DEMANDING TIMES

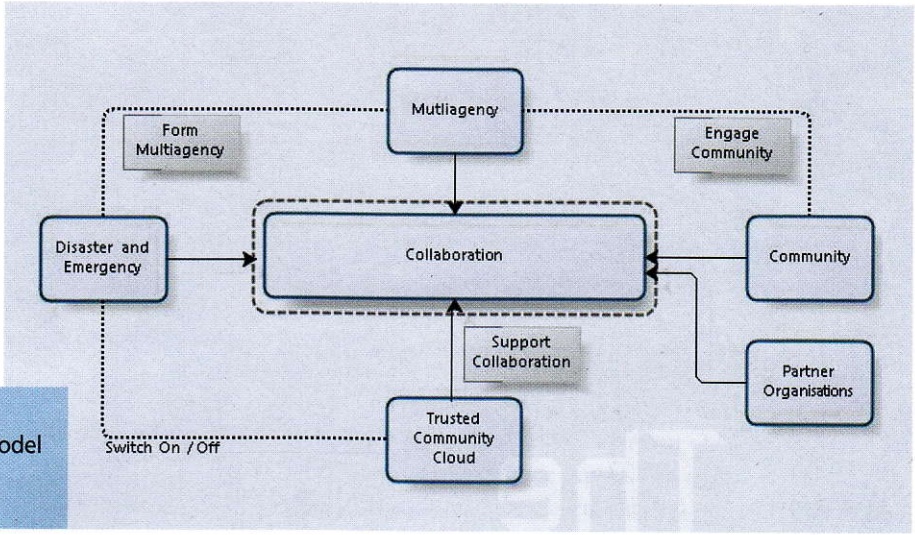
How a trusted community Cloud can aid disaster management

BY DR ASIF Q GILL AND ROB LIVINGSTONE

Information technology has long had an essential role behind-the-scenes in disaster management (DM), providing the necessary support to the emergency services agencies for collaborating, mitigating, preparing, responding to and recovering from natural or man-made disasters. The emergence of on-demand elastic Cloud technology is laying the foundation to upend the conventional approach to DM, which sometimes may fail due to the unpredictable spike in the demand for computing resources. The core benefit of Cloud technology is that it allows the quick and elastic provisioning of computing power, storage, memory, servers and information systems as services during a period of disaster.

Disaster management

The effective management of natural or man-made disasters requires a multi-agency response to co-ordinate volunteers and official response unit activities. Based on the severity and spread of a disaster, a number of volunteers, partner organisations and multiple government emergency services agencies such as medical, police, fire and army may be engaged. DM requires efficient and reliable systems and infrastructure for the sourcing, storage, management and distribution of large amount of real-time data — geo-spatial, for example — which is key to supporting the collaboration and co-ordination activities of different organisational units at different levels.



A trusted community Cloud model

Elastic demand requires an elastic Cloud

You never know when a disaster will strike and what additional computing resources you will need. Traditional silo systems and fixed infrastructure for DM come under pressure where scalable shared computing environment is required to deal with the unpredictable spike for a need in computing resources during a disaster. The recent flooding in 2011 in Thailand increased the unpredictable demand for storage needs, which consequently resulted in the shortage of hard drives. DM systems and infrastructure must have the ability to scale up and scale down to support the dynamic nature of a disaster as it evolves.

Cloud is a pool of shared computing resources that can be provisioned based on the elastic unpredictable demand and, unlike the traditional approach, can be (but not always, depending on the vendor) billed based on actual usage (pay-as-you-use). There are three fundamental Cloud service models — software-as-a service (SaaS), platform-as-a-service (PaaS) and infrastructure-as-a-service (IaaS) — with the option to deploy them in the public off-site, private off-site/on-site, community, and hybrid Cloud environment. Cloud does not require you to bind resources for DM during the non-disaster situation and allows for rapid provisioning and scaling of resources if disaster escalates.

A trusted community Cloud

Despite the current focus on traditional Cloud, there are still security concerns. In order to address the issues associated with Cloud security, a closed-box Cloud execution environment can be helpful for emergency services agencies. A trusted community Cloud environment is a set of shared closed-box computing resources, which can be provided and used by only one or more agencies (for example, government agencies with a shared mission or requirements) for confidentially sharing information and co-ordinating disaster related activities. A trusted community Cloud would allow emergency service agencies to share data centres and Cloud services in order to facilitate inter-agency collaboration and cost sharing during and after disaster and non-disaster circumstances.

A case of on-demand trusted community Cloud model

An individual emergency services agency, such as the police, may work independently by using its individual technology and organisational environment during normal or non-disaster circumstances. It may then switch on its shared trusted community Cloud environment for collaborating and sharing information with other agencies, such as fire, army or medical, as well as community and partner organisations during emergency and disaster circumstances. This is an example of an on-demand trusted community Cloud; once everything goes back to normal, agencies may take their data out of the shared trusted community Cloud and switch off the trusted Cloud when it is not needed.

This would allow emergency services to share cost and benefits of on-demand shared trusted community Cloud service model for collaborative disaster management. Emergency services agencies can work with a common on-demand shared trusted community Cloud infrastructure during a disaster where, and when, necessary. It would ensure emergency services can readily access a trusted community Cloud that is readily scaled and made available when required. They can also keep their own systems that may not support on-demand collaboration during a non-disaster state.

Whether governments have the capabilities to effectively oversee this sort of inter-agency strategic collaboration by the smart design, selection and deployment of appropriate Cloud technologies remains to be seen.

Dr Asif Q Gill is an independent IT analyst, author, speaker and research fellow at the University of Sydney, specialising in strategic business technology innovation, assessment and adoption. He has extensive industry experience across several sectors including manufacturing, automotive, educational services, IT services, financial services and the banking industry. Contact him at ***asif.qumer@sydney.edu.au*** *or* ***asif.gill@aqgill.com****. Rob Livingstone is a regular contributor to* CIO *magazine.*