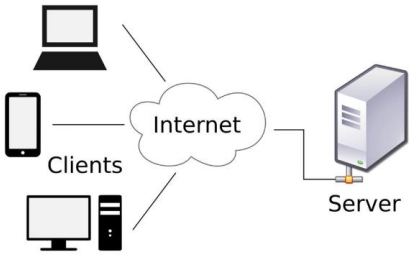
Azure AZ-900

Introducción

Modelo Cliente-servidor

El modelo cliente-servidor es un modelo que nos ayuda a saber el funcionamiento de una aplicación, donde los clientes hacen uso de servicios proporcionados por el servidor



Modelos de servicios.

On-Premise (IT Tradicional)

El modelo On-Premise hace referencia a cuando la compañía tiene sus propios servidores en un lugar y ellos se encargan al 100% de mantenimiento, OS, almacenamiento, etc.

- Escalado limitado
- Pago de electricidad, refrigeración, etc.
- Añadir software y sustituir cuando es necesario.
- Sin prevención para posibles catástrofes.
- Supervisar un equipo 24 horas.
- Control total.

Cloud Computing (nube)

Con Cloud Computing los problemas de mantenimiento, OS y persistencia del servidor se encargará una empresa externa, Azure te renta los servidores y servicios y te cobra por ello.

- Plataforma de servicios pagando solo por lo que se usa.
- Eliges la capacidad de tus servidores.
- Acceso a recursos al instante.
- Fácil acceso

Modelos de pago

- Por tiempo y capacidad de computación.
- Por almacenamiento.
- Por transferencia de datos fuera de Azure.

Ventajas de Cloud

- Cambia el gasto de capital (CAPEX) por gasto operativo (OPEX) (compra vs renta).
- Saber la capacidad exacta de cómputo que necesitas.
- Aumento de velocidad, agilidad y escalabilidad.
- No hay gasto en mantenimiento.
- Disponibilidad global rápida.

Tipos de Cloud

- *Privado:* No expuestos al público, satisface necesidades empresariales específicas.
- *Publico*: Controlada por proveedor de servicios (AWS, Azure, Google Cloud).
- *Hibrido*: Puedes tener servidores tanto en tu oficina como en Azure a la vez, aprovechando el potencial de ambos.

Tipos de servicios de Cloud

IAAS – Infrastructure as a Service

Se renta una infraestructura virtualizada de un servidor, no te encargas del aspecto físico de servidor, pero si configuras el OS, aplicaciones, actualizaciones.

- Máquinas virtuales en Azure (Azure VM)

PAAS – Platform as a Service

Ofrece una plataforma para el despliegue de la aplicación, solo te preocupas por el desarrollo, no por el OS del servidor, ni mucho menos el mantenimiento

- Azure App Service, Heroku, vercel

Azure AZ-900

SAAS – Software as a Service

El proveedor ofrece tanto la infraestructura y la aplicación, por lo que el solo eres el usuario final.

- Google docs (Word en la nube), Gmail, Microsoft 365

Definiciones

Gobernanza: Conjunto de políticas, procesos y controles que una empresa implementa para gestionar sus servicios en la nube de manera segura, eficiente y alineada con sus objetivos de negocio, (como acceso basado en roles, seguridad, costos, estandarización).

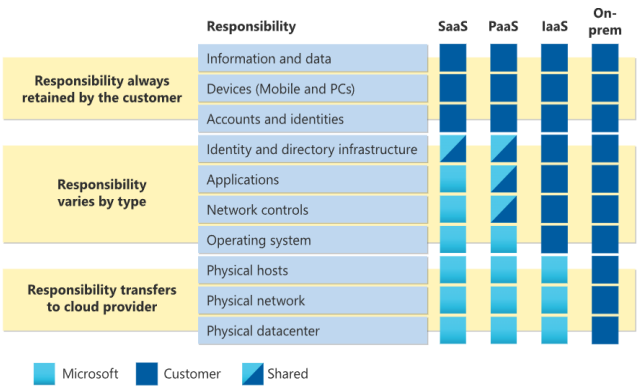
Confiabilidad: Capacidad de sus sistemas y servicios para funcionar de manera consistente y predecible sin interrupciones (alta disponibilidad).

Previsibilidad: Se refiere a la capacidad de las empresas para anticipar y planificar con confianza los servicios en la nube. Garantiza un rendimiento, costos y operaciones predecibles.

Manejabilidad: Refiere a las herramientas, servicios y prácticas que permiten a los usuarios controlar, administrar y supervisar sus recursos.

Seguridad: La seguridad en Azure se basa en un modelo de responsabilidad compartida, donde Microsoft protege la infraestructura y los clientes protegen sus datos y aplicaciones

Responsabilidad compartida



Infraestructura global

Regiones:

Se tienen regiones o *instalaciones en todo el mundo*, estas regiones tienen o pueden no tener algunos servicios, ser más caras o baratas, cada región se divide en zonas de disponibilidad (AZ), cada región está aislada de las demás (us-east-1).

- **Emparejadas:** Pares de regiones de Azure que se agrupan para alta disponibilidad. Se empareja con otra región dentro de la misma ubicación geográfica, para que se mantengan separadas físicamente para protegerse contra desastres (puedes replicar datos en esa región par).
- **Soberanas:** Nubes completamente aisladas, diseñadas para entidades con requisitos estrictos de soberanía, como gobiernos o industrias específicas.

Zonas de disponibilidad AZ:

Dentro de una región, existen varias zonas de disponibilidad. Son centros de datos separados físicamente, pero conectados a baja latencia.

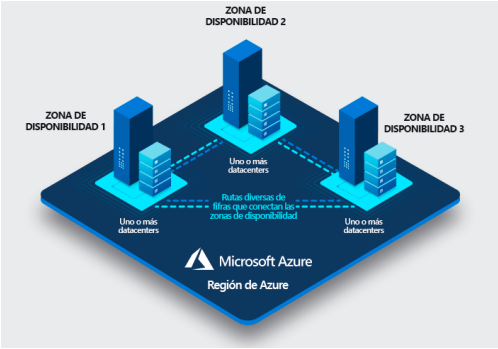
Es una agrupación lógica de *uno o más centros de datos* que están físicamente separados.

Región

├─ AZ1 (data centers separados)

├─ AZ2 (otro data center)

└─ AZ3 (otros más)



Azure AZ-900

Punto de presencia:

Un Punto de Presencia (PoP) es una ubicación física en la red, compuesta por infraestructura de telecomunicaciones diseñada para distribuir y optimizar el tráfico de datos entre los usuarios finales y la red global del proveedor.

Reduce la distancia 'lenta' en Internet público y usa la red privada rápida de Azure para llegar a regiones lejanas.

Recursos y grupos

Recurso:

Es todo aquel servicio real ofrecido por Azure que se consume y se paga por ello.

- Máquina virtual
- Base de datos SQL
- Storage account
- App Service
- VNet
- Key Vault

Grupo de recursos:

Es un contenedor que contiene recursos relacionados a un proyecto para su fácil administración, por ejemplo, un servidor, una base de datos y un front que conforma una misma app.

Solo organiza, etiqueta y administra.

- Aplicar permisos (RBAC)
- Aplicar políticas (Azure Policy)
- Borrar todo junto

Suscripciones:

Una suscripción es la cuenta de cobro y el contenedor más grande de administración en Azure.

Es donde:

- Se facturan los recursos
- Se aplican límites y cuotas
- Se configuran permisos de alto nivel

Todo lo que creas en Azure vive dentro de una suscripción.

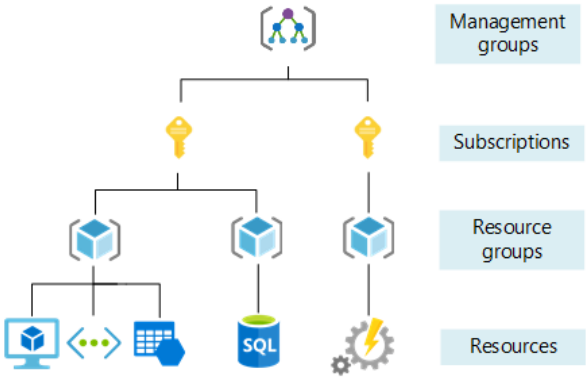
Sirve para:

- Separar costos por proyectos.
- Asignar permisos diferentes.
- Evitar borrar recursos por accidente.
- Tener límite de uso.

```
Suscripción: Proyecto A (facturación + permisos)
└── Grupo de Recursos: Sistema de Ventas
        ├── Recurso: Base de datos SQL
        ├── Recurso: App Service (hosting web)
        └── Recurso: Máquina Virtual servidor
```

Grupos de administración:

Un grupo de administración es un contenedor que permite organizar varias suscripciones para aplicar políticas, permisos y control de manera centralizada. Puedes aplicar *Azure Policy, roles y permisos* a las suscripciones dentro del grupo de una sola vez.



Azure AZ-900

Tipos de Servicios

Globales: Estos servicios no dependen de la región donde vivan tus recursos, y muchas veces tienen PoPs alrededor del mundo.

- Azure Active Directory (Azure AD)
- Azure Policy & Blueprints
- Azure Traffic Manager
- Azure Front Door
- Azure DNS
- Azure Resource Manager (ARM)
- Azure Monitor / Log Analytics / Application Insights (parte global)
- Azure Key Vault

Regionales: Están disponibles o no, dependiendo de la región donde se vaya a crear, que son los demás servicios que no son globales.

Formas de usar Azure

Azure Portal: Es la versión web para usar Azure en vez del Azure CLI, nos permite interactuar con todo lo que ofrece.

Azure CLI / Azure PowerShell: Ofrece una línea de comandos en consola para la crear recursos y administrarlos.

Azure SDK / API: Para interactuar con Azure desde tu código de programación.

Puedes usar la CLI directamente desde el Azure Portal con ***Cloud Shell*** que requiere un recurso para almacenamiento.

También puede usarse desde la ***Azure Mobile App*** para usar Azure directamente desde el teléfono.

Plantilla de Azure Resource Manager (ARM)

Son archivos JSON que describen la infraestructura y la configuración de una solución en Azure, permitiendo la implementación declarativa y automatizada de recursos.

Ejemplo de plantilla de arquitectura:

```
{
  "$schema": "...",
  "parameters": {
    "vmName": { "type": "string" }
  },
  "resources": [
    {
      "type": "Microsoft.Compute/virtualMachines",
      "name": "[parameters('vmName')]",
      "location": "eastus",
      "properties": {
        "hardwareProfile": { "vmSize":
"Standard_B1s" }
      }
    }
  ]
}
```

Servicios de Azure

Azure Advisor

Es un servicio consultor personalizado en la nube para seguir las mejores prácticas del uso de Azure para mejorar la rentabilidad, confiabilidad y rendimiento

El servicio de Advisor nos recomienda como:

- Reducir gastos innecesarios.
- Aumentar la seguridad.
- Confiabilidad (recomendaciones para evitar que nuestra app se caiga).
- Aumentar el rendimiento.

Azure Virtual Machines (VM)

Es un servicio (***IaaS***) de computación en la nube de Microsoft Azure que te permite crear y administrar máquinas virtuales (VM) con sistemas operativos como Linux y Windows, aquí puedes alojar tus aplicaciones de servidor (HTTP o análisis de datos).

Con VM puedes:

- Balancear cargas y auto escalar (horizontal y verticalmente).
- Automatizar el aprovisionamiento de máquinas como necesites.
- Administrar la conexión de red de las máquinas.

Puedes elegir el tamaño, la capacidad de procesamiento, la imagen de sistema operativo al iniciar, un script inicial.

También genera un par de claves para poderte a conectar a tu máquina virtual por SSH.

Cuando crea una máquina virtual, también se crean automáticamente los recursos:

- Ip pública.
- Grupos de seguridad.
- Red virtual.
- Interfaz de red.
- Clave SSH.
- Network watcher.

Estos recursos también se cobran, por lo que, para eliminar una máquina virtual, se recomienda eliminar la maquina y todo lo relacionado (el grupo de recursos completo).

Para pagarlas se puede pagar con:

- Pago por uso.
- Planes de ahorro (1-3 años) para cargas constantes de largo plazo.
- Instancias reservadas (1-3 años) similar a plan de ahorro para empresas con varias maquinas
- Instancias spot (más baratas porque son sobrantes, pero pueden ser interrumpidas como subasta)

Formas de asignación de la maquina

- Compartir uso de hardware con otros usuarios a través de la virtualización de un servidor
- Host dedicado (un servidor físico completo para una empresa)
- Instancias aisladas (no compartes el host con otros clientes, pero no rentas el host completo)
- Reservar capacidad a petición (apartas recursos para asegurarte que habrá capacidad disponible).

Scale Sets (Conjunto de escalado)

Conjunto de máquinas virtuales idénticas para balancear las cargas y se pueden gestionar como una única unidad.

Se puede automatizar si hay mucha demanda, que se alce una máquina virtual idéntica en el scale set automáticamente.

Tipo de escalado:

Vertical: Aumentas la capacidad de la/las máquinas virtuales como RAM, procesamiento o memoria para soportar la carga (obviamente la capacidad es limitada por la tecnologia).

Horizontal: Aumentas la cantidad de máquinas virtuales, (si 5 no aguantan, 10 si lo haran)

Gracias al escalado horizontal, podemos tener varias máquinas idénticas en diferentes zonas de disponibilidad o incluso regiones, para que, si falla una zona, aun pueda funcionar la aplicación.

Elasticidad: No solo crecen en función de la carga, sino que también puedes decrecer si no hay demanda.

Agilidad: Se usa este término para referirse a que estos cambios de agregar o quitar, son rápidos y eficientes gracias a la nube.

Azure App Services

Para evitar toda la configuración de una arquitectura de una aplicación para los desarrolladores, se usa App Services (***PaaS***),

App Services usa otros servicios como:

- Azure Virtual Machines
- Networking (VNet, Load Balancer, IP, DNS interno)
- SQL Databases
- Storage (Blob / Files / Queue)
- Azure Front Door / Application Gateway (Load balancer)
- Monitoring / Diagnostics (Azure Monitor, Application Insights)
- SSL / Key Vault (opcional)

Al ser una Plataforma como servicio, no te preocupas por configurar el load balancer o el sistema operativo de las VM.

Se usa para Web Apps, Web Apps con contenedores, API apps.

Azure Container Registry

Para publicar en un repositorio privado tus imágenes de Docker, similar a lo que haría DockerHub, el cual es un repositorio público de imágenes de Docker, Azure Container Registry es útil para publicar tus imágenes y versiones de Docker.

Azure Container Instances

Permite ejecutar las imágenes en un contenedor sin necesitar una máquina virtual completa, levantas un contenedor con una imagen pública o tuya privada para ejecutar una aplicación. También expone una ip publica para que puedas conectarte al contenedor.

ACI se ejecuta bajo demanda, por lo que el contenedor solo se levanta cuando lo solicitas, si no se solicita el contenedor por sí solo no genera gasto, a diferencia de una máquina virtual que cobra solo por estar encendida, este ejecutando o no.

Azure Kubernetes Service

Es el servicio de Kubernetes totalmente gestionado por Azure para:

- Escalar automáticamente los contenedores.
- Desplegar aplicación rápidamente en los contenedores
- Configurar los contenedores para que trabajen en conjunto

Azure Virtual Desktop

Es una plataforma de virtualización de aplicaciones y escritorios en la nube de Microsoft que permite a los usuarios acceder a escritorios remotos de Windows desde cualquier lugar y dispositivo.

Azure Function

Servicios serveless (ya no es necesario gestionar servidores, no significa que no haya servidores, solo que no se van a gestionar)

- Escribes una función (Python, C#, JavaScript).
- Subes la función a la nube (Azure Functions o AWS Lambda).
- Configuras un trigger (desencadenador): HTTP request, Mensaje en cola, tareas programadas.
- La plataforma ejecuta tu función solo cuando se activa el trigger y no te preocupas de nada más.

Azure Virtual Network

Crea una red virtual en la nube de Azure para la conexión de recursos, por ejemplo, conectar una máquina virtual con una base de datos, aísla los servicios para que solo tu y las persones que autoricen accedan a ellos, también puedes conectarla a tu red local de tu empresa y controla el tráfico con seguridad avanzada.

Azure AZ-900

Puedes tener subredes públicas (desde internet) y privadas.

Puedes tener 2 vnets emparejadas de azure, siempre y cuando no se empalmen las ips.

Una máquina virtual claro que puede conectarse a una base de datos sin una VNet, pero esta conexión saldría a internet, sin embargo, con una VNet, tendríamos un comportamiento como una VLAN, por lo que la latencia sería mucho menor, al ser una conexión mas directa.

Grupos de seguridad

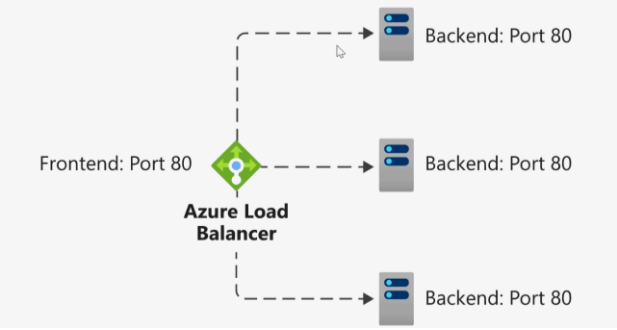
Controla el trafico de entrada y salida a recursos de azure para permitir y denegar el trafico mediante reglas de entrada y salida (como una Access list en redes, donde hay reglas y se ordenan por prioridad), las reglas están conformadas por:

- Origen (red o ip especifica)
- Destino (red o ip especifica)
- Permitir o denegar
- Protocolo o puertos al que aplica la regla

Azure Load Balancer

Distribuye el tráfico de red entre varias máquinas virtuales para mejorar el rendimiento y la disponibilidad de las aplicaciones. Funciona en la capa 4 (TCP/UDP) del modelo OSI y puede enrutar el tráfico a instancias saludables.

Esto es para cuando hay muchos usuarios usando los servidores, sea capaz de redireccionar el tráfico de forma equitativa a las máquinas virtuales y todo el peso no caiga en una sola máquina.



Azure VPN Gateway

Azure VPN Gateway es un servicio que conecta tu red privada (o tus dispositivos) con una red virtual en Azure (VNet) de manera segura a través de una VPN cifrada (por Internet).

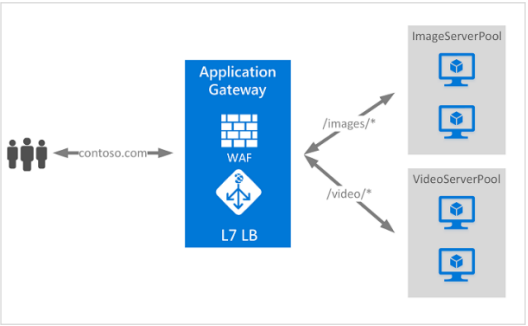
- ***VPN S2S (Site to Site):*** Permite conectarte a las redes locales a redes de Azure de forma directa.
- ***VPN P2S (Point to Site):*** Permite conectarte desde un dispositivo local a redes de Azure de forma directa.

Azure Application Gateway

Es un balanceador de carga a nivel de aplicación. Sirve para dirigir el tráfico HTTP/HTTPS que llega a tus aplicaciones en Azure.

Igual que un load balancer, pero enfocado a una capa 7, especializado en apps web, para redirigir a un recurso correcto.

- La solicitud HTTP llega al Application Gateway, no directamente a servidores.
- El Application Gateway analiza la solicitud HTTP.
- Según reglas, envía esa solicitud al servidor correcto:
  - ***/api/**** → a tus máquinas virtuales con la API
  - ***/imágenes/**** → a un almacenamiento de blobs por ejemplo
  - */* → a un servidor web.
- Luego, el Gateway devuelve la respuesta al usuario final.



Azure AZ-900

Azure Content Delivery Network (CDN)

Azure CDN es una red global de servidores distribuidos que almacena en caché (cachea) tu contenido cerca de los usuarios para que se cargue más rápido y consuma menos ancho de banda.

Los servidores perimetrales tienen una copia de tu sitio o archivos en muchas partes del mundo, para reducir la latencia entre tus usuarios alrededor del mundo. (Protege automáticamente contra DDos).

Azure Express Route

Es el servicio que da una forma directa de conectarte a la red de azure sin pasar por internet público, por lo que da mucha más seguridad y velocidad

Es una **conexión privada y dedicada** entre tu infraestructura local (tu empresa) y los servicios de Azure, ideal para la transferencia de grandes volúmenes de datos.

Azure Blob Storage

Blob = Binary large object

Azure Blob Storage es un servicio de almacenamiento de objetos en la nube de Microsoft Azure.
Sirve para guardar grandes cantidades de datos no estructurados, como archivos, audio, imágenes, videos, documentos, log files, backups o datos de aplicaciones.

- Escalable
- Disponible
- Protegido (con Entra ID o RBAC)
- Optimizado para datos grandes
- Administración de datos e inmutabilidad

Tipos de Blobs

- Bloque
- Append
- Page

Niveles de acceso en blob storage

- ***Hot:*** Para archivos accedidos frecuentemente pero que no duraran mucho guardados en el servidor (acceso más barato, almacenamiento más caro).
- ***Cold:*** Para archivos que se accederán menos, pero durarán más tiempo almacenados (acceso más caro, almacenamiento más barato).
- ***Archive:*** Tiene los costos más bajos, pero los tiempos de acceso son los más altos

Azure Disk Storage

Proporciona discos virtuales (VHD) de alto rendimiento para máquinas virtuales de Azure

Cuando creas una máquina virtual (VM) en Azure, necesitas almacenamiento para:

- Instalar el sistema operativo (Windows o Linux)
- Guardar datos, aplicaciones o archivos.

Ese almacenamiento se da a través de Azure Disk Storage, que crea discos virtuales (VHDs) conectados a la VM.

Tiene tasa de error anual de 0%, Azure administra las copias de seguridad y garantiza tamaño.

Tipos:

- ***HDD:*** Mecánico perfecto para backups
- ***SDD Estándar:*** Relación costo y rendimiento
- ***SDD Premium:*** De alto rendimiento ideal para base de datos.
- ***Ultra Disk:*** Workloads muy exigentes (bases de datos grandes)

Azure File Storage

Es un servicio de almacenamiento de archivos en la nube de Microsoft que permite crear recursos compartidos de archivos seguros y sin servidor.

Azure AZ-900

Permite crear carpetas compartidas en la nube, accesibles desde varios equipos, servidores o servicios, como si fueran un disco de red tradicional.

- Standard File Share (HDD)
- Premium File Share (SDD)

Perfecto para el acceso de archivos desde máquinas virtuales de Azure o desde servidores on-premise.

Azure Archive Storage

Para datos raramente accedidos, que necesitan almacenarse por un largo periodo de tiempo.

Recomendado para guardar archivos de cumplimiento legal que raramente se van a necesitar, pero se requiere tenerse, además de que Archive Storage es muy seguro, es un servicio que trabajo sobre blob, por lo que muchas características de Blob Storage funcionan igualmente aqui.

Redundancia de almacenamiento:

Si una copia falla de los datos, la otra esta disponible, Azure Storage siempre crea multiples copias de tus datos

Opciones de redundancia

- Una única zona, en misma región (LRS)
- En múltiples zonas, en misma región (ZRS)
- En múltiples regiones, solo una zona por región (GRS)
- En múltiples regiones y múltiples zonas (GZRS)

A mayor redundancia mayor costo, en todas las opciones, siempre tendrás un mínimo de 3 copias.

Azure Data Box

Para migraciones de datos a Azure cuando hay una gran cantidad de datos, pero un ancho de banda muy limitado para esta transferencia.

Microsoft te envia un dispositivo de almacenamiento físico a donde estas, para que no requieras internet para transferencia de datos hacia/desde Azure.

Tu colocas tus archivos en ese dispositivo (o los recoges) y Microsoft luego recoge ese dispositivo para que lo veas reflejado en Azure.

- Solicitas el dispositivo físico y te llega.
- Copias tus datos.
- Envías el dispositivo de vuelta.
- Microsoft carga los datos a Azure.
- Microsoft borra los datos del dispositivo físico.

Azure Migrate

Es una plataforma de Azure que te ayuda a descubrir, evaluar y migrar tus servidores, bases de datos, aplicaciones y máquinas virtuales desde tu entorno local o de otra nube hacia Azure.

Antes de migrar, normalmente no sabes:

- Qué servidores tienes ni cómo dependen unos de otros.
- Cuánto costará tenerlos en Azure.
- Si son compatibles o necesitan cambios

Azure Migrate analiza todo eso automáticamente y te da un plan detallado para migrar sin errores.

Azure AZ-900

Azure Cosmos DB

(PaaS) Servicio de base de datos NoSQL ya dada por azure, es totalmente administrado por Azure y escalable, permite guardar documentos, grafos, etc.

Tiene una replicación rápida para tener copias de tus datos en diferentes regiones de Azure.

Azure SQL Database

Azure SQL Database es una base de datos relacional en la nube de Microsoft, basada en SQL Server, pero totalmente administrada por Azure, por lo que es escalable y con alta disponibilidad con redundancias automáticas de Azure y segura (con Firewall integrado).

- Guarda los datos en tablas con filas y columnas (como en Excel).
- Puedes definir relaciones entre tablas (por ejemplo, un cliente puede tener varios pedidos).
- Usa el lenguaje T-SQL (Transact-SQL) para consultar y modificar los datos

Introducción a Autenticación y Autorizaciones

Autenticación: Saber si existe en el sistema.

Autorización: Ya sabemos que existe, ver si tiene los permisos necesarios

Política: Conjunto de reglas para un grupo.

Para comprender el funcionamiento de servicios como Entra ID o Entra Connect, necesitaremos entender Active Directory.

Active Directory

Active Directory es un servicio de directorio utilizado en empresas para administrar sus usuarios, equipos y recursos dentro de una red. Los equipos y usuarios pertenecen a un dominio, que funciona como una identidad organizativa común.

A través de Active Directory es posible:

- Crear y gestionar usuarios y grupos
- Definir permisos de acceso a recursos (accesos, impresoras, aplicaciones)
- Aplicar restricciones mediante GPO (Group Policy)

Las GPO (las reglas) se aplican al dominio o a unidades organizativas (OU, que dentro tienes los grupos de usuarios y usuarios,) permiten establecer reglas, como:

- Restringir la instalación de software
- Bloquear configuraciones del sistema
- Forzar políticas de contraseña
- Configurar el entorno de trabajo de los usuarios

LAS GPO NO SE APLICAN A USUARIOS O GRUPOS DE USUARIOS DIRECTAMENTE

El servidor que ejecuta Active Directory y aplica estas reglas se conoce como Controlador de Dominio (Domain Controller).
Este servidor se encarga de autenticar a los usuarios y validar sus permisos cada vez que inician sesión en una computadora perteneciente al dominio.

Azure Entra ID

"Microsoft Entra ID" es el nuevo nombre de Azure Active Directory (Azure AD).

Es el sistema de seguridad en la nube de Azure que gestiona quién eres (identidad) y a qué recursos puedes acceder (autenticación y autorización) dentro de Azure, Microsoft 365, y otras aplicaciones, es similar a Active Directory, pero en Azure.

Funciones:

- Autenticación (Login)
- Autorizacion (Permisos a recursos)
- Gestión de usuarios y grupos
- Single Sign-On (SSO) (única constraseña)
- Integración con apps externas

Azure AZ-900

- Seguridad avanzada

Es un gestor de inicio de sesiones de aplicaciones externas a azure

- Microsoft Entra ID administra las identidades (usuarios, grupos, roles).
- Azure RBAC (Role-Based Access Control) usa esas identidades para controlar permisos sobre los recursos (VMs, Storage, Bases de datos, etc.).

Microsoft Entra ID
|
├── Usuarios y grupos (para manejar auth en apps tuyas AD)
|
└── Se integran con Azure RBAC (IAM en AWS)
  |
  ├── Asignas roles a usuarios o grupos
  | ├── Owner
  | ├── Contributor
  | └── Reader
  |
  └── Esos roles definen qué pueden hacer en recursos Azure como VM, Storage, SQL, App Services, etc.

Entra ID = Active Directory (identidades, login, grupos)
RBAC = IAM (permisos sobre recursos)

Inquilino: Un inquilino (tenant) en Microsoft Entra ID es, en esencia, una organización o espacio aislado de identidades dentro del sistema de Microsoft (una instancia solita para tu empresa), *un inquilino puede tener varias suscripciones, una suscripción siempre pertenece a un inquilino*.

Imagina que Microsoft Entra ID es un edificio enorme (la nube de Microsoft).
Cada empresa u organización que usa Azure o Microsoft 365 tiene su propio piso exclusivo en ese edificio (un piso es un inquilino totalmente aislado de los otros, pero con permisos puede ir a visitar otro inquilino (piso)).

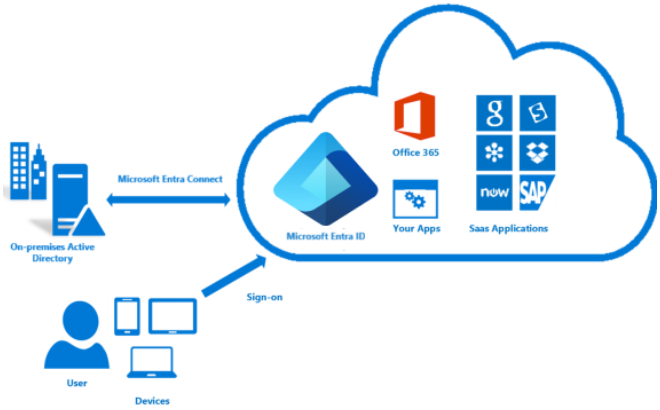
Entra ID puede integrarse con entornos híbridos (Azure + on-premises Active Directory) usando Azure AD Connect para sincronizar identidades, y aplicar autenticación y SSO de manera centralizada.

Lock: Protegen recursos de Azure, bloquean la eliminación o modificación de recursos.

Azure Entra Connect

Sincroniza tu Active Directory local con Azure Entra ID (grupos y usuarios, pero no sincroniza GPO, los permisos a accesos a recursos se tienen que crear).

- **Sincroniza usuarios, grupos y contraseñas (de local a Azure)**
- Permite inicio de sesión único (SSO)
- Conecta tu mundo on-premise con el cloud
- Seguridad avanzada (Multifactor y políticas condicionales)



Azure Entra Connect Health

Ayuda a supervisar y conocer mejor la infraestructura de identidad local, lo que garantiza la confiabilidad del entorno.

Entonces Azure AD Connect Health te avisa sobre:

- Alertas
- Logs
- Métricas de rendimiento
- Diagnósticos del servicio

Azure AZ-900

Confianza cero: Estrategia de seguridad para diseñar e implementar el siguiente conjunto de reglas de seguridad:

- Comprobación explicita (siempre se autoriza y auntentica).
- Acceso con privilegios mínimos necesarios para usuarios.
- Asunción de que hay brechas, se comprueban siempre todas las solicitudes.

Autenticación Multifactorial (MFA): Se solicita un proceso adicional para inicio de sesión, como pedir un código en el teléfono móvil o lectura de huella digitar extra.

Se exige siempre uno o varios métodos como:

- Algo que conoces (contraseñas).
- Algo que tienes (un código en tu telefono).
- Algo que forma parte de ti (huella o rostro).

Acceso Condicional: Solo dar acceso al destino en base a orígenes como:

- Pertenece a un grupo o usuario.
- Ubicación de la IP.
- Dispositivo.
- Aplicación.
- Microsoft Defender para nube

Single Sign-On (SSO): Método de autenticación que permite a usuarios iniciar sesión con solo una sola credencial en varios sistemas independientes.

Azure Active Directory Domain Services (Azure AD DS)

Servicio gestionado por Azure que facilita la implementación de servicios de dominio en Azure.

Proporciona servicios de dominio tradicionales que se tenía en AD local, pero ahora, gestionados por Azure, como:

- LDAP
- Kerberos
- NTLM
- Controladores de dominio
- Un bosque AD administrado

Para aplicaciones normalmente legacy que necesitan estos servidores de dominio viejos.

Introducción a seguridad en Azure

Enpoint Privado: Una interfaz de red privada que conecta de manera segura un servicio de Azure (como una base de datos, almacenamiento, web app, etc.) a tu red virtual (VNet), sin pasar por Internet pública.

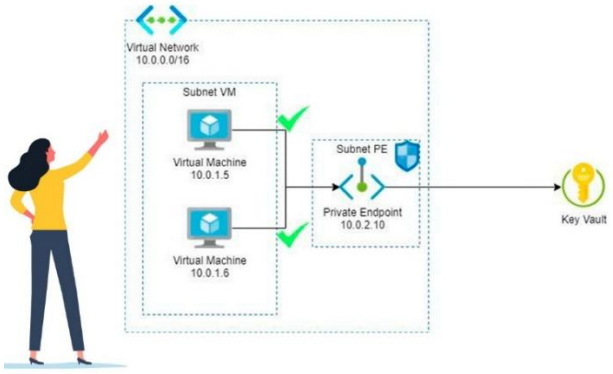
Supón que tienes:

- Una máquina virtual en una VNet (10.0.0.0/16).
- Una base de datos SQL de Azure (myapp.database.windows.net).

Sin Private Endpoint
Tu VM se conecta a la base de datos a través de Internet, usando la IP pública del servicio.

Con Private Endpoint
Creas un Private Endpoint para el SQL Server dentro de tu VNet (por ejemplo, 10.0.1.5). Entonces:

- Tu VM se conecta a esa IP privada.
- El tráfico viaja por la red privada de Azure, por lo que es más rápido y seguro.
- El servicio SQL ya no necesita exposición pública, aumentando la seguridad ante ataques.



Azure AZ-900

Azure Key Vault

servicio en la nube de Microsoft Azure diseñado para **almacenar y administrar de forma segura** secretos, claves de cifrado y certificados.

- **Guardas tus secretos en el Key Vault**
  Por ejemplo, guardas ahí la contraseña de tu base de datos o la clave de tu API.
- **Das permiso a quien puede usarlos**
  Tú decides qué personas o aplicaciones pueden abrir esa caja fuerte y leer las contraseñas dentro.
- **Tu aplicación los pide cuando los necesita**
  En lugar de tener la contraseña escrita en el código o en un *env* (lo cual es peligroso), se extraen encriptadas desde un SDK de azure con Key Vault.

Sin Key Vault: En tu código pones:

```
password = "1234abcd!
```

o lo extraes con un env en codigo

Con Key Vault:

Guardas la contraseña dentro del Key Vault.

En tu código con el SDK de Azure solo pones:

```
pswd = getSecretFromKeyVault("db-paswd");
```

Microsoft Defender for Cloud

Es una plataforma de seguridad en la nube que te ayuda a:

- Proteger tus recursos de Azure (máquinas virtuales, bases de datos, redes, etc.)
- Detectar vulnerabilidades y amenazas
- Dar recomendaciones para mejorar la seguridad
- Responder ante ataques o configuraciones inseguras

El servicio analiza tus recursos, detecta inseguridades y te da una puntuación de seguridad (Secure Score) con recomendaciones concretas, como cifrar conexiones, etc.

También tiene Defender Plans para detectar vulnerabilidades y protegerlos como Base de datos o máquinas virtuales.

Azure Policy

Ayuda a aplicar los estándares de una organización y evaluar el cumplimiento a escala, para poner políticas a los recursos

Si no quieres dejar que creen un recurso en X región, se usa Azure Policy

Azure Blueprints

Es una herramienta que sirve para definir, automatizar y aplicar un conjunto de configuraciones y recursos estándar en tus suscripciones o entornos de Azure.

Imagina que en tu empresa necesitas crear 10 entornos iguales (por ejemplo, para distintos proyectos o equipos), ejemplo:

Cada entorno debe tener:

- Una red virtual configurada
- Un grupo de recursos
- Políticas de seguridad
- Roles y permisos
- Un Key Vault y una base de datos

En lugar de hacerlo a mano cada vez, creas un Blueprint con todo eso definido.
Luego, cada vez que necesites un entorno nuevo, simplemente "aplicas el blueprint" y Azure lo crea automáticamente con las configuraciones correctas.

Usa internamente ARM para crear infraestructura con plantillas, pero combina y añade políticas, configuraciones y seguridad para los recursos.

Azure AZ-900

Azure Monitor

Azure Monitor es el servicio de monitoreo y observabilidad de Microsoft Azure.

Su función es recolectar, analizar y actuar sobre los datos de ***rendimiento y estado de tus recursos.***

- ***Recopila datos***
  Azure Monitor obtiene información de recursos, por ejemplo: Máquinas virtuales (CPU, RAM, disco, red), Bases de datos.
- ***Analiza los datos***
  Grafica los datos en dashboards e identifica tendencias o anomalías.
- **Actúa automáticamente**
  Puedes configurar alertas y acciones automáticas cuando algo se sale de los parámetros normales.

Se usa por ejemplo si:

- Si una VM supera el 90% de CPU → manda correo o mensaje a Teams.
- Si un servicio deja de responder → reinicia automáticamente el recurso.

Azure Service Health

Azure Service Health es un servicio gratuito que te notifica y muestra el estado de los servicios de Azure que tú estás usando.
Te avisa si algo anda mal en Azure por parte de Azure (por ejemplo, una caída, mantenimiento o problema regional) que podría afectar tus recursos.

Puedes configurar alertas personalizadas (por correo, SMS, Teams, webhook, etc.) para que te avise automáticamente si hay:

- Interrupciones de servicio (outages)
- Degradación de rendimiento
- Mantenimientos planificados
- Cambios importantes

Azure Cost Managment

Es la herramienta de Azure que sirve para ver, analizar y controlar tus gastos en la nube.

- Ver reportes y gráficos de consumo y costos por servicio o suscripción.
- Establecer **presupuestos y alertas** (por ejemplo: “avísame si gasto más de $500”).
- Detectar **recursos inactivos o sobredimensionados** para ahorrar dinero.
- Comparar costos reales vs. planeados.

Azure Pricing Calculator

Es una herramienta web que sirve para estimar cuánto te costará usar los servicios de Azure antes de crearlos.

- Permite seleccionar servicios (VMs, bases de datos, storage, etc.).
- Configuras región, tamaño, cantidad y horas de uso.
- Te muestra un costo mensual estimado.

El costo varía según la región

La transferencia de datos solo se cobra si es fuera de Azure

Azure AZ-900

Resumen importante para estudiar:

Conceptos Basicos

On-premise: Servidores en local

Cloud Computing: Servidores rentados por proveedor de servicios

---

Cloud privado: Servidores en local

Cloud público: Dado por un proveedor de servicios

Cloud Hibrido: Usa tanto local, como con proveedor como Azure

---

On-Premise: Todo lo administras tu

Iaas: Te dan tu computo, tu configuras todo menos lo físico

PaaS: Una plataforma donde subes tu app y ya, solo desarrollas (Vercel).

SaaS: Básicamente solo eres el usuario de la aplicación final.

En Azure y AWS pagas por:

- Tiempo/capacidad
- Transferencia fuera de Azure
- Almacenamiento

Usas Azure en 3 formas posibles

- **Azure Portal:** Es la versión web.
- **Azure CLI / Azure PowerShell:** Un cabron a puro comando de consola.
- **Azure SDK / API:** Para interactuar con Azure desde tu código de programación.

Azure tiene regiones alrededor del mundo para tener acceso a nivel global, dentro de regiones hay zonas de disponibilidad, en las zonas hay datacenters

- Region > Zonas de disponibilidad > Datacenters

Un punto de presencia no es un datacenter, es como un repetidor para acceder lo más cercano a la red de Azure

---

Un managment group maneja suscripciones (pagos por proyecto), las suscripciones tienen grupos de recursos, los grupos de recursos tienen recursos (los servicios de Azure)

Servicios más importantes

Azure Virtual Machines: Máquinas virtuales de servidor para rentar cómputo y subir por ejemplo backend.

Azure* Resource Manager*: Para desplegar tu arquitectura de forma rápida a base de una plantilla en JSON.

Azure Container Registry: Subir tus imagenes de Docker a Azure

Azure Container Instances: Correr contenedores con tus imágenes.

Azure App Services: Paas para solo subir tu web app sin problemas

Azure Function: Funciones ejecutadas en computo serveless, al momento.

Azure Virtual Network: Conectar con una red virtual (como LAN) tus recursos de Azure.

Grupo de seguridad: Decidir que IP se conectan a una VM y cuales salen

Azure Load Balancer: Distribuye peticiones en capa 4 para distintas VMs

Azure AZ-900

Azure Load Balancer: Distribuye peticiones en capa 4 para distintas VMs

Azure VPN Gateway: Conectarte a una red virtual de Azure (s2s -> red a red, s2p -> Azure a dispositivo)

Azure Application Gateway: Balanceador de carga capa 6 que decide en base al endpoint de la URL.

Azure Express Route: Conectarte a la red de azure sin pasar por internet público para gran volumen de datos

Azure Blob Storage: Almacenar fotos, videos, audios en servidores de Azure, puede usarla un VM para mandar a almacenar fotos de un sistema ahí.

- Hot: Mas barato el acceso
- Cold: Mas barato el almacenamiento
- Archive: Mas barato el almacenamiento que todos, pero lentísimo para acceder al archivo.

Azure Disk Storage: Lo usan las VM como disco duro, similar vaya, hay HDD y SDD

Azure Migrate: Asistente de ayuda para migrar de local a Azure, comparando y dando sugerencias.

Azure Cosmos DB: Base de datos en Azure no relacional (como Mongo por ejemplo)

Azure SQL Database: Base de datos en Azure relacional (como SQL Server por ejemplo)

Azure monitor: Para generar ***alertas y monitorear recursos*** en base a su estado “Una máquina virtual está al 90% de capacidad -> alerta”.

Azure Service Health: Si ***Azure mismo*** va a afectarte en un servicio, por este medio se te avisa.

Azure Advisor: Recomienda como reducir gastos, buenas prácticas y seguridad en tus recursos.

Lock: Protege recursos de Azure, ***bloquean la eliminación o modificación.***

Azure Blueprints: Sirve para crear entornos completos con ***políticas en masa*** (repetititvos).

Microsoft Entra ID: Sirve para gestionar ***usuarios, roles, grupos, contraseñas*** y accesos (con RBAC).

Azure Policy: Que se puede hacer, en ***donde*** y como, “No se puede crear VM en Mexico Central”

Entra ID con RBAC: Controla ***quién*** puede hacer qué, “desarrolladores y Juan no pueden crear VMs”

Atte: Luis Jesus Mata Ruiz ISC09B