White Paper

20 Questions for CIOs on Hybrid Clouds

Executive Summary

At ScienceLogic we've had the benefit of observing a number of hybrid cloud deployments up close. All sectors of IT users — from small to large enterprises, governmental groups, and even Cloud Service Providers (CSPs) who themselves have begun to offer managed cloud services from third party platforms — touch the hybrid cloud environment. CIOs, especially, face new challenges in deploying or expanding their enterprise presence in the cloud. This white paper examines four critical areas — migration, security, costs, and visibility — where CIOs can make major differences in the successful execution of hybrid cloud strategies. We've listed 20 fundamental questions CIOs can discuss with both their internal deployment groups and their external Cloud Service Provider/System Integrator in preparation for a migration to or an expansion of hybrid cloud services.

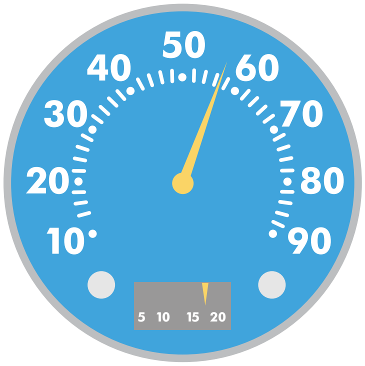
The Continued Growth in Private Clouds

Within traditional enterprise data centers, heavy investment in virtualization continues to grow, despite a shift in investments toward other automation and management tools. Gartner's latest Magic Quadrant for x86 servers estimates at least 70% of x86 workloads are virtualized. In August 2013, a Wikibon survey projected the number would rise to around 84% by the early 2015. The Gartner report also shows that while VMware continues to dominate amongst large enterprises, its relative share of the hypervisor market is decreasing, and the average number of hypervisors types being deployed per data center is falling from 1.82 to 1.67 per data center.

Enter the Hybrid Cloud

With all this investment in hypervisors, one might expect to find that traditional data center workloads in private data centers are exploding. Instead, according to Cisco's recent Global Cloud Index, workloads installed at traditional data centers are projected to grow at a CAGR of just 6% over a five year period (2012 to 2017), while the growth of enterprise workloads in cloud data centers will reach 30% CAGR in the same timeframe. More significantly, many researchers believe we've already breached the midpoint and that 51% of installed workloads being deployed now reside in cloud data centers. The era of the hybrid cloud environment is upon us.

The Cisco study also points out that cloud economics — including server cost, resiliency, scalability, and product lifespan — promote migration of workloads across servers, both inside the data center and across data centers, even those in different geographic areas. Often, several workloads distributed across servers can support a single end-user application. This approach can generate multiple streams of traffic within and between data centers, in addition to traffic to and from the end user.



51% of installed workloads now reside in cloud data centers

The Need for Leadership at the Top

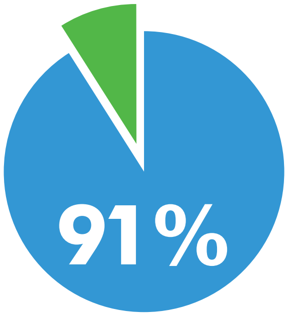
Perhaps most disconcerting in these statistics is the lack of preparation and development of an overall cloud strategy by top management. Many CIOs are navigating blindly into these uncharted waters — increasing their chance of failure. According to Logicalis in Australia, the majority of CIOs (52%) do not have a formal cloud strategy, yet fully half of those same CIOs have a private cloud and 46% of them use cloud in the form of SaaS. The good news is they see the writing on the wall: almost three-fourths (72%) believe the role of the CIO will change significantly in the coming years, demanding a more educated, skilled, and prepared group of internal experts to execute their enterprise cloud strategies.

Based on our experience — and, admittedly, on our role as a major player in the coming of the hybrid cloud environment — we at ScienceLogic offer these considerations for CIOs who want to enter or expand into this new world. Based on concerns we have heard from customers and others at organizations puzzling over hybrid cloud, we've broken down the hybrid cloud essentials into four areas: migration, security, costs, and visibility. To make it easy, we've couched the exercise into a series of 20 Questions & Answers you can discuss with your internal deployment groups and your external Cloud Service Provider/System Integrator in preparation for a migration to or an expansion of hybrid cloud services.

Migrating to the Cloud

1. Do you know what migration is going to cost you?

The benefits of moving workloads off-premises are much more than just a shift from CapEx to Opex. While inherent cost efficiencies exist, they may not be obvious at the outset. In a recent Changewave study, 49% of enterprises surveyed said that migrating to the cloud had no impact on their budget for other IT products and services, while 21% said that it even decreased their budget, and 12% had no idea what the fiscal impact was. The same data viewed another way shows that the vast majority of those migrating to the cloud (91%) will increase (37%) or maintain their current spend (54%). So CIOs should look beyond absolute dollar costs: most enterprises speak of agility and flexibility as greater drivers of cloud migration, particularly with respect to the launching of greenfield apps. In essence, the opportunity cost of slow deployment and TCO are the big picture considerations when considering migration to the cloud.



Percentage of enterprises migrating to the cloud who will increase or maintain current spend.

2. Why move to the Cloud rather than stay in-house?

While SaaS is the explosive grower in the world of cloud computing, IaaS is gaining ground, and for good reason. Arguably, the CIO's hardest task is facilitating mission critical applications, and these are often customized with specific, sometimes extensive, infrastructure needs — hence, the enterprise growth in adopting IaaS. Gartner's CIO Report from February 2014 cites similar trends: business intelligence/analytics was generally seen as the top application being outsourced to the cloud, followed by mobile applications, digital marketing content, CRM, and collaborative apps, all infrastructure intensive. (Email and hosting services have long been outsourced to hosting providers for the same reason.) Those mission critical applications CIOs keep in-house tend to be legacy ERP, accounting and financial apps, and highly secure and legacy customized applications. Core applications tend to be renovated with modern software, and are often consigned to private clouds by many enterprises.

3. How do you burst and move workloads out?

A new breed of managed hosting providers and VARs are available to assist enterprises with migration to external cloud data centers. From this need, trusted advisors have evolved to help in a variety of specific areas: configuration migration

(Racemi and RiverMeadow), data migration (Broad Peak Partners), orchestration (Scalr and Citrix), configuration automation (Chef and Puppet), performance management (ScienceLogic and New Relic), direct connections (Equinix and Telx), and even reference architectures from a variety of cloud, data center, software, MSP, and SI providers.

4. What problems about Day 2 operations should you anticipate?

After migrating to the cloud, CIOs must remember to focus on the degree of transparency and control required for a hybrid cloud environment. Once you move a workload to a cloud provider for efficiency and agility reasons, viewing the health and availability of the delivered business services end-to-end is difficult now that resources are split between on-premises and off-premises. You could look at deployed instances in a third party cloud, using the local cloud tools, but you really wouldn't see the correlation of the application running on top of those instances with the ones running on-premises. Your trouble detecting the relationship is made worse by the fact that, for example, seeing how storage relates to your compute cycles in a different environment is difficult, if not impossible. The real issue, then, is that you're unable to know when a real outage or performance problem occurs in this hybrid world, let alone perform root cause analysis.

5. How can you accelerate migration and unlock benefit and value early?

Speeding up a migration is usually a question of internal preparedness. The CIO's greatest asset is an educated, informed IT staff. In December 2013, a ScienceLogic survey of 1,000 IT professionals showed that half of all respondents participating in cloud initiatives within their organizations needed more education on technology. The respondents to the survey also noted that their current skill sets did not adequately prepare them to do their jobs well in the coming year. More specifically, the top area that these respondents believed they needed more education on was in cloud technologies. To address this need for greater cloud skills among IT professionals, more and more cloud providers and software vendors are offering online courses for both the business and technical staff. Also, more intuitive tools are making control and visibility in the cloud easier than ever for cloud operations.

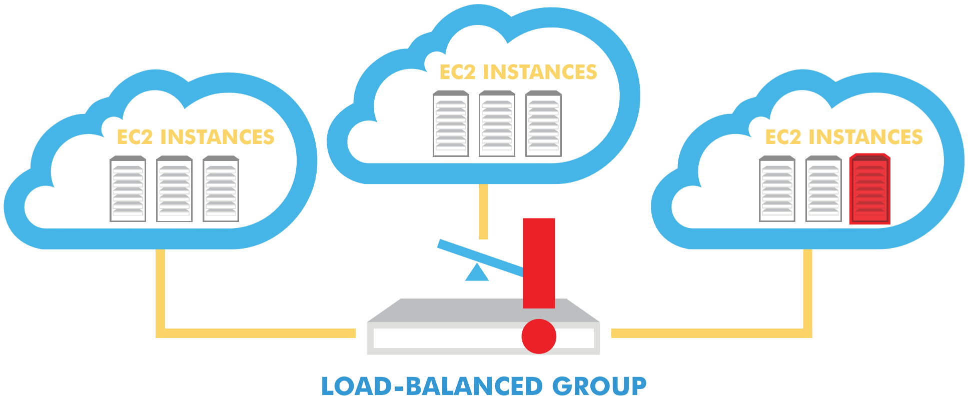
Security in the Cloud

6. What security and assurances should you look for?

According to a recent CIF Study, 98% of companies have never experienced a breach of security when using a cloud service. The security risks inherent in clouds do not necessarily make them any more vulnerable than many of today's top tier private data centers. Still, to provide customers with greater peace of mind, individual cloud providers offer different degrees of advanced security that minimize, if not mitigate, varying levels of risk. Most Managed Service Providers (MSPs) providers, for example, include a base level of intrusion detection (IDS) and prevention (IPS). But, increasingly, Cloud Service Providers (CSPs) are offering layered security models, starting with single sign-on with authenticated devices, multi-factor authentication (MFA), encrypted data storage, secure VPN connections, private subnets, and other options that all come at increased expense.

7. Where are the less obvious vulnerabilities in hybrid cloud environments?

Aside from the typical security considerations mentioned above, a number of softer, less apparent



If a group of load balanced AWS instances spread across multiple regions has an issue, it is difficult to find the instance causing the problem instance.

vulnerability points exist when operating in third party clouds. For example, in AWS each Virtual Private Cloud (VPC) requires its own set of security policies. But with so many organizations deploying hundreds of VPCs, human error becomes more likely, allowing the wrong instance to be deployed to the wrong VPC. This scenario could engender a whole host of security challenges or compliance issues, and once all of your instances are deployed, determining whether they are all deployed in the correct VPC isn't easy. Here is where — and why — having the right visibility becomes critical.

8. What happens when my cloud fails?

Over the past eight years, we've observed a number of disasters that occurred for a variety of reasons, resulting in, at times, significant downtime from top cloud providers. In each case, organizations have thrown up their collective IT arms in disgust at the cloud provider's failing. In reality, the onus was actually on the cloud customer who should have gauged beforehand the relative importance of downtime attributable to mechanical, electrical, human, or even software failure. Having a DR/backup plan should be your norm, as should an SLA attached to your IT crown jewels. Similarly, having duplicate instances in the same availability zone, for example, is a recipe for disaster — historic and geographic redundancy data is increasingly available from cloud platforms, although not always collected by the CSP itself.

9. Will I be locked into any foolish/unsecure/underperforming decisions?

Exit strategies, contract lock-in, and data ownership are among the top concerns identified by a Cloud Security Alliance (CSA) Information Systems Audit and Control Association (ISACA) survey. Unlike in the past, current vendor lock-in is not about interoperability between infrastructure components, but rather about being locked into a single service or data center serviced by a single telecommunications carrier. What's more, the administration tools the cloud providers may give you to configure and maintain the application will be, for the most part, controlled by the cloud provider. You should ensure that your CSP understands these concerns and provides you with adequate liberty relative to migration tools, network density, and contract flexibility.

10. What are the risks for information security and data sovereignty?

These security and compliance concerns are becoming more pressing than ever. Many Cloud Service Providers mistakenly under-advertise their regulatory compliance. Asking for their accreditation is usually a good place to start, but be aware of the nuances in the accreditations. For example, PCI DSS is a proprietary information security standard that specifies 12 requirements for compliance, each with a number of sub-requirements. Most CSP's will be focused on meeting the first control objectives around building and maintaining a secure network, which entails deploying a firewall and not providing vendor supplied defaults for system passwords. Many CSPs may become level 1 PCI DSS service providers, but getting to additional levels requires the ability to handle a significant upscale in transactions and other requirements. It's important to understand your own industry since healthcare, finance, retail, and government have standards that may necessitate a multi-cloud solution. In fact, the Cloud Industry Forum's newly released survey of a broad spectrum of organizations in the UK showed that, for companies with more than 200 employees, as many as 48% had 2-5 different cloud-based services. The percentage was even higher for small businesses.

Managing Costs & Getting Value for Your Money

11. Do you know your total cost of ownership (TCO)?

All too often, hybrid cloud migrations result in sticker shock, especially following a series of cloud IaaS deployments without any reservation or contract in place. Lack of control over the total volume of auto scaling allowed for instances only makes the sticker shock worse. Money spent in one place, however, can mitigate expenses elsewhere. For more strategic cloud deployments, you should carefully balance the seemingly high cost of an IaaS deployment with the historical operations, MTTR, licensing, human resources, networking, storage, and hardware maintenance and operational costs. Despite the fact that these are often sunk costs — plus the fear of insufficient budget for a move to the cloud — very defendable calculators are available to show the long term TCO reduction possible with the cloud, if all variables are included.

12. Are you getting the best bang for the buck/cost per performance?

Notwithstanding number eleven's TCO discussion, the recent Cloud Industry Forum survey confirmed that ROI vs. on-premises delivery was not the main reason for choosing the cloud. Rather, the primary measuring sticks for making the move were flexibility of delivery (58%), scalability (65%), and general performance expectations alongside operational cost savings (15%). The challenge for a CIO who wants to examine cost as a justification, however, lies in the fact that not all clouds make historical performance metrics available, at least from a per region perspective. In our experience, we've found a material difference in performance, even with cloud platforms stretching across multiple regions that come at costs outweighing lower prices.

13. Are you aware of your overprovisioned, forgotten resources and runaway workloads?

Just as virtualization resolved the issue of physical server sprawl in the data center, only to be replaced by VM sprawl, so too does the benefit of cloud services introduce both a benefit and a longer-term hidden threat, namely the abstraction of infrastructure control that increases over time.

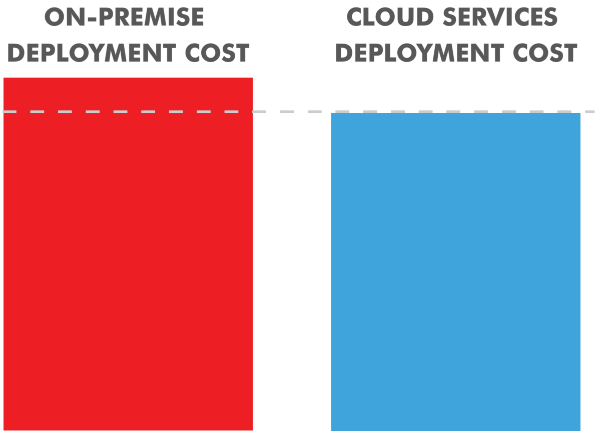
As an example, many users within AWS are firing up EC2 instances alongside numerous EMR (Elastic Map Reduce, which uses Hadoop to process large amounts of data) instances for specific jobs. Once complete, they will often shut down the EC2 instances but forget about the EMR jobs. Those EMRs are no longer running but still sitting out in the ether unused and costing the company money for unnecessary resources. Once the EC2 instance is removed, detecting the idle existence of the EMRs out in the ether is impossible without outside assessment — hence, the need for independent tools to keep track of these scenarios.

14. Do you know the right payment model for your cloud deployment?

It is a well known but fascinating fact, that AWS has dropped its prices 42 times since 2006. Furthermore, the cost of an Amazon EC2 instance has decreased 56% in just the past two years. This in turn has motivated many other cloud providers to both reduce the cost of their cloud offerings and disperse the overall cost of their cloud solutions by offering a series of discrete cloud modules or components that are often difficult to quantify. The difficulty with Cloud platforms is that there is the added challenge of using spot prices (instances whose prices that are bid on and used until a higher bid comes through), on-demand pricing (by the hour), and reserved instances (for dedicated or committed resources). Add to that the approximately 40 services offered by AWS, and the complexity and ability to aggregate, plan and limit cost can be a challenge.

15. How do you optimize for cost and scale?

According to the Cloud Industry Forum, users of cloud services on average are achieving a 9% cost savings over-on-premise deployments. The ways to get those savings, however, are highly nuanced. Planning is essential, as the best public cloud economic models require commitment from executive sponsors and the rest of the organization. Understanding and striving to achieve your current and desired future cost thresholds, especially as they pertain to KPIs or desired outcomes, is where most companies fall short. Employing tools that show cost thresholds (and trajectories) alongside performance metrics (IOPS, for example) as well as offer some understanding of risk (and health), especially when deploying on shared infrastructure, is achievable, but should be planned for in advance of a move to the cloud.



Cloud services on average are achieving a 9% cost savings over on-premises deployments.

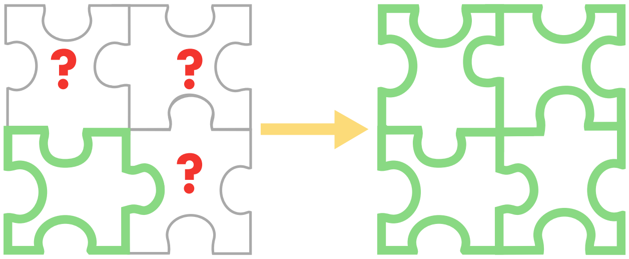
Visibility in the Cloud

16. To what extent is lack of visibility and control holding you back?

As cloud platforms begin to be consumed on an IT services basis, so too should IT service management become more than just about SLAs. Having real confidence in your decision to migrate workloads to the cloud requires that you enjoy transparency and visibility in that cloud environment. That confidence will, in turn, lead to trust in both the decision maker — you — and the cloud itself. Although cultural change and internal acceptance are ongoing topics, the expanded message is really about helping C-levels feel assured of their decisions through adequate control and security measures. Achieving such assurance is no easy task and requires a modern approach to keeping the costs down for doing so. Transparency and visibility into the cloud, in this instance, are essential and, ultimately, cost effective.

17. Do you know whether the service health and performance of your workloads are uncompromised?

Most legacy monitoring and management systems are able to take a latency measurement from an end user perspective to the applicable web service. Others simply show the uptime and availability of a physical piece of infrastructure. But since not all hiccups in infrastructure cause issues for end consumers, what's truly needed is the ability to have visibility and control of the physical IT infrastructure, and to see separately how related services that rely on that infrastructure are performing. Even more important is the ability to correlate data metrics in intelligent ways that illuminate the health and risk a critical service will begin to face in the coming hours, days, or weeks. That's exactly what a modern monitoring system should be able to do. Only through the collection of data, the normalization of that data, and the presentation of results in an intuitive format can analytics be truly useful and actionable, including those driven by monitoring tools. In a hybrid cloud environment, such insight becomes even more critical for CIOs who need to maintain control of all elements across the IT spectrum.



To deliver the new breed of hybrid services organizations will need to see the entire infrastructure, not just one or two pieces.

18. Can you safely manage delivery of the new breed of hybrid IT services?

The 2013 ScienceLogic survey of enterprises attending Cloud Expo showed an extremely low level of support for point tools (6%). This is understandable, given what the market has experienced through the sprawl of point tools — large inefficiencies as well as unnecessary costs per tool are likely results of their overuse. The trend away from point tools has several causes: the changing nature of hybrid cloud environments, the lack of true integration among corporate acquisitions, as well as the advent of converged infrastructure. Vendors have done a poor job of converging the management tools for those technologies, leaving the door open for vendor-agnostic monitoring and management specialists to fill the gaps. Delivering the new breed of hybrid IT services will depend on choosing the right vendor-agnostic monitoring and management solutions for your organization.

19. What should you be asking of your service providers?

Recent analysis undertaken by the Enterprise Strategy Group found that within cloud storage SLAs alone, there were a number of variations. MSPs offering bulk storage services online typically have cloud SLAs spelling out what users are entitled to for recourse. Typical service availability reads at a traditional 99.99% level of uptime. The shortcoming in this form of SLA is that it still represents approximately nine hours of annual downtime. Nine hours is a lot of time when critical business applications are involved. That's why the more progressive SLAs include the response time of the web service, how often a retry is allowed, retention policies, number of copies, and a tiered credit guarantee with higher credits for lower service levels delivered. CSPs can offer geographically dispersed options to increase backup and recovery, and by default, service levels. Hence, the need for more strenuous management tools in the era of cloud that add increased visibility, control, and assurance to private cloud applications.

20. Can all of these questions and fears be answered and mitigated by the correct people, process, and tools?

As stated throughout this paper, CIOs and their organizations need the right people, which means skilled and up-to-date IT staff. Processes are often particular to the individual organization, its goals, and its resources. The correct tools are the ones that everybody needs and are easy to use; they update regularly to ever-changing characteristics of what they work on; and they adapt to all configurations. In particular, we have found that the correct tools can reduce the dependency on additional human resources, and more often than not, will actually help the alignment of internal processes. For example, having a series of escalation procedures and remediation procedures aligned to a variety of the most common performance and security issues in the cloud is a must. The correct tool accomplishes this by first looking at the business policies demanded of the cloud, and then associates all of the possible monitoring and alerts around those business policies to automated actions. The correct tool can restructure the way in which operations are done day to day for maximum efficiency, on-premises or in the cloud.

Winning in the Cloud

The CIO's best strategy for successful deployment in the cloud is, stated simply, to have a strategy in place. That process requires assembling knowledgeable IT staff, which may involve some continuing education. Making your internal deployment groups and your external Cloud Service Provider/System Integrator part of the process is also key to a successful migration to or expansion of any hybrid cloud environment. Most importantly, asking the right questions ahead of time will save you from learning embarrassing answers later. At ScienceLogic, we stand ready to share our experience and knowledge in hybrid cloud migrations and expansions, with both questions and answers.

About ScienceLogic

ScienceLogic delivers the next generation IT monitoring platform for the network of everything. Over 15,000 global Service Providers, enterprises, and government organizations rely on ScienceLogic every day to significantly enhance their IT operations. With over 1,000 dynamic management Apps included in the platform, our customers are able to intelligently maximize efficiency, optimize operations, and ensure business continuity. We deliver the scale, security, automation, and resiliency necessary to simplify the ever-expanding task of managing resources, services, and applications that are in constant motion.

ScienceLogic won InfoWorld's 2013 Technology of the Year award, Red Herring's Global 100 Award, Deloitte's Technology Fast 500™, and MSPmentor 250, among other worldwide recognitions of excellence. For more information, visit www.sciencelogic.com.

Contact Us

Americas	Europe	Asia-Pacific
+1.800.724.5644	+44 (0) 203.603.9889	+61 2 9959 2426
info@sciencelogic.com	info-eu@sciencelogic.com	info-apac@sciencelogic.com