



Computação Forense na Computação na Nuvem

jorge.fonseca@upe.br



Quem sou eu?



Jorge.fonseca
@upe.br

- Professor UPE
- Filho do Cin-UFPE, criado no CESAR

Indústria e Academia

@jcbfonseca

Crime Digital



Fonte: Melo Medeiros Advogados

“toda a atividade onde um computador ou uma rede de computadores é utilizada como uma ferramenta, uma base de ataque ou como meio de crime”

Fonte: wikipedia

Internet: Facilitador (“anonimato”)

Forense Computacional



Fonte: Dominando IT

- Suporte para a solução de crimes digitais
- evolução de técnicas de recuperação de dados
 - Complexo na era do BigData

Cloud Computing



Cloud Computing

Escalabilidade



Cloud Computing

1 Máquina
Vários Servidores

Escalabilidade

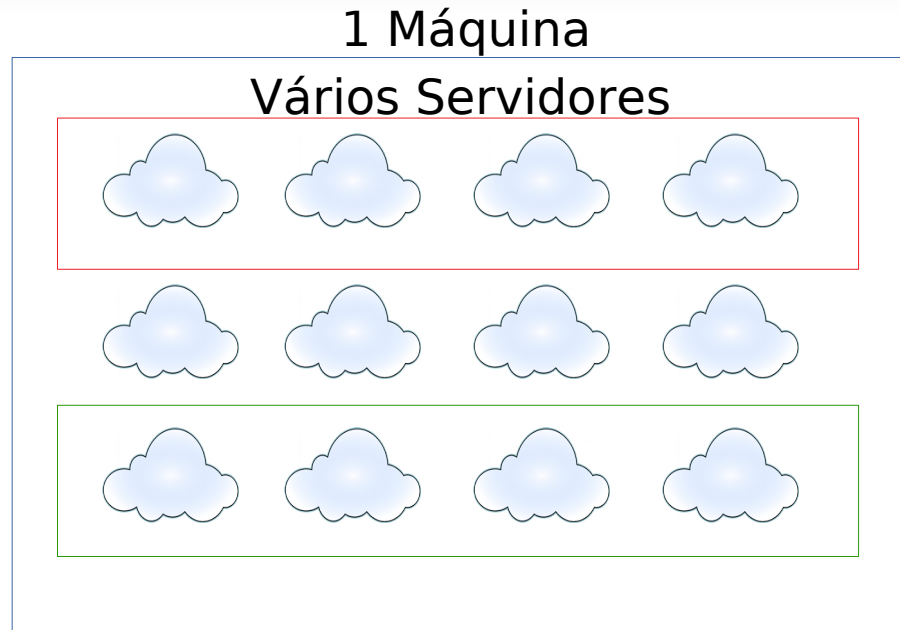


Virtualização



Cloud Computing

Escalabilidade

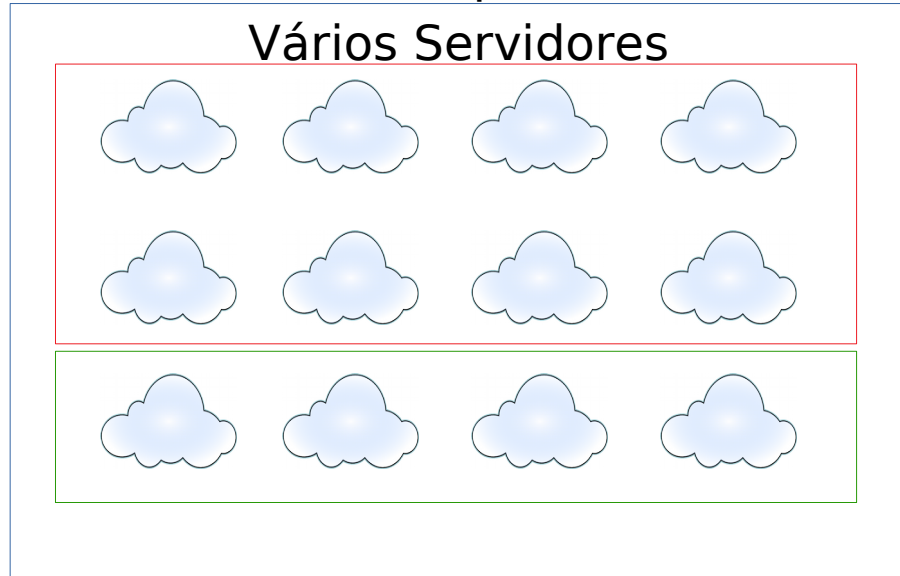


Virtualização
N usuários



Cloud Computing

1 Máquina
Vários Servidores



Escalabilidade
Elasticidade

Virtualização
N usuários



Cloud Computing

n Máquinas, n servidores



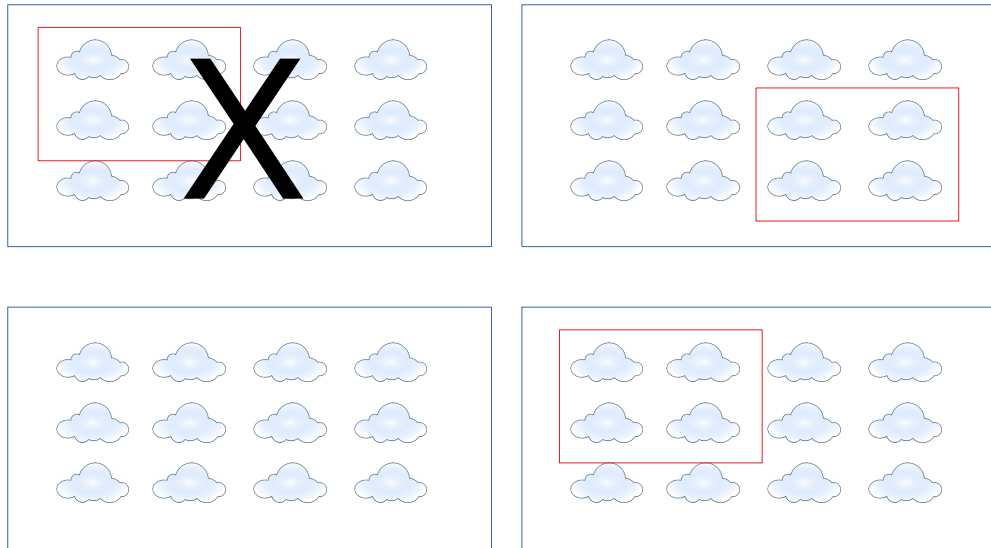
Escalabilidade
Elasticidade
Disponibilidade

Virtualização
N usuários



Cloud Computing

n Máquinas, n servidores



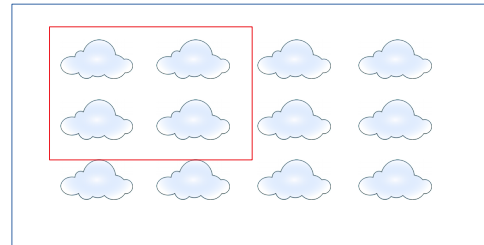
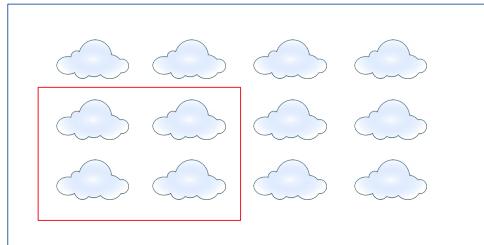
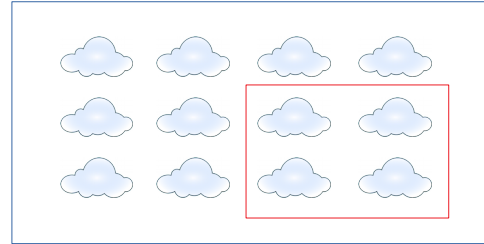
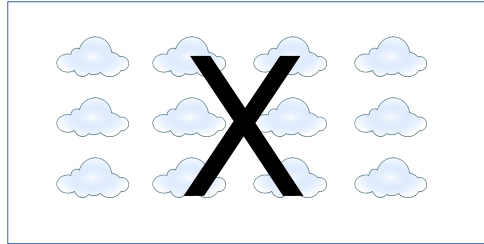
Escalabilidade
Elasticidade
Disponibilidade

Virtualização
N usuários



Cloud Computing

n Máquinas, n servidores



Escalabilidade
Elasticidade
Disponibilidade

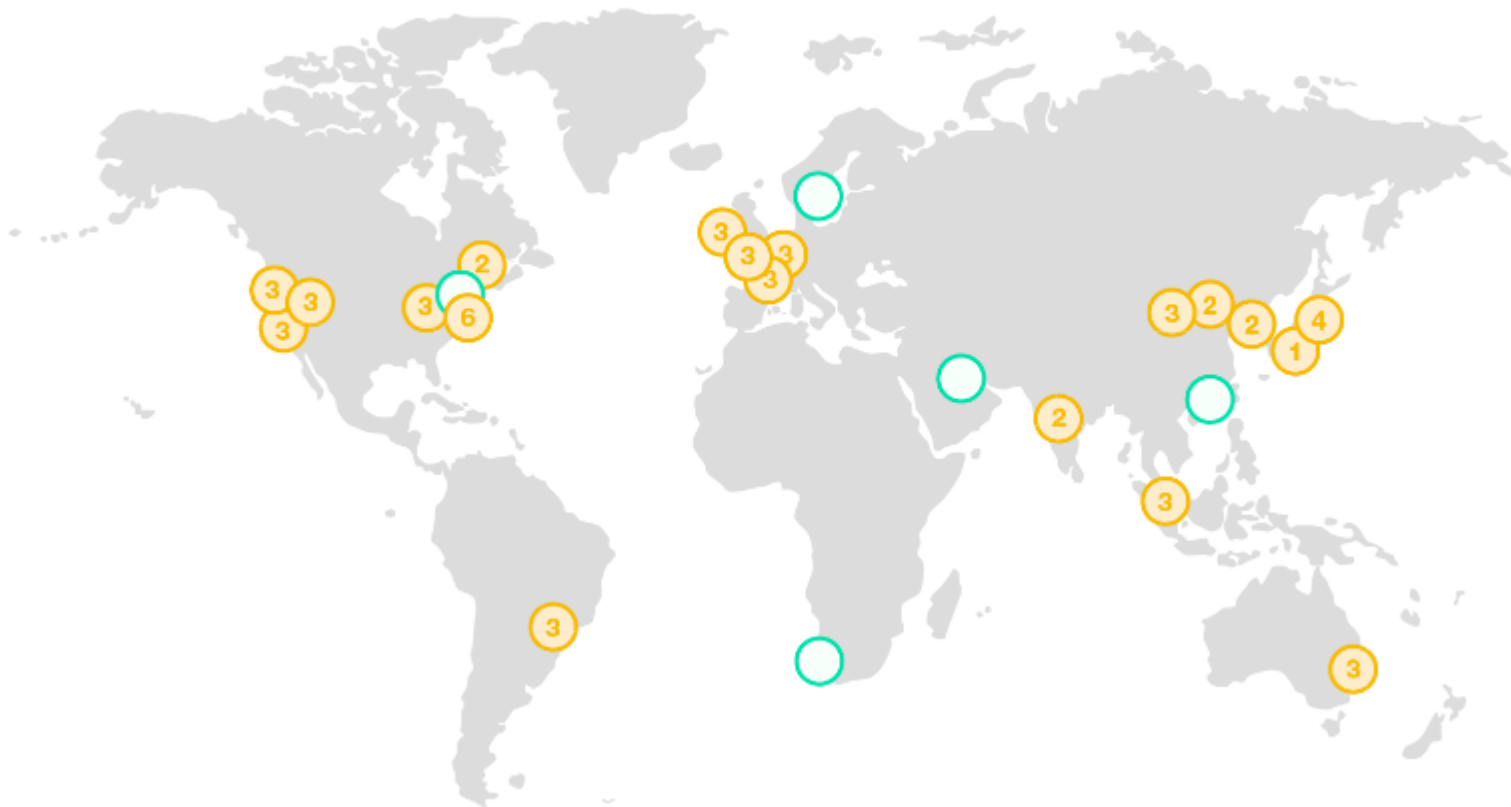
Virtualização
N usuários



N máquinas, n servidores - pelo mundo

Amazon CDN - (Content Delivery Network)

Infraestrutura global



Características da Computação na Nuvem

1. **Particionamento do conteúdo/dados** em **diferentes países** (ou dados replicados)
2. Uso de **máquinas virtuais (Vms)** que podem não mais estar ativas (em **diferentes localizações/regiões**)
3. Características multi-usuário
 - É possível remoção a VM?
4. O modelo “cliente-servidor” e sua inerente **distribuição**

Características da Computação na Nuvem

1. **Particionamento do conteúdo/dados** em **diferentes países** (ou dados replicados)
2. Uso de **máquinas virtuais (Vms)** que podem não mais estar ativas (em **diferentes localizações/regiões**)
3. Características multi-usuário
 - É possível remoção a VM?
4. O modelo “cliente-servidor” e sua inerente **distribuição**

Problemas do Direito

1. **Conflito** de soberanias
2. De **princípios** e **direitos** dos usuários
3. Interesse **jurídico** e legítimo dos Estados
4. Da sociedade de prevenir as **infrações penais**

Google - Balões

Projeto do Google usa balões para levar internet a áreas remotas

G1 - 2013

Balões gigantes levarão web a velocidades similares as das redes 3G. Primeiro teste do 'Project Loon' começou neste sábado na Nova Zelândia.



ct Loon' navega por meio da estratosfera, onde existem diferentes camadas de vento (Foto: Divulgação)

2014 - Piauí

2018 - first commercial agreement - Telkom Kenya

to bring internet access to some of Kenya's most inaccessible regions

Balão do Google sobrevoa Palmas e intriga moradores: 'parece água viva gigante'

Balão do Projeto Loon cai no interior do Amazonas, diz Google

Dinâmica na rota dos balões - E o direito, como fica?

Internet em Alto Mar (sem fio)

Internet sem fios em alto mar? Sim, é possível

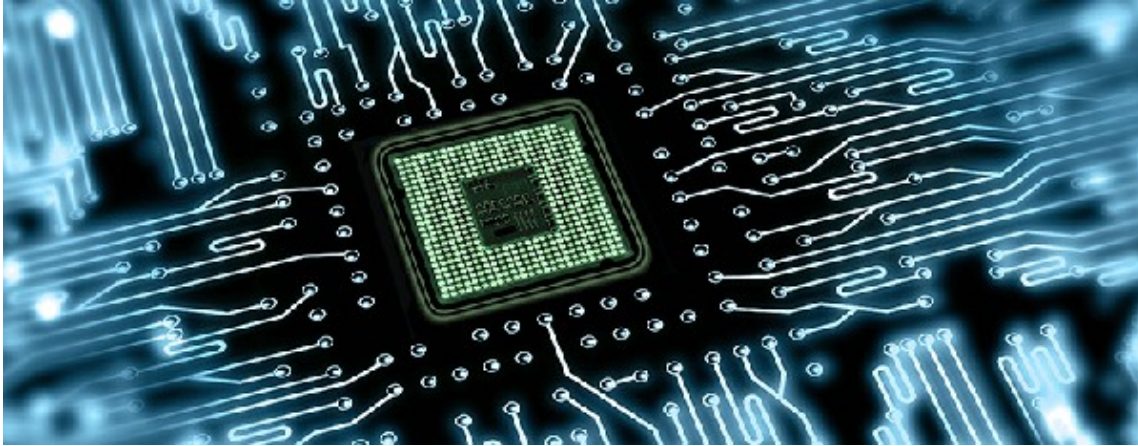
Projecto pioneiro do INESC TEC está a ser desenvolvido em parceria com uma empresa norueguesa.

LUÍSA PINTO - 13 de Janeiro de 2016, 16:11



- Princípio da "liberdade do alto-mar"
- Terra de Ninguém?
- E o direito?

Computação Forense



Fonte: unifacs

Ciência da Computação

Indissociáveis (?)

Ciência do Direito



Fonte: Exame

slide 19

Blog Especialista (?)

Como investigar em nuvem?

A investigação forense em nuvem necessita de metodologias, procedimentos e ferramentas para a obtenção de resultados concretos com valor probatório.

Conheça os procedimentos necessários para realizar uma investigação forense em nuvem:

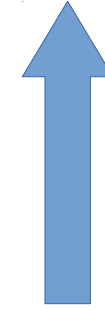
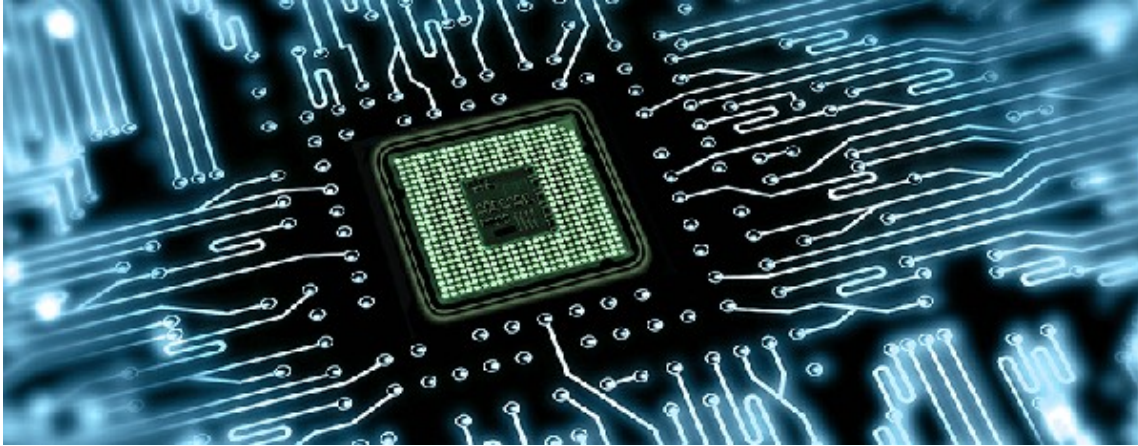
- 1 Identifique o provedor de nuvem que precisa ser investigado;
- 2 Utilize um computador conectado à internet;
- 3 Acesse a conta de armazenamento em nuvem utilizando login e senhas fornecidas pelo suspeito ou encontradas em arquivos pessoais ou outros meios;
- 4 Utilize softwares para capturar telas do processo e tráfegos de rede;
- 5 Verifique todos os arquivos disponíveis, datas e horários de acessos, computadores, usuários e IP's associados.
- 6 Faça uma cópia dos arquivos verificados no passo anterior;
- 7 Analise os arquivos e dados salvos;
- 8 Produza o laudo pericial com base na análise feita anteriormente;

Dúvida

Existe uma solução técnica que garanta a **coleta extraterritorial de provas criminais eletrônicas em ambiente de computação em nuvem**, sem que ocorra **violação à soberania de Estado estrangeiro**?



Computação Forense



Evolução

Indissociáveis (?)



Evolução



... Bom, mas tecnicamente falando...

Computação faz parte (é meio) de tudo
Se for permitido: é possível



Fonte: patrus

Armazenamento (tamanho, tempo)
Virtualização: Snapshots

Amazon Instance - Fortinet Analyzer

Launch on EC2:

Fortinet FortiAnalyzer-VM Centralized Logging/Reporting On-Demand

1-Click Launch

Review, modify and launch

Manual Launch

With EC2 Console, API or CLI

Click "Launch with 1-Click" to launch this software with the settings below

The default settings are provided by the software seller and AWS Marketplace.

Software Pricing

Subscription Term

- Hourly
- Annual

Applicable Instance Type

t2.small
c4.large
c4.2xlarge
d2.4xlarge
m4.large
m4.xlarge
m4.2xlarge
m4.4xlarge

Hourly fee

\$0.00 / hour

Find instance details in EC2 instance section below.

Version

v5.4.2, released 04/06/2017

Region

US East (N. Virginia)

Price for your Selections:

\$0.02 / hour

\$0.02 t2.small EC2 Instance usage fees +

\$0.00 hourly software fee

Additional taxes may apply.

\$0.05 per GB-month of provisioned storage

EBS Magnetic volumes

\$0.05 per 1 million I/O requests

EBS Magnetic volumes

Launch with 1-click

You will be subscribed to this software and agree that your use of this software is subject to the pricing terms and the seller's End User License Agreement (EULA) and your use of AWS services is subject to the AWS Customer Agreement.

Cost Estimator

\$17.28 / month

Additional taxes may apply.

t2.small EC2 Instance usage fees

Assumes 24 hour use over 30 days

Software Charges

\$0.72 / month

\$0.72 hourly software fees for t2.small

Amazon Instance - Fortinet Analyzer



Amazon Instance - Fortinet Analyzer

The screenshot shows the FortiWiFi 60D management interface. The left sidebar lists various system settings, with 'Log & Report' expanded to show 'Log Settings'. The main content area is titled 'Log Settings' and includes the following configuration options:

- Local Log: Memory
- Remote Logging and Archiving:
- Send Logs to FortiAnalyzer/FortiManager: (indicated by a red arrow)
- IP Address: [] (indicated by a red arrow) [Test Connectivity]
- Upload Option: Realtime
- Encrypt Log Transmission:

Below the settings is a bar chart titled 'Logs Sent to FortiAnalyzer Daily'. The Y-axis represents the amount of data in MB, ranging from 0B to 7.00MB. The X-axis shows dates from Apr 05 to Apr 11. The chart shows data for Apr 08, Apr 09, Apr 10, and Apr 11. The bars are stacked with Traffic Log (yellow), Event Log (black), and Web Filter Log (blue).

Date	Traffic Log (MB)	Event Log (MB)	Web Filter Log (MB)	Total (MB)
Apr 05	0.00	0.00	0.00	0.00
Apr 06	0.00	0.00	0.00	0.00
Apr 07	0.00	0.00	0.00	0.00
Apr 08	2.50	0.00	0.20	2.70
Apr 09	4.00	0.00	0.50	4.50
Apr 10	5.50	0.00	1.00	6.50
Apr 11	4.50	0.00	0.80	5.30

Below the chart are additional settings:

- Send Logs to FortiCloud:
- Send Logs to Syslog:
- Log Settings: Local Traffic Log
- Event Logging: (indicated by a red arrow)
- Event Logging options (all checked):
 - Enable All
 - System activity event
 - VPN activity event
 - Compliance Check Event
 - Endpoint event
 - User activity event
 - HA event
 - WiFi activity event
 - Router activity event
 - Explicit web proxy event

Amazon Instance - Fortinet Analyzer

Log View

Traffic

Add Filter

All Devices

Last 1 Hour

GO

Column Settings

Tools

admin

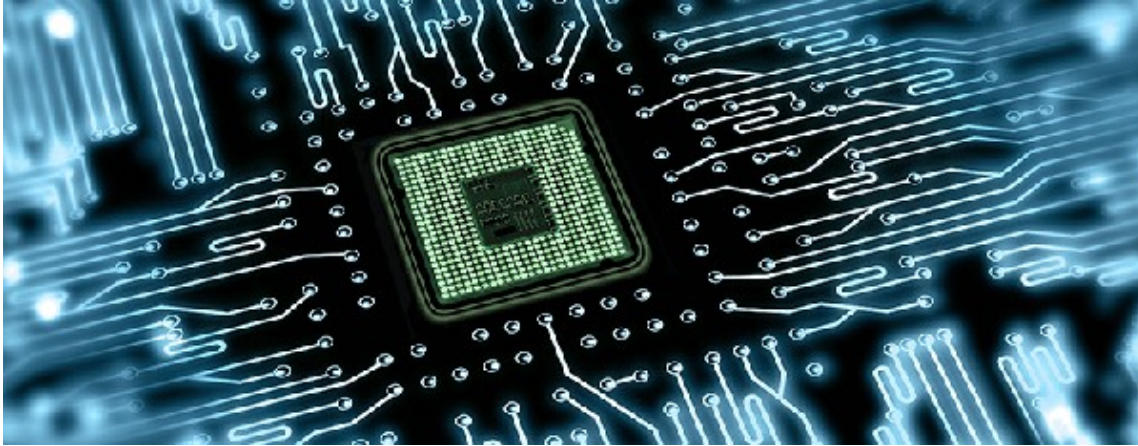
#	Date/Time	Device ID	Action	Source	Destination IP	Service	Sent/Received	User	Application	Security Event List
1	17:46:25	FWF60D46130040...	✓	192.168.1.110	157.56.52.48	udp/40016	158.0 B/49.0 B		udp/40016	
2	17:46:25	FWF60D46130040...	✓	192.168.1.110	172.16.100.100	DNS	67.0 B/440.0 B		DNS	
3	17:46:20	FWF60D46130040...	✓	192.168.1.110	172.18.28.126	HTTP	397.0 B/456.0 B		HTTP	
4	17:46:10	FWF60D46130040...	✓	192.168.1.110	172.18.3.190	tcp/7680	361.0 B/247.0 B		tcp/7680	
5	17:46:10	FWF60D46130040...	✓	192.168.1.110	172.18.3.190	tcp/7680	361.0 B/247.0 B		tcp/7680	
6	17:46:10	FWF60D46130040...	✓	192.168.1.110	172.18.3.182	tcp/7680	361.0 B/247.0 B		tcp/7680	
7	17:46:10	FWF60D46130040...	✓	192.168.1.110	172.18.3.172	tcp/7680	361.0 B/247.0 B		tcp/7680	
8	17:45:50	FWF60D46130040...	✓	192.168.1.110	111.221.77.152	udp/40018	61.0 B/48.0 B		udp/40018	
9	17:45:50	FWF60D46130040...	✓	192.168.1.110	157.56.52.25	udp/40036	61.0 B/957.0 B		udp/40036	
10	17:45:40	FWF60D46130040...	✓	192.168.1.110	52.84.246.88	HTTP	613.0 B/1.3 KB		HTTP	WEB 1
11	17:45:35	FWF60D46130040...	✓	192.168.1.110	172.18.3.250	tcp/8013	2.2 KB/700.0 B		tcp/8013	
12	17:45:35	FWF60D46130040...	✓	192.168.1.110	172.18.3.250	tcp/8013	172.0 B/92.0 B		tcp/8013	
13	17:45:35	FWF60D46130040...	✓	192.168.1.110	157.55.130.155	udp/40032	160.0 B/49.0 B		udp/40032	
14	17:45:35	FWF60D46130040...	✓	192.168.1.110	157.55.56.149	udp/40014	159.0 B/49.0 B		udp/40014	
15	17:45:30	FWF60D46130040...	✓	192.168.1.110	172.18.3.190	tcp/7680	361.0 B/247.0 B		tcp/7680	
16	17:45:30	FWF60D46130040...	✓	192.168.1.110	172.18.3.182	tcp/7680	361.0 B/247.0 B		tcp/7680	
17	17:45:30	FWF60D46130040...	✓	192.168.1.110	172.18.3.191	tcp/7680	361.0 B/247.0 B		tcp/7680	
18	17:45:30	FWF60D46130040...	✓	192.168.1.110	172.18.3.191	tcp/7680	361.0 B/247.0 B		tcp/7680	
19	17:45:25	FWF60D46130040...	✓	192.168.1.110	65.55.44.54	HTTPS	2.1 KB/8.1 KB		HTTPS	WEB 1
20	17:45:20	FWF60D46130040...	✓	192.168.1.110	172.18.28.126	HTTPS	1.8 KB/2.3 KB		HTTPS	
21	17:45:20	FWF60D46130040...	✓	192.168.1.110	172.18.28.126	HTTPS	16.9 KB/11.4 ...		HTTPS	WEB 1
22	17:45:15	FWF60D46130040...	✓	192.168.1.110	172.18.28.131	HTTPS	274.6 KB/194...		HTTPS	WEB 1
23	17:45:03	FWF60D46130040...	✓	192.168.1.110	192.168.42.40	tcp/7680	152.0 B/0.0 KB		tcp/7680	
24	17:45:03	FWF60D46130040...	✓	192.168.1.110	65.52.108.116	HTTPS	2.1 KB/8.1 KB		HTTPS	WEB 1
25	17:45:03	FWF60D46130040...	✓	192.168.1.110	192.168.100.126	HTTPS	11.6 KB/99.1 ...		HTTPS	WEB 1
26	17:45:03	FWF60D46130040...	✓	192.168.1.110	172.16.100.100	DNS	79.0 B/494.0 B		DNS	
27	17:45:03	FWF60D46130040...	✓	192.168.1.110	172.16.100.100	DNS	77.0 B/497.0 B		DNS	
28	17:45:03	FWF60D46130040...	✓	192.168.1.110	157.55.130.146	udp/40006	159.0 B/49.0 B		udp/40006	
29	17:45:03	FWF60D46130040...	✓	192.168.1.110	65.55.223.34	udp/40010	63.0 B/48.0 B		udp/40010	
30	17:45:03	FWF60D46130040...	✓	192.168.1.110	157.55.130.176	udp/40001	157.0 B/79.0 B		udp/40001	
31	17:45:03	FWF60D46130040...	✓	192.168.1.110	65.55.223.25	udp/40012	157.0 B/78.0 B		udp/40012	
32	17:45:03	FWF60D46130040...	✓	192.168.1.110	172.18.3.190	tcp/7680	361.0 B/247.0 B		tcp/7680	
33	17:45:03	FWF60D46130040...	✓	192.168.1.110	172.18.3.182	tcp/7680	361.0 B/247.0 B		tcp/7680	
34	17:45:03	FWF60D46130040...	✓	192.168.1.110	172.18.3.191	tcp/7680	361.0 B/247.0 B		tcp/7680	
35	17:45:03	FWF60D46130040...	✓	192.168.1.110	172.16.100.100	DNS	60.0 B/206.0 B		DNS	
36	17:45:03	FWF60D46130040...	✓	192.168.1.110	172.18.3.250	tcp/8013	2.2 KB/772.0 B		tcp/8013	

50 Items per page

1 2 3

Display Details

Computação Forense



Indissociáveis (?)

Porque não evoluem “juntas”?



Amazon Instance - Fortinet Analyzer

When running this product, you will be charged in accordance with the pricing dimension(s) listed on the detail page. Charges may vary based on your usage or by the size of the instance you choose to run this software on.

In addition to these software fees you are responsible for charges associated with your use of AWS services, including EC2 usage.

You can review pricing for this software here: https://aws.amazon.com/marketplace/pp/ref=bill_eml_2?sku=15imtxrv8tqhacbg2uw7fafr2.

If you have questions, please contact us: https://aws.amazon.com/marketplace/help/contact-us/ref=bill_eml_2

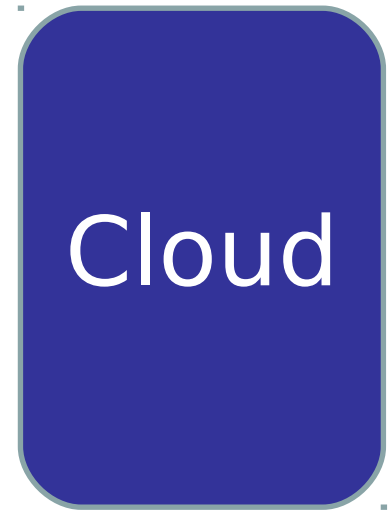
-- The AWS Marketplace Team

This message was produced and distributed by Amazon Web Services, Inc. and affiliates, 410 Terry Ave. North, Seattle, WA 98109-5210.

Fog Computing



Fog Computing

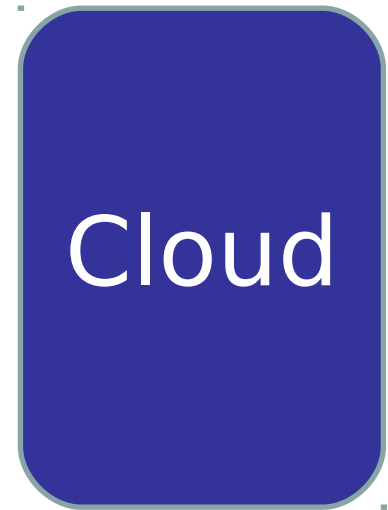


Fog Computing

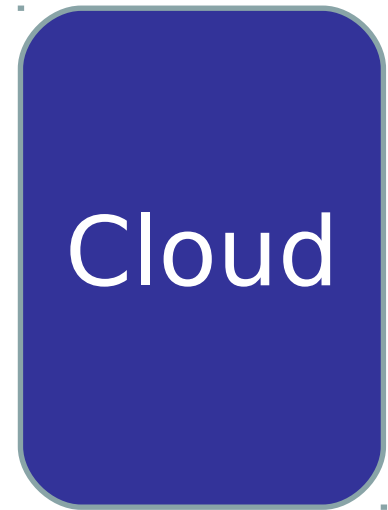
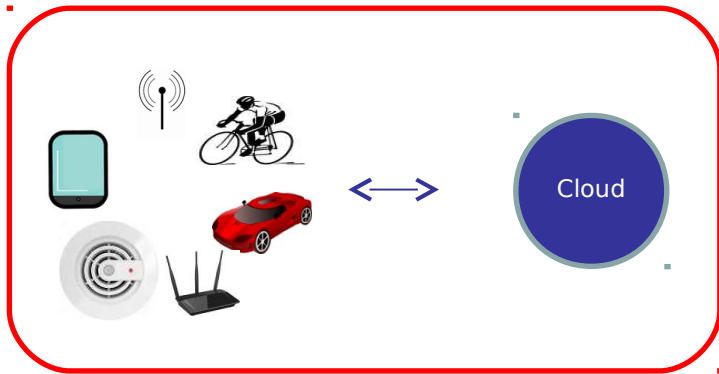


Cloud

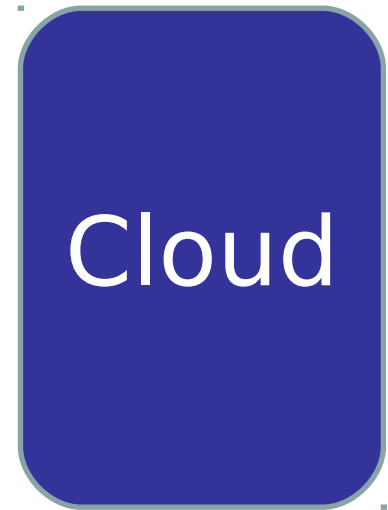
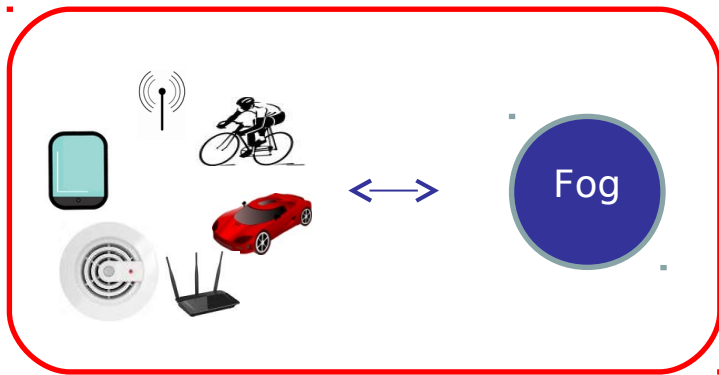
Fog Computing



Fog Computing

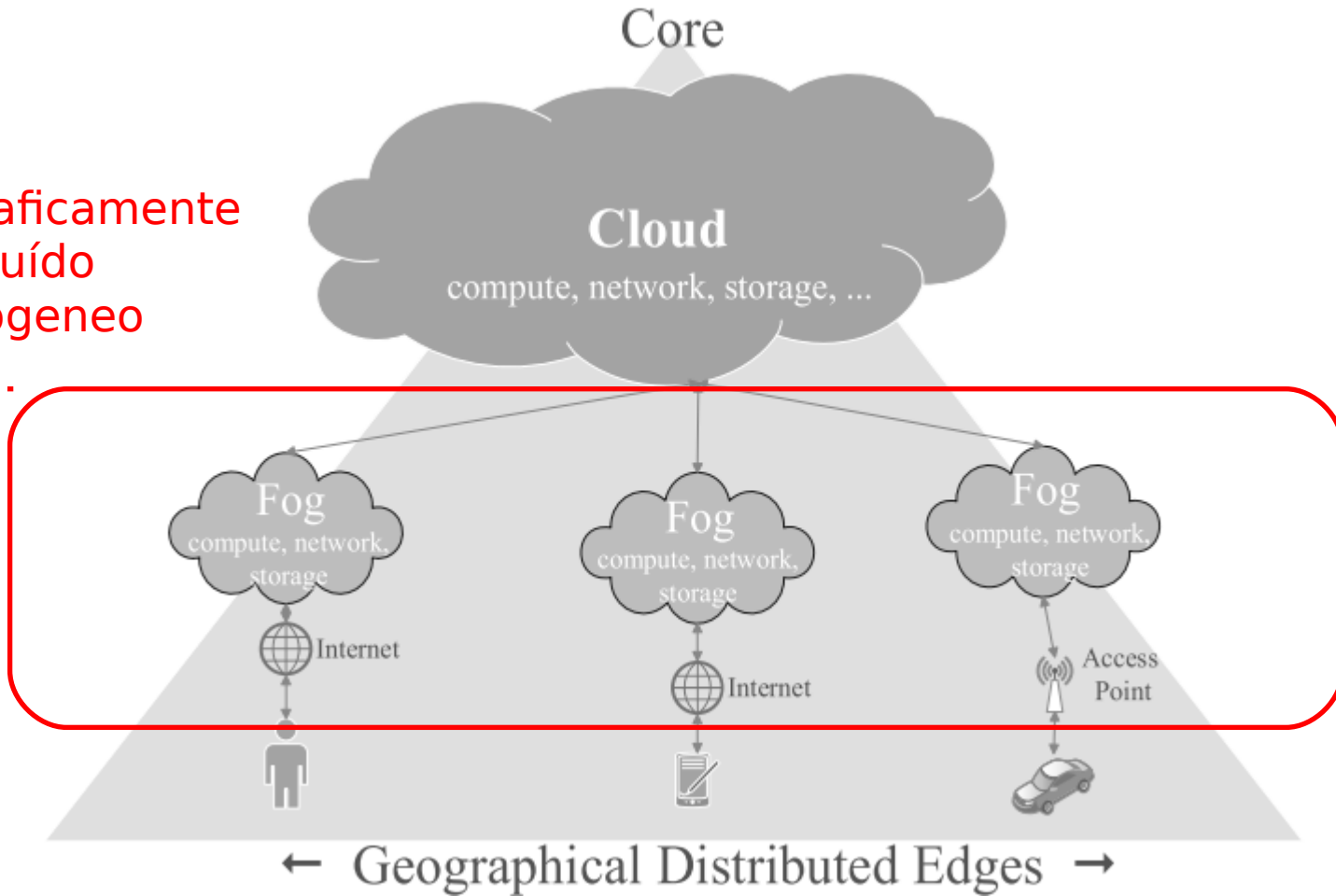


Fog Computing



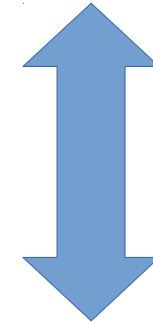
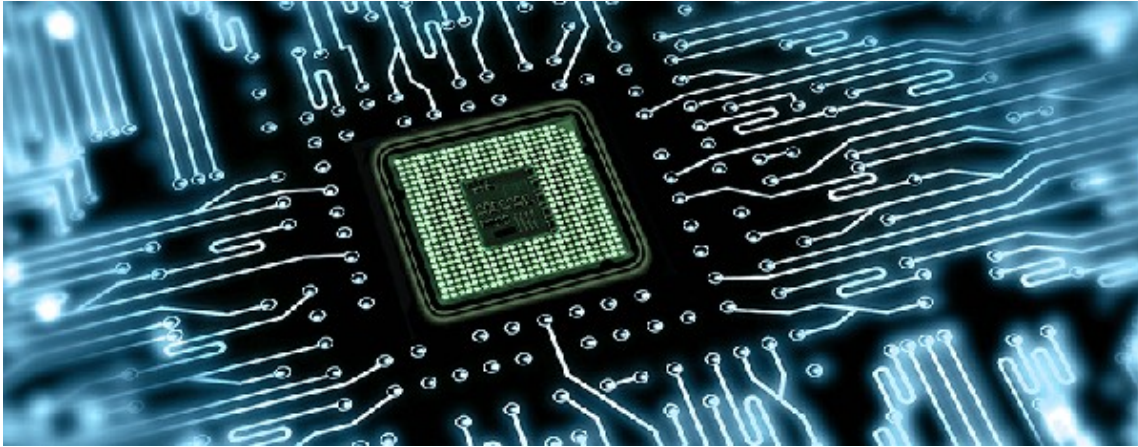
Fog Computing

- Geograficamente Distribuído
- Heterôgeneo



Fonte: (Bonomi et al; 2014)

Computação Forense - Mensagem Final



Evolução

Indissociáveis

Na prática: de forma pró-ativa



Computação Forense - Mensagem Final

Regulamentação vs. Inovação



k31645574 www.fotosearch.com

“Estamos aqui para permitir o que você quer criar, e não para falar o que voce NAO pode fazer.”



Computação Forense na Computação na Nuvem

jorge.fonseca@upe.br

