5 reasons to avoid off-the-shelf disaster recovery solutions - blueAPACHE

Canonical: https://www.blueapache.com/blog/5-reasons-avoid-off-shelf-disaster-recovery-solutions

Details:

2017

We explain why your disaster recovery approach should reflect your applications, recovery priorities and operational needs.

The global Disaster Recovery as a Service (DRaaS) market is anticipated to expand at an astounding 36 percent Compound Annual Growth Rate (CAGR) from 2014 to 2022, rising from a value of USD 621.3 million in 2013, according to a report by Transparency Market Research. The rapid growth may instil confidence that the offerings are becoming mature, and that generic off-the-shelf solutions will meet your DRaaS requirements, meet compliance requirements and offer an adequate level of business continuity to appease the broader stakeholders. Unfortunately, this is where many organisations fall down. When a disaster strikes the survival of your business may well depend on the quality, accuracy and timing of disaster recovery (DR) solution and procedures. Here are five simple reasons why the off-the-shelf approach may not be the best solution for you:

Affordability

The recovery requirements of individual organisations vary widely depending on the nature of the business – business continuity for an online shopping site, for instance, will entail completely different requirements as compared to those of a local brick and mortar grocery store. When devising a custom DR plan with your DRaaS provider, Service Level Agreements (SLA) can cover a whole gamut of factors including Recovery Point Objective (RPO), Recovery Time Objective (RTO), the level of technical support required, the support coverage and penalties for not meeting SLAs and other critical factors. Each of these components has an associated cost and the first step towards finding your DR solution is understanding and defining your organisation’s tolerance for downtime and data loss. Consider RTO as an example. RTO is the duration of time and a service level within which a business process must be restored after declaring a disaster in order to avoid unacceptable consequences associated with a break in business continuity. The RTO for mission-critical applications, those that you cannot function without, could be in milliseconds; however other applications that are less critical may be recovered within a few hours or even days without significant impact to your business operations. Customising your DRaaS solution based on the criticality of each system and application will help devise a financially feasible level of DR and will aid the speed and success of the recovery.****

Data security, data sovereignty and privacy requirement

Data security, sovereignty and privacy are important considerations for any organisation; particularly those in government, finance or healthcare sectors. The ability and experience of your DRaaS provider to deal with the data sovereignty requirements specific to your industry can be critical to some organisations. With enterprises managing data and application complexities across multiple cloud infrastructure platforms, there’s a risk of private or sensitive data being moved and stored offshore in foreign countries. Australian data stored in datacentres overseas will be subject to International laws that are less stringent than the laws at home that safeguard individual and corporate privacy. In order to remain compliant with Australian data sovereignty laws, your organisation needs to address how sensitive information will be maintained and accessed when a DR plan has been activated.

Cloud Flux – today isn’t the same as tomorrow

As more cloud platforms emerge and businesses are storing their critical data in disparate public, private and hybrid cloud environments around the world, the concept of DRaaS is also changing to accommodate the varying, unique needs of organisations to protect, manage and utilise their data across heterogeneous environments and split across several physical sites. Solutions that are available from a cloud environment today, may move to a different platform tomorrow. If you want data from this solution securely replicated as part of your business continuity model, you have to ensure that your DRaaS provider has the ability to provide a technology agnostic, platform agnostic and vendor agnostic solution tailored to meet your stated business continuity objectives.****

Legislation and Regulations

Australian laws and regulations require that organisations enact several forms of security controls including encryption of stored data, logging and monitoring and strong access and data handing controls. These regulations apply regardless of where or how the sensitive information is stored and processed. Legal obligations may also include the need to demonstrate compliance with periodic internal and / or external audits. Not all off-the-shelf DR options will include these capabilities, as some DRaaS service providers may only include these as add-on features at an additional cost. The burden of ensuring that key legal requirements are being met falls largely on individual organisations. In order to mitigate such risks, it is imperative that key issues around data ownership (from a regulatory and contractual perspective), data custodian (the party responsible for protecting data from being compromised), data use and data retention (minimum or maximum periods of time to retain data) are addressed with your DRaaS provider.****

DR test planning

If established DR processes are not tested periodically to ensure that all its components are working as expected, then your organisation only has a DR hope, not a DR Plan. A rigorous and on-going testing schedule is the single most important part of any DR plan. Before the widespread adoption of DRaaS, conducting DR testing was difficult, time consuming, and risky. Although DRaaS enables organisations to automate the management of virtual machines, backups and replication, designing a test plan and conducting the tests until they are satisfactory is not a job for the inexperienced. It is important to tailor your DR test plan because testing as much as you can, as often as you can may not always be technically or financially viable. A custom DR test plan should outline not just how your environment will be tested, the method, scope and frequency of tests, but also the process to rectify non-complaint findings, in order to truly ensure the success of your DR solution. To learn more about DRaaS or help set up a bespoke solution tailored to meet your organisation’s disaster recovery and business continuity objectives, contact the our account team .

How fast was the global DRaaS market expected to grow, ?

According to a report by Transparency Market Research cited in the article, the global Disaster Recovery as a Service (DRaaS) market was anticipated to expand at a 36 percent Compound Annual Growth Rate (CAGR) from 2014 to 2022, rising from a value of USD 621.3 million in 2013.

Why are data security, sovereignty, and privacy concerns raised as a reason to avoid off-the-shelf DR solutions?

as enterprises manage data across multiple cloud platforms, there's a risk that private or sensitive data gets stored offshore, where it becomes subject to less stringent international laws than Australian privacy laws. Organisations must ensure their DR plan addresses how sensitive information will be maintained and accessed to remain compliant with Australian data sovereignty laws, something generic providers may not guarantee.

Why is DR test planning highlighted as a key reason to avoid off-the-shelf DR solutions?

The article argues that without periodic testing of DR processes, an organisation only has a 'DR hope,' not a real DR plan. A custom DR test plan should outline how the environment will be tested, along with the method, scope, and frequency of tests, and the process to rectify non-compliant findings—something a generic off-the-shelf solution is unlikely to provide tailored to the organisation's needs.

Who should organisations contact to set up a bespoke DR solution according to your article?

We advise readers to contact our account team (via the site's contact page) to learn more about DRaaS or to help set up a bespoke solution tailored to their organisation's disaster recovery and business continuity objectives.