

# Speaking of Cloud

A more granular definition of public versus private cloud helps organizations understand the range of available options and select the most appropriate cloud IaaS solution for their needs.

Sometimes a single word can fully encompass a complex concept. Other times, one word simply isn't enough. It all depends upon your perspective.

Legend has it, for example, that Arctic peoples have many more words for "snow" than do people of more temperate climates. Legend or not, it expresses the notion that differences in language reflect differing views of the world.

When it comes to cloud computing, one word may be enough to define consumer-oriented cloud services. For consumers, the word "cloud" adequately describes IT services accessed remotely via the Internet. The word conveys the sense of abstraction of computing into the unknown.

IT professionals, in contrast, generally break down the concept further into "public cloud," describing services made available to large groups, and "private cloud," describing a cloud infrastructure operated exclusively for an organization. Then there is the "hybrid cloud" that combines public and private cloud infrastructures through technology that enables data and application portability.

As cloud computing matures, however, these terms have become insufficient to describe the various procurement, deployment and management options that are available within the cloud. Organizations need a bigger vocabulary to help them make informed decisions about today's cloud Infrastructure-as-a-Service (IaaS) offerings.

## Defining Cloud IaaS

The National Institute of Standards and Technology (NIST), a non-regulatory arm of the Commerce Department, has developed a definition of cloud comput-

ing that will serve as a foundation for the federal government's use of cloud models, architectures and deployment strategies. The NIST defines cloud IaaS as the ability of the cloud provider to provision processing, storage, networks and other fundamental computing resources such that the customer is able to deploy and run arbitrary operating systems and applications. In the NIST definition, the customer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications and possibly limited control of select networking components (e.g. host firewalls).

This definition makes basic presumptions about the ownership and management of the cloud environment that are not necessarily true, according to Vince Conroy, CTO of FusionStorm.

"The NIST definition presumes that the service provider owns hardware, software and other technology assets used to deliver the cloud services, and houses these resources in its data center. It also presumes that the service provider manages and controls most, if not all, of those resources," he said. "However, it is just as likely that the customer will own assets and that the assets will be housed in the customer's data center. The customer may also manage the cloud infrastructure, or there may be a hybrid model with different boundaries of management. Those are valid options in today's cloud IaaS environment."

## Five Characteristics

Furthermore, the NIST definition fails to encompass the full spectrum of IaaS options available in today's cloud computing marketplace. Conroy says cloud IaaS solutions



800.228.TECH

[www.fusionstorm.com](http://www.fusionstorm.com)

- IT Consulting
- Technology Solutions
- Managed/Hosted/Cloud

are better defined by five distinct characteristics, each of which has a “public” and “private” component. Each of these characteristics can be combined in many different ways.

“Three of those characteristics are who owns the resources, where the resources are located, and who manages those resources,” he said. “You also have to ask whether the environment is multitenant or dedicated — is the cloud infrastructure dedicated to serving one customer or does it serve multiple customers? This distinction applies even if the customer hosts the environment. You can have a multitenant cloud that sits inside of a customer’s facility that serves different business units within the company.

“The final question is what audience of users is being served? Is it users who are only on the customer’s private network or does it include users on the public Internet who securely authenticate into those systems, or even non-authenticated public users? Again, the terms ‘public’ and ‘private’ are insufficient to answer this question.”

The “public cloud,” as that term is typically used, refers to an infrastructure owned by the service provider, located in the service provider’s facility, managed by the service provider, and serves multiple customers who access it via the public Internet. The classic private cloud is just the opposite: the infrastructure is owned by the customer, located in the customer’s data center, managed by the customer, and is dedicated only to that customer’s internal users. However, these scenarios merely represent the two endpoints on the full spectrum of possible cloud IaaS options.

## Financial and Operational Impacts

The appropriate combination of the five “public versus private” characteristics depends upon the needs of the business and the application. For example, who owns the infrastructure — the service provider or the customer — determines whether the cloud IaaS environment is an operational or capital expense.

The location of the infrastructure also has financial implications, even if the customer owns the assets. A customer’s onsite data center requires real estate and may incur substantially greater power and cooling costs than a cloud provider’s data center. There are operational impacts as well.

“Obviously, whether the service provider or the customer manages the infrastructure impacts the allocation of operational resources,” said Conroy. “It may also affect SLAs. When the service provider manages the infrastructure, the IT manager has the ability to hold a third party accountable for the performance and uptime of the system. That may be harder to do with an internal group.”

## Decision Drivers

Service provider ownership of the assets delivers two of the key benefits of cloud IaaS — increased flexibility and decreased risk. In a legacy model, IT managers must request more capital funds if they buy too little IT infrastructure, or face scrutiny if they buy too much and underutilize that infrastructure. In a cloud IaaS environment, IT managers don’t need a crystal ball to see how much infrastructure they will need to support changing business requirements. They gain financial, operational and business agility through the ability to quickly scale the infrastructure on demand.

However, the IT resources needed for any given application often dictate the location of the infrastructure and whether or not it is dedicated to the customer.

“A preproduction application in a test-and-development environment might work perfectly well in a multitenant infrastructure hosted by a service provider in the classic public cloud model,” said Conroy. “A resource-intensive production application might also be hosted by the service provider but on dedicated infrastructure serving only private users. However, end-user

remote access and mobility requirements may dictate public Internet access for certain applications and resources.”

The customer’s security and regulatory compliance requirements affect decisions across all five characteristics. Are there adequate “hard” and “soft” security measures? Does the service provider’s data center meet regulatory requirements? Has the service provider’s staff been vetted? What access restrictions and logging functions are in place?

“Once these critical issues have been addressed, the customer should have a clearer picture of the appropriate combination of cloud characteristics needed to meet particular business needs and application requirements,” Conroy said.

## Remaining Barriers

The five cloud characteristics illustrate how a more granular definition of public versus private cloud can help customers overcome key concerns regarding cloud IaaS and select a cloud service provider based upon business and application requirements. Barriers remain, however. Further refinement of the cloud model is needed to fully address customer concerns regarding cloud adoption.

One issue is transparency. Customers want more than SLAs. They want the ability to see what’s going on inside the IaaS architecture as well as the performance and availability of the cloud components behind it.

“Some large, well-publicized public cloud outages have exposed the fact that the cloud providers were not as transparent as they could have been about how the cloud operated internally,” Conroy said. “Cloud providers should learn from these mistakes and provide customers with a high degree of visibility into the IaaS environment.”

Customers also want greater flexibility and choice. For example, some customers need to integrate dedicated servers into the cloud environment to support legacy or non-x86 platforms that cannot be virtualized. Too many cloud service providers have created inflexible platforms that cannot easily adapt to those kinds of requirements.

Customers want an easy solution for disaster recovery and business continuity. Cloud should be an enabler rather than an inhibitor of business continuity, and cloud IaaS providers should offer a simple means for performing backup and disaster recovery within the cloud.

“Customers also want the ability to easily move workloads back and forth between internal systems and various cloud providers. As a consequence, they want to mitigate against proprietary solutions that create cloud lock-in,” said Conroy.

## Conclusion

The cloud adoption dialog remains focused on the public versus private cloud debate, seemingly limiting the customer’s choices to either building out a private cloud infrastructure in-house or accepting the potential risks inherent in the public cloud. This either-or scenario does not encompass all of the options available in the cloud IaaS marketplace.

Customers need a more robust language to describe the various ways in which a cloud infrastructure may be procured, deployed, managed and accessed. Just as Eskimos may have many words for “snow,” IT managers need a vocabulary that goes beyond “public” and “private” to discuss the cloud environment.

By breaking down cloud IaaS into five characteristics, each of which may be “public” or “private,” IT managers can make informed decisions regarding cloud IaaS solutions. Selecting a service provider that most closely matches business and application needs is critical to reaping all the benefits of scalable cloud infrastructure while meeting specific financial, operational, security and access requirements.