WHITEPAPER

THE THREE CRUCIAL COMPONENTS YOU MUST CONSIDER BEFORE MIGRATING YOUR DATA TO CLOUD

In the cloud, it's substance that counts. You need to cut through the hype and look beneath the surface at a cloud provider's infrastructure, network and security.

TRADITIONAL STORAGE HAS REACHED ITS LIMIT

The amount of data generated today is growing at an astonishing rate, doubling in volume every two years. Just two days of current global data production from all sources — five quintillion bytes — is equal to the total amount of information created by all the world's conversations ever, according to research at the University of California, Berkeley.

It's just the beginning. By 2020, there will be 4300% increase in annual data generation. There will be 35 zettabytes living in and travelling through the Internet. Enterprises will have generated 28 zettabytes and be managing 10.5 zettabytes. Traditional storage technologies such as NAS and SAN, now stretched to their limits, will be useless for storing and managing all that data. One thing is clear in this rapidly emerging environment — the future belongs to cloud storage.[1]

BUT NOT ALL CLOUDS ARE ALIKE

There are significant and substantial differences between each cloud storage provider's offering. That's why it's absolutely necessary to carefully scrutinise the three key components of a provider's offering — infrastructure, network, and security.

INFRASTRUCTURE: THE KEY ELEMENTS THAT MAKE A BIG DIFFERENCE

The infrastructure is the guts of the system — the hardware and software components that store and manage your data at the data centre. The individual components include such thing as servers, storage hardware, virtualisation software, and operating systems.

The infrastructure needs to be flexible and scalable to provide elastic capacity while delivering optimum performance. Access should also be provided through an industry-standard Web services API (application programming interface) based on the SOAP (Simple Object Access Protocol) or REST (Representational State Transfer) protocol.

Capacity must be available on demand and provisioning more capacity should be instant and transparent on a pay-as-you-go basis, enabling an administrator to serve hundreds of users and easily manage petabytes of storage capacity. The infrastructure should also be accessible throughout the life of the data, which means automatic data migration to allow hardware upgrades without interrupting service.

Most important, the cloud provider must own or own in partnership the data centres where data is stored to ensure dependability and accountability. Data centres should also be geographically dispersed — and in the areas where your offices and users are located to enable fast, reliable, global access.

INFRASTRUCTURE CHECKLIST

Look for the following attributes in your cloud provider's data centres:

✓ Data centre ownership

✓ Strategic data centre partnerships

✓ Network and hardware performance

✓ Wide geographic distribution

✓ Reliability and fault tolerance

✓ Provisioning time and time to scale up or down

✓ Embedded infrastructure monitoring and alerting mechanisms

✓ Comprehensive Service Level Agreement (SLA)

THE NETWORK: THE SPECIFIC CAPABILITIES YOU MUST HAVE

Cloud storage requires a highly flexible, scalable, reliable, and seamless global network. Look for the following capabilities and features:

- **Scalability.** A network optimised for cloud storage needs to easily scale in the total volume of storage capacity and the number of sites that it provides for storage. That's why it's so important to choose a provider that owns, operates, and has complete control over its underlying network. Without ownership, a provider cannot ensure that the capacity you need will be there when you need it.

- **Accessibility.** It's important that a provider's network support both legacy and newly emerging access protocols and offer a wide range of future-proof connectivity options. Your enterprise needs this to assure a seamless and scalable growth path.

- **Bandwidth.** Depending on business use cases, available bandwidth is a critical consideration. For example, a media content distributor that streams audio and video programming to users worldwide needs high bandwidth and throughput. As your enterprise UCC and video conferencing needs will grow along with your storage needs, your bandwidth and throughput requirements will skyrocket. You'll need a cloud provider that has a global presence with nodes distributed worldwide and especially in the key locations where you currently operate as well as the new markets you're targeting.

- **Reliability.** Any service interruption or data corruption costs you plenty in time, money, and lost opportunities. That's why you need a high-performance storage cloud that delivers a proven and superior level of availability, durability, and data integrity. That includes conducting continuous background data integrity checks to systematically verify and automatically repair any corrupted files.

- **Performance.** Your cloud storage provider needs to demonstrate optimum levels of throughput, IOPS, and latency. If your application throughput requirements total hundreds of GBs, you need to make sure that your provider's network can deliver it. Equally important, if your applications are latency sensitive, make sure that your provider's storage platform enables latency optimisation.

- **Ownership/Partnership.** With ownership comes responsibility and accountability. Having a cloud provider that owns and operates its own global network helps ensure that the performance, capacity, scalability, and reliability that you sign up for will be delivered. In addition, look for a provider that extends its reach through high-quality global partnerships that touch all geographic areas where you have or intend to develop markets.

- **Provider-owned network.** There are great advantages in choosing a cloud provider that is also a Tier 1 ISP. Such a provider gives your enterprise a direct connection to your cloud storage platform. Another huge advantage of working with a Tier 1 provider is that if there is a problem with access, you only need to deal with one provider which makes solving the issue faster, easier, and far less complicated.

NETWORK CHECKLIST

In evaluating a cloud storage provider, evaluate these specific network attributes to help ensure that you get the performance and reliability you need:

✓ Scalability

✓ Accessibility

✓ Bandwidth

✓ Reliability

✓ Network ownership

✓ Provider-owned network

SECURITY: THE PROTECTIONS YOU NEED IN THE CLOUD

It's essential to thoroughly review a cloud provider's security measures to ensure good governance and the highest level of data security. First, review their information security policies and procedures to make sure that they adhere to proven standards, such as ISO 27001. This standard strictly defines the accepted policies and procedures covering all legal, physical, and technical security controls involved in an organisation's information risk management procedures.

More than 50% of the respondents to the "Cloud Usage Risks and Opportunities Report" by the Cloud Security Alliance listed storage as the most risky cloud application according to their organisation's definition of risk.[2]

Next, get granular and make sure that they have the following security components in place: data encryption both in storage and in transit, virtual firewalling, Role Based Access Controls (RBAC), SIEM integration, HTTP over SSL protection, IPSec tunnelling — and especially DDoS protection and dedicated VDOM.

The provider should also demonstrate that it conducts regular, independent audits, and penetration tests — and is open to sharing the results with you. It's also highly recommended to check the provider's staff vetting and management processes to confirm that they follow industry best practises.

The 2015 Data Breach Industry Forecast from Experian found that employees caused nearly 60% of security incidents the previous year.[3]

CLOUD SECURITY CHECKLIST

Look for a cloud provider that offers comprehensive, integrated, managed security bundled with its cloud storage service and includes the following components:

✓ DDoS Protection

✓ Dedicated VDOM

✓ Role Based Access Controls (RBAC)

✓ Virtual Firewalling

✓ SIEM Integration

✓ HTTP over SSL Protection

✓ IPSec Tunnelling

THE BOTTOM LINE

Cloud is forcing enterprises to take a new architectural approach to everything. Cloud services are especially compelling and inevitable because they deliver huge benefits that the classic approach to business service design and application architecture can't provide.

Looking ahead, solutions must be developed that do not depend on brute-force throughput over relatively slow and inconsistent WAN links. This requires more sophisticated architectures that sensibly locate compute and storage resources near one another and limit long-distance communications to more lightweight demands. The focus going forward must be on newer systems of engagement while postponing moving legacy services and systems of record to the cloud which can be counterproductive. In conclusion, the best path forward is to evolve quickly, but responsibly.

Let us show you what we can do for you to make your enterprise more efficient, productive, and collaborative. Visit us today at tatacommunications.com/IZO.

[1] www.csc.com/big_data/flxwd/83638-big_data_just_beginning_to_explode_interactive_infographic

[2] www.techrepublic.com/article/cloud-security-10-things-you-need-to-know/

[3] www.techrepublic.com/article/cloud-security-10-things-you-need-to-know/

For more information, visit us at www.tatacommunications.com/IZO

Contact Us | **Share** ✉ 🐦 in