Going DevOps in GovCloud
Trials and Travails

John Mallinger
Brian Davenport
GovCloud 101 – Status and Capabilities

• Commercial Clouds provide regions for Government and DoD Users

• DoD Cloud Computing Security Resource Guide:
  • Impact Level (IL) 1: Public Release
  • Impact Level (IL) 2: Non-Controlled Unclassified Information
  • Impact Level IL) 3: No longer used
  • Impact Level (IL) 4: Controlled Unclassified Information – including export controlled, personally identifiable information, or protected health information
  • Impact Level (IL) 5: Controlled Unclassified Information that requires higher level of protection – including National Security Systems (NSS)
  • Impact Level (IL) 6: Classified information up to Secret

• DoD and Federal Cloud options (Examples):
  • AWS GovCloud: IL5
  • Microsoft Azure – DoD Government Region: Provisional IL5
  • IBM SmartCloud: IL5
  • Oracle Federal Managed Cloud Services: IL5
  • MilCloud 2.0 (DISA): Provisional IL5
  • AWS Secret Region: Provisional IL6

Approved for Public Release
GovCloud for Scalable DevOps

• Cloud Deploy Trades:
  • All Development or I&T Environments only
  • Operational Deployment in a cloud
  • SaaS, IaaS, or PaaS

• Strategies:
  • Local Data Center – all development and checkout on-premises
  • Cloud Development – users remotely connect to cloud for development and I&T DevOps pipelines
  • Hybrid Development
    • Software Development and Build / Unit Test in data center
    • Scalable software integration environment in cloud

Approved for Public Release
Hybrid Development Summary

• Build and Checkout pipeline runs on developer change commit
  • Development, Build, and Unit Test occur in local environment
  • Deploy and Checkout into software integration sandbox within GovCloud
• GovCloud provides massive on-demand scalability for software integration
  • Instantiate 50+ node environment for each build delivery to run automated checkout
  • Tear down environment after checkout is complete (1 – 4 hours)
  • Massive parallel pipeline – up to 50x environments can run, limited only by licensing
Network Architecture

Cisco Cloud Services
Router

Local Build Environment

WAN Link to AWS

NAT and Port Translation

Cisco Cloud Services Router

VPC-1

Cisco Cloud Services Router

VPC-N

Approved for Public Release
Physical Architecture

**Core Infrastructure:**
- Directory Services
- DNS
- Shared Storage
- Load Balancer
- Deploy Automation

**Middleware:**
- Application Servers
- Enterprise Service Bus
- Databases

**Mission Software:**
- Server Applications
- User Interfaces

**Embedded Test:**
- Test Workstations
- Test Automation
- Test Drivers

**Virtual Servers & Virtual Workstations**

**Approved for Public Release**
Designing for GovCloud

• Design for virtualization
  • Drives both cost savings and improved performance
  • Utilize larger number of VMs with smaller CPU and memory allocations

• Dynamic management of footprint based on utilization
  • Define core footprint and assess scalability needs and strategy
  • Reserved vs. On-Demand allocations of nodes

• Leverage Cloud-Specific Infrastructure and Design
  • Load balancers, storage arrays, and networks are all very different in the cloud

• Configuration Management in the Cloud
  • Managing and purging AMIs and DevOps Pipeline builds and results
Going from GovCloud back to Data Centers

• AWS simplifies deploys – and can push integration challenges downstream

• Things that broke back in the data center:
  • Hardware Driver – Operating System compatibility issues
  • Network port bonding configuration
  • Fiber NIC card-switch compatibility

• AWS also abstracts virtualization setup and configuration
  • Virtualization software drives specific scripting and configuration – not universally portable
  • VMWare setup and provisioning drove additional develop and integration
  • Can convert VMs to AMIs and back – not always easy or fast

Approved for Public Release
Lessons Learned

• Legacy Physical Architecture not optimized for virtualization
  • Virtual machine performance optimized with increased count of smaller VMs

• Network performance paces cloud usage
  • WAN connection design drives data transfer and latency
  • WAN outages can stop all program development – design for redundant connections

• The cloud is different than physical compute infrastructure in data centers
  • Legacy designs need to change and adapt to the cloud
  • A fully integrated cloud deploy doesn’t translate to working data center deploy

• Deploy operational systems to the cloud wherever possible
  • If you can do so, this really simplifies migration from development to production
  • Streamlined cloud deploys allow updates in minutes or even seconds