DRAFT - ICT Project Guidance

Design:   
Cloud Based Infrastructure   
Using Azure (Microsoft)

Version:

0.1

Author:

Sky Sigal, Solution Architect

## Description

This document provides guidance on how to develop quality Azure based cloud infrastructure and services as required for delivering cloud based services that are secure, available, monitorable and maintainable.

## Synopsis

The use of Azure networking, storage, communication and monitoring services are described, with guidance on when to use or avoid.

## Contents

[Description 1](#_Toc145232973)

[Synopsis 1](#_Toc145232974)

[Contents 2](#_Toc145232975)

[Synopsis 3](#_Toc145232976)

[Introduction 3](#_Toc145232977)

[Heading Level 3 3](#_Toc145232978)

[Heading Level 4 3](#_Toc145232979)

[Appendices 4](#_Toc145232980)

[Appendix A - Document Information 4](#_Toc145232981)

[Images 4](#_Toc145232982)

[Tables 4](#_Toc145232983)

[References 4](#_Toc145232984)

[Review Distribution 4](#_Toc145232985)

[Audience 4](#_Toc145232986)

[Structure 4](#_Toc145232987)

[Diagrams 4](#_Toc145232988)

[Terms 5](#_Toc145232989)

## Introduction

BOSSCARD/ RAID: Background [], Objective, Options, Scope[In/Out], Stakeholders [Users], Constraints, Assumptions, Risks, Dependencies, Decisions, Deliverables.

Issues

Resolution

Benefits

Risks

Approach

The general approach advocated in this document is to avoid

* Prefering Isolation of Services over
* Prefer monitoring not by access but by Feeds.

Deployment

Web Service

Service consumers use a service agent (i.e., a web browser) to consume services provided by web servers.

The legacy approach to making a web service was to develop a physical or virtual device, install a licensed operating system on it, configure and harden it, install a web server on it, before deploying the web service to it.

Maintaining the services and infrastructure under the actual web service was expensive: the operating system and or the web server would require regular patching before it became out of support, requiring provisioning a whole new device to repeat the whole preparation process before being able to port the system to it.

Choice

App Services

## Domain Name

## Azure Service Domain

Azure provides Domain Name Registration services via Azure Service Domain.

Customers purchase custom domains and assign them to their services like Azure Web Functions, App Services, VMs, etc.

Advantages:

Considerations:

* Can create new or map existing active domains without downtime by preemptive binding.
* Your organisation may mage domains via an alternate domain service.

Links:

* Example how to[[1]](#footnote-2).

## Azure App Service Certificates

Managed certs are free. Standard Certs are approximately $67/year, Wildcard certs are approximately $300/year.

## Azure Front Door

Azure Front Door (AFD) is a Content Delivery Network (CDN) that combines CDN

Comes in two flavours:

* Standard: provides static & Dynamic content acceleration, global load balancing, SSL offloading, domain & certificate management, enhanced traffic analytics, *basic* security capabilities.
* Premium: includes the above, plus WAF, BOT protection, Azure Private Link, Microsoft Threat Intelligence, Security Analytics, Private Linking.

**Advantages:**

**Considerations:**

* There is a base cost per month
  + Standard: ($35)
  + Premium: ($330)
* There is an outbound data transfer from Edge to Client (approx. $0.1/GB)
* There is trivial per request pricing ($0.01/first 250 million requests).

## API Gateway

The service is offered as part o f Azure API Management[[2]](#footnote-3).

## Web Application Firewall (WAF)

WAF’s are a specific form of application firewall that filters, monitors and blocks HTTP traffic to an from a web service.

By inspecting attacks exploiting know vulnerabilities (eg: SQL injection, cross site scripting, file inclusion, improper configuration),

Advantages:

* Protect against the Open Web Application Security Project (OWASP)’s Top 10.

Considerations:

* Already included, if using Azure Front Door, Premium.
* Pricing is: approximately $30-100/month for a medium project.

Disadvantages:

* Acting as a Reverse Proxy, introduces performance degradation.
* Requires significant memory for buffering requests, especially on sites where users uploade media.
* Easily bypassed by attackers.
* Are not an ultimate security solution, rather they are meant to be used in conjunction with other network perimeter security solutions such as network firewalls and intrusion prevention systems to provide a holistic defence strategy.
* Not recommended as there are potentially better options (e.g., better to validate code via pipeline checks than in production[[3]](#footnote-4)).

## Static Web Serving

Azure provides Azure Static Web Apps.

[Azure Static Web Apps – App Service | Microsoft Azure](https://azure.microsoft.com/en-us/products/app-service/static)

Advantages:

* Excellent option to consider for plugins that can invoke APIs of the core without giving access to back end code.

Considerations:

* Unpacked Storage space: 2GB
* Cost: $9/month + $0.2/GB over an initial free 100GB.
* First class integration with GitHub & Azure DevOps.
* Custom domains & free SSL certificates.

Disadvantages:

* As per Azure functions discussed below, the price can start off low, but grows under volume to being more expensive than App Services.

References:

* <https://learn.microsoft.com/en-us/azure/static-web-apps/overview>

## Azure Function

**Considerations:**

* Possibly not required if already using a dynamic Static Web Apps
* OData has been done, but it’s not supported out of the box[[4]](#footnote-5).

**Disadvantages:**

* Cheaper when low use, but grows to being more expensive than App Services

## Azure App Services

Managed infrastructure where Azure is responsible for the device, OS, etc.

By default, one gets a Shared environment, or one can get an Isolated environment where one can protect it within a virtual VM ware, although its about 3 to 4 times more expensive.

Advantages:

* Fully managed platform.
* Automatic Scales and global availability.
* ASEv3 deploys into a subnet in one of your Azure Virtual Networks (VNets) permitting

Considerations:

* Costs:
  + Shared: an S2 (2 cores) is approximately $150/month. A Premium (P2V2) is double that.
  + Isolated: (2 cores) is approximately $400 to 600/month.
* Run on Kubernetes

Disadvantages:

Virtual Servers

Avoid.

Storage

Networking

Appendices

Appendix A - Document Information

### Versions

* 1. Initial Draft

### Images

[Figure 1: TODO Image 2](#_Toc144995112)

### Tables

[Table 1: TODO Table 3](#_Toc145048484)

[Table 2: TODO Table 2 3](#_Toc145048485)

### References

* *ICT Project Guidance – Design – Cloud Based Infrastructure Basics*

**There are no sources in the current document.**

### Review Distribution

The document was distributed for review as below:

|  |  |
| --- | --- |
| Identity | Notes |
| Sandy Britain, Solution Architect |  |
| Dries Venter, DevOps Specialist |  |
| Matt Duguid, DevOps Specialist |  |
|  |  |

### Audience

The document is technical in nature, but parts are expected to be read and/or validated by a non-technical audience.

### Structure

Where possible, the document structure is guided by either ISO-\* standards or best practice.

### Diagrams

Diagrams are developed for a wide audience. Unless specifically for a technical audience, where the use of industry standard diagram types (ArchiMate, UML, C4), is appropriate, diagrams are developed as simple “box & line” monochrome diagrams.

### Terms

Refer to the project’s Glossary.

##### IT

: acronym for Information, using Technology to automate and facilitate its management.

##### ICT

: acronym for Information & Communication Technology, the domain of defining Information elements and using technology to automate their communication between entities. IT is a subset of ICT.

1. [Buy a custom domain - Azure App Service | Microsoft Learn](https://learn.microsoft.com/en-us/azure/app-service/manage-custom-dns-buy-domain) [↑](#footnote-ref-2)
2. [Azure API Management - Overview and key concepts | Microsoft Learn](https://learn.microsoft.com/en-us/azure/api-management/api-management-key-concepts) [↑](#footnote-ref-3)
3. https://en.wikipedia.org/wiki/Web\_application\_firewall#cite\_note-2 [↑](#footnote-ref-4)
4. [Support OData queries · Issue #1044 · Azure/Azure-Functions (github.com)](https://github.com/Azure/Azure-Functions/issues/1044) [↑](#footnote-ref-5)