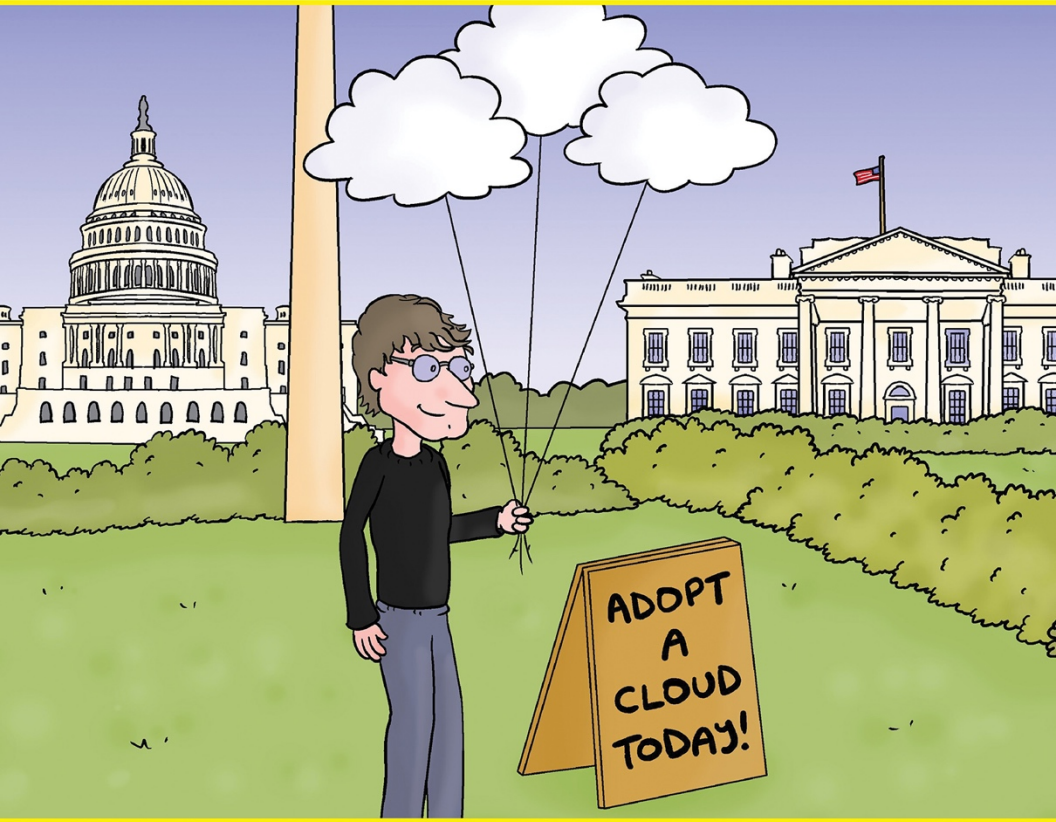
ConversationalGeek®

Conversational Cloud Adoption in Federal Government

By Andrey Zhuk (Cloud Solutions Architect, CTG Federal)



In this book, you will learn:

- How to be smart about adopting cloud within your agency.
- The basics of cloud planning as well as some of the common misconceptions.
- Some of the keys tools available to help you on your cloud journey.

Sponsored by

DELL Technologies

vmware®

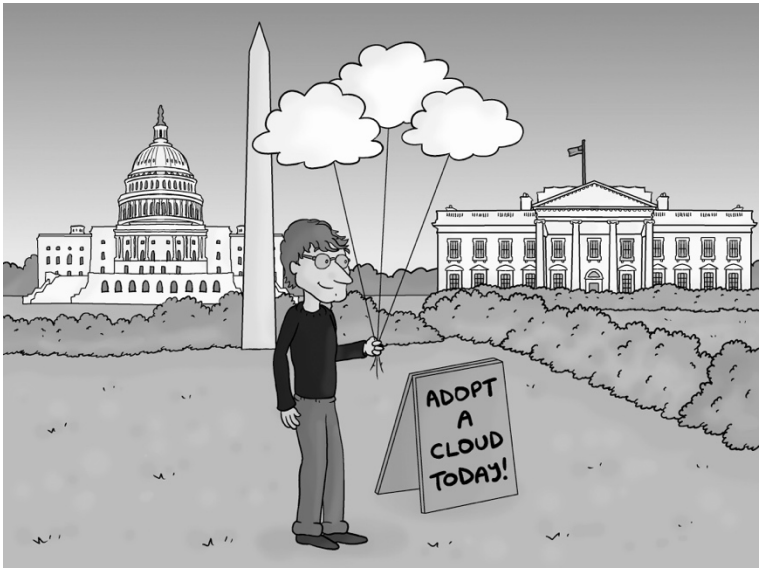
Sponsored by Dell Technologies and VMware

Dell Technologies is a unique family of businesses that provides the essential infrastructure for organizations to build their digital future, transform IT and protect their most important asset, information. The company services customers of all sizes with the industry's most comprehensive and innovative portfolio from the edge to the core to the cloud.

VMware Government Solutions leverage two decades of success and innovation in the government data center to transform agency operations and mission outcomes in the Digital Age. Our interoperable compute, cloud, mobility, networking, and security solutions form a secure and flexible digital foundation that enables agencies to reliably deliver the apps, services, and experiences changing government operations and society. Agencies leverage VMware solutions as part of their long-term IT modernization strategy, building and maintaining more secure, resilient, and modern information technology to enhance mission delivery, drive new value and efficiencies, and improve citizen engagement and satisfaction with agency services the world over.

Conversational Cloud Adoption in Federal Government

By Andrey Zhuk



ConversationalGeek®

Conversational Cloud Adoption in Federal Government

Published by Conversational Geek® Inc.

www.conversationalgeek.com

Trademarks

Warning and Disclaimer

Additional Information

For general information on our other products and services, or how to create a custom Conversational Geek book for your business or organization, please visit our website at ConversationalGeek.com

Publisher Acknowledgments

All of the folks responsible for the creation of this guide:

Author:	Andrey Zhuk
Project/Copy Editor:	Pete Roythorne
Content Reviewer(s):	Bettina Chavanne
	Jeremiah Sanders
	Mansour Yusuf
	Crissy Gafney

Note from the Author

Hello and welcome. On behalf of the entire Conversational Geek family, I would like to personally thank you for picking up a copy of Conversational Cloud Adoption in Federal Government ebook. The goal of this publication is to provide a 101-level introduction to cloud computing and, more specifically, adoption of cloud technologies by the U.S. Federal Government.

There is a lot of information floating around the internet about the benefits of cloud, cloud policy, migration strategies, technical challenges, misconceptions, etc. This ebook condenses all that information into concise bits of knowledge that you can easily use in your future cloud conversations with friends, colleagues, and customers.

Andrey Zhuk

Cloud Solutions Architect

CTG Federal

The “Conversational” Method

We have two objectives when we create a “Conversational” book: First, to make sure it’s written in a conversational tone so that it’s fun and easy to read. Second, to make sure you, the reader, can immediately take what you read and include it into your own conversations (personal or business-focused) with confidence.

These books are meant to increase your understanding of the subject. Terminology, conceptual ideas, trends in the market, and even fringe subject matter are brought together to ensure you can engage your customer, team, co-worker, friend, and even the know-it-all Best Buy geek on a level playing field.

“Geek in the Mirror” Boxes

We infuse humor into our books through both cartoons and light banter from the author. When you see one of these boxes it’s the author stepping outside the dialog to speak directly to you. It might be an anecdote, it might be a personal experience or gut reaction and analysis, it might just be a sarcastic quip, but these “geek in the mirror” boxes are not to be skipped.

Greetings. Within these boxes I can share just about anything on the subject at hand.

Read ’em!

Federal Government Adoption of the Cloud

"I'd like the Gov't Cloud with everything on it."

In order to understand the U.S. federal government's approach to cloud adoption, one must first grasp how policy drives those decisions.

We'll start with how "Cloud Smart" lays out a clear plan for adopting cloud at your agency. We'll then review the basics of planning for data migration, the practical challenges of migrating to the cloud, and also debunk some myths

surrounding cloud adoption. We will end with a practical section on some of the industry tools available to help you on your cloud journey.

US Federal Government and the Cloud: A Brief History

In order to understand the drivers behind federal government's approach to cloud migration, it is worth briefly reviewing the key milestones that have shaped government cloud adoption so far.

Planning for Cloud Adoption

In December 2010, the White House published a "25-Point Implementation Plan to Reform Federal IT Management"[1] laying out the groundwork for cloud adoption by federal agencies.

Cloud First

In February 2011, the White House published the "Federal Cloud Computing Strategy," which became known as the "Cloud First" policy[2]. The policy alluded to the Federal Risk and Authorization Program (FedRAMP), which was officially

---

[1] Vivek Kundra, U.S. Chief Information Officer, A 25-Point Implementation Plan to Reform Federal IT Management, December 9, 2010, **www.dhs.gov/sites/default/files/publications/digital-strategy/25-point-implementation-plan-to-reform-federal-it.pdf** ("25-Point Plan").

[2] Vivek Kundra, U.S. Chief Information Officer, Federal Cloud Computing Strategy, February 8, 2011, **obamawhitehouse.archives.gov/sites/default/files/omb/assets/egov_docs/federal-cloud-computing-strategy.pdf** ("Cloud First").

established later that year by the Office of Management and Budget (OMB).

FedRAMP PMO Established

In 2012, the General Services Administration (GSA) established the FedRAMP Program Management Office (PMO). The FedRAMP PMO mission is "to promote the adoption of secure cloud services across the federal government by providing a standardized approach to security and risk assessment[3]."

Cloud Smart

In June 2019, the federal CIO issued the Cloud Smart Strategy to provide agencies with practical implementation guidance to achieve the potential of cloud-based technologies. The new strategy is founded on three key pillars of successful cloud adoption: security, procurement, and workforce.

As Suzette Kent, former U.S. federal CIO, explains: "These elements embody the interdisciplinary approach to IT modernization that the federal enterprise needs in order to provide improved return on its investments, enhanced security, and higher quality services to the American people."

Federal Cloud Computing Strategy – The Official Line in a Nutshell

Understanding official policy is important for navigating the cloud adoption journey within the federal government. The policy that governs federal cloud adoption is the 2019 Cloud Smart Strategy, and its three pillars (security, procurement, and workforce).

---

[3] Steven Van Roekel, Federal Chief Information Officer, FedRAMP Policy Memo, December 8, 2011, **www.fedramp.gov/assets/resources/documents/FedRAMP_Policy_Memo.pdf**

The Cloud Smart Strategy "encourages agencies to think of cloud as an array of solutions that offer many capabilities and management options to enhance mission and service delivery." Next, "Cloud Smart operates on the principle that agencies should be equipped to evaluate their options based on their service and mission needs, technical requirements, and existing policy limitations."

Finally, "agencies need to weigh the long-term inefficiencies of migrating applications as-is into cloud environments against the immediate financial costs of modernizing in advance or replacing them altogether."[4]

Understanding the official guidance can be helpful in leading your customers on the cloud adoption journey and ultimately being able to support their mission.

Now let's look at the three pillars we mentioned above.

Pillar I: Security

This section of the Cloud Smart Strategy calls for focus on the data layer, and moving protection closer to where data resides. Traditionally, the focus of security was on network and physical infrastructure layers. With migration to the cloud, these are becoming abstracted due to the change in responsibility of these layers to cloud providers. So the focus is shifting to the actual data. The 2019 Cloud Smart security pillar also brings

---

[4] Suzette Kent, U.S. Federal Chief Information Officer, Federal Cloud Computing Strategy, June 24, 2019, **www.whitehouse.gov/wp-content/uploads/2019/06/Cloud-Strategy.pdf** ("Cloud Smart")

attention to complying with existing security policies and programs. These programs are Trusted Internet Connections (TIC)[5], Department of Homeland Security (DHS) Continuous Diagnostics and Mitigation (CDM) Program[6] and FedRAMP.

It is worth noting that adoption of cloud services in federal government is forcing changes to the traditional TIC hub-and-spoke paradigm. The new draft TIC 3.0 guidance documents[7] advocate for Zero-Trust Architecture approaches and recommend a direct-to-CSP connectivity model, while also embracing next generation security technologies, such as Cloud Access Security Broker (CASB) and Secure Access Secure Edge (SASE).

On the FedRAMP front, when selecting cloud vendors for your agency, make sure to check with FedRAMP Marketplace[8] to see if the vendor is FedRAMP Authorized and at what security level (Moderate / High / FedRAMP+). We'll provide a table summarizing these classification levels later in this ebook.

SASE (pronounced Sassy), a Gartner-coined term, is really starting to take off. Not so long ago we talked about web gateways as a service, CASBs, and VPNs. Now the marketplace is shifting to offer "Security Stack in the Cloud as a Service." Many vendors are jumping on board, including VMware, Menlo, McAfee, Netskope, Palo Alto Networks, and Zscaler.

---

[5] www.cisa.gov/trusted-internet-connections

[6] www.cisa.gov/cdm

[7] www.cisa.gov/publication/tic-30-core-guidance-documents

[8] marketplace.fedramp.gov/

Pillar II: Procurement

The second pillar focuses on cloud technology procurement and cloud vendor management. This section calls for smarter contracting practices to eliminate duplication of services, and emphasizes minimizing overall cost to the government. This is what's referred to as "Category Management." I invite you to read the official OMB Memo M-19-13[9].

The procurement pillar also addresses cloud Service Level Agreements (SLAs). The cloud has brought forth changes in the traditional "SLA." Cloud Smart Strategy encourages procurement organizations to review Title 48, § 12.301 of the Federal Code of Regulations (CFR)[10] to make sure they are including appropriate contractual clauses.

Finally, the procurement pillar covers security requirements for contracts based on the federal CIO's High Value Asset (HVA) memorandum[11]. In a nutshell, "agencies must now ensure that contracts impacting their HVAs, including those managed and operated in the cloud, include requirements that provide agencies with continuous visibility of the asset."

Pillar III: Workforce

The final pillar calls on government agencies to upskill, retrain, and recruit key talent for cybersecurity, acquisition, and cloud engineering. Key topics covered include:

---

[9] M-19-13, Category Management: Making Smarter Use of Common Contract Solutions and Practices, March 20, 2019, **www.whitehouse.gov/wp-content/uploads/2019/03/M-19-13.pdf**

[10] Code of Federal Regulations, Title 48, § 12.301, **www.govinfo.gov/content/pkg/CFR-2014-title48-vol1/pdf/CFR-2014-title48-vol1-sec12-301.pdf**

[11] M-19-03, Enhancing the High Value Asset Program, December 10, 2018, **www.whitehouse.gov/wp-content/uploads/2018/12/M-19-03.pdf**

- Identifying skill gaps for current and future work roles
- Reskilling and retaining current federal employees
- Recruiting and hiring to address skill gaps
- Employee communication, engagement, and transition strategies
- Removing barriers to hiring talent expeditiously

The workforce section includes extensive references to various legislature, policies, and labor laws, as well as the NIST Cybersecurity Workforce Framework (NIST SP 800-181)[12]. If you're a federal government leader involved in human resource management, you should review the Cloud Smart Strategy document and familiarize yourself with the referenced documents.

Federal IT Modernization Considerations for Cloud Adoption

Now that we have the policy stuff covered, let's get technical and geek out a little. I would like to begin by sharing some insights from my colleague, recently retired Lieutenant Colonel Jeremiah Sanders of the United States Air Force (USAF), a co-founder of Kessel Run, who now serves as Federal Strategist for VMware. Below are general considerations for IT modernization vis-à-vis cloud.

You know your agency's mission and key requirements and are looking to keep IT modernization toward the top of your priority list. How do you select vendors/cloud providers while

---

[12] National Institute of Standards and Technology, National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework, NIST Special Publication 800-181, August 2017, csrc.nist.gov/publications/detail/sp/800-181/final

watching your agency's bottom line? Here are five key things to keep in mind:

1. The number one rule of retaining relevance in the digital age is: Don't build what you can buy, and don't buy what you can rent. It is imperative to employ a modular, consumption-based approach to enterprise services across the tech stack and to select solutions that prevent lock-in and ensure long-term portability and the *power of choice* for underlying CSPs.

   As you move up the tech stack, managed configuration and automation services from CSPs and other vendors are powerful tools that make it easier for your software developers to build and deliver applications at scale, and the government should absolutely leverage these vendor-managed capabilities.

   However, the government must pay careful attention to ensure these powerful abstraction layers and services don't lock the applications and data into competition-crushing CSP environments. Ensure these abstractions afford CSP-agnostic portability to support multi-cloud and hybrid-cloud operations.

2. Maximize the power of layered abstraction and automation through the entire tech stack.

3. Reduce the barrier to entry and recurring training costs for your team by deploying simplified solutions that solve many hosting and management problems at scale. These should be consolidated to as few panes of glass as possible, across the hybrid cloud landscape. This approach reduces the cost and complexity of managing and securing cloud-native apps and legacy systems in the inter-years of digital transformation.

4. Take a critical, bare-metal-up look at the solution space with a preference for software-defined networking, datacenter, infrastructure, cloud management platforms, application development and ops management platforms, security, and digital end-user workspace solutions. Niche appliances should rarely be a part of your tech stack any longer. You want to consolidate on software-defined solutions for ease of configuration, deployment, recurring operations cost, and plug-and-play replacement as the IT rate of change affords more elegant solutions.

5. Another factor in choosing those modular, software-defined abstraction layers should be their ability to deliver built-in, validated configuration and deployment automation, as well as cloud-centric machine learning/artificial intelligence (ML/AI) management engines that elevate the value proposition by driving operational efficiencies and reducing labor costs.

Planning for Cloud Migration

In terms of a practical approach to cloud migration, the steps are similar whether you are operating in a commercial environment or within the confines of a federal agency.

When working with the government, bureaucracy is unavoidable. If your agency is moving to the cloud, having a simple checklist of workloads to migrate is not sufficient. You probably want to start with a strategy document that provides a high-level overview of your agency's mission and use cases, and how those use cases will be enhanced by using cloud. Here are some items to consider in your strategy document:

- Types of services your agency is looking to adopt: IaaS, PaaS, or SaaS

- Type of cloud you are migrating to (public, private, hybrid)
- Single CSP or multi-cloud (this is most applicable to IaaS)
- Risk Management Framework (use NIST SP 800-37 Rev 2 for this)[13]
- Budgeting
- Management
- Security
- Types of data stored in the cloud and required protections
- Compliance and regulations pertaining to data in motion and data at rest
- Disaster Recovery (DR) and Continuity of Operations (COOP) requirements
- Stakeholder communication and notification requirements

Once your cloud migration strategy has been formalized and approved, we can move on to the practical planning of the migration. (VMware has a great Quick Reference guide to get you started[14], too.)

1. Start with defining stakeholders, roles, and processes.

---

[13] National Institute of Standards and Technology, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, NIST Special Publication 800-37 Rev. 2, December 2018, csrc.nist.gov/publications/detail/sp/800-37/rev-2/final

[14] VMware, Practitioners Quick Reference for Cloud Migration, March 2019, vforum.vmware.com/content/dam/digitalmarketing/vmware/en/images/microsites/apj-vforum/au-pdf/multi-cloud/vmware-a-practitioners-guide.pdf

2. Identify the business or mission functions you want to migrate to the cloud.
3. Identify dependencies and associated workloads. This is critical for understanding the scope of your migration.
4. Use quantitative and qualitative strategies to evaluate workloads and select the appropriate "5-R's" migration strategy for each:
    a. Retain – Optimize and Retain existing app, as-is
    b. Rehost/migrate – move app to cloud and rehost. This is a potential interim step used to reduce legacy infrastructure footprints and consolidate app operations alongside cloud-native and containerized workloads in the intra-years of digital transformation.
    c. Replatform – Put apps in containers and run in Kubernetes (K8s). This is a common approach when legacy implementation has limited technical debt and the expected frequency of functional changes is limited.
    d. Rewrite – Rewrite apps using cloud native technologies. This is common with high technical debt legacy implementations where frequent functional changes are expected.
    e. Retire – Retire traditional apps and convert to new SaaS apps. Government business operations use-cases such as HR, financial management, logistics management, payroll, healthcare, etc. are ripe for this use case.
5. Formulate design requirements:
    a. Compute, storage, network, and data protection requirements. Remember, the cloud is elastic, and the power of modern

application development approaches is in the delivery of mission value at speed while retaining built-in flexibility, abstraction, and anti-fragility, allowing for an amorphous architecture as underlying infrastructure needs of the apps change.

   b. Security and compliance requirements.

   c. Change management and automation requirements.

   d. Application development and application lifecycle requirements.

6. Define project timetable.
7. Define initial key performance indicators (KPI).
8. Based on design requirements and size of the cloud environment:

   a. Pilot your migration. Start with a subset of workloads, validate operation and conduct end-user acceptance testing. Test, review, and make adjustments as needed.

   b. Sequence your migrations to migrate the rest of the workloads.

Container Security is a new and growing market in the cloud-sphere. When looking at Container Security solutions, make sure the products you are considering can do these three things:

1. Cloud Security Posture Management (CSPM)
2. Vulnerability Assessment for container images
3. Container micro-segmentation

Practical Challenges of Going to the Cloud in Federal Government

Security

Aside from navigating the existing acquisition process, the biggest hurdle for cloud adoption in federal government is security. It's not that cloud services are inherently insecure. Quite the opposite. It's just that in the context of the federal government, there are a number of unique security requirements, data classification policies, and regulatory hurdles that need to be managed.

No government agency wants to think about their Microsoft Office 365 tenant being co-located with a corporation from a foreign nation state in the same data center.

This is why FedRAMP authorization is so important. It provides federal agencies with assurance that a given CSP meets stringent security requirements to appropriately protect government data. FedRAMP is a government-wide program that provides a standardized approach to continuous monitoring, authorization, and security assessment for cloud services and products.

This allows a CSP to be assessed by the FedRAMP program and for that assessment to be used across multiple organizations. FedRAMP is based on NIST SP 800-53; the gold standard for security control frameworks. FedRAMP evaluates cloud service providers through a comprehensive two-step process. The model is based on a uniform set of standards, which are used to evaluate whether a CSP implements adequate information security and controls.

- Audits and Authorization: A Third-Party Assessment Organization (3PAO) approved by FedRAMP audits the CSP to ensure proper instrumentation of security controls and overall cyber readiness.

- Ongoing Audits and Authorization: In order to maintain an adequate status, the authorized CSP continues to undergo 3PAO audits and assessments.

By offering a standardized approach to authorization, security assessment and continuous monitoring for cloud services and products, the FedRAMP program helps federal organizations save considerable expense and time.

A cloud provider usually needs agency sponsorship to start the FedRAMP authorization process. However, it is also possible to receive FedRAMP authorization without agency sponsorship.

A CSP can submit a Business Case to the FedRAMP Joint Authorization Board (JAB). If JAB finds the solution valuable, they will sponsor the CSP's product to get FedRAMP authorized.

So, if a CSP is FedRAMP-approved, am I good to go? Not always. If you are in the civilian space, you may still have to go through your agency's internal Authority to Operate (ATO) process. However, if you are in Defense or Intel, there is a lot more work to do. If you simply must have the cloud service and there is a pressing mission need, there is an "easy button" route of getting a waiver from agency leadership, but these are usually one-off exceptions to the rule.

If you are to follow a formal process, you still need to translate the FedRAMP Authorization level to DoD Impact Level (IL). This is something that a CSP is required to work on internally, but they usually need a sponsor from the agency to get approved.

To make it easy to understand, I've put together a handy table. You are welcome!

DoD IL	Common Name	Classification	Example Systems	IaaS Clouds	People Requirements
2	FedRAMP Moderate	FISMA Moderate, Publicly Releasable Information	Public Websites, Library Systems	100+ FedRAMP Marketplace, AWS East/West, GovCloud, Azure	US Persons Only
N/A	FedRAMP High	FISMA High	Security Systems	AWS GovCloud, CSRA (MilCloud), Azure	Single Scope Background Investigation (SSBI) to Top Secret (TS)
4	FedRAMP+	Unclass / CUI (Sensitive)	HR Systems, Defense Industrial Base	AWS East/West (Limited Services), AWS GovCloud (Limited Services) – uC2S	SSBI to TS
5	FedRAMP+	Unclassified Mgmt / Mission	Email Systems	AWS GovCloud (Limited Services), Azure (Limited Services)	SSBI to TS
6	Secret C2S, GovCloud	Secret	SIPRNET	Secret C2S	Secret to TS
7	C2S	Top Secret / SCI	JWICS	C2S Cloud (AWS), MilJWICS – C2S Int-A, B, C	TS/SCI Polygraphed

Moving Apps to the Cloud

Instead of deploying an overprovisioned set of resources in the cloud, you can create scaling groups within your cloud provider to automatically spin up and spin down additional resources as demand rises or falls. This can eliminate the need for a costly application re-write while allowing you to still take advantage of the rapid elasticity and scalability of the cloud.

It is also worth pointing out that lift-and-shift is not always bad. While lift-and-shift does not address legacy application architecture impediments, such as the inability to elastically scale, portability, etc., in some cases it can be the first step toward digital transformation on the road to cloud adoption. Lifting and shifting can free up funds and human resources for other projects, not to mention getting rid of the legacy "boat anchor" physical infrastructure.

In some situations, lifting and shifting may be unavoidable. We usually run into these scenarios when it comes to legacy integrations. For example, an agency is relying on a custom application written by an employee who left the agency decades ago. Re-writing the application to support the new cloud environment may not be an option. There are too many interdependencies with other components of the system, and no one is brave enough to take on the challenge of reverse-engineering.

There may still be options to modernize, like putting on a new front end, or using a web application firewall (WAF), or incorporating a load balancer to re-write HTTP/HTTPS requests on the fly (think VMware's AVI Networks, F5 Big-IP or Imperva). Another option is to leverage a hybrid cloud approach to modernization. You can still keep legacy applications on-premises while leveraging the cloud for new development. There are also options of bringing a piece of the cloud on-premises by leveraging offerings like AWS Outposts or Azure Stack.

Shadow IT

At this stage, it is also worth touching on the subject of Shadow IT. Having performed Shadow IT assessments for dozens of federal agencies, I can tell you we typically see thousands of shadow services: everything from questionable media streaming and unsanctioned anonymous cloud storage, to PDF converters and even email services in Russia and China.

There are two conversational threads that tend to come out of these assessments. The first thread focuses on security. How do we control, limit, or block these shadow services? This is where I would discuss using a CASB or a next generation web gateway product with a gigantic Shadow IT registry of services and ability to dynamically track ephemeral URLs of services like Netflix, Hulu, and Dropbox.

The second thread tends to be a little broader and more focused on long-term cloud adoption within the agency. If you see many employees using unsanctioned PDF tools or cloud storage, maybe it is worth investing in a sanctioned PDF solution and take a look at an approved, FedRAMP-authorized cloud storage provider. But this is more of a short-term play. What we will see going forward is IT departments starting to offer SaaS services internally via an App Store-like capability similar to VMware's Workspace ONE.

We already see this happening in big commercial corporations. Why not within the US federal government? Ultimately, you should start thinking about your Helpdesk / IT department evolving into more of an internal agency Managed Service Provider (MSP).

Consider a Cloud Access Security Broker (CASB) to secure your SaaS applications. A big use case for CASB is Data Loss Prevention (DLP). Think of an employee creating a sensitive document in O365 via a web browser and then sharing it. No endpoint DLP solution will be able to catch this. You need a CASB.

Cloud Misconceptions

In this section I would like to cover a few misconceptions about moving to the cloud, especially in the context of the U.S. federal government. Despite a strong push to modernize federal IT systems and adopt the cloud, there are a number of people who remain resistant to the cloud concept.

Misconception 1: Cloud is the cheaper way to go

This was something that was touted in the early days of the cloud. With its consumption-based model, cloud computing offers instant cost savings. In practice, what we've observed is that for many legacy monolithic applications, simply lifting and shifting to the cloud did not yield the much-lauded financial benefits. There are numerous reasons to move to the cloud, as we discussed earlier. But for some workloads, you may not see an immediate drop in operational costs due to misalignment of resource requirements and cloud service tiers, and underutilization of cloud resources.

Misconception 2: Cloud is not secure

This may have been the case in the early days of the cloud, circa 2010. However, this is far from the truth in 2020. The proliferation of industry-mandated security frameworks, such

as FedRAMP, CIS Benchmarks, NIST SP 800 series, increased sophistication of security tools, and CSP support for dedicated security classification enclaves make it possible to accommodate the security requirements of virtually any workload. For the DoD and IC community we see CSPs standing up dedicated cloud environments, such as C2S, and Secret C2S.

There is a cloud with security requirements for every use case. Moreover, it is important to grasp the economies of scale in the form of *speed* that come from using widely adopted, vendor-managed, cloud-based services. Today's cybersecurity environment is hyper-dynamic, with new threat actors and vectors appearing daily. In this environment, the *time* required to limit exposure to threats is the enemy. Put another way, *speed* is the new security, and vendor-managed services offer incomparable cybersecurity *speed* relative to government-build/managed solutions.

Misconception 3: We need to have a multi-CSP strategy for DR/COOP

This is a misconception that stems from the traditional data center view of Disaster Recovery (DR) and Continuity of Operations (COOP). The major cloud providers have a multitude of resiliency and availability features. Cloud provider services are broken up into regions, which are usually based on geography. Each region is further subdivided into Availability Zones (AZs), which, in most cases, are actual physically separate data centers.

Depending on the region, AZ separation may be sufficient to meet your Agency's DR/COOP requirements. For even greater resiliency, you can even set up failover between different geographical regions. For example, Microsoft Azure allows you to configure paired regions, which, by design, are at least 300 miles apart and offer direct physical connectivity. Bottom line, while there are likely economic or operational efficiency factors that drive the multi-cloud discussion, there is no need to

consider a multi-CSP solution for DR/COOP, unless it is to meet some mission-specific requirement.

Misconception 4: To take advantage of the cloud, we have to rework our entire enterprise-wide architecture

Retooling the entire IT architecture to accommodate the cloud is probably not the right approach to cloud adoption. This misconception stems from terms like “cloud native” being thrown around. Cloud native refers to applications developed in the cloud, using cloud-based technologies, such as VMware’s Tanzu Application Services and Azure Cosmos DB.

The better approach would be to evaluate what cloud technologies support your agency’s mission today (cloud object storage, for example), start integrating those into your workflows, and at the same time begin thinking about what other technologies you can leverage in the future.

It’s an iterative process. Adopting the cloud does not have to be an all-or-nothing event.

Misconception 5: If we decide to adopt the cloud, all our storage and compute should take place in the cloud

There is really no reason to subscribe to this “all-cloud” paradigm. Federal agencies already have existing on-premises infrastructure you may want to leverage. Evaluating your existing mission-specific requirements should provide you with insights as to what part of your existing infrastructure should be migrated into the cloud realm.

You should also be looking at hybrid cloud solutions like VMware Cloud Foundation, or leverage cloud provider offerings like Azure Stack.

The Big Takeaways

I hope you've enjoyed reading about federal cloud adoption.

1. Policy is not only important, it's critical. Familiarize yourself with the Cloud Smart strategy: www.whitehouse.gov/wp-content/uploads/2019/06/Cloud-Strategy.pdf
2. Bookmark marketplace.fedramp.gov and visit frequently to check on FedRAMP authorization status for cloud vendors you are considering. You can also use the FedRAMP marketplace to look up other agencies using the same cloud vendor, as well as 3PAO security assessors that performed the FedRAMP assessment.
3. When selecting cloud service providers, try to choose solutions that prevent vendor lock-in and ensure long-term portability, so you retain the option to switch providers down the road.
4. Try to go with the simplest solution possible. Your goal should be to reduce complexity, which creates barriers of entry to personnel and drives up technical training costs. Minimize the number of panes of glass for system management.
5. Stop buying niche appliances. Aim to consolidate on software-defined solutions for ease of configuration, maintenance, and upgrade simplicity.
6. Start seriously considering and investing in cloud-centric ML/AI tools. These solutions are becoming increasingly mature and are becoming invaluable for security and AIOps applications.
7. Realize that you may have a number of legacy applications that cannot be migrated to the cloud. In these situations, consider taking on a hybrid cloud

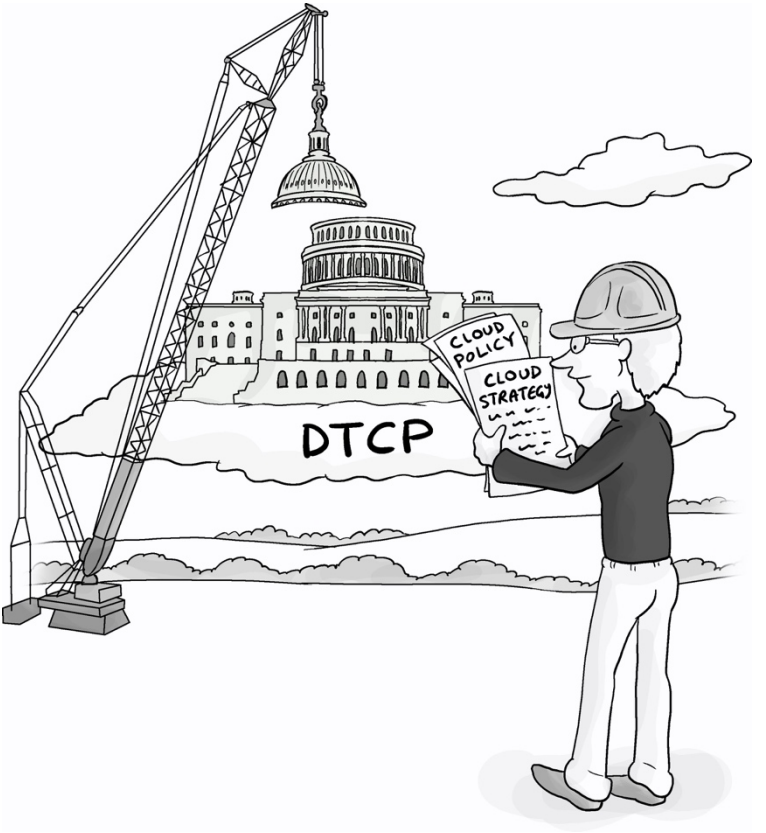
approach. There are both cloud provider native tools and those provided by third-party vendors to help you setup a hybrid cloud data center. VMware's Cloud Foundation offers singularly powerful implementation options for migrating to and operating hybrid clouds.

8. Start thinking of your IT department as a Managed Service Provider (MSP). They are not just there to fix computers and issue new laptops, they are also a service provider (or "internal reseller") of SaaS, IaaS, and PaaS in your agency. Along with building better applications with user-centered design principles, this should eliminate your shadow IT problem.

9. Cloud is not always cheaper. Generally speaking, to make the cloud truly cost effective, your applications need to be re-architected to take advantage of micro-services architecture and cloud-native technologies. There are ways to reduce operational cost for legacy apps deployed in the cloud, including simplifying the parallel operation of legacy VM-based apps, cloud-native apps and containerized apps using VMware's Tanzu capabilities, but they will never be as cost-effective as true cloud-native applications.

10. The final BIG takeaway is this: Public Cloud is not a panacea. Despite what cloud providers want you to believe, going 100% public cloud is not a one-size-fits-all solution. Traditional data centers are not going away.

Vendor Sponsors: How Dell Technologies and VMware can enable your cloud adoption



In our final chapter, we discuss how Dell Technologies and VMware technologies enable cloud adoption in the U.S. federal government. VMware's software-defined data center (SDDC) technologies are a cornerstone of many software-enabled government systems today. But there is always room to grow, and there is a real opportunity to leverage VMware's

foundational value proposition: build, run, manage, connect, and protect any app on any cloud, on any device.

VMware – Federal Cloud Adoption in Safe Hands

VMware helps agencies prioritize the development and delivery of modern apps as part of their digital transformation strategy.

VMware's approach to digital transformation opens the door to the broader VMware value proposition across its five pillars: App Modernization, Multi-Cloud, Virtual Cloud Networks, Intrinsic Security, and Digital Workspace.

VMware solutions drive a fundamental shift in how technology enables software delivery: zero-trust-based, intrinsically secure access to omnipresent cloud-based applications and data that flow and operate seamlessly across multi-cloud, hybrid cloud, and edge devices (including bring-your-own) use-cases.

Because VMware offers the most-established and lowest-risk solutions and services required to bring the benefits of modernized applications and infrastructure to bear, it is best placed to help move the needle on empowering the government to deliver optimal citizen experiences. Reducing the risk and complexity of developing, deploying, and operating cloud-based capabilities at Day 2 hyper-scale.

VMware products and services are essential as the government moves from the physical data center and client/server era into the cloud. VMware provides speed to operations for legacy applications in the cloud, end-to-end intrinsic security through the technology stack, out-of-the-box configuration and deployment automation, and a secure and efficient digital workspace environment for today's distributed workforce. Helping secure any device for any employee who accesses apps and data from anywhere.

These solutions include powerful yet familiar AI-driven management planes to enable fast user adoption and improved operational efficiencies. Furthermore, only VMware provides the comprehensive set of modular capabilities necessary to ensure the government retains the power of choice among the dynamic landscape of cloud, hardware, and SaaS providers needed to deliver agency system use-cases.

Dell Technologies – Cloud with the Agility, Control, and Performance of On-Premises

Dell Technologies Cloud Platform (DTCP) was introduced in 2019. The new on-premises DTCP is built on the company's flagship hyper-converged infrastructure, VXRail, as well as VMware Cloud Foundation, which is VMware's hybrid cloud solution that provides integrated cloud infrastructure and cloud management services to run applications in both private and public environments.

Dell Technologies has also validated designs that allow partners and customers to build Dell Technologies Cloud Platforms using traditional servers, networking and storage arrays inclusive to Dell EMC Unity and PowerMax. The cloud platforms are built to be flexible in order to meet a variety of workloads and performance needs.

With DTCP, customers are offered a set of consumption-based and as-a-service offerings on the industry's broadest infrastructure portfolio that delivers IT with agility of cloud and the control, performance, and predictability of on-premises infrastructure.

Microsoft Azure Stack and Dell EMC

We've previously alluded to Azure Stack and how it can act as an extension of cloud infrastructure on-premises. In addition to its Azure public cloud, Microsoft (through hardware partners) offers Azure Stack, a purpose-built, preconfigured solution that

provides a hybrid cloud extension for compute, storage, networking, security, and other resources. Azure Stack lets organizations choose where they keep applications, based on business, technological, and regulatory compliance requirements, while maintaining a consistent framework, processes, and tools.

Applications developed on Azure or Azure Stack can be deployed in either location to support necessary data customization, latency, and data protection objectives without any code changes. Azure Stack uses only Microsoft-approved hyperconverged infrastructure that can be deployed in enterprise data centers or managed service providers.

With Azure Stack, organizations can run IaaS and PaaS services from their on-premises data centers with the same administrative experience and tools that they use with Azure, including management, security, and authentication. Payment options include pay-as-you-go or annual subscription.

Dell EMC Cloud for Azure Stack is a hyperconverged, hybrid cloud platform that uses Dell EMC Cloud for Microsoft Azure Stack Hub to deliver on-premises Azure Stack IaaS and PaaS consistent with the Azure public cloud experience. Dell EMC brought a wealth of experience from several product lines to build the Dell EMC Cloud for Microsoft Azure Stack. As a result, instead of incurring the cost and time burdens of buying and building a hybrid cloud infrastructure on their own, organizations can leverage this preconfigured stack that can be deployed and operated by data center staff or a CSP.

The solution was designed to enable organizations to focus on delivering Azure resources and services to end-users rather than on purchasing, setting up, and tuning infrastructure.

Dell EMC Tactical Azure Stack Hub

Dell EMC Tactical System for Microsoft Azure Stack Hub ("Tactical Azure Stack Hub") is the first hybrid cloud platform

that is designed to deliver Azure Stack Hub capabilities beyond the data center to tactical, remote, and harsh environments. It provides a familiar and consistent experience for deploying and managing Azure-based services in the field and enables a wide range of use cases for government, military, energy, and mining applications.

Tactical Azure Stack can also be used in forward deployments and mobile environments in marine, aerospace, and other demanding conditions, with or without network connectivity. For cloud operators, developers, and tenants, there are no differences between Tactical Azure Stack Hub and Azure Stack Hub deployed on premises.

Developed and fully engineered through the exclusive partnership with Tracewell Systems, Tactical Azure Stack Hub is based on Dell EMC networking switches and PowerEdge servers, and Tracewell's expertise in ruggedized systems. Its core components are identical to the Dell EMC all-flash Data Center Azure Stack Hub offering and the solution is available in select regions from Dell EMC and authorized partners.

NOTES

Dell Technologies trusted Hybrid Cloud

Enabling Cybersecurity and Operational Outcomes

DELL Technologies

Get conversational about migrating to the cloud in a federal government setting.

Microsoft 365 is taking the world by storm, but it can be Unlike in the commercial space where cloud adoption is driven by forces of capitalism, a lot of U.S. federal government cloud adoption is driven by policy. This means it's essential that you have a good understanding of the policy basics. This book is designed to give you the tools that will help you align your cloud projects with these core policies and navigate the practical challenges of moving to the cloud in the Fed.

About Andrey Zhuk

Andrey Zhuk is a Cloud Security Architect at CTG Federal, where he helps U.S. government agencies adopt new cloud services and secure agency assets in the cloud. Andrey is an experienced cloud, cyber, and network architect with over 13 years of experience in U.S. federal government space.