CDW·G PEOPLE WHO GET IT™

PRIVATE CLOUD AND SOFTWARE AS A SERVICE

Cloud models deliver the advantages of a shared IT infrastructure, plus the security and control that agencies require.

Executive Summary

Despite the promised benefits of cloud computing and software as a service (SaaS) – greater flexibility and scalability, infrastructure cost avoidance, "anywhere access" to applications and data – concerns about security and governance have made some organizations hesitant to turn over a chunk of their IT systems to a third-party service provider.

But the value proposition of cloud computing is too great and the budgets of public sector agencies are too strained not to explore ways to deploy cloud-based resources and still be able to satisfy an agency's security needs.

Cloud computing enables on-demand access via a network connection to a shared pool of IT resources, including computing power, data storage and applications. Google Mail (Gmail) was an early, prominent example of cloud computing. This e-mail application lived on servers located somewhere in the Internet "cloud" and offered users gigabytes of storage for their messages, attachments and more.

Today, entire enterprise messaging platforms live in the cloud, along with office suites, business management software, unified communications and other enterprise applications. IT departments can deploy such cloud-based systems quickly and easily, add capacity as needed, and pay for the exact amount of application services they need – all without buying,

TWEET THIS!

Table of Contents

configuring, managing and patching a data center's worth of their own servers.

Many of today's most popular cloud-based systems reside in the "public" cloud, meaning any person or organization interested in porting applications and resources to a vendor's cloud system can do so. That vendor's public cloud (including its servers, storage and software) is therefore shared among its customers.

For some IT departments, particularly those in federal, state and local government agencies that are entrusted with the public's information, the idea of running even a portion of their infrastructure on a shared, public platform raises a red flag. However, agencies can still enjoy the considerable IT benefits of cloud computing by moving systems to a "private" cloud.

In a private cloud, pooled resources are not shared with just any paying customer. They may be dedicated to one agency, or to more than one agency in a collaborative arrangement. Similar to a public cloud, a private cloud may exist in a third party's data center, or it may be built in-house, using the same flexible, scalable, virtualized technologies that a cloud provider uses.

Whether an agency chooses to host a private cloud with a third party or build one itself, it must prepare for the migration: from choosing what IT systems can live in the cloud, to virtualizing its assets, to establishing governance processes for securing the cloud and offering its services to agency customers. Only then can the agency realize the myriad benefits of private cloud computing.

Ultimately, once a private cloud is built and working, one significant benefit of such a secure deployment is the ability to roll out additional cost-effective cloud services, including infrastructure as a service (IaaS), platform as a service (PaaS) and SaaS.

The Private Cloud

In the federal government, it is estimated that in fiscal year 2010, 30 cents of every IT dollar was spent on data center infrastructure. Moreover, according to a 2010 survey conducted by the Office of Management and Budget, agencies have been using less than 30 percent of their server capacity.

Those numbers are telling, and they're at the heart of a "cloud-first" campaign to promote the evaluation of cloud computing options by government agencies before making new investments in IT. According to OMB, roughly one-quarter of federal IT spending could move to the cloud.

In fact, government agencies at all levels are exploring cloud computing as a way to better manage IT budgets and infrastructure. In its 2011 report *Case for Cloud Computing in State Government*, the National Association of State Chief Information Officers (NASCIO) stated that "Cloud computing has arrived as a serious alternative for state government."

As government interest in cloud computing grows, agencies' needs for security and control have steered them toward private clouds.

Clouds in General

To understand the concept of a private cloud and how it might securely enable a government organization to align its IT operations with a flexible, services-based approach, it pays to understand cloud computing in general, because a private cloud is a purpose-designed means of achieving the same benefits.

IT systems generally include software, hardware and storage dedicated to an enterprise application. For example, an agency has its e-mail server (with associated storage), its database server (with its storage), and so on.

Over the years, data centers have filled up with single-purpose servers, each requiring maintenance and power. In recent years, to ease the maintenance burden and build more energy-efficient data centers, IT departments have begun to virtualize their servers.

Instead of running one server per application, they've consolidated the number of physical servers by using virtualization software and technology such as blade servers. This lets one server or a smaller group of servers do the job of many single-purpose servers.

Cloud computing is not virtualization per se, but virtualization is a foundational technology for cloud computing. The National Institute of Standards and Technology (NIST) defines cloud computing as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (such as networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

In the cloud, a farm of servers collectively delivers applications, data storage and other IT resources to the same users that an IT department serves. But instead of those resources living in a traditional data center, they're accessible through a client interface (usually a web browser) over a high-speed network.

The most common cloud, referred to as the public cloud, is run by a third-party service provider. An organization contracts with the cloud service provider to deliver the applications it wants, store the organization's data, and ramp up or down access to applications and data as needed.

The organization doesn't need to maintain the servers. Instead, it can pay for computing services per user and avoid many of the support and capital expenditure costs associated with running a data center.

Private vs. Public Clouds

Selecting a private cloud model is not a trivial decision. Having started down the path of cloud computing, agencies cannot

Flavors of Private

Although many government agencies understand the benefits of cloud computing and are actively seeking a cloud strategy, security concerns, primarily, are steering them toward a different cloud platform, namely a private cloud. As defined in the *Federal Cloud Computing Strategy*, a private cloud "is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise."

An agency can adopt a private cloud in one of two ways: either on a separate, dedicated cloud infrastructure that is hosted and managed by a cloud service provider, or on a cloud infrastructure that is built in the agency's own data center.

In early 2011, the Department of Agriculture became one of the first federal agencies to move its e-mail and collaboration systems into a cloud operated by Microsoft. USDA's cloud services are housed on dedicated servers in secure facilities.

It's important to note that cloud computing decisions don't come down to simply public vs. private. There are models by which an agency can reap the benefits of cloud computing in general, plus the security, availability and compliance of private cloud computing, while still tailoring the solution to its particular situation.

Hybrid Cloud

The first option is a "hybrid" cloud model. Not all agency applications require the security of a private cloud, and not all private clouds can scale as big and as quickly as some agency applications require. A hybrid cloud infrastructure comprises two or more clouds, including private and public clouds, linked by standard or proprietary protocols.

For example, an agency's e-mail application may live in a public cloud while its ERP systems may live in a private cloud, but users access them through one interface.

A hybrid cloud also enables what is called "cloud bursting," by which a private cloud can reach into a public cloud for additional resources as needed.

The National Association of State CIOs (NASCIO), in its June 2011 report *Capitals in the Clouds*, states that organizations using a hybrid cloud should pay special attention to classification and labeling of data "to ensure that data are assigned to the correct cloud type."

Community Cloud

The second model is a "community" cloud. A community cloud is shared by several organizations, usually based on a shared mission or interest. The organizations may also have shared governance requirements to address security or compliance issues. And like a private cloud, a community cloud may be either hosted by a third party or built on an agency site. A community cloud can also spread the cost of the infrastructure across agencies.

By adopting a private cloud infrastructure, agencies can better position themselves to take advantage of a related IT services model, namely software as a service (SaaS). To date, the concept of accessing hosted enterprise and productivity applications over a network has enjoyed less traction in government than it has in the private sector.

Businesses have long utilized SaaS applications such as customer relationship management software from Salesforce.com, enterprise resource management software from SAP and others, and more recently, office productivity suites such as Google Apps for Business and Microsoft Office 365.

SaaS providers essentially build their own secure private clouds from which to serve applications to the public. Agencies that are interested in the private cloud option can do the same thing for their users.

simply determine that, because of security or other concerns, they must adopt a private cloud.

For example, if an agency wants to build its own private cloud, it will still need to invest in data center infrastructure and hire cloud computing experts. Moreover, although a private cloud can offer an IT department complete control, it may not provide the same scalability as a community or public cloud.

Therefore when deciding between private and public cloud models, an agency must evaluate its own policies, processes and applications to decide whether some or all of its IT infrastructure can be served in a private cloud. Some of the most compelling reasons that an IT department might pursue a private cloud strategy include:

- **Security:** Many agencies have security requirements, including encryption and authentication policies, that a public cloud might not meet. So a private cloud is a better option.
- **Availability:** Some public sector IT departments may have very high availability requirements for their applications, and the agency must determine whether a public cloud provider can ensure that uptime.
- **Compliance:** Agencies must comply with various information security standards, such as Payment Card Industry (PCI) standards for accepting credit or debit card payments, or Health Insurance Portability and Accountability Act (HIPAA) standards for protecting health information. A private cloud may better protect such agencies from audit deficiencies, data loss or exposure, or unauthorized access.

- **Control:** If an agency chooses to build its own cloud in its own data center, it has total control over the hardware it runs, the software it deploys (including the patches it chooses to implement — or not) and more.

In general, private clouds are more customizable than public clouds. On the flip side, public clouds are more scalable. And some applications can live securely in the public cloud.

For example, many agencies have moved their e-mail systems to public cloud platforms such as Microsoft Office 365 and Google Apps for Government. These agencies have determined that e-mail is akin to a commodity utility service (and that in some cases it's as secure in a cloud as it is on their own servers).

Increasingly, IT departments are considering the hybrid approach to cloud computing. After analyzing their infrastructure and weighing risk, many have determined that some applications can live in a public cloud and others in a private cloud (and some legacy or sensitive applications cannot run in a cloud at all).

Hosted or Build Your Own?

A private cloud can be hosted by a third party and separated (logically and physically) from the public cloud, or it can be built and managed inside an agency's own data center. Agencies face a similar choice with regard to a community cloud, wherein multiple agencies or departments with similar needs, missions or applications run federated cloud services.

Deciding between a hosted private cloud and one that an agency builds itself is not trivial. Although the migration paths are similar — from virtualizing assets to establishing new IT governance policies — the models are very different and require unique commitments on the part of the IT group.

The Hosted Model

Why might an agency choose a private cloud hosted by a third party?

1. The third party constantly manages the hosted cloud so that it's up to date.

2. The hosted service provider already has cloud experts on staff.

3. The service provider can manage billing for cloud services, application provisioning, etc. And the agency can fine-tune service-level agreements (SLAs).

4. Should the agency require more resources, the service provider may allow cloud bursting between the agency's private cloud and the service provider's much larger public cloud.

5. Depending on the service provider, the hosted private cloud could include the necessary authentication, encryption and identity management as well as other security measures.

SaaS in the Cloud

Many government agencies have adopted cloud computing as part of their IT infrastructure. By and large, these have been public cloud deployments. Although private cloud computing is relatively new, some agencies plan to adopt the secure private model to deliver SaaS. Among them are the following agencies.

NIST

The National Institute of Standards and Technology is considering moving its IT service ticketing system to a private cloud as part of a larger move to an IT Service Management (ITSM) model for providing services to end users. NIST wants to migrate the trouble-ticket system to the cloud, in part so that IT can focus more on other applications that directly affect the agency's mission.

In the long run, NIST hopes that other departments, such as telecommunications, security and building maintenance, will be able to use the cloud-based ticketing system.

Census

The U.S. Census Bureau plans to use a private cloud to deploy a virtual desktop infrastructure (VDI) and reduce the costs associated with providing and maintaining desktop service. The agency is also looking to the private cloud and VDI to comply with the *Telework Enhancement Act of 2010*.

By running virtual machines in the cloud and ensuring that sensitive data resides on cloud-based storage, Census aims to protect the data while enabling workers to be productive remotely. The Census cloud will reportedly support single sign-on and two-factor authentication.

Utah Department of Technology Services

Utah implemented a hybrid cloud approach that combines some public cloud services with private cloud services for specialized access and security requirements. The Beehive State supports a number of public services where individual county and city governments pay only for their usage.

In addition, the state's Department of Technology Services (DTS) is now completing a private cloud. The state is moving many of its applications, which previously resided on about 1,800 physical servers in more than 35 locations, to a virtual platform of 400 servers. This initiative is expected to save $4 million in annual costs for the state. Going forward, DTS plans to extend virtualization to desktops across the state.

Sources: U.S. Government Cloud Computing Technology Roadmap, Volume 2, Release 1.0: Useful Information for Cloud Adopters and the Federal Cloud Computing Initiative website, info.apps.gov.

An agency exploring a hybrid approach to cloud computing (part private, part public) will need to consider how the technologies match up between the two. If an agency uses the same service provider for each part of its cloud, integration should be relatively simple.

If not, or if the agency's private cloud is built internally, the compatibility of certain underlying technologies (security technologies in particular) must be considered. For instance, the service provider should use the same cloud security technologies used by the internal private cloud.

Also, some cloud providers partner with other companies to supplement their cloud services. An agency that hosts a private or hybrid cloud with a service provider must perform due diligence to understand exactly where the cloud resources come from.

Tactical Advice: SaaS Security

Learn more about the growing popularity of hosted SaaS security solutions here: CDWG.com/cloudta

Build Your Own

Of course, an agency may decide to forgo third-party hosted cloud services and build its own private cloud. This strategy comes with significant implications. A build-your-own private cloud requires an ongoing IT infrastructure investment. It also requires an IT staff skilled in cloud technologies.

Still, the internal private cloud may be the only way to realize the benefits of cloud computing while adhering to security and IT governance policies. Plus, it may be the best path toward ultimately delivering software as a service to end users.

Agencies can look at building an internal private cloud as a step toward moving to a hosted private cloud or even a public cloud deployment. In building an internal private cloud, the agency's IT department will develop cloud expertise, including the skills needed to deploy cloud services.

A build-your-own private cloud offers benefits that include the following:

- **Control:** Building a cloud in an agency's own data center creates a situation similar to what the agency is used to — IT professionals managing and monitoring their own infrastructure, in this case employing cloud computing skills and technologies.
- **Security and compliance:** Part of the control factor is the ability to secure the agency's private cloud with preferred technologies. Moreover, running an in-house private cloud may help an agency comply with security regulations.
- **Application portability:** Should the agency's IT department decide to move applications to another computing platform, having all associated data in-house could make porting applications easier than if the department had to export data from a third-party cloud.
- **Customization:** Because hosted cloud services support many organizations, IT departments often are limited to the application configurations that the host provides. However, if applications reside in an in-house private cloud, the agency is able to customize them.

IT infrastructure cost is among the biggest factors when considering a build-your-own private cloud. Although an agency building its own private cloud must continue to invest in infrastructure, the cloud may ultimately pay cost dividends in terms of IT support and management savings.

Still, agencies can identify ways of saving on their cloud infrastructures, either through redeploying resources that are freed up during the required consolidation/virtualization process, or through leasing cloud equipment.

Private Cloud in a Box

When an agency decides it wants to build its own private cloud, many vendors can offer the necessary hardware, software, storage, security and networking components. One strategy the IT department should consider is an end-to-end integrated solution — a "private cloud in a box."

Cloud computing is new enough that interoperability among disparate parts cannot always be assured. And validating cloud platforms can take time. Companies such as HP (CloudSystem), IBM (BladeCenter Foundation for Cloud), NetApp (FlexPod) and VCE (Vblock) offer integrated, validated cloud systems.

For example, a Vblock system includes EMC storage, Cisco Systems networking hardware, VMware virtualization software, RSA security products and more. The company preconfigures the cloud system and validates its operation before it is installed.

Migrating to the Private Cloud

For many public-sector IT departments, migrating to a private cloud may feel like a logical next step from an infrastructure point of view. That's because so many IT departments have spent years standardizing on commodity servers, operating systems and enterprise applications. And many have spent recent years consolidating their data centers using technology such as blade servers and virtualization.

In fact, for many agencies, virtualization will be a foundational element of their move to a private cloud. Virtualization creates an abstract version of a data center's underlying resources, including servers and storage, so that they can become pooled resources in the cloud.

Regardless of where an agency's private cloud will reside, migration should begin with fundamental decisions, such as which applications to migrate to the cloud. Proprietary, legacy programs are not the best candidates for the cloud.

The IT department also must determine the agency's cloud computing needs. This could be simple, as in knowing how many e-mail accounts to migrate to a cloud. Or it may be more complex, as in calculating how many virtual machines a cloud must support for cloud-based application development or other services.

Private Cloud Technology

If an agency plans to build its own private cloud, it must continue to invest in data center technologies, but with an eye toward delivering applications and resources as services. Some of these technologies, which are already common in public sector infrastructures, are key to private cloud deployment:

- **Virtualization technology:** Virtualization spans a whole host of computing resources, from server and storage virtualization to application and client virtualization. Hypervisor software, for example, a critical virtualization technology, allows multiple instances of an operating system (known as "guests") to run concurrently on the same server.

  Application virtualization is important because it establishes the foundational cloud capabilities of self-service and rapid provisioning. IT departments no longer have to touch every desktop computing or other client device in order to load application software for workers to use.

- **Storage technology:** Storage area networks (SANs) give data centers that are migrating to a private cloud the scalable, persistent storage they need. By their nature, SANs provide consolidated storage connected to servers. They pool storage resources across a high-speed network and make them available regardless of how an application is accessed.

  For years, SANs were complex and pricey to deploy, but within the past decade, both cost and complexity have fallen to the point where widespread adoption by even small agencies is possible.

- **Security:** Security inside a cloud differs from traditional security, which depends on firewalls and intrusion detection systems to monitor network traffic. For example, when moving workloads among virtual machines on the same server, agencies need virtual security products to detect unauthorized data traffic. Cloud-based virtual firewalls and identity management systems will continue to evolve as products mature and cloud-based threats are better understood.

- **Bandwidth:** An application's performance sometimes depends on the speed of the network connecting the user to the cloud service. Cloud-based e-mail may not suffer from network latency issues, but other enterprise applications might. Depending on the application services an agency plans to migrate to its private cloud, it may consider high-speed 10 Gigabit Ethernet (10 Gig-E) network connections necessary.

- **Provisioning, management and metering tools:** These are perhaps the most cloud-centric foundational technologies. Many of today's agency data centers may already include virtualized assets, SANs, identity management tools and 10 Gig-E network links.

  But the secret sauce of a private cloud platform is the suite of tools that enable an IT staff to rapidly provision resources; deploy virtual operating systems, services and applications; monitor server utilization and system resources; and track usage information for possible billing and accounting purposes.

Migrating to a Hosted Private Cloud

If an agency is planning to migrate to a hosted private cloud, the bulk of the legwork is in choosing the right provider. To start with, the agency must grill potential service providers about their security practices. Even though the cloud will be private, how does the service provider ensure that other tenants in its cloud can't inadvertently access the agency's data?

How will data be encrypted — both at rest and in transit? What firewalls are in place? What authentication is used? And do the systems adhere to relevant security regulations, such as the Federal Information Security Management Act (FISMA) or the Federal Information Processing Standards publications?

Agencies will also need information about service providers' servers: their redundancy, in order to ensure uptime; and their physical location, in order to comply with regulations that govern where in the world an agency's data may reside.

Other important criteria for choosing among hosted private cloud providers include how the agency's data will be backed up and made recoverable in the cloud; how the IT department will be able to monitor its cloud services and what alerts it can expect; and what type of support — including support in migrating data to the cloud — the company will provide.

Agencies must understand how much they will pay for hosted cloud services. The industry is in its very early stages, and some agencies may encounter confusion about what a service provider will charge, for instance, per user. Therefore, be certain that costs are clearly spelled out and incorporated into an enterprise agreement.

After an agency has chosen a private cloud provider and determined what data and applications to migrate to the cloud, it must prepare for migration with as little disruption to daily operations as possible. If the cloud provider also offers the SaaS platform that the agency plans to use, such as e-mail or unified communications, getting the application up and

running for end users is usually straightforward. Migrating the agency's data, however, takes time and planning.

For example, if an agency plans to migrate its e-mail to a hosted private cloud, it may require separate software and consulting services, especially if it's changing platforms. The agency may also want to decide what data to migrate. Does the entire e-mail database need to move to the cloud, or just a few years' worth? Does all of the data need to migrate at once, or can it move department by department?

IT Governance in the Cloud

Regardless of how a public-sector agency plans to deploy a private cloud, one thing it cannot outsource is IT governance. Cloud computing elevates IT governance to greater than ever importance. Through solid IT governance, an agency can take care of the following:

- Make sure IT resources are deployed and utilized in accordance with relevant policies and regulations;
- Control, maintain, support and provision IT resources in a streamlined manner;
- Ensure that the private cloud and its resources are providing measurable business value to the agency and supporting its mission.

IT departments are increasingly likely to offer users IT as a service, through data center consolidation and virtualization. Deploying a private cloud platform represents the leading edge of the services model.

At the heart of delivering IT as a service are common practices such as IT Service Management (ITSM) and the Information Technology Infrastructure Library (ITIL). ITSM is a process-based approach to aligning IT services delivery with an agency's needs, instead of managing IT as individual systems and components. ITIL is a set of best practices for implementing ISTM. It is currently in version 3.0. IT professionals can study ITIL and earn various levels of certification.

Just as virtualization is a foundational technology for cloud computing, ITSM and ITIL form the cloud's governance foundation. But many other tools and technologies in cloud computing factor heavily into governance.

When it comes to hosting private clouds with a third party, the SLA is one of the most important governance documents. The SLA should spell out the amount of resources (computing, storage, bandwidth) that the provider will commit to the agency's private cloud. It should also specify what level of availability the agency should expect, how the agency will be notified of service interruptions, and what financial credits it can expect from the service provider for outages.

The SLA should include requirements for supporting other governance provisions, such as reports that detail the performance of the cloud and adherence to security and compliance requirements. Usage reports let IT departments implement pay-for-service programs within the agency.

Best Practices: Cloud Liftoff

Find more guidance for getting started in the cloud in this article: CDWG.com/cloudbp

Governance and the Build-Your-Own Cloud

When an agency builds its own private cloud, ITSM and ITIL take on even greater importance, because the IT department must undertake the management and monitoring of the cloud itself. An internal cloud should include, among other elements:

- Core cloud management software for handling everything, from verifying that a virtual machine is running (and determining if not, why not), to logging audit messages in a database
- A cloud orchestration platform, which may include other pieces of the cloud management system, such as metering and billing, but primarily serves to automate the provisioning of pooled resources for an end user
- A change management database for tracking the creation and deletion of virtual machines
- A self-service portal where services (infrastructure, platform or software) can be chosen from a catalog listing of available services
- A chargeback system, which allows consumption of cloud resources to be metered and their costs reported back to the consuming department

With a private cloud deployment, there are solutions and IT considerations that also factor into overall IT governance. For example, assuming an agency's entire IT infrastructure is not migrating to the cloud, an IT department may need to integrate the cloud monitoring and alerting capabilities with its overall enterprise management system. Alerts of problems in the cloud must be clearly identified as such and routed to the department's automated help-desk system.

Ultimately, through a well-planned private cloud migration and a governance model that embraces the IT department's role in services management, the agency is in a position to deploy widespread SaaS and all that it entails. If the private cloud is internal, the IT department will want to build a SaaS platform, including (depending on the service) an application database, application server and identity management system.

With agencies trying to do more with less and adopting an IT services approach to applications and resources, taking advantage of a private cloud model to enable SaaS may finally open doors that IT departments have been hesitant to walk through for years. Thanks to the security, control and compliance afforded by private clouds, government agencies can reap the same benefits of services-based computing that other enterprises already enjoy.

NIST Tackles Cloud Computing

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*. Although NIST is a federal agency of the Commerce Department, it is quick to point out that the roadmap under development is not intended to be U.S. government–centric. It is written for federal agencies, other governmental bodies, academia, industry and wherever else it might apply.

SP 500-293 was released in two parts. Part 1, *High-Priority Requirements to Further USG Agency Cloud Computing Adoption*, details what NIST has identified as necessary solutions, technologies and processes for enabling cloud computing by government agencies. In SP 500-293, each requirement is illustrated and substantiated.

For example, according to NIST, interoperability, portability and security standards are required because "while data, software, and infrastructure components that enable cloud computing (e.g., virtual machines) can currently be ported from selected providers to other providers, the process requires an interim step of manually moving the data, software, and components to a non-cloud platform and/or conversion from one proprietary format to another."

According to NIST, the 10 requirements for cloud computing by government agencies are:

1. International voluntary consensus-based interoperability, portability and security standards

2. Solutions for high-priority security requirements

3. Technical specifications to enable development of consistent, high-quality service-level agreements (SLAs)

4. Clearly and consistently categorized cloud services

5. Frameworks to support seamless implementation of federated community cloud environments

6. Technical security solutions that are decoupled from organizational policy decisions

7. Defined, unique government regulatory requirements, technology gaps and solutions

8. Collaborative parallel strategic "future cloud" development initiatives

9. Defined and implemented reliability design goals

10. Defined and implemented cloud service metrics

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

TWEET THIS!

CDW·G PEOPLE WHO GET IT™