

Instituto Tecnológico y de Estudios Superiores de Monterrey

Inteligencia Artificial Avanzada para la Ciencia de Datos II (Gpo 501)



**Tecnológico
de Monterrey**

Diseño de Arquitectura en la Nube

Equipo 5

Jorge Eduardo De León Reyna - A00829759

David Esquer Ramos - A01114940

Francisco Mestizo Hernández - A01731549

Adrián Emmanuel Faz Mercado - A01570770

Noviembre 20, 2023

1. Introducción

En el presente informe, se detalla la arquitectura propuesta para el entorno en la nube de DataTech, una empresa que busca optimizar sus operaciones y garantizar la eficiencia en el manejo de aplicaciones, bases de datos y almacenamiento de datos.

Este diseño se ha concebido con el objetivo de proporcionar una infraestructura flexible, escalable y segura que cumpla con los rigurosos requisitos de rendimiento y disponibilidad de la empresa. La combinación estratégica de máquinas virtuales, bases de datos en la nube, almacenamiento seguro y redes virtuales bien definidas, respaldada por servicios de App Service, ofrece un marco integral que permite a DataTech gestionar sus aplicaciones y datos de manera eficaz y centrarse en su misión principal sin comprometer la seguridad ni la eficiencia operativa.

En las secciones subsiguientes, se explorará en detalle cada componente de esta arquitectura, destacando su funcionamiento y beneficios para el éxito continuo de DataTech en el ámbito de la computación en la nube.

2. Arquitectura propuesta y justificación

A continuación se muestra el diagrama de arquitectura propuesta para la situación problema de Datatech, así como también la explicación y justificación del funcionamiento de cada uno de los componentes seleccionados.

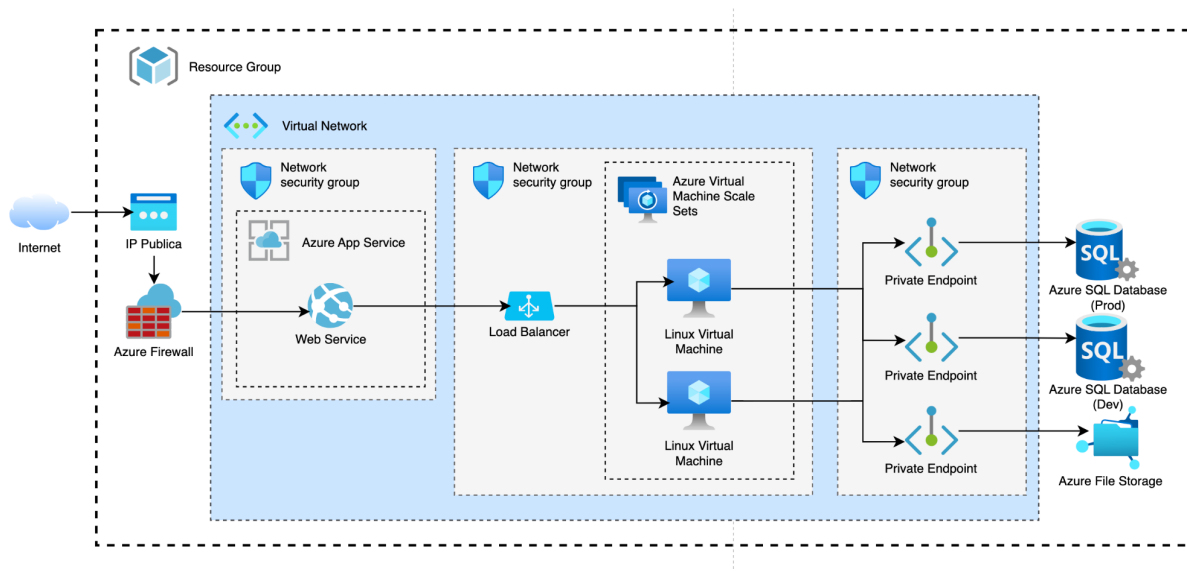


Diagrama editable:

https://drive.google.com/file/d/1396_tjQd7VL2Pd2HN5o7ggnsCL3gTJlI/view?usp=sharing

2.1 Descripción general

Como se puede apreciar en el diagrama de arquitectura, se propone una arquitectura basada en los servicios de nube de Azure. Los servicios de nube de Azure permiten implementar distintos componentes que permiten construir arquitecturas de nube robustas, seguras y adaptables a las necesidades de cada entorno. En este caso, se hace uso de los siguientes elementos principales:

1. Virtual Network Service
2. Azure App Service
3. Azure Virtual Machine Scale Sets
4. Azure Load Balancer
5. Azure Firewall
6. Azure SQL Database
7. Azure File Storage

2.2 Justificación de selección y descripción de componentes

A continuación se explica con mayor detalle el funcionamiento de cada uno de los componentes que constituyen la arquitectura de nube propuesta, así como también la justificación para haber seleccionado los mismos:

- a. **Azure Virtual Network Service:** Azure Virtual Network permite la creación de redes privadas en la nube, permitiendo la conexión segura de recursos como máquinas virtuales y servicios en la nube.

Este servicio permitirá configurar redes virtuales para aislar y organizar recursos. Facilita la conectividad segura entre servicios, como la comunicación entre aplicaciones web en Azure App Service y bases de datos en Azure SQL Database.

- b. **Azure App Service:** Azure App Service es un servicio administrado que permite la implementación y escalabilidad de aplicaciones web y APIs sin gestionar directamente las máquinas virtuales subyacentes.

Ideal para este caso ya que simplifica la implementación de aplicaciones web sin preocuparse por la infraestructura subyacente. Proporciona escalabilidad automática y opciones de gestión centralizada para el desarrollo y despliegue eficientes de aplicaciones.

- c. **Azure Virtual Machine Scale Sets:** Azure Virtual Machine Scale Sets facilita la implementación y gestión de un conjunto de máquinas virtuales idénticas, escalando automáticamente según la demanda.

Es esencial para mantener la escalabilidad y la alta disponibilidad de las aplicaciones. Permite gestionar conjuntos de máquinas virtuales de manera eficiente, ajustándose dinámicamente a cambios en la carga de trabajo.

- d. **Azure Load Balancer:** Azure Load Balancer distribuye el tráfico de red entre múltiples máquinas virtuales para garantizar la escalabilidad y la disponibilidad.

Es importante para equilibrar la carga de trabajo entre las instancias de la aplicación, asegurando que ninguna máquina virtual esté sobrecargada. Mejora el rendimiento y la confiabilidad de las aplicaciones.

- e. **Azure Firewall:** Azure Firewall proporciona funciones avanzadas de seguridad, filtrado de paquetes y control de aplicaciones para proteger las redes virtuales en Azure.

Permite garantizar la seguridad de las conexiones entre las redes virtuales y controlar el tráfico de red. Ayudará a la empresa a aplicar políticas de seguridad coherentes en toda la infraestructura.

- f. **Azure SQL Database:** Azure SQL Database es un servicio de base de datos relacional totalmente administrado que proporciona rendimiento, seguridad y escalabilidad.

Es ideal para este caso al ofrecer una base de datos administrada sin la necesidad de gestionar la infraestructura subyacente. Proporciona opciones avanzadas de respaldo y recuperación, así como escalabilidad según las necesidades de la aplicación.

- g. **Azure File Storage:** Azure File Storage proporciona un almacenamiento en la nube seguro y escalable para archivos y datos no estructurados, accesible mediante el protocolo SMB.

Es crucial para DataTech almacenar y compartir archivos entre aplicaciones y equipos. Azure File Storage ofrece escalabilidad y seguridad para gestionar eficientemente datos no estructurados en la nube.

Estos servicios forman una combinación integral de servicios que proporcionan a DataTech la infraestructura necesaria para implementar, gestionar y asegurar sus aplicaciones y datos en la nube de manera eficaz y segura.

3. Proyección de Costos

Debido a que no se cuenta con estimaciones de uso de la infraestructura propuesta a continuación se muestra un aproximado del costo promedio mensual de esta arquitectura. Los siguientes datos se basan en la calculadora de precios de Microsoft Azure. Esta herramienta permite hacer estimaciones en base a casos de uso. A continuación se muestra el costo esperado mensual acorde a un uso promedio según la definición del proveedor.

Service category	Service type	Region	Description	Estimated monthly cost
Redes	Virtual Network		Este de EE. UU. (Virtual Network 1): 100 GB Outbound Data Transfer; Este de EE. UU. (Virtual Network 2): 100 GB Outbound Data Transfer	\$4.00
Compute	App Service	West US	Basic Tier; 1 B1 (1 Core(s), 1.75 GB RAM, 10 GB Storage) x 730 Hours; Windows OS; 0 SNI SSL Connections; 0 IP SSL Connections; 0 Custom Domains; 0 Standard SLL Certificates; 0 Wildcard SSL Certificates	\$54.75
Compute	Virtual Machine Scale Sets	West US	1 D1 (1 vCPU, 3.5 GB RAM) x 730 Hours (Pay as you go), Windows (License included), OS Only	\$102.20
Compute	Virtual Machines	East US	1 D2 v3 (2 vCPUs, 8 GB RAM) x 730 Hours (Pay as you go), Windows (License included), OS Only; 0 managed disks – S4; Inter Region transfer type, 5 GB outbound data transfer from Este de EE. UU. to Este de Asia	\$137.24
Redes	Traffic Manager	East US	0 million DNS queries/mo, 0 Azure endpoint(s), 0 Fast Azure endpoint(s), 0 External endpoint(s), 0 Fast External endpoint(s), 0 million(s) of user measurements, 0 million(s) of data points processed.	\$0.00
Redes	Azure Firewall	West US	Standard tier, 1 Logical firewall units x 730 Hours, 0 GB Data processed	\$912.50
Bases de datos	Azure SQL Database	East US	Single Database, vCore, General Purpose, Provisioned, Standard-series (Gen 5), Locally Redundant, 1 - 2 vCore Database(s) x 730 Hours, 32 GB Storage, RA-GRS Backup Storage Redundancy, 0 GB Point-In-Time Restore, 0 x 5 GB Long Term Retention	\$372.97
		Licensing Program	Microsoft Customer Agreement (MCA)	
		Total		\$1,583.66

4. Sugerencias a futuro

A continuación se proponen algunas sugerencias para implementar en el futuro las cuales ayudarán a robustecer más la solución propuesta anteriormente en áreas como la seguridad, el monitoreo y la gestión más eficiente de la infraestructura:

- 1. Implementación de Azure Key Vault para la Gestión de Secretos:** Integrar Azure Key Vault para la gestión segura de secretos y claves de la aplicación, siguiendo el principio de "least privilege" al limitar el acceso solo a quienes necesitan dichos secretos, garantizando que los privilegios se asignen de manera estricta y mínima para prevenir así accesos innecesarios. Esta implementación mejoraría significativamente la seguridad de la arquitectura al centralizar y gestionar de manera segura las credenciales y secretos utilizados por las aplicaciones y servicios en la nube, contribuyendo así a un entorno más seguro y protegido.
- 2. Incorporación de Azure Monitor y Azure Security Center:** Implementa Azure Monitor para la supervisión proactiva del rendimiento y Azure Security Center para la gestión de la seguridad. Estas herramientas proporcionan una visibilidad más completa y un monitoreo avanzado de la infraestructura, permitiendo la detección temprana de posibles problemas de rendimiento y la aplicación de políticas de seguridad avanzadas para proteger la plataforma contra amenazas y vulnerabilidades.
- 3. Despliegue de Azure Bastion para Acceso Seguro a Máquinas Virtuales:** Integra Azure Bastion como una solución segura y administrada para el acceso remoto a las máquinas virtuales. Simplificará la administración remota de las máquinas virtuales al eliminar la necesidad de configuraciones complejas de acceso mediante RDP o SSH, proporcionando una capa adicional de seguridad para la gestión de las máquinas virtuales.

5. Conclusiones

Adrián Faz: Esta actividad de diseño de una arquitectura en la nube me permitió darme cuenta que es de suma importancia analizar cuidadosamente los requerimientos del cliente, comprendiendo sus necesidades específicas y alineando la arquitectura

con sus objetivos. De igual forma, pude reforzar la idea de que la escalabilidad, el rendimiento y la alta disponibilidad son factores críticos en la toma de decisiones del diseño, pues estos aspectos permiten que la empresa se adapte a las cambiantes demandas del mercado. Además de ello, tuve la oportunidad de conocer diferentes herramientas y plataformas que se pueden utilizar para gestionar este tipo de arquitecturas en la nube, cada una cumple con una función específica y hay un sinfín de ellas, pero es por eso también que se requieren ingenieros que puedan entender adecuadamente las necesidades del cliente y así diseñar una que sea justo lo que necesita. Finalmente, pude también reforzar la idea de que no solamente se trata de cumplir con los requisitos del cliente, sino también de garantizar la protección de los datos y recursos críticos, y esto se puede validar mediante diferentes principios y servicios que están disponibles. En resumen, esta actividad me permitió aprender sobre cómo diseñar una arquitectura en la nube de manera eficiente, segura y alineada con las necesidades del cliente.

Jorge de León: Al llevar a cabo el diseño de la arquitectura en la nube para este caso de uso reforcé mi comprensión sobre la importancia de considerar cuidadosamente cada servicio y componente para satisfacer los requisitos específicos de una empresa. Con esto en cuenta, la selección y combinación de servicios como Azure Virtual Network, App Service y Azure SQL Database, no solo son cruciales para la funcionalidad técnica, sino también para lograr una implementación eficiente y fácil mantenimiento. Además, considerar aspectos como la seguridad, el monitoreo y la gestión de identidades aporta capas esenciales para garantizar un entorno en la nube seguro y resiliente. Esta actividad ha fortalecido mi capacidad para diseñar arquitecturas en la nube coherentes y escalables, considerando no solo la funcionalidad individual de cada componente, sino también su integración acorde a las necesidades presentes.

Francisco Mestizo: Con esta actividad me di cuenta que el plantear el diseño de arquitectura para el software de una empresa que funciona con servicios de la nube es muy importante. Primero, porque se tienen que seleccionar los servicios que la empresa realmente necesita, con los requerimientos que se ajustan al sistema. Así, solamente se paga lo necesario o lo que la empresa tiene presupuestado.

También la actividad me sirvió para conocer más los servicios de Azure y sus especificaciones, para entender cómo se pueden aplicar a soluciones de software reales.

David Esquer: El diseño de la arquitectura en la nube para DataTech ha sido una experiencia enriquecedora, destacando la importancia de seleccionar y combinar servicios de Azure como Virtual Network, App Service y SQL Database. Esta elección no solo atiende a la funcionalidad técnica, sino que también se enfoca en la eficiencia y facilidad de mantenimiento. La integración de aspectos como seguridad, monitoreo y gestión de identidades es crucial para asegurar un entorno en la nube seguro y resiliente. Este proyecto ha fortalecido la habilidad de diseñar arquitecturas coherentes y escalables, considerando la interacción y sinergia de cada componente, y alineando con las necesidades y objetivos de la empresa.

6. Referencias

1. <https://azure.microsoft.com/es-mx/pricing/calculator/>
2. <https://learn.microsoft.com/en-us/azure/architecture/example-scenario/infrastructure/wordpress-iaas>
3. <https://azure.microsoft.com/es-mx/pricing/details/cloud-services/#pricing>
4. <https://learn.microsoft.com/es-es/azure/architecture/guide/>
5. <https://azure.microsoft.com/es-mx/products/app-service>
6. <https://azure.microsoft.com/es-es/products/azure-sql/database>
7. <https://learn.microsoft.com/es-es/azure/firewall/overview>
8. <https://azure.microsoft.com/en-us/products/storage/files>