

Look Before You Leap:

Some questions to ask about *Cloud Computing*

VASCAN Conference

October 5, 2009

Steve Werby, VCU

Jim Jokl, UVa



Why is it called “cloud” computing?

- Metaphor for the Internet
- Why a cloud?



What are the characteristics of cloud computing?

- Internet-based
- Service-based
- Elastic
- Subscriber business model
- Rapidly and easily provisioned
- Shared

Cloud Computing

Delivery models, benefits, reality

Some Cloud Service Delivery Models

- Application Level
 - Google and Microsoft Student Email
- Core Infrastructure Level
 - Amazon, etc, Virtual Machines
 - Rackspace.com & Physical Servers
- Services Engines
 - Example: Google Applications Engine
 - Traditionally hosting Python scripting
 - Now supports a Java environment too

Some Cloud Computing Benefits

- Scalability
 - A firm with a large installed base should be able grow you service quickly if demand surges
- Fast startup
 - Especially while a project is in “entrepreneur mode”
- Often includes additional license models
 - e.g., just pay for what you need/consume
- You are renting a service
 - No capital costs
 - Need less hard to find technical staff
 - Can back out of a service more easily

The Rose Colored Glasses Syndrome?

- Are all of the world's problems really solved by switching to cloud-based services?
- Some preliminary thoughts / considerations
 - During some “event”, who is the priority?
 - Lock-in
 - But can happen on the local software side too
 - How do you get your data out?
 - Service Shutdown: is your .com going away?
 - Operational \$ vs. Capital costs: who wins
 - Google and Microsoft campus email: cost vs. value
 - But what about the profit
 - Does centralized efficiency allow a company to make money and still give you a better deal?
- All of the normal outsourcing questions still apply

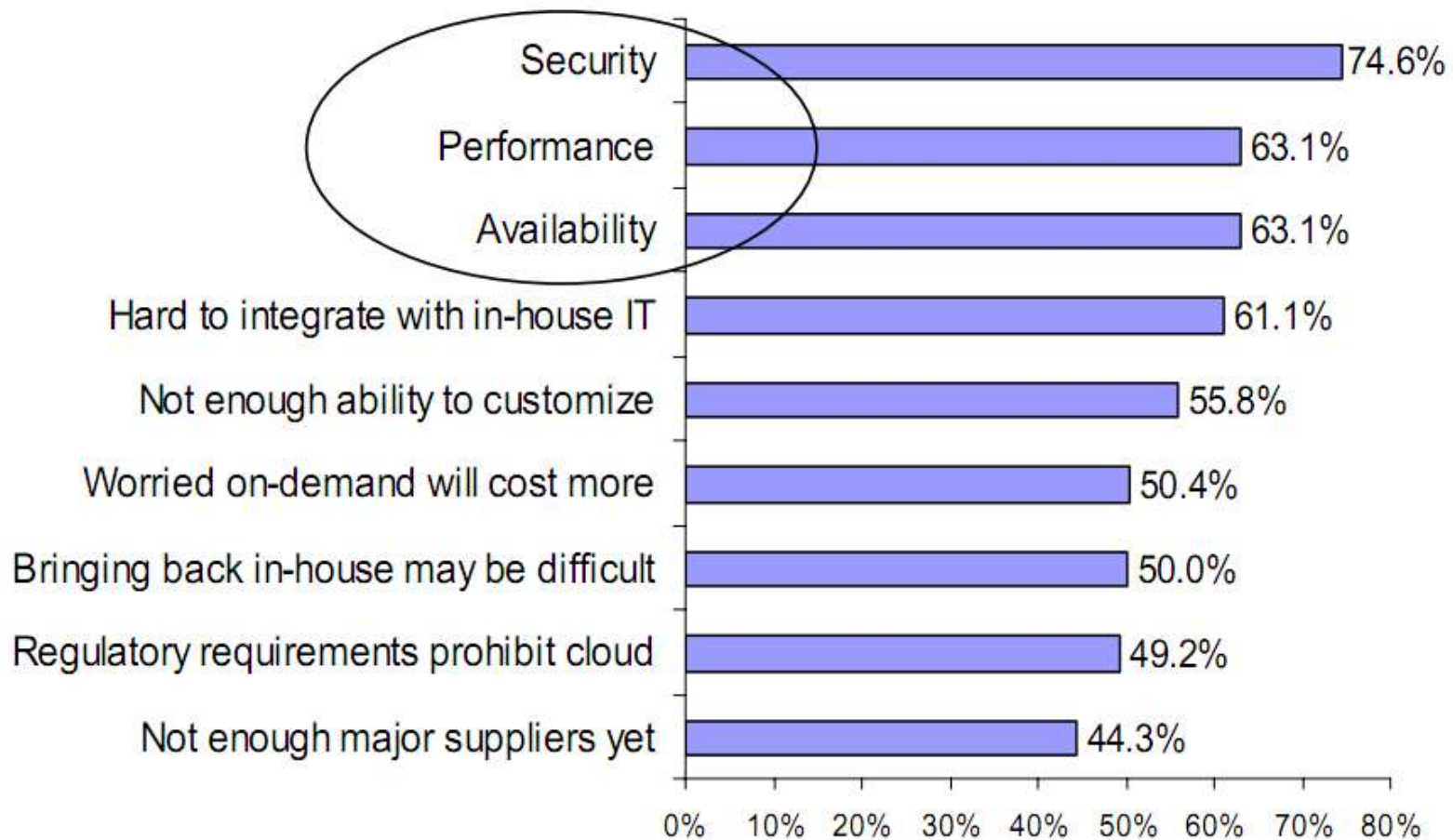
Cloud Computing is Here to Stay

- Leverage its Assets
 - Use available contracts
 - Build a computing architecture that facilitates its use
- Manage its Risks
 - Available contracts
 - Proper governance structures
 - Use cost models that match our environment

Cloud Computing

Assessment and challenges

Not Without Challenges



Common Themes when Assessing Cloud Computing

- How prepared is your organization?
- How prepared is the provider?
- How well is it working for others?
- What will we gain?
- What are the risks?
- What are the controls?

Governance and Risk Management

- What are the provider's information security management policies and procedures?
- Can the provider ensure they'll comply with your requirements?
- How are risk assessments performed?
- What service level agreements are in place?

Legal

- What federal laws, state laws and standards apply?
- Are there conflicts between the laws governing your organization and the provider?
- How will subpoenas be handled?
- Does the provider's contract absolve it of responsibility for disruptions and leaks?
- What else can the provider do with your data?

Compliance and Audit

- How will your internal and 3rd party auditors conduct an audit of the system?
- Can provider ensure that they'll comply with your requirements? Will they even agree to?

Some Technical and Management Considerations

Some topics to consider as you leverage more cloud-based services

Security Management

- We know how to do this in a traditional in-sourced environment
- Technical aspects
 - Cryptography, Firewalls, and VPNs
 - IDS/IPS, Patching, and Anti-virus
 - etc, etc, etc
- Policy aspects
 - Data Classification and Data Stewardship
 - Desktop management and Security Awareness
 - Institutional standards

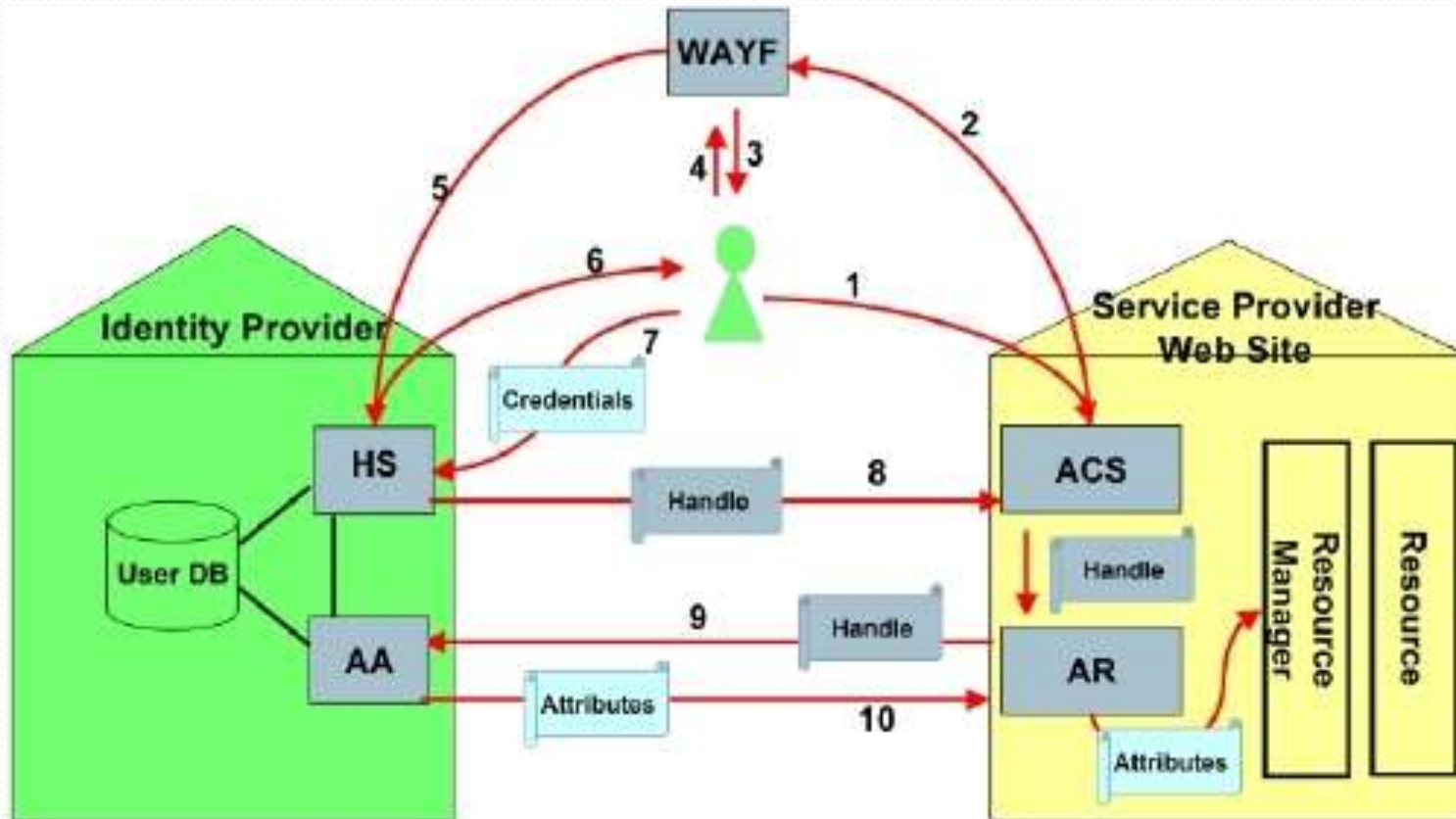
Security Management

- How do we manage security in an out-sourced environment?
- How do we motivate the vendor to protect our data?
 - Contracts, penalty clause?
 - Audits?
 - Damage to their reputation?
- Out-sourcing may be harder with highly sensitive data
 - But, most data isn't highly sensitive
 - Some data lends itself to be redacted

Identity and Access Management

- How your campus does this can greatly impact your ability to easily leverage cloud-based services
- Build based on standards
 - NIST 800-63 for Identity Management
 - SAML for interoperability
- Do spend time on documentation
- Participate in Higher Education activities
 - Shibboleth and InCommon
 - Work has been done in this area for years

Shibboleth Process Flow



© SWITCH

Reference: <http://shibboleth.internetz.edu/tech-intro.html>

Shibboleth and InCommon

- InCommon Federation
 - 117 Higher Education Participants – 10/1/2009
 - 42 Sponsored Partners
 - Microsoft, Apple, etc
 - Many higher education service providers (JSTOR, OCLC, etc)
 - www.incommonfederation.org
- Shibboleth is based on SAML
 - Enables interactions with many others; Google
 - Local example: [VIVA and PBS Videos](#)

Storage and Virtualization

- How does your provider store data?
 - How is your data protected from that of others?
 - Who at the service provider can access or modify your data?
 - Is data replicated across physical sites, between local sites?
 - How/Do they do backups?
 - If you delete data, is it really deleted?
 - How does the provider make their money?
 - Are they allowed to search and/or use your data?
 - Remember: there may be a significant cost associated with data loss, even in the case of non-sensitive data

Storage and Virtualization

- Most of the same questions apply to Server, Database, and Application Virtualization
 - Who shares the core VM infrastructure with you?
 - How is cross-VM security implemented
 - Who can modify your VM configurations, firewall rules, and other equivalent security parameters?
 - Who manages security settings and access control for cloud-based applications?
 - What policy is used?
 - How is patch management handled?
 - Remember: there can be a significant financial loss from the improper modification of even non-sensitive data

Data Center Practices

- Do you know where your data and servers live?
 - Is there a reason to care?
- Can the provider migrate your data and services for their convenience ?
 - Or, is the location fixed to match up with your Disaster Recovery (and legal) practices?
- What level of 24x7 support can you count on?
 - Contract / SLA vs. what really happens

What if Something Bad Happens?

- Natural disaster
- Provider negligence
- Data breach



Business Continuity and Disaster Recovery

- What are the provider's critical infrastructure risks?
Environmental risks?
- What are the provider's business continuity and DR plans?
 - How often are they tested?

E-Discovery

- Who is assigned roles and responsibilities for data holds, searches and testimony?
 - What will it cost?
- Is the provider capable of retaining data as required?

Incident Response

- Who will be liable when there's a breach?
- How will be notified if there's a breach?
 - To what extent will we be involved in response?
- Has the vendor successfully supported investigations with similar needs to mine?

Portability

- How easily can data be exported?
- What other providers offer the service?
- What if the provider goes out of business?

Is the Cloud Right for You?

- What will we gain?
 - Can we survive without this?
 - How compelling are the advantages?
- What are the risks?
 - Impact of failure in CIA?
 - Are the risks understood?
- Are we ready?
- Where to start?

Wrap Up

Cloud Computing Provides Many Good Solutions

- However, there is too much hype
 - Not everything is right for or easy to implement in a cloud-based solution
- However, mixed in with the hype are many good opportunities that we can leverage now
- Focus your contracts to cover unexpected events
 - Rome Reborn
- Maintain local expertise

Discussion & Questions

- Who is using Cloud-based Services?
 - What challenges have you encountered?
 - Has any of the shine worn off of the rose colored glasses?
- Does anyone have example contracts?
 - That you are proud of or happy with?
- Any good disaster stories to share?
 - These are rare, and that should tell us something



Thank You