Designing a Highly Secured, Hybrid, Multi-Cloud Infrastructure for an Enterprise

A Precise Software Solutions Presentation:
Ben Duan, Chief Technology Officer
Steven Kahn, Engineering Lead

June 26, 2019
ABOUT PRECISE
Precise Software Solutions, Inc. (Precise) is a nimble and fast-growing SBA 8(a) certified small business focusing on strategy and IT consulting services to public sector customers. We are proud of our strong reputation for overcoming obstacles and delivering innovative, quality work with measurable results. For detail information, please visit us at www.precise-soft.com
Agenda

01 About Precise Software Solutions
02 Multi-Cloud Adoption Strategy
03 Cloud Account Management
04 Hybrid Network Architecture
05 Backup and Recovery
06 Security Overview
07 Multi-Cloud Management
08 Cloud Center of Excellence

Please visit us at www.precise-soft.com
Multi-Cloud, Hybrid Cloud Adoption

**Why Multi-Cloud**

- Leverage best of breed vendor solutions
- Benefit from competing vendor pricing
- Avoid vendor lock-in
- Mitigate risks

**Why Hybrid Cloud**

- Integration with on-premises systems
- Cloud as disaster recovery site
- Data Center extension to the cloud
- Centralized on-premises Data Center and cloud management
- Centralized security management
- ATO requirements

Please visit us at www.precise-soft.com
A Hybrid, Multi Cloud Case Study

Customer to implement hybrid cloud to:
✓ Meet cloud-first, Cloud-smart mandate
✓ Meet FITARA requirement to improve enterprise virtualization ratio
✓ Extend on-premises data centers to the cloud
✓ Implement next-generate cloud native applications
✓ Migrate on-premises systems to the cloud
✓ Leverage cloud as DR options
✓ Maintain consolidated data center and cloud security and operation management on premises

Customer to implement IaaS in both AWS and Azure to:
✓ Give business options to choose cloud service providers (CSPs)
✓ ATO AWS to high to host mission critical systems
✓ Utilize enterprise license agreement with Microsoft to simplify cloud acquisition process
✓ Leverage enterprise license discount with Microsoft to reduce Windows VM cost

OUR TASK
✓ To design and implement enterprise IaaS in AWS and Azure
✓ To achieve AWS to high, Azure to moderate ATO
✓ Single pane of glass cloud management on both AWS and Azure

Please visit us at www.precise-soft.com
Design Considerations

- Design for Security Compliance
- Design for HA, Reliability and Performance
- Design for Consistent Cloud Architecture
- Cloud as Extension of On-premises Data Center
- Leverage Existing Customer Best Practices and Tools
- Leverage CSP Reference Architectures
- Consistent Management for Multi-cloud

Please visit us at www.precise-soft.com
Multi-Account Structure

Core Accounts
- Logging: Centralized logs
- Security: Config rules, security tools
- Shared services: AD, deployment tools, patching, monitoring, anti-virus.

Business Unit Accounts
- Enterprise Shared Accounts: For business units that wish to share account and environments. Include Dev, Test, Pre-prod, Prod.
- Business Unit Accounts: For business wish to have separated accounts and environments
Hybrid Cloud High Level Architecture

- Shared Cloud Networks for Shared Tools and other Shared Environments
- Optional Business Unit Networks for Optimal Use of Resources
- Flexible Hybrid Architecture
  - Improved Bandwidth
  - Better Traffic Isolation
  - Increased Stability
  - Cost Separation
  - Direct Connect or Internet (TIC)
- Local Shared Tools to Reduce Network Latency and Egress Charges
VPC Network Reference Architecture

- Adopting AWS Best Practices for Hybrid Cloud
- Separate subnets for Web, App and DB tiers
- Inter-subnet traffic managed and inspected by Gateway devices
- High Availability Across Multiple Availability Zones
- Full deployment of AWS CloudTrail, CloudWatch, and AWS Config
- Audit logs captured in centralized S3 logs bucket
- Database HA?

Source: AWS - Standardized Architecture for NIST-based Assurance Frameworks on AWS

Please visit us at www.precise-soft.com
Best Practices for Hybrid Cloud Implementation
- Separate subnets for Web, App and DB tiers
- Implement Cross-zone Load Balancing to Create Multi-tier highly available applications
- ExpressRoute is Primary Communication to On-Premises; VPN is Secondary

Source: Microsoft – Azure Reference Architecture: Connect an on-premises network to Azure using ExpressRoute with VPN failover
Hybrid Cloud Design Option 1

- 3rd Party Virtual Gateways
- Improved Cloud Traffic Management and IDS/IPS capability
- Consistent Security Policy Across Enterprise
- Dedicated Gateways Per Environment
- Cloud Environments extend On-Premises Environments
- Security VPC for North-South Communication

Please visit us at www.precise-soft.com
Hybrid Cloud Design Option 2

- More Consistent with On-premises Environment
- Control by On-Premises Security Team
- Routing Controlled by Virtual Gateways
- VPN Communication to Management

Please visit us at www.precise-soft.com
## Cloud DR Options

<table>
<thead>
<tr>
<th>Solution</th>
<th>Description</th>
<th>RTO, RPO</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hot Standby</td>
<td>Servers at DR site are running 24x7. Data are replicated from primary site to DR site in real time. When disaster happens at primary site, switching global DNS or global load balancer will effectively switch the system to DR site</td>
<td>Low RTO ~ minutes - hours RPO ~ minutes</td>
<td>Very high</td>
</tr>
<tr>
<td>Cold Standby</td>
<td>Servers at DR site are shutdown. Data are replicated from primary site to DR site in real time. When disaster happens at primary site, servers at DR site will be brought up, and global DNS or load balancer will switch to point to DR site</td>
<td>Moderate RTO ~ hours - days RPO ~ minutes</td>
<td>High</td>
</tr>
<tr>
<td>Replication</td>
<td>No servers at DR site for the system, but data are replicated real time from primary site to DR site. When disaster happens at primary site, servers need to be built at DR site, and connect/mount to the data. Global DNS or load balancer will switch to point to DR site</td>
<td>High RTO ~ days - weeks, RPO ~ minutes - hours</td>
<td>Moderate</td>
</tr>
<tr>
<td>Backup</td>
<td>No servers at DR site for the system. No real time data replication. Primary site data are periodically backed up to DR site. When disaster happens at primary site, servers need to be built at DR site, data need to be restored at DR site. Global DNS or load balancer will switch to point to DR site</td>
<td>Very high RTO ~ weeks –months RPO ~ hours-days</td>
<td>Low</td>
</tr>
</tbody>
</table>
## Security in Depth

<table>
<thead>
<tr>
<th>Layers</th>
<th>AWS</th>
<th>Azure</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS Security</td>
<td>Customer approved RHEL and Windows AMIs with timely security patching</td>
<td></td>
</tr>
<tr>
<td>Network security</td>
<td>• 3rd Party Virtual firewall monitor and inspect all inter-subnet traffic</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Security groups</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Access control lists</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Elastic Load Balancers</td>
<td></td>
</tr>
<tr>
<td>Authentication and Access</td>
<td>• PIV authentication</td>
<td>• Azure IAM</td>
</tr>
<tr>
<td>Management</td>
<td>• Identity Provider identity federation for AWS and Azure Management Portal access</td>
<td>• Azure Key Vault</td>
</tr>
<tr>
<td></td>
<td>• Identity Provider solution for individual VM console access</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• VDI jump-box</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• AWS IAM</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• AWS KMS</td>
<td></td>
</tr>
<tr>
<td>Centralized Account Management</td>
<td>• Active Directory</td>
<td></td>
</tr>
<tr>
<td>Intrusion Detection and</td>
<td>• 3rd Party IDS Vendor</td>
<td></td>
</tr>
<tr>
<td>Prevention</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configuration Management</td>
<td>• 3rd party configuration tools, Ansible, Chef etc.</td>
<td>• Azure Configuration manager</td>
</tr>
<tr>
<td></td>
<td>• AWS Config Rules</td>
<td>• Azure Powershell</td>
</tr>
<tr>
<td></td>
<td>• Lambda scripts</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• CloudFormation</td>
<td></td>
</tr>
<tr>
<td>Logging and Auditing</td>
<td>• CloudTrail</td>
<td>• Azure Activity Log</td>
</tr>
<tr>
<td></td>
<td>• CloudWatch</td>
<td>• SIEM</td>
</tr>
<tr>
<td></td>
<td>• AWS Config</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Centralized S3 log bucket</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• SIEM</td>
<td></td>
</tr>
<tr>
<td>Data security</td>
<td>• EBS, S3, RDS encryption enforcement by Config Rules</td>
<td>• Azure disk encryption, Azure SQL database encryption</td>
</tr>
<tr>
<td>Anti Virus</td>
<td>• End Point Protection Vendor</td>
<td></td>
</tr>
</tbody>
</table>
Cloud Resource Authentication

Federation Access Control for Console and Resources

- Implement PIV card for multi-factor authentication
- One unique Account for both on-premises and public clouds
  - One consistent process for add, update, and delete
- Authentication occurs on-premises
- Keep some local accounts as backup

Please visit us at www.precise-soft.com
Virtual Machine Authentication

Access Control for Virtual Machines

- Implement PIV card for multi-factor authentication
- Linux domain join to Windows
- One unique Account for both on-premises and public clouds
- One consistent process for add, update and delete
- Consistent with on-premises access to Servers

Please visit us at www.precise-soft.com
Central Audit Logging

Cloud Audit Logs
- Integrated with on-premises Security Information and Event Management (SIEM)
- Enable your organization to perform log analysis across the enterprise
- Consider the scope of logs sent to on-premises

Please visit us at www.precise-soft.com
Miscellaneous Security Processes

Cloud Services vs. On-premises tools

**Recommendation**: On-premises works for hybrid cloud solution

- Vulnerability Scanning – Golden Images
  - Establish Golden Images Early
  - Scanning locally
  - Integrate Vulnerability Tracking with Existing Process

- Patch Management – Windows, Linux
  - Local Patch Repositories
  - Proxies

- Anti-Virus Protection
  - Local Virus Update Repositories

Please visit us at www.precise-soft.com
Compliance – Assess, Authorize (ATO), Monitor

- Federal Risk Authorization Management Program (FedRAMP) - 2011
  - Completed by Cloud Service Providers
  - FedRAMP Marketplace Listing
  - Based on NIST SP 800-53 controls (low, medium, high categories)
  - Completed by Government Agencies
  - Coordinate w/ Security early in the Design Process
  - Based on NIST SP 800-53 controls (low, medium, high categories)
    - Authorize Infrastructure, Services, & Custom Applications

Recommendations
- Assess Controls early in the Design Process
- Divide Controls into Policy and Technical Categories
- Assess Risk for Controls not met

Please visit us at www.precise-soft.com
**Design for Compliance – AWS NIST Quick Start**

Quick Start provides guidance to meeting NIST SP 800-53 controls!

Please visit us at www.precise-soft.com

---

### AWS Quick Start Architecture Comments for NIST SP 800-53 Controls

<table>
<thead>
<tr>
<th>Family</th>
<th>Control (Major)</th>
<th>Control (Sub-part)</th>
<th>Title</th>
<th>Description</th>
<th>Control Description</th>
<th>AWS Quick Start</th>
<th>Category Influence</th>
<th>Category Responsibility</th>
<th>Security Control Implementation Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AUDIT AND ACCOUNTABILITY</td>
<td>AU-0</td>
<td>AU-0</td>
<td>SYNCHRONIZATION WITH AUTHENTIC TIME SOURCE</td>
<td>Provides time stamps for audit records that can be mapped to Certified Universal Time (UTC) for Research &amp; Mass Data (MID) and meets <a href="https://example.com">Assignment organization defined granularity of time stamps</a></td>
<td>AU-0-06</td>
<td>Yes Information Systems</td>
<td>Shared</td>
<td></td>
<td>In this architecture, AWS CloudTrail, S3 bucket logging, Elastic Load Balancer (ELB) logging, and RDS MySQL server logging are enabled, with the EC2 instance level (instance level) application running proxy server, and EC2 based NAT instances in AWS Regions where Managed NATGateways are not available. Use Amazon DNS AMIs, which have NAT configuration by default to open and access the org resource. Use NAT resource to access, manage, or generate by AWS. For more information, see <a href="http://example.com">http://example.com</a></td>
</tr>
<tr>
<td>AUDIT AND ACCOUNTABILITY</td>
<td>AU-8</td>
<td>AU-8</td>
<td>SYNCHRONIZATION WITH AUTHENTIC TIME SOURCE</td>
<td>The information system:</td>
<td>AU-8-03</td>
<td>Yes Information Systems</td>
<td>Shared</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AUDIT AND ACCOUNTABILITY</td>
<td>AU-8</td>
<td>AU-8</td>
<td>SYNCHRONIZATION WITH AUTHENTIC TIME SOURCE</td>
<td>Integrates the internal information system objects (Assignment organization defined granularity) with <a href="https://example.com">Assignment organization defined granularity of time stamps</a></td>
<td>AU-8-03</td>
<td>Yes Information Systems</td>
<td>Shared</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>AU-8</td>
<td>AU-8</td>
<td>SYNCHRONIZATION WITH AUTHENTIC TIME SOURCE</td>
<td>Integrates the internal information system objects (Assignment organization defined granularity) with <a href="https://example.com">Assignment organization defined granularity of time stamps</a></td>
<td>AU-8-03</td>
<td>Yes Information Systems</td>
<td>Shared</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Multi-Cloud Management

Hybrid Cloud Management reference architecture
(Cloud Standard Customer Council)
Cloud Center of Excellence

Core Values

Innovation
Brings innovative solutions to leverage technology innovations in the Cloud marketplace

Predictability & Decision Making
Provides on demand Cloud analytics covering impact, service levels, monitoring, utilization, costs comparison, compliance and demand forecasting for strategic decision making

Leadership & Capability Development
Provides leadership, management and strategic workforce planning, and critical acquisition, ongoing capability development to meet future demands and innovation

Multi Vendor Management
Concentrates on key vendors for optimal efficiency and cost effectiveness, ROI/ROV management and governance

Governance
Promotes Cloud rationalization, reference architecture and implementation, standardization across the enterprise.

Operational Efficiency & Agility
Improves Cloud operation efficiency and agility via automation leveraging Infrastructure as Code, DevOps technologies

Solution Delivery Life Cycle Support
Ensures cloud aspects of requirements definition, solution design, architectures, development, testing and implementation and migration are supported

People: Digital Workforce

Please visit us at www.precise-soft.com
Cloud Center of Excellence Key Focus Areas

Ensuring cloud workload is well-architected to enhance mission effectiveness and reduce mission risks

Cost and operational efficiency
- Infrastructure as Code, CI/CD pipelines for end-to-end cloud infrastructure provisioning and application deployment

Architectures Standards
- Reference architectures and implementations for typical solutions
- Standard cloud service catalogs
- Templates for design, test, infrastructure provisioning, O&M

Cloud adoption
- Advocate cloud value proposition
- Assist in the entire EPLC lifecycle of cloud projects
- Cross functional seminars and knowledge sharing

AUTOMATION
REFERENCE ARCHITECTURE & IMPLEMENTATION
ACTIVE BUSINESS ENGAGEMENT
Thank You!

www.precise-soft.com  ben.duan@precise-soft.com  steven.kahn@precise-soft.com

1445 Research Blvd. Suite #500
Rockville, MD 20850

@2019 Precise Software Solutions