E-Guide

Preparing for the cloud: Understanding the infrastructure impacts

Eight essential tips for a successful cloud migration

Contents

The move to the cloud is happening – and it's happening now. *But before you jump start your cloud migration project, be sure you understand how to adequately prepare your infrastructure for the transition.*

Hear from Bob Plankers, renowned industry guru and virtualization and cloud architect expert for a major Midwestern university, as he discuss the impact of a cloud migration on all aspects of your data center infrastructure and offers advice for readying your environment and IT team for the task. Learn more about how the cloud will affect security, networking, service management and more.

Prepping data center infrastructure for a cloud migration

By: Bob Plankers, Contributor

For good reason, clouds are a popular topic in IT. They offer numerous benefits, such as pay-as-you-go billing models, seemingly infinite resources and the ability to place workloads around the globe to boost capacity. Still, as you consider a cloud migration, you will likely have to make changes to your data center infrastructure and your organization to prepare for the move. You need to think carefully about the impact on all aspects of data center infrastructure and on IT teams.

Before taking on a cloud migration project, you need to take a step back and evaluate the wisdom of the move. It's critical to make the business case for why a migration to the cloud makes sense -- and the fact that the cloud is en vogue is not enough. So, assuming that you already have a private cloud, why would you want to add public cloud capabilities? Perhaps you want to broaden your disaster recovery (DR) options by running work-loads from a different location. Or maybe you want to add workloads, but are constrained by capacity limitations at your on-site data center. Or perhaps your reasoning for the move to a hybrid cloud model is financial. The pay-as-you-go aspect of public clouds can shift capital expenditures to operational ones and free you from unpleasant leases and forklift upgrades.

It is critical for all levels of your IT organization to know what the goals of this move are, so your organization can make solid decisions. It is also important to include all IT teams --including application, system, network and storage administrators -- in these plans. Their knowledge will be key to solid preparation for implementing a hybrid cloud.

Assess existing infrastructure and set goals

As you consider moving to a cloud model, the first step is to assess where your infrastructure is now. Do you already have a private cloud and want to bridge the gap between it and a public cloud? Perhaps you are on the path to virtualization, but you haven't progressed to a cloud. And while the term "cloud" has many meanings, it doesn't just mean greater degrees of virtualization; it also involves a push to-ward centralization and automation. In particular, this move toward centralization makes the cloud as much about people and process as it is about technology.

Gather technical requirements

Once your organization has made its business goals for a hybrid cloud clear, develop technical requirements with your staff. Do the applications you want to move need to scale? Perhaps you need load-balancing capabilities, not just for service availability, but also so you can distribute workloads and automatically redistribute resources to accommodate the peaks and valleys of cloud demand. Do applications require secure communication to a back-end database that will continue to live in your data center? Do you need services to run from particular parts of the globe for support or DR reasons?

Once you have identified your technical needs, consider public cloud provider offerings objectively. For example, perhaps some providers natively support your virtual private network (VPN) concentrator or a network tunneling technology your engineers are already comfortable with, thereby making secure networking easier. At this stage, it's also important to gather performance data. Knowing how much network and storage I/O your applications generate enables you to size network connections and virtual machines that reside in the public cloud and to select from differing service tiers offered by public cloud vendors.

Contents

Select hybrid cloud tools

Several self-service cloud portals can connect your on-premises infrastructure to public cloud infrastructure. Most work with a subset of public cloud providers, so knowing your technical requirements and organizational goals is important to match a tool set with providers' capabilities, as well as with your own infrastructure.

There are several aspects to consider. First, how well do these tools manage existing heterogeneous infrastructure? Do they require completely new infrastructure, or do they plug into what you have already built? Where do these tools run? Do they get installed in a legacy data center or run in the cloud? Some tools, like VMware's vCloud Connector, plug in directly to existing infrastructure, but that has implications for DR. You would need to plan for your primary site becoming unavailable and ensure that you fully protect your management infrastructure.

Can these tools access more than one public cloud? What about accessing a provider's different locations? Are these tools capable of doing chargeback and real-time reporting of costs and performance metrics across all sites? Does it help monitor and meet service-level agreements (SLAs)? Does it create a service catalog from which users can choose? How does it help manage templates and configurations? How does it handle authentication? Is there an audit trail? At this stage, you need to ask all these questions.

Implement security safeguards

Once you have selected a cloud provider and a tool set, you need to address the multifaceted issue of security. To begin, determine how the tools and the cloud provider will interact with your data center and grant them access through network- and host-based firewalls if necessary. This might be tricky with offsite, hosted tools, as private clouds' management interfaces are often on completely internal, private networks.

Contents

You need to implement authentication and access control for the new hybrid cloud tool as well. Perhaps the tool has its own authentication systems, so you need to recreate your users and your access control policies in its user database. For example, when an employee leaves the company, you need to revoke his cloud access at the same time as you revoke his onsite access. You also might need to grant access to your internal help desk for password resets. If the tool uses existing authentication systems, you may need to make those systems more robust, especially if one of your goals is DR. Without a robust authentication system, consider what would happen if your primary site went down and users were still trying to access these systems.

If you have sensitive data that is stored in a public cloud, investigate encryption technologies for that data. Securing network connectivity among sites is also important, and it may require changes or additional purchases. You also need to consider how to store important data, like cloud application programming interface (API) keys and encryption keys. Access to them is important in an emergency, but they also grant powerful access rights to whoever knows them. This is a good time to take steps to protect these access rights but also to make them available when needed, protecting them as you would an administrator password, logging access and changing access information periodically.

How a cloud migration affects existing data center infrastructure

By: Bob Plankers, Contributor

Preparing for a move to the cloud includes vital steps, such as analyzing technical requirements and implementing security protocols. However, even with the best planning, you can still encounter obstacles. Once you've prepped for a cloud migration project, you need to explore the impact on data center configuration management, networks and storage.

The hybrid cloud puzzle involves several complex pieces, but they are not insurmountable problems. Rather, these problems benefit from new, better solutions that arise every month. If you and your organization take the nontechnical messages of cloud computing -- namely centralization and automation -- to heart, you will find yourself becoming more flexible and more able to take advantage of solutions as they emerge and, most likely, save money in the process.

Building service catalogs, templates to automate configuration management

A primary benefit of public clouds is the ability to dynamically scale systems and resources to match workloads. This saves money because you don't need to size your system for a yearly peak workload, just for today's workload. But to rapidly scale systems, staff will need to build and maintain good virtual machine templates to use with these tools. They will also likely need to explore some automated configuration management.

Implementing configuration management in the form of tools like Chef and Puppet isn't simple. It opens the door to extreme levels of automation and change control, which saves staff time, prevents outages and assists with security by keeping all OS configurations in sync. As with authentication, you need to consider your goals so that you can properly design these systems to be robust during site outages. Staff also may need training, and you may need to build additional infrastructure -- such as separate configuration repositories and servers, firewall rules, etc. -- to support these new tools.

Retrofitting networking to your cloud migration project

Networking is central to what makes the cloud possible. A successful hybrid cloud implementation is dependent on good networking practices, excellent and comprehensive monitoring and rapid troubleshooting. Adding reliable and available connectivity to multiple sites, load balancing, dynamic scaling and security requires staff time and considerable skill.

Moving workloads out of a data center to a public cloud can stress an organization's external network connections. You may choose to make a single network connection redundant to help guarantee that a problem with one provider doesn't take all your company's products offline. These tasks aren't simple and need to be planned carefully with a network engineering team. It also is important that the application and system administrators work together with the network engineers for sizing and troubleshooting.

More traffic on network connections may mean more traffic through firewalls, intrusion-detection devices and intrusion-prevention devices that were never sized for that amount of traffic. Scaling them up and adding redundancy is a must to prevent single points of failure from taking hybrid cloud applications offline. Likewise, intrusion detection and prevention systems need to be configured so that communications from white-listed remote hosts aren't interrupted.

Implementing service management

A robust monitoring technology indicates the state and performance of every system in your data center. But as you move to the cloud, are these systems extensible, and will they work for the cloud? Perhaps. The technologies for on-premises virtual environments may work for public cloud environments as well. Other considerations might emerge, such as disaster recovery. If the primary site is down, how can you manage and monitor systems? Perhaps you choose to replicate your management services as well, or create a secondary monitoring system at the alternate site.

Real-time performance metrics are also important, and access to them depends on the cloud provider you choose. Performance metrics ensure that technical staff can troubleshoot a problem, help inform the automatic scaling features of hybrid clouds and are often used for chargeback, billing and reporting. Using a monitoring tool or service that can automatically trigger scaling up or down is a key part of the move toward a hybrid cloud, but it is often overlooked until later in the process. A chargeback process that is aware of up-to-the-minute charges from cloud providers is also a must. Choose tools with good programming interfaces and have IT staff that can configure and manage those tools and integrate them into your company's business processes.

Good service management techniques don't stop once a service is partially or completely in the cloud. Adapting internal configuration management databases and other tools to the cloud is important. Some of this work is

Contents

strictly process-oriented, rather than technological, though there are likely good integration possibilities. In some cases, tracking certain assets in a traditional configuration management database is impossible, given the dynamic nature of the cloud.

Moving from a private cloud to a hybrid cloud requires planning and implementation work throughout a data center. Basic assumptions that have built up over decades need to be rethought, tools need to be re-evaluated and all parts of an infrastructure likely need to be changed in a careful way. Having clear goals in mind informs much of this work, which is often about communication just as it is about technical implementation.

Don't ignore storage and backup

In the race to the cloud, IT management often overlooks storage and backup needs. But with good communication of business requirements and solid work on technical requirements, these problems can be mitigated.

First, not all cloud storage is the same. Consider that most on-premises storage is sized in two ways: performance and price per gigabyte. But in the cloud you often see only one fee: price per gigabyte. When you select a public cloud provider, inquire about performance options. Many inexpensive-seeming providers use slower SATA disk arrays to drive down costs. But if your applications require additional performance, you may find yourself without options. Many providers have begun to add service tiers that guarantee certain levels of storage performance, and selecting a provider that does so allows you to save money where performance isn't necessary but spend money selectively to make performance-sensitive applications work well. Choosing a provider that allows you to move dynamically between these tiers may be of interest, especially as unanticipated performance requirements crop up.

Second, backup needs are often overlooked with hybrid clouds. First, do you plan to use your legacy system to back up cloud-based virtual machines? How will that affect network traffic? Just as important, how will that affect your bill, as most providers charge fees per gigabyte of traffic moved off the network? Perhaps the cloud provider offers backup solutions internally that are cost-effective but will require different processes and procedures for restoring data than your already-established systems. You may also want to consider enabling encryption for backups, especially for third-party shared services. Encryption of backups is not a simple thing and will require procedural changes to securely store encryption keys, as well as testing of restores and encryption key changes.

Contents

TechTarget

Contents

Free resources for technology professionals

TechTarget publishes targeted technology media that address your need for information and resources for researching products, developing strategy and making cost-effective purchase decisions. Our network of technology-specific Web sites gives you access to industry experts, independent content and analysis and the Web's largest library of vendor-provided white papers, webcasts, podcasts, videos, virtual trade shows, research reports and more —drawing on the rich R&D resources of technology providers to address market trends, challenges and solutions. Our live events and virtual seminars give you access to vendor neutral, expert commentary and advice on the issues and challenges you face daily. Our social community IT Knowledge Exchange allows you to share real world information in real time with peers and experts.

What makes TechTarget unique?

TechTarget is squarely focused on the enterprise IT space. Our team of editors and network of industry experts provide the richest, most relevant content to IT professionals and management. We leverage the immediacy of the Web, the networking and face-to-face opportunities of events and virtual events, and the ability to interact with peers—all to create compelling and actionable information for enterprise IT professionals across all industries and markets.

Related TechTarget Websites

- SearchCloudComputing
- SearchDataCenter