# Government takes lead in cloud efforts

## Bright days ahead for the cloud

ebook

An SC Magazine publication

Sponsored by

# Bright days ahead for the cloud

Cloud computing can change the way we live our lives, and the government is leading efforts, reports Stephen Lawton

If you are headed to a federal data center, there is no need for an umbrella, but do expect clouds with a chance of high-performance computing. Following President Obama's call for generating savings in the federal budget by taking advantage of the cost-savings from using cloud computing, several federal cloud projects are underway, with some already serving user communities.

From the General Services Administration's (GSA) Apps.gov to ProjectForge from the Defense Information Systems Agency (DISA) to the high-performance computing clouds of NASA's Nebula to the Department of Energy's Magellan Project, government agencies are fast-tracking cloud virtualization environments as possible alternatives to the rapid growth of standalone federal data centers.

Federal employees today can access a variety of business, productivity and social media applications from the GSA's Apps.gov site, such as a fax application that charges as little as $.05 per page, to the Advanced Sourcing Application Platform, which sells for $5.5 million. Dozens of programs already are available through this site, which also offers a variety of free applications approved for government use. Overall, computing services are available in 33 categories.

The government hopes to be able to leverage public clouds for a variety of applications, but still will need the security of private clouds, says James Staten, vice president and principal analyst in the infrastructure and operations group at Forrester Research. While noting that some ad hoc IT resource-sharing has taken place in the past, the president's focus on the cloud marks the first time there has been a concerted effort to provide to federal workers the economies of scale offered by the cloud.

But while building out a cloud environment has its technological benefits — a more centralized IT infrastructure would be easier to manage and support — it does pose some automation challenges, Staten says. Today, it can take from a few days to weeks to provision a new server for an enterprise application, he notes. The promise of the cloud is that the time will be reduced significantly, resulting in greater productivity, but today there can be issues putting automation, such as special security protocols, on top of the existing cloud technology. Some technology does not yet scale well, he notes.

The government's current path to the cloud is spearheaded by Vivek Kundra, the federal chief information officer who works out of the Office of Management and Budget in the White House. Kundra is implementing President Obama's plan to reduce overall government expenses and the government's impact on the environment by implementing cloud computing for federal agencies. Some $30 million was set aside in the 2009 federal budget, growing to $100 million this year.

Kundra will not be formulating cloud computing policy, but he he will be leading the effort, with all of the CIOs in various government agencies reporting indirectly to him. While he will not directly oversee all IT budgets within the government, he will be able to approve or disapprove IT plans, Staten says.

"Those [CIOs] who get on the [cloud computing] bus will get their budgets; those that don't, won't," he says.

One of Kundra's key responsibilities, and biggest challenges, will be to get the CIOs throughout the government to buy into the cloud computing program to the point where they not only dedicate resources through a federal CIO council for peer review of proposals, but also accept that in a cloud environment they might not have as much control over all computing resources as they did in the past, says Jon Oltsik, se-



**27%**

*compound annual growth rate projected for cloud services*

*– IDC*

nior principal analyst at Enterprise Strategy Group, a Milford, Mass.-based consulting and research firm.

"CIOs across every federal agency are spending way too much time on building yet another data center, rolling out more networks and focusing on security, where they could consolidate," Kundra told participants at The Brookings Institution forum on the Economic Advantages of Cloud Computing in April. "What they're taking the attention off of is actually improving the lives of the American people through delivering better technology.

> "Key management is really hard to do now."
>
> *–Tim Grance, NIST*

Kundra noted that over the past decade, the U.S. government went from 432 data center to more than 1,100, while server utilization in some facilities is running at only seven percent. He cited several examples where government agencies, such as the Department of Interior, already are embracing cloud applications – moving more than 80,000 email addresses to the cloud. As well, the Department of Health and Human Services signed an agreement with Salesforce.com for the deployment of electronic health records.

Part of the challenge faced by cloud providers is settling on a standard definition of the term "cloud computing." The federal government, for the most part, is following the definition outlined by the National Institute of Standards and Technology (NIST): "A model for enabling 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. "

Despite that, NIST's Tim Grance, program manager for cyber and network security, points out that NIST itself is not creating the U.S. government standard for cloud security, but rather is "helping to define cloud computing" by creating and testing user cases and helping to direct the discussion on security.

The cloud is all about scale, Grance says. It is not just about managing physical assets, but rather the stream of virtual services. Today, there are several components to managing that stream that do not work well in cloud environments.

"Key management is really hard to do now," he says, adding that since resources can be spread among multiple systems across a wide range of locations, ensuring that users have the right credentials to access data and applications is a challenge as the infrastructure grows. Cloud-based identity management has many of the same challenges, he says.

## Government only

One possible approach to overcoming these challenges is to build a single, internally managed cloud environment strictly for the U.S. government, says ESG's Oltsik. A private cloud for sensitive government and military data, such as the cloud managed by DISA, could be used for highly classified or sensitive documents, while a second, less-secure private cloud could be built for general government business.

The cloud also could be used for government archive data that would reduce overall IT costs and reduce energy use, he says.

Security, of course, is a prime concern. In a report published by the Government Accountability Office (GAO) in July, IT executives at 22 of 24 major U.S. agencies surveyed by the General Services Administration (GSA) raised concerns about cloud security, saying "that they are either concerned or very concerned about the potential information security risks associated with cloud computing." The GSA identified several concerns, including the possibility that ineffective or non-compliant security provider security controls could lead to vulnerabilities affecting



**$42b**

*is the amount IT customers are expected to spend on cloud computing by 2012*

*– IDC*

the confidentiality, integrity and availability of agency information; the potential loss of governance and physical control over agency data and information when an agency cedes control to the provider for the performance of certain security controls and practices; the insecure or ineffective deletion of agency data by cloud providers once services have been provided and are complete; and potentially inadequate background security investigations for service provider employees that could lead to an increased risk of wrongful activities by malicious insiders.

> "The essence of cloud computing is giving up some security."
> – *Susan Coghlan, Argonne Leadership Computing Facility*

Today, says Forrester's Staten, whichever agency has the highest security requirement dictates who can have access to certain servers. For example, if the U.S. Army is storing classified intelligence data on a specific server, it could veto the use of that system by the human resource department from another organization to store data on that same physical server, even if the data is stored on a different virtual machine. The possibility that a clerk with a low security clearance could have access to classified data on the same physical server is not acceptable, he says.

To overcome such issues, DISA's Forge.mil DoD cloud exists on a private cloud where all physical servers are housed in secure data centers on U.S. military bases. By doing so, DISA ensures that all physical servers, and therefore all data, is under the military's direct control. None of the Forge.mil data is stored on servers accessible by third parties.

Further, Forge.mil provides shared and private infrastructures the ability to create multiple projects, DISA technical support, and other administrative functions that provide enhanced role-based access control over project artifacts, the site states. It already has more than 300 projects live and 6,000 DoD members, according to its website. The program is open to U.S. military, and DoD civilians and contractors. Access requires a valid DoD common access card or a PKI certificate issued by a DoD-approved External Certificate Authority.

Another DISA program is the Rapid Access Computing Environment (RACE) service, which provides a streamlined process for the provisioning and subsequent development, testing, certification and accreditation and deployment of applications to a DISA Defense Enterprise Computing Center (DECC). DISA Computing Services Directorate (CSD) provides hosting, networking, security and connectivity, and offers the package to DoD customers as a service.

## Not for all implementations

Not all applications are appropriate for cloud computing on traditional Windows servers, notes Susan Coghlan, associate division director at the Argonne Leadership Computing Facility, housed at the Argonne National Laboratory. Coghlan heads the Magellan Project— a two-year research program designed, in part, to explore whether cloud computing can help meet the demand for scientific computing. According to the Department of Energy, which runs the lab, "The number of scientists who would benefit from mid-range computing far exceeds the amount of available resources."

Coghlan says that many of the applications that scientists run on these high-performance computers, some of the most powerful computers in the world, would not be able to run on popular cloud infrastructures. Many of the applications do not work correctly in virtual environments, and many require greater bandwidth and hardware resources, such as graphics processors and faster connections to memory, than is available in cloud environments built on commodity hardware and virtualization



**9%**

*of customer spending will involve IT cloud services in 2012*

*– IDC*

operating systems. "Virtualization can play a problematic role," she says.

Another major difference between the Magellan Project and other cloud computing efforts within the federal government is the operating environment itself. Magellan is built entirely on open source software. Much of the development work on Magellan requires Department of Energy engineers to make changes to the operating system's kernel. While that is possible when using open source software, that cannot be done using a commercial operating system, she notes.

As in the commercial application environment, the scientific community also has significant security concerns, she says. "The essence of cloud computing is giving up some security," she notes. By allowing a third party, be it an outsourced service provider or the IT department in a different government agency, the data's owner is, by definition, relinquishing control over their data because their access and control over a physical infrastructure is absent after moving to the cloud. Additionally, unlike traditional data centers, which usually are built in traditional office- and industrial-type buildings, the NASA's Nebula data centers are far more mobile — shipping containers. Each shipping container data center can hold up to 15,000 CPU cores, or 15 petabytes of storage, while proving 50 percent more energy efficient than traditional data centers, according to NASA. To date, however, NASA has built only one container, which is located at the Ames Research Center in Silicon Valley.

Each account holder gets 100GB of storage with their account – with Nebula focusing on free and open source software. It is open to NASA's internal project groups and is part of the OMB's test-bed cloud computing operations. Nebula's pricing and terms of service are still under final review.

## Bright future

The future of cloud computing in the federal government is bright. Not only does federal CIO Kundra believe that significant cost savings and reduced environmental impact can be generated by cloud computing, he envisions further changes.

"Imagine an environment where we're able to look at any given agency, use the data that the government has democratized, and share the performance of that agency the same way we share YouTube videos today," he told the Brookings audience. "We can't even imagine today the potential of cloud computing as we look forward. But the interception of high-processing power, cheaper cost and the ubiquitous access to broadband networks that, for the first time, are able to deliver content in ways we couldn't imagine before, that's going to fundamentally change the way we live our lives." ■

---

*For more information, please contact Illena Armstrong, editor-in-chief,* SC Magazine, *at illena.armstrong@haymarketmedia.com.*



**$5.5m**

*expected savings by the city of Los Angeles over five years as a result of moving email and productivity tools to the cloud for over 34,000 city employees*

*– Vivek Kundra, "State of Public Sector Cloud Computing"*

Sponsor

Thawte is a leading global Certification Authority. Our SSL and code signing digital certificates are used globally to secure servers, provide data encryption, authenticate users, protect privacy and assure online identifies through stringent authentication and verification processes. Our SSL certificates include Wildcard SSL Certificates, SGC SuperCerts and Extended Validation SSL Certificates.


Masthead

EDITORIAL

**EDITOR-IN-CHIEF** Illena Armstrong
*illena.armstrong@haymarketmedia.com*

**DEPUTY EDITOR** Dan Kaplan
*dan.kaplan@haymarketmedia.com*

**MANAGING EDITOR** Greg Masters
*greg.masters@haymarketmedia.com*

DESIGN AND PRODUCTION

**ART DIRECTOR** Brian Jackson
*brian.jackson@haymarketmedia.com*

**SENIOR PRODUCTION** Krassi Varbanov
*krassi.varbanov@haymarketmedia.com*

U.S. SALES

**ASSOCIATE PUBLISHER, VP OF SALES** Gill Torren
(646) 638-6008 *gill.torren@haymarketmedia.com*

**EASTERN REGION SALES MANAGER** Mike Shemesh
(646) 638-6016 *mike.shemesh@haymarketmedia.com*

**WESTERN REGION SALES MANAGER** Matthew Allington
(415) 346-6460 *matthew.allington@haymarketmedia.com*

**NATIONAL INSIDE SALES EXEC.** Brittany Thompson
(646) 638-6152 *brittany.thompson@haymarketmedia.com*