Instituto Tecnológico y de Estudios Superiores de Monterrey

Cloud computing | Actividad 6 - Cloud migration

Integrantes:

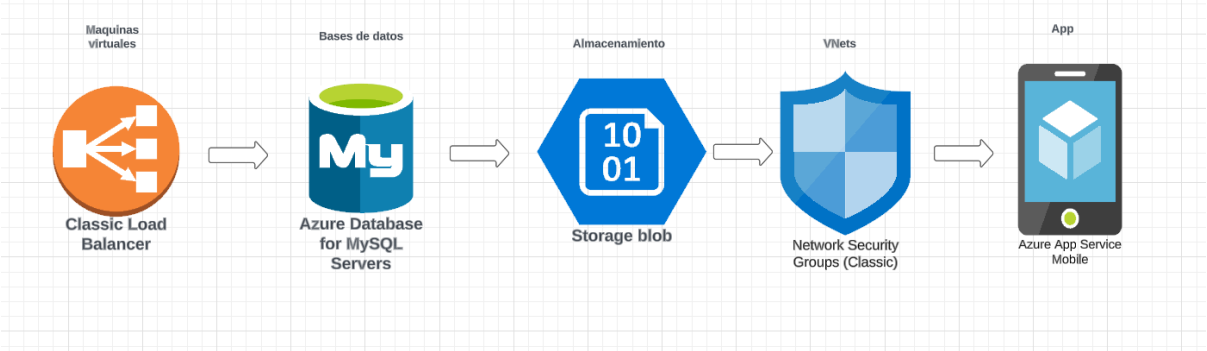
Diego Alberto Baños Lopez	A01275100
Carlos David Lozano Sanguino	A01275316
Carol Arrieta Moreno	A01275465

Monterrey, Nuevo León, México 20 de Noviembre del 2023

Profesor: Félix Ricardo Botello Urrutia

Inteligencia artificial avanzada para la ciencia de datos II (Gpo 501)

Diagrama de la arquitectura propuesta para el escenario.



Informe Detallado Cloud Migration

DataTech ha decidido migrar sus aplicaciones y servicios a la nube para mejorar la escalabilidad, disponibilidad y seguridad de sus operaciones. Como parte del equipo Cloud en nuestra consultoría de TI, hemos diseñado una arquitectura en la nube que cumple con estos requisitos y garantiza un rendimiento óptimo, alta disponibilidad y seguridad robusta. En este informe, detallaremos la arquitectura propuesta, incluyendo máquinas virtuales, bases de datos IaaS y PaaS, almacenamiento en la nube, configuración de VNets y servicios de App Service. También abordaremos las medidas de seguridad implementadas, incluyendo el principio de least privilege, modelo zero trust, segmentación de redes, NSG y encriptación.

Arquitectura en la Nube Propuesta

1. Máquinas Virtuales

1.1. Selección del tamaño y tipo
Hemos recomendado el uso de máquinas virtuales de la serie D de Azure, que ofrecen un equilibrio óptimo entre rendimiento y costo. Seleccionamos tamaños específicos basados en los requisitos de carga de trabajo y utilizamos escalabilidad automática para ajustar la capacidad según la demanda.

1.2. Distribución de carga y Grupos de Disponibilidad
Implementamos un equilibrio de carga utilizando Azure Load Balancer para distribuir el tráfico de manera uniforme entre las máquinas virtuales. Además, configuramos Grupos de Disponibilidad para garantizar la alta disponibilidad y la tolerancia a fallos.

2. Bases de Datos IaaS y PaaS

2.1 Bases de Datos Relacionales - Azure SQL Database (PaaS)
2.1.1 Características de Azure SQL Database
2.1.1.1 Escalabilidad Automática

Azure SQL Database ofrece escalabilidad automática, ajustando dinámicamente los recursos de la base de datos según la carga de trabajo. Esto asegura un rendimiento óptimo incluso en momentos de demanda variable.

2.1.1.2 Rendimiento Optimizado
Las bases de datos alojadas en Azure SQL Database se benefician de la infraestructura de alto rendimiento de Azure. Esto incluye almacenamiento SSD de alto rendimiento y optimizaciones a nivel de red, garantizando un acceso rápido y eficiente a los datos.

2.1.1.3 Respaldo y Recuperación Automáticos
Azure SQL Database proporciona funciones automáticas de respaldo y recuperación. Los datos se respaldan regularmente, y en caso de un fallo, se puede realizar una recuperación rápida a un punto específico en el tiempo.

2.1.1.4 Seguridad Avanzada
Se implementan medidas de seguridad avanzadas, como cortafuegos de base de datos, control de acceso basado en roles y encriptación avanzada. Esto asegura la confidencialidad e integridad de los datos almacenados.

2.1.2 Configuración Personalizada para DataTech
Dentro de Azure SQL Database, configuramos características específicas para satisfacer las necesidades de DataTech. Esto incluye la definición de índices para optimizar consultas y la configuración de políticas de retención de datos para cumplir con los requisitos de almacenamiento a largo plazo.

2.2 Bases de Datos No Relacionales - Máquinas Virtuales con Software de Base de Datos Instalado (IaaS)
2.2.1 Flexibilidad de Elección de Software
Para bases de datos no relacionales, proponemos el uso de máquinas virtuales con software de base de datos instalado, como MongoDB o Cassandra. Esto proporciona a DataTech la flexibilidad de elegir el software que mejor se adapte a sus necesidades específicas.

2.2.2 Optimizaciones de Rendimiento y Configuración de Seguridad
Configuramos cuidadosamente las máquinas virtuales para optimizar el rendimiento de la base de datos no relacional. Esto incluye la asignación de recursos adecuados, la configuración de índices según sea necesario y la aplicación de medidas de seguridad para proteger los datos almacenados.

2.2.3 Estrategias de Respaldo y Recuperación
Establecemos estrategias de respaldo y recuperación específicas para las bases de datos no relacionales, considerando las características y requisitos particulares del software de base de datos utilizado. Esto garantiza la disponibilidad y la integridad de los datos en caso de fallos.

3. Storage Account - File Share

3.1.1 Selección de Tipo de Almacenamiento

Dentro de Azure Storage Accounts, seleccionamos cuidadosamente el tipo de almacenamiento que mejor se adapta a los requisitos de DataTech. Utilizamos Azure Blob Storage para almacenar grandes cantidades de datos no estructurados, garantizando un acceso eficiente y una alta durabilidad.

3.1.2 Configuración de Redundancia
Configuramos la redundancia a nivel de Storage Account para mejorar la disponibilidad y la durabilidad de los datos. Utilizamos la redundancia geográfica para replicar los datos en diferentes regiones de Azure, asegurando la continuidad del servicio incluso en situaciones de desastre.

3.1.3 Control de Acceso
Implementamos medidas de control de acceso a nivel de Storage Account para garantizar que solo usuarios autorizados tengan acceso a los datos almacenados. Configuramos políticas de seguridad y asignamos permisos según el principio de least privilege, limitando el acceso a las operaciones esenciales.

3.2 File Shares
3.2.1 Configuración de File Shares
Dentro de Azure Storage Accounts, creamos File Shares para facilitar el intercambio de archivos entre aplicaciones y equipos en DataTech. Configuramos estas comparticiones de archivos con atención a los siguientes aspectos:

3.2.1.1 Políticas de Retención y Versionado
Establecemos políticas de retención para definir la duración del almacenamiento de los archivos y configuramos el versionado para rastrear y gestionar las versiones de los archivos. Esto asegura la integridad y disponibilidad de los datos a lo largo del tiempo.

3.2.1.2 Acceso Seguro a File Shares
Implementamos reglas específicas en el control de acceso a File Shares para reforzar la seguridad. Esto incluye la autenticación basada en Azure Active Directory (AAD) para garantizar la identidad de los usuarios y el acceso seguro a los archivos compartidos.

3.2.1.3 Integración con Aplicaciones y Sistemas
Configuramos la integración de File Shares con aplicaciones y sistemas relevantes en DataTech. Aseguramos una comunicación segura y eficiente entre las aplicaciones que acceden a los archivos almacenados en File Shares y la infraestructura subyacente.

3.3 Monitoreo Continuo y Optimización
Implementamos un sistema de monitoreo continuo utilizando Azure Monitor para supervisar la utilización del almacenamiento, el rendimiento y la integridad de los datos. Establecemos alertas automáticas para detectar cualquier anomalía y optimizamos la configuración según las métricas y patrones observados.

En conjunto, la configuración detallada de Azure Storage Accounts y File Shares garantiza un almacenamiento en la nube seguro, eficiente y escalable para DataTech, cumpliendo con sus requisitos específicos de capacidad, rendimiento y seguridad.

4. Configuración entre VNets

4.1 Diseño de VNets y Subredes

En la construcción del diseño de Virtual Networks (VNets) y subredes para la arquitectura de DataTech, nos enfocamos en la creación de una infraestructura de red que proporcione la conectividad necesaria entre los diferentes componentes, al tiempo que garantiza un aislamiento adecuado para fortalecer la seguridad y la eficiencia operativa.

4.1.1 Definición de VNets y Subredes

4.1.1.1 VNets

Creamos múltiples Virtual Networks para segmentar lógicamente la infraestructura de DataTech. Estos VNets están diseñados de acuerdo con la distribución lógica de los servicios y aplicaciones.

4.1.1.1.1 VNet para Aplicaciones Web

Un VNet específico se dedica a las aplicaciones web de DataTech, asegurando una separación clara y proporcionando un entorno aislado para estas aplicaciones.

4.1.1.1.2 VNet para Bases de Datos

Otro VNet se reserva para las bases de datos, proporcionando un entorno dedicado y aislado para garantizar la seguridad y el rendimiento de las operaciones de base de datos.

4.1.1.1.3 VNet para Almacenamiento

Un tercer VNet se configura exclusivamente para las necesidades de almacenamiento, garantizando una conectividad eficiente y segura para la gestión de archivos y datos no estructurados.

4.1.1.2 Subredes

Dentro de cada VNet, definimos subredes específicas para albergar diferentes componentes de la arquitectura. Esto asegura una segmentación clara y permite la aplicación de reglas de conectividad específicas a cada conjunto de recursos.

4.1.1.2.1 Subred para Aplicaciones Web

Configuramos una subred dedicada para las aplicaciones web, asignando rangos de direcciones IP específicos y estableciendo reglas de conectividad para permitir el tráfico necesario.

4.1.1.2.2 Subred para Bases de Datos

Creamos una subred exclusiva para las bases de datos, asegurando un entorno aislado y aplicando reglas de conectividad específicas para la comunicación segura entre las aplicaciones y las bases de datos.

4.1.1.2.3 Subred para Almacenamiento

Establecemos una subred específica para el almacenamiento, garantizando una conectividad eficiente y segura para la gestión de archivos y datos no estructurados.

4.1.2 NSG y Conectividad

4.1.2.1 Network Security Groups (NSG)

Implementamos NSGs en cada subred para controlar el tráfico de red. Definimos reglas específicas para permitir o denegar el acceso a los recursos, asegurando una postura de seguridad robusta.

4.1.2.1.1 Reglas Específicas

Configuramos reglas en los NSGs para permitir solo el tráfico esencial para el funcionamiento de cada componente. Esto incluye reglas detalladas para la comunicación entre aplicaciones web y bases de datos, así como entre aplicaciones web y servicios de almacenamiento.

4.1.2.2 Conectividad
Establecemos reglas de conectividad entre las diferentes subredes y VNets. Garantizamos que solo las comunicaciones necesarias estén permitidas, manteniendo un aislamiento adecuado y reduciendo la superficie de ataque.

4.1.3 Seguridad y Enrutamiento
4.1.3.1 Segmentación de Redes
Implementamos la segmentación de redes mediante la asignación de VNets y subredes específicas para cada componente. Esto reduce la exposición de recursos críticos y limita la propagación de amenazas.

4.1.3.2 Enrutamiento Adecuado
Configuramos las tablas de enrutamiento para guiar el tráfico de manera eficiente entre las subredes y VNets. Aseguramos que el enrutamiento sea adecuado para la arquitectura específica de DataTech, evitando posibles cuellos de botella.

5. App Service
Para albergar las aplicaciones web de DataTech, hemos implementado Azure App Service, ofreciendo una configuración detallada para cumplir con los requisitos de escalabilidad, seguridad y operación sin problemas.

5.1 Selección de Planes de Servicio
5.1.1 Análisis de Requisitos
Realizamos un análisis exhaustivo de los requisitos de rendimiento, capacidad y características específicas de las aplicaciones web de DataTech. Basándonos en esta evaluación, seleccionamos los planes de servicio de Azure App Service que mejor se ajustan a las necesidades identificadas.

5.1.2 Planes de Servicio Seleccionados
Elegimos el plan de servicio adecuado, considerando aspectos como el número de instancias, la capacidad de proceso, la memoria y el rendimiento de la red. Por ejemplo, optamos por el plan Premium para garantizar características avanzadas como la asignación dedicada de instancias y mayor capacidad de almacenamiento.

5.2 Configuración de Dominios Personalizados
5.2.1 Registro de Dominios
Facilitamos la integración de dominios personalizados para las aplicaciones web de DataTech. Registramos los dominios relevantes a través de Azure Domain Services y configuramos los registros DNS correspondientes para dirigir el tráfico de manera eficiente a las aplicaciones web.

5.2.2 Configuración de Dominios en App Service
Dentro de Azure App Service, configuramos los dominios personalizados para cada aplicación web. Establecemos reglas de redirección y configuramos la fuerza del cifrado SSL para garantizar la seguridad de las comunicaciones.

5.3 Certificados SSL
5.3.1 Adquisición de Certificados
Adquirimos certificados SSL de entidades de certificación confiables para cada dominio personalizado utilizado por DataTech. Garantizamos que los certificados cumplen con los estándares de seguridad y cifrado necesarios.

5.3.2 Implementación en App Service
Integramos los certificados SSL adquiridos en Azure App Service. Configuramos la asignación de certificados a cada aplicación web para habilitar conexiones seguras mediante el protocolo HTTPS.

5.4 Escalabilidad Automática
5.4.1 Configuración de Escalabilidad
Implementamos la escalabilidad automática en Azure App Service, basada en reglas predefinidas y métricas específicas. Configuramos umbrales de carga para aumentar o disminuir dinámicamente el número de instancias según la demanda del usuario.

5.4.2 Monitoreo Continuo
Establecemos un sistema de monitoreo continuo utilizando Azure Monitor para supervisar las métricas de rendimiento y carga. Configuramos alertas automáticas para detectar cualquier anomalía en la carga y activar acciones de escalabilidad según sea necesario.

5.5 Integración con Servicios de Bases de Datos
5.5.1 Configuración de Conexiones
Configuramos las conexiones entre las aplicaciones web y los servicios de bases de datos. Utilizamos las cadenas de conexión seguras y aplicamos el principio de least privilege al asignar permisos de acceso mínimos necesarios.

5.5.2 Pruebas de Integración
Realizamos pruebas exhaustivas para garantizar la integridad y eficiencia de las conexiones entre las aplicaciones web y las bases de datos. Validamos la operación sin problemas y la seguridad de la transmisión de datos.

Medidas de Seguridad Implementadas

Con el objetivo de fortalecer la seguridad en la infraestructura de DataTech, hemos implementado medidas específicas que se alinean con los distintos aspectos del diseño en la nube. A continuación, detallamos la aplicación de estas medidas en relación con los puntos previamente establecidos:

1. Principio de Least Privilege
Aplicación en Máquinas Virtuales (Punto 1)
Selección del Tamaño y Tipo: Los permisos asignados a las máquinas virtuales siguen el principio de least privilege, garantizando que solo tengan acceso a recursos y operaciones necesarios para su función específica.
Aplicación en Bases de Datos (Punto 2)

Configuración de Conexiones: La asignación de privilegios en las conexiones entre aplicaciones y bases de datos se basa en el principio de least privilege, asegurando que solo se otorguen los accesos mínimos requeridos.
Aplicación en App Service (Punto 5)
Configuración de Dominios Personalizados: Los permisos de acceso a los dominios personalizados se gestionan según el principio de least privilege, garantizando que solo las aplicaciones web necesarias tengan acceso.

2. Modelo Zero Trust

Aplicación en Configuración de VNets (Punto 4)
Segmentación de Redes: La implementación del modelo zero trust se refleja en la segmentación de redes, donde cada interacción entre VNets se valida de forma independiente antes de permitir el acceso.
Aplicación en Configuración de App Service (Punto 5)
Configuración de Conexiones: El modelo zero trust se aplica en la configuración de conexiones entre las aplicaciones web y los servicios de bases de datos, asegurando que cada interacción sea validada antes de permitir el acceso.

3. Segmentación de Redes y NSG (Network Security Groups)

Aplicación en Configuración de VNets (Punto 4)
NSG y Conectividad: Los NSGs se utilizan para reforzar la segmentación de redes, permitiendo únicamente las conexiones necesarias entre subredes y VNets.
Aplicación en Configuración de Storage Account (Punto 3)
Control de Acceso: Las reglas de NSG se implementan en las subredes que acceden a Azure Storage Accounts, garantizando la seguridad y limitando la exposición de recursos.

4. Encriptación

Aplicación en Configuración de Storage Account (Punto 3)
Encriptación: La encriptación se aplica tanto en reposo como en tránsito en Azure Storage Accounts, asegurando la protección de los datos no estructurados y archivos almacenados.
Aplicación en Configuración de Bases de Datos (Punto 2)
Seguridad Avanzada: La encriptación se implementa como parte de las medidas de seguridad avanzada en las bases de datos, proporcionando una capa adicional de protección para los datos almacenados.

Referencias

Máquinas Virtuales:

- **Tamaños de VM de Azure:**

Lauradolan. (2023, June 15). VM sizes - Azure Virtual Machines. Microsoft Learn. https://learn.microsoft.com/en-us/azure/virtual-machines/sizes

- **Grupos de Disponibilidad**

Anaharris. (2023, September 22). What are Azure availability zones? Microsoft Learn. https://learn.microsoft.com/en-us/azure/reliability/availability-zones-overview?tabs=azure-cli

- **Escalabilidad automática**

Ju-Shim. (2023, April 11). Azure Virtual Machine Scale Sets overview - Azure Virtual Machine Scale Sets. Microsoft Learn. https://learn.microsoft.com/en-us/azure/virtual-machine-scale-sets/overview

Bases de Datos IaaS y PaaS:

- **Azure SQL Database**

MashaMSFT. (n.d.). Azure SQL Database documentation - Azure SQL. Microsoft Learn. https://learn.microsoft.com/en-us/azure/azure-sql/database/?view=azuresql

Storage Account - Fileshare:

- **Azure Storage Accounts:**

MashaMSFT. (n.d.). Azure SQL Database documentation - Azure SQL. Microsoft Learn. https://learn.microsoft.com/en-us/azure/azure-sql/database/?view=azuresql

- **File Shares en Azure Storage**

Khdownie. (2023, January 20). Introduction to Azure files. Microsoft Learn. https://learn.microsoft.com/en-us/azure/storage/files/storage-files-introduction

Configuración entre VNets:

- Azure Virtual Network documentation:

Asudbring. (n.d.). Azure Virtual Network Documentation - Tutorials, quickstarts, API references. Microsoft Learn. https://learn.microsoft.com/en-us/azure/virtual-network/

App Service:

- Azure App Service documentation:

SyntaxC. (n.d.). Azure App Service documentation - Azure App Service. Microsoft Learn. https://learn.microsoft.com/en-us/azure/app-service/