

Deploy a private cloud to minimise losses

By [Simon Hwang](#)

12 Apr 2019

The past month has focused the spotlight sharply on the necessity to deal with the real possibility of having a loss of access to one's data. Locally, load shedding challenged business continuity and made prospering in a tough market even more difficult.



Simon Hwang, APAC President at Synology

Globally, the public cloud - namely Gmail and Google Drive - were affected by service disruptions, going down on 13 March 2019 for approximately four hours. Gmail users reported having trouble saving email drafts, sending emails, attaching and accessing attachments, while Google Drive users experienced trouble uploading and downloading files.

The silver lining common to both load shedding and public cloud failure is that these disruptions have brought to light the value of having contingencies in place. Clearly, it's not a smart move to be wholly reliant on a singular power source, or a singular public cloud.

While the former can be addressed with a generator, inverter, or if you have the funds solar power, the latter is answered by deploying a Network Attached Storage (NAS).

These are based on the private cloud architecture and provide file sync services, collaboration suite, corporate communication app, mail services, and high availability services simultaneously, assisting businesses to minimize the risks posed by public cloud services anomalies.

Best practise

If being solely reliant on a public cloud is a bad move, then what should businesses be doing?

The best practice is to back up data stored on the public cloud to a local NAS, in order to protect valuable data such as mails, contacts, calendar, and documents. In the event of a public cloud failure, businesses can still obtain the latest data and provide uninterrupted services to their customers.

This is critical, as prolonged downtime can result in a business losing the trust of its customers, and their continued support to its competitors. Furthermore, having a NAS provides businesses with the benefits of saving data for audits and preventing employees from accidentally or maliciously deleting data.

Admittedly, the threshold of deploying public cloud services may be lower than a private one. However, this is offset by the fact that once the public cloud services are affected by anomalies, the losses caused by services disruption will be considerable. Thus it's strongly suggested that businesses establish a private cloud system in order to ensure maximum service uptime and data autonomy.

Backup benefits

For companies that already use public cloud services, Synology offers Active Backup for Office 365 and Active Backup for G Suite to protect Office 365 and G Suite data, minimising their risk of data becoming corrupted or being lost.

Protecting against public cloud failure is not the only benefit that NAS deployment offers. It also offers peace of mind in the event of a business being attacked by ransomware. Having an additional backup on a local NAS device can mean the difference between having to shell out thousands of Bitcoin to a nefarious attacker, versus simply reinstalling your latest backup onto a clean drive.

While no-one can guarantee that there won't be more instances of public clouds failing or power outages, businesses certainly can prepare themselves for the next occasion, and ensure that the lifeblood of their business, namely data, is secure in every eventuality.

To be frank, even as new technologies come with new risks, there's no excuse for being unprepared. Backing up your SaaS data is not only what businesses should do; it's what they must do. Doing so can ensure that when a disaster strikes, your

business can ride out the storm unscathed.

ABOUT THE AUTHOR

Simon Hwang, APAC President at Synology

For more, visit: <https://www.bizcommunity.com>