SECURITY MEETING

6ª Edição - 10 de Maio de 2013
Auditório Agostinho da Silva
Campo Grande 376, 1749-024 Lisboa, Portugal

Cloud Security

Miguel P. Correia
Instituto Superior Técnico / INESC-ID

TÉCNICO LISBOA

FCT

inesc id lisboa

Nuvem: *computing as a utility*

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

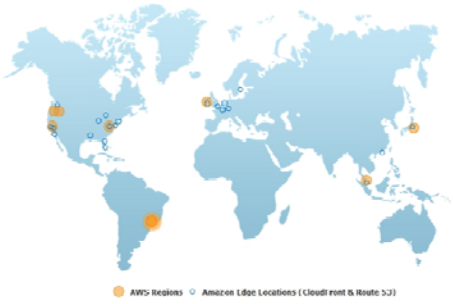
2

Nuvem: por trás da ficha

- Centros de dados de grandes dimensões…
  - Google: 900 mil servidores
  - Microsoft: 500 mil
  - …

Microsoft's Chicago datacenter

…espalhados por todo o mundo



datacenters da Amazon

Modelos de serviço

- Infrastructure as a Service (IaaS)
  - Serviço = alojamento de máquinas virtuais (VMs) ou storage
  - Ex: Amazon EC2/S3, IBM SmartCloud, Rackspace Cloud, MS SkyDrive
- Platform as a Service (PaaS)
  - Serviço = execução de aplicações num ambiente específico
  - Ex: Google AppEngine, Force.com, Windows Azure
- Software as a Service (SaaS)
  - Ex: Gmail, Google Drive, Microsoft Office 365, Yahoo Mail
- a moda do *aaS pegou: XaaS, CaaS, NaaS, MaaS, DaaS, FaaS,…

Modelos de implementação

- Nuvem pública
  - existe um fornecedor de serviço e clientes
- Nuvem privada
  - nuvem pertence à organização que a utiliza
- Nuvem comunitária
  - nuvem privada de um conjunto de organizações com interesses comuns
- Nuvem híbrida
  - combinação de nuvens de 2 dos modelos anteriores

5

Tópicos

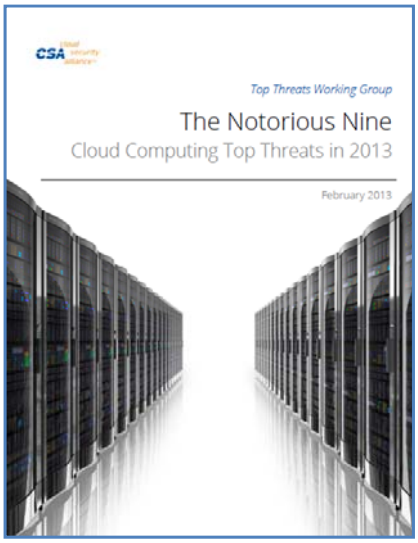
1. Insegurança na nuvem
2. Segurança na nuvem
3. Sistema DepSky

6

1. INSEGURANÇA NA NUVEM

7

Ameaças à/na nuvem



8

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 ou no software de gestão permite acesso de atacante aos dados de vários clientes
  - *"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)

2. Perda de dados

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

Ma.gnolia Suffers Major Data Loss, Site Taken Offline

By Michael Calore | January 30, 2009 | 12:56 pm | Categories: Uncategorized

ma.gnolia

Cloud computing takes hit in Sidekick data loss

Share |

The "cloud" turned stormy for Microsoft Corp. this weekend, after a technical glitch apparently wiped out personal data for users of the T-Mobile Sidekick smartphone.

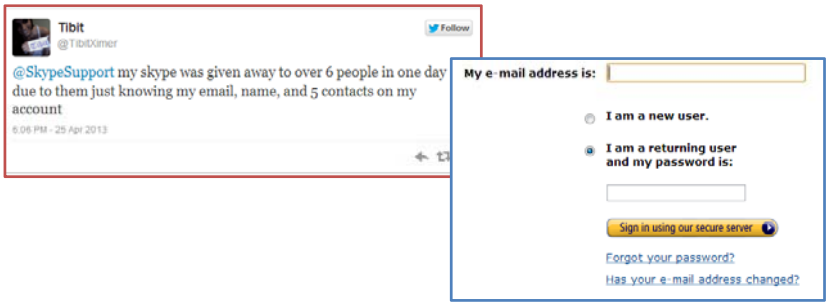
A Microsoft unit aptly named Danger Inc. based its operation on the cloud model, which provides computing power and storage at big remote datacenters.

In theory, if the phones were lost or destroyed, the photos, contacts, to-do lists and calendars still would be available. That supposedly offered a big advance in safety, security and efficiency.

10

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



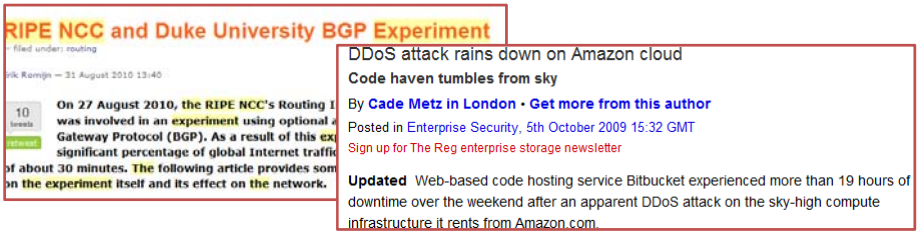
4. APIs inseguras

- Na nuvem a superfície de ataque de uma aplicação é expandida com a interface de gestão
  - Interface web, *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 (Georgiev et al., ACM CCS'12)

12

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

Erik Romijn — 31 August 2010 13:46

10 tweets retweet

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

15

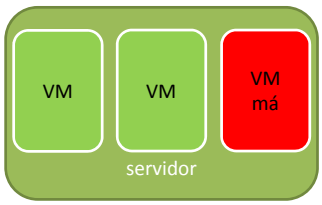
8. Diligência insuficiente

- 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 a facilidade de mudar para outro fornecedor (*vendor lock-in*)?

16

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

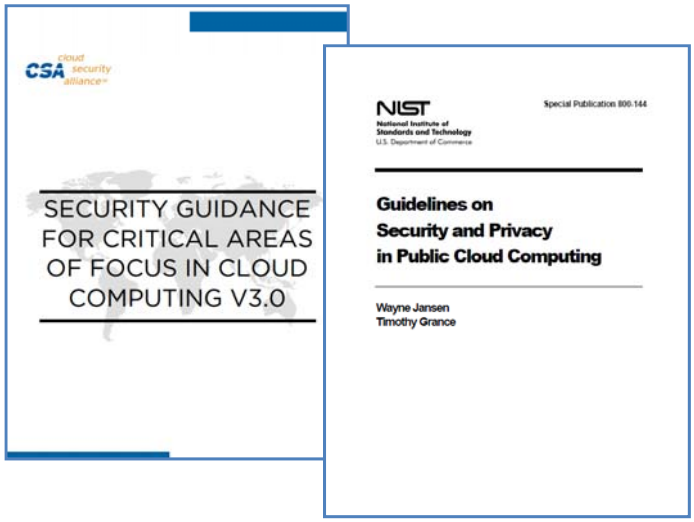


17

2. SEGURANÇA NA NUVEM

18

Boas práticas de segurança



19

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

20

Segurança na nuvem: 6 fases

1. Especificar requisitos
2. Avaliar o risco
3. Avaliar a fiabilidade do fornecedor
4. Exprimir os requisitos no contrato
5. Criar controles
6. Avaliar o desempenho

21

1. 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?

22

2. Risco de mudar para a nuvem

- Analisar dados a pôr na nuvem
  - Informação pessoal (privacidade)
  - 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

23

3. 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

4. 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

25

5. 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)

26

6. Avaliar o desempenho

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

27

3. SISTEMA DEPSKY

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

28

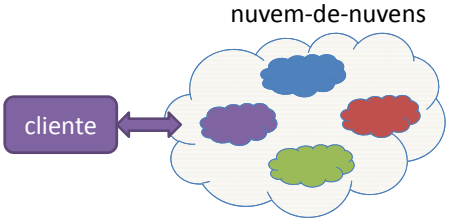
Falhas acontecem

- 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 *vendor lock-in*?
- Solução: não confiar numa nuvem

29

DepSky: nuvem-de-nuvens

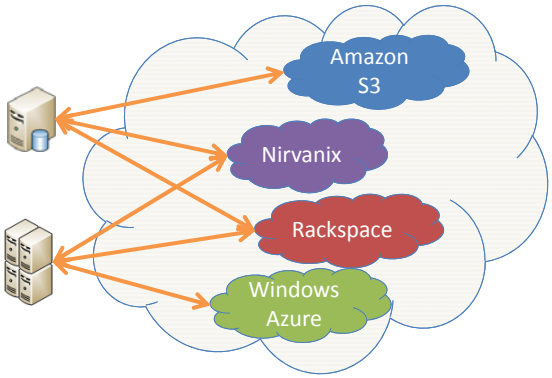
- Ideia: não confiar numa nuvem, confiar no conjunto
  - Replicação+diversidade para tolerância a faltas
- DepSky – nuvem-de-nuvens para armazen. de dados; tolera:
  - Corrupção de dados numa nuvem
  - Indisponibilidade de uma nuvem
  - Violação de dados (cifrando)
  - *Vendor lock-in*
  - Bónus: leituras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



30

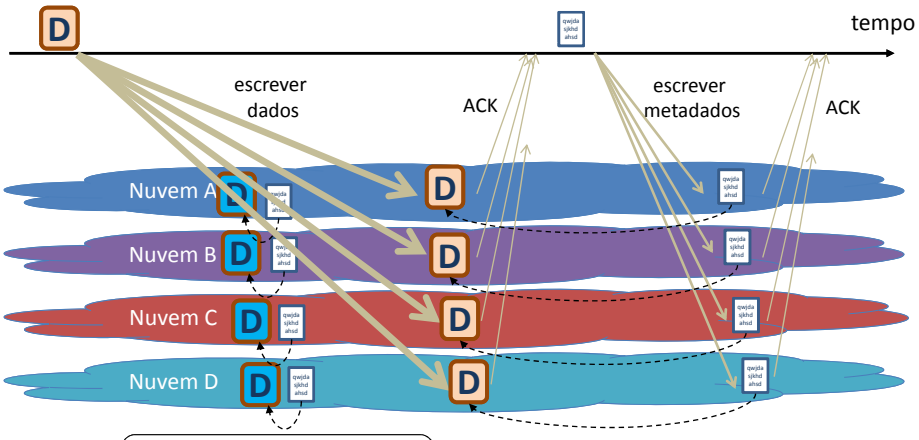
DepSky

- 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



31

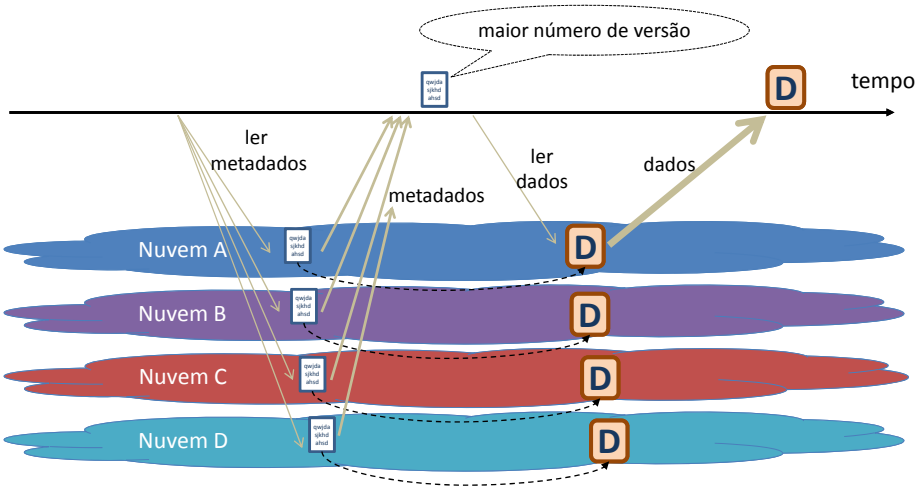
Protocol de escrita



Assumir já guardada uma versão do ficheiro

32

Protocolo de leitura

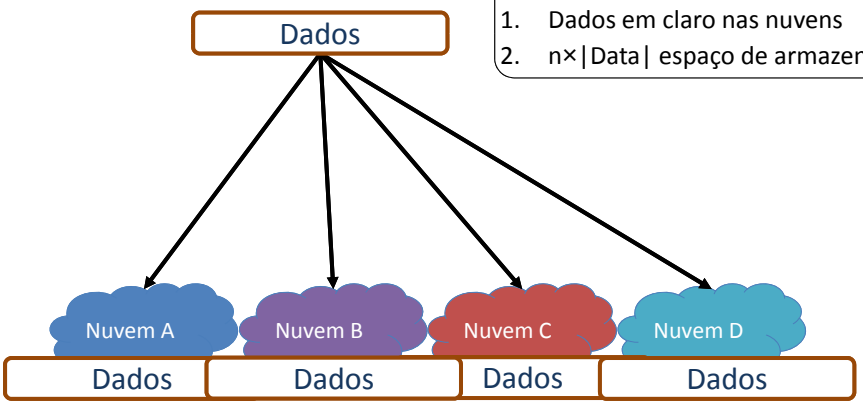


Dados obtidos de outras nuvens se for preciso

33

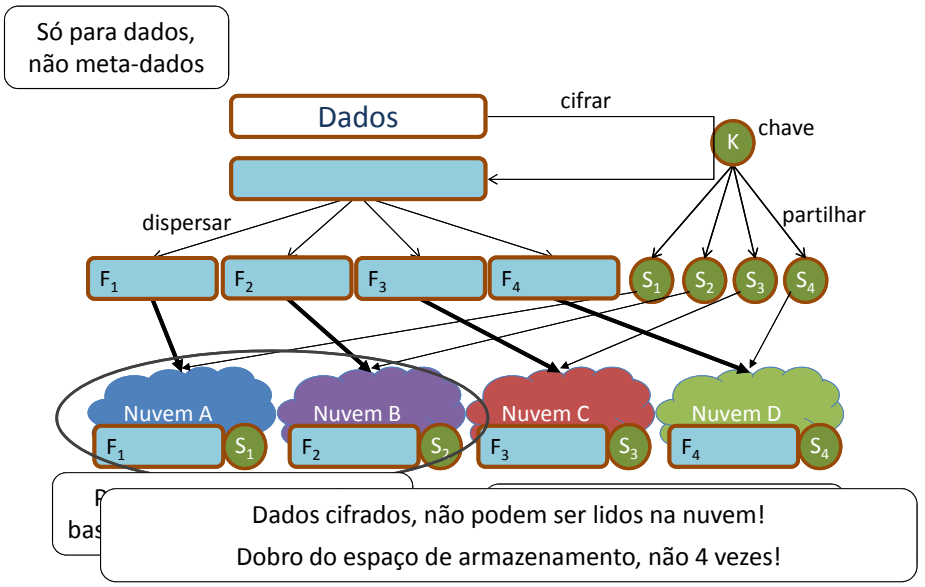
Limitações dessa versão

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



34

Erasure codes / secret sharing

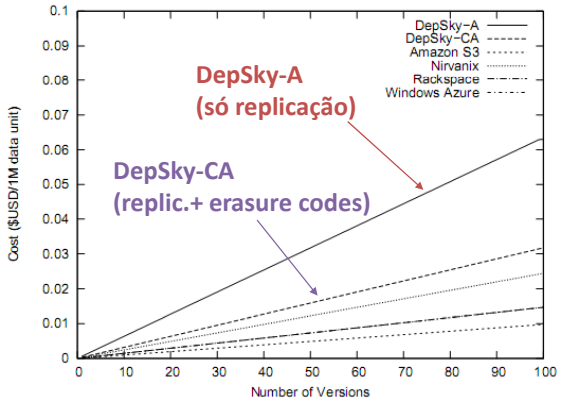


Avaliação de desempenho

- 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

36

Custo de armazenamento

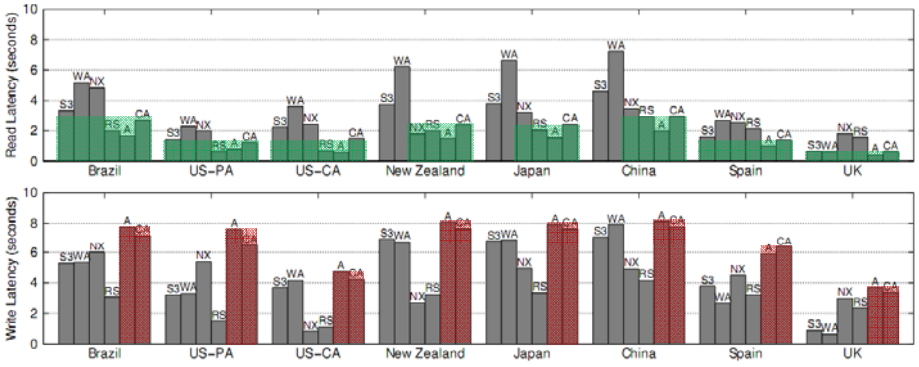


custo DepSky-CA ≈ 2×(custo médio das nuvens)

37

Latência (100KB)

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



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

38

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 com sucesso / pedidas
- Dois factores: disponibilidade da nuvem e da internet

39

CONCLUSÕES

40

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

41

SECURITY MEETING

Página pessoal – http://homepages.gsd.inesc-id.pt/~mpc/

Projecto RC-Clouds – http://rcclouds.gsd.inesc-id.pt/

Blog – http://www.seguranca-informatica.net/

TÉCNICO LISBOA

inesc id lisboa