JANUARY 2013

CLOUD COMPUTING

Finding the right fit among constantly evolving cloud options

800.800.4239 | CDW.com/cloudguide

CDW REFERENCE GUIDE

A guide to the latest technology for people who get IT

CDW PEOPLE WHO GET IT

WHAT'S INSIDE:

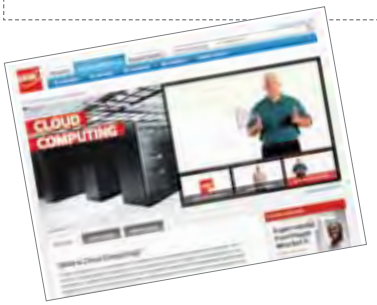
800.800.4239 | CDW.com/cloudguide

PRIVATE CLOUDS, UNINHIBITED VALUE PROPOSITION

WHAT IS A CDW REFERENCE GUIDE?

At CDW, 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.



VISIT

CDW.com/cloud for more information on cloud computing.

SCAN IT

Download a QR code reader on your mobile device to scan and see what Charles Barkley thinks about cloud collaboration.

GET m.CDW.com ON THE GO

m.cdw.com is now available anywhere with our new mobile-friendly website or download the CDW app for your iPhone from the App Store.

A Walk in the Clouds

This maturing technology gets better with age.

DO YOU UNDERSTAND CLOUD COMPUTING? If you're like most IT managers, you probably have a solid grasp of the basics, but you also realize that this technology is changing constantly. Staying abreast of rapidly evolving cloud technologies is getting more difficult by the day, thanks to a wide range of new applications and service models, as well as the new management and security challenges that arise with every innovation.

But there are payoffs — in lower costs, higher efficiency and greater reliability — for those who can keep up. That's where this *Cloud Computing Reference Guide* fits in. It offers a fresh look at the world of clouds as adoption rates climb across all types of industries and best practices mature to address past concerns, delivering on the technology's promise.

Just as important, this guide shows how cloud computing has changed even within the past year or two as related IT trends reshape how organizations define and capitalize on clouds. Case in point: the consumerization of IT.

It offers the upside of increased productivity for workers who can decide which technology tools will help them become more effective in their jobs. But there's a downside to greater choice when it comes to clouds. Some workers are making technology decisions independent of IT expertise and creating "rogue" clouds that may result in unnecessary costs and open up new security risks.

IT managers are also looking for ways to address the mobility trend and the need for anywhere, anytime access to information created by the latest generation of tablets, notebooks and smartphones. Some answers for a growing number of organizations are built around on-demand cloud services that can meet these mobile requirements efficiently and securely.

These and other developments are encouraging IT managers to fundamentally rethink their cloud strategies, including what applications they send to the cloud. As a result, on-demand solutions for unified communications and collaboration or business continuity and disaster recovery are part of a growing list of next-generation cloud applications. And as they're reconsidering cloud services, administrators are also exploring new, hybrid delivery models with an eye to combining the best characteristics of traditional approaches.

But no matter how quickly cloud technologies evolve, they continue to present IT departments with management challenges. In some cases, that may mean finding the right tools for monitoring both physical and virtual IT resources or for automatically allocating and balancing workloads. Of course, securing information as it flows between cloud users and providers, as well as when it's housed in a cloud, is a priority.

This guide will take a closer look at the major IT trends that are changing cloud computing. It will also explore the latest best practices for migrating to private clouds or to public services. Finally, the guide will lay out the latest thinking for ensuring the security and availability

of data and applications in the cloud.

IT managers know that change is constant when it comes to technology. They also know that with the right resources, they'll see a big payoff when they successfully embrace the latest in what cloud computing has to offer.

The Big Picture

With all the hype around cloud computing these days, it's easy to forget the fundamentals — exactly what clouds are, and just as important, what they're not. After all, depending on who's doing the defining, the cloud moniker has been applied to everything from a third-party software application delivered on demand (valid) to piggybacking onto a neighbor's unsecured Wi-Fi network (dubious at best).

Fortunately, clarity doesn't have to be elusive when it comes to clouds. Remembering some simple and straightforward definitions can help IT managers ground cloud computing in reality and frame discussions about where it fits in the organization's current and long-term plans.

First, a working definition: Cloud computing is simply software and computing resources that are delivered on demand, as a service. Of course, there are times when a more detailed definition is required; for instance, when IT managers are presenting a formal proposal to senior executives or negotiating the terms of a service-level agreement (SLA). That's when the National Institute of Standards and Technology's widely accepted cloud definition comes in handy.

According to NIST, cloud computing is "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

Whether IT managers choose a working description or a formal definition, the essential elements common to both come down to a handful of key characteristics:

- On-demand, self-service resources
- Broad network access
- Resource pooling
- Rapid elasticity or expansion of capabilities
- The ability to measure service deliveries

Once IT managers focus on these core concepts and strip away the marketing fluff around cloud computing, they find there's a lot to like about the model.

5 Reasons to Consider Clouds

The growing popularity of clouds can be traced to how well the characteristics of the cloud model translate into concrete benefits, for commercial and public-sector organizations alike. Topping the list are the following:

RAPID DEPLOYMENT | By eliminating the installation of on-premises software and hardware, a cloud solution can be deployed much faster, within minutes in some cases.

RAPID SCALABILITY | The ability to easily and rapidly increase or decrease available cloud resources allows organizations to accurately align IT services with changes in demand and seasonal cycles. In the past, IT managers had to plan for peak usage rates, which often meant that excess capacity sat idle during nonpeak periods. The combination of rapid deployment and scalability makes organizations more agile.

For example, when a higher than expected spike in demand for a microbrewer's new product materializes, IT managers can immediately dial up the computing capacity needed to fulfill all the incoming orders. If demand eventually levels off, IT administrators can dial down the computing power and no longer pay for resource levels that aren't needed anymore.

CLOUDS CONTINUE TO **GAIN TRACTION**

IT managers across many types of industries are expanding their cloud adoption strategies. For example, 75 percent of organizations that responded to recent polling by technology research firm Gartner said they will be pursuing a private cloud strategy by 2014. The public sector is equally enthralled.

In the federal government, where cloud-first policies reign, 50 percent of agency IT managers in fall 2012 said they are beginning or advancing existing cloud adoptions. This represents a 10 percent rise from a year ago, according to *InformationWeek's* Federal Cloud Computing Survey.

EASE OF MANAGEMENT | When an outside cloud provider is responsible for the day-to-day management and support of servers, storage systems and other core resources, the IT department is free to focus on more strategic activities, such as working with business or program managers to devise new types of services or address emerging productivity problems.

MOBILITY | In an age of ubiquitous smartphones, tablets and notebooks, organizations need a framework for securely delivering applications and data to workers, wherever they happen to be working. Clouds can do this by delivering centralized resources to mobile devices via an Internet browser.

Not only does this result in anywhere, anytime access to information, it facilitates greater collaboration within the workforce. For example, first responders can send real-time damage reports to a cloud-based emergency management application so decision-makers in a central command center can coordinate rescue efforts in the aftermath of a hurricane.

TIGHTER FINANCIAL CONTROLS | The multitenancy model of cloud computing, in which multiple users share resources and reduce the costs that any single customer pays, represents a money-saving alternative to traditional technology investments. In addition, organizations reduce their capital expenses by avoiding upfront purchases of on-premises hardware and software.

Subscription fees for cloud resources, in turn, become operating expenses that are more predictable, even with the ups and downs of demand cycles. Pay-as-you-go costs are also often easier to justify than spending for big-ticket infrastructure components.

A Range of Choices

When it's time to evaluate how and where cloud computing may benefit the business or mission goals of an organization, IT managers must consider the unique characteristics of various cloud options. These variations fall within two major groups: deployment and service models.

There are three main deployment alternatives to choose from: public, private and hybrid clouds.

Public clouds: These clouds are built and managed by independent service providers who deliver IT resources based on the SLAs they negotiate with customers. The actual resources may vary according to the customer's needs, ranging from a complete solution that covers entire IT infrastructures and development environments to something more modest, such as an e-mail or sales-force management application. The public cloud option provides easy scalability and frees IT staffs from having to implement and manage resources that fall under an SLA.

Private clouds: These clouds create pools of shared resources for scalability and efficiency, but they're designed and managed solely for the needs of their owners. The internal IT staff or a third-party contractor manages the private cloud, and scalability is limited to how much the organization can invest in underlying technologies. In return, organizations can tailor private clouds more to their liking and take direct control of security practices.

Hybrid clouds: These clouds consist of two or more clouds and combine the strengths of both public and private models. For example, an organization may keep a mission-critical financial application within its own data center to preserve customizations and security policies that address unique business needs, but link it to computing resources in a public cloud so it has scalable processing power to meet demand spikes when, for example, closing monthly books or compiling quarterly financial disclosures.

At Your Service

IT managers can also evaluate clouds according to the type of services they deliver. These are three widely used service models:

SOFTWARE AS A SERVICE | SaaS provides a complete software application available on demand to end users, typically via a web browser. SaaS eliminates upfront capital investments and management responsibilities for in-house IT staff. It's also an option for quickly launching a new application. For example, if the bring-your-own-device (BYOD) trend takes hold in an organization, the IT department can quickly take control by subscribing to a SaaS-based mobile device management solution.

PLATFORM AS A SERVICE | A boon for application developers, PaaS solutions provide (typically through a web browser) the underlying infrastructure and development tools required to build and deploy cloud applications that are delivered on demand. Benefits include increased accessibility to the latest tools for making developers more productive, which shortens the time required to give in-house users or customers enhanced services.

INFRASTRUCTURE AS A SERVICE | IaaS supports network architects with on-demand computing, storage and networking resources in an infrastructure designed for flexibility and scalability. The payoff is increased speed when addressing competitive opportunities or challenges. Organizations are also able to better predict monthly costs and avoid excess spending for underutilized resources that are needed only during occasional peak demands.

Mature Best Practices

When cloud computing was new, IT managers understandably moved cautiously before making widespread commitments to this new computing model. But as adoption rates climb across commercial industries and the public sector, mature best practices are emerging to address past concerns.

These include how to ensure that data and applications remain secure in multitenant environments and as information passes to and from clouds and customers. As Chapter 6 explores in detail, cloud adopters now have a clear set of security technologies and policies to protect their environments.

Similarly, as subsequent chapters show, organizations now have a clear roadmap for addressing concerns about maintaining reliable performance and availability with clouds, integrating them with existing infrastructures and negotiating SLAs that reduce the risks of vendor lock-in. ■

Cloud's Horizon

Cloud computing is transforming — here are the drivers.

CLOUD COMPUTING CONTINUES TO EVOLVE RAPIDLY. Here's a guide to five major trends that will likely have the greatest effect on an IT department's cloud strategies in the months ahead.

Consumerization of IT

Mention consumerization of IT and most people immediately think of all the personal smartphones and tablets that workers are bringing to their jobs because these familiar and easy-to-use devices make them more productive. But a growing body of research shows hardware isn't the only technology flying under the IT department's radar thanks to consumerization. Departments and individuals are also subscribing to cloud-based SaaS applications and IaaS services in a similar attempt to jump-start projects or acquire new capabilities.

Unfortunately, expediency can have unintended consequences. New security risks and compliance breaches can quickly arise when the IT group doesn't control or even fully understand what services are in play and where the organization's data resides. At the very least, the organization can no longer accurately track its total IT costs if a large segment of services are off-budget. In this scenario, the chances are high that the organization may be paying for redundant subscriptions to some applications and services.

How pervasive are these rogue cloud services? According to *The Wall Street Journal*, one survey found that 43 percent of IT decision-makers knew of cases where someone circumvented the IT department to access services that were not sanctioned by the organization. The most common reason: to reduce the time it takes to go through normal acquisition channels.

Fortunately, IT managers who understand that the cloud landscape is changing can also take advantage of new methods for keeping rogue clouds under control. One aid is to adopt key best practices outlined in the Information Technology Infrastructure Library (ITIL), an industry-standard framework for better IT management.

In particular, by creating a services catalog with a self-service interface, IT managers can give users ready access to all available resources to help reduce the chances that they'll look elsewhere and sign up for duplicate services. A streamlined process for expediting requests for new capabilities also increases the chances that users will go through proper IT channels for new services rather than taking an ad-hoc approach.

Ubiquitous Mobility

The new era of cloud computing also presents a variation on the-chicken-or-the-egg dilemma — is the rise of ubiquitous mobile applications boosting demand for clouds, or is the flexibility of cloud computing spurring mobility? The answer, of course, is yes to both.

With mobility becoming a fact of business life, workers need access to the same applications and data while they're traveling as when they're at their home base. Clouds can do this by delivering the full lineup of

data center resources through a browser interface or lightweight mobile app to mobile hardware.

That means organizations can reliably turn mobile devices that were designed primarily for consumers (such as tablets and smartphones) into business-ready tools that help improve productivity and enhance customer service. For example, inspection agencies, hotels and even auto-dealer service departments are now assigning tablets to roving staffers who can enter constituents' data on the spot or help customers avoid lines at check-in counters.

But productivity isn't an IT manager's only concern. BYOD-fueled mobility can open up many new security risks. Fortunately, clouds can address these concerns as well, with mobile device management (MDM) solutions that track and provision user devices, wipe data from lost or stolen hardware and create sandboxes that separate business and personal data stored on portable gear.

For highly regulated sectors, such as healthcare, clouds can also manage and maintain records of when and how protected information was accessed to help organizations demonstrate compliance with the Health Insurance Portability and Accountability Act (HIPAA) and other laws.

New Cloud-based Applications

In the past, when IT managers talked about moving applications to the cloud, they typically focused on low-hanging fruit — e-mail applications, sales-force automation solutions or backup storage capacity. As cloud computing matures, organizations are moving to more sophisticated cloud-based applications that play bigger roles in keeping their organizations running smoothly.

One case in point is unified communications and collaboration (UCC). By closely linking voice, video, instant messages, online chats and conferencing applications, UCC is becoming more important than ever as workforces become more mobile and collaborative. But building on-premises UCC solutions requires not only upfront investments for servers, software, storage and networking resources, but also the technical expertise to integrate all these separate elements into a cohesive platform that enables seamless communication.

Cloud-based solutions can shorten the time it takes to realize UCC value by eliminating the acquisition and integration phases. With cloud solutions, organizations can quickly get the features they need up and running and have the option of adding additional functions over time as new capabilities become necessary. And because the cloud-based UCC solution is accessible anywhere there's a secure Internet connection, the capabilities are available to employees on the road or in branch offices, as well as to trusted partners that play a pivotal role in decision-making processes.

IT managers are also seeing cloud-based solutions as important options to consider when it comes to backing up and archiving data. The financial consideration is similar to UCC's. Because upfront capital investments aren't necessary, organizations can significantly reduce the time required to justify the spending and then procure, implement, test and manage an on-premises infrastructure.

Just as important, IT shops can decide to contract only for the capacity they need without paying in advance for anticipated future levels of storage. But as requirements change over time, IT managers can contract for additional capacities. This level of control and flexibility means organizations

OPERATING SYSTEMS **BECOME CLOUD AWARE**

Applications and service models aren't the only areas being influenced by cloud technology. So too are enterprise operating systems, which are adding new capabilities designed to support cloud implementations. A prime example is Microsoft Windows Server 2012, which arrived late last summer with a number of new features for the cloud.

Organizations that adopt the updated operating system can take advantage of embedded tools for automatic management and self-service provisioning of shared processing and storage resources. Windows Server 2012 also simplifies the management of hybrid clouds by creating secure ties between private and public cloud services.

For example, with Identity Federation, Windows Server 2012 maintains security for applications that reside either on-premises or in the cloud. It accomplishes this through central authentication and authorization services, according to Microsoft. In addition, virtual private networks secure communications between data centers and cloud providers.

The new edition of Windows Server 2012 also addresses the growing relationship between clouds and mobile workforces through virtual desktop infrastructure (VDI) technologies. These VDI capabilities deliver a Windows environment, running in the data center, to mobile devices such as tablets and notebooks.

can closely align spending with actual usage rather than rely on estimates that may result in unnecessary costs.

Cloud-based solutions for business continuity and disaster recovery offer similar economic advantages, plus one additional benefit. During times of tight budgets, organizations may understand the importance of continuity and disaster recovery, but struggle to justify duplicate resources that run in standby mode without providing value during normal, noncrisis situations.

Rather than investing in dedicated equipment that mirrors the production environment, organizations can contract for cloud continuity and disaster recovery solutions that avoid these capital costs. Such cloud-based solutions also offer the advantage of sending critical data to a distant location that likely won't be threatened if a local or regional disaster hits the home office.

Big data is a big deal for many today. This umbrella term describes the phenomenon of digital information that's being created at a blistering pace and in a wide variety of formats. For example, the latest *Digital Universe Study* by IT research organization IDC estimates that 1.8 zettabytes (that's 1.8 trillion gigabytes) of data were created in 2011 alone. IDC adds that data volumes will expand 50 times by the end of the decade.

Cloud solutions promise more than just a way to manage the volume, variety and growth rates of electronic information. The right on-demand services can offer data aggregation and analysis tools to slice and dice vast reserves of information. For example, this could help outdoor-equipment manufacturers better predict the performance features that enthusiasts will crave for trail bikes next year, or help government social-service agencies understand what programs are most effective in reducing recidivism rates among recent parolees.

Whether the payoff is increasing sales, boosting customer loyalty or improving public safety, effective big-data strategies can help organizations perform their duties more effectively. Turnkey applications delivered as a SaaS solution, or IaaS resources that support an organization's industry-specific analytics, give IT managers two important options for shortening the time it takes to reap big-data benefits.

Hybrid Delivery Models

Hybrid clouds are blurring the traditional boundaries between public and private models for good reason — they give organizations greater flexibility to maintain in-house control of mission-critical resources while also providing a safety valve for fast access to outside services when additional computing power and storage capacities are necessary. But integrating and managing public and private clouds is still a work in progress.

Among the challenges is a lack of standards that apply to both public clouds and internal legacy applications, needed to facilitate smooth collaboration between these two environments. As a result, IT administrators need new or upgraded management tools that treat internal and external IT services as one large pool of resources.

These tools must cut across different architectures to help organizations migrate information and applications across hybrid environments. Security is another concern. New rules and governance mechanisms must be in place to regulate and protect data and programs that span on-premises and on-demand systems.

New Management Challenges

When evaluating cloud services, the IT team should look closely at the vendor's track record for keeping pace with the evolution of cloud management tools. Without the latest controls, customers may not be able to fully benefit from a cloud's ability to dynamically allocate resources.

/// THE BEST CLOUD IMPLEMENTATIONS EXHIBIT SELF-HEALING CHARACTERISTICS. \\\

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.

For example, the best cloud implementations exhibit self-healing characteristics. If one component, such as a virtual machine or a blade server crashes, management controls should be in place to automatically move affected workloads to alternative virtual or physical machines. This relieves IT managers from having to constantly monitor IT control panels to step in when problems occur.

Similarly, some specialized tools automatically keep workloads evenly balanced, guarding against performance problems if one set of servers or memory resources becomes overtaxed while other resources are running below their optimal utilization rates. Leading cloud management tools can even reassign workloads as demands change throughout the day. As a result, a virtual machine may run on a high performance server during regular business hours, but automatically migrate to less powerful hardware at night when demand levels drop. ■

Migrating to the Cloud

Achieving maximum return on investment requires preparation.

In their own ways, public, private and hybrid clouds offer fast access to necessary IT resources without the expensive and time-consuming procurement processes that can plague on-premises implementations. But to fully take advantage of cloud computing, IT managers must avoid haphazardly contracting for individual services and instead create a cohesive plan for moving to the cloud.

That starts with building a solid onsite foundation and then layering on appropriate on-demand applications, infrastructures and development platforms.

Virtualization – Laying the Foundation

Technically, virtualization isn't mandatory for moving to the cloud. But from a practical standpoint it creates a foundation that IT managers can build on from the start and that will support cloud implementations as they grow over the subsequent months and years. The reason: virtualization is an effective first step toward embracing the core cloud characteristics of dynamic resource pools and on-the-fly allocations.

Virtualization accomplishes this by cutting the traditionally close ties between physical equipment and related software, data and operating systems. And today, administrators can apply virtualization to a wider than ever range of data center components, including servers, end-user clients, storage systems and networking capabilities.

Abstracting and aggregating these resources ushers in easy load balancing to keep utilization rates at optimum levels, as well as the ability to shift workloads easily to address constantly changing resource requirements. For example, in a highly virtualized data center, IT managers can quickly shift a workload from virtual machines to virtualized storage systems should the need arise.

Once IT managers button down these agility-enhancing capabilities within their main data center, it's a small step to creating shared resources in a private cloud to support core applications or connecting with a public service for applications, infrastructures and development platforms.

To understand the potential of virtualization, consider its impact on enterprise servers. Although actual numbers vary according to a variety of factors, IT managers in some cases have achieved large-scale consolidation of physical servers at ratios as high as 20 virtual servers to one physical machine. Not only does this level of consolidation significantly reduce capital spending for hardware, additional cost benefits are reaped through lower power consumption and reduced management overhead.

Storage virtualization offers similar benefits. 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. With fewer dedicated disks, it's easier to manage capacity and optimize storage utilization.

Today, many organizations are taking virtualization even further. For some, that means 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.

For IT administrators, desktop virtualization eases upgrades, patching and policy enforcement. For users, it supports access to needed IT services and data, regardless of the device they are using. That opens up opportunities to access the same data and applications remotely as in main offices.

Similarly, application virtualization turns physical applications into virtual services that run in isolation from one another and underlying operating systems. As with desktop virtualization, the IT staff can manage each virtual instance of an application from a central console.

Licensing and Cloud

Moving to widespread virtualization and the cloud requires organizations to consider a range of new questions, such as how does migrating from traditional environments effect licensing for software and applications? The answers aren't clear-cut because many vendors of virtualization software, operating systems and business applications insert some unique requirements into contracts that cover virtualized and cloud environments. This lack of clarity prompts many IT departments to seek help from outside experts to stay compliant.

For example, CDW's Software License Manager is a free service that keeps track of software licenses and versions, plus contract start and end dates. The CDW Software Asset Manager subscription service offers these capabilities along with visibility to all IP-addressable hardware and software on the network.

A Realistic Migration Strategy

As best practices for private and public clouds continue to evolve, IT managers have a broader range of choices about what applications and services are most appropriate for moving to the cloud. For many organizations, the best option is a staged approach that starts with general-purpose business services and then moves to business-critical applications.

For example, almost any type of organization can benefit from cloud-based e-mail systems or business automation suites with word processors, spreadsheets and presentation applications. Activities in the application development department are good initial candidates because 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.

Migrating these types of common enterprise applications and services to the cloud can be approached as something of a pilot 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 can lay the groundwork essential for the gradual rollout of a cloud strategy.

Having achieved positive results with a pilot, the organization can move on to more complex types of services, such as large-scale unified

5 STEPS TO OPTIMIZE A DATA CENTER FOR CLOUD

For most organizations, the question isn't whether to adopt cloud computing, it's how quickly. If it's a given that clouds are here to stay, IT managers can make some immediate design changes to optimize their existing data centers with clouds in mind. Here are five fundamental moves:

1. **INCREASE SERVER VIRTUALIZATION RATES** | By extending virtualization, IT managers will see an even greater payoff in reduced expenses and higher utilization rates for physical equipment. They'll also be well-positioned to easily move data and applications to both private and public clouds.
2. **ADOPT STORAGE VIRTUALIZATION** | Many of the same benefits, including easy provisioning to clouds, accrue with virtualized storage systems.
3. **UNIFY STORAGE** | These solutions support both block and file storage, along with relevant protocols, all in one unit. RAID, load balancing and management tools are other common features of unified storage solutions, allowing IT managers to optimize storage while purchasing and supporting fewer devices.
4. **VIRTUALIZE NETWORKS** | Software-based switches create opportunities for hardware consolidation and dynamic resource allocations, which go hand in hand with cloud strategies.
5. **TAKE ADVANTAGE OF DATA CENTER FABRICS** | These solutions bring servers, networks and storage systems together in a cohesive framework. This gives IT administrators central control over physical, virtual and cloud environments and makes it easier to manage pools of shared resources.

communications and collaboration, business continuity/disaster recovery, and customer relationship management (CRM) systems. As the organization gains trust in the cloud model and its service providers, it may move to more mission-critical services, such as third-party data center infrastructures and enterprise resource planning (ERP) applications, including core accounting programs.

How can IT managers best determine what moves to the cloud and when? Start with an inventory of the organization's entire applications portfolio and then factor in any additions expected over the next two to three years. With this lineup in place, organize and prioritize each item according to what must remain in-house because of security or performance concerns.

Some mission-critical applications that support core enterprise processes might need to remain on dedicated resources. Other questionable cloud choices include programs that pull information from multiple databases or those that would require significant modification to benefit from migration to the cloud.

Key considerations include each application's interface and whether it remains generally unchanged over time. The most obvious cloud candidates have static, easy-to-use interfaces and are programs that run on industry standard platforms and commodity hardware.

By contrast, interfaces that are frequently tweaked or revised can add complexities that make dynamic provisioning and self-service access difficult. Similarly, highly customized applications that are frequently upgraded may not be the best fit for commodity-oriented cloud settings, whether private or public.

Next, assess the possible cost benefits of running these programs in a cloud. Applications or services that will likely see the fastest investment returns after a cloud migration should be at the top of the list.

In addition, consider applications with similar service-level requirements. Supporting a large range of SLAs may increase management overhead and drive up costs. Other considerations are services that must scale rapidly to accommodate changing conditions or those with variable workloads.

Sometimes, an organization will face a trigger event that can speed its cloud decision-making. Such events may include the launch of a new business process, an expansion of the organization's services or a large-scale hardware or software upgrade, such as an upgrade to the new Windows 8 operating system. Consider a cloud-first policy to make sure this option is at least considered during any project definition process.

Network Planning

Developing a game plan for migrating applications and services to private or public clouds isn't the only challenge IT managers face. For either deployment model to work effectively in a real-world setting, network connections must be in place to keep communications running smoothly between clouds and end users. Any bottlenecks or breakdowns in network and Internet connections will have a direct effect on cloud performance.

That makes upfront planning and assessment of the current networking infrastructure essential. Begin network evaluations by considering capacity. Estimate likely traffic volumes to and from the cloud based on the number of expected users and cloud servers that will be running. Then judge whether the existing infrastructure is at its upper limits for accommodating these volumes or whether there's room for growth. Schedule upgrades as necessary.

Next, evaluate network speed. High-speed pipelines, such as 10-Gigabit Ethernet, and broadband Internet connections are a must for many cloud applications.

Strengthening IT Governance

The need for strong IT service management and governance becomes even more important in the cloud model, primarily because IT managers dynamically provision services instead of tying them to dedicated physical resources in the enterprise infrastructure.

Organizations that have not embraced IT service management will want to do so as a preparatory step in their migration to the cloud. Fortunately, they have help: The IT Infrastructure Library framework provides formal guidance for identifying, planning, delivering and supporting IT services to the organization.

In addition to best practices, ITIL offers an extensive list of resources designed to help organizations in a wide range of cloud areas. This includes service delivery best practices that aid the transition to dynamically provisioned services.

The ITIL framework also 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 retire virtual machines.

Learning to Manage Change

Cloud computing has always represented change — for end users and how they access applications and services, as well as for the IT staff itself. For many IT professionals, cloud computing and its self-service model can upend established practices and appear threatening. Common concerns include loss of administrative control over service delivery, increased operational workloads and loss of "ownership" of IT resources as computing, storage, database and network resources are all wrapped up and delivered as a service, rather than managed separately.

But none of these need be deterrents. Senior IT leaders should make training a high priority for IT teams as well as for end users as the organization makes its move to the cloud. ■

Private Clouds, Uninhibited Value Proposition

Enabling broader operational gains begins with cloud computing.

For many organizations, their initiation into cloud computing begins with a private cloud — and for good reason. Not only do private clouds deliver on the business and technical benefits promised by the cloud model as a whole, but the returns also come without IT managers having to address the possible risks of sending sensitive information to third-party service providers.

By keeping servers, databases, storage systems and applications private, the IT department can demonstrate how clouds work to skeptical business managers and senior executives and help alleviate any concerns they may have. Over time, the organization can expand its cloud strategy to include public and hybrid models where appropriate.

Beyond this proof-of-concept characteristic, what is there to like about private clouds? The short answer: a lot.

According to industry analysts, more than 70 percent of data center budgets are typically devoted simply to maintaining the existing hardware and software. That includes routine service and maintenance, regular software updates and myriad management duties. This leaves little money or staff time for developing the exciting and potentially game-changing innovations that can help organizations grow and provide better service.

Private clouds can change this. Some organizations report that private clouds significantly reduce the managerial overhead associated with traditional data centers. This and other streamlining opportunities can shrink the costs of routine maintenance to less than 50 percent of the total IT budget, which potentially represents enterprisewide savings of hundreds of millions of dollars for large organizations, according to some reports.

But the benefits of private clouds go beyond just saving money. Savvy organizations plow their newfound cash reserves back into IT operations for investments in new initiatives, such as mobile applications, that can have an immediate positive effect on worker productivity and customer service.

Ready to Serve

Financial considerations aren't the only incentives for adopting private clouds. The strategy also enables IT departments to create a services approach that lets staff dial up technology resources from a service catalog. These on-demand services mean IT administrators can more quickly address the changing demands of workers by avoiding the extended time and capital expenses associated with purchasing new equipment and then testing and moving it into a production environment.

Traditional implementation processes like these can mean that end users don't see the new capabilities they need for weeks or months. Private clouds can shrink that timeframe into days or hours with pools of IT resources that stand ready for provisioning.

Private clouds also provide a reliable technical framework for what some industry observers are calling the post-PC era. As organizations seek greater agility by expanding the mix of end-user devices, they're combining traditional desktop PCs with all-in-ones, notebooks and ultrabooks, thin clients, tablets and smartphones. Private clouds can deliver essential information and applications from a centrally managed location to any type of hardware a staff member may need to use to work more effectively.

Organizations that adopt a private cloud may also find their resources are more available than in traditional data center settings. That's because clouds incorporate self-healing tools that help operations continue normally, even if individual components in the cloud encounter problems.

For example, if one of the physical servers in a private cloud crashes, management tools can spot the problem and automatically move the workload to another server in the cloud's resource pool. In addition to achieving higher levels of business continuity, this level of flexibility and automation ensures that IT managers don't spend all their time worrying about the health of core components, such as servers, storage systems and memory reserves. Instead, they can have their staffs apply technical expertise to more strategic activities.

Security in the Cloud

Industry surveys show that, right or wrong, security remains one of the primary holdups for more widespread adoption of cloud services. Private clouds can alleviate many of these concerns and also address some knotty challenges that arise over regulatory compliance.

Private clouds mitigate security fears for a number of reasons. First, if the cloud is on-premises, data doesn't travel to and from end users and the cloud via public networks. So there's less chance that unauthorized people can steal information during transport. Similarly, because data doesn't reside within a third-party provider's data center, IT managers aren't required to perform extensive upfront security audits and ongoing assessments of the service's security activities.

Second, public clouds typically allow all the various cloud clients to share resources in a multitenant service model. For example, this means that two competitors in the retail industry may theoretically store customer data in the same public cloud database.

HOW CDW JUMP-STARTS PRIVATE CLOUD IMPLEMENTATIONS

Private clouds may ultimately reduce complexity for data center operations, but achieving that goal isn't always easy. For help, IT organizations can tap the expertise of CDW and its certified data center architects, who can assist with every phase of choosing and leveraging the right solutions. The approach includes:

- **DATA CENTER WORKSHOPS** | The cornerstone of the CDW Private Cloud Accelerator engagement, this half-day session with a data center architect provides a technical discussion of today's data center optimization technologies and best practices.
- **DISCOVERY WORKSHOPS** | Based on information gathered in the Data Center Workshop, CDW will recommend a series of Discovery Workshops to capture a complete and accurate picture of an organization's current data center environment. Discovery Workshops are led by solution architects highly specialized in the topic areas. The solution architects will document and address performance issues and inefficiencies in the current environment and offer advice for optimizing the infrastructure.

/// PRIVATE CLOUD SAFEGUARDS EXIST ONLY IF THE I.T. STAFF IS WELL-VERSED IN THE LATEST SECURITY PRACTICES AND TECHNOLOGIES. \\\

Finally, many organizations must comply with various information security standards, such as the Payment Card Industry Data Security Standard (PCI DSS) for accepting credit or debit card payments, or the Health Insurance Portability and Accountability Act (HIPAA) for protecting health information. In other cases, public-sector agencies and commercial organizations may be required to store critical information within domestic geographic regions. With private clouds, IT managers can ensure that compliance requirements are met and easily gather data necessary for reports to auditors.

Of course, these private cloud safeguards exist only if the IT staff is well-versed in the latest security practices and technologies. That may not always be the case, even in an IT department with a deep bench of expertise. The reason: security threats and best practices are constantly changing. And in some cases, the dedicated resources available in public clouds may actually be better able to protect sensitive information than a client's own IT administrators.

But for many reasons (from financial and reliability benefits to security controls) private clouds remain one of the most popular options for organizations that are actively moving to cloud computing. In fact, the private cloud market is poised for compound annual growth of 21.5 percent through 2015, according to a recent report, *Private Cloud Computing Market & Forecast to 2015: Worldwide Analysis* from Renub Research.

Cloud in a Box Takes Off

What's new with private clouds? Most significant, they are becoming easier to design and launch than ever before. One reason is cloud in a box, or the converged infrastructure option.

These solutions enable IT managers to acquire all the necessary computing, storage, virtualization, network and management components necessary for a private cloud as a single integrated product that's already been certified to work together properly. A number of these exist, including Vblock, from the Virtual Computing Environment (a joint venture of VMware, EMC and Cisco Systems); FlexPod, from Cisco Systems and NetApp; IBM CloudBurst; and HP CloudSystem.

The benefits are becoming clear. For example, one cloud service provider's management team chose to implement a private cloud using VCE's Vblock. In addition to helping the organization launch the private cloud quickly, the precertified solution saved time and effort in the long term.

In the past, patches might have arrived at different times for EMC, Cisco and VMware technology — it was up to the service provider to understand how each patch worked with the other patches. Those complexities are now gone because VCE sends one patch that incorporates all the updates from the three members of the joint venture. Similarly, the service provider needs to contact only one manufacturer representative if a performance problem or service issue arises.

Whether the IT manager chooses a cloud-in-a-box solution or assembles

the components separately, a clean-slate approach to building private clouds avoids many of the technical incompatibilities that arise when trying to piece together legacy equipment and software. However, building from scratch isn't always feasible financially, leaving the IT department tasked with finding ways to use legacy infrastructure as a foundation for the private cloud.

That's not necessarily bad. In addition to maximizing existing investments, this situation also allows IT organizations to gradually build out the private cloud in a step-by-step process that starts with virtualization and then moves to setting up dynamic resource pools and other private cloud capabilities. In this way, staffers can hone their cloud expertise while end users grow to understand how their department can benefit from the agility and business efficiency enabled by private clouds.

Taking Control of the Cloud

It's not enough to assemble the various components of a private cloud and expect that everything will run smoothly from that point forward. IT managers also need orchestration to manage the environments over time and address the changing resource requirements of their organization. As a result, a wide variety of tools are now available from vendors of virtualization technology, as well as in third-party solutions, to help keep private clouds in shape.

These programs typically base their actions on historical information about demand cycles or by monitoring real-world conditions. So if a tool sees that a virtual machine is running low on memory, it can proactively assign additional resources to the affected area.

Once in place, automated orchestration and monitoring solutions can deliver other important benefits. Often, the central management consoles in these tools can significantly reduce the amount of time data center staff must devote to managing and provisioning IT resources.

There are also programs designed specifically for application monitoring in the private cloud. The goal is for IT departments to maintain high availability and reduce service disruptions for applications in virtualized environments.

This is possible because the tools can watch over the application portfolio and send immediate alerts if an application fails for any reason. Depending on the problem, the solution might restart a failed application or work with other infrastructure management programs to ensure that the application fails over to a healthy virtual machine.

Still more tools are available to keep private clouds humming, such as programs that optimize storage systems and facilitate rapid provisioning of storage resources by creating standard images of virtual machine disk files. These files can be reused when new virtual machines are created.

But IT managers must choose their tools carefully — some only work with a particular virtualization platform. Organizations with multiple virtualization technologies need to find solutions designed for cross-platform reach.

Start with a Solid Design

If an organization makes the decision to launch a private cloud, what steps must it take to pull off the plan? Cloud veterans and consultants cite four key moves:

1. **CONSOLIDATE AND STREAMLINE THE DATA CENTER** | By restricting the variety of hardware platforms and running highly compatible hardware, IT managers can more easily achieve the dynamic provisioning and resource pooling goals of cloud computing. The IT department can further its streamlining efforts by moving to blade servers, deploying storage area networks (SANs) and boosting network bandwidth by migrating to 10-Gigabit Ethernet network links.
2. **VIRTUALIZE WHEREVER POSSIBLE** | The immediate return will be a reduction in physical hardware requirements, higher device utilization rates and savings on power costs. Over time, virtualization will provide additional benefits, such as the

HOSTED vs. BUILD YOUR OWN

Weighing the Benefits of Two Paths to a Private Cloud

Hosted Benefits	Build Your Own Benefits
Service-provider management	Control over the infrastructure
Service-provider experience and expertise	Security via preferred technologies
Service-provider handles billing management	Application portability
Cloud bursting option if needed	Customization of apps

flexibility to dynamically provision and reprovision workloads, storage volumes, memory capacities and other resources to quickly address business or mission needs.

3. **IMPLEMENT TECHNOLOGIES THAT AUTOMATICALLY ORCHESTRATE WORKLOADS** | This includes specialized tools that balance the workload among all the individual servers in the private cloud while ensuring that each application has the power it needs to meet existing demands.
4. **DETERMINE WHICH APPLICATIONS ARE RIGHT FOR RUNNING IN A PRIVATE CLOUD** | Although hard-and-fast rules don't exist, one common practice is to use private clouds for common business services, such as e-mail systems, which do not require the full power of dedicated servers and related resources. More complex applications or those that are upgraded frequently may run best on their own dedicated resources.
5. **IMPLEMENT SERVICE METERING** | A key characteristic of clouds, both public and private, is self-service provisioning of resources and service metering. Catalogs show users what IT resources are available from the cloud, display their associated costs, and then give users a way to quickly procure the right resources in the right volume for their needs. Metering shows the ongoing costs of these services based on usage, which gives individuals, the IT department and the financial department a clear understanding of IT expenses.

/// PRIVATE CLOUDS REQUIRE NEW SKILLS AMONG THE IT STAFF. \\\

When a Private Cloud Isn't the Answer

Although private clouds have a lot to offer, they aren't right for every organization. Before making a move, IT managers should carefully evaluate a handful of practical concerns that may ultimately become deal breakers for a private cloud.

Network connections are often the weak link in cloud performance. Any interruption in these pipelines could bring operations to a standstill. Organizations should be prepared to invest in high-speed networks, such as 10-Gigabit Ethernet.

Data management is another concern. Large data sets can quickly overburden available bandwidth on some network segments. IT shops that are considering placing applications with large data sets in a cloud need to guard against these performance degradation issues.

Private clouds require new skills among the IT staff. Technical personnel should be well-versed in virtualization and cloud concepts, such as IT service delivery and multitenancy architectures. Hiring these workers and keeping their skills up to date is expensive, and there are no guarantees of a lengthy tenure from them as long as demand is high for these services.

Finally, security is never a subject to gloss over. 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 mean organizations need to continuously invest in personnel and technology to protect digital assets. ■

Going Public: Cloud Services

A variety of options are available among public cloud services.

Establishing public cloud services is a relatively easy undertaking. Once an SLA is nailed down and any data-integration steps are completed, organizations can quickly benefit from a host of new on-demand IT services. This helps explain why public clouds are growing at unprecedented rates.

Citing new data by the technology research organization IDC, eWeek reports that worldwide spending for public IT cloud services could surpass $40 billion in 2012 and hit almost $100 billion by 2016. IDC also forecasts that from 2012 to 2016, these services will experience a compound annual growth rate of 26.4 percent, roughly five times higher than what the IT industry as a whole will record.

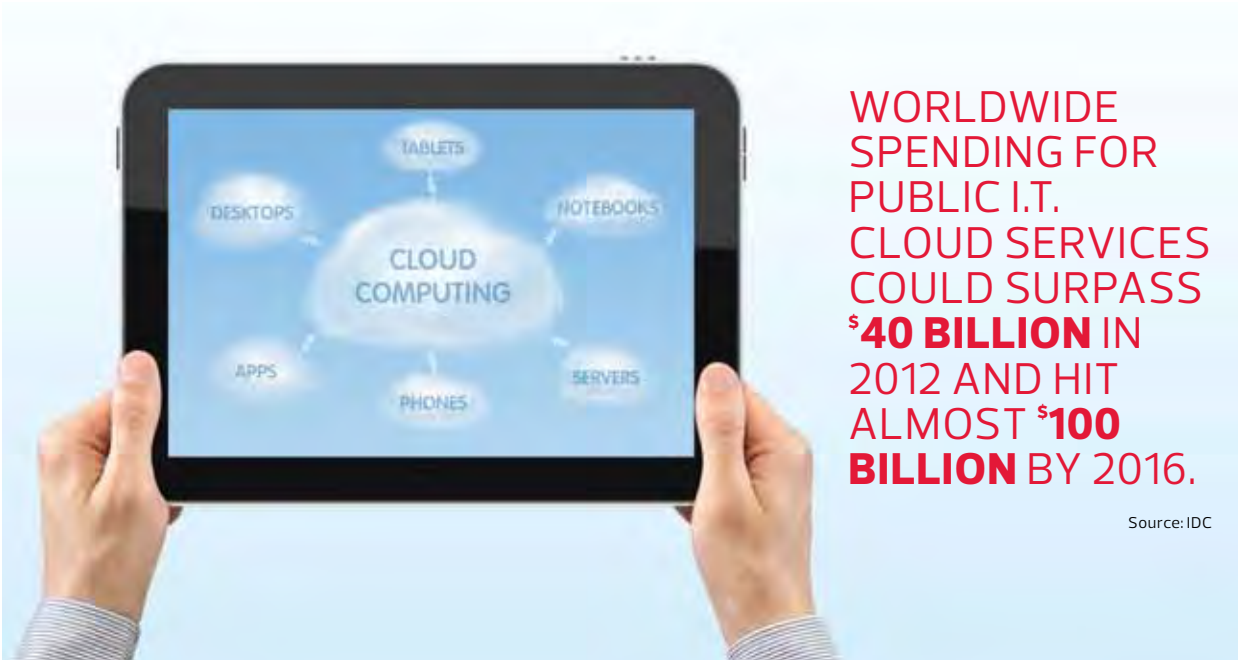
What else is fueling such high adoption rates? Other drivers include the diversity and flexibility of today's public clouds. These characteristics give organizations new opportunities for subscribing to the latest versions of many enterprise applications, connecting to almost limitless data center resources or tapping into the latest development platforms. Here's a look at three main options IT managers can choose from.

OPTION 1: Software as a Service

SaaS solutions deliver full versions of business applications on demand, typically through a web browser. SaaS eliminates the need for many costly infrastructure expenses related to hosting an application on-premises. As a result, organizations can take advantage of highly mobile SaaS applications to increase the productivity and collaboration opportunities of workers who use the software.

In addition, members of the IT department benefit because there are no related servers or applications to maintain. Add to that the fact that the subscription model offers a predictable cost structure and less complex licensing issues, and it's easy to see why SaaS sells.

Popular SaaS solutions include business productivity applications, such as Microsoft's Office 365 and



WORLDWIDE SPENDING FOR PUBLIC I.T. CLOUD SERVICES COULD SURPASS **$40 BILLION** IN 2012 AND HIT ALMOST **$100 BILLION** BY 2016.

Source: IDC

Cisco's WebEx web conferencing platform. Other options available via the SaaS model range from security solutions for protecting e-mail and filtering web traffic to systems for IT management, mobile device management, unified communications and collaboration, and backup programs.

Along with providing the latest capabilities in these software categories, SaaS can enhance agility and productivity by enabling IT departments to roll out new functions quickly, and do so within a predictable cost structure. For example, hosted e-mail security and web filtering solutions remove the burden of dedicated infrastructure expenses and ensure that an organization is always running the most up-to-date protection. Hosted management software allows for hassle-free deployment, particularly with remote offices.

OPTION 2: Platform as a Service

PaaS solutions not only encompass resources for the underlying IT infrastructure, they also deliver all the development tools required to build and deploy cloud applications. Microsoft Azure and Force.com (from Salesforce.com) are two popular PaaS solutions.

PaaS provides improved accessibility to platforms and tools that can make an organization more agile and productive, speeding the time it takes for IT departments to deliver new or modified applications to users or customers. There are no upfront infrastructure costs with PaaS, and the ability to scale the solution as necessary can bring additional value to organizations.

PaaS-based application integration tools also reduce complexity for users by integrating cloud and on-premises applications. Finally, PaaS resources are available to handle the creation of business intelligence (BI) applications, such as databases, dashboards, reporting systems and data analysis systems.

OPTION 3: Infrastructure as a Service

IaaS solutions consist of computing, storage and networking resources delivered on demand as a service. IaaS also is highly flexible and scalable, so an organization's infrastructure resources can grow to meet constantly changing needs. Top solutions include CDW's colocation and managed services; Verizon's Terremark; Time Warner's NaviSite; and CenturyLink's Savvis.

The benefits of IaaS are greater cost predictability and increased organizational agility through rapid scalability. IaaS service providers deliver pay-as-you-go processing power, dynamic storage capacity and almost limitless reserves of network bandwidth. This means organizations can provision as little or as much additional service as they need at any given time without facing resource shortages.

Just as important, IT managers can scale back IaaS capacities when demand subsides, so the organization never pays for unneeded resources. This is a welcome change from traditional IT procurement practices, in which hardware had to be ordered, delivered, installed and tested, and often extra underutilized capacity had to be

IaaS FLAVORS

7 Popular Infrastructure as a Service Offerings

Compute as a service	Provides compute capacity including servers, OS access, firewalls, routers and load balancing
Web hosting	Provides website hosting, high performance during peak traffic and load balancing
Storage as a service	Provides easy storage provisioning, transferring of data to tiered storage options and easy addition and removal of storage
Disaster recovery and backup as a service	Provides uninterrupted access to data and apps, may offer continuous data protection
Desktop as a service	Provides hosting and serving of virtual desktops, allows for quick provisioning, access, running and deactivation
Servers as a service	Provides access to short-term extensive compute power
Networking as a service	Provides networking resources on demand, such as firewalls, load balancing and WAN acceleration services

kept on hand for demand spikes.

Along with scalable computing power, IaaS can quickly bring flexible storage capacity on line. 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.

IaaS also extends to networking and security resources. One leading managed-network services provider offers monitoring and management support for both wide area networks and local area networks. The best solutions will provide services for the initial design as well as for implementation, security and 24-hour management support.

Finally, newer IaaS solutions offer a fast track for desktop virtualization. They enable organizations to rapidly deploy virtual desktops to end users and allow them to access data and information via any device with a network connection. These options also provide a secure, centralized management environment and inherently solve the challenge of disaster recovery at the network endpoint.

4 Apps That Deserve a Closer Look

As public cloud offerings become more mature, organizations are turning to this option for some vital enterprise IT applications and resources that used to be dedicated exclusively to on-premises solutions. For example, cloud-based ERP is attracting a growing number of converts. The reason: Cloud essentials such as dynamic provisioning help IT departments match the changing resource needs of end users.

Clouds also make it possible to implement an additional ERP module within the suite in a matter of hours or days if a new business demand or challenge arises. This all happens without expensive and time-consuming procurement cycles or strains on the capital budget for new servers and associated technology. And once the ERP application is running, updates, security patching and other duties fall to the service provider, not the IT department.

The challenge is to make sure a cloud-based ERP provides all the functions and reliability the organization requires. Choosing a mission-critical system, such as ERP, may require extra comparison shopping and due diligence to ensure that the service provider can deliver on its promises.

IT managers should clearly document costs for both standard and premium services, nail down uptime guarantees and discuss the penalties the service provider would face if the SLA isn't met. Organizations might also explore whether it's possible to customize the basic ERP platform — and at what cost — in addition to what services the provider offers for integrating the on-demand solution with related on-premises applications.

As more organizations understand the power of sharing ideas and information, they also realize the value of cloud-based unified communications and collaboration implementations. These solutions overcome the time, expense and integration challenges of on-premises projects designed to tie together conferencing and video, telephony, instant messaging and e-mail systems. The Cisco Hosted Collaboration Solution is a leading provider of such services.

IT managers should evaluate cloud-based UCC alternatives for their ability to help users seamlessly collaborate using any available communications channel. The solutions should also simplify access

CDW: A TRUSTED PARTNER *FOR PUBLIC CLOUDS*

Whether SaaS, IaaS or PaaS, CDW has long-standing partnerships with top cloud services providers. In addition, our internal staff of cloud experts can aid with vendor evaluation, proof of concept, deployment and migration. Start learning more about CDW's SaaS, IaaS and PaaS solutions: **CDW.com/cloud**

to information by displaying all messages within a single interface.

In addition, the best UCC systems should let users access messages anywhere, any time and on any device, especially mobile devices. Finally, the cloud-based option should enable IT departments to support collaboration without compromising security.

Clouds are also being tapped for disaster recovery. Cloud-based backup services can reduce the costs of investing in duplicate, often underutilized, systems that provide value only when disaster strikes. By contrast, the cost for many cloud-based DR systems is limited only to data storage when the organization is operating normally. In addition, the cloud model offers a quick way to establish resources for offsite data replication.

Cloud-based security services let organizations offload the responsibility for launching and maintaining security to a third-party cloud host. Because SaaS service providers specialize in security, organizations can take advantage of expertise that may run deeper than what their in-house IT department can provide. And because these experts are dedicated to security, they are more likely to be aware of the latest threats and best practices.

These capabilities come with the advantage of predictable costs. Organizations pay set monthly fees, typically calculated on a per-user basis, and avoid the upfront capital expenses for hardware and software required for in-house solutions. Organizations are also insulated from unexpected expenses associated with a new and emerging threat.

Considerations Before Signing a Contract

Public clouds may offer a host of performance, financial and practical advantages, but finding the right solution requires careful analysis of the computing model's strengths and weaknesses. One of the most fundamental considerations is whether the multitenancy architecture of a public cloud is the right choice for a particular environment.

With multitenancy, multiple customers share the same servers, applications, databases and storage resources. Technologies exist to wall off these customers' assets securely, but success depends on how well a service provider actually implements and manages these safeguards. This question is enough to make some executives skeptical about public clouds, especially for use with highly sensitive or regulated information.

Security fears are understandable, but one of the promises of the public cloud is that offloading some IT management responsibilities to

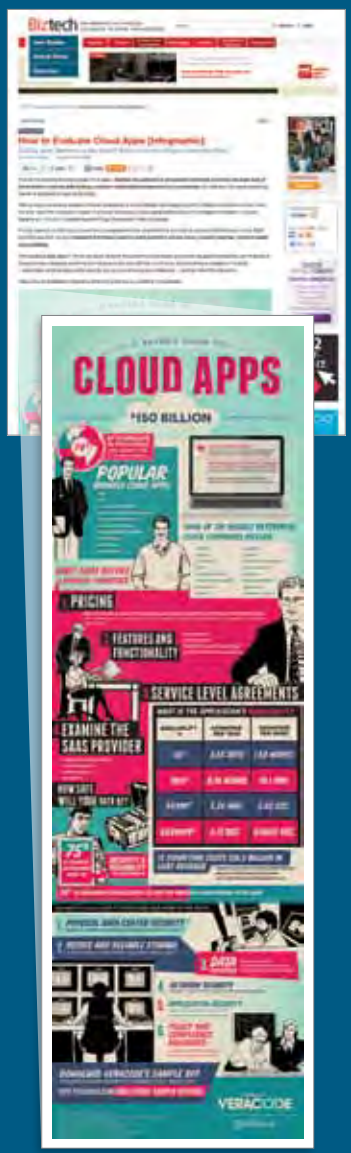
8 QUESTIONS TO ASK BEFORE YOU SIGN AN SLA

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

INFOGRAPHIC
EVALUATING CLOUD APPS

This colorful infographic from Veracode offers some great tips on determining if a cloud app is right for your organization:

CDW.com/cloudguide2



SOURCE: Veracode

outside specialists can, under the right circumstances, actually improve the overall security stance. So how can IT managers bridge the gap between healthy skepticism and public cloud acceptance? The answer is to develop a security strategy tailored for public clouds (for details, see Chapter 6).

Organizations also fear locking data into a single vendor's cloud infrastructure and data formats, which could make it difficult to quickly switch to another provider if problems occur. Along these lines, some IT managers also struggle with nuts-and-bolts technology issues associated with public clouds. The answer to both fears is due diligence.

For example, using an outside service provider makes an organization completely reliant on the provider's network connections. This means any performance glitch in the network could bring down important enterprise operations.

High-speed WAN or Internet connections are a must for ensuring that users receive the performance levels they need. IT managers should analyze traffic to and from 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.

Do the Numbers Add Up?

When evaluating public clouds, IT managers need to assess the costs of these flexible services versus traditional on-premises solutions. The first step in doing this is to understand the costs of the legacy environment. The IT department must look beyond the infrastructure's capital investments in hardware and software and factor in expenses for IT personnel, service and support activities, upgrades, maintenance activities and facilities costs, including power and cooling.

Similar sleuthing is required to understand the true costs of a public option. In this case, dig deeper than just the top-level subscription fees when comparing expenses with on-premises solutions, or when evaluating one service provider's proposal against that of a competitor. Hidden costs may include investments needed for any necessary internal upgrades, such as faster network connections.

Also, IT managers should make no assumptions about what a provider will deliver as standard service. If something isn't specifically spelled out in the SLA, it's likely an option that may accrue an extra cost. For example, disaster recovery solutions often set a standard price for backing up and storing data, but then layer on extra charges if a client needs to recover lost information or run in backup mode until production systems are restored.

Cost comparisons will help uncover the potential payback of a public cloud solution, but IT managers shouldn't base their entire assessment on financial considerations. Public clouds may deliver value in other ways that may ultimately be more important than day-to-day costs.

Enhanced business agility that helps establish a foothold in a new market, the ability to provide public services more efficiently in the aftermath of an emergency, or greater assurance that mission-critical systems will always be available may be the most compelling reasons to embrace public clouds. ■

7 Heaven: Steps to Cloud Security

Security in the cloud isn't a problem if adequately planned for.

Cloud computing has long struggled with an image problem — not that clouds aren't actually efficient or scalable or don't provide a new way for IT departments to rein in capital expenses. The sticking point for many organizations has been (and still is) a deep concern about cloud security.

However, data about public and private cloud adoption rates — which show annual growth percentages of 26.4 and 21.5, respectively (per data from IDC and Renub Research) — indicate that organizations are coming to terms with their cloud security fears.

But many prudent IT managers still keep close tabs on this area. In fact, when technology researcher IDC recently asked IT executives to rate their organization's concerns about the risks associated with cloud deployments, 86 percent put data security and privacy at the top of the list. Close behind were concerns about compliance and security governance, as well as identity and access management.

Fortunately, IT departments have more resources than ever to mitigate security threats. The keys are careful research when investigating cloud service providers and ongoing diligence to assure that data and applications stay safe once they're running in the cloud. Here are seven problem areas that deserve special attention.

1. Safety in Numbers?

SECURITY PROBLEM | Multitenancy strategies and cloud computing are joined at the hip. Whether in private implementations or in public cloud services, the ability to create common IT resources that are shared by multiple end users is essential for keeping costs low. But this model raises some fundamental questions about how to safely wall off sensitive information from unintended data leaks or outright intrusion attempts by other tenants.

SOLUTION | The concerns are valid, and they should provide a framework for lengthy discussions with cloud providers about security policies and practices. Due diligence includes getting documentation about the specific methods that assure separation of data and resources.

It's also important for customers to understand a provider's formal response plan if an internal or external threat arises. Finally, confirm with service providers how they use virtual LANs to further separate the activities of multiple customers in the same cloud.

2. Keeping Sensitive Data Close

SECURITY PROBLEM | A cloud customer's internal governance policies (and in some cases, formal regulatory controls) require that special care be given to sensitive or classified data, and that clear audit trails be created to show who accesses the information.

SOLUTION | Organizations should be selective about what information they store in the cloud. Easy choices are cloud-based services for nonessential resources, such as web servers that support information that's already openly published online. Other obvious cloud candidates include business automation applications, development and testing

resources and e-mail systems.

IT departments can comfortably adopt cloud solutions for these areas without incurring unnecessary risks. By contrast, organizations should carefully consider the security ramifications of moving financial information, personal data about customers or constituents and intellectual property to a public service.

In some cases, IT managers must also determine whether the data will physically reside in a domestic data center or an offshore facility. Get appropriate guarantees if organizational policies or legal requirements mandate that resources stay within the home country's boundaries.

3. Encryption Is Key

SECURITY PROBLEM | Without proper controls, sophisticated hackers can intercept communications flowing across wide area networks, which could jeopardize data as it travels to and from cloud customers and providers.

SOLUTION | Take advantage of strong encryption technologies to scramble data into unrecognizable bits and bytes while in transit and after it's reached its destination in the cloud. In addition to offering encryption capabilities, cloud providers should also establish dedicated virtual private networks to further secure communications.

4. Security for the Long Term

SECURITY PROBLEM | Merely understanding a cloud provider's established security policies and technologies doesn't give a clear picture of how competently and diligently the provider will manage those practices on a daily basis. The result: misplaced trust that could make a cloud client more vulnerable to security breaches.

SOLUTION | Go beyond the initial upfront investigation into the provider's security practices by insisting on reports that demonstrate ongoing compliance. Ask for regular updates for how the service provider keeps security technologies, operating systems, hypervisors and patches up to date.

Also inquire about what security and auditing standards the provider abides by. Common guidelines include the Statement on Standards for Attestation Engagements No. 16, also known as SSAE 16, which covers reporting on controls at service organizations. In addition, the ISO/IEC 27000 series of standards outlines information security standards.

5. Thwarting Drive-by Thieves

SECURITY PROBLEM | Web browsers can be the source of security gaps. A common practice among cybercriminals is to infect websites with keystroke loggers and other malware, which then allow cyberthieves to hijack cloud accounts.

SOLUTION | Web content filters should be in place to monitor Internet traffic for viruses and other security hacks. Content filters closely examine the data packets of all information that streams in through firewalls or proxy servers. The filters analyze the traffic using profile information created to screen out known viruses, spyware and other dangers. IT managers can also work with cloud providers to create blacklists of sites known to be sources of keyloggers or other dangerous programs.

6. Understanding Emerging Threats

SECURITY PROBLEM | Because public clouds contain so much valuable information for so many customers, hackers will increasingly target these implementations as potential jackpots.

SOLUTION | Inquire about the service provider's intrusion detection/intrusion prevention capabilities. These systems use analytics to look for traffic patterns that are a tip-off to the likely presence of a known virus or a hacker.

The analyses can also determine whether customers are accessing data and applications in expected ways or if anomalies warrant a closer investigation. For example, if a database holding sensitive financial data is accessed at 3 a.m., the intrusion detection and prevention system may step into action.

Another frequently used safeguard is a security information event management (SIEM) system, which also applies statistical analysis to probe event logs when monitoring databases, applications and storage systems. If the SIEM solution notices unusual behavior, it can alert cloud administrators and document the activities for subsequent forensic analysis.

7. Avoiding Misunderstandings

SECURITY PROBLEM | Not all cloud security issues are technical. Sometimes gaps arise because of confusion about whether a cloud customer or the service provider is responsible for a particular aspect of security.

SOLUTION | Clearly define roles and responsibilities when negotiating service-level agreements — and don't make assumptions about any security practices. For example, a cloud customer may see that a service is capable of the highest levels of data encryption.

However, the service may only offer this as an option for an additional fee. Comprehensive discussions up front will guard against unpleasant surprises and data breaches in the future. ■

GET AN OUTSIDE OPINION

Third-party auditing firms are becoming an important resource for helping IT managers ensure that cloud service providers maintain high levels of security on an ongoing basis. The technology consulting company Gartner predicts that 40 percent of organizations will require certification of independent security testing by 2016.

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.

Big data

A broad term, big data describes the phenomenon of digital information being created in high volumes, at increasing rates and in a variety of formats.

Broad network access

An essential cloud characteristic, broad network access facilitates network capabilities and their access through standard mechanisms that promote use by heterogeneous platforms. These can include notebook or tablet systems 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.

Consumerization of IT

This term refers to the trend of end users lobbying for familiar and sometimes consumer-oriented hardware and software to use in their jobs, based on the idea that using these familiar technologies will make them more productive.

Desktop as a service

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.

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 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) networking components, such as host firewalls.

IT Infrastructure Library

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

IT Service Management

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

Metered service

Metered 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 consumer.

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, 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 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 users. The organization (or a third party) can manage the cloud, which can exist onsite 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.

Rogue cloud

A rogue cloud is a cloud service contracted by someone outside the IT organization and without IT's knowledge or approval.

Server virtualization

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

Service catalog

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

Service-level agreement

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

Software as a service

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

Unified communications and collaboration

These platforms link voice, video, instant messaging, presence, online chats and conferencing applications together to enhance communications and idea sharing. UC collaboration (UCC) is becoming an important cloud-based solution.

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, including desktop PC, notebook computer, tablet, smartphone or thin client.

Index

ABOUT THE CONTRIBUTORS

NATHAN COUTINHO is an Enterprise Solution Manager for CDW's System Solutions Practice. He has more than 15 years of experience in IT with various roles in consulting, engineering, management and technical sales. He manages a national practice of Data Center Field Solution Architects as well as the strategy and execution for technology labs at CDW. Other responsibilities including evaluating emerging technologies and educating clients on the trends and directions in the market, with a primary focus on big data, business continuity, cloud, data center optimization and mobility. Nathan graduated from Indiana State University with a Bachelor of Science in management information systems.

PAUL SCHAAPMAN is a Data Center 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 mobility is affecting cloud computing strategy
- Navigating today's cloud management tools
- Determining the right apps for software as a service
- Addressing cloud security concerns