Project Success Plan: Cloud Migration

A guide for transitioning to a cloud-based infrastructure.

In this guide

In this e-guide:

Due to rapid advancement in cloud technology and the well-publicized benefits of utilizing cloud services, IT pros have become the voice of reason, objectively weighing the pros – flexibility, scalability, cost-savings – against the cons – security risks, management challenges. Determining when/where cloud is appropriate, and where it can have the most benefit in your organization, by critically assessing your infrastructure is the only means of devising a sound migration strategy.

So, what cloud tools are available? What obstacles will you run into? Where do you begin? This comprehensive guide walks readers through the entire process of a migration to cloud infrastructure, from the initial phases of a cloud planning through to the monitoring and management of a fully-transitioned cloud environment.

In this guide

What is Cloud Computing

http://searchcloudcomputing.techtarget.com/definition/cloud-computing

Cloud computing is a general term for the delivery of hosted services over the Internet.

Cloud computing enables companies to consume compute resources as a utility -- just like electricity -- rather than having to build and maintain computing infrastructures in-house.

Cloud computing promises several attractive benefits for businesses and end users. Three of the main benefits of cloud computing include:

- Self-service provisioning: End users can spin up computing resources for almost any type of workload on-demand.
- Elasticity: Companies can scale up as computing needs increase and then scale down again as demands decrease.
- Pay per use: Computing resources are measured at a granular level, allowing users to pay only for the resources and workloads they use.

Cloud computing services can be private, public or hybrid.

In this guide

Private cloud services are delivered from a business' data center to internal users. This model offers versatility and convenience, while preserving management, control and security. Internal customers may or may not be billed for services through IT chargeback.

In the public cloud model, a third-party provider delivers the cloud service over the Internet. Public cloud services are sold on-demand, typically by the minute or the hour. Customers only pay for the CPU cycles, storage or bandwidth they consume. Leading public cloud providers include Amazon Web Services (AWS), Microsoft Azure, IBM/SoftLayer and Google Compute Engine.

Hybrid cloud is a combination of public cloud services and on-premises private cloud – with orchestration and automation between the two. Companies can run mission-critical workloads or sensitive applications on the private cloud while using the public cloud for bursty workloads that must scale on-demand. The goal of hybrid cloud is to create a unified, automated, scalable environment which takes advantage of all that a public cloud infrastructure can provide, while still maintaining control over mission-critical data.

Although cloud computing has changed over time, it has always been divided into three broad service categories: infrastructure as a service (IaaS), platform as a service (PaaS) and software as service (SaaS).

In this guide

IaaS providers such as AWS supply a virtual server instance and storage, as well as application program interfaces (APIs) that let users migrate workloads to a virtual machine (VM). Users have an allocated storage capacity and start, stop, access and configure the VM and storage as desired. IaaS providers offer small, medium, large, extra-large, and memory- or compute-optimized instances, in addition to customized instances, for various workload needs.

In the PaaS model, providers host development tools on their infrastructures. Users access those tools over the Internet using APIs, Web portals or gateway software. PaaS is used for general software development and many PaaS providers will host the software after it's developed. Common PaaS providers include Salesforce.com's Force.com, Amazon Elastic Beanstalk and Google App Engine.

SaaS is a distribution model that delivers software applications over the Internet; these are often called Web services. Microsoft Office 365 is a SaaS offering for productivity software and email services. Users can access SaaS applications and services from any location using a computer or mobile device that has Internet access. .

Next article

In this guide

Key terms to understand

Infrastructure as a Service (IaaS)
http://searchcloudcomputing.techtarget.com/definition/Infrastructure-as-a-Service-IaaS
Infrastructure as a Service (IaaS) is a form of cloud computing that provides virtualized computing resources over the Internet. IaaS is one of three main categories of cloud computing services, alongside Software as a Service (SaaS) and Platform as a Service (PaaS).

In an IaaS model, a third-party provider hosts hardware, software, servers, storage and other infrastructure components on behalf of its users. IaaS providers also host users' applications and handle tasks including system maintenance, backup and resiliency planning.

IaaS platforms offer highly scalable resources that can be adjusted on-demand. This makes IaaS well-suited for workloads that are temporary, experimental or change unexpectedly.

Other characteristics of IaaS environments include the automation of administrative tasks, dynamic scaling, desktop virtualization and policy-based services.

IaaS customers pay on a per-use basis, typically by the hour, week or month. Some providers also charge customers based on the amount of virtual machine space they use. This pay-as-you-go model eliminates the capital

In this guide

expense of deploying in-house hardware and software. However, users should monitor their IaaS environments closely to avoid being charged for unauthorized services.

Because IaaS providers own the infrastructure, systems management and monitoring may become more difficult for users. Also, if an IaaS provider experiences downtime, users' workloads may be affected.

For example, if a business is developing a new software product, it might be more cost-effective to host and test the application through an IaaS provider. Once the new software is tested and refined, it can be removed from the IaaS environment for a more traditional in-house deployment or to save money or free the resources for other projects.

Leading IaaS providers include Amazon Web Services (AWS), Windows Azure, Google Compute Engine, Rackspace Open Cloud, and IBM SmartCloud Enterprise.

Platform as a Service (PaaS)
http://searchcloudcomputing.techtarget.com/definition/Platform-as-a-Service-PaaS
Platform as a service (PaaS) is a cloud computing model that delivers applications over the Internet. In a PaaS model, a cloud provider delivers hardware and software tools -- usually those needed for application development -- to its users as a service. A PaaS provider hosts the hardware

In this guide

and software on its own infrastructure. As a result, PaaS frees users from having to install in-house hardware and software to develop or run a new application.

PaaS does not typically replace a business' entire infrastructure. Instead, a business relies on PaaS providers for key services, such as Java development or application hosting. For example, deploying a typical business tool locally might require an IT team to buy and install hardware, operating systems, middleware (such as databases, Web servers and so on) the actual application, define user access or security, and then add the application to existing systems management or application performance monitoring (APM) tools. IT teams must then maintain all of these resources over time. A PaaS provider, however, supports all the underlying computing and software; users only need to log in and start using the platform – usually through a Web browser interface.

Most PaaS platforms are geared toward software development, and they offer developers several advantages. For example, PaaS allows developers to frequently change or upgrade operating system features. It also helps development teams collaborate on projects.

Users typically access PaaS through a Web browser. PaaS providers then charge for that access on a per-use basis. Some PaaS providers charge a flat monthly fee to access the platform and the apps hosted within it. It is

In this guide

important to discuss pricing, service uptime and support with a PaaS provider before engaging their services.

Since users rely on a provider's infrastructure and software, vendor lock-in can be an issue in PaaS environments. Other risks associated with PaaS are provider downtime or a provider changing its development roadmap. If a provider stops supporting a certain programming language, users may be forced to change their programming language, or the provider itself. Both are difficult and disruptive steps.

Common PaaS vendors include Salesforce.com's Force.com, which provides an enterprise customer relationship management (CRM) platform. PaaS platforms for software development and management include Appear IQ, Mendix, Amazon Web Services (AWS) Elastic Beanstalk, Google App Engine and Heroku.

PaaS is one of three main categories of cloud computing services. The other two are software as a service (SaaS) and infrastructure as a service (IaaS).

Software as a Service (SaaS)

http://searchcloudcomputing.techtarget.com/definition/Software-as-a-Service

Software as a Service (SaaS) is a software distribution model in which applications are hosted by a vendor or service provider and made available to customers over a network, typically the Internet.

In this guide

SaaS is becoming an increasingly prevalent delivery model as underlying technologies that support Web services and service-oriented architecture (SOA) mature and new developmental approaches, such as Ajax, become popular. Meanwhile, broadband service has become increasingly available to support user access from more areas around the world.

SaaS is closely related to the ASP (application service provider) and on demand computing software delivery models. IDC identifies two slightly different delivery models for SaaS. The hosted application management (hosted AM) model is similar to ASP: a provider hosts commercially available software for customers and delivers it over the Web. In the software on demand model, the provider gives customers network-based access to a single copy of an application created specifically for SaaS distribution.

Benefits of the SaaS model include:

- easier administration
- automatic updates and patch management
- compatibility: All users will have the same version of software.
- easier collaboration, for the same reason
- global accessibility

In this guide

The traditional model of software distribution, in which software is purchased for and installed on personal computers, is sometimes referred to as software as a product.

Private cloud (internal cloud or corporate cloud)

http://searchcloudcomputing.techtarget.com/definition/private-cloud

Private cloud is a type of cloud computing that delivers similar advantages to public cloud, including scalability and self-service, but through a proprietary architecture. Unlike public clouds, which deliver services to multiple organizations, a private cloud is dedicated to a single organization.

As a result, private cloud is best for businesses with dynamic or unpredictable computing needs that require direct control over their environments.

Public and private cloud deployment models differ. Public clouds, such as those from Amazon Web Services or Google Compute Engine, share a computing infrastructure across different users, business units or businesses. However, these shared computing environments aren't suitable for all businesses, such as those with mission-critical workloads, security concerns, uptime requirements or management demands. Instead, these businesses can provision a portion of their existing data center as an on-premises -- or private -- cloud.

In this guide

A private cloud provides the same basic benefits of public cloud. These include self-service and scalability; multi-tenancy; the ability to provision machines; changing computing resources on-demand; and creating multiple machines for complex computing jobs, such as big data. Chargeback tools track computing usage, and business units pay only for the resources they use.

Public cloud

http://searchcloudcomputing.techtarget.com/definition/public-cloud

A public cloud is one based on the standard cloud computing model, in which a service provider makes resources, such as applications and storage, available to the general public over the Internet. Public cloud services may be free or offered on a pay-per-usage model.

The main benefits of using a public cloud service are:

- Easy and inexpensive set-up because hardware, application and bandwidth costs are covered by the provider.
- Scalability to meet needs.
- No wasted resources because you pay for what you use.

The term "public cloud" arose to differentiate between the standard model and the private cloud, which is a proprietary network or data center that

In this guide

uses cloud computing technologies, such as virtualization. A private cloud is managed by the organization it serves. A third model, the hybrid cloud, is maintained by both internal and external providers.

Examples of public clouds include Amazon Elastic Compute Cloud (EC2), IBM's Blue Cloud, Sun Cloud, Google AppEngine and Windows Azure Services Platform.

Hybrid cloud

http://searchcloudcomputing.techtarget.com/definition/hybrid-cloud

Hybrid cloud is a cloud computing environment which uses a mix of on-premises, private cloud and public cloud services with orchestration between the two platforms. By allowing workloads to move between private and public clouds as computing needs and costs change, hybrid cloud gives businesses greater flexibility and more data deployment options.

For example, an enterprise can deploy an on-premises private cloud to host sensitive or critical workloads, but use a third-party public cloud provider, such as Google Compute Engine, to host less-critical resources, such as test and development workloads. To hold customer-facing archival and backup data, a hybrid cloud could also use Amazon Simple Storage Service (Amazon S3). A software layer, such as Eucalyptus, can facilitate private cloud connections to public clouds, such as Amazon Web Services (AWS).

In this guide

Hybrid cloud is particularly valuable for dynamic or highly changeable workloads. For example, a transactional order entry system that experiences significant demand spikes around the holiday season is a good hybrid cloud candidate. The application could run in private cloud, but use cloud bursting to access additional computing resources from a public cloud when computing demands spike. To connect private and public cloud resources, this model requires a hybrid cloud environment.

Another hybrid cloud use case is big data processing. A company, for example, could use hybrid cloud storage to retain its accumulated business, sales, test and other data, and then run analytical queries in the public cloud, which can scale to support demanding distributed computing tasks.

Public cloud's flexibility and scalability eliminates the need for a company to make massive capital expenditures to accommodate short-term spikes in demand. The public cloud provider supplies compute resources, and the company only pays for the resources it consumes.

Despite its benefits, hybrid cloud can present technical, business and management challenges. Private cloud workloads must access and interact with public cloud providers, so hybrid cloud requires API compatibility and solid network connectivity.

In this guide

For the public cloud piece of hybrid cloud, there are potential connectivity issues, SLA breaches and other possible public cloud service disruptions. To mitigate these risks, organizations can architect hybrid workloads that interoperate with multiple public cloud providers. However, this can complicate workload design and testing. In some cases, workloads slated for hybrid cloud must be redesigned to address the specific providers' APIs.

Management tools such as Egenera PAN Cloud Director, RightScale Cloud Management and Scalr Enterprise Cloud Management Platform help businesses handle workflow creation, service catalogs, billing and other tasks related to hybrid cloud.

Service-level agreement (SLA)

http://searchitchannel.techtarget.com/definition/service-level-agreement

A service-level agreement (SLA) is a contract between a service provider and its internal or external customers that documents what services the provider will furnish.

SLAs originated with network service providers, but are now widely used by telecommunication service providers and cloud computing service providers. Corporate IT organizations, particularly those that have embraced IT service management (ITSM), enter SLAs with their in-house customers (users in other departments within the enterprise). An IT department creates an SLA

In this guide

so that its services can be measured, justified and perhaps compared with those of outsourcing vendors.

SLAs measure the service provider's performance and quality in a number of ways. Some metrics that SLAs may specify include:

- Availability and uptime -- the percentage of the time services will be available
- The number of concurrent users that can be served
- Specific performance benchmarks to which actual performance will be periodically compared
- Application response time
- The schedule for notification in advance of network changes that may affect users
- Help desk response time for various classes of problems
- Usage statistics that will be provided.

In addition to establishing performance metrics, an SLA may include a plan for addressing downtime and documentation for how the service provider will compensate customers in the event of a contract breach. SLAs, once established, should be periodically reviewed and updated to reflect changes

In this guide

in technology and the impact of any new regulatory directives (changes to the PCI DSS standard, for instance).

In this guide

Why Consider a Cloud Migration Project?

http://searchcloudcomputing.techtarget.com/feature/To-cloud-or-not-to-cloud-Whats-your-cloud-migration-strategy

Over the past decade, cloud services have rapidly become one of the most defining technologies in IT. The hype surrounding cloud services may make it seem like all of an organization's resources should be migrated to the cloud immediately. There is no denying that, in certain cases, cloud services can be tremendously beneficial. In others, however, a cloud migration probably doesn't make sense.

Organizations need to take a hard look at their existing investments in infrastructure -- from hardware to application portfolios to network architecture and beyond -- to determine if a move will be beneficial. Some of the migration questions are technical, such as whether a given application can perform adequately in the cloud; some questions will involve nontechnical, budgetary issues, such as whether a cloud migration is cost-effective given current investments in infrastructure.

Here we explore factors that should guide a cloud migration strategy and help determine whether to move on-premises workloads to the cloud.

In this guide

One of the first considerations is an organization's existing data center investment. Despite technologies such as server virtualization, there are real costs associated with deploying on-premises servers. There are not only licensing costs involved, but also costs associated with hardware resource consumption and support infrastructure. As such, there is almost always a significant investment associated with an on-premises server. Outsourcing a server's data and/or functionality to the cloud may mean abandoning your on-premises investment unless an on-premises server can be repurposed.

Although this rip-and-replace approach to cloud migrations may not make financial sense for organizations that have a large investment in an on-premises data center, an organization can still benefit from migrating certain on-premises resources to the cloud.

No matter how good it is, any server hardware eventually becomes obsolete. Enterprise-class organizations have traditionally coped with this expected obsolescence by adopting a hardware lifecycle policy. An organization, for example, might choose to retire servers after five years. That being said, an organization could integrate a cloud services roadmap into its hardware lifecycle policy. Doing so allows IT teams to migrate on-premises resources to the cloud instead of moving them to newer hardware.

In this guide

The prospect of using cloud services is often particularly attractive for smaller organizations and startups. In the case of a smaller organization, the use of cloud services provides access to enterprise-class hardware and fault-tolerant features that would otherwise be unaffordable. Similarly, startups can benefit from cloud services because they can get their operations running quickly without having to invest in on-premises data center resources.

Application requirements for a cloud migration

In the case of application servers, administrators must consider whether the application can function in the cloud. Likewise, the application's performance must be considered.

Compatibility usually isn't a big problem for newer applications that run on top of modern operating systems. It is also easy to assume that performance won't be an issue for such applications because most cloud providers will allow hardware resources to be allocated to hosted servers on an as-needed basis. However, two major considerations must be taken into account for such applications.

The first is performance. Even though you can provision the hosted application server with nearly unlimited compute and memory resources, Internet bandwidth may impede application performance. It does little good

In this guide

to have a high-performance hosted application server if Internet bandwidth limitations stand in the way of a good user experience.

The second consideration is application portability. Although it is often easy to migrate a virtualized application server to the cloud, the application might have external dependencies that rule out (or greatly complicate) a cloud migration. For example, the application might have an Active Directory dependency or require access to an on-premises SQL server database.

For older applications that run on legacy operating systems, a move to the cloud may not be an option. Lab testing is the only way to know how an application will behave in a cloud environment. Testing helps determine the steps that are involved in moving the app there.

Another consideration for moving application servers to the cloud is hardware scalability. Some IT analysts have suggested that cloud services are ideal for hosting hardware-intensive workloads because cloud services generally offer nearly unlimited scalability. While a cloud service provider can usually scale its offerings to meet even the most demanding workloads, this scalability comes at a price.

Infrastructure as a Service providers such as Microsoft and Amazon Web Services charge customers a resource consumption-based monthly fee. As such, a cloud-based high-performance computing environment can become cost-prohibitive. Recently a client told me, for example, that it costs more

than $10,000 per month to operate a single high-performance application in the cloud. The bulk of the cost is due to CPU and disk I/O consumption.

Virtualization will ease a cloud migration

Regardless of organizational size, one of the considerations is whether the workloads targeted for cloud migration have been virtualized. In some cases, it's much easier to move workloads to the cloud if on-premises servers have already been virtualized. In fact, some providers will allow an organization to port virtual machines directly to the cloud. If on-premises servers have not been virtualized, a migration to the cloud is likely still possible, but the process may involve more work.

Cloud infrastructure considerations

Another factor to consider is the on-premises network. If an organization plans to keep resources on-premises (even temporarily), the cloud network must function as an extension of the on-premises Active Directory forest. This means that the organization will typically have to deploy cloud-based domain controllers, DNS servers and possibly DHCP servers. More importantly, the organization will have to figure out how to establish a secure communications path between the cloud-based virtual network and the on-premises network.

In this guide

This requirement usually isn't a deal-breaker for organizations with an existing on-premises network, but it does mean that a significant amount of planning may be required before beginning the migration process.

As an organization contemplates the risks and benefits of cloud migration, it is important to keep in mind that cloud migrations are not an all-or-nothing proposition. Organizations do not have to go "all in" with cloud migrations. In most cases, it will make sense to move certain services to the cloud while continuing to operate others on-premises.

Next article

In this guide

Why not migrate to the cloud?

Understanding public cloud risks and costs

http://searchcloudcomputing.techtarget.com/feature/Understanding-public-cloud-risks-and-costs

Public cloud services offer enterprises several advantages. They allow for flexible and affordable virtual machine deployments and can boost an organization's data backup and workload-scaling capabilities. However, public cloud isn't without its drawbacks.

After understanding the benefits of public cloud, as laid out in this series' first article, it's important to look at the critical disadvantages before entering the project planning phase. The next article in this series focuses on purchasing criteria and preparing a vendor request for proposal (RFP). Finally, the series will compare market-leading services against established criteria and against each other to help you select the best public cloud service for your environment.

Multi-tenant environment

One of public cloud's biggest disadvantages is its multi-tenant environment. The host server running your virtual machine (VM) likely is hosting other companies' VMs. Because of this, public cloud providers don't give you

In this guide

access to the hypervisor, so you can't install host-level utilities, such as antivirus software or backup agents. This also means you can't join a hypervisor to an existing domain or cluster. There are also security implications, as well as potential downtime from cloud or WAN failure.

In addition, public cloud providers own the hardware and control the underlying software, so they can make low-level changes at will. Consider how much work you put into planning a server OS or other type of upgrade. Normally, an organization will perform extensive testing prior to upgrading the OS to make sure there are no adverse effects. Conversely, a public cloud provider can make low-level changes to the infrastructure without notifying customers in advance. These types of changes can impact customer workloads.

Unpredictable costs

Another disadvantage of running VMs in the cloud is that costs can be wildly unpredictable. Public cloud providers are not known for using simple billing models.

Typically, you are billed based on the resources you consume. This includes storage resources, but also CPUs, memory and storage I/O. Resource consumption may be billed differently at different times of the day, and not all activity is treated equally. There are cloud providers that differentiate

between various types of CPU functions, billing those functions at different rates.

Because public cloud providers use complicated billing formulas, it can be difficult to estimate the cost of running cloud workloads. They can vary each month based on how heavily the workloads are used. Fortunately, some cloud providers have portals that customers can use to monitor costs and establish safety stops if costs are approaching designated thresholds.

Backups become complicated

Another disadvantage is how public clouds can complicate your backup processes. If you have mission-critical VMs running in the cloud, you need a way to back them up.

While most cloud service providers perform their own backups, they don't necessarily offer restoration services for customers. As such, you may need to back up your cloud-based VMs to your local data center or to a backup server running on a different public cloud.

This can be complex because most of the off-the-shelf backup products support data backup to the cloud, but not from the cloud. A cloud data backup increases the consumption of storage I/O, network I/O and WAN bandwidth, which may also increase costs.

In this guide

There are a number of advantages and disadvantages to running VMs in the public cloud. Whether an organization should take advantage of the public cloud depends largely on the organization's individual needs. After reading about the benefits and disadvantages of public cloud, check out other articles in this series on the buying process for public cloud virtual server services, public cloud purchasing criteria and cloud market comparisons.

Four things your public cloud provider will never tell you

http://searchcloudcomputing.techtarget.com/tip/Four-things-your-public-cloud-provider-will-never-tell-you

While we continue to move quickly into the public cloud, there is a lot that goes on behind the scenes of many service providers you might find disturbing. Most companies that leverage public clouds are unaware, and perhaps want to be unaware, of some practices behind closed doors. Or, to put it better: things your public cloud provider will never, ever tell you. Let's cover the top four.

1. Their disaster recovery plans won't work as advertised. While most public cloud providers spend many PowerPoint slides selling you on their public cloud's resiliency around outages, most have less-than-sophisticated approaches and rarely test these resiliency services.

In this guide

The problem is that they have spent so much time and money building public cloud services -- such as storage, compute, development, and the like -- many of their disaster recovery services have not received the attention they deserve.

We've seen a few examples of this in outages over the last several years. Mostly it's been an inability to fail over to other zones or regions when needed, usually due to problems that should have been fairly easy to spot and fix.

The good news is, public cloud providers are improving at disaster recovery, and they will provide better resiliency services in the near future. The bad news is, you thought the services were there all along.

2. They have provided information to the government without your knowledge. We all know about the NSA scandal by now, where it came to light that, in some instances, the government was monitoring your data stored in and moving through clouds. A series of revelations by former CIA contractor Edward Snowden shows that the United States, the United Kingdom and perhaps other governments routinely spy on a broad range of Internet services -- although not in the targeted ways most people were led to believe. In many instances, the public cloud provider knew this was going on, typically in response to secret court orders that compelled them to hand over the data.

In this guide

Of course, cloud providers responded with new privacy features and hopes that the damage to their credibility won't get any worse. According to the Washington Post, "Google is racing to encrypt the torrents of information that flow among its data centers around the world in a bid to thwart snooping by the NSA and the intelligence agencies of foreign governments." However, to many who leverage public clouds, this seems like more of a pretrial, and it will take some time to regain trust.

3. They can see your data. Most cloud providers are quick to point out that they can't see your data; only you can. However, that's not always the case.

In some instances, public cloud providers can indeed see your data, and take a quick look. Sometimes they are authorized by the company, or a person who works for a public cloud provider may take a peek for the fun of it. In any event, if you don't do the encryption yourself, it's a potential issue.

To be fair, I suspect that most public cloud providers don't look, nor care about what you store on their cloud. At least, not unless the government calls and has a court order, which relates to the problem above.

4. They are not always cheaper than traditional systems. Sometimes yes, and sometimes no. Most of the time there is a cost benefit to leveraging public clouds. However, you must look at your own cost benefits within your own business to really determine if using the public cloud is indeed cost-effective.

In this guide

Many businesses have already made a significant investment in infrastructure, and thus moving to cloud computing and leaving that infrastructure unused may not be the right move. Indeed, they could lose millions in the move to the cloud versus taking advantage of investments already made. You have to stop and run the numbers, and most cloud providers don't make that very clear.

Nothing should be too surprising here. Public clouds are not perfect, and they are a business. Thus, public cloud providers will act in their own selfish interests, including spinning information and sometimes just not keeping you informed. That said, public cloud continues to provide value. As time moves on, public cloud will get better at providing value. No matter what they tell you.

In this guide

Compare the market-leading public cloud providers

http://searchcloudcomputing.techtarget.com/feature/Compare-the-market-leading-public-cloud-providers

You've done your homework and determined you need to extend your data center to the public cloud. You've researched the technology and determined the criteria you will use to make your purchasing decision. Now, it's time to choose the public cloud provider to host your virtual machines.

But which provider offers the services and support that best matches your environment and needs?

This is the final article in a series about cloud computing buying decisions. The first article described the benefits of hosting virtual servers in the cloud, while the second detailed public cloud costs and risks.

The third article detailed the purchasing criteria to include in your vendor request for proposals (RFPs) to make sure you get the right services for your environment.

This article compares four leading public cloud providers -- Amazon Web Services (AWS), Google, Microsoft and Rackspace -- and how well they meet the following seven criteria:

- VM migration support
- Custom image support
- Image library
- Autoscaling
- Network connectivity
- Storage choices
- Regional support

1. VM migration support

As public and hybrid clouds increase in popularity, it's important for organizations to be able to move virtual machines (VMs) from an on-premises hypervisor into the public cloud, and to bring those workloads back in house if necessary.

AWS offers the most seamless VM migration path of all the major cloud providers, although Microsoft is not far behind. AWS provides a graphical interface called the AWS Management Portal for vCenter which allows virtualization admins to manage their Amazon-based resources through VMware vCenter. The portal also makes it possible to migrate VMware VMs

to the public cloud.

Microsoft built its Azure public cloud on top of Windows Server and Hyper-V. Because Azure runs the same software as many on-premises networks, it is relatively easy to migrate VMs between local data centers and Azure. The process isn't seamless, but is relatively easy once connectivity is established between Azure and a local network.

Google does not support VM migrations into the Google Compute Engine cloud. However, there are third-party providers, such as Cohesive Networks, which allows VMs to be imported into Google Compute Engine.

Rackspace does not offer a way to migrate VMs to and from the cloud. It does, however, provide a service called RackConnect that's geared toward hybrid clouds.

2. Custom image support

Cloud providers generally allow VMs to be built from predefined images, but these generic OS images don't always meet an organization's needs. As such, a cloud provider should allow custom virtual machine images to be created and used.

AWS provides Amazon EC2 API tools which can be used to import VM images into the Amazon cloud. AWS allows for the importing of:

- VMware ESX and VMware Workstation VMDK images;
- Citrix XenServer virtual hard disk (VHD) images;
- Microsoft Hyper-V VHD images for Windows Server 2003, Windows Server 2003 R2, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012 and Windows Server 2012 R2; and
- Red Hat Enterprise Linux (RHEL) 5.1-5.11, 6.1-6.6 (using Cloud Access), Centos 5.1-5.11, 6.1-6.6, Ubuntu 12.04, 12.10, 13.04, 13.10, 14.04, 14.10, and Debian 6.0.0-6.0.8, 7.0.0-7.2.0.

Microsoft makes it fairly easy to create a custom image. The easiest way is to create a virtual hard disk file and import it into Azure. Although you can build VHD-based images from scratch, System Center Virtual Machine Manager can help with the image creation process.

Rackspace supports the creation of custom images, which can be imported and exported from its cloud environment. Rackspace also provides a custom API that can be used to share custom images.

Google supports the importing of raw device mapping images, Amazon Machine Images and VirtualBox Images.

3. Image library

In this guide

Although many organizations try to minimize the number of server operating systems they use, heterogeneous environments are becoming much more common, especially in the cloud. A good cloud provider should offer a variety of server OS choices.

Rackspace offers a broad selection of server operating systems. It provides nearly a dozen different Linux variants, including Ubuntu, Red Hat Enterprise Linux and CentOS. In addition, Rackspace offers Windows Server 2008 and Windows Server 2012. Windows Server images can be preloaded with SQL Server or with SharePoint. The versions that are offered vary depending on the operating system you select. The available Windows Server 2008 images include Base OS, SQL Server 2008, SQL Server 2012, and SharePoint 2010. The available Windows Server 2012 images include R1 base image, R2 base image, R1 with SQL Server 2012, R1 with SharePoint 2013 and R2 with SQL Server 2014.

Microsoft provides a variety of operating system images including Windows Server, Ubuntu, CoreOS, CentOS, SUSE, Oracle and Puppet Labs. Windows images can be deployed using only the base operating system, or they can include Microsoft server products such as SharePoint, SQL Server, BizTalk Server, Visual Studio or Microsoft Dynamics.

AWS provides Windows-based images, as well as a variety of Linux images. The available Linux flavors include Red Hat Enterprise Linux, SUSE Linux, Ubuntu, Fedora, Debian, CentOS, Gentoo Linux, Oracle Linux and FreeBSD.

In this guide

Google offers a collection of premium operating systems, including Red Hat Enterprise Linux, SUSE and Windows Server.

4. Autoscaling

Workloads do not typically experience linear demand; instead, demand increases and decreases over time. Ideally, a cloud provider should allow workloads to automatically scale up or down in response to current demand.

Rackspace provides an autoscale feature that expands or shrinks your cloud according to a set of user-defined rules. These rules can include a schedule allowing workloads to scale up just prior to an expected demand spike, and scale down when the event passes.

Microsoft includes a Scale page in the Azure interface. You can use this page to manually scale an application, or you can set parameters that will be used to automatically scale the workload.

Google has an autoscaler that scales a workload up or down based on changing demand, and can be used with a managed instance group.

AWS provides autoscaling capabilities that can be enabled on a group basis.

5. Network connectivity

In this guide

Network connectivity is another important consideration when choosing a public cloud provider. There should be a way to connect your on-premises network to your cloud network, and the provider should offer various connectivity features.

AWS offers something it calls Enhanced Networking. This service is available for Windows and Linux VMs, and offers higher-performance networking than what is delivered out of the box. Enhanced Networking is specifically designed to provide low latency and low jitter, and is enabled by default for Amazon Machine Images based on Windows Server 2012 R2 and Linux HVM.

Rackspace offers several networking options. Extreme Networking, for example, is Rackspace's high-bandwidth solution that uses twin bonded 10 Gbps connections. A more generic Rackspace option is Cloud Networks, which allows for multi-tier software-defined networks. Rackspace also offers cloud load balancers and IPv6 support.

Google Compute Engine provides all the basic cloud networking capabilities, but also cloud load balancing and cloud DNS. In addition, Google offers an interconnect feature that allows customers to establish connectivity to the Google cloud either directly or via VPN.

Microsoft designed Azure to easily support hybrid clouds. Although you can define virtual networks within Azure, it is also possible to connect Azure to

your corporate network through point-to-point VPN. By doing so, the Azure network acts as an extension of an on-premises network. For instance, a cloud application might access a local SQL Server database.

6. Storage choices

Storage needs vary depending on workloads. Some workloads can use commodity storage without any issues, while others require high-performance storage. As such, a cloud provider should offer a variety of storage options.

Amazon EC2 includes basic storage for VMs, but the service is really designed to connect to Amazon's Elastic Block Store (EBS) service, which is designed to be scalable, flexible and fault tolerant. For instance, storage can be provisioned as general purpose, with solid-state disk (SSD) and hard disk drive (HDD) options available, or Provisioned IOPS. Furthermore, Amazon EBS supports the use of point-in-time consistent snapshots. AWS also offers a variety of fault tolerant storage configurations.

Microsoft provides basic storage for its Azure VMs. In addition, Microsoft offers premium storage for high-performance workloads. Premium storage is based on SSDs, while standard storage uses rotational HDDs. Premium storage allocation is flexible; you can define multiple disks per VM and allocate up to 32 TB of premium storage to a single VM. Premium storage

can achieve up to 50,000 IOPS per VM with extremely low latency, especially for read operations.

Google offers three different storage options. Cloud Datastore is a managed, NoSQL schema-less database for storing non-relational data. For database storage, Google offers a fully managed MySQL database. For more generalized storage, Google offers Cloud Storage, which is essentially object storage that can be managed programmatically through an available API.

Rackspace provides two main storage options: No Spinning Disks and Cloud Block Storage. As the name implies, the No Spinning Disks option is a pure SSD storage solution, and is available for VMs and bare-metal cloud servers. Cloud Block Storage, on the other hand, is available only for virtual servers. Cloud Block Storage can consist of SSD or spinning disks, and can be connected to VMs via a 10 Gbps connection.

7. Regional support

Sometimes business or regulatory requirements mandate hosting resources in a specific geographic region. That being the case, a cloud provider should ideally give its customers a choice of where VMs will be hosted.

AWS allows VM instances to be hosted in specific regions. It also designates

In this guide

various Availability Zones within those regions that are far enough apart from one another to be insulated against disasters.

Google allows you to choose the regions where your VMs are hosted. However, there are some hardware differences between the various regions, and each has multiple zones. Google's available regions include locations in the U.S., Ireland, Germany, South America and Asia. Some resources, such as VM images, are not region-specific.

Microsoft has defined 17 different regions for Azure, including locations throughout the U.S., Europe, Asia, South America and Australia.

Rackspace has cloud data centers in the U.S., London, Hong Kong and Sydney, Australia. The company uses these data centers to provide redundancy and guaranteed uptime. Rackspace does not offer the ability to confine a VM to a specific region.

Going with the right public cloud provider can make all the difference in providing an effective extension to your on-premises data center. Examining prices and features may be difficult, so make sure you put together a solid RFP to compare apples to apples and select the right service for your environment and business needs.

In this guide

Top considerations for choosing a cloud provider

http://searchcloudcomputing.techtarget.com/feature/Top-considerations-for-choosing-a-cloud-provider

Let's face it: choosing a cloud provider is no easy feat.

In addition to the vast array of vendors to choose from -- ranging from startups to 800-pound gorillas like AWS -- many target multiple sectors of the cloud computing market, such as infrastructure as a service, platform as a service and software as a service.

There are, however, steps you can take to simplify the cloud provider decision-making process. But be sure to involve both the business and IT leaders in your organization before making the final call.

Know your business objectives -- and ensure your provider does, too

Before signing with a cloud provider, make sure that provider is fully committed to understanding your business and the specific objectives you hope to achieve with cloud, said Puneet Shivam, head of U.S. and global co-head of the outsourcing vertical at Avendus Capital, Inc., a financial services firm based in New York.

In this guide

To do this, listen to what providers promise you, Shivam said. If they only boast technical gains -- such as 99.9% uptime -- it could be a red flag. Instead, opt for a provider that can speak to the business advantages you would gain through their service, such as higher customer retention or streamlined product delivery.

"If they are too focused on only technology outcomes, then they may deliver excellent technology, but may not be relevant to your business," Shivam said.

Organizations within a specific vertical market -- such as financial services, healthcare or retail -- should ensure providers have knowledge of their specific market. This might mean, in some cases, your organization opts for a smaller, niche provider -- even if they're used alongside services from a larger player like Amazon Web Services (AWS), Shivam said.

SumAll, a New York-based marketing analytics firm, did just that. After using AWS' infrastructure as a service (IaaS) platform for roughly a year, SumAll switched to Rackspace. It was Rackspace's 2013 acquisition of ObjectRocket -- a MongoDB database as a service provider -- that convinced SumAll to make the switch, said Dane Atkinson, CEO and co-founder of SumAll.

SumAll creates reporting dashboards that allow organizations to track and analyze the effectiveness of their social media marketing campaigns. The

In this guide

company grew quickly, with more than 350,000 businesses having deployed SumAll since its launch in 2011. As a result, it required an IaaS platform that could scale quickly to keep pace, while meeting its unique, big data analysis needs.

Rackspace -- especially after the ObjectRocket buy -- became a "specialty" vendor for SumAll, Atkinson said. AWS, which still hosts a small portion of SumAll's workloads, is more of a commodity provider.

"We needed something that was more responsive to what we were building -- and [Rackspace and ObjectRocket] were the ones," Atkinson said.

Another important factor when choosing a cloud provider is to give business leaders -- not just IT -- a seat at the table, according to Shivam. This ensures your business objectives are communicated clearly, and ultimately understood, by the provider.

"Technology is getting closer to the business," Shivam said. "So what's happening is that some of the decision-making and selection and management will necessarily pass into the business units."

SumAll involved both IT and business leaders in its decision to switch from AWS to Rackspace, Atkinson said.

"Because of the dollar amounts -- we spend millions of dollars a year on our infrastructure -- it's a significant portion of our costs and is probably our second biggest line item, so it becomes a business decision," he said.

Security and cost

The location of a cloud provider's data centers should also be considered, said Catherine Spence, principal engineer and cloud architect at Intel and chair of the Technical Coordination Committee for the Open Data Center Alliance (ODCA).

"When we talk about the location of the data centers, if [your] application is very sensitive, you want it to be close to where your users are," Spence said. "So, look at where your users are. You want to get the best user experience for them, which might lead to where you want to host that application geographically."

Global enterprises should be especially cognizant of where a provider hosts data. This is because security and compliance regulations can vary drastically country-to-country, particularly in Europe, said Ed Simmons, executive director of platform engineering at financial services firm UBS.

"If you are a worldwide organization, your rules around data are somewhat location-specific. So the key things are data, latency and the availability of the network and the price to move data around," said Simmons, who also co-

chairs the ODCA's Infrastructure Workgroup. "Obviously, from a resiliency standpoint, you probably want providers that have data centers in multiple locations or at least far enough away from each other that they aren't on the same electrical grid."

Security and cost are also significant factors. Unfortunately, comparing vendors' costs and security prowess isn't always easy. In many cases, it's simply not an apples-to-apples comparison. What's more, tracking down information related to a provider's costs and security strategy can be tough.

But there are some options.

"From a security perspective, obviously how [a provider] secures their network, their data and your data is very important," Simmons said. "One of the interesting questions that has come up a lot is transparency in how they do that stuff. That's a new area that people are really starting to talk about."

In an effort to standardize how the market evaluates a cloud provider's security, the Cloud Security Alliance (CSA) and British Standards Institution (BSI) launched in 2013 the Security Trust and Assurance Registry (STAR) certification program. Through the program, service providers undergo a third-party assessment of their security environments. Providers who achieve the certification are then listed as such in the CSA STAR Registry, giving existing and potential customers better insight into how robust their security is.

In this guide

Steps are also being taken to simplify how a business evaluates the cost of working with one cloud provider versus another. The ODCA, for instance, has published a Proof of Concept document, highlighting ways to compare performance and ROI metrics between two providers. However, the industry still lacks a definitive, standardized way for performing vendor cost comparisons, said Simmons.

"It's incredibly complicated and incredibly non-linear," he said.

As a result, the ODCA is now pushing for an industry-wide "Cloud Facts" label. Similar to the Nutrition Facts label on food, this would give IT pros a snapshot into a provider's performance, cost and other key metrics, making it easier to compare them to the competition.

Atkinson, for his part, urged other organizations to perform "reference checks" -- especially when it comes to support -- before taking the leap.

"I would certainly, in the future, call a couple customers through my own network that are using [that provider] to see how it's worked out," Atkinson said. "I mean, we have been here at 3 o'clock at night, and [Rackspace] has gone into the office to help. You don't realize how important that is until you actually need it."

In this guide

Private cloud hardware planning

http://searchcloudcomputing.techtarget.com/tip/Private-cloud-hardware-planning-critical-for-new-projects

Identifying the most cost-effective approach to the cloud is not easy. Budgetary constraints and commonsense indicate enterprises will take a phased approach to cloud, except in the occasional greenfield installments. And when planning out cloud infrastructures organizations, should take into account hardware, capacity, storage and networking requirements.

A large enterprise might break a cloud installation into three annual phases to allow future replacement cycles to take place as a rolling three-year upgrade, which evens out acquisition costs over time. Additionally, legacy systems need to coexist with the new cloud infrastructures. While mainframes rarely figure into the cloud equation, storage arrays can be repurposed -- especially newer purchases.

Virtualization originally drove enterprises to servers without drives, but the realities of virtualized I/O performance created high-end server configurations with local fast storage -- typically solid-state drives (SSD) or flash. These "instance stores" are surrogates for drives in un-virtualized systems.

Likewise, the processor structure differs depending on the server's target service. For big data analytics, high-end processors with large memory

capability are the best configurations; Web-servers and general computing could use inexpensive, diskless low-core count x64 or ARM64 engines packed as 1/2U servers.

Segregating use cases into big engine/small engine operations allows IT teams to create two or more heterogeneous sub-clouds. And managing them from a single console shouldn't be too difficult.

Capacity planning for private cloud

Capacity planning is the next step in your private cloud project. A large part of successful capacity planning is to look at daily, weekly and monthly cycles to establish variations in the workload. This should give an instance count for level-loading.

Next, look at peak excursions and determine how to handle them. This includes flexible start times and job priorities, which can be baked into orchestration policies. This analysis yields the number of instances required for an evenly loaded system with typical excursions.

It's good to add extra units for unexpected events, plus a small quantity to cover failures and lay down a plan to add more units, as needed, for expansion. Firewalls, software-defined networks and storage require additional instances. Perform a similar utilization analysis for each sub-cloud in your project.

In this guide

Defining storage requirements

Networked storage is another element in cloud infrastructure. The days of expensive "enterprise" drives are disappearing as SSDs replace high-end Serial-Attached SCSI (SAS) disks. Auto-tiering and caching software is changing the tiering structure to a (smaller) primary SSD array and a (larger) inexpensive bulk store. Even with less capacity in the primary, all of the active data will fit in most environments and will be delivered 1,000 times faster.

Deduplication is a way to expand the capacity of storage by as much as six times. And with drives jumping from 1 TB to 10 TB in just the last three years, the number and physical footprint of new-age arrays can be smaller.

Storage prices also are dropping rapidly, and for many similar reasons. Additionally, software-defined storage is poised to decouple high-end features from the arrays and eliminate the need for complex and expensive high-end arrays.

Networking options continue to advance

Much like storage, networking is also going through a transition -- and at a much faster pace. Software-defined networks promise to make network configuration agile and allow fast, automated orchestration of virtualized networks. The compute functions move onto standard virtual machines,

In this guide

while switching is done on commodity silicon.

All of this bodes well for infrastructure costs in your new cloud. However, there are still some options to save more money and work. Modular systems, such as containerized data center pods or rack-level installations, save a great deal of start-up effort and can be implemented faster than traditional approaches.

Converged systems take this a step further, defining a combination of servers, networking and storage that are pre-integrated and managed through a common console. These limit the need for separate organizational siloes, with corresponding improvements in efficiency and staffing levels.

Planning the infrastructure for the cloud is not magic; it requires a systematic approach. The rapid evolution of hardware technologies can complicate the decision-making process. Buying only what you need and evaluating the cloud project quarterly can ease the process and help to maintain optimal performance in your private cloud.

In this guide

Budgeting

http://searchcloudcomputing.techtarget.com/answer/Who-should-be-crafting-my-cloud-budget

How should IT and non-IT teams plan cloud budgets?

Unlike traditional IT budgets, cloud budgets are a team effort. In fact, there should be three business groups involved in cloud budget planning: business management, IT administrators and finance experts. To achieve the best cloud outcome and budget, each faction needs to communicate and collaborate.

Business managers should drive the discussion because the service -- whether delivered on-premises or through a service provider -- should meet a clear business need. Business leaders should also spearhead the testing and evaluation of prospective services

Meanwhile, the finance or executive group approves cloud expenditures. To determine whether a capital or operation expenditure is the best payment approach for the services, this group also uses financial analysis concepts, such as net present value (NPV) or cost-benefit ratios.

Lastly, the IT staff must assess whether the current infrastructure is ready for cloud service integration. This group makes any necessary upgrades or changes, and will liaise with the cloud provider to ensure smooth integration.

In this guide

Typically, IT also monitors and manages ongoing cloud performance.

For example, a business group decides to use big data analytics to identify sales opportunities. Following the model above, business leaders would drive the big data discussion, and likely consult with IT about implementation options. A business could deploy hundreds or even thousands of servers and storage to process big data tasks on-premises. However, the finance group, along with C-level executives, might want to avoid the necessary capital expense for such a deployment. Additionally, IT may lack the necessary staff or expertise.

Rather than deploy the analytics on-premises, the company could choose big data cloud services, such as those from SAP, IBM or Oracle. In this model, the company only pays for computing while analytical tasks are actually performed. The company can scale back or turn off unnecessary computing resources. Cloud services, as a result, can make big data projects more affordable and less complex.

Cloud services might seem like a strike against IT, but they actually have a positive impact on in-house IT teams. Third-party services also include third-party support, eliminating IT's burden of daily "firefighting." This, in turn, allows IT to devote more time to mission-critical applications and strategic, long-term projects.

In this guide

Ultimately, cloud budget planning is similar to all IT budget planning; the goal is to understand and control costs, while maximizing business productivity and value.

Staffing skills

IT job market evolves around cloud computing technology

http://searchcloudcomputing.techtarget.com/tip/IT-job-market-evolves-around-cloud-computing-technology

The constant evolution of technology creates various ripple effects, especially within the IT job market. At one time, for example, project teams included at least one COBOL programmer. But now, few organizations even look for that skill -- and white-hot cloud computing technology may be to blame. As businesses embrace the cloud, new job titles and skill sets emerge.

Some of the changes are minor and incremental. For example, a cloud architect is similar to a traditional systems architect. These IT pros focus on high-level design challenges and develop broad frameworks that companies

In this guide

rely on for building new applications. In addition, cloud architects are responsible for building cloud adoption plans and monitoring and managing a cloud service.

While a systems architect evaluates server hardware and network design, a cloud architect tackles infrastructure as a service, software as a service (SaaS) and platform as a service, as well as public, hybrid and private clouds. Because of cloud design complexities, there are many variations of the cloud architect role, such as Cloud Operations/Platform Architect, Cloud Infrastructure Solutions Architect and Cloud Consumption Architect.

Another cloud computing IT role -- the cloud engineer -- deals with the nitty-gritty technical issues. With traditional infrastructure, a system engineer concentrated on issues such as server operating systems and storage system type. In comparison, a cloud engineer operates in a more virtual world, in which layered software -- such as VMs and cloud OSes -- mask hardware nuances. Rather than build traditional hardwired, hardware-centric data centers, cloud engineers dabble with software-defined data center services.

The constant evolution of technology creates various ripple effects, especially within the IT job market. At one time, for example, project teams included at least one COBOL programmer. But now, few organizations even look for that skill -- and white-hot cloud computing technology may be to

In this guide

blame. As businesses embrace the cloud, new job titles and skill sets emerge.

Some of the changes are minor and incremental. For example, a cloud architect is similar to a traditional systems architect. These IT pros focus on high-level design challenges and develop broad frameworks that companies rely on for building new applications. In addition, cloud architects are responsible for building cloud adoption plans and monitoring and managing a cloud service.

While a systems architect evaluates server hardware and network design, a cloud architect tackles infrastructure as a service, software as a service (SaaS) and platform as a service, as well as public, hybrid and private clouds. Because of cloud design complexities, there are many variations of the cloud architect role, such as Cloud Operations/Platform Architect, Cloud Infrastructure Solutions Architect and Cloud Consumption Architect.

Another cloud computing IT role -- the cloud engineer -- deals with the nitty-gritty technical issues. With traditional infrastructure, a system engineer concentrated on issues such as server operating systems and storage system type. In comparison, a cloud engineer operates in a more virtual world, in which layered software -- such as VMs and cloud OSes -- mask hardware nuances. Rather than build traditional hardwired, hardware-centric data centers, cloud engineers dabble with software-defined data center services.

In this guide

Many companies deploy at least one cloud application. As enterprises look to connect different systems, new titles, such as cloud integration specialist, emerge. A cloud integration specialist navigates integration issues and educates buyers on system compatibility challenges.

Additionally, companies are increasingly adding OpenStack specialists to cloud development teams. Enterprises use the open source technology to simplify cloud integration and, as a result, OpenStack interest is growing. According to 451 Research, worldwide revenues for OpenStack business models will exceed $1.7 billion by 2016.

Cloud computing technology is not only redefining IT job roles; industry certifications represent another area of change. Previously, project team members obtained broader certifications. For example, IT pros could receive a Microsoft Certified Systems Engineer certification, which signifies Windows OS expertise. But today, companies prefer IT staff members to have vast knowledge of specific cloud platforms, such as Amazon Web Services, or specific SaaS providers, like Salesforce.

New management and orchestration tools represent another ripple effect of cloud's growing popularity. Enterprises that adopt cloud often use Puppet Enterprise, an open source IT automation software tool. Job site Indeed.com currently lists 6,850 available Puppet job opportunities. These individuals oversee the various stages of the IT infrastructure lifecycle, which includes configuring, provisioning, managing and patching cloud infrastructure.

In this guide

Additionally, organizations desire new programming skills. Chef, a stack-oriented programming language, has programs that look like cooking recipes. These programs include a title, a list of variables, data values and stack manipulation instructions. Chef is designed to scale, provision and deploy services quickly, which meshes with how cloud operates.

As cloud's popularity continues to change the skill sets that businesses find desirable, the days of high demand for COBOL programmers are seemingly over.

Internal cloud technology broker is another emerging title. In the past, IT was in charge of all technology negotiations. Today, other departments, especially marketing and finance, buy apps that will benefit their groups. A cloud technology broker provides buying advice and negotiation support to other divisions. The goal is to ensure that purchasing decisions are sound and the technology is compatible with existing systems.

Cloud also reshaping IT certifications, toolsets

Cloud computing technology is not only redefining IT job roles; industry certifications represent another area of change. Previously, project team members obtained broader certifications. For example, IT pros could receive a Microsoft Certified Systems Engineer certification, which signifies Windows OS expertise. But today, companies prefer IT staff members to

In this guide

have vast knowledge of specific cloud platforms, such as Amazon Web Services, or specific SaaS providers, like Salesforce.

New management and orchestration tools represent another ripple effect of cloud's growing popularity. Enterprises that adopt cloud often use Puppet Enterprise, an open source IT automation software tool. Job site Indeed.com currently lists 6,850 available Puppet job opportunities. These individuals oversee the various stages of the IT infrastructure lifecycle, which includes configuring, provisioning, managing and patching cloud infrastructure.

Additionally, organizations desire new programming skills. Chef, a stack-oriented programming language, has programs that look like cooking recipes. These programs include a title, a list of variables, data values and stack manipulation instructions. Chef is designed to scale, provision and deploy services quickly, which meshes with how cloud operates.

As cloud's popularity continues to change the skill sets that businesses find desirable, the days of high demand for COBOL programmers are seemingly over.

Cloud Career Advice

http://searchcloudcomputing.techtarget.com/tip/How-to-make-enterprise-IT-hire-you-in-a-cloud-career

Cloud computing is rapidly growing in importance, so a quest to rule the cloud is a good career goal. As a group, cloud admins cover a lot more

In this guide

territory than their earth-bound compatriots. Although the cloud opens up new ways to do business, challenges exist in a number of areas. And that's where a skilled admin can shine in a cloud career.

The difficulties facing cloud aren't just technology issues. While a technology base is essential for a cloud career, it often finishes in second place to a combination of business skills. The pace of agility is increasing in the cloud. Cross-vendor clouds, software as a service (SaaS) mashups and the evaluation of cost models are all important future evolutions, and they will need admins to drive them forward. In order to handle this agile cloud environment, IT pros must figure out which cloud opportunities make sense and how to mix and match cloud services and continuously measure cloud successes and failures.

In sync with figuring financial issues related to the cloud, being able to negotiate provider service-level agreements (SLAs) is a crucial skill. Being able to be hardnosed when problems occur or the supplier falls down on SLAs is useful, too, because it develops the professional respect admins need to handle these issues.

The technical skills of a cloud computing pro

Despite all of this emphasis on nontechnical skills, a cloud admin role is fundamentally technical, especially in areas of security, integration and big

In this guide

data analysis. If you can reach expert level in all or some of these crucial areas, you'll find yourself in a solid cloud computing career.

Cloud security. Many people believe that public clouds are inherently insecure, but the evidence proves otherwise. In fact major cloud providers do a better job securing data than private data centers do. The modern cloud admin is up to speed on security best practices. Issues like the recent Target, Home Depot and JP Morgan hacks force the security table to the top of the list, so being prepared is important.

In addition, the cloud is growing in concert with the mobile market. Bring your own device, or BYOD, policies and the explosion of mobile apps bring their own security challenges. Cloud pros who learn to create a stable, secure environment for company activities on any mobile device are valuable, especially if you can articulate the approaches you espouse.

Integration. It's becoming commonplace to see mashups of in-house legacy apps and SaaS or COTS-based services in the cloud. Therefore, the ability to talk the talk and be a subject matter expert in integration is a solid career path. It's important to understand the range of data integration tools to reduce risk and implementation times dramatically.

Big data. More advanced cloud skills focus on the promise and mystery of the fastest area of IT growth --big data. Big data is tied to the also-growing

In this guide

Internet of Things, which describes an explosion of data sources, analytics and business intelligence that surpasses everything we've achieved with data thus far.

Big data is a completely different worldview -- there's Hadoop and GPUs, object storage, HPC clusters running MapReduce-type parallel operations, and so many more skills to be mastered. Being facile with big data is what sets admins apart. This is especially vital with strong financial pressures to move part of the processing onto cloud infrastructure, as well as rent SaaS apps rather than buy apps or write in-house code.

Next article

In this guide

Public vs. Private vs. Hybrid

http://searchcloudcomputing.techtarget.com/opinion/Public-private-and-hybrid-clouds-Beware-of-cloud-washing

"Public clouds are homogenous; private clouds are heterogeneous." That's the statement Bob Muglia, former president of Microsoft's Server and Tools Business, made at a developer conference a few years ago. And this statement was flawed on two points.

The relative diversity of cloud computing resources has never been part of the cloud discussion, nor is it a differentiator among cloud deployment models. The complexities of implementing the on-demand elasticity and resource-pooling characteristics of a cloud also make heterogeneity impractical. However, Muglia's quote was useful to highlight the perception that there are technical differences between public and private clouds. In reality, cloud deployment models only differentiate the degree of infrastructure sharing that's permitted in an environment. Aside from that, private cloud is no different from any other cloud. And cloud washing only further confuses matters.

The National Institute of Standards and Technology definition of cloud shows three sections: essential characteristics, service models and deployment models. Cloud washing is tough to define since the three sections have no interdependencies; there is no structure that says public

clouds have one set of characteristics and private clouds have a different set. Selecting a deployment model is primarily a business decision with a small security component. Do the requirements of the organization permit the sharing of infrastructure? If not, a private cloud is the correct path.

Where does cloud washing come into play? Private clouds are viewed as a combination of cloud's hyperefficiency and ease of provisioning with the control that enterprise IT wants. This permits participation in the cloud while lowering the perceived risk. However, the potential return on investment is low, as it offers only a slight improvement over current methods like virtualization.

The Capex vs. Opex cloud promises

Much of the cloud conversation has been focused on public clouds, and the public cloud's many benefits only apply at a much lesser degree than those of private clouds. A big topic with public cloud has been the exchange of the Capex model for the Opex model, which moves spending from a large up-front number to one distributed over time.

There are several problems with this model in the enterprise, foremost of which is the challenge of variable cost in a budgeting system based on fixed costs. But assuming the variable cost model can work in the enterprise, on-premises private clouds do not offer this benefit.

In this guide

Capex is still required ahead of demand. Most likely, it will involve a larger spend than with a legacy model.

Private cloud essentials

Now that we've covered the difference between the benefits of public cloud versus private cloud, we should look at some private cloud characteristics. Here's a brief analysis of the five crucial cloud features, as applied to the private cloud model:

1. On-demand self-service: good, but it creates a risk of resources being allocated and parked.
2. Broad network access: good, but storage strategy needs careful consideration.
3. Resource pooling: good, but homogeneity is needed if self-service requirement is to be met.
4. Rapid elasticity: good if enough capacity is available. But enough capacity requires a reserve; a reserve requires Capex beyond the current needs of the organization. Utilization requires an application architectural model that uses the cloud-scaling model.
5. Measured service: Getting better, but it's only useful if accounting is integrated.

In this guide

With the current focus on self-service, private cloud offers little improvement over the existing virtualization model and maintains the same risks as the existing model -- complexity, poor resource utilization, etc. It's important to establish a process to ensure thoughtful allocation of resources and the recovery of unused resources.

Private clouds can meet all of the requirements and provide the value of cloud computing; however, additional effort is required to implement and apply them. Remember, clouds solve Web-scale problems, and those methods can help fix some enterprise-scale problems.

On-demand self-service and rapid elasticity are the two key characteristics of cloud computing, but leveraging them in the enterprise requires a very different approach to consuming IT resources. For example, workloads that are separated by a schedule can use the same resources. This requires that each workload can consume a common set of resources rather than custom-configured servers. This affects application development and operation.

Seasonal workloads are best run in a hybrid cloud model, which can significantly affect development and operation. Creating the core of the application to run in a private cloud during off-peak times and drawing in resources from an external cloud for peak periods requires a sophisticated architecture.

In this guide

So, is a private cloud for you? To determine if it's the best cloud model for your organization, ask these four questions:

1. Do you have a business problem that can be solved using cloud techniques?
2. Are your security and regulatory challenges sufficient to block consideration of public cloud?
3. Is the up-front Capex of a private cloud offset by improved productivity and/or profits?
4. Can your organization change how it applies technology to business solutions?

If a private cloud best serves your business needs, then deploy one. But make sure it's a real private cloud -- not a cloud-washed virtualized data center.

Next article

In this guide

Planning for migration

Cloud migration checklist

http://searchcloudcomputing.techtarget.com/opinion/What-to-include-on-your-cloud-migrations-checklist

While on-premises data center technology isn't necessarily on the brink of extinction, cloud computing is a relatively new option with many benefits, including scalability, agility and cost efficiency. As a result, many enterprises migrate their applications and data to the cloud. But before taking that leap, there are many points to consider.

Moving enterprise data and applications outside the firewall and into the cloud is no small feat. To ensure everyone within an organization is on the same page, cloud migrations typically require an in-depth sales pitch that covers costs, tools, security, governance and talent, among other considerations.

To craft a successful cloud migration strategy, here are six tasks that should be on your checklist.

1. Consider the application or data

While the promise of improved flexibility and scalability make cloud migrations seem like a can't-miss venture, not every application is right for

the cloud. Legacy applications, mission-critical workloads and sensitive data -- such as credit card information -- may not be suited for the public cloud. However, to take advantage of cloud computing without jeopardizing mission-critical information, enterprises can use either a private or hybrid cloud.

It's also important to consider the amount of resources each application uses. The public cloud is a multi-tenant environment, which means applications share resources. And while autoscaling in the public cloud scales resources up or down based on demand, noisy neighbors can be an issue. High spikes in demand can also run up bandwidth costs and hinder an app's performance.

2. Evaluate costs

Many organizations move to the cloud because it's cost efficient. Cloud migrations reduce hardware and IT staffing expenses. However, the financial benefits differ for each application. Any application with demand levels that randomly increase or decrease, such as mobile applications, yield a greater return on investment when moved to the cloud . But applications that use legacy enterprise hardware -- such as earlier versions of an Oracle database -- might actually be more expensive to run in the cloud.

Meanwhile, hidden expenses can be an additional burden for enterprises migrating to the cloud, so organizations need to plan for network and

bandwidth costs. And although there are pricing calculators to track cloud costs, such as Amazon Web Services CloudWatch and Microsoft Azure Pricing Calculator, accuracy is often an issue.

3. Choose your cloud flavor

Application and cost considerations weigh heavily on organizations contemplating cloud migration. But choosing the right cloud environment is just as important. And while public, private and hybrid clouds all have benefits, organizations must determine which model best meets their needs.

Public clouds, such as those from Amazon Web Services (AWS) or Google, provide a highly scalable environment with a pay-per-usage model -- but there's a flip side. Due to lack of control and multi-tenancy, highly regulated industries, such as healthcare and financial services, are poor fits for the public cloud.

Private clouds offer more control in an on-premises environment, but management falls upon the organization's shoulders. Unlike public cloud users, private cloud users are responsible for security, performance monitoring and more. And although a hybrid cloud offers the best of both cloud worlds -- a mixture of private and public cloud services with orchestration between them -- performance issues like latency and dependency can still arise.

4. Rethink governance and security

A cloud migration can often disrupt an organization's governance strategy. For example, governance methods that worked for traditional on-premises systems probably won't work for the cloud. And, as organizations move data to the public cloud, enterprise control decreases and more responsibility falls on the shoulders of the cloud providers. Therefore, organizations must shape their governance strategies to rely less on internal security and control, and more on their cloud provider's offerings. Enterprises also should ensure the provider's certifications are up-to-date.

Security concerns are a common deterrent for organizations considering cloud migrations, so it's important to plan ahead for potential breaches, failover and disaster recovery. However, any additional security tools or services can increase overall cloud costs.

5. Prepare for cloud-to-cloud migration challenges

Cloud migrations aren't just a transition from on-premises technology to the cloud; they can also migrate data from one cloud to another. These cloud-to-cloud migrations include moves from one provider to another, as well as migrations between private and public clouds. However, the migration process from private clouds to public clouds can be difficult. While third-party tools -- such as those from Accenture or Racemi -- are available to

help, there is no comprehensive tool to handle the entire migration process. Therefore, some enterprises choose to architect their own services.

Additionally, cloud-to-cloud migrations involve considerable manual labor. To prepare for migration from one provider to another, enterprises need to test their applications and make all necessary configurations for virtual machines, networks, operating systems and more.

6. Define your cloud migration strategy

Once you've considered your data, costs, security and the challenges of cloud-to-cloud migrations, it's time to come up with a migration game plan. One important aspect of this plan is deciding what to do with leftover on-premises technology. In some cases, an enterprise can repurpose hardware to avoid letting it simply collect dust.

Organizations also need to determine migration timeframes for their data and applications. While some choose to migrate everything to the cloud all at once, this can be a challenging -- and risky -- proposition. It's often more effective to break the migration down by workload, starting with less critical applications.

After taking all of these factors into consideration, determine whether a cloud migration is your best option. Overall hardware and infrastructure investment, as well as application performance and other issues, should be

In this guide

evaluated in any decision. The cloud is a rapidly evolving technology and many organizations are reaping its benefits, but it's still not for everyone.

How a cloud migration affects existing data center infrastructure

http://searchcloudcomputing.techtarget.com/tip/How-a-cloud-migration-affects-existing-data-center-infrastructure

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

In this guide

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

In this guide

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.

In this guide

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 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.

In this guide

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.

Cloud application migration and management

http://searchcloudcomputing.techtarget.com/feature/Cloud-app-management-from-migration-to-monitoring

Businesses moving applications to the cloud has become the norm, and why not? While applications gobble up storage space and bandwidth in a data center, the cloud is often a more cost-efficient alternative that eliminates heavyweight servers. Some applications, such as email and other communications, can be moved with ease. However, the cloud is not a one-size-fits-all platform.

In this guide

Enterprises need to be cautious with applications that contain sensitive data. Additionally, admins will want to ensure the apps perform as well in the cloud as they did on-premises. Finally, managing who can -- and who can't -- spin up a new virtual machine can help keep cloud costs under control.

Choosing the right applications for the cloud is just as essential as managing them properly once they're up and running. Here are five important questions to ask when moving applications to a cloud platform and to ensure solid cloud app management.

Which applications are right for the cloud?

Determining which applications are right for the cloud ultimately depends on which cloud platform you plan to use. For the most part, private cloud's benefits of more control and better security appeal to admins who want to hold on to mission-critical apps. While the private cloud keeps data on-premises, that doesn't necessarily guarantee security. Access and identity management, such as authentication and user authorization, is critical to ensure only specific users can access their data -- and no one else's. Hybrid clouds, which combine the control of private cloud with the ability to move "bursty" or seasonal workloads to the public cloud as needed, are gaining love from enterprises.

But which applications are right for the cloud? Communication and collaboration services are solid options. Enterprises often move email and

In this guide

collaborative apps to the cloud for the cost savings and to focus their time and management energy on other aspects of the business, such as development.

Do I need to re-architect my applications for the cloud?

Not all applications are a cloud-match right off the bat. Enterprises may need to re-architect legacy applications before they will perform properly on a cloud platform. Re-architecting apps for the cloud will allow those companies to take full advantage of cloud's agility, elasticity and scalability. The flexible nature of cloud computing can improve application performance and return on investment.

But re-architecting apps for the cloud is no walk in the park. Some applications were not well designed from the beginning and are poorly coded and unstable. Often, enterprises are forced to rewrite code and reshape the application to run smoothly in the new environment.

What are the keys to cloud application migration?

It's easy to understand why businesses migrate applications to the cloud. But before you move an application, enterprise IT must determine if the app is cloud-ready. To minimize risk, choose to move the low-hanging fruit of applications first, including non-mission-critical workloads.

In this guide

The next step to a successful cloud app migration is to choose where it will go. And this ultimately depends upon the apps' use case and how hands-on admins want to be with it. Is it best to move the application to software as a service, in which a SaaS provider hosts the entire application and admins have very little to do management-wise? Or is it a customer-facing application with cyclical or peak usage times that can go into public cloud to take advantage of its scalability?

Finally, enterprises need to consider costs and security. Cloud computing and cloud migrations can become budget-busters if you're not careful. Cloud provider cost calculators are helpful to determine app migration costs, but aren't always 100% accurate. And all companies should have a cloud provider backup plan for cloud vendors that don't live up to expectations.

How can I monitor my cloud apps' performance?

Performance monitoring is essential for any cloud application. Continuous monitoring allows admins to handle any issues or disruptions immediately to avoid further disaster. Many public cloud providers offer their own monitoring tools. Google Cloud Monitoring is one option that helps admins find performance problems within Google's cloud. Amazon Web Services' CloudWatch is another tool that monitors AWS application metrics. There are also endless supplies of third-party application monitoring and management tools that pick up where native tools leave off. In addition to

monitoring tools, admins should regularly test applications and study performance trends.

What are the latest cloud application trends?

Containerization dominates cloud headlines, and Docker containers are at the forefront. Formerly dotCloud, Docker is an open-source container platform for building and running applications. Its app portability has caught the eye of many providers -- including Google, AWS and Microsoft, among others. Joyent recently rolled the dice on Docker, and combined its container-based infrastructure with Docker containers. Google also furthered its Docker relationship with the alpha release of Google Container Engine. The company previously released Kubernetes, an open source container manager. And with Google's latest container developments, cloud users can expect AWS to follow suit. Enterprises looking to build new applications in the cloud should keep an eye on Docker innovations to determine if they meet their needs.

Next article

In this guide

Calculating ROI

http://searchcloudcomputing.techtarget.com/tip/True-cloud-value-goes-beyond-basic-ROI

Those charged with calculating the true value of cloud computing often refer to the old CapEx versus OpEx model. If we adopt public cloud and avoid purchasing hardware and software, that will save use money, right? It's not that simple.

So, what's an IT leader to do to establish cloud value for your organization? There are no rules or solid models that you should use every time. As always, it's a matter of understanding your business and the impact that any new technology can have upon it. Cloud computing is no different.

The old way of defining the value of cloud computing through cost efficiencies and the ability to avoid capital expenses is falling out of favor. The reasoning becomes more apparent as we gather data points about the value of a public cloud computing model. Our old way of defining cloud value gives no consideration to several key issues:

- Existing investments made in IT infrastructure, including hardware, software and data center space
- The need to change staff and add skill sets

- The value of agility and time-to-market, as applied to the business in the next 24 months
- The new costs of improving security and governance

The ability to determine the return on investment (ROI) of cloud computing is not a simple modeling exercise. Understanding and calculating the business values of cloud computing -- public, private or hybrid -- requires a complex and dynamic analysis that is unique to the problem domain you're trying to address.

Updated best practices for finding cloud value

The value of cloud computing depends directly upon the type of business, as well as the core business processes and specific problems you're looking to solve. Additionally, you need to determine how much value you actually gain from the increased agility and time-to-market, which are core benefits of cloud-based platforms.

Here's where the problem gets more complex. You can't take generic models and tools, apply them to your enterprise IT model and hope it gives you the right answer. If you can't take the time to figure out what makes your business different, you're not likely to figure out the true ROI you will obtain from the use of cloud-based resources.

In this guide

Returning to our list above, these are good guidelines to inverse, as they will get you to the right set of numbers.

First, consider existing investments made in IT infrastructure. Understand the difference between hardware and software, into which you've already sunk costs. These resources are not likely to be cost-effective to replace -- versus hardware and software that is no longer providing value. Therefore, it would be beneficial to outsource these resources to the cloud. What should be replaced and how much can be saved?

Second, consider the staff changes and skill sets, and project the changes cloud-based resources will have on your staff. This allows you to see the changes that need to occur in terms of talent -- including replacing or removing some staff positions -- as well as updating your existing staff with cloud skills. How much will this cost and how disruptive will it be?

Third, consider the value of agility and time-to-market as a value attribute to your business -- this is typically where the ROI can be found. However, the value of agility and compressing time-to-market is wholly dependent upon the type of organization you are and the weight your organization puts on it. For instance, if you're a high-tech company, then time-to-market and agility advantages are typically prioritized. If you're a paper plant that has not changed the product or business processes in 20 years, then neither likely holds much worth.

In this guide

Finally, consider the costs of improving security and governance. These are typically not addressed until the cloud is deployed, and thus have a tendency to erode or remove the value altogether. Cloud-based platforms typically require updated security approaches and technologies, which cost a lot of money. What's more, governance should be automated when using cloud, which is expensive. These costs can be as much as 30% to 40% of the final cloud resource deployment costs and certainly drive more training and staff costs.

Next article

In this guide

Expert Tips and Advice

A comprehensive look at the path to cloud migrations
Despite roadblocks in the process, cloud migrations can bring significant rewards. To successfully move to the cloud, organizations need to carefully craft a migration strategy, assess risks and plan for surprises – find out the key steps to take inside.
http://searchcloudcomputing.techtarget.com/essentialguide/A-comprehensive-look-at-the-path-to-cloud-migrations

IT just scratching surface of cloud computing technology
With wide-ranging implications on apps, devices and more, cloud is more than an IT project or strategy. Are you prepared for IT's next big shift? Discover key factors IT pros often overlook when preparing for the cloud.
http://searchcloudcomputing.techtarget.com/tip/IT-just-scratching-surface-of-cloud-computing-technology

Virtualization to cloud: Planning, executing a private cloud migration
This essential guide will help enterprise IT on the path from virtualization to building a private cloud, from the planning stages to selecting the best tools to help along the way.
http://searchcloudcomputing.techtarget.com/essentialguide/Virtualization-to-cloud-Planning-executing-a-private-cloud-migration

Devise a cloud security strategy for governance needs
IT breaches stir up cloud security concerns across organizations. To limit potential issues, enterprises must establish a cloud security strategy that considers governance needs, tools, providers and more.
http://searchcloudcomputing.techtarget.com/tip/Devise-a-cloud-security-strategy-for-governance-needs

The evolution of DevOps in the cloud
Tools like Puppet and Chef have helped enable DevOps in the cloud, but hurdles remain when it comes to managing and analyzing cloud-based apps. Realize how cloud computing is changing the DevOps game.
http://searchcloudcomputing.techtarget.com/tip/The-evolution-of-DevOps-in-the-cloud

Next article

In this guide

Getting more PRO+ exclusive content

This e-guide is made available to you, our member, through PRO+ Offers – a collection of free publications, training and special opportunities specifically gathered from our partners and across our network of sites.

PRO+ Offers is a free benefit only available to members of the TechTarget network of sites.

Take full advantage of your membership by visiting http://pro.techtarget.com/ProLP/

Images; Fotalia