Technology Strategies Notes Revisited

Volume 2, Special Issue 3
October 2015

Office of Technology Strategies (TS), Architecture, Strategy & Design (ASD)

Technology Strategies

Defining OI&T's "To Be" Technology Vision

The TS office within OI&T's Architecture, Strategy & Design (ASD) interacts not only with the ASD pillar offices, but also with multiple stakeholders within OI&T and with strategic offices across the enterprise. TS works closely with IT and business owners to capture business rules and provide technical guidance as it relates to Data Sharing across the enterprise, specifically for interagency

A VA Executive's Guide to Past Notes: Cloud Computing

INTRODUCTION

This TS Note revisits several previous TS Notes and combines their highlights into one document. This provides readers one location where they can find overviews, examples and benefits of a larger IT concept, and use them in strategic or investment decisions. The TS Note series has covered three topics in Cloud Computing to date, as well as a related TS Note on virtualization. This TS Note will revisit these Cloud topics and their relation to VA's IT Vision.

WHAT IS CLOUD COMPUTING?

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.

In order to maximize the benefits that Cloud Computing brings, solutions should demonstrate the following essential characteristics:

- On-demand self-service
- Broad network access
- Resource pooling
- Rapid elasticity

Depending on the organization and project requirements, there are three different service models to choose from for optimal success.

SOFTWARE-AS-A-SERVICE (SaaS)

In 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. The Cloud model has no physical need for indirect distribution since it is not distributed physically and is deployed almost instantaneously. Benefits include application customization, more frequent software update, and collaboration opportunities across cloud instances. Challenges include data security and integration and compatibility issues with legacy or other cloud systems.

PLATFORM-AS-A-SERVICE (PaaS)

The PaaS consumer does not manage or control the underlying cloud infrastructure, but has control over the deployed applications. PaaS can be delivered in two ways: as a public cloud service from a provider, where the consumer controls software deployment and configuration settings, and the provider provides the networks, servers, storage and other services to host the consumer's application; or as software installed in private data centers or public infrastructure as a service and managed by internal IT departments. PaaS models include public, private, mobile, and open. The primary advantage of PaaS is that it allows for higher-level programming with radically reduced difficulty.

INFRASTRUCTURE-AS-A-SERVICE (IaaS)

With 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). A third party provider hosts hardware, software, servers, and other infrastructure components on behalf of the user. They handle tasks like maintenance, backup, and host users' applications. The advantage to IaaS is access to highly scalable resources that can be adjusted on-demand. However, because providers own infrastructure resources, private management can be difficult and relies on provider services (which may be interrupted).

Deployment Models:

- Private cloud: The cloud infrastructure is provisioned for exclusive use by a single organization comprising

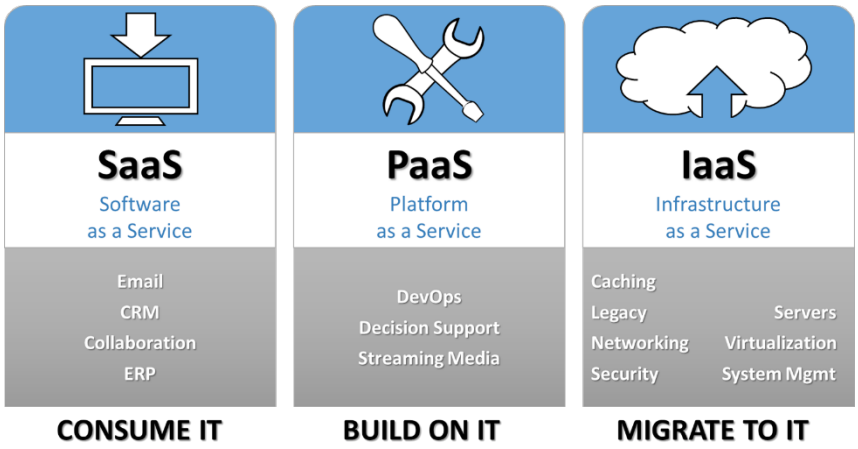

Figure 1: Cloud Service Models

Continued on Page 2

Technology Strategies Notes Revisited

Volume 2, Special Issue 3
October 2015

A VA Executive's Guide to Past Notes: Cloud Computing

Continued from Page 1

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.
- Public cloud: The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by one or several organizations.
- Hybrid cloud: The cloud infrastructure is a composition of two or more distinct cloud infrastructures that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability.

PRIVACY & SECURITY

In a report that reflected the consensus among surveyed industry experts, the Cloud Security Alliance (CSA) identified the top nine cloud computing threats of 2013. According to CSA, the top three threats are data breaches, data loss, and service traffic hijacking. In order to address these and other threats, there are six specific areas of the cloud computing environment that require substantial security attention:

- Encrypting the data is one way for organizations to secure data at rest and data in transit from prying eyes
- Strong authentication protocol for users, applications, processes, and devices
- Use virtual machines and a hypervisor to ensure robust separation between data belonging to different customers
- Each customer should have his or her legal and regulatory experts inspect provider's policies and practices to guarantee they cover cloud-related legal and regulatory issues
- Customers need an incident response plan for the possibility of cloud provider security breaches or user misbehavior

Virtualized Environments

Traditional computing environments are made up of any number of servers that each run only one operating system (OS) and application at a time. This narrow usage means servers utilize only a small amount of their capacity. In order to meet requirements for several applications or OSs, traditional architecture requires a wasteful amount of energy, physical space, and monetary resources. In a virtualized environment, the OS and application bundle, known as a "virtual machine," run on top of the existing hardware. This infrastructure also allows several virtual machines to run independently of each other on the same hardware. Virtualization can help extend the life of older client software, reduce capital expenditures and operating costs, and increase the flexibility of data (archiving, optimizing, en-

The Notorious Nine: Top Threats in Cloud Computing in Recent Years

1. Data Breaches
2. Data Loss
3. Account or Service Traffic Hijacking
4. Insecure Interfaces and APIs
5. Denial of Service
6. Malicious Insiders
7. Abuse of Cloud Services
8. Insufficient Cloud Vendor Due Diligence
9. Shared Technology Vulnerabilities

CLOUD COMPUTING AT VA

VA is actively establishing long-term strategies and governance mechanisms to ensure that all cloud services comply with the latest Federal standards and are properly integrated into the IT infrastructure. Specifically, VA is completing a Cloud Security Handbook as part of the "Cloud First" policy (VA Directive 6517), and it requires all cloud services that have business agreements with VA to be accredited by a process known as the Federal Risk and Authorization Management Program (FedRAMP). In addition, VA's future IT environment will rely more and more on the use of Cloud service models to build a robust networking infrastructure for VA users. The Enterprise Technology Strategic Plan (ETSP) describes the following transition activities:

- Expansion of internal IaaS and PaaS offerings
- Implementation of Adaptive Cloud Environment (ACE) to provide IaaS capabilities and support services in a standardized orderable environment
- Implement a cloud broker to aggregate, integrate and customize internal and external cloud services

The ETSP also identifies strategies for three levels of access to enterprise cloud services – for more information please check out the ETSP here.

Ultimately, VA's IT Vision relies on an IaaS model that makes applications available on a Cloud Computing platform and gives users access to enterprise applications on the IT infrastructure.

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 TS Note editions here. (http://www.techstrategies.oit.va.gov/docs_ctsnotes.asp).