TIP Publication Date
January 30, 2014

Cloud Components – Part 1

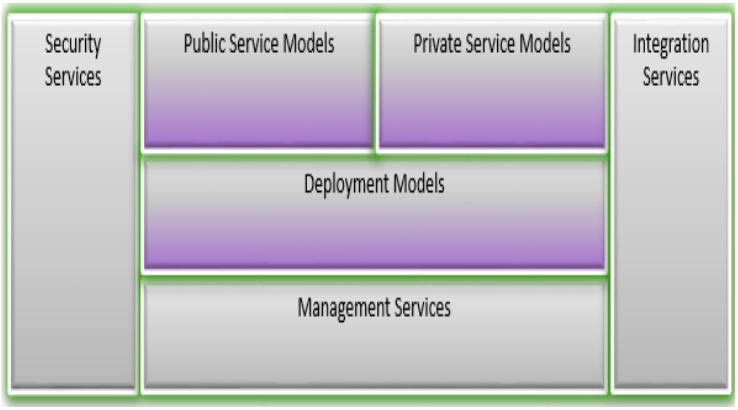
More Than Meets the Eye

One of the topics we see on multi-year strategy decks, discussed in hallway conversations, and often written about is the term "going to the cloud". This term is often used as a way of saying that we are going to move on premise applications into a cloud-based environment, or replace existing applications and switch to the SaaS based equivalent. In general, there is nothing wrong the statement or intent. However, it is my personal opinion that we are taking this too lightly without understanding the true impact on your IT processes and technology layers.

This paper will outline the different components that in most cases, cannot be omitted, and at the very least should be identified during your "going to the cloud" activities. Think of this as a conceptual model, if you will.

There are 5 distinct layers or domains that you will need to address in some form or fashion. They are:

1. Security Services
2. Management Services
3. Integration Services
4. Deployment Models
5. Cloud Service Models



The Integration Services, Deployment, and Cloud Service Models will be described further in Cloud Components – Part 2.

Understanding these layers will help you in setting reasonable expectations, fine-tune your implementation strategy, and increase the accuracy of your budget estimates.

Next I will describe some of the key functions/observations within the above mentioned layers or domains. Please note that I only cursory mention the Deployment Models (Private, Public, Hybrid, and Community) and Cloud Service Models such as PaaS, SaaS, IaaS, etc. in this paper, since I assume most readers will be familiar with these.

I will also introduce a subjective "Effort Indicator" – where effort is a subjective indicator of complexity relative to the Cloud Deployment Model of choice – where two "+" signs are considered double the effort compared to a single "+" sign.

> *In a recent survey "33% said getting to the cloud cost more than anticipated, citing unexpected expenses in setting up a cloud architecture or in the transition of existing systems. Once implemented, 31% said they encountered unexpected integration costs between the cloud and their existing systems. Thirty percent worried about data loss in the cloud, the privacy risk and loss of control over their own operations." – KPMG - 2013*

Security Services

Of all the articles written about cloud, security is the one that is seen most prevalently as the highest risk factor, but when dealt with this in a serious and diligent matter, you will see that the top-tier cloud providers have an extremely robust security architecture in place. Nonetheless, the following sections need to be worked out to ensure compliance with your company's security policies:

Data and Privacy Protection

This element includes physical access protection of the facility, backup/restore particulars (data retention/data destruction), transnational access to data, data locations(s), as well as individuals. [1]

Application Security

Depending on what Cloud Service Model you operate, the following items need attention; trust the image, hardening hosts, securing inter-host communication, manage the application keys. In addition for PaaS, put in place secure design and coding patterns as to match the technology specific application security standards and application security assurance tools for software built on this platform. An enterprise looking to extend its current secure development lifecycle will have to develop this knowledge and tools.

Compliance and Monitoring

The four basic elements to understand are:

- Cloud computing typically increases an organization's reliance on the cloud providers' logs, reports, and attestations in proving compliance. The organization's ability to monitor actual

[1] ***Source: Cloud computing: its impact on privacy, jurisdiction, security, lawful access, ownership and permanence of data*** **—- Patrick D Flaherty and Giancarlo Ruscio**

activities and verify security conditions within the cloud is usually very limited and there are no standards or commercial tools to validate conformance to policies and SLAs.

- Co-Tenancy and Noisy or Adversarial Neighbors: Cloud computing introduces new risk resulting from co-residency, which is when different users within a cloud share the same physical requirement to run their virtual machines.
- Cloud services are typically virtualized, which adds a hypervisor layer to the traditional IT services stack. This new layer in the service stack introduces opportunities for improving security and compliance, but also creates new attack surfaces and potential exposure to risks. Organizations must evaluate new monitoring opportunities and the risks presented by the hypervisor layer and account for them in policy definition and compliance reporting.
- Cloud services raise access and protection issues for user data and applications, including source code. Who has access, and what is left behind when you scale down a service; ways to protect data from the virtual infrastructure administrators and cloud co-tenants; and encryption of data—at rest, in transit, and eventually in use—would become basic requirements to establish as well as "data destruction."

Identity and Access Management [2]

The following should be considered:

- Identity Provisioning: The secure and timely management of on-boarding and off-boarding of users in the cloud. Further, enterprises that have invested in user management processes within an enterprise will seek to extend those processes to cloud services.
- Authentication: Authenticating users in a trustworthy and manageable manner is a vital requirement. Organizations must address authentication-related challenges such as credential management, strong authentication, delegated authentication, and managing trust across all types of cloud services.
- Federation: This plays a vital role in enabling organizations to authenticate their users of cloud services using the organization's chosen identity provider (IdP). In that context, exchanging identity attributes between the service provider (SP) and the IdP securely is also a requirement. Organizations considering federated identity management in the cloud should understand the various challenges and possible solutions to address those challenges with respect to identity lifecycle management, available authentication methods to protect confidentiality, and integrity, while supporting non-repudiation.
- Authorization and User Profile Management: The requirements for user profiles and access control policy vary, depending on whether the user is acting on their own behalf (such as a consumer) or as a member of an organization (such as an employer, university, hospital, or other enterprise). The access control requirements in SPI environments include establishing trusted user profile and policy information, using it to control access within the cloud service, and doing this in an auditable way.

[2] ***Source: Cloud Security Alliance***

Cloud Deployment Model	Public	Private	Hybrid
Security Services Effort*	+++	++	+++

"At Trexin, we have been through a number of security focused sessions with our customers and cloud providers, and in the vast majority of cases, the security and audit capabilities provided by the mainstream cloud providers has exceeded the requirements of the customer. In only a few cases, a procedural exception had to be requested - or the cloud deployment model had to be adjusted from public to private based on US Government ITAR compliance restrictions to name a more extreme example." – Ton Roelandse – Senior Principal

Management Services

A broad range of disciplines operational in nature, which have all to do with managing the delivery of cloud applications and services, and efficient operation of the cloud infrastructure. Its complexity comes under pressure, i.e. increases when applied in hybrid and multi-cloud environments. Management Services activities are typically least involved in traditional SaaS applications such as Salesforce, but are becoming very involved with PaaS or IaaS type Cloud Service Models.

Self Service

Empowers access to fully governed, standardized and customizable applications and platforms. For cloud-based applications and services, there are significant cost and time to market advantages achievable, and should include flexible governance, compliance, and security policies and enforcement all build into the Self Service component.

Workload Pattern Analysis

Calls for mechanisms to characterize and predict server workload continuously so that the capacity of the supporting infrastructure can closely match the needs of new applications or computing tasks. In a typical PaaS implementation, it is your software that needs to understand and trigger the needed capacity/elasticity actions. In addition, you need to understand your workload consumption in much granular detail as to ensure you are not paying for a workload that is not performing any action.

Workflow Administration

A central point to ensure co-ordination of application specific tasks such as maintaining the application state, tracking workflow executions and logging their progress, holding and dispatching of tasks, controlling which tasks each of your application hosts will be assigned to execute

Service Level Agreements

In a cloud environment, with multiple vendors, internal IT services, and combinations of PaaS, IaaS, SaaS and other forms, an SLA architecture is needed to collect, collate and measure, and report on the end-to-end performance that is provided.

Workload Management

Intelligent workload management is a computing model that enables IT organizations to manage physical, virtual and cloud environments as a unified, fully integrated system. Intelligent workload management provides the tools to build, secure, manage and measure an integrated stack of application, middleware and operating system-a mix that constitutes modern workloads.

Orchestration and Provisioning

The composition of architecture, tools and processes by humans to deliver a defined service, the stitching of software and hardware components together to deliver a defined service, the connecting and automating of work flows when applicable to deliver a defined service.

Monitoring

As more and more environments are moving toward virtualization, one common challenge has emerged: how to achieve the necessary visibility and control of a virtual infrastructure when managing a cloud infrastructure. To realize true cost savings from a virtualization or cloud investment, users must be able to run virtual machines densely enough to maximize consolidation, yet be assured that their workloads are still running as well as they were before being virtualized—with plenty of room for expansion.

Cloud Deployment Model	Public	Private	Hybrid
Management Services Effort	+++	++	+++

Conclusion

There is more than meets the eye when “going to the cloud”. The key takeaway is that you need to understand the behavior of your applications and services and their interactions in a lot more detail to effectively utilize all the advantages a cloud-based approach has to offer. In addition, you need to operate this infrastructure as efficiently and make it as lean as possible. The items listed in this paper need to be considered, although not all of them will apply or need to be in place on day one of your being in the cloud. In Cloud Components – Part 2 I will address the remainder of the domains, as well as introduce a conceptual architecture diagram. Stay tuned.

This TIP was written by Ton Roelandse, who specializes in Applied Cloud Technologies and other cool topics. Ton welcomes comments and discussion on this topic and can be reached at ton.roelandse@trexin.com.