

4 Key Steps to a Successful Cloud Migration Strategy

The truth in information.

Organizations are still a ways out from adopting a public cloud computing model that is worry-free and cost-efficient.

According to IDG's *2016 Cloud Computing Survey*, the average enterprise has 26% of its IT environment in a private cloud and 13% in the public cloud. Small and medium sized businesses have 21% in a private cloud and 17% in the public cloud.

While public cloud adoption is increasing, it's still in the early stages. The improved security measures implemented by cloud providers is accelerating the move to a cloud computing model, even for critical IT services.

CONSIDER THIS BEFORE ADOPTING A PUBLIC CLOUD COMPUTING MODEL

The difficulty of migrating workloads to the cloud depends on several factors: the time sensitive nature of the move, the amount of data and the complexities of the IT services to be moved.

Most organizations have a set budget and timeline to accomplish this, and failure to migrate per the business plan can have expensive consequences.

Making it into the public cloud like Amazon Web Services (AWS) and Microsoft Azure, doesn't necessarily mean a stress-free business life. For a successful migration and business environment, there are some important factors that need to be considered.

- **How do I ensure successful migration?** Before spending time, effort and dollars migrating business workloads, it's essential to ensure a positive outcome. Without a way to test that your migration will work and that your business workloads will work optimally in the cloud after the move, you may be leaving things to chance—which is never a good strategy. You need to be able to test your migration strategy before you put it into action.
- **Will I lose control of my workloads once they are in the cloud?** Adopting public clouds into your already multi-vendor, multi-platform environment can cause fragmentation issues which in turn lowers visibility into business IT health. Maintaining real-time visibility is important so you can make well informed business decisions and easily ensure that your business is meeting service continuity objectives such as recovery time objectives and recovery point objectives.
- **How resilient is the public cloud?** Even the most robust perceived public clouds can go down due to something as simple as human error, as the world saw in early 2017. If this occurs, your business will be impacted by economic loss including lost revenue, lost productivity, lost time and loss of value and reputation. The bottom line is that no cloud is failsafe; however there are measures that you can take to ensure minimal risk to your business in case of a cloud catastrophe.
- **Will I be locked-in?** Similar to hypervisor technologies, cloud vendors want to ensure your business loyalty, which means that getting out of the cloud may not be as easy as getting into the cloud. If your business priorities change at some time in the future you may need to move your business applications back to on-premises or even to another cloud. You need to stay flexible and agile so you can adapt easily as your business goals change. To do this you need to ensure you aren't putting all your eggs into one basket—or in this case one cloud.

FOUR KEY STEPS TO ENSURE A SUCCESSFUL CLOUD MIGRATION STRATEGY

There are four key steps to creating a successful and stress-free cloud migration journey: testing and re-testing your migration strategy before runtime; ensuring your visibility into business IT health once you are in the cloud; making sure you are resilient against cloud outages; and being prepared to move out of the cloud if necessary. Let's examine each of these in more detail.

1. TEST AND RE-TEST BEFORE YOU MIGRATE

A successful migration starts with a successful test. Similar to disaster recovery testing that ensures smooth failovers when needed, a migration test helps ensure that your business workloads will run in the cloud successfully after migration. There are multiple aspects to this strategy. First you need to replicate your business data to the cloud. Then you need to ensure that the testing solution you are using creates a real-time copy of the replicated data. This copy then gets attached to your test workload on the compute instance before it is brought online. This is important because you don't want to connect directly to the replicated data stream which could possibly cause production issues. Finally, you want to be able to repeat tests easily without manual efforts or downtime to the business. This is important because IT environments are constantly changing and can be impacted by configuration drift. Being able to perform repeatable and automated migration testing before the actual migration is the only way to be assured that the plan will work.



2. ENSURE CONTINUED VISIBILITY INTO BUSINESS IT HEALTH

Visibility into business IT health is vital to guarantee compliance to internal and external regulations and to ensure that your business is meeting critical service level objectives. But with business workloads spread across on-premises and public clouds, gaining real-time visibility into IT health can be difficult. While cloud adoption is on the rise it's mostly a limited percentage of business services that make it to the public cloud today.

Most organizations continue to have legacy and critical workloads hosted on-premises. Organizations have business applications spread across multiple geographic locations and one or more clouds. This geographic fragmentation can cause operational fragmentation—there may be multiple teams managing these business workloads, visibility into IT health is lowered due to lack of real-time information, and operational expenditure costs can increase due to different tools being used across on-premises and cloud environments. Overall, operational risk is increased which can lead to downtime—never a good thing.

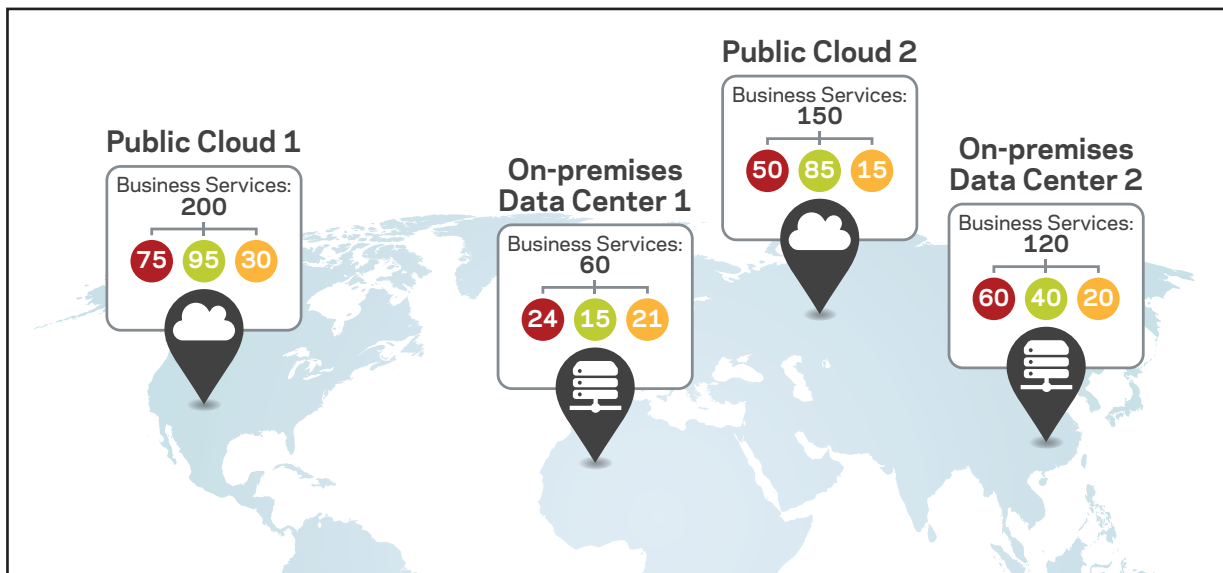


Figure 1 – Attaining single pane of glass visibility into business health is even more important in a multi-cloud world

3. ADD A RESILIENCY SAFEGUARD

Cloud isn't always failsafe and your business workloads are your responsibility, not your cloud providers' responsibility. If your cloud provider experiences an outage, your business may likely be impacted by financial and reputation loss. Depending on your industry and the related business continuity regulations you need to meet, you could also face harsh regulatory fines for downtime of critical IT services, especially in the financial services, banking and healthcare industries. It's your job to stay vigilant and be prepared for an outage that is not in your control. To do this, you should implement a resiliency solution for your public cloud workloads that is different from the basic resiliency add-ons available through your cloud provider. A robust solution will be able to alert your business instantaneously when an outage occurs, and easily failover your workloads to another zone or region in the cloud or even back to your on-premises environments.

4. BE PREPARED TO MIGRATE OUT OF THE CLOUD IF AND WHEN YOU NEED TO

Vendor lock-in is one of the top three concerns organizations have about the public cloud according to IDC's 2016 Cloud Computing survey, after concerns about where the data is stored and the security of cloud computing solutions. Similar to hypervisor technology vendors and OS vendors, cloud platform vendors would prefer to have your sole business, which is why most public cloud vendors offer their own free native tools to migrate solutions to their cloud. But business goals and decisions are not constant—goals today may not stay the same in five or ten years. What happens if your business needs to move workloads back to on-premises in the future? You need to be prepared.

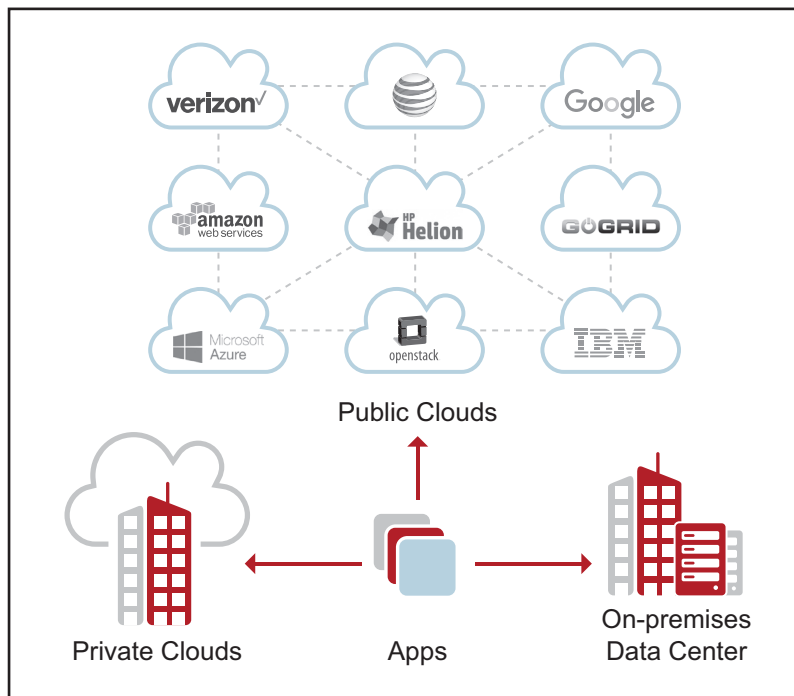


Figure 2 -An agile business has the ability to seamlessly move workloads to the cloud, from the cloud, and also between clouds

VERITAS RESILIENCY PLATFORM HELPS ACCELERATE YOUR CLOUD MIGRATION STRATEGY WITH THE RIGHT APPROACH

Veritas Resiliency Platform helps organizations seamlessly and confidently move their business workloads, including complex applications, between on-premises and public clouds simply and with a single click. Organizations benefit from the fully automated and non-disruptive migration testing that helps ensure successful and predictable migrations. They can additionally stay agile and flexible with the option to failback IT services back to on-premises environments as needed, or another cloud. Learn more about [Veritas Resiliency Platform](#).

NEXT STEPS: PROTECT YOUR CRITICAL BUSINESS ASSETS ACROSS YOUR HYBRID CLOUD

86% of Global Fortune 500 enterprises trust Veritas with their most critical asset—their information. Visit [veritas.com](#) to learn more about protecting your information with unified business resiliency.

ABOUT VERITAS TECHNOLOGIES LLC

Veritas Technologies LLC enables organizations to harness the power of their information, with solutions designed to serve the world's largest and most complex heterogeneous environments. Veritas works with 86 percent of Fortune 500 companies today, improving data availability and revealing insights to drive competitive advantage.

Veritas Technologies LLC
500 East Middlefield Road
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (866) 837 4827
veritas.com

For specific country offices and contact numbers, please visit our website.
<https://www.veritas.com/about/contact.html>

VERITAS™

V0418 4/17