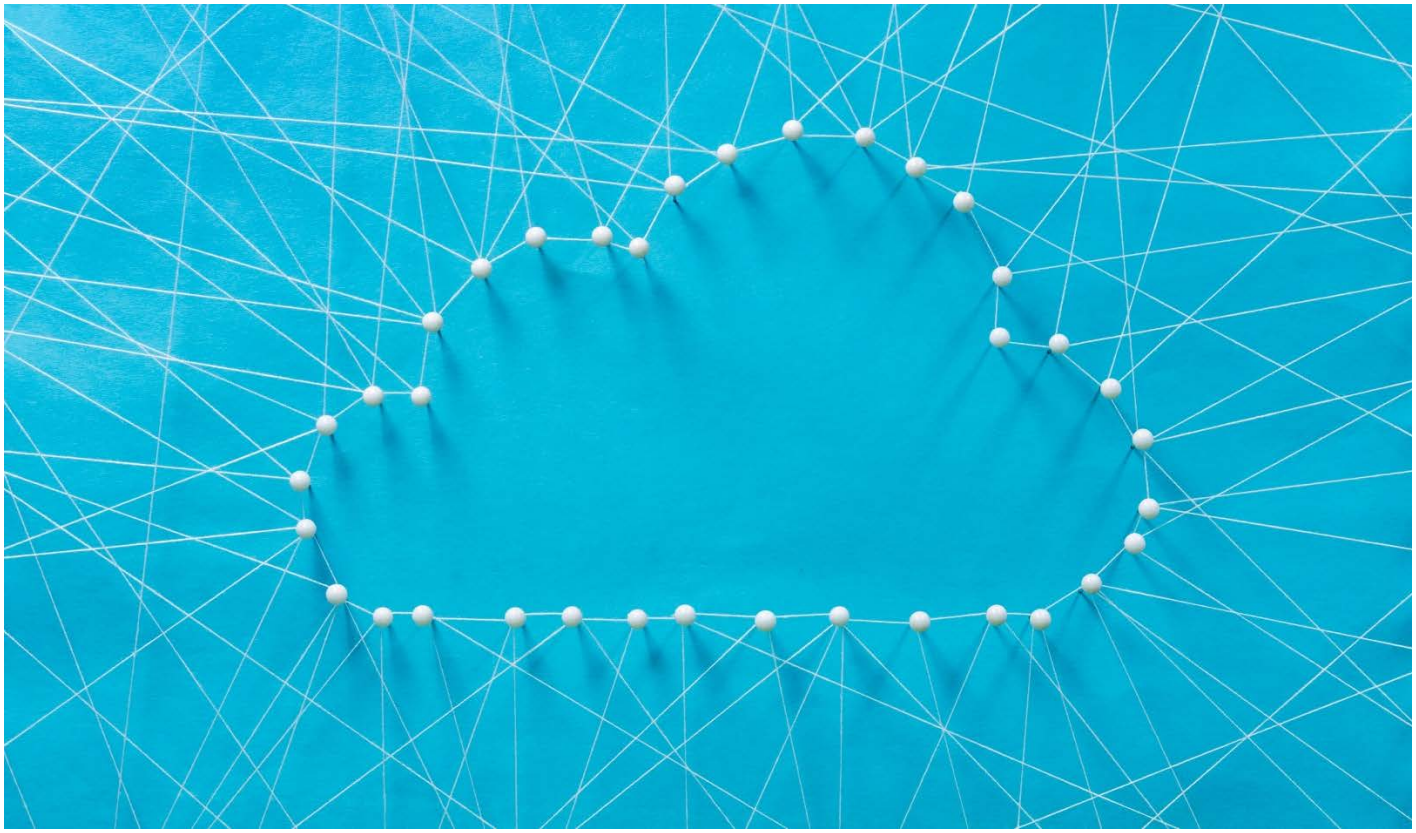


Integrated Multi-Cloud Management for the Federal Government

Doug Bourgeois and Sean VanDruff
Deloitte Consulting LLP

Introduction

In 2010, the federal CIO, in collaboration with the Office of Management and Budget (OMB), instituted a government- wide Cloud First Policy. Since the inception of this policy, agencies have been working to adopt and harness the transformational abilities that cloud services can provide. Many agencies first focused on lower risk projects, such as moving email and public facing websites to the cloud. Since realizing initial successes, they have turned their focus to migrating applications to FedRAMP accredited public clouds, and further development of private clouds. This offers the ability to automatically provision cloud virtual infrastructure, thereby helping to increase responsiveness to mission priorities. Accordingly, IT organizations have worked diligently on developing and implementing strategies for cloud consumption, and have made steady progress in adopting the new service models. Federal cloud adoption has progressed beyond these initial approaches and has moved toward implementations such as cloud platforms, various Software as a Service (SaaS) solutions, and hybrid clouds. Recognizing these enhancements, the federal government is expected to spend

more than $4 billion on cloud technologies and services in 2017. Thus a new challenge is emerging that is analogous to the "server sprawl" that the IT industry experienced in the 1980's and 1990's. Federal agencies have realized that their users and applications are now spread across several clouds without the means to centrally view, secure, or manage these environments effectively. In many instances, cloud services are being adopted directly by the business and mission areas of agencies, which may create an environment in which pockets of cloud exist throughout the organization and where the CIO does not have insight into all of the isolated cloud environments.

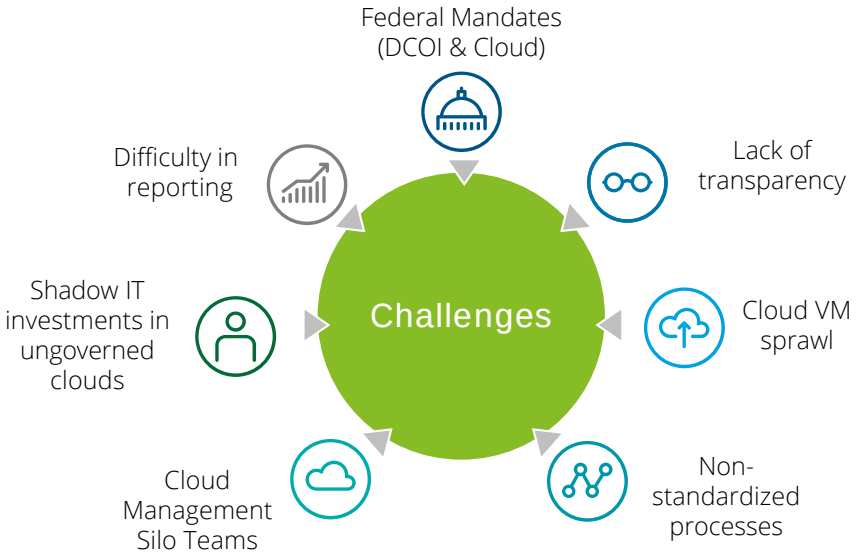
Some are calling this phenomenon "cloud sprawl", can create many challenges for the IT organization when it comes to reporting, monitoring, and securing all the cloud usage across the agency.

Challenges of Federal IT

Federal IT executives typically face budget pressures and increased IT regulations while attempting to accommodate exponentially growing mission demands. The transition from legacy physical data center architecture and operations to modernized software defined data center (SDDC) and cloud infrastructure has created a wide array of challenges. Oftentimes, along with the challenges come opportunities for providing new efficiencies and enhanced capabilities.

Figure 1 shows some of the specific challenges typically facing federal IT leaders. Mandates, such as the Federal Information Technology Acquisition Reform Act (FITARA) and the Data Center Optimization Initiative (DCOI), require CIOs to increase virtualization, increase use of cloud services, and to deploy automated monitoring and reporting capabilities across all data centers and IT environments. CIOs have

Figure 1. Common Challenges Facing Federal IT



been typically tasked with managing not just their own services and infrastructure, but understanding all IT investments across their agency.

To help combat shadow IT investments (often using cloud service providers), CIOs should engage their organizations, and provide a unified dashboard and reporting/management capability for all clouds. This unified dashboard likely eases some of the issues in regards to a lack of transparency and difficulty in reporting. Agencies have Virtual Machines (VMs) for applications deployed in isolated labs, on some user desktops, in external clouds, and in data centers throughout their organizations.

They also have migrated applications to multiple clouds –public and private. These applications and VM instances belong to different business groups, which often do not follow standardized processes or governance. A key reason is that current policies that govern federal IT are typically not designed for cloud and modern service delivery approaches, therefore, often bypassed. Further complicating the situation are outdated security policies that neither align to the current cybersecurity environment nor account for much of the infrastructure abstracted through software and virtualization.

This limits policy effectiveness and decreases the ability of agencies to adequately defend their infrastructure and networks. Due to many disparate data sources, CIOs have a herculean task in reporting metrics. This challenge can undermine efforts to meet laws, mandates, and directives, such as FITARA and DCOI. To this end, common tools, frameworks, processes, and procedures are important to help guide agency approaches migration to the cloud; aligning all cloud efforts to the same governance; and providing reporting, metrics, cost transparency and analytics. Siloed cloud management teams often involve each team having experts with special skills, serving in the same role and capacity across the enterprise. Additionally, some teams may only interact with one vendor or set of technologies, limiting their ability to integrate with other teams and tools. These challenges can provide a significant opportunity for federal IT leaders to change the way they do business, and provide a single tool to their organizations to integrate, standardize and enhance their IT infrastructures. With the proper tools, policies, and procedures, CIOs can convince their shadow IT consumers to "join the club" and integrate with their cloud management tools, offering speed and simplicity of operations.

Addressing CIO Challenges

The widespread nature of common management difficulties, listed above, especially in a period of tight budgets with enhanced regulatory requirements, suggests that facing these matters now is crucial. These entrenched challenges can be found throughout federal organizations. To be able to meet the increasingly demanding customers, federal IT decision makers have reached a tipping point - how does an agency address cloud adoption and cloud management within its organization while meeting the need for holistic metrics reporting, understanding the full cost of services, and keeping the networks and data secure? As these agencies modernize their infrastructure, organizations likely need to reform their governing processes, and a well-designed cloud management solution should provide the capabilities that can support them.

Why Multi-cloud Management

An effective cloud management solution addresses many of the previously stated issues through providing a common platform that allows numerous cloud providers to be managed through a single multi-tenant portal for the various stakeholders across the organizations. This allows the application of standardized policy, procedure, governance, and cybersecurity workflows and controls for disparate system and application stakeholders supporting the mission. It also enables the organization to more easily collect, analyze, consolidate, and report performance and utilization metrics allowing for service usage and cost transparency of all cloud services to which it's connected. The points below summarize key features that should be considered for a well designed and implemented multi-cloud management platform, and describe some of the typical benefits:

- **Security consistency** standardizes policies and controls across any cloud public or private to enable enforcement and compliance with security requirements and controls.
- **Micro-segmentation** enhances the perimeter security model through granular and automated network compartmentalization that provides a more workload-centric security posture.
- **FedRAMP-ready** capability enables an accelerated ATO, A&A, security certification, etc.
- **Standard toolset and interface** provides ease and efficiency of cross-cloud management capabilities including performance, utilization, deployment, and reporting.
- **Workload portability** gives the user the capability to run an application where most appropriate given the workload profile throughout its lifecycle or perhaps its seasonal demand. Workload portability also allows users to avoid vendor lock in.
- **Services Agility** is the ability to quickly address demand through adapting and offering new cloud capabilities through an application programming interface (API) based architecture.
- **Complete Cloud Stack** which includes not only IaaS, but also DevOps and Cloud Native abilities, and allows the organization to incrementally adopt modernized application architectures while supporting traditional IaaS based systems.
- **Cloud Business Management** provides cost and usage transparency reporting across all clouds in a standardized reporting or invoicing/ show-back format.

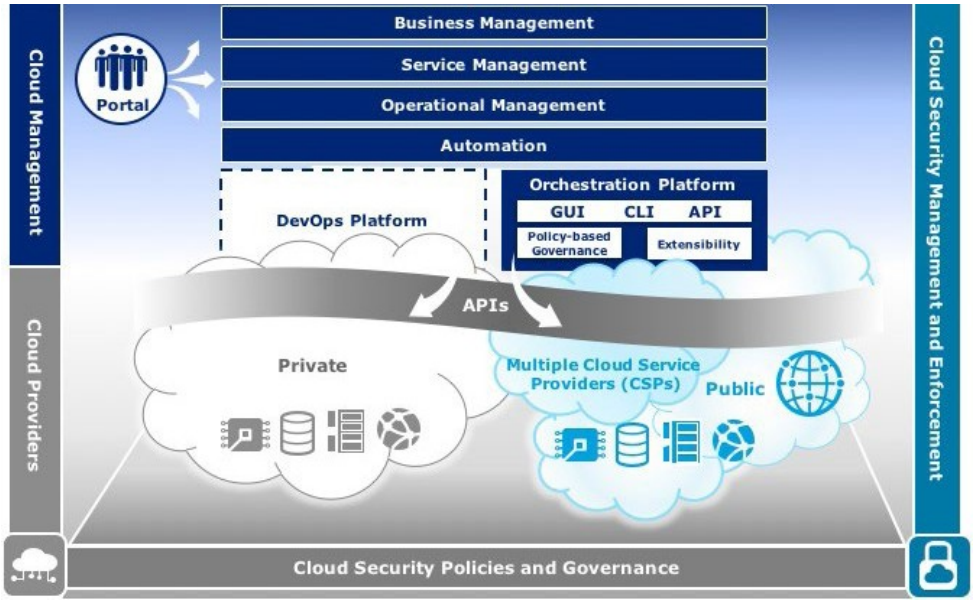
When these features and capabilities are brought together in a cloud solution, they can provide a more holistic and integrated cloud management package with security built in from the beginning. This helps enable quicker deployment, faster security accreditation, and accelerated adoption of cloud services. Ultimately this can mean better time to value for the CIO, the IT organization, and the mission or program areas that depend on them for service.

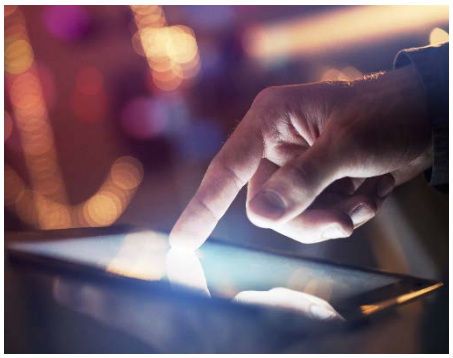
What is Integrated Multi-Cloud Management?

An effectively designed multi-cloud management approach, depicted in Figure 2, categorizes functions and capabilities into a layered model. The foundation of this model is a framework that consists of Common Security Policies and Governance. These policies are enforced by tightly integrating the Cloud Security Management and Enforcement capabilities across each layer of the cloud management stack as well as extending them into the cloud provider environment. The Cloud Management stack consists of five integrated layers with each one providing a specific set of capabilities, which are complementary to the overall solution. Each solution layer is summarized in the points below:

- **The Business Management** layer facilitates informed decision making. This layer includes the tool set that provides transparency and control over the costs and quality of IT services, enabling the decision makers to align IT with the mission by comparing the costs of workloads between the private cloud and multiple public clouds.
- **The Service Management** layer provides a common unified portal to allow users with role based authorization to request IT Services across clouds. It includes a workflow management and automation capability to implement a service catalog and governance that spans the entire multi-cloud operational environment in a manner that is streamlined for the user.

Figure 2. Multi-Cloud Management Framework





- **The Operational Management** layer offers a single pane of glass command and control panel, which provides operations staff cloud administration, performance monitoring/tuning, risk mitigation, and troubleshooting capabilities.
- **The Automation** layer provides consistent deployment and management of IT services while reducing manual processes, and helping to limit human error and ensure compliance with policies. It enables significant operational efficiencies by reclaiming inactive resources that may be repurposed to other applications based on dynamic mission demands.
- **The Orchestration platform** enables the automation of complex IT tasks to adapt and extend service delivery and operational management across clouds. The orchestration platform is the engine by which Automation and Operational Management provides deployment, remediation and adherence to industry-standards and/or organizational policies.
- **Application Programming Interfaces (APIs)** - The MCM solution is extensible, and is able to recognize the most common APIs and can interact with IT management and an organization's private cloud as well as the major Cloud Service Providers that have achieved a FedRAMP security authorization.
- **The DevOps** platform is one of the key components of the MCM; it allows the solution to be forward-facing, providing the required tools to enable continuous integration and delivery, decreased management complexity, and faster problem resolution. The DevOps platform manages the version control of the code library, simulates the operation aspects of containers, and automates the deployment and management of "cloud native" applications via policies.

Use Cases for MCM

A robust multi-cloud management solution provides a targeted toolset and operational framework that enables an IT organization to meet existing or impending cloud adoption challenges.

During the multi-cloud planning and requirements process, the organization should address perspectives from different stakeholders and actors. These viewpoints are often referred to as use cases or user stories. For example, IT executives may demand federally mandated consumption and capacity reports; developers typically require a cloud-native environment for their applications; and IT operations managers often need disaster recovery options without large CAPEX investments. In addition to these examples, there are other high-priority, yet fundamental use cases that should be present in an integrated multi-cloud management solution as summarized below.

Further Considerations and Conclusion

Cloud services are becoming the norm across much of the federal government, which presents both opportunities and challenges. An effective and sustainable IT operations model involves a seismic shift in how cloud services are procured and managed. Without this shift, cloud management and consolidated reporting are likely to become the next weight on the CIO's back, reducing his or her impact and effectiveness.

Deloitte.

Use Case Name	Description	Primary Actors
Workload Comparison and Analysis	• Evaluates and assesses the workloads, based on security cost, and architecture	policies, System/Application Owner, TBM stakeholders, Infrastructure PMs
Automated Provisioning	• Provision workloads to any cloud on-demand • Stand up dev/test/lab environments as needed • Consumption model for billing and cost modeling	System/Application Owner, Developer/ Tester, Infrastructure Team
Security Policy Deployment	• Provide ready-to-use profiles for security settings (FISMA H/M/L) • Support micro-segmentation on the fly • Limit administrative rights to protect against insider threat	System/Application Owner, ISSO, CISO
Disaster Recovery and Backup	• Rapidly standup workloads in cloud in DR scenarios • Backup data to cloud for low-cost, high availability access • Tiered services based on business need	IT Operations, System/ Application Owner
Hybrid Cloud	• Migrate workloads between on-premises and public as required • Develop off-premise and move into production on-premises • Monitor and report on all cloud resources in single dashboard	IT Operations, Infrastructure Team, System and Application Owner
Cloud Native Development & Operations	• Support cloud native development with on-demand containers and tools to support applications through SDLC • Provide tools, management and reporting for container deployment and configuration	Application Developer, DevOps team
Cloud to Cloud Migration	• Migrate workloads between cloud providers (public/on-premises) • Develop off-premises and move into production on-premises	System/Application Owner, Infrastructure/ based on cost efficiency or other drivers DevOps Team
Enhanced Reporting	• Capacity, consumption, cost, service availability • Advanced analytics such as trending and forecasting • Enable reporting to meet Federal requirements (DCOI & FITARA)	IT & Business Executives, Infrastructure/ DevOps Team, System Owners

Understanding considerations and lessons learned from an ally that "has been there and done that" can help with effective cloud service implementation and maturing technology business management capabilities. The table below summarizes some key considerations that should be addressed while planning for cloud implementation projects.

Agencies should carefully consider how they are operationalizing these cloud services to help ensure the issues IT service organizations have faced in the past do not continue to proliferate or materialize in modern cloud environments. Employing a multi-cloud management solution that covers the planning, development, deployment, security accreditation, and operational management requirements in an end- to-end and holistic manner is important to federal agencies' effectiveness in this new world of IT services. When done correctly, the solution can result in greater efficiency, speed to delivery, reporting, and performance, which all drive greater productivity in the operation of the mission. From a business management perspective, the proper integrated cloud management solution offers greater insight into areas such as utilization, trending, forecasting, costs of services, as well as their level of adoption, which should lead to future cost savings. In this time where shrinking budgets and limited funding are commonplace, agencies may have to adopt these cost savings approaches to be able to meet mission requirements.

Technology Considerations	Organizational Considerations
• Understand how new cloud projects will integrate with current architectures and existing environments • Evaluate current technology skillsets and capabilities of current staff and contracts • Carefully evaluate the implications of the cloud platform options • Map proposed technology skillsets and capabilities to current skillsets and capabilities • Perform IT landscape assessment and risk framework impact analysis • Carefully consider the integration of core infrastructure services and providers as part of automation planning and design efforts	• Understand pain points for the IT service organization, and the consumers of the services • Align and develop common enterprise framework and taxonomy for cloud service consumption and reporting • Build stakeholder consensus across the organization through proof of concepts and demonstrations of real-life solutions • Build staff knowledge, skills, and organizational credibility through incremental enhancement of foundational services • Understand existing IT support contracts and their limitations and address them as part of the project

Contact us:

Doug Bourgeois
Managing Director
Deloitte Consulting LLP
dbourgeois@deloitte.com
+1.571.814.7157

Sean VanDruff
Specialist Leader
Deloitte Consulting LLP
svandruff@deloitte.com
+1.215.446.4314

Andrey Aminov
Specialist Master
Deloitte Consulting LLP
aaminov@deloitte.com
+1.571.882.7811

Ryan Kamauff
Senior Consultant
Deloitte Consulting LLP
rkamauff@deloitte.com
+1.571.814.6321