



# INNOVATION CELL

LEVERAGING OUR NATION'S INNOVATORS

## INITIAL ENTERPRISE CHALLENGE: MULTI-CLOUD ORCHESTRATION

CHALLENGE ISSUED:  
04.20.2016

POC: TIM MARTIN, INNOVATION CELL ASSESSMENT LEAD





## **INITIAL ENTERPRISE CHALLENGE: MULTI-CLOUD ORCHESTRATION**

### **DESCRIPTION OF NEED/PROBLEM**

The Naval Enterprise Network (NEN) and the Navy needs an automated tool set to provide fully integrated multi-cloud analysis and orchestration. Cloud orchestration scope for NEN will include external Cloud Service Providers (CSP), on premise managed cloud services, and on premise virtual and physical infrastructure. The need exists to investigate and identify a single orchestration toolset to prevent cloud vendor lock-in (i.e. vendor or technology dependency) and enable service automation orchestration while evaluating the potential security, risk, cost, and functional benefits.

### **IDENTIFIED REQUIREMENTS**

**Automated analysis of targeted workloads (deployment of workload analysis tool, functional modeling against workloads, cost modeling using multiple CSPs)**

- Deployment of client based or clientless workload modeling capability
- Automated report/output of workload requirements
- Automated import of current CSP published cost rates
- Automated import of manually provided CSP rates (discounted rates, on premise cloud service rates, Defense Information Systems Agency (DISA) rates, Data Center Application Optimization (DCAO) rates, etc.)
- Automated modeling of workload against available rates per provider



- Automated simultaneous modeling of performance against provider prices (trade-off price vs performance)

**Seamless integration with CSPs and other commercial virtualization front-ends**

**Single pane of glass for automation, orchestration and workload management across multiple CSPs (prevent the need for support staff to specialize in particular CSP front-end)**

**Automated/semi-automated creation and movements of workloads**

- Support physical workload image creation (lift and shift physical to virtual)
- Support virtual workload image creation (lift and shift virtual to virtual)
- Ability to enable full workload implementation (single click DevOps)
- Ability to select components of workload (select components for DevOps)
- Support customizable service library with selectable components & configurations
- Ability to support templates of predefined components
- Automated ability to spin up new resource based on utilization (automated burst, scale-out, scale-up, scale-back)
- Automated workload move from physical infrastructure to CSP Cloud services
- Automated seamless workload move from one CSP to another without reimaging (no cloud vendor lock-in)
- Automated multi-CSP orchestration management (example, data on one location/CSP and processing in another)
- Ability to separate and move applications, components, and data to or from any environment

**Capability to support Continuity of Operations Plan (COOP)/Disaster Recovery (DR)**

- Ability to define automated response thresholds and objectives for automation responses
- Automated workload duplication across CSPs to support redundancy
- Automated ability to move/increase workload on one CSP when another is unavailable
- Automated ability to burst/failover to virtual based on predefined physical workload performance parameters
- Use of automation rule sets to execute automated COOP based on predefined COOP scenarios

**Automated spending controls and notifications**

- Predefine spending limits by workload
- Automate spending threshold notifications
- Automated real-time spend monitoring
- Support multi-tenant/layered spending controls



### **Additional technical requirements**

- Support Role Based Access Control (ability to control user capabilities based on individual or Administrative Domain (AD) group)
- Admin and/or end user self-service portal
- Compliance with all applicable DOD and DON security requirements (e.g. DISA Security Technical Implementation Guidelines, Information Assurance Vulnerability Management)
- Support AES 256 encryption at rest and in transit
- Support PKI based user authentication
- FIPS compliant

### **USE CASES**

- Administrator movement of physical application workload and related data to a CSP
- Administrator workload movement of data alone to a CSP
- Administrator movement of physical application workload and related data spanning multiple CSPs
- Administrator workload movement of data alone spanning multiple CSPs
- Administrator development of default failover/DR/COOP policies for a workload across physical, virtual, internal cloud, and external CSP services
- Administrator performing initial cost/performance analysis against workload prior to orchestration
- Administrator performing cost/performance analysis against a workload already being orchestrated
- Administrators developing/maintaining baseline configurations on individual servers/workloads/devices/etc. (component library)
- Administrator developing/maintaining baseline configurations of full workload templates
- Non-Administrator customer access and execution of workload templates for DEV/TEST environment
- Non-Administrator customer adding baseline servers/workloads/devices to a DEV/TEST environment
- Administrator configuring performance/cost thresholds
- Non-administrator customer updating performance/cost thresholds for their workload
- Enterprise level cost and usage monitoring
- Customer pass-through of cost and usage monitoring to customers for their workload by workload
- Customer pass-through of cost and usage monitoring to customers for their workload by workload by organization



- HA/DR/COOP planning
- HA/DR/COOP test execution of COOP plans

## **POLICY**

There is no policy related specifically to cloud or Multi-Cloud Orchestration. Multi-Cloud orchestration significantly reduces human resource interaction with cloud orchestration, and enables higher levels of service at lower costs. Multi-Cloud Orchestration supports, to a great extent, policy requirements for cost reduction, High Availability, Disaster Recovery, and Continuity of Operations.

## **REFERENCES**

- TBD

## **SPECIAL RESPONSE INSTRUCTIONS**

In responding to this EC, at a minimum, please address the items listed below:

1. Please provide a solution architecture diagram and a descriptive overview of a possible solution that addresses the needs outlined in this Enterprise Challenge.
2. Describe how this solution's capabilities align with the identified requirements.
3. Describe this solution's capability to natively support private and public cloud infrastructures and provide automated integration with Cloud Service Providers.
4. Please describe any product capabilities that may be considered distinguishing factors (product differentiators).
5. Identify solution's system and software requirements.
6. Describe the solution's software licensing model (per server, per workload, per CPU, per capacity utilization, etc.).
7. If this solution has been deployed previously, please provide example customers to include any Federal Government or DOD customers.

### **TO RESPOND TO THIS ENTERPRISE CHALLENGE**

1. Download the **"Respond to an Enterprise Challenge" pdf form**, available on the Innovation Cell website
2. Complete the form then submit it via email to **PEOEISInnovationCell@navy.mil**