Slow and Steady: Toward the Hybrid Cloud Ideal

More agencies than ever are moving at least some data, applications and infrastructure to the cloud. In doing so, they are saving money while increasing efficiency, flexibility, collaboration, reliability and security. Moving some resources to the cloud also satisfies the federal government's Cloud Smart mandate, which requests agencies to strongly consider switching to cloud resources when it can better serve the mission, improve citizen services or increase security.

At the same time, not everything belongs in the cloud. Sometimes, it's about data privacy or reasons of national security. And sometimes, agencies have legacy data and applications that simply won't work in the cloud. These factors are leading most agencies to adopt a hybrid strategy, which allows them to get the best out of both environments— on-premises resources and multiple clouds.

According to Lloyd Granville, deputy CTO, DoD & Intel Community at NetApp, "The military functions not only on multiple levels of data classifications but on a global scale and at many times behind a disadvantaged network path such as satellite or intermittent communications pathways that are either denied, degraded, or overworked. That fact alone dictates that a hybrid-cloud solution works best for continuous operations. For now, the on-prem environment is still a must for a forward-deployed entity to conduct business."

So hybrid cloud is the answer, but now you have to address migration. Not all methods of moving data to the cloud work equally well. While it's certainly possible to migrate resources using protocols, upload scripts and synchronization tools, the data will reach the cloud, but at a cost. It will inevitably require some manual intervention and may cause data governance and compliance issues. The migrated data and applications also could end up synchronizing well with some cloud platforms, but not others. That's a problem if an agency has two teams using the same data; one relying on AWS GovCloud while the other uses Azure Government, for example.

Different Special Operations units utilize varying vendor network and services hardware to manage their data from the tactical edge to the core. This can be simplified by using software-defined storage systems on their tactical hardware from the edge to the core data centers. "KLAS, PacStar, and Dtech systems are seen across the battlefield providing small form factor support to the warfighter. Regardless of what hardware the data resides on, NetApp provides solutions that the military can use to move that data to the cloud and even between multi-cloud environments. We also have a partner program to certify operations on those ruggedized solutions," Granville said.

Moving to a hybrid cloud strategy can be addressed with a tried and true process.

A three-step process

The first step in creating a workable hybrid model requires laying the right foundation. While some resources can be easily moved to the cloud, others, especially those with large, data sets, can be more complicated. For those workloads, it helps to use a good storage architecture or framework to help move the data. NetApp has multiple technologies that will easily handle those workloads and utilizing a Data Fabric, seamlessly transition the on-prem data to a multi-cloud environment that can potentially be shared by various commands as missions dictate.

The storage framework you choose should fully automate the process of moving data between on-premises and cloud environments and work well with all major cloud vendors, including AWS, GovCloud, Azure Government and Google Cloud. To facilitate this agencies already using NetApp solutions should consider a simple upgrade to Cloud Volumes OnTAP. Once the foundation is complete, the next step is finding a way to synchronize data across on-premises environments, multiple clouds and into cloud-based applications, such as Microsoft Office 365. Synchronizing data properly means ensuring that it remains aligned no matter where it exists.

"Ensuring alignment across all resources requires adding object-based storage to the mix. With object storage, data is stored with its metadata and unique identifiers, ensuring that it will be synchronized properly," explained Sean Applegate, chief technology officer at Swish Data, a provider of technology solutions and engineering services to the federal government. "Object storage also is the best format for performing

effective analysis on large amounts of unstructured data."

As the DOD utilizes more and more object storage, NetApp has technologies for software-defined storage that will support file block and object. These technologies can serve as an object storage repository tool, perfect for unstructured data that continually grows, may be retained forever, is rarely updated, and is meant to be accessed by multiple application services across geographical boundaries.

In addition to making sure resources are synchronized, it's also important to make sure that they can be moved around when needed. This requires a tool that will automatically convert files of other types into object-based storage formats. For example, NetApp's CloudSync can convert unstructured NFS files into the right format in the cloud.

Once the data and associated applications are fully integrated into the hybrid environment, the last step is finding a way to monitor the data and get value from it. That means being able to keep track of metrics like capacity, latency and speed. With this type of information, agencies can make better choices about allocation and cost optimization.

In large organizations like federal agencies, where multiple teams put resources into various locations, monitoring can be difficult. "An integrated fabric foundation can be a big help here," Applegate said. He recommended choosing a platform that can centralize analytics across all on -premise and cloud environments. The solution also should integrate with as many different systems and storage types as possible.

One tool that provides all of these features is NetApp's Cloud Insights. It can connect to all on-premises data centers and clouds, which allows it to analyze how long it takes to backup or restore data, and notify users of any storage issues.

"With this type of insight, agencies can, for example, find that they are using certain data types on certain clouds and other types in other environments, which can provide clues about how to reallocate resources," explained Steve Chesney, a public cloud services account manager and solutions architect for NetApp's DOD and Intel customers. "From a cost optimization perspective, it can help you understand where you are spending money. Are you getting a good value for putting your data in that particular cloud, or would it be more cost-effective to put it elsewhere?"

That type of insight is critical to how well missions run. Not only does it help the Army introduce change in a controlled manner, but it gives security teams the ability to manage risk effectively in real-time. In addition, it increases the confidence in the team's ability to identify issues and remediate them in real-time.

While making these changes may seem overwhelming, they don't have to be. "Start slowly," Applegate said, "and don't be afraid to take your time testing things out. Either start with one small test project or one division, or get through the first phase and live with it for a few months or years until you feel comfortable moving on," he said.

Security in a Multi-Cloud World

While there are many benefits to a hybrid cloud environment, agencies tend to feel a bit differently about security. Fair or not, many believe that security in the cloud isn't as good as security on-premises.

In a way, they are right. After all, if you have all of your data locked down in your data center, so it's much harder—but not impossible—for hackers to reach it. In the cloud, concerns about data breaches, account hijacking, malware injection, denial of service attacks and insecure APIs remain.

With more resources than ever in the cloud, agencies are understandably concerned about data protection. With the right processes and tools, however, exposing sensitive data shouldn't be a big concern.

First, follow government and industry best practices for data security. Also consider automating cloud policy enforcement. Using an architecture that can actually help enforce those policies across on-premises and cloud assets by proactively setting and enforcing them is even better. There are plenty of tools out there to perform these tasks, as well as identifying misconfigurations and enforcing security best practices and compliance framework.

It's also important to incorporate tools that track the location of sensitive data at all times, and can monitor and audit exactly who is accessing specific resources, when they accessed it, both pre- and post-incident. In addition, choose infrastructure tools with encryption and key management, data protection for both data at rest and in transit, and FIPS 140-2 compliance.

For agencies undertaking a cloud migration project, Swish Data's Applegate recommends addressing security issues prior to migrating data to the cloud. "If you do it proactively before migrating your data, you can significantly reduce your risk," he said.