
Robert Bohn, John Messina
Information Technology Laboratory

April 8, 2011
Outline

• Objective
• Working Group background
• NIST Cloud Computing Reference Architecture
  – Actors
  – Roles
  – Activities & Functions
• NIST Cloud Computing Taxonomy
• Next Steps
Objective

Develop a vendor neutral reference architecture consistent with the NIST Cloud Computing definition

Three service models
- Software as a Service (SaaS)
- Platform as a service (PaaS)
- Infrastructure as a Service (IaaS)

Four Deployment models
- Private cloud
- Community cloud
- Public cloud
- Hybrid cloud

Five Essential Characteristics
- On-demand self-service
- Broad network access
- Resource pooling
- Rapid elasticity
- Measured service

Determine the “What” of Cloud Computing, not the “How”
Reference Architecture & Taxonomy Working Group Background

- Kick off Meetings: January 10 & 12, 2011
- 12 Reference Architecture, 11 Taxonomy meetings
- Mailing list membership: Ref Arch 498, Tax 411
- Organizations >215
- US Army, DHS, DOJ, DOT, NARA, NASA, NSA, EMC, GSA, ATT, Amazon, CA Technologies, Cisco, HP, IBM, Intel, Microsoft, Oracle, VmWare, Virtual Global, TM Forum, IEEE, CSA, Tech America, Johns Hopkins University, Deloitte, Fujitsu, SAIC, BAH, etc...
Acknowledgements

Dr. Fang Liu, Jin Tong, Dr. Jian Mao: Knowceean Consulting Inc.
Dr. Robert Bohn, John Messina: NIST ITL
Dawn Leaf, NIST Senior Executive for Cloud Computing

With broad contributions from members of the NIST Reference Architecture and Taxonomy Working Group and the Reference Architecture Analysis Team:

Randy Baklini, Gregg Brown, Frederic De Vaulx, Michele Drgon, Anne Frantzen, Babak Jahromi, Dean Kemp, Cary Landis, Eugene Luster, Bob Marcus, Gary Mzzaferro, Hung Nguyen, Marlin Pohlman, Alan Sill, Ken Stavinoha, Pat Stingley, Tom Young and Jay Levine
NIST Cloud Computing Reference Architecture

Actors and their Roles

Cloud Consumer
Person or organization that maintains a business relationship with, and uses service from Cloud Providers.

Cloud Provider
Person, organization or entity responsible for making a service available to Cloud Consumers.

Cloud Auditor
A party that can conduct independent assessment of cloud services, information system operations, performance and security of the cloud implementation.

Cloud Carrier
The intermediary that provides connectivity and transport of cloud services from Cloud Providers to Cloud Consumers.

Cloud Broker
An entity that manages the use, performance and delivery of cloud services, and negotiates relationships between Cloud Providers and Cloud Consumers.
The NIST Cloud Computing Reference Architecture

Cloud Consumer

- Cloud Auditor
  - Security Audit
  - Privacy Impact Audit
  - Performance Audit

Cloud Provider

- Service Layer
  - SaaS
  - PaaS
  - IaaS
- Resource Abstraction and Control Layer
- Physical Resource Layer
  - Hardware
  - Facility
- Cloud Service Management
  - Business Support
  - Provisioning/Configuration
  - Portability/Interoperability
- Cloud Carrier

Cloud Broker

- Cloud Intermediation
- Service Aggregation
- Service Arbitrage

Information Technology Laboratory Cloud Computing Program
### Cloud Consumer/Provider Activities

<table>
<thead>
<tr>
<th>Service Model</th>
<th>Consumer Activities</th>
<th>Provider Activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>SaaS</td>
<td>Uses application/service for business process operations</td>
<td>Installs, manages, maintains and supports the software application on a cloud infrastructure.</td>
</tr>
<tr>
<td>PaaS</td>
<td>Develops, tests, deploys and manages applications hosted in a cloud environment</td>
<td>Provisions and manages cloud infrastructure and middleware for the platform consumers; provides development, deployment and administration tools to platform consumers.</td>
</tr>
<tr>
<td>IaaS</td>
<td>Creates/installs, manages and monitors services for IT infrastructure operations</td>
<td>Provisions and manages the physical processing, storage, networking and the hosting environment and cloud infrastructure for IaaS consumers.</td>
</tr>
</tbody>
</table>
Cloud Provider - Top-level View

Cloud Provider

- Service Deployment
- Service Orchestration
- Cloud Service Management
- Security
- Privacy
Cloud Provider – Service Deployment

• A cloud system can be operated in one of the following four deployment models:
  – **Private cloud:** The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.
  – **Community cloud:** The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.
  – **Public cloud:** The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.
  – **Hybrid cloud:** The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).
Example Services Available to a Cloud Consumer

- **SaaS Consumer**
  - ERP
  - Human Resources
  - Social Networks
  - Financials
  - Content Management
  - Email & Office Productivity
- **PaaS Consumer**
  - Collaboration
  - CRM
  - Document Management
- **IaaS Consumer**
  - Database
  - Storage
  - CDN
  - Backup & Recovery
  - Compute
  - Platform Hosting
  - Services Management
- **Cloud Provider**
  - Business Intelligence
  - Development & Testing
  - Application Deployment
  - Integration

**Information Technology Laboratory Cloud Computing Program**
Cloud Provider – Service Orchestration

Software as a Service

Platform as a Service

Infrastructure as a Service

Service Layer
- SaaS
- PaaS
- IaaS

Resource Abstraction and Control Layer

Physical Resource Layer
- Hardware
- Facility

Information Technology Laboratory Cloud Computing Program
Cloud Provider – Cloud Service Management

Cloud Service Management

<table>
<thead>
<tr>
<th>Business Support</th>
<th>Provisioning /Configuration</th>
<th>Portability /Interoperability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer Mgmt</td>
<td>Rapid Provisioning</td>
<td>Data Portability</td>
</tr>
<tr>
<td>Contract Mgmt</td>
<td>Resource Change</td>
<td>Copy Data To-From</td>
</tr>
<tr>
<td>Inventory Mgmt</td>
<td>Monitoring &amp; Reporting</td>
<td>Bulk Data Transfer</td>
</tr>
<tr>
<td>Accounting &amp; Billing</td>
<td>Metering</td>
<td>Service Interoperability</td>
</tr>
<tr>
<td>Reporting &amp; Auditing</td>
<td>SLA Management</td>
<td>Unified Management Interface</td>
</tr>
<tr>
<td>Pricing &amp; Rating</td>
<td></td>
<td>System Portability</td>
</tr>
<tr>
<td></td>
<td></td>
<td>VM Images Migration</td>
</tr>
<tr>
<td></td>
<td></td>
<td>App/Svc Migration</td>
</tr>
</tbody>
</table>

Cloud Consumers

Cloud Brokers

Information Technology Laboratory Cloud Computing Program
Cloud Provider – Security & Privacy

• **Security**
  – *Authentication and Authorization*: Authenticate and authorize cloud consumers using credentials that have been established previously.
  – *Availability*: Ensure timely and reliable access to and use of information.
  – *Confidentiality*: Protect the confidentiality of the data objects written into clouds by preserving authorized restrictions on access and disclosure.
  – *Identity management*: Enforce identity and access control policies on users accessing cloud.
  – *Integrity*: Guard against improper information modification or destruction, and include ensuring information non-repudiation and authenticity.
  – *Security monitoring & Incident Response*: Conduct ongoing automated monitoring of the cloud provider infrastructure to demonstrate compliance with cloud-consumer security policies and auditing requirements.

• **Privacy**
  – Protect the assured, proper, and consistent collection, processing, communication, use and disposition of personal information (PI) and personally identifiable information (PII) on the cloud.
Cloud Auditor

• A cloud auditor can evaluate the services provided by a cloud provider in terms of security controls, privacy impact, performance, etc.
  – For security auditing, a cloud auditor can make an assessment of the security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

• Auditing is especially important for federal agencies and “agencies should include a contractual clause enabling third parties to assess security controls of cloud providers” (by Vivek Kundra, Federal Cloud Computing Strategy, Feb. 2011.).
Cloud Broker

• As cloud computing evolves, the integration of cloud services can be too complex for cloud consumers to manage.
• The major services provided by a cloud broker include:
  – *Service Arbitrage*: Service arbitrage is similar to service aggregation, with the difference in that the services being aggregated aren’t fixed. Service arbitrage allows flexible and opportunistic choices for the broker. For example, the cloud broker can use a credit-scoring service and select the best score from multiple scoring agencies.
  – *Service Intermediation*: A cloud broker enhances a given service by improving some specific capability and provides the value-added service to cloud consumers.
  – *Service Aggregation*: A cloud broker combines and integrates multiple services into one or more new services. The broker will provide data integration and ensure the secure data movement between cloud consumer and multiple cloud providers.
Cloud Carrier

• Provide access to cloud consumers through network, telecommunication and other access devices, eg: Network access devices include computers, laptops, mobile phones, mobile internet devices (MIDs), etc.

• Arranges Service Level Agreements (SLAs) with a cloud provider to provide a consistent level of service and may be required to provide dedicated and encrypted connections.

• Distribution can be provided by network and telecomm carriers or a transport agent.
The NIST Cloud Computing Reference Architecture

Cloud Consumer
- Cloud Provider
  - Service Layer
    - SaaS
    - PaaS
    - IaaS
  - Resource Abstraction and Control Layer
    - Physical Resource Layer
      - Hardware
      - Facility
  - Cloud Service Management
    - Business Support
    - Provisioning/Configuration
    - Portability/Interoperability
- Cloud Auditor
  - Security Audit
  - Privacy Impact Audit
  - Performance Audit
- Cloud Carrier
- Cloud Broker
  - Service Intermediation
  - Service Aggregation
  - Service Arbitrage

Information Technology Laboratory Cloud Computing Program
Taxonomy: The science of categorization, or classification, of things based on a predetermined system. (Webopedia)

Main Attributes:
• Typically a controlled vocabulary with a hierarchical tree-like structure
• Terms in a taxonomy have relationships with other terms
• Usually in the form of a parent (broader) / child (narrower)

Benefits:
• Encompasses and labels all significant concepts within a given domain
• Allows users to understand the context of each label
Examples Terms and Definitions

Level 1:

• **Cloud Service Provider** – Person, organization or higher-level system responsible for making a service available to service consumers.

Level 2:

• **Cloud Service Management** – Cloud Service Management includes all the service-related functions that are necessary for the management and operations of those services required by or proposed to customers.

Level 3:

• **Public Cloud** - The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services. [NIST Definition of Cloud Computing]

Level 4:

• **Data Portability** – The ability to transfer data from one system to another without being required to recreate or reenter data descriptions or to modify significantly the application being transported. [Federal Standard 1037C]
Next Steps

Summary: The projected deliverables for the RA/Taxonomy Team by the end of September 2011 are:

• Version 2.0 of NIST Cloud Computing Reference Architecture which includes a more detailed description of security and privacy.

• Version 2.0 of NIST Cloud Computing Taxonomy which includes
  – Security & Privacy
  – Updated SaaS taxonomy to reflect USG Business Use Cases.
  – Newly identified additional taxonomies to support USG Business Use Case

• Document – NIST Cloud Computing Reference Architecture Analysis of USG Target Business Use Cases
Questions?
The NIST Cloud Computing Reference Architecture

Cloud Consumer

Cloud Auditor

Cloud Carrier

Cloud Provider

Service Layer
- SaaS
- PaaS
- IaaS

Resource Abstraction and Control Layer

Physical Resource Layer
- Hardware
- Facility

Cloud Service Management
- Business Support
- Provisioning/Configuration
- Portability/Interoperability

Security

Privacy

Cloud Broker

Service Intermediation

Service Aggregation

Service Arbitrage

Information Technology Laboratory Cloud Computing Program