Cloud Migration, Application Modernization and Security for Partners

Tom Laszewski
Matt Yanchyshyn
AWS Migration Methodology
Migration Challenges

- People, Process, Technology
- Knowledge & Training
- Not Primary Business Activity
- Attempting Too Much at Once
- Migration Experience
- Fear
Migration Methodology

**Plan**
- Discover
  - Assessment & Profiling
  - Prioritization
  - Data requirements & classification
  - Business logic & Infrastructure dependencies
- Design
  - Detailed migration plan
  - Estimate effort
  - Security & risk assessment
- Transform
  - Network topology
  - Migrate
  - Deploy
  - Validate
- Transition
  - Pilot testing
  - Transition to support
  - Release management
  - Cutover & Decommission
- Operate
  - Staff Training
  - Monitoring
  - Incident Management
  - Provisioning
- Optimize
  - Monitoring-driven optimization
  - Continuous Integration and Continuous Deployment

**Build**

**Run**

**App Migration Assessment**

**Re-hosting (Lift & Shift)**

**App Portfolio Optimization**

**Re-platforming (Lift & Reshape)**
Planning your Migration

Migrating to the cloud can take one of many paths
End-state Architecture
Design and architecture of the cloud environment is important to enable cloud benefits such as agility and cost savings.

<table>
<thead>
<tr>
<th>Networking</th>
<th>Security</th>
<th>Governance</th>
<th>Data Management</th>
<th>Monitoring</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Convergence of on-premises and cloud</td>
<td>• SSO</td>
<td>• Billing &amp; cost management</td>
<td>• RPO/RTO</td>
<td>• Notifications &amp; alerting</td>
</tr>
<tr>
<td>• Cloud-oriented protocols</td>
<td>• Access policies</td>
<td>• Service catalogs</td>
<td>• Retention policies</td>
<td>• Application level awareness</td>
</tr>
<tr>
<td>• IP scheme and addressing</td>
<td>• Least privilege</td>
<td>• Configuration management</td>
<td>• Replication</td>
<td>• Thresholds</td>
</tr>
<tr>
<td>• VPC and Account configuration</td>
<td>• Audits</td>
<td>• Architecture Standards</td>
<td>• Storage optimization</td>
<td>• Service desk integration</td>
</tr>
<tr>
<td></td>
<td>• Compliance</td>
<td>• SLA/SLO</td>
<td>• ILM</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Intrusion detection &amp; prevention</td>
<td>• Procurement</td>
<td>• Data quality</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Logging</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## On-Premises Infrastructure Mapped to AWS

<table>
<thead>
<tr>
<th>Technology</th>
<th>On-Premises</th>
<th>AWS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td>VPN, MPLS</td>
<td>Amazon VPC, AWS Direct Connect</td>
</tr>
<tr>
<td>Storage</td>
<td>DAS, SAN, NAS, SSD</td>
<td>Amazon EBS, Amazon S3, Amazon EC2 Instance storage, distributed &amp; clustered FS on Amazon EC2</td>
</tr>
<tr>
<td>Compute</td>
<td>Hardware, virtualization</td>
<td>Amazon EC2, Amazon ECS, Amazon Lambda</td>
</tr>
<tr>
<td>Content delivery</td>
<td>3rd party CDN</td>
<td>Amazon CloudFront</td>
</tr>
<tr>
<td>Databases</td>
<td>MS SQL Server, MySQL, Oracle, DB2, PostgreSQL, MongoDB, ...</td>
<td>Amazon RDS, Amazon DynamoDB, Amazon ElastiCache, DB software on Amazon EC2</td>
</tr>
<tr>
<td>Load balancing</td>
<td>Hardware and software load balancers</td>
<td>Amazon ELB, software load balancers</td>
</tr>
<tr>
<td>Scaling &amp; cluster management</td>
<td>Hardware and software clustering tools</td>
<td>Auto Scaling, software clustering solutions</td>
</tr>
<tr>
<td>DNS</td>
<td>BIND, Windows Server, 3rd-party</td>
<td>Amazon Route 53, 3rd-party DNS software on EC2</td>
</tr>
<tr>
<td>Technology</td>
<td>On-Premises</td>
<td>AWS</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Analytics &amp; Data Warehouse</td>
<td>Hadoop, Vertica, Cassandra, specialized hardware and software</td>
<td>Amazon EMR, Amazon Redshift, software on Amazon EC2</td>
</tr>
<tr>
<td>Messaging and workflow</td>
<td>RabbitMQ, ActiveMQ, Kafka, …</td>
<td>Amazon SQS, Amazon SNS, Amazon SWF, software on EC2</td>
</tr>
<tr>
<td>Caching</td>
<td>Redis, Memcached, …</td>
<td>Amazon ElastiCache, Memcached, SAP Hana</td>
</tr>
<tr>
<td>Archiving</td>
<td>Tape library, off-site data storage</td>
<td>Amazon S3, Amazon Glacier</td>
</tr>
<tr>
<td>Email</td>
<td>Email software</td>
<td>Amazon SES</td>
</tr>
<tr>
<td>Identity, authorization &amp; authentication</td>
<td>AD/ADFS, LDAP, SAML, 3rd-party…</td>
<td>AWS IAM/STS, Amazon Cognito, Amazon Directory Service, AD &amp; LDAP on Amazon EC2</td>
</tr>
<tr>
<td>Deployment &amp; Configuration Management</td>
<td>Chef, Puppet, Salt, Ansible, PowerShell DSC</td>
<td>AWS CloudFormation, AWS OpsWorks, AWS Elastic Beanstalk, AWS CodeDeploy, AWS ECS,</td>
</tr>
<tr>
<td>Management and monitoring</td>
<td>CA, BMC, Rightscale</td>
<td>Amazon CloudWatch, Amazon Config, Amazon CloudTrail, AWS Trusted Advisor</td>
</tr>
</tbody>
</table>
Security comes first!
AWS is responsible for the security of the cloud
Customers configure their security in the cloud.

Customer applications & content
- Platform, Applications, Identity & Access Management
- Operating System, Network, & Firewall Configuration
- Client-side Data Encryption
- Server-side Data Encryption
- Network Traffic Protection

AWS Foundation Services
- Compute
- Storage
- Database
- Networking

AWS Global Infrastructure
- Availability Zones
- Regions
- Edge Locations
AWS Security Offerings

**Auditability**
- Compliance reports

**Visibility**
- AWS CloudWatch
- AWS CloudTrail
- AWS Config
- “Describe” APIs

**Control**
- AWS IAM
- AWS CloudHSM
- AWS CloudFormation
- AWS KMS
Defense-in-Depth

Physical
- AWS Compliance Program
- Third Party Attestations

Network
- Security Groups
- VPC Configuration
- Web Application Firewalls
- Bastion Hosts
- Encryption In-Transit

Data Security
- Logical Access Controls
- User Authentication
- Encryption At-Rest

System Security
- Hardened AMIs
- OS and App Patch Mgmt.
- IAM Roles for EC2
- IAM Credentials

Encryption
- In-Transit
- At-Rest

DATA
Encryption: Data at Rest

Volume Encryption
- EBS Encryption
- OS tools
- AWS Marketplace/Partner

Object Encryption
- S3 Server Side Encryption (SSE)
- S3 SSE w/ Customer Provided Keys
- Client-Side Encryption

Database Encryption
- RDS MSSQL TDE
- RDS ORACLE TDE/HSM
- RDS MYSQL KMS
- RDS PostgreSQL KMS
- Redshift Encryption
Built-In Firewall: Security Groups and NACLs

- **VPC Security Groups** (mandatory)
  - Instance level, stateful
  - Supports ALLOW rules only
  - Default deny inbound, allow outbound
  - Use as “whitelist” – least privilege

- **VPC NACLs** (optional)
  - Subnet level, stateless
  - Supports ALLOW and DENY
  - Default allow all
  - Use as “blacklist”/“guardrails” (port 135, 21, 23…)

- Separation of duties
- Changes audited via AWS CloudTrail
- Additional cost for SGs/NACLs: $0
AWS partner solutions extend & enhance security

- Some examples:
  - Cisco CSR (VPN)
  - Sophos UTM (firewall, …)
  - Alert Logic Web Security Manager (WAF)
  - Alert Logic Threat Manager (NIDS)
  - Trend Micro Deep Security (IDPS)
  - Trend Micro SecureCloud (encryption)
  - Dome9 SecOps (security group audit & management)
  - …
Migration Approach & Best Practices
Identifying Applications to Move

**Standalone** applications are **easy** to move

Application with **loosely coupled SOA-based** integrations are **good candidates**

Tightly integrated application needs more planning

‘Low hanging fruit’
- Dev/Test applications, Self-contained Web Applications (LAMP stack), social Media Product Marketing Campaigns, training Environments, Pre-sales Demo Portal, Software Downloads, Trial Applications

Watch out for
- 32 bit, non-Linux/Windows, multi-cast (Oracle RAC), client/server applications, engineered systems (Exadata, Netezza), massive file servers, vertically challenged software/applications
Getting a bread box estimate: Minimum information

**Compute:** Number of servers/VMs including RAM, CPU, OS, and boot drive size (Amazon EC2)

**Storage** mapping to transactional, backup, archival, and log/file system/applications (Amazon EBS, Amazon Glacier, and Amazon S3)

**Region** where processing is happening

Data transfer out for **Networking**

Internet or dedicated **Networking** including security requirements (Amazon Direct Connect and VPN)
Getting a bread box estimate: Nice to have

**Backup requirements** for each workload that can not be supported by EBS Snapshots

**HA requirements** for each workload (ELB, Route53)

**Scalability requirements** for each workload (ELB, Route53, Auto Scaling, CloudFront)

**DR requirements** for each workload

**Storage IOPS** requirements for each workload

**Compute** requirements for management/monitoring
Getting a bread box estimate: Really Nice

**Workload** stratification file servers, security, RDBMS, ERP, Big data, security, management/monitoring etc.

**HIPPA and PCI requirements for each workload**

**HPC requirements for each workload**

Extremely high **CPU, Memory** requirements

Top **3rd party vendors** for packaged apps
IDS/IPS, WAF, management, monitoring, logging, etc.)
Invest in Proof of Concept Early

Proof of concept will **answer** tons of **questions** and get your feet wet with AWS **quickly**

Will help identify **gaps** and **touch points**

Give you a good **estimation** of the migration costs

Give you a good **estimation** of the AWS runtime costs
Migrating Data into AWS Cloud

- **File transfer** to Amazon S3 or EC2 using S/FTP, SCP, UDP, Attunity
- **NFS** mount accessible from on premise and AWS
- Configure on-premises **backup application** (like NetBackup, CA, CommVault, Riverbed) to use Amazon S3
- **AWS Storage Gateway** for asynchronous backup to Amazon S3
- **AWS Import/Export service**: Ship your disk to AWS
- **Database backup** tools like Oracle Secure Back
- **Database replication** tools like GoldenGate, DbVisit
- **AWS Direct Connect** 100 Mbps to 10 Gbps
Migrating Data onto AWS

Data Size* relative to internet bandwidth and latency

Data Velocity Required

GBs

One-time upload w/ constant delta updates

TBs

UDP Transfer Software (e.g., Aspera, Tsunami, ...)
Attunity Cloudbeam
AWS Storage Gateway,
Riverbed, NFS

Transfer to S3 Over Internet

AWS Import / Export

Days

Hours

* relative to internet bandwidth and latency
Enforce consistent security on your hosts

Configure and harden EC2 instances based on security and compliance needs

- Host-based Protection Software
- Restrict Access Where Possible
- Connect to Existing Services

AMI catalog -> Launch instance -> EC2 -> Configure instance

Your instance

- User administration
- Whitelisting and integrity
- Malware and HIPS
- Vulnerability management
- Audit and logging
- Hardening
- Operating system

Configure and secure EC2 instances according to your needs.
Separate static assets & move servers away from the edge

- Inbound HTTP
- CloudFront
- Amazon S3
- WAF
- Dynamic
- Static
- App
- Peering
- VPC
Identity & Access Management

Create appropriate principles, authorization and privileges for AWS resources

AWS Identify and Access Management

- User
- User
- User
- Groups
- Roles
- Policies

Multi-Factor Authentication

- Hardware
- Virtual
- IAM AWS Administrative Users
- Root Account

**Note:** Always associate the account owner ID with an MFA device and store it in a secured place!
### AWS IAM Hierarchy of Privileges

**Enforce principle of least privilege with Identity and Access Management (IAM) users, groups, and policies and temporary credentials**

<table>
<thead>
<tr>
<th>Permissions</th>
<th>Example</th>
</tr>
</thead>
</table>
| Unrestricted access to all enabled services and resources. | Action: `*`  
Effect: Allow  
Resource: `*`  
(implicit) |
| Access restricted by Group and User policies | Action: `[‘s3:*’,’sts:Get*’]`  
Effect: Allow  
Resource: `*` |
| Access restricted by generating identity and further by policies used to generate token | Action: `[ ‘s3:Get*’ ]`  
Effect: Allow  
Resource: `arn:aws:s3:::mybucket/*` |
Principle of least privilege with IAM

• Login to an account with a less privileged user
  – Read-only
  – EC2 Launch-only

• Change role for privileged action
  – Administer IAM
  – Terminate Instance
  – Delete snapshots

Protection against accidents or mistakes
(e.g. similar to DisableApiTermination=true)
Consolidate your IAM users

- Put all IAM users and groups in one account
- All other accounts use AWS IAM Roles

**Best Practices:**
- Tie into consolidated billing hierarchy
- Users in IAM account are only authorized to assume roles in other accounts
- No AWS-billable resources in this account
Governance through IAM policies

... "Effect": "Deny",
"Action": "ec2:RunInstances",
"Resource": [
],
"Condition": {
  "ArnNotEquals": {
  }
}
],
"Effect": "Allow",
"Action": "ec2:RunInstances",
"Resource": [
  "arn:aws:ec2:region:account:security-group/sg-12345678"
] }
"Condition": {
  "StringEquals": {
    "ec2:ResourceTag/BillingCode": "4000"
  },
  "StringEquals": {
    "ec2:ResourceTag/Environment": "Prod"
  }
...
Implementing “smart” AWS policies

• The 5 W’s of auditability:
  – Who?
  – What?
  – Where?
  – When?
  – Why?

  Controlled by AWS IAM

  Not Controlled by IAM

• What we really want is an “if and only if” statement:
  – You can deploy this change in production “if and only if” it actually worked in test
Federate with AWS Directory Service & IAM

AWS Directory Services

- Directory Users
  - IAM_Admins
  - Read_Only
  - EC2_Admin
  - Group ‘n’

- Directory Groups
  - IAM_Admins
  - Read_Only
  - EC2_Admin
  - Role ‘n’

- IAM Role Mapping
  - IAM_Admin
  - Read_Only
  - EC2_Admin

- Role ‘n’

Mgmt Acct

Acct 1
- IAM Roles
  - IAM_Admin
  - Read_Only
  - EC2_Admin

Acct 2
- IAM Roles
  - IAM_Admin
  - Read_Only
  - EC2_Admin

Acct ‘n’
- IAM Roles
  - IAM_Admin
  - Read_Only
  - EC2_Admin
  - Role ‘n’

Amazon Web Services management console

Forgot Password?
Case Studies
Case study 1: Cognizant & HIPAA
Case study 2: ScienceLogic & Kellogg