CLOUD COMPUTING

ISSUE 3, VOLUME 2
OFFICE OF TECHNOLOGY STRATEGIES (TS)

INTRODUCTION

In a previous Tech Insight, we explored virtualization technology, a computing environment that serves as the backbone of this Tech Insight's topic, cloud computing. As discussed in A VA Executive's Guide to Virtualization, virtualization software allows several operating systems and applications, bundled together as "virtual machines," to run independently of each other on the same hardware. This Tech Insight explores cloud computing, perhaps the most recognizable application of virtualization technology. Although adoption of full-scale cloud computing may not fit every particular business line, the technology is being implemented across public and private industry, and should be considered by executives and IT stakeholders as a key component of VA's IT strategy.

OVERVIEW

Cloud computing is generally defined as a type of computing that relies on sharing computing resources rather than using local servers or personal devices to handle applications. Cloud computing aims to perform tens of trillions of computations per second in consumer-oriented applications by leveraging networks of large groups of servers with specialized connections to spread data-processing chores across them. Apple's artificial intelligence iPhone assistant, Siri, is a good example of cloud computing in action. The application enables users to send messages, schedule appointments, make calls, find restaurants and more, storing user preferences in the cloud to allow Siri to better understand and contextualize commands. According to the National Institute of Standards and Technology (NIST), the cloud computing platform is composed of five essential characteristics, comes in three types of service models, and can be deployed in four different ways.

Essential Characteristics:

- *On-demand self-service*: A consumer can automatically and unilaterally provision computing capabilities, such as server time and network storage, as needed without requiring human interaction with each service provider.

- *Broad network access*: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).
- *Resource pooling*: The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.
- *Rapid elasticity*: Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and in-ward commensurate with demand.
- *Measured service*: Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, band-width, and active user accounts).

Service Models:

- *Software-as-a-Service (SaaS)*: The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.
- *Platform-as-a-Service (PaaS)*: The consumer does not man-age or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.
- *Infrastructure-as-a-Service (IaaS)*: The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

Deployment Models:

- *Private cloud*: The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units).
- *Community cloud*: The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations).
- *Public cloud*: The cloud infrastructure is provisioned for open use by the general public. It may be owned, man-aged, and operated by a business, academic, or government organization, or some combination of them.
- *Hybrid cloud*: The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are

bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

BENEFITS OF CLOUD COMPUTING

Although the results of adopting cloud computing may vary across specific business lines, the Congressional Research Service (CRS) has found that there are several benefits public agencies gain from making the switch. These include, but are not limited to:

- *Cost Reduction*: Cloud computer platforms use resources more efficiently than local servers. Furthermore, users pay only for the resources and workloads they actually use.
- *Energy Efficiency*: Cloud computing data centers benefit from economies of scale to run more efficiently than local servers.
- *Service Availability*: Cloud computing systems make it easy for any device with an Internet connection to access files or software.
- *Organizational Elasticity*: Cloud systems can make it easier to upgrade operating systems and applications. Organizations can easily scale up or down as computing needs increase and decrease.
- *Service Reliability*: Cloud systems can save data onto multiple servers.
- *Data Security*: Cloud-providing companies such as Yahoo, Google, and Amazon also have the financial resources to purchase the tools necessary to ensure that networks remain safe.

CURRENT CHALLENGES

CRS has also identified several challenges, however, that federal agencies such as VA may face when attempting to mi-grate to cloud computing. Although cloud providers can facilitate cutting-edge security, for example, the government consistently faces advanced, persistent threats to its data. System-wide security updates are necessary more often for federal agencies than for private sector organizations. Data safety and cloud jacking, where someone steals the pass-word to your IaaS service, are top concerns in cloud computing. Entrusting a third-party organization with your data seems risky, but thorough vendor vetting, encryption of sensitive data, and exporting of non-mission critical services to the cloud first are ways to significantly mitigate this risk.

Other challenges include government agencies' tendency to adopt new technologies sluggishly, which can be due to in-grained cultures and outdated ancillary IT infrastructure. Migration to the cloud can also involve high initial costs, which can serve as a roadblock to realizing efficiencies in the future.

Finally, in order to maximize their return on investment (ROI) in cloud computing, organizations need to avoid overpaying vendors by determining the right package of delivery and service models for their business line. Measuring ROI can be particularly challenging when it comes to cloud computing, so industry experts recommend focusing on overall value rather than dollars. Factors that can provide "soft" ROI include increased agility, flexibility, scalability, improved processes, streamlined development platforms, and more strategic use of IT resources.

If you have any questions about cloud computing, don't hesitate to ask TS (askTS@va.gov) for assistance or more information. Check out earlier Tech Insight editions here.

TS TECH INSIGHT SERIES

The monthly Tech Insight series aims to help readers make better decisions and be more informed customers (of Office of Information & Technology's products and services) by providing them with high-level overviews of technology issues that impact or will impact VA's Information Technology (IT) environment. Tech Insights introduce topics in an easily digestible fashion by presenting background information on the topic, clearly explaining its importance within VA, and providing recommendations for success from TS. View all TS Tech Insights here.

DISCLAIMER: This document includes links to websites outside VA control and jurisdiction. VA is not responsible for the privacy practices or the content of non-VA websites. We encourage you to review the privacy policy or terms and conditions of those sites to fully understand what information is collected and how it is used.