UNDERSTANDING, CREATING, AND SECURING YOUR HYBRID CLOUD

OUTSCALE

Excellence as a Service

Introduction

In the early days of Cloud computing, the only Cloud that existed was public. It was a third-party, vendor-owned platform offering multi-tenancy Infrastructure as a Service. Times has changed.

Over the years, we've seen scores of new Cloud service models (PaaS, DaaS, etc.) and deployment methods (private, baremetal) hit the market. As is often the case, each of these fits into a slightly different use case. Although industry commentators, in the interest of drumming up controversy, are wont to stack them against one another.

Perhaps one of the most interesting of these service models is Hybrid, which blends public and private.

Coincidentally, it's also one of the models best-suited to adoption by businesses.

Why Does The Hybrid Cloud Matter To Your Business?

Established companies with existing IT infrastructure and commitments often have neither the desire nor the ability to migrate lock, stock and barrel into the public Cloud. There are two primary reasons, though both are somewhat spurious.

- Security – For the most part, the narrative that private Clouds are inevitably more secure than public Cloud platforms is an expensive canard. The expertise to build secure Cloud platforms resides with public Cloud vendors and very rarely with the IT departments of other companies. But there are legitimate reasons why a business would want to keep some of its data in-house.

- Legacy systems – Many companies have extensive, business critical IT infrastructure so integrated into their operations that it cannot simply be abandoned. Hybrid Clouds can be used to bring some of the benefits of Cloud computing to these organizations. For instance, many legacy banking IT platforms are built around a batch processing model that does not meet the real time needs of customers. Hybrid Clouds allow banks to wrap real-time systems around their existing batch processing systems.

Real-time environments aside, the benefits of a hybrid Cloud far outweigh any perceived drawbacks:

- Redundancy – Public, Cloud-based redundancy for private infrastructure is a less expensive, more flexible method of creating resilient networks.
- Mixed Environments - Some applications are better dealt with on private infrastructure because of a need for extremely low latencies or a desire to avoid having to push workloads through the public Internet. Most organizations that require very low latency systems don't require them for every workload, so a mixed environment allows them to benefit from the flexibility of public Clouds when they offer the best solution.

It is rare to see a solution that solves all possible problems. The public Cloud comes close to it, but there are scenarios in which private infrastructure deployments are still optimal. Hybrid Clouds allow businesses to leverage the specific benefits of each. Not only that, they allow unprecedented agility through Cloud bursting, which we will discuss next.

Cloud Basics: What Is Cloud Bursting?

The major benefit of Cloud computing is the ability to scale quickly, deploying additional resources as the need arises. Cloud bursting is the answer here. It allows even businesses with existing. in-house architecture to tap into this scalability.

Here's a simple example: you host a relatively popular eCommerce store on in-house servers. Each holiday season, traffic exceeds the capacity of your hardware, resulting in a poor shopping experience. Purchasing extra servers is not an option, as they will remain idle for most of the year.

In order to accommodate the additional traffic, you can plan to "burst" into the Cloud.

When traffic exceeds the resources of the in-house infrastructure, new requests can be routed to a synced copy of the site in the Cloud. The Cloud portion of what is now a hybrid Cloud can then be scaled according to demand. As traffic hits its peak, more Cloud servers can be brought online, and then they can be spun down as demand wanes.

In reality, Cloud bursting is somewhat more complex. Synchronizing in-house and Cloud architecture is far from easy. But it's not an unconquerable task, as Dotan Horovits has explained. After all, the problem of load balancing databases, the only major difference is accounting for potential latencies introduced by the addition of a Cloud component - is already well understood.

Other organizations outside of web hosting have periodic resource demands as well, of course. A business in bio-informatics may occasionally need to burst workloads such as DNA sequencing, while a sales company may occasionally require additional power to process user databases. Huge amounts of data, only processed on occasion, can be managed thanks to Cloud bursting.

But what if that data is highly-sensitive? Is the Cloud secure enough to protect it? The short answer, as you'll see, is yes.

Why You Need To Stop Worrying About Cloud Security

Although Cloud computing has gained far more widespread acceptance in recent years, security continues to be a barrier to Cloud adoption. Though public perception still leans towards considering the Cloud an inherently insecure medium, regardless of evidence that shows the contrary. These concerns represent one of the most significant obstacles to Cloud adoption. In many cases, it seems that even organizations who have adopted the Cloud are still a touch squeamish about it.

A 451 Research survey of IT executives, for example, found that nearly 70% consider security their main concern regarding the public Cloud.

These concerns are largely misplaced. While it's certainly true that an organization's information on the Cloud will be at risk if they fail to take the proper steps to protect it, the same is true for any hosting solution. Cloud applications and services are not inherently more or less secure than traditional application infrastructure. They are simply subject to a different gallery of risks.

The chaos was created by the discovery of the Heartbleed bug last April, which allowed hackers to acquire everything from user passwords to server encryption keys seems to counteract such a claim. Shouldn't the presence of a mega-bug like this have anyone concerned about security running for the hills?

No. Not really. Though we are not dismissing the seriousness of Heartbleed, bugs like it don't really come along every day. Plus, it didn't just impact the Cloud, either. Many shared hosts and VPNs were impacted by the vulnerability too. Avoiding the Cloud simply because one's concerned about Heartbleed (or similar bugs) is like avoiding traditional alternatives because of paranoia about employee theft. It simply doesn't represent a meaningful reason to avoid adopting the Cloud.

Cloud computing is no more, or less, insecure than any of its alternatives. It offers a host of amazing benefits. So long as a business practices proper risk management and selects the right vendor, there's nothing to fear.

With that in mind, it's worth noting that you can't afford to grow complacent. The Cloud is not inherently insecure, no. At the same time, however, there are risks.

Public vs. Private: The Difference in Security

Hybrid Clouds are becoming increasingly popular among medium and large companies because of an intuitive understanding that hybrid Clouds combine the best of both worlds: the security of a private Cloud and the convenience of the public Cloud. Although that way of thinking makes sense theoretically, real world scenarios rarely match the theory.

A public Cloud is a large network of physical servers. Generally, these consist of a virtualization layer, and an API, which gives clients access to on-demand scalable infrastructure without having to invest in hardware. The physical infrastructure is shared between multiple clients, none of which have privileged access to underlying architecture.

A private Cloud is exactly what it sounds like. It provides the same virtual resources but the underlying hardware is controlled by one organization, and only they can deploy resources on it. Private Clouds are often hosted in the company's own data center, but they can also be colocated at a third-party data center.

A hybrid Cloud combines both, often as part of a strategy of data segregation. Business critical and sensitive information is handled on the private component, while less sensitive data is handled by the public component.

The risk with Cloud hosting is not that the underlying physical hardware is shared - strict segmentation is a well understood problem - but that management, security and privacy best practices aren't in place to ensure that data stays safe. By creating a hybrid Cloud, companies may in fact be compromising the security of their data. By hosting sensitive information in a private Cloud, they may be creating a false sense of security.

It's important that businesses take measures to protect any critical data they host in the Cloud, because it's rare that someone will do it for them.

Conclusion

There was a time that the public Cloud was the only Cloud avaiable. Those days, however, are long behind us. Today, there are scores of different deployment models and service models.

As you've seen here, hybrid Clouds are among the most compelling, from a business standpoint, and your organization stands to gain a great deal by implementing them.