

An Intalio White Paper

Ismael Chang Ghalimi, CEO — May 2010

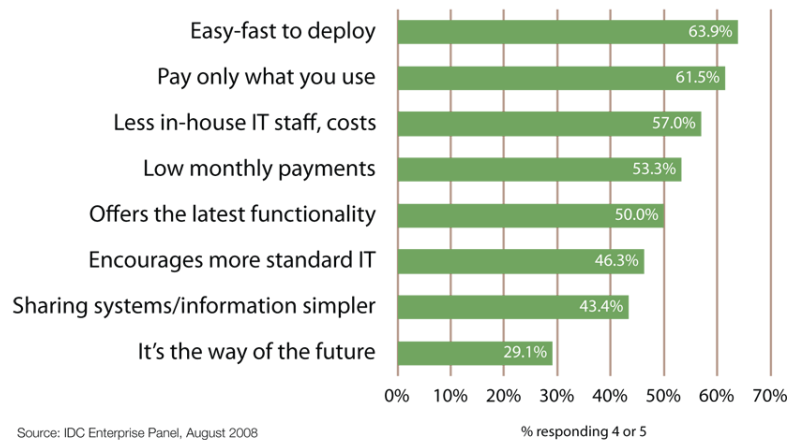
# The Case for Private Clouds

While early proponents of the Cloud Computing revolution make the headlines claiming that private clouds are not "true" clouds, customers know better and are deploying them faster than public cloud operators can roll new data centers out. Here is what they like about Private Clouds.

## Introduction

In 1943, Thomas J. Watson, then President of International Business Machines (IBM), allegedly<sup>1</sup> said, "I think there is a world market for maybe five computers." Today, industry pundits make similarly flawed predictions, claiming that all the market needs is maybe five clouds: Amazon Web Services, Force.com, Google AppEngine, Microsoft Azure, and whatever IBM comes up with. Clearly, Cloud Computing is generating a lot of interest among Chief Information Officers:

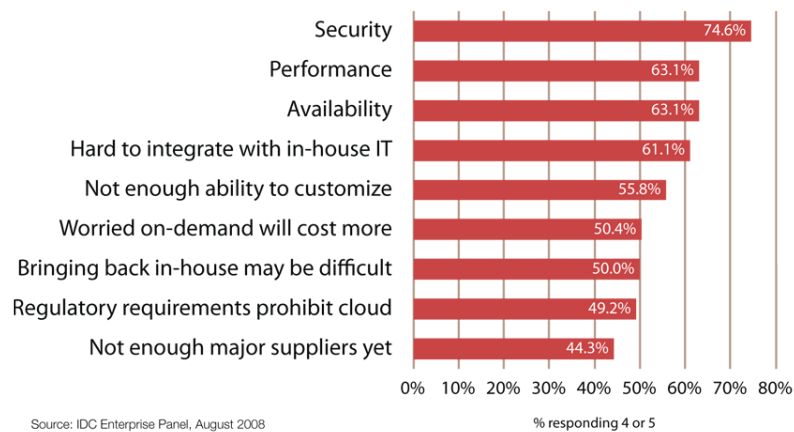
**Q: Rate the benefits commonly ascribed to the "cloud"/on-demand model**  
(1=not important, 6=very important)



Yet, however you define Cloud Computing<sup>2</sup>, this evolutionary step in the 50 years long evolution of distributed computing goes far beyond the few public clouds available today. And while simple principles of economy of scale will most likely limit the number of general-purpose public clouds, most of the action will take place on private and virtual private clouds, served from private and virtual private networks. And this is a good thing. A world where just five public clouds operated by five corporations serve all data and applications would be a pretty scary place to live in. CIOs agree:

**Q: Rate the challenges/issues ascribed to the “cloud”/on-demand model**

(1=not significant, 6=very significant)



Source: IDC Enterprise Panel, August 2008

The need for private and virtual private clouds is driven by a combination of factors, many of which were clearly outlined by Gartner's Bruce Robertson in his recent article titled Top Five Cloud-Computing Adoption Inhibitors<sup>3</sup>. Bruce felt compelled to add a sixth one (Vendor Viability), and we took the liberty to add a few others, while slightly altering their designations for clarity purposes.

## Risk Management

When using the services of a public cloud provider, your options for risks assessment are rather limited. While compliance to industry standards such as SAS 70<sup>4</sup> or the publishing of auditable availability metrics in a trust.salesforce.com<sup>5</sup> fashion can provide some level of comfort, they are not sufficient for proper risk management. Deploying a private cloud in your own data-center, or in the data-center of a trusted third-party (such as your local telecommunications service provider), will give you a more complete picture of the risks inherent to cloud computing.

## Location

As the saying goes, real estate is about three things: Location, Location, Location. While this might be counter-intuitive for those of us confusing cloud computing with ethereal computing (a made-up term for a common misconception about cloud computing), the location of clouds really does matter, be it when talking about meteorology or computing. The geographic location of the servers powering a cloud has direct implications on how it will perform, and whether it will comply to specific regulations or not. For example, desktop virtualization requires low latency, which itself demands geographic (or network) proximity. Similarly, most database-driven applications will work only if the application sits really close to the data. And if you're a retail bank, the data you collect about a customer must remain in the customer's country, as stated by law in many countries. While the largest public cloud providers usually have multiple Points of Presence (Salesforce.com has some in two countries: North America and Singapore), many local cloud providers will emerge in order to provide geographic proximity to customers in the World's 195 countries (at the time of writing).

## Portability

An application developed with Force.com can only run on the Force.com public cloud. And while many public cloud providers like to talk about interoperability, their objectives are to lock customers up with a proprietary architecture, API, or programming language. The choice is clear: Bluepill, half a dozen public clouds reluctantly agreeing to half-baked interoperability standards. Redpill, millions of private and virtual private clouds built on top of a common infrastructure. With no hesitations, I take the redpill<sup>6</sup>.

## Resilience

While we are writing this article, it is becoming clear that Microsoft/Danger lost all the data stored by customers on their Sidekick smartphones. Contacts, calendar entries, to-do lists, and photos are gone, following a botched SAN upgrade undertaken without proper data backup. Data loss is a huge concern for consumers and corporate customers alike, and private clouds provide an answer to this. For consumers, the deployment of reverse backup solutions such as the Egnyte Local Cloud<sup>7</sup> provides a virtually failsafe solution, at a very low cost. For corporate customers, the use of a private cloud implementing proper data backup and disaster recovery policies will significantly reduce the risk of catastrophic data loss.

## Security

Many security experts claim that most corporations cannot afford the legions of systems administrators employed by the likes of Amazon or Google to secure their public clouds, then conclude that public clouds are inherently more secure than private ones. This is either naive, dishonest, or plainly stupid. First, currently available public clouds are utterly primitive when it comes to security. For example, VPN access is both a novelty there (Amazon just released the Amazon Virtual Private Cloud<sup>8</sup>), and the very best they can offer (forget about two-factor authentication with devices like RSA SecurID<sup>9</sup>). Second, the security of most public clouds currently available has

been successfully breached over the past few years, usually through Denial-of-Service attacks or phishing methods, and the pace at which such events occur does not seem to be slowing down. Third, and maybe most importantly, a small number of homogeneous public clouds creates massive single points of failure. In essence, if a significant amount of the World's computing and storage needs are addressed by half a dozen public clouds, any vulnerability in the security infrastructure of any of these clouds will expose over 15% of the World's IT assets to unimaginable risks. This primitive architecture simply makes no sense at all, and in a weird twist goes against the Internet's distributed architecture, which enabled cloud computing at the first place. If we want secure cloud computing, we want millions of private clouds, not just 5 public ones.

## Confidentiality

Data confidentiality is one of the most difficult things to guarantee in a cloud computing environment. There are several reasons for that: First, as public clouds grow, the number of people working for the cloud provider who actually have access to customer data (whether they are entitled to it or not) grows as well, thereby multiplying the number of potential sources for a confidentiality breach. Second, the needs for elasticity, performance, and fault-tolerance lead to massive data duplication and require aggressive data caching, which in turn multiply the number of targets a data thief can go after. Third, end-to-end data encryption is not yet available. What this means is that while data can be encrypted when transiting between the end-user's client and the cloud's server, and can also be encrypted when stored on the cloud's server, it must be decrypted on the cloud's server when being processed for a query or a transaction, unless fully homomorphic encryption<sup>10</sup> is used. But until such a technology goes out of the few labs where it is currently being developed (which will take some time), data confidentiality will be maximized by using a large number of private clouds managed by trusted parties.

## Regulations

Local regulations will most certainly be the strongest driver for the deployment of private clouds. Many vertical industries such as financial services and healthcare, as well as the overall public sector mandate that certain classes of data be stored and processed locally, in some cases by local service providers. While the deployment of local Points of Presence by private cloud operators will address such requirements in some cases, it will not be sufficient in countless others, and the deployment of local private clouds will be necessary.

## Service Level Agreement

Another powerful driver for the deployment of private clouds will be the need for specific Service Level Agreements that public cloud operators cannot address, either because they're not compatible with their business models, or because they cannot be supported by their technical architectures. For example, most public clouds today deliver three nines uptime (99.9%, or downtime less than nine hours per year), and four nines is a distant dream for all of them (52m36s). All the while, many customers demand five nines availability (5m16s), which requires a technical architecture and a set of procedures significantly different from the ones deployed by most public cloud operators. Another area of concern is related to data ownership, as stated by user agreements. While some service providers are pretty clear about it, others remain dangerously ambiguous, making their clouds totally unsuitable for a broad range of applications.

## Control

Last but not least, the need for overall control will be the one predicated the use of private clouds for most organizations. While this alternative form of cloud computing might not offer the same economics or the same level of elasticity as the ones delivered by their public counterparts, it will always provide the extra level of control that large organizations crave for.

- 
- <sup>1</sup> [http://en.wikipedia.org/wiki/Thomas\\_J.\\_Watson - Famous\\_misquote](http://en.wikipedia.org/wiki/Thomas_J._Watson - Famous_misquote)
  - <sup>2</sup> <http://www.intalio.com/benefits-of-cloud-computing>
  - <sup>3</sup> [http://www.gartner.com/DisplayDocument?doc\\_cd=167920](http://www.gartner.com/DisplayDocument?doc_cd=167920) (Gartner Account Required)
  - <sup>4</sup> [http://en.wikipedia.org/wiki/Statement\\_on\\_Auditing\\_Standards\\_No.\\_70:\\_Service\\_Organizations](http://en.wikipedia.org/wiki/Statement_on_Auditing_Standards_No._70:_Service_Organizations)
  - <sup>5</sup> <http://trust.salesforce.com/trust/status/>
  - <sup>6</sup> <http://en.wikipedia.org/wiki/Redpill>
  - <sup>7</sup> [http://www.egnyte.com/corp/local\\_drive.html](http://www.egnyte.com/corp/local_drive.html)
  - <sup>8</sup> <http://aws.amazon.com/vpc/>
  - <sup>9</sup> <http://www.rsa.com/node.aspx?id=1156>
  - <sup>10</sup> <http://www-03.ibm.com/press/us/en/pressrelease/27840.wss>



Intalio, Inc.  
World Headquarters  
644 Emerson Street, Suite 200  
Palo Alto, CA 94301  
United States

Worldwide Inquiries:  
Tel: +1 (650) 596-1800  
Fax: +1 (650) 596-1801  
info@intalio.com  
www.intalio.com



Intalio is committed to developing practices and products that help protect the environment.

Copyright © 2010, Intalio and/or its affiliates. All rights reserved. This document is provided for information purposes only and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Intalio is a registered trademark of Intalio, Inc. and/or its affiliates. Other names may be trademarks of their respective owners.