Shared Services Canada (SSC)

Cloud Computing: Outstanding Challenges

Architecture Framework Advisory Committee

Transformation, Service Strategy and Design

July 16, 2013
<table>
<thead>
<tr>
<th>TIME</th>
<th>TOPICS</th>
<th>PRESENTERS</th>
</tr>
</thead>
<tbody>
<tr>
<td>9:00 – 9:10</td>
<td>Opening Remarks, Objectives &amp; June Meeting Review</td>
<td>B. Long, Chair, W. Daley, Vice-Chair</td>
</tr>
<tr>
<td>9:10 – 9:15</td>
<td>Cloud Computing: Recap from Feb AFAC meeting</td>
<td>Chairs</td>
</tr>
<tr>
<td>9:40 – 10:20</td>
<td>Round Table</td>
<td>All</td>
</tr>
<tr>
<td>10:20 – 10:30</td>
<td>Health Break</td>
<td></td>
</tr>
<tr>
<td>10:30 – 11:00</td>
<td>Cloud Computing Service Architecture</td>
<td>P. Littlefield</td>
</tr>
<tr>
<td>11:00 – 11:45</td>
<td>Round Table</td>
<td>All</td>
</tr>
<tr>
<td>11:45 – 12:00</td>
<td>Closing Remarks</td>
<td>Chair</td>
</tr>
</tbody>
</table>
Cloud Computing

Recap from Feb AFAC
Source: NIST
ENTERPRISE SECURITY

- All departments share one operational zone
- Domains and zones where required
- Classified information below Top Secret
- Balance security and consolidation
- Consolidated, controlled, secure perimeters
- Certified and accredited infrastructure

SERVICE MANAGEMENT

- ITIL/ITSM framework
- Standardized service levels/availability levels
- Inclusive of scientific and special purpose computing
- Standardized application and infrastructure lifecycle management
- Smart evergreening
- Full redundancy – within data centres, between pairs, across sites

CONSOLIDATION PRINCIPLES

1. As few data centres as possible
2. Locations determined objectively for the LT
3. Several levels of resiliency and availability (establish in pairs)
4. Scalable and flexible infrastructure
5. Infrastructure transformed; not “fork-lifted” from old to new
6. Separate application development environment
7. Standard platforms which meet common requirements (no re-architecting of applications)
8. Build in security from the beginning

BUSINESS INTENT

- Business to Government
- Government to Government
- Citizens to Government
GC Community Cloud
• Internal services for GC community
• SSC-provided cloud services to the GC
• Secured perimeter
• Multi-Domain (Protected-B to Secret)

GC Hybrid Cloud
• Secured extension of GCnet to vendor
• Vendor-provided cloud services to the GC

GC Public Cloud
• Some public-facing GC presence
• Limited development/test capacity
CHALLENGE: Managing identity, federation, and access control

DESCRIPTION:
• Transformation, migration to Role-Based Access Control (RBAC) and the ICAM strategy

MITIGATIONS:
• ICAM implementation schedule
• GC-wide directory strategy & architecture
• Migration from departmental based security to role-based access control

FORWARD AGENDA ITEMS:
• ICAM architecture & standards
• GC Directory architecture & standards

Note: Where we left off in Feb 2013
Cloud Computing

ICAM Service Architecture
Topic Objectives

• Describe scope, vision and goals
• Present a high-level strategic plan for GC ICAM
• Seek feedback and input
• Questions/discussion
What is Identity, Credential, and Access Management (ICAM)?

ICAM represents the **intersection of digital identities** (and associated attributes), **credentials**, and **access control** into one comprehensive approach. The following figure illustrates the core components of ICAM:

**Key ICAM Service Areas:**
- Identity Management
- Credential Management
- Access Control Management (Physical, Logical)
- Monitoring, Auditing & Reporting
- Identity Broker
IT Service Elements & Cyber & IT Security

SSC

Distributed Computing
- Email
- Labelling
- Calendar
- Mobile Device Management
- Email-Fax Integration
- Directory

Data Centre
- OS
- ITSM Tools
- System Management
- Storage
- Floor Space
- Cooling
- Power

Networks
- Voice Conference
- Video Conference
- Intra-Bldg Connectivity
- Inter-Bldg Connectivity
- Intra-DC Connectivity
- Inter-DC Connectivity

External Services

IT Security
- SOC/SIEM
- ICAM
- Anti-virus Anti-spam
- HIP
- SRA
- IDS/IPS
- Perimeter Security
- Crypto/VPN

GC Partners

Partner Specific
- Application Security
- Data Security
- WTS Security

Partner Specific

Partner Specific

Web/Portals
- Search
- Doc/Record Management

DBMS
- Enterprise Svc Bus

WTS

Application Security

Data Security

WTS Security

Intra-Bldg Connectivity

Inter-Bldg Connectivity

Intra-DC Connectivity

Inter-DC Connectivity

Voice Conference

Video Conference

ICAM
## ICAM Drivers and Risks

<table>
<thead>
<tr>
<th>DRIVERS</th>
<th>RISKS</th>
<th>CHALLENGES</th>
</tr>
</thead>
</table>
| Increase Security | • Emerging internal and external threats  
• GC dependency on IT to fulfill program & citizens’ requirements  
• Limited GC policy and standards enforcement capability  
• Silo security solutions | • Moving to a single domain  
• Transition from silo ICAM solutions to enterprise service  
• Transformation into a service culture (people, process and technology)  
• Shared risk in the context of ICAM since departments and SSC both have responsibility | |
| Improve Service | • High pace of transformation within GC  
• User expectation for anywhere, anytime services  
• GC partner expectation and relationship | • IM challenges: data tagging and retention during transitions and ensuring standardised implementation of IM policies across GC departments/agencies | |
| Generate Savings | • Duplication and fragmented technologies and processes | |
Bringing it all together - Internal

SSC employees & contractors with

myKEY

✓ GC-SRA

✓ GC-WiFi

GC-LAN

GCnet Unified Authentication

GC Cloud Computing

CWA

B2B

ILMS

GEDS

STSI

Desktop
GC ICAM High-Level View

**Identity Management**
- Background investigation
- On-boarding
- Authoritative attributes
- Lifecycle management of identity and attributes

**Credential Management**
- Sponsorship
- Enrolment
- Creation of credentials at multiple levels of assurance
- Issuance
- Lifecycle management of credentials

**Access Management**
- Resource Management
- Privilege Management
- Policy Management
- Logical Access
- Physical Access

**Trusted Access:** “One you, one identity, one card, few credentials” GC ICAM Vision
‘As-Is’ vs. ‘To-Be’

**TODAY**

- Fragmented ICAM
- Departmental Efficiency
  - Department/Program Specific
  - Application Driven
  - Non-Standards Based
  - Ad-hoc Security
  - Fragmented Service Management

**FUTURE**

- GC Enterprise ICAM
- Enterprise Efficiency
  - GC Enterprise
  - User-Centric/Service-Driven
  - Standards Based
  - Holistic Security
  - Unified Service Management

**Major Transition Streams**

Policies

Process

Governance

Technology
* Worker is a generic term used to describe a uniquely identifiable person (e.g. employee, consultant, interchange) within the GC.
ICAM Current State Examples

<table>
<thead>
<tr>
<th>ICAM Service Area</th>
<th>Enterprise Service</th>
<th>Dept. Specific Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity Management</td>
<td>Pay System (PayMod)</td>
<td>Many</td>
</tr>
<tr>
<td>Credential Management</td>
<td>GC-ICMS &amp; Cyber Authentication</td>
<td>Few</td>
</tr>
<tr>
<td>Access Management</td>
<td>GC-SRA</td>
<td>Many</td>
</tr>
<tr>
<td>Directory Services</td>
<td></td>
<td>Many</td>
</tr>
<tr>
<td>Security Policy Management</td>
<td></td>
<td>Many</td>
</tr>
<tr>
<td>Cryptography</td>
<td></td>
<td>Few</td>
</tr>
<tr>
<td>Audit &amp; Reporting</td>
<td></td>
<td>Many</td>
</tr>
<tr>
<td>Others</td>
<td></td>
<td>Many</td>
</tr>
</tbody>
</table>
ICAM Services in the Government of Canada

**Entities**
- **Persons**
  - GC Worker
- **Non-persons**
  - device
  - application

**GC ICAM Services**
- **Identity Management**
- **Credential Management**
- **Access Control Management**
  - Physical Access
  - Logical Access
- **Identity Broker**

**Monitoring, Auditing and Reporting**

*Worker is a generic term used to describe a uniquely identifiable person (e.g. employee, consultant, interchange) within the GC.*
* Worker is a generic term used to describe a uniquely identifiable person (e.g. employee, consultant, interchange) within the GC.
ICAM Program: Major Stages

**STAGES**

**COMMON IDENTITY**
- GC Enterprise Identity Management Service
- Increased trust in identity
- Better security posture
- GC common identity attributes

**OUTCOMES**

**DECOUPLING CREDENTIAL**
- Standardised credential services options
- Reduced credential service coupled in application layer
- Guideline for application owners to use the service

**LEVERAGE ACCESS MANAGEMENT**
- Standardise physical access services
- Improve and augment use of identity and credential for logical access management
- Data tagging
- Business access logic and services automated
ICAM Transformation Strategy

Program continuous improvement towards maturity

Release 1:
- Common Identity
- Decoupling Credential
- Access Management
- Policies
- Process
- Governance
- Technology

Release 2:
- Common Identity
- Decoupling Credential
- Access Management
- Policies
- Process
- Governance
- Technology

Release 3:
- Common Identity
- Decoupling Credential
- Access Management
- Policies
- Process
- Governance
- Technology

Maturity Model

Time
## ICAM Program: Basics

<table>
<thead>
<tr>
<th>Specific Areas of Focus</th>
<th>What we think we know...</th>
<th>Others...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Architecture</td>
<td>• Multiple levels, PKI, other</td>
<td>• Are there other architectures that we should consider?</td>
</tr>
<tr>
<td></td>
<td>• Federated, centralized, hybrid</td>
<td></td>
</tr>
<tr>
<td>Policy, Process and Frameworks</td>
<td>• GC Policy Suite (examples)</td>
<td>• Are there other implications that we need to consider?</td>
</tr>
<tr>
<td></td>
<td>• Process (HR, clearance etc..)</td>
<td></td>
</tr>
<tr>
<td>Standards</td>
<td>• PIV, SAML?</td>
<td>• Are there other emerging standards that we should consider?</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security</td>
<td>• ITSG-33, RBAC, ABAC</td>
<td>• Any other security requirements that we should consider?</td>
</tr>
<tr>
<td>Directory Architecture</td>
<td>• AD Centric, LDAP, Open</td>
<td>• Anything else that we should consider?</td>
</tr>
<tr>
<td>Getting to next level</td>
<td>• Detailed component service architectures</td>
<td>• Any other considerations?</td>
</tr>
<tr>
<td></td>
<td>• Agreement on ICAM processes</td>
<td></td>
</tr>
<tr>
<td>Next Steps</td>
<td>• Governance structure</td>
<td>• Other next steps?</td>
</tr>
</tbody>
</table>
Questions - Engaging Discussion

• How can open standards contribute to a long term sustainable service?

• In the context of existing GC strategies and priorities, what model would be the most suitable and why (federated versus non-federated model)?

• How cost efficiency can be met with departmental variety of requirements (e.g. credential on hard token versus soft token)?

• While working with/from multiple authoritative sources, what are the challenges we will be facing on standardisation, data integrity, data standard?

• Based on industry experience:
  – How would you compare the level of complexity for the technology aspect versus the business aspect (e.g. policy/process)?
  – What has been the successes or failure related to directory services using any of Active Directory and LDAP (or others)?
  – Is anyone aware of an existing modern enterprise use case model & framework?
Health Break
**CHALLENGE:** Connecting resources across clouds & customer premises

**DESCRIPTION:**
- People, process & technology required for multi-CSP, internal IT service management (ITSM) orchestration

**FORWARD AGENDA ITEMS:**
- CSB architecture & standards
- Internal ITSM architecture & standards

**MITIGATIONS:**
- Cloud service broker architecture/standards
- Internal ITIL/ITSM architecture/standards
- GC Identity, Credential, Access Management (ICAM)
- Security & privacy controls

*Note:* Where we left off in Feb 2013
Cloud Computing

Service Architecture
SSC Data Centre & Infrastructure Challenges

• Defining a **practical service catalogue** covering SSC’s core data centre mandate

• Developing a **realistic set of achievable milestones** within an evolving maturity model

• Arriving at a **set of building blocks** upon which to build out the desired IaaS and PaaS capabilities

• **Leveraging industry** in the most efficient and focused manner

• Developing a **set of frameworks and standards** to support workload mobility within and across public and private clouds

The GC is mandated to foster an open and competitive landscape for infrastructure assets and services
Closed Private Cloud Approaches: *The Problem Statement*

- Concerns with current infrastructure solutions:
  - OEM-sponsored
  - Tight cross-component integration
  - Workload mobility outside the framework… support concerns
  - Limited substitutability and choice
  - Limits healthy competition

Tightly integrated vertical stacks for private clouds…

Limit flexibility, choice, and competitiveness…

Have lingering concerns of long-term viability.

*Will these directions negate the benefits of cloud and bring us back to proprietary lock-ins?*
Problem Statement:
Multiple independent proprietary technology stacks

Many available offerings, which supplier?

Converged Infrastructure (definition)
First Generation Private Cloud Efforts

Evolutionary Progress

Automation & Efficiency → Only partially addressed

1. Server Virtualization
   - How to efficiently provision new VMs?
   - How to move workloads between clouds?

Service Providers

2. Cloud Data Centres
   - How to accommodate multiple hardware suppliers?

Users

3. Cloud Federation
   - How to leverage and integrate with public clouds?

Admins

It is not just about virtualization. SSC has begun the journey but early in evolution...
The Advent of an Open Source Cloud Operating System

- Meets SSC workload mobility business requirements
  - Within and across our SSC data centres
  - From GC private cloud data centres to public cloud data centres
  - From the public cloud back to our private cloud
- The GC cannot commit everything to one vendor strategy
- There is only one way to accomplish this: through endorsed open standards
- Is it inevitable that public and private clouds…

... will be built on an Open Cloud Operating System?
Outcomes if SSC doesn’t adopt & standardize on a framework

- Disjoint IaaS technology stacks
- Redundant investment in element managers
- Multiple independent technology pillars each with their own lock-in constraints
- Increased training costs
- Inconsistent service levels due to unbalanced skills and expertise across the stovepipes
- Reduced agility
- More procurement constraints and contract confusion
- Lack of a clear cohesive vision to our partner departments/agencies and vendor ecosystem

- The case for change
CI & Discrete Infrastructure under an “Open Framework”

**Enterprise Systems Management**
(including ITSM, ITIL, eTOM services)

**Open Cloud Operating System**
(Provisioning, Deployment, Configuration)

- Standard API-compliant features & extensions
- Component Managers (Crowbar, Puppet, JuJu, Chef, Fuel)

**Converged Infrastructure**
- Compute Resources (Racks & Blades)
- Network Components
- Storage Components

- Open Cloud Operating System
- Common ESM Platform(s)
- Common Provisioning Platform
- CI infrastructure supported
- Non-CI based infrastructure also supported
• Mandate a “Cloud Operating System”
• Mandate support for multiple “hypervisors” running in the compute nodes
• Mandate that VMs must be provisioned from the “Cloud Operating System” including
  – Compute nodes
  – *Network switches and addressing*
  – *Storage*
• Mandate that VM images come from an image catalogue
• Mandate that “bare metal” deployments must be supported
• Mandate that the ecosystem of support components and tools be Open Architecture compliant
  – All domain components must work within the Open Architecture API framework

• Describe desired capabilities of an Enterprise Systems Management (ESM) solution, including the affected areas within the ITSM and ITIL disciplines

• Specify that the ESM capability must provide support and integration with both:
  – The converged infrastructure components i.e. the light blue boxes
  – The discrete components i.e. the red, green, and brown boxes

• Disallow any domain-specific or component-specific proprietary element managers
PaaS Platform Deployment within the IaaS Framework

Pre-configured, pre-integrated and lifecycle-managed infrastructure and platforms (IaaS and PaaS)

Enterprise Management
(Enterprise Architecture, Service Management, Design & Orchestration, Vendor Relationship Management, Partner/Client Relationship)

Self Service Catalogue/Portal

Enterprise Service Management, Capacity Management

Standard Platforms
(ERP, DBMS, Web, App, File, Print, VDI, DW)

Windows Standard
Windows HA
Linux Standard
Linux HA

Standards-based Open Cloud Framework

Virtual Compute (Hypervisor)

x86 Servers
Storage

Retained or Supplier Processes (TBD)
• Solutions provisioning
• Applications interoperability

Supplier Processes
• Lifecycle management
• Capacity management
• Incident management
• Asset management
• Helpdesk support

ecoSystem Supplier Processes
• Supplier diversity for on-going best value
• Workload portability through open standards

Retained GC Functions
Alternative IT Infrastructure Service Delivery Opportunities
Questions for AFAC Members

• Do you believe that SSC should adopt a framework such as OpenStack as an underlying strategy for internal workloads?

• Are there any other realistic non-proprietary alternatives?

• How committed do you believe service providers and OEMs are to OpenStack?
  – Are they modeling their cloud framework around OpenStack?
  – Are they incorporating OpenStack support in their cloud products and service offerings?

• Are system integrators able to provide support to OpenStack-centric projects?

• Are there criteria for workloads that would allow SSC to ease into OpenStack adoption in a measured and phased way?

• Do you believe that SSC should mandate OpenStack support in its tendering processes? Where, when, and to what degree?

• Do you have any feedback on the related role of ESM in an OpenStack context? How much emphasis should be placed on ESM integration?
Next Steps - Roundtable

• Member Feedback

• Next Meeting – Agenda
  – ICAM conclusion
  – Cloud Computing Service Architecture conclusion
  – Directory Services introduction
Additional Material
OpenStack – A Realistic Alternative?
Why OpenStack?

• **Control and Flexibility.** Open source platform means **never** being locked to a proprietary vendor, and modular design can integrate with legacy or third-party technologies to meet enterprise business needs.

• **Industry Standard.** More than 60 leading companies from over a dozen countries are participating in OpenStack, including IBM, Cisco, Citrix, Dell, HP, Intel and Microsoft, and new OpenStack clouds are coming online across the globe.

• **Proven Software.** Run the same software that today powers some of the largest public and private clouds in the world.

• **Compatible and Connected.** Compatibility with public OpenStack clouds means enterprises are prepared for the future—making it easy to migrate data and applications to public clouds when conditions are right—based on security policies, economics, and other key business criteria.
Popular OpenStack Use Cases

- Commercial service providers offering an IaaS compute platform
- Internal IT service provider organizations provisioning compute resources to partner subscribers
- Rapid deployment of Dev/Test environments
- Processing of big data applications
  - Document libraries
  - Archiving systems
  - Personal cloud storage systems e.g. Box.net, Dropbox
- Hosting of conventional multi-tiered Web applications
- Scaling compute up and down to meet demand for Web resources and applications
- Taking IT infrastructure challenges out of the equation for business owners
OpenStack Value Proposition

- Addresses real cloud provider concerns
  - Increases ability to control TCO
  - Limits both vendor and provider lock-in
  - Allows for massive scalability
  - Offers support for multiple hypervisors (KVM, Xen, VMware, Hyper-V, etc.)
  - Based on an open extensible framework for:
    - Execution components
    - Management components
  - Leverages standardized APIs enabling a rich cloud ecosystem

- OpenStack’s cloud operating system is commoditizing the IaaS market from provider-specific approaches to a single open and vibrant ecosystem of contributors.
High Level Strategy

Portal & Self Service Catalogue
(SSC Intellectual Property)

Pure Play Multi-Cloud Management Services
(Orchestration, Governance, Financial Control, Brokering, ICAM, Reporting)

Hybrid Cloud Services

Public Cloud Services
IaaS
PaaS
SaaS

GC Community Cloud Services

- Application mobility
- Deployment agility
- Open
- On-going competition
- Low/no entrance barriers

Current Dept. Virtualized Workloads
Proprietary
Specialized

Mid-long term
Short term

Strategic Application Refactoring

Strategic Target

High Level Strategy

• Application mobility
• Deployment agility
• Open
• On-going competition
• Low/no entrance barriers