ATARC

FEDERAL CLOUD & DATA CENTER SUMMIT

JUNE 13, 2018 | MARRIOTT METRO CENTER | WASHINGTON, DC

On behalf of the Advanced Technology Academic Research Center, I am proud to announce the release of a White Paper documenting the MITRE-ATARC Cloud Technology Collaboration Symposium held on April 17, 2018 in Washington, D.C. in conjunction with the ATARC Federal Cloud & Data Center Summit.

I would like to take this opportunity to recognize the following session leads for their contributions:

MITRE Chair: Justin Brunelle

Challenge Area 1: The Next-Gen Cloud: What should we do to prepare?

Government Lead: Dr. Michael Valivullah, USDA NASS
Industry Lead: Scott Robertson, IBM
MITRE Lead: Vidyababu Kuppusamy

Challenge Area 2: DevSecOps: How can it help handle arising cloud security challenges?

Government Lead: Tim Murray, DHS USCIS
Industry Lead: Nate Johnson, Microsoft
Industry Lead: Stephen Kovac, Zscaler
MITRE Lead: Nicole Gong Parrish

Challenge Area 3: Data Center Migration and Consolidation: What Questions Should You Ask?

Government Lead: Bill Hunt, OMB
Industry Lead: Tony Vicinelly, Nlyte Software
MITRE Lead: Mano Malayanur

Challenge Area 4: From Cloud to Edge: Handling IoT in the Cloud

Government Lead: Eric Simmon, NIST
Industry Lead: Matt Mandrgoc, Check Point Software
MITRE Lead: Andrew King

Challenge Area 5: Cloud Migration Aids: Gaps and Successes

Government Lead: Mike Cassidy, DOJ USTP
Industry Lead: Hayri Tarhan, Oracle
MITRE Lead: AJ Bognar

Below is a list of government, academic and industry members who participated in these dialogue sessions:

Challenge Area 1: The Next-Gen Cloud: What should we do to prepare?

Bryant Carroll, MITRE; Ronny Chan, IHS; Jon Chaplin, TechTrend; Jerome Giles, IBM; Tom Harrell, NIH; Steven Hunt, NASA; Mike Lawlor, Peace Corps; Coby Loessberg, Oracle; Daniel Park, DOJ; Bill Patterson, Corning; Clifton Persaud, House of Reps; Faheem Rathore, GSA; Sahar Sadeghian, MITRE; Susan Tsui, DHS ICE; Jeff Willis, MIS Sciences

Challenge Area 2: DevSecOps: How can it help handle arising cloud security challenges?

Donna Glassley, Cisco; Guled Hersi, DOS; Donald Hicks, DOS; Hai Jiang, ARC; Mark Kagan, Panoptes Intelligence; Sean Lang, LOC; Uyen Nguyen, DoD; Joel Offenberg, NASA; Mojgan Pedoeim, IBM; Tammy Rinard, DHS FEMA; Joshua Seely, Peace Corps; Jacob Stenzler, CSRA; Keith Sullenberger, House of Reps; Maggie Trinh, ITA; Josh Ziman, Cisco

Challenge Area 3: Data Center Migration and Consolidation: What Questions Should You Ask?

Brian Bonacci, Equinix; Anne Marie DiNardo, GSA; Colin Ferguson, Corning; Robert Hyers, IRS; Sherman Jones, Treasury; Anton-Marcellus Luddington, DoD; Jared Miller, Corning; Ceresh Perry, USACE; Anupama Rai, LOC; Robert Weaver, DHS

Challenge Area 4: From Cloud to Edge: Handling IoT in the Cloud

Frank Lancaster, Check Point Software; Jay Lippincott, Equinix; Jacques Malebranche, GSA; Michael Moldavsky, Peace Corps; Nadia Nicole Lee, DoS; Kevin Osborne, DHS; Marc Wine, VA

Challenge Area 5: Cloud Migration Aids: Gaps and Successes

Sasikiran Balsa, DOJ; Dharitri Banarjee, CGI Federal; Chris Brehany, DHS; John Broderick, BLM; Rob Creekmore, MITRE; Kevin Cuellar, CGI Federal; Ronald Davis, NIH; Vibha Dhawan, MITRE; Erin Drury, Corning; Jerry Jackson, Carnegie Mellon SEI; Thomas Kale, DoS; Bella Lu, OPM; Chiranjeevi Panuganty, CGI Federal; John Sun, DHS; Dan Twomey, GSA; Audrey Winston, MITRE; Jiam-Mei Wu, DHS FEMA

Thank you to everyone who contributed to the MITRE-ATARC Cloud Collaboration Symposium. Without your knowledge and insight, this White Paper would not be possible.

Sincerely,

George Thomas Suder

Tom Suder
President, Advanced Technology Academic Research Center (ATARC)
Host organization of the ATARC Federal Cloud & Data Center Summit

FEDERAL IT SUMMIT SERIES

JUNE 2018 FEDERAL CLOUD & DATA CENTER SUMMIT REPORT[*]

August 24, 2018

Justin F. Brunelle, AJ Bognar, Vibha Dhawan, Nicole Gong Parrish,
Andrew King, Vidyababu Kuppusamy, Mano Malayanur
The MITRE Corporation

Tim Harvey and Tom Suder
The Advanced Technology Academic Research Center

[*] APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED. CASE NUMBER 18-2725-1.

Contents

1 Abstract

The most recent installment of the Federal Cloud & Data Center Summit, held on June 13, 2018, included five MITRE-ATARC (Advanced Technology Academic Research Center) Collaboration Sessions. These collaboration sessions allowed industry, academic, government, and MITRE representatives the opportunity to collaborate and discuss challenges the government faces in cloud computing and data center modernization. The goal of these sessions is to create a forum to exchange ideas and develop recommendations to further the adoption and advancement of cloud computing and data center management techniques and best practices within the government.

Participants representing government, industry, and academia addressed five challenge areas in the federal cloud and data center domains: The Next-Gen Cloud: What should we do to prepare?; DevSecOps: How can it help handle arising cloud security challenges?; Adapting Data Center Policy for Speedy Cloud Migration; From cloud to edge: Handling IoT in the cloud; and Cloud Migration Aids: Gaps and Successes.

This white paper summarizes the discussions in the collaboration sessions and presents recommendations for government, academia, and industry while identifying intersecting points among challenge areas. The sessions identified actionable recommendations for the government, academia, and industry which are summarized below:

> FedRAMP has been effective at providing guidance, but government practitioners cited a lack of templates for migration, adoption, and acquisition (e.g., reference architectures) for more novice cloud practitioners and organizations. Also desired were initial migration and cloud adoption roadmaps. Future efforts in cloud standardization within the government should focus on providing these resources.
>
> Workforce retention and development remain primary challenges. Government organizations using cloud should continue to emphasize training.
>
> Aligning larger organizations and large numbers of applications during a cloud migration – including prioritization of efforts – is challenging (e.g., maintaining a list of applications to be migrated). Organizations migrating to cloud environments should acknowledge the scale of migration efforts, prepare effectively, and plan for staged migrations.
>
> DevOps can improve the security posturing of applications and assist with migration efficiency and effectiveness, but requires a (potential) cultural change

and team-wide buy-in. Cloud development teams should adopt DevOps best practices and invest in restructuring teams to best adopt agile practices.

2 INTRODUCTION

During the most recent Federal Cloud & Data Center Summit, held on June 13, 2018, five MITRE-ATARC (Advanced Technology Academic Research Center) Collaboration Sessions gave representatives of industry, academia, government, and MITRE the opportunity to discuss challenges the government faces in cloud computing and data center modernization. Experts who would not otherwise meet or interact used these sessions to identify challenges, best practices, recommendations, success stories, and requirements to advance the state of cloud computing and data center technologies and research in the government. Participants ranged from the CTO, CIO, and other executive levels from industry and government to practitioners from government, industry, and MITRE to researchers, students, and professors from academia.

The MITRE Corporation is a not-for-profit company that operates multiple Federally Funded Research and Development Centers (FFRDCs) [12]. ATARC is a non-profit organization that leverages academia to bridge between government and corporate participation in technology. MITRE works in partnership with ATARC to host these collaborative sessions as part of the Federal Cloud & Data Center Summit. The invited collaboration session participants across government, industry, and academia worked together to address challenge areas in cloud computing and data center management, as well as identify courses of action to be taken to enable government and industry collaboration with academic institutions. Academic participants used the discussions as a way to help guide research efforts, curricula development, and to help produce graduates ready to join the work force and advance the state of cloud and data center research and work in the government.

This white paper is a summary of the results of the collaboration sessions and identifies suggestions and recommendations for government, industry, and academia while identifying cross-cutting issues among the challenge areas.

3 COLLABORATION SESSION OVERVIEW

Each of the five MITRE-ATARC collaboration sessions consisted of a focused and moderated discussion of current problems, gaps in work programs, potential solutions, and ways forward regarding a specific challenge area. At this summit, sessions addressed five topics.

- The Next-Gen Cloud: What should we do to prepare?
- DevSecOps: How can it help handle arising cloud security challenges?

- Adapting Data Center Policy for Speedy Cloud Migration
- From cloud to edge: Handling IoT in the cloud
- Cloud Migration Aids: Gaps and Successes

This section outlines the goals, themes, and findings of each of the collaboration sessions.

3.1 The Next-Gen Cloud: What should we do to prepare?

The *The Next-Gen Cloud: What should we do to prepare?* session focused on cloud computing as a disruptive technology for the government agencies and acknowledging that it is likely not the only evolution of computing that will be adopted by the government in the near-term. For example, hyperconvergence and software-defined data centers are already shaping the next stage in the evolution of computing. This session discussed emerging cloud deployment models, future cloud technologies, integration standards and formats, architectures, and services to help the government "get ahead" of future evolutions in cloud computing.

The current approach to cloud adoption predominantly emphasizes modernizing legacy applications and hosting them in the cloud via Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). However, barriers such as government policies (e.g., for organizational and workforce retooling) and long cycles of acquisition are preventing innovation from occurring in cloud adoption.

This session had four key goals:

- Discuss the next generation of cloud services "on the horizon";
- Explore the mechanisms by which government cloud users can anticipate or prepare for next generation cloud adoption;
- Develop recommendations to the government and industry, based on session's discussion, for easing government adoption of the next-generation cloud computing and services; and
- Specifically discuss the notion of hyper-convergence and software defined data centers.

3.1.1 Challenges

The collaboration session discussions identified the following challenges with preparing for the next generation of cloud evolution:

- Lack of strategic direction and approaches;
- Difficulty performing organizational transformation (People, Process, and Technology to support digital transformation); and
- Driving change through building next-generation cloud-native apps.

3.1.2 Discussion Summary

The session began with capturing participants' expectations and the challenges that they encountered in adopting next-generation cloud. Discussion ranged from setting the definition of next-generation cloud to overcoming agencies' cultural barriers in implementing solutions that leverage cloud-native applications. Each identified challenge was discussed at length in the collaboration session. Collation of those discussions revealed common themes that warranted further discussion and collaboration. The following topics were among the most actively discussed in this context:

- Engaging the Senior Leadership Team, FedRAMP Program Management Office (PMO), business, and IT stakeholders to adopt a cloud first strategy to drive change;
- Cultural aspects in identifying and making foundational change;
- Integrating commercial solutions with modernization efforts and technical skills development;
- Security and privacy;
- Evolving technical and operational policies to facilitate adoption of next-generation cloud, cloud migration, and cloud transition; and
- Application rationalization and architecting solutions to meet business objectives and desired outcomes.

Government senior leadership teams and IT managers continue to seek guidance with respect to cloud services and re-usable frameworks and architectures. Specifically, there is a need for architectural guidance in the development of new capabilities to meet business objectives and drive mission outcomes. Application migration, integration of cloud architectures, and deployments of legacy systems continue to evolve. Thus, the government is seeking reference architectures to guide the adoption of next-generation cloud services involving these topics.

The participants also expressed that in certain cases there is a mismatched evolution occurring in their agency with one part of the organization moving fast and the modernization of their mission-critical applications moving slowly. This is in part due to retirement of subject matter experts (SMEs) who are knowledgeable about these mission critical legacy systems and the slow development of new skill sets for existing staff who cannot keep pace with technology. Often, 20% percent of the workforce performs 80% of the work and the more highly-skilled employees are harder to retain due to market conditions. The attrition of these staff members adds to the delays affecting the ongoing modernization efforts.

Digital modernization cannot be fully achieved without retooling an organization's people, processes, and technologies. Maintaining and managing in-house technical expertise is expensive and cannot be sustained over the long term. Building partnership models between public and private sectors will help mitigate some of the risk. Promoting work force management through the business of IT by linking IT investments directly to business outcomes will also be required going forward.

Common service enablement, implementation of the Confidential Information Protection and Statistical Efficiency Act (CIPSEA) [1] and adoption of the shared service model through GSA Center of Excellence (CoE)[1] will enhance interoperability and provide the ability to accelerate cloud adoption.

Data standardization and governance models need to be established (and must remain vendor neutral/vendor agnostics) prior to the adoption of multi-cloud and hybrid-cloud models. The "lift-and-shift" approach is a common cloud migration option, replicating in-house applications in the cloud. Taking this approach without a re-design is not always the most cost-efficient migration strategy, nor does it take full advantage of next-generation cloud offerings. Not all applications are cloud-ready (or even cloud-suitable) and should be treated differently when moving to a cloud-based implementation or deployment. Resource-intensive applications, such as those used for big data analysis and image rendering, are better candidates for re-architecting than lift-and-shift. New technologies such as blockchain [6] and cloud-based solutions (e.g., Artificial Intelligence (AI)) solve specific problems and need to be evaluated thoroughly prior to adoption.

While the use and adoption of next-generation cloud is still an emerging capability in the government, it is evolving more rapidly than the government can react. Emerging cloud architectures are difficult to adopt and need to be developed through public and private partnership models. A *blue ocean strategy*[2] provides strategic agility by focusing on creating

[1] https://www.gsa.gov/about-us/organization/federal-acquisition-service/technology-transformation-services/it-modernization-centers-of-excellence

[2] https://www.blueoceanstrategy.com/what-is-blue-ocean-strategy/

new business value. Emerging architectures should also incorporate security controls that provide conventional risk management capabilities.

In short, participants are calling for reference architectures for next-generation cloud adoption, guidance on where to look, and what to measure.

3.1.3 Recommendations

The participants in the *The Next-Gen Cloud: What should we do to prepare?* collaboration session identified several important findings and recommendations.

Strategic Direction and Approaches: Organizations should develop a sustainable business model for next-generation cloud adoption and develop methods to provide measures (effectiveness and performance) for that business model. Organizations should then have a compelling strategic vision or business case for the cloud that identifies the ultimate goals, values (i.e., return on investment (ROI)), and challenges of the transition. Organizations should also develop an IT modernization roadmap to support their vision. This roadmap should be collaboratively developed with business and IT and should be communicated across stakeholders such as the users, maintainers, and auditors. Some of the key steps include the following:

1. Identify next stages of cloud computing evolution to better match the current application implementations to candidate cloud architectures and technologies;
2. Plan for incorporating next-generation cloud technologies in the strategic mission, vision, goals to align business needs with the proposed IT infrastructure;
3. Develop an IT Roadmap for implementation to ensure necessary resources and funding; and
4. Create a stakeholder-centric strategic technology plan for next-generation cloud to generate a full mapping of business requirements to the proposed technical solution.

Senior leadership should review and update agency cloud goals periodically. It should inspire, energize, and attract commitment to the initiative and be regularly communicated by leadership to all stakeholders. It is critical that senior stakeholders commit to this vision and seek to obtain buy-in from key stakeholders across the organization.

Application modernization is business modernization. Align business priorities and understand where business needs are driving the organization to modernize. Invest in modernization efforts that align with the organization's mission and vision that support the organization's business priorities.

Develop an IT Modernization Roadmap to support next-generation cloud adoption, providing the foundation for a cloud-centric architecture that can help the organization decide on risk management and investment priorities.

People, Process, and Technology to support digital transformation: Strengthen the partnership between IT and business users; organizations should establish integrated project teams, identify SMEs or "power users", and deliver functional software frequently. Some of the key building blocks include the following:

1. Become organizationally agile enough to adopt to changing needs and technologies in terms of workforce alignment, knowledge, skillset, development, and training;
2. Refine or create processes needed to make use of next-gen cloud services; and
3. Build a sustainable infrastructure for solution deployment using a Multi-Cloud or Hybrid Cloud Environment[3].

Disruptive trends in technology force learning organizations to become agile and respond to changes. Agile organizations can take advantage of this digital revolution and bring transformational value to their business.

An Organizational Change Management (OCM) Framework should be adopted to promote agility across the organization (both business and IT). Assess and develop a Knowledge, Skills, & Abilities (KSAs) transfer and training strategy so the organization can effectively operate in the new or transitioning environment.

As cloud technologies integrate components of IT and provide new capabilities, designing and implementing adjustments to an organization will reward the organization for its alignment with change by enabling smoother transitions to the desired end states. Areas for focused change include the organization's structure, roles and responsibilities, human capital, and workforce management practices and policies (e.g., recruiting, hiring, staffing, workload balancing, human resources).

Creating and implementing a communications strategy that clearly articulate the business value of the next-generation cloud, while acknowledging the challenges that the transition may present is another key step toward the desired changes. Establishing specific performance metrics, both for the transition itself and the associated business processes being affected by the transition, is essential for measuring true progress and operational readiness.

A well-designed, centrally managed cloud platform helps agencies meet the requirements of FISMA [2] and FITARA [9] while also giving teams the flexibility to use the technologies and

[3] A hybrid cloud environment utilizes multiple cloud deployment models, such as a combination of private and community clouds [11].

tool chains they determine are most suitable. It also supports the self-servicing of operations, as needed, to deploy and operate their systems.

Digital innovation and transformation provides an organization the opportunity to reinvent itself by rethinking how business can more effectively and efficiently meet the organization's mission. The next-generation cloud provides great opportunity to redesign critical business processes, make them more efficient, and automate them where applicable.

Building next-generation cloud-native apps: As the technology evolves, every user and smart device becomes cloud-enabled. Cloud computing and cloud based presence of people and devices will continue to flourish. The wide spread deployment of smart edge devices – along with many new applications, open APIs, and technology frameworks – created the need to extend the reach of the traditional cloud computing towards the edge. Some of the key building blocks to create next-generation cloud-native apps includes:

1. Identify and leverage emerging computing architectures to develop re-usable frameworks;
2. Establish standards for application integration and data (e.g., exchanges, formats, interoperability, storage/archiving, security); and
3. Plan for continuous integration and continuous deployment.

A layered, hierarchical, and distributed architecture supports building cloud-native applications. Leveraging emerging architectures such as microservice and microservice architectures, serverless framework and serverless architectures, Software-Defined Data Centers (SDDC), Software-Defined Networking (SDN), and Software-Defined Storage (SDS), common APIs, kubernetes, Cloud Native Computing Foundation (CNCF), and cloud foundry can help build the foundation for using the next-generation cloud.

A strong foundation with resiliency and security in the forefront is essential. Containerized middleware and services with prebuilt container images can greatly accelerate solution deployment. Exposing and integrating some the organization's existing applications should be done through APIs. Building reusable assets that can be easily leveraged to build new capabilities, can help to augment existing applications. Integrating other applications into the ecosystem should be accomplished by leveraging a common set of APIs.

Modern cloud deployments require modern practices – when performed properly (via public and private cloud services) – can substantially reduce an organization's investment in infrastructure, shrink the time to deliver services, reduce operational complexity and maintenance costs, and provide better security and compliance outcomes.

Modern agile and DevOps principles and practices need to be employed when building and operating information systems [7]. Using these approaches can substantially reduce cost and time to-market while increasing reliability. Leveraging cloud-based DevOps practices and cloud-native architectures can help meet architectural and security goals, increase utilization, and reduce costs. Employing DevOps (and focusing on the security benefits of DevOps) practices promotes continuous integration and deployment which increase availability, reduce cycle times, and improve auditability.

3.2 DevSecOps: How can it help handle arising cloud security challenges?

The *DevSecOps: How can it help handle arising cloud security challenges?*[4] session discussed cloud security as a continuing, prominent concern with government cloud adoption. This session aimed to discuss the applicability of this concept to cloud adoption, security automation in terms of DevOps, and to identify methods of reducing security risks for cloud adopters.

This session had three goals:

- Recommend approaches for DevOps to improve security for government cloud users;
- Identify challenges for implementing automation in cloud security; and
- Identify specific culture changes and best practices for government to handle the security challenges.

3.2.1 Challenges

The collaboration session identified six challenges with implementing DevSecOps for government cloud adopters.

1. Security training and compliance monitoring is insufficient.
2. Collaboration and communication among teams is often challenging; specific issues include:

[4] This paper recognizes that current industry standard language is still evolving; readers should note that the term *DevSecOps* is often regarded as an unnecessary specification of the inclusion of security into DevOps. In other words, DevOps can be applied to and inclusive of security best practices without requiring that security be specifically included in the term. This paper will use the term DevSecOps to remain consistent with the session title, but acknowledges the differing opinions on the use of the term DevSecOps versus DevOps.

  - Project managers, developers, and security personnel do not *speak the same language*;
  - Security processes are not aligned with the development cycle;
  - Developers need to understand the security requirements and security staff need to understand the development process; and
  - It is not clear what the cloud environment security requirements are and how responsibility ownership is assigned.

3. Understanding the difference between “pass” a requirement and what it means to be “done” when assessing task progress; participants believed the following steps are needed to solve the issues:

   - Create a checklist upfront;
   - Identify the processes and steps must apply; and
   - Define the rules and tools to perform the automation.

4. There is a need to understand good quality code and identify code-defects or vulnerabilities before automation.

5. Special cases in which legacy systems that do not fit the default automated security process complicate the practices.

6. Build continues monitoring scanning profiles for vulnerabilities in the cloud environment.

3.2.2 Discussion Summary

The session started the discussion with the basics on understanding the two terms: “DevOps” versus “DevSecOps”. Industry standards around the terms are still evolving, and the opinions and perceptions of how security is impacted and included in DevOps principles with respect to each term varies.

A traditional model starts with an effort to develop a product or system first, and implement the deployment operations as the next step, then build security into the products, following by the Authority to Operate (ATO) process. The term *DevSecOps* refers to the focus on building and integrating the security into DevOps practices. It is an approach for bridging the traditional gaps between IT security and operations teams to break silo thinking and speed up safe delivery to meet today's agile process approach. The emerging practice requires a change in cultures where these departments were separate. DevSecOps emphasizes building shared ownership and responsibility for the security aspects in the delivery process, eliminating communications and bureaucratic barriers. DevSecOps originally focused on automating security and testing, but now it also encompasses more operations-centric controls.

In today's government IT approach, most organizations adopt the agile methodologies which require the product managers to identify business requirements upfront and organizations to have specific requirements on information sharing (which entails the security requirements to be identified early in the development process). DevSecOps is often associated with a focus on secure DevOps with shared responsibility within the team.

Participants identified the need for education regarding DevOps among stakeholders, to include leadership and security team members, and what – specifically – DevSecOps means for cloud. Because of the ambiguity of this term, there is a need for a lexicon and common language between the development, security, and policy domains. Properly implementing DevOps procedures, incorporating security, and adopting the appropriate culture can help prioritize security needs for a development team. Periodic cross-role-based training events are also needed. Developers need security training to understand what security procedures the operations team must apply and specific requirements for an ATO. Using this approach, security requirements can be built-in. In contrast, the security team needs to understand the develop process and basic development procedures for implementing the security requirements. In addition to training needs, the following items were among the most actively discussed in this context:

- Education and communication;
- Understanding the operation life cycle:
  - How to handle a legacy critical system, including support software and life cycle review, security review;
  - Environment assessment; and
  - Monitoring the environment.
- Gathering the hardware, software inventory, understand the vulnerabilities, risks, and threats; and
- Tools, best practices, understanding FedRAMP risk-based decision, how continuous monitoring Cloud Service Providers (CSP) is handled by FedRAMP authorization.

3.2.3 Recommendations

The participants in the *DevSecOps: How can it help handle arising cloud security challenges?* collaboration session identified the following important findings and recommendations:

- Increase the emphasis on training and education as the highest priority;
- Emphasize team-wide understanding of the operations life-cycle and security requirements in the cloud environment;
- Adopt appropriate culture change and form an integrated team to include developers, security personnel, operation, and testing members into one team;
- Ensure proper understanding of cloud configuration management and automate only good quality code; and
- Leverage tools (specifically, open source tools for automation), follow DevOps best practices, and use FedRAMP for security monitoring strategy guidance.

The session ended by touching on some legal issues, Service Level Agreements, and Organizational Level Agreements discussions. Further discussion on these topics were recommended for a future summit.

3.3 Adapting Data Center Policy for Speedy Cloud Migration

The *Adapting Data Center Policy for Speedy Cloud Migration* session considered the challenges associated with data center migrations, particularly to cloud environments[5]. A spirited discussion ensued on a wide-range of topics starting with understanding the rationale for a push towards cloud adoption, lack of sufficient clarity and knowledge of the portfolio of applications managed by an agency, lack of consideration of the cost of migrations, lack of sufficient guidelines for migrations to cloud environments, and concerns about cloud computing itself.

In response, several solutions were offered by the participants. A starting point for gathering information regarding the applications in an agency is to report an agency's High Value Assets (HVAs) to the Office of Management and Budget (OMB). The process of application rationalization enables agencies to assess – among other things – the applications readiness

[5] This session also served as a follow-on to the August 2017 Federal Cloud & Data Center Summit [4] in which participants shared that the government is typically "good" at using data centers and less so at using cloud environments.

for cloud migrations. FITARA enables agency Chief Information Officers (CIOs) be part of the decision making process. A new guidance on cloud adoption is being planned by OMB in 2019 [10] that is expected to be holistic, and would consider the Data Center Optimization Initiative (DCOI) mandate[6].

This session encouraged the discussion of the types of questions agencies should ask prior to data center migration and examine cloud services and the operation between clouds and traditional data centers. This included the following:

- Recommended cloud policy changes to ease migration and
- Identify specific aspects of government policy specific to successful data center operation (as opposed to cloud).

3.3.1 Challenges

Several challenges were discussed by the session participants related to an agency's efforts in cloud adoption. Key challenges discussed are described below, in no specific order.

- Cost of migrations
- Whether or not DevOps practices should be adopted during migrations
- Unclear rationale for migration
- Lack of knowledge of the applications is often a challenge
- Lack of migration *playbooks*
- Migration prioritization is inexact
- Cloud adoption may cause loss of expertise through *brain-drain* and attrition

3.3.2 Discussion Summary

The discussions around these challenges focused on the challenges unique to data center migration to cloud environments and the associated disciplines that aid in the migration.

During migrations to the cloud from data centers, the costs of cloud adoption are often overlooked; the cost is often hard to quantify for several reasons (e.g., lack of knowledge about the application in the required level of detail, level of readiness of the application to

[6] `https://datacenters.cio.gov`

run in cloud environments). Similarly, the question of whether DevOps processes should be adopted along with migrations was raised during the discussion. The participants suggested that unless process improvements take place along with cloud adoption, there would not be much benefit to cloud adoption.

Often, the motivation and rationale for a migration from a data center to a cloud environment is unclear. Participants mentioned that often, cloud adoptions are pursued due to a mandate, and the rationale for the migrations is either not explained or is poorly defined. The questions to be asked by agencies pursuing cloud migrations need to include "What business problem is being solved?" and "What does success look like?" The problem is compounded by the fact that different stakeholders are involved, including the Congress, OMB, Agency CIO, Bureau CIO, and others. Further, decision makers remain dependent upon SMEs to inform them of best practices due to a lack of in-house deep technical knowledge on migration challenges. For instance, the boundaries of accreditation of an application requires specifics and deep technical knowledge to identify.

Participants mentioned the benefit of having standardized migration practices, but that the resources are sometimes unavailable or unknown. For example, governance processes that should accompany cloud adoption efforts (e.g., feasibility studies and CONOPS), playbooks, and guidelines; these resources are often unavailable. The DHS acquisition life-cycle framework [8] was offered as an example of the existing governance processes with CloudNation[7], cloud.gov[8], and CIO.gov[9] suggested as additional resources. Summits and conferences (such as the Federal Cloud & Data Center Summits) are sources for success stories and best practices. Industry documents often provide step-by-step processes that can inform government starting points for migrations. DCIO also offers approaches to data center optimization including podcasts and templates.

Prior to and during a migration, there needs to be prioritization of what moves to the cloud and that takes in a holistic view of the entire suite of applications. For instance, some applications may never move to the cloud due to their unsuitability for cloud environments.

Finally, the participants cited a lack of talent in the government due to *brain-drain* to industry for higher paying positions. As a result, government teams may not understand the cloud.

[7] http://cloudnation.co

[8] https://cloud.gov

[9] https://www.cio.gov

3.3.3 Recommendations

The participants in the *Adapting Data Center Policy for Speedy Cloud Migration* collaboration session identified several important findings and recommendations.

- Optimization requires application rationalization not just relocating applications to a different set of racks.
- OMB required reports contain first pass of the details of applications (HVAs).
- FITARA empowers CIOs by “bringing them to the table” (as decision-makers and policy makers).
- Cost analyses and comparisons need to be done; some examples are shallow, but others are solid.
- Cloud adoption has huge workforce implications that must be recognized and for which agencies must be prepared.
- OMB is planning the release of a new, holistic cloud policy/guidance that takes into account many considerations including the expiring DCOI mandate.

3.4 From cloud to edge: Handling IoT in the cloud

The *From cloud to edge: Handling IoT in the cloud* session discussed the Internet of Things (IoT) as a pervasive technology and is nearly constantly enabled or paired with cloud computing. As adoption of these devices continues, it will be increasingly important for the government to provide cloud services to enable their performance (e.g., via data analysis services). This session focused on the actions that the government can take to prepare cloud services and environments to support IoT. Smart cities, public safety, and traffic are all potential topics impacted by the discussions during this session, along with discussion on the unique challenges or best practices for handling IoT data in a cloud and exploring the data handling and service recommendations to and from IoT endpoints.

This session had three goals:

- Identify actions the government can take to prepare their cloud services for IoT;
- Recommended investments for IoT data services; and
- Identify the role – or the needs – of industry products to enable IoT endpoints to consume cloud data.

3.4.1 Challenges

The collaboration session discussions identified several challenges with cloud-enabled IoT architectures.

- **Provisioning and management** What would an IoT edge and constrained device provisioning strategy entail? Secure and consistent update techniques and procedures, inclusive of rollback features, are paramount.
- **Data strategy** What fundamentals should be considered when establishing an IoT to cloud data strategy? This includes data formats, data security and integrity, semantics, transport protocols, and the idiosyncrasies associated with connecting heterogenous (and perhaps incompatible) IoT edge and constrained devices to standardized cloud services.
- **Provenance and ownership** How is the legitimacy of generated and stored data determined? Who owns it once we have it (e.g., it is stored in the cloud, although generated at the edge)? How is governance established once the data crosses the boundary between the edge and the cloud?
- **Metrics** How do we determine "value"? That is, what metrics can be employed to measure the utility of any generated, stored, and processed data?

3.4.2 Discussion Summary

As can be gleaned from the key challenges discussed in the previous section, there was a very active discussion on the challenge topics.

Most of the conversations centered on three core themes: the IoT edge (what is it and where does it start and end), the context (how does the information from the edge get utilized), and the cloud data (final resting place of "the context" – what is it, how does it get used, how is it protected, who owns it, etc.).

The group's discussion focused on the establishment of best practice guides to help address these challenges – not as an effort to proscribe a specific solution, but as a driver for the creation of a clarification reference that explores both the *lingua-franca* of IoT and cloud integration, and generalized approaches for managing specific IoT to cloud challenges.

3.4.3 Recommendations

The participants in the *From cloud to edge: Handling IoT in the cloud* collaboration session identified several important findings and recommendations.

- **Provisioning and management** Various open source and commercial projects exist for provisioning and managing IoT edge and constrained devices which provide a mechanism for addressing this challenge area. With this in mind, the collaboration session participants discussed the importance of establishing an IoT device provisioning "best practices guide" in which devices are categorized by their type (in terms of industry utilization and capability). This effort would ideally be a collaboration between government, industry, academia, and consortia.
- **Data strategy/provenance/ownership** Various data messaging formats and session-layer protocols exist enabling IoT device to cloud communications. As noted previously, various challenges exist when considering how best to manage and govern this data. The participants' recommendation is to establish an IoT to cloud data strategy development guide that assists the reader in establishing a context for asking, and answering, many of the questions posed by the aforementioned challenge. As with the previously recommendation, this effort would ideally be a collaboration between government, industry, academia, and consortia.
- **Metrics and value** Perhaps less important for industry and more relevant for government is the establishment of key data generation, collection, storage, and utilization metrics to assist with ascertaining the value of IoT investments and the data these systems provide via cloud-based services for public consumption.

In summary, the collaboration session uncovered numerous challenges associated with handling IoT in the cloud, and identified steps that would be helpful for both government and industry to address these areas of concern, especially as more data collection devices are connected to the internet.

3.5 Cloud Migration Aids: Gaps and Successes

The *Cloud Migration Aids: Gaps and Successes* session discussed the increasing need for migration planning and management tools by Federal Government cloud adopters. However, these tools are often scarce, vendor-specific, or custom-designed (i.e., with limited reusability).

This session focused on migration efforts, success stories, and future needs from the perspective of the tools and aids used in the migration process. The discussions included migration success stories and associated tools used, identified gaps in current government migration tools and aids, and the benefit, applicability, and requirements for future migration aids.

This session had three goals:

- Recommended migration tool requirements;
- Itemized properties of successful migration activities and associated tools; and
- Identified potential role of migration aids in government cloud efforts.

3.5.1 Challenges

The collaboration session discussions identified the following challenges facing the use of cloud migration tools:

- The IT workforce needs new skills to help federal agencies migrate to and operate in the cloud;
- Traditional network transport capabilities and practices within federal agencies hinder cloud migration activities;
- Cloud migration and adoption compels federal agencies to reconsider how to implement and manage security; and
- Cloud billing is complex and requires detailed management and expertise.

3.5.2 Discussion Summary

The discussion during this session focused on a few major threads:

- The need for the IT workforce to maintain expertise;
- The need of organizations to consider the impacts of traditional networks and the constraints they impose on cloud;
- The need to revise traditional security management approaches to support cloud migration and adoption;

- Cloud billing and cost management; and
- The ability to of organizations to share recommendations, best practices, and lessons learned across the community.

The session participants discussed the need for the IT workforce to be experts in both procurement of cloud services as well as the management of cloud resources and services.

The participants also discussed the need of government adopters to consider the impacts of traditional networks and the constraints they impose on cloud adoption. Trusted internet connections (TICs) continue to limit access to the cloud. The diversity and numbers of routers across the network create multiple points of failure and potential network traffic bottlenecks. The diversity and numbers of firewalls across the network create multiple points of failure and potential network traffic bottlenecks. There is also insufficient accountability of network devices such as firewalls and routers. Field sites require sufficient bandwidth to access cloud resources and services (testing is required to identify acceptability). There remains a coordination gap between government cloud adopters, CSPs, and telecommunications service providers. Finally, the participants mentioned that using meet-me points should be used that allow for well-managed concentration hubs between cloud and telecommunications providers.

The topic of security management approaches and cloud migration focused on recommended best practices and guidelines. Government adopters should revise traditional security management approaches to support cloud migration and adoption. Cloud security is shared between the CSP and government adopter. As part of the shared security, the stakeholders should determine if the monitoring logs stored in the CSP's environment contain sensitive data and could have a potential impact on Federal agency's security requirements. In conjunction, security monitoring tools are critical and adopters should review on-premise tools and see if they are adequate to manage/monitor cloud services. Cloud-native security monitoring tools may provide better capabilities than traditional on-premises solutions for cloud services. Regardless of approach, all services require monitoring, including alerting as necessary. Federal agencies need to be aware of what cloud services are or are not FedRAMP authorized.

A common topic of discussion at past cloud summits is the need to effectively manage billing from CSPs. This session's participants recommended that CSPs provide detailed billing information that can be overwhelming to validate for correctness. At a minimum, federal agencies need to have a "Cloud Billing Expert" who can readily discern billing inconsistencies. In addition, commercial tools are available that can help parse out the billing to the appropriate organization, department or group within the Federal agency.

There is also a need to effectively share cloud migration and adoption lessons learned and best practices across federal agencies. Many federal agencies have made significant advances in migrating applications to the cloud and in acquiring cloud services. Any one federal agency may capture the lessons it has learned or best practices implemented in their cloud journey. However, this information is not easily shared due to many factors – federal IT members extremely busy especially folks with cloud expertise, sensitive information where sharing is limited, etc. Deliberate and effective sharing of lessons learned and best practices has the potential to drive down future costs for implementing cloud computing across the Federal government.

Lastly, the participants discussed the the wide variety of tools available in the marketplace to help manage the migration of applications to the cloud and to assist with managing applications once deployed to the cloud. These tools can be categorized as having pre-migration, migration, and post-migration capabilities. Pre-migration tools provide capabilities to assess the cloud readiness of applications, right-size applications for cloud hosting, determine suitable cloud hosting environments for applications and perform cost analysis for cloud hosting. Migration tools provide capabilities to provision, configure, and deploy applications to the cloud. Post-migration tools provide capabilities to manage and optimize hosted applications in the cloud and to support cloud operations. Some capabilities include workload optimization, cost optimization, and aggregated invoicing to support chargeback.

3.5.3 Recommendations

The participants in the *Cloud Migration Aids: Gaps and Successes* collaboration session identified several important findings and recommendations.

Federal agencies should develop and implement training programs to grow a work-force. This workforce should have the following features and characteristics:

- Understands cloud procurement activities and the ability to effectively coordinate and communicate cloud service requirements to the contracting officer;

- Understands the differences between what a CSP can deliver vice what is advertised;

- Understands the long-term commitments associated with contracting with a CSP and the implications of vendor-lock in;

- Teaches the correct skill sets to manage cloud migration and adoption activities;

- Plans and implements DevOps in an agile environment;
- Increases coordination among the federal agency lines of business owners, contracting officer and CSP; and
- Develops a training plan for cloud adoption within an agency.

Federal agencies need to enable network accessibility to the cloud. Cloud adopters should focus on reevaluating and – as necessary – rearchitecting overly complex network designs, including the reduction and/or consolidation of firewalls and routers. They should also increase discovery capabilities to identify and inventory all network devices and consider the use of meet-me points to mitigate current TIC challenges. Another recommendation is to consider the reduction in the number of field sites to reduce network demands. Adopters should increase coordination among the federal agency lines of business owners, contracting officer, and CSP. Similarly, adopters should increase coordination among government, CSPs, shared service providers and telecommunications providers. Finally, there should be an investment in increasing discovery and inventory of all network devices to include firewalls and routers.

Federal agencies need to revise their security approach for operating in the cloud. This includes reevaluating and, as necessary, rearchitecting overly complex network designs, including the reduction and/or consolidation of firewalls and routers. The IT providers should focus on increasing discovery capabilities to identify and inventory all network devices as well as assigning the security management and monitoring requirements between the federal agency, CSP and third party managed service providers. Project owners should consider conducting security tool *bake-offs* to determine best fit for the federal agency, including cloud-native vice on-premises security tools. If an on-premise security solution exists, consider a hybrid approach to include cloud-native security monitoring, as well.

Federal agencies need to develop and implement a cloud billing management capability. At a minimum, identify and train at least one individual on understanding cloud billing and services cost model; this may include the need to certify the individual for a CSP (e.g., architect level to fully understand cloud services). Government agencies should consider how to expand billing expert capabilities across the federal agency to at least the department level (e.g., the basic organizational unit of cloud services consumption). Cloud managers should implement tagging which allows the costs of cloud resources to be associated with a unique organization, department or group and facilitates chargeback and invoicing. To drive down cloud computing costs, use automated tools to analyze cloud resource utilization including identification of resources that are over-provisioned to drive down cloud costs. Finally, agencies should analyze the cloud bill on a regular basis to help detect anomalies/inefficiencies in the usage of cloud services for the agency.

Federal agencies need to conduct market research on tools available in the marketplace that can expedite cloud migration activities or support cloud operations. Federal agencies need to share lessons learned and best practices on cloud migration and adoption activities. This includes continuing to participate in government-wide cloud forums, such as the Federal Cloud & Data Center Summit, to be able to exchange lessons learned and best practices. Further, General Services Administration may want to consider establishing an electronic forum where federal agencies can post lessons learned and best practices; this media could also provide a section for CSPs to share best practices.

4 Summit Recommendations

As with past Federal Cloud & Data Center Summit discussions, the collaboration sessions discussions had a common set of themes.

FedRAMP has been effective at providing guidance, but government practitioners cited a lack of templates for migration, adoption, and acquisition (e.g., reference architectures) for more novice cloud practitioners and organizations. Also desired were initial migration and cloud adoption roadmaps. Future efforts in cloud standardization within the government should focus on providing these resources.

Workforce retention and development remains a primary challenge. Government organizations using cloud should continue to emphasize training, and identify creative ways to incentivize workers to remain in the public sector.

Aligning larger organizations and large numbers of applications during a cloud migration – including prioritization of efforts – is challenging (e.g., maintaining a list of applications to be migrated). Organizations migrating to cloud environments should acknowledge the scale of migration efforts, prepare effectively, and plan for staged migrations. This complexity is amplified with the relationship between IoT, data centers, and the target cloud environment.

DevOps can improve the security posturing of applications and assist with migration efficiency and effectiveness, but requires a (potential) cultural change and team-wide buy-in. Cloud development teams should adopt DevOps best practices and invest in restructuring teams to best adopt agile practices to bridge the gaps between decision makers, practitioners, and SMEs.

5 Conclusions

The June 2018 Federal Cloud & Data Center Summit highlighted several challenges facing the Federal Government's adoption of cloud computing and data center modernization efforts.

- There is an increasing desire and need for standardized guides for cloud adoption, migration, and use.
- Government recognizes a need to creatively incentivize cloud experts to stay in government to prevent brain drain to industry.
- Acquisition and budgeting remains a challenge, and the challenge is amplified by the complex relationship between IoT, data centers, and cloud.
- There is a need to bridge the gap between decision makers, practitioners, and industry SMEs.

The session participants identified various recommendations for overcoming these challenges (Section 4). While cloud is becoming more mainstream in government IT, there are still challenges in the areas of security, migration, and acquisition. The ATARC working groups [3] are continuing to investigate these concerns, as will future summits. The trends from prior summits [5, 4] suggest that the challenges identified this year will continue to be mitigated through the various efforts within government, academia, industry, and standards bodies.

Acknowledgments

The authors of this paper would like to thank The Advanced Technology Academic Research Center and The MITRE Corporation for their support and organization of the summit.

The authors would also like to thank the session leads and participants that helped make the collaborations and discussions possible. A full participant list is maintained and published by ATARC on the FedSummits web site[10].

[10] https://www.atarc.org/events/cloud-summit-2018-06-13/

REFERENCES

[1] 107th United States Congress. Confidential Information Protection and Statistical Efficiency Act of 2002. https://www.bls.gov/bls/cipsea.pdf, 2002.

[2] 113th Congress. Federal Information Technology Acquisition Reform Act (FITARA). https://www.congress.gov/bill/113th-congress/house-bill/1232, 2014.

[3] ATARC. ATARC Cloud Innovation Lab. https://www.atarc.org/working-groups/cloud/, 2017.

[4] J. F. Brunelle, S. Anand, G. Barmine, M. Spina, K. Warren, A. Winston, M. Javid, A. Kemmer, C. Kim, S. Masoud, T. Harvey, and T. Suder. August 2017 ATARC Federal Cloud & Data Center Summit Report. Technical report, The MITRE Corporation; The Advanced Technology Academic Research Center, 2017.

[5] J. F. Brunelle, S. Anand, R. Cagle, C. Kim, M. Kristan, M. Spina, K. Warren, T. Harvey, and T. Suder. February 2017 ATARC Federal Cloud & Data Center Summit Report. Technical report, The MITRE Corporation; The Advanced Technology Academic Research Center, 2017.

[6] D. Bryson, D. Penny, D. C. Goldberg, and G. Serrao. Blockchain Technology for Government. Technical report, The MITRE Corporation, 2017.

[7] M. Casagni, M. Heeren, R. Cagle, R. Eng, J. Flamm, S. Goldrich, D. Hanf, M. Kristan, J. F. Brunelle, T. Suder, and T. Harvey. March 2018 Federal DevOps Summit Report. Technical report, The MITRE Corporation; The Advanced Technology Academic Research Center, 2018.

[8] Department of Homeland Security. Acquisition Management Directive. https://www.dhs.gov/sites/default/files/publications/01.%20Directive%20102-01%20Acquisition%20Management%20Directive_0.pdf, 2015.

[9] Department of Homeland Security. Federal information security modernization act (fisma). https://www.dhs.gov/fisma, 2016.

[10] S. Friedman. OMB drafts new 'Cloud Smart' strategy. https://fcw.com/articles/2018/06/13/cloud-smart-omb-friedman.aspx, 2018.

[11] P. Mell and T. Grance. The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology. Technical Report Special Publication 800-145, National Institute of Standards and Technology, 2011.

[12] The MITRE Corporation. FFRDCs – A Primer. `http://www.mitre.org/sites/default/files/publications/ffrdc-primer-april-2015.pdf`, 2015.