

Architecture Framework Advisory Committee (AFAC) Enabling Application Containerization

Discussion Summary

April 8, 2019 (13:00 to 16:00 EDT)

Event purpose statement

The Government of Canada (GC) is championing the development and implementation of Application Containerization; however, it also recognizes the need to transform GC architecture to support this new reality, manage its downstream effects, and support new services for Canadians.

Highlights

Containers are a key enabler to application workload automation. Container-enabled automation can bring agility, speed and stability to an organizations application provisioning development processes. In some instances, organizations saw; a significant reduction in both, their average application provisioning timelines (90days to 15 days), and in their Mean Time To Respond (MTTR).

Containers and their automation allow for infrastructure as code to be standardized often resulting in a shift between the developer and operator roles.

Blended support models, where some organisations are responsible for infrastructure services and others for application development are common within industry. The re-definition of traditional roles and responsibilities with the support of good governance have proven to be instrumental in easing challenges brought on by the advent container technologies and supporting methodologies such as DevOps, Continuous Integration and microservices.

Key Considerations

The culture and process change that is required to fully benefit from a container enabled environment needs to come from the business. It is recommended that an organisation's approach to enabling container-use be iterative and avoid the common mistake of "big bet". It is recommended to start small, look for quick wins and areas of risk that can be brought down early, and continuously, through rapid experimentation and proof of concepts.

Investment in workforce training and skills development along with the adoption of a "centre of excellence" type approach is strongly encouraged as a means to better support organizational adoption and ease business disruptions.

The advent of containers present a change to the existing IT security paradigm. Security is no longer mainly an IT infrastructure consideration and consequently, traditional roles and responsibilities surrounding security will need to shift. Innovative concepts and tools such as zero trust networking and automated security solutions amongst others are being looked at as a means to address evolving security concerns.

Containers are not a one size fits all solution. Compatibility with some Commercial Off The Shelf (COTS) products remains lacking and the cost/ benefit/ impact of transforming some particular workloads can be prohibitive and present little value.

The GC should recognize that this transformation is an iterative approach and that there is no end state architecture. The idea is to build a system with the intention to evolve. Consistent, incremental change should be the technical goal. Furthermore, the GC could benefit from leveraging an open source/ inner source model (E.g. make everything visible such as code, issues, fixes, releases) and empower departments to implement features themselves.

