NIST Cloud Computing Reference Architecture

Conference Paper · July 2011

DOI: 10.1109/SERVICES.2011.105 · Source: DBLP

5 authors, including:

R. Bohn
National Institute of Standards and Technology
19 PUBLICATIONS **1,404** CITATIONS

NIST Cloud Computing: Reference Architecture

Robert Bohn, John Messina
Information Technology Laboratory
National Institute of Standards and Technology

October 18th, 2011

NIST National Institute of Standards and Technology U.S. Department of Commerce

NIST: Mission

To promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life

©Robert Rathe

NIST At A Glance

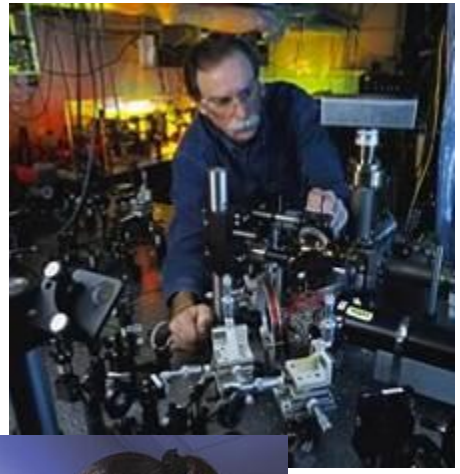
Major Assets

~ 2,900 employees

~ 2600 associates and facilities users

~ 1,600 field staff in partner organizations

~ 400 NIST staff serving on 1,000 national and international standards committees



© Geoffrey Wheeler

©Robert Rathe

Major Programs

NIST Laboratories

Baldridge National Quality Program

Manufacturing Extension Partnership

National Voluntary Laboratory Accreditation Program (NVLAP)

Why NIST?

- US government agencies need Cloud Computing **standards & guidance** to accelerate effective adoption
- Private sector and U.S. government agencies must work together to identify highest priority USG Cloud Computing **security**, **interoperability**, & **portability** requirements & gaps
- **Neutral, objective** party is instrumental in encouraging innovation & "a level playing field" for U.S. industry

NIST Cloud Computing Program Goal

The NIST Cloud Computing Program and initiative to build a *USG Cloud Computing Technology Roadmap* is one of several complementary and parallel U.S. government cloud computing initiatives defined in the broader Federal Cloud Computing Strategy, February 2011

Accelerate the federal government's adoption of cloud computing

- Build a USG Cloud Computing Technology Roadmap which focuses on the highest priority USG cloud computing security, interoperability and portability requirements
- Lead efforts to develop standards and guidelines in close consultation and collaboration with standards bodies, the private sector, and other stakeholders

Overview

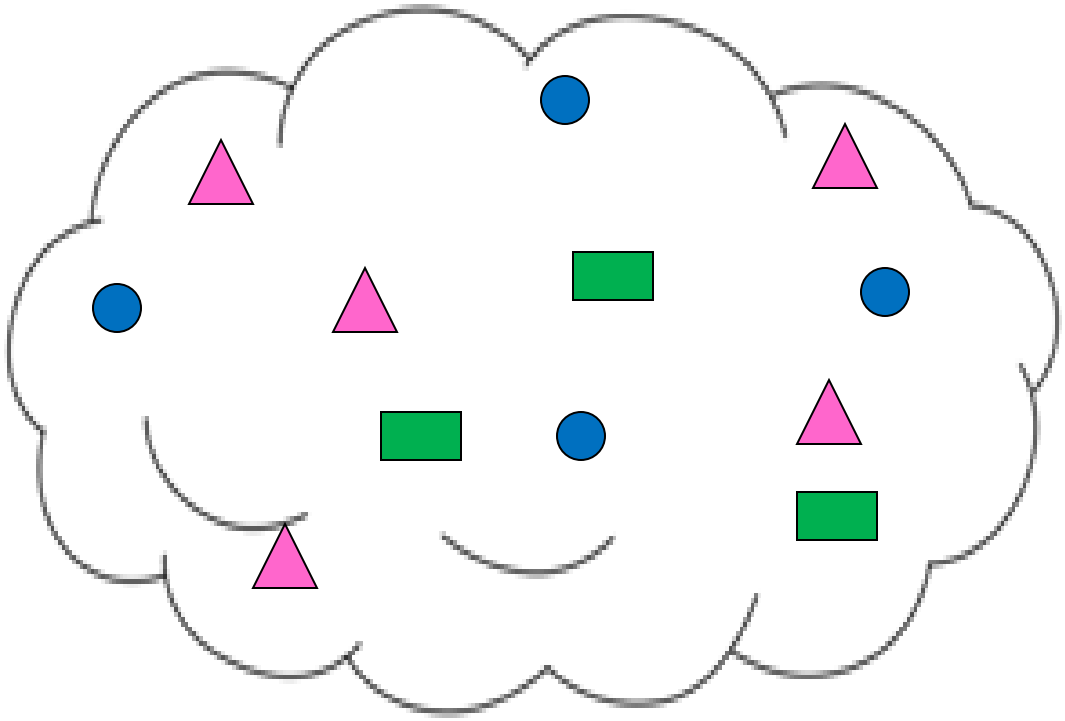
- Definition of Cloud Computing
- Reference Architecture / Taxonomy Activity
- Taxonomy & Vocabulary
- Reference Architecture
- Mapping Discussion

"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."

Service Models
-Software as a Service (SaaS)
-Platform as a Service (PaaS)
-Infrastructure as a Service (IaaS)

Deployment Models
-Public
-Private
-Community
-Hybrid

Essential Characteristics
-On demand self-service
-Broad network access
-Resource Pooling
-Rapid Elasticity
-Measured Service



A Cloud

Information Technology Laboratory Cloud Computing Program

NIST National Institute of Standards and Technology U.S. Department of Commerce

Reference Architecture Basics

What is it?

Provides a blueprint of all the components and decisions that must be made to construct particular functionality or area of interest.

How is it useful?

- *Creating standards*
- *Education*
- *Improving communication*
- *Creating clear roles & responsibilities*
- *Allowing a comparison between different things*
- *Ensuring consistency and quality across the development and delivery process*

Example: Building a car

A car needs…

Some means of propulsion

A steering mechanism

Some moving mechanism on a road

A place to put passengers

Storage capacity

How to generate power to propel the car ?

Interactions with other parts

Need some way to connect power to moving mechanism
Need to control it (start, stop, increase, decrease power)
Depending on its placement, there may be more or less room for passengers and storage

Patterns for generating power

- Internal Combustion Engine Pattern
- Steam Engine Pattern
- Sterling Engine Pattern
- Electric Engine Pattern

Making patterns more concrete

- Internal Combustion
  - One Stroke Pattern
  - Two Stroke Pattern
  - Wankel Pattern

Reference Architecture and Taxonomy Working Group

Goals: lead interested USG agencies and industry to define a neutral cloud computing reference architecture and taxonomy to extend the NIST cloud computing model to:

- use as a frame of reference to facilitate communication
- to illustrate and understand various cloud services in the context of an overall cloud computing model
- use as a tool to communicate and analyze candidate security, interoperability, and portability candidate standards and reference implementations

Process: The Working Group will leverage the existing, publicly available work, plus the work of the other NIST Working Groups, to develop a NIST Cloud Computing Roadmap that can be incorporated into the USG Cloud Computing Roadmap.

Output: NIST SP500-292 Cloud Computing Reference Architecture

Taxonomies

The science of categorization, or classification, of things based on a predetermined system. (Webopedia)

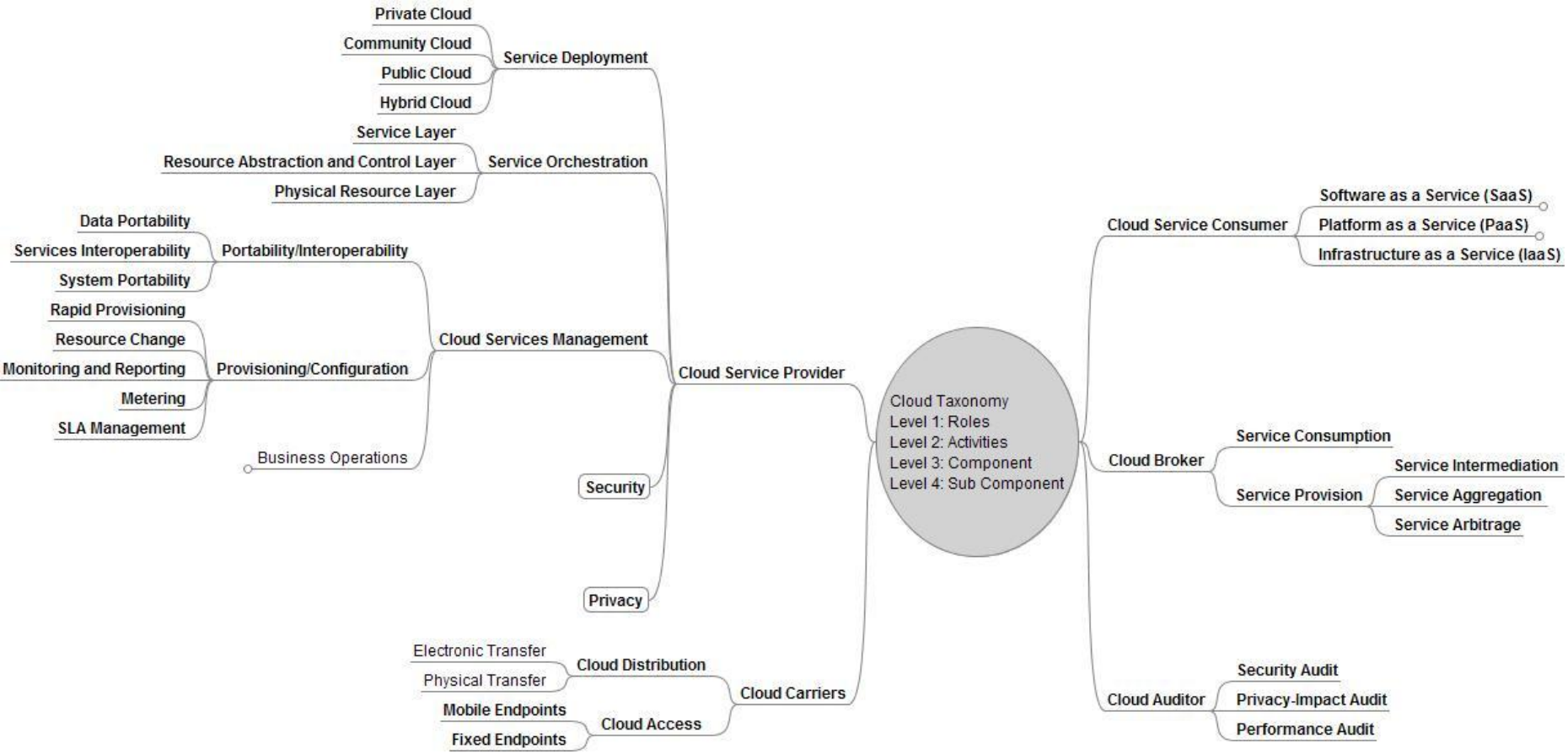
Main Attributes:

- 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

RA Taxonomy / Mindmap



Taxonomy Cloud 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]

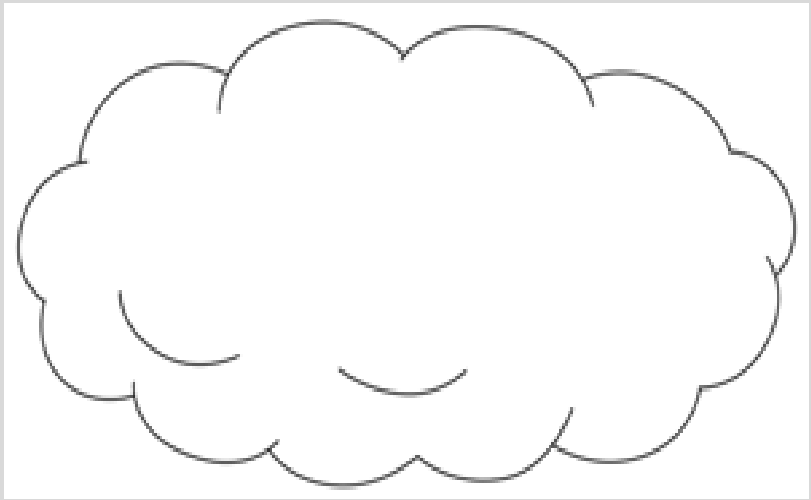
NIST Cloud Computing Reference Architecture
Actors and their Roles

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

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

Cloud Provider

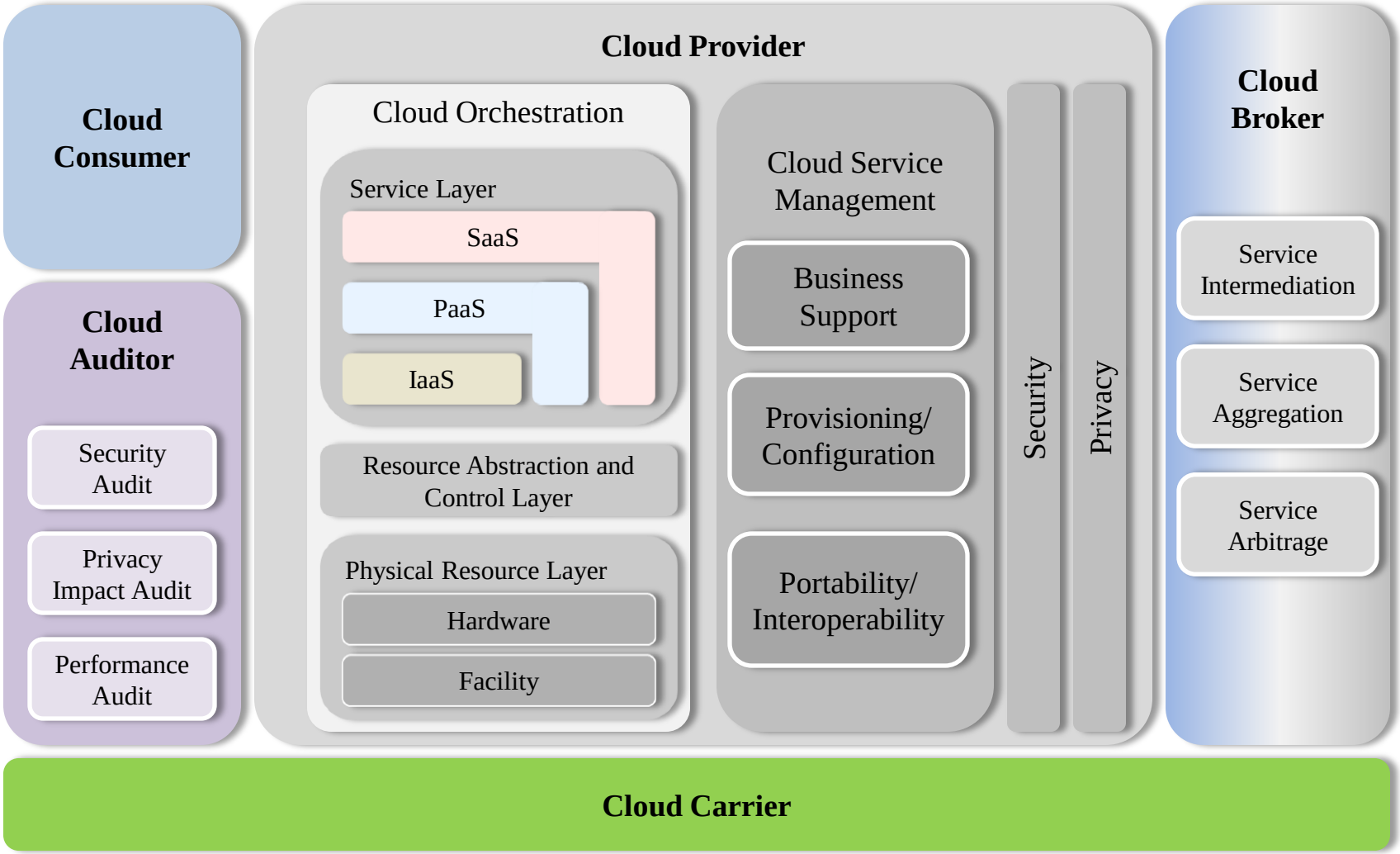
Person, organization or entity responsible for making a service available to *Cloud Consumers.*



Cloud Broker
An entity that manages the use, performance and delivery of cloud services, and negotiates relationships between *Cloud Providers* and *Cloud Consumers.*

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

The NIST Cloud Computing Reference Architecture



NIST National Institute of Standards and Technology U.S. Department of Commerce

Cloud Provider

- ***Cloud Provider*:** Person, organization or entity responsible for making a service available to *Cloud Consumers.*
- Cloud providers perform different tasks for different service models.

Provider Type	Major Activities
SaaS	Installs, manages, maintains and supports the software application on a cloud infrastructure.
PaaS	Provisions and manages cloud infrastructure and middleware for the platform consumers; provides development, deployment and administration tools to platform consumers.
IaaS	Provisions and manages the physical processing, storage, networking and the hosting environment and cloud infrastructure for IaaS consumers.

- The activities of cloud providers are discussed in greater detail from the perspectives of *Service Deployment, Service Orchestration, Cloud Service Management , Security* and *Privacy*.

Cloud Carrier

Cloud Carrier: The intermediary that provides connectivity and transport of cloud services between *Cloud Providers* and *Cloud Consumers*.

- Provide access to cloud consumers through network, telecommunication and other access devices.
  - Example: Network access devices include computers, laptops, mobile phones, mobile internet devices (MIDs), etc.
- Distribution can be provided by network and telecomm carriers or a transport agent.
  - ***Transport agent:*** A business organization that provides physical transport of storage media such as high-capacity hard drives.
- A cloud provider shall set up SLAs with a cloud carrier to provide a consistent level of service. In general, the cloud carrier may be required to provide dedicated and encrypted connections.

Cloud Broker

Cloud Broker: An entity that manages the use, performance and delivery of cloud services and negotiates relationships between *Cloud Providers* and *Cloud Consumers*.

The major services provided by a cloud broker include:

- ***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.
- ***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.

Cloud Auditor

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

- 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" (*Federal Cloud Computing Strategy, Feb. 2011*.).

Mapping Process

- What is your role in the Reference Architecture?
  - Cloud Provider
  - Auditor
  - Broker
- Identify the major activities for a given role using the NIST Taxonomy for Cloud Computing. For a Cloud Provider there are 5 major sub-roles
  - Service Deployment
    - Service Orchestration
    - Cloud Service Management
    - Security
    - Privacy
- Identify the major components of your architecture and find the similar component in the NIST Reference Architecture
  - Service Orchestration
    - Identify your physical resources
    - Methods of control & resource abstraction
    - Service layers

Questions?

NIST Cloud Computing Collaboration Site

http://collaborate.nist.gov/twiki-cloud-computing/

NIST Cloud Computing Home Page

http://www.nist.gov/itl/cloud

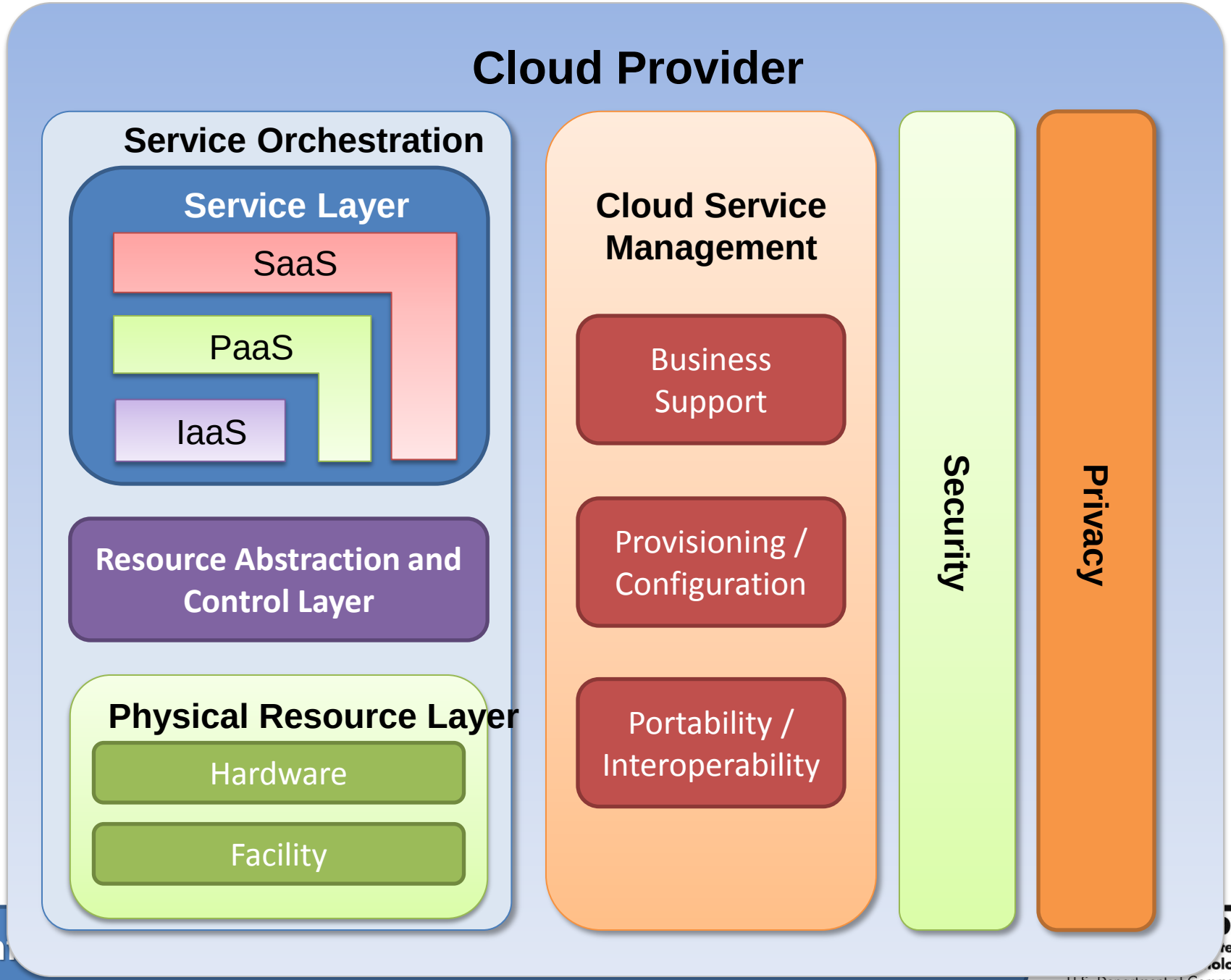
Contact:

Dawn Leaf dawn.leaf@nist.gov
Robert Bohn robert.bohn@nist.gov
John Messina john.messina@nist.gov

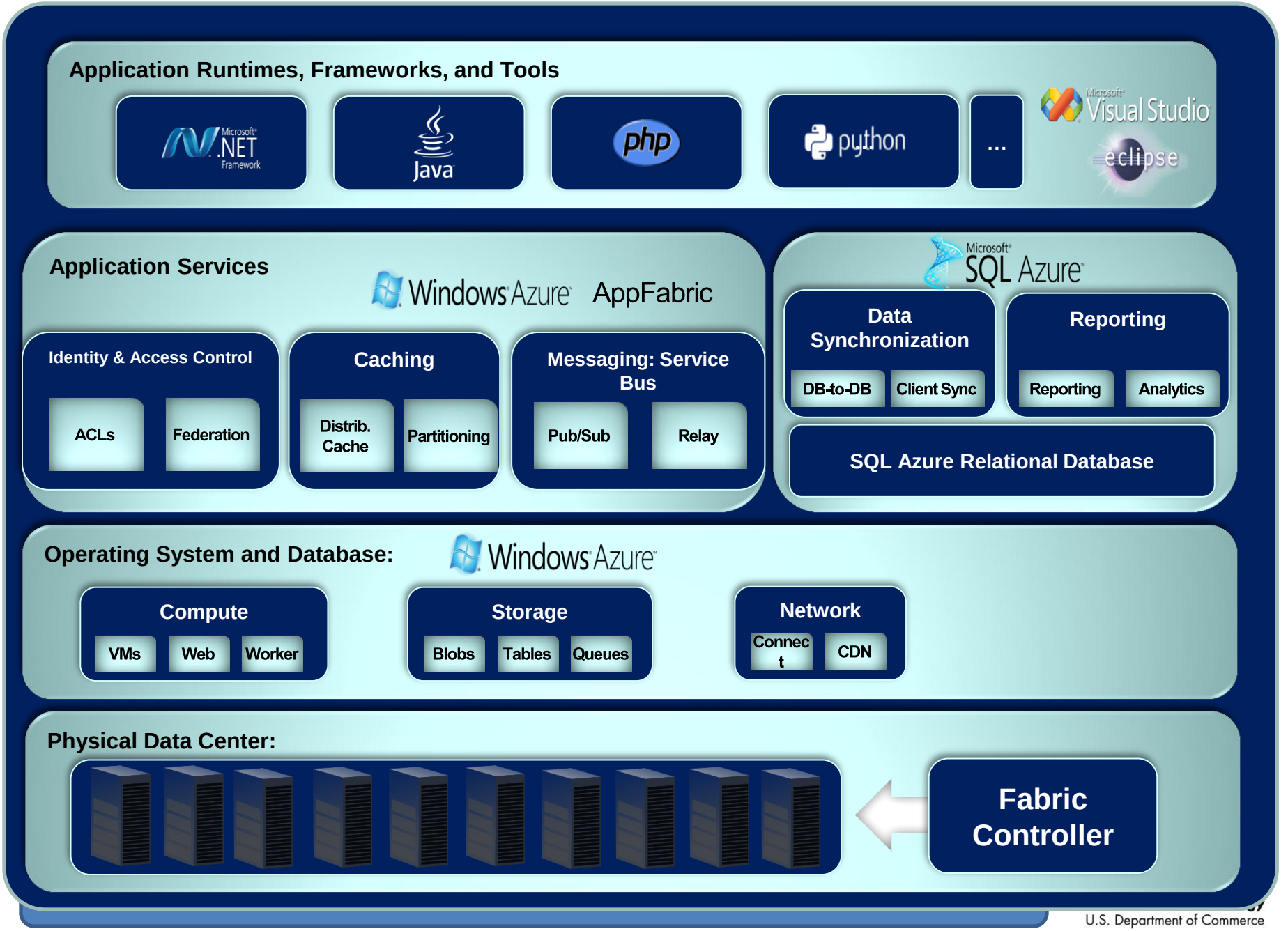
Microsoft's Cloud Computing Reference Model Mapping

October 18th, 2011

Dustin Sell
Federal Azure Lead
Microsoft Corporation


Cloud Provider
Service Orchestration
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

Windows Azure Platform



Thank You