

CLOUD COMPUTING: WEATHERING THE INCIDENT MANAGEMENT STORM

BY JEREMY ZOLLO & ETHAN BRINKMAN-HANSEN

The National Incident Management System (NIMS) and the National Response Framework (NRF) promote real-time collaboration and information sharing across all phases of incident management – preparedness, mitigation, response, and recovery. These policies endorse proven practices such as the Incident Command System/Unified Command and multi-agency coordination.

The value of these practices are realized as the size and the impact of an incident increases because emergency responders from various agencies, organizations, and geographic locations must coordinate their operations effectively, disseminate information quickly, and distribute resources and assets seamlessly to protect lives and property.

Underlying these operations are IT services, networks, and software applications that enable the extension of services to the incident area, to mission-critical support teams, and to facilities such as emergency operations centers, joint field offices, and incident command posts. While basic connectivity can be established during these multi-agency events, it results in significant



“in-house” infrastructure costs. Additionally, “basic connectivity” may mean responding agencies are left with limited or no access to their enterprise applications (e.g., GIS, asset tracking systems, personnel management, reporting tools, purchasing systems, and financial databases), which are essential to servicing the needs of victims and supporting various agency missions.

Leveraging Cloud Computing in Incident Management

Cloud computing represents the latest trend in application hosting – data and applications are hosted by “cloud providers” on multiple servers in centralized data centers to deliver web-based

applications, application platforms, and services extending IT capabilities. The primary difference between cloud computing and previous models is “scale.” The premise is that as the scale of the cloud infrastructure increases, the incremental time and cost of application delivery decreases.

Cloud computing incorporates concepts such as software as a service (SaaS), distributed computing, and strong network backbones, allowing computers to access and manipulate data anywhere an internet connection is available. If there is a need to scale up to accommodate sudden demand, necessary resources can be added using a web browser. The cloud computing model allows dynamic

and remote control processing, memory, data storage, and network bandwidth, providing the ability to specify and deploy computing capacity on demand.

Enhanced Interagency Coordination During a Disaster: To enhance mission integration among response agencies, cloud technology can serve as a medium to provide real-time, online collaboration and coordination during an incident or event. It provides the ability to stand up your applications faster, cheaper and enables you to bring the cloud down once the incident has subsided. All stakeholders in the incident can share resources and operate in a multi-tenancy environment that fosters information sharing. And because the cloud solution is a shared online resource, mission-critical information, IT support, and situational awareness outside of an incident area can be easily communicated, regardless of location. Users with similar needs can access the same type of services and capabilities provided by their own agency infrastructure in a disaster area. These capabilities can be used on demand, in real time based on either a fixed fee subscription or pay-as-you-go (i.e., paying for the service and data space used).

Reduces Operations and Maintenance (O&M) and IT Infrastructure Costs: Agencies involved in disaster response have heavily invested in enterprise IT infrastructure equipment that is either under-utilized or running at over capacity. Maintaining this equipment requires continual hardware and software upgrades to keep up with today's technology and increased security requirements. Cloud computing reduces major hardware costs—service providers maintain the infrastructure, and users subscribe to the service as needed.

Software services can also be centralized within the cloud rather than loading and maintaining software on each individual end user's equipment (e.g., laptop, servers). By outsourcing IT infrastructure processing power, agencies can scale their enterprise IT infrastructure when needed for emergency response situations and access just in time processing. This eliminates the need to invest major capital in expensive back-end infrastructure that is not used

on a daily basis. IT personnel costs can also be reduced because the ability to maintain and manage IT infrastructure during an incident will be the primary responsibility of the cloud provider.

Efficient and Flexible IT Backbone: The dynamic nature of disaster response requires tools that can be as flexible as emergency responders in a disaster area. Because cloud service providers maintain IT infrastructure in their own data centers, agencies have increased mobility because they are not burdened by delivering and establishing their own traditional IT infrastructure during a disaster. They benefit from user scalability, high availability, and accessibility to resources. With access to the cloud anywhere there is internet connectivity, emergency responders can provide support to on-site incident responders without having to be physically located within the incident area.

Considerations for Cloud Computing Implementation

While cloud computing is a powerful tool for the incident response community, there are still serious challenges such as maintaining reliable connectivity, developing standardization, and addressing security concerns. These issues require further study and piloting to ensure the technology's success in the incident response environment.

The potential exists for cloud service providers to encounter lapses in service due to unplanned outages or disrupted Internet connectivity. Also, the cloud is only as reliable as the network it is riding on. If agency network bandwidth is limited then the cloud experience will be limited as well. Cloud service providers must establish failover solutions to ensure reliability of the cloud and establish service level agreements (SLA) with agencies that describe the technology and service requirements under normal operation and downtime situations.

Cloud computing is not a standardized technology. Agencies using individual clouds run the risk of incompatibility if clouds from other service providers are used by agencies during a disaster response. Standardization of cloud computing for incident response agencies will enable them to use cloud services

from any provider that meets their incident requirements. Development of policies and governance for cloud computing will be a critical factor for the government to embrace the concept.

Maintaining data security using an external IT service provider requires extensive planning and development of security protocols. Cloud service providers will need to receive certification and accreditation (C&A) similar to other secure communications systems to ensure the integrity and security of data are maintained. Government agencies may also need to change C&A processes to account for the cloud computing model. Additionally, service providers will need to ensure that personnel meet the necessary security requirements. SLAs need to be developed that not only address performance, but also data security (e.g., encryption, data center locations, secure personnel). Moreover, agencies using cloud computing services will need to work with cloud service providers to determine who has access to the data in the cloud, where the data is located, and the types of encryption schemes and security offerings that best suit their needs. Possible security threats must be carefully examined to ensure all aspects of the cloud are properly encrypted to protect all sensitive information flowing into and out of the cloud.

ABOUT THE AUTHORS

Jeremy Zollo (zollo_jeremy@bah.com) is an Associate with Booz Allen Hamilton based in Mclean VA and has over 15 years experience in the analysis, design, implementation and management of emergency communications systems and IT projects for all levels of government. He currently serves as the Program Manager overseeing FEMA's Disaster Emergency Communications (DEC) Program.

Ethan Brinkman-Hansen (brinkman-hansen_ethan@bah.com) is a Senior Consultant with Booz Allen Hamilton based in Mclean VA and a firefighter. He specializes in emergency communications and response operations for all levels of government. He currently leads emergency communications planning efforts within FEMA's DEC program.

VISIT THE ONLINE GUIDE AT
www.disaster-resource.com