Phacil
See the Possibilities

Cloud Computing: A Formula for Rapid Legacy Application Integration

By Rafael Collado, Phacil Co-Founder

Mr. Rafael Collado is a successful engineer and IT systems executive, specializing in the telecommunications and IT industries. He has developed network management and diagnostic systems, and designed communications processors for the US Government and private companies. For more information on Mr. Collado, please visit the Management page.

Introduction

Federal spending will face increasing pressure to raise productivity and lower costs as deficits continue, forcing the country to stretch every taxpayer dollar. The Department of Defense will see vigorous attempts to cut not only large weapons programs, but also will feel pressure on their information technology assets to deliver productivity or performance increases that will save money. Everyone will be asked to do more with less.

Several information technology architectures have emerged to help stretch IT budget dollars by reducing duplication, better matching resources to requirements and stream-lining the provisioning/sustainment of information technology assets. Service Oriented Architectures (SOA) and virtualization have been the most heavily touted. Cloud Computing is emerging as a way to get those benefits without the substantial overhead penalty in terms of times and costs associated with either SOA or stand alone virtualization.

Most vendors can readily make the case for all that their new technologies promise, but typically at the great expense of migrating from your existing platform. Cloud Computing can conceptually offer the best of both worlds by providing a format to reach legacy applications through the use of the newest platform technologies. Cloud Computing can extend the useful life of legacy applications, thereby increasing the return on investment and also permitting the expenditure of scarce financial resources on where they are actually necessary.

What is "Cloud Computing?"

The National Institute of Standards and Technology's Information Technology Laboratory defines "Cloud Computing" as "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." The Cloud Computing model, therefore, can be used as an architectural way to approach many of the challenges faced when integrating legacy capabilities with emerging technologies.

From the definition, it is clear that Cloud Computing is not a tangible technology, but a way of extracting or leveraging a broad range of technologies in a manner that is shared (multi-tenancy), massively scalable, elastic (loosely coupled), pay as you go and highly self-provisioned. This means that it is an intellectual commodity architecture with no proprietary elements. Making it more plain or clear, "Brand Y's" Cloud should, conceptually, be the same as "Brand X's" Cloud. If there is any difference at all, it is in how quickly, economically and efficiently the given exponent can execute or deliver the Cloud capability.

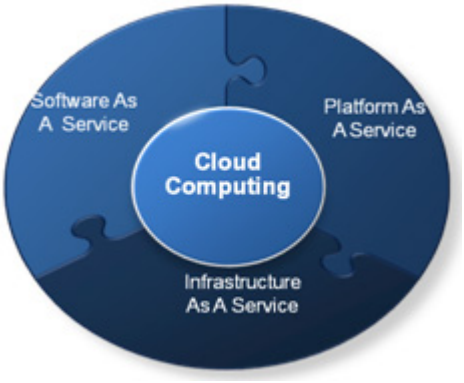

Figure 1: Classical Cloud Computing Components

The concept of Cloud Computing is broad. In its most comprehensive interpretation, Cloud Computing includes the concepts or models of (1) Software as a Service (SaaS), (2) Platform as a Service (PaaS) and (3) Infrastructure as a Service (IaaS). As it relates to this paper's purpose of showing how legacy applications can quickly be leveraged or combined with emerging technologies in a Federal agency or DoD service enterprise, we will focus on an SaaS focused Cloud implementation. By SaaS, we mean that the legacy software elements that will be incorporated in the Cloud Computing enterprise must be network accessible (browser/thin client), managed by their respective agency/service and delivered in a turn-key self-provisioned manner.

We chose to simplify our perspective of Cloud Computing and focus on the SaaS component because, for the most part, the value enterprises need to extract most quickly is that contained in applications used on a daily basis to accomplish their missions.

Cloudy Applications (Three Step Stairway to Clouds)
It is relatively easy to implement a Cloud Computing system as compared to other enterprise integration techniques. In most instances a Cloud Computing environment proof of concept can be achieved in three steps.

First step in the use of Cloud Computing is identifying critical applications (or low hanging fruit) that can offer immediate economic benefit to the agency or service. Certain mission planning applications, requirements definitions (e.g., DOORS) or earned value management (EVM) applications fit these characteristics. Office applications (word processing, spreadsheets, presentations, databases) are typically the most easily supported because of the commonality of their file structures.

Second step is determining each application's level of network accessibility. Network accessibility is the critical determinant of whether an application can be integrated into a Cloud (is “cloudy”). Applications that depend on database access are typically among the easiest because they may have ready-made application program interfaces (APIs) or web based customer facing interfaces that permit the browser access favored by the Cloud. These remotely executing applications commonly use an application server to identify the services users need. Common application servers include Red Hat JBoss Application Server, Apache Geronimo, Oracle WebLogic® (formerly BEA) and IBM® WebSphere® Application Server.

Third step is identifying the compatibility with the enterprise's identity, authorization and overall security framework. In the DOD or Federal environment, any applications currently running would have been provisioned in a manner consistent with DoD or Federal security standards. Single Sign On (SSO), CAC card access and other existing methodologies could be leveraged from the underlying Federally sanctioned infrastructure.

Figure 2: Three Step Stairway to Clouds

Cloud Computing Frameworks

There are many Cloud Computing frameworks. Among the popular public ones are Amazon's EC2 and Google Apps. Since its debut in 2006, 8.4 million EC2 instances have been launched. Impressive as these statistics are, Government and Defense enterprises consider the Public Cloud as non starters. Reasons include data security and SLA concerns, data compliance/governance regulations and the complexity of migrating secure legacy applications. The most popular frameworks for building more secure private Cloud Computing environments are Microsoft Azure, Eyeos and Eucalyptus.

Azure is Microsoft's proprietary .NET based Cloud Computing framework. Windows Azure platform AppFabric, formerly called ".NET Services", provides an architectural construct that permits developers to connect applications and services in the Cloud or on-premises. This includes applications running on Windows Azure, Windows Server and a number of other platforms including Java, Ruby, PHP and others. It provides a Service Bus for connectivity across network and organizational boundaries, and Access Control for federated authorization as a service. With Microsoft's prevalence in the Federal space it would not be beyond conception that for the right price a private Federal of Azure could be had.

Eyeos is an open source platform that provides a secured web-based desktop-like environment and a set of libraries for easy development of web applications. It could be stood up in a private environment and made compatible with the FISMA guidelines. The idea behind Eyeos is that whole application components of an enterprise system can be executed or accessed through the web browser. The client must have only a web browser to work with Eyeos and all its resident or collaborative applications, including Office applications and Personal Information Managers (PIMs). The Cloud system would be workstation hardware independent.

Another secure framework is the Ubuntu Eucalyptus. Eucalyptus is an open source software infrastructure for implementing an on-premise Cloud Computing system using an organization's IT infrastructure, without modification, special-purpose hardware or reconfiguration. Eucalyptus turns data center resources such as machines, networks, and storage systems into a Cloud that is controlled and customized by local IT. With Eucalyptus, businesses of any size can leverage their own IT resources to get the benefits of Cloud Computing without the concerns of lock-in, security ambiguity and unexpected storage costs that can be associated with public Clouds.

Eucalyptus is the only Cloud architecture to support the same application programming interfaces (APIs) as public Clouds, and today Eucalyptus is fully compatible with the Amazon AWS public Cloud infrastructure. The Eucalyptus design gives users the flexibility to seamlessly move applications from on-premise Eucalyptus Clouds to public Clouds, and vice versa. Eucalyptus also makes it easy to deploy "hybrid" Clouds, which use public and private Cloud resources together to get the unique benefits of each. Eucalyptus runs on a wide range of popular Linux distributions, including Ubuntu, for which it has been specially packaged to improve ease of installation and maintenance.

Finally, custom executions based on modified application interfaces could be assembled into a Federal or DoD specific framework.

Conclusion

Whether implemented using web services, a collection of APIs or custom code, Cloud Computing is an ideal way to quickly prototype integrated applications that can be accessed through thin clients. They offer moderate performance and are low cost, scalable and rapidly deployable.