**AWS Migration Assessment**

**(Confidential)**

Table of Contents

Document Control 4

This document is a controlled document. On receipt of this document, please discard any earlier versions of this document. This document is valid on the day it is issued. The current master version of this document is stored at: 4

https://app.box.com/folder/45149516447 (Aecom Box share) 4

All files referenced from this document are stored in this location. All historical versions of this document are stored in the Versions sub-directory of the above location. 4

Revision History 4

Revision Details 4

Key Contacts 4

Aecom Contacts 4

AWS Contacts 4

Conventions 5

Numbering 5

Definitions 5

Abbreviations 5

Code/File References 5

Draft Missing/Review Items 5

About Aecom 6

About Amazon Web Services (AWS) 6

Introduction 7

Document Approach 7

In Scope Items 7

Out of Scope 8

High Level Discovery 8

Infrastructure Overview 8

Network 8

Data Center Specifics - FTServices 8

Data Center Specifics - Rackspace 8

Data Center Specifics – Azure 9

Region Mapping 9

Storage 9

Compute 9

Connectivity 9

Potential Shared Services and Tools 9

Microsoft Exchange 9

Active Directory 10

Backups 10

Monitoring and Alerting 10

Patching 10

Inventory Collection and Discovery 10

Automation and Deployment 11

Compliance & Governance 11

Data Sovereignty 11

Pre-requisites 11

AWS Training 11

Application Discovery 12

Operating Systems Supported in AWS 12

Application Workload Migration Patterns 13

Application Migration Tools 14

Applications Profiled during migration assessment 14

Application: Sharepoint 2013 and 2010 (Rackspace) 15

Application: Geographic Information System and Portal (Rackspace) 16

Application: Projectwise (Rackspace) 20

Application: Cityworks (Rackspace) 23

Application: AQM Apps (Rackspace) 23

Application: TaaS, TaaS-DevTest, Internal-NPS-Digital, TaaS-DFAT, ThoughtLeadership, eTimeTrack (Azure) 24

Application: aecomservices, aecomservicesdev, aecomservicestest (Azure) 24

AWS Pilot 26

Azure Migration 26

FTServices Migration 26

Rackspace Migration 28

Project Plan 29

Migration Approach and Plan 29

Recovery Plan 30

Test Plan 31

Application Workload Testing 31

AWS Environment Validation 31

Launch Plan 32

Prior to Launch 32

Launch 32

Post Launch 32

Operations Plan 34

Knowledge Transfer 34

Cost Optimisation 34

AWS Architecture 35

AWS Accounts 35

DirectConnect 35

Production Internal Operations Account and Extranet Account VPC Design 37

Security 38

NACLs 38

Security Groups 39

CloudFormation 41

Appendices 41

Appendix I: Application Characteristics Matrix 41

Document Control

This document is a controlled document. On receipt of this document, please discard any earlier versions of this document. This document is valid on the day it is issued. The current master version of this document is stored at:

<https://app.box.com/folder/45149516447> (Aecom Box share)

All files referenced from this document are stored in this location. All historical versions of this document are stored in the Versions sub-directory of the above location.

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Authors | Status |
| 19 Jan 2018 | 0.1 |  | Draft |
| 27 Jan 2018 | 0.2 |  |  |

Revision Details

|  |  |
| --- | --- |
| Version | Revision Details |
| 19 Jan 2018 | Initial draft migration assessment |
| 27 Jan 2018 | Added AWS Architecture Section |

Key Contacts

Key contacts for the Migration Assessment Project are as follows.

Aecom Contacts

|  |  |  |
| --- | --- | --- |
| Name | Role | Email |
|  | Director, Technical Strategy |  |
|  | IT Manager |  |
|  | IBM GTS |  |

AWS Contacts

|  |  |  |
| --- | --- | --- |
| Name | Role | Email |
|  | Cloud Infrastructure Architect |  |
|  | Engagement Manager |  |
|  | Practice Manager |  |
|  | Enterprise Solutions Architect |  |
|  | Principal Sales |  |

Conventions

This document uses the following style conventions.

Numbering

All sections bounded by a heading are numbered using section dot sub-section notation, this is for ease of reference when the document is being discussed.

Definitions

Defined terms or terms used frequently throughout this document are initially presented in sentence case and then throughout the rest of the document are presented using a capitalised first letter convention. For example, the reference to this document as the migration plan is presented like this and defined as Migration Plan.

Abbreviations

Abbreviations are shown in brackets immediately after the term that will be abbreviated. Throughout the rest of the document, the abbreviation will be used but the term may also be used where it makes sense to do so. For example, Amazon Web Services is abbreviated to AWS.

Code/File References

Any code examples or references to files are presented using the Courier New font in bold. For example, a file reference would look like this: filename.txt.

Draft Missing/Review Items

Whilst this document is in Draft status, any items requiring input, which are incomplete or require further clarification are marked with three red asterisk’s (e.g. \*\*\*). The asterisks are assigned to the nearest header, which contains the content to provide as much context as possible; this has the effect of showing incomplete items within the table of contents. Items marked in this way must be resolved before the document can be marked with the Final status.

About Aecom

AECOM is an American multinational engineering firm that provides design, consulting, construction, and management services to a wide range of clients. AECOM has approximately 87,500 employees, and is number 156 on the 2016 Fortune 500 list.

About Amazon Web Services (AWS)

In 2006, Amazon Web Services (AWS) began offering IT infrastructure services to businesses in the form of web services -- now commonly known as cloud computing. One of the key benefits of cloud computing is the opportunity to replace up-front capital infrastructure expenses with low variable costs that scale with your business. With the Cloud, businesses no longer need to plan for and procure servers and other IT infrastructure weeks or months in advance. Instead, they can instantly spin up hundreds or thousands of servers in minutes and deliver results faster.

Today, Amazon Web Services provides a highly reliable, scalable, low-cost infrastructure platform in the cloud that powers hundreds of thousands of businesses in 190 countries around the world. With data center locations in the U.S., Europe, Brazil, Singapore, Japan, and Australia, customers across all industries are taking advantage of the following benefits:

**Low Cost**

AWS offers low, pay-as-you-go pricing with no up-front expenses or long-term commitments. We are able to build and manage a global infrastructure at scale, and pass the cost saving benefits onto you in the form of lower prices. With the efficiencies of our scale and expertise, we have been able to lower our prices on 15 different occasions over the past four years.

**Agility and Instant Elasticity**

AWS provides a massive global cloud infrastructure that allows you to quickly innovate, experiment and iterate. Instead of waiting weeks or months for hardware, you can instantly deploy new applications, instantly scale up as your workload grows, and instantly scale down based on demand. Whether you need one virtual server or thousands, whether you need them for a few hours or 24/7, you still only pay for what you use.

**Open and Flexible**

AWS is a language and operating system agnostic platform. You choose the development platform or programming model that makes the most sense for your business. You can choose which services you use, one or several, and choose how you use them. This flexibility allows you to focus on innovation, not infrastructure.

**Secure**

AWS is a secure, durable technology platform with industry-recognized certifications and audits: PCI DSS Level 1, ISO 27001, FISMA Moderate, FedRAMP, HIPAA, and SOC 1 (formerly referred to as SAS 70 and/or SSAE 16) and SOC 2 audit reports. Our services and data centers have multiple layers of operational and physical security to ensure the integrity and safety of your data

Introduction

This document will be presented to Aecom following the AWS migration assessment which begins on Jan 3rd 2018 and ends Jan 24th 2018. During the initial kick off meeting, AWS presented a high-level plan of next 3 weeks which included interviews with respective teams from Rackspace, FTServices and Azure (collectively known as environments). Part of the assessment includes a Pilot migration of 1 or more applications from each environment.

This document presents key information captured during the migration assessment and will act as the migration plan used to provide Aecom with a proposal for supporting the migration phase of the project.

As first step towards understanding the overall scope of migrating to the cloud, including migration cost analysis, Aecom engaged AWS to perform an assessment of its current infrastructure, security, operations and application portfolio. The goals of the assessment were the following:

Discovery of servers and applications running in Aecom data centers hosted in Rackspace, Q9 (FTServices) and the Azure Cloud.

Provide high-level summary of “discovered” infrastructure (Application and Platform as a Service Inventory) and categorize:

Applications/servers that can be “Re-Hosted” with minimal changes/effort to AWS

Applications/servers that will need re-platform, re-factor, and/or re-architecture

Platform services that will need a re-platform, re-factor, and/or re-architecture

Project high-level timeline to move apps to AWS regions.

Document Approach

This section outlines the approach taken by AWS to achieve the above objectives and outcome of the assessment. List of activities completed by AWS, Aecom and IBM:

Deep dive into major Aecom work streams – Security, Operations, Infrastructure, and Application Portfolio during a 3 week assessment.

Application Inventory clean up and analysis to determine an initial migration approach.

Detailed analysis of the critical and complex application workloads.

In Scope Items

The Migration Planning Project considers the following items to be in scope:

Review of current FTServices, Rackspace, and Azure environments.

Review of current approach to infrastructure management and monitoring.

Review of current approach to infrastructure operations.

Provide spreadsheet of all servers and services within FTServices, Rackspace and Azure and provide an assessment of the migration difficulty (easy, medium, hard) and migration methodology (re-platform, re-host, re-factor, etc).

Pilot of one or more applications in FTServices, Rackspace and Azure.

Out of Scope

Any systems or processes not listed in the previous section are considered out of scope for the purpose of this project. Should items be discussed which should be in scope, the previous section will be updated to reflect this and a new version of this migration assessment issued.

High Level Discovery

During the migration assessment, Aecom provided a detailed overview of their technical and business environment as well as broader business outcomes to be delivered from the migration project.

This section of the migration assessment provides a summary of the high-level discovery and leads to the individual sections of the plan providing more in-depth discovery of network, storage, compute and application workload environments.

Infrastructure Overview

Aecom operates infrastructure globally, meeting the needs of business users, customers and partners around the world.

Network

For the purposes of this assessment, we focused on the following environments:

FTServices Q9 datacenter

Remote sites have VPN connections into this datacenter

Rackspace datacenter

Clients have IPSec VPN tunnels into the ASA in this datacenter

Azure Cloud (no connection from Azure to AECOM)

Data Center Specifics - FTServices

FTServices Q9 datacenter contains the following components

4 physical VM hosts

6 Citrix XenApp servers

3 backup and recovery servers

1 EMC VNX Storage array

2 Data Domain replicated storage devices

Target for Netbackup: file level backups, SQL Server agent based backups

Target for Synamtec Enterprise Vault email archiving

Provides CIFS

39 virtual machines

Contains ft-serv.com domain

Data Center Specifics - Rackspace

Rackspace datacenter contains the following attributes:

132 virtual machines

Most workloads are external client facing

Contains aecomnet.com and aecom.online domains

Load balancing is handled by F5 appliances

Data Center Specifics – Azure

Azure Cloud contains the following attributes:

34 databases (DbaaS)

43 AppServices

3 Api Management Services

44 virtual machines

64 storage accounts

11 load balancers

Azure AD points to aecom.net.com

Region Mapping

Aecom wishes to run their application workloads in geographic locations that maintain close proximity to their users. This is in order to achieve the lowest possible latency. Therefore, the following regions have been mapped to their existing data center locations and user locations:

|  |  |
| --- | --- |
| Existing Data Center | Map to AWS Region: |
| FTServices | TBD (data sovereignty) |
| Rackspace | TBD |
| Azure | TBD |

Storage

The EMC VNX storage array from FTServices Q9 will be vacated once all the VMs are migrated into AWS. FTServices is not using CIFS or NFS on the VNX array. The redundant Data Domain dedup storage devices should be migrated to another functioning datacenter.

Compute

Compute resources are distributed around the world and managed on a regional basis. Information was provided by the Aecom team directly in the form of spreadsheets for each environment.

Connectivity

Connectivity to Data Centers

Aecom utilizes a global MPLS cloud to connect most corporate networks to all data centers.

Connectivity to AWS

Aecom has indicated that they wish to install AWS Direct Connect to provide high-speed connectivity the AWS Region(s)

Potential Shared Services and Tools

Microsoft Exchange

FTServices migrated their active Exchange users to Office 365. They have legacy Exchange servers that are for old inactive users.

Active Directory

Active Directory servers will be need to be built in AWS to host the ft-serv.com, aecomnet.com, and aecom.online (resource) domains.

Backups

IBM is deploying Spectrum Protect (managed by the IBM CMB team) in the AECOM environment to replace a number of disparate legacy backup systems. There are two options for backing up AECOM VMs and data in AWS:

Create CMB SP infrastructure (backup servers and storage) in AWS on AWS compute and EBS storage resources "close" to the VMs and data that need to be backed up. This is the recommended and supported solution.

Backup VMs and data in AWS to backup servers and storage in the AECOM datacenters over the AECOM-AWS network connection. This is likely to be very expensive in terms of network traffic but may be a short term solution until we have CMB SP up and running in AWS.

Monitoring and Alerting

IBM ITM/Netcool: This is the standard agent-based monitoring and alerting toolset. We should be able to install OS/database/application ITM agents on AECOM VMs in AWS for standard monitoring as normal. We should also be able to ping these with the existing Netcool ping probes over the AECOM-AWS network link. I don't think we will need any additional M&EM infrastructure (e.g. new ITM RTEMS or ping probes) in AWS. However, hypervisor or hardware level monitoring will no longer be available through these tools in AWS.

Solarwinds: Again, basic VM agent installation and monitoring should work but no access to the hypervisor means no extended physical, host, cluster, virtualization, etc. monitoring, performance, and capacity information will be available.

Patching

IBM BigFix: This is an IBM tool for automated patching, security health checking and compliance, possibly software inventory and distribution, and other automations. All of these primarily depend on a BigFix agent being deployed to the VMs so there shouldn't be any issues in AWS (though, again, no hypervisor level access for security compliance checks, etc.) There may be a need for one or more BigFix relays to be created in AWS if and when we have a large number of VMs in AWS but initially I don't see any problems.

Other standard system management tools such as SCCM should also continue to work normally on AWS VMs, though we will probably need to setup some additional infrastructure in AWS (e.g. at least a few of AD DCs for the NA and other domains?)

Inventory Collection and Discovery

IBM TADDM: This is an IBM tool for inventory collection and application and dependency discovery. Since TADDM is agentless, I don't see any problems here either. We should still be able to use WMI/SSH to collect configuration and inventory information from AWS VMs. We shouldn't need any additional infra in AWS for this and TADDM should be able to update SNOW CMDB as normal. I don't think we use any additional asset management tools (e.g. Flexera?) in AECOM in the server environment.

Automation and Deployment

Future IBM management tools such as Dynamic Automation, RCP, Chef, etc. should also mostly work in AWS assuming the network bandwidth between AECOM and AWS is sufficient and there are no network latency (or network cost) issues. We should also be able setup tools servers and infrastructure in AWS where needed.

Compliance & Governance

Data Sovereignty

TBD for FTServices. This will determine the selected AWS Region to migrate the FTServices workloads into.

Pre-requisites

A number of pre-requisites were identified during the kick off workshop which we feel should be addressed before the migration project commences. These are set out here.

AWS Training

In order to provide effective and efficient AWS support, internal Aecom will need to train their workforce on various AWS services. Migrating to the cloud will provide opportunity to Aecom staff to not only get AWS hands-on experience, but also learn best practices from AWS professional services. By performing skills assessments, training, certification and mentoring Aecom can close the gap between current and projected talent needs to maximize velocity and employee satisfaction.

Application Discovery

This section provides a summary of the current Application landscape and a report of the results of an initial assessment performed on the Aecom Application portfolio to determine a migration path to AWS. Initial application discovery was performed and cross referenced to the spreadsheets provided for FTServices, Rackspace and Azure.

Operating Systems Supported in AWS

The following Operating Systems are supported in AWS and were used in the algorithm for determination of the migration path for each application workload:

Windows (32- and 64-bit)

Microsoft Windows Server 2003 (Standard, Datacenter, Enterprise) with Service Pack 1 (SP1) or later (32- and 64-bit)

Microsoft Windows Server 2003 R2 (Standard, Datacenter, Enterprise) (32- and 64-bit)

Microsoft Windows Server 2008 (Standard, Datacenter, Enterprise) (32- and 64-bit)

Microsoft Windows Server 2008 R2 (Standard, Datacenter, Enterprise) (64-bit only)

Microsoft Windows Server 2012 (Standard, Datacenter) (64-bit only)

Microsoft Windows Server 2012 R2 (Standard, Datacenter) (64-bit only)

Microsoft Windows Server 2016 (Standard, Datacenter) (64-bit only)

Microsoft Windows 7 (Professional, Enterprise, Ultimate) (US English) (32- and 64-bit)

Microsoft Windows 8 (Professional, Enterprise) (US English) (32- and 64-bit)

Microsoft Windows 8.1 (Professional, Enterprise) (US English) (64-bit only)

Microsoft Windows 10 (Home, Professional, Enterprise, Education) (US English) (64-bit only)

Linux/Unix (64-bit)

Ubuntu 12.04, 12.10, 13.04, 13.10, 14.04, 14.10, 15.04, 16.04, 16.10

Red Hat Enterprise Linux (RHEL) 5.1-5.11, 6.1-6.9, 7.0-7.3 (6.0 lacks required drivers)

SUSE Linux Enterprise Server 11 with Service Pack 1 and kernel 2.6.32.12-0.7

SUSE Linux Enterprise Server 11 with Service Pack 2 and kernel 3.0.13-0.27

SUSE Linux Enterprise Server 11 with Service Pack 3 and kernel 3.0.76-0.11, 3.0.101-0.8, or 3.0.101-0.15

SUSE Linux Enterprise Server 11 with Service Pack 4 and kernel 3.0.101-63

SUSE Linux Enterprise Server 12 with kernel 3.12.28-4

SUSE Linux Enterprise Server 12 with Service Pack 1 and kernel 3.12.49-11

CentOS 5.1-5.11, 6.1-6.6, 7.0-7.2 (6.0 lacks required drivers)

Debian 6.0.0-6.0.8, 7.0.0-7.8.0, 8.0.0

Oracle Linux 6.1-6.6, 7.0-7.1

Fedora Server 19-21

Application Workload Migration Patterns

|  |  |
| --- | --- |
| **Migration Pattern** | **Guideline** |
| Retain | No change to the current application. Decision made by customer based on future business plans and/or dependencies. Examples of these include non-supported applications such as mainframes or applications that have dependencies to physical environments (i.e.: Telco lines terminating in particular locations) |
| Retire | Part of rationalization effort. Application is no longer seen as demonstrating adequate business value or will be replaced by Saas offering. Costs here relate to the process of decommission an asset in the enterprise and the communication and coordination that comes with that effort. Examples of these include outdated platforms/applications or workloads that can run natively in AWS (managed database offerings, SQS, Mobile Push, etc...) |
| Re-host | Very small amount of data associated with this application / workload. Low number of dependencies, this workload / app was used in silo or a very small number of user group for a very specific functionality. Basic technical requirements such as a standard server running one workload (i.e.: terminal server, jump box, single team uses a COTS app installed on it, etc...). No change in architecture or performance requirements. Typical re-hosting application examples or LAMP stacks or single-tenant workloads. |
| Re-platform | Upgrade/change the OS version or migrate to AWS managed services. Examples would be unsupported/EOL platforms (Windows 2000, 2003, AIX). |
| Re-architect | Modify various components of the application to take advantage of AWS services (i.e.: Elasticache, S3, EBS, etc…). The distinction here with re-factoring is that you make changes to certain settings or configuration files not necessarily overhaul the underlying application code. Examples of these would be adding a caching layer or database read replicas to improve the availability and performance of the application queries. |
| Re-factor | Re-write, modify, or decouple pieces of the application. The functionality remains unchanged for the most part but the inner workings operate differently to leverage the elastic nature of the cloud. Example of this could be having the application switch from using MQTT on-premises to SQS in AWS or re-rewriting application code to integrate with DynamoDB or SQS. |

Application Migration Tools

|  |  |
| --- | --- |
| **Migration Tool** | **Description** |
| VM Import/Export | VM Import/Export enables you to easily import virtual machine images from your existing environment to Amazon EC2 instances and export them back to your on-premises environment. This offering allows you to leverage your existing investments in the virtual machines that you have built to meet your IT security, configuration management, and compliance requirements by bringing those virtual machines into Amazon EC2 as ready-to-use instances. You can also export imported instances back to your on-premises virtualization infrastructure, allowing you to deploy workloads across your IT infrastructure.  Use cases:  Suitable as a fallback when live migration tools such as CloudEndure do not work. Also suitable for development workloads in order to reduce costs by buying less 3rd party migration licenses. |
| AWS Server Migration Service | AWS Server Migration Service (SMS) is an agentless service which makes it easier and faster for you to migrate thousands of on-premises workloads to AWS. AWS SMS allows you to automate, schedule, and track incremental replications of live server volumes, making it easier for you to coordinate large-scale server migrations.  Use cases:  For production workloads that have hypervisor level access (FTServices) |
| CloudEndure | CloudEndure enables organizations to migrate even the most complex workloads to the Amazon Web Services (AWS) Cloud without downtime, disruption, or data loss. Through continuous, block-level replication, automated machine conversion, and application stack orchestration, CloudEndure simplifies the migration process and reduces the potential for human error. Whether you are migrating to or across AWS, CloudEndure Live Migration gives you the flexibility and security you need to succeed in today’s fast-paced digital ecosystem.  Use cases:  For production workloads that do not have hypervisor level access (Rackspace). |

Applications Profiled during migration assessment

Aecom, AWS and IBM met with the respective application owners to do a deep-dive on the business critical and complex applications being hosted in FTServices, Rackspace and Azure. Below are the key findings and recommendations for each application.

Application: Sharepoint 2013 and 2010 (Rackspace)

App Owners:

Samir Dobrik

Chris Luton – IT Manager

Sharepoint 2013

Single 2013 Production farm

10 servers for Sharepoint 2013

3 Web servers with 2 F5s sitting in front using round robin)

200 FQDNs point to the same VIP

3 app servers (clustered at the application level). Sharepoint has it’s own native load-balancing

01 and 02 are the core servers, 04 has some core services as well as search and indexing functions

Databases are on 2 separate servers

Sps02 (hosts content databases for Sharepoint)

Sps01 (reporting services, config databases, service bus)

No replication is happening between the databases

1 OWA (Office Web Access – view Word or Excel in the web browser)

10,000 accounts in Okta; > 4000 users

Okta has integration into Sharepoint

Sharepoint 2010

Sharepoint 2010 is 100% AD authentication

2 web and 1 DB server

Risks

No known risks

Recommendation

Re-platform in AWS by building new servers and migrating the content databases. The application has too many interdependencies to migrate using a cloning strategy.

Application: Geographic Information System and Portal (Rackspace)

App Owners:

Jerry Welmaker - DBA cloud env sql and oracle, external facing sites for clients

Joseph Weyl - manages GIS servers and ESRI technology

GIS Production environment

3 web Windows IIS servers.

Certificates are bound on the web server

Web adapter has internal load balancer

All 3 servers proxy connect back to GIS over a certain port

2 add-on products each have a web adapter

Geocore text (HTML5 JS viewer)

Cartopac – mobile data collection, offline data collection. Login to site to go to project, take offline to take field data connection.

GIS servers (4 machines, 3 app server renders image)

Each has OS and data drive

Fileshare consists of OS and data drive

Database server tier consists of a single database

Drives are broken into MDF/LDF

Citrix environment hooks into this

Communicates with Portal at a high level

Risks

No known risks

Recommendation

Re-platform using ESRI CloudBuilder

Portal

6 machines

For Aecom staff to use. Collect field data and send back.

Risks

No known risks

Recommendation

Re-host by cloning current Portal machines



Application: Projectwise (Rackspace)

App Owners:

Kevin Albright – team leader

Carl Brock – Developer

Kestutis Gircys

Projectwise (Global collaboration tool for engineering) Production Environment:

5 hub datacenters around the world, 7 in the cloud

Each datacenter is identical

Rackspace hosts the North American hub

A tool called Project hub maintains an inventory of server names

Server architecture

Integration server (traffic cop)

Database (acts as the backbone)

File server (provides file shares)

Web gateway (4 main servers)

Uses aecomnet.com internal AD domain

All other components are hosted in Azure (Bentley Cloud)

Does not leverage load balancing (F5s)

Risks:

Gordy Howell is a 3 billion dollar project (project hosted in Projectwise) that cannot afford any downtime or changes in configuration

Server names cannot change (IP changes might be possible)

Go-live resync could potentially affect 500 people working on the project

Any server name changes would require 200 proxies to be changed

Recommendation:

Projectwise was not migrated to the Bentley cloud due to the risks stated above, a full evaluation of the business impact needs to be assessed before any migrations are to take place.

Application: Cityworks (Rackspace)

Cityworks Production Environment:

5 Cityworks servers (VMs) each one serves a different client

Each client is distinct 3rd party

Client (Honolulu) connects to SQL servers

Client is using local storage. Stores a location in c:\temp\image.jpeg

Windows server with IIS (Web)

F5 handles SSL offloading

Cityworks is mostly the same version

Designated file store

Dependencies:

Cityworks has API calls, need to validate API calls will work in new location

Clients connect into Rackspace using an IPSec tunnel

Clients connect using Citrix

Cityworks talks to ArcGis for large attachments

Recommendation:

Migrate using a re-host cloning strategy if possible since each server hosts a distinct client

Application: AQM Apps (Rackspace)

App Owners:

1. Patrick Edwards

AQM Apps displays air monitoring data:

AQM Production Environment:

1. Web/App server – stores images < 500 GB

Oracle 11 is the app server

F5 -> ssl certs -> web server

Apache is written in mod plsql an Oracle embedded programming language

1. Database server is shared with Guy Browning app

Reads are occasional, writes are constant due to replication

SQLnet replicates data from Denver datacenter to this database

Database is internal only

Plsql is stored on the DB

Application: TaaS, TaaS-DevTest, Internal-NPS-Digital, TaaS-DFAT, ThoughtLeadership, eTimeTrack (Azure)

App Owner:

1. Andrew Frasier

Results:

There was a resistance migrating to AWS from the application owner due to his challenges with AWS in the past.

Recommendation:

Due to the complexity of re-platforming from Azure to AWS servers and multiple interdependencies and possible code and deployment changes, we will need to do a deeper dive into the applications along with full support of the application owner.

Application: aecomservices, aecomservicesdev, aecomservicestest (Azure)

App Owner:

1. Marta Muszynska

Subscriptions:

1. Scoe-01
2. Scoe-01-msdn-devtest

Recommendation:

These subscriptions will need a follow up interview with the developers to determine a refined level of effort estimate based on reviewing the code and possible code changes. The complexity of this migration will be difficult because of the number of integrated Azure services involved.

AWS Pilot

The key outcome of the AWS pilot was to demonstrate to the Aecom team about the viability of migrating their workloads into AWS from their different datacenters. As part of the pilot, we also leveraged different migration tools in order to migrate the workloads. Those migration tools included VM Import/Export, AWS Server Migration Service, CloudEndure, and re-platforming.

Azure Migration

We leveraged CloudEndure to install an agent on an Azure VM in order to migrate into AWS. Once the server was migrated, Timothy Fitzgerald logged into the VM and ran functionality and UAT tests.

FTServices Migration

For FTServices we leveraged the native AWS Server Migration Service (SMS) in order to migrate the VMs. We first created the required Roles within AWS to run the service and then installed the SMS ova agent on the FTServices VCenter. After the services were brought up we selected the appropriate VMs to migrate into AWS. Two applications were successfully migrated into AWS. The first is an FTP server which included the FTP server itself as well as a gateway. After the migration was successful, Ken Wong from the FTS team needed to make configuration changes on the server in order to have full functionality. The second server was a self-service tool. After logging into the sel-service tool successfully, Ken was able to make a change in the console of the tool and the change was propagated to the FTS Active Directory servers.

Below is a screenshot of the FTP server seen from the gateway.

FTP Server from the internet

Rackspace Migration

The migration from Rackspace to AWS involved using the AWS VM Import/Export and CloudEndure tools.

The first app migrated was ArcGis by doing a re-platform and a clean server build. Joe Weyl from the ArcGis team was able to install the application on top of the brand new OSes. Later on, the ArcGis database was migrated to the server for functionality tests.

Below is a screenshot of a successful functionality test for ArcGis.

The second app migrated from Rackspace was Oracle Contract Management. We initially tried to migrate this app using CloudEndure but the transfer rate was slow (1 MB/sec) for some unknown reason. We then decided to migrate the app using VM Import/Export instead.

After the app was migrated we validated its functionality as seen below.

The GoodSync server was the last app that was migrated from Rackspace. We used CloudEndure to migrate this app successfully.

Project Plan

Migration Approach and Plan

In general, the overall approach that AWS prefers to take when enabling mass migrations is shown below.

This assessment covers some of the aspects of the Planning at a high level. On-going discovery and assessment is a hallmark of the planning phase.

Work is divided into time-boxed segments called sprints (also known as iterations) with specific outcomes. This short-term focus allows within a longer term plan allows for focused work to be completed without interruption. A sprint can be of any length but is typically two weeks in a migration effort.

For a successful mass migration, efficient execution is imperative in order keeping the migration time to a minimum to manage costs and risks. In order to do this, it is equally important to design and plan ahead of the migration. This is shown above in the Plan, Activate and Execute steps, although the planning and activation can normally take place with some overlap.

Recovery Plan

An oft-overlooked but significant part of the migration planning process is preparation of recovery/rollback strategy to mitigate risk if the migration process or application workload go-live execution encounters problems. If there is a problem during the go-live event, or if the process is taking longer than the go-live event window allows, the ability to execute a full recovery is critical. This is even more critical if a given application workload has an existing SLA with customers limiting downtime – this is a time when a recovery plan can help prevent costly business disruptions.

Recovery plans require a complete picture of the application workload including upstream and downstream dependencies, databases, networking, SLAs, disaster recovery plans etc. Therefore, a recovery plan requires an in-depth understanding of the application gathered during the discovery phase and is developed for each application workload separately.

Application workload migration recovery plans should include the following activities at a minimum:

1. Plan for notification of development and operations teams of rollback
2. Procedure for performing rollback database synchronization using backup, read-replica, or synchronization tool
3. Procedure for locking down new database to prevent changes and unlocking original on-premise database
4. Functional testing of the on-premises application workload for validation
5. Procedure for validating that all up & downstream dependencies have been properly rolled back to previous configuration
6. Procedure for updating DNS or configuration entries to point to on-premises application workload

Test Plan

The migration test plan is one of most important aspects of the overall migration strategy because it governs how each application workload is validated to function and perform in AWS, at a level equal or greater than the original infrastructure. Each application workload will require an individual test plan containing procedures for executing automated or manual functional, performance and user acceptance tests. Additionally, there will need to be validation of the AWS supporting infrastructure configuration required for the application to run properly in the cloud. Finally, the Business will need to sign-off that the application has been validated and is ready for production (go-live) status.

Application Workload Testing

When considering the migration test plan, it is important to note that an individual test plan and acceptance criteria should be drafted for each application workload. Ideally all application tests should be automated to facilitate an efficient testing feedback loop. Manual testing will significantly slow down the validation of the application and may delay application go-live. A comprehensive test plan should minimally contain the following:

**Functional Tests:** These tests exercise the functionality of the application(s). These typically include a combination of automated and manual tests.

**Performance Tests:** These test will assess performance under varying levels of load. This should be compared to results of performance tests taken in the legacy on premise environment.

**User Acceptance Tests:** These tests should be executed by the end users of the application(s) once the final data migration has completed.  The purpose of these tests is for the end users to decide if the application is sufficiently usable to meet it’s primary function in the organization.

AWS Environment Validation

The AWS environment should be validated to ensure the infrastructure is configured properly to support the application in operations. The following are examples of items that should be validated before approving operational readiness:

1. Primary/secondary failover
2. Availability Zone (AZ) independence
3. Backup and restore of application in AWS
4. Monitoring of the application in AWS
5. Security tools and compliance in the cloud

**Business Sign-off**

Before moving an application workload to operations, the sign-off acknowledges that all necessary testing has been completed and that the switch from on-premise to AWS can be completed.

Launch Plan

The migration Launch Plan describes the activities required to launch an application workload into full production status after it has migrated to AWS. Beginning with a Go/No-Go decision and notification of all support teams, the cutover to the application workload in AWS begins and traffic to the on-premise application workload is phased out. The application launch/go-live is typically a choreographed event, where a conference bridge is set up for technical discussions, every activity is monitored and views are set up to provide real-time status.

The Launch of a single or group of application workloads may involve tabletop exercise where all of the key stakeholders participate to ensure a complete buy-in and understanding about every detail of the launch event. In conjunction with Table Top exercises, the migration team will develop run-books that detail every step of the launch in an ordered procedure. The run-book may include procedures for shutdown/startup, application configuration instructions, test plans, and contingency plans if something goes wrong, with procedures for troubleshooting or rollback.

The following list common activities that should be detailed in a migration Launch Plan:

Prior to Launch

Business sign-off of UAT testing

Meeting with Stakeholders to review and confirm Launch Event

Review and approval of Recovery/Contingency Plans

Table Top Exercise #1 to describe approach, schedule and timing of events

Table Top Exercise #2 to discuss recovery plans, roles and team availability

Table Top Exercise #3 Runbook review

Confidence Reboots, DR and Failover testing

Confirm Go-live Readiness

Notify Aecom’s respective teams (if applicable)

Final Go/No-Go Decision

Launch

Perform final database synchronization using backup, read-replica, or synchronization tool

Lock old database from changes

Validate all upstream and downstream dependencies have been properly integrated

Change name resolution or configuration entries to point to the application workload in AWS

Re-validate functionality of the application in the cloud after name resolution changes have been made

Post Launch

Begin post launch support activities including service monitoring and management, security monitoring, patching etc.

Perform post migration review to collect lessons learned

Execute technical decommission activities and release original on premise resources

Ensure ownership and escalation channels are properly established

Update operations runbooks/playbooks for the newly migrated application

Operations Plan

Knowledge Transfer

The following key areas have been identified as needing immediate support and eventual knowledge transfer to the Aecom and IBM team.

1. CloudFormation
2. Security in AWS
3. Network performance in AWS

Cost Optimisation

Following completion of the Migration Project, AWS will work with Aecom to optimise costs. Techniques that can be applied include leveraging reserved instances wherever possible, shutting down un-used servers (example of shutting down test servers over weekends) and leveraging automation to ensure server shutdowns and restarts happen seamlessly and at the appropriate times.

AWS Architecture

AWS Accounts

Based on the information provided in the migration assessment, a decision needs to be made around the way the workloads will be organized within AWS. Based on our preliminary analysis we recommend the following 5 AWS accounts:

1. Master Billing Account – Payer account for consolidated billing
2. Production Internal Operations Account – Main production account that will house FTServices, Azure Cloud and traditional data center workloads
3. Extranet Account – Client facing account that will house most workloads from Rackspace. It will also be used for projects and workloads that are mostly client facing
4. Self Service Account – Will be used for single-click self-service applications/servers
5. Logging Account – Account where the logs from all other accounts will be aggregated

DirectConnect

Aecom will utilize AWS DirectConnect for connectivity into the AWS region being used for the Migration Project.

Below is an architectural diagram representing the AWS account structure as well as the DirectConnect(DX) connection points into AWS. An IPSec VPN could be setup for the DirectConnect as a redundant link in case the DX fails.

Production Internal Operations Account and Extranet Account VPC Design

On the basis that Aecom accept the recommendation for the account set out in the AWS Accounts section, the proposed high-level VPC design is as follows:

1. A ‘shared infrastructure’ VPC containing any shared services across all workloads (e.g. AD/DNS, SSO, monitoring, logging)
2. A Development and Production VPC containing their respective workloads
3. Configured so that no two VPC’s share the same network ranges
4. Ability to cross-link VPC’s using VPC Peering if required at a later date
5. Shared infrastructure VPC will be peered with the Development and Production VPCs
6. Each VPC to be organized into subnets tiers to support:
   1. Public Subnet Tier
      1. DMZ Subnet – connects to the Internet Gateway (IGW) and thereby the internet.
   2. Private Subnet Tiers
      1. Management Tier – used for in-band management for devices such as the F5s and virtual firewalls
      2. Web Tier – used for web servers
      3. App Tier – used for application and file servers
      4. Database Tier – used for database servers and Relational Database Service (RDS)
7. Each VPC will be architected to use multiple availability zones (Multi-AZ)
8. Configuration of a virtual firewall in each VPC (one per public subnet for resilience) to provide outbound connectivity to the internet.

Below is an architectural diagram of the Production Internal Operations Account

Security

The security design is based off of AWS best practices which is captured within the [NIST Compliance on AWS Quick Start](https://aws.amazon.com/quickstart/architecture/accelerator-nist/). The VPC and security components herein are an adaptation of the NIST Quick Start along with specific Aecom requirements. The [security controls matrix](https://s3.amazonaws.com/quickstart-reference/enterprise-accelerator/nist/latest/assets/NIST-800-53-Security-Controls-Mapping.xlsx) (Microsoft Excel spreadsheet) shows how the Quick Start components map to NIST, TIC, and DoD Cloud SRG security requirements.

NACLs

Network Access Control Lists (NACL’s) will be used to control egress and ingress of traffic. One design principle could be to allow traffic amongst all the public and private subnets. This will mean that all the traffic passing between tiers such as from DMZ to Web, or from App to DB, will need to pass through a virtual firewall. In other words, east-west traffic between tiers will pass through a virtual firewall.

Below is an architectural diagram of the network ACLs. Each subnet will have its own NACL.

Security Groups

We will create 4 “layers” or types of security groups, 3 main and 1 ad-hoc for support purposes.  When auditing each instance and workload, each layer would be analyzed to create the final group set for the instance.

Management - This layer will be designed to allow communication to a common core system used for IT management and other control plane functions. Examples are AD/DNS, Monitoring systems, RDP and SSH. Most if not all instances will have this layer applied.

Common - This layer will be a common sets of ports respective to application tiers and allows for easy application for common services.  Examples would be HTTP/HTTPS, FTP, etc.

App - This layer will be specific to the application stacks and will be used for communication primarily between application servers, but also to allow external access to machines on custom ports.

Support - This layer will be used for support and triage events.

CloudFormation

It is recommended that CloudFormation scripts be used to create the aforementioned AWS components. Those components include but are not limited to:

VPCs, Subnets, NACLs, Security Groups

AWS Cloudtrail, VPC Flow Logs, AWS Config, CloudWatch Logs, Archive Logs, S3 Lifecycle policies

Firewall and load balancing appliances

IAM accounts and instance profiles

Appendices

Appendix I: Application Characteristics Matrix