Migrating Microsoft Applications to AWS like an Expert

Danny Jenkins, Solutions Architect

August 2018
What Will You Takeaway From This Session?

• This is a 300 level session
• Holistic approach to migrating Microsoft Workloads
• Move fast…dive deep where necessary
• QR codes are frustrating – Links on the website
  http://unicornshop.lol
Who Are Unicorn Shop?

“To enable anyone with the dream of being a unicorn to look like one”

Unicornshop.lol

- Online ecommerce offering
- Brick and mortar stores
- CMS, back office applications
- .NET and SQL custom applications
- Email hosted in O365

Issues:
- Wasted resources
- Capex vs Opex model
- Developers restrained and can’t help the business speed up
Migration Approach

- Application Review
- Active Directory
- Automation

- Approach
- Database Migration
- What next?

- Landing Zone
- Application Migration
Our Web Store (PCI Compliant)

- PCI compliant workload
- Need to restrict user access to some components
- Limited to specific services
- Need to monitor access patterns
Our CMS Deployment

- Legacy threat management SPOF
- Unable to keep up to date with threat definition templates
Microservices Deployment

Web logs
Database Logs

Microservices Fleet

Vendor API
Business Insights
So Let’s Go!! ....Almost...

**Strategy**
- Existing IT estate evaluation

**Plan**
- Planning & Discovery

**Build & Migrate**
- Application design
- Migration & Validation
  - Application 1
  - Application 2

**Run**
- Operation

**Services from AWS ecosystem**
- AWS Application discovery service
- AWS DMS
- AWS SMS
- Amazon Cloudwatch
- AWS Config

---

© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.
Approaching The Migration With The 6 R’s

Retain garages
Retire "-"
Rehost
Replatform
Refactor
Repurchase "Launch"
Building Our Landing Zone

- Multiple accounts in Organisations + SCPs
- How to create a monolithic identity approach (don’t judge me quite yet...)
- Amazon GuardDuty event execution
- AWS Config enforcing encryption demo
- Connectivity to support our Hybrid state during migration
Let’s Deploy Our Organisation’s Structure

```
{
"Version": "2012-10-17",
"Statement": [
  {
    "Effect": "Allow",
    "Action": [
      "ec2:*",
      "cloudwatch:*"
    ],
    "Resource": "*"
  }
]
}
```
Identity As A Monolith?

Administrator account

CloudFormation template

Stack Set

Target account A

Target account B

Target account C

Target account B

Region 1

Region 2
Cross account roles

- Identity Account
  - Admins

- Dev Account
  - Admin role

- Prod Account
  - Admin role
Demo
Amazon GuardDuty – Event Execution

aws events put-rule --name Test --event-pattern "{"source":["aws.guardduty"]}"

aws events put-rule --name Test --event-pattern "{"source":["aws.guardduty"],"detail-type":["GuardDuty Finding"],"detail":{"severity":[5.0,8.0]}}"

aws events put-targets --rule Test --targets Id=1,Arn=arn:aws:lambda:us-east-1:111122223333:function:<your_function>
Our CMS Threat Management Layer

Threat gateway

Web 01
Web 02
Web 03
Web 03
App 01
App 02
SQL 01
SQL 02

© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.
AWS WAF – Managed web application firewall
AWS WAF – Working with managed rulesets

- PCI
- OWASP Top 10
- Bot protection
- SQLi/XSS
- IP reputation
- CMS protection
Let’s Get Our Networking Right...

Customer routers

AWS direct connect routers

Public traffic

Private traffic

Amazon S3

VPC

Landing Zone
Single domain extended to multiple sites

- Availability Zone A
  - Private subnet
  - DC3
  - Cost 10
  - company.local

- Availability Zone B
  - Private subnet
  - DC1
  - Munich
  - DC2
  - Berlin
  - DC4
  - Cost 50
  - Corporate Network

- One single identity, data center extension mode (rely on Active Directory sites, read-only or not)

© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.
One subdomain per site
One forest per site and trust

Availability Zone A
- Private subnet DC3
- DC4

Availability Zone B
- Private subnet DC1
- DC2
- Munich
- Berlin
- company.local
- Corporate Network

AWS Directory Service

© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.
ADMT Migration details

- Availability Zone A
- Availability Zone B
- Corporate Network
- Domain
- client
- AWS Directory Service
- PES Install
- company.local
- Forest Trust
- VPC
## What Next? Migrating Databases – Which approach?

<table>
<thead>
<tr>
<th>Migration method</th>
<th>Amazon RDS Target</th>
<th>Amazon EC2 Target</th>
<th>Downtime</th>
<th>DB Objects</th>
<th>Cross-Engine</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup/Restore</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes (hrs)</td>
<td>Data, Schemas, Stored Procedures, Triggers, Indexes</td>
<td>No</td>
</tr>
<tr>
<td>Import/Export Bulk Copy</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes (mins-hrs)</td>
<td>Data, Schemas, Stored Procedures, Triggers, Indexes</td>
<td>No</td>
</tr>
<tr>
<td>SQL Log Shipping</td>
<td>No</td>
<td>Yes</td>
<td>Minimal (secs-min)</td>
<td>Pre-create the DB, sync</td>
<td>No</td>
</tr>
<tr>
<td>Hybrid Architecture</td>
<td>No</td>
<td>Yes</td>
<td>Minimal (secs-min)</td>
<td>Pre-create the DB, sync</td>
<td>No</td>
</tr>
<tr>
<td><strong>AWS DMS</strong></td>
<td>Yes</td>
<td>Yes</td>
<td>Minimal (secs-min)</td>
<td>With SCT (Data, Schemas, Stored Procedures, Triggers, Indexes)</td>
<td>Yes (SCT)</td>
</tr>
</tbody>
</table>
Users Accessing On Premise

On-premise DB

AWS DB

© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.
Migrating Database Writes Across

On-premise CMS DB

AWS DMS

AWS DB

Database Migration

© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.
Endpoint Update and On Premise Decommission

Decommission
CMS DB

AWS DMS
AWS DB

Database Migration

© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.
What To Migrate After SQL Server?

Fan out / deploy multiple systems in parallel:

• Exchange
• SharePoint
• Skype for Business
• System Centre Configuration Manager
• System Centre Operations Manager
• Etc...
Windows? Containers? Actually Yes...

State in containers, you can but what is the goal?

For unicornshop, short lived stateless apps

How to migrate apps to containers? Containers are portable..

Do you have a CICD process already?
ECS With 2 Autoscaling Groups

Example spot pricing

<table>
<thead>
<tr>
<th>C4</th>
<th>1a</th>
<th>1b</th>
<th>1c</th>
<th>On-Demand</th>
</tr>
</thead>
<tbody>
<tr>
<td>8XL</td>
<td>$0.50</td>
<td>$0.27</td>
<td>$0.29</td>
<td>$1.76</td>
</tr>
<tr>
<td>4XL</td>
<td>$0.21</td>
<td>$0.30</td>
<td>$0.16</td>
<td>$0.88</td>
</tr>
<tr>
<td>2XL</td>
<td>$0.08</td>
<td>$0.07</td>
<td>$0.08</td>
<td>$0.44</td>
</tr>
<tr>
<td>XL</td>
<td>$0.04</td>
<td>$0.05</td>
<td>$0.04</td>
<td>$0.22</td>
</tr>
<tr>
<td>L</td>
<td>$0.01</td>
<td>$0.01</td>
<td>$0.04</td>
<td>$0.11</td>
</tr>
</tbody>
</table>

Instance diversity

- m4.xlarge
- m3.xlarge
- c4.xlarge
- c3.xlarge
- r4.xlarge
- r3.xlarge

© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.
Scheduled Tasks? .Net Core 2.0 Lambda

- Upload Users
- S3 Bucket: Data dropped in S3, Schedule / event triggered
- Lambda function: Pull data from CSV file, Perform ETL, Insert data into SQL table
- DB in private subnet
- VPC private subnet

© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.
Automation Is Key, How Do I Automate Updates?

1. Start temporary instance
2. AWS latest Windows AMI
3. Update EC2 Config or EC2 Launch
4. Update PV drivers and run Windows updates
5. Invoke user provided scripts
6. Run a sysprep / Generalise
7. Custom AMI ready for deployment
8. Stop temporary instance
Searching for a solution to host its MSFT SharePoint sites, the company chose AWS because of cost, and to improve operational efficiency.

By running on AWS, Dole can launch a new SharePoint website in minutes, host business intelligence and mobile applications globally, and estimates savings of more than $350,000 in operating expenses.

“We can grow anytime we want, we don’t have to go and acquire new hardware”

Joanna Dyer – Director, IT Solutions
Wrapping It Up

• Understand the dependency chain in your Microsoft applications

• Build your migration plan around the dependency chain

• Know how Microsoft licensing on AWS works and plan accordingly
Thank you!