Phil Goodwin
Research Director, Storage Systems and Software

How to Optimize Your Multicloud Strategy

May 2017

IDC research indicates that over 90% of enterprise-scale organizations plan to make use of multiple clouds in the next several years. However, many IT organizations struggle to keep up with scaling, pooling, migrations, and the rapid pace of change that are the hallmarks of cloud IT operations.

The following questions were posed by OneNeck to Phil Goodwin, research director within IDC's Storage Systems and Software practice, on behalf of OneNeck's customers.

Q. **In an increasingly hybrid IT world, what are the benefits of a multicloud strategy?**

A. There are several benefits to having a multicloud strategy, but let's focus on just three of them. First, there is significant differentiation among cloud providers. Cloud is not a case where service providers are very similar. In fact, providers have a high degree of differentiation.

For example, some feature low costs, some have white-glove service, and others specialize in certain application support. IT organizations can select a provider suited to a particular use case or workload, or they may choose to select a national or regional provider because of size.

Second, we find that many organizations are using a multicloud strategy to avoid vendor lock-in. Cloud providers are subject to business problems just like anyone else, and organizations want to know that they can get their data out if they need to.

Third, application deployment models are evolving rapidly. Having deployment options can help IT organizations go to market faster with new applications based upon specialized requirements as well as increasing agility to meet unforeseen requirements.

Q. **Managing multiple cloud services can become challenging. What should an enterprise consider that will help?**

A. Well, it would be great to have one tool that would let an organization have an enterprise data management strategy across all applications and environments, but those tools are still evolving. It will probably be several years before they reach a point of maturation and can be deployed at an enterprise level.

Therefore, IT managers need to look for cloud providers that can give them complete insight into an application environment and any other aspect of their cloud environment. Security, encryption policies, data access mechanisms, service-level agreements, and monitoring are particularly important considerations.

Self-service portals are another differentiating factor among cloud providers, and this is an area that IT managers should examine carefully when evaluating providers. The self-service portal can save a significant amount of time, as well as cost, in terms of giving users and IT managers the tools they need at their fingertips.

Data protection is an often overlooked area with cloud providers. IT users assume that data protection mechanisms and practices are in place, and usually they are. But what's in place may not meet the service-level requirement for the organization. IT managers must make sure data protection, as well as access and recovery capabilities, meet their organization's specific needs.

Q. **As security attacks continue to rise, how can organizations protect themselves when utilizing multiple clouds?**

A. Simply having different workloads in different clouds provides some level of protection. If one cloud environment suffers an attack, it won't propagate to another workload area.

It's also important that IT managers work with their cloud providers to assess vulnerabilities and service-level requirements to ensure that they contract for the right level of services for the application that they have deployed. In terms of a best practice, IDC recommends some sort of air gap in the data protection scheme to physically isolate an attack. In some cases, this might include multiple clouds; for example, one cloud environment for operations and another for data protection.

Back in the days of tape, an air gap was inherent to the process, but today, with automated replication, users need to be sure that the air gap is architected into their solution.

Q. **IDC predicted in 2016 that hybrid cloud architectures would continue dominating enterprise cloud strategies. The need to integrate traditional noncloud systems with modern cloud infrastructure and cloud-native applications creates friction and operational challenges across many organizations. How are these challenges addressed?**

A. It's fair to say that most organizations today have both on-premises and off-premises cloud workloads. We are finding that organizations are addressing challenges on a workload-by-workload basis.

Not all applications are candidates for cloud deployment, but the fastest-growing area is certainly cloud-native application deployment. To cope with these diverse workload deployment models, IT organizations need to begin adopting enterprise data management strategy practices.

The common element to all deployments is data, so that's the place to focus. Data management includes obvious things like availability, protection, and so on. Leading-edge companies, though, are looking for new ways to monetize data.

In other words, how can the organization utilize the data to gain better insights into customers, operations, or markets? In many cases, the data is there, but the means of utilizing it are not, in part because the data may be spread out. Enterprise data strategies and tools can help businesses gain valuable insights into their data.

Q. What are the top 5 considerations an enterprise should keep in mind as it embarks on a hybrid IT journey?

A. Our first recommendation would be to have clear business goals in mind, whether better service delivery or lower costs. Know what your priorities are and what you need from a provider so that you can ensure that the provider addresses those issues. Keep those needs at the forefront when evaluating providers.

Second, focus on the application or workload deployment, not on the infrastructure. This may be for on-premises, software-as-a-service, or hybrid cloud workloads. But regardless, IT organizations need to focus on the most efficient platform for any specific workload.

Third, data protection is the tip of the cloud spear for most organizations. Disaster recovery and archiving are the hottest areas, but organizations also use cloud for backup and archive services. Data protection is probably the easiest entry point into the cloud, and often it has the clearest ROI.

Fourth, consider how the cloud provider's people and process fit your requirements. This may include technical support as well as professional services. In a hybrid cloud, you and your cloud provider are a team. The provider's processes should be compatible with the way you do business, and the provider's level of support should augment your own.

Fifth, don't be afraid to assess and reevaluate your on-premises and cloud deployments. Situations change, goals evolve, and requirements change. Having a multicloud strategy can give you the agility to meet unforeseen circumstances.

ABOUT THIS ANALYST

Phil Goodwin is a research director within IDC's Storage Systems and Software research practice. He provides detailed insight and analysis on evolving industry trends, vendor performance, and the impact of new technology adoption. Mr. Goodwin is responsible for producing and delivering timely, in-depth market research with a specific focus on data protection, business continuity and disaster recovery, and data availability. Mr. Goodwin takes a holistic view of these markets and covers risk analysis, service-level requirements, and cost/benefit calculations in his research.