Architecture for ECA Migration to Azure

For Electrical Contractors Association

Commercial in Confidence

**Version –** 0.12

**Issue -** Released

**Author -** Nigel Wardle

**Date -** 11/07/2019

**Copyright -** Ultima 2018

Table of Contents

[1.0 Document Control 3](#_Toc519517885)

[1.1 Authority 3](#_Toc519517886)

[1.2 Identity 3](#_Toc519517887)

[1.3 Revision History 3](#_Toc519517888)

[1.4 Distribution List 3](#_Toc519517889)

[1.5 Principal Contact 3](#_Toc519517890)

[2.0 Document Conventions 5](#_Toc519517891)

[2.1 Glossary of Terms 5](#_Toc519517892)

[3.0 Introduction 6](#_Toc519517893)

[3.1 Summary 6](#_Toc519517894)

[3.2 Requirements 6](#_Toc519517895)

[3.3 Constraints 6](#_Toc519517896)

[3.4 On-going Projects 6](#_Toc519517897)

[4.0 Services 7](#_Toc519517898)

[4.1 ECA 7](#_Toc519517899)

[4.2 Policy and SLA 7](#_Toc519517900)

[4.3 Legacy 8](#_Toc519517901)

[5.0 Azure Technology 10](#_Toc519517902)

[6.0 Azure Architecture 13](#_Toc519517903)

[6.1 Kentico 13](#_Toc519517904)

[6.2 Kentico App Plan 14](#_Toc519517905)

[6.3 Kentico Media Storage 14](#_Toc519517906)

[6.4 Member App Plan 14](#_Toc519517907)

[6.5 Member App .NET Version 14](#_Toc519517908)

[6.6 Session State 14](#_Toc519517909)

[6.7 Claims based authentication 14](#_Toc519517910)

[6.8 Watchdog 16](#_Toc519517911)

[6.9 File Archive 18](#_Toc519517912)

[6.10 Environments 19](#_Toc519517913)

[6.11 RBAC 19](#_Toc519517914)

[6.12 xxs 20](#_Toc519517915)

# Document Control

## Authority

|  |  |  |  |
| --- | --- | --- | --- |
| Signatory | Name | Role | Organisation |
| Technical Authority | Nigel Wardle | Senior Technical Consultant | Ultima |
| Reviewer | John Duffield | Project Manager | Ultima Business Solutions |

## Identity

|  |  |
| --- | --- |
| Issue Type | Draft |
| Date Issued | 11/07/2018 |
| Title | Architecture for ECA Migration to Azure |
| File Name | Architecture for ECA Migration to Azure.docx |

## Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Status | Comment |
| 0.12 | 11/07/2018 | Draft | Issued |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## Distribution List

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Role | Company | Email Address |
| Steven Hall | Group Head of Information Systems | ECA | Steven.Hall@eca.co.uk |
| Alaric Turner | Network Manager | ECA | Alaric.Turner@eca.co.uk |
| Kurt Malmstrom |  | ECA | Kurt.Malmstrom@eca.co.uk |
| Tony Hopkins |  | ECA | Tony.Hopkins@eca.co.uk |
| Jason Grant | Development | ECA | Jason.Grant@eca.co.uk |
| Paul OShea |  | ECA | Paul.OShea@eca.co.uk |
| Chris Kirk | Senior Technical Consultant | Ultima Business Solutions | Chris.Kirk@ultima.com |
| Tom Hennell | Account Director | Ultima Business Solutions | Tom.hennell@ultima.com |

## Principal Contact

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Tom Hennell | Telephone | +44 333 0158452 |
| Role | Account Director | Email | Tom.hennell@ultima.com |
| Address | Gainsborough House, Manor Park, Basingstoke Road, Reading, Berkshire, RG2 0NA | | |
|  |  | | |

# Document Conventions

Each section in the document will contain a table such as the following, explaining why we made our recommendations. This is followed by general information about the subject to ensure you understood our thinking.

|  |  |
| --- | --- |
|  | Decision  This symbol indicates a decision has been made and what it is. The following text will also provide the rationale regarding that decision. |

|  |  |
| --- | --- |
|  | Decision TBC  This symbol indicates a design decision has yet to be confirmed |

|  |  |
| --- | --- |
|  | Important Information Follows  This symbol indicates that valuable information will follow, and special note should be taken. This might be a pre-requisite that is required for the design component. |

|  |  |
| --- | --- |
|  | **Ultima Recommendation**  Ultima recommends that you use X technology to fulfil this requirement |
| **Why we made this recommendation for your environment**  We made this decision based on your requirement for X. This is fulfilled by this in the following way… |
|  | **Why we discounted other solutions**  Alternative solution X was discounted because… |
|  | **Alternatives we didn’t discount**  Although not a direct recommendation, the following solutions would also meet your requirements. Our overall recommendation considers the whole environment for the most efficient solution. Some of these may meet this specific need better but be worse overall.  Solution 1 – This solution would meet needs better here but is less efficient overall…  Solution 2 – This solution would also meet this need but not others in the environment and so would be a point solution |

## Glossary of Terms

We may use the following terms in this document and will not explain them each time so have included them here for your reference.

|  |  |  |  |
| --- | --- | --- | --- |
| Term | Description | Term | Description |
| PaaS | Platform as a Service | IaaS | Infrastructure as a Service |
| SaaS | Software as a Service | HA | Highly Available |
| Scale Up | Increase the size of nodes to increase scale | Scale Out | Add nodes to increase scale |
| IoT | Internet of Things | VM | Virtual Machine |

# Introduction

## Summary

The section below provides a high level, version of the requirement as provided by the Client.

Electrical Contractors Association (ECA) have traditionally been a ‘working hours’ organisation. Due to recent technical and operational issues encountered, consideration of a resilient cloud adoption with 24/7 management has been accelerated. ECA host several internally and externally facing line of business websites and applications with shared SQL backends. ECA are particularly interested in re-working these sites and applications to utilise Azure’s PaaS offerings. Applications that cannot initially take a PaaS transformation are being considered to remain on premise until a PaaS solution becomes possible and sufficient resourcing becomes available.

## Finance

A move to Azure will initiate a change from a CapEx model to one of OpEx. The OpEx model of the cloud demands that a monthly, quarterly or yearly bill is paid based on the usage throughout that period. If the bill goes unpaid then the service stops and worst case data and servers are removed from the service. From another perspective, however, generally usage is based on how busy your business is and so the more you have used, the more revenue will have been generated to cover those costs.

## Requirements

The following known requirements were captured. These are things which are planned but may not currently be a part of the solution.

* To demonstrate resilience and scalability and so be better able to pursue new business opportunities
* Urgent desire to improve availability and reduce outages
* Restructure of resources
* Re-architecting websites and applications to fit a PaaS solution
* Re-working of on premise workloads to integrate with PaaS solutions until workloads can in turn be moved to PaaS
* Reliable connectivity to the Azure environment is required as some sites used internally have a high impact if offline
* 24/7 managed service of Azure environment

## Constraints

The following is a list of constraints which may affect the solution going forward:

* On premise SQL connectivity to SQL Azure

## On-going Projects

* Office365 POC

# Services

This section details the services within the scope of this engagement. For ECA, the details were captured during site meetings.

|  |  |
| --- | --- |
| Service Name | Description |
| ECS Card Manager/Rules Engine | Private website and/or Silverlight applications |
| Financial services | Private Silverlight application |
| SSRS | MS SQL Server Reporting Services |
| ECA Connect | Private internal website |
| Watchdog | Private Windows services |
| eca.co.uk | Public Kentico CMS version 9.0 |
| ecsexams.org.uk | Public Kentico CMS version 9.0 |
| Ecscard.org.uk | Public Kentico CMS version 9.0 |
| File archive | Copy Azure based data files to archive storage |

## ECA

## Policy and SLA

|  |  |
| --- | --- |
| Service Priority | This service is required by the business and there will be an immediate impact if the service is unavailable. The service must be online within a short timeframe.  No planned downtime is acceptable within the operating hours of this service. Unplanned downtime must be minimised. |
| Availability | 24x7 |
| Backup retention | There was no specific backup retention known for this service, and so initially a 30-day rolling backup will be used. |
| Archive requirements | File archive is included |
| Disaster Recovery | Required, but provided through high availability offered by multi region deployment |
| Compliance requirements | None |

### Connectivity

This section details the present topology of the service; including users, sites, servers and links.

|  |  |
| --- | --- |
| Role | Description of interaction |
| Public | Public access is required to the public web sites. |
| Company Users | Team access a different web interface to add and manage content. |
| Developers | Least privilege access is required by developers to update code. |
| Administrators | Access is currently required by administrators for managing the server estate. |

## Legacy

The current on premise systems include Silverlight technology. This will not be transferred to Azure but will remain active on-premise being eventually replaced by an HTML5 based solution. Silverlight connectivity to Azure SQL will require re-engineering. This could be achieved using SQL Logins.

|  |  |
| --- | --- |
| Site | Link type and bandwidth |
| Sevenoaks | -Mb |
| Swanley | -MB |
| Branch Offices | -Mb |

### Current Systems

This section details the current make-up of the service in terms of servers, hardware and software.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Product | Type | CPU | Memory | Operating System | Description |
| ECA Connect | VM | 2 | 6 | Windows Server 2012R2 | IIS Web Server, Silverlight |
| ECS Card | VM | 2 | 6 | Windows Server 2012R2 | IIS Web Server, Silverlight |
| Financial | VM | 2 | 6 | Windows Server 2012R2 | IIS Web Server, Silverlight |
| SSRS | VM | 4 | 8 | Windows Server 2012R2 | IIS Web Server |
| Watchdog | VM | 4? | 8? | Windows Server 2012R2 | Windows Service(s) |
| Eca.co.uk | VM | 2 | 6 | Windows Server 2012R2 | IIS Web Server – Kentico 11 |
| Ecscard.org.uk | VM | 2 | 6 | Windows Server 2012R2 | IIS Web Server – Kentico 11 |
| Ecsexams.org.uk | VM | 2 | 6 | Windows Server 2008R2 | IIS Web Server – Kentico 11 |

|  |  |
| --- | --- |
| Other Equipment (switches, load balancers, firewalls etc.) Name | Description of role in service |
|  |  |
|  |  |

# Azure Technology

### Accounts

|  |  |
| --- | --- |
|  | Important Information Follows  The ECA is currently is investigating EA or CSP agreements, accounts and subscriptions. A separate subscription for this new work is recommended for isolated billing. Within this subscription different Resource Groups should be created for each environment (Dev, UAT, Prod) and region. |

### VM

Azure Virtual machines can host an instance of MS Windows (or flavours of Linux) onto which additional applications such as IIS and SQL Server can be installed. A VM can be manually scaled up or down (increased or decreased in size). Other VMs can be pre-provisioned in advance and turned on or off either manually or using an Automation Account with a scheduled Runbook PowerShell script.

### Express Route

|  |  |
| --- | --- |
|  | Important Information Follows  The ECA is currently is investigating ExpressRoute as a way of connecting from on premise into Azure. |

### Web Apps

Web Apps provide a PaaS option in Azure. Single instance Web Apps meet the SLA by virtue of the Site Control Manager extension that can spin up another instance upon failure. Web Apps in Standard Tier can be configured for custom domain, auto-scaling, auto backup and IP address whitelisting. Unless a Web App is running in Premium tier (significantly more expensive currently) it will be provisioned on a public IP address. Azure Web Apps by default have ARR headers turned on maintaining session state (e.g. shopping basket) by directing requests back to the same server by cookie - if the web app is scaled out with multiple instances. An improved approach is to delegate session state management to a third-party store which means any Web App can service a request. In Azure Web Apps, this can be Redis Cache, SQL Server. Other non-supported stores include Table store or CosmosDB.

### Traffic Manager

Traffic Manager is a DNS based technology that supports load balancing and failover between application instances across multiple Azure datacentres and on-premise implementations. If a failover application is additionally provisioned in a separate location, then Traffic Manager can provide DNS services to route the traffic according by configuration and availability.

Deployment of the application to more than one regional datacentre can support high availability. Azure Traffic Manager set in Priority mode (Failover) can be used to direct browser traffic to the chosen primary European regional datacentre. Upon detection of non-availability, it will redirect traffic to the failover secondary European datacentre. The default time to live (TTL) of Traffic Manager profile may mean users not being re-directed to the failover for up to five minutes. The TTL can be decreased but it is a trade off against the frequency of DNS queries being made by the client resolver.

### Application Gateway

Azure Application Gateway is a dedicated service, offering various layer 7 load balancing capabilities. it is comprised of multiple worker instances for scalability and high availability. It allows customers to optimize web farm productivity by offloading CPU intensive SSL termination to the application gateway. It also provides other layer 7 routing capabilities including round robin distribution of incoming traffic, cookie-based session affinity, URL path-based routing, and the ability to host multiple websites behind a single Application Gateway. It provides a rich set of diagnostics and logging capabilities for better manageability. SSL certificates are hosted here.

### CDN

Azure CDN can be used for increased performance of delivery of static media files. This PaaS service caches static files in Edge Servers located geographically across the globe, including London. The CDN will forward traffic to the datacentre using Traffic Manager as the DNS resolver. A custom domain will be required on the CDN, e.g. a CNAME DNS record: eca.org --> eca.azureedge.net

|  |  |
| --- | --- |
|  | Important Information Follows  A CDN can be implemented to exceed the current on premise caching capabilities. Azure CDN can be implemented regardless of what web server is used. |

### Application Insights

Azure Application Insights monitors applications to help you detect and diagnose performance issues and exceptions. It works for the Web Apps feature of Azure App Service. Free to use.

### Logic App

A logic app is a PaaS option to execute a workflow of steps. Each step uses a connector to delegate work to. Connectors include SQL, Outlook, File etc. An example is a Logic app with an Outlook connector. An email can be sent as part of a workflow or just be the only step. Logic app includes a manual trigger -HTTP Post or a scheduled trigger. The customer is charged for execution of the logic app and for every step executed.

### Function app

Function apps accept code via the portal. This includes C#, JavaScript etc. It is an alternative to compiled code deployed from Visual Studio

### SQL Azure

SQL Azure delivers predictable performance at multiple service levels, dynamic scalability with no downtime, built-in business continuity, and data protection, all with near-zero administration. It additionally provides Geo-Replication supporting writable primary database and failover readable secondary databases. Performance can be configured from Basic through Standard, Premium to PremiumRS and changed without downtime. Scaling units are measured in DTUs. Full database backups occur weekly, differentials every few hours and logs every ten minutes. For standard tier, backups are retained for 35 days.

### SQL Azure Elastic Pool

SQL Database elastic pools are a simple, cost-effective solution for managing and scaling multiple databases that have varying and unpredictable usage demands. The databases in an elastic pool are on a single Azure SQL Database server and share a set number of resources at a set price. Cost savings can be made if the ECA organisation is running many databases.

### SQL Azure DTU verses vCore

Previously MS used the DTU for scaling/pricing where if high storage was required a corresponding high-performing tier had to be chosen which impacted cost. MS have recently added in Preview vCore that makes it easier to scale CPU and Storage separately, also making it easier to make like for like comparisons with on premise SQL Server.

### Backup

In Standard Mode Tier, Azure Web Apps support backup to Blob Store by default.

For IaaS virtual machines, web applications should be configured to use Azure backup to the Azure Backup vault.

### Redis Cache

Redis Cache can be integrated into Azure Web Apps for both session state and general data caching

### Azure Search

Azure search can be integrated with Azure Web Apps content and SQL content as part of Kentico

### RBAC/AAD

Role Based Access Control (RBAC) will need to be setup for an Azure migration. This grants administrators, developers and other personnel access to the Azure components typically through the Azure Portal through AD group membership that is linked to an Azure role.

|  |  |
| --- | --- |
|  | Important Information Follows  Load testing must not be performed in any applications hosted in the Production App Plan as this will reduce resources available to Prod as throttling is applied when reaching the limits of the tier/performance level of the App Plan. |

# Azure Architecture

## Kentico

There will be two separate instances of Kentico version 11.



## Kentico App Plan

Each Kentico instance can have its own app plan – providing independent setting of both Tier and Performance level. Alternately a shared App Plan can be used for both instances – per environment. A shared app plan will provide cost savings but flexibility. Initially an App Plan of Standard S3 is expected (4 core, 7GB RAM).

## Kentico Media Storage

Kentico 9 supports blob-based storage. Kentico recommend blob-based storage for Media files only.

## Member App Plan

Each member app instance e.g. eca.co.uk, can have its own app plan – providing independent setting of both Tier and Performance level. Alternately a shared App Plan can be used for instances – per environment. A shared app plan will provide cost savings but flexibility. Initially an App Plan of Standard S3 is expected (4 core, 7GB RAM).

## Member App .NET Version

|  |  |
| --- | --- |
|  | Important Information Follows  Microsoft is moving towards container-based deployments. Initially this was Docker but more recently a push for Kubernetes. It is unclear whether there will be a future container dependency on .NET Core. Therefore, it is strongly recommended that ASP.NET Core be used for any green field or re-engineering of web applications. It is assumed that newer versions of Kentico will include support for ASP.NET Core |

## Session State

Microsoft currently recommends scale out of resources in preference to scale up. To support scale out, out of process Session State management is a requirement for Kentico. Microsoft currently supports Redis and SQL Azure for session state. If incorporated this should additionally support operational automated scale up/down. Non Kentico web apps, e.g. member applications, can also benefit from out of proc by having improved load balance by switching off ARR.

## Claims based authentication

From version 9, Kentico supports claims-based authentication. If configured, when a user requires authentication, she is redirected to a 3rd party identity provider (OAuth2) login page. The current Kentico 9 documentation refers to Azure Active Directory Federation Services as an identity provider. When implemented, ADFS provides a proxy which can indirectly authenticate users against on premise AD accounts, however it is not a viable solution to add ECA members to on-premise AD. AAD B2C, if supported, is potentially a much better solution as an identity provider. AAD B2C supports delegated authentication to consumer accounts held at Microsoft (Hotmail, live & Office 365) as well as Google, Facebook, LinkedIn etc. AAD B2C keeps a record of all authenticated users but not passwords. Premium options include authentication auditing. AAD B2C charges only apply on a sliding scale above 50K accounts and 50K authentications per month. A staff member of ECA when authenticating to B2C will actually be authenticated by account in local AAD.



|  |  |
| --- | --- |
|  | Important Information Follows  Current payment options include PAYG, CSP and EA. Not all technologies are supported for all options. As of writing Azure B2C is not currently supported for CSP but is on the roadmap. |

### SQL Azure

SQL Azure database supports DTU and vCore pricing. vCore pricing is in preview but is a definite improvement and recommended.

Depending on the number of ECA databases and the overlap of required resources on an hour by hour basis it may be more cost effective to configure an Elastic Database Pool. SQL Databases will need cleansing and use BacPac formats to deploy.



## Multi Region

The Kentico and internal app services in the primary region can be deployed as duplication into a separate region. All persistent data will require replication between regions. SQL Geo Replication can be used to copy data from the primary region into the secondary. In normal operation data access to SQL from both regions will be to the primary region SQL. Upon failure of the primary region the secondary app services can be pointed to the secondary SQL.

## Traffic Manager

Multiple Traffic Manager (TM) profiles can be setup to load balance between App Services in the different regions. TM supports various schemes for routing of traffic via DNS but all schemes provide failover support for network traffic.

## CDN

ECA may choose to implement CDN for static files for improved performance particularly for Kentico media files.

## Watchdog

The current watchdog provides multiple services that access file, SQL and email services. There are two approaches to moving to the cloud. Serverless cloud based or a more coding approach. Each has its merits and downsides

### Watchdog option 1

A piece of watchdog functionality can be implemented using a serverless (no App Plan) Logic App, only paying per execution and for each step. Logic Apps can be configured with connectors to build quite complicated workflows. More functionality can be provided by Function Apps – but these are not serverless and require an App Plan. Logic Apps can also leverage WebApi code hosted in Azure API Apps



### Watchdog option 2

Each required service can be re-engineered from original code, re-written as new code, exposed as a set of stateless operations in an API and deployed to an Azure API App. Optionally the APIs can be managed by Azure API Management.



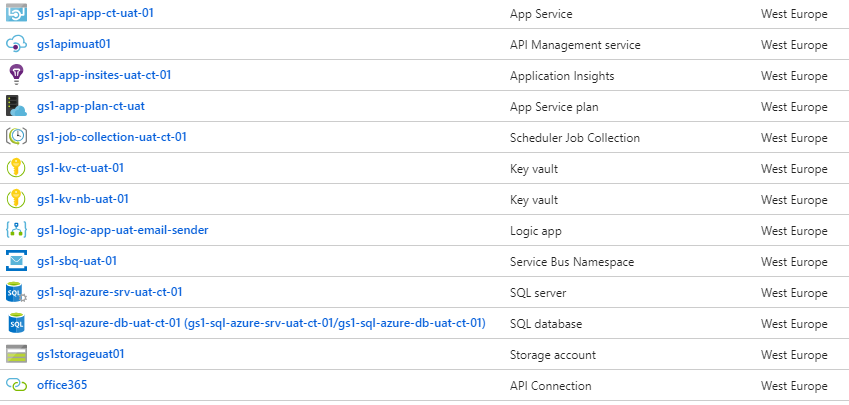
|  |  |  |
| --- | --- | --- |
|  | Logic App | API App |
| For | Very flexible deployment | Visual Studio Debug support |
|  | Easily changed without code upload if used with Function Apps | Migration of old code makes dev easier |
|  | Pay per execution and for each step | Source control easy |
|  | Can be developed in VS and kept under source control | App Service slots |
|  |  |  |
| Against | Difficult to debug | Even minor changes require re-deployment of code |
|  | Steep learning curve for Logic App and Connectors | 24 hours a day charge |
|  | Polling option can be expensive |  |
|  | No code swap facility |  |

## File Archive



## Environments

Its is very common to configure at least three separate environments within Azure PaaS. These include Dev UAT and Prod/PreProd. This is in addition to separate applications that may require their own resource group. Each environment is typically configured in a separate resource group with either multiple or shared App Plans – if App Services are used. For Web Apps it is normal to use a PreProd slot which can be swapped with the default Prod slot as part of deployment. Below is an example of a UAT environment.



## RBAC

ECA staff will require granular access to Azure base resources. Role Based Access Control can provide this functionality. Typically, the roles (which include: Owner, Contributor and Reader) are applied at the resource group level.

## xxs