InsideCounsel

Technology: Cloud computing 101

Examining the impediments to the adoption of cloud computing

BY JOHN COWLING, DANIEL NELSON
August 31, 2012 • Reprints

Cloud computing is exploding worldwide. Consider the following facts:

- The world's biggest datacenters occupy more than 1 million square feet, enough to house 17 football fields.
- 5.75 million new servers are installed annually just for online services.
- 36 percent of all data centers use cloud computing.
- Cloud users report saving 21percent on applications moved to the cloud.

The primary impediments to the adoption of cloud computing, in order of importance to consumers of cloud services, are: security, interoperability, vendor lock-in, regulatory compliance, reliability, complexity, privacy and pricing. These concerns raise contract drafting issues for cloud computing contracts. Part 1 will cover security, interoperability and vendor lock-in. Part 2 will address the remaining issues.

1. Security

Service level agreements (SLAs) should contain provisions describing the infrastructure and security for the cloud service. The customer should define the security parameters and security monitoring promised by the service provider in the SLA in specific and measurable ways. Without these specifics, it will be hard to evaluate security and to know whether the service provider is delivering the security promised. For example, provisions commonly describe what intrusion monitoring and incident reporting the vendor will provide. The SLA may also provide the customer with the ability to periodically audit the

security of the provider. The SLA may contain provisions defining load testing parameters and data portability testing.

Surveys have shown that many consumers of cloud services do not monitor security aspects of their cloud services on a continuous basis, in spite of security being a top concern for respondents. For example, availability is frequently addressed in the SLA and monitored by the customer. Other security parameters are often not well-covered in the SLA or, if covered, are not monitored sufficiently. For example, if the SLA provides for penetration tests, failover or backup testing, the customer should implement a program to make sure the testing is actually performed and the results are reported. The program should be covered in the SLA. Another issue is that data portability testing is often overlooked and not tested. In all cases, security and testing reports should be reviewed and retained in case a problem develops.

Also consider whether there should be penalties for noncompliance. Many SLAs contain detailed security definitions and monitoring, but no specific provisions addressing the consequences for failing to comply. Boilerplate provisions addressing breaches of the contract are often too general to provide meaningful remedies for breaches of the SLA. Compliance and penalty provisions should be crafted to incentivize the vendor to provide the required service levels.

2. Interoperability

Interoperability refers to the ability of the cloud service to interact with other services. There are two aspects of interoperability for cloud computing: interoperability within a single cloud (vertical interoperability) and interoperability between clouds (horizontal interoperability). Interoperability within a single cloud is how the cloud software integrates with other applications or devices that the customer uses. Interoperability between clouds refers to the ability of the customer to transfer data to or switch to another cloud provider.

Vertical interoperability usually involves significant technical issues but relatively insignificant contract issues. The SLA and other contract documents should specifically address the technical issues: providing for the development of specific specifications, setting out the testing protocols, delineating acceptance signoffs, addressing bug fixes and setting out the implementation schedule. The contract should also address customization issues such as the cost of customization, how much customization is permitted (many cloud services only allow limited customization), how

customizations will be addressed in major upgrades and service releases, and ownership of customizations or ancillary applications developed for the customer.

3. Vendor lock-in

Horizontal interoperability (also called portability) presents significant risk to customers and, therefore, presents significant contract issues. Some of the risks presented by using cloud services are:

- Unacceptable increases in cost at the time of contract renewal
- Prevention or delay in the ability to switch to the same or similar service at a lower price
- A provider goes out of business or ceases to offer services
- A business dispute with the provider.

The customer needs to address these issues in the contract and review the vendor provisions carefully. For example, many cloud contracts contain “data hostage clauses” that, in case of a dispute between the customer and the vendor where the vendor claims that the customer improperly terminated the contract, the vendor is permitted to hold on to the customer’s data until the customer pays a termination fee or liquidated damages. Other areas to evaluate carefully and negotiate where appropriate are automatic renewal provisions and price escalation provisions. Often these issues are linked; the vendor wants to lock in the customer with automatic renewals and the customer wants protection from excessive price increases over time. A balance needs to be reached between these two interests.

The contract should specifically address how the customer can receive its data from the cloud provider in a usable format upon termination of the relationship, or if the provider chooses to discontinue all or part of the service. The contract should set out the cost of providing the data as well as the form and the logistics of doing so.