Cloud Computing – Challenges and Opportunities

Yousef Khalidi
Distinguished Engineer
Windows Azure
Overview

- Cloud Computing: higher agility and lower cost
  - Require new application, hardware, and operational models
- Cloud Architectural Elements
  - Windows Azure as an example
- Challenges
  - Targeting apps to cloud – new and existing apps
  - Security and trust – in large public shared clouds
  - Hybrid clouds – necessary, yet introduce new cross cloud issues
- Predictions & Conclusions
  - One size does not fit all – spectrum of clouds
  - Need new cloud application model
Why Embrace the Cloud?

- Greater agility
  - Resource and business agility
- Reduced cost
  - Increased utilization, capex -> opex
- Cloud as communication hub
  - Data sharing across devices

- High-scale sharing is key
  - Economies of scale
  - Elasticity
  - Increased utilization
Three Dimensions of Cloud Computing

Style of computing with dynamically scalable and virtualized resources provided as a service typically over the Internet

**App Model**
- Scale-out, service oriented,
- Replicated state, stored in network

**Hardware Model**
- Shared, scale-out, industry-standard hardware
- At cloud provider, partner, or on-premises

**Operations Model**
- Manage services not servers
- Usage tracking and chargeback
Cloud Architecture Elements

- **Efficient compute fabric**
  - Machine and network virtualization & resource management

- **Each node is a cache state**
  - Scale-out model, expect failures, reconstruct state from elsewhere

- **Automation**
  - Reduce cost, increase agility, remove human from loop

- **Modeling to capture intent and constraints**
  - Key to enabling automation

- **An application model**
  - Simplify and enable automation; geared toward scale-out services

- **Platform services and APIs**
  - Increase programmer agility, reduce duplication, enforce policies
Windows Azure Growing Global Presence

North America Region
- North Central
- South Central

Europe Region
- North Europe Sub-region
- West Europe Sub-region

Asia Pacific Region
- East Asia Sub-region
- South East Asia Sub-region
Development and Operations Tools

Windows Azure SDK
• Includes a development fabric for running and debugging code locally

Windows Azure Tools for Microsoft Visual Studio
Windows Azure Tools for Eclipse for PHP and Java

Web portal, including billing
RESTful management APIs
Service lifecycle management
Challenges

- Targeting applications to the cloud
  - Forklift approach does not work

- Security, trust, and regulations
  - Particularly in shared environments

- Hybrid clouds
  - Necessary, yet introduce new cross-cloud issues
Targeting Apps to Cloud

Questions To Consider
- Application State
- Application Scale
- Data Sensitivity
- Connectivity Needs
- Application Portability
- Latency Between Components
- Regulation and Compliance

Some Easy Cases
- e.g., website sharing public data

Often, Forklift Approach Will Not Work
- Careful decomposition needed
<table>
<thead>
<tr>
<th>Application Data</th>
<th>State must be replicated, by app directly or in a replicated store</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Configuration &amp; Installation</td>
<td>Configuration state only a cache; no lengthy install step</td>
</tr>
<tr>
<td>Application Scale</td>
<td>App must scale horizontally (scale-out) not vertically (scale-up)</td>
</tr>
<tr>
<td>Application Dependencies</td>
<td>App must be able to run on cloud platform with no special hardware needs</td>
</tr>
<tr>
<td>Latency Needs</td>
<td>Shared cloud systems may not guarantee uniform/low latency among app components</td>
</tr>
<tr>
<td>Connectivity Needs</td>
<td>Intra- and inter- app connectivity needs must be clear and can provided by platform</td>
</tr>
<tr>
<td>Data Sensitivity</td>
<td>Public clouds may not be able to host all sensitive data</td>
</tr>
<tr>
<td>Security and Regulation</td>
<td>Location and type of cloud matters – see next slides</td>
</tr>
</tbody>
</table>
Cloud Security Considerations

- Identity and Access Management
  - Federate from on-premises to the cloud
  - Federate across organisation and country borders

- Application operational processes
  - Should be integrated into the organisation’s security management

- Communication and endpoint Integrity
  - Applications and clients are no longer behind firewall

- Compliance and Risk Management
  - Cloud customers still responsible for compliance and risk management
Regulations and National Boundaries

- Do you know where your data resides?
- Hybrid clouds can span national boundaries
- Many governments regulates where data can live
  - And where it cannot
- Policy controls are needed for data & applications
  - Driven by regulations and business needs
Hybrid Clouds

Public Cloud

Hosted Private cloud

Secure Cloud Federation

PRIVATE CLOUD

INTERNAL IT
Cloud Spectrum and Tradeoffs

Public Cloud:
- Highest scale and sharing
- Least control and isolation

Hosted Private Cloud:
- Least scale and sharing
- Most control and isolation

Private Cloud:
- Least scale and sharing
- Most control and isolation

- One size does not fit all
- Cost, agility and control tradeoffs
- Target apps to right environment
Evolving into Hybrid Clouds

Specialized cloud offerings will evolve, e.g., per segment industry, geo locations.

Secure Cloud Federation

Evolve from custom virtualized infrastructure to packaged platforms.
Secure Cloud Federation

**CLOUD**
- Data Synch and Caching
- Application Connectivity
- Federated Identity and Access Control
- Secure Network Connectivity

**ENTERPRISE**
Predictions

Cloud Application Model will be the Default
Scale-out, service oriented; the rest will be “legacy”

Public Clouds will Become More Mature
But private clouds will not go away

More Specialized Clouds - Per-industry, Per-geo, ...
Cloud federation and cloud brokers will be prevalent
Hybrid clouds will be the norm

Security and Management Across Cloud Boundaries
Services distributed across clouds by default
Policy-driven secure connectivity mechanisms will be needed
Summary

- Cloud computing: It’s still very early
- Once size does not fit all
  - Spectrum of clouds
  - Security will span multiple clouds and locales by default
  - Must consider location, control, and level of risk tolerance
- Need new cloud application model
  - Scale-out by default, including data storage and management
  - Adjusts to available cloud hardware and network