Interoperable Clouds

A White Paper from the Open Cloud Standards Incubator

Version: 1.0.0
Status: DMTF Informational
Publication Date: 2009-11-11
Document Number: DSP-IS0101

Abstract

This white paper describes a snapshot of the work being done in the DMTF Open Cloud Standards Incubator, including use cases and reference architecture as they relate to the interfaces between a cloud service provider and a cloud service consumer. The goal of the Incubator is to define a set of architectural semantics that unify the interoperable management of enterprise and cloud computing. This paper summarizes the core use cases, reference architecture, and service lifecycle. These building blocks will be used to specify the cloud provider interfaces, data artifacts, and profiles to achieve interoperable management.

Table of Contents

List of Figures

List of Tables

1 Executive Summary

Cloud computing is an approach to delivering IT services that promises to be highly agile and lower costs for consumers, especially up-front costs. This approach impacts not only the way computing is used but also the technology and processes that are used to construct and manage IT within enterprises and service providers.

Coupled with the opportunities and promise of cloud computing are elements of risk and management complexity. Adopters of cloud computing ask questions such as the following:

- How do I integrate computer, network, and storage services from one or more cloud service providers into my business and IT processes?
- How do I manage security and business continuity risk across several cloud providers?
- How do I manage the lifecycle of a service in a distributed multiple-provider environment in order to satisfy service-level agreements (SLAs) with my customers?
- How do I maintain effective governance and audit processes across integrated datacenters and cloud providers?
- How do I adopt or switch to a new cloud provider?

Figure 1 illustrates these challenges within the cloud computing environment.

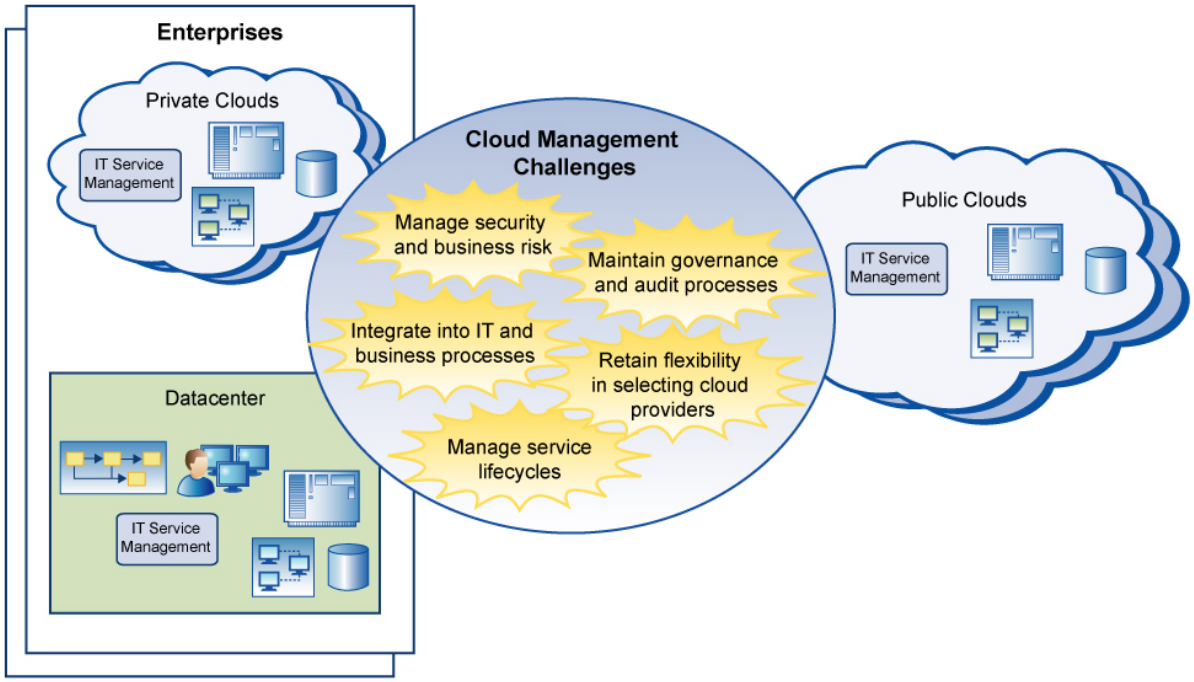

Figure 1 – Cloud Adoption Challenges

The DMTF formed the Open Cloud Standards Incubator to assess the impacts of cloud computing on management and virtualization standards and to make recommendations for extensions to better align with the requirements of cloud environments. Some changes may impact DMTF standards, while others will require coordination with other industry and standards groups. The goal is to aid the industry in

addressing challenges that affect the interoperability, portability, and security of cloud computing environments.

2 Introduction

The definitions of cloud computing — including private and public clouds, Infrastructure as a Service (IaaS), and Platform as a Service (PaaS) — are taken from work by the National Institute of Standards and Technology [NIST-1]. In part, NIST defines cloud computing as "… a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (for example, networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

NIST defines four cloud deployment models:

- public clouds (cloud infrastructure made available to the general public or a large industry group)
- private clouds (cloud infrastructure operated solely for an organization)
- community clouds (cloud infrastructure shared by several organizations)
- hybrid clouds (cloud infrastructure that combines two or more clouds)

The environment under consideration by the Open Cloud Standards Incubator includes all of these deployment models. The main focus of the Incubator is management aspects of IaaS, with some work involving PaaS. These aspects include service-level agreements (SLAs), quality of service (QoS), workload portability, automated provisioning, and accounting and billing.

The fundamental IaaS capability made available to cloud consumers is a cloud service. Examples of services are computing systems, storage capacity, and networks that meet specified security and performance constraints. Examples of consumers of cloud services are enterprise datacenters, small businesses, and other clouds.

Many existing and emerging standards will be important in cloud computing. Some of these, such as security-related standards, apply generally to distributed computing environments. Others apply directly to virtualization technologies, which are expected to be important building blocks in cloud implementations. (The dynamic infrastructure enabled by virtualization technologies aligns well with the dynamic on-demand nature of clouds.) Examples of standards include SLA management and compliance, federated identities and authentication, and cloud interoperability and portability.

Figure 2 shows the scope of the Open Cloud Standards Incubator and the benefits of extending management and virtualization standards.

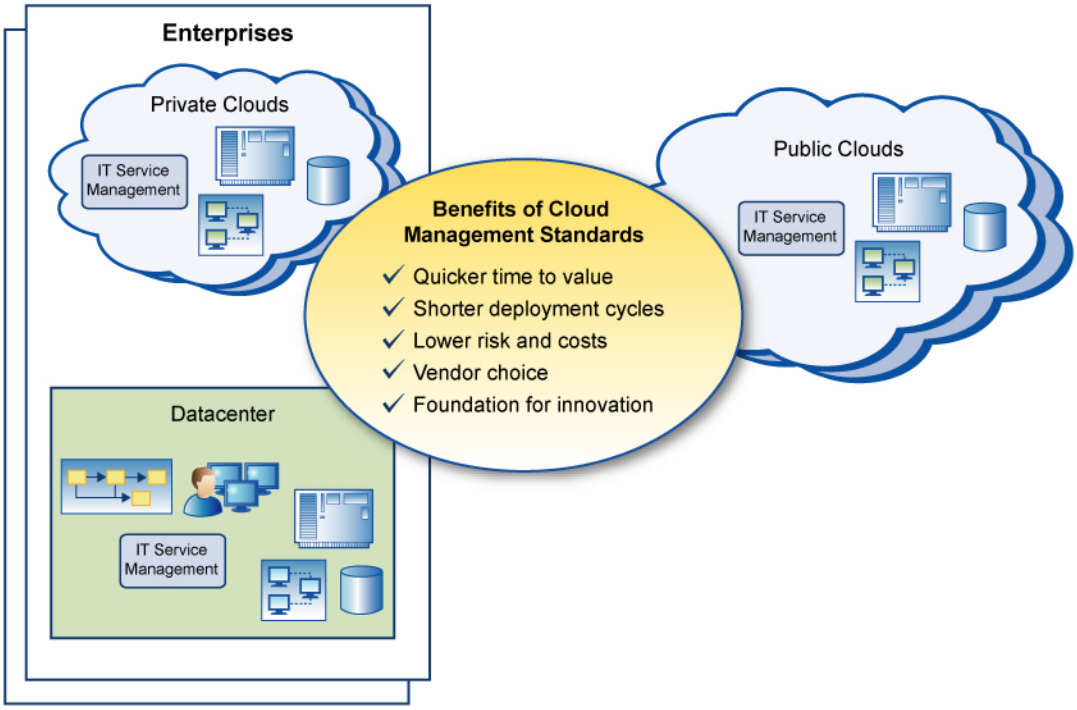

Figure 2 – Scope and Benefits of DMTF Open Cloud Standards Incubator

The Open Cloud Standards Incubator addresses the following aspects of the lifecycle of a cloud service:

- description of the cloud service in a template
- deployment of the cloud service into a cloud
- offering of the service to consumers
- consumer entrance into contracts for the offering
- provider operation and management of instances of the service
- removal of the service offering

When practical, existing standards (or extensions to them) will be integrated into the recommended solution. Examples of standardization areas include resource management protocols, data artifacts, packaging formats, and security mechanisms to enable interoperability.

This white paper analyzes the relationship between the cloud provider and the cloud consumer from the perspective of use cases, service lifecycle, and reference architecture to address the requirements for the interface between the provider and consumer.

3 Usage Scenarios

Given the multiple competing proposals for interfaces to clouds and the nascent stage of the industry, it is important for users to use standard interfaces to provide flexibility for future extensions and to avoid becoming locked into a vendor. With the backing of key players in the industry, this aspect of portability is a primary value that standards-based cloud infrastructure offers. This section describes three scenarios that show how cloud consumers and providers may interact using interoperable cloud standards. These scenarios are examples only; many more possibilities exist.

- The first scenario (see section 3.1) shows how building on standards provides flexibility to do business with a new provider without excessive effort or cost.
- The second scenario (see section 3.2) describes some of the ways that multiple cloud providers may work together to meet the needs of a consumer of cloud services.
- The third scenario (see section 3.3) describes how different consumers with different needs can enter into different contractual arrangements with a cloud provider for data storage services.

3.1 Cloud Portability (Working with Multiple Providers)

The following scenario illustrates how a growing company can leverage a standard cloud interface that is appropriate for its growth stage and processing requirements to expand its use of cloud computing services across multiple cloud service providers.

XYZ Corp is a services company that started small but experienced explosive growth. To keep their costs down, XYZ Corp began with a small datacenter and decided to rely on a cloud service provider offering IaaS services. The company heard about CloudCoA, a company that provided reliable cloud IT services at low cost. Although other cloud service providers existed, CloudCoA had the advantage of being based on DMTF standards. XYZ Corp liked the vendor flexibility that this approach offered, and it decided to use CloudCoA for the additional IT services that it might need in the future. Fortunately for XYZ Corp, business grew rapidly and the company's IT needs started growing tremendously in scale and scope.

Although CloudCoA was initially able to cope with the growth, the needs of XYZ Corp soon surpassed what CloudCoA could provide. Not only did the home office experience significant IT growth, but significant growth of the business in the European Union caused XYZ Corp to open a branch office in Germany. Although CloudCoA could provide IT services with sufficient capabilities and performance in the U.S., regulatory and compliance restrictions forced XYZ Corp to look for cloud vendors within the EU member countries.

Because all of XYZ Corp's IT processes were based on standards-based cloud services, the company found many providers with whom it could contract. They contracted with two new providers, CloudCoB and CloudCoC, to fill in the gaps and add spare capacity for future growth.

For the branch office in Germany, XYZ Corp used CloudCoC, which provided good services in the area. The only effort that the company needed to make to reuse its IT applications, scripts, and processes for CloudCoC was to establish a business relationship with CloudCoC and use their services, without any significant IT service disruption.

At the home office, the company decided to augment the services of CloudCoA with those from CloudCoB. With a simple change in its IT applications and scripts, the company was able to use CloudCoB for all new business while continuing to use CloudCoA for existing accounts.

Figure 3 illustrates how standard interfaces helped XYZ Corp's IT operations evolve over time to match business growth.

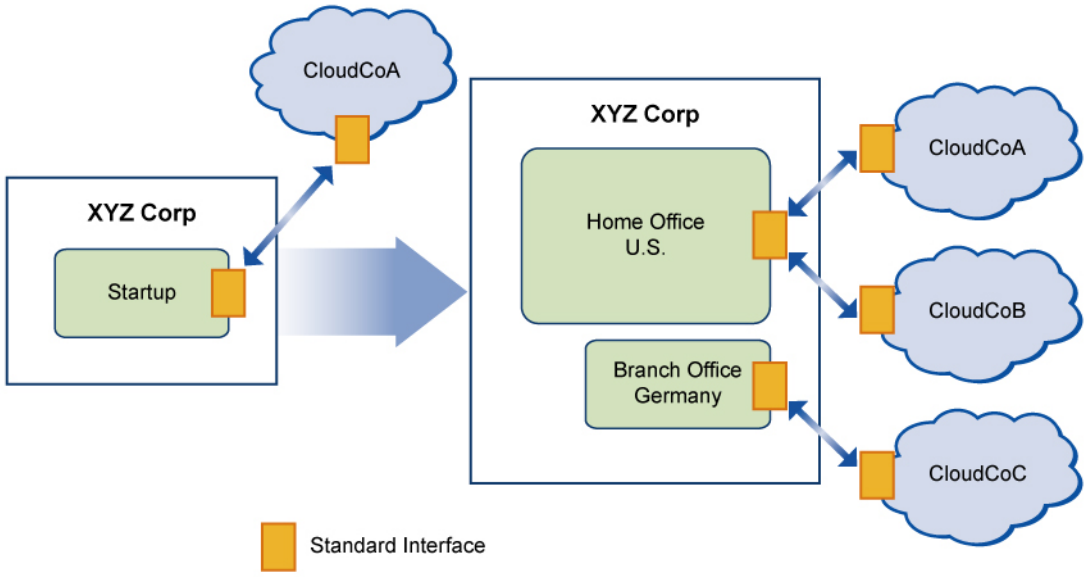

Figure 3 – Standards Ease Corporate IT Evolution and Avoid Vendor Lock-in

3.2 Federating Cloud Providers

Figure 4 shows an enterprise datacenter in the role of a cloud consumer, receiving computing capacity from a cloud (Cloud 1). A usage scenario for this datacenter is testing a new application. Such tests require a large amount of capacity; however, these tests occur sporadically over time, and maintaining sufficient computing resources for these tests within the datacenter would be expensive. Outsourcing the computing resources to a cloud is a good way to achieve the required high capacity at an acceptable cost.

The datacenter interacts with Cloud 1's service catalog to request

- the type of service
- its configuration details
- SLA details such as capacity, availability, and performance
- other constraints, such as network security

If the request is honored, a service manager provides the interface used to manage the deployed service, including access information. The datacenter may then interact directly with the allocated virtual machines (VMs); in Figure 4 this interaction is represented by the dashed line between the datacenter and a VM. The figure necessarily omits details, such as how virtual images are deployed onto the VM hypervisors.

Figure 4 also shows the following examples of how a datacenter may interact with more than one cloud provider:

- Cloud 2 provides extra computing capacity to Cloud 1 when workload requests exceed Cloud 1's own capacity. If the datacenter's request exceeds its capacity, Cloud 1 requests capacity through Cloud 2's service catalog. After granting the capacity, Cloud 2's service manager provides the VM access details, which Cloud 1's service manager relates to the datacenter. In

this federation model, the datacenter may not be aware that the computing capacity is hosted by Cloud 2 instead of Cloud 1.

- A cloud consumer such as the datacenter may request and receive services from multiple clouds. In this example, the datacenter requests services from both Cloud 1 and Cloud 3. This could be done for various reasons. Cloud 3 might support a different type of computing service or different SLA parameters than Cloud 1. Perhaps only Cloud 3 provides storage services. Or, the datacenter might want to have two sources for the same type of service as a way to minimize catastrophic risk. In these cases, Cloud 1 and Cloud 3 do not interact with each other, and quite possibly are not aware of the existence of the other.
- A cloud broker is a cloud that provides services to cloud consumers but might not host any of its own resources. In this example, the broker federates resources from Cloud 1 and Cloud 2, making them available transparently to cloud consumers. As in the first federation example, the cloud consumers interact only with the broker cloud when requesting services, even though the delivered services come from other clouds.

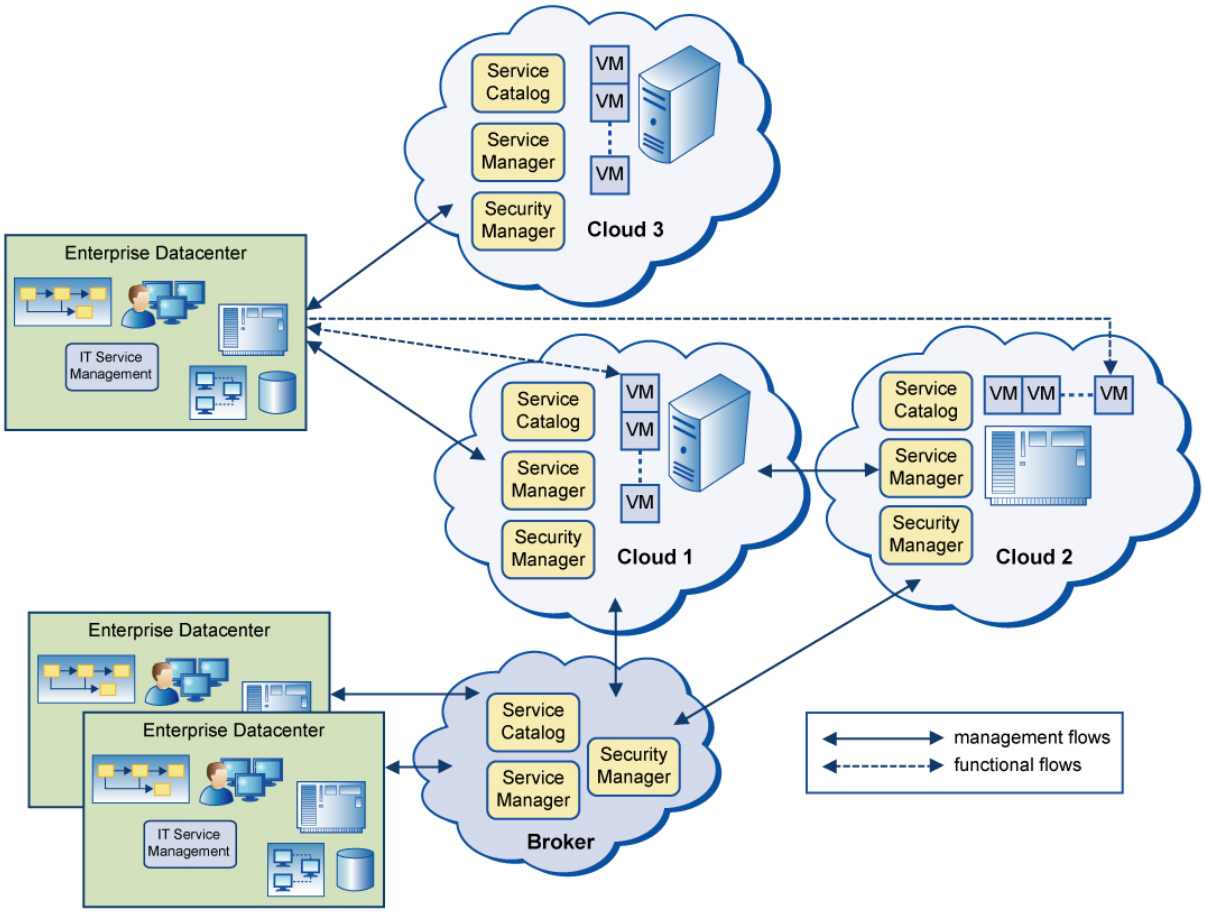

Figure 4 – Cloud Deployment Scenarios

3.3 Adapting Services to Varying Requirements

Cloud Data Retention Service Co. (CDRSC) provides a cloud data retention management service, which it offers publicly. CDRSC stores documents that it receives. Consumers of the CDRSC service enter into a contract and SLA that guarantee the following conditions:

- Data is secure and is accessible only through a properly authorized request.
- Upon receipt of an authorized request, either from the consumer or from a regulatory or legal authority, the documents are promptly and confidentially delivered to the requestor.
- When the retention period is over, documents are promptly and irretrievably destroyed.

CDRSC offers a multi-tenant cloud storage service, which is used by consumers with varying requirements (for example, small, medium, and large enterprises, as shown in Figure 5). CDRSC is constrained by the contract that it offers to its consumers to strictly partition consumer data and certify that no commingling of data occurs between tenants. The service contract also specifies certifiable assurance that necessary security measures are in place to prevent potential data breaches caused by attackers or adversaries. Additionally, multiple protection requirements may be specified in the service contract by a single customer. For example, a company may choose to store both public data and confidential data using CDRSC's cloud storage service. The level of protection and the retention policies for the two types of data are different, and CDRSC must support such policies.

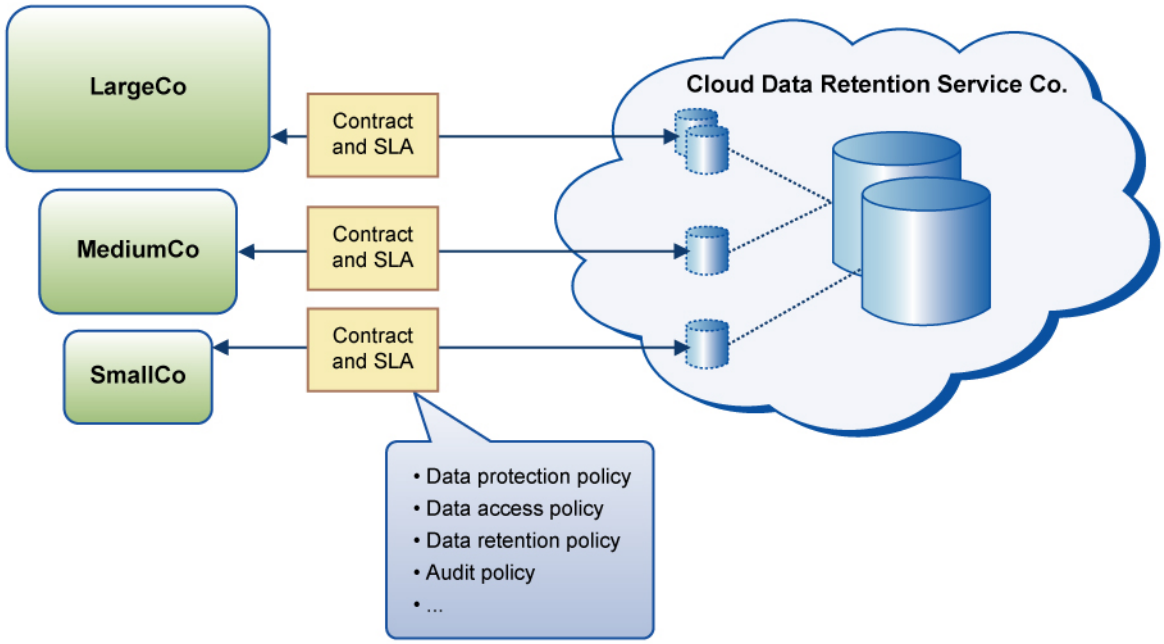

Figure 5 – Multi-Tenant Cloud Data Storage Scenario

In addition, CDRSC is contractually obliged to comply with regulatory agencies. For example, some of the documents stored by CDRSC contribute to the financial reporting of their customer LargeCo, a corporation that must comply with Sarbanes-Oxley (SOX) regulations. Documents that materially contribute to LargeCo's financial reports must be stored in strict and transparent compliance with SOX regulations that prevent unauthorized changes to or destruction of documents or leakage of information

that could contribute to insider trading or other forms of fraud. LargeCo pays CDRSC for a guarantee to LargeCo and its auditors and regulators that LargeCo is in SOX compliance with regard to storage of critical financial documents.

4 Cloud Service Lifecycle

In the Open Cloud Standards Incubator's model, cloud consumers contract with cloud providers for services. A cloud service has a set of distinct lifecycle states. Figure 6 describes the individual service states of the service lifecycle and the use cases associated with each state.

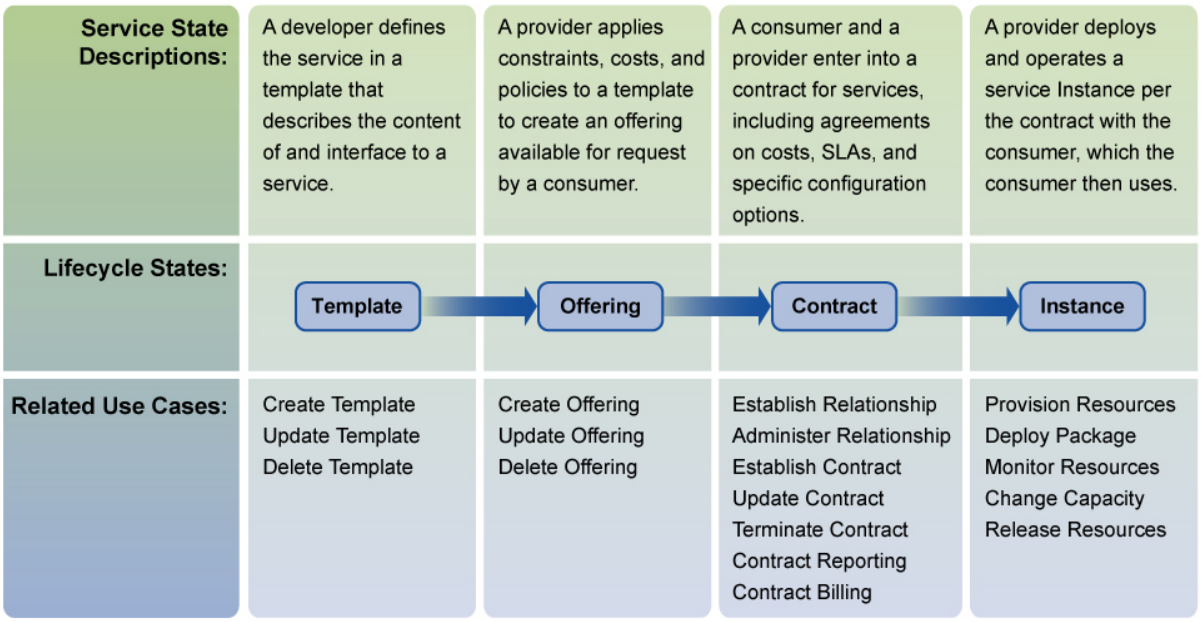

Figure 6 – Cloud Service Lifecycle and Use Cases

After a developer has created the components of a service, the developer begins the process of making it available to cloud consumers by creating a template that defines the content of and interface to the service. The service could be as simple as a single VM or as complex as an *n*-tier application that is packaged using Open Virtualization Format [OVF-1]. The template is then customized by the provider to create a service offering for consumption by one or more consumers. An offering is the unit that a consumer requests by establishing a contract with the provider for that offering. The provider provisions a service instance that satisfies the constraints defined in the offering and the template, and the consumer uses the instance as defined in the contract. After the contract is terminated, the provider reclaims the instance and its supporting resources.

Table 1 provides an example of the lifecycle states and illustrates the activities associated with the use cases for those states.

195 **Table 1 – Example Scenario of Lifecycle States and Associated Activities**

Lifecycle State	Example Activities
Create Service Template Publish Service Template Create Offering	ProviderCo offers IaaS through a website. It decides to offer a service template that consists of a server with two or four processors, 6 or 8 GB of RAM, and 100 GB of storage. The consumer is offered a choice of proprietary and open-source operating systems, HTTP servers, and database managers. In addition, ProviderCo offers storage as a service in 100 GB increments. The company creates 12 templates for various options. Its business plan is to sell standardized computing units and storage units, both on a per-month basis. The company publishes these templates, with contractual information such as costs and billing policies, as offerings in their online service catalog. ProviderCo's customers order computing and storage units, and request that they be provisioned using the published template. Although the consumers are required to pay for all units that they order, they receive a discount for units that are ordered but not provisioned.
Establish Relationship	ConsumerCo is a recently established manufacturing company with a rapidly expanding customer base. ConsumerCo has an established IT department and a datacenter that was designed for 50 servers and currently has insufficient capacity. The ConsumerCo management has decided to extensively increase use of online ordering with their suppliers and customers, but they do not want to invest in expanding their datacenter. Therefore, they decide to obtain network, computing, and storage resources from a public cloud and to link these online web service resources to the existing inventory and fulfillment systems in their datacenter. ConsumerCo's first step is to establish a relationship with an IaaS provider, ProviderCo. A business manager in ConsumerCo's IT department links to the ProviderCo cloud service portal, sets up an account for ConsumerCo using the service catalog interface, and registers three ConsumerCo roles as authorized to request resources from ProviderCo within the limits of the ConsumerCo account using the security manager interface.
Establish Contract	Fred from ConsumerCo has been charged with designing and rolling out an online order management system with ConsumerCo's largest supplier. Fred determines that he needs up to three servers, each with a 4-processor, high-speed class with 8 GB of RAM and up to 500 GB of storage. He uses the security manager and service manager interfaces to interact with ProviderCo, authenticates using the established role, and requests the resources. ProviderCo offers ConsumerCo a contract, which Fred accepts.
Provision Resource Deploy Virtual Image	Fred requests that all the resources be provisioned immediately. At the same time, he specifies a service template that determines the operating system type, some deployed software, and the storage. The image is deployed when the resource is provisioned. Using the configuration manager interface on the portal, Fred accesses the servers and configures them to use the network and storage resources from ProviderCo and to connect to the inventory management system in ConsumerCo's datacenter. He then adds the online service to ConsumerCo's SLA management system.
Change Resource Capacity	Using the service monitor interface, ConsumerCo's SLA management system monitors the performance of the online service based on the SLA, including tracking CPU usage and memory page faults. Usage is lower than anticipated for the system, and the management system requests a deactivation of two servers by using the change manager interface. Later, the management system detects increased load on the service, and it issues a request to activate an additional server.
Contract Reporting Contract Billing	At the end of the first month, the business manager at ConsumerCo requests a report on the contract from ProviderCo. He receives a report through the service manager interface showing the initial deployment and the subsequent release and reactivation of resources. The report shows that the system is typically using two servers during the day and only one server overnight. In the week leading up to the end of the quarter, all three servers were often active during the day. Later, he receives a bill for five provisioned computing units and five provisioned storage units, at $5.00 per terabyte-day and $0.13 per CPU hour.

Lifecycle State	Example Activities
Update Contract Administer Relationship	Business increases at ConsumerCo, and management decides to expand the capacity of their original contract. The ConsumerCo business manager links to ProviderCo and increases the account limit by an additional 25 computing units and 25 storage units. He also adds three additional engineers to the account, making a total of six authorized roles that can request contracts and configure resources.
Terminate Contract	The market for ConsumerCo's products collapses. Fred terminates the contract with ProviderCo, which frees the servers and associated storage. The ConsumerCo business manager terminates the relationship with ProviderCo, which removes the access roles and sends the final bill to ConsumerCo.

5 Cloud Service Reference Architecture

The lifecycle narrative in section 4 cited some example functional interfaces that cloud consumers need to establish services with cloud service providers. This section introduces the conceptual Cloud Service Reference Architecture (Figure 7), which describes key components — such as actors, interfaces, data artifacts, and profiles — and the interrelationships among these components.

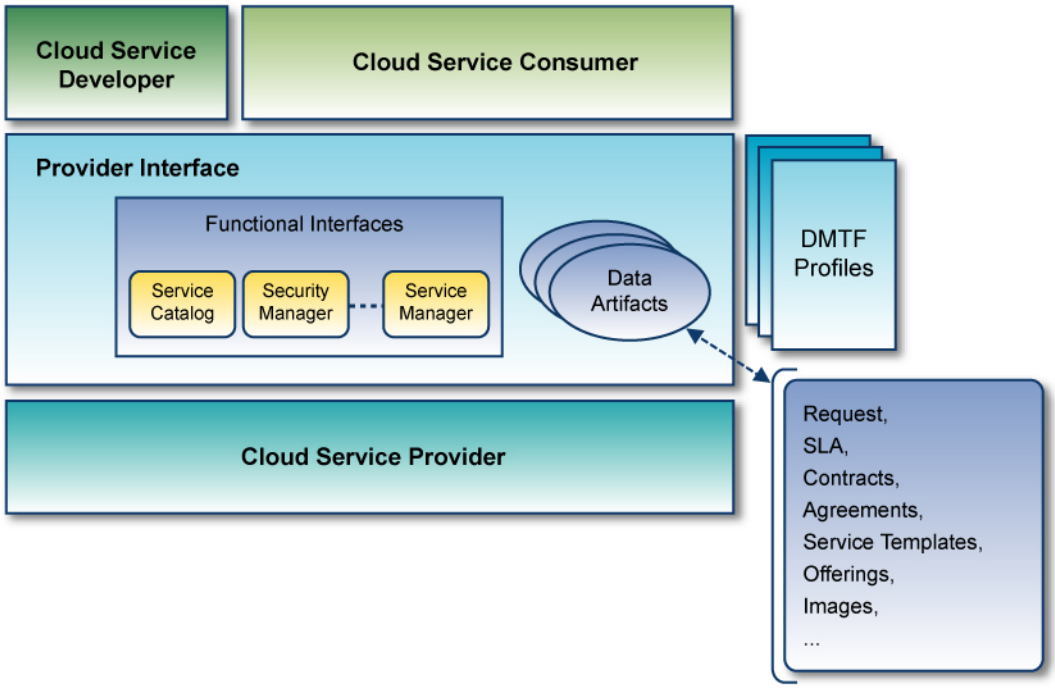

Figure 7 – Cloud Service Reference Architecture

5.1 Actors

The architecture has three primary actors: Cloud Service Provider, Cloud Service Consumer, and Cloud Service Developer. An organization may simultaneously play the roles of any combination of these actors.

- The Cloud Service Provider makes services available to Cloud Service Consumers at agreed service levels and costs. The services may be of any type or complexity. The provider manages the technical infrastructure required for providing the services and provides billing and other reports to consumers.
- The Cloud Service Consumer represents an organization or individuals who contract for services with Cloud Service Providers and then use those services. The Cloud Service Consumer could be another cloud who is a provider to other consumers. The consumer is responsible for selecting the appropriate services, arranging payment for the services, and performing the administration necessary to use those services, such as managing user identities.
- The Cloud Service Developer designs and implements the components of a service. The developer describes the service in a service template. The developer interacts with the Cloud Service Provider to deploy the service components, based on the description in the templates, which the provider may customize before making them available as service offerings.

5.2 Interfaces and Data Artifacts

A provider interface defines how the developer and consumer interact with the provider. This architecture differentiates between service endpoints that accept (and respond to) messages over a protocol based on some message exchange pattern (functional interfaces) and the data elements and operations that an interface can support (data artifacts). The interface comprises both functional interfaces and data artifacts.

- Functional interfaces, such as Service Catalogs and Service Managers, are programming interfaces (for example, APIs). Through these interfaces, developers and consumers interact with providers to request, deploy, administer, and use services. Examples of likely functional interfaces are:
  - A Service Catalog, through which service offerings are offered, requested, and managed
  - A Security Manager, through which the security-related aspects of a cloud are managed
  - A Service Manager, through which instances of deployed services are managed and modified
- Data artifacts are exchanged over the functional interfaces. In this context, a data artifact definition describes the semantic content and the specific format (for example, the XML schema definition that describes the XML payload). Examples of data artifact types include service requests, service level-agreements (SLAs) and other contracts, service templates, service offerings, and images that contain applications. For example, a customizable contract template that includes the customer request, SLA, and security requirements is needed to support the service catalog interface. SLA, security requirements, and resource specifications are used to build offerings.

5.3 DMTF Profiles

DMTF profiles are normative specializations or extensions of the interfaces and artifacts, or combinations of them, which are useful in addressing certain contexts, such as those of interest to a security manager or a contract billing administrator. Profiles may be used to simplify the interactions and the potentially complex definitions and negotiation needed to request, manage, and use services. A profile may also

specify the use of particular standards that are useful in the profile's target environment and use cases. A profile represents a view into the provider interface.

6 Next Steps

This section describes the deliverables and alliances of the Open Cloud Standards Incubator.

6.1 Deliverables

Figure 8 outlines the Incubator's scope and deliverables. The Phase 1 deliverables — reference architecture, taxonomy, use cases, priorities, submissions from vendors, and existing standards and initiatives — will be analyzed to deliver one or more Cloud Provider Interface informational specification documents, which will be the basis for the development of future cloud standards. These documents will describe functional interfaces, protocols, operations, security, and data artifacts. Phase 2 will deliver a recommendation for each standard, which will include the gaps and overlaps as well as abstract use cases (usage scenarios that describe one or more business contexts) applicable to the sub-domain of each standard.

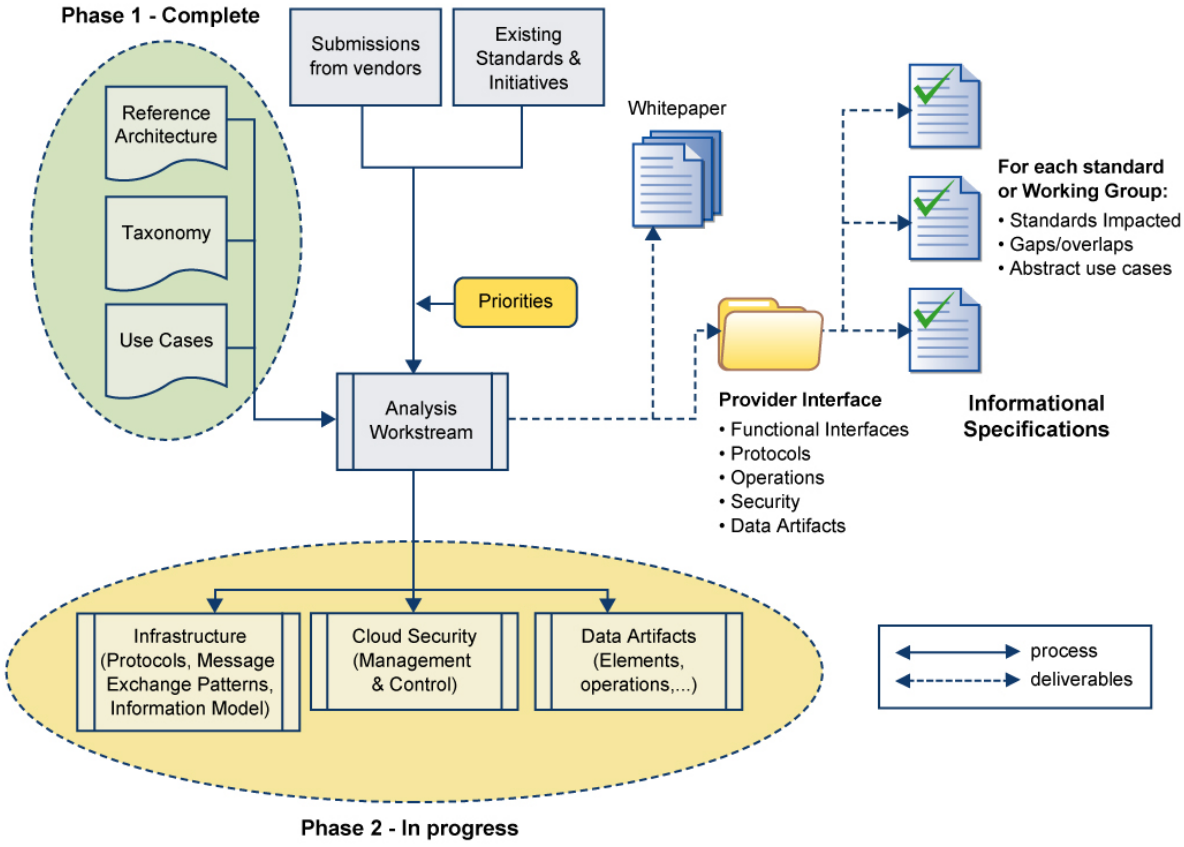

Figure 8 – Open Cloud Standards Incubator Process and Deliverables

6.2 Alliances

The DMTF values working with affiliated industry organizations such as the Open Grid Forum, Cloud Security Alliance, TeleManagement Forum (TMF), Storage Networking Industry Association (SNIA), and National Institute of Standards and Technology (NIST). The DMTF has also established formal synergistic relationships with other standards bodies. The intent of these alliance partnerships is to provide mutual benefit to the organizations and the DMTF.

Alliances play an important role in helping the DMTF to provide a unified view of management initiatives. For example, SNIA has produced an interface specification for cloud storage. The Open Cloud Standards Incubator will not only leverage that work but also collaborate with SNIA to ensure consistent standards. The Incubator expects to leverage existing DMTF standards including Open Virtualization Format (OVF), Common Information Model (CIM), CMDB Federation (CMDBf), CIM Simplified Policy Language (CIM-SPL), and the DMTF's virtualization profiles, as well as standards from affiliated industry groups.

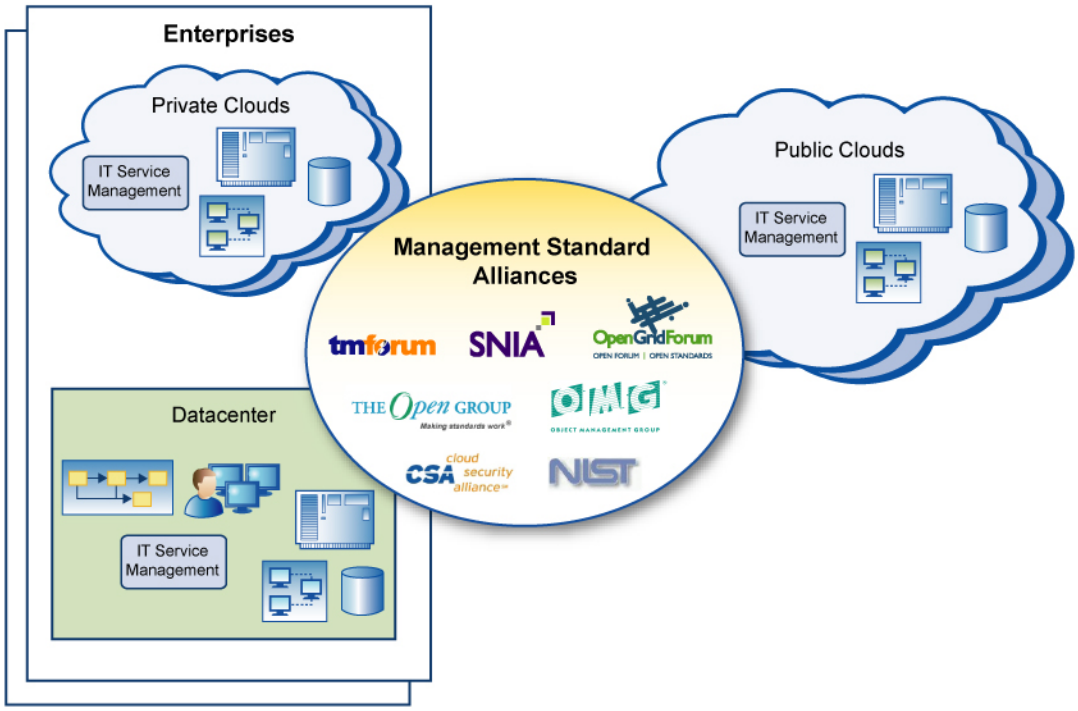

Figure 9 – Alliances

Because the goal of the Incubator is to develop information specifications on interoperable cloud management, the work scope is quite large. The use cases, reference architecture, and lifecycle described in this white paper will necessarily extend to topic areas outside the scope of the DMTF. The expectation, therefore, is that the DMTF alliances (see Figure 9) will be leveraged to create that interoperable management solution.

The development of standards is an inherently collaborative process. The Incubator team expects the collaboration to leverage the expertise not only in the companies represented in the Open Cloud Standards Incubator but also in the community at large.

7 Conclusion

The goal of the Open Cloud Standards Incubator is to enable portability and interoperability between private clouds within enterprises and hosted or public cloud service providers. The Incubator leverages existing bodies of work, along with the experiences of members, customers, and service providers, to recommend standards for interoperable clouds.

A first step has been the development of use cases, a service lifecycle, and a reference architecture. Although this body of work will be extended over time, in collaboration with alliance partners, the current and future work will define provider interfaces consisting of data artifacts, interface protocols, and security. This is a significant step forward in developing interoperable cloud management.

Bibliography

[NIST-1] *NIST Definition of Cloud Computing*, http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc

[OVF-1] DMTF DSP0243, *Open Virtualization Format Specification 1.0*, http://www.dmtf.org/standards/published_documents/DSP0243_1.0.pdf