Architecture for ECA Migration to Azure

For Electrical Contractors Association

Commercial in Confidence

**Version –** 0.11

**Issue -** Released

**Author -** Nigel Wardle

**Date -** 11/07/2019

**Copyright -** Ultima 2018

Table of Contents

[1.0 Document Control 3](#_Toc519082591)

[1.1 Authority 3](#_Toc519082592)

[1.2 Identity 3](#_Toc519082593)

[1.3 Revision History 3](#_Toc519082594)

[1.4 Client Distribution List 3](#_Toc519082595)

[1.5 Principal Contact 4](#_Toc519082596)

[2.0 Executive Summary 5](#_Toc519082597)

[2.1 Requirement Summary 5](#_Toc519082598)

[2.2 The Current Environment 6](#_Toc519082599)

[2.3 Solution Overview 7](#_Toc519082600)

# 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 | Released |
| 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 |
| 0.1 | 11/07/2018 | Released | 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.

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

|  |  |
| --- | --- |
|  | Design 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, baselined 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 take a PaaS transformation approach are being considered for an IaaS migration or extension to the cloud.

## 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 is preferred
* Utilising IaaS VMs for workloads that cannot be migrated to PaaS is considered
* 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:

* Unknown

## 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.  Recovery would be required following a service affecting disaster such as building loss. |
| 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 | No specific archiving requirements were known at the time of the workshop. Long term retention may be required for this site for legal purposes to ensure that content on a given day can be shown when required. It is believed that the database itself holds this information, however, and so further archives will not be kept. |
| Disaster Recovery | Required. |
| 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. |

|  |  |
| --- | --- |
| Site | Link type and bandwidth |
| Sevenoaks | xMb |
| yy | 500Mb |

### Current Systems

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

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Server Name | Type | CPU | Memory | Operating System | Description including software and role |
|  | VM | 4 | 12 | Windows Server | IIS Web Server |
|  | Physical | 32 | 128 | Windows Server | SQL Server |

|  |  |
| --- | --- |
| Other Equipment (switches, load balancers, firewalls etc.) Name | Description of role in service |
| SteelApp | Load Balancer |
| Checkpoint | Firewall |

# 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.

|  |  |
| --- | --- |
|  | Important Information Follows  To meet SLAs of 99.95% uptime there must be a minimum of 2 VMs as a load balanced pair in an availability set to meet the fault and update domain requirements. |

### Web Apps

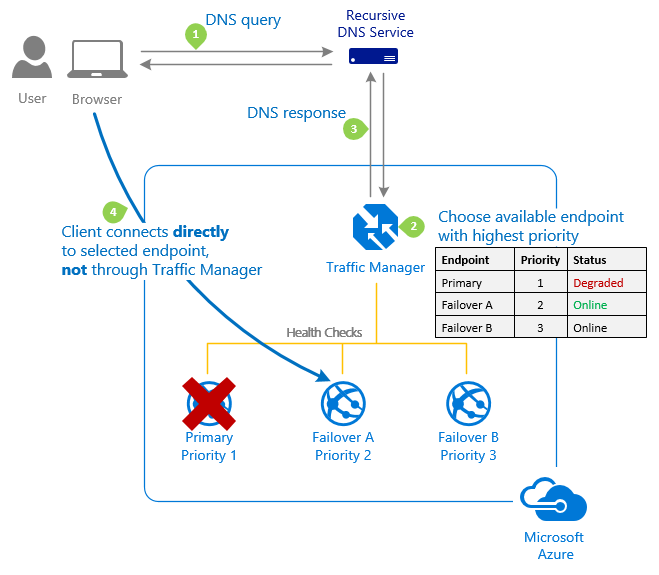
Web Apps provide a PaaS option in Azure. Single instance Web Apps meet the SLA by virtue of the Site Control Manager extension that can spin up another instance upon failure. Web Apps in Standard Tier can be configured for custom domain, auto-scaling, auto backup and IP address whitelisting. Unless a 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, 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 each and 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.

### 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 non-production 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. |

### Private Internal Applications

#### ECA Connect

A Microsoft ASP.NET MVC website. Users are currently authenticated using on-premise Active Directory (AD) Windows login. Connectivity to MS SQL Server is through an AD trusted login mapped to SQL Roles. There is currently tight coupling between the trusted login and local auditing. User generated files are stored in the local web server file system or network accessible locations. Current specification: 2012R2, 6GB, 2 cores, 50Gb Data drive. Azure equivalent: App Service Plan S3 Standard (4 Core, 7GB RAM) set for auto-scale. Highly possible to be reduced to S2 Standard. See additional documentation for pricing.

#### ECS Card Manager/Rules Engine

This website uses a combination of Silverlight and/or MVC and uses AD authentication. Extensive dependency on roles for access. Use of local file system. A Reliance on SSRS. Supports scan of files to local storage and OCR. Watchdog Windows Service processes files. This is an essential application as 60,000 cards were printed over the previous year. Card processing is carried out at the Swanley site which is also used as a BCP site. Current specification: 2012R2, 6GB, 2 cores, 50Gb Data drive. Azure equivalent: App Service Plan S3 Standard (4 Core, 7GB RAM) set for auto-scale. Could be reduced to S2 Standard. See additional documentation for pricing.

#### Financial services

Silverlight application for Direct Debit. WCF RIA. Current specification: 2012R2, 6GB, 2 cores, 50Gb Data drive. Azure equivalent: App Service Plan S3 Standard (4 Core, 7GB RAM) set for auto-scale. Could be reduced to S2 Standard. See additional documentation for pricing.

#### SSRS

SQL Server Reporting Services (SSRS) is not currently supported as a PaaS option in Azure. SSRS therefore must be hosted in an Azure VM pair. SSRS can connect to SQL Azure databases. Microsoft states that for the SLA, a VM must be deployed as a pair in an availability set. There is a lot of flexibility in choosing a VM pair size. The D4S\_V3 Standard VM can be considered: 4 vCPUs, 8GB RAM, 8 Data disks, 8000 Max IOPS, 32 GB Local SSD, Premium disk support, Load balancing. If this is found to be overprovisioned, then dropping down to D2SV3 Standard can be considered.

#### Watchdog – Windows Services

These services include movement of local or network-based files, execution of data transfer to/from MS SQL Server and connections to MS Exchange Server.

### Public External Applications

#### eca.co.uk

This website is hosted using Kentico CMS version 9.0. It has a SQL Server back end and local file storage. Current specification: 2012R2, 4GB, 2 cores, 40Gb Data drive. Azure equivalent: App Service Plan S3 Standard (4 Core, 7GB RAM) set for auto-scale. Could be reduced to S2 Standard. See additional documentation for pricing.

#### ecscard.org.uk

This website is hosted using the Kentico CMS version 9.0. It has a SQL Server back end and local file storage. Current specification: 2008R2, 2 cores, 6GB RAM, 180GB Data drive. Azure equivalent: App Service Plan S3 Standard (4 Core, 7GB RAM) set for auto-scale. Could be reduced to S2 Standard. See additional documentation for pricing.

#### ecsexams.org

This website is hosted using the Kentico CMS version 9.0. This application uses SQL Server back end and local file storage. Current specification: 2008R2, 2 cores, 6GB RAM, 180GB Data drive. Azure equivalent: App Service Plan S3 Standard (4 Core, 7GB RAM) set for auto-scale. Could be reduced to S2 Standard. See additional documentation for pricing.

### File archive

Requirement to copy Azure based data files to archive storage. This will most likely require custom code as part of the Watchdog.

### Azure Web Apps

Almost all the applications discovered are Microsoft based web applications using underlying technologies of either ASP.NET MVC or Silverlight running under IIS on-premise. Migration of web applications to Microsoft Azure Platform as a Service (PaaS) is the preferred option. Azure Web Apps is the recommended destination for migration but comes with limitations, in that Azure Active Directory (AAD) is the preferred authentication identity provider and storage of user file data should be external to the Web App. Azure Web Apps can be configured at run time to execute in various performance tiers, including free mode.

Porting current on-premise web applications to Azure Web Apps will require re-engineering of applications that have dependencies on AD to support AAD authentication and a granular level of user authorisation. Azure Web Apps support Azure AD Groups for authorisation or application roles. <https://github.com/Azure-Samples/active-directory-dotnet-webapp-groupclaims>

Data files storage should either be ported to Azure Storage Blob Store, with application users having indirect access, or possibly to a SQL Azure database. All data hosted in Blob Store is encrypted by default. <https://code.msdn.microsoft.com/How-to-store-the-in-SQL-6c6a46b5>

The current Kentico CMS is running version 9.0. Version 11.0 provides better support for media files. Any custom extensions supporting file uploads to Blob Store are likely require additional coding. Kentico CMS can be migrated on-premise to version 11.0 but will likely still need be re-configured, moving from local file storage to Blob store. There is an Azure Marketplace option for installation of Kentico v11.0 on Azure.

Each Web App needs to be deployed into an App Service Plan. The plan can be scaled to suit the needs of the application. It is expected that there will be DEV, UAT and Prod/Pre-Prod environments in the primary Azure region. For the Prod/Pre-Prod environment the App Plan can be set to Standard Mode supporting auto scale, auto backup etc. The other environments can be configured with separate App Service Plans configured to start in Free mode. Environments can be configured in both North Europe and West Europe regions, with traffic being directed using Azure Traffic Manager. DEV and UAT are only provisioned in the primary region.

It is important to understand that an Azure App Plan relates to a traditional Web Farm. A single Azure App Plan can be shared by multiple Azure Web Apps. It is possible to make savings by internal and external Prod Web Apps sharing the same App Plan due to internal Web Apps being busy during the working day and external Web Apps being busy over evenings and weekends. Prod Web App Auto-Scale can level out any unexpected transitory or overlap resource demands as necessary. Azure Web Apps can be configured to use AAD authentication and are likely require re-engineering to extract the incoming Service Principle for user or group level authorisation.

Azure Web Apps execute with a public IP address but can be secured at the application layer (IP whitelisting etc). The higher specification and costlier Premium App Plan option: ‘App Service Environment’ ASE, hosts applications in an Azure Virtual Network.

### Express Route

ASE allows you to deploy your application with private connectivity over a Site to Site VPN or ExpressRoute circuit. ExpressRoute provides a faster and more reliable connection that does not travel over the public internet. ExpressRoute would be deployed to connect ECA’s MPLS network to Azure\*. \*An assumption has been made that the MPLS provider supports ExpressRoute connectivity. At this stage there does not appear to be a requirement for an Azure Site Recovery (ASR) option.

### WatchDog

The Watchdog application(s) can deployed to an Azure VM pair but it is debatable as to the benefits. Microsoft states that to maintain an SLA, a VM must be deployed as a pair in an availability set. Watchdog access to Azure SQL databases is supported but access to local files, and possibly MS Exchange, will most likely require re-engineering. Hence the code within the Watchdog will most likely need to be ported and hosted elsewhere. Hosting could be in an Azure Web-Job, or a Web App. Web App or Web-Jobs can use resources of current App Plans or could have a dedicated App Plan. WatchDog interfaces in a Web App can be exposed via a WebAPI. Azure Scheduler is an option to trigger WebAPI code from a CRON.

### SQL Azure

Each SQL Server database can be migrated to a SQL Azure Database. SQL Azure Server does not currently support trusted AD authentication but only SQL logins. The performance level of each individual SQL Azure database can be adjusted to match demand in units of DTU’s. SQL Azure database has built in backup functionality. SQL Azure supports replication to secondary read only databases in other Azure regions.

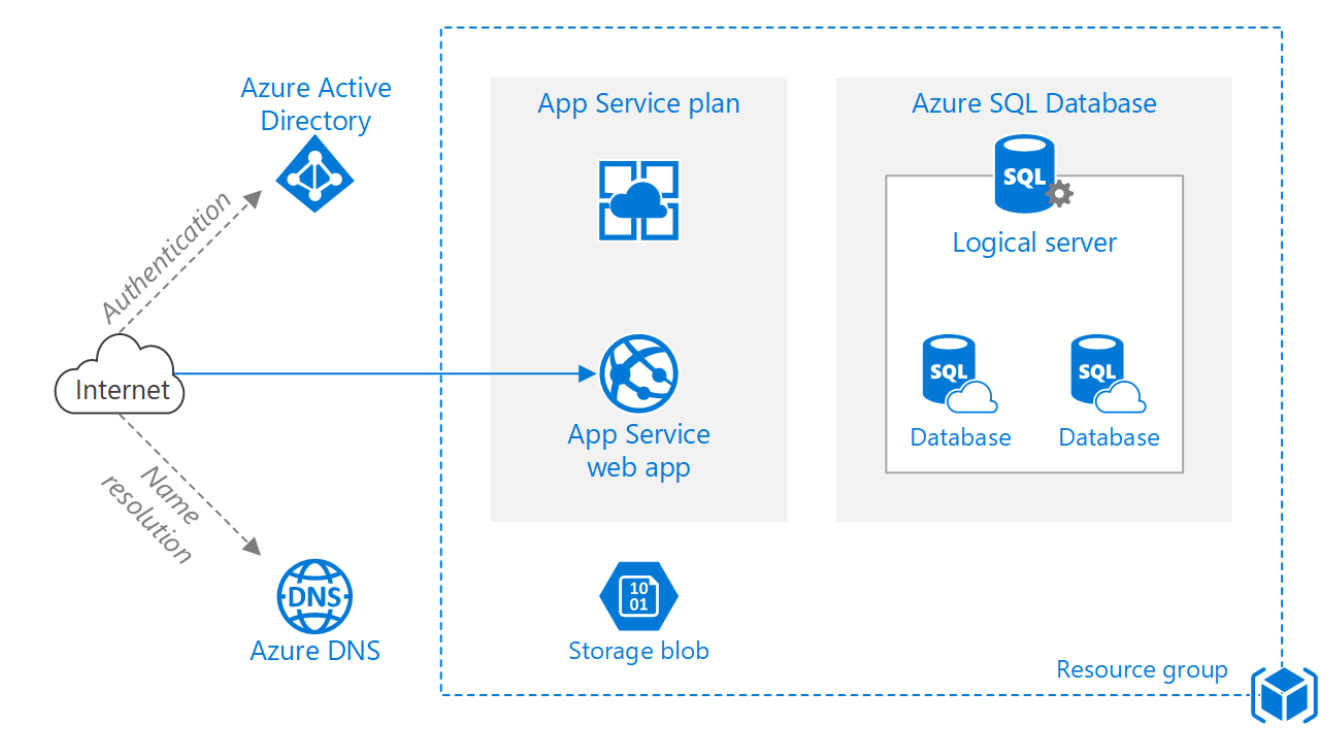
### SSRS

SSRS can be hosted in a VM. It is the customer’s responsibility to install and configure on VM.

### Azure AD

ECA having an Azure tenancy can use or provision a new Azure AD directory. The directory should be synchronised with on-premise AD using AD Connect. This can then support AD authentication for users connecting to Web Apps and ECA staff managing Azure through Role Based Access Control (RBAC). It is the customers responsibility to perform any on-premise AD fixes/configuration before connectivity to AAD can be made.

### Concepts



### Key Benefits

By adopting this solution, the Client can expect the following business benefits to be delivered.