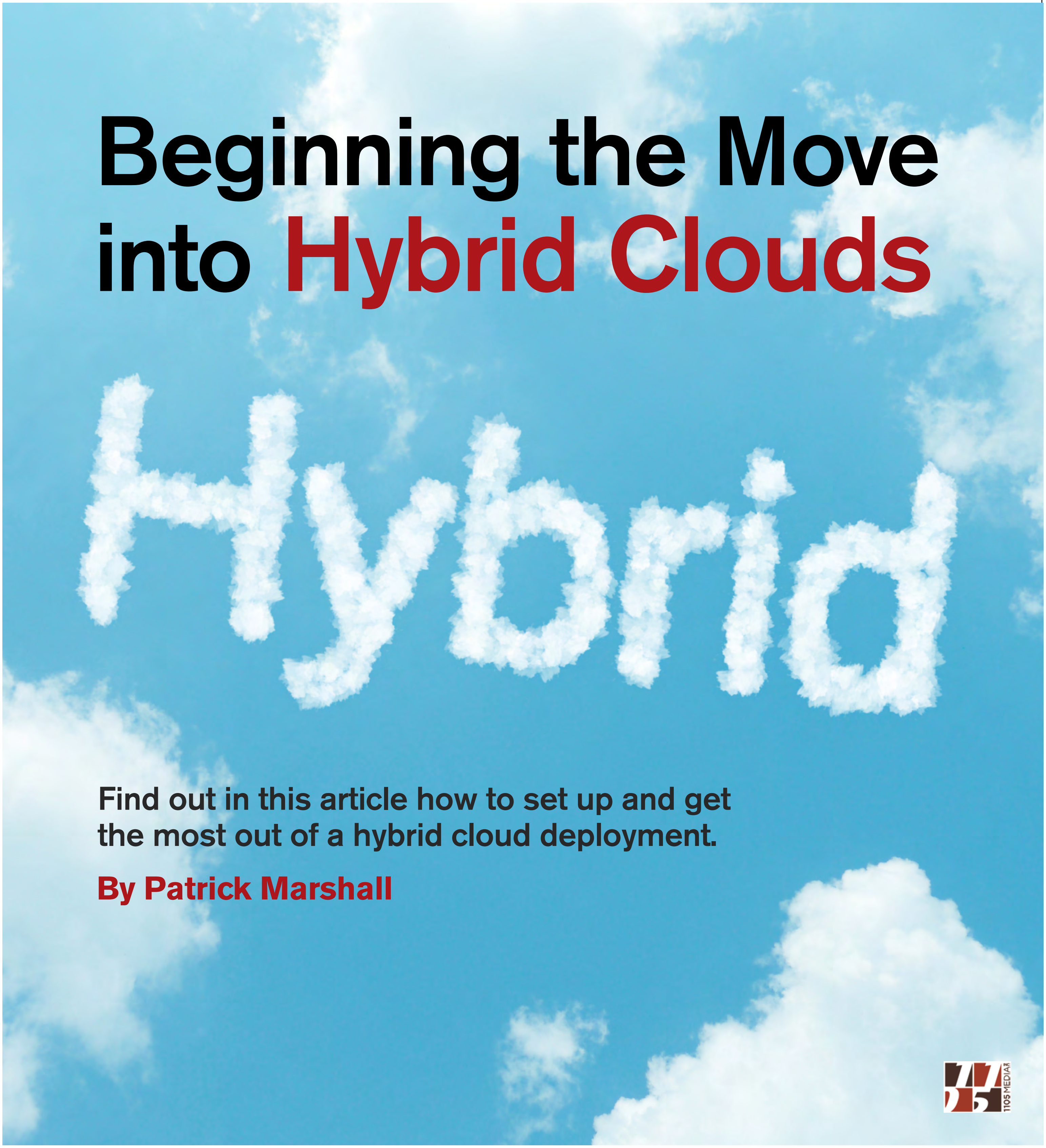
CONTENT BY

ADTMAG
APPLICATION DEVELOPMENT TRENDS

SPONSORED BY

rackspace®

Beginning the Move into Hybrid Clouds



Find out in this article how to set up and get the most out of a hybrid cloud deployment.

By Patrick Marshall

1105 MEDIA

Moving your organization into the cloud can mean many different things. It can be as simple as offering limited datasets in a public cloud or as complicated as offering applications that deliver some capabilities to users in the public cloud and other capabilities to users in the private cloud. And new products are emerging to help manage an organization's cloud applications and their security. As a result, even those organizations that have moved some operations to the cloud will want to consider when it's time to gain more flexibility and savings by moving more operations to the cloud.

Beyond just the decision to move into the cloud, organizations need to figure out what type of cloud will be used. For many professional and government organizations, the answer is a hybrid cloud that features the best aspects of both public and private clouds. Many cloud services and providers offer this as an option, with public data open and easy to access with private or confidential information only available for authorized users – all in the same overall network. Even as they are rapidly evolving, cloud services – and more specifically, hybrid cloud services – are quickly becoming a standard resource in enterprises and even small businesses. If your organization hasn't already implemented a cloud strategy for deploying data and applications, it is almost certainly exploring plans to do so.

Beyond just the decision to move into the cloud, organizations need to figure out what type of cloud will be used.

For most organizations, the move to the cloud will be gradual, primarily because not all legacy applications can be efficiently ported to cloud environments. Even if it takes time, however, moving more operations to the cloud is inevitable because the advantages are clear.

Among the most obvious benefits are:

Saving money – Cloud services are generally significantly less expensive than the cost of maintaining on-site servers and networks. By one estimate, an organization would have to deploy between 5,000 and 15,000 servers to get the per server marginal cost down to that of cloud vendors. And costs for infrastructure as a service (IaaS) have been dropping significantly.

Pay-as-you-go – Apart from overall savings, some organizations will prefer cloud service's pay-as-you-go model over having to make capital outlays for equipment and ongoing payments for products used to support the infrastructure, such as antivirus, encryption, data archiving and other services.

Scalability and elasticity – Unlike on-site servers and networks, cloud services offer organizations the potential for rapid expansion of resources to meet demands.

Flexibility in sitting staff – All that is required for remote staff to connect to the organization's resources is Internet access.

Streamlining infrastructure maintenance – Servers are serviced and maintained offsite by the cloud service provider, who also performs software updates and patches. Most maintenance and repair operations can be performed with no downtime for hosted clouds.

At the same time, some organizations have serious concerns about moving mission-critical or sensitive data and applications into public clouds, both because of the possibility of connectivity outages and data security vulnerabilities. As a result, many organizations are turning to private clouds, which are hosted on separate servers that may be on-site or off-site. Private clouds typically are accessed via private leased lines or over encrypted connections on public networks. Understandably, private clouds are more expensive to implement than public clouds, though they are generally more flexible and can be less expensive than traditional infrastructure.

Designing hybrid clouds effectively requires close consideration of the nature of an organization's existing IT assets.

Many organizations, in fact, will want to consider implementing hybrid clouds, which combine public and private clouds. Designing hybrid clouds effectively, however, requires close consideration of the nature of an organization's existing IT assets as well as, moving forward, the degree of integration required between public and private clouds and between both clouds and the organization's existing infrastructure.

Designing your hybrid cloud

For the organization's IT staff, implementing and managing a hybrid cloud solution has more in common with traffic management than it does with building a traditional network. For starters, you won't have to worry about the hardware, operating systems and adding storage. Instead, that challenge becomes more focused on what workloads to direct to which cloud services and, potentially, which to keep, at least for a time, in the data center.

Even if the organization is building an entirely new infrastructure from scratch, there are decisions to make about what applications and data should be sited in the public cloud and which should be hosted in a private cloud. And if the organization has critical legacy applications that are not well-suited for the cloud, provisions will have to be made for transitioning away from those applications or rewriting code to make them suitable for the cloud.

The fact is, cloud service vendors differ in what configurations they support most efficiently. For example, most have employed virtual machines to accommodate legacy applications, while others are beginning to turn to Linux containers. Depending on which type of technology is used, there may be performance implications for your specific workloads.

It's critical to consider the nature of your organization's existing workloads as well as the desired future architecture before selecting the best mix of cloud services and providers.

Accordingly, it's critical to consider the nature of your organization's existing workloads as well as the desired future architecture before selecting the best mix of cloud services and providers. While eventually moving most or all workloads to the cloud may make sense for many organizations, in short, that move may best take place in stages.

Many recently developed enterprise applications were written using modular, or "tiered," architectures that allow workloads to be dispersed and processed separately. A web interface, for example, could be most effectively sited in a public cloud, which offers the on-demand scalability of resources that users may require. The module that contains the business logic may, depending on security concerns, be hosted in a private cloud or it may remain in the data center. The data tier is yet another module.

Many older applications, however, weren't written with such portability or distributed processing in mind. What's more they may have specific hardware or operating system requirements, or require outdated drivers, that may be difficult or impossible to replicate in a cloud environment. Many financial-trading applications, for example, have been optimized to run on specific hardware and are performance intensive, which makes them unlikely to be candidates for the cloud.

Because of such considerations, only 30 percent to 40 percent of enterprise applications are currently running in the cloud. Most of these applications are web applications, e-mail, collaboration tools, and sales force automation tools.

In general, the best candidate applications for the cloud are:

- Applications that have unpredictable workloads, such as many web apps.
- Applications that require easy storage expansion, such as e-mail.
- Applications that will be accessed remotely and/or in collaborative environments.
- Standalone applications or applications that do not integrate with applications not also in the cloud.

Do you need to integrate your hybrid cloud?

Most organizations that have implemented both public clouds and private clouds use each resource for different purposes. A website or an e-mail application might be hosted in a public cloud for easy access, while applications and data that require a higher level of security may be restricted to a private cloud.

Most organizations that have implemented both public clouds and private clouds use each resource for different purposes.

Some vendors, however, use "hybrid cloud" to refer to architectures in which a private cloud is actually integrated with – rather than just coexisting with – a public cloud.

One type of integration supported by some major cloud service providers – including Microsoft and VMWare – is "cloud bursting." When a workload running on a private cloud "spikes" its demand for resources beyond what is available in the private cloud, cloud bursting pushes part of the workflow into the organization's public cloud to prevent processing delays.

Currently, however, this option has not been widely adopted because of concerns about security and availability in the public cloud. After all, if data is thought critical enough to incur the additional costs and inconvenience of hosting it in a private cloud or an on-premises data center, why would one want it spilling into a public cloud when demand is high? As those concerns eventually abate, however, we can expect more interest in cloud bursting.

"Hybrid cloud" is also used by some to refer to actual integration of workflows across public and private clouds, such that some operations and/or data are performed in a more secure private cloud or on-premise data center, while other workflows or the results of workflows are available on the public cloud.

Implementing this type of hybrid cloud requires either custom development of applications or adoption of a hybrid cloud integration application from a cloud services vendor.

Assess security needs

Despite popular concerns about cloud security, major cloud services providers offer security that is at least equal to, and in many cases, exceeds that available in many enterprise data centers.

Specific security levels and certifications of cloud providers varies, however, so you'll want to ensure that the vendor you select actually supports your requirements. For example, if your organization's data is subject to regulatory standards – such as the Health Insurance Portability and Accountability Act (HIPAA) or the PCI Data Security Standard (PCI DSS) – you'll want to make sure the vendor has received the appropriate certifications.

If your organization's data is subject to regulatory standards, you'll want to make sure the vendor has received the appropriate certifications.

For IaaS- and PaaS-level security, in addition to inquiring about any regulatory standards your organization requires, you'll want to ask more general questions of vendors you are considering, including:

- What security procedures are in place at the datacenter?
- How have vendor staff been vetted and what access do they have to customers' data?
- How are users authenticated?
- What level of encryption is employed?

At the same time, don't overlook user data, especially in public clouds, the security of which may not be directly addressed by the cloud provider. Are Social Security numbers or credit card numbers contained in e-mails or other documents that are residing in cloud storage?

Applications are coming to the market to provide additional layers of security for such vulnerabilities, though these applications often only work with specific cloud services. CloudLock, for example, scans workflows in Google Drive, for unencrypted data and encrypt it using AES 256-bit encryption. nCrypted, a recent startup, specializes in locating unencrypted files in cloud storage repositories – including DropBox, Microsoft OneDrive and Google Drive – and encrypting them in .zip containers.

Unified management

With the organization's applications and data spread across multiple public and private clouds, as well as certain mission-critical or legacy applications still running in on-premises data centers, IT managers are faced with the challenges of managing data silos.

The major vendors offer products for managing the entire spectrum of workloads and infrastructure. Even when the management tools are gathered together in one package, however, the different IT environments require different skills and knowledge on the part of IT managers. Eventually, as legacy applications are rewritten or abandoned, we can expect the task of integrating and managing workloads to be simplified and streamlined.

The major vendors offer products for managing the entire spectrum of workloads and infrastructure.

Selecting technologies and vendors

While cloud services providers offer scalability and relieve the organization of the burden of maintaining underlying IT resources, the intimate and ongoing nature of that relationship means selecting a vendor or vendors is even more critical than usual. The organization will be counting on the vendor for ongoing performance, not just for delivering a piece of equipment and replacing or repairing it if the equipment malfunctions. Accordingly, there are several factors to consider in selecting vendors.

Service level agreements

What level of service will the vendor promise to deliver and what penalties are imposed if the vendor fails to deliver? Also, consider the range of services covered by the agreement. It should include not just network availability, but also such things as migration services, and guarantees against host failure and datacenter interruptions.

Transparency

Guarantees of service levels are great, it's even better when the vendor provide tools that allow you to monitor performance. It's better to detect problems before your customers are actually complaining. Has the vendor been up front about previous performance problems? Does the vendor offer a dashboard that displays a running record of the status of its various services?

Persistence or backup

In the event of an outage, what happens to any data and transactions in your workflows? Not all cloud vendors support data persistence, so if there's an outage data may be lost.

Support

Does the vendor provide 24x7x365 support? And can support be reached via multiple channels, including not just telephone, but also e-mail and online chat? Just as important, does the vendor report historical response times?

Granular billing

One of the primary lures of moving to the cloud is the promise of resource availability on demand. If there's a spike in traffic that requires more resource bandwidth, it can be made immediately available. The customer will, of course, be charged more for those additional resources. It's important, therefore, to know how granular the billing for resources is. If the organization's workflows regularly experience large spikes for short durations, for example, it's better if billing is computed by the minute rather than by the hour.

One of the primary lures of moving to the cloud is the promise of resource availability on demand.

Cloud service brokers

The number of factors to consider in selecting cloud options and vendors has given rise to a new industry: cloud service brokers.

Cloud service brokers specialize in selecting the most efficient mix of cloud services for the client's applications and workflows. CSB's can also be used to select the most appropriate cloud service providers and to negotiate contracts. Some clients may also employ CSB's to work with cloud service providers to customize the client's services. **ADT**

Patrick Marshall has been writing on technology since 1984, when he began reviewing software for PC World. He was a writer and editor for InfoWorld, test center director and writer for Federal Computer Week, and an editor and writer for Government Computer News. Currently, in addition to writing for the Tech Writer's Bureau, he is a columnist for The Seattle Times and Government Computer News.

rackspace®

ADTMAG
APPLICATION DEVELOPMENT TRENDS