

Cloud Computing Security Considerations

Joe St Sauver, Ph.D.
Security Programs Manager, Internet2
joe@uoregon.edu or joe@internet2.edu

Internet2 Joint Techs
Salt Lake City, Utah
4:10-4:30PM, Tuesday, 2/2/2010

<http://www.uoregon.edu/~joe/cloud-computing-security/>

Disclaimer: all opinions strictly my own.

Introduction

Some Cautions About Today's Talk/Topic

- As you likely already know, there's a LOT of hype associated with cloud computing. I'm sorry about that (but I can't fix that)
- Cloud computing is a huge topic. It encompasses diverse models and technologies, even though users and the trade press tend to lump them under a common name. Covering all potential security issues in 20 minutes is simply impossible.
- For that matter, please note that we're still discovering many of the security issues which will challenge cloud computing!
- Why? In part, that's because cloud computing is still a work-in-progress. Because it is rapidly evolving, what I tell today you may quickly become irrelevant or obsolete.
- Nonetheless, there's so much thrust behind cloud computing that we simply don't have the option of sitting back and waiting to understand address cloud computing security issues.

What's Driving Cloud Computing? Drivers Include...

- Thought leaders: Amazon, Google, Microsoft and many other Internet thought leaders have all aligned behind the cloud
- The economy: Because cloud computing should theoretically help sites avoid major new capital expenditures (capex) while also controlling some ongoing operational expenses (opex), cloud computing is potentially a "lifesaver" for financially strapped businesses, including many major universities.
- The Feds: Cloud computing has *substantial* momentum in Washington DC: it was featured in the just-released federal IT budget; Vivek Kundra, the federal CIO, has championed creation of <http://apps.gov/>, a “one-stop shop” for cloud computing services for federal agencies; DISA has created a very successful cloud computing project called “RACE;” and Howard Schmidt, the new federal cyber security coordinator, has said that securing cloud computing will be a top priority.⁴

Federal IT Budget Grows To \$79.4 Billion

Tech spending in the U.S. government's just-released fiscal 2011 budget will go toward open government, cloud computing, cybersecurity, procurement, and performance management.

By J. Nicholas Hoover, [InformationWeek](#)

Feb. 1, 2010

URL: <http://www.informationweek.com/story/showArticle.jhtml?articleID=222600650>

President Obama's fiscal 2011 budget includes \$79.4 billion for federal IT spending, a 1.2% bump from the \$78.4 billion 2010 budget level.

That number includes bullet point like \$364 million for the operations of the Department of Homeland Security' National Cyber Security Division, a 30% increase in the budget for the Federal Aviation Administration's next-generation air traffic control system, new spending on health IT and increased spending to upgrade IT at the Small Business Administration.

The budget also lays out a number of key administration strategies for IT over the next year. For example, data center glut has become a major problem for the federal government, with the number of federal data centers jumping from 432 in 1998 to more than 1,100 last year, and the administration hopes to reverse this trend, it notes in the budget. Though the timing is unclear, the Office of Management and Budget plans to release a strategy to reduce both the number and cost of federal data centers.

The budget paints government cloud computing efforts -- which federal CIO Vivek Kundra has looked toward as a partial solution to some of the government's data center problems -- with a broad brush, saying only that, "after evaluation in 2010, agencies will deploy cloud computing solutions across the government" and pointing to both Apps.gov and the importance of security in cloud computing.

Apps.Gov (Currently a Bit of A Work In Progress)

The screenshot shows the Apps.Gov website interface. At the top, there's a navigation bar with links for Home, Business Apps, Productivity Apps, Cloud IT Services, and Social Media Apps. On the right side of the header, there are links for Welcome, Register, Log In, a shopping cart icon showing 0 items for \$0.00, and Contact Us, Cloud FAQs, and Vendor FAQs.

In the main content area, the URL is HOME > Cloud IT Services. There's a search bar with the placeholder "SEARCH FOR" and a dropdown menu set to "All Categories".

Cloud IT Services

You've got servers, storage, development, testing, and production teams - and on it goes. Need a better solution to reduce cost and implement projects faster? Try GSA's Cloud IT Services where you get storage, webhosting, and virtual machines - all hosted in the cloud!

The page features three service cards:

- Cloud storage**: Get scalable storage of your data on the cloud rather than on your own dedicated servers. Status: Coming Soon.
- Virtual machines**: The processing power that you need for your website or application on the cloud. Status: Coming Soon.
- Web hosting**: Hosting of your web applications on the cloud - 24x7. Status: Coming Soon.

[Home](#) | [Register](#) | [Order History/Status](#) | [Cloud FAQs](#) | [Vendor FAQs](#) | [Contact Us](#)

*** WARNING ***

This is a U.S. General Services Administration computer system that is "FOR OFFICIAL USE ONLY." This system is subject to monitoring. Therefore, no expectation of privacy is to be assumed. Individuals found performing unauthorized activities are subject to disciplinary action including criminal prosecution.

[Privacy and Security](#)

DISA's RACE

www.disa.mil/race/  Google

THIS IS THE RAPID ACCESS COMPUTING ENVIRONMENT.

Brought to you by DISA's Computing Services Directorate.
Developmental testing has never been so simple.

With RACE, you can customize, purchase, and receive your platform within 24 hours. You can now order RACE Development, Test, and Production virtual environments to support your life cycle requirement.

This quick-turn computing solution uses the revolutionary technology of cloud computing to give you the platform that you need today, quickly, inexpensively and, most importantly, securely. All you need is a government credit card or completed MIPR.

So if you're tired of wasting time, energy, and money developing on less accommodating, less scalable platforms, **get in the RACE.**


FAST. SECURE. FLEXIBLE.

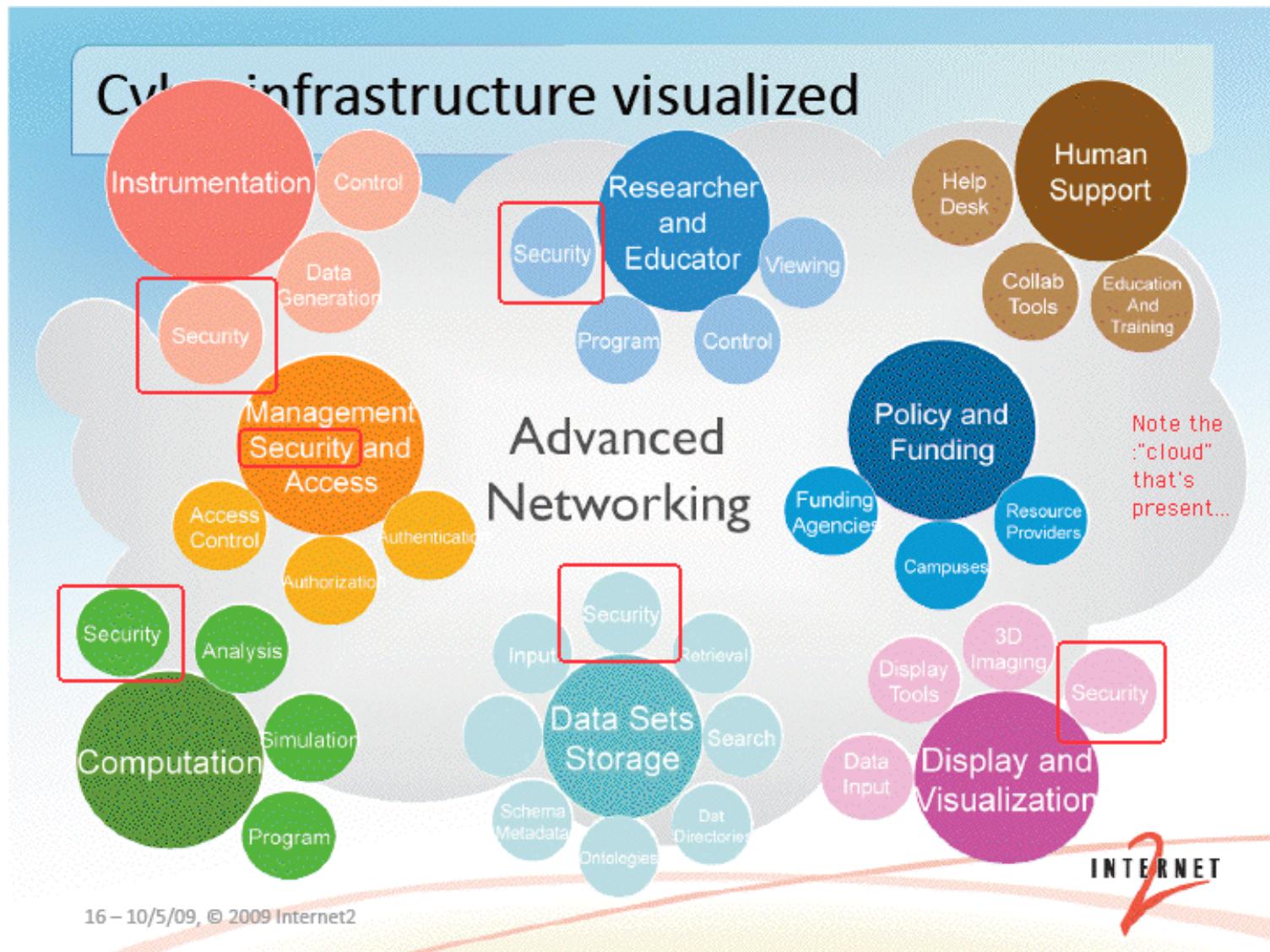


Offers You the Pole Position in Developmental and User Testing:	Road-Tested and Secure Computing Environment:
<ul style="list-style-type: none">• 24-hour provisioning• Online self-service• Credit card or MIPR payment options• Month-to-month service• Capacity on demand• No annual maintenance fees• No capital investment required• Pay only for what you need• 365/24/7 service desk support• Costs per month/image	<ul style="list-style-type: none">• DECC standard platforms• Developed under DoD IA standards• NIPR connectivity• Multiple virtual configurations available: 1-4 CPU, 1-8 GB memory, 60 GB of storage• LAMP stack• STIG'd (Application Development STIG) operating environment• Your choice of operating environments:<ul style="list-style-type: none">◦ MS Windows◦ Red Hat Linux

Our Community Is Also Pressing Ahead

- Cloud computing seem to be turning up on pretty much every networking and security mailing list I'm on
- You've heard/will be hearing a number of cloud computing talks during this week's meeting, which is probably not surprising since cloud computing was one of Joint Tech's explicit focus areas.
- But I'm seeing clouds everywhere, not just here at Joint Techs.
- Heck, I'm even seeing "clouds" (with frequent references to security!) appear in things like the last Internet2 Member Meeting "Introduction to Internet2" talk

"Cyberinfrastructure Visualized: A Cloud, With Lots of "Security" References"



Why Is "Security" Everywhere on That Slide?

- Security is generally perceived as a huge issue for the cloud:

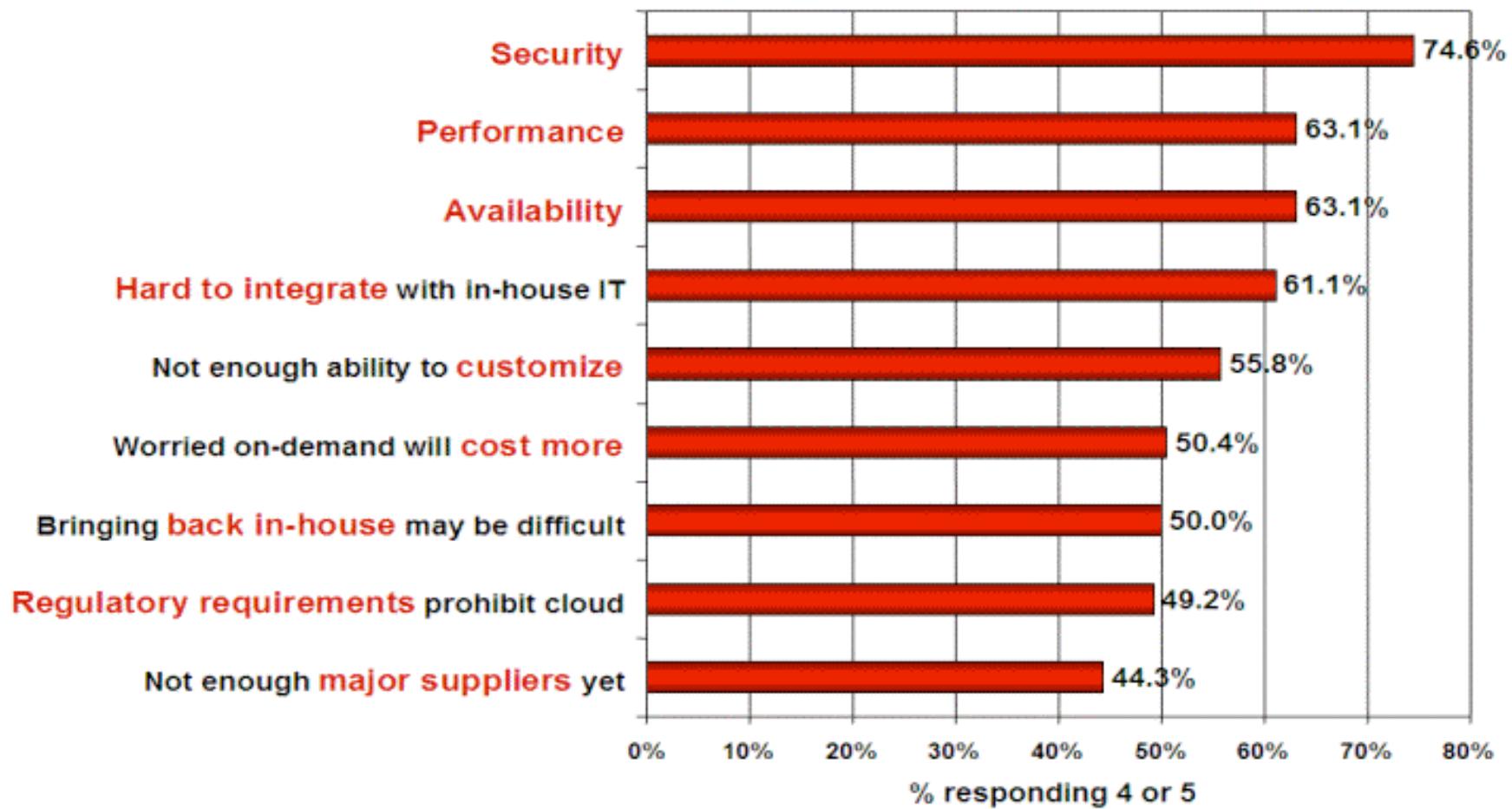
During a keynote speech to the Brookings Institution policy forum, “Cloud Computing for Business and Society,” [Microsoft General Counsel Brad] Smith also highlighted data from a survey commissioned by Microsoft measuring attitudes on cloud computing among business leaders and the general population.

*The survey found that while 58 percent of the general population and 86 percent of senior business leaders are excited about the potential of cloud computing, **more than 90 percent of these same people are concerned about the security, access and privacy of their own data in the cloud.***

Another Data Point for Clouds and Security

Q: Rate the challenges/issues ascribed to the 'cloud'/on-demand model

(1=not significant, 5=very significant)



Source: IDC Enterprise Panel, August 2008 n=244

Source: <http://www.csric.nist.gov/groups/SNS/cloud-computing/cloud-computing-v26.ppt>
at slide 17

Cloud Computing Is Many Different Things to Many Different People

- All of the following have been mentioned from time to time as examples of “cloud computing:”
 - Amazon Web Services including the Elastic Compute Cloud (EC2), Amazon Simple Storage Service (S3), etc.)
 - Rackspace Cloud (formerly Mosso)
 - Google’s App Engine
 - Windows’ Azure Platform (production/for-fee as of today!)
 - the OGF (including its Open Cloud Computing Interface)
 - SETI@Home, Folding@Home, distributed.net, etc.
 - outsourced campus email service (to Gmail or Live.com), or outsourced spam filtering (e.g., to Postini or Ironport)
 - use of virtualization (e.g., VMware) to host departmental systems either on local servers, or on outsourced VPS
- In reality, some of those activities are not (strictly speaking) what's usually defined as "cloud computing,"

Some Generally Accepted Characteristics

- Most people would agree that true cloud computing...
 - usually has low or zero up front capital costs
 - largely eliminates operational responsibilities (e.g., if a disk fails or a switch loses connectivity, you don't need to fix it)
 - for the most part, cloud computing eliminates knowledge of WHERE one's computational work is being done; your job is being run "somewhere" out there in the "cloud"
 - offers substantial elasticity and scalability: if you initially need one CPU, that's fine, but if you suddenly need 999 more, you can get them, too (and with very little delay!) If/when demand drops, you can scale your usage back, too
 - cloud computing leverages economies of scale (running mega data centers with tens of thousands of computers is far less expensive (per computer) than running a small machine room with just a modest cluster of systems)

Some "Clouds" Won't Necessarily Have All of Those Characteristics

- For instance, if your site is running a **local private cloud**:
 - there WILL be capital expenditures up front,
 - you (or someone at your site) WILL still care about things like hardware failures, and
 - you likely WON'T have the illusion of a seemingly infinite inventory of processors (or memory or disk)

Nonetheless, a local private cloud service may functionally work the same way as a public cloud service, and hybrid cloud models may even combine private and public cloud services in a fairly seamless way.

- Ubuntu's enterprise cloud offering is a nice example of this.

Cloud computing on Ubuntu | Ubuntu

http://www.ubuntu.com/cloud

Cloud computing on Ubuntu | Ubu... +

ubuntu

▶ Ubuntu ▶ Server ▶ **Cloud** ▶ Support ▶ Community ▶ Partners ▶ News

Why Ubuntu? Private cloud Public cloud Consulting Training Support Management

Ubuntu private cloud is compatible with the Amazon EC2 public cloud

- Immediacy and elasticity behind the firewall
- Migrate between public and private clouds easily
- Burst to public clouds when needed

[Why Ubuntu?](#)

[Private Cloud »](#)

Ubuntu Enterprise Cloud

Private clouds offer immediacy and elasticity in your own IT infrastructure. Using Ubuntu

[Public Cloud »](#)

Ubuntu on Amazon EC2

Amazon's Elastic Computing (EC2) cloud allows you to build on-demand virtual systems with

Will Your Campus Offer Private Cloud Services?

- If you haven't been thinking about offering private cloud services, I would suggest that you might want to, including thinking hard about any potential security issues associated with doing so.

So What About *Security* in the Cloud?

For the remainder of this talk, we'll outline some of the security issues you might run into when using cloud computing

In Some Ways, "Cloud Computing Security" Is No Different Than "Regular Security"

- For example, many applications interface with end users via the web. All the normal OWASP web security vulnerabilities -- things like SQL injection, cross site scripting, cross site request forgeries, etc., -- all of those vulnerabilities are just as relevant to applications running on the cloud as they are to applications running on conventional hosting.
- Similarly, consider physical security. A data center full of servers supporting cloud computing is internally and externally indistinguishable from a data center full of "regular" servers. In each case, it will be important for the data center to be physically secure against unauthorized access or potential natural disasters, but there are no special new physical security requirements which suddenly appear simply because one of those facilities is supporting cloud computing

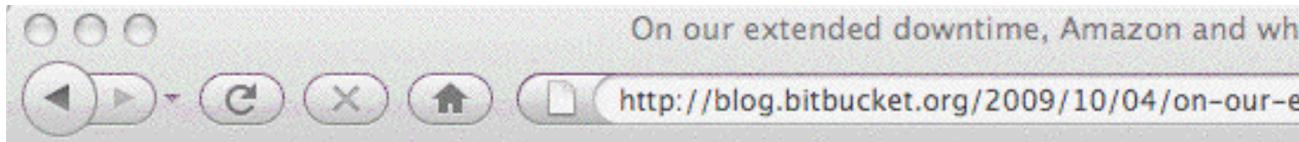
There Are Some Unique Cloud-Related Areas Which We're NOT Going To Worry About Today

- Contracting for Cloud Services: Even though contractual terms (including things like SLAs) can be used to mitigate some risks, I'm not a lawyer, and I'm not going to pretend to be one, so we're not going to cover issues related to contracting for cloud services. Fortunately, NACUA did a great job discussing this topic in a recent seminar, see www.nacua.org/meetings/VirtualSEminars/december2009/home.html
- Compliance, Auditing and eDiscovery: Because this meeting is primarily about research and education, not business processes and university administration, we will not consider the potential need for cloud computing to be compliant with Payment Card Industry security standards, FERPA, HIPAA, GLBA, or other related compliance mandates.
- So what are some cloud-related security issues?

The "A" in The Security "C-I-A" Objectives

- Computer and network security is fundamentally about three goals/objectives:
 - confidentiality (C)
 - integrity (I), and
 - availability (A).
- **Availability is the area where cloud based infrastructure appears to have had its largest (or at least most highly publicized) challenges to date.**
- For example, consider some of the cloud-related outages which have been widely reported...

Bitbucket, DDoS'd Off The Air



On our extended downtime, Amazon and what's coming

As many of you are well aware, we've been experiencing some serious downtime the past couple of days. Starting Friday evening, our network storage became virtually unavailable to us, and the site crawled to a halt.

We're hosting everything on Amazon EC2, aka. "the cloud", and we're also using their EBS service for storage of everything from our database, logfiles, and user data (repositories.)

Amazon EBS is a persistent storage solution for EC2, where you get high-speed (and free) connectivity from your instances, while it's also replicated. That gives you a lot for free, since you don't have to worry about hardware failure, and you can create periodic "snapshots" of your volumes easily.

While we were down, it was unknown to us what exactly the problem was, but it was almost certainly a problem with the EBS store. We've been working closely with Amazon the past 24 hours resolving the issue, and this post will outline what exactly went wrong, and what was done to remedy the problem.

Symptoms

What we were seeing on the server was high load, even after turning off anything that took up CPU. Load is a result of stuff "waiting to happen", and after reviewing iostat, it became apparent that the "bio wait" was very high, while the "I/O" connections per second was very low for our

Maintenance Induced Cascading Failures



More on today's Gmail issue

Tuesday, September 01, 2009 6:59 PM

Posted by Ben Treynor, VP Engineering and Site Reliability Czar

Gmail's web interface had a widespread outage earlier today, lasting about 100 minutes. We know how many people rely on Gmail for personal and professional communications, and we take it very seriously when there's a problem with the service. Thus, right up front, I'd like to apologize to all of you — today's outage was a Big Deal, and we're treating it as such. We've already thoroughly investigated what happened, and we're currently compiling a list of things we intend to fix or improve as a result of the investigation.

Here's what happened: This morning (Pacific Time) we took a small fraction of Gmail's servers offline to perform routine upgrades. This isn't in itself a problem — we do this all the time, and Gmail's web interface runs in many locations and just sends traffic to other locations when one is offline.

However, as we now know, we had slightly underestimated the load which some recent changes (ironically, some designed to improve service availability) placed on the request routers — servers which direct web queries to the appropriate Gmail server for response. At about 12:30 pm Pacific a few of the request routers became overloaded and in effect told the rest of the system "stop sending us traffic, we're too slow!". This transferred the load onto the remaining request routers, causing a few more of them to also become overloaded, and within minutes nearly all of the request routers were overloaded. As a result, people couldn't access Gmail via the web interface because their requests couldn't be routed to a Gmail server. IMAP/POP access and mail processing continued to work normally because these requests don't use the same routers.

It's Not Just The Network: Storage Is Key, Too

T-Mobile: we probably lost all your Sidekick data

By Chris Ziegler posted Oct 10th 2009 3:45PM

BREAKING



Well, this is shaping up to be one of the biggest disasters in the history of cloud computing, and certainly the largest blow to Danger and the Sidekick platform: T-Mobile's now reporting that personal data stored on Sidekicks has "almost certainly has been lost as a result of a [server failure](#) at Microsoft/Danger." They're still looking for a way to recover it, but they're not giving users a lot of hope -- meanwhile, servers

See <http://www.engadget.com/2009/10/10/t-mobile-we-probably-lost-all-your-sidekick-data/>

However, see also: Microsoft Confirms Data Recovery for Sidekick Users
<http://www.microsoft.com/Presspass/press/2009/oct09/10-15sidekick.mspx>

And Let's Not Forget About Power Issues

The screenshot shows a web browser window with the URL <http://www.datacenterknowledge.com/archives/2009/06/11/lightning-strike-triggers-amazon-ec2-outage>. The page title is "Lightning Strike Triggers Amazon EC2 Outage". Below the title, it says "June 11th, 2009 : Rich Miller". The main content discusses an outage at Amazon's EC2 service due to a lightning strike, which affected customers in one availability zone for over four hours before being resolved.

Lightning Strike Triggers Amazon EC2 Outage

June 11th, 2009 : Rich Miller

Some customers of Amazon's EC2 cloud computing service were offline for more than four hours Wednesday night after an electrical storm damaged power equipment at one of the company's data centers. The problems began at about 6:30 pm Pacific time, and most affected customers were back online by 11 p.m., according to Amazon's [status dashboard](#). The company said the outage was limited to customers in one of Amazon's four availability zones in the U.S.

"A lightning storm caused damage to a single Power Distribution Unit (PDU) in a single Availability Zone, the company reported. "While most instances were unaffected, a set of racks does not currently have power, so the instances on those racks are down. We have technicians on site, and we are working to replace the affected PDU."

EC2 previously experienced extended outages in [February 2008](#) and [October 2007](#).

Mitigating Cloud Computing Availability Issues

- Risk analysts will tell you that when you confront a risk, you can try to eliminate the risk, you can mitigate/minimize the impact of the risk, or you can simply accept the risk.
- If you truly require non-stop availability, you can try using multiple cloud providers, or you could use public and private cloud nodes to improve redundancy.
- Some cloud computing services also offer service divided into multiple "regions." By deploying infrastructure in multiple regions, isolation from "single-region-only" events (such as the power outage mentioned previously) can be obtained.
- Availability issues may also be able to be at least partially mitigated at the application level by things like local caching.
- Sometimes, though, it may simply make financial sense for you to just accept the risk of a rare and brief outage.
(Remember, 99.99 availability==> 52+ minutes downtime⁵/yr)

Mitigating Data Loss Risks

- The risk of data loss (as in the T-Mobile Sidekick case) is an exception to the availability discussion on the preceding slide. Users may be able to tolerate an occasional service interruption, but non-recoverable data losses can kill a business.
- Most cloud computing services use distributed and replicated global file systems which are designed to insure that hardware failures (or even loss of an entire data center) will not result in any permanent data loss, but I believe there is still value in doing a traditional off site backup of one's data, whether that data is in use by traditional servers or cloud computing servers.
- When looking for solutions, make sure you find ones that backs up data FROM the cloud (many backup solutions are meant to backup local data TO the cloud!)

Cloud Computing And Perimeter Security

- While I'm not a huge fan of firewalls (as I've previously discussed at the Spring 2008 I2MM in "Cyberinfrastructure Architectures, Security and Advanced Applications," see <http://www.uoregon.edu/~joe/architectures/architecture.pdf>), at least some sites do find value in sheltering at least some parts of their infrastructure behind a firewall.
- There may be a misconception that cloud computing resources can't be sheltered behind a firewall (see for example "HP's Hurd: Cloud computing has its limits (especially when you face 1,000 attacks a day)," Oct 20th, 2009, <http://blogs.zdnet.com/BTL/?p=26247>)
- Contrast that with "Amazon Web Services: Overview of Security Processes" (see the refs at the back). AWS has a mandatory inbound firewall configured in a default deny mode, and customers must explicitly open ports inbound,₂₇

Cloud Computing & Host-Based Intrusion Detection

- While I'm not very enthusiastic about firewalls, I am a big fan of well-instrumented/well-monitored systems and networks.
- Choosing cloud computing does not necessarily mean forgoing your ability to monitor systems for hostile activity. One example of a tool that can help with this task is OSSEC (the Open Source Host-Based Intrusion Detection System), an IDS which supports virtualized environments:



Virtualization/Vmware

OSSEC allows you to install the agent on the guest operating systems or inside the host (Vmware ESX). With the agent installed inside the VMware ESX you can get alerts about when a VM guest is being installed, removed, started, etc. It also monitors logins, logouts and errors inside the ESX server. In addition to that, OSSEC performs the CIS checks for Vmware, alerting if there is any insecure configuration option enabled or any other issue.

Cloud Computing Also Relies on the Security of Virtualization

- Because cloud computing is built on top of virtualization, if there are security issues with virtualization, then there will also security issues with cloud computing.
- For example, could someone escape from a guest virtual machine instance to the host OS? While the community has traditionally been somewhat skeptical of this possibility, that changed with Blackhat USA 2009, where Kostya Kortchinsky of Immunity Inc. presented "Cloudburst: A VMware Guest to Host Escape Story", see
<http://www.blackhat.com/presentations/bh-usa-09/KORTCHINSKY/BHUSA09-Kortchinsky-Cloudburst-SLIDES.pdf>
- Kostya opined: "VMware isn't an additional security layer, it's just another layer to find bugs in" [put another way, running a virtualization product increases the attack surface]

Choice of Cloud Provider

- Cloud computing is a form of outsourcing, and you need a high level of trust in the entities you'll be partnering with.
- It may seem daunting at first to realize that your application depends (critically!) on the trustworthiness of your cloud providers, but this is not really anything new -- today, even if you're not using the cloud, you already rely on and trust:
 - network service providers,
 - hardware vendors,
 - software vendors,
 - service providers,
 - data sources, etc.

Your cloud provider will be just one more entity on that list.

Cloud Provider Location

- You actually want to know (roughly) where your cloud lives.
- For example, one of the ways that cloud computing companies keep their costs low is by locating their mega data centers in locations where labor, electricity and real estate costs are low, and network connectivity is good.
- Thus, your cloud provider could be working someplace you may never have heard of, such as The Dalles, Oregon, where power is cheap and fiber is plentiful, or just as easily someplace overseas.
- If your application and data do end up at an international site, those systems will be subject to the laws and policies of that jurisdiction. Are you comfortable with that framework?
- Are you also confident that international connectivity will remain up and uncongested? Can you live with the latencies involved?

Cloud Provider Employees

- If you're like most sites, you're probably pretty careful about the employees you hire for critical roles (such as sysadmins and network engineers). But what about your cloud provider? If your cloud provider has careless or untrustworthy system administrators, the integrity/privacy of your data's at risk.
- How can you tell if your cloud provider has careful and trustworthy employees? Ask them!
 - Do backgrounds get checked before people get hired?
 - Do employees receive extensive in-house training?
 - Do employees hold relevant certifications?
 - Do checklists get used for critical operations?
 - Are system administrator actions tracked and auditable on a *post hoc* basis if there's an anomalous event?
 - Do administrative privileges get promptly removed when employees leave or change their responsibilities?

Cloud Provider Transparency

- You will only be able to assess the sufficiency of cloud provider security practices if the cloud provider is willing to disclose its security practices to you.
- If your provider treats security practices as a confidential or business proprietary thing, and won't disclose their security practices to you, you'll have a hard time assessing the sufficiency of their security practices. Unfortunately, you may need to consider using a different provider.
- Remember: "Trust, but verify." [A proverb frequently quoted by President Reagan during arms control negotiations]
- I'm not known for being a big Microsoft cheerleader, but Microsoft deserves recognition for promoting both their Cloud Computing Advancement Act and pressing cloud vendors to police themselves when it comes to transparency. See www.microsoft.com/presspass/presskits/cloudpolicy/

An Example of The Wrong Approach

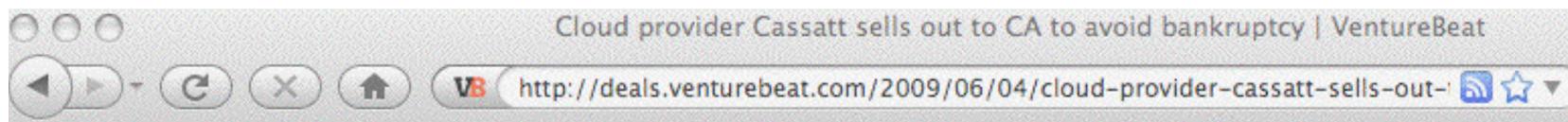
The screenshot shows a web browser window with the following details:

- Title Bar:** Cloudsecurity.org Interviews Guido van Rossum: Google App Engine, Python and Security
- Address Bar:** http://cloudsecurity.org/blog/2008/07/01/cloudsecurityorg-interviews-guido-van-rossum-google-app-engine-python-and-security.html
- Content Area:**
 - Section Header:** The Interview
 - Text:** *cloudsecurity.org: What security principles did you follow for App Engine?*
 - Text:** GvR: While I can't share any specifics on what we're doing to secure App Engine, I can say that the main principle we've followed could be called "defense in depth". We're not relying exclusively on a secure interpreter, or any other single security layer, to protect our users.
 - Text:** *cloudsecurity.org: Please provide some examples of how those principles played out in terms of the current implementation?*
 - Text:** GvR: Sorry, we don't divulge such information.

Source: <http://cloudsecurity.org/blog/2008/07/01/cloudsecurityorg-interviews-guido-van-rossum-google-app-engine-python-and-security.html>

Provider Failures Are Also A Real Possibility

- Even for a red-hot technology like cloud computing, there is no guarantee that your providers will financially survive. What will you do if your provider liquidates?



Cloud provider Cassatt sells out to CA to avoid bankruptcy

June 4, 2009 | Camille Ricketts | View commentsComments | Share | 0 tweet

Cassatt, the San Jose, Calif.-based provider of cloud computing environments, has sold its assets to public IT management firm CA for an undisclosed sum. The company has been in trouble for a while now, announcing its intentions to find a buyer back in April after burning through \$100 million in venture capital.

CA will also inherit select employees from Cassatt. The cloud company had been backed by Hewlett-Packard, In-Q-Tel, New Enterprise Associates, Portcullis Partners, Quatris Fund and Warburg Pincus, reports VentureWire.

Pen Testing; Working Incidents In The Cloud

- Standard pen testing processes which you may use on your own infrastructure may not be an option in an outsourced environment (the cloud provider may not be able to distinguish your tests from an actual attack, or your tests may potentially impact other users in unacceptable ways)
- If you do have a security incident involving cloud-based operations, how will you handle investigating and working that incident? Will you have the access logs and network traffic logs you may need? Will you be able to tell what data may have been exfiltrated from your application?
- What if your system ends up being the origin of an attack? Are you comfortable with your provider's processes for disclosing information about you and your processes/data?

OECD, The Cloud, and Privacy

Security, Privacy, and Accountability

41. *Privacy and security.* Many of the most successful and most visible applications of Cloud computing today are consumer services such as e-mail services, social networks, and virtual worlds. The companies providing these services collect terabytes of data, much of it sensitive, personal information, which then is stored in data centres in countries around the world. How these companies, and the countries in which they operate, address privacy issues will be a critical factor affecting the development and acceptance of Cloud computing.

42. Who will have access to billing records? Will government regulation be needed to allow anonymous use of the Cloud and to put strict controls on access to usage records of Cloud service providers? Will government regulators be able to adapt rules on the use of private, personal information when companies are moving terabytes of sensitive information from employees and customers across national borders? Companies that wish to provide Cloud services globally must adopt leading-edge security and auditing technologies and best-in-class practices. If they fail to earn the trust of their customers by adopting clear and transparent policies on how their customers' data will be used, stored, and protected, governments will come under increasing pressure to regulate privacy in the Cloud. And if government policy is poorly designed, it could stymie the growth of the Cloud and commercial Cloud services.

Cloud Computing and Public Policy, 14 October 2009

[http://www.olis.oecd.org/olis/2009doc.nsf/ENGDATCORPLOOK/NT00004FC6/\\$FILE/JT03270509.PDF](http://www.olis.oecd.org/olis/2009doc.nsf/ENGDATCORPLOOK/NT00004FC6/$FILE/JT03270509.PDF)

World Privacy Forum Privacy In The Clouds Report

From: "Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing,"
Released February 23, 2009, <http://www.worldprivacyforum.org/cloudprivacy.html>

I. Introduction and Summary of Findings.....	4
Cloud Computing Today: Issues and Implications	4
Findings	6
II. When Can a Business Share Information with a Cloud Provider?	8
HIPAA and Business Associate Agreements.....	8
Tax Preparation Laws.....	9
Violence Against Women Act	10
Legally Privileged Information	10
Professional Secrecy Obligations	10
III. Consequences of Third Party Storage for Individuals and Businesses.....	11
Compelled Disclosure to the Government.....	11
<i>United States v. Miller</i>	11
<i>Electronic Communications Privacy Act (ECPA)</i>	12
<i>USA PATRIOT Act</i>	14
Disclosure to Private Parties.....	14
<i>HIPAA and compelled disclosures</i>	14
<i>Fair Credit Reporting Act</i>	15
<i>Other privacy laws</i>	15
<i>Bankruptcy of a cloud provider</i>	16
<i>Trade secrets</i>	16
IV. Other Cloud Computing Issues.....	17
Terms of Service and Privacy Policy	17
<i>Scope of rights claimed by cloud service providers</i>	17
<i>Changeable terms of service</i>	18
<i>Termination of services</i>	18
Location of Cloud Data and Applicable Law.....	18
Ownership and Transfer of a Cloud Provider	20

Additional Cloud Computing Security Resources

- "AWS Security Whitepaper," http://s3.amazonaws.com/aws_blog/AWS_Security_Whitepaper_2008_09.pdf
- "Cloud Computing Security: Raining On The Trendy New Parade," BlackHat USA 2009,
www.isecpartners.com/files/Cloud.BlackHat2009-iSEC.pdf
- "ENISA Cloud Computing Risk Assessment," November 20th, 2009, www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport
- "Presentation on Effectively and Securely Using the Cloud Computing Paradigm v26," 10/7/2009, NIST,
<http://www.csrc.nist.gov/groups/SNS/cloud-computing/cloud-computing-v26.ppt>
- "Security Guidance for Critical Areas of Focus in Cloud Computing, V2.1," December 2009, Cloud Security Alliance,
<http://www.cloudsecurityalliance.org/csaguide.pdf>

Thanks for The Chance To Talk Today!

- Are there any questions?