Cloud Security & Identity Management

Sanjeev Kumar (skumar1@statestreet.com)

October 30, 2012
NIST: “Cloud is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.”

Leveraging Cloud Computing / Service Oriented Delivery

5 essential characteristics, 3 service models 4 deployment models

Gartner: “Cloud is a style of computing where scalable, elastic IT-related capabilities are provided ‘as a service’ to customers using Internet technologies.”
Business and IT Benefits
- Think about Capability Cloud in terms of business services to enable agility and innovation with improved security and quality with compliance and regulation conformance
- Standards based LEAN IT – Renovate IT Perception in Business
- Reduced cost & improved speed

Key Measures/Metrics
- Measure what matters most
- Adjust and recalculate – cloud will evolve and mature iteratively

Construction Costs
- Move what makes sense
- Understand and prioritize Best-fit solutions
- Embrace composition, service and ASD paradigm

Organization Design/Capabilities
- Matrix/Transformational

Funding
- ROI and TCO scanning

Engagement Model (RASCI)
- Business, App Owners, Dev Vendors & Strategic Partners

Clear Communication Plan
- Communicate roadmap, sequence of steps & dependencies, target dates for cloud env readiness, milestones for “attention continuum”

Right Skill Sets
- Engage Right resources
- “Cloud is what you make it”
- Roles and responsibilities – Cloud workers

Standards
- VUI, REST, Functional & Data Rights management

Automation Processes and Tools
- Hypervisors/Micro kernels
- Application deployment models

Business Continuity
- Dynamic & Rapid provisioning, SLA driven elastic computing, Active-Active for improved QoS/SLA

BR & DR
- Business Resumption and DR in-built, Async data replication

Process Efficiency (Cloud Best Practices/Guidelines)
- Standardization, automation, commoditization → business process, code & data reuse
- Strong GRC and open source lightweight stack

Security Efficiency
- SSO and Data Rights Management
- Identity federation, SAML, WS*, ACL, XACML, OpenID

Data Efficiency/Information Life Cycle Management
- Tiered storage and data security/access standards
- Data Warehouse Appliances for performance
- Robust BI, Reporting, Analytics frameworks

Other Emerging Trends

Business Strategy & Process

Projects & Applications

Organization & Governance

Building Blocks

Value Creation

Cloud Rollout Roadmap
- Major activities, sequence and dependencies, risk mitigation plans, resource, funding, vendor engagement, milestones and metrics to measure success

Private Cloud Ready Apps (Feasibility/Validation)
- Application Survey and Deep-Dive Architecture Review. Non business critical trading systems preferred in wave 1

Cloud Migration Factory Service/Refactoring
- Technical (Automation, Workflow, Deployment etc.) Governance and Organizational Framework for bulk app migration to cloud/app modernization

Infrastructure-As-A-Service (IaaS)
- Dynamic provisioning, SLA driven elastic computing, Metered payment, Active-Active for improved QoS/SLA

Platform-As-A-Service (PaaS)
- Build capability clouds (collaboration, analytics etc.)
- Development and Test Clouds
- Integration and Information/Data Access Services

Business Process-As-A-Service (BaaS)
- Shared Business Services
- BPP on Demand (Workflow and Rules Driven)

Software-As-A-Service (SaaS)
- Use Cloud Migration Framework to refactor and deploy apps in cloud
- Service oriented asynchronous, decoupled, stateless systems
- Extract consumers from resources

Authentication, Authorization & Access Control
- User, Application and Service level Authentication (2/multi factor, SAML, Certificate, OpenID, XACML, IDaaS etc.) & Authorization, Session Management and granular role based access control of services

Provisioning and Security Controls
- SSO and Data Entitlement, Message validation and content scanning to detect XML injections, Security Control Curbs via Governance
<table>
<thead>
<tr>
<th>Identity Mgmt Task</th>
<th>Consumer User</th>
<th>Corporate User</th>
<th>Web Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Access Control Model</td>
<td>RBAC, ACL</td>
<td>RBAC, ACL</td>
<td>ACL, RBAC if requested for specific user</td>
</tr>
<tr>
<td>2a Authoritative Source</td>
<td>The user, Local registration or OpenID</td>
<td>The user's organization</td>
<td>SPML or SAML</td>
</tr>
<tr>
<td>User Data</td>
<td>The user</td>
<td></td>
<td>SPML or SAML</td>
</tr>
<tr>
<td>2b Authoritative Source</td>
<td>The cloud provider</td>
<td>The user's organization</td>
<td>Information owner</td>
</tr>
<tr>
<td>Policy Data</td>
<td>The cloud provider</td>
<td>The cloud provider</td>
<td>SPML or SAML</td>
</tr>
<tr>
<td>Privacy Policy</td>
<td>The cloud provider implement locally</td>
<td>The user's organization</td>
<td>client organization</td>
</tr>
<tr>
<td></td>
<td>The user</td>
<td></td>
<td>SPML or SAML</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>SPML or SAML</td>
</tr>
<tr>
<td>3 Privacy Policy</td>
<td>The cloud provider implement locally</td>
<td>The user's organization</td>
<td>XSPA (Cross Enterprise security and privacy authorization) profile for XACML</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>XSPA (Cross Enterprise security and privacy authorization) profile for XACML</td>
</tr>
<tr>
<td>4 Access Control Policy</td>
<td>XACML</td>
<td>XACML</td>
<td>XACML</td>
</tr>
<tr>
<td>Format</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5 Policy Transmission</td>
<td>N/A</td>
<td>SPML or SAML 2.0 profile of XACML</td>
<td>SPML or SAML 2.0 profile of XACML</td>
</tr>
<tr>
<td>6 User Profile</td>
<td>Oauth</td>
<td>SAML Assertion</td>
<td>SAML Assertion</td>
</tr>
<tr>
<td>Transmission</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7 Policy Decision</td>
<td>N/A</td>
<td>XACML, SAML2.0</td>
<td>XACML, SAML2.0 profile of XACML</td>
</tr>
<tr>
<td>Request</td>
<td></td>
<td>profile of XACML</td>
<td></td>
</tr>
<tr>
<td>8 Policy Decision</td>
<td>Do within application</td>
<td>Do within application</td>
<td>Do within application or externalize to web service gateway product.</td>
</tr>
<tr>
<td>Enforcement</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Locally specified ACLs for non-corporate entities</td>
<td>XACML for policy specification from Policy Administration Point</td>
<td></td>
</tr>
<tr>
<td></td>
<td>OAuth to share with other sites</td>
<td>OAuth to share with other sites</td>
<td></td>
</tr>
<tr>
<td>9 Audit Logs</td>
<td>Log activity – encrypt with time stamp</td>
<td>Log activity – encrypt with time stamp</td>
<td>Log activity – encrypt with time stamp</td>
</tr>
</tbody>
</table>