Six ways to fail with your enterprise cloud

OVHcloud

vmware®

Cloud computing has become firmly entrenched in mainstream IT. With digital transformation taking hold across all industries, organisations are turning to multi-cloud strategies to better adjust to new market demands. For enterprises, a key element of this approach is private cloud, which is considered inherently more secure than public cloud[1].

Though an enterprise private cloud offers more control over the physical environment and unmatched customisation capabilities, building your private cloud presents its own set of issues…

Security breaches

Data breaches, compromised credentials, broken authentication, hacked interfaces and APIs – 2018 has seen more than its fair share of massive security breaches. Weekly reports of cyberattacks and breaches don't help to alleviate security concerns about cloud computing.

This leads many organisations to believe their data is safest in-house, in their custom-built cloud environments. The reality is that hosted environments are as secure as those on-premises, if not even more. They are designed and maintained by security experts who understand cloud security challenges and know how to mitigate them.

DDoS attacks

Distributed denial of service (DDoS) attacks remain a major concern for all digital companies. Over the course of years, the attackers have become increasingly sophisticated in their methods, and with new technologies, like the Internet of Things (IoT), come new threats.

A DDoS attack overloads a web server, and if successful, renders a website inaccessible for hours, or even days. This can cause a loss of revenue and customer trust. Anti-DDoS protection is therefore no longer just a nice-to-have feature for enterprises; it's a core security system. However, on-premises protection will never match industry-leading systems' capacity to mitigate attacks.

[1] *An IDC Infobrief, June 2019.*

“Being a cloud service provider, we receive and mitigate over 2,000 DDoS attacks each day. Our anti-DDoS system protects all customers by default. There is a very simple reason behind this: a DDoS attack, if not mitigated, can result in collateral damage. It means that not only does the target experience the attack, but all neighbouring servers in the rack also will. The VAC (a combination of technologies developed by OVHcloud to mitigate DDoS attacks) only activates when an attack is detected. However, for customers with specific security needs, we provide constant traffic filtering; in other words, a permanent activation of the VAC”

Jakub Słociński, Network Innovation Manager at OVHcloud.

Physical security and redundancy

Most organisations don’t have the same physical security features offered by third-party datacentres, which can put their valuable data at risk. A reputable datacentre will be a fortress, with strictly monitored access and barbed-wire fencing. Video surveillance and motion detection systems will be in continuous operation, as will fire detection and extinguishing systems.

Today, constant accessibility, high availability, and resilience are key elements for many IT services. Achieving the same level of redundancy for an in-house private cloud would be an ambitious task. Double electrical power supplies, power generators, UPS devices and redundant network links all add up to high maintenance costs, not to mention requiring a high level of in-house expertise.

Compliance concerns

The PCI DSS standard lists over 250 controls and security features that need to be set up to process payment card data securely. Private cloud grants greater control over security, but that doesn't make regulatory compliance any easier.

Maintaining compliance should always be at the forefront of planning, particularly when multiple types of regulated data are in play, such as payment card data, sensitive business intelligence and customer data. It's a time-consuming and expensive process, often requiring an organisation to employ an IT expert that's familiar with these regulations. In addition, the IT team will need to continuously monitor systems, develop clear security incident procedures, and use data encryption to ensure that compliance requirements are constantly met.

Performance issues

Performance is a well-known issue in dynamic virtualised environments. It's difficult to predict how changes at the infrastructure level will affect application performance, as even a simple software update can unbalance a closed ecosystem. To make sure you get the most out of your infrastructure, it's therefore crucial that you put a continuous process to validate the cloud's performance in place. For every new deployment and core change, you need to have a realistic performance test, preferably an automated one that can expose issues at an early stage. Having such a process in place protects your company from unnecessary costs, and allows you to keep close control over the price/performance ratio.

Capacity overbuying

Whether you're building your private cloud with OpenStack or VMware, there is always the same major challenge: how to achieve agility and scalability when managing an internal infrastructure? When maintaining one's own infrastructure, an increase in capacity will require more hardware equipment. When unable to precisely predict the capacity they will need, IT teams often overbuy, to ensure they can deliver the expected resources when needed. As a result, the organisation ends up with high investment costs and a feeble promise of scalability.

It's debatable whether an on-premises infrastructure can truly become the "cloud", as the definition of the cloud highlights flexibility and scalability, without having to invest in additional hardware. However, though many assume that a private cloud just means "on-premises", this doesn't have to be the case. A private cloud is an infrastructure used solely by one organisation; its resources are not shared, but isolated and dedicated. A hosted private cloud provides organisations with the necessary means to gain agility and increase operational efficiency, while mitigating the common risks that come with enterprise clouds. In a hosted private cloud environment, part of the control and responsibility for security is relinquished to a trusted service provider. In light of this, choosing the right vendor, with a proven record when it comes to security, is essential if these challenges are to be overcome.

OVHcloud is a global, hyper-scale cloud provider that offers businesses industry-leading performance and value. Founded in 1999, the group manages and maintains 30 datacentres across four continents, deploys their own fibre-optic global network and controls the entire hosting chain. Relying on their own infrastructures, OVHcloud offers simple and powerful solutions and tools that put technology at the service of business, and revolutionise the way that our more than one million customers around the world work. Respect for individuals, freedom and equal opportunities for access to new technology have always been firmly rooted principles of the company. "*Innovation for Freedom*".