Best Practices in Cloud Migration: Mission Drivers First, Technology Second

By: Jeff Johnson, Subject Matter Expert

Introduction

When it comes to cloud migration, there is no one-size-fits-all model for federal agencies. Cloud comes in all shapes and sizes—and what fits for one agency's mission needs, might not fit for another. However, no matter the desired result, there are a few important steps that all agencies should follow to ensure a successful cloud migration.

In this article, I will walk you through four recommended steps, as well as provide examples of their real-world application for a federal agency. We will also discuss the importance of understanding your agency's mission drivers first, before jumping headfirst into the technology.

Background

Although federal agencies are only recently adopting public cloud, the technology itself has been around for quite some time. In 1963, the Defense Advanced Research Projects Agency (DARPA) provided funding to MIT to develop technology that would allow "a computer to be used by two or more people, simultaneously." In the 1970s, virtualization paved the way for modern cloud infrastructure; and in 1999, Salesforce became one of the first companies to use the cloud to deliver software programs to end users (Dataversity.net). Fast forward to the 2000s and sophisticated cloud offerings emerged from the likes of Amazon Web Services, Google, IBM, and Oracle. Today, there are hundreds of cloud service providers (CSP) and cloud implementation partners in the market.

Guidance

In 2018, the Office of Management and Budget issued a long awaited update to its legacy Federal Cloud Computing Strategy ("Cloud First"). Known as Cloud Smart, the new strategy aims to offer practical implementation guidance for cloud computing. It also redefines the term given its broad—and often misleading—use for any technology solution provided by an outside vendor. Cloud Smart defines cloud "as a solution that exhibits five essential characteristics of cloud computing, as defined by [the National Institute of Standards and Technology] NIST: on-demand service, broad network access, resource pooling, rapid elasticity, and measured service (cloud.cio.gov)."

Agency IT leaders are already well versed in operating within strict regulatory environments – and the same holds true for the cloud. In the interest of brevity, I will not get into all of the applicable cloud mandates. However, I will tell you that it is vitally important to understand the implications of the NIST 800 series (144/145/146 and 30/34/37/137…), FedRAMP, FISMA, the Committee on National Security Systems, and the Department of Defense Cloud Computing Security Requirements Guide as you think about migrating data and applications to the cloud, as a federally regulated environment.

There are three delivery models and four deployment models for any cloud engagement. There are also branches off the models, such as Database as a Service (DBaaS), XaaS, etc. that are off-shoots of Software a a Service (SaaS).

Delivery Models

- Infrastructure as a Service (IaaS): The consumer is able to provision processing, storage, networks and other fundamental computing resources on-demand. The CSP is responsible for managing and controlling the underlying cloud infrastructure.
- Platform as a Service (PaaS): The consumer can deploy applications onto cloud infrastructure using programming languages and tools supported by the CSP. The CSP is responsible for managing and controlling the underlying cloud infrastructure.
- Software as a Service (SaaS): The consumer is able to use the CSPs applications running on a cloud infrastructure. The CSP is responsible for managing and controlling the underlying cloud infrastructure, where the consumer still has primary responsibility for its own data.

Deployment Models

- Private Cloud – All computing resources are privately hosted for one agency.
- Public – All computing resources are publicly hosted by a CSP.
- Hybrid – A combination of two or more distinct cloud infrastructures (private, community or public).
- Community – Computing resources are shared by two or more agencies that have shared concerns (i.e. security or compliance).

Getting Started

While you might be tempted to jump headfirst into the cloud, it is impossible to design your future if you do not understand your current state. That leads us right into step one of four for a successful cloud migration.

Step 1: Baselining Your Current State & Defining the "To Be"

What is your mission case? What is your vision? What are your barriers to adoption? Answering these questions and more in specific strategy documents is an important first step. For example, an agency can create the following types of documents that will facilitate a successful cloud migration:

- Cloud Strategy Document: This document is typically 10-15 pages in length and is developed by an internal, cross-functional Cloud Council. It answers questions such as what is your mission statement? Who are the key stakeholders? What type of cloud delivery and deployment model(s) will you use? How will cloud be a business accelerator for your agency?

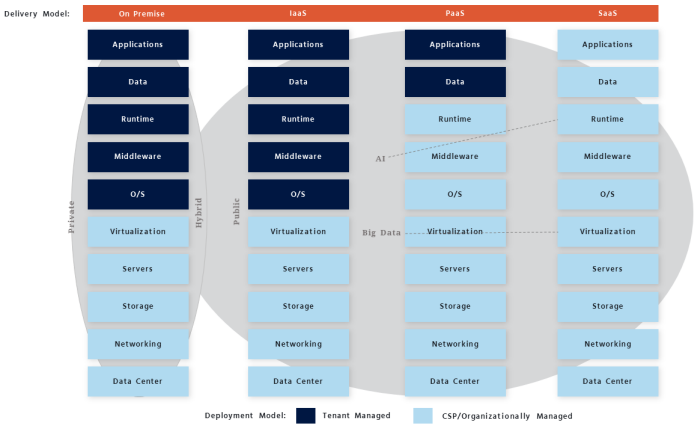

Figure 1: Cloud Delivery & Deployment Models Overview

- Cloud Acquisition Plan: Cloud has drastically changed the way agencies procure IT services. Consumption-based pricing means that IT departments have to be smart about budgeting and forecasting, and plan ahead for surge uses (for example tax season for the Internal Revenue Service). This document clearly defines your agency's strategy to handle these challenges.
- System Design Document (SDD): As I mentioned above, you must document the "as is" before you can think about the "to be." The SDD is a living architecture of your complete IT environment. The example below shows a real-world capture of the "as is" state for one federal law enforcement agency, as well as the desired "to be" state in the cloud. Capturing these two states can be a very complex and detailed undertaking, but is the cornerstone of success.

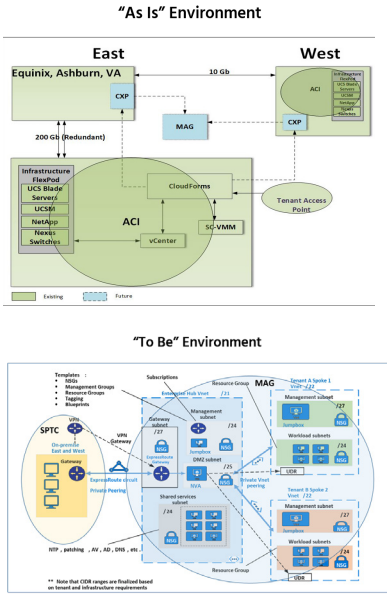

Figure 2: Example of "As Is" and "To Be" Environments

Step 2: Establishing a Governance Model

Cloud governance is the people, processes, and technology associated with your cloud infrastructure, security, and operations. Without a defined governance model, your cloud environment can quickly get out of control.

Deploying cloud ultimately comes down to orchestration and automation. Therefore, you must clearly define the order in which things can occur with a minimal amount of human intervention. You do that by creating templates and an inheritance model. For example, if I want all of my users to have the same set of resources with no variation, I can define that at the management group layer and everything below that layer will inherit the same elements. You can take that a step further and create blueprints to enforce behavior within the confines of your organizational restraints and security requirements. See the example below.

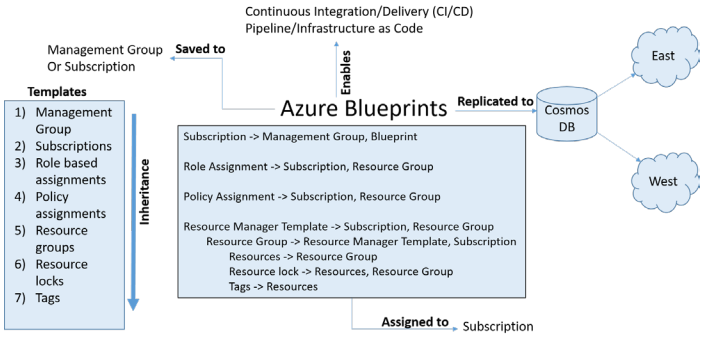

Figure 3: Example Governance Model

FedRAMP also comes into play here. If you know that you have received a FedRAMP Authority to Operate (ATO) at the Moderate level, by default every service you deploy needs to align with FedRAMP Moderate. You can do that from the bottom up, but then you would have to go back and re-authorize for each service. It is far easier (and less time consuming!) to create a template environment that can be replicated globally (e.x. Every disk with an OS deploys in a bold image format).

Step 3: Understanding Identity & Network

Before you ever think about deploying any form of cloud, you need to think deeply about how you will handle identity and networking. For the benefits of cloud to truly be realized, single sign on and federation are typical core requirements. The network becomes increasingly complex as traffic and routing cross between on and off premise environments.

From the outset, you need to include all key stakeholders from both a business and a technology perspective (network, ID, app deployment) to ensure you aren't overlooking important connection points.

The examples below demonstrate real-world definitions of hybrid identity access and cloud access points for a federal agency's cloud environment.

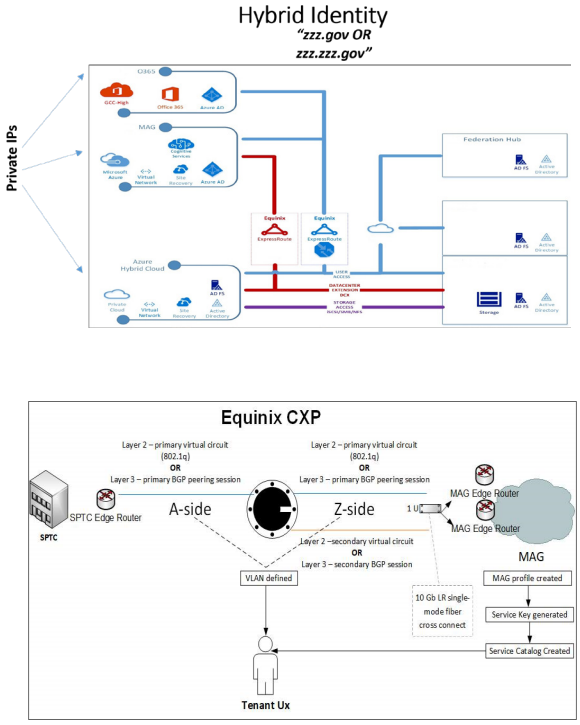

Figure 4: Examples of Hybrid Identity & Cloud Access Points

Step 4: Evolving to the Public Cloud

The cloud is not a single destination, but a journey—and many agencies are using a multi-phased approach to get there. They might start with a small, IaaS delivery on a private cloud to maintain greater control over their data and ensure a seamless end user experience with a consistent level of service. Then, once comfortable, they expand their services "up the stack" to a PaaS environment for their developers. A little bit further down the road, they begin migrating select applications to a SaaS environment—and eventually they find themselves in the public cloud.

There is no "right" way to the cloud. However, the right thing is thinking about cloud migration holistically. You have to ask yourself early on – what are we going to be delivering and what is my phased approach for getting there?

The example below shows a three-year phased approach on Microsoft Azure for a federal agency. As you can see, they started by standardizing IaaS services and providing a consistent UX. In 2020 they plan to expand IaaS with additional services for virtual machine images and hybrid storage. In 2021 they will introduce managed services for disk storage and bulk data.

Microsoft Azure for Government (MAG) Service Catalog			
PHASE	I CY2019 Standardize IaaS services – consistent uX	II CY2020 Expand IaaS with additional services	III CY2021+ Introduce managed services
SERVICE			
Compute			
Virtual Machines	Azure Virtual Machine	Azure Virtual Machine Images	
Pre-defined templates	QuickStart Templates and Blueprints		
Horizontal Scaling		• Virtual Machine Scale Sets • Autoscale	
Server-less		• Functions • Event Grid	
NTP	**Third party (existing license?)		
Containers	Container Service • Azure Kubernetes Service (AKS) • Azure App Service • Azure Container Instances • Azure Batch • Azure Service Fabric • Container Registry	Container Service • Azure Kubernetes Service (AKS) • Azure App Service • Azure Container Instances • Azure Batch • Azure Service Fabric • Container Registry	
Storage	Specify organizational storage regulation/policy; tenant specifies data tiering, RPO, RTO, storage lifecycle.		
Object	Block Blob		
Disk	Disk Storage (HDD/SSD)		Disk Storage – Managed (HDD/SSD)
Shared File System			Files
Archiving	Azure Archive Storage		
Backup	Azure Backup		
Hybrid Storage		StorSimple	
Bulk Data			• Import/Export • Databox

Figure 5: Example of a Phased-approach to Cloud Migration

Conclusion

The bottom line is you cannot talk about the cloud without first understanding the mission. If you have not clearly articulated the drivers behind the technology, it will never deliver the anticipated value or fulfill mission requirements. Additionally, not every agency will make it to PaaS and SaaS, and that is okay. What is important is that your journey to the cloud meets your agency's needs—and that you follow an efficient, streamlined path to get there.

Cloud Lake Technology is a trusted cloud advisor for the federal government. As a Small Disadvantaged Business (SDB) and wholly owned subsidiary of Akima, an Alaska Native Corporation (ANC), our team of experts are deeply qualified and passionate about helping agencies in their journey to the cloud. Our services span the full implementation lifecycle, from planning to post-implementation and support for driving end user adoption and future expansion. We can help your agency evaluate its current environment, plan/prep for migration, implement robust cloud security policies, and perform testing and Disaster Recovery validation in the new cloud environment. Whether you are looking for end-to-end services, or support for only a piece of the transition, our cloud experts stand ready to support you. Learn more at www.cloudlakellc.com.