1.1¿Qué es el cloud computing ?

El cloud computing permite “alquilar”en la nube un equipo con las características que quieras, el equipo está en un centro de datos de un proveedor de nube, en vez de físicamente con usted. Esto le permite pagar solo por los servicios que use. Además, otra persona se encarga del mantenimiento del equipo y de que funcione interrumpidamente. Cada proveedor de nube tiene su propia oferta de servicios, pero los servicios básicos que todos proporcionan son la potencia de proceso y el almacenamiento:

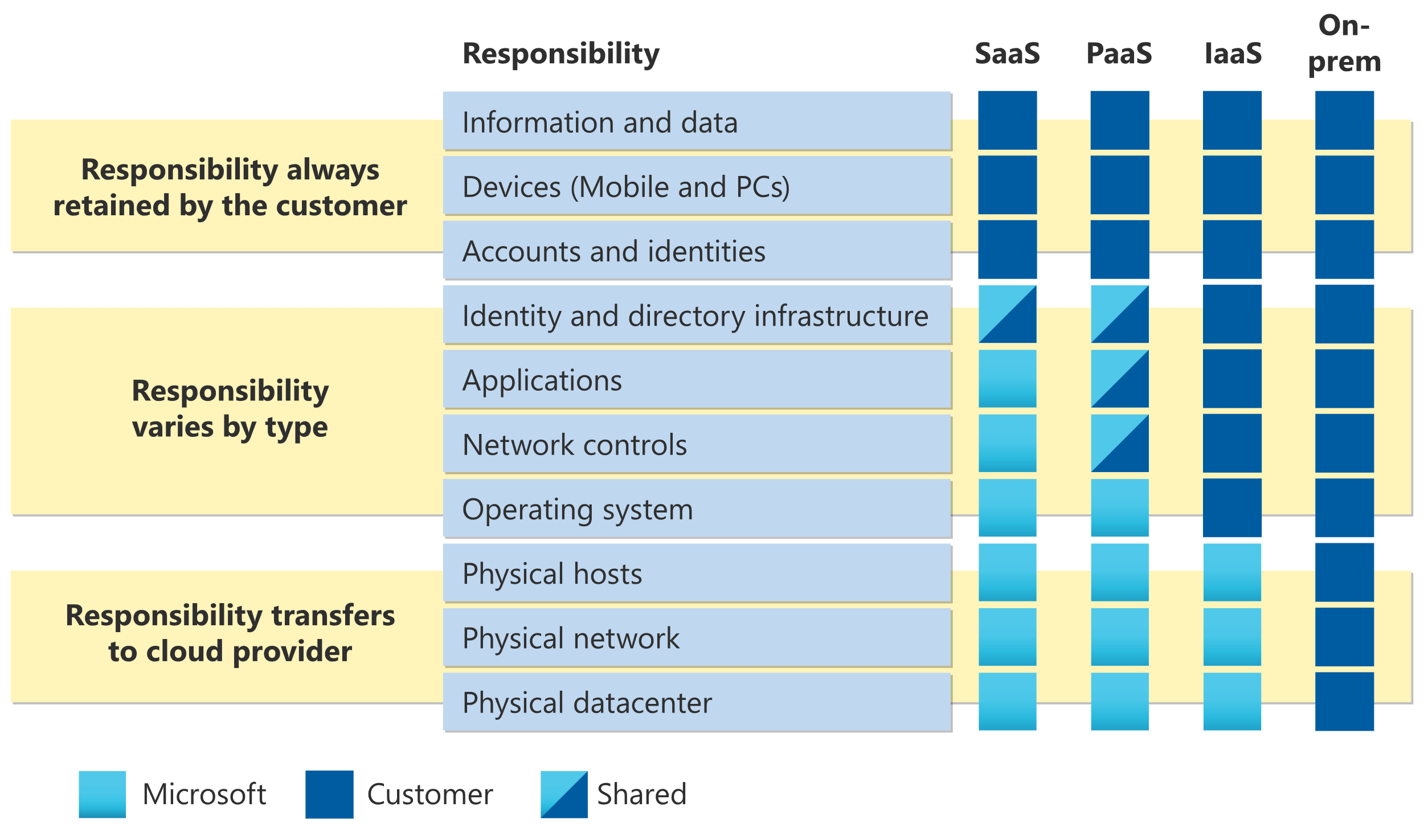
* La potencia de proceso es el volumen de proceso que puede asumir el equipo.
* El almacenamiento es el volumen de datos que puede guardar en el equipo

1.2modelo de responsabilidad compartida

El modelo de responsabilidad compartida está muy vinculado a los tipos de servicio en la nube:

infraestructura como servicio (IaaS),plataforma como servicio (PaaS) y software como servicio (SaaS).

IaaS sitúa la mayor responsabilidad en el consumidor y el proveedor de servicios en la nube es el responsable de los conceptos básicos de seguridad física, energía y conectividad. En el extremo opuesto, SaaS sitúa la mayor parte de la responsabilidad en el proveedor de servicios en la nube. PaaS, siendo un punto intermedio entre IaaS y SaaS, se encuentra en algún lugar del medio y distribuye uniformemente la responsabilidad entre el proveedor de nube y el consumidor.



Siempre será responsabilidad tuya:

* La información y los datos almacenados en la nube.
* Los dispositivos que pueden conectarse a la nube (teléfonos móviles, equipos, etc.).
* Las cuentas e identidades de las personas, servicios y dispositivos de la organización

El proveedor de nube siempre es el responsable de:

* El centro de datos físico
* La red física
* Los hosts físicos

El modelo de servicio determinará la responsabilidad de cosas como lo siguiente:

* Sistemas operativos
* Controles de red
* APLICACIONES
* Identidad e infraestructura

**1.3Definición de modelos en la nube**

Nube pública:Un proveedor de nube de terceros crea, controla y mantiene una nube pública.

Una nube híbrida es un entorno informático que usa nubes públicas y privadas en un entorno interconectado.

|  |  |  |
| --- | --- | --- |
| **Nube pública** | **Nube privada** | **Nube híbrida** |
| No hay gastos de capital para escalar verticalmente. | Las organizaciones tienen un control total de los recursos y la seguridad. | Proporciona la máxima flexibilidad. |
| Las aplicaciones pueden aprovisionarse y desaprovisionarse rápidamente. | Los datos no se colocan con los datos de otras organizaciones. | Las organizaciones determinan dónde se van a ejecutar sus aplicaciones. |
| Las organizaciones solo pagan por lo que usan. | Debe adquirirse hardware para la puesta en funcionamiento y el mantenimiento. | Las organizaciones controlan la seguridad, el cumplimiento o los requisitos legales. |
| Las organizaciones no tienen un control total de los recursos y la seguridad. | Las organizaciones son responsables del mantenimiento y las actualizaciones del hardware. |  |

Nubes múltiples: En un escenario de varias nubes, se usan varios proveedores de nube pública. Tal vez use diferentes características de diferentes proveedores de nube. O quizás haya iniciado su recorrido en la nube con un proveedor y esté en proceso de migración a otro proveedor.

La administración de la nube se hace con Azure Arc , un conjunto de tecnologías que ayudan a administrar el entorno en la nube.

**1.4Descripción del modelo basado en el consumo**

Al comparar los modelos de infraestructura de TI(tecnología de la información), hay dos tipos de gastos que se deben tener en cuenta:

* Los gastos de capital suelen ser un gasto por adelantado único para comprar o proteger recursos tangibles.Un edificio nuevo, volver a pavimentar el aparcamiento…
* Los gastos operativos es gastar dinero en servicios o productos a lo largo del tiempo. Alquilar un centro de convenciones, alquilar un vehículo de empresa…

La informática en la nube se encuentra(Cloud Computing) en la partida de gastos operativos porque funciona en un modelo basado en el consumo.

**2.1** **Descripción de las ventajas de la alta disponibilidad y la escalabilidad en la nube**

**Alta disponibilidad**

Al implementar una aplicación, un servicio o cualquier recurso de TI, es importante que los recursos estén disponibles cuando sea necesario. La alta disponibilidad se centra en garantizar la máxima disponibilidad, independientemente de las interrupciones o eventos que puedan producirse.

**Escalabilidad**

La escalabilidad hace referencia a la capacidad de ajustar los recursos para satisfacer la demanda. Si de pronto experimenta un tráfico máximo y los sistemas están sobrecargados, la capacidad de escalar implica que puede agregar más recursos para controlar mejor la mayor demanda.

**Escalado vertical**

Especificaciones de cada instancia(la cpu,ram,mem…De cada ordenador que alquilas).

**Escalado horizontal**

El numero de instancias.Por ejemplo, si hay mucha demanda, podría agregar máquinas virtuales o contenedores adicionales, mediante el escalado horizontal.

**2.2Descripción de las ventajas de la confiabilidad y la previsibilidad en la nube**

**Confiabilidad**

La confiabilidad es la capacidad de un sistema de recuperarse de los errores y seguir funcionando.

La nube, debido a su diseño descentralizado, admite de forma natural una infraestructura confiable y resistente. Con un diseño descentralizado, la nube le permite implementar recursos en regiones de todo el mundo. Con esta escala global, incluso si se produce una catástrofe en una región, otras siguen en funcionamiento.

**Predicción**

La previsibilidad en la nube le permite avanzar con confianza. La previsibilidad se puede centrar en el rendimiento o los costos.

**Rendimiento**

La previsibilidad del rendimiento se centra en predecir los recursos necesarios para ofrecer una experiencia positiva para los clientes. Si de repente necesita más recursos, el escalado automático puede implementar recursos adicionales para satisfacer la demanda y, después, reducir horizontalmente cuando disminuya. O bien, si el tráfico se concentra principalmente en un área, el equilibrio de carga ayudará a redirigir parte de la sobrecarga a áreas con menos estrés.

**Coste**

La predicción de costos se centra en pronosticar el costo del gasto en la nube. Con la nube, puede realizar el seguimiento del uso de recursos en tiempo real, supervisar los recursos para asegurarse de que los usa de la manera más eficaz y aplicar análisis de datos para buscar patrones y tendencias que ayuden a planear mejor las implementaciones de recursos.

**2.3 Descripción de las ventajas de la capacidad de administración en la nube**

 Hay dos tipos de administración para la informática en la nube sobre los que obtendrá información en esta serie y ambos son excelentes ventajas.

**Administración de la nube**

La administración de la nube trata sobre administrar los recursos en la nube. En la nube, puede hacer lo siguiente:

* Escalar automáticamente la implementación de recursos en función de las necesidades.
* Implementar recursos basados en una plantilla preconfigurada, lo que elimina la necesidad de realizar la configuración manual.
* Supervisar el estado de los recursos y reemplazar automáticamente los recursos con errores.
* Recibir alertas automáticas basadas en métricas configuradas, de modo que esté informado del rendimiento en tiempo real.

**Administración en la nube**

La administración en la nube trata sobre cómo puede administrar el entorno y los recursos en la nube. Puede administrarlos de las siguientes maneras:

* Mediante un portal web.
* Con una interfaz de línea de comandos básica.
* Mediante las API.
* Mediante PowerShell.

**3.1Descripción de la infraestructura como servicio**

La infraestructura como servicio (IaaS) es la categoría más flexible de servicios en la nube, ya que proporciona el máximo control para los recursos en la nube. En un modelo de IaaS, el proveedor de nube es el responsable de mantener el hardware, la conectividad de red (a Internet) y la seguridad física. Todo lo demás será responsabilidad suya: configuración de red, configuración de base de datos y almacenamiento, etc. Con IaaS, lo que haces básicamente es alquilar el hardware en un centro de datos en la nube, pero puedes hacer lo que quieras con ese hardware.

**Escenarios:**

Algunos escenarios comunes en los que IaaS puede tener sentido incluyen los siguientes:

* Migración mediante lift-and-shift: estás poniendo en marcha recursos en la nube similares al centro de datos local y, después, simplemente mover las cosas que se ejecutan localmente para que se ejecuten en la infraestructura IaaS.
* Pruebas y desarrollo: has establecido configuraciones para entornos de desarrollo y pruebas que necesita para replicar rápidamente. Puedes poner en marcha o apagar rápidamente los diferentes entornos con una estructura IaaS, a la vez que mantiene un control total.

**3.2Descripción de la plataforma como servicio**

La plataforma como servicio (PaaS) es un punto intermedio entre alquilar espacio en un centro de datos (infraestructura como servicio) y pagar por una solución completa e implementada (software como servicio). En un entorno PaaS, el proveedor de nube mantiene la infraestructura física, la seguridad física y la conexión a Internet. También mantienen los sistemas operativos, el middleware, las herramientas de desarrollo y los servicios de inteligencia empresarial que componen una solución en la nube. En un escenario de PaaS, no tiene que preocuparse por las licencias ni la aplicación de revisiones para los sistemas operativos y las bases de datos.

PaaS es ideal para proporcionar un entorno de desarrollo completo sin el molesto de mantener toda la infraestructura de desarrollo.

**Escenarios**

Algunos escenarios comunes en los que PaaS pueden encajar incluyen:

* Marco de desarrollo: PaaS ofrece un marco que los desarrolladores pueden usar para desarrollar o personalizar aplicaciones basadas en la nube. De una manera similar a como se crea una macro de Excel, PaaS permite que los desarrolladores creen aplicaciones a través de componentes de software integrados. Se incluyen características de la nube, como escalabilidad, alta disponibilidad y funcionalidad multiinquilino, lo que permite reducir la cantidad de codificación que deben realizar los desarrolladores.
* Análisis o inteligencia empresarial: las herramientas proporcionadas como servicio con PaaS permiten a las organizaciones analizar y extraer sus datos, buscar información y patrones y predecir resultados para mejorar la previsión y otras decisiones empresariales.

**3.3Descripción del software como servicio**

Software como servicio (SaaS) es el modelo de servicio en la nube más completo desde el punto de vista del producto. Con SaaS, básicamente la que hace es alquilar o usar una aplicación totalmente desarrollada. El correo electrónico o el software financiero conectividad son ejemplos comunes de una implementación de SaaS.

Aunque el modelo de SaaS puede ser el menos flexible, también es el más sencillo de poner en marcha. Requiere la menor cantidad de conocimientos técnicos o experiencia para utilizarlo en toda su dimensión.

**Escenarios**

Algunos escenarios comunes para SaaS son los siguientes:

* Correo electrónico y mensajería
* Aplicaciones de productividad empresarial
* Seguimiento de finanzas y gastos

**4.¿Qué es Azure?**

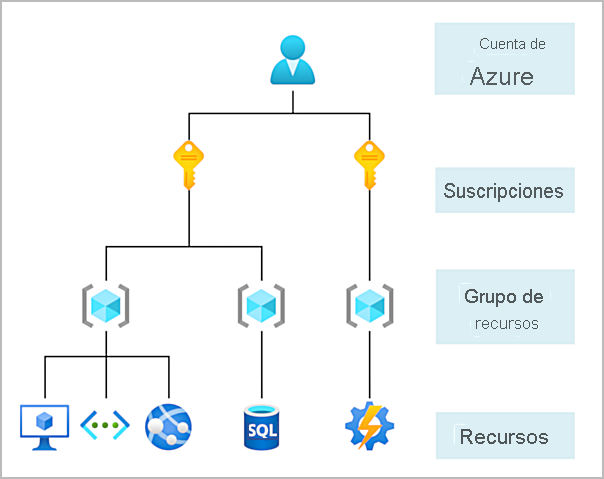
Azure es un conjunto de servicios en la nube en expansión constante.

**¿Que ofrece Azure?**

Ofrece la libertad de compilar, administrar e implementar aplicaciones en una red global masiva mediante sus herramientas y plataformas que ofrece:

* Crear según términos propios: tienes varias opciones. Si mantiene un compromiso con el código abierto y admite todos los lenguajes y marcos, puede compilar como quiera e implementar donde quiera.
* Funcionamiento sin problemas en el entorno híbrido: ya sea en el entorno local, en la nube o en el entorno perimetral, le apoyaremos donde esté. Integre y administre los entornos con herramientas y servicios diseñados para una solución de nube híbrida.
* Confianza en la nube: obtén seguridad desde el principio, respaldada por un equipo de expertos, y un cumplimiento proactivo de confianza para las empresas consolidadas, los gobiernos y las nuevas empresas.

Azure proporciona más de 100 servicios que permiten hacer todo tipo de cosas,Por ejemplo, Azure proporciona servicios de inteligencia artificial (IA) y aprendizaje automático (ML).

**4.1Introducción a las cuentas de Azure**

Para crear y usar los servicios de Azure, necesita una suscripción de Azure.Se pueden tener varías subscripciones por cada cuenta ,cada una de ellas controlará un grupo de recursos distinta y será totalmente independiente de las demás.

Ver foto:

**4.2Descripción de la infraestructura física de Azure**

->Infraestructura física:

La infraestructura física de Azure comienza con los centros de datos,instalaciones con recursos organizados en bastidores, con potencia dedicada, refrigeración e infraestructura de red.Como proveedor de nube global, Azure tiene centros de datos en todo el mundo. Los centros de datos se agrupan en regiones de Azure o Azure Availability Zones.

---->Regiones:

Una región es un área geográfica del planeta que contiene al menos un centro de datos, aunque podrían ser varios cercanos y conectados mediante una red de baja latencia. Azure asigna y controla los recursos de forma inteligente dentro de cada región para garantizar que las cargas de trabajo están bien compensadas.

----->Availability Zones:

Las zonas de disponibilidad son centros de datos separados físicamente dentro de una región de Azure. Cada zona de disponibilidad consta de uno o varios centros de datos. Una zona de disponibilidad se configura para constituir un límite de aislamiento. Si una zona deja de funcionar, la otra continúa trabajando.

Para garantizar la resistencia, se configuran un mínimo de tres zonas de disponibilidad independientes en todas las regiones habilitadas. Pero no todas las regiones de Azure admiten actualmente las zonas de disponibilidad.

**4.3Uso de las zonas de disponibilidad en sus aplicaciones**

A fin de proteger la información en caso de error, deberás asegurarse de que los servicios y datos son redundantes. Si hospedas tu infraestructura, configurar su propia redundancia requiere la creación de entornos de hardware duplicados. Azure puede ayudar a que la aplicación tenga alta disponibilidad a través de zonas de disponibilidad.

Las zonas de disponibilidad son principalmente para las máquinas virtuales, los discos administrados, los equilibradores de carga y las bases de datos SQL. Los servicios de Azure que admiten zonas de disponibilidad se dividen en tres categorías:

-Servicios de zona: ancla el recurso a una zona específica (por ejemplo, máquinas virtuales).

-Servicios de redundancia de zona: la plataforma se replica automáticamente entre zonas (por ejemplo, almacenamiento con redundancia de zona, SQL Database).

-Servicios no regionales: los servicios siempre están disponibles en las ubicaciones geográficas de Azure y son resistentes a las interrupciones de toda la zona, así como a las de toda la región.

**Pares de región**

La mayoría de las regiones de Azure se emparejan con otra región de la misma zona geográfica (por ejemplo, EE. UU., Europa o Asia) que se encuentre como mínimo a 500 km de distancia. Este enfoque permite la replicación de recursos en una zona geográfica que ayuda a reducir la probabilidad de que se produzcan interrupciones provocadas por eventos como desastres naturales, disturbios sociales… que afecten a una región completa. Por ejemplo, si una región de un par se ve afectada por un desastre natural, los servicios conmutarán por errorautomáticamente a la otra región de su par de regiones.

**Regiones soberanas**

Las regiones soberanas son instancias de Azure que están aisladas de la instancia principal de Azure. Es posible que tengas que usar una región soberana con fines legales o de cumplimiento.

Entre las regiones soberanas de Azure se incluyen las siguientes:

US DoD (centro), US Gov Virginiay más: Estas regiones son instancias físicas y lógicas con aislamiento de red de Azure para asociados y agencias de la administración pública de EE. UU. Estos centros de datos están operados por personal estadounidense sometido a evaluación

Este de China, Norte de China y más: Estas regiones están disponibles gracias a una asociación exclusiva entre Microsoft y 21Vianet, por la cual Microsoft no mantiene directamente los centros de datos.

**4.4Descripción de la infraestructura de administración de Azure**

La infraestructura de administración incluye recursos de Azure y grupos de recursos, suscripciones y cuentas.

**Recursos y grupos de recursos de Azure**

Un recurso es el bloque de creación básico de Azure. Todo lo que cree, aprovisione, implemente, etc., es un recurso. Máquinas virtuales (VM), redes virtuales, bases de datos, servicios cognitivos, etc., se consideran recursos dentro de Azure.

Al crear un recurso, es necesario colocarlo en un grupo de recursos. Los grupos de recursos proporcionan una manera cómoda de agrupar recursos. Al aplicar una acción a un grupo de recursos, se aplicará a todos los recursos que contiene. Si elimina un grupo de recursos, se eliminarán todos los recursos que contiene. Si concede o deniega el acceso a un grupo de recursos, habrá concedido o denegado acceso a todos los recursos que contiene. Los grupos de recursos no se pueden anidar, lo que significa que no se puede colocar el grupo de recursos B dentro del grupo de recursos A,pero sí se pueden mover recursos de un grupo de recurso a otro

Al aprovisionar recursos, es conveniente pensar en la estructura del grupo de recursos que mejor se adapte a las necesidades.

**Suscripciones de Azure**

En Azure, las suscripciones son una unidad de administración, facturación y escala. Al igual que los grupos de recursos son una manera de organizar lógicamente los recursos, las suscripciones permiten organizar lógicamente los grupos de recursos y facilitar la facturación.

Una cuenta puede tener varias suscripciones, pero solo es obligatorio tener una.

Hay dos tipos de límites de suscripción que puede utilizar:

* **Límite de facturación**: Este tipo de suscripción determina cómo se factura una cuenta de Azure por el uso de Azure. Puede crear varias suscripciones para diferentes tipos de requisitos de facturación. Azure genera facturas e informes de facturación independientes para cada suscripción, de modo que pueda organizar y administrar los costos.
* **Límite de control de acceso**: Azure aplica las directivas de administración de acceso en el nivel de suscripción, por lo que puede crear suscripciones independientes para reflejar distintas estructuras organizativas. Por ejemplo, dentro de una empresa hay diferentes departamentos a los que se pueden aplicar directivas de suscripción de Azure distintas. Este modelo de facturación le permite administrar y controlar el acceso a los recursos que los usuarios aprovisionan con suscripciones específicas.

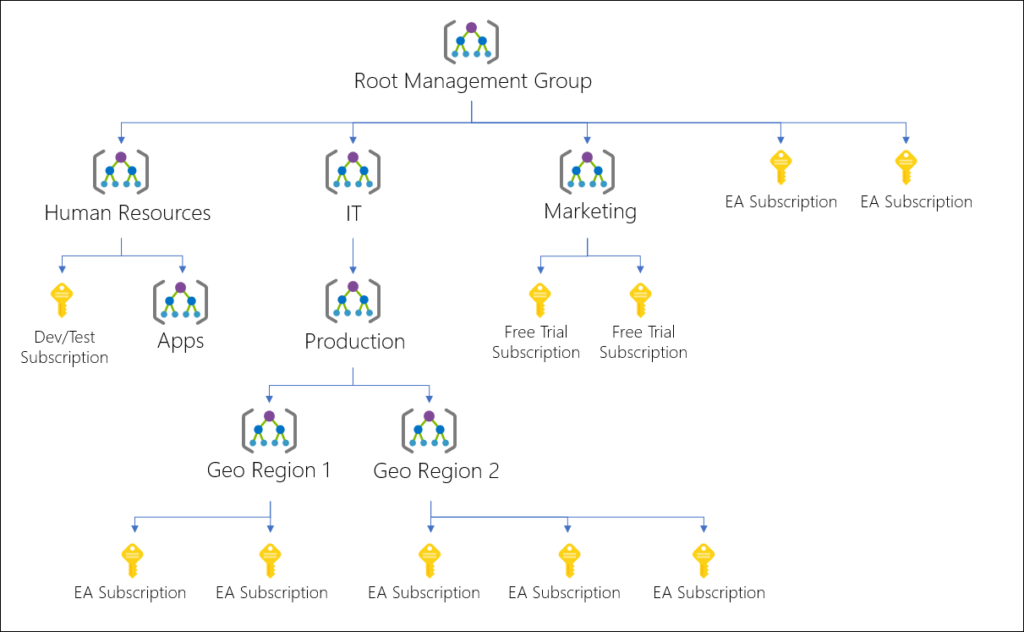
**Creación de una suscripción de Azure adicional**

De forma similar al uso de grupos de recursos para separar los recursos por función o acceso, es posible que quiera crear suscripciones adicionales con fines de administración de recursos o facturación. Por ejemplo, puedes optar por crear suscripciones adicionales para separar lo siguiente:

* **Entornos**: puedes optar por crear suscripciones con el fin de configurar entornos independientes para el desarrollo y las pruebas.Este diseño es especialmente útil porque el control de acceso a los recursos se produce en el nivel de suscripción.
* **Estructuras organizativas**: puedes crear suscripciones para reflejar las distintas estructuras organizativas. Por ejemplo, podría limitar un equipo a recursos de bajo costo, al tiempo que permite que el departamento de TI tenga un alcance completo. Este diseño permite administrar y controlar el acceso a los recursos que los usuarios aprovisionan en cada suscripción.
* **Facturación**: puedes crear suscripciones adicionales con fines de facturación. Dado que los costos se agregan primero en el nivel de suscripción, es posible que quieras crear suscripciones para administrar y realizar un seguimiento de los costos en función de sus necesidades. Por ejemplo, puede que quieras crear una suscripción para las cargas de trabajo de producción, y otra suscripción para las cargas de trabajo de desarrollo y pruebas

**Grupos de administración de Azure**

Las suscripciones se organizan en contenedores llamados grupos de administración, a los que se aplican condiciones de gobernanza. Todas las suscripciones de un grupo de administración heredan automáticamente las condiciones que tenga aplicadas, de la misma manera que los grupos de recursos heredan la configuración de las suscripciones y los recursos heredan de los grupos de recursos. Los grupos de administración proporcionan capacidad de administración de nivel empresarial a gran escala con independencia del tipo de suscripciones que tenga. Los grupos de administración se pueden anidar.



Algunos ejemplos de cómo podría usar los grupos de administración podrían ser los siguientes:

* **Crear una jerarquía que aplique una directiva**. Podría limitar las ubicaciones de las máquinas virtuales a la región Oeste de EE. UU. en un grupo denominado Producción. Esta directiva se heredará en todas las suscripciones descendientes de ese grupo de administración y se aplicará a todas las máquinas virtuales de esas suscripciones. El propietario de los recursos o las suscripciones no puede modificar esta directiva de seguridad, lo que permite una gobernanza mejorada.
* **Proporcionar acceso de usuario a varias suscripciones**. Al mover varias suscripciones bajo un grupo de administración, puede crear una asignación del control de acceso basado en roles (RBAC) en el grupo de administración. La asignación de RBAC de Azure en el nivel de grupo de administración significa que todos los grupos de administración secundaria, las suscripciones, los grupos de recursos y los recursos bajo ese grupo de administración también heredarían esos permisos. Una asignación en el grupo de administración puede permitir a los usuarios tener acceso a todo lo que necesitan, en lugar de crear scripts de Azure RBAC sobre las distintas suscripciones.

Datos importantes sobre los grupos de administración:

* Se admiten 10 000 grupos de administración en un único directorio.
* Un árbol de grupo de administración puede admitir hasta seis niveles de profundidad. Este límite no incluye el nivel raíz ni el nivel de suscripción.
* Cada grupo de administración y suscripción solo puede admitir un elemento primario.

**5.Descripción de Azure Virtual Machines**

Con Azure Virtual Machines (VM), puedes crear y usar máquinas virtuales en la nube. Estas máquinas virtuales proporcionan una infraestructura como servicio (IaaS) en forma de un servidor virtualizado y se pueden usar de muchas formas. Como sucede en un equipo físico, puedes personalizar todo el software que se ejecuta en la máquina virtual. Las máquinas virtuales son una opción ideal cuando necesitas lo siguiente:

* Control total sobre el sistema operativo (SO).
* Capacidad de ejecutar software personalizado.
* Usar configuraciones de hospedaje personalizadas.

Una máquina virtual de Azure te ofrece la flexibilidad de la virtualización sin necesidad de adquirir y mantener el hardware físico que ejecuta la máquina virtual. Pero, como oferta de IaaS, tendrá que configurar, actualizar y mantener el software que se ejecuta en la máquina virtual.

Incluso puedes crear o usar una imagen ya creada para aprovisionar rápidamente máquinas virtuales. Al seleccionar una imagen de máquina virtual preconfigurada, podrás crear y aprovisionar una máquina virtual en cuestión de minutos. Una imagen es una plantilla que se usa para crear una máquina virtual y puede que ya incluya un sistema operativo y otro software, como herramientas de desarrollo o entornos de hospedaje web.

Azure también puede administrar la agrupación de máquinas virtuales con características como conjuntos de escalado y conjuntos de disponibilidad.

**Conjuntos de escalado de máquinas virtuales**

Los conjuntos de escalado le permiten administrar, configurar y actualizar de forma centralizada un gran número de máquinas virtuales en cuestión de minutos. El número de instancias de máquina virtual puede aumentar o disminuir automáticamente según la demanda, o bien puede establecerlo para que se escale en función de una programación definida. Los conjuntos de escalado de máquinas virtuales también implementan automáticamente un equilibrador de carga para asegurarse de que los recursos se usan de forma eficaz.

**Conjuntos de disponibilidad de máquinas virtuales**

Los conjuntos de disponibilidad están diseñados para garantizar que las máquinas virtuales escalen las actualizaciones y tengan una conectividad de red y potencia variadas, lo que evita que se pierdan todas las máquinas virtuales debido a un solo fallo de energía o de la red.

Los conjuntos de disponibilidad lo hacen mediante la agrupación de las máquinas virtuales de dos maneras: dominio de actualización y dominio de error.

* **Dominio de actualización**: agrupa las máquinas virtuales que se pueden reiniciar al mismo tiempo. Esto le permite aplicar actualizaciones mientras sabe que solo una agrupación de dominios de actualización estará sin conexión a la vez. Se actualizarán todas las máquinas de un dominio de actualización. A un grupo de actualizaciones que realiza el proceso de actualización se le asigna un tiempo de 30 minutos de recuperación antes de que se inicie el mantenimiento en el siguiente dominio de actualización.
* **Dominio de error**: agrupa las máquinas virtuales por fuente de alimentación común y conmutador de red. De forma predeterminada, un conjunto de disponibilidad dividirá las máquinas virtuales en un máximo de tres dominios de error. Esto ayuda a protegerse frente a un error de alimentación física o de la red al tener las máquinas virtuales en dominios de error diferentes (por tanto, conectadas a diferentes recursos de alimentación y red).

Lo mejor de todo es que la configuración de un conjunto de disponibilidad no supone ningún costo adicional. Solo paga por las instancias de máquina virtual que cree.

Poner foto de la presentación

**Traslado a la nube con máquinas virtuales**

Las máquinas virtuales también son una opción excelente cuando se mueve de un servidor físico a la nube (también conocido como Lift-and-shift). Puedes crear una imagen del servidor físico y hospedarla en una máquina virtual con pocos o ningún cambio. Al igual que un servidor local físico, debes mantener la máquina virtual: es responsable de mantener el sistema operativo y el software instalados.

**Recursos de máquina virtual**

Al aprovisionar una máquina virtual, también tendrás la oportunidad de elegir los recursos asociados a esa máquina virtual, como los siguientes:

* Tamaño (propósito, número de núcleos de procesador y cantidad de RAM)
* Discos de almacenamiento (unidades de disco duro, unidades de estado sólido, etc.)
* Redes (red virtual, dirección IP pública y configuración de puertos)

**5.1Descripción de Azure Virtual Desktop**

Otro tipo de máquina virtual es Azure Virtual Desktop. Azure Virtual Desktop es un servicio de virtualización de escritorios y aplicaciones que se ejecuta en la nube. Te permite usar una versión hospedada en la nube de Windows desde cualquier ubicación. Azure Virtual Desktop funciona en dispositivos y sistemas operativos, y funciona con aplicaciones que puede usar para acceder a escritorios remotos o a la mayoría de exploradores modernos.

**Aumento de la seguridad**

Azure Virtual Desktop proporciona administración centralizada de la seguridad de los escritorios de los usuarios con Azure Active Directory (Azure AD). Puedes habilitar la autenticación multifactor para proteger los inicios de sesión de los usuarios. También puedes proteger el acceso a los datos mediante la asignación a los usuarios de controles de acceso basados en roles (RBAC) detallados.

Con Azure Virtual Desktop, los datos y las aplicaciones se separan del hardware local y El escritorio y las aplicaciones reales se ejecutan en la nube, lo que significa que se reduce el riesgo de dejar datos confidenciales en un dispositivo personal. Además, las sesiones de usuario están aisladas en entornos de una o varias sesiones.

**5.2Descripción de contenedores de Azure**

A diferencia de las máquinas virtuales, no se administra el sistema operativo de un contenedor,sino solo la aplicación.

Los contenedores son un entorno de virtualización. Al igual que la ejecución de varias máquinas virtuales en un solo host físico, se pueden ejecutar varios contenedores en un solo host físico o virtual.Son ligeros y se han diseñado para crearse, escalarse horizontalmente y detenerse de forma dinámica. Los contenedores están diseñados para permitirle responder a petición a los cambios. Con los contenedores puede reiniciar rápidamente en caso de bloqueo o interrupción del hardware.

Los contenedores son una excelente opción si quiere ejecutar varias instancias de una aplicación en un solo equipo host.

Los contenedores se usan normalmente para crear soluciones mediante una arquitectura de microservicios. Esta arquitectura es donde se dividen las soluciones en partes más pequeñas e independientes. Por ejemplo, se puede dividir un sitio web en un contenedor que hospeda el front-end, otro que hospeda el back-end y un tercero para el almacenamiento. De esta forma, puede separar partes de la aplicación en secciones lógicas que se pueden mantener, escalar o actualizar independientemente.

**5.3Descripción de Azure Functions**

Azure Functions es una opción de proceso sin servidor controlada por eventos que no necesita el mantenimiento de máquinas virtuales ni contenedores. Si compila una aplicación mediante máquinas virtuales o contenedores, esos recursos deben "ejecutarse" para que la aplicación funcione. Con Azure Functions, un evento activa la función, lo que reduce la necesidad de mantener los recursos aprovisionados cuando no hay ningún evento.El uso de Azure Functions es idóneo si solo le interesa el código que ejecuta el servicio y no la infraestructura o la plataforma subyacente.

**5.4Descripción de las opciones de hospedaje de aplicaciones**

Si necesita hospedar la aplicación en Azure, es posible que cambie inicialmente a una máquina virtual (VM) o a contenedores. Las máquinas virtuales proporcionan el máximo control del entorno de hospedaje y le permiten configurarlo exactamente como desea. Las máquinas virtuales también pueden ser el método de hospedaje más conocido si no está familiarizado con la nube. Los contenedores, con la capacidad de aislar y administrar individualmente diferentes aspectos de la solución de hospedaje, también pueden ser una opción sólida y atractiva.

Hay otras opciones de hospedaje que puede usar con Azure, incluido Azure App Service.

**Azure App Service**

Admite varios lenguajes, incluidos .NET, .NET Core, Java, Ruby, Node.js, PHP o Python. También admite entornos de Windows y Linux.Permite implementaciones automatizadas desde GitHub, Azure DevOps o cualquier repositorio Git para admitir un modelo de implementación continua.

**Tipos de servicios de aplicaciones que puede hospedar**

Con App Service, puede hospedar la mayoría de los estilos de servicio de aplicación más comunes, como los siguientes:

* Aplicaciones web: mediante ASP.NET, ASP.NET Core, Java, Ruby, Node.js, PHP o Python. Puede elegir Windows o Linux como sistema operativo del host.
* Aplicaciones de API: puede compilar API web basadas en REST mediante el lenguaje y el marco que prefiera. Se obtiene compatibilidad completa con Swagger y la posibilidad de empaquetar y publicar la API en Azure Marketplace. Las aplicaciones producidas se pueden consumir desde cualquier cliente basado en HTTP o HTTPS.
* Trabajos web:Se puede usar la característica WebJobs para ejecutar un programa (.exe, Java, PHP, Python o Node.js) o un script (.cmd, .bat, PowerShell o Bash) en el mismo contexto que una aplicación web, aplicación de API o aplicación móvil. Los trabajos web suelen usarse para ejecutar tareas en segundo plano como parte de la lógica de aplicación.
* Aplicaciones móviles: Use la característica Mobile Apps de App Service a fin de compilar rápidamente un back-end para aplicaciones iOS y Android. Con unos pocos clics en el Portal de Azure, puede realizar lo siguiente:
  + Almacenar los datos de aplicaciones móviles en una base de datos SQL basada en la nube.
  + Autenticar a clientes con proveedores sociales comunes, como MSA, Google, Twitter y Facebook.
  + Enviar notificaciones de inserción.
  + Ejecutar lógica de back-end personalizada en C# o Node.js.

App Service controla la mayoría de las decisiones sobre la infraestructura que se tratan en el hospedaje de aplicaciones accesibles desde la web:

* La implementación y administración se integran en la plataforma.
* Los puntos de conexión se pueden proteger.
* Los sitios se pueden escalar rápidamente para controlar cargas de tráfico elevado.
* El equilibrio de carga integrado y el administrador de tráfico proporcionan alta disponibilidad.

**5.5Descripción de las redes virtuales de Azure**

Las redes virtuales y las subredes virtuales de Azure permiten a los recursos de Azure, como las máquinas virtuales, las aplicaciones web y las bases de datos, comunicarse entre sí, con los usuarios de Internet y con los equipos cliente en el entorno local.

Las redes virtuales de Azure proporcionan las importantes funcionalidades de red siguientes:

Aislamiento y segmentación: La red virtual de Azure permite crear varias redes virtuales aisladas. Al configurar una red virtual, se define un espacio de direcciones IP privadas con intervalos de direcciones IP públicas o privadas. El intervalo IP solo existe dentro de la red virtual y no es enrutable en Internet. Después, puede dividir ese espacio de direcciones IP en subredes y asignar parte del espacio de direcciones definido a cada subred con nombre.( Para la resolución de nombres, puede usar el servicio de resolución de nombres integrado en Azure. También puede configurar la red virtual para que use un servidor DNS interno o externo.)

* Comunicación con Internet:Puede permitir conexiones entrantes desde Internet mediante la asignación de una dirección IP pública a un recurso de Azure o la colocación del recurso detrás de un equilibrador de carga público.
* Comunicación entre recursos de Azure: Puede hacerlo de dos maneras:1.Las redes virtuales no solo pueden conectar máquinas virtuales, sino también otros recursos de Azure, como App Service Environment para Power Apps, Azure Kubernetes Service y conjuntos de escalado de máquinas virtuales de Azure.2.Los puntos de conexión de servicio se pueden conectar a otros tipos de recursos de Azure, como cuentas de almacenamiento y bases de datos de Azure SQL.
* Comunicación con los recursos locales: permiten vincular entre sí los recursos del entorno local y dentro de la suscripción de Azure. De hecho, puede crear una red que abarque tanto el entorno local como el entorno en la nube. Existen tres mecanismos para lograr esta conectividad:
  + Las conexiones de red privada virtual de punto a sitio se establecen desde un equipo ajeno a la organización a la red corporativa. En este caso, el equipo cliente inicia una conexión VPN cifrada para conectarse a la red virtual de Azure.
  + Las redes virtuales privadas de sitio a sitio vinculan el dispositivo o puerta de enlace de VPN local con la puerta de enlace de VPN de Azure en una red virtual. De hecho, puede parecer que los dispositivos de Azure están en la red local. La conexión se cifra y funciona a través de Internet.
  + Azure ExpressRoute proporciona una conectividad privada dedicada a Azure que no se desplaza por Internet. ExpressRoute es útil para los entornos donde se necesita más ancho de banda e incluso mayores niveles de seguridad.
* Enrutamiento del tráfico de red : De forma predeterminada, Azure enruta el tráfico entre las subredes de todas las redes virtuales conectadas, las redes locales e Internet. También puede controlar el enrutamiento e invalidar esa configuración del siguiente modo:
  + Las tablas de rutas permiten definir reglas sobre cómo se debe dirigir el tráfico. Puede crear tablas de rutas personalizadas que controlen cómo se enrutan los paquetes entre las subredes.
  + El Protocolo de puerta de enlace de borde (BGP) funciona con puertas de enlace de VPN de Azure, Azure Route Server o Azure ExpressRoute para propagar las rutas BGP locales a las redes virtuales de Azure.
* Filtrado del tráfico de red: Las redes virtuales de Azure permiten filtrar el tráfico entre las subredes mediante los métodos siguientes:
  + Los grupos de seguridad de red son recursos de Azure que pueden contener varias reglas de seguridad de entrada y salida. Estas reglas se pueden definir para permitir o bloquear el tráfico en función de factores como el protocolo, el puerto y las direcciones IP de destino y origen.
  + Las aplicaciones virtuales de red son máquinas virtuales especializadas que se pueden comparar con un dispositivo de red protegido. Una aplicación virtual de red ejerce una función de red determinada, como ejecutar un firewall o realizar la optimización de la red de área extensa (WAN).
* Conexión de redes virtuales: Puede vincular redes virtuales entre sí mediante el emparejamiento de red virtual. El emparejamiento permite que dos redes virtuales se conecten directamente entre sí. El tráfico de red entre redes emparejadas es privado y se desplaza por la red troncal de Microsoft, y nunca entra en la red pública de Internet. El emparejamiento permite que los recursos de cada red virtual se comuniquen entre sí. Estas redes virtuales pueden estar en regiones distintas, lo que permite crear una red global interconectada con Azure.

Las rutas definidas por el usuario (UDR) permiten controlar las tablas de enrutamiento entre subredes dentro de una red virtual o entre redes virtuales. Esto permite un mayor control sobre el flujo de tráfico de red.

* Los puntos de conexión públicos tienen una dirección IP pública y son accesibles desde cualquier parte del mundo.
* Los puntos de conexión privados existen dentro de una red virtual y tienen una dirección IP privada en el espacio de direcciones de esa red virtual.

**Descripción de las redes privadas virtuales de Azure**

Una red privada virtual (VPN) usa un túnel cifrado en otra red. Normalmente, las VPN se implementan para conectar entre sí dos o más redes privadas de confianza a través de una red que no es de confianza (normalmente, la red pública de Internet). El tráfico se cifra mientras viaja por la red que no es de confianza para evitar ataques de interceptación o de otro tipo. Las VPN pueden permitir que las redes compartan información confidencial de forma segura.

**Puertas de enlace de VPN**

Una puerta de enlace de VPN es un tipo de puerta de enlace de red virtual. Las instancias de Azure VPN Gateway se implementan en una subred dedicada de la red virtual y permiten la conectividad siguiente:

* Conectar los centros de datos locales a redes virtuales a través de una conexión de sitio a sitio.
* Conectar los dispositivos individuales a redes virtuales a través de una conexión de punto a sitio.
* Conectar las redes virtuales a otras redes virtuales a través de una conexión entre redes.

Todas las transferencias de datos se cifran en un túnel privado mientras atraviesan Internet. Solo se puede implementar una única instancia de puerta de enlace de VPN en cada red virtual. Sin embargo, se puede usar una puerta de enlace para conectarse a varias ubicaciones, que incluye otras redes virtuales o centros de datos locales.

Al implementar una instancia de VPN Gateway, especifique el tipo de red privada virtual, es decir, basada en directivas o basada en rutas. La principal diferencia entre estos dos tipos de VPN es cómo se especifica el tráfico que se va a cifrar. En Azure, ambos tipos de puertas de enlace de VPN usan una clave previamente compartida como único método de autenticación.

* Las instancias de VPN Gateway basadas en directivas especifican de forma estática la dirección IP de los paquetes que se deben cifrar a través de cada túnel. Este tipo de dispositivo evalúa cada paquete de datos en función de los conjuntos de direcciones IP para elegir el túnel a través del cual se va a enviar el paquete.
* En las puertas de enlace basadas en rutas, los túneles IPSec se modelan como una interfaz de red o una interfaz de túnel virtual. El enrutamiento IP (ya sean rutas estáticas o protocolos de enrutamiento dinámico) decide cuál de estas interfaces de túnel se va a usar al enviar cada paquete. Las redes privadas virtuales basadas en rutas son el método preferido para conectar dispositivos locales. Son más resistentes a los cambios de la topología, como la creación de subredes.

Si necesita alguno de los siguientes tipos de conectividad, use una instancia de VPN Gateway basada en rutas:

* Conexiones entre redes virtuales
* Conexiones de punto a sitio
* Conexiones de varios sitios
* Coexistencia con una puerta de enlace de Azure ExpressRoute

**Escenarios de alta disponibilidad**

Si va a configurar una VPN para mantener la información segura, también querrá asegurarse de que es una configuración de VPN de alta disponibilidad y tolerante a errores. Hay varias maneras de maximizar la resistencia de la puerta de enlace de VPN.

**Configuración de activo-en espera**

De forma predeterminada, las instancias de VPN Gateway se implementan como dos instancias en una configuración de activo-en espera, incluso si solo ve un recurso de VPN Gateway en Azure. Cuando el mantenimiento planeado o la interrupción imprevista afectan a la instancia activa, la instancia en espera asume de forma automática la responsabilidad de las conexiones sin ninguna intervención del usuario. Durante esta conmutación por error, las conexiones se interrumpen, pero por lo general se restauran en cuestión de segundos si se trata del mantenimiento planeado y en un plazo de 90 segundos en el caso de las interrupciones imprevistas.

**Activo/activo**

Al incorporar compatibilidad con el protocolo de enrutamiento de BGP, también puede implementar puertas de enlace VPN en una configuración del tipo activo/activo. En esta configuración, se asigna una IP pública única a cada instancia. Después, se crean túneles independientes desde el dispositivo local a cada dirección IP. Se puede ampliar la alta disponibilidad mediante la implementación de un dispositivo VPN local adicional.

**Conmutación por error de ExpressRoute**

Otra opción de alta disponibilidad consiste en configurar una instancia de VPN Gateway como una ruta segura de conmutación por error para las conexiones ExpressRoute. Los circuitos ExpressRoute tienen resistencia integrada. Sin embargo, no son inmunes a los problemas físicos que afectan a los cables que entregan conectividad ni a las interrupciones que afectan a la ubicación completa de ExpressRoute. En escenarios de alta disponibilidad, en los que existe un riesgo asociado a una interrupción de un circuito ExpressRoute, también puede aprovisionar una instancia de VPN Gateway que usa Internet como un método alternativo de conectividad. De este modo, puede garantizar que siempre haya una conexión a las redes virtuales.

**Puertas de enlace con redundancia de zona**

En las regiones que admiten zonas de disponibilidad, se pueden implementar puertas de enlace VPN y ExpressRoute en una configuración con redundancia de zona. Esta configuración aporta una mayor disponibilidad, escalabilidad y resistencia a las puertas de enlace de red virtual. Implementar puertas de enlace en Azure Availability Zones separa de forma física y lógica las puertas de enlace dentro de una región, al mismo tiempo que protege la conectividad de red local en Azure de errores de nivel de zona. Estas puertas de enlace requieren diferentes referencias de almacén (SKU) de puerta de enlace y usan direcciones IP públicas estándar en lugar de direcciones IP públicas básicas.

**5.4Describir Azure ExpressRoute**

ExpressRoute le permite ampliar las redes locales a la nube de Microsoft mediante una conexión privada con la ayuda de un proveedor de conectividad. Esta conexión se denomina circuito ExpressRoute. Con ExpressRoute, puede establecer conexiones con servicios en la nube de Microsoft, como Microsoft Azure y Microsoft 365. Esto le permite conectar oficinas, centros de datos u otras instalaciones a la nube de Microsoft. Cada ubicación tendría su propio circuito ExpressRoute.

La conectividad puede ser desde una red de conectividad universal (IP VPN), una red Ethernet de punto a punto o una conexión cruzada virtual a través de un proveedor de conectividad en una instalación de ubicación compartida. Las conexiones de ExpressRoute no pasan por la red pública de Internet. Esto permite a las conexiones de ExpressRoute ofrecer más confiabilidad, más velocidad, latencia coherentes y mayor seguridad que las conexiones normales a través de Internet.

**Características y ventajas de ExpressRoute**

El uso de ExpressRoute como servicio de conexión entre Azure y las redes locales tiene varias ventajas.

* Conectividad a servicios en la nube de Microsoft en todas las regiones dentro de la región geopolítica.
* Conectividad global a los servicios de Microsoft en todas las regiones con Global Reach de ExpressRoute.
* Enrutamiento dinámico entre la red y Microsoft a través del Protocolo de puerta de enlace de borde (BGP).
* Redundancia integrada en todas las ubicaciones de configuración entre pares para una mayor confiabilidad.

**Conectividad con los Servicios en la nube de Microsoft**

ExpressRoute permite el acceso directo a los siguientes servicios en todas las regiones:

* Microsoft Office 365
* Microsoft Dynamics 365
* Servicios de proceso de Azure, como Azure Virtual Machines
* Servicios en la nube de Azure, como Azure Cosmos DB y Azure Storage

**Conectividad global**

Puede permitir que Global Reach de ExpressRoute intercambie datos entre los sitios locales si conecta los diferentes circuitos ExpressRoute. Por ejemplo, supongamos que tiene una oficina en Asia y un centro de datos en Europa, ambos con circuitos ExpressRoute que los conectan a la red de Microsoft. Puede usar Global Reach de ExpressRoute para conectar esas dos instalaciones, lo que les permite comunicarse sin transferir datos a través de la red pública de Internet.

**Enrutamiento dinámico**

ExpressRoute usa el BGP. BGP se usa para intercambiar rutas entre las redes locales y los recursos que se ejecutan en Azure. Este protocolo permite el enrutamiento dinámico entre la red local y los servicios que se ejecutan en la nube de Microsoft.

**Redundancia integrada**

Cada proveedor de conectividad usa dispositivos redundantes para garantizar que las conexiones establecidas con Microsoft tengan alta disponibilidad. Puede configurar varios circuitos para complementar esta característica.

**Modelos de conectividad de ExpressRoute**

ExpressRoute admite cuatro modelos que puede usar para conectar la red local con la nube de Microsoft:

* Ubicación de CloudExchange
* Conexión Ethernet de punto a punto
* Conexión universal
* Directamente desde sitios de ExpressRoute

**Ubicación compartida en un intercambio en la nube**

La ubicación conjunta hace referencia al centro de datos, la oficina u otras instalaciones que se encuentran físicamente en un intercambio en la nube, como un ISP. Si la instalación tiene la ubicación compartida en un intercambio en la nube, puede solicitar una conexión cruzada virtual a la nube de Microsoft.

**Conexión Ethernet de punto a punto**

La conexión Ethernet de punto a punto hace referencia al uso de una conexión punto a punto para conectar la instalación a la nube de Microsoft.

**Redes universales**

Con la conectividad universal, puede integrar la red de área extensa (WAN) con Azure si proporciona conexiones a las oficinas y los centros de datos. Azure se integra con la conexión WAN para proporcionarle una conexión, como la que tendría entre el centro de datos y las sucursales.

**Directamente desde sitios de ExpressRoute**

Puede conectarse directamente a la red global de Microsoft en una ubicación de emparejamiento distribuida estratégicamente por todo el mundo. ExpressRoute Direct proporciona conectividad dual de 100 Gbps o 10 Gbps, que es compatible con la conectividad activa/activa a escala.

**Consideraciones sobre la seguridad**

Con ExpressRoute los datos no viajan a través de la red pública de Internet y, por tanto, no se exponen a los posibles riesgos asociados a las comunicaciones de Internet. ExpressRoute es una conexión privada de la infraestructura local a la infraestructura de Azure. Incluso si tiene una conexión ExpressRoute, las consultas de DNS, la comprobación de la lista de revocación de certificados y las solicitudes de Azure Content Delivery Network se siguen enviando a través de la red pública de Internet.

**5.5Describir Azure DNS**

Azure DNS es un servicio de hospedaje para dominios DNS que ofrece resolución de nombres mediante la infraestructura de Microsoft Azure. Al hospedar dominios en Azure, puede administrar los registros DNS con las mismas credenciales, API, herramientas y facturación que con los demás servicios de Azure.

**Ventajas de Azure DNS**

Azure DNS saca provecho del ámbito y la escala de Microsoft Azure para proporcionar numerosas ventajas, incluidas las siguientes:

* Confiabilidad y rendimiento
* Seguridad
* Facilidad de uso
* Redes virtuales personalizables
* Registros de alias

**Confiabilidad y rendimiento**

Los dominios DNS de Azure DNS se hospedan en la red global de servidores de nombres DNS de Azure, y proporcionan resistencia y alta disponibilidad. Azure DNS usa redes de difusión por proximidad para que el servidor DNS más próximo disponible responda a cada consulta de DNS para proporcionar un mejor rendimiento y una mayor disponibilidad para el dominio.

**Seguridad**

Azure DNS se basa en Azure Resource Manager, que proporciona características tales como:

* Control de acceso basado en rol de Azure (Azure RBAC) para controlar quién accede a acciones específicas en la organización.
* Registros de actividad: para supervisar cómo un usuario de su organización modificó un recurso o para encontrar errores al solucionar problemas.
* Bloqueo de recursos para bloquear una suscripción, un grupo de recursos o un recurso. Los bloqueos impiden que otros usuarios de la organización eliminen o modifiquen de forma accidental recursos críticos.

**Facilidad de uso**

Azure DNS puede administrar registros DNS para los servicios de Azure y también proporciona el servicio de nombres de dominio para los recursos externos. Azure DNS está integrado en Azure Portal y usa las mismas credenciales, la misma facturación y el mismo contrato de soporte técnico que los demás servicios de Azure.

Como Azure DNS se ejecuta en Azure, significa que puede administrar los dominios y registros con Azure Portal, cmdlets de Azure PowerShell y la CLI de Azure multiplataforma. Las aplicaciones que requieren la administración automática de DNS se pueden integrar con el servicio mediante las API REST y los SDK.

**Redes virtuales personalizables con dominios privados**

Azure DNS es compatible con dominios DNS privados. Esta característica permite usar nombres de dominio personalizados propios en las redes virtuales privadas, en lugar de limitarse a los nombres proporcionados por Azure.

**Registros de alias**

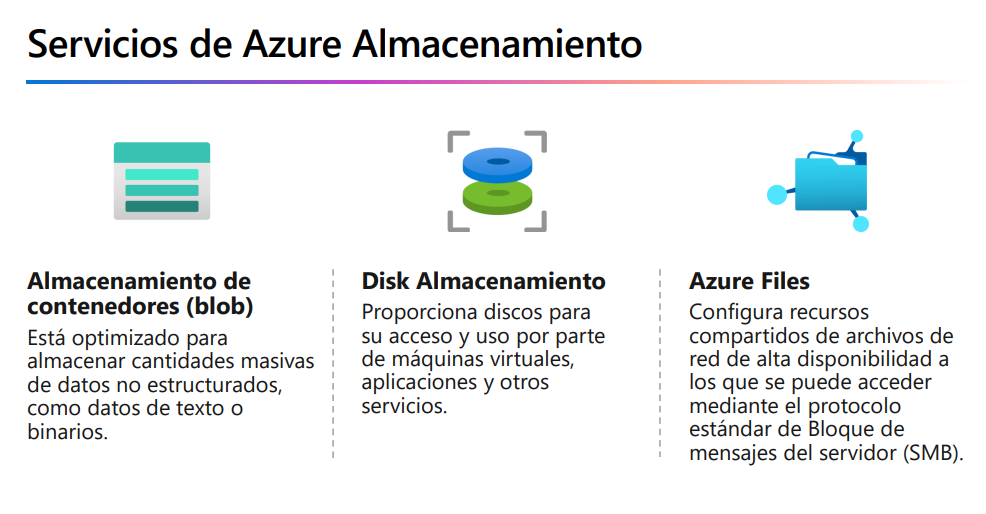
Azure DNS también admite conjuntos de registros de alias. Puede usar un conjunto de registros de alias que haga referencia a un recurso de Azure, como una dirección IP pública de Azure, un perfil de Azure Traffic Manager o un punto de conexión de Azure Content Delivery Network (CDN). Si cambia la dirección IP del recurso subyacente, el conjunto de registros de alias se actualiza sin problemas durante la resolución DNS. El conjunto de registros de alias apunta a la instancia de servicio, y la instancia de servicio está asociada con una dirección IP.

**6.Descripción de las cuentas de almacenamiento de Azure**

Una cuenta de almacenamiento proporciona un espacio de nombres único para los datos de Azure Storage al que se puede acceder desde cualquier lugar del mundo a través de HTTP o HTTPS.

Al crear la cuenta de almacenamiento, primero seleccionará el tipo de cuenta de almacenamiento. El tipo de cuenta determina los servicios de almacenamiento y las opciones de redundancia, y afecta a los casos de uso.

**Descripción de los servicios de almacenamiento de Azure**

La plataforma de Azure Storage incluye los servicios de datos siguientes:

**Blob Storage**

Azure Blob Storage es no estructurado, lo que significa que no hay ninguna restricción en cuanto a los tipos de datos que puede contener. Blob Storage puede administrar miles de cargas simultáneas, cantidades enormes de datos de vídeo, archivos de registro en constante crecimiento y es accesible desde cualquier lugar con conexión a Internet. Una ventaja del almacenamiento en blobs con respecto al almacenamiento en disco es que no requiere que los desarrolladores piensen en discos o los administren. Los datos se cargan como blobs y Azure se encarga de las necesidades de almacenamiento físico.

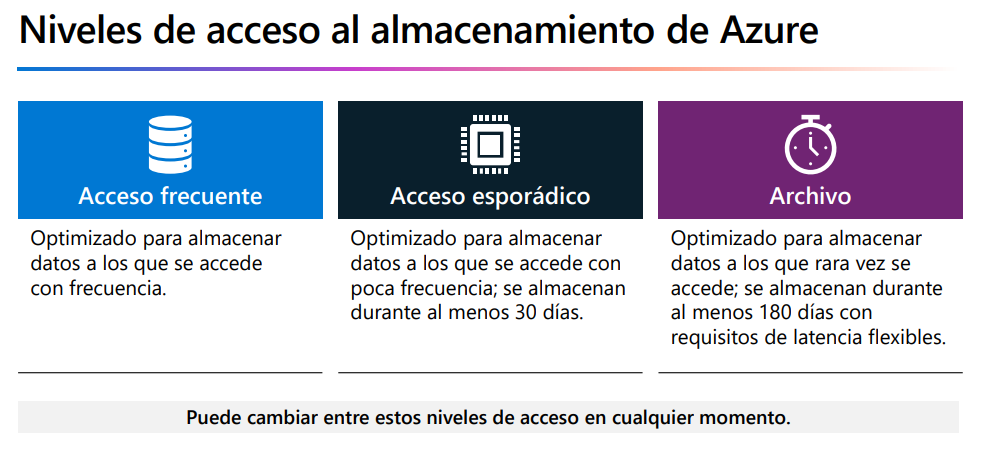
 muy conveniente para lo siguiente:

* Visualización de imágenes o documentos directamente en un explorador.
* Almacenamiento de archivos para acceso distribuido.
* Streaming de audio y vídeo.
* Almacenamiento de datos para copia de seguridad y restauración, recuperación ante desastres y archivado.
* Almacenamiento de datos para el análisis en local o en un servicio hospedado de Azure.

Se puede acceder a los objetos de Blob Storage desde cualquier lugar del mundo a través de HTTP o HTTPS. Los usuarios o las aplicaciones cliente pueden acceder a los blobs mediante direcciones URL, la API REST de Azure Storage, Azure PowerShell, la CLI de Azure o una biblioteca cliente de Azure Storage. Las bibliotecas de cliente de almacenamiento están disponibles para varios lenguajes, como .NET, Java, Node.js, Python, PHP y Ruby.

**Niveles de Blob Storage**

Azure Storage ofrece diferentes niveles de acceso para el almacenamiento de blobs, lo que le ayuda a almacenar datos de objetos de la manera más rentable. Entre los niveles de acceso disponibles se incluyen:

Cabe considerar:

* Solo los niveles de acceso frecuente y esporádico se pueden establecer en el nivel de cuenta. El nivel de acceso de archivo no está disponible en el nivel de cuenta.(signifca que para sacar un archivo de archive tienes que meterlo en un nivel de acceso frecuente esporádico…)
* Los niveles frecuente, esporádico y de archivo se pueden establecer en el nivel de blob durante la carga o después de esta.
* Los datos del nivel de acceso esporádico pueden tolerar una disponibilidad ligeramente inferior, pero aun así requieren una gran durabilidad, una latencia de recuperación y unas características de rendimiento similares a las de los datos de acceso frecuente. En el caso de los datos de acceso esporádico, un contrato de nivel de servicio (SLA) con una disponibilidad ligeramente inferior y unos costos de acceso mayores, en comparación con los datos de acceso frecuente, es aceptable a cambio de unos costos de almacenamiento menores.
* El almacenamiento de archivo almacena datos sin conexión y ofrece los menores costos de almacenamiento, pero los mayores costos de acceso y rehidratación de datos.

**Azure Files**

Azure Files ofrece recursos compartidos de archivos totalmente administrados en la nube a los que se puede acceder mediante los protocolos SMB (Bloque de mensajes del servidor) o NFS (Network File System) estándar del sector. Los recursos compartido de archivos de Azure Files se pueden montar simultáneamente mediante implementaciones locales o en la nube. A los recursos compartidos de archivos SMB de Azure se puede acceder desde clientes Windows, Linux y macOS. A los recursos compartidos de archivos NFS de Azure Files se puede acceder desde clientes Linux y macOS. Además, los recursos compartidos de archivos SMB de Azure Files se pueden almacenar en la caché de los servidores de Windows Server con Azure File Sync, lo que permite un acceso rápido allí donde se utilizan los datos.

**Ventajas clave de Azure Files:**

* **Acceso compartido**: lo que significa que puede reemplazar perfectamente los recursos compartidos de archivos en local por recursos compartidos de archivos de Azure sin preocuparse de compatibilidad de aplicaciones.
* **Totalmente administrado**: los recursos compartidos de Azure Files pueden crearse sin necesidad de administrar ni el hardware ni un sistema operativo.
* **Scripts y herramientas**: se pueden usar cmdlets de PowerShell y la CLI de Azure para crear, montar y administrar recursos compartidos de archivos de Azure como parte de la administración de las aplicaciones de Azure. Los recursos compartidos de archivos de Azure se pueden crear y administrar mediante Azure Portal y el Explorador de Azure Storage.
* **Resistencia**: no tratar con problemas de red o interrupciones del suministro eléctrico local.
* **Capacidad de programación intuitiva**: las aplicaciones que se ejecutan en Azure pueden tener acceso a los datos en el recurso compartido mediante las API de E/S del sistema de archivos. Por tanto, los desarrolladores pueden aprovechar el código y los conocimientos que ya tienen para migrar las aplicaciones actuales. Además de las API de E/S del sistema, puede usar las Bibliotecas de cliente de Azure Storage o la API de REST de Azure Storage.

**Queue Storage**

Una cola puede contener tantos mensajes como el espacio que tenga la cuenta de almacenamiento (pueden ser millones). Cada mensaje individual de la cola puede llegar a tener un tamaño máximo de 64 KB. Las colas se utilizan normalmente para crear un trabajo pendiente del trabajo que se va a procesar de forma asincrónica. Queue Storage se puede combinar con funciones de proceso como Azure Functions para realizar una acción cuando se recibe un mensaje. Por ejemplo, podría hacer que el botón enviar en el sitio web desencadene un mensaje en Queue Storage. Después, podría usar Azure Functions para desencadenar una acción una vez recibido el mensaje.

**Disk Storage**

Conceptualmente, son iguales que un disco físico, pero están virtualizados, lo que ofrece mayor resistencia y disponibilidad que un disco físico. Con los discos administrados, lo único que debe hacer es aprovisionar el disco.

**Descripción de la redundancia de almacenamiento de Azure**

La redundancia garantiza que la cuenta de almacenamiento cumple sus objetivos de disponibilidad y durabilidad, aunque se produzcan errores.

A la hora de decidir qué opción de redundancia es la más adecuada para su escenario, intente buscar un equilibrio entre bajo costo y alta disponibilidad. Entre los factores que ayudan a determinar qué opción de redundancia debe elegir se incluye:

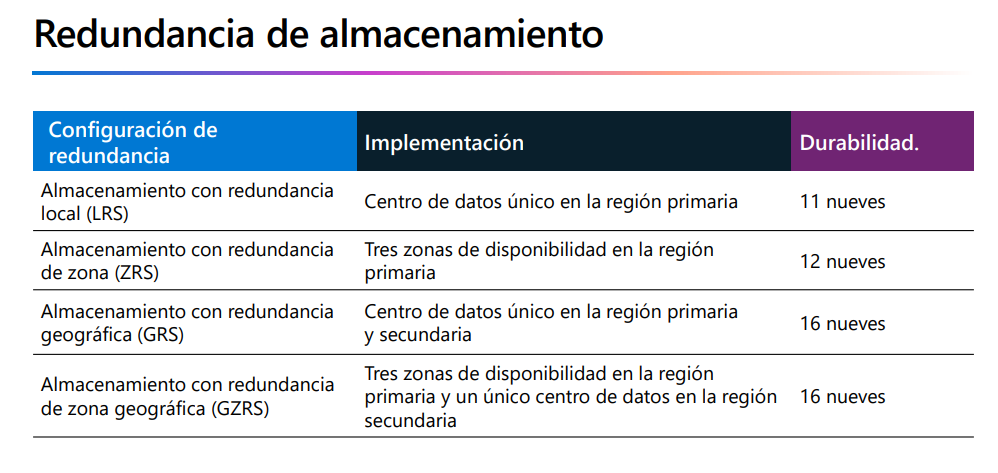
* Cómo se replican los datos en la región primaria.
* Si los datos se replican en una segunda ubicación que está alejada geográficamente de la región primaria, para protegerse frente a desastres regionales.
* Si la aplicación necesita acceso de lectura a los datos replicados en la región secundaria en caso de que la región primaria deje de estar disponible.

Tipos de redundancias:

* Almacenamiento con redundancia local (LRS)
* Almacenamiento con redundancia geográfica (GRS)
* Almacenamiento con redundancia geográfica con acceso de lectura (RA-GRS).
* Almacenamiento con redundancia de zona (ZRS)
* Almacenamiento con redundancia de zona geográfica (GZRS)
* Almacenamiento con redundancia de zona geográfica con acceso de lectura (RA-GZRS)

**Redundancia en la región primaria**

Los datos de una cuenta de Azure Storage siempre se replican tres veces en la región primaria. Azure Storage ofrece dos opciones para replicar los datos en la región primaria, el almacenamiento con redundancia local (LRS) y el almacenamiento con redundancia de zona (ZRS).



LRS es la opción de redundancia de costo más bajo y ofrece la menor durabilidad en comparación con otras opciones. LRS protege los datos frente a errores en la estantería de servidores y en la unidad. No obstante, si se produce un desastre como un incendio o una inundación en el centro de datos, es posible que todas las réplicas de una cuenta de almacenamiento con LRS se pierdan o no se puedan recuperar.

Con ZRS, los datos son accesibles para las operaciones de escritura y lectura incluso si una zona deja de estar disponible. Si alguna zona deja de estar disponible, Azure realiza las actualizaciones de la red, como el redireccionamiento de DNS.

Microsoft recomienda usar ZRS en la región primaria para escenarios que requieren de alta disponibilidad. También se recomienda ZRS para restringir la replicación de datos dentro de un país o región para cumplir los requisitos de gobernanza de datos.

Azure Storage ofrece dos opciones para copiar los datos en una región secundaria: almacenamiento con redundancia geográfica (GRS) y almacenamiento con redundancia de zona geográfica (GZRS). GRS es similar a ejecutar LRS en dos regiones, y GZRS es similar a ejecutar ZRS en la región primaria y LRS en la región secundaria.

De manera predeterminada, los datos de la región secundaria no están disponibles para el acceso de lectura o escritura a menos que haya una conmutación por error a la región secundaria. Si la región primaria deja de estar disponible, puede conmutar por error a la región secundaria. Una vez completada la conmutación por error, la región secundaria se convierte en la región primaria y se pueden leer y escribir datos de nuevo.Con esto explicado ya podemos ver cuales son los tipos de cuenta de almacenamiento de Azure.

**Tipos de cuentas de almacenamiento de Azure:**

| **Tipo** | **Servicios admitidos** | **Opciones de redundancia** | **Uso** |
| --- | --- | --- | --- |
| De uso general estándar, v2 | Blob Storage (incluido Data Lake Storage), Queue Storage, Table Storage y Azure Files | LRS, GRS, RA-GRS, ZRS, GZRS, RA-GZRS | Tipo de cuenta de almacenamiento estándar para blobs, archivos, colas y tablas. Se recomienda para la mayoría de los escenarios con Azure Storage. Si desea compatibilidad con el sistema de archivos de red (NFS) en Azure Files, utilice el tipo de cuenta de recursos compartidos de archivos Premium. |
| Blobs en bloques Premium | Blob Storage (incluido Data Lake Storage) | LRS, ZRS | Tipo de cuenta de almacenamiento Prémium para blobs en bloques y blobs en anexos. Se recomiendan para escenarios con altas tasas de transacciones, que utilizan objetos más pequeños o que requieren una latencia de almacenamiento constantemente baja. |
| Recursos compartidos de archivos Prémium | Azure Files | LRS, ZRS | Tipo de cuenta de almacenamiento Prémium solo para recursos compartidos de archivos. Se recomienda para empresas y aplicaciones de escalado de alto rendimiento. Use este tipo de cuenta si desea una cuenta de almacenamiento que admita recursos compartidos de archivos de Bloque de mensajes del servidor (SMB) y NFS. |
| Blobs en páginas Premium | Solo blobs en páginas | LRS | Tipo de cuenta de almacenamiento prémium solo para blobs en páginas. |

**Identificación de las opciones de migración de datos de Azure**

Azure admite la migración en tiempo real de la infraestructura, las aplicaciones y los datos mediante Azure Migrate, así como la migración asincrónica de datos mediante Azure Data Box.

**Azure Migrate**

Azure Migrate es un servicio que le ayuda a migrar desde un entorno local a la nube. Azure Migrate funciona como centro para ayudarle a administrar la valoración y la migración del centro de datos local a Azure. Ofrece lo siguiente:

* **Plataforma de migración unificada**: un único portal para iniciar, ejecutar y realizar un seguimiento de la migración a Azure.
* **Rango de herramientas**: Rango de herramientas para la evaluación y migración .
* **Assessment and migration** (Evaluación y migración): en el centro de Azure Migrate, puede evaluar y migrar la infraestructura local a Azure.

### Herramientas integradas

Además de trabajar con herramientas de ISV(•ofertas de proveedores de software independientes (ISV).), el centro de Azure Migrate también incluye las siguientes herramientas para ayudar con la migración:

* **Azure Migrate: Discovery and assessment** (Azure Migrate: detección y evaluación). Detecte y evalúe servidores locales que se ejecutan en VMware, Hyper-V y servidores físicos para preparar la migración a Azure.
* **Azure Migrate: Server Migration** (Azure Migrate: migración del servidor). Migre máquinas virtuales de VMware, máquinas virtuales de Hyper-V, servidores físicos, otros servidores virtualizados y máquinas virtuales de la nube pública a Azure.
* **Data Migration Assistant**. Data Migration Assistant es una herramienta independiente para evaluar servidores de SQL Server. Ayuda a identificar posibles problemas que bloquean la migración. Identifica características no admitidas, nuevas características que puede aprovechar después de la migración y la ruta de acceso correcta para la migración de la base de datos.
* **Azure Database Migration Service**. Migre bases de datos locales a máquinas virtuales de Azure en las que se ejecutan SQL Server, Azure SQL Database o instancias administradas de SQL.
* **Web app migration assistant** (Asistente de migración de aplicación web). Azure App Service Migration Assistant es una herramienta independiente para evaluar sitios web locales para la migración a Azure App Service. Use Migration Assistant para migrar aplicaciones web de .NET y PHP a Azure.
* **Azure Data Box**. Use los productos de Azure Data Box para trasladar grandes cantidades de datos sin conexión a Azure.Una vez recibido el dispositivo, puede configurarlo rápidamente mediante la interfaz de usuario web local y conectarlo a la red. Una vez que haya terminado de transferir los datos (ya sea dentro o fuera de Azure), simplemente devuelva Data Box. Si va a transferir datos a Azure, los datos se cargan de forma automática una vez que Microsoft vuelve a recibir Data Box. El servicio de Data Box se encarga de realizar el seguimiento de todo el proceso en Azure Portal.

**Casos de uso de Azure Data Box**

Data Box es ideal para transferir tamaños de datos con más de 40 TB en escenarios sin conectividad de red limitada.

distintos escenarios donde se puede usar Data Box para importar datos en Azure:

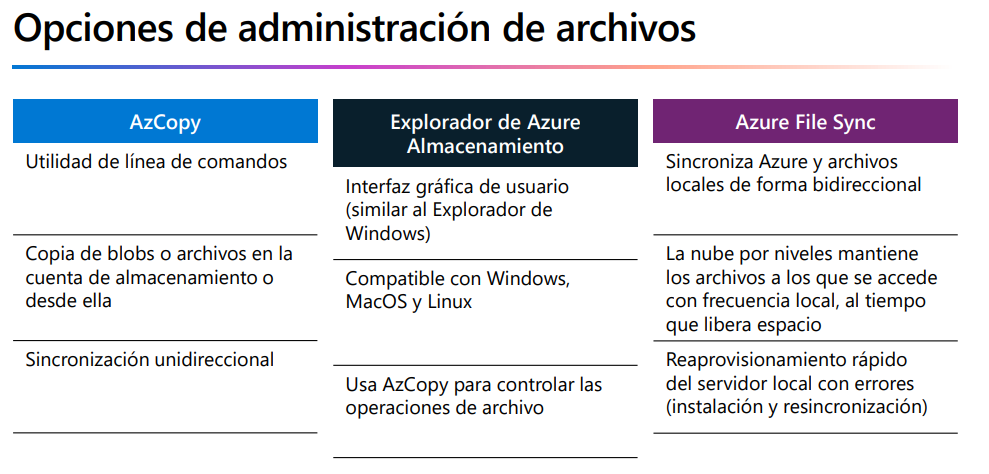
* Migración única: cuando se mueve gran cantidad de datos locales a Azure.
* Traslade una biblioteca multimedia de cintas sin conexión a Azure para crear una biblioteca multimedia en línea.
* Migre la granja de máquinas virtuales, SQL Server y las aplicaciones a Azure.
* Traslade los datos históricos a Azure para un análisis exhaustivo y generar informes con HDInsight.
* Transferencia masiva inicial: cuando se realiza una transferencia masiva inicial con Data Box (inicialización) seguida de transferencias incrementales a través de la red.
* Cargas periódicas: cuando se genera periódicamente una gran cantidad de datos y es necesario moverlos a Azure.

Estos son los distintos escenarios donde se puede usar Data Box para exportar datos a Azure.

* Recuperación ante desastres: cuando se restaura una copia de los datos de Azure en una red local. En un escenario de recuperación ante desastres habitual, se exporta una gran cantidad de datos de Azure se exporta a Data Box. Microsoft luego los envía a Data Box y, en poco tiempo, los datos se restauran en un entorno local.
* Requisitos de seguridad: cuando necesita poder exportar datos de Azure debido a los requisitos de seguridad o de la administración pública.
* Migración de vuelta al entorno local o a otro proveedor de servicios en la nube: cuando quiera mover todos los datos de vuelta al entorno local o a otro proveedor de servicios en la nube, exporte los datos a través de Data Box para migrar las cargas de trabajo.

Una vez que los datos del pedido de importación se cargan en Azure, los discos del dispositivo se limpian. Si el pedido es de exportación, los discos se borran una vez que el dispositivo llega al centro de datos de Azure.

**Identificación de las opciones de movimiento de archivos de Azure**

 -AzCopy, puede copiar archivos entre cuentas de almacenamiento, cargarlos, descargarlos e incluso sincronizarlos. AzCopy incluso se puede configurar para trabajar con otros proveedores de nube para ayudar a mover archivos entre nubes.

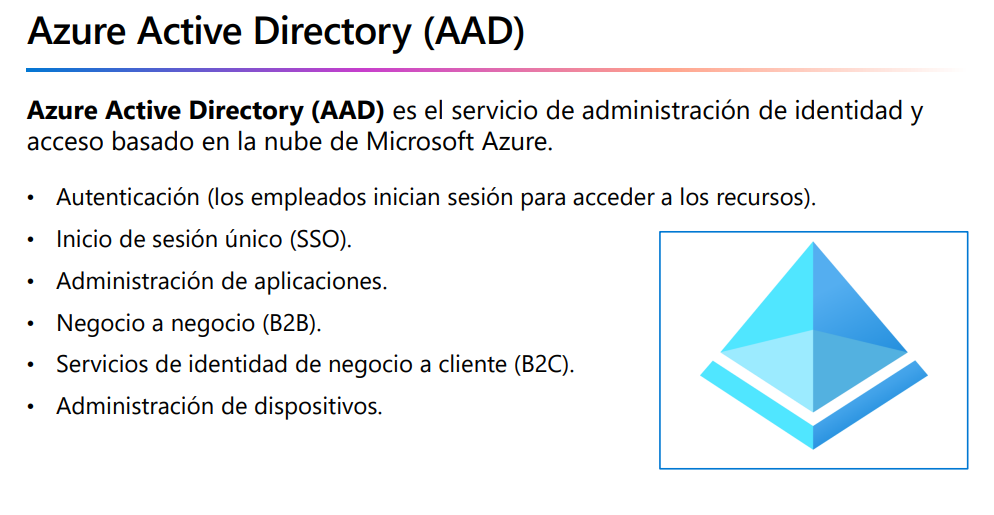
-Explorador de Storage de Azure, puede cargar en Azure, descargar desde Azure o moverse entre cuentas de almacenamiento.

-Azure File Sync es una herramienta que permite centralizar los archivos compartidos en Azure Files y mantener la flexibilidad, el rendimiento y la compatibilidad de un servidor de archivos de Windows.

Con Azure File Sync, puede:

* Usar cualquier protocolo disponible en Windows Server para acceder a sus datos de forma local, como SMB, NFS y FTPS.
* Tener todas las cachés que necesite en todo el mundo.
* Reemplazar un servidor local con errores instalando Azure File Sync en un nuevo servidor del mismo centro de datos.
* Configurar la nube por niveles para que los archivos a los que se accede con más frecuencia se repliquen localmente, mientras que los archivos a los que se accede con poca frecuencia se mantienen en la nube hasta que se soliciten.

# **7.Descripción de los servicios de directorio de Azure**



Si protege las identidades de forma local con AAD, Microsoft no supervisa los intentos de inicio de sesión. Si conecta Active Directory con Azure AD, Microsoft puede detectar intentos de inicio de sesión sospechosos para ayudarle a proteger su entorno sin costo adicional. Por ejemplo, Azure AD puede detectar intentos de inicio de sesión desde ubicaciones inesperadas o dispositivos desconocidos.

Usado por:

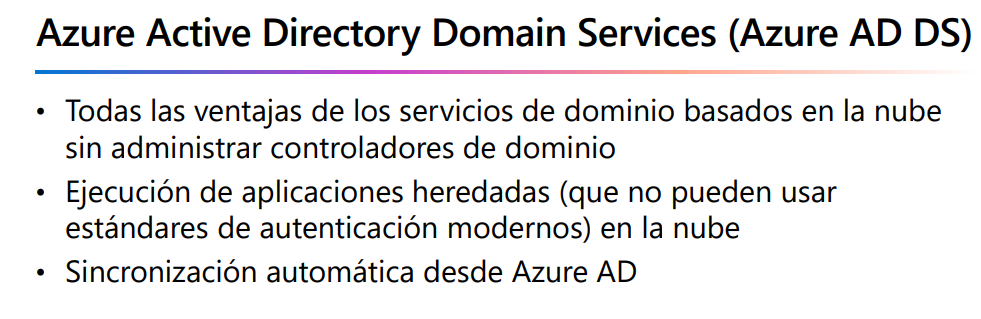
* **Administradores de TI**. Los administradores pueden usar Azure AD para controlar el acceso a las aplicaciones y los recursos en función de sus requisitos empresariales.
* **Desarrolladores de aplicaciones**. Con Azure AD, los desarrolladores pueden agregar funcionalidad a las aplicaciones que compilan mediante un enfoque basado en estándares. Por ejemplo, pueden agregar funcionalidad de SSO a una aplicación o habilitar una aplicación para que funcione con las credenciales existentes de un usuario.
* **Usuarios**. Los usuarios pueden administrar sus identidades y realizar acciones de mantenimiento como el autoservicio de restablecimiento de contraseña.
* **Suscriptores de servicios en línea**. Los suscriptores de Microsoft 365, Microsoft Office 365, Azure y Microsoft Dynamics CRM Online ya usan Azure AD para autenticarse en su cuenta.

## ¿Qué hace Azure AD?

Azure AD proporciona servicios como:

* **Autenticación**: comprobación de la identidad para acceder a aplicaciones y recursos. También incluye funciones como el autoservicio de restablecimiento de contraseña, la autenticación multifactor, una lista personalizada de contraseñas prohibidas y servicios de bloqueo inteligente.
* **Inicio de sesión único**: gracias al inicio de sesión único (SSO). Los usuarios tienen un solo nombre de usuario y una sola contraseña para acceder a varias aplicaciones. Cuando los usuarios cambian de rol o dejan una organización, las modificaciones de acceso se asocian a esa identidad, lo que reduce considerablemente el esfuerzo necesario para cambiar o deshabilitar cuentas
* **Administración de aplicaciones**: con Azure AD, puede administrar las aplicaciones en la nube y locales. Características como Application Proxy, las aplicaciones SaaS, el portal Aplicaciones y el inicio de sesión único proporcionan una mejor experiencia de usuario.
* **Administración de dispositivos**: además de cuentas de usuarios individuales, Azure AD admite el registro de dispositivos. El registro permite administrar los dispositivos a través de herramientas como Microsoft Intune. También permite que las directivas de acceso condicional basadas en dispositivos limiten los intentos de acceso a solo aquellos que proceden de dispositivos conocidos, independientemente de la cuenta de usuario solicitante.

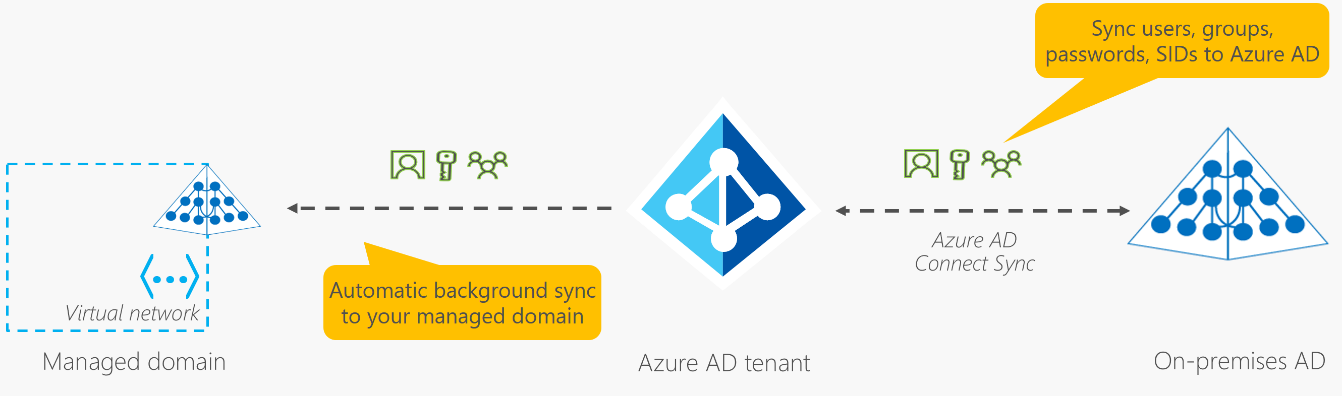
## ¿Qué es Azure Active Directory Domain Services?



Azure AD DS se integra con el inquilino de Azure AD existente. Esta integración permite a los usuarios iniciar sesión en los servicios y las aplicaciones conectados al dominio administrado con sus credenciales existentes. También puede usar grupos y cuentas de usuario existentes para proteger el acceso a los recursos. Estas características proporcionan una migración mediante lift-and-shift más fluida de los recursos locales a Azure.

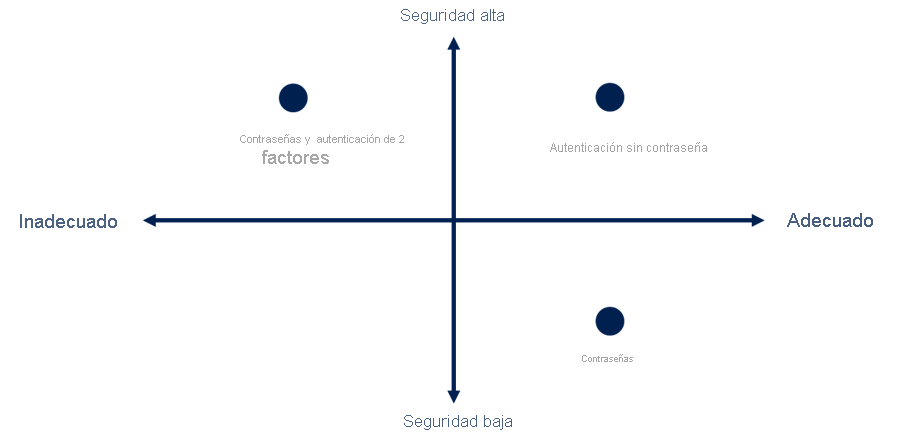
### ¿Cómo funciona Azure AD DS?

Cuando cree un dominio administrado de Azure AD DS, defina un espacio de nombres único. Este espacio de nombres es el nombre de dominio. Después, se implementan dos controladores de dominio de Windows Server en la región de Azure seleccionada. Esta implementación de controladores de dominio se conoce como "conjunto de réplicas".

No es necesario administrar, configurar ni actualizar estos controladores de dominio. La plataforma Azure administra los controladores de dominio como parte del dominio administrado, incluidas las copias de seguridad y el cifrado en reposo mediante Azure Disk Encryption. 

# **7.1Descripción de los métodos de autenticación de Azure**

La autenticación es el proceso de establecimiento de la identidad de una persona, servicio y dispositivo. Requiere que la persona, el servicio o el dispositivo proporcionen algún tipo de credencial para demostrar quiénes son.



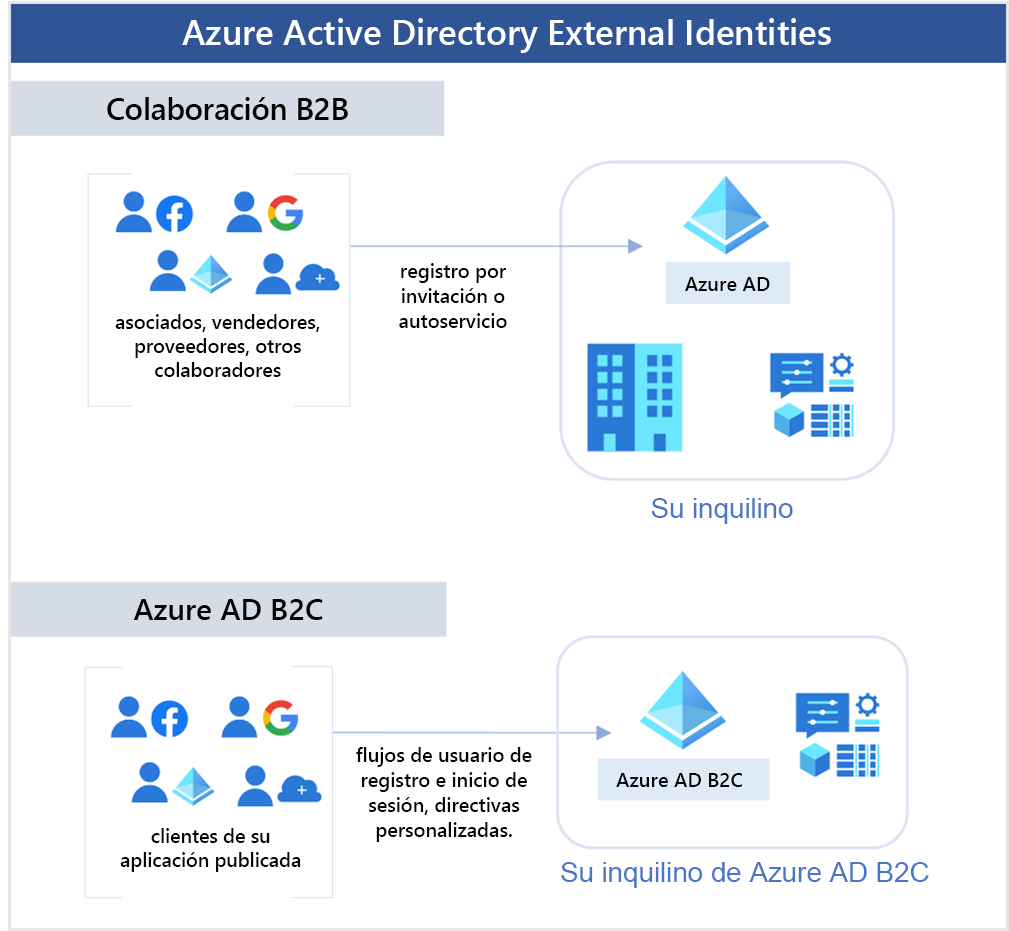
Tipos:

* El inicio de sesión único (SSO) [Del que hemos hablado antes]
* Azure AD Multi-Factor Authentication es un servicio de Microsoft que proporciona funcionalidades de autenticación multifactor. Azure AD Multi-Factor Authentication permite a los usuarios elegir una forma adicional de autenticación durante el inicio de sesión, como una llamada de teléfono o una notificación de aplicación móvil. Se requieren dos o más elementos para una autenticación completa. Estos elementos se dividen en tres categorías:
  + Algo que el usuario sabe: puede ser una pregunta de seguridad.
  + Algo que el usuario tiene: se puede tratar de un código que se envía al teléfono móvil del usuario.
  + Algo que el usuario es: normalmente, algún tipo de propiedad biométrica, como la huella dactilar o el escaneo facial.

La MFA ayuda a protegerse frente a las contraseñas en riesgo en situaciones en las que la contraseña se vio comprometida, pero el segundo

* autenticación sin contraseña : La autenticación sin contraseña debe configurarse en un dispositivo para que funcione.Se podrá autenticar sin usar una contraseña con:
  + Windows Hello para empresas: La información biométrica y las credenciales de PIN están vinculadas directamente al equipo del usuario, lo que impide el acceso de cualquier persona que no sea el propietario.
  + Aplicación Microsoft Authenticator: Puede permitir que el teléfono del empleado se convierta en un método de autenticación sin contraseña. Reciben una notificación en su teléfono, comprueban que el número mostrado en la pantalla coincide con el de su teléfono y, a continuación, usan datos biométricos (huella dactilar o reconocimiento facial) o el PIN para confirmarlo.
  + Claves de seguridad FIDO2: Las claves de seguridad FIDO2 son un método de autenticación sin contraseña permite a los usuarios y a las organizaciones mediante una clave de seguridad externa o una clave de plataforma integrada en un dispositivo. Estas llaves de seguridad de FIDO2 suelen ser dispositivos USB, pero también pueden usar Bluetooth o NFC.

**7.2Descripción de identidades externas de Azure**

Azure AD External Identities hace referencia a todas las formas en que puede interactuar de forma segura con usuarios externos a su organización. Si quiere colaborar con asociados, distribuidores o proveedores, puede compartir los recursos y definir cómo los usuarios internos pueden acceder a organizaciones externas. El proveedor de identidades administra la identidad del usuario externo y el usuario administra el acceso a sus aplicaciones con Azure AD o Azure AD B2C para mantener protegidos los recursos. 

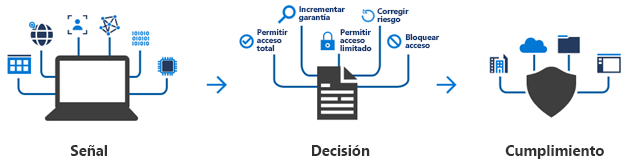
Las siguientes funcionalidades componen External Identities:

* **Colaboración de empresa a empresa (B2B)**: colabore con usuarios externos y permítales usar su identidad preferida para iniciar sesión en las aplicaciones de Microsoft u otras aplicaciones empresariales (aplicaciones SaaS, aplicaciones desarrolladas de forma personalizada, etc.). Los usuarios de colaboración B2B se representan en el directorio, normalmente como usuarios invitados.
* **Conexión directa B2B**: establezca una confianza mutua y en dos sentidos con otra Azure AD para una colaboración sin problemas. La conexión directa B2B actualmente es compatible con los canales compartidos de Teams, lo que permite a los usuarios externos acceder a sus recursos desde sus instancias principales de Teams. Los usuarios de conexión directa B2B no se representan en el directorio, pero son visibles desde el canal compartido de Teams y se pueden supervisar en Teams informes del centro de administración.
* **Empresa a cliente de Azure AD (B2C)**: publique aplicaciones SaaS modernas o aplicaciones desarrolladas de forma personalizada (excepto aplicaciones de Microsoft) para consumidores y clientes, mientras usa Azure AD B2C para la administración de identidades y acceso.

También puede asegurarse fácilmente de que los usuarios invitados tengan el acceso adecuado.

**7.2Descripción del acceso condicional de Azure**

El acceso condicional es una herramienta que usa Azure Active Directory para permitir (o denegar) el acceso a los recursos en función de señales de identidad. Estas señales incluyen quién es el usuario, dónde se encuentra y desde qué dispositivo solicita el acceso. El acceso condicional también proporciona una experiencia de autenticación multifactor más pormenorizada para los usuarios. Por ejemplo, es posible que al usuario no se le solicite un segundo factor de autenticación si está en una ubicación conocida. Pero si sus señales de inicio de sesión son inusuales o su ubicación es inesperada, es posible que se le exija un segundo factor de autenticación.



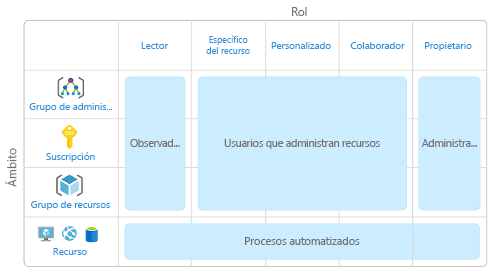
**¿Cuándo se puede usar el acceso condicional?**

El acceso condicional resulta útil en los casos siguientes:

* Para acceder a una aplicación en función del rol, la ubicación o la red del solicitante. Por ejemplo, podría requerir MFA para administradores, pero no para usuarios normales
* Para requerir el acceso a los servicios solo a través de aplicaciones cliente aprobadas. Por ejemplo, podría limitar qué aplicaciones de correo electrónico pueden conectarse al servicio de correo electrónico.
* Exija que los usuarios accedan a la aplicación solo desde dispositivos administrados.
* Para bloquear el acceso desde orígenes que no son de confianza, como ubicaciones desconocidas o inesperadas.

**7.4Descripción del control de acceso basado en roles de Azure**

El principio de privilegios mínimos indica que solo debe conceder acceso al nivel necesario para completar una tarea. En vez de definir los requisitos de acceso detallados de cada individuo y, después, ir actualizándolos a medida que se vayan creando más recursos o se unan nuevos miembros al equipo, Azure permite controlar el acceso a través del control de acceso basado en roles de Azure (RBAC de Azure). Azure proporciona roles integrados que describen las reglas de acceso comunes de los recursos en la nube. También podemos definir nuestros propios roles. Cada rol tiene un conjunto asociado de permisos de acceso que tienen que ver con ese rol. Cuando se asignan usuarios o grupos a uno o varios roles, reciben todos los permisos de acceso asociados.



Los observadores, los usuarios que administran recursos, los administradores y los procesos automatizados muestran los tipos de usuarios o cuentas que se suelen asignar a cada uno de los distintos roles.

Por ejemplo:

* Cuando asignamos el rol Propietario a un usuario en el ámbito del grupo de administración, dicho usuario podrá administrar todo el contenido de todas las suscripciones dentro de ese grupo de administración.

RBAC de Azure se aplica a cualquier acción que se inicie en un recurso de Azure que pasa por Azure Resource Manager. Resource Manager es un servicio de administración que proporciona una forma de organizar y proteger nuestros recursos en la nube.

Normalmente, se accede a Resource Manager a través de Azure Portal, Azure Cloud Shell, Azure PowerShell y la CLI de Azure. RBAC de Azure no aplica permisos de acceso en el nivel de aplicación ni de datos. La seguridad de la aplicación debe controlarla la propia aplicación.

**7.5Descripción del modelo de Confianza cero**

Confianza cero es un modelo de seguridad que supone el peor de los escenarios posibles y protege los recursos con esa expectativa. Presupone que hay una vulneración y comprueba todas las solicitudes como si provinieran de una red no controlada.

el modelo de seguridad de Confianza cero, que se basa en estos principios rectores:

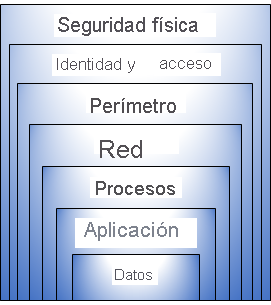
* **Comprobar explícitamente**: realice siempre las operaciones de autorización y autenticación en función de todos los puntos de datos disponibles.
* **Usar el acceso de privilegios mínimos**: limite el acceso de los usuarios con Just-in-Time y Just-Enough-Access (JIT/JEA), directivas que se adaptan al nivel de riesgo y protección de datos.
* **Asumir que hay brechas**: minimice el radio de expansión y el acceso a los segmentos. Comprobación del cifrado de un extremo a otro. Utilice el análisis para obtener visibilidad, impulsar la detección de amenazas y mejorar las defensas.



**7.5Descripción de defensa en profundidad**

Una estrategia de defensa en profundidad usa una serie de mecanismos para ralentizar el avance de un ataque dirigido a adquirir acceso no autorizado a los datos.

Puede visualizar la defensa en profundidad como un conjunto de capas, con los datos que se van a proteger en el centro y todas las demás capas en funcionamiento para proteger esa capa de datos central.

****Cada capa proporciona protección de modo que, si se produce una brecha en una capa, ya existe otra en funcionamiento para evitar una mayor exposición. Este enfoque elimina la dependencia de cualquier capa de protección única.

Aquí tiene una breve descripción del rol de cada capa:

* La capa de seguridad física es la protección física del acceso a los edificios y el control del acceso al hardware de proceso del centro de datos.
* La capa de identidad y acceso controla el acceso a la infraestructura y al control de cambios.
  + En esta capa, es importante que realice lo siguiente:
    - Controle el acceso a la infraestructura y al control de cambios.
    - Use el inicio de sesión único (SSO)y la autenticación multifactor.
    - Audite los eventos y los cambios.
* La capa perimetral usa protección frente a ataques de denegación de servicio distribuido (DDoS) para filtrar los ataques a gran escala antes de que puedan causar una denegación de servicio para los usuarios.
  + En esta capa, es importante que realice lo siguiente:
  + Use protección contra DDoS para filtrar los ataques a gran escala antes de que puedan afectar a la disponibilidad de un sistema para los usuarios.
  + Use firewalls perimetrales para identificar los ataques malintencionados contra la red y alertar sobre ellos.
* La capa de red limita la comunicación entre los recursos a través de controles de acceso y segmentación.
  + En esta capa, es importante que realice lo siguiente:
  + Limite la comunicación entre los recursos.
  + Deniegue de forma predeterminada.
  + Restrinja el acceso entrante de Internet y limite el saliente cuando sea apropiado.
  + Implemente conectividad segura a las redes locales.
* La capa de proceso protege el acceso a las máquinas virtuales.
  + En esta capa, es importante que realice lo siguiente:
  + Proteja el acceso a las máquinas virtuales.
  + Implemente la protección del punto de conexión de los dispositivos y mantenga los sistemas revisados y actualizados.
* La capa de aplicación ayuda a garantizar que las aplicaciones sean seguras y estén libres de vulnerabilidades de seguridad.
  + En esta capa, es importante que realice lo siguiente:
  + Garantice que las aplicaciones son seguras y están libres de vulnerabilidades.
  + Almacene los secretos de aplicación confidenciales en un medio de almacenamiento seguro.
  + Convierta la seguridad en un requisito de diseño en todo el desarrollo de aplicaciones.
* La capa de datos controla el acceso a los datos empresariales y de clientes que es necesario proteger.
  + En casi todos los casos, los atacantes intentan conseguir datos:
  + Almacenados en una base de datos.
  + Almacenados en discos en máquinas virtuales.
  + Almacenados en aplicaciones de software como servicio (SaaS), como Office 365.
  + Administrados mediante el almacenamiento en la nube.

**7.7Descripción de Microsoft Defender for Cloud**



La implementación de Defender for Cloud es fácil, ya está integrada de forma nativa en Azure.

Cuando sea necesario, Defender for Cloud puede implementar automáticamente un agente de Log Analytics para recopilar datos relacionados con la seguridad. En el caso de las máquinas de Azure, la implementación se controla directamente. En entornos híbridos y con varias nubes, los planes de Microsoft Defender se amplían a máquinas que no son de Azure con la ayuda de Azure Arc.

Las características de Defender for Cloud le permite detectar amenazas en:

* Servicios de PaaS de Azure: puede detectar amenazas dirigidas a servicios de Azure como Azure App Service, Azure SQL, la cuenta de Azure Storage y otros servicios de datos. También puede realizar la detección de anomalías en los registros de actividad de Azure mediante la integración nativa con Microsoft Defender para aplicaciones en la nube.
* Servicios de datos de Azure: Defender for Cloud incluye capacidades que le ayudarán a clasificar automáticamente los datos en Azure SQL. También puede obtener evaluaciones de las posibles vulnerabilidades en los servicios de Azure SQL y Azure Storage, además de recomendaciones sobre cómo mitigarlas.
* Redes: Defender for Cloud le permite limitar la exposición a los ataques por fuerza bruta. Si reduce el acceso a los puertos de las máquinas virtuales mediante el acceso de máquina virtual Just-In-Time, puede proteger la red al prevenir el acceso innecesario. Puede establecer directivas de acceso seguro en los puertos seleccionados, solo para usuarios autorizados, direcciones IP o intervalos de direcciones IP de origen permitidos y durante un período limitado.

### Defensa de los recursos híbridos

Puede agregar funcionalidades de Defender for Cloud a su entorno de nube híbrida para proteger los servidores que no sean de Azure.

Defender for Cloud también puede proteger los recursos de otras nubes (como AWS y GCP).

Por ejemplo, si ha conectado una cuenta de Amazon Web Services (AWS) a una suscripción de Azure, puede habilitar cualquiera de estas protecciones:

* Las características de CSPM de Defender for Cloud se extienden a los recursos de AWS. Este plan sin agente evalúa los recursos de AWS según las recomendaciones de seguridad específicas de AWS e incluye los resultados en la puntuación de seguridad. También se evaluará el cumplimiento de los recursos de los estándares integrados específicos de AWS (AWS CIS, AWS PCI DSS y Procedimientos recomendados de seguridad fundamentales de AWS). La página de inventario de recursos de Defender for Cloud es una característica habilitada para varias nubes, que permite administrar los recursos de AWS junto con los de Azure.
* Microsoft Defender para contenedores amplía la detección de amenazas de contenedores y defensas avanzadas a los clústeres Linux de Amazon EKS.
* Microsoft Defender para servidores proporciona detección de amenazas y defensas avanzadas en las instancias de EC2 con Windows y Linux.

## Evaluación, protección y defensa

Defender for Cloud cubre tres necesidades vitales a medida que administra la seguridad de los recursos y las cargas de trabajo en la nube y en el entorno local:



### Defender

Las dos primeras áreas se centraban en evaluar, supervisar y mantener su entorno. Defender for Cloud también le permite defender su entorno proporcionando alertas de seguridad y características avanzadas de protección contra amenazas.

#### Alertas de seguridad

Cuando Defender para la nube detecta una amenaza en cualquier área del entorno, genera una alerta de seguridad. Alertas de seguridad:

* Descripción de los detalles de los recursos afectados
* Sugerencia de pasos para la corrección
* Suministro, en algunos casos, de una opción para desencadenar una aplicación lógica en la respuesta

Tanto si Defender para la nube genera una alerta como si la recibe desde un producto de seguridad integrado, puede exportarla. La protección contra amenazas de Defender para la nube incluye el análisis de la cadena de eliminación de fusión, que correlaciona de manera automática las alertas del entorno en función del análisis Cyber Kill Chain, para ayudarle a comprender mejor todo el proceso de un ataque, dónde empezó y qué tipo de impacto tuvo en los recursos.

#### Protección contra amenazas avanzada

Defender for Cloud proporciona características avanzadas de protección contra amenazas para muchos de los recursos implementados, incluidas las máquinas virtuales, las bases de datos SQL, los contenedores, las aplicaciones web y la red. Entre las protecciones se incluyen la protección de los puertos de administración de las VM con acceso Just-in-Time y controles de aplicaciones adaptables para crear listas de permitidos con las aplicaciones que deben o no ejecutarse en las máquinas.

**AZ-204**

Azure App Service es un servicio basado en HTTP para hospedar aplicaciones web, API de REST y back-ends para dispositivos móviles. Puede desarrollar en su lenguaje o marco de programación favorito. Las aplicaciones se ejecutan y escalan fácilmente en los entornos Windows y Linux.

**Compatibilidad integrada con el escalado automático**

En Azure App Service se integra la capacidad de escalar o reducir verticalmente, o bien escalar o reducir horizontalmente. En función del uso de la aplicación web, puede escalar o reducir verticalmente los recursos de la máquina subyacente en la que se hospeda la aplicación web.