Computação e Segurança na Nuvem

Miguel P. Correia

1º Workshop de Cloud Computing– Açores, 12 de Abril de 2013

TÉCNICO LISBOA FCT inesc id lisboa

Tópicos

1. Computação em nuvem
2. Insegurança na nuvem
3. Segurança na nuvem
4. Sistema DepSky

2

1. COMPUTAÇÃO EM NUVEM

3

Nuvem: *computing as a utility*

- Pay-as-you-go
- CAPEX vs OPEX
- Elasticidade

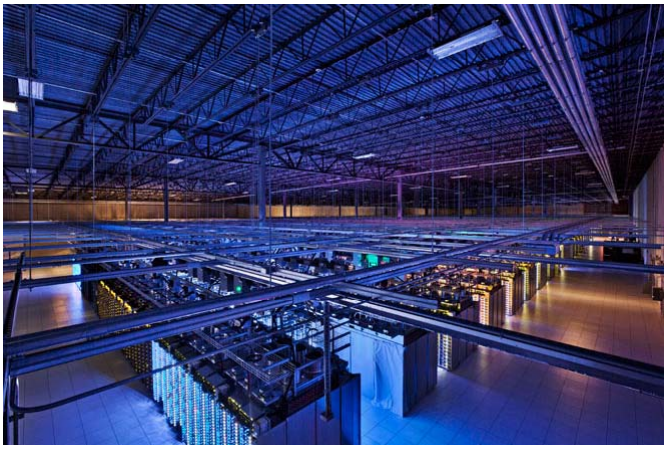
4

Nuvem: por trás da ficha

- Centros de dados de grandes dimensões…
  - Google: 900 mil servidores
  - Microsoft: 500 mil
  - Yahoo!: 100 mil
  - Rackspace: 75 mil
  - Facebook: 60 mil
  - Amazon EC2: 40 mil
  - estimativas para 2011

Microsoft's Chicago datacenter

Nuvem: por trás da ficha

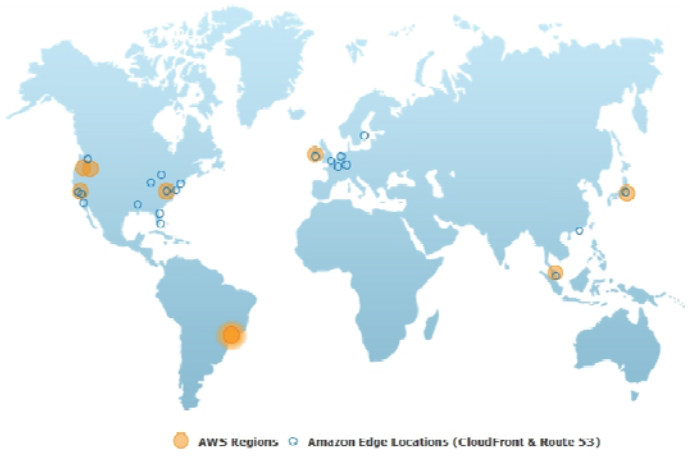


Google: a server room in Council Bluffs, Iowa

6

Nuvem: por trás da ficha

- …e espalhados por todo o mundo



7

Modelos de serviço

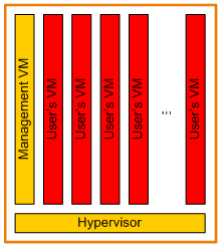
- O NIST definiu três: IaaS, PaaS, SaaS

  - mas a moda pegou: XaaS, CaaS, NaaS, MaaS, DaaS,…

8

Infrastructure as a Service (IaaS)

- Serviço = alojamento de máquinas virtuais (VMs)
  - Cada servidor tem um hipervisor que virtualiza o hardware
  - Cada servidor corre várias VMs, tip. de vários clientes
  - Cliente instala o seu próprio software nas VMs: SO, servidor web,…
- Serviços comerciais
  - Amazon EC2, IBM SmartCloud, Rackspace Cloud, …



Infrastructure as a Service (IaaS)

- Demonstração: criar instâncias na Amazon EC2 e *computing as a utility*

http://aws.amazon.com

10

IaaS: storage

- Serviço = armazenamento de ficheiros
- Serviços comerciais
  - Amazon S3, Apple iCloud, DropBox, Microsoft SkyDrive



11

Platform as a Service (PaaS)

- Serviço = execução de aplicações num ambiente específico
  - Cliente desenvolve aplicações que correm no ambiente da nuvem
  - Ex: desenvolve aplicações web em Java/Python/Go que correm nos servidores da nuvem, com um SGBD da nuvem, etc.
- Serviços comerciais
  - Google AppEngine, Force.com, Windows Azure

Software as a Service (SaaS)

- Serviço = aplicações web prontas a usar
- Serviços comerciais
  - Gmail, Google Drive, Google Apps for Business, Microsoft Office 365, Yahoo! Mail, Facebook,…

Modelos de serviço

IaaS PaaS SaaS

Perde-se controle

Simplifica-se a administração

14

Pay-as-you-go

- Amazon EC2: serviço = máquinas virtuais
  - Paga-se por: nº de VMs reservadas, tipo de VM (recursos), horas/mês, dados recebidos/enviados (GB/mês), IPs usados, etc.
  - *ex: 10 instances, Linux, type Medium, utilization Medium, contract 1 year, usage 732 hours/month, 10GB in/out = ~460 $/month*
- Amazon S3: serviço = armazenamento de ficheiros
  - Paga-se por: dados armazenados, pedidos, dados descarregados
  - *0.125 $/GB armaz., 0.01 $/1000 pedidos, transf. de dados 0.120 $/GB*

(custos calculados em Maio 2012)

15

Modelos de implementação

- Nuvem pública
  - o verdadeiro modelo *computing as a utility*; existe um fornecedor de serviço e clientes
- Nuvem privada
  - nuvem pertence à organização que a utiliza
- Nuvem comunitária
  - nuvem privada que pertence a um conjunto de organizações com interesses comuns
- Nuvem híbrida
  - combinação de nuvens de 2 dos modelos anteriores


NIST
National Institute of Standards and Technology
U.S. Department of Commerce

The NIST Definition of Cloud Computing (Draft)

Recommendations of the National Institute of Standards and Technology

Peter Mell
Timothy Grance

16

2. INSEGURANÇA NA NUVEM

17

Internet: um mundo perigoso

286M+
Threats

Polymorphism and new delivery mechanisms such as Web-attack toolkits continued to drive up the number of malware variants in common circulation. In 2010, Symantec encountered more than 286 million unique variants of malware.

93%
Increase in Web Attacks

A growing proliferation of Web-attack toolkits drove a 93% increase in the volume of Web-based attacks in 2010 over the volume observed in 2009. Shortened URLs appear to be playing a role here too. During a three-month observation period in 2010, 65% of the malicious URLs observed on social networks were shortened URLs.

260,000
Identities Exposed per Breach

This was the average number of identities exposed in each of the data breaches caused by hacking throughout the year.

42%
More Mobile Vulnerabilities

In a sign that the mobile space is starting to garner more attention from both security researchers and cybercriminals, there was a sharp rise in the number of reported new mobile operating system vulnerabilities—up to 163 from 115 in 2009.

6,253
New Vulnerabilities

Symantec recorded more vulnerabilities in 2010 than in any previous year since starting this report. Furthermore, the new vendors affected by a vulnerability rose to 1,914, a 161% increase over the prior year.

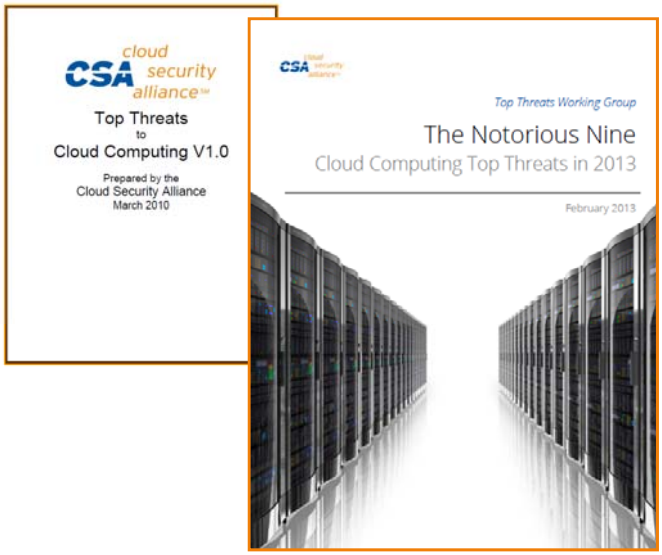
1M+
Bots

Rustock, the largest botnet observed in 2010, had well over 1 million bots under its control. Grum and Cutwail followed, each with many hundreds of thousands of bots.

Números relativos a 2010 - Symantec Internet Security Threat Report, Vol 16, April 2011

18

Ameaças à/na nuvem



19

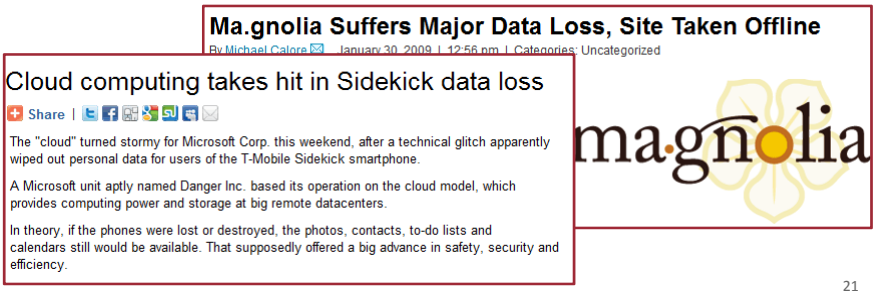
1. Violação de dados

- Dados sensíveis de um utilizador / empresa caem da mão de terceiros
- Não é específico da nuvem, mas esta introduz novos vectores de ataque
  - Vulnerabilidade numa aplicação de um cliente permite acesso de atacante às de vários clientes
  - Vulnerabilidade no software de gestão permite acesso entre VMs
  - *Side channel* permite roubar chaves criptográficas entre VMs

20

2. Perda de dados

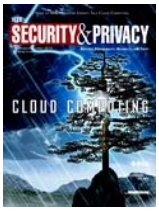
- Na nuvem os dados não estão sob controle do cliente e…
- Ma.gnolia perdeu todos os dados dos clientes, 12 TB (Fev. 09)
- Danger Inc. / Sidekick perdeu contactos, notas, fotos, etc. dos seus utilizadores; demorou dias a recuperar (Out. 2009)



21

3. Sequestro de contas ou tráfego

- Na nuvem há contas, vulneráveis a ataques como: *phishing*, acesso usando *passwords* roubadas, escuta de comunicação,…
- Na nuvem esses vectores de ataque permitem acesso aos sistemas e dados da empresa cliente
- *"there're some things that will never go into [our cloud], for example, our SAP back end"*
  - Representante de um grande fornecedor de nuvem na "Cloud Computing Roundtable" (IEEE Sec&Priv. Nov/Dec'10)



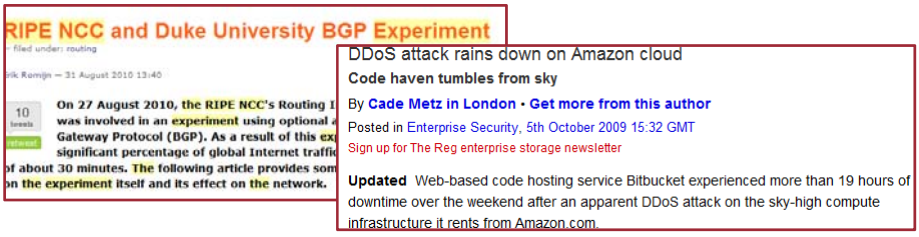
4. APIs inseguras

- Na nuvem a superfície de ataque de uma aplicação é expandida com a interface de gestão
  - Como a que vimos da Amazon AWS, *web services,* REST
- Essa interface pode ter:
  - Vulnerabilidades que permitem personificar um utilizador legítimo: SQLI, XMLI, XSS, CSRF, etc.
  - Exemplo: biblioteca Java da Amazon EC2 validava incorrectamente certificados digitais SSL; permitia ataques *man-in-the-middle* (Georgiev et al., ACM CCS'12)

23

5. Negação de serviço (indisponibilidade)

- O risco da negação de serviço é menor na nuvem
  - Recursos, elasticidade, distribuição geográfica
  - CloudFlare, web hosting tolerante a ataques DDoS (Lulz)
- No entanto:
  - Alguns ataques podem ser eficazes – Bitbucket, Amazon 2009
  - Indisponibilidade parcial da Internet – Ago. 2010
  - Indisponibilidade da nuvem – tantos e tantos casos… (WinAz 29/2/12)


RIPE NCC and Duke University BGP Experiment

filed under: routing

On 27 August 2010, the RIPE NCC's Routing I
was involved in an experiment using optional
Gateway Protocol (BGP). As a result of this ex
significant percentage of global Internet traffi
of about 30 minutes. The following article provides som
on the experiment itself and its effect on the network.

DDoS attack rains down on Amazon cloud

Code haven tumbles from sky

By Cade Metz in London • Get more from this author

Posted in Enterprise Security, 5th October 2009 15:32 GMT

Sign up for The Reg enterprise storage newsletter

Updated Web-based code hosting service Bitbucket experienced more than 19 hours of downtime over the weekend after an apparent DDoS attack on the sky-high compute infrastructure it rents from Amazon.com.

6. Insider malicioso

- Na nuvem os administradores, quem tem acesso aos dados, são desconhecidos; são de confiança?
  - CyberLynk (Mar'09)
  - Google (2010)

CRIMINAL JUSTICE

Producer Sues ISP and its Fired Employee, Saying Hack Destroyed Season of Kids' TV Series

Posted Apr 1, 2011 4:13 PM CDT
By Intern

Email Print Reprints Share / Save

A new lawsuit alleges a fired employee hacked into his former company's
deliberately destroyed an entire season of a syndicated children's TV sh

EXCLUSIVE

GCreep: Google Engineer Stalked Teens, Spied on Chats (Updated)

We entrust Google with our most private communications because we assume the company takes every precaution to safeguard our data. It doesn't. A Google engineer spied on four underage teens for months before the

7. Abuso de serviços da nuvem

- A nuvem oferece muitos recursos, que podem ser usados para fins ilegítimos

Pirate Bay ditches servers and switches to the cloud

Looking for new ways to avoid raids and the seizure of its information-full servers, the file-sharing service moves all of its content to the cloud.

by Dara Kerr | October 17, 2012 5:21 PM PDT

Follow

306 339 10 16 More + Comments 15

In the midst of threats of a possible police raid, the Pirate Bay decided to armor itself and become literally raid-proof. It's ditched its servers and moved to several cloud-hosting providers in different countries around the world.

"Slowly and steadily we are getting rid of our earthly form and ascending into the next stage, the cloud," the Pirate Bay wrote in a blog post. "Our data flows around in thousands of clouds, in deeply encrypted forms, ready to be used when necessary. Earth bound nodes that transform the data are as deeply encrypted and reboot into a deadlock if not used for 8 hours."

The Pirate Bay

26

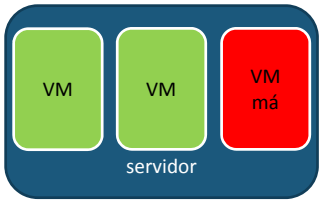
8. Diligência insuficiente

- Risco de empresas migrarem para a nuvem sem se aperceberem suficientemente das implicações
  - Qual é a disponibilidade oferecida?
  - É cumprida?
  - O que acontece se não for cumprida? (*money-back guarantees*)
  - Qual é o custo de tirar os dados da nuvem (*vendor lock-in*)?
  - …

27

9. Tecnologias partilhadas

- Na nuvem os recursos são partilhados por diversos utilizadores, alguns dos quais podem ser maliciosos
- Vulnerabilidade no hipervisor, VM de administração, *side channel,…* podem permitir a uma VM atacar outra

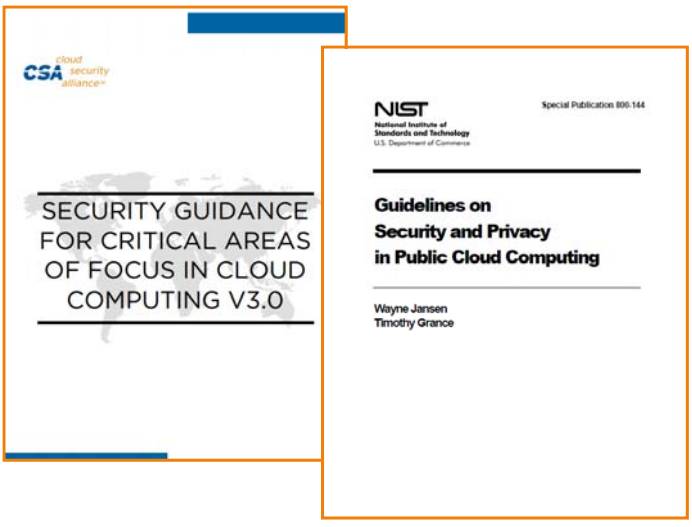


28

3. SEGURANÇA NA NUVEM

29

Boas práticas de segurança



30

Boas práticas?

"We don't know what we're doing,
but we're doing the same as them,
so don't sue us."

Bruce Schneier@IBWAS'09

31

Segurança na nuvem: 6 fases

- Especificar requisitos de segurança e privacidade
- Avaliar os riscos da mudança para a nuvem
- Avaliar a fiabilidade do fornecedor escolhido
- Exprimir os requisitos de segurança no contrato
- Criar controles para protecção de dados/aplicações na nuvem
- Avaliar o desempenho do serviço de nuvem

32

Requisitos segurança/privacidade

- Especificar requisitos; categorias:
  - Legais (p.ex., dados saírem do país, PCI)
  - Disponibilidade
  - Controle de acesso físico e lógico
  - Protecção de dados
  - Reporte e resposta a incidentes
  - Continuidade de serviço
  - Auditoria independente
  - etc.

- Derivar grau de controle necessário, IaaS/PaaS/SaaS?

33

Risco

- Analisar dados a pôr na nuvem
  - Privacidade, existência de informação pessoal
  - Outros dados sensíveis: dados relevantes para investigação criminal, documentos obtidos sob *non-disclosure agreement*, código fonte, etc.
- Analisar tecnologia e procedimentos do fornecedor
  - Técnicas usadas para isolamento entre clientes
  - Mecanismos para *backup* e recuperação de dados
  - Mecanismos para controle de acesso a dados e autenticação
  - Procedimentos para resposta a incidentes e recuperação de desastres

34

Fiabilidade do fornecedor

- Avaliar fiabilidade do fornecedor escolhido
  - Analisar a informação do fornecedor sobre segurança
  - Pedir ao fornecedor para demonstrar capacidades de segurança
  - Pedir avaliação independente
  - Contactar clientes actuais sobre nível de satisfação
- Aspectos a avaliar
  - Experiência do pessoal técnico, qualidade do treino em segurança
  - *Accountability* de acesso a servidores
  - Tipo e eficácia dos serviços de segurança
  - Historial de incidentes do fornecedor

Obrigações contratuais

- Exprimir os requisitos de segurança no contrato
  - Divisão clara entre responsabilidades do cliente e do fornecedor
  - Políticas e procedimentos
  - Níveis de serviço e respectivos custos
  - Processo de verificação de nível de serviço
  - Interface entre cliente e fornecedor
  - Restrições de localização e co-locação de dados
  - Obrigações do fornecedor em caso de terminação do contrato
  - Direitos sobre os dados armazenados (incluindo a sua propriedade)
  - Obrigações em rel. a resposta a incidentes e recuperação de desastres

36

Gestão de informação / seg. dados

- Criar controles para protecção de dados e aplicações
  - Usar o *data security lifecycle* para identificar exposição de dados (especialmente armazenar, arquivar, destruir)
  - Monitorizar acessos dos funcionários à nuvem
  - Bloquear acessos indevidos
  - Cifrar dados críticos
  - Fazer gestão segura de chaves criptográficas
  - Garantir segurança aplicacional (principal vector de violação de dados)

37

Avaliar o desempenho

- Avaliar de forma contínua o desempenho do fornecedor (QoS vs SLA)
- Fazer análise/teste periódicos do estado de segurança do sistema

38

4. SISTEMA DEPSKY

Trabalho conjunto c/Alysson Bessani, Paulo Sousa, B. Quaresma, F. André

39

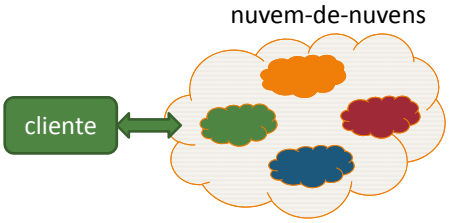
Falhas acontecem

- E se…
  - A nuvem corromper os dados (Sidekick, Ma.gnolia, CyberLink…) ou
  - A nuvem estiver indisponível (Win.Azure, EC2, AppEngine,…) ou
  - Houver uma violação de dados (Gmail/Gtalk,…) ou
  - Existir um problema de *lock-in*?
- Solução: não confiar numa nuvem

40

DepSky: nuvem-de-nuvens

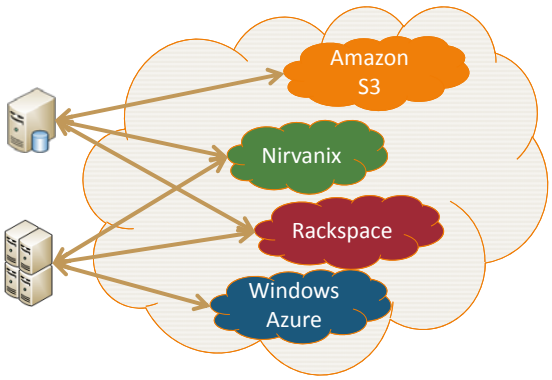
- Ideia: não confiar numa nuvem, confiar no conjunto
  - Replicação+diversidade para tolerância a faltas
- DepSky – nuvem-de-nuvens para armazen. de dados; tolera:
  - Corrupção de dados numa nuvem
  - Indisponibilidade de uma nuvem
  - Violação de dados (cifrando)
  - *Lock-in*
  - Bonus: leituras + rápidas



41

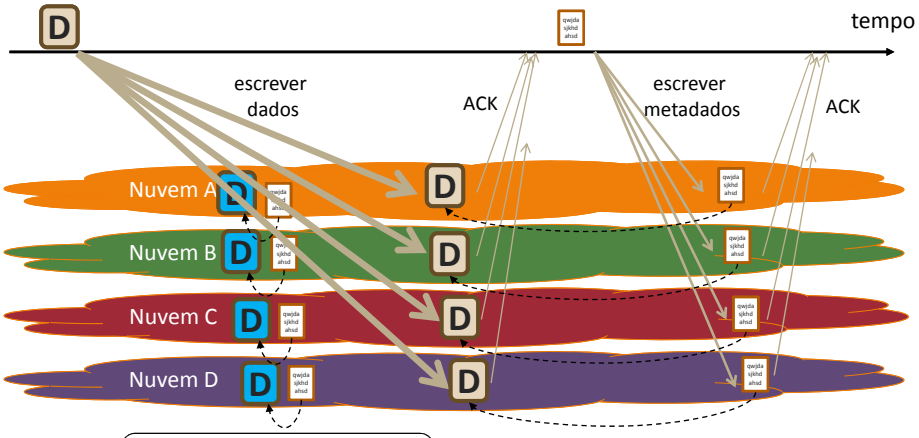
DepSky

- Fornece o mesmo serviço de um serviço de nuvem de armazenamento (ex: Amazon S3): *read, write, create,…*
- Não muda as nuvens originais; é um *proxy* do lado do cliente



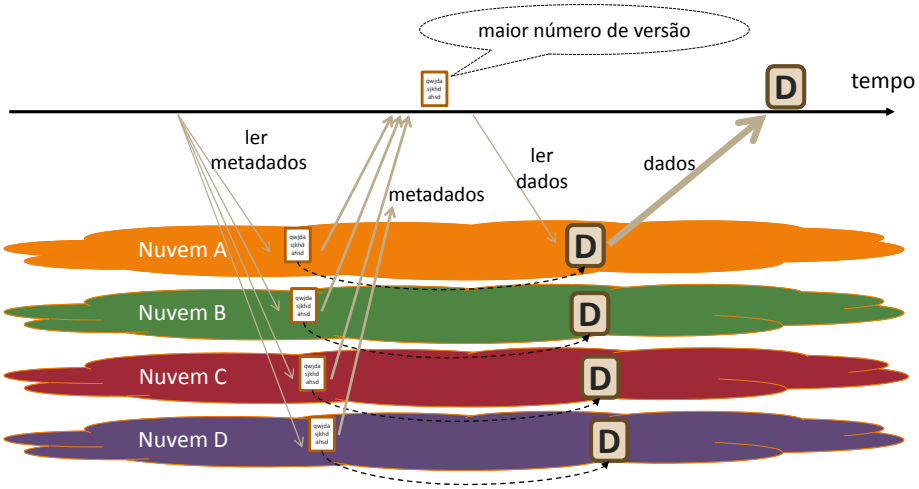
42

Protocol de escrita



43

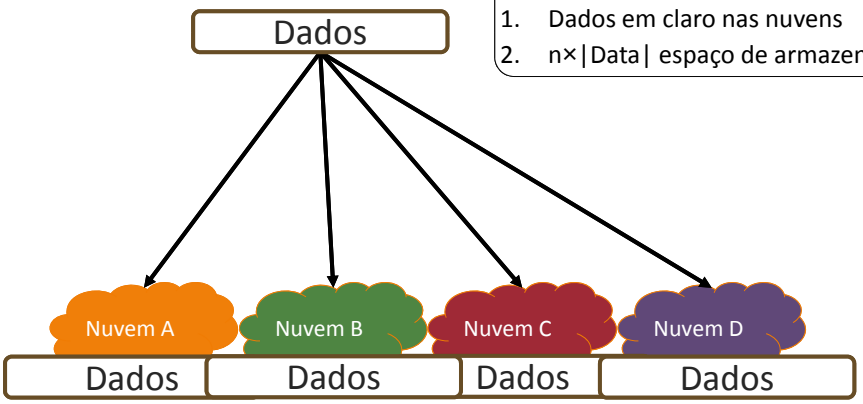
Protocolo de leitura



44

Limitações dessa versão

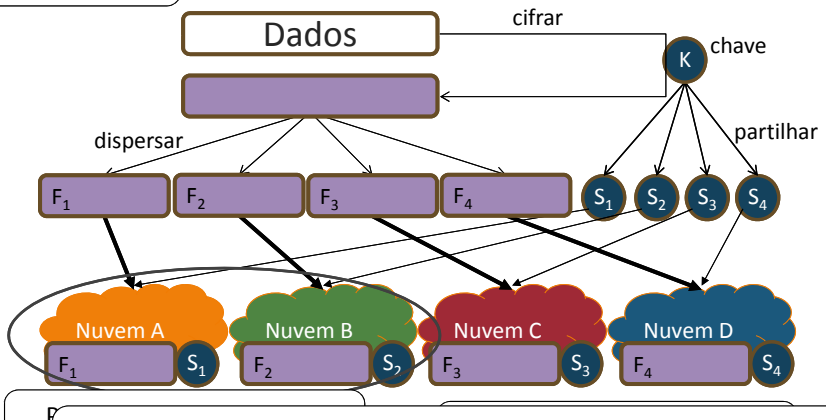
Limitações
1. Dados em claro nas nuvens
2. n×|Data| espaço de armazen.



45

Erasure codes / secret sharing

Só para dados, não meta-dados



Dados cifrados, não podem ser lidos na nuvem!

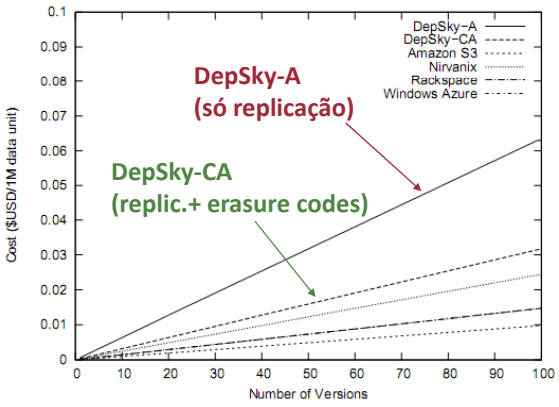
Dobro do espaço de armazenamento, não 4 vezes!

Avaliação de desempenho

- Protótipo: ~3000 LOCs (Java), REST API, HTTPS
- DepSky, 2 versões: **A** (*availability*), **CA** (av. + *confidentiality*)
- Ambiente experimental
  - 4 nuvens comerciais: **S3** (Amazon S3), **WA** (Windows Azure), **NX** (Nirvanix SDN) and **RS** (Rackspace)
  - Clientes em 8 máquinas do PlanetLab por todo o mundo
  - 3 clientes/máquina a ler/escrever ficheiros 100KB, 1M, 10M
  - 437000+ leituras/escritas em finais de 2010

47

Custo de armazenamento

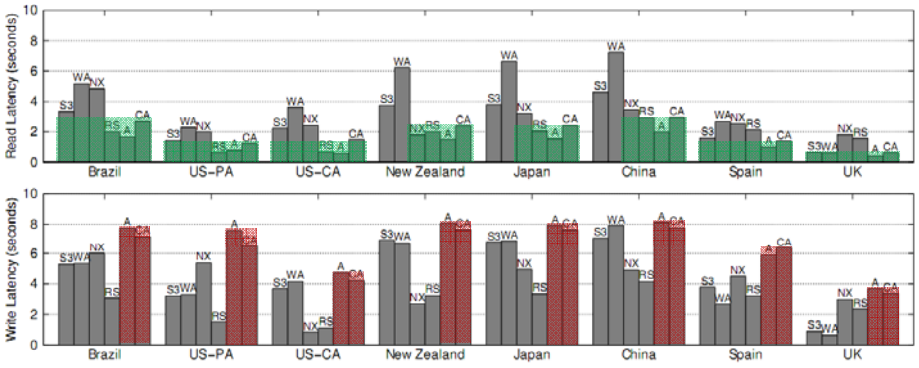


custo DepSky-CA ≈ 2×(custo médio das nuvens)

48

Latência (100KB)

A latência de **leitura** é próxima da **melhor** latência



A latência de **escrita** é próxima da **pior** latência

49

Disponibilidade medida

Location	Reads Tried	DepSky-A	DepSky-CA	Amazon S3	Rackspace	Azure	Nirvanix
Brazil	8428	1.0000	0.9998	1.0000	0.9997	0.9793	0.9986
US-PA	5113	1.0000	1.0000	0.9998	1.0000	1.0000	0.9880
US-CA	8084	1.0000	1.0000	0.9998	1.0000	1.0000	0.9996
New Zealand	8545	1.0000	1.0000	0.9998	1.0000	0.9542	0.9996
Japan	8392	1.0000	1.0000	0.9997	0.9998	0.9996	0.9997
China	8594	1.0000	1.0000	0.9997	1.0000	0.9994	1.0000
Spain	6550	1.0000	1.0000	1.0000	1.0000	0.9796	0.9995
UK	7069	1.0000	1.0000	0.9998	1.0000	1.0000	1.0000

- Disponibilidade = nº operações c/sucesso / pedidas
- Dois factores: disponibilidade da nuvem e da internet

50

CONCLUSÕES

51

Conclusões

- Nuvem: uma oportunidade para as empresas e organizações
- Segurança da nuvem: um factor a ter em conta
  - Várias ameaças, vimos 9
  - Não é gratuita, vários passos: requisitos, risco, fornecedor, contrato, controles, monitorizar
  - Provavelmente melhor do que a de SMEs
  - Dados (muito) críticos talvez não devam ir para a nuvem
  - Muita investigação interessante em curso

52

Obrigado! Perguntas?

- Página pessoal – *http://homepages.gsd.inesc-id.pt/~mpc/*
- Projecto RC-Clouds – *http://rcclouds.gsd.inesc-id.pt/*

TÉCNICO LISBOA

inesc id lisboa