEVICE ubuntu-vg ubuntu-lv	(new) new,	to be formatted as ext4,	TYPE LVM volume group mounted at /	SIZE 18.222G 10.000G
[	/dev/xvda partition partition	1 new, 2 new,	BIOS grub spacer to be formatted as ext4,	local disk mounted at ∕boot	20.000G 1.000M 1.771G
	partition	3 new.	PV of LVM volume group ub	untu-vg	18.2256

Vamos em edit (Editar)





Done Reset Back [ Help ]

## **Configuração HD - Sistema**



	Storage configura	ation					
	FILE SYSTEM SUMM	ARY					
	MOUNT POINT [ / [ /boot		TYPE new ext4 new ext4	DEVICE T new LVM new part	YPE logical vol ition of lo	lume cal disk	
	AVAILABLE DEVICES						
	DEVICE [ ubuntu–vg (new) free space				TYPE LVM volume	e group	SIZE 18.222G 8.222G
	[ Create so		Editin	g logical	volume ubu	ntu−lv of	ubuntu-v
	i create vo		Name:	<u>u</u> buntu	-1v		
	USED DEVICE DEVICE [ ubuntu-vg	Size (ma	× 18.222G)	: 10.000	G		
			Format	: [ ext4		• ]	
	[ /dev/xvda partition partition		Mount	: [/		• 1	
					[ Save [ Cancel	1 1	
						0 ex	emplo (
	E por fim vai	mos ir	em			de 2	OGb e j
	ave e depois	s em D				vamo ao	os dígit lado de
_og Forens	е					18.2	22G pa
17-R25-MINER					Done Reset Back	] max	que ap

Kiraz

V1.

[Help]

## **Configuração HD - Sistema**



acima o nosso HD sistema é ficou 50% "pra trás". Agora tar o Size (max) que aparece lo campo, no caso acima é ara sua instalação digitar o parecerá ao lado do campo.

### FILE SYSTEM SUMMARY

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

### AVAILABLE DEVICES

### USED DEVICES

[	DEVICE ubuntu–vg ubuntu–lv	(new n	) ew,	to be	formatted	as ext	TYPE LVM volume , mounted at	group /	SIZE 18.222G 18.222G
	/dev/xvda partition partition partition	1 n 2 n 3 n	ew, ew, ew,	BIOS ( to be PV of	grub spacer formatted LVM volume	as ext⊄ e group	local disk 4, mounted at ubuntu–vg	∕boot	20.000G 1.000M 1.771G 18.225G









# **Configuração HD - Sistema**



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

Inctal	1100	0110	$\tau \circ m$
THEFT		- <u>-</u>	LEIII





# **Configuração HD - Sistema**

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.

KKKKKKKK	КККККК	iiii			
К:::::К	K:::::K	i::::i			
К:::::К	K:::::K	iiii		V1.17-R25-MINER	
К:::::К	K:::::K				
KK:::::K	K:::::KKK	iiiiiiirrrrr rrr	rrrrr aaaaaaaaaaaaa	2222222222222222222	
K:::::K	K:::::K	i:::::ir::::rrr:::	:::::r a::::::::::a	Z:::::::::::::::Z	
K:::::K	(::::K	i::::ir::::::::	::::::r aaaaaaaaa::::::a	Z::::::::::::Z	
K::::::	::::K	i::::irr::::::rrr	rr:::::r a::::a	ZZZZZZZZ::::::Z	
K::::::	::::K	i::::i r:::::r	r:::::r aaaaaaa:::::a	Z:::::Z	
K:::::K	(:::::K	i::::i r:::::r	rrrrrraa:::::::::::	Z:::::Z	
K:::::K	K:::::K	i::::i r:::::r	a::::aaaa::::::a	Z:::::Z	
KK:::::K	K:::::KKK	i::::i r:::::r	a::::a a:::::a	Z:::::Z	
K::::::K	K:::::K	i:::::ir:::::r	a::::a a:::::a	Z:::::ZZZZZZZZ	
K::::::K	K:::::K	i:::::ir:::::r	a:::::aaaa::::::a		
K::::::K	K:::::K	i:::::ir:::::r	a:::::::::aa:::	az::::::::::::::z	
KKKKKKKKK	KKKKKKK	iiiiiiiirrrrrr	aaaaaaaaa aaa	azzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzz	
				OG FORENSE	
Por favor,	faça logi	n para acessar.			
Usuário:					

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

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



## Finalização

