Why Microsoft Azure is the right choice for your Public Cloud, a Consultants view

by Simon Conyard

In my view, Microsoft® Azure is fast becoming the trusted platform of choice for SMB and Enterprise customers. In this article, I explore Microsoft Azure and highlight what I see are the top 5 reasons why you should consider using Microsoft Azure for your public cloud.

What is Microsoft Azure?

Introduced in October 2008, Microsoft Azure (or Windows Azure as it was then known), is Microsoft's Public Cloud offering, that consists of an increasing number of cloud-based **Azure Services** that are available to consume in multiple **Azure Regions.**

With close integrations to Microsoft technologies in the private cloud, and hosting Azure native versions in the public cloud, Azure provides services that developers and IT professionals can utilise; enabling them to migrate, create, connect and manage new applications, solutions and services.

Over the last 10 years, Azure has gone through a program of continuous improvement and development, with services currently available across 38 Azure regions. Microsoft Azure is constantly evolving and adapting to a cloud connected world, offering support for Microsoft technologies, toolsets and frameworks, and an increasing number of open source technologies; as well as options for multiple architecture models from server-less functions to IaaS.

What are Azure Services?

Azure Services are the evolving set of products that can be purchased and operated within the Azure public cloud. These services include Infrastructure (IaaS), Platform (PaaS) and Software as a Service (SaaS) offerings, and can be categorised into the following product types;

- Compute
- Networking
- Storage
- Web + Mobile
- Monitoring + Management
- Containers
- Databases
- Data + Analytics
- AI + Cognitive Services
- Developer Tools
- Internet of Things
- Enterprise Integration
- Security and Identity

Azure enables you to deploy IaaS services to run virtual server workloads, PaaS services to run web or mobile applications and SaaS services for Identity management; all of which are hosted and delivered from Microsoft's global network of data centres.

What is an Azure Region?

38
Azure regions
More than AWS and Google combined

Azure is generally available in 38 regions; each region is strategically located and made up from multiple data centres. Within each of these data centres, services are built with fault tolerance for networking, compute, storage and power. These **Fault Domains** help to ensure that no single point of failure can result in a service outage and unplanned outages are mitigated. For planned outages, Azure provides **Update Domains.** Utilising **Availability Sets** to create a logical grouping of VMs, you can ensure that your VMs span both Fault and Update Domains.

By deploying VMs across Fault and Update Domains within a region, or utilising Azure PaaS or SaaS, you can access services balanced across multiple data centres. This provides an Azure SLA of 99.95%, resulting in high availability and resilience benefits.

How do you connect to Azure Services?

Hosting services within the public cloud requires robust connectivity options that fit several use cases; within the cloud one size does not fit all. Azure provides connectivity methods to cover all scenarios, with connections to hosted services via the **Internet, Point-to-Site Virtual Private Networks (VPNs), Site-to-Site VPNs** and **ExpressRoute.**

Internet

What is this? Access to hosted services via the public internet.

How does it work? Azure provides options to create public IP addresses, manage web domains and manage network security for most offered services, with additional options for Content Delivery Networks (CDN).

When should you use? Use this for providing public access to hosted systems such as websites, mobile apps or public APIs, or delivering public content to multiple geographic locations.

When shouldn't you use it? Don't use this when you need to provide private connections to hosted systems.

Point to Site VPN

What is this? An individual user VPN service.

How does it work? It uses the Windows VPN client with SSL certificates to provide a secure VPN tunnel to Azure hosted systems over the public internet.

When should you use? Use when you need to provide secure private access to Azure hosted systems for a small number of individuals, or for concept, prototyping or evaluation purposes.

When shouldn't you use it? Don't use this when you need to provide secure private access to a site, or need to manage access for many users.

Site to Site VPN

What is this? A site VPN service.

How does it work? It uses a compatible VPN device to connect an on-premises network to an Azure virtual network over an IPsec/IKE VPN tunnel.

When should you use? Use when you need to provide a site with private secure access to Azure hosted systems. Ideal for small scale production services or development and test environments.

When shouldn't you use it? Don't use this when you need to secure, high speed, low latency connections for an organisation to Azure hosted services.

ExpressRoute

What is this? Azure ExpressRoute can be considered as an extension to your WAN.

How does it work? It's a private, secure connection to Azure, that doesn't go over the public internet, and is facilitated by a connectivity provider. ExpressRoute offers increased reliability, faster speeds and lower latency connectivity to Azure.

When should you use? Use ExpressRoute to establish secure private connectivity to Azure hosted systems when you need low latency, high speed access. It can be used to provide access to mission critical systems, extend on-premises data centre services or to use Azure as a backup and recovery location.

When shouldn't you use it? ExpressRoute is ideally suited for large scale, production mission critical systems and services. If you are in concept, prototype or development phases, then you should consider one of the alternative connection methods.

My Top 5 Reasons for using Azure

With the fundamentals of Microsoft Azure covered, why should it be right choice for your public cloud. Here are my top 5 reasons.

1. Identity Management

Making the transition to cloud services means thinking about how customers, developers and administrators are going to access those services.

Azure Active Directory (Azure AD) provides access to a comprehensive identity and access management cloud solution; with a robust set of capabilities to manage users and groups, enabling you to secure access to both on-premises and cloud applications. This includes pre-integration for Salesforce and Office 365, and the capability to integrate and provide **Single Sign On** (SSO) to any cloud or on-premises web application.

Using industry standard protocols such as **SAML 2.0, WS-Federation, OAuth 2.0 and OpenID Connect** provides your developers with an effective way to integrate identity management into applications and services. In addition, the REST based **Graph API** enables developers to read and write to the directory from any platform.

It is ideal for managing access to cloud and on-premises services, providing domain services in the cloud and managing consumer identity and access management.

Chances are your internal directories are built on Active Directory. By extending on-premises Active Directory, instead of reinventing or redeploying directory services, can secure cloud services and resources, reuse existing skills and resources, and avoid password management complexities with SSO integrations.

Azure AD is offered at an enterprise scale as a highly available service with an SLA of 99.9%.

2. The Trust Centre

One of the main arguments against cloud implementation is compliance, therefore providing information regarding the **security, compliance and certifications** held by a cloud service provider is a key consideration.

Microsoft provide access to the **Trust Centre**, a valuable resource for learning how Microsoft implement and support security, privacy, compliance and transparency across all cloud products and services. It contains information tailored to specific roles within the organisation, ranging from business leaders, administrators, security professionals and compliance teams.

Within the Trust Centre, Microsoft publish details and provide access to all held compliances, the services to which they apply and **access external audit reports**.

A visit to the Microsoft trust centre will highlight just how seriously security is taken. Azure holds many compliances, all of which are maintained within the trust centre at:

https://www.microsoft.com/en-us/trustcenter/compliance/complianceofferings

Highlights include, **PCI DSS Level 1 version 3.1, UK G-Cloud, UK cyber Essentials PLUS, ISO 9001/22301/27001/27017 and 27018.**

The Trust Centre provides an invaluable and referenceable resource that can help answer security and compliance questions and issues, freeing up resources to deliver Azure services.

3. Azure App Service

Azure boasts an impressive array of developer tools, hosting options and language support. For the enterprise and SMB, a move to the Azure cloud provides an opportunity to rearchitect existing, or develop new services to take advantage of PaaS.

The **Azure App Service** provides a PaaS platform, which means you no longer need to worry about managing Operating System (OS) updates, or even install and update framework runtimes. Packaged with scaling features and integrations for code management, and when coupled with **CDN** and **Azure Traffic Managers** (Load Balancers), the Azure App Service provides a **highly available, global and resilient service.**

The Azure App Service provides options for **Web Apps, Mobile Apps and API Apps**, with support for **Python, PHP, Node.JS, Java, HTML5 and C#**.

The Azure App Service **Isolated tier** provides a dedicated environment to run your applications and services, **offering network isolation** with additional performance and scale.

The Azure App Service provides a platform that can scale with requirements, and be configured for global reach and resilience with charging based upon usage.

4. Azure Service Bus

Complex enterprise environments often require information to be exchanged between the many systems that make up the enterprise to provide business services to customers. On-premises services, such as BizTalk, conduct these orchestrations passing, and if required, transform data between systems.

The **Azure Service Bus** (ASB) provides a highly available cloud messaging service; with **brokered messaging** between client and server, structure **First In First Out** (FIFO) messaging and **publish/subscribe** capabilities. This enables you to reliably scale solutions across the Azure platform, integrating Web Apps with Azure SQL databases and storage.

However, ASB is not just for use within Azure. Configuring the **Hybrid Connections** featured within the **Service Bus Relay** enables you to connect to existing assets without complex firewall, network and VPN configurations as traffic is passed secured over HTTPS.

With ASB, not only can an enterprise or SMB manage and orchestrate messaging within the Azure platform, it can link to existing data and resources. This opens the potential for cloud scalable front ends to be orchestrated with on-premises resources.

5. Azure Stack

Much of the conversation around cloud migrations focuses on moving existing services to cloud platforms. With **Azure Stack,** Microsoft have introduced a potential game changer to the Hybrid cloud arena, built to provide Azure cloud functions and features into the on-premises environment.

Azure Stack takes the cloud application model and moves it to on-premises, providing **Web** and **Mobile services**, **Server-less** computing, **Containers** and **Micro Architectures**. This opens up the possibility to apply these in updating and extend legacy applications, without leaving the on-premises environment.

Development teams are therefore provided with a consistent environment and one set of common development tools, application models, self-service portals and APIs, helping to maximise productivity and reusability between environments.

This means that they can develop applications in Azure or Azure stack, with the flexibility to deploy to either environment and meet compliance or policy requirements, **without changing any code.**

Azure Stack and the hardware it runs on is delivered as an integrated system, provided by **Dell EMC, HPE** and **Lenovo.** Azure stack can be used to **reinvent legacy** applications, gain **flexibility** and **accelerate** your journey to the Azure public cloud.

Azure is an evolving platform with features, solutions and services that cover; the Internet of Things, Big Data and Analytics, Identity Management, Storage, Development, Content Delivery, Enterprise Integration, Hybrid deployments, Compliance, Security, Nested Virtualisation and Artificial Intelligence. Whilst this paper only covers my top reasons, there are many more compelling arguments as to why Microsoft Azure should be considered the right choice for your public cloud provider.

You can find more information on Microsoft Azure here.

To find out more about Microsoft Azure and how you can benefit from Xtravirt's Cloud services, please contact us and we'll be happy to use our wealth of knowledge and experience to assist you.

About the Author

Simon Conyard is an Xtravirt Technical Consultant with over 17 years' experience in the IT industry. He has extensive knowledge of practical implementation and operational experience with a range of infrastructure and data centre technologies. His specialist areas include Infrastructure Architecture, Infrastructure Management, Integration and Business Alignment.

Xtravirt is a leading, independent provider of enterprise virtualisation solutions. We deliver data centre, workspace and cloud transformational solutions to clients across public and private sectors, both in the UK and internationally.

xtravirt

Dedicated to smarter business