Cloud Computing Reference Architecture

Barry Denby

Griffith College Dublin

April 23, 2020

What will be discussed here

- An example standard reference architecture will be discussed here.
- The idea is that if there is a standard architecture it will make it easier for consumers to move from one cloud to the other.
- Or integrate different cloud services together.
- This was one of the earliest attempts at trying to standardise anything to do with the cloud.

Why was this produced

- The US Government wants to move more of its processing to cloud services as a way of reducing costs.
- In order to do this there needs to be standardisation and interoperability in the cloud.
- NIST recognised that this requires standards for security, data portability, and service interoperability.
  - Without these the US Government are hesitant to move more to the cloud.
- The overall goal of this document is to get standards for cloud computing in place.

What the model actually defines

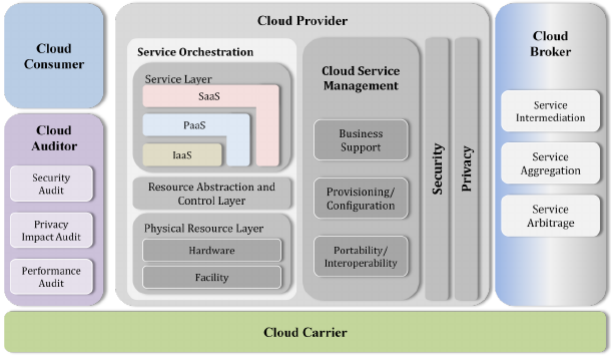
- A reference architecture that is not tied down to any vendor or implementation.
- Defines a set of actors, activities, and functions to be used in the development of cloud computing architectures.
- A set of views and descriptions as a basis for discussing the characteristics, uses, and standards for cloud computing.
- Only focuses on "what" cloud services provide, not a "how to" design a solution and implementation.

NIST use for the model

- Illustrate and understand the various cloud services in the context of an overall cloud computing conceptual model.
- Technical reference to allow clients to understand, discuss, categorize and compare cloud services.
- Facilitate analysis of candidates standards for security interoperability, portability, and reference implementations.
-

NIST conceptual reference model

- The NIST cloud computing reference model is shown below.



NIST conceptual reference model

- The NIST model on the previous slide defines five major actors in a cloud system.
  - Cloud Consumer
  - Cloud Provider
  - Cloud Broker
  - Cloud Auditor
  - Cloud Carrier
- Each actor is considered to be an entity that participates in a transaction or process and/or performs tasks in cloud computing.
- The definitions for each will follow on the next slide.

NIST actor definitions

- Cloud Consumer: A person or organisation that maintains a business relationship with, and uses services from cloud providers.
- Cloud Provider: A person, organisation, or entity responsible for making a service available to interested parties.
- Cloud Auditor: A party that can conduct independent assessment of cloud services, information system operations, performance, and security of the cloud implementation.

NIST actor definitions

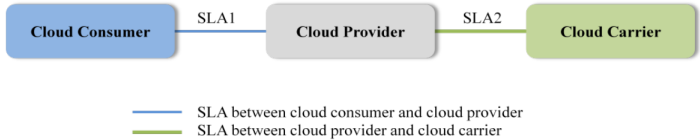
- Cloud Broker: An entity that manages the use, performance and delivery of cloud services, and negotiates relationships between cloud providers and cloud consumers.
- Cloud Carrier: An intermediary that provides connectivity and transport of cloud services from cloud providers to cloud consumers.

Example scenarios with this model

- A cloud consumer may request service from a cloud broker instead of a cloud provider.
- Cloud broker will either combine multiple services or enhance an existing service.
- The cloud providers are thus invisible to the consumer as the broker deals with providers directly.

Example Scenarios with this model

- A cloud consumer may interact with a cloud provider directly for service.
- The cloud provider may also interact with a cloud carrier who will provide transport from provider to client and vice versa.
- Thus there are two separate SLAs to be observed here.



Example Scenarios with this model

- A cloud auditor wishes to conduct an independent assessment of the operation and security of a cloud service implementation.
- This will involve interaction with both the Cloud Consumer and the Cloud Provider

Cloud Consumer

- As stated previously a cloud consumer is a person or organisation that maintains a business relationship with, and uses services from cloud providers.
- They are the principle stakeholder for a cloud computing service. Without consumers the service would not exist or be required.
- They will browse service catalogues from providers, request the appropriate services, setup contracts with a provider and use the services they acquired.
- The cloud consumer will then be billed by the provider for the services provided

Cloud Consumer

- Cloud consumers require SLAs to specify the technical performance requirements that the cloud provider must fulfil
- SLAs will also mention limitations and obligations the the consumer must accept and abide by when using the services provided.
- Typically these SLAs and associated pricing are non-negotiable unless for very large cases
- Consumers are also free to choose other providers with more favourable pricing and terms

Cloud Provider

- As stated previously a cloud provider is a person, organisation, or entity responsible for making a service available to interested parties
- A cloud provider acquires and manages the computing infrastructure required for providing the services, runs the cloud software that provides the services and delivers services to consumers through network access
- A cloud provider will provide to a consumer the following
  - Service Deployment
  - Service Orchestration
  - Cloud Service Management
  - Security
  - Privacy

Cloud Provider

- How they provide these things to the consumer will depend on the model of Cloud Computing that is provided
- For SaaS the provider will manage and control applications and infrastructure
- For PaaS the provider will manage infrastructures, runtime software, databases, and middleware. They will also provide development tools
- For IaaS the provider will acquire and manage the physical infrastructure and will provide resources through service interfaces and resource abstractions

Cloud Auditor

- As stated previously a cloud auditor is a party that can conduct independent assessment of cloud services, information system operations, performance, and security of the cloud implementation
- Audits are performed to verify conformance to standards through review of objective evidence
- A cloud auditor can evaluate the services provided by a cloud provider in terms of security controls, privacy impact, performance etc

Cloud Auditor

- For security an auditor will assess security controls to determine if the controls are implemented correctly, operating as intended and producing the desired results for the given security requirements.
- Security auditing will also verify if the system complies with regulatory bodies
- Will also audit privacy to ensure confidentiality, integrity, and availability of an individuals data
- Again to check if it complies with the necessary regulations

Cloud Broker

- As stated previously a cloud broker is an entity that manages the use, performance and delivery of cloud services, and negotiates relationships between cloud providers and cloud consumers
- The reason for these entities is that currently the integration of multiple cloud services is a complex task that may be too difficult for a cloud consumer
- A cloud consumer may request a cloud broker to request and integrate the necessary cloud services for their needs.

Cloud Broker

- The broker would then be responsible for managing the performance and delivery of the services to the consumer
- A cloud broker can provide a service in one of three ways
- Service Intermediation: Where a broker will take an existing service, and extend it with additional capabilities and services that are provided to the consumer

Cloud Broker

- Service Aggregation: Where a broker will combine and integrate multiple services into one or more new services
  - Must secure data movement between providers and provide for data integrity
- Service Arbitrage: Similar to Aggregation but the aggregated service are not fixed and can be swapped out for different services or different vendors.

Cloud Carrier

- As stated previously a cloud carrier is an intermediary that provides connectivity and transport of cloud services from cloud providers to cloud consumers
- They provide access through network telecommunications and other access devices.
- The distribution of cloud services is provided by a network and telecommunication carriers who will setup a communication link with the provider
- There will be an SLA made here between the provider and the carrier to ensure consistent level of service and performance

Cloud Computing Reference Architecture: Architectural Components

- Also necessary in the reference architecture is the technical architectural components that will make up the cloud that is provided by a provider
- The architectural components are the following:
  - Service Deployment
  - Service Orchestration
  - Cloud Service Management
  - Security
  - Privacy

Service Deployment

- Service deployment how the services are deployed to the cloud
- This was covered all in the Cloud Deployment Models lecture but in short there are five main types
  - private
  - community
  - public
  - hybrid
  - multicloud

Service Orchestration

- Service Orchestration refers to the composition of system components to support the cloud providers activities in arrangement, coordination and management of cloud computing resources in order to provide cloud services to consumers
- This is represented as a three layer model which groups together the three types of system components Cloud Providers need to compose and deliver their services

Service Orchestration

- At the bottom is the physical resource layer which includes all computer, network, storage components, and also physical infrastructure like power, cooling, communications etc.
- Above this is the resource abstraction and control layer which contains the system components a provider uses to manage access to resources. this includes VMMs, VMs, virtual storage etc
- At the top is the service layer where cloud providers will define the interfaces through which consumers will access the computing services

Service Orchestration

- This is where either an IaaS, PaaS, or SaaS service is defined
- It is not necessary that they are stacked one on top of the other as they can be defined separately

Cloud Service Management

- Cloud Service Management includes all service-related functions that are necessary for the management and operation of those services required by cloud consumers.
- This can be described in one of three ways:
  - Business support
  - Provisioning and configuration
  - Portability and Interoperability
- Business support deals with business related services to clients. This includes: customer management, contract management, inventory management, accounting and billing, reporting and auditing, pricing and rating

Cloud Service Management

- Provisioning and Configuration deals with providing resources to clients and tracking their usage. This includes: rapid provisioning, resource changing, monitoring and reporting, metering, and SLA management
- Portability and Interoperability deals with how easy to move data and applications from one platform to another and also how easy it is to communicate and coordinate with different clouds

Security

- Essential and should be enforced at all layers and actors in the model
- Cloud based systems need to address the areas of: authentication, availability, confidentiality, identity management, integrity, audit, security monitoring, incident response, and security policy management
- Most importantly in a cloud system there is not one single actor that is responsible for security.
- It is shared between providers and consumers. Both must actively provide security.

Privacy

- Cloud providers should protect any personal information that is handed over to the cloud
- This extends to proper and consistent collection, processing, communication and use of personal information
- This includes personal information and personally identifiable information
- The former where you know who it belongs to, the later is where you can derive who it belongs to