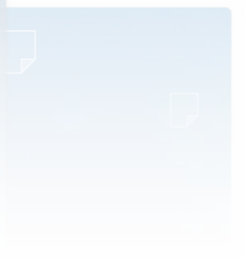
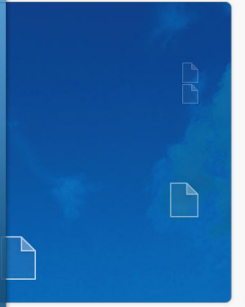




The Cloud Controversy— IT Alternative or IT Architecture?



The Cloud Controversy— IT Alternative or IT Architecture?



Table of Contents

Overview	3
The cloud controversy—IT alternative or IT architecture?	3
Cloud as an IT architecture for self-service, elasticity, and scalability	4
Federation—embracing cloud while preserving policy	5
Introducing Atmos	5
Conclusion—cloud is an opportunity for IT, not a threat	6

Overview

Cloud computing is certainly a hot topic, and many are even heralding it as an alternative to the IT function. We don't see it that way at EMC. We believe there is an approach to cloud that enables the IT organization to deliver the financial and functional benefits of cloud computing to the business units, while simultaneously preserving the integrity of enterprise IT policies. This perspective introduces the key concept of resource federation—an IT architecture that embraces the flexible resource management of cloud computing for both internal resources as well as external resources—those provided by cloud service providers. With federation, the IT organization can provide the flexibility and self-service capability that business units demand, without compromising the integrity of corporate policies for compliance and risk management.

The first EMC® offering that delivers this federated architecture is EMC Atmos®—an information storage and distribution technology that combines massive scalability with scriptable policy for automated data placement across internal and external networks. Atmos is a proof point for the benefits of cloud computing as an emerging IT architecture, and EMC is your trusted guide for embracing the emerging architecture of cloud computing.

The cloud controversy—IT alternative or IT architecture?

In his 2008 book, “The Big Switch: Rewiring the World, from Edison to Google”, Nicholas Carr compared IT to the power industry and proclaimed there would be a “big switch” from internally maintained IT resources to externally maintained IT resources provided as a utility—just like electricity. One year later, the hype of cloud computing is almost deafening, with most of the noise being generated by the debate over whether or not cloud represents a fundamental shift away from internal IT capacity. Similar to the SaaS debate regarding the future of software delivery, the cloud debate tends to cast things in black and white instead of shades of gray. Marc Benioff, the founder and CEO of salesforce.com, famously declared “the end of software” as the rallying cry for the salesforce.com marketing machine. And it worked very well as a marketing gimmick, with salesforce.com garnering the lion's share of attention among the SaaS players. But, software did not disappear. The landscape of software delivery simply shifted to balance traditional applications managed by IT with on-demand capability provided by SaaS providers. For certain types of applications, SaaS is simply a more economical approach; for others, not so much.

The rhetoric around cloud is also a marketer's dream because declaring a massive shift that displaces the IT status quo grabs lots of media coverage. But a recent study by the consulting company, McKinsey & Company, suggests that cloud is simply not the most economical way to run many types of enterprise workloads. However, the study also claims that the benefit of a fundamental cloud technology, virtualization, is a credible approach for the IT function to more effectively deliver IT resources to the business units that consume them. Virtualization, coupled with a lightweight management approach and protocols that can operate at web scale, offers the opportunity for the IT function to implement a more elastic and more scalable approach to infrastructure delivery. This approach not only improves the utilization and effectiveness of the internal resources, but also builds a bridge to the consumption of external capacity provided by cloud vendors.

Rather than viewing cloud as a competitive alternative to IT, EMC views cloud as an emerging architecture for more-efficient IT. A cloud architecture provides for loose coupling of applications and data to the physical resources, while also enabling a self-service, elastic, pay-as-you-go approach for infrastructure resource allocations. Virtualization, lightweight management, and web-scale protocols all contribute to this cloud architecture. The final element is an automated policy management system that preserves the IT disciplines of risk management and compliance. With this emerging cloud architecture, the IT function can deliver the benefits and flexibility of cloud computing to the business units, while simultaneously lowering costs and risk to the enterprise.

Cloud as an IT architecture for self-service, elasticity, and scalability

Before embracing cloud as an architecture, the IT function should consider why cloud is popular at all. In many cases, the developers in the business units are using cloud vendors to avoid the bureaucracy and rigid management associated with the resources provided by the IT function. Cloud providers deliver a frictionless, self-service capability for developers to take what they need, pay for what they use, and return the resources when they are done—with very few management strings attached. It is unlikely that this flexibility and elasticity is provided by their IT departments.

Cloud can also provide a level of scalability that is virtually impossible for the IT function to deliver. Consider an application for proprietary trading that needs to run a massive number of Monte Carlo simulations during a brief window of time. Imagine the response of IT to a request for 1000 server hosts delivered to production in 30 minutes for three hours of simulation cycles with no further requirement beyond that period. Very few organizations can scale to that type of request—far fewer than the number that could benefit from that type of capability.

Similar scenarios exist in the area of data management for some organizations. Imagine a media company that is releasing a political comedy sketch video on the run-up to the presidential election. Based on response to the live recording, they are requesting 100 copies of the video to be placed with 15 different network carriers across five continents for the first 30 days after release. After that time, only five copies will be required—all on the local network. Again, the scalability and elasticity of this type of business requirement is not something that is easily managed by a 100 percent captive resource approach to infrastructure delivery. How does the IT staff respond to this requirement for both scale and elasticity?

But what about risk management and compliance? Who is thinking about risk when the business units deploy applications to the cloud? Likely the answer is the obvious one—no one. But if cloud provides such obvious value associated with self-service, elasticity, and scalability, where does this tension with risk and compliance lead the IT organization? Is it possible to have your cake and eat it too? The answer is yes, through adoption of the key elements of a cloud architecture—virtualization, lightweight management, and web-scale protocols—along with a policy management system that enables federation of internal resources with those provided by the cloud vendors, while preserving risk management and compliance mandates.

Where to begin

In any enterprise application portfolio, there are some applications and datasets that are great candidates for migration to a cloud architecture and others that are not well suited to this approach at all. The ideal candidates for migrating to a cloud architecture are those applications that have significant variability in workload demand, along with those datasets that have high access requirements, but are generally static in their state (lots of reads but few writes). Good application candidates include workloads like development/test, periodic analysis workloads, and pipeline processing workloads (design simulations, rendering, etc.). Good dataset candidates for cloud include design files and analysis that need to be accessed by multiple partners in a supply chain, video/audio/images/document publications that are generally available to the public with significant demand, and any of the supporting data for the applications that are candidates for cloud computing cycles.



Federation—embracing cloud while preserving policy

A federation is simply a union of member entities that preserves the integrity of the policies of the individual members. Members get the benefits of the union while retaining control over their internal affairs. In the case of a technology infrastructure federation, the primary benefit of the union is the lower cost and risk associated with a pool of technology assets, which are available across a diversified set of independent networks. Simply put, a federated architecture enables each application workload to run on the network with the lowest risk adjusted cost of execution.

To understand the concept of “risk adjusted cost of execution,” let’s look at a few examples. External clouds are popular with startups because these companies perceive outlays of scarce capital dollars for hardware and data centers to be a high-risk proposition. So, they run almost all of their application workloads on a variable cost cloud service in lieu of spending dollars on capital equipment. For enterprises that already own servers and data centers, the lowest risk adjusted cost of execution for most applications is to run them on the internal network. Ideally, however, these large enterprises can establish an architecture to respond to variable application workload demands by federating their internal capacity with external resources provided by their service providers.

Consider a digital media company that wishes to expand service from the continental U.S. to Europe. In order to deliver a high level of service and performance in Europe, the provider can set up wholly owned, local operations on a European network or participate in a federated technology service that charges a variable fee based upon the actual usage of resources on the European network. During the early stages of entering the new market, the provider gets a smaller startup cost, and therefore a lower risk, for a high level of performance by federating with a European network provider.

Another consideration for embracing an architecture that enables federation can be illustrated with a concept borrowed from the world of financial asset management. Asset diversification is a common approach for managing risk. In the case of application assets, a lower risk profile for any given application and/or data can be achieved through federation. By diversifying production applications and data across multiple networks, the owner of the applications and data lowers the risk of localized network performance problems leading to unacceptable customer service. This is the very essence of good disaster recovery practices, yet with federation, disaster recovery can be implemented in a manner that lowers risk at a fraction of the cost of a wholly owned disaster recovery approach.

Critical to the concept of federation is the preservation of unique member policies. Members can only benefit from federation to the extent that the use of the federated resources does not conflict with internal policies. A simple example could be a large Swiss financial services firm. In the case of public research, the firm publishes to its worldwide client base, it makes sense to use federated storage such that the research is available at a high-performance level across multiple continents. However, in the case of local client records, policy may prohibit client information from leaving the wholly owned networks located within the country where each individual client is served. An ideal federation scenario lets the financial services provider attribute policy to application and data assets in a manner that assures compliance, while also capitalizing on the benefits of the federation.

At EMC, our approach to cloud capability is one modeled on the concept of federation. With our technology, customers will benefit from the availability of resources on multiple networks, while preserving the integrity of the internal policies that govern compliance and risk. We will deliver the benefits of federation through a unique combination of equipment, EMC-hosted cloud services and third-party service provider infrastructure. These resources become available to our customers’ applications through a combination of RESTful APIs, a unique policy authoring and enforcement environment, and the privacy protection measures enabled by our RSA® technology.

Introducing Atmos

EMC developed the Atmos™ family of products with the concept of federation as a key requirement. With EMC Atmos, customers can automatically place data objects on the network. This offers the best customer service performance profile, while simultaneously preserving the policies that govern risk management, without any headaches associated with complex, ad-hoc system administration routines. Data is federated between Atmos and Atmos onLine via a scalable, scriptable policy management system that is unique to the Atmos family.

The EMC Atmos offering is a multi-petabyte platform for the efficient storage and geographic distribution of digital content in a single, unified namespace. By building intelligence at the software layer and providing built-in data services, it enables full control of data handling at the object level. Through a scriptable policy engine, customers can easily define where content should be placed and replicated based upon requirements such as popularity, traffic, or business demands.

EMC Atmos also supports flexible access methods by providing both web services and file system capabilities—enabling a multitude of business needs by easily integrating with virtually any application. Atmos will also seamlessly federate with Atmos onLine, EMC's enterprise cloud storage service.

EMC Atmos onLine is a storage service built upon the Atmos technology and operated by EMC. Atmos onLine cloud storage service requires no hardware, is self-provisioned, and is globally accessed via the Internet and Web Service APIs. EMC Atmos onLine offers seamless integration with Atmos via the RESTful APIs and the policy engine. This combination of technology enables enterprises to federate data between Atmos and Atmos onLine based upon the customer service, cost, and risk policies that are defined within the policy engine. All of this capability is provided without incremental management burdens typically associated with merging the capabilities of various internal and external platforms.



Conclusion—cloud is an opportunity for IT, not an alternative to IT

If viewed as an architecture instead of a competitive threat, cloud offers the IT function an opportunity to deliver a more-effective infrastructure to the business units—one with greater scalability, elasticity, and lower costs. All of these benefits can be delivered within an acceptable risk and compliance posture through a federated architecture that balances internal resources with external resources via automated policy enforcement. EMC is leading the way with Atmos—the first storage platform that offers the benefits of a truly federated architecture by seamlessly combining the resources of the internal network with those offered by cloud service providers. Atmos offers a first step in our commitment to helping our customers embrace cloud in a manner that delivers the benefits of scalability, elasticity, and lower costs, while preserving the IT disciplines of risk management and compliance.



EMC Corporation
Hopkinton
Massachusetts
01748-9103
1-508-435-1000
In North America 1-866-464-7381
www.EMC.com