MARCH 2012

CLOUD COMPUTING

Harnessing this technology to reduce costs and boost agility

800.808.4239 | CDWG.com/cloudguide

CDW·G REFERENCE GUIDE

A guide to the latest technology for people who get IT

CDW·G PEOPLE WHO GET IT™

WHAT'S INSIDE:

800.808.4239 | CDWG.com/cloudguide

Visit CDWG.com/cloud for more information on cloud computing.

What is a CDW·G Reference Guide?

At CDW·G, we're committed to getting you everything you need to make the right purchasing decisions — from products and services to information about the latest technology.

Our Reference Guides are designed to provide you with an in-depth look at topics that relate directly to the IT challenges you face. Consider them an extension of your account manager's knowledge and expertise. We hope you find this guide to be a useful resource.

SCAN IT

Download a QR code reader on your mobile device to scan and discover the best practices for implementing cloud in your organization.

Welcome to the Cloud

The underlying concepts and components of this new computing environment and where it's headed

Call it Cloud 2.0. After years spent fully clarifying exactly what cloud computing is and how it can reshape IT departments, this important collection of technologies, architectures and management frameworks has finally achieved mainstream status.

Recent research shows how far cloud acceptance has come. CDW's 2011 *Cloud Computing Tracking Poll* found that 84 percent of IT managers now say their organizations rely on at least one cloud application.

Similarly, the *Global Cloud Computing Study*, sponsored by AMD in 2011, found that 35 percent of U.S. enterprises are investigating cloud computing and nearly 40 percent use cloud solutions for hosting data, running remotely hosted applications or both. Those numbers — a combined total of 75 percent — highlight how cloud computing has clearly influenced the IT roadmaps of a wide spectrum of organizations.

The reason? Cloud environments can address core operational and technical goals. Done right, the use of cloud can boost the overall efficiency of an IT department, which in turn has the potential to save money and make operations more agile and effective.

For these reasons, 19 percent of the respondents to the AMD survey list cost reductions as the prime driver for their cloud plans, while 35 percent identify cloud computing as a tactical move to address specific needs.

Cloud Clarity

Unfortunately, the era of Cloud 2.0 doesn't necessarily herald the end of cloud hype. IT managers must still guard against those who play fast and loose with cloud claims and definitions. A good dose of reality is available from the U.S. government's National Institute of Standards and Technology (NIST), which provides the go-to reference for formal definitions.

But working definitions are also valuable: Many IT managers see cloud computing as a model for enabling convenient, on-demand access to a shared pool of configurable and rapidly provisioned computing resources, including networks, servers, storage, applications and services. The following key elements fill out this description.

Resource pooling: Applications, processing power, storage volumes, memory and other IT capabilities exist as pools that systems and users can draw from as needed.

The dynamic nature of these pools means users can tap into additional power to meet demand spikes — for example, heavy number crunching to close month-end financial books or assisting an order processing system during busy times. Once demand subsides, users relinquish the extra resources, which become available to other users.

Self-service: IT resources exist for the taking, either automatically or by request. For instance, end users could click on a simple menu to book server time or reserve additional storage capacity. Best of all, provisioning happens without calling in the IT department.

GAME CHANGER: HOW THE CLOUD IMPROVES OPERATIONS

The Traditional Way	The Cloud Way
Individuals and workgroups rely on dedicated hardware, storage and software resources.	Users access shared resources that exist as services available from a central repository.
Software resides on client computers.	Software resides in private or public data centers.
Enterprises must support different versions of applications for PCs and mobile devices.	Users can access mission-critical software from a variety of client devices.
To boost computing power or roll out new capabilities to users, IT departments work through lengthy procurement, provisioning and implementation processes.	New or expanded services can be provisioned on demand, typically without IT department intervention.
Overprovisioning of computing capabilities is necessary to accommodate demand spikes.	Dynamically allocated pools of hardware and software drive down idle or underutilized resources.

Rapid elasticity: Quick rightsizing of IT resources helps eliminate the costly overprovisioning that often plagues organizations. In the past, it was necessary to prepare for temporary demand spikes by installing more computing power than typically needed, which left expensive high-end resources sitting idle much of the time.

Depending on the individual cloud strategy, an IT department can reduce or even eliminate capital expenditures and keep underutilized resources to a minimum.

Measured service: Usage monitors meter resources being drawn from the cloud for clear data about costs, service-level performance and consumption patterns, making budgeting for operational expenses more accurate.

Broad network access: High-speed networks provide the pipelines that connect users to cloud resources. This promotes anywhere, anytime access to applications, data and processing power, whether end users are at their desks, on the road or working from a home office. Clouds provide similar flexibility in the choice of client hardware by accommodating everything from traditional desktop and notebook systems to tablets and smartphones.

Break from the Past

Cloud benefits represent a clear break from traditional IT operations that tied users to dedicated hardware, storage resources and network devices. Although generally effective for giving users the computing power they need most of the time, the traditional client–server approach often proves too rigid for the fast-paced world in which processing demands increase without much warning.

In the past, bringing a new server online could take months to accommodate procurement planning, purchasing, implementation and testing. And the consequences could be painful — too few resources could result in poor service to an important client or user, or a costly delay in responding to a new opportunity.

Dynamic, self-service resource pools overcome these problems by breaking the ties between applications and their underlying infrastructure. The result is a new computing framework that can make processing capacity available in near–real time.

Foundation for Innovation

IT innovations don't arise in a vacuum, so as more organizations embrace cloud, they're also adopting other new capabilities. Fortunately, the ripple effects of today's more mature cloud technologies are providing a foundation for other emerging IT developments.

For example, some organizations are finding concrete operational benefits from bring-your-own-device (BYOD) strategies that allow staff mobile devices to serve double duty as personal and professional gear. Anywhere, anytime availability of enterprise resources via the cloud means those workers have all the resources they need on their devices, yet IT managers can keep close tabs on security and data management.

The rise of governance frameworks, such as the IT Infrastructure Library (ITIL), also dovetails nicely with cloud strategies. ITIL provides the discipline and guidance organizations need as they transition from traditional IT environments to a cloud future.

For example, ITIL defines a services management approach to IT, which is a key first step for cloud implementations. This and many other resources are becoming available for organizations seeking guidance in the cloud. ■

Choosing the Right Cloud

How to pick the right model and platform before migrating a single file, app or system

Cloud computing appeals to organizations big and small primarily because of how effectively it addresses two fundamental (if conflicting) goals within IT departments. First, it can make data centers more efficient. Second, it simultaneously cuts upfront capital investments and ongoing management and maintenance costs.

IT managers can't accomplish these goals with a one-size-fits-all cloud solution, which is why cloud computing has grown — and continues to evolve — into a diverse set of architectures and service models. None is inherently better or worse than another. In fact, enterprises can mix and match cloud options to serve the needs of individual workgroups and departments.

Four Deployment Options

The first step in choosing the right cloud solution is to understand the similarities and differences of the four primary deployment models.

Private Clouds

Private clouds tend to be the least disruptive of the options available. An enterprise's internal IT department, or in some cases an outside service provider, maintains close control of the computing resources, fairly similar to how a traditional data center operates.

The difference is that workgroups don't use hardware and software provisioned specifically for them. Instead, they draw on a pool of shared resources available on demand.

Private clouds help avoid the culture shock of moving hardware, software, applications and data offsite. This approach also helps calm uneasiness about trusting third parties to handle security, privacy, availability and regulatory compliance. (See Chapter 5 for a detailed look at private clouds.)

Public Clouds

Public clouds are the flip side of inside-the-firewall private clouds. A service provider manages a public cloud, and clients typically share resources in a multitenancy arrangement, which means they use compartmentalized portions of the same servers, applications and storage systems.

The main draw of the public cloud is reduced costs: Multiple tenants share the costs of the underlying infrastructure. In addition, little or no infrastructure investment is required of users, who nevertheless enjoy unprecedented levels of IT service and resource scalability. The result is greater efficiency and increased agility at a relatively low cost. (Chapter 6 offers a comprehensive look at public clouds.)

Community Cloud

A public cloud variation that alleviates multitenancy concerns is the community cloud, in which a relatively small number of organizations with similar needs share a common infrastructure — and the associated costs.

The savings may be less than when large numbers of public cloud users foot the bill, but the smaller size and shared interests of a community cloud

can mitigate privacy, security and compliance fears. Similar to a private cloud, the community option can reside either within an organization's data center or at an external site.

Hybrid Cloud

There's also the hybrid cloud model, which mixes and matches the best elements of private, public and community clouds. For example, an enterprise may run a private cloud for day-to-day operations but contract for additional resources made available from a public cloud to weather a demand spike.

The best cloud deployment model will depend on several factors, including cost, control, performance, scalability, security and service requirements.

Efficiency as a Service

IT managers must also decide which services to migrate to the cloud. The options available break down into three categories.

Software as a Service

The most mature and widely used option is software as a service. With SaaS, users access applications hosted within a service provider's cloud infrastructure. Users don't own the applications or the underlying infrastructure of servers, operating systems, storage systems and network resources.

That's good from a capital expense viewpoint, but potentially troublesome in terms of flexibility: Applications come as-is, with little or no opportunity for customization.

Small- or midsize organizations' limited budgets and IT staff obviously can benefit from this model. Large enterprises can also benefit from this approach by offloading routine services to a third-party provider and devoting internal resources to strategic and mission-critical activities.

Platform as a Service

A step up in cloud sophistication is platform as a service. PaaS offerings go beyond delivering a prepackaged application via the cloud, instead providing the entire computing platform and solutions stack. This allows enterprises to run custom applications or use the solution's programming environment to create new solutions.

As with SaaS, subscribers avoid upfront provisioning costs and ongoing expenses for infrastructure maintenance and management. PaaS gives users control of the specific capabilities of their applications as long as the in-house development staff is comfortable with the PaaS provider's choices for programming languages, interfaces, development tools and database support.

Infrastructure as a Service

Infrastructure as a service delivers processing power, security tools, storage capacity and network bandwidth as on-demand services. As an organization grows, it therefore can avoid new investments in these components.

IaaS users don't directly control or have access to the technologies running in the offsite infrastructure; the cloud provider manages these. A core component of most IaaS offerings is the service catalog, an online tool for finding and provisioning available services.

Client Flexibility

Flexibility is at the core of all these cloud choices — the ability of users to not only access important resources anywhere and anytime there's a secure network connection, but to do so using many types of devices. Endpoint devices can range from traditional desktop and notebook computers to diskless thin clients, tablets and smartphones.

This is possible because of the principal cloud framework, which separates physical hardware from computing resources such as operating systems and applications.

IT departments can expect flexibility to expand further with the evolution of completely web-based clients. Browser interfaces will ultimately be the only technology that users need to connect their chosen hardware to sophisticated IT resources. For now, desktop clients remain the most common way for users to access cloud services. ■

THE DAAS DUO

Two emerging service models have joined the familiar SaaS, PaaS and IaaS options. Although the names of both newcomers share the same acronym, DaaS, they perform quite different IT services.

The first, data as a service, offers users a method for tapping into large storehouses of information on demand wherever and whenever they need them.

This form of DaaS will likely be a welcome tool for enterprises that must handle "big data," massive influxes of information that must be quickly absorbed, analyzed and used. Think NASA faced with analyzing flight information in real time during and immediately following a mission launch, or Wal-Mart plotting final seasonal orders from suppliers based on Black Friday sales.

The other new service model is desktop as a service, an outgrowth of client virtualization trends such as virtual desktop infrastructure. This DaaS lets IT managers rely on service providers to manage virtual desktops, reducing the need for in-house data center investments to do so.

Both DaaS options are so new that at present their widespread appeal is hard to gauge. But they highlight how cloud models will continue to evolve to solve highly specialized IT challenges.

Scenarios Where the Cloud Delivers

Addressing a variety of network and system problems with cloud-driven solutions

Cloud computing represents a fundamental change in how enterprises acquire and deliver IT resources. But before embarking on an ambitious cloud strategy, IT managers need a clear idea of the potential benefits they can achieve, and they must be able to communicate these advantages to bring senior management and end users on board.

One way to make the case for cloud computing is to focus on six long-standing IT challenges, and how organizations can solve them with the right cloud strategy.

Problem No. 1: Continuous Investment Outlays

IT departments are under constant pressure to implement new services to support the core missions of their organizations. But supporting these requests in traditional IT environments requires ongoing investments in new hardware and software. In an era of tight budgets, organizations find themselves making hard choices about which potential initiatives to fund and which to prioritize, delay or shelve entirely.

The Solution: Reduce capital expenditures by avoiding investments in additional on-premise hardware and applications. Instead, contract for cloud services that are paid for through operational spending that's easier to justify.

The diversity of cloud computing options (ranging from internal private clouds to pay-as-you-go public clouds) increases the chances that IT shops can acquire the services they need at costs that are in line with their current budgets.

For example, 52 percent of IT executives participating in the CDW 2011 *Cloud Computing Tracking Poll* cite reduced capital expenses as one of the top benefits of their cloud strategies. The poll's respondents also say they saved an average of 21 percent in annual costs by migrating applications to the cloud.

In addition to cost reductions, clouds can lower the risk of making the wrong decisions about promising but unproven technologies. Rather than gamble on a capital investment, IT managers can choose cloud providers that offer the most innovative services at the best prices.

Cloud technology also offers some important ancillary financial benefits not directly tied to capital expenditures. For example, many enterprises have seen their power and cooling costs rise significantly as traditional data centers grow and more densely packed servers generate higher levels of heat. Shifting to third-party cloud providers relieves energy demands and reduces utility bills.

Organizations can also gain better insight into their IT-related costs through the use of monitors that are a staple of both public and private cloud models. Metering allows for accurate chargebacks to individual departments for the services they use and can even fundamentally alter the role of the IT department. As IT departments evolve to become service providers, they may transform from a cost center to a revenue unit with profit-and-loss responsibility.

CASE STUDY

The Dynamics of Cloud Security

Read about how three government agencies with unique security concerns deployed cloud technology:

CDWG.com/cloudcs

Problem No. 2: Inefficient Use of IT Resources

Most traditional data centers suffer the unnecessary costs of underutilized servers and storage arrays, often because enterprises purchase excess capacity in anticipation of periodic demand spikes. Unfortunately, this expensive excess capacity remains idle most of the time.

The Solution: Dynamic scalability available from cloud architectures can ensure more effective resource utilization. IT managers can quickly draw from a shared resource pool, rather than stockpiling extra components.

Similarly, an IT administrator can use public cloud capacity to avoid delays when rolling out new services. Instead of provisioning and implementing new servers and storage devices, a process that can take weeks or months, the IT department simply draws capacity from an infrastructure as a service provider for on-demand services available within hours, or even minutes.

Problem No. 3: Innovation Stymied by Routine Tasks

Technology research organizations estimate that up to 70 percent of IT spending goes to "keeping the lights on" — slang for maintaining existing IT systems. What about the remaining 30 percent of the budget? That's all that's left to fund innovation and strategic projects that might give the organization a competitive edge or allow it to provide better services.

The Solution: In an age of specialization, public cloud providers dedicate significant staff time to implementing the latest software upgrades and infrastructure enhancements. This essential differentiator creates a ripple effect that benefits cloud users, who can quickly adopt technology advancements even as internal IT budgets shrink or stay at existing levels.

Access to innovative technologies isn't the only benefit. Because IT teams spend less time handling routine maintenance tasks, they have more time to work on strategic initiatives that can result in operational and organizational improvements.

Problem No. 4: Slow Adoption of New Applications

IT managers face constant pressure from users to support new applications, including mobile, collaboration and social networking tools. Traditional IT environments and tight IT budgets make it difficult to quickly procure, implement and support these demands in a timely fashion.

The Solution: Clouds offer flexible support for new apps. Elasticity, scalability and self-service access to on-demand resources in the cloud let IT shops quickly respond to changing requirements.

For example, self-service cloud-based portals give mobile workers access to essential operational services, whether they're using notebooks, tablets, smartphones or traditional desktop PCs. Similarly, collaboration software (available as a service via private or public clouds) instantly delivers enterprise-class applications for calendaring, e-mail, file sharing, instant messaging, social networking and web conferencing.

Problem No. 5: Underutilized IT Expertise

Because so much time and effort goes into maintaining current operations in traditional IT environments, routine tasks can inundate highly trained (and highly paid) technology staff. As a result, enterprises don't take full advantage of IT expertise to develop new efficiencies and improve operations or services.

The Solution: Moving portions of the IT infrastructure to the cloud can relieve maintenance and management burdens, allowing the organization to use its internal staff more strategically.

This also reduces the need to train staff or hire additional personnel to handle the growing complexity of systems in the data center. IT shops can use cloud services to handle the most complex demands and retain a core IT staff. The internal team can then focus on strategic initiatives and managing any traditional environments that remain in the data center.

CDW·G'S COMPLETE SAAS PORTFOLIO

Software as a service (SaaS) providers offer many office productivity applications, including word processing and spreadsheet programs, calendar, e-mail and human resources management solutions.

Users typically access SaaS applications via a web browser or other thin client interface. New back-office applications geared for IT departments are also becoming more common, with options available for technology service management, spam filtering and intrusion prevention.

For example, the CDW·G cloud solutions catalog includes the following SaaS applications:

- **Microsoft Business Productivity Online Standard Suite:** This is a set of messaging and collaboration tools consisting of Exchange Online for e-mail and calendaring; SharePoint Online for portals and document sharing; Office Communications Online for presence, instant messaging and peer-to-peer audio calls; and Office Live Meeting for web and video conferencing.
- **Microsoft Office 365:** This package combines the familiar Microsoft Office desktop suite with online versions of communications and collaboration services, such as Exchange Online, SharePoint Online and Lync Online.
- **CDW·G Software License and Software Asset Manager:** Software License Manager (a free service) keeps track of software licenses and versions plus start and end dates. The Software Asset Manager (subscription service) offers these capabilities along with visibility to all IP-addressable hardware and software on the network.

Problem No. 6: Growing Security Demands

New threat profiles, increasingly sophisticated cybercriminals and complex technologies that must be integrated into a unified protection strategy are just a few reasons why IT security is more challenging than ever. But as complexities and threat levels increase, IT managers find it ever more difficult to fund security efforts and maintain the requisite expertise among their staffs.

The Solution: Competitive pressures force cloud providers to maintain the highest levels of security with up-to-date architectures and in-house talent. By relying on cloud security experts, organizations often find their overall data protection levels improve.

Although clouds can relieve some security burdens, enterprises still need to do their part. First, they'll need strong assurances, written into service-level agreements (SLAs), that unauthorized users cannot gain access to their data.

In addition, organizations may need to tighten up existing security and perhaps add additional layers to match the service provider's measures. For example, as IT shops allow access to cloud-resident applications, they need to effectively address user authentication and identity management.

When making use of multiple cloud services, IT security professionals may want to consider establishing a unified access management scheme. Through a single sign-on approach, the IT security team can reduce its management burden (and also the number of passwords in use, which typically hardens passwords as well). ■

CHAPTER 4

A Map to the Cloud

What it takes to begin a ramp-up to cloud services

Cloud computing has a lot to offer today's enterprises, including antidotes to rising capital expenditures, growing server and storage inefficiencies, and delays in bringing new technology innovations to users while those innovations are still new.

But achieving any of these benefits requires a healthy dose of upfront planning and adhering to best practices when it comes to implementation. Why? Because cloud computing is not only a fundamental change for the IT department, it represents a significant shift in how people access technology to do their jobs.

So what does it take to launch a cloud strategy or convert a pilot project into an enterprisewide implementation? The first step is to view cloud computing as a long-term undertaking for both the IT department and the organization's units. To do that, start by creating a multiyear plan to identify and prioritize applications and services that will move to a private or public cloud environment.

Enterprises that take this long-range view can count themselves as part of a slim but sensible majority. Fifty-one percent of cloud users say they've defined a five-year technology roadmap for their organizations, according to the CDW 2011 *Cloud Computing Tracking Poll*.

Prepare for Pushback

Although IT staff may be the best ones to sketch out early milestones and timelines, it's important that the IT team work closely with senior executives, department managers and other influential staff members.

Cross-fertilization of ideas ensures that the cloud strategy isn't seen as an initiative exclusive to the IT department, which is essential for buy-in from top management and end users. Change-management hurdles will arise when moving to an on-demand approach to IT services, and early buy-in can help create a culture able to take on those hurdles and adjust well to change.

NO SHORTCUTS: CALCULATING CLOUD TCO

There aren't any easy formulas to help organizations determine the total cost of ownership (TCO) for new cloud projects. Instead, IT managers must spend time researching their expenses for current IT operations and comparing that information with comparable cost data for launching and maintaining a cloud environment. Here are two helpful starting points.

1. **Profile the existing environment.** This requires combing through invoices and budgets for capital and operations spending that documents hardware investments and fees for software licenses. Next, fold in related expenses for IT personnel, service and support activities, upgrades, and routine maintenance.

   Also factor in facilities costs, including power and cooling. Finally, estimate the unnecessary capital and operational expenses associated with underutilized or excess resources common to traditional IT environments. Don't ignore downtime associated with upgrades and routine maintenance or the opportunities lost because of delays in adopting technology innovations.

2. **Gather similar statistics for the proposed cloud project.** Subscription rates for a public or hybrid cloud solution can come from a service provider's proposal or industry estimates available from market research firms.

   But don't ignore hidden costs that exist for cloud services. Evaluate investments for hardware upgrades and any virtualization work. Finally, estimate how the switchover to a services model and the resulting cultural changes will affect staff productivity.

   It may take time for a multiyear cloud plan to present a clear cost advantage over the current environment. But organizations ready for a long-term commitment will see the numbers move in their favor through more efficient operations, increased productivity and greater agility.

Here are some examples of typical cultural fallout: Department heads may initially balk at sharing resources with other workgroups or with strangers in public clouds. Other managers may balk at paying for IT services (in the form of chargebacks) that in the past appeared to be free.

Even IT administrators aren't immune to some cloud-induced discomfort, because relying on third-party service providers takes away their direct control over how services are delivered.

In addition to helping organizations work through any initial cultural hurdles, these teams of cross-departmental representatives should make up permanent steering committees that handle implementation and governance issues going forward.

A Virtualized Foundation

Although rolling out cloud across the enterprise is not strictly a technology venture, the IT department will need to do a fair amount of prep work. One of the biggest technical pushes will involve the adoption of virtualization technologies throughout the organization.

Virtualization provides a foundation for cloud services because it breaks the tight bond between hardware and associated software and data that exists in traditional IT environments. It's an essential first step to creating the shared pools of resources and dynamic provisioning of workloads that are at the core of the cloud model. Cloud projects can benefit from virtualization at all levels: server, storage, client and application.

Many enterprises are well versed in server and storage virtualization today. According to industry estimates, 30 to 40 percent of server infrastructures are already virtualized. Tech analysts predict that percentage will continue to grow as organizations shed management and security concerns about virtualization.

Virtualization has become a successful data center technology for two primary reasons. First, it enables large-scale consolidation of physical servers. A 20-to-1 virtual server to physical server ratio is possible in theory, but ratios vary depending on numerous variables. Second, but no less significant, server virtualization can slash IT capital expenditures and lessen ongoing operational costs.

Storage virtualization offers similar benefits in cloud environments. Once IT administrators virtualize storage, they can create shared volumes and use thin provisioning technology to allocate disk storage among multiple users based on their minimum requirements at any given time. Fewer dedicated disks mean better capacity management and optimized storage utilization.

Increasingly, organizations are turning their attention to desktop virtualization, which separates operating systems, applications and associated data from end users' physical devices. This lets IT departments centrally manage and deliver desktop environments from the data center.

4 FOUR KEYS: SECURING VIRTUALIZED ASSETS

As enterprises increase their use of virtualization and gradually adopt cloud computing, they face a host of new security challenges unique to these environments. Here are four areas to focus on.

1. **Data encryption:** Encrypting data is essential for protecting sensitive information while at rest or when traveling to and from private, public, hybrid or community clouds.
2. **Hypervisor security:** Traditional firewalls and intrusion prevention systems (IPSs) cannot monitor traffic within the virtualized environment. Organizations need to use a combination of configuration and management policies, plus specialized hardware and software tools, to secure the hypervisor, the central control center for virtualized resources. Also, place security controls within virtual servers to harden them individually on the same physical host.
3. **Establish trust zones:** An additional way to mitigate inter-VM threats is through the use of virtual security software that creates trusted network segments. These segments group VMs with similar trust levels and let IT administrators monitor VM-to-VM traffic and enforce security policies.
4. **Hybrid cloud challenges:** Organizations need to upgrade security in any private cloud segment they manage to match levels in associated public cloud services they procure. IT shops and cloud providers will need to standardize on the cloud-specific security technologies, including virtual firewalls. IT administrators should also consider using proxy servers that intercept sensitive data for local delivery rather than via the cloud.

I.T. SERVICE MANAGEMENT

One of the biggest changes cloud computing brings is managing IT as a service rather than a resource. At the heart of delivering this service are common practices such as IT Service Management (ITSM) and the IT Infrastructure Library (ITIL).

ITSM is a process-based approach to aligning IT services delivery with an organization's needs, instead of managing IT as individual systems and components. (ITIL offers guidance on implementing ITSM.)

Just as virtualization is a foundational technology for cloud computing, ITSM (and ITIL) form the cloud's governance foundation.

For IT administrators, desktop virtualization eases upgrades, patching and policy enforcement. For users, it supports access to needed IT services and data, no matter the client being used.

Similarly, application virtualization turns physical applications into virtual services that run in isolation from one another and underlying operating systems. As with desktop virtualization, IT staff can manage each app's virtual instances from a central console. Isolating apps as virtual instances also means that no two will conflict with each other.

Regardless of how many end-user systems and apps an organization has, easing deployment and migration processes will lay valuable groundwork for a dynamic, self-service cloud computing environment.

Help with Governance

Because cloud computing is a long-term initiative with an influence across the enterprise, organizations need a solid governance framework to ensure a successful initial implementation of their cloud services and a method for managing these services over time. Fortunately, governance resources exist that embrace a services approach to IT and can be integrated into an organization's processes for managing cloud technology.

One of the oldest is the IT Infrastructure Library, a set of guidelines for identifying, planning, delivering and supporting IT services. The extensive list of ITIL resources can help implementers in a wide range of cloud areas.

ITIL offers service delivery best practices that aid the transition to dynamically provisioned services. It supports change management, which can ensure that IT administrators follow the organization's policies and track their actions in a central repository as they create and deprovision virtual machines. ITIL guidelines for IT service catalogs will also let technology managers determine which of their services are best provisioned from

a cloud self-service portal.

Organizations looking for help transitioning to private cloud infrastructures may also benefit from the resources of VCE, a consortium formed by Cisco Systems and EMC, with investments from Intel and VMware.

VCE created Vblock Infrastructure Platforms, sets of pretested virtualization, networking, computing, storage, security and management technologies. VCE also offers open application programming interfaces for building capabilities according to ITIL guidelines for service catalogs, tiered SLAs, and chargebacks and metering in multitenancy environments.

Finally, the Open Group Architecture Framework offers IT managers a methodology for designing enterprise architectures. Its Cloud Computing Work Group is now developing a secure cloud architecture based on open systems.

Trigger Events

Particular situations or "trigger events" may induce an enterprise to start down the cloud path. These can include large-scale hardware or software upgrades, the need for a new process or an expansion of the organization's activities.

When it's time to take that first step, IT staff need to determine what types of applications or services will likely recoup the fastest returns on investment from a move to the cloud. Likely candidates will also include services in the organization that must scale rapidly or require variable workloads.

Activities in the application development department are good initial candidates. Programmers often need to spin up a test bed to evaluate a new software or service and then swiftly reconfigure that environment for their next project.

IT managers can build on early pilot successes by demonstrating how one department benefits from dynamically allocated services without racking up new capital costs. By promoting early achievements and establishing a cross-functional steering committee, an organization will lay the groundwork essential for a gradual rollout of its cloud strategy. ■

NIST SP 500-293

In November 2011, the National Institute of Standards and Technology released the first draft of *Special Publication 500-293, U.S. Government Cloud Computing Technology Roadmap*, which details necessary solutions, technologies and processes for enabling cloud computing by government agencies (or any organization for that matter).

The November 2011 draft of NIST's two-part SP 500-293 roadmap can be downloaded at nist.gov/itl/cloud/index.cfm

The Private Cloud

Reaping the core benefits of cloud computing while keeping precious assets secure

Internal private clouds deliver on much of the cloud vision, including on-demand resources, pay-as-you-go pricing and unprecedented levels of scalability. And they offer an additional advantage: There's a comfort factor that comes with being inside the organizational firewall. This familiarity may be important to managers and end users who aren't ready to trust outside service providers with important applications, data and performance promises.

Another attractive facet of private clouds is that IT departments have likely already laid the foundation for this computing model through widespread use of commodity x86 server hardware and standardized operating systems and software platforms.

But even with these advantages, organizations still need to overcome cultural reticence because the cloud concept challenges some users' ideas of IT normalcy. For example, multitenancy rules are integral to fully realized private clouds, meaning that applications for the accounting and legal departments might run in the same virtual pool as programs for the facilities and human resources staffs. That idea may unnerve some users.

Having to address these types of concerns can leave IT managers wondering if creating a private cloud is worthwhile. But before this concern is even considered, there are many other questions that need to be answered about whether a private cloud is the right fit for an organization.

Is a Private Cloud the Right Choice?

First things first: IT managers need to honestly assess their enterprise's private cloud readiness. The answers to five particular questions will go a long way toward making that determination.

1. **Are you prepared to give users the autonomy they'll expect?** Quick provisioning of IT resources should be available to end users. For example, developers may decide they need four virtual machines, storage resources and dedicated network bandwidth.

A successful private cloud will make these resources available via a self-service portal where users provision and size the capabilities on the fly to fit their needs. If the IT department can't deliver on these expectations, the time may not be right for a private cloud.

2. **Has the enterprise sufficiently standardized its procedures?**
   One way to know if an IT shop has reached this stage is whether or not it has an architectural framework that supports standardized operating, deployment and maintenance capabilities. Organizations that follow ITIL guidelines for IT service management are more likely to be able to answer this question in the affirmative.

3. **How far is the enterprise willing to take automation?**
   Extensive automation is important in a private cloud for a number of reasons. The more smoothly IT managers can move workloads throughout the environment, the more efficient and cost-effective an internal private cloud becomes. Although many organizations have started weeding out manual processes, they're often a long way from fully embracing automation.

4. **Will end users willingly share resources?**
   Asked another way, is the IT department and senior management ready to educate, train and coax staff members to accept a model built on shared services? The challenge is that most users like the idea of having their data on dedicated servers and storage systems and may require carrot-and-stick incentives to change their habits.

5. **Is the organization ready to charge IT usage fees?**
   The cloud's pay-as-you-go nature means organizations can bill or at least track and report on the use cost of IT services. If an IT shop chooses to initiate a chargeback approach, then appropriate metering and tracking software will be part of the cloud's deployment requirements.

   This process also serves to increase awareness among departments and users of the true costs associated with IT services. Keep in mind that while metered usage is part of the formal cloud definition, failure to charge for that use isn't necessarily an internal private cloud deal-breaker.

Design Checklist

If all of this cloud questioning indicates that the enterprise is indeed ready to launch a private cloud, it's time to examine the existing infrastructure in detail. Most organizations will probably find that they have some cloud building blocks in place, yet fall short in other areas.

Therefore, the focus of design and development efforts will vary depending on where the organization stands on each of the following pre-cloud technology requirements.

- **Consolidated infrastructure:** The more streamlined the systems operation, the easier it is for IT administrators to manage and optimize cloud service delivery and application performance.

  The IT department can accomplish streamlining in these areas by consolidating server hardware with chassis filled with blade servers, deploying storage area networks (SANs) and boosting network bandwidth by migrating to 10-Gigabit Ethernet (10 Gig-E) network links.

- **Dynamic resource pooling:** Many organizations rely on virtualization as the foundation for resource sharing in private clouds. Virtualization is a cloud-enabling technology because it abstracts and aggregates data center resources, turning them into logical pools shared among users. For example, in a highly virtualized data center, a workload could easily move from virtual machines to virtualized storage should the need arise.

  Virtualization may be a go-to technology for dynamic resource pooling, but it's not the only choice. Other options include using products that enable rapid reprovisioning or high-performance computing clusters in which excess capacity provides the underpinnings for the pools.

- **Resource management:** Automation is the watchword when it comes to managing resources in a fully functioning private cloud. Because of this, IT managers should work to replace any manual processes that they currently use to orchestrate resource assignments whenever new service requests materialize.

  The goal is to have automated processes available for mapping virtual-to-physical resources and for helping resource managers gather and deploy operating system and application images, as well as storage and network resources.

- **Self-service interface:** Private cloud users should be able to access services from a self-service portal in a manner that meshes with their roles in the organization. Typically, users select the services they need using an IT services catalog — without having to also request the back-end resources required for supporting that service.

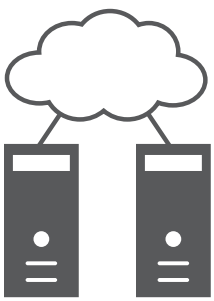
  In addition to choosing specific applications from the catalog, users should be able to select desired performance characteristics, such as "high speed" or "high availability." Ideally, the self-service interface would remain consistent no matter what changes take place on the back end.

- **IT service management:** The widely used ITIL framework is a good starting point for essential private cloud best practices, including creating processes and service policies; building the services catalog; applying capacity, configuration, demand and performance management; monitoring service health; and implementing metering, chargeback and reporting.

  In addition, an internal private cloud requires a program that acts as a service governor to dynamically optimize available resources against service requests based on a range of factors. These can include service-level agreements, operational policies and scheduled service demands. In the absence of a service governance tool, IT shops will need to handle this orchestration manually.

- **Metered service:** Most mature private cloud implementations charge departments for the services they use based on pricing published in the IT services catalog. Some organizations may not be ready for this level of chargeback at the time they launch a private cloud. Nevertheless, experts suggest it's good practice to meter service use in order to best determine how to use resources efficiently.

PRIVATE CLOUD GOTCHAS



Private clouds aren't for everyone. Here are some concerns to address before making a move:

- **Network connections:** The weak link in cloud performance is the reliability of network and Internet connections (for hybrid clouds). Any interruption in these pipelines can bring operations to a standstill. High-speed network (think 10-Gigabit Ethernet) and broadband Internet connections are a must.

- **Data management:** Data sets may be so large that they overburden available bandwidth on some network segments. IT shops considering migrating applications with large data sets to the cloud need to guard against such performance degradation issues. One answer: Move end-user clients into the cloud.

- **IT expertise:** Private clouds need the support of IT talent that's well versed in virtualization and cloud concepts, such as IT service delivery and multitenancy. Hiring these workers and keeping their skills tuned can be expensive.

- **Security:** Keeping IT resources within the confines of a private cloud may sound preferable to sending sensitive data out to a public cloud, but risks remain. Increasingly sophisticated hacking techniques require enterprises to continually invest in personnel and technology to protect their digital assets — a requirement that can be mitigated by finding an outside cloud provider with a staff of security specialists.

Private Cloud Variation: The Hybrid Cloud

Is hyperscalability on your IT wish list? Then a private cloud infrastructure might not be the answer. Private clouds are far more scalable than a traditional IT infrastructure, but not as much as a cloud service offered from a public network. There is an option that can bridge the best of these two cloud worlds: hybrid clouds.

A combination of private and public deployments, hybrids let an enterprise keep the core of its cloud resources in-house while allowing it to tap into the nearly unlimited resources of a public cloud service when demand spikes or other challenges arise.

The trick is to determine workloads that will run equally well in either type of environment. Additionally, the IT organization must be able to lock down security controls so that service can burst into the public cloud without a delay.

The IT team also will need to determine whether its existing application performance, systems monitoring and network management tools are adequate for managing the private cloud infrastructure. The IT shop may need more specialized tools.

Build with Care

With design goals in place, building out the private cloud is the next step. In some cases, IT departments will craft their cloud from scratch using new technology acquired specifically for the project.

Today, if organizations take that route, there are "cloud in a box" solutions that offer preintegrated and tested hardware and software bundled with cloud components, such as self-service portals, cost-allocation engines and tools for automated resource management.

From-scratch clouds avoid the integration hassles inherent in weaving together mismatched legacy products, but they're not always practical given real-world constraints. It's more likely that IT managers will find themselves using legacy infrastructure as a foundation for their private cloud.

There are advantages: Organizations can build the cloud gradually by expanding virtualization and then introducing dynamic resource pooling, automated resource management, a self-service interface and usage-based billing as time and resources permit. This offers benefits by methodically bringing technical staff and users up to speed with cloud environments and their ability to improve IT agility and boost efficiency.

But building a private cloud infrastructure, even slowly, is a considerable challenge. IT administrators will need to address a variety of factors, ranging from legacy applications and infrastructures to scalability practices and budgets.

Migrating to the Cloud

Once an enterprise determines its readiness for an internal private cloud, it must decide which of its applications will be most appropriate to run in that environment. To do so, IT managers should evaluate cloud suitability by first considering each application's interface. The most obvious candidates have static, easy-to-use interfaces. In general, they should run on standardized platforms and commodity hardware, and they shouldn't require massive scale-out.

First and foremost among consideration criteria is cost-effectiveness. The more consistency that can be built into a cloud service in a private cloud, the more cost-effective that service will be. In addition, consider apps with similar SLA requirements. Supporting a large range of SLAs creates a variegated infrastructure — and this heterogeneity, in turn, drives up deployment and management costs.

Conversely, apps that require high degrees of customization and are continuously targeted for upgrades and improvements probably are not suitable for deployment in an internal private cloud. The continuous rate of change to the interfaces can prove

GETTING STARTED

CDW·G account managers and certified specialists can assist organizations in developing private cloud solutions for their particular IT environments.

The CDW·G approach includes:

- an initial discovery session to understand the goals, requirements and budget
- an assessment of the existing environment and definition of project requirements
- detailed vendor evaluations, recommendations, designs and proof of concept
- procurement, configuration and deployment of the chosen solution
- ongoing product lifecycle support

too taxing for the dynamically provisioned, self-service model. Some mission-critical apps that support core operational processes also might need to remain on dedicated resources.

Identifying legacy apps eligible for cloud computing is only a first step. It's also wise to cull from the list any apps too rigid to take advantage of the elastic nature of cloud computing (such as programs that pull information from multiple databases, for instance).

And any app needing modification or a full rearchitecting to benefit from migration to the cloud should be moved down on the list of priorities. Seems obvious, right? But failure to think about and plan for adapting apps for use in the cloud can negate the benefits of moving services to this environment.

The same considerations apply to legacy hardware. Server updates will happen as part of the virtualization process, so organizations will likely have newer hardware migrating into their private cloud infrastructure. Trying to squeeze additional value out of older, less flexible hardware may prove counterproductive in the dynamic cloud infrastructure.

As with any major IT project, organizations must carefully examine both the capital and operational costs associated with building and managing a private cloud infrastructure, as well as how they'll show ROI.

Finally, managers shouldn't gloss over the possibility that the self-service, automated characteristics of a private cloud will prove unsettling for the IT staff. The antidote is to educate them about the long-term benefits available from the private cloud.

Management Guidelines

Like any complex IT installation, private clouds require ongoing post-deployment management and maintenance. Organizations need to cultivate a holistic, end-to-end view of the IT environment, including the private cloud infrastructure. Cloud management tools present a single view for monitoring and assessing performance of physical and virtual machines as well as multitiered applications and services.

These tools should span both the traditional physical components and virtual environments, and as appropriate reach into the public cloud, too. In addition, IT organizations that have instituted or are planning to use chargeback mechanisms for their private cloud services should look for tools that provide real-time usage metering. The more automated this capability, the easier it will be to implement.

Besides understanding management requirements and picking the most appropriate tools for these needs, IT managers can ease cloud management burdens by simplifying and optimizing their self-service catalogs.

A service catalog, providing services uniquely suited to the users' needs, should be built upon interchangeable resources for maximum flexibility. The IT team also will need to develop an understanding of how users will consume the services.

A goal of continuous improvement should underpin private cloud management practices. To achieve this, the IT staff should constantly assess the performance of the enterprise's processes, resource consumption rates and usage trends.

Doing so dovetails with one of the primary benefits of a private cloud infrastructure: the ability to adapt quickly to changing requirements. An informed awareness of how the cloud operates, coupled with a solid understanding of end-user needs, will position the cloud as an invaluable resource for the organization. ■

REAPING THE BENEFITS

Private clouds bring the concept of self-service, on-demand IT resources to an organization's internal data center, or in some cases to a facility exclusively maintained by an outside service provider.

Many organizations start to build a private cloud as an evolutionary step. It allows them to establish an IT services management framework that will make future transition to public cloud services feasible. Other advantages include:

- reduced hardware, software, maintenance and management costs
- rapid provisioning of resources and on-the-fly scalability
- more efficient use of limited IT staff
- increased staff productivity
- inside-the-firewall control over IT assets

The Public Cloud

Secure, reliable and flexible — this cloud form's unique opportunities

Public clouds provide ideal foundations for all types of cloud deployment models, including platform as a service and software as a service. But the infrastructure as a service model is becoming especially attractive.

The reasons are clear: Third-party service providers deliver pay-as-you-go processing power, dynamic storage capacity and scalable network bandwidth. IaaS users, therefore, are never caught in a resources gap if they need to meet new service demands. They just dial up as little or as much processing capacity as they need to meet their requirements.

On-demand IaaS resources from a public cloud also let organizations scale back during lulls, meaning they don't have to pay for capacity they won't need. Contrast this with traditional IT environments where long provisioning cycles for new resources require IT managers to maintain extra capacity that's typically underutilized much of the time. That's an especially difficult ROI case to make when budgets are as closely scrutinized as they are today.

But organizations must carefully evaluate the pros and cons of public cloud options. One of the biggest considerations is a basic element of the public cloud business model: multitenancy, the idea that multiple subscribers will share the same servers, applications, databases and storage resources.

Technologies exist to wall off services securely, but success depends on how well service providers execute their security efforts. Public clouds raise security and regulatory concerns that may restrict how some organizations use this option.

Other concerns include fears about locking data into a single vendor's cloud infrastructure and data formats, which could make it difficult to switch to another provider if problems occur. And there are some deployment issues to consider as well, such as service costs, service-level agreements and vendor management.

All of which means that for IaaS deployments via public cloud to be successful, IT shops must formulate clear migration plans that include a healthy dose of due diligence.

Service Options

Public clouds shouldn't be confused with their older cousins, hosting services. Third-party providers may perform a similar role in maintaining and managing services for a client's enterprise, but there's one big difference between the venerable hosting solution and public cloud computing. Hosting services provide infrastructure to support a predetermined level of capacity that subscribers have earmarked up front.

The capacity is dedicated to individual customers, and it's static. If a user needs additional or fewer resources, the host must reprovision accordingly. Missing in this model are some of the essential characteristics that make public clouds so flexible, including self-service, on-demand resource allocation and freedom from having to accurately gauge capacity needs up front.

So how much of an enterprise's IT needs can pubic clouds deliver today? The list is extensive. IaaS provides a comprehensive range of services that includes servers, storage, networks, load-balancing technology and security. Organizations can move entire blocks of services, such as web applications or e-mail, out to an external cloud and take advantage of almost limitless scalability without paying for dedicated servers and storage.

The ability to provision servers from a public cloud allows the IT group to acquire computing capacity on a per-project basis (and much more quickly than when hardware had to be ordered, delivered, installed and tested).

Powering up servers on demand works well in both staging and production environments, and many IaaS offerings give users choices in the configuration characteristics of the servers they'll be accessing, including operating systems and memory allotments.

Similar benefits exist for data storage. Organizations can store production files and backup copies on a public cloud provider's arrays. And as with processing power, IT managers can scale storage capacity up or down according to prevailing demand.

A great deal of Web 2.0 data gets stored in the cloud by default, but cloud storage's usefulness goes far beyond that. For example, accommodating high I/O operations per second (from rich-media content or the unpredictable growth of digital archives, for example) is another area where cloud storage pays off.

Of course, IaaS isn't the only public cloud service model. Enterprises can choose PaaS solutions to host entire computing platforms and solution stacks needed for an application during testing, development and, if desired, deployment.

Providers also deliver a range of SaaS-based enterprise applications. The choice of applications grows constantly and includes everything from office productivity suites and e-mail to collaboration, sales force automation and web hosting.

At the top of the list in popularity are online office productivity suites and conferencing services, according to the latest CDW *Cloud Computing Tracking Poll*. What do most applications delivered via public clouds have in common? They're often general-purpose programs that can easily move off-premises so that internal IT staffers can devote more time to mission-critical projects.

Security Concerns

No matter what public cloud deployment model an organization chooses, relying on a third-party provider carries risks. Numerous surveys conducted since the rise of cloud computing show that IT managers have a broad range of concerns that they need to address before public clouds become a viable option. Ranking at the top is security.

For example, when asked what, if anything, is holding their organization back from adopting or further implementing cloud computing, 41 percent of the respondents in the CDW 2011 *Cloud Computing Tracking Poll* cite security — specifically, respondents say their organizations' management and users don't trust cloud data security. And how do the IT managers themselves feel? Almost as many (40

CASE STUDY

IlliniCloud

Learn how a statewide community cloud initiative is allowing Illinois schools to share resources:

CDWG.com/cloudcs2

percent) acknowledge that they also believe their facilities are more secure than the cloud.

Security concerns are understandable, but one of the promises of public cloud is that offloading some IT management responsibilities to outside specialists can actually improve an enterprise's overall security posture. How can IT managers bridge the gap between healthy skepticism and safe operations? By developing a security strategy tailored for public clouds.

To do so, many start by meeting with members of the internal security, compliance and auditing teams to establish security requirements. The overriding goal isn't just to make cloud computing more secure; organizations also must be able to audit their activities.

To accomplish these dual goals, the security team should focus on some core elements that will take on new importance with pubic clouds. This requires detailed discussions with potential cloud providers about their security strategies and whether regularly updated

HOW TO FEEL SECURE IN A PUBLIC CLOUD

The opportunity to reduce IT costs is one of the main attractions of public cloud services, and multitenancy is a key ingredient that providers use to make that happen. But is multitenancy safe?

Some IT managers balk at the notion of sharing portions of applications, databases and storage systems with other organizations, fearing that an unintended breach or a nefarious cotenant may expose sensitive information.

The concern is valid, but it shouldn't be a reason to reject public clouds outright. Here are a few ways that cautious organizations can feel more secure in a multitenant environment:

- **Trust but verify:** Ask a cloud provider to document its technologies and procedures for securely separating tenants and how it will lock down the environment if someone attempts to thwart these safeguards.
- **Drill into the details:** Get a clear picture of how the provider keeps technologies and security patches up to date. Also understand whether data and applications will physically reside in domestic data centers or in offshore facilities. Get appropriate guarantees if organizational policies or legal requirements mandate that resources stay within the home country's boundaries.
- **Don't go all-in:** Use public clouds to support systems for information that won't harm the organization if it's exposed to outsiders. Alternately, continue to keep nonpublic financial information, intellectual property and staff personal information inside the firewall.
- **Don't view encryption as just a check-off item:** Ask your security experts to evaluate a potential provider's choice of encryption technology and how well it implements cryptography to protect data flowing into, out of and at rest within the cloud.

certifications of these measures are available to customers.

It's also important to identify management controls that authenticate and regulate users and administrators when they access cloud resources. Data encryption should be in place to protect information while stored in multitenancy environments and as it passes from the cloud environment to users and back again. IT managers should also look to new data loss prevention (DLP) technologies, which can monitor and control data flow into and out of the enterprise.

Finally, organizations should redouble security best practices that have become standard in traditional environments, including mandating that passwords be changed every 90 days and daily monitoring of new hardware and software security patch releases.

The challenge is logistical because some measures will be the responsibility of service providers, others will fall on the organization's shoulders, and some must be addressed by both. IT managers need to determine up front if they'll be able to work with a potential provider to achieve a high level of coordination.

Sticker Shock

Cloud security may be top of mind for many IT managers, but cost follows a close second. This concern ranked one percentage point below security, according to the CDW tracking poll. Part of the cloud cost challenge for managers is accurately determining what's being spent on current IT operations.

An IT department will need to look at more than capital investments in hardware and software to determine total cost of ownership (TCO). What the organization spends on IT personnel, service and support activities, upgrades, maintenance activities, and facilities (including power and cooling) must also be determined.

When comparing cost data to a cloud provider's pricing, look beyond subscription fees. IT managers should also identify costs for any necessary internal upgrades in networking or security technologies. And don't make assumptions about what's a standard or optional cloud service. For example, a provider may offer data recovery as part of its continuity package, but if that service isn't listed in the standard contract, it may be a costly option.

CLOUD COMPUTING TRACKING POLL

Get the full results of the CDW 2011 *Cloud Computing Track Poll* here:

CDWG.com/cloudpoll

By breaking out the hard costs to maintain the existing environment, an organization can make cost comparisons to different cloud options and see the likely financial impact. But even this analysis won't tell the whole story.

Remember, the public cloud model isn't entirely about cutting costs. Organizations also have to determine how much they value other potential advantages, such as the chance to eliminate underutilized or excess capacity and the ability to free IT personnel from daily maintenance tasks so they can focus on strategic initiatives.

Enterprises will need to devote time and research to determine the final answer, but the result will be a clearer picture of a public cloud's initial and long-term cost profile.

Compliance Considerations

Depending on the organization, concerns about regulatory compliance may dictate the terms of a public cloud relationship. Highly regulated industries, such as healthcare and banking, need providers that can maintain audit trails to prove compliance with the Healthcare Insurance Portability and Accountability Act (HIPAA) and/or Sarbanes–Oxley (SOX) rules.

Similarly, some laws governing data protection for public sector agencies require highly sensitive information to be stored in domestic facilities. Discussions with cloud providers must address any government or internal data management and verification requirements.

Important questions during these discussions would include: Where does the data reside? Who has access to the data — and how is that monitored for auditing purposes? What data protection mechanisms and disaster recovery strategies are in place? Will auditors be able to review a provider's overall security practices?

Finally, enterprises should address one other fundamental concern: What are the risks associated with relying on a single vendor for a sizable portion of the organization's IT resources?

First, be sure any applications that run in a public cloud are easy to duplicate if the provider goes dark for any reason. Portability of data and applications is essential to guard

against service problems that might cause the organization to have to procure cloud service elsewhere.

Other concerns center on nuts-and-bolts technology issues. For example, using an outside service provider makes an organization completely reliant on its network connections. Any glitch in these pipelines could bring operations to a standstill. High-speed WAN or Internet connections are a must for ensuring that users receive the performance levels they need. It's not enough to consider the theoretical ratings of these network connections.

IT managers also must analyze their traffic patterns flowing to the public cloud to determine if especially large data sets will be part of normal operations or make up occasional spikes. Applications with intense I/O computations moving multiple terabytes of information may overwhelm cloud connections. Organizations should factor in performance considerations such as these when deciding what services are appropriate for a public cloud.

Choosing a Provider

Following the internal analysis to determine the appropriateness of a public cloud migration, associated risks and technical considerations, it's time to focus more closely on the makeup of individual providers.

A prime consideration is the provider's viability as a company. It's important to get a thorough explanation of the business plan of any potential provider. In addition, researching into the experience of the management team and the depth of expertise throughout the IT ranks is valuable.

Also, determine whether the provider maintains the complete end-to-end cloud infrastructure or if it outsources portions. If a provider uses subcontractors, these partners need to pass the same level of scrutiny as the prime provider.

What follows is a checklist of issues that should be addressed.

Security: Given the ongoing concerns of IT managers, competency in this area will be a chief factor in the selection process. The following security protocols need to be a part of any service agreement:

- Assurances, backed by technology implementation, that one tenant can't gain access — either intentionally or by mistake — to another tenant's data on a shared server
- Encryption of data in transit and at rest
- Firewalls at the network perimeter as well as on host servers
- Use of authentication and secure passwords
- Regular reviews and security updates

Server infrastructure: Before setting a deal for cloud service, the IT team should determine the make, model and configuration of the servers that would operate in the public cloud infrastructure. Also, understand the provider's replacement procedures for failed or problematic machines. Ask how the provider handles server redundancy for backup operations and the general geographical regions and environmental conditions that exist in these locations.

Storage systems: As with servers, public cloud users should have a clear idea of the types of storage the provider uses and the technical reasons that led to these choices. Information on how quickly storage can be added or removed, and at what cost, is also vital.

Backup and recovery: Any hindrance

WHAT WORKS WELL IN THE PUBLIC CLOUD?

The following service offerings have proven to be good fits for the public cloud:

- Highly scalable processing power
- Scalable storage for production and backup files
- Storage for digital content that requires high input/output operations per second
- Testing and development platforms
- General-purpose and noncritical applications

to accessing data in the cloud is not acceptable. Dig into hosting candidates' backup procedures; be sure to get details on frequency, location and mean time to recovery.

Monitoring: Organizations should expect continuous monitoring along with automated alerts, real-time dashboard visibility into provided services and access to performance statistics and trend analyses.

Service interface: The cloud agreement needs to provide details on the service interface. Will users have access to cloud services via a web front end or some other sort of client interface? Should the provider's back end change, will that be transparent from the user perspective?

Support: In the cloud, support from an experienced staff with broad expertise needs to be available 24x7. Depending on application requirements, an organization may require advanced support as well. For example, will the cloud provider help in porting data and applications to its cloud?

Negotiating SLAs

At the core of the relationship between an organization and a cloud services provider is a service-level agreement. The SLA sets performance guarantees for the procured services. The agreements also spell out remediation options when service levels fall short.

Unfortunately, SLAs remain an immature and still evolving area in cloud computing. Sticking points include how best to assign accountability for problems.

IT managers should make sure that their SLAs answer the following questions:

- How quickly will the cloud services be up and running?
- How quickly can service levels be adjusted as use demands rise and fall?
- Does the SLA apply to the infrastructure as a whole or does it cover each individual machine?
- How often will downtime occur for scheduled maintenance, and how will disruptions be scheduled?
- Will the provider accept an exit clause allowing termination of the contract without penalty in the case of recurring incidents?
- What types of service problems result in refunds? What types receive service credits? What are the redemption procedures in each case?
- How will reports analyzing performance against agreed-upon metrics be provided (and how often)?
- How will the cloud be monitored for regulatory compliance?

Migrating (with Care)

Once cloud choices have been finalized and an SLA approved, all that's left is moving the organization's data to the provider's infrastructure.

Before the migration, IT shops must test the scalability of the infrastructure as well as its on-demand responsiveness. Promises don't always meet reality. It's better to know this before the migration than after. Depending on an IT organization's capabilities and the nature of the procured public cloud services, assistance from the service provider during the migration process may make sense.

IT organizations usually can expect SaaS deployments to be fairly routine, with applications quickly becoming ready for use. But porting data and on-premises applications to a cloud infrastructure will typically be more difficult. As part of a migration plan, an IT organization may need to call on its provider to help optimize apps.

As with any IT deployment, it makes sense to ramp up migration, evaluating services for hiccups and making adjustments as needed. But one thing is certain: The potential points of failure will be fewer (if nearly nonexistent). After all, that's a chief reason for making the move to a public cloud. ■

This glossary serves as a quick reference to some of the essential terms touched on in this guide. Please note that acronyms are commonly used in the IT field and that variations exist.

Glossary

Application virtualization

A type of client virtualization, application virtualization allows applications to run as virtual services in isolation from one another and from any underlying operating systems.

Broad network access

An essential cloud characteristic, broad network access facilitates network capabilities and their access through standard mechanisms that promote use by heterogeneous thin- or thick-client platforms. These can include notebook or tablet systems, personal digital assistants and smartphones.

Cloud computing

Cloud computing generally refers to a computing environment that enables convenient, on-demand network access to a shared pool of configurable resources (networks, servers, storage, applications and services). These resources can be rapidly provisioned and released with minimal management effort or service provider involvement.

Cloud providers

Cloud providers are organizations that offer a product or platform based on virtualization of computing resources coupled with a utility-based payment model.

Cloud storage

In a cloud storage arrangement, files or data backups are uploaded and stored on a cloud provider's arrays. Storage capacity can scale up and down on demand.

Community cloud

In a community cloud, several organizations share an infrastructure, which supports a specific collection of users with similar missions, security requirements, governance policies and compliance considerations. It may be managed by a vendor or other third party and can exist on or off premises.

Data as a service (DaaS)

DaaS providers manage large storehouses of information that they make available on demand to customers. DaaS can help organizations manage massive influxes of information needed for internal operations, analyzing market trends and improving customer service. This is one of two cloud service models abbreviated as DaaS (see also desktop as a service).

Desktop as a service (DaaS)

An outgrowth of client virtualization capabilities (such as virtual desktop infrastructure), DaaS can manage virtual desktops and reduce the need for in-house data center investments supporting virtual environments. This is one of two cloud service models abbreviated as DaaS (see also data as a service).

Dynamic resource pooling

This term refers to the massing of a service provider's computing resources to serve multiple customers using a multitenant model, with different physical and virtual resources (such as storage, processing or memory) dynamically assigned and reassigned according to users' requirements.

Hybrid cloud

A hybrid cloud is a cloud infrastructure composed of two or more clouds (private, community or public) that remain unique entities bound together by standardized or proprietary technology. The hybrid model enables data and application portability, such

as failover to a cloud service for load balancing between types of clouds.

Infrastructure as a service (IaaS)

IaaS provides users with the ability to provision processing, storage, networks and other component computing resources. The user controls operating systems, storage and deployed applications, and (possibly) select networking components, such as host firewalls.

IT Infrastructure Library (ITIL)

ITIL is a globally recognized collection of best practices for IT service management.

IT service management (ITSM)

ITSM is a systems discipline philosophically centered on an organization's perspective of IT's contribution to the enterprise.

Measured service

Measured service refers to how cloud systems automatically control and optimize resource use by leveraging a metering capability at the level of abstraction appropriate to the particular service (storage, processing, bandwidth or active user accounts). Resource usage can be monitored, controlled and reported, providing transparency for both the provider and user.

Multitenancy

In this cloud model, users share portions of the same servers, applications, databases or other IT resources. Multitenancy distinguishes cloud services from hosting services, in which a third-party provider manages resources for the exclusive use of a customer.

National Institute of Standards and Technology (NIST)

NIST, an agency within the U.S. Commerce Department, has crafted a series of cloud definitions as well as guides aimed at promoting effective and secure cloud computing.

Network virtualization

This form of virtualization combines the available resources in a network by segmenting bandwidth into channels that are independent of one another and can be assigned (and reassigned) to servers or devices in real time.

On-demand self-service

This essential cloud feature allows users to unilaterally provision computing capabilities, such as server time and network storage, as needed without human interaction by the service provider.

Platform as a service (PaaS)

PaaS gives a user the ability to deploy applications created using programming languages and tools supported by the provider. The user controls the deployed applications and possibly application hosting environment configurations.

Private cloud

A private cloud is an infrastructure operated within an organization to provide cloud services to its end users. The organization or a third party can manage the cloud, which can exist on- or offsite. A private cloud can also be hosted on a public cloud infrastructure.

Public cloud

A public cloud is an infrastructure available to multiple organizations and run by a cloud services provider.

Rapid elasticity

With this cloud feature, users can quickly provision capabilities, in some cases automatically. To the user, capabilities available for provisioning appear unlimited.

Server virtualization

This form of virtualization lets a single server take on the roles of several, running multiple operating systems and applications within compartmentalized virtual machines.

Service catalog

A service catalog is a cloud provider's listing of available services as well as their costs, performance guarantees and provisioning instructions.

Service-level agreement (SLA)

An SLA establishes the benchmarks for monitoring a cloud provider in meeting a user's service requirements.

Software as a service (SaaS)

SaaS lets users access a provider's applications running on a cloud infrastructure. The apps are accessible from various client devices through a thin client interface such as a web browser.

Storage virtualization

This form of virtualization pools physical storage from multiple network devices (typically within a storage area network) that can be managed from a central console.

Total cost of ownership (TCO)

TCO is a metric that can be used when comparing the cost of a cloud computing service with on-premises deployment.

Virtual security

The term refers to a theory that through the proper use of virtualization technologies in the cloud, a provider can develop a security infrastructure safe from hackers.

Virtualized desktop computing

With this form of virtualization, the user's client operating system, applications and associated data run as a virtualized desktop on a central server. Users can access their virtualized desktops from almost any device, from a desktop PC or notebook computer to a smartphone or thin client.

Index

ABOUT THE CONTRIBUTORS

NATHAN COUTINHO is a solutions manager for CDW with a focus on virtualization. He has more than 11 years of experience in IT, covering various roles in management, technical sales and consulting. His current responsibilities include evaluating and educating clients about trends and directions in the server, client and storage virtualization spaces.

PAUL SCHAAPMAN is a solution architect for CDW. With more than three decades of experience in IT infrastructure, he has a strong background in virtualization (server and client), server and storage engineering, IT architecture, and IT consulting. Paul was awarded VMware's Virtual Vanguard Award in 2007 for his work on a large virtual infrastructure for the Virginia Farm Bureau.

LOOK INSIDE FOR MORE INFORMATION ON:

- How to squeeze the most value from a cloud deployment
- Determining the right cloud arrangement for an organization
- Guidance on managing new cloud infrastructures
- How bring-your-own-device (BYOD) programs fit into the cloud