Navigating Thunderstorms: Managing Risks in the Cloud

Daren Kinser – Auditor, UCSD
Jennifer McDonald – Auditor, UCSD

Agenda

- Cloud Computing Technical Overview
- Cloud Related Applications
- Identified Risks
- Assessment Criteria

Cloud Computing – What Is It?

- National Institute of Standards and Technology (NIST): "Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models."1

1. Mell, Peter and Tim Grance. "The NIST Definition of Cloud Computing" The National Institute of Standards and Technology. September 2011. http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

Five Characteristics

- On-Demand Self-Service
- Broad Network Access
- Resource Pooling
- Rapid Elasticity
- Measured Service

Three Service Models

- Software as a Service (SaaS) - Applications hosted by an outside party and accessed via the internet. Avoids the need for complex in-house software installation and management. Examples: Salesforce.com

- Infrastructure as a Service (IaaS) – Resources owned by an outside party and used on a contractual basis.(storage, servers, etc.) Examples: Amazon Elastic Cloud (EC2), Amazon Simple Storage Service (S3), and Rackspace.

- Platform as a Service (PaaS) - Platforms provided by an outside party used for building/running applications. Overlaps with SaaS.
  Example: Google App Engine

Other “Service Models”

- Network as a Service (NaaS)
- Storage as a Service (SaaS)
- Security as a Service (SECaaS)
- Data Base as a Service (DBaaS)
- Data as a Service (DaaS)

Four Deployment Models

- Public - Services offered to anyone regardless of affiliation. All users share the same resources.
- Community – Cloud infrastructure is provisioned for use by organizations with similar interests.
- Private - Services and resources are supplied by and/or to only a select group like a private company, University, etc.
- Hybrid - Using a public cloud provider to build a private cloud. This may also include connections from the cloud resources to the local or other remote resources. Some companies may desire a private cloud but prefer that it's hosted off site.

Advantages

- Elasticity of Computing Resources
- Economy
- Easy Collaboration
- Levels Playing Field
- Reliability
- Disaster Recovery

Disadvantages / Concerns/ (Risks?)

- Security and Privacy
- Availability/Reliability
- Data Ownership
- Performance
- Data Leakage To Public Clouds

Cloud Example: Amazon

- Growth
  - AMAZON in 2003 = $5B revenue business
  - Every day they are adding enough new server capacity to handle all of Amazon globally when they were a $5Billion dollar company in 2003.
- Amazon Web Services (AWS) Physical Locations
  - Regions - physical places in the world where they have infrastructure and data centers they call "Availability Zones“(25).
  - 9 Regions: 1 East Coast U.S., 2 West Coast U.S., 1 Europe, 1 Singapore, 1 Tokyo, 1 Brazil, 1 Australia, 1 U.S. Government only cloud called "GovCloud".

Cloud Example: Amazon (cont.)

- Amazon EC2 – Elastic Compute Cloud
  - IaaS
- Amazon S3 – Simple Storage Service
  - SaaS – Storage as a Service
  - Used by Dropbox, Tumblr, Pinterest
- Amazon Redshift – Big Data
  - DBaaS

Cloud Example: Windows Azure

- Infrastructure, Web, Mobile, Big Data, Development and Testing, Identity/Access Management, Media, Storage/Backup/Recovery
- PaaS – Web Sites, Hosted Applications
- IaaS – Virtual machines,
- Compliance
  - HIPAA
  - SSAE 16/ISAE 3402 Attestation - control objectives are appropriately designed and that the controls safeguarding customer data are operating effectively

Why Now?

- Bandwidth Increases
- Virtualization
- Mobile Devices: Smart Phones, Tablets
- Cheap Storage
- HTML 5

Patchy Clouds With a Chance of Rain

- Governance
  - Contracts and Service Level Agreements are in place
  - Compliance with Regulatory Standards
- Vendor Management
  - Risk Assessment
  - Details specified in contract and Service Level Agreements
- Business Process – Financial and Operational
- Technical – Security and Privacy

Campus Cloud Related Applications

Private Cloud Activity

- Storage – San Diego Super Computer (SDSC)
- Infrastructure – Virtual Machine Hosting (SDSC)
- Integrated Financial Information System (IFIS)
- Personnel Payroll System (PPS)

Public Cloud Activity (Hosted Solutions)

- MarketPlace (SciQuest)
- Google Apps
- Possible Future Agreements
  - Microsoft
    - Azure
    - 365

Assessment Criteria

- Type of Data to Store
  - PII, PHI, Personal or Financial Information, Academic Records, Human Subjects/Research Data, other sensitive data
- US Location only?
- Data Retention and Destruction
  - Hardware – Dedicated or Shared?
  - Is data subject to retention or destruction requirements?
- Grant Requirements
  - Local Policy Requirements
- Encryption Methods – Security and Privacy
  - Is data encrypted in transit? At rest?
  - How is authentication and access secured? SSL?

Assessment Criteria (cont.)

- Business Continuity
  - Large or frequent data uploads/ downloads?
  - Latency tolerance?
  - Disaster Recovery
  - Redundancy – Amazon Web Services -April 2011, the company's data center in Virginia suffered from a devastating bout of issues regarding connectivity and latency.
- Contract Clause
  - Audit Clause? Has anything been agreed to that cannot be undone?
- Breach Notification
  - Does the contract support IS-3 'Third Party Agreements' for breach notification?"
- UC Cost
  - Does the service provide comparable or enhanced service at a reduced cost?
- Is there a system wide agreement already in place?

Resources

- Recent Advances Delivered by HTML 5 in Mobile Cloud Computing Applications: A Survey
  - http://dl.acm.org/ft_gateway.cfm?id=2371355&ftid=1290956&dwn=1&CFID=240121200&CFTOKEN=68253737
- Campus Agreements
  - http://www.ucop.edu/purchserv/psa_db/pubregisterindex.php?mode=1&id=37
- HIPAA/HITECH
  - http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/hitechenforcementifr.html
- Vendor Resources
  - Windows Azure Compliance:
    - http://www.windowsazure.com/en-us/support/trust-center/compliance/
  - Windows Azure HIPAA Implementation Guidance:
    - http://download.microsoft.com/download/8/4/8/8483B6A9-1865-4D17-B6F1-5B66D5C29B10/Windows%20Azure%20HIPAA%20Implementation%20Guidance.pdf
  - Amazon Compliance
    - http://aws.amazon.com/compliance/
  - Dropbox Compliance
    - https://www.dropbox.com/help/238/en
  - Dropbox Privacy
    - https://www.dropbox.com/privacy

jemcdonald@ucsd.edu dkinser@ucsd.edu