

# AZUR CERTIFICADO

AZ-900

Microsoft Azure  
Fundamentos



Tutoriales Dojo  
Guía de estudio y hojas de trucos



## TABLA DE CONTENIDO

<b>INTRODUCCIÓN</b>	<b>4</b>
<b>DESCRIPCIÓN GENERAL DEL EXAMEN DE AZ-900 MICROSOFT AZURE FUNDAMENTALS</b>	<b>5</b>
Detalles del examen	5
Dominios de examen	8
Sistema de puntuación de exámenes	8
Beneficio del examen	9
<b>GUÍA DE ESTUDIO DEL EXAMEN AZ-900 MICROSOFT AZURE FUNDAMENTALS</b>	<b>10</b>
<b>HOJAS DE TRUCOS AZUR</b>	<b>17</b>
DESCRIPCIÓN GENERAL AZURE	17
Conceptos de Azure Cloud	17
Azure CapEx frente a OpEx	19
Modelos de servicios en la nube de Azure Modelos de arquitectura en la nube de Azure Infraestructura global de Azure	20
Herramientas de usuario de Azure	24
PRECIOS AZUR	26
CALCULAR	28
Máquinas virtuales de Azure	30
Servicio de aplicaciones de Azure	34
Azure Container Instances (ACI) Azure	40
Kubernetes Service (AKS) Azure Container Registry (ACR) Azure Batch	43
Azure CycleCloud	45
Azure Service Fabric	47
<a href="https://docs.microsoft.com/en-us/azure/service-fabric/service-fabric-overview">https://docs.microsoft.com/en-us/azure/service-fabric/service-fabric-overview</a> Escritorio virtual de Windows	50
ALMACENAMIENTO	52
Descripción general de Azure Storage	53
Almacenamiento de blobs de Azure	54
Almacenamiento en disco de Azure	60
Archivos de Azure	64
Almacenamiento en cola de Azure	66



---

Almacenamiento de tablas de Azure	71
Almacenamiento de archivos de Azure	72
BASE DE DATOS	73
Azure Cosmos DB	73
Azure SQL	75
Azure Database Migration Service (DMS) Azure	77
Database for MySQL y PostgreSQL	78
REDES Y ENTREGA	
DE CONTENIDO	79
Azure Virtual Network (VNet) Azure	79
Load Balancer	81
Puerta de enlace de VPN de Azure	84
Puerta de enlace de aplicaciones de Azure	86
Azure Content Delivery Network (CDN)	87
Administrador de tráfico de Azure	89
DNS de Azure	90
Puerta de entrada azul	91
Azure ExpressRoute	92
SEGURIDAD	93
Azure Active Directory (AD)	93
Cortafuegos de Azure	95
Protección contra DDoS de Azure	97
Centro de seguridad de Azure	99
Azure Key Vault	100
Azure Information Protection (AIP)	101
Azure Advanced Threat Protection (ATP)	102
Azure Sentinel	103
Ofertas de cumplimiento de Microsoft	104
SEGUIMIENTO Y GESTIÓN	106
Monitor de Azure	106
Estado del servicio de Azure	108
Política de Azure	109
Asesor de Azure	110
Blueprints de Azure	111
Administrador de cumplimiento de Azure	112
Azure RBAC	113
SOLUCIONES	115
Azure Internet de las cosas (IoT)	115

---



---

Azure Big Data	117
Aprendizaje automático de Azure	118
Azure sin servidor	119
Azure DevOps	120
<b>OTRAS NOTAS AZURAS</b>	<b>121</b>
Bus de servicio de Azure	121
<b>COMPARACIÓN DE SERVICIOS AZURE</b>	<b>123</b>
Azure Virtual Machines vs aplicación web	123
Azure Container Instances (ACI) frente a Azure Kubernetes Service (AKS) Azure Functions frente a Logic Apps frente a Event Grid	124
Conjunto de escala de Azure frente a conjunto de disponibilidad Blob de Azure frente a disco frente a almacenamiento de archivos	125
Almacenamiento con redundancia local (LRS) frente a almacenamiento con redundancia de zona (ZRS) frente a (GRS) Azure Load Balancer frente a App Gateway frente a Traffic Manager	126
Grupo de seguridad de red (NSG) frente a grupo de seguridad de aplicaciones Centro de seguridad de Azure frente a Sentinel	127
Azure Policy frente al control de acceso basado en roles de Azure (RBAC)	128
<b>SERVICIOS AWS vs AZURE</b>	<b>134</b>
Calcular	135
Almacenamiento	137
Bases de datos	138
Redes	140
Seguridad e Identidad	142
<b>OBSERVACIONES FINALES</b>	<b>144</b>
<b>SOBRE LOS AUTORES</b>	<b>145</b>



## INTRODUCCIÓN

Con el rápido avance de la tecnología, las empresas están adoptando tecnologías más nuevas que ayudarán a sus negocios a transformarse y crecer. Microsoft Azure es una de las tecnologías emergentes que puede aprovechar en esta era, ya que muchas empresas están cambiando sus infraestructuras existentes en la nube. A diferencia de la configuración tradicional, la computación en la nube le permite obtener recursos bajo demanda con un solo clic en su plataforma, incluidos los servidores, el almacenamiento, las bases de datos, las redes, los análisis, la inteligencia artificial y mucho más.

Microsoft Azure ofrece una gama de servicios en la nube, según las necesidades de su negocio. Estos servicios se actualizan continuamente y cada año se agregan nuevas funciones para brindar satisfacción al cliente. Dado que los recursos y servicios de Azure son demasiado amplios, **Certificación de Microsoft Azure** El programa ofrece diferentes rutas de certificación que ayudarán a los aspirantes a candidatos y profesionales de TI a validar sus habilidades y conocimientos para maximizar las soluciones creadas en la nube.

Microsoft Azure es el segundo mayor proveedor de servicios en la nube del mercado después de AWS, y muchas empresas ahora están adoptando un multicloud estrategia, lo que hace que sea aún más beneficioso para los profesionales de TI como usted ampliar su conjunto de habilidades y aprender múltiples tecnologías en la nube. Aprender es mucho más divertido si lo fusiona con varios servicios en la nube. Será un viaje emocionante y agradable para ti, y el primer paso es convertirte

**AZ-900 Fundamentos de Microsoft Azure** certificado. Este libro electrónico lo ayudará a familiarizarse con los conceptos básicos de la nube, así como con los servicios centrales de Microsoft Azure, que son los componentes básicos que lo ayudarán a aprobar el examen y hacer un cambio profesional exitoso hacia la computación en la nube.

**Nota:** Hemos tenido especial cuidado en elaborar estas guías de estudio y hojas de trucos; sin embargo, esto está destinado a ser solo un recurso complementario cuando se prepara para el examen. Recomendamos encarecidamente trabajar en sesiones prácticas y exámenes de práctica para ampliar aún más sus conocimientos y mejorar sus habilidades para tomar exámenes.



## DESCRIPCIÓN GENERAL DEL EXAMEN DE AZ-900 MICROSOFT AZURE FUNDAMENTALS

El programa de certificación de Microsoft Azure valida las habilidades y los conocimientos técnicos para crear aplicaciones seguras y confiables basadas en la nube utilizando la plataforma Azure. Al aprobar con éxito el examen de Microsoft Azure, las personas pueden demostrar su experiencia a sus empleadores actuales y futuros. El examen AZ-900 Microsoft Azure Fundamentals es actualmente el certificado más básico que puede obtener y también es conocido por ser el más fácil entre todos los exámenes de certificación de Azure.

### Detalles del examen

El examen AZ-900 Microsoft Azure Fundamentals está destinado a candidatos que tienen el conocimiento y las habilidades necesarias para demostrar de manera efectiva una comprensión general de Azure Cloud, independientemente de los roles técnicos específicos abordados por otras certificaciones de Microsoft (por ejemplo, administrador asociado y desarrollador asociado). . El examen se compone de diferentes tipos de preguntas.

Para los tipos de preguntas de opción múltiple, tendrá que elegir una respuesta correcta de entre cuatro opciones.

A company is planning to deploy its suite of enterprise applications to Microsoft Azure, where each application has several dependencies and subcomponents. The company must also control and manage the patching activities of the underlying operating system of the servers.

What type of cloud deployment solution should you recommend?

- Infrastructure as a Service (IaaS)
- Platform as a Service (PaaS)
- Software as a Service (SaaS)
- Functions as a service (FaaS)

Para los tipos de enunciados de preguntas, marque la frase subrayada si es correcta. Si es incorrecta, reemplace la opción que hace que la declaración sea correcta.



*Instructions: Check the underlined phrase. If it is correct then choose "No change is needed" and if it is wrong, select the option that makes the statement correct.*

If a resource group has been applied with a CanNotDelete lock, then the administrator can directly delete it without removing the lock.

- No change is needed
- the administrator must remove the lock first before it can be deleted.
- the administrator must modify the associated Azure Policy first before it can be deleted.
- the administrator must delete the associated CanNotDelete tag first before it can be deleted.

Para las preguntas de arrastrar y soltar, haga coincidir los elementos arrastrándolos a sus descripciones correctas.

*Instructions: Drag the appropriate item from the column on the left to its description on the right. Each correct match is worth one point.*

**ANSWER OPTIONS**

**ANSWER AREA**

⋮ NIST

A non-regulatory agency of the United States government that defines industry standards.

⋮ Azure Government

An independent, non-governmental organization that defines international standards that are used in all industries across the globe.

⋮ ISO

A regulation on data protection and privacy in the European Union and the European Economic Area.

⋮ GDPR

A dedicated cloud for US federal, state, and other partner agencies.



Para los tipos de preguntas desplegables, seleccione la respuesta correcta de la lista desplegable de opciones.

Azure App Service and Azure Virtual Machines are services that you can use in Azure. For each service, you have to determine its correct type of cloud service model.

Select the correct answer from the drop-down list of options. Each correct selection is worth one point.

Azure Virtual Machines

Azure App Service

Para los tipos de preguntas de Hotspot, como múltiples Sí / No, evalúe si las declaraciones presentadas relacionadas con un tema determinado son correctas / incorrectas.

For each of the following items, choose Yes if the statement is true or choose No if the statement is false. Take note that each correct item is worth one point.

Questions	Yes	No
Azure virtual machines are billed on a per-hour basis.	<input type="radio"/>	<input type="radio"/>
When you delete a virtual machine in Azure, by default, any disks that are attached to the VM are deleted.	<input type="radio"/>	<input type="radio"/>
Disks attached to stopped virtual machines do not incur costs.	<input type="radio"/>	<input type="radio"/>

Puede realizar el examen a través de la supervisión en línea o en un centro de pruebas cercano.

Código de examen:	AZ-900
Prerrequisitos:	Ninguna
No. de preguntas:	30-40
Rango de puntuación:	100-1000
Costo:	99 USD
Puntaje de aprobación:	700
Límite de tiempo:	90 minutos



## Dominios de examen

El examen AZ-900 Microsoft Azure Fundamentals tiene seis áreas para evaluar sus habilidades, cada una con su correspondiente peso y cobertura temática. Las habilidades que se miden son: conceptos de nube (15-20%), servicios básicos de Azure (30-35%), soluciones básicas y herramientas de administración en Azure (10-15%), seguridad general y funciones de seguridad de red (10-15%) , Funciones de identidad, gobernanza, privacidad y cumplimiento (20-25%) y acuerdos de nivel de servicio y administración de costos de Azure (10-15%).

### Conceptos de nube

- Identificar los beneficios y las consideraciones del uso de servicios en la nube.
- Describir las diferencias entre categorías de servicios en la nube.
- Describir las diferencias entre los tipos de computación en la nube.

### Servicios básicos de Azure

- Describir los componentes arquitectónicos centrales de Azure
- Describir los recursos principales disponibles en Azure

### Soluciones principales y herramientas de administración en Azure

- Describir las soluciones principales disponibles en Azure
- Describir las herramientas de administración de Azure

### Funciones de seguridad general y de red

- Describir las características de seguridad de Azure
- Describir la seguridad de la red de Azure

### Funciones de identidad, gobernanza, privacidad y cumplimiento

- Describir los principales servicios de identidad de Azure.
- Describir las características de gobierno de Azure
- Describir los recursos de privacidad y cumplimiento

### Acuerdos de nivel de servicio y administración de costos de Azure

- Describir métodos para planificar y administrar costos.
- Describir los acuerdos de nivel de servicio (SLA) de Azure y los ciclos de vida del servicio.

## Sistema de puntuación de exámenes

Puede obtener una puntuación de 100 a 1.000 con una puntuación mínima de 700 cuando realiza el examen AZ-900 Microsoft Azure Fundamentals. Microsoft utiliza un modelo de puntuación escalado para asociar puntuaciones en varios tipos de exámenes que pueden tener diferentes niveles de dificultad. Su informe completo de calificaciones le será enviado por correo electrónico entre 1 y 5 días hábiles después de su examen. Sin embargo, tan pronto como termine su examen, verá inmediatamente una notificación de aprobado o reprobado en la pantalla de prueba.



---

Para las personas que, lamentablemente, no aprueban sus exámenes, deben esperar 24 horas antes de que se les permita volver a tomar el examen. No existe un límite estricto en la cantidad de intentos que puede volver a tomar un examen.

Una vez que reciba su informe de calificación por correo electrónico, el resultado también debe guardarse en su cuenta de certificación de Microsoft. El informe de calificación contiene una tabla de su desempeño en cada dominio e indicará si ha alcanzado el nivel de competencia requerido para estos. Tenga en cuenta que no necesita adquirir competencia en todas las áreas para aprobar el examen. En la primera parte del informe, habrá un resumen de desempeño por sección de examen que resalta sus fortalezas y debilidades, lo que puede ayudarlo a determinar las áreas en las que necesita mejorar.

#### Beneficio del examen

Si aprueba con éxito cualquier examen de certificación de Microsoft, recibirá un **Insignia digital certificada**. Puede mostrar sus logros a sus colegas y empleadores agregando estas insignias digitales a sus firmas de correo electrónico, perfil de Linkedin o en sus cuentas de redes sociales. Para ver sus insignias, simplemente vaya a la sección "Panel de control" de su cuenta Acclaim.

Puede visitar la página oficial de preguntas frecuentes sobre certificaciones de Microsoft para ver las preguntas más frecuentes sobre cómo obtener la certificación y otra información sobre la certificación de Microsoft:

<https://docs.microsoft.com/en-us/learn/certifications/certification-exam-policies> .



## GUÍA DE ESTUDIO DEL EXAMEN AZ-900 MICROSOFT AZURE FUNDAMENTALS

El examen de certificación AZ-900 Microsoft Azure Fundamentals está destinado a personas que desean tener un conocimiento básico al aventurarse en la nube. Aunque la prueba AZ-900 es la más fácil de lograr entre todos los exámenes de certificación de Azure, aún necesita aprender y comprender correctamente los conceptos de la computación en la nube y conocer los conceptos básicos de los servicios de Azure.

En el examen de conceptos básicos de Microsoft Azure (o AZ-900 para abreviar), las preguntas evaluarán su capacidad para:

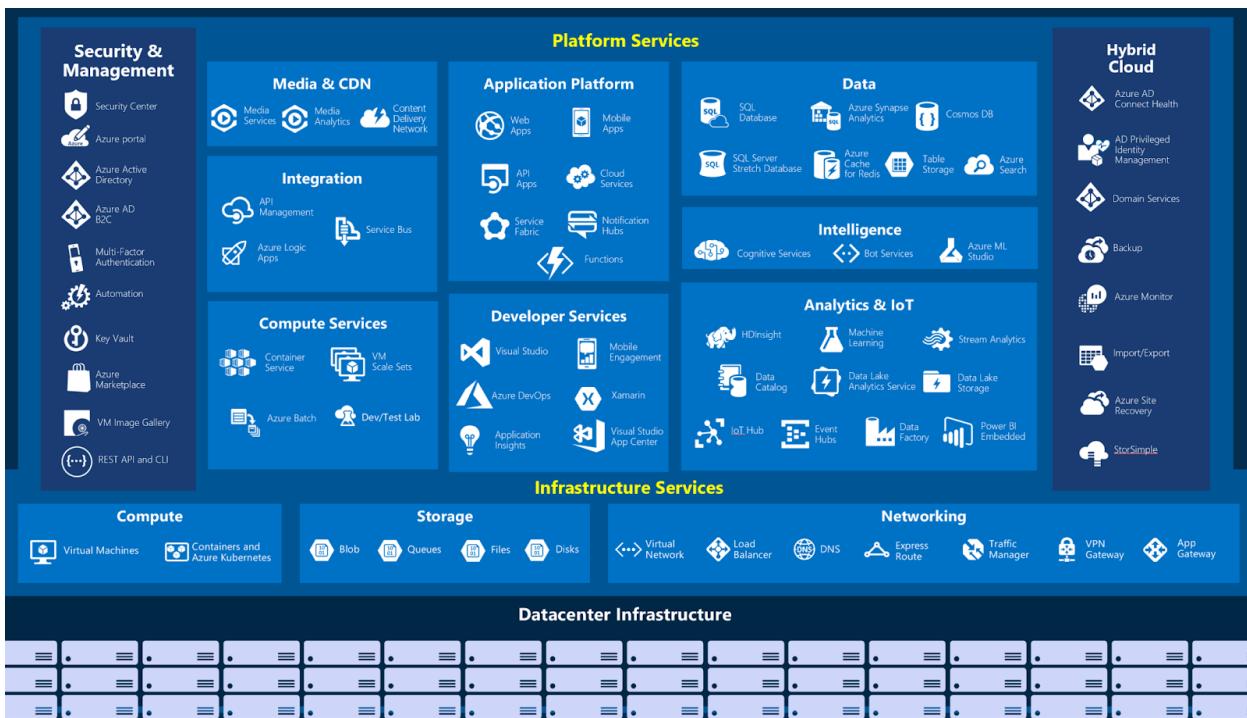
- Describir conceptos de nube
- Describir los servicios básicos de Azure
- Describir las soluciones principales y las herramientas de administración en Azure
- Describir las funciones generales de seguridad y seguridad de la red
- Describir las funciones de identidad, gobernanza, privacidad y cumplimiento
- Describir los acuerdos de nivel de servicio y administración de costos de Azure

Dado el alcance del examen anterior, también debe estar familiarizado con los conceptos de computación, almacenamiento, redes, soporte de aplicaciones y desarrollo de aplicaciones. Esta guía tiene como objetivo ayudarlo a aprobar su examen en su primer intento.

### Materiales de estudio

Los materiales de estudio principales que puede usar para su revisión son: Ruta de aprendizaje de Azure Fundamentals, Documentación de Azure , Tutoriales Dojo's Azure Cheat Sheets y nuestros exámenes de práctica AZ-900.

Tener una cuenta de Azure lo ayudará a comprender mejor los conceptos escritos en la documentación, ya que el examen en sí contiene diferentes tipos de preguntas (opción múltiple, declaración, arrastrar y soltar, hotspot y menú desplegable) para evaluar sus conocimientos sobre estos servicios.



Puede encontrar detalles adicionales sobre su examen AZ-900 en este [Esquema de habilidades del examen de Azure](#).

Para obtener más información sobre cada uno de los dominios del examen AZ-900, puede tomar estos materiales de capacitación gratuitos del sitio de Microsoft:

1. [Explore los conceptos de la nube de Microsoft Azure: aprenda y comprenda los fundamentos de la plataforma Azure.](#)
2. [Distinguir los servicios principales de Microsoft Azure: explore los productos, las soluciones y las diferentes herramientas de administración principales disponibles en Azure.](#)
3. [Examine la seguridad, la privacidad, el cumplimiento y la confianza de Microsoft Azure: estude los conceptos básicos de cómo puede proteger la conectividad de su red, la diferencia entre autenticación y autorización y varias herramientas de seguridad para proteger su cuenta.](#)
4. [Revise los precios, los acuerdos de nivel de servicio y los ciclos de vida de Microsoft Azure: explore los factores que afectan su costo al usar los servicios de Azure.](#)

#### Servicios de Azure en los que centrarse

Azure ofrece una amplia documentación y varias rutas de aprendizaje para todos sus servicios. Conocer los conceptos básicos y los servicios de Azure lo ayudará a aprobar fácilmente el examen AZ-900, que puede allanar el camino hacia una carrera gratificante en la computación en la nube. Le sugiero que lea las Hojas de trucos de Azure de Tutorials Dojo, que proporcionan resúmenes de viñetas de los conceptos más importantes sobre los diferentes servicios de Azure.



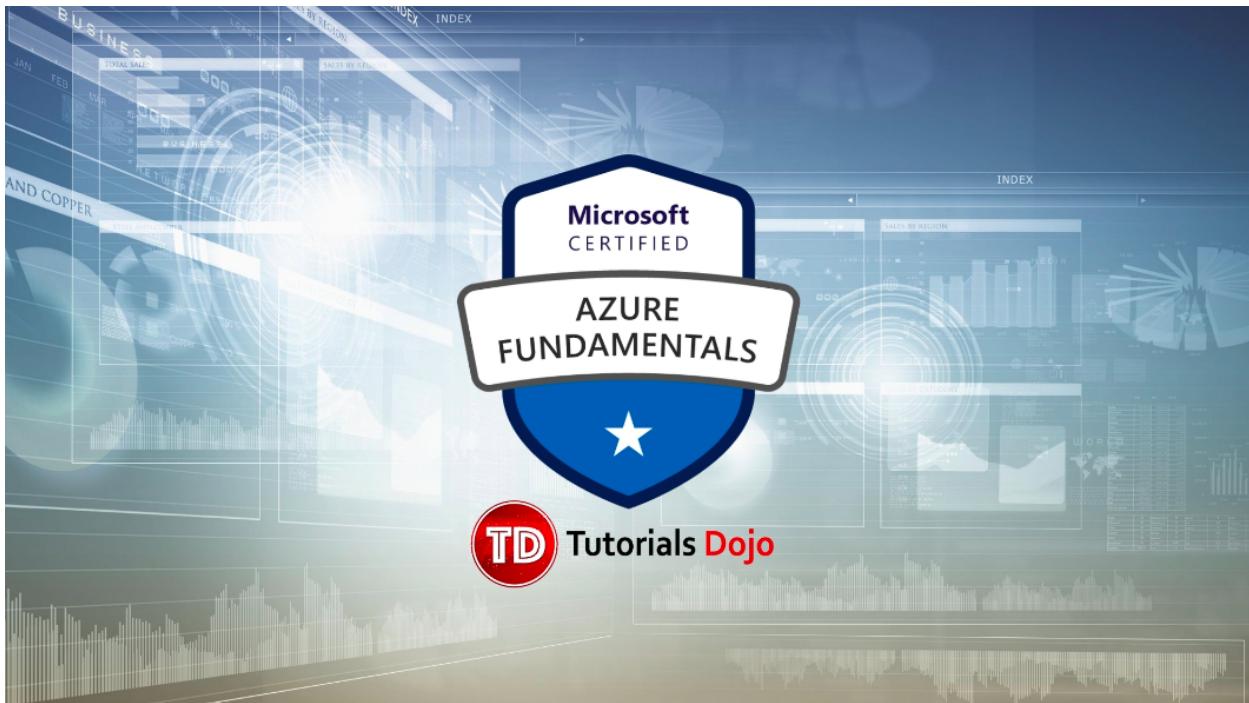
Conceptos en los que debe centrarse:

1. Conceptos de la nube: debe poder comprender los diversos conceptos de la computación en la nube, como los beneficios, las economías de escala, los modelos de implementación y los tipos de servicios en la nube.
2. Calcular - Estudiar los diferentes tipos de servicios informáticos y sus casos de uso.
3. Almacenamiento - Azure ofrece muchos tipos de servicios de almacenamiento, según sus necesidades. Comprenda qué son estos tipos y en qué se diferencian entre sí.
4. Red - Este es el bloque de construcción fundamental para lanzar sus recursos. Estudie los diferentes tipos de servicios de redes y las características que admite cada uno de ellos.
5. Seguridad - Comprenda cómo puede proteger su cuenta en Azure. También necesita conocer los distintos servicios de seguridad que puede utilizar en diferentes escenarios.

Aparte de estos, debe conocer las diferencias entre Azure Portal , CLI , Potencia Shell y Cloud Shell. También es importante familiarizarse con la interfaz del portal, ya que hay preguntas que muestran una imagen del portal y le piden que seleccione la respuesta que coincide con la imagen.

## Valide su conocimiento

Después de revisar los materiales de capacitación y lectura que brindamos anteriormente, recomendamos tomar un examen de práctica primero antes de reservar su examen AZ-900. Tutoriales Dojo ofrece un conjunto de primera Pruebas de práctica AZ-900 Microsoft Azure Fundamentals . En combinación con nuestras hojas de referencia y esta guía de estudio, estamos seguros de que le ayudarán a aprobar el examen.



Ejemplos de preguntas del examen de práctica

### Pregunta 1

Una empresa planea implementar su conjunto de aplicaciones empresariales en Microsoft Azure, donde cada aplicación tiene varias dependencias y subcomponentes. La empresa también debe controlar y administrar las actividades de parcheo del sistema operativo subyacente de los servidores.

¿Qué tipo de solución de implementación en la nube debería recomendar?

1. Infraestructura como servicio (IaaS)
2. Plataforma como servicio (PaaS)
3. Software como servicio (SaaS)
4. Funciones como servicio (FaaS)

Respuesta correcta: 1

**Infraestructura como servicio (IaaS)** es una infraestructura informática instantánea, aprovisionada y administrada a través de Internet. Es uno de los tipos de servicios en la nube, junto con software como servicio (SaaS), plataforma como servicio (PaaS) y sin servidor.

IaaS se escala rápidamente hacia arriba y hacia abajo con la demanda, lo que le permite pagar solo por lo que usa. Le ayuda a evitar el gasto y la complejidad de comprar y administrar sus propios servidores físicos y otros centros de datos.



infraestructura. Cada recurso se ofrece como un componente de servicio independiente y solo necesita alquilar uno en particular durante el tiempo que lo necesite.

Un proveedor de servicios de computación en la nube, como Azure, administra la infraestructura, mientras usted compra, instala, configura y administra su propio software: sistemas operativos, middleware y aplicaciones.

También puede usar Azure Virtual Machines, que es una infraestructura como servicio (IaaS), para alojar el conjunto de aplicaciones empresariales y administrar las actividades de parcheo del sistema operativo subyacente de los servidores.

Por tanto, la respuesta correcta es: **Infraestructura como servicio (IaaS)**.

**Plataforma como servicio (PaaS)** es incorrecta porque se trata de un tipo de servicio en la nube que le permite concentrarse en desarrollar sus aplicaciones y servicios al permitir que el proveedor de servicios en la nube maneje las tareas administrativas de la infraestructura de la aplicación subyacente. No permite a los clientes controlar y administrar las actividades de parcheo del sistema operativo subyacente de los servidores.

**Software como servicio (SaaS)** es incorrecta porque este tipo de servicio en la nube solo permite a los clientes conectarse y utilizar sus aplicaciones basadas en la nube a través de Internet, y no implementar sus aplicaciones personalizadas. Al igual que PaaS, no permite a los clientes controlar y administrar las actividades de parcheo del sistema operativo subyacente de los servidores que utiliza.

**Función como servicio (FaaS)** es incorrecta porque se trata simplemente de una plataforma informática sin servidor impulsada por eventos. Los servidores subyacentes están abstractos y no son accesibles para el usuario final.

#### Referencias:

<https://azure.microsoft.com/en-au/overview/what-is-iaas>  
<https://azure.microsoft.com/en-au/overview/what-is-azure/iaas/#overview>  
<https://docs.microsoft.com/en-us/learn/modules/principles-cloud-computing/5-types-of-cloud-services ht>  
<https://docs.microsoft.com/en-us/azure/security/fundamentals/paas-deployments>

#### Pregunta 2

¿Cuál de las siguientes es una solución de seguridad basada en la nube que aprovecha las señales de Active Directory locales para identificar, detectar e investigar amenazas avanzadas, identidades comprometidas y acciones internas maliciosas dirigidas a su organización?

1. Azure AD Connect Health
2. Azure Advanced Threat Protection (ATP)
3. Protección de la información de Azure
4. Estado del servicio de Azure

Respuesta correcta: 2



---

**Protección contra amenazas avanzada de Azure (ATP)** es una solución de seguridad basada en la nube que aprovecha las señales de Active Directory locales para identificar, detectar e investigar amenazas avanzadas, identidades comprometidas y acciones internas maliciosas dirigidas a su organización.

Azure ATP permite a los analistas de SecOp y a los profesionales de seguridad que luchan por detectar ataques avanzados en entornos híbridos:

- Supervise a los usuarios, el comportamiento de la entidad y las actividades con análisis basados en el aprendizaje
- Proteja las identidades y credenciales de los usuarios almacenadas en Active Directory
- Identifique e investigue las actividades sospechosas de los usuarios y los ataques avanzados a lo largo de la cadena de eliminación
- Proporcione información clara sobre incidentes en un cronograma simple para una clasificación rápida

Azure ATP supervisa y analiza la información y las actividades de los usuarios en su red, como los permisos y la pertenencia a grupos, creando una línea de base de comportamiento para cada usuario. Luego, Azure ATP identifica anomalías con inteligencia incorporada adaptativa, lo que le brinda información sobre actividades y eventos sospechosos, y revela las amenazas avanzadas, los usuarios comprometidos y las amenazas internas que enfrenta su organización. Los sensores patentados de Azure ATP monitorean los controladores de dominio de la organización, proporcionando una vista completa de todas las actividades de los usuarios desde cada dispositivo.

Azure ATP le proporciona información invaluable sobre las configuraciones de identidad y las mejores prácticas de seguridad sugeridas. A través de informes de seguridad y análisis de perfil de usuario, Azure ATP ayuda a reducir drásticamente la superficie de ataque de su organización, lo que dificulta comprometer las credenciales de usuario y promover un ataque. Las rutas de movimiento lateral visual de Azure ATP lo ayudan a comprender rápidamente exactamente cómo un atacante puede moverse lateralmente dentro de su organización para comprometer cuentas confidenciales y ayuda a prevenir esos riesgos por adelantado. Los informes de seguridad de Azure ATP lo ayudan a identificar usuarios y dispositivos que se autentican mediante contraseñas de texto sin cifrar y brindan información adicional para mejorar la postura y las políticas de seguridad de su organización.

Por tanto, la respuesta correcta es: **Protección contra amenazas avanzada de Azure (ATP)**.

**Salud de Azure AD Connect** es incorrecta porque se trata simplemente de una herramienta de Microsoft diseñada para cumplir y lograr sus objetivos de identidad híbrida, como la sincronización de hash de contraseña, la autenticación de paso a través, la integración de federación, la sincronización y la supervisión del estado. Tampoco aprovecha las señales de Active Directory locales.

**Protección de la información de Azure** es incorrecta porque es solo un servicio que se utiliza principalmente para ayudar a las organizaciones a etiquetar y clasificar sus documentos y correos electrónicos confidenciales.

**Estado del servicio de Azure** es incorrecta porque este servicio solo proporciona orientación y soporte personalizados cuando los problemas en los servicios de Azure afectan sus recursos. Esta no es una solución de seguridad basada en la nube que aproveche su



---

Señales de Active Directory locales para identificar, detectar e investigar amenazas avanzadas, identidades comprometidas y acciones internas maliciosas dirigidas a su organización.

**Referencias:**

<https://docs.microsoft.com/en-us/azure-advanced-threat-protection/what-is-atp>  
<https://docs.microsoft.com/en-us/azure-advanced-threat-protection/atp -arquitectura>

Mira nuestro [Exámenes de práctica de conceptos básicos de Microsoft Azure AZ-900](#) para más preguntas de prueba de práctica con explicaciones detalladas.

Debe descansar un poco antes del día de su examen y revisar las notas que haya escrito. Dado que el examen AZ-900 no se compone de preguntas basadas en escenarios y estudios de casos, el examen en sí debería ser sencillo.



## HOJAS DE TRUCOS AZUR

### DESCRIPCIÓN GENERAL AZURE

#### Conceptos de Azure Cloud

- Terminologías de la nube: **Alta disponibilidad, tolerancia a fallas, recuperación ante desastres, escalabilidad, elasticidad, y Agilidad**

#### Alta disponibilidad

- Si el hardware falla, puede obtener una copia nueva y exacta en muy poco tiempo
- Utilice clústeres (un grupo de máquinas virtuales) para garantizar una alta disponibilidad.

#### Tolerancia a fallos

- La tolerancia a fallas es parte de la resiliencia de la computación en la nube
- **Cero tiempo de inactividad** - si un componente falla, un componente de respaldo toma su lugar

#### Recuperación de desastres

- Planifique la recuperación de sistemas comerciales críticos:
  - **Objetivo de tiempo de recuperación (RTO)** es el tiempo que tarda después de una interrupción en restaurar el proceso empresarial a su nivel de servicio
  - **Objetivo de punto de recuperación (RPO)** es la cantidad aceptable de pérdida de datos medida en el tiempo antes de que ocurra el desastre
- Servicios de respaldo y recuperación ante desastres:
  - **Copia de seguridad de Azure** - simplificar la protección de datos y ahorrar costes
  - **Recuperación del sitio de Azure**: mantenga su negocio en funcionamiento con el servicio de recuperación ante desastres
  - **Almacenamiento de archivos de Azure**: almacenar datos de uso poco frecuente en la nube

#### Escalabilidad

- Puede aumentar o disminuir los recursos y servicios utilizados en un momento determinado, según la demanda o la carga de trabajo.
  - **Escala vertical** - agregar recursos para aumentar la potencia de un servidor existente
  - **Escala horizontal** - agregar más servidores que funcionan juntos como una unidad
- Utilizar **conjuntos de escalas** para escenarios críticos

#### Elasticidad



- Amplíe o reduzca rápidamente los recursos informáticos
- Aprovisiona automáticamente más recursos informáticos para manejar el aumento del tráfico. Una vez que el tráfico comienza a normalizarse, la nube desasigna automáticamente los recursos adicionales para reducir los costos.

#### Agilidad

- La capacidad de diseñar, probar y lanzar aplicaciones de software rápidamente que estimulan el crecimiento empresarial.
- La agilidad de la nube permite a las empresas concentrarse en otras preocupaciones como la seguridad, la supervisión y el análisis, en lugar de aprovisionar y mantener los recursos.

#### Fuentes:

<https://docs.microsoft.com/en-us/learn/modules/principles-cloud-computing/3-bene-fits-of-cloud-computing>

<https://docs.microsoft.com/en-us/azure/virtual-machines/cargas-de-trabajo/sap/sap-arquitectura-alta-disponibilidad-scenarios>

<https://azure.microsoft.com/en-us/solutions/backup-and-disaster-recovery/>



## Azure CapEx frente a OpEx

### Gastos de capital (CapEx)

- Costo inicial en infraestructura física
- Debe planificar sus gastos al inicio de un proyecto o período presupuestario.
- Costos de computación de CapEx:
  - **Costos del servidor** - agrupación de servidores, fuentes de alimentación redundantes y fuentes de alimentación ininterrumpidas
  - **Costos de almacenamiento** - almacenamiento centralizado y almacenamiento tolerante a fallas para aplicaciones críticas.
  - **Costos de red** - cableado, commutadores, puntos de acceso, enruteadores, redes de área amplia y conexiones a Internet.
  - **Costos de respaldo y archivo** - mantenimiento de respaldo y consumibles como cintas.
  - **Costos de recuperación ante desastres y continuidad de la organización**: recuperarse de un desastre y continuar operando utilizando generadores de respaldo.
  - **Costos de infraestructura del centro de datos**: costos de construcción y equipo de construcción.
  - **Personal técnico** - experiencia técnica y mano de obra para instalar, implementar y administrar los sistemas en el centro de datos y en el sitio de recuperación ante desastres.

### Gasto operativo (OpEx)

- Sin costo inicial, pero paga el servicio / producto a medida que lo usa
- OpEx es particularmente atractivo si la demanda fluctúa o se desconoce
- Costos de computación OpEX:
  - **Alquiler de software y funciones personalizadas** - responsabilidad de desaprovisionar los recursos cuando no estén en uso para que pueda minimizar los costos.
  - **Cargos de escala basados en uso / demanda en lugar de hardware o capacidad fijos** - planifique el tráfico de respaldo y el tráfico de recuperación de desastres para determinar el ancho de banda necesario.
  - **Facturación a nivel de usuario u organización**: al utilizar un servicio en la nube dedicado, podría pagar según el uso y el hardware del servidor.

### Fuentes:

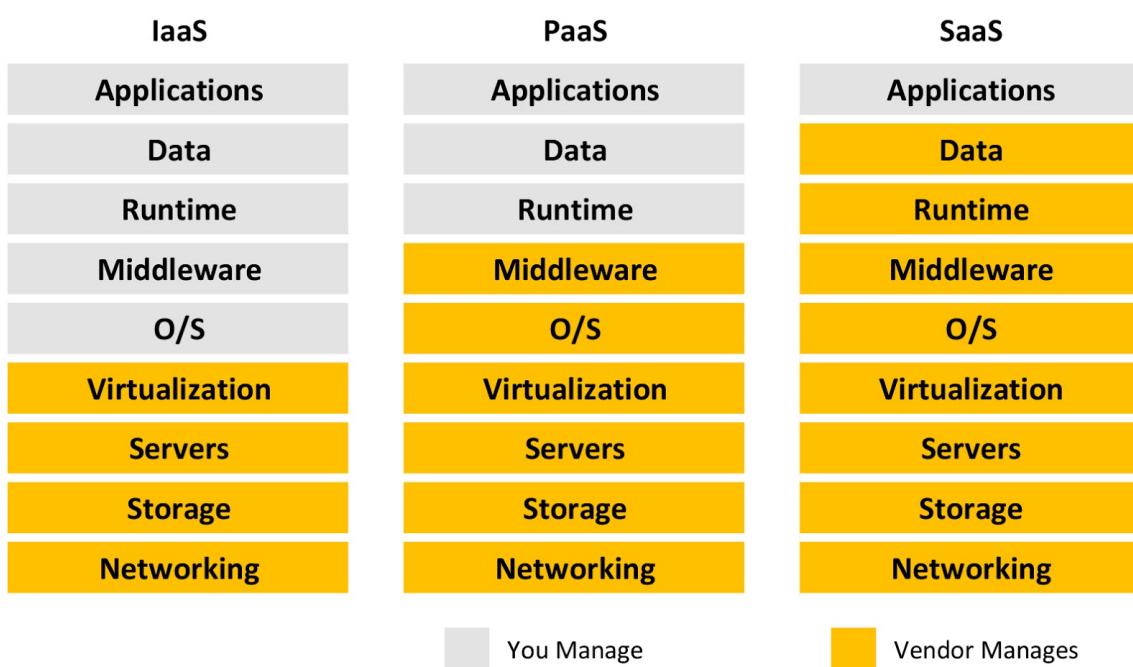
<https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/strategy/business-outcomes/fi-scal-outco>

mes

<https://docs.microsoft.com/en-us/learn/modules/principles-computacion-en-la-nube/3c-capex-vs-opex>

### Modelos de servicios en la nube de Azure

- Los tres modelos de servicios de computación en la nube son **IaaS**, **PaaS**, y **SaaS**.
- También puedes usar **computación sin servidor** para eliminar la necesidad de administrar la infraestructura.
- los **modelo de responsabilidad compartida** determina las tareas de seguridad que maneja el proveedor de la nube y manejado por el cliente.
  - Azure es responsable de proteger la infraestructura, como los hosts, la red y el centro de datos.
  - El cliente es responsable de proteger sus datos, terminales, cuentas y administración de acceso.
- IaaS, PaaS y SaaS tienen diferentes niveles de servicios administrados:



### Infraestructura como servicio (IaaS)

- La mayoría de la gestión de usuarios
- Eres responsable de gestionar el **sistemas operativos, datos, y aplicaciones**.
- IaaS le ayuda a ampliar los recursos rápidamente para cumplir con los picos necesarios para su aplicación.
- Usado en los siguientes escenarios:
  - Migración de cargas de trabajo:** Mueve las aplicaciones existentes a la nube.
  - Prueba y desarrollo** - configurar y desmontar rápidamente entornos de prueba y desarrollo. IaaS permite escalar los entornos de desarrollo y pruebas de forma rápida y económica.
  - Almacenamiento, respaldo y recuperación:** Simplifique la planificación y gestión de los sistemas de copia de seguridad y recuperación.
  - Alojamiento de páginas web** - menos costoso que el alojamiento web tradicional.



- **Computación de alto rendimiento (HPC)** - grupos de computadoras que ayudan a resolver problemas complejos que involucran millones de variables o cálculos.
- **Análisis de big data** - para conjuntos de datos masivos que requieren una gran cantidad de potencia de procesamiento.

#### Plataforma como servicio (PaaS)

- Menos gestión de usuarios
- Los sistemas operativos son administrados por el proveedor de la nube, mientras que el usuario es responsable de las aplicaciones y los datos que ejecuta y almacena.
- PaaS ofrece toda la funcionalidad que necesita para soportar todo el ciclo de vida de las aplicaciones web: **construir, probar la aplicación, implementar el código fuente, administrar, y actualización** dentro del mismo entorno integrado.
- Usado en los siguientes escenarios:
  - **Marco de desarrollo** - un marco para crear o personalizar aplicaciones basadas en la nube.
  - **Analítica o inteligencia empresarial** - encontrar conocimientos y patrones, y predecir resultados para mejorar las decisiones comerciales.

#### Software como servicio (SaaS)

- Requiere la menor cantidad de manejo.
- Permite a las organizaciones centrarse en el aspecto empresarial en lugar de gestionar la infraestructura, la seguridad y la aplicación.

Cloud Type	IaaS	PaaS	SaaS
Examples	Azure Virtual Machines	 Azure Storage  Azure SQL Databases  Azure App Service	 Office 365  Dynamics CRM Online  Skype



Tutorials Dojo	IaaS	PaaS	SaaS
Costs	No upfront costs. Users pay only for what they consume.	No upfront costs. Users pay only for what they consume.	No upfront costs. Users pay a subscription, typically on a monthly or annual basis.
User Responsibility	Purchase, installation, configuration, and management of their own software, operating systems, middleware, and applications.	Custom development of their own applications. Allows the user to focus on the application or workload they want to run. Not responsible for managing the underlying server or infrastructure.	Users just use the application software Not responsible for any maintenance or management of the underlying software.
Cloud Provider Responsibility	Ensures that the underlying cloud infrastructure (such as virtual machines, virtualization, storage, and networking) is available for the user.	Operating system management, network, and service configuration. Typically responsible for everything apart from the application that a user wants to run. Provide the user a complete managed platform on which to run the application.	Provision, management, and maintenance of the application software.
Examples	Azure Virtual Machines	Azure Storage Azure SQL Databases Azure App Service	Office 365, Skype, and Dynamics CRM Online

Tutorials Dojo

Tutorials Dojo

## Computación sin servidor

- Función como servicio (FaaS)
- Simplemente implementa el código con una plataforma sin servidor y se ejecuta con alta disponibilidad.
- Escala hacia arriba y hacia abajo dinámicamente para satisfacer las demandas de cada carga de trabajo en segundos.
- UN modelo de pago por ejecución que cobra una facturación por debajo del segundo solo por el tiempo y los recursos necesarios para ejecutar el código.

### Notas del examen AZ-900:

Es importante que comprenda la seguridad en la nube. Microsoft Azure proporciona un modelo de responsabilidad compartida que lo ayudará a comprender las responsabilidades del proveedor de la nube y del cliente. Las responsabilidades varían según el modelo de servicio en la nube.

### Fuentes:

- <https://docs.microsoft.com/en-us/learn/modules/principles-cloud-computing/5-types-of-cloud-services>
- <https://azure.microsoft.com/en-us/overview/what-is-iaas/>
- <https://azure.microsoft.com/en-us/overview/what-is-paas/>
- <https://azure.microsoft.com/en-us/overview/what-is-saas/>



<https://azure.microsoft.com/en-us/overview/serverless-computing/>



## Modelos de arquitectura en la nube de Azure

- La computación en la nube es la entrega de servicios a través de Internet que lo ayuda a reducir sus costos operativos, ejecutar su infraestructura de manera eficiente y escalar a medida que cambian los requisitos comerciales.
  - Beneficios de la computación en la nube:
    - Costo: elimina los gastos de capital.
    - Escala global: capacidad de escalar elásticamente.
    - Rendimiento: el hardware informático siempre se actualiza a la última generación.
    - Seguridad: los datos almacenados en la nube tienen un amplio conjunto de políticas, tecnologías y controles.
    - Velocidad: los recursos informáticos se pueden aprovisionar en minutos.
    - Productividad: permite al cliente centrarse en los requisitos comerciales en lugar de configurar centros de datos en el sitio.
    - Fiabilidad: disponibilidad de sus recursos en todo momento.
- Tres métodos de implementación de la computación en nube: **Público vs Privado vs Híbrido**.
- El modelo que elija para la implementación en la nube depende de su presupuesto, seguridad, escalabilidad y necesidades de mantenimiento.

### Nube pública

- Concéntrese en mantener sus aplicaciones sin tener que preocuparse por comprar, administrar o mantener el hardware en el que se ejecuta.
- Puede utilizar varios proveedores de nube pública de diferente escala.

Ventajas	Desventajas
Alta escalabilidad / agilidad	Requisitos de seguridad específicos
Precios de pago por uso	Políticas gubernamentales, industria estándares o requisitos legales
No es responsable de las actualizaciones y el mantenimiento del hardware.	No eres el propietario del hardware o los servicios y tampoco puedes administrarlos como quieras.
El conocimiento técnico requerido es mínimo.	Mantener una aplicación heredada puede ser difícil de cumplir

### Nube privada

- Un centro de datos local dedicado configurado para ser un entorno de nube que proporciona a los usuarios de su organización acceso de autoservicio a los recursos informáticos.
- El dolor de cabeza de mantener sus servicios de hardware y software está en sus manos.
- Puede usar una nube privada cuando una organización tiene datos que no se pueden poner en la nube pública, quizás por razones legales.



Ventajas	Desventajas
Se admite cualquier escenario o configuración de aplicaciones heredadas.	CapEx involucrado - el costo principal es la adquisición del equipo.
Tienes control (y responsabilidad) sobre la seguridad	Para escalar, debe comprar, instalar y configurar nuevo hardware
Requisitos de cumplimiento o seguridad en su organización	Las nubes privadas requieren conocimientos y experiencia en TI

#### Nube híbrida

- Le permite mover datos y aplicaciones entre **privado y público** nubes.
- Cuando hay un aumento en la demanda en su nube privada, puede "irrumpir" a la nube pública para obtener recursos informáticos adicionales.

Ventajas	Desventajas
Mantener una infraestructura privada para activos sensibles.	Más caro que seleccionar un modelo de implementación, ya que implica algún costo de inversión por adelantado
Aproveche los recursos de la nube pública cuando sea necesario.	Puede ser más complicado de configurar y administrar
Con la capacidad de escalar a la nube pública, paga por potencia de cómputo adicional solo cuando es necesario.	
Le permite usar su propio equipo para cumplir con los requisitos de seguridad y cumplimiento en su organización.	

#### Fuentes:

<https://azure.microsoft.com/en-us/overview/what-are-private-public-hybrid-clouds/>

<https://docs.microsoft.com/en-us/learn/modules/principles-cloud-computing/4-cloud-deployment-models>



## Infraestructura global de Azure

### Regiones

- Cada región tiene más de un centro de datos, que es una ubicación física.
- Un grupo de centros de datos implementados en un perímetro de latencia definida y conectados a través de una red regional dedicada de baja latencia.
- Criterios para elegir una Región:
  - **Ubicación** - una región más cercana a sus usuarios minimiza la latencia
  - **Características** - algunas características **no están disponibles** en todas las regiones
  - **Precio** - el precio de los servicios varía de una región a otra. Cada región está emparejada dentro de la misma área geográfica. Si la región principal tiene una interrupción, puede **failover** a la región secundaria
- Puede utilizar regiones emparejadas para **replicación**
- 
- Regiones que son únicas en lo que respecta al cumplimiento:
  - **Nube de gobierno de Azure** - solo los gobiernos federales, estatales, locales y tribales de EE. UU. y sus socios tienen acceso a esta instancia dedicada
  - **Región de China** - el centro de datos está ubicado físicamente dentro de China y no tiene conexión fuera de China, incluidas otras regiones de Azure

### Zonas de disponibilidad

- Cada zona de disponibilidad es una ubicación física dentro de una región
- Una zona se compone de uno o más centros de datos con instalaciones independientes de alimentación, refrigeración y redes.
- Los servicios de Azure que admiten zonas de disponibilidad se dividen en dos categorías:
  - **Servicios zonales** - un recurso está anclado a una zona específica
  - **Servicios con redundancia de zona** - se replica automáticamente en todas las zonas

#### Notas del examen AZ-900:

Tenga en cuenta que cada zona de disponibilidad está aislada o separada físicamente. Para proteger sus servicios de puntos únicos de falla, debe replicar sus aplicaciones y datos en más de una zona de disponibilidad.

### Grupos de recursos

- Un contenedor que contiene recursos relacionados
- Cada recurso solo puede existir en un **grupo de recursos único**
- Puede agregar o quitar recursos a cualquier grupo de recursos en cualquier momento
- Le permite mover un recurso de un grupo de recursos a otro
- Los recursos de varias regiones pueden estar en un grupo de recursos
- Puede dar acceso a los usuarios a un grupo de recursos
- Los recursos pueden interactuar con otros recursos en diferentes grupos de recursos
- Un grupo de recursos tiene una ubicación o región, ya que almacena metadatos sobre los recursos.



**Azur Administrador de recursos (ARM)**

- Una capa de administración que le permite crear, actualizar y eliminar recursos dentro de su cuenta. Puede implementar, administrar y monitorear recursos como grupo
- **Plantilla de administrador de recursos** se utiliza principalmente para distribuir los recursos de forma coherente y repetida. Defina las dependencias entre los recursos para que se implementen en el orden correcto. Etiquete recursos para organizar de forma lógica todos los recursos de su suscripción.
- Puede verificar los costos de un grupo de recursos que comparten la misma etiqueta.

**Azur Recuperación del sitio**

- Recuperación ante desastres de Azure como servicio (DRaaS)
- Puede minimizar los problemas de recuperación secuenciando el orden de las aplicaciones de varios niveles que se ejecutan en varias máquinas virtuales.
- Mantenga las aplicaciones disponibles de forma local a Azure o Azure a otra región de Azure durante las interrupciones con la recuperación automática.

**Fuentes:**

<https://docs.microsoft.com/en-us/learn/modules/explore-azure-infrastructure/>  
<https://docs.microsoft.com/en-us/azure/availability-zones/az-overview> <https://azure.microsoft.com/en-us/global-infrastructure/government/>  
<https://docs.microsoft.com/en-us/azure/china/overview-operations>  
<https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/overview>  
<https://azure.microsoft.com/en-us/services/site-recovery/>



## Herramientas de usuario de Azure

- Administre sus recursos de Azure a través de; **Portal, CLI, Powershell, y Cloudshell**

### Azur Portal

- Cree, gestione y supervise todos los recursos en una sola consola, desde aplicaciones web sencillas hasta aplicaciones complejas en la nube.
- Características del portal:
  - **Personalizar** - cree sus propios paneles, diseños, flujos de trabajo y colores
  - **Control de acceso** - control de acceso de grano fino a todos sus recursos
  - **Manejo de costos** - realizar un seguimiento de los costos actuales y proyectados
  - **Multiplataforma** - disponible a través de dispositivos web y móviles
  - **Mercado** - una tienda en línea que consta de miles de ofertas de productos integradas, como:
    - Imágenes de máquina virtual
    - Aplicaciones administradas
    - Soluciones de software como servicio
    - Servicios de consultoría y gestionados

#### Notas del examen AZ-900:

Le recomendamos que explore el Portal de Azure. Definir cada servicio solo en las hojas de trucos no le ayudará a comprender cómo utilizar el portal para configurar sus servicios. Simulándolo usted mismo, podrá recordar y comprender las diferentes configuraciones del portal.

### Azur CLI

- La interfaz de línea de comandos (CLI) funciona en Windows, Mac y Linux Puede crear y administrar recursos
- de Azure con un conjunto de comandos Está diseñado para que pueda trabajar con Azure rápidamente, con
- especial atención **automatización**.

### Azur Potencia Shell

- Totalmente compatible con Azure con módulos y **cmdlets**
  - **cmdlet** es un comando ligero, que se usa en PowerShell. PowerShell proporciona potentes funciones
  - para la automatización. PowerShell también utiliza **Administrador de recursos de Azure** manipular los recursos
- de Azure

### Azur Cloud Shell

- Un interactivo **shell accesible mediante navegador** para administrar los recursos de Azure. Puedes elegir
- entre **Intento o Potencia Shell**
- Acceso al shell desde cualquier lugar mediante la aplicación web o móvil que adjunta Cloud Shell **Archivos**
- de Azure compartir para conservar sus datos



- También ofrece un integrado **editor de archivos** construido sobre el editor Monaco de código abierto

	Windows	Linux	macOS
Azure CLI	✓	✓	✓
Azure Portal (via web browser)	✓	✓	✓
Azure PowerShell	✓	✓	✓
Azure Cloud Shell (via web browser)	✓	✓	✓

Tutorials Dojo

#### Aplicación móvil de Azure

- Puede supervisar el estado y la salud de sus recursos de Azure
- Supervise sus métricas y alertas y tome las acciones necesarias para solucionar problemas comunes.
- Puede ejecutar comandos a través de la CLI de Azure o PowerShell para administrar sus recursos de Azure.

#### Fuentes:

<https://azure.microsoft.com/en-us/features/azure-portal/>  
<https://docs.microsoft.com/en-us/cli/azure/>  
<https://docs.microsoft.com/en-us/powershell/azure/>  
<https://docs.microsoft.com/en-us/azure/cloud-shell/overview>



## PRECIOS AZUR

- Azure ofrece instancias reservadas y de pago por uso para los precios. Factores de precios de Azure:
  - Tamaño y tipo de recurso.
  - Las diferentes ubicaciones de Azure tienen diferentes precios de servicios.
  - El ancho de banda de sus servicios.
  - Se cobra cualquier transferencia de datos entre dos zonas de facturación diferentes.
    - **Ingreso (datos en)** = gratis
    - **Salida (salida de datos)** = cobrado en función de los datos que salen de los centros de datos de Azure
- Factores que pueden reducir costos:
  - Comprando un **instancia reservada** términos de uno o tres años), puede reducir significativamente los costos hasta en un 72 por ciento en comparación con los precios de pago por uso.
  - UN **capacidad reservada** es un compromiso por un período de uno o tres años para SQL Database y SQL Managed Instance.
  - **Beneficio híbrido** le permite usar sus licencias de Windows Server y SQL Server habilitadas por Software Assurance en Azure.
  - Si compra una capacidad informática no utilizada, puede obtener grandes descuentos de hasta el 90 por ciento en comparación con los precios de pago por uso. UN **detectar máquina virtual** es para cargas de trabajo que pueden tolerar interrupciones.
- Todos los recursos pertenecen a un **suscripción**.
  - Una cuenta de Azure puede tener varias suscripciones.
  - Organice sus recursos y suscripciones usando **Grupos de administración de Azure. Gestión de costes de Azure** le brinda una vista detallada de los costos actuales y proyectados. Para cuentas nuevas, el **Nivel gratuito de Azure** está disponible.
    - La capa gratuita ofrece un uso limitado de los productos de Azure sin cargo durante 12 meses.
    - También obtiene un crédito de \$ 200 que puede gastar durante los primeros 30 días.
    - Más detalles en <https://azure.microsoft.com/en-us/free/>

### Notas del examen AZ-900:

En los primeros 30 días de una cuenta gratuita de Azure, todos los recursos que usa se deducen del crédito de \$ 200. Después de 30 días, deberá actualizar a una suscripción de pago por uso para que pueda seguir teniendo acceso a todos los productos gratuitos de la cuenta gratuita.

- Calcule sus costos mensuales esperados usando **Calculadora de precios de Azure**.
- **Calculadora de costo total de propiedad (TCO)**
  - Calcule el ahorro total durante un período de tiempo mediante Azure.
  - Compara costos y ahorros con los entornos locales y de ubicación conjunta.



- Azur Planes de soporte:
  - **Básico** - incluido para todos los clientes de Azure.
  - **Desarrollador** - recomendado para entornos de no producción. Acceso limitado al soporte técnico durante el horario comercial solo por correo electrónico.
  - **Estándar** - apropiado para entornos de carga de trabajo de producción. Tiene acceso 24 horas al día, 7 días a la semana, a los ingenieros de soporte técnico de Azure por teléfono o correo electrónico.
  - **Profesional Directo** - adecuado para cargas de trabajo críticas para la empresa. Tiene acceso 24 horas al día, 7 días a la semana, a los ingenieros de soporte técnico de Azure por teléfono o correo electrónico. Proporciona acceso al soporte de operaciones, los administradores de entrega de ProDirect y las API de soporte.

	BASIC	DEVELOPER	STANDARD	PROFESSIONAL DIRECT
Scope	Included for all Azure customers	Trial and non-production environments	Production workload environments	Business-critical dependence
Billing and subscription management support	✓	✓	✓	✓
24/7 self-help resources, including Microsoft Learn, Azure portal how-to videos, documentation, and community support	✓	✓	✓	✓
Ability to submit as many support tickets as you need	✓	✓	✓	✓
Azure Advisor—your free, personalized guide to Azure best practices	✓	✓	✓	✓
Azure health status and notifications	✓	✓	✓	✓
Third-party software support with interoperability and configuration guidance and troubleshooting		✓	✓	✓
24/7 access to technical support by email and phone		Available during business hours by email only.	✓	✓
Case severity and response time		Minimal business impact (Sev C): Within eight business hours <sup>1</sup>	Minimal business impact (Sev C): Within eight business hours <sup>1</sup> Moderate business impact (Sev B): Within four hours Critical business impact (Sev A): Within one hour	Minimal business impact (Sev C): Within four business hours <sup>1</sup> Moderate business impact (Sev B): Within two hours Critical business impact (Sev A): Within one hour
Architecture Support		General guidance	General guidance	Guidance from a pool of ProDirect delivery managers
Tutoriales Dojo				A single view to managing your active support tickets
Operations Support				Service reviews and advisory consultation from a pool of ProDirect delivery managers
Training				Webinars led by Azure engineers
Proactive Guidance				From a pool of ProDirect delivery managers

<sup>1</sup> For most countries and regions, business hours are from 9:00 AM to 5:00 PM (local time) Monday through Friday, excluding holidays. For North America, business hours are from 6:00 AM to 6:00 PM (Pacific time), Monday through Friday, excluding holidays. In Japan, business hours are from 9:00 AM to 5:30 PM, Monday through Friday, excluding holidays.



#### Acuerdo de nivel de servicio (SLA)

- Es el compromiso de Microsoft por el tiempo de actividad y la conectividad de un servicio.
- Puede obtener un crédito de servicio si Microsoft no cumple con el acuerdo de nivel de servicio.
- Los SLA compuestos incluyen varios recursos (*con diferentes niveles de disponibilidad*) para apoyar una aplicación.
- Los SLA para implementaciones multirregionales distribuyen la aplicación en más de una región para lograr alta disponibilidad y usan Azure Traffic Manager para la conmutación por error si falla una región.

#### Notas del examen AZ-900:

Tenga en cuenta que Azure ofrece diferentes SLA para cada servicio. Para calcular el SLA compuesto total de una aplicación, tendría que multiplicar el SLA de cada servicio.

Por ejemplo,

- Aplicaciones web de App Service (SLA) = 99,95%
- Base de datos SQL (SLA) = 99,99%

El SLA compuesto es  $99,95\% \times 99,99\% = 99,94\%$ . Podríamos ver que el SLA es más bajo que los SLA individuales ya que varios servicios tienen más puntos de falla potenciales.

Durante su examen, puede usar el botón de la calculadora si necesita calcular el SLA compuesto.

#### Ciclo de vida del servicio

- **Vista previa privada** solo está disponible para algunos clientes para el acceso temprano a nuevas tecnologías y funciones.
- **Vista previa pública** realiza el servicio en la fase pública y puede ser utilizado por cualquier cliente para evaluar las nuevas funciones, pero el SLA no se aplica.
- **Disponibilidad general** es el lanzamiento del servicio al público en general y está totalmente respaldado por SLA. Las actualizaciones de Azure le permiten obtener las últimas actualizaciones de cualquier producto y característica de Azure.



	Private Preview	Public Preview	General Availability
Access	Subset of Azure customers <i>(By Invitation)</i>	All Azure customers	All Azure customers
Subject to Service Level Agreement (SLA)	No	No	Yes
Covered by Microsoft Customer Support Services	No	Yes	Yes

Tutorials Dojo

**Fuentes:**

<https://azure.microsoft.com/en-us/pricing/>

<https://docs.microsoft.com/en-us/azure/cost-management-billing/cost-management-billing-overview>

<https://docs.microsoft.com/en-us/azure/architecture/framework/resiliency / business-metrics>

<https://azure.microsoft.com/en-us/support/legal/preview-supplemental-terms/>



## CALCULAR

### Máquinas virtuales de Azure

- Máquinas virtuales basadas en Linux y Windows.

#### Características

- Entornos de servidor llamados **maquinas virtuales**.
- Un sistema operativo de paquete e instalaciones adicionales en una plantilla reutilizable se denominan **Imágenes de VM**.
- Admite varias con configuraciones de CPU, memoria, almacenamiento y capacidad de red para sus máquinas virtuales, conocidas como **serie de máquinas virtuales**.
  - Series A, Bs, D y DC para uso general
  - Serie F para computación optimizada
  - Serie E y M para memoria optimizada
  - Serie Ls para almacenamiento optimizado
  - Serie G para memoria y almacenamiento optimizados
  - Serie H para informática de alto rendimiento
  - Serie N para GPU optimizada
- Contener las máquinas virtuales mediante un **grupo de recursos**.
- Asegure la información de inicio de sesión para sus máquinas virtuales usando **pares de claves**.
- Volúmenes de almacenamiento persistentes para sus datos usando **Disco Azure**.
- Varias ubicaciones físicas para implementar sus recursos, como máquinas virtuales y disco Azure, conocidas como **Regiones y Zonas de disponibilidad**.
- Puede replicar sus datos en zonas de disponibilidad o conjuntos de disponibilidad.
- Las máquinas virtuales de Azure tienen un disco de sistema operativo y un disco temporal para almacenamiento a corto plazo. Metadatos, conocidos como **etiquetas**, que puede crear y asignar a sus recursos de VM.
- Las redes virtuales que puede crear están lógicamente aisladas del resto del entorno de Azure y, opcionalmente, pueden conectarse a su propia red, conocida como **Red virtual de Azure o VNet**.
- Agregue un script que se ejecutará en la máquina virtual mientras se aprovisiona llamado **datos personalizados**.
- Un firewall le permite especificar los protocolos, puertos y rangos de IP de origen que pueden llegar a sus máquinas virtuales usando **grupos de seguridad de red**.

#### Estado de VM

- **Comienzo** - ejecute sus máquinas virtuales. Se le factura continuamente mientras su máquina virtual está en funcionamiento.
- **Reanudar** - algunas actualizaciones requieren un reinicio. En estos casos, las máquinas virtuales se apagaran mientras Azure aplica parches a la infraestructura y luego se reiniciarán.
- **Detener** - es solo un apagado normal. Si la máquina virtual se encuentra en un estado desasignado, se le seguirá cobrando por el almacenamiento necesario para el disco del sistema operativo.
- También puede eliminar directamente las máquinas / recursos virtuales. Eliminar las máquinas virtuales seleccionadas es irreversible.



VM STATE	BILLED	DETAILS
Starting	Yes	The initial starting state of virtual machines as they're going through the boot cycle. This period is billed as the virtual machines are running.
Running (Started)	Yes	The running state of the virtual machine.
Stopped	Yes	You are billed for allocated cores, but not software licences.
Deleted (Deallocated)	No	Cores are no longer allocated to the virtual machine, and are no longer billed.

Tutorials Dojo

#### Discos

- Seleccione un tipo de disco de sistema operativo con HDD estándar, SSD estándar y SSD premium. Cada máquina virtual
- tiene un disco de sistema operativo adjunto. El disco del sistema operativo tiene una capacidad máxima de 2048 GiB.
- 
- Cada máquina virtual contiene un disco temporal que proporciona almacenamiento a corto plazo solo para archivos de página o de intercambio. Los datos del disco
- temporal pueden perderse durante un evento de mantenimiento o cuando vuelve a implementar una VM.
- Puede habilitar la compatibilidad ultra disco para un alto rendimiento, alto IOPS y almacenamiento en disco de baja latencia constante.
- Una máquina virtual con una capacidad de Ultra Disk habilitada resultará en un cargo de reserva incluso sin conectar un Ultra Disk.
- Una zona de disponibilidad admite discos administrados.
- Obtiene una latencia de lectura / escritura más baja en el disco del sistema operativo con el disco del sistema operativo efímero y una nueva imagen más rápida de la máquina virtual. No incurres en ningún costo de almacenamiento con los discos de SO efímeros.

#### Anfitrión dedicado

- Proporcione servidores físicos que puedan albergar varias máquinas virtuales.
- Le permite cumplir con los requisitos normativos y de cumplimiento que requieren que sea el único cliente que utilice el servidor físico que albergará sus máquinas virtuales.
- Tiene el control de los eventos de mantenimiento programados de Azure, donde puede optar por las ventanas de mantenimiento.
- Traiga sus licencias de Windows existentes con Software Assurance para reducir costos.



- UN **Grupo anfitrión** consta de uno o más hosts dedicados.
- Cuando creas un **anfitrión**, se asignará automáticamente a un servidor físico y se creará dentro de un grupo de hosts. Un host puede constar de varias máquinas virtuales.

#### Precios

- Pague sobre la marcha: pague las instancias que utiliza por segundo, sin compromisos a largo plazo ni pagos por adelantado.
- Reservado: realice un pago inicial bajo y único para una instancia, resérvelo por un período de uno o tres años.
- Spot: solicite capacidad informática no utilizada, lo que puede reducir sus costos de manera significativa. Los precios al contado le ofrecen hasta un 90 por ciento en comparación con los precios de pago por uso.

#### Copia de seguridad y recuperación

- Una instantánea es una copia completa del sistema operativo o del disco de datos de una máquina virtual. Las instantáneas son útiles para realizar copias de seguridad, recuperación de desastres y resolución de problemas.
- Con el **copia de seguridad habilitada** opción, se hará una copia de seguridad de su VM en la bóveda de Recovery Services con la política de copia de seguridad predeterminada, o su política de copia de seguridad personalizada y se le cobrará según el precio de la copia de seguridad.
- **Recuperación del sitio de Azure** permite a las organizaciones cumplir con sus requisitos de continuidad empresarial y recuperación ante desastres (BCDR) al hacer que los datos de sus máquinas virtuales se repliquen en una región secundaria y se realicen una comutación por error en caso de un tiempo de inactividad.
- Puede configurar la recuperación ante desastres de máquinas virtuales de Azure desde una región principal a una región secundaria mediante **Recuperación del sitio de Azure**.

#### Conjuntos de escalas

- Cree y administre un grupo de máquinas virtuales con equilibrio de carga para brindar alta disponibilidad a sus aplicaciones.
- Escale automáticamente su aplicación a medida que cambie la demanda.
- Admite hasta 1000 instancias de VM. Pero si crea y carga sus propias imágenes de VM personalizadas, el límite es 600.
- Utilizar **Monitor de Azure** para automatizar la recopilación de información de las máquinas virtuales en su conjunto de básculas.
- Sin costo adicional para escalar conjuntos. Solo paga por los servicios informáticos subyacentes, como máquinas virtuales, equilibradores de carga o almacenamiento en disco administrado.

Guión	Grupo manual de VM	Conjunto de escala de máquina virtual
Agregar VM adicional instancias	Para crear, configurar y asegurar el cumplimiento de el proceso manual.	Cree automáticamente a partir de una configuración central.
Equilibrado del tráfico y distribución	Proceso manual en creando y configurando el Load Balancer o	Crear y integrar Load Balancer o Application Gateway.



	Puerta de enlace de aplicaciones.	
Alta disponibilidad y redundancia	Crear conjunto de disponibilidad o distribuir y realizar un seguimiento máquinas virtuales en Zonas de disponibilidad a mano.	Distribuir máquinas virtuales en zonas de disponibilidad o conjuntos de disponibilidad automáticamente.
Escalado de máquinas virtuales	Monitoreo manual y Automatización de Azure.	Escala automática basada en métricas, Aplicación Insights o por horario.

Scenario	Manual group of VMs	Virtual Machine Scale Set
Add additional VM instances	Manual process to create, configure, and ensure compliance	Automatically create from central configuration
Traffic balancing and distribution	Manual process to create and configure Azure load balancer or Application Gateway	Can automatically create and integrate with Azure load balancer or Application Gateway
High availability and redundancy	Manually create Availability Set or distribute and track VMs across Availability Zones	Automatic distribution of VM instances across Availability Zones or Availability Sets
Scaling of VMs	Manual monitoring and Azure Automation	Autoscale based on host metrics, in-guest metrics, Application Insights, or schedule



	Scale Set	Availability Set
Description	A group of load balanced VMs that can automatically increase or decrease in response to demand or a defined schedule.	A logical grouping of VMs within a datacenter
Virtual Machine Distribution	VMs are automatically distributed across fault domains (FD), update domains (UD) and Availability Zones	VMs are automatically distributed across fault domains (FD) and update domains (UD).
Fault tolerant if a single data center fails	Yes	No
Fault tolerant if the primary Azure region fails	No	No

Tutorials Dojo

## Supervisión

- **Estado de recursos de Azure** le ayuda a diagnosticar problemas que afectan sus recursos.
- Capture la salida de la consola en serie y las capturas de pantalla de la máquina virtual con **diagnóstico de arranque**.
- Habilite los diagnósticos de invitados del sistema operativo para obtener las métricas cada minuto
- Apague automáticamente las máquinas virtuales para una mayor rentabilidad con **habilitar el apagado automático** opción.

## Red

- Puede aprovisionar una máquina virtual que tenga una dirección IP pública estática.
- Habilite la conexión en red acelerada para baja latencia y alto rendimiento en la interfaz de red.
- Distribuya el tráfico entre máquinas virtuales mediante Load Balancer.

## Seguridad

- De forma predeterminada, el acceso a la VM está restringido a fuentes en la misma red virtual.
- Puede controlar puertos, conectividad entrante y saliente con reglas de grupo de seguridad.
- Con la identidad administrada asignada por el sistema, todos los permisos necesarios se pueden otorgar a través del control de acceso basado en roles de Azure.
- Cifre sus datos en reposo con una clave administrada por la plataforma o una clave administrada por el cliente.
- De forma predeterminada, el cifrado en reposo utiliza una clave administrada por plataforma.
- Cifre el sistema operativo y los discos de datos con Azure Disk Encryption.
- El disco temporal no está cifrado mediante cifrado del lado del servidor a menos que habilite el cifrado en el host.



---

**Fuentes:**

<https://docs.microsoft.com/en-us/learn/patterns/azure-fundamentals/>  
<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/overview> <https://azure.microsoft.com/en-us/pricing/details/virtual-machines/series/>  
<https://docs.microsoft.com/en-us/azure/virtual-machine-scale-sets/overview>



## Servicio de aplicaciones de Azure

- Una plataforma totalmente administrada (PaaS) para crear, implementar y escalar sus aplicaciones web. Diferentes tipos de servicios de aplicaciones: **Aplicaciones web, aplicaciones web para contenedores, y Aplicaciones API**
- Parchea y mantiene automáticamente el sistema operativo y los marcos de lenguaje. App Service
- puede ampliarse o expandirse de forma manual o automática. App Service admite los siguientes idiomas:
  - .NET
  - .NET Core
  - Java
  - Rubí
  - Node.js
  - PHP
  - Pitón
- Un **Plan de servicio de aplicaciones** es una colección de recursos informáticos necesarios para que se ejecute una aplicación web. Cada plan de App Service consta de un **región, número y tamaño de máquinas virtuales y nivel de precios**.
- Nivel de precios del plan de App Service:
  - **Computación compartida - Gratis y Compartido** son los dos niveles base. Estos niveles asignan cuotas de CPU a cada aplicación que se ejecuta en los recursos compartidos, pero los recursos no se pueden escalar horizontalmente.
  - **Computación dedicada - Se compone de Básico, Estándar, Premium, y PremiumV2** niveles. A medida que aumenta el nivel, tendrá más máquinas virtuales para escalar.
  - **Aislado** - Una máquina virtual dedicada que proporciona las máximas capacidades de escalamiento horizontal.

### Notas del examen AZ-900:

#### ¿Cuándo usamos Azure App Service frente a otras opciones de proceso?

La ventaja de usar Azure App Service es que es PaaS. Esto significa que solo necesita definir la configuración de su entorno y Azure se encargará de la integración y el aprovisionamiento de servidores por usted. Después de eso, simplemente puede cargar su aplicación y ya tendrá un entorno de trabajo completo. Administrar App Service es muy fácil, ya que no es necesario que comprenda cómo funcionan juntos los diferentes servicios antes de poder iniciar su aplicación.

### Tipos de servicios de aplicaciones:

- **Aplicaciones web**
  - Sitio web y aplicaciones en línea alojadas en la plataforma administrada de Azure.
  - Cree e implemente aplicaciones web de misión crítica que escalen con su negocio.
  - Es compatible con el autoescalamiento y el equilibrio de carga para brindar resistencia y alta disponibilidad.
- **Aplicaciones web para contenedores**
  - Implemente y ejecute aplicaciones en contenedores en Azure.



- Todas las dependencias se envían dentro del contenedor.
- Aplicaciones API
  - Exponga y conecte sus datos de backend.
  - Conecte otras aplicaciones mediante programación.

## Despliegue

- Componentes de implementación en App Service:
  - Fuente de implementación: es donde se almacena el código de la aplicación.
  - Build Pipeline: lee su código y pone la aplicación en un estado de ejecución
  - Mecanismo de implementación: le permite colocar su aplicación en el directorio / wwwroot. También es compatible con puntos finales Kudu, FTP y WebDeploy.
- **Centro de implementación** le permite elegir la ubicación de su código, así como compilar e implementar en la nube. También tiene entrega continua incorporada para contenedores.
- Intercambia contenido de la aplicación y elementos de configuración con **ranuras de despliegue**.
- App Service admite la implementación continua de código y contenedores. Puedes usar **caché local** y ranuras
- de implementación para evitar tiempos de inactividad. Servicio de aplicaciones **diagnósticos** le ayudará a
- solucionar problemas de su aplicación.

## Seguridad

- Protocolos de App Service: HTTPS, TLS 1.1 / 1.2 y FTPS
- El nombre de dominio predeterminado utiliza HTTP. También puede proteger su dominio personalizado mediante un certificado SSL / TLS.
- **Puntos finales de servicio** le permite restringir el acceso desde una red virtual.
- La primera regla de restricción de IP tiene una **Negar todo** regla con una prioridad de 2147483647.
- Autenticación de servicio a servicio:
  - Identidad del servicio: puede usar la identidad de la aplicación para acceder al recurso remoto.
  - En nombre de (OBO): le permite acceder a un servicio remoto mediante un inicio de sesión delegado.

## Integración de VNet

- Permite que su aplicación acceda a recursos en su red virtual.
  - Integración de red virtual regional
    - Necesita tener una subred dedicada a los servicios con los que se integra.
    - Bloquee el tráfico saliente mediante grupos de seguridad de red.
    - La tabla de ruta le permite enviar tráfico saliente. Integración de VNet
  - requerida por la puerta de enlace
    - Permite el acceso a los recursos en la red virtual de destino.
    - **Red de sincronización** le permite sincronizar certificados e información de red.
    - Tú también puedes **agregar rutas** para el tráfico de salida c.



### Conexiones híbridas

- Utiliza la combinación de host: puerto.
- Proporciona acceso de red a su aplicación mediante un punto final TCP.
- Admite el acceso a múltiples redes desde una sola aplicación.
- Aloje su punto final de conexión híbrida con un agente de retransmisión o **Administrador de conexiones híbridas (HCM)**.
- Puede ejecutar varios HCM en una máquina separada para lograr una alta disponibilidad.

### Precios

- Se le cobra por segundo en el plan de App Service.
- Se le cobrará por las aplicaciones mientras están detenidas. Se le cobra por la salida de datos
- cuando usa la integración de VNet. Se le cobra por cada oyente en una conexión híbrida
- 

### Fuentes:

<https://azure.microsoft.com/en-us/services/app-service/>

<https://docs.microsoft.com/en-us/azure/app-service/overview>



## Instancias de contenedor de Azure (ACI)

- Ejecute contenedores sin administrar servidores.
- Para aplicaciones impulsadas por eventos, implemente rápidamente desde sus canales de desarrollo de contenedores, ejecute el procesamiento de datos y cree trabajos.
- Azure Container Instances es un servicio regional.

### Características

- Los contenedores tienen menos gastos generales que las máquinas virtuales y se pueden implementar de forma coherente.
- Todas las dependencias de una aplicación se incluyen en la imagen del contenedor.
- Las aplicaciones que se ejecutan en contenedores se pueden implementar fácilmente en múltiples sistemas operativos y plataformas de hardware.
- Seleccione una fuente de imagen usando **Imágenes de inicio rápido**, **Azure Container Registry**, y **Docker Hub**.
- Cree una imagen de contenedor solo cuando la necesite y procese los datos a pedido.
- Puedes elegir **siempre** reinicie el contenedor independientemente de cómo se detuvo, para reiniciar solo si **ha fallado**, para salir con éxito, o para **Nunca** Reanudar.
- Le permite configurar un comando para que se ejecute primero cuando se ejecuta el contenedor.
- Los recursos se pueden etiquetar con valores que defina, para ayudarlo a organizarlos e identificarlos.
- De forma predeterminada, las instancias de contenedor de Azure no tienen estado.
- No puede implementar una imagen de un registro local en ACI.

### Almacenamiento

- Puede montar recursos compartidos de Azure Files en su ACI para almacenamiento persistente.
- Para montar un recurso compartido de archivos de Azure como volumen en Azure Container Instances, necesita: Nombre de la cuenta de almacenamiento, Nombre del recurso compartido y Clave de la cuenta de almacenamiento.

### Redes

- Elija entre tres opciones de red: pública, privada y ninguna.
- La IP privada aún no está disponible para contenedores de Windows.
- Aún no se puede acceder a ninguno de los contenedores IP (registros) mediante la CLI.
- Etiqueta de nombre DNS: <*tutorialsdojo*>, <*region*>. azurecontainer.io

### Seguridad

- Implemente Azure WAF frente a aplicaciones web críticas alojadas en ACI para una inspección adicional del tráfico entrante.
- Use Azure Key Vault para proteger claves y secretos de cifrado para aplicaciones en contenedores.

### Precios

- Paga según lo que necesita y se le factura por segundo.
- Se facturan las direcciones IP públicas asignadas a su grupo de contenedores.



- 
- Se le factura por cada GB y vCPU que consume su grupo de contenedores.

**Fuentes:**

<https://docs.microsoft.com/en-us/azure/container-instances/container-instances-overview>

<https://azure.microsoft.com/en-us/services/container-instances/#overview>



## Servicio de Azure Kubernetes (AKS)

- Una herramienta de código abierto para orquestar y administrar muchas imágenes y aplicaciones de contenedores.
- Le permite implementar un clúster de Kubernetes administrado en Azure.

### Características

- Utiliza clústeres y pods para escalar e implementar aplicaciones.
- Kubernetes puede implementar más imágenes de contenedores según sea necesario.
- Admite escalado horizontal, autorreparación, equilibrio de carga y administración de secretos.
- Monitoreo automático de la carga de la aplicación para determinar cuándo escalar el número de contenedores utilizados.
- Le permite replicar arquitecturas de contenedores.
- Use Kubernetes con regiones de Azure compatibles e instalaciones locales mediante **Pila de Azure**.
- Las imágenes que usa AKS provienen de Azure Container Registry.
- Utilizar **Asesor de Azure** para optimizar sus implementaciones de Kubernetes con recomendaciones personalizadas en tiempo real.

### Componentes

- UN **plano de control** es un recurso administrado de Azure. Es donde se ejecutan los componentes, incluido el servidor API y la base de datos del clúster (etcd).
  - kube-apiserver: permite la comunicación para herramientas de gestión (kubectl).
  - etcd: un almacén de valores clave dentro de Kubernetes.
  - kube-planificador: define qué nodos deben ejecutarse en la carga de trabajo.
  - kube-controller-manager: supervisa los controladores más pequeños que manejan las operaciones de los nodos y la replicación de los pods.
- Kubernetes ejecuta una aplicación en su instancia usando **vainas**.
- UN **nodo** se compone de varias vainas, y **grupos de nodos** son un grupo de nodos con la misma configuración. Utilizar una **selector de nodo** para controlar dónde se debe colocar una cápsula.
- Puede ejecutar al menos 2 nodos en el grupo de nodos predeterminado para asegurarse de que su clúster funcione de manera confiable. Los pods de varios contenedores se colocan en el mismo nodo y permiten que los contenedores comparten los recursos relacionados. Puede especificar límites máximos de recursos que eviten que un pod determinado consuma demasiados recursos informáticos del nodo subyacente.
- UN **despliegue** determina el número de réplicas (pods) que se crearán, pero primero debe definir un archivo de manifiesto en formato YAML.
- Con **StatefulSets**, puede mantener el estado de la aplicación dentro de un solo ciclo de vida del pod. Los recursos se agrupan lógicamente en un **espacio de nombres**, y un usuario solo puede interactuar con recursos dentro de sus espacios de nombres asignados.

### Almacenamiento

- Los volúmenes persistentes proporcionan el almacenamiento de archivos y discos de Azure.
- Cree un recurso de Kubernetes DataDisk con Azure Disk.



- Monte un recurso compartido de SMB 3.0 respaldado por una cuenta de Azure Storage en pods con Azure Files.
- Los volúmenes que se definen y crean como parte del ciclo de vida del pod solo existen hasta que se elimina el pod. AKS tiene cuatro clases de almacenamiento iniciales:
  - predeterminado: usa el almacenamiento Azure StandardSSD para crear un disco administrado.
  - Managed-premium: usa el almacenamiento de Azure Premium para crear Managed Disk.
  - archivo azure: utiliza el almacenamiento estándar de Azure para crear un recurso compartido de archivos de Azure.
  - azure file-premium: utiliza el almacenamiento de Azure Premium para crear un recurso compartido de archivos de Azure.
- Si no se especifica StorageClass para un volumen persistente, se usa el StorageClass predeterminado.

#### Seguridad

- Con Kubernetes RBAC, puede crear roles para definir permisos y luego asignar esos roles a usuarios con enlaces de roles.
- Puede limitar el tráfico de red entre los pods de su clúster con las políticas de red de Kubernetes.
- Aplicación de reglas dinámicas en varios clústeres con Azure Policy.
- Los clústeres de AKS integrados en Azure AD pueden otorgar a los usuarios o grupos acceso a los recursos de Kubernetes dentro de un espacio de nombres o en todo el clúster.
- Proteja las rutas de comunicación entre espacios de nombres y nodos con Azure Private Link.

#### Precios

- Solo paga por máquinas virtuales, almacenamiento asociado y recursos de red.
- No hay ningún cargo por la gestión de clústeres.

#### Versiones

- Utiliza versiones semánticas: [mayor]. [Menor]. [Parche]
- Un usuario tiene 30 días desde la eliminación de la versión para actualizar a un parche compatible y continuar recibiendo soporte.
- Azure actualiza el clúster automáticamente si ha dejado de ser compatible con más de 3 versiones menores.
- No se admite la degradación de una versión.

#### Fuentes:

<https://docs.microsoft.com/en-us/azure/aks/intro-kubernetes>  
<https://azure.microsoft.com/en-us/services/kubernetes-service/>



## Registro de contenedores de Azure (ACR)

- Un servicio para administrar las imágenes de su contenedor y los artefactos relacionados.
- ACR es un servicio regional.

### Características

- Mantenga un registro de las imágenes de contenedores válidas actuales.
- Los registros (SKU) están disponibles en tres niveles: Básico, Estándar y Premium.
- Puede usar la función de replicación geográfica de los registros Premium para escenarios de distribución de imágenes de contenedor y replicación avanzada.
- Optimice la creación, prueba, envío e implementación de imágenes en Azure con [Tareas de Azure Container Registry](#).
- Soporta ACR Tasks **tarea rápida, tareas activadas automáticamente, y tarea de varios pasos**
- Etiquete sus contenedores con etiquetas estables y únicas.

### Conceptos

- **Registro**
  - Un registro es una colección de repositorios para almacenar y distribuir imágenes de contenedores.
  - Debe estar autenticado antes de poder extraer y enviar imágenes.
- **Artefacto**
  - La dirección de un artefacto contiene loginUrl, repositorio y etiqueta
    - [loginUrl] / [repositorio:] [etiqueta]
- **Repositorio**
  - Un repositorio es un grupo de imágenes de contenedores similares y otros artefactos.
  - Identifique repositorios y artefactos similares con espacios de nombres.
- **Imagen**
  - Las imágenes se utilizan en las tareas de ACR.
  - Una imagen de contenedor consta de etiquetas, capas y un manifiesto.
  - Las imágenes huérfanas se generan presionando repetidamente imágenes modificadas con etiquetas idénticas.

### Mejores prácticas

- Si coloca su registro cerca de los hosts de su contenedor, ayudará a reducir tanto la latencia como los costos.
- Cuando implementa contenedores en varias regiones, puede utilizar la función de replicación geográfica.
- ACR admite espacios de nombres anidados que le permiten compartir un solo registro en varios grupos.
- Hay dos situaciones principales al autenticarse con un ACR:
  - Identidad individual: le permite extraer o enviar imágenes de la máquina de desarrollo.
  - Identidad de servicio / sin cabeza: le permite crear e implementar canalizaciones donde el usuario no está involucrado directamente.
- ACR le permite eliminar imágenes por etiqueta, por resumen de manifiesto y por repositorio.



## Tareas

- **Rápido Tarea**
  - Verifique sus definiciones de compilación automatizadas y detecte problemas potenciales antes de enviar su código.
  - Cree y envíe una única imagen de contenedor a un registro de contenedor a pedido, en Azure, sin necesidad de una instalación local de Docker Engine.
- **Tarea de activación**
  - Puede crear una imagen utilizando uno o más activadores en:
    - Actualización del código fuente
    - Actualización de la imagen base
    - Calendario
- **Tarea de varios pasos**
  - Flujos de trabajo basados en contenedores múltiples
  - Con las tareas de varios pasos en ACR Tasks, tiene un control más granular sobre la creación de imágenes, las pruebas. Los recursos de registro eliminados, y flujos de trabajo de parches de sistemas operativos y marcos.
- como los repositorios, las imágenes y las etiquetas, no se pueden recuperar después de la eliminación.

## Etiquetado

- Utilice etiquetas estables para mantener imágenes base para sus compilaciones de contenedores.
- Si la imagen actualizada tiene una etiqueta estable, la imagen etiquetada previamente no está etiquetada, lo que da como resultado una imagen huérfana.
- Puede usar etiquetas únicas para implementaciones, particularmente en un entorno donde varios nodos pueden escalar.

## Red

- Puede conectarse a su ACR a través de puntos finales públicos y privados.
- Una conexión de punto final privada solo está disponible para Premium SKU.

## Seguridad

- Cifra el contenido del registro en reposo con claves administradas por el servicio o claves administradas por el cliente.
- La clave administrada por el cliente solo está disponible para el SKU Premium.
- Puede habilitar una clave administrada por el cliente solo cuando crea un registro.
- Autenticar a través de **Azure Active Directory** usuario, entidad de servicio, inicio de sesión de administrador o mediante la identidad administrada de Azure.

## Precios

- Se le cobrará (GiB / día) por el almacenamiento de imágenes.
- A los usuarios se les cobrará el precio de SKU anterior hasta el momento del cambio y se les cobrará el precio de SKU nuevo después de que se haya realizado el cambio.
- Se aplican tarifas de red estándar a la salida de la red.



- 
- Si replica un registro en las regiones que desea, se le cobrarán tarifas de registro premium para cada región.

**Fuentes:**

<https://docs.microsoft.com/en-us/azure/container-registry/container-registry-intro>

<https://azure.microsoft.com/en-us/services/container-registry/>



## Lote Azure

- Un servicio que ejecuta trabajos por lotes de computación paralela y de alto rendimiento (HPC) a gran escala en Azure.
- Le permite ejecutar trabajos en un grupo de máquinas virtuales Linux o Windows.

### Componentes

- UN **tarea** representa una unidad de cálculo y un **trabajo** es una colección de tareas.
- **Prioridad de trabajo** los valores van desde la prioridad más baja hasta la más alta.
- Para especificar ciertos límites para sus trabajos, puede usar **limitaciones laborales**:
  - Tiempo máximo de reloj de pared: las tareas finalizan si el trabajo dura más del tiempo especificado.
  - Número máximo de reintentos de tareas: si la tarea falla, se pondrá en cola para ejecutarse nuevamente. UN **tarea del administrador de trabajos** contiene la información necesaria para crear las tareas necesarias para el trabajo.
- **Trabajos programados** le permiten crear trabajos recurrentes. Ejecutar simultáneamente en más de un nodo de cálculo
- con un **Tarea de instancias múltiples**.
- Con **dependencias de tareas**, la tarea depende de la finalización de otras tareas antes de su ejecución.

### Precios

- Sin cargo adicional por usar Azure Batch y solo se le cobrará por los recursos subyacentes consumidos.

### Fuentes:

<https://docs.microsoft.com/en-us/azure/batch/batch-technical-overview>

<https://azure.microsoft.com/en-us/services/batch/>



## Azure CycleCloud

- Organice y gestione entornos informáticos de alto rendimiento (HPC) en Azure.
- Le permite aprovisionar infraestructura para sistemas HPC, implementar programadores HPC familiares y escalar la infraestructura automáticamente para ejecutar trabajos de manera eficiente a cualquier escala.

### Características

- **Programador agnóstico** - utilice programadores HPC estándar o amplíe los complementos de ajuste de escala automático de CycleCloud para que funcionen con su propio programador.
- **Administrar recursos informáticos** - administre máquinas virtuales y conjuntos de escalado para proporcionar un conjunto de recursos informáticos para satisfacer los requisitos de carga de trabajo.
- **Recursos de autoescala** - ajustar el tamaño del clúster y los componentes automáticamente según la carga de trabajo, la disponibilidad y los requisitos de tiempo.
- **Supervisar y analizar** - recopile métricas a nivel de nodo y analice los datos de rendimiento mediante una herramienta de visualización.
- **Clústeres de plantillas** - le permite compartir las topologías de su clúster.
- **Agente de CycleCloud (llamado Jetpack)** - Instalado por Azure CycleCloud en cada máquina virtual para proporcionar las siguientes funciones:
  - Configuración de nodo
  - Sincronización distribuida
  - Chequeo de salud

### Fuentes:

<https://docs.microsoft.com/en-us/azure/cyclecloud/overview?view=cyclecloud-7>

<https://azure.microsoft.com/en-us/features/azure-cyclecloud/>



## Azure Service Fabric

- Una plataforma de sistemas distribuidos que ayuda a empaquetar, implementar y administrar microservicios y contenedores escalables y confiables.
- Cree microservicios y aplicaciones basadas en contenedores con el lenguaje de programación que elija, incluidos .NET Core 2.0, C # y Java. Admite dos tipos de microservicios:
  - **Apátridas** - No mantiene un estado mutable fuera de una solicitud y su respuesta del servicio, como pasarelas de protocolo y proxies web.
  - **Con estado** - Mantiene un estado de autoridad mutable más allá de la solicitud y su respuesta. Permite flujos de trabajo de bajo contacto
- para aprovisionar, implementar, parchear y monitorear aplicaciones con Service Fabric **gestión del ciclo de vida de las aplicaciones**.
- Admite la implementación de múltiples instancias de aplicaciones. UN **clúster de tejido de servicio** es un conjunto de máquinas virtuales en las
- que se implementan y administran sus microservicios.

## Seguridad

- Cree o importe un certificado con Azure Key Vault.
- Use Azure Firewall para complementar las reglas de su grupo de seguridad de red existente para controlar el acceso a su clúster.

## Precios

- Se le cobra según la cantidad de CPU virtuales y GB de memoria asignados a cada VM.
- Se le cobra según el tamaño, la cantidad de discos y la cantidad de transferencias de datos salientes.

## Fuentes:

<https://azure.microsoft.com/en-us/services/service-fabric/>

<https://docs.microsoft.com/en-us/azure/service-fabric/service-fabric-overview>



## Escritorio virtual de Windows

- Una solución de virtualización de aplicaciones y escritorios totalmente administrada en la nube.
- Admite dispositivos Windows, Mac, iOS y Android.
- Asigne varios usuarios a una sola máquina virtual utilizando un sistema operativo cliente.

## Conceptos

- **Grupos de host** son una colección de máquinas virtuales idénticas. Los tipos de grupos de hosts son:
  - Personal
    - Asignación automática: el servicio asignará automáticamente al usuario a un host disponible.
    - Asignación directa: puede asignar un usuario a un host específico. Agrupados
  - Puede establecer el número máximo de usuarios que tienen sesiones simultáneas en un solo host
  - Amplitud: primer equilibrio de carga: asigna uniformemente a sus usuarios en el grupo de hosts.
  - Profundidad: primer equilibrio de carga: asigna completamente a los usuarios en una sola máquina virtual.
- Una agrupación lógica de aplicaciones instaladas en un host de sesión se denomina **grupo de aplicaciones**.
  - RemoteApp: los usuarios solo pueden acceder a las RemoteApps que seleccionó.
  - Escritorio: los usuarios pueden acceder completamente al escritorio. Una agrupación lógica de
- grupos de aplicaciones se denomina **espacios de trabajo**.

## Seguridad

- Use Azure Active Directory para una experiencia de inicio de sesión coherente para sus usuarios.
- Puede configurar MFA y controles de acceso condicional para determinar el acceso según su identidad, dispositivo y ubicación.
- Admite diferentes tipos de autenticación.
  - Autenticación de host de sesión
  - Identidad híbrida
  - Inicio de sesión único (SSO)
- Use Azure RBAC para asignar múltiples roles a sus usuarios: Colaborador, Lector y Operador

## Precios

- Se le cobran los siguientes componentes:
  - Máquinas virtuales y almacenamiento de SO
  - Disco de datos y almacenamiento de perfiles de usuario
  - Redes

## Fuentes:

<https://docs.microsoft.com/en-us/azure/virtual-desktop/overview>  
<https://azure.microsoft.com/en-us/services/virtual-desktop/>



## ALMACENAMIENTO

### Descripción general de Azure Storage

- Una cuenta de almacenamiento de Azure contiene **blobs, archivos, colas, tablas, y discos**.
- Tipos de cuentas de almacenamiento: **Uso general (v2 y v1), BlockBlobStorage, FileStorage, y BlobStorage**
- Todas las cuentas de almacenamiento se cifran mediante el cifrado del servicio de almacenamiento (SSE) para los datos en reposo. Puntos finales de cuentas de almacenamiento:
  - **Almacenamiento de blobs:** <https://tutorialsdojo.blob.core.windows.net>
  - **Almacenamiento de mesa:** <https://tutorialsdojo.table.core.windows.net>
  - **Almacenamiento en cola:** <https://tutorialsdojo.queue.core.windows.net>
  - **Archivos de Azure:** <https://tutorialsdojo.file.core.windows.net>. Los niveles de acceso a file.core.windows.net son: Hot, Cool y Archive
    - Caliente
      - Los costos de almacenamiento más altos, pero los costos de acceso más bajos.
      - Almacene los datos a los que se accede con frecuencia.
      - De forma predeterminada, se crean nuevas cuentas de almacenamiento en el nivel activo. Frio
    - - Menores costos de almacenamiento, pero mayores costos de acceso.
      - Almacene los datos a los que se accede con poca frecuencia (al menos 30 días).
      - Puede utilizar un nivel de acceso genial para realizar copias de seguridad a corto plazo. Archivo
    - - Los costos de almacenamiento más bajos, pero los costos de recuperación más altos.
      - Almacene datos a los que rara vez se accede (al menos 180 días).
      - Los datos deben almacenarse durante mucho tiempo.



	Premium performance	Hot tier	Cool tier	Archive tier
<b>Availability</b>	99.9%	99.9%	99%	Offline
<b>Availability (RA-GRS reads)</b>	N/A	99.99%	99.9%	Offline
<b>Usage charges</b>	Higher storage costs, lower access, and transaction cost	Higher storage costs, lower access, and transaction costs	Lower storage costs, higher access, and transaction costs	Lowest storage costs, highest access, and transaction costs
<b>Minimum object size</b>	N/A	N/A	N/A	N/A
<b>Minimum storage duration</b>	N/A	N/A	30 days <sup>1</sup>	180 days
<b>Latency (Time to first byte)</b>	Single-digit milliseconds	milliseconds	milliseconds	hours <sup>2</sup>

● La redundancia de almacenamiento incluye: almacenamiento con redundancia local (LRS), almacenamiento con redundancia de zona (ZRS), almacenamiento con redundancia geográfica (GRS), almacenamiento con redundancia de zona geográfica (GZRS)

- Almacenamiento con redundancia local (LRS)
  - Una estrategia de redundancia de bajo costo.
  - Sus datos se copian sincrónicamente tres veces dentro de la región principal. Almacenamiento con redundancia de zona (ZRS)
  - Redundancia para alta disponibilidad.
  - Los datos se copian de forma sincrónica en tres zonas de disponibilidad de Azure en la región principal.
- Almacenamiento con redundancia geográfica (GRS)
  - Redundancia transregional.
  - En la región principal, los datos se copian sincrónicamente tres veces y luego se copian de forma asincrónica en la región secundaria.
  - Habilite el almacenamiento con redundancia geográfica de solo lectura (RA-GRS) para acceder a los datos en la región secundaria.
- Almacenamiento con redundancia de zona geográfica (GZRS)
  - Redundancia tanto para alta disponibilidad como para máxima durabilidad.
  - Los datos se copian de forma sincrónica en tres zonas de disponibilidad de Azure en la región principal y luego se copian de forma asincrónica en la región secundaria.
  - También puede habilitar RA-GZRS para leer datos de acceso en la región secundaria.



	Locally-Redundant Storage (LRS)	Zone Redundant Storage (ZRS)	Geo-redundant storage (GRS)
Replication	Replicates your data 3 times within a single physical location synchronously in the primary region.	Replicates your data across 3 Azure Availability Zones synchronously in the primary region	Replicates your data in your storage account to a secondary region
Redundancy	Low	Moderate	High
Cost	Provides the least expensive replication option	Costs more than LRS but provides higher availability	Costs more than ZRS but provides availability in the event of regional outages
Available if a node went down within a data center?	Yes	Yes	Yes
Available if the entire data center (zonal or non-zonal) went down?	No	Yes	Yes
Available on region-wide outage in the primary region?	No	No	Yes
Has read access to the secondary region if the primary region is unavailable?	No	No	Yes

Tutorials Dojo

- La transferencia de datos a una cuenta de almacenamiento diferente se puede realizar de forma automática o manual. Puede migrar datos
- manualmente usando:
  - AzCopy utiliza una utilidad de línea de comandos.
  - La biblioteca de movimiento de datos está diseñada para operaciones de transferencia de datos fáciles, confiables y de alto rendimiento similares a AzCopy.
  - La API REST o la biblioteca cliente le permite crear una aplicación personalizada para migrar sus datos.

#### Tipos de cuentas de almacenamiento

- **Cuentas v2 de uso general**
  - Admite tablas de colas de Data Lake Gen2, blobs y archivos.
  - Ofrece los precios de capacidad por gigabyte más bajos para Azure Storage.
- **Cuentas v1 de uso general**
  - Admite blobs, archivos, discos, colas, tablas.
  - Puede actualizar una cuenta v1 de uso general a una cuenta v2 de uso general sin tiempo de inactividad y sin copiar los datos.
  - Puede usar cuentas v1 de uso general, ya que las cuentas v2 de uso general y las cuentas de Blob Storage solo admiten el modelo de implementación de Azure Resource Manager.



- Si no necesita una gran capacidad para un ancho de banda de replicación geográfica significativa o de transacciones intensivas, GPv1 es una opción adecuada.

- **Cuentas BlockBlobStorage**

- Proporciona una latencia baja y constante y tasas de transacción más altas.
- Actualizar una cuenta de Blob Storage a una cuenta v2 de uso general no tiene tiempo de inactividad y no es necesario copiar los datos.
- No admite niveles de acceso a archivos calientes, fríos y
- Puede usar BlockBlobStorage para almacenar datos de objetos no estructurados como blobs en bloque o agregar blobs.

- **Cuentas de FileStorage**

- Solo admite archivos compartidos.
- Ofrece ráfagas de IOPS.



Almacenamiento Cuenta Tipo	Soportado Servicios	Soportado Performance niveles	Soportado Acceso Niveles	Cifrado de Replicación Opciones	Deployment Modelo	
General-propósito V2	Blob, archivo, Cola, Mesa, Disco, y datos Lago Gen2	Estándar, Prima	Fresco caliente, Archivo	LRS, GRS, RA-GRS, ZRS, GZRS (avance), RA-GZRS (avance)	Recurso Gerente	Cifrado
General-propósito V1	Blob, archivo, Cola, Mesa y Disco	Estándar, Prima	N / A	LRS, GRS, RA-GRS	Recurso Gerente, Clásico	Cifrado
BlockBlob Almacenamiento	Blob (bloque manchas y adjuntar solo manchas)	Prima	N / A	LRS, ZRS	Recurso Gerente	Cifrado
Almacenamiento de archivos Blob	Solo archivo	Prima	N / A	LRS, ZRS	Recurso Gerente	Cifrado
BlobStorage Blob	Bloque estándar manchas y adjuntar solo manchas)		Fresco caliente, Archivo	LRS, GRS, RA-GRS	Recurso Gerente	Cifrado

#### Seguridad

- Para otorgar acceso a su cuenta de almacenamiento, la solicitud debe incluir una **Autorización** encabezamiento.
- Si la autenticación de la identidad es exitosa, entonces **Azure Active Directory** devuelve un token que se utilizará para autorizar la solicitud a Azure Storage Services.
- Puede utilizar la autorización de clave compartida para construir una cadena de conexión.
- La firma de acceso compartido le permite tener un control granular sobre quién puede acceder a sus datos.
- Cuando copia un archivo sin los metadatos para el cifrado, el contenido del blob no se puede recuperar nuevamente.

#### Precios

- Se le cobra según su región, tipo de cuenta, nivel de acceso y capacidad de almacenamiento.
- Las operaciones de replicación y lectura / escritura también generan costos.
- Si sus datos no se están ejecutando en la misma región, se le cobrará por la salida de datos.



---

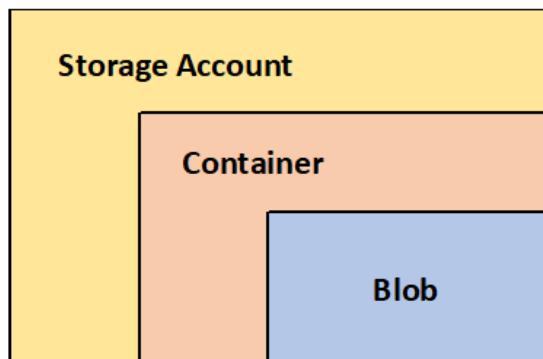
**Fuentes:**

<https://docs.microsoft.com/en-us/azure/storage/common/storage-account-overview?toc=/azure/storage/blobs/toc.json>

<https://docs.microsoft.com/en-us/azure/storage/common/storage-account-create?tabs=azure-portal>

## Almacenamiento de blobs de Azure

- **segundo inario Large Transmisión exterior**ect
- **Almacenamiento de objetos** solución para la nube.
- Almacena todo tipo de archivos: imagen, video, audio, copias de seguridad de archivos de registro, etc.



- **Cuenta de almacenamiento**
  - Espacio de nombres único en Azure para sus datos.
  - Si el nombre de su cuenta de almacenamiento es *tutoriales dojo*, entonces el punto de conexión predeterminado para Blob Storage es:  
*http://tutorialsdojo.blob.core.windows.net*
- **Envase**
  - Organiza un conjunto de blobs que son similares a un directorio en un sistema de archivos.

### Tipos de blobs

- **Bloquear**
  - Almacene datos binarios y de texto hasta 4,7 TB.
  - Obtenga una vista previa de blobs de bloques más grandes de hasta 190,7 TiB.
- **Adjuntar**
  - Ideal para registrar datos de máquinas virtuales.
- **Página**
  - Almacene archivos de acceso aleatorio de hasta 8 TB de tamaño
  - Almacene archivos de disco duro virtual (VHD).

### Niveles de acceso admitidos

- **Caliente**
  - Objetos de acceso frecuente.
  - Más rentable, mientras que los costos de almacenamiento son más altos.
  - Predeterminado en nuevas cuentas de almacenamiento.
- **Frio**
  - Datos a los que se accede con poca frecuencia.



- Más rentable, pero con un costo de acceso más alto que el nivel activo.
- Los datos permanecen durante al menos 30 días.

- **Archivo**

- Archivos de acceso poco frecuente.
- El costo más bajo para almacenar datos pero el costo de acceso más alto.
- Los datos permanecen durante al menos 180 días.

- **Política de gestión del ciclo de vida**

- UN *conjunto de reglas de gestión del ciclo de vida* tiene un conjunto de reglas que definen acciones que se aplican a un grupo de objetos.

Action set   Filter set   Review + add

Each rule definition includes an action set and a filter set. The action set applies the tier or delete actions to the filtered set of objects. The filter set limits rule actions to a certain set of objects within a container or objects names.

Rule name \* tutorials-dojo ✓

Status  Disabled  Enabled

Blobs

Move blob to cool storage  
Days after last modification 30 ✓

Move blob to archive storage  
Days after last modification 60 ✓

Delete blob  
Days after last modification 90 ✓

i Any blob that is moved to Archive is subject to an Archive early deletion period of 180 days. Additionally, any blob that is moved to Cool is subject to a Cool early deletion period of 30 days.

- Le permite transferir sus datos a los niveles de acceso adecuados.
- Elimina blobs al final de sus ciclos de vida.





## Características

- **Control de versiones**
  - Identificado por un ID de versión.
  - Habilite el control de versiones y restaure una versión anterior de un blob para recuperar sus datos.
  - Si deshabilita el control de versiones del blob, no elimina los blobs, las versiones ni las instantáneas existentes.
- **Instantáneas**
  - Una versión de solo lectura de un blob que se tomó en un momento determinado.
  - Las instantáneas persisten hasta que se eliminan explícitamente.
- **Replicación de objetos**
  - Copia blobs en bloque de forma asíncrona entre una cuenta de almacenamiento de origen y una cuenta de destino.
  - Una cuenta de origen puede tener hasta dos cuentas de destino. Pero no puede haber más de dos cuentas de origen en la cuenta de destino.
- **Sitio web estático**
  - Sirva su sitio web estático directamente desde un contenedor de almacenamiento llamado \$ web.
  - CORS no es compatible.
  - Puede otorgar acceso de solo lectura en sus recursos con un nivel de acceso público.
  - Habilitar **Red de entrega de contenido de Azure (CDN)** almacenar en caché el contenido de un sitio web estático.
  - Puede usar Azure CDN para configurar un extremo de dominio personalizado.

## Seguridad

- Azure Storage usa cifrado AES de 256 bits.
- Clave administrada por el cliente
  - Con Azure Key Vault, puede cifrar y descifrar datos en Blob Storage y en Azure Files.
- Clave proporcionada por el cliente
  - Un cliente puede incluir su propia clave de cifrado para un control granular.



Gestión de claves parámetro	Administrado por Microsoft administrado por el cliente proporcionado por el cliente	llaves	llaves
Cifrado / descifrado en operaciones	Azur	Azur	Azur
Azure Storage servicios apoyados	Todos	Almacenamiento de blobs, Azure Archivos	Almacenamiento de blobs
Almacenamiento de claves	Tienda de claves de Microsoft	Azure Key Vault	Llave propia del cliente Tienda
Rotación de clave responsabilidad	Microsoft	Cliente	Cliente
Control clave	Microsoft	Cliente	Cliente

**Fuentes:**

<https://azure.microsoft.com/en-us/services/storage/blobs/>

<https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blobs-introduction>

[https://docs.microsoft.com/en-us/azure/storage/blobs/storage-lifecycle-management-concepts?tabs=azure-p ortal](https://docs.microsoft.com/en-us/azure/storage/blobs/storage-lifecycle-management-concepts?tabs=azure-portal)



## Almacenamiento en disco de Azure

- **Almacenamiento a nivel de bloque** volúmenes para Azure Virtual Machines.
- El almacenamiento en disco es un disco administrado que está diseñado para una disponibilidad del 99,999%.
- Puede crear 50.000 discos de máquina virtual para cada región.

### Características

- Diferentes tipos de opciones de almacenamiento: **HDD estándar**, **SSD estándar**, **SSD premium**, y **Ultra disco** volúmenes de hasta 64 TiB.
- El disco del sistema operativo tiene una capacidad máxima de 2048 GiB.
- El tamaño máximo del disco de datos es 32,767 GiB.
- Los discos administrados están integrados con **conjuntos de disponibilidad** para garantizar que los discos de VM estén separados entre sí en un conjunto de disponibilidad para evitar un único punto de falla.
- Puede asignar permisos específicos para un disco administrado a uno o más usuarios usando **Azure RBAC**.
- Puede utilizar el disco temporal para almacenar datos como archivos de página o de intercambio.
- Los discos de SO efímeros son para aplicaciones sin estado.
- Adjunte un disco administrado a varias máquinas virtuales simultáneamente mediante discos compartidos de Azure.
- Con las instantáneas, puede realizar una copia de seguridad de sus discos administrados en cualquier momento.

### Tipos de disco

- **HDD estándar**
  - De bajo costo y adecuado para copias de seguridad.
  - **Escribir latencias bajo 10ms.**
  - **Leer latencias bajo 20ms. SSD**
- **estándar**
  - Rendimiento constante a niveles de IOPS más bajos.
  - Mayor confiabilidad, escalabilidad y menor latencia en HDD.
- **SSD premium**
  - Disco de alto rendimiento y baja latencia para máquinas virtuales.
  - **IOPS y rendimiento consistentes.**
  - Ofertas **disco estallando** y puede aumentar sus IOPS por disco hasta 3500 y su ancho de banda hasta 170 Mbps.
  - Límite máximo de ráfaga de 30 minutos
- **Ultra disco**
  - Alto rendimiento, IOPS y almacenamiento en disco de baja latencia constante.
  - Solo admite lecturas y escrituras no almacenadas en caché.
  - No es compatible con instantáneas de disco, imágenes de máquina virtual, conjuntos de disponibilidad, hosts dedicados de Azure ni cifrado de disco de Azure.
  - No se admite la integración con Azure Backup o Azure Site Recovery.



Detalle	HDD estándar	SSD estándar	SSD premium	Ultra disco
Tipo de disco	HDD	SSD	SSD	SSD
<b>Guion</b>	Apoyo, no critico, infrecuente acceso	Servidores web, y ligero aplicaciones de empresa	Producción y rendimiento-se sensible cargas de trabajo	IO intensivo cargas de trabajo, arriba bases de datos de nivel, y otra transacción-hea cargas de trabajo vy
Tamaño máximo de disco	32,767 GiB	32,767 GiB	32,767 GiB	65.536 GiB
Rendimiento máximo 500 MB / s		750 MB / s	900 MB / s	2000 MB / s
IOPS máx.	2000	6.000	20.000	160.000

## Cifrado

- **Cifrado del lado del servidor (SSE)** lo realiza el servicio de almacenamiento.
- **Cifrado de disco de Azure (ADE)** se puede habilitar en el sistema operativo y los discos de datos.
- Cifrado mediante cifrado AES de 256 bits.
- De forma predeterminada, los discos administrados utilizan claves de cifrado administradas por plataforma.
- Con Azure Key Vault, puede importar sus claves RSA o generar nuevas claves RSA.
- Para HDD estándar, SSD estándar y SSD premium: la desactivación o eliminación de la clave apagará automáticamente todas las VM con discos que utilicen esa clave.
- Si deshabilita o elimina una clave, cualquier máquina virtual con **ultra discos** el uso de la tecla no se apagará automáticamente.
  
- Una vez que habilita el cifrado de extremo a extremo, los discos temporales y los discos de SO efímeros se cifran con claves administradas por la plataforma.

## Precios

- El tamaño del disco administrado se factura según el tamaño aprovisionado. Las instantáneas se cobran en función del tamaño utilizado.
- Las transferencias de datos salientes generan facturación por el uso de ancho de banda.
- Se le cobra por la cantidad de transacciones que realiza en un disco administrado (la cantidad de operaciones de lectura y escritura de datos realizadas).

## Fuentes:

<https://azure.microsoft.com/en-us/services/storage/disks/>

<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/managed-disks-overview>



## Archivos de Azure

- Ofrece almacenamiento de archivos basado en la nube totalmente administrado al que se puede acceder a través del protocolo de bloque de mensajes de servidor (SMB) estándar de la industria.

### Características

- Monte su recurso compartido de archivos de Azure desde Windows, Linux o macOS.
- Sincronización de archivos de Azure** le permite acceder a sus datos desde SMB, REST o incluso de forma local.
- Cifre los datos en reposo y en tránsito mediante SMB 3.0 y HTTPS.
- Levante y cambie las aplicaciones a la nube, donde los datos de la aplicación se mueven a Azure Files y la aplicación continúa ejecutándose localmente.
- Almacene los archivos de configuración en una ubicación centralizada donde se pueda acceder a ellos desde muchas instancias de aplicaciones.
- Azure Files proporciona la capacidad de tomar **compartir instantáneas** de acciones de archivo.

### Niveles de almacenamiento

- Acciones de archivo premium (SSD)**
  - Alto rendimiento y baja latencia, en milisegundos de un solo dígito para la mayoría de las operaciones de E / S.
  - Para cargas de trabajo intensivas en IO.
- Archivos compartidos estándar (HDD)**
  - Rendimiento confiable para cargas de trabajo de E / S que son menos sensibles a la latencia.
- Si creó un archivo compartido premium o estándar, no puede convertirlo automáticamente al otro nivel.

Detalle	Prima	Estándar
<b>Modelo de facturación</b>	Modelo de facturación aprovisionado, pague por la cantidad de almacenamiento que proporciona en lugar de la cantidad de almacenamiento que realmente solicita.	Modelo de pago por uso, el factura aumentará si usa (leer / escribir / montar) el Comparta más archivos de Azure.
<b>Opciones de redundancia</b>	Está disponible para almacenamiento con redundancia local (LRS) y redundante de zona (ZRS).	Está disponible para redundancia local, redundante de zona, geo-redundante (GRS), y redundante de zona geográfica (GZRS) almacenamiento.
<b>Tamaño máximo del archivo compartido</b>	Aprovisionado para hasta 100 TiB.	5 TiB por defecto, 100 TiB para redundante local o zona



		almacenamiento redundante cuentas.
<b>Disponibilidad regional</b>	Los recursos compartidos de archivos no están disponibles en cada región, pero el soporte de zona redundante es disponible en un subconjunto más pequeño de regiones.	Disponible en todas las regiones de Azure.

#### Dispositivos soportados

- Para usar un recurso compartido de archivos de Azure fuera de la región de Azure, el sistema operativo debe admitir SMB 3.0.
- Para montar un uso compartido de archivos de Azure en Windows, debe tener acceso al puerto 445.

Versión de Windows	Versión SMB	Montable en Azure VM	Montable En las instalaciones
Servidor de windows 2019	SMB 3.0	si	si
Windows 10	SMB 3.0	si	si
Servidor de windows Semi anual canal2	SMB 3.0	si	si
Servidor de windows 2016	SMB 3.0	si	si
Windows 8.1	SMB 3.0	si	si
Servidor de windows 2012 R2	SMB 3.0	si	si
Servidor de windows 2012	SMB 3.0	si	si
Ventanas 7 3	SMB 2.1	si	No
Servidor de windows 2008 R2	SMB 2.1	si	No



- Los clientes de Linux también pueden acceder al almacenamiento de archivos a través del protocolo SMB.

Distribución de Linux	SMB 2.1 <i>(Se monta en máquinas virtuales dentro de la misma región de Azure)</i>	SMB 3.0 <i>(Se monta desde las instalaciones y entre regiones)</i>
Ubuntu	14.04+	16.04+
Red Hat Enterprise Linux (RHEL)	7+	7.5+
CentOS	7+	7.5+
Debian	8+	10+
openSUSE	13.2+	42.3+
SUSE Linux Enterprise Servidor	12+	12 SP3 +

### Cifrado

- De forma predeterminada, se cifra con claves administradas por Microsoft y es responsable de rotarlas de forma regular.
- Con las claves administradas por Microsoft, también puede optar por administrar sus propias claves, lo que le da control sobre el proceso de rotación.
- Con claves administradas por el cliente, el almacenamiento de archivos de Azure está autorizado para acceder a sus claves para cumplir con las solicitudes de lectura y escritura de sus clientes.

### Redes

- SMB usa el puerto 445.
- Accesible desde cualquier lugar, a través del punto final público de la cuenta de almacenamiento.
- Recursos compartidos de archivos de Azure a través de una conexión ExpressRoute o VPN:
  - Hacer un túnel en una red virtual, incluso si el puerto 445 está bloqueado.
  - Los puntos finales privados le brindan una dirección IP dedicada desde dentro del espacio de direcciones de la red virtual.
  - Le permite configurar el reenvío de DNS.

### Azur Sincronización de archivos

- Transforme un servidor de Windows local (o en la nube) en un caché rápido de su recurso compartido de archivos de Azure. Solo se admiten los volúmenes NTFS; ReFS, FAT, FAT32 y otros sistemas de archivos no son compatibles. El servicio admite la interoperabilidad con los espacios de nombres DFS (DFS-N) y la replicación DFS (DFS-R).



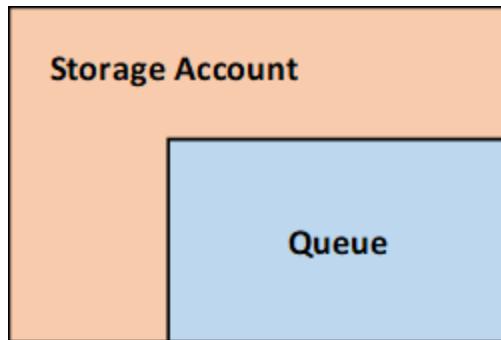
**Fuentes:**

<https://azure.microsoft.com/en-us/services/storage/files/>  
[https://docs.microsoft.com/en-us/azure/storage/files / storage-files-introduction](https://docs.microsoft.com/en-us/azure/storage/files/storage-files-introduction)  
[https://docs.microsoft.com/en-us/azure/storage/files / storage-how-to-use-files-windows](https://docs.microsoft.com/en-us/azure/storage/files/storage-how-to-use-files-windows)  
[https://docs.microsoft.com/en-us/azure/storage/files / storage-how-to-use-files-linux](https://docs.microsoft.com/en-us/azure/storage/files/storage-how-to-use-files-linux)



### Almacenamiento en cola de Azure

- Colas duraderas para servicios en la nube de gran volumen.
- Almacene una gran cantidad de mensajes.
- Los mensajes en cola pueden tener un tamaño de hasta 64 KB.



### Características

- Cola de mensajes asíncrona para comunicarse entre los componentes de la aplicación.
- Construido para ser escalable y resistir la falla de componentes individuales
- Supervise la longitud de la cola para agregar elasticidad a su aplicación e hiberne o implemente nodos adicionales según la demanda del cliente.

### Precios

- Sin costos iniciales ni tarifas de cancelación.
- solo paga por lo que usas.

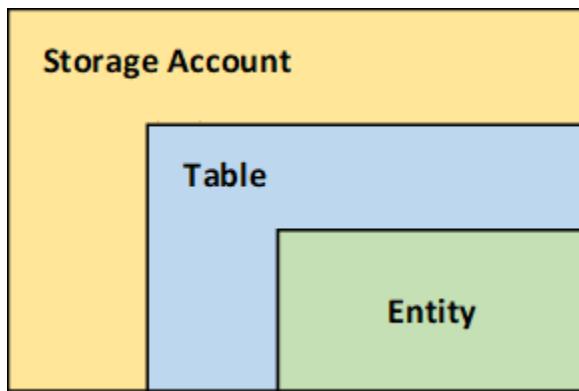
### Fuentes:

<https://azure.microsoft.com/en-us/services/storage/queues/>

<https://docs.microsoft.com/en-us/azure/storage/queues/storage-queues-introduction>

## Almacenamiento de tablas de Azure

- Un almacén de valores-clave NoSQL para grandes conjuntos de datos semiestructurados.
- Admite un esquema de datos flexible.
- Realiza consultas basadas en OData.



## Características

- Le permite almacenar y consultar grandes conjuntos de datos estructurados y no relacionales. Y a medida que crece la demanda, sus tablas se ampliarán.
- Amplíe sin tener que fragmentar manualmente su conjunto de datos.
- Los datos se replican tres veces dentro de una región utilizando almacenamiento con redundancia geográfica.
- Un **entidad** tiene un límite de 1 MB de tamaño.
- Almacene conjuntos de datos que no requieran combinaciones complejas, claves externas o procedimientos almacenados, y se pueden desnormalizar para un acceso rápido.
- El almacenamiento de tablas se utiliza para almacenar conjuntos de datos flexibles, como datos de usuario para aplicaciones web, información de dispositivos u otros tipos de metadatos que requiere el servicio.
- Puede almacenar cualquier cantidad de entidades en una tabla, hasta el límite de capacidad de la cuenta de almacenamiento.

## Fuentes:

<https://azure.microsoft.com/en-us/services/storage/tables/>

<https://docs.microsoft.com/en-us/azure/storage/tables/table-storage-overview>



## Almacenamiento de archivos de Azure

- Almacene datos a los que se accede con poca frecuencia y que se conservan durante un período de 180 días.
- Las instantáneas no se aplican al almacenamiento de archivos.

### Características

- Es compatible con 2 prioridades de rehidratación: **Alto** y **Estándar**
  - **Estándar (predeterminado)** - La solicitud de rehidratación puede demorar hasta 15 horas.
  - **Alto** - la solicitud de rehidratación puede terminar en menos de 1 hora para objetos de menos de 10 GB de tamaño. Respaldo a largo plazo,
- respaldo secundario y conjuntos de datos de archivo.
- Los costos de almacenamiento más bajos, pero los costos de rehidratación y acceso de datos más altos.
- Para leer datos en el almacenamiento de archivos, primero debe cambiar el nivel de blob a caliente o frío. Cumplimiento y datos
- de archivo que deben conservarse y a los que casi nunca se accede. El almacenamiento de archivos solo admite blobs en
- bloque.
- Si un blob está en el nivel de archivo, no se puede sobrescribir, a diferencia de lo que ocurre en el nivel activo o frío. El almacenamiento
- de archivos no se puede configurar como un nivel de acceso de cuenta predeterminado. El almacenamiento de archivos está disponible
- inicialmente en regiones seleccionadas.
- Las etiquetas de índice de blobs se pueden leer, configurar o modificar mientras están en el archivo. Solo puede
- copiar blobs de archivo dentro de la misma cuenta de almacenamiento.
- Transferencia de datos cifrados a la nube mediante HTTPS y claves AES de 256 bits para proteger automáticamente los datos en reposo.

### Casos de uso

- Se utiliza principalmente en la retención de copias de seguridad a largo plazo.
- Si necesita minimizar su costo, use Archive Storage para crear una solución de archivo de contenido de bajo costo.
- El almacenamiento de archivos proporciona almacenamiento seguro y compatible a nivel mundial para datos confidenciales.
- También puede utilizar el almacenamiento de archivos si tiene una gran cantidad de datos que deben conservarse.

### Precios

- Los blobs se almacenan durante al menos 180 días en el nivel de archivo. Eliminar o rehidratar blobs archivados antes del número mínimo de días incurrirá en tarifas de eliminación anticipada.
- Los cargos por el acceso a los datos aumentan a medida que el nivel se enfria. Para los datos en el nivel de acceso frío y de archivo, se le cobra un cargo de acceso a datos por gigabyte por lecturas.

### Fuentes:

<https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-storage-tiers?tabs=azure-portal>

<https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-rehydration?tabs=azure-portal>

<https://azure.microsoft.com/en-us/services/storage/archive/>



## BASE DE DATOS

### Azure Cosmos DB

- Base de datos distribuida globalmente que admite NoSQL.
- Un servicio de base de datos completamente administrado con **distribución global llave en mano** y transparente **replicación multimaestro**.

#### Características

- Cosmos DB ofrece cifrado en reposo.
- Replica todas las particiones en todas las regiones.
- CosmosDB ofrece lecturas y escrituras de milisegundos de un solo dígito en todas las regiones.
- Admite la comutación por error automática durante una interrupción regional.
- Niveles de coherencia: **Intensidad fuerte, limitada, sesión, prefijo consistente, y Eventual**
- Puede configurar estándar (manual) o **auto escala** rendimiento aprovisionado en sus bases de datos y contenedores.
- Supervise tanto las RU / s máximas de autoescala aprovisionadas como el rendimiento actual (RU / s) del sistema con **Monitor de Azure** métrica.

#### Niveles de consistencia

- **Fuerte** - Se garantiza que las lecturas devuelvan la versión confirmada más reciente de un artículo.
- **Caducidad limitada** - es para latencias de escritura bajas pero requiere una garantía de pedido global total.
- **Sesión** - Se garantiza que las lecturas respeten las garantías de prefijo consistente, lecturas monótonas, escrituras monótonas, lectura-sus-escrituras y escritura-sigue-lectura.
- **Prefijo consistente** - las actualizaciones que se devuelven contendrán algunos prefijos de todas las actualizaciones.
- **Eventual** - no tiene garantía de pedido de lecturas.

#### Seguridad

- El cifrado en reposo se aplica automáticamente.
- Utiliza cifrado AES-256 en todas las regiones.
- Puede usar las claves administradas por Microsoft o las claves administradas por el cliente.
- Dos tipos de claves para autenticar usuarios:
  - Master Keys para recursos administrativos.
  - Tokens de recursos para los recursos de la aplicación.
- Detectar actividades sospechosas que indiquen intentos inusuales y potencialmente dañinos de acceder o explotar bases de datos con **Protección avanzada contra amenazas**.

#### Precios

- Escala elásticamente el rendimiento y el almacenamiento aprovisionados para sus bases de datos de acuerdo con sus necesidades y solo pague por el rendimiento y el almacenamiento necesarios.



- El rendimiento de Cosmos DB por segundo y el consumo de unidades de solicitud varían según la operación y el documento JSON.
- Las copias de seguridad adicionales se facturarán como el total de GB de datos almacenados (*las dos primeras copias son gratuitas*).
- Aprovisiona el número de RU para su aplicación por segundo en incrementos de 100 RU por segundo. Se le factura por horas.
- Con el escalado automático para contenedores, paga por hora por las RU / s más altas a las que el sistema escaló en una hora.

**Fuentes:**

<https://docs.microsoft.com/en-us/azure/cosmos-db/introduction>

<https://azure.microsoft.com/en-us/free/cosmos-db/>



## Azure SQL

- Una base de datos completamente administrada construida sobre el motor de SQL Server. Durabilidad
- SLA hasta 99,995%.
- Tipo de recurso de bases de datos SQL:
  - Base de datos única: ofrece almacenamiento a hiperescala y sin servidor (hasta 100 TB).
  - Elastic Pool: una colección de bases de datos con un conjunto compartido de recursos.
  - Servidor de base de datos: administre grupos de bases de datos únicas y grupos elásticos.
- **Instancias administradas de SQL** son para migraciones "lift-and-shift" a la nube.
  - Las características del motor de base de datos de SQL Server y Azure SQL están disponibles en la Instancia administrada de SQL.
    - Beneficios de PaaS: Azure se encargará de toda la gestión de la infraestructura.
    - Continuidad comercial: los datos están protegidos con copias de seguridad automatizadas.
    - Seguridad y cumplimiento: admite la implementación de VNet nativa y se expone solo a través de una dirección IP privada.
    - Operaciones de administración: implemente automáticamente nuevas instancias, actualice las propiedades de la instancia y elimine las instancias que ya no son necesarias.
  - Automatice la migración de instancias de SQL Server existentes a instancias administradas de SQL con el servicio de migración de datos de Azure.
  - El beneficio híbrido de Azure para SQL Server le permite intercambiar licencias existentes para obtener tarifas con descuento en la instancia administrada de SQL.
- **Máquinas virtuales SQL** se utilizan para aplicaciones que requieren acceso a nivel de SO. Niveles de servicio basados
- Punto final: <*nombre\_servidor*>.database.windows.net
- en vCore:
  - El propósito general es para cargas de trabajo comunes. cargas de
  - La hiperescala es apropiada para el procesamiento de transacciones en línea (OLTP) y transacciones híbridas trabajo analíticas (HTAP).
  - Business Critical es mejor para aplicaciones OLTP con altas tasas de transacción y baja latencia de E / S.
- **Azur Beneficio híbrido para SQL Server** le permite utilizar sus licencias de SQL Server para pagar una tarifa reducida en Azure SQL.
- **Azure Data Studio** es una moderna herramienta de base de datos multiplataforma con fragmentos de código personalizables, IntelliSense ultrarrápido, definiciones útiles y una terminal integrada para ejecutar otras herramientas SQL.

## Supervisión

- Puedes usar **Perspectivas inteligentes** para monitorear continuamente su uso de Azure SQL y detectar eventos disruptivos que pueden conducir a un rendimiento deficiente de la base de datos.
- **Azure SQL Analytics** se puede utilizar para monitorear sus bases de datos en múltiples suscripciones. Puede recopilar y visualizar métricas clave de rendimiento de sus bases de datos y le permite crear reglas y alertas de supervisión personalizadas.



- **Sintonización automática** en Azure SQL supervisa continuamente las consultas ejecutadas en su base de datos y automáticamente mejora el rendimiento mediante inteligencia artificial.

#### Redes

- Las conexiones de punto final privadas brindan acceso a todas las bases de datos en el servidor.
- Permite las comunicaciones de todos los recursos dentro del límite de Azure con reglas de firewall.

#### Seguridad

- Puedes usar **Seguridad de datos avanzada (ADS)** para clasificación de datos, evaluación de vulnerabilidades y protección avanzada contra amenazas.

#### Precios

- Los recursos se facturan por hora a una tarifa fija basada en el nivel de servicio y el tamaño de cálculo que elija.
- Se le factura por el tráfico de Internet saliente.

#### Fuentes:

<https://docs.microsoft.com/en-us/azure/azure-sql/azure-sql-iaas-vs-paas-what-is-overview>

<https://azure.microsoft.com/en-us/services / sql-database />



#### Servicio de migración de base de datos de Azure (DMS)

- Acelera la migración de sus datos a Azure.
- Permite migraciones fluidas desde múltiples fuentes de bases de datos.
- Para realizar una migración en línea, debe crear una instancia basada en el **nivel de precios premium**.

#### Características

- Migra su base de datos y los objetos del servidor con un tiempo de inactividad mínimo.
- Admite la migración de Microsoft SQL Server, MySQL, PostgreSQL, MongoDB y Oracle a Azure desde las instalaciones y otros proveedores de la nube.
- Puede utilizar DMS para migraciones de bases de datos operativas y almacenes de datos.
- Automatice la migración de datos con **Azure PowerShell**.
- Utilizar **Azure Migrate** para descubrir su estado de datos local y evaluar la preparación para la migración.
- Puede crear hasta 2 servicios DMS por suscripción.

#### Precios

- Las migraciones únicas del nivel DMS Standard son de uso gratuito.
- El nivel premium de DMS se factura a una tarifa por hora basada en la capacidad informática aprovisionada.

#### Fuentes:

<https://docs.microsoft.com/en-us/azure/dms/dms-overview>  
<https://azure.microsoft.com/en-us/services/database-migration/>



## Base de datos Azure para MySQL y PostgreSQL

- Servicios de bases de datos relacionales PaaS
- Mitigue el tiempo de inactividad de la base de datos con capacidades de alta disponibilidad, redundancia y resistencia. Le permite escalar verticalmente cuando sea necesario.
- Reciba alertas basadas en las métricas de sus servidores. Proteja los datos confidenciales en reposo y en tránsito. Backups automatizados, hasta 35 días.
- Opciones de implementación de PostgreSQL: **Servidor único y Hiperescala (Citus)**
- Niveles de precios de servidor único: Básico, Uso general y Optimizado para memoria.
  - **Básico** - cargas de trabajo de rendimiento de E / S y cómputo ligero.
  - **Propósito general** - un cómputo y una memoria equilibrados con cargas de trabajo de rendimiento de E / S escalables.
  - **Memoria optimizada** - para cargas de trabajo de bases de datos de alto rendimiento que requieren rendimiento en memoria.

### PostgreSQL - Hiperescala (Citus)

- Fragmentación: escala horizontalmente en varias máquinas.
- Admite la paralelización de consultas para obtener respuestas más rápidas en grandes conjuntos de datos.
- Se utiliza principalmente para aplicaciones multiinquilino, análisis operativo en tiempo real y cargas de trabajo transaccionales de alto rendimiento.

### Fuente:

<https://docs.microsoft.com/en-us/azure/mysql/overview>

<https://docs.microsoft.com/en-us/azure/postgresql/overview>



## REDES Y ENTREGA DE CONTENIDO

### Red virtual de Azure (VNet)

- Puede crear una red virtual en la nube dedicada a su cuenta de Azure. Es el bloque de construcción fundamental donde puede lanzar recursos de Azure.
- Azure VNet es la capa de red de las máquinas virtuales de Azure.
- Una red virtual abarca todas las zonas de disponibilidad de la región. Después de crear una red virtual, puede agregar una o más subredes en cada zona de disponibilidad.

#### Conceptos clave

- UN **red virtual** (VNet) le permite especificar un rango de direcciones IP para la VNet, agregar subredes, asociar grupos de seguridad de red y configurar tablas de rutas.
- UN **subred** es un rango de direcciones IP en su red virtual. Puede iniciar recursos de Azure en una subred específica. Utilizar una **subred pública** para los recursos que necesitan conectarse a Internet y un **subred privada** para recursos que no estarán conectados a Internet.
- Para proteger los recursos de Azure en cada subred, use **grupos de seguridad de red**.

#### Caso de uso de VNet

- VNet con una única subred pública.
- VNet con subredes públicas y privadas (NAT).

#### Subredes

- Cuando crea una red virtual, debe especificar un rango de direcciones IPv4 para la red virtual en forma de bloque CIDR (*ejemplo: 10.0.0.0/16*).
- Un bloque CIDR no debe superponerse con ningún bloque CIDR existente que esté asociado con su red virtual.
- Puede agregar varias subredes en cada zona de disponibilidad de la región de su red virtual.
- Tipos de subredes:
  - Subred pública
  - Subred privada
  - Subred de puerta de enlace
- El tamaño del bloque CIDR de una dirección IPv4 está entre una máscara de red / 16 (65.536 direcciones IP) y una máscara de red / 29 (8 direcciones IP).
- Las 5 direcciones reservadas en cada bloque CIDR no están disponibles para su uso y no se pueden asignar a ninguna máquina virtual.
- Puede delegar una subred para que la utilice un servicio dedicado.

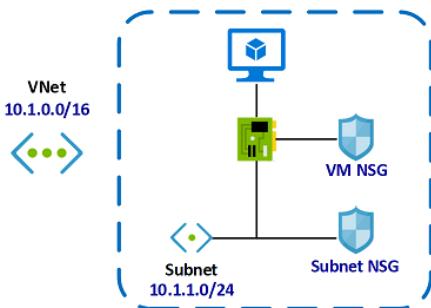
#### Seguridad

- Grupos de seguridad de red: controla el tráfico entrante y saliente de los recursos de Azure.
- Grupo de seguridad de la aplicación: le permite definir una política de seguridad de red del grupo de máquinas virtuales.

- Puedes usar **Verificación de flujo IP** de Azure Network Watcher para comprobar qué regla de seguridad de red permite o deniega el tráfico.
- Con la directiva de punto final de servicio de VNet, puedes filtrar el tráfico de VNet de salida a Azure Storage.

#### Notas del examen AZ-900:

Comprender cómo proteger su red virtual es muy importante. Recuerde siempre que puede asociar su grupo de seguridad de red en la subred de red virtual y las interfaces de red.



#### Componentes de la red virtual

- Puerta de enlace NAT
  - Permite que sus recursos de red virtual tengan una conexión solo saliente.
  - Un recurso de puerta de enlace NAT puede utilizar hasta 16 direcciones IP estáticas.
  - Puede utilizar varias subredes en una puerta de enlace NAT.
- Las tablas de ruta se utilizan para determinar hacia dónde se dirige el tráfico de la red.
  - Una subred solo se puede asociar con una tabla de rutas.
  - Si varias rutas contienen el mismo prefijo de dirección, la selección se basará en la siguiente prioridad: ruta de fija por el usuario, ruta BGP y ruta del sistema.
- Puede conectar redes virtuales entre sí mediante **Emparejamiento de redes virtuales**.
- Si necesita conectarse de forma privada a un servicio, puede utilizar **Punto de conexión privado de Azure** impulsado por Azure Private Link.

#### Precios

- Se le cobra por la dirección IP pública y la dirección IP reservada dentro de su red virtual.
- Se le cobrará por los datos de entrada y salida de VNet Peering.
- Se le cobrará por las horas de recursos de la puerta de enlace NAT y los datos procesados (por GB).

#### Fuentes:

<https://azure.microsoft.com/en-us/services/virtual-network/>

<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-overview>



## Balanceador de carga de Azure

- Distribuye el tráfico de red entrante a través de múltiples objetivos.
- Le permite enrutar el tráfico según la dirección IP de origen y el puerto a una dirección IP y puerto de destino.

### Características

- El equilibrador de carga admite protocolos basados en TCP / UDP.
- Se escala automáticamente a medida que aumenta el tráfico.
- La decisión de equilibrio de carga se basa en la siguiente conexión de tupla:
  - Puerto y dirección IP de origen
  - Puerto y dirección IP de destino
  - Protocolo
- NAT le permite controlar el tráfico de red entrante y saliente.
  - Reglas de entrada: tráfico permitido a una máquina virtual o instancia específica en el grupo de backend.
  - Reglas de salida: permiten que todos los recursos se comuniquen con Internet.
- Controle el flujo de tráfico dentro de su red virtual privada mediante un equilibrador de carga interno. Puedes usar un **balanceador de carga público** para permitir conexiones salientes para sus máquinas virtuales. Azure Load Balancer es compatible con IPv6.
- Niveles de equilibrador de carga: **Básico** y **Estándar**

### Componentes

- Un grupo de VM o instancias en un conjunto de escala de VM que atiende la solicitud entrante se llama **grupo de backend**.
- Determine el estado de salud de las instancias del grupo de backend con **sondas de salud**.
  - Comportamiento de prueba de salud: si las sondas en un grupo de backend fallan, dejará de recibir tráfico hasta que comience a pasar las sondas de salud nuevamente.
- Equilibrador de carga estándar **zonas de disponibilidad**:
  - Zonal = zona única
  - Zona redundante = múltiples zonas



Detalles	Balanceador de carga básico	Balanceador de carga estándar
Tamaño del grupo de backend	Admite hasta 300 instancias.	Admite hasta 1000 instancias.
Grupo de backend puntos finales	Un único conjunto de disponibilidad para VM o conjunto de escalado de VM.	Una única red virtual para cualquier máquina virtual o conjunto de escalado de máquina virtual.
Sondas de salud	TCP, HTTP	TCP, HTTP, HTTPS
Prueba de salud inactiva comportamiento	Las conexiones TCP permanecen activas en una instancia inactiva. Todas las conexiones TCP terminan cuando todas las sondas están inactivas.	Las conexiones TCP permanecen activas en un sondeo de instancia inactivo y en todos los sondeos inactivos.
Zonas de disponibilidad	No disponible	Zona redundante y zonal Fronteras para el tráfico entrante y saliente c.
Diagnóstico	Registros de Azure Monitor	Azure Monitor multidimensional métrica
Puertos HA	No disponible	Disponible para balanceador de carga interno
Seguro por defecto	Abierto por defecto. Grupo de seguridad de red opcional.	Cerrado a flujos entrantes a menos que lo permita un grupo de seguridad de la red. Tenga en cuenta que se permite el tráfico interno de la red virtual al balanceador de carga interno.
Reglas de salida	No disponible	NAT saliente declarativa configuración
Reinicio de TCP en múltiples	No disponible	Disponible en cualquier regla
interfaces inactivas	Solo entrante	Entrante y saliente
administración Operaciones	60-90 + segundos típico	La mayoría de las operaciones <30 segundos
SLA	No disponible	99,99%



## Precios

- Se le cobra según la cantidad de reglas de salida.
- Se le facturan las primeras cinco reglas de equilibrio de carga.
- No se le cobra por las reglas de NAT.

## Fuentes:

<https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-overview>

<https://azure.microsoft.com/en-us/services/load-balancer/>



## Puerta de enlace de VPN de Azure

- Una arquitectura de nube híbrida segura.
- Está compuesto por una subred de puerta de enlace, un túnel y una puerta de enlace local. Protocolos: conexiones de puerta de enlace VPN de seguridad de protocolo de Internet (IPsec) e intercambio de claves de Internet (IKE): **VNet-to-VNet**, **sitio a sitio**, y **Punto a sitio**
- Cree una conexión segura desde su red local a una red virtual de Azure con una VPN de sitio a sitio.
- La conexión de red virtual a red virtual se enruta automáticamente al espacio de direcciones actualizado, si actualizó el espacio de direcciones en la otra red virtual.
- Si necesita establecer una conexión a su red virtual desde una ubicación remota, puede usar una VPN punto a sitio (P2S).
- También puede tener una puerta de enlace VPN con más de una red local mediante una conexión de varios sitios.

Detalles	Sitio a Sitio	Punto a sitio
<b>Servicios apoyados</b>	Servicios en la nube y máquinas virtuales	Servicios en la nube y máquinas virtuales
<b>Anchos de banda</b>	Normalmente, IPsec agregado de <1 Gbps	Basado en el SKU de la puerta de enlace
<b>Protocolos</b>		Túnel de enchufes seguros Protocolo (SSTP), OpenVPN e IPsec
<b>Enrutamiento</b>	Admitimos PolicyBased (enrutamiento estático) y RouteBased (VPN de enrutamiento dinámico)	RouteBased (dinámico)
<b>Resistencia de la conexión</b>	activo-pasivo o activo-activo	activo pasivo
<b>Caso de uso</b>	Escenarios de desarrollo / pruebas / laboratorio y producción a pequeña escala cargas de trabajo para servicios en la nube y máquinas virtuales	Escenarios de creación de prototipos, desarrollo, pruebas y laboratorio para servicios en la nube y máquinas virtuales

## Precios

- Se le factura por hora por los costos de cómputo de la puerta de enlace VNet.
- Se le cobrará por la transferencia de datos de salida desde la puerta de enlace de red virtual.
- La puerta de enlace VPN solo le cobra cuando transfiere datos entre dos regiones diferentes, excepto con VPN punto a sitio.



---

**Fuentes:**

<https://azure.microsoft.com/en-us/services/vpn-gateway/>

<https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpngateways>



### Puerta de enlace de aplicaciones de Azure

- Un equilibrador de carga de tráfico web.
- Le permite distribuir el tráfico entrante según las propiedades de la solicitud HTTP, como URL y encabezados de host.
- La puerta de enlace de aplicaciones tiene cuatro niveles: **Estándar, Estándar V2, WAF, y WAF v2**
- Puede utilizar la misma puerta de enlace de aplicaciones para hasta más de 100 sitios web con alojamiento de varios sitios. Establezca las unidades de escala mínima y máxima según sus necesidades.
- Azure Application Gateway frente a Azure Load Balancer
  - Una puerta de enlace de aplicaciones opera en la capa 7.
  - Un equilibrador de carga funciona en la capa 4.
- Puede usar IP pública y privada en la interfaz.

#### Características

- Proteja sus datos con SSL de un extremo a otro.
- Enrute el tráfico según la ruta de la URL o el encabezado del host.
- Proteja sus aplicaciones de vulnerabilidades web comunes con WAF.
- Escala automáticamente según la carga de tráfico de su aplicación web.
- Con las cookies gestionadas por la puerta de enlace, puede dirigir el tráfico posterior desde una sesión de usuario al mismo servidor.

#### Precios

- Se le cobra por instancia, por GB y por hora de puerta de enlace.
- También se le cobran unidades de capacidad (*calculado por hora o por hora parcial*).

#### Fuentes:

<https://docs.microsoft.com/en-us/azure/application-gateway/overview>

<https://azure.microsoft.com/en-us/services/application-gateway/>



## Red de entrega de contenido de Azure (CDN)

- Una red distribuida de servidores que ofrece contenido web más cerca de los usuarios.
- Las CDN almacenan el contenido de la caché en **servidores de borde** para minimizar la latencia del usuario final.

### Características

- Mejora el rendimiento de las páginas web dinámicas mediante la aceleración de sitios dinámicos.
- Puede establecer dos tipos de reglas de almacenamiento en caché en Azure CDN:
  - Regla de almacenamiento en caché global: anula cualquier encabezado de directiva de caché HTTP.
  - Regla de almacenamiento en caché personalizada: puede establecer una regla para que coincida con rutas de acceso específicas y extensiones de archivo.
- Tipos de origen:
  - Almacenamiento
  - Sitio web de Storage Static
  - Servicio de almacenamiento en la nube
  - Aplicación Web
  - Origen personalizado
- Habilite HTTPS para mitigar las amenazas de seguridad en la red de distribución de contenido. Exporte métricas de uso básicas desde su CDN mediante registros de diagnóstico.
- Con la geofiltración, puede establecer reglas para diferentes rutas para permitir o bloquear contenido en países / regiones seleccionados.
- Punto final de CDN: <*tutorialsdojo*>.azureedge.net

### Cómo funciona el almacenamiento en caché

- Acceda a los datos rápidamente almacenando los datos en un servidor de origen.
- Si el archivo en el servidor de origen se ha actualizado, la caché debe actualizar su versión de recurso.
- Encabezados de directiva de caché HTTP de Azure CDN:
  - Cache-Control: comportamiento de almacenamiento en caché de un navegador.
  - Caduca: una fecha de caducidad basada en la fecha.
- Validadores de caché HTTP de Azure CDN:
  - ETag: una cadena que es única para cada archivo.
  - Última modificación: el servidor de origen compara la fecha con el encabezado de recurso de la última modificación.
    - Código de estado 200 = Modificado
    - Código de estado 304 = No modificado
- Comportamiento de almacenamiento en caché predeterminado:
  - Respete el origen: respete los encabezados de la directiva de caché de respuesta HTTP, si existen.
  - Duración de la caché de CDN: cuánto tiempo se almacena en caché un recurso en la CDN de Azure.

### Precios

- Se le cobra según la cantidad de reglas.
- Se le cobrará por las transferencias de datos salientes.



#### Limites

- El límite para los siguientes recursos es 25:
  - Perfiles CDN
  - Puntos finales de CDN por perfil
  - Dominios personalizados por endpoint

#### Fuentes:

<https://azure.microsoft.com/en-in/services/cdn/>

<https://docs.microsoft.com/en-us/azure/cdn/cdn-overview>



## Administrador de tráfico de Azure

- Un equilibrador de carga de tráfico basado en DNS.
- Mejora la capacidad de respuesta de sus aplicaciones enviando la solicitud al punto final más cercano.
- Ofrece una gama de **métodos de enrutamiento de tráfico y opciones de monitoreo de endpoints**.

### Características

- Es resistente al fracaso.
- Puede obtener información procesable sobre sus usuarios mediante un **vista de tráfico**.
- Mejore la disponibilidad de sus aplicaciones mediante el uso de controles de estado del administrador de tráfico.
- Ofrece comutación por error automática cuando falla un punto final.
- Puntos finales de Traffic Manager: **Azure, externo, y Anidado**
- Combine múltiples métodos de enrutamiento de tráfico usando **Perfiles de gestor de tráfico anidados**.

### Métodos de enrutamiento

- Prioridad: le permite establecer un criterio de valoración principal para todo el tráfico.
- Ponderado: distribuya el tráfico de acuerdo con los pesos.
- Rendimiento: dirige a los usuarios al extremo más cercano.
- Geográfico: dirija a los usuarios a un punto final específico.
- Multivalor: puntos finales para direcciones IPv4 / IPv6.
- Subred: asigne un grupo de rango de direcciones IP de usuario final a un punto final específico.

### Precios

- Se le cobra según la cantidad de consultas DNS recibidas. También se le cobrará por cada punto final supervisado.
- Puede reducir los cargos por consultas de DNS configurando un TTL más grande. Se le cobrará por la cantidad de puntos de datos utilizados en la vista de tráfico.

### Fuentes:

<https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-overview>

<https://azure.microsoft.com/en-us/services/traffic-manager/>



## DNS de Azure

- Le permite alojar su zona DNS y administrar sus registros DNS. La zona DNS le permite
- configurar una zona DNS pública y privada. Conjuntos de registros de alias:
  - - A: asigna el host a IPv4.
    - AAAA: asigna el host a IPv6.
    - CNAME: crea un registro para apuntar a otro dominio. Un límite de 20
- conjuntos de registros de alias por recurso.
- Utiliza la red Anycast para enrutar a los usuarios a los servidores de nombres más cercanos. Puede
- supervisar las métricas de su zona DNS mediante Azure Monitor.
  - QueryVolume: tráfico de consultas recibido.
  - RecordSetCount: el número de conjuntos de registros en su DNS.
  - RecordSetCapacityUtilization: porcentaje de utilización de la capacidad de su juego de registros.
- **DNS privado de Azure** le permite utilizar su nombre de dominio personalizado en su red virtual privada.
- El registro de alias le permite apuntar su dominio simple o ápice a un administrador de tráfico o un punto final de CDN.

## DNS privado

- Le permite administrar y resolver nombres de dominio en una red virtual.
- Configure un DNS de horizonte dividido para crear zonas con el mismo nombre.
- También es compatible con todo tipo de registros DNS: A, AAAA, CNAME, MX, PTR, SOA, SRV y TXT.
- Una red virtual se puede vincular a una sola zona privada. Pero puede vincular varias redes virtuales a una sola zona DNS.
- El espacio de IP privado en la red virtual vinculada permite el DNS inverso.

## Seguridad

- Para evitar la eliminación accidental de zonas, puede aplicar un bloqueo "No se puede eliminar".
- Cree un rol personalizado para asegurarse de que no tenga un permiso de eliminación de zona.
- Puede implementar un firewall DNS para mitigar los problemas de seguridad relacionados con el DNS.

## Precios

- Facturado según la cantidad de zonas DNS alojadas.
- Se le cobra según la cantidad de consultas DNS recibidas.

## Fuentes:

<https://azure.microsoft.com/en-us/services/dns/>  
<https://docs.microsoft.com/en-us/azure/dns/dns-overview>



#### Puerta de entrada azul

- Un servicio que utiliza la red global de Microsoft para mejorar la disponibilidad y el rendimiento de sus aplicaciones para sus usuarios locales y globales.
- Funciona en la capa HTTP / HTTPS y utiliza una **protocolo anycast basado en TCP dividido** para garantizar que sus usuarios se conecten al punto de presencia de Front Door más cercano.
- Admite una variedad de **métodos de enrutamiento de tráfico y supervisión del estado del backend** opciones para diversas necesidades de aplicaciones y modelos de commutación por error automáticos.
- Con **Enrutamiento basado en URL**, enruta el tráfico a grupos de backend según las rutas URL de la solicitud. Puede configurar más de un sitio web en la misma puerta principal con **alojamiento de varios sitios**.
- Utilizar a **ffinidad de sesión basada en cookies** para redirigir la sesión del usuario al mismo backend de la aplicación. Redirigir el tráfico según el protocolo, el nombre de host, la ruta y la cadena de consulta con **Redireccionamiento de URL. Reescritura de URL** le permite configurar una ruta de reenvío personalizada que copiará cualquier parte de la ruta entrante que coincida con una ruta comodín en la ruta reenviada.
- Front Door admite conectividad IPv6 de extremo a extremo y protocolo HTTP / 2.

#### Seguridad

- Si necesita que su nombre de dominio sea visible en su URL de Front Door, debe tener un dominio personalizado. Front Door también admite certificados administrados o certificados TLS / SSL personalizados.
- Puede crear reglas personalizadas para proteger su carga de trabajo HTTP / HTTPS de la explotación mediante Azure Web Application Firewall.

#### Precios

- Se le cobrará en función de lo siguiente:
  - Transferencias de datos entrantes y salientes
  - El número de reglas de enrutamiento
- Front Door tiene un límite de 100 dominios personalizados. Se le cobrará por dominios adicionales.

#### Fuentes:

<https://azure.microsoft.com/en-us/services/frontdoor/>

<https://docs.microsoft.com/en-us/azure/frontdoor/front-door-overview>



## Azure ExpressRoute

- Le permite establecer una conexión privada entre su centro de datos local o red corporativa a su infraestructura de nube de Azure.
- Más seguras, fiables y rápidas que las conexiones VPN convencionales.
- Admite el enrutamiento dinámico entre su red y Microsoft a través del protocolo Border Gateway Protocol (BGP). La conexión es redundante en cada ubicación de emparejamiento para una mayor confiabilidad.

### Características

- Las conexiones ExpressRoute permiten el acceso a los servicios de Microsoft Azure y los servicios de Microsoft Office 365 desde su red local.
- Proporciona conectividad a todas las regiones dentro de un **región geopolítica**.
- Para extender la conectividad a través de fronteras geopolíticas, puede habilitar **ExpressRoute Premium**.
- **Alcance global de ExpressRoute** le permite intercambiar datos en sus entornos locales conectándolos a sus circuitos ExpressRoute.
- **ExpressRoute Direct** proporciona conectividad dual de 100 Gbps que admite conectividad de escala activa / activa.
- Opciones de ancho de banda admitidas hasta 10 Gbps.
- **Complemento Premium ExpressRoute ( para circuito ExpressRoute)** proporciona las siguientes capacidades:
  - Aumento de los límites de ruta de 4000 a 10000 rutas para el emparejamiento público y privado de Azure.
  - Acceso global a servicios en cualquier otra región.
  - Aumente el número de enlaces VNet (*de 10 a un límite mayor*) en todos los circuitos ExpressRoute.

### Casos de uso

- Transferencia de grandes conjuntos de datos.
- Desarrollar y utilizar aplicaciones que utilizan fuentes de datos en tiempo real.
- Crear entornos híbridos que satisfagan los requisitos reglamentarios que exigen el uso de conectividad privada.

### Precios

- Modelos de facturación:
  - Datos ilimitados: toda la transferencia de datos entrantes y salientes es gratuita.
  - Datos medidos: toda la transferencia de datos entrantes es gratuita, pero la transferencia de datos salientes se factura por GB. La tasa de transferencia de datos varía según la región.
- La facturación de ExpressRoute comienza cuando se emite una clave de servicio al cliente. Si el servicio está activo para el **mes entero**, se le facturará la tarifa mensual independientemente de su uso. Sin embargo, si canceló el servicio **durante el mes**, luego se le cobrará por las horas utilizadas.

### Fuentes:

<https://docs.microsoft.com/en-us/azure/expressroute/expressroute-introduction>

<https://azure.microsoft.com/en-us/services/expressroute/>



## SEGURIDAD

### Azure Active Directory (AD)

- Un servicio de gestión de identidades y accesos que le ayuda a acceder a recursos internos y externos. Licencias de Azure AD: **Gratis**,
- **Premium P1, Premium P2 y Paga sobre la marcha**
  - Gratis: administración de usuarios y grupos en su directorio local
  - Premium P1: permite el acceso a recursos locales y en la nube.
  - Premium P2: proporciona una característica adicional denominada Azure AD Identity Protection.
  - Pago por uso: ofrece una función llamada Azure AD B2C.

#### Características

- Puedes usar **Autenticación de Azure AD** para un restablecimiento de contraseña de autoservicio, MFA, lista personalizada de contraseñas prohibidas y bloqueo inteligente.
- Le permite administrar identidades externas usando **Azure AD B2B**.
- **Azure AD B2C** es una identidad de empresa a cliente como servicio que le permite controlar cómo sus usuarios se registran, inician sesión y administran sus perfiles cuando usan sus aplicaciones.
- Puede administrar el acceso en sus aplicaciones en la nube con **acceso condicional**.
- Con **Administración de dispositivos de Azure AD**, le permite administrar y configurar identidades de dispositivos.
- Si necesita administrar servicios de dominio como unirse a un dominio, política de grupo y autenticación, puede usar **Servicios de dominio de Azure AD**.
- **Gobernanza de identidad** asegura que solo las personas autorizadas tengan el acceso correcto a recursos específicos.
- Apoyos **identidad híbrida** para acceder a recursos en la nube o en las instalaciones.
- Use Azure AD Connect para lograr sus objetivos de identidad híbrida:
  - Un método de inicio de sesión que utiliza la sincronización de hash de contraseña.
  - La autenticación PassThrough permite a los usuarios utilizar la misma contraseña en las instalaciones y en la nube.
  - Habilite la integración de la federación para iniciar sesión en los servicios basados en Azure AD sin tener que volver a ingresar sus contraseñas.
  - Sincronización entre su entorno local y Azure AD.
  - Supervisión del estado con Azure AD Connect Health.

#### Notas del examen AZ-900:

Puede configurar Azure AD unirse durante una experiencia de primera ejecución de Windows 10 (*Todos los dispositivos con Windows 10 excepto Windows 10 Home*). Para verificar si un dispositivo está unido a su Azure AD, puede echar un vistazo a la **Acceder al trabajo o la escuela** diálogo en su dispositivo.



## Supervisión

- Supervise los patrones de uso y seguridad de su entorno con **Informes y supervisión de Azure AD**.
- Con **Azure AD Connect Health**, puede ver alertas, monitorear el rendimiento y verificar los análisis de uso de su Active Directory local y Azure AD.

## Seguridad

- Detecte vulnerabilidades potenciales y resuelva acciones sospechosas con **protección de identidad**.
- Azure AD PIM lo ayuda a controlar el acceso dentro de su organización.
- Puede utilizar valores predeterminados de seguridad para habilitar MFA en su organización.
- Habilitar **valores predeterminados de seguridad** lo protege de ataques comunes relacionados con la identidad.
- Tu usas **bloquear la autenticación heredada** si un usuario está utilizando una aplicación heredada.
- **Puntuación segura de identidad** le ayuda a verificar sus configuraciones si están alineadas con las mejores prácticas de seguridad de Microsoft.
- Puede bloquear a los intrusos que intentan adivinar las contraseñas de sus usuarios o usar métodos de fuerza bruta en Azure AD mediante **bloqueo inteligente**.
- Gestione, controle y supervise el acceso a recursos importantes de su organización con **Gestión de identidad privilegiada (PIM)**.

## Fuentes:

<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-whatis>

<https://azure.microsoft.com/en-us/services/active-directory/>



## Cortafuegos Azure

- Un servicio que usa una dirección IP pública estática para proteger sus recursos de VNet.
- Azure Firewall es compatible con PCI, SOC, ISO, ICSA Labs y HITRUST.

### Características

- Un servicio de firewall con estado.
- Puedes habilitar **tunelización forzada** para enrutar el tráfico vinculado a Internet a un firewall adicional o dispositivo de red virtual.
- Límite el tráfico de salida a un **FQDN** lista, incluidos los comodines.
  - Filtre cualquier tráfico saliente del protocolo TCP / UDP.
  - Para usar FQDN en sus reglas, debe habilitar el proxy DNS. Denegar el tráfico de una dirección IP maliciosa
- con **filtrado basado en inteligencia de amenazas**.
  - Tiene las reglas de mayor prioridad y siempre se procesará primero.
  - Modos de inteligencia de amenazas: desactivado, solo alerta, alerta y denegación
- Con un proxy DNS, un cortafuegos escucha el puerto 53 y reenvía las solicitudes DNS a un servidor DNS. Puede minimizar la complejidad
- de crear una regla de seguridad mediante un **Etiqueta de servicio**.
- Asocie hasta 250 direcciones IP públicas en su firewall. Es compatible con la traducción SNAT y DNAT.
  - SNAT: NAT de origen para el tráfico VNet saliente.
  - DNAT: NAT de destino para el tráfico de red entrante. C. Registros de
- diagnóstico de Azure Firewall (formato JSON):
  - Registro de reglas de aplicación
  - Registro de reglas de red
- Puede almacenar todos sus registros en una cuenta de almacenamiento, centros de eventos y registros del monitor de Azure. Métricas de Azure
- Firewall:
  - Recuento de aciertos de reglas de aplicación / red
  - Datos procesados
  - Rendimiento
  - Estado de salud del firewall
  - Utilización del puerto SNAT
- Para gestionar varios cortafuegos, puede utilizar **Administrador de firewall de Azure**.
- Proteja sus implementaciones de VDI mediante las reglas DNAT de firewall de Azure y el filtrado de inteligencia de amenazas.

### Precios

- Se le cobra por cada implementación de firewall
- Se le cobrará por los datos procesados por su firewall

### Fuentes:

<https://azure.microsoft.com/en-us/services/azure-firewall/>



<https://docs.microsoft.com/en-us/azure/firewall / descripción general>



## Protección contra DDoS de Azure

- Le permite proteger sus recursos de Azure contra ataques de denegación de servicio (DoS).
- La protección DDoS (capas 3 y 4) ofrece dos niveles de servicio: **Básico** y **Estándar**.

### Características

- **Básico**
  - Habilitado por defecto (gratis).
  - Mitiga los ataques de red comunes.
  - Tanto el básico como el estándar protegen las direcciones IP públicas IPv4 e IPv6.
- **Estándar**
  - Tiene capacidades avanzadas para protegerlo contra ataques a la red, como registro, alertas y telemetría.
  - Mitiga los siguientes ataques:
    - Ataques volumétricos: inundan la capa de red con ataques.
    - Ataques de protocolo: aproveche una debilidad en las capas 3 y 4.
    - Ataques de capa de recursos: un ataque de capa 7 que interrumpe la transmisión de datos entre hosts.
  - Le permite configurar alertas al inicio y finalización de un ataque. Los datos de métricas se conservan durante 30 días.
  - Proporciona políticas de mitigación autoajustadas (TCP / TCP SYN / UDP) para cada IP pública.

Característica	Básico	Estándar
Supervisión activa del tráfico y detección siempre activa	si	si
Ataque automático mitigaciones	si	si
Garantía de disponibilidad	Región Azure	Solicitud
Políticas de mitigación	Ajustado para el volumen de la región de tráfico de Azure	Ajustado para el volumen de tráfico de la aplicación
Métricas y alertas	No	Registros de recursos y métricas de ataques en tiempo real a través de Azure Monitor
Informes de mitigación	No	Mitigación posterior al ataque informes



Registros de flujo de mitigación	No	Flujo de registro NRT para integración SIEM
Política de mitigación personalización	No	Involucre a expertos en DDoS

#### Precios

- La protección básica DDoS brinda protección sin cargo adicional.
- La protección DDoS estándar es un servicio de pago. Se le cobrará por los datos procesados cada mes (por GB).

#### Fuente:

<https://azure.microsoft.com/en-us/services/ddos-protection/>

<https://docs.microsoft.com/en-us/azure/virtual-network/ddos-protection-overview>

<https://docs.microsoft.com/en-us/azure/security/fundamentals/ddos-best-practices>



## Centro de seguridad de Azure

- Administra todas las funciones de seguridad de Azure.
- Detecte vulnerabilidades, restrinja su exposición a amenazas y detecte y responda rápidamente a los ataques.
- **Puntuación segura de Azure** le permite obtener evaluaciones continuas y recomendaciones de seguridad. Le ayuda a detectar actividades inusuales y prevenir amenazas en sus cargas de trabajo de PaaS.
- Proteja sus máquinas virtuales con la gestión de la configuración y las vulnerabilidades, el refuerzo de la carga de trabajo y la EDR del servidor.
- También es compatible con el monitoreo avanzado para rastrear y administrar el cumplimiento y la gobernanza. Le permite proteger sus recursos utilizando niveles estándar o gratuitos.

## Conceptos

- Security Center muestra la **puntuación segura** de su cuenta. Cuanto mayor sea la puntuación, menor será el nivel de riesgo identificado.
- **Recomendaciones** ayudarlo a corregir posibles vulnerabilidades de seguridad en sus recursos de Azure.
- **Controles de seguridad** ayudarlo a implementar un conjunto de recomendaciones de seguridad. Después de corregir todas las recomendaciones, se reflejará en su puntuación de seguridad general.
- Para ayudar a cumplir con los requisitos de seguridad de su organización, puede definir una **política de seguridad** en sus cargas de trabajo.
- Puede investigar rápidamente el problema y recomendaciones sobre cómo remediar un ataque utilizando **alertas de seguridad**.
- Azure Security Center justo a tiempo ( **JIT** ) le permite bloquear el tráfico entrante a sus máquinas virtuales de Azure.

## Precios

- Con el nivel estándar, se le cobra
  - Por hora para máquinas virtuales, servicios de aplicaciones, base de datos SQL
  - Por transacciones para almacenamiento y mensajes de IoT
  - Por mes para dispositivos IoT
  - Por imagen para ACR
  - Por vCore / hora para AKS

## Fuentes:

<https://azure.microsoft.com/en-us/services/security-center/>

<https://docs.microsoft.com/en-us/azure/security-center/security-center-intro>



## Azure Key Vault

- Un servicio que le permite almacenar tokens, contraseñas, certificados y otros secretos.
- También puede crear y administrar las claves utilizadas para cifrar sus datos.

### Características

- **Eliminación suave** permite recuperar un almacén de claves eliminado y sus objetos durante el tiempo de retención que usted designe.
- El período de retención de una bóveda eliminada es de 7 a 90 días.
- Con eliminación suave y **protección de purga** habilitado, no purgará una bóveda u objeto en el estado eliminado hasta que haya expirado el período de retención.
- Puede conectarse a una bóveda de claves a través de
  - Un punto final público en todas las redes
  - Un punto final público en redes seleccionadas
  - Un punto final privado
- Comparta el acceso a sus aplicaciones y recursos sin revelar sus credenciales.

### Conceptos

- **UN inquilino** es una representación de una organización.
  - Azure Active Directory le permite publicar aplicaciones multiinquilino.
  - El inquilino de Azure Active Directory (B2C) representa una colección de identidades.
- **UN propietario de la bóveda** le permite crear un almacén de claves y configurar un registro de auditoría de quién tiene acceso a secretos y claves.
- **UN consumidor de bóveda** solo puede realizar acciones en los activos dentro de la bóveda de claves si el propietario de la bóveda otorga acceso al consumidor.
- Un elemento administrable en Azure se llama **recurso**, y **grupos de recursos** son contenedores que contienen recursos relacionados.
- **Principal de servicio** le da control sobre los recursos a los que se puede acceder. Al mismo tiempo, un **identidad gestionada** elimina la necesidad de crear y administrar entidades de servicio directamente, ya que proporciona a los servicios de Azure una identidad administrada automáticamente en Azure AD.
- Puede identificar una instancia de Azure AD dentro de su suscripción de Azure mediante un **ID de inquilino**.

### Precios

- Se le cobrará si la clave se ha utilizado al menos una vez en los últimos 30 días (*basado en la fecha de creación de la clave*).
- Se le cobra por cada versión histórica de una clave.

### Fuentes:

<https://docs.microsoft.com/en-us/azure/key-vault/general/overview>  
<https://azure.microsoft.com/en-us/services/key-vault/>



#### Protección de la información de Azure (AIP)

- Puede proteger sus documentos y correos electrónicos aplicando etiquetas. Se pueden aplicar etiquetas:
  - Automáticamente: administradores
  - Manualmente - usuarios
  - Por combinación - recomendaciones
- Le permite rastrear sus datos compartidos y revocar el acceso si es necesario. Configure políticas
- basadas en la confidencialidad de sus datos.
- Compartir datos con otras personas será seguro y usted tiene el control de quién puede editar, ver e imprimir. El contenido del etiquetado
- incluye:
  - Clasificación
  - Marcas visuales
  - Metadatos
- Puede utilizar etiquetas predeterminadas o etiquetas personalizadas. Las
- etiquetas de clasificación predeterminadas son:
  - Personal
  - General
  - Confidencial
  - Altamente confidencial

#### Fuentes:

<https://azure.microsoft.com/en-us/services/information-protection/>

<https://docs.microsoft.com/en-us/azure/information-protection/what-is-information-protection>



#### Protección contra amenazas avanzada de Azure (ATP)

- Le permite identificar, detectar e investigar amenazas avanzadas en su organización. Le permite monitorear las actividades y la información del usuario.
- Identifique e investigue amenazas avanzadas a lo largo de toda la cadena de eliminación de ataques ciberneticos:
  - **Reconocimiento** - identificar los intentos de los atacantes de obtener información.
  - **Credenciales comprometidas** - Se detectará cualquier intento que comprometa las credenciales del usuario.
  - **Movimientos laterales** - ataques para acceder a cuentas confidenciales.
  - **Dominio de dominio** - el atacante tiene las credenciales para acceder a su controlador de dominio.
  - **Exfiltración** - transferencia de datos no autorizada.
- También puede remediar ataques maliciosos con la Protección contra amenazas avanzada de Windows Defender.

#### Fuentes:

<https://azure.microsoft.com/en-us/features/azure-advanced-threat-protection/>  
<https://docs.microsoft.com/en-us/azure-advanced-threat-protection/what-is-atp>



## Centinela azur

- Una solución SIEM y SOAR nativa de la nube.
- Ofrece una vista panorámica de toda su empresa.
- Sentinel es un servicio inteligente de análisis de seguridad e inteligencia de amenazas que proporciona detección de alertas, visibilidad de amenazas, búsqueda proactiva y respuesta a amenazas.
- Métodos de conexión de datos en Sentinel: integración de servicio a servicio, soluciones externas a través de API y soluciones externas a través de un agente.
- Roles de Azure Sentinel: lector, respondedor y colaborador.

## Gestión de amenazas

- Sentinel ofrece las siguientes funciones: recopilar, detectar, investigar y responder.
- Obtenga información rápidamente sobre sus datos con Azure Sentinel **Libros de trabajo**.
- Investigar y resolver posibles amenazas con **incidentes grupos de alertas relacionadas**).
- Puede automatizar tareas y simplificar la orquestación de seguridad utilizando **libros de jugadas**.
- Sentinel proporciona **investigación profunda** herramientas para encontrar la causa raíz de una posible amenaza a la seguridad.
- **Caza** le permite encontrar problemas en sus datos.

## Precios

- La retención de datos se cobra después de 90 días.
- Se le cobrará por los datos ingeridos (por GB).

## Fuentes:

<https://docs.microsoft.com/en-us/azure/sentinel/overview>

<https://azure.microsoft.com/en-in/services/azure-sentinel/>



## Ofertas de cumplimiento de Microsoft

- **Centro de confianza de Microsoft** proporciona acceso a información sobre seguridad, privacidad y cumplimiento.
  - Seguridad: proporciona información sobre gestión de identidad y acceso, protección de información y amenazas, y seguridad en la nube.
  - Privacidad: proporciona información sobre cómo puede proteger sus datos en reposo y en tránsito.
  - Cumplimiento: proporciona información sobre requisitos específicos de la industria, informes de auditoría y responsabilidad compartida.
- **Declaración de privacidad de Microsoft** explica cómo Microsoft recopila datos personales, cómo los usa y las razones por las que necesitan compartir datos personales.
- Los términos y condiciones cuando compra licencias para productos y servicios en línea a través de los programas de licencias por volumen de Microsoft se documentan en **Términos de servicios en línea (OST)**.
- Los **Enmienda de protección de datos (DPA)** establece las responsabilidades del cliente y Microsoft con respecto a la recopilación y protección de los datos del cliente y los datos personales de acuerdo con Azure.

## Instituto Nacional de Estándares y Tecnología (NIST)

- NIST mantiene estándares de medición y orientación para ayudar a las organizaciones a evaluar el riesgo.
- NIST lanza un Marco para mejorar la ciberseguridad de la infraestructura crítica (FICIC) para fortalecer la ciberseguridad de las redes federales y las infraestructuras críticas.
- El Marco de Ciberseguridad (CSF) del NIST consta de estándares, pautas y mejores prácticas para gestionar los riesgos relacionados con la ciberseguridad.
- Cree rápidamente soluciones NIST CSF en Azure utilizando Azure Security and Compliance NIST CSF Blueprint.

## Reglamento general de protección de datos (GDPR)

- GDPR establece nuevas reglas para las organizaciones que ofrecen bienes y servicios a los ciudadanos en la Unión Europea.
- También recopila y analiza datos de residentes de la UE. El GDPR se aplica sin importar dónde se encuentre su empresa.
- GDPR otorga a las personas ciertos derechos para administrar los datos personales recopilados por una organización a través de una Solicitud de sujeto de datos (DSR).
- GDPR requiere que una organización proporcione información oportuna sobre DSR, violaciones de datos y que lleve a cabo evaluaciones de impacto de protección de datos (DPIA).

## Organización Internacional de Normalización (ISO)

- ISO proporciona estándares internacionales para proteger a los consumidores y usuarios finales de productos y servicios.
- La Comisión Electrotécnica Internacional (IEC) es una organización que prepara y publica estándares internacionales para tecnologías eléctricas, electrónicas y relacionadas.
- ISO / IEC 27001 es un estándar de gestión de seguridad de la información diseñado para llevar la seguridad de la información bajo un control de gestión explícito.



- Si a una empresa se le ha otorgado una certificación ISO, significa que ha establecido estándares y principios generales en el inicio, implementación, mantenimiento y mejora de la gestión de la seguridad de la información.
- Puedes usar **Portal de confianza de servicio** para proporcionar informes de cumplimiento auditados.

**Notas del examen AZ-900:**

Le sugerimos que lea la siguiente información antes de realizar el examen:

- La Declaración de privacidad de Microsoft le ayuda a comprender los datos personales que procesa Microsoft, cómo los procesa y con qué fines.
- Eche un vistazo al Centro de confianza de Microsoft si le preocupa la seguridad de los datos y cómo Microsoft cumple con los requisitos legales y de privacidad.
- Explore todos los informes de auditoría de los servicios de Microsoft Cloud sobre los estándares de protección de datos y los requisitos regulatorios en el Portal de confianza de servicios de Microsoft.

**Fuentes:**

<https://docs.microsoft.com/en-us/microsoft-365/compliance/offering-nist-csf?view=o365-worldwide>

<https://docs.microsoft.com/en-us/microsoft-365/compliance / gdpr? view = o365-worldwide>

<https://docs.microsoft.com/en-us/microsoft-365/compliance/offering-iso-27001?view=o365-worldwide>



## SEGUIMIENTO Y GESTIÓN

### Monitor de Azure

- Herramienta de monitoreo para sus recursos y aplicaciones de Azure.
- Un servicio para mostrar las métricas de sus recursos. También puede configurar alertas que envían notificaciones cuando se sobrepasa un umbral.

### Características

- Las métricas representan un conjunto de puntos de datos ordenados por tiempo que se publican en Azure Monitor.
- Las métricas recopiladas se almacenan durante un máximo de 93 días.
- Comparta sus paneles con otros usuarios mediante Azure Dashboards.
- Los datos se almacenan como un conjunto de registros en Log Analytics o Application Insights.
- Puedes utilizar **análisis de registros** para recopilar y almacenar los datos de varias fuentes de registro y utilizar un lenguaje de consulta personalizado para consultarlos.
- Application Insights lo ayuda a detectar y diagnosticar problemas en aplicaciones y dependencias.
- Cuando se encuentran condiciones importantes en sus datos de monitoreo, puede crear un **regla de alerta** para identificar y abordar problemas.
- Puede exportar métricas de uso básicas desde su punto final de CDN con registros de diagnóstico.

### Log Analytics

- Todos los datos de registro obtenidos por Azure Monitor se almacenarán en un área de trabajo de Log Analytics
- Consulta registros simples a avanzados.
- Los datos se recuperan de un espacio de trabajo mediante una consulta de registro escrita con Kusto Query Language (KQL).
- Si la consulta incluye espacios de trabajo en 20 regiones o más, se bloqueará la ejecución de su consulta.
- Los resultados de Log Analytics están limitados a un máximo de 10,000 registros.
- Con un agente de análisis de registros, puede recopilar registros y datos de rendimiento de dispositivos físicos o virtuales fuera de Azure.
- El agente de análisis de registros no puede enviar datos a Azure Monitor Metrics, Azure Storage o Azure Event Hubs.

### Perspectivas de la aplicación

- Le permite monitorear eventos y métricas personalizados.
- Supervise los registros de seguimiento de diagnóstico desde su aplicación.

### Precios

- Usted paga por la ingestión y retención de datos en Log Analytics (por GB / mes).
- Se le factura por la cantidad de métricas que tiene por mes.
- No hay cargos por alertas de criterios de salud.



---

**Fuentes:**

<https://docs.microsoft.com/en-us/azure/azure-monitor/overview>

<https://azure.microsoft.com/en-us/services/monitor/>



## Estado del servicio de Azure

- Le brinda una vista personalizada del estado de sus servicios y regiones de Azure. Azure Service Health se compone de tres servicios:
  - Estado de Azure: le informa de las interrupciones del servicio en Azure.
  - Service Health: le ayuda a tener una vista personalizada del estado de sus servicios en una región.
  - Estado de los recursos: proporciona información sobre el estado de sus recursos de Azure. Eventos activos en el
- estado del servicio:
  - Problemas de servicio
  - Mantenimiento planificado
  - Avisos de salud
  - Avisos de seguridad
- Realice un seguimiento de las alertas y los problemas en tiempo real y obtenga informes completos una vez resueltos.
- Puede configurar alertas para notificarle sobre problemas de servicio activos y futuros. Los usuarios de Azure pueden usar Service Health sin costo adicional.

## Fuentes:

<https://docs.microsoft.com/en-us/azure/service-health/overview>

<https://azure.microsoft.com/en-us/features/service-health/>



## Política de Azure

- Asegúrese de que los recursos cumplan con un conjunto de reglas.
- Administre sus políticas en una ubicación centralizada donde puede realizar un seguimiento de su estado de cumplimiento y verificar los recursos que no cumplen.
- Seleccionar entre **políticas integradas y políticas personalizadas**.
- Implementar barandas adecuadas y evaluar el cumplimiento en toda la organización Política frente a RBAC
- - Una política mantiene el cumplimiento del estado del recurso, mientras que RBAC se centra en controlar las acciones del usuario en diferentes ámbitos.
  - Incluso si el usuario tiene acceso para realizar una acción, si el resultado es un recurso que no cumple con las normas, la política seguirá bloqueando la opción de creación o actualización.
- El formato JSON se utiliza para crear una política.
- Puede gestionar la evaluación y el resultado con **proveedor de recursos**, y los resultados se informan a Azure Policy.
  
- Orden de evaluación de la política: deshabilitado, agregar / modificar, denegar y auditar los efectos de la política de
- Azure:
  - Agregar: agrega campos adicionales al recurso solicitado.
  - Auditoría: un evento de advertencia para un recurso no conforme.
  - AuditIfNotExists: audita los recursos cuando se cumple la condición.
  - Denegar: evita que la solicitud antes de enviarse al proveedor de recursos.
  - DeployIfNotExists: si se cumple la condición, le permite ejecutar una implementación de plantilla.
  - Deshabilitado: le permite deshabilitar una sola asignación, en lugar de deshabilitar todas las asignaciones bajo esa política.
  
  - Modificar: administrar etiquetas de recursos. Determine los recursos
- asignados con **asignaciones de políticas**.

## Fuentes:

<https://azure.microsoft.com/en-us/services/azure-policy/>

<https://docs.microsoft.com/en-us/azure/governance/policy/overview>



## Asesor de Azure

- Advisor analiza sus configuraciones y ofrece recomendaciones personalizadas y prácticas. Proporciona las mejores prácticas relevantes para ayudarlo a mejorar:
  - Costo
  - Seguridad
  - Fiabilidad
  - Excelencia operativa
  - Actuación
- Las recomendaciones de acceso están disponibles sin costo adicional.

The screenshot shows the Azure Advisor Overview page. On the left, there's a sidebar with sections like Recommendations (Cost, Security, Reliability, Operational Excellence, Performance, All recommendations), Monitoring (Alerts (Preview), Recommendation digests), and Settings (Configuration). The main area has five cards:

- Cost**: You are following all of our cost recommendations. See list of cost recommendations.
- Security**: 2 Recommendations. 2 High impact, 0 Medium impact, 0 Low impact. 1 Impacted resource.
- Reliability**: You are following all of our reliability recommendations. See list of reliability recommendations.
- Operational Excellence**: You are following all of our operational excellence recommendations. See list of operational excellence recommendations.
- Performance**: You are following all of our performance recommendations. See list of performance recommendations.

## Fuentes:

<https://azure.microsoft.com/en-us/services/advisor/>

<https://docs.microsoft.com/en-us/azure/advisor/advisor-overview>



## Blueprints de Azure

- Crea plantillas para entornos de Azure estándar y repetibles que cumplen con los requisitos de cumplimiento y los estándares operativos de una organización.
- Admite los siguientes recursos como artefactos:
  - Asignaciones de roles
  - Asignaciones de políticas
  - Plantillas de Azure Resource Manager (ARM)
  - Grupos de recursos
- Proporciona **bloqueo de recursos** para evitar cambios no deseados.
- Un Blueprint puede tener sus propios parámetros, pero estos solo se pueden crear si se desarrolla un Blueprint desde la API REST en lugar de Azure Portal.
- Rol de blueprints: propietario, colaborador, colaborador de blueprint, operador de blueprint
- Con Blueprints, tiene una ubicación centralizada para la administración del entorno, incluida la implementación, el control de versiones y la actualización.
- Si sus suscripciones están en el mismo Blueprint de Azure, puede actualizar varias suscripciones a la vez. También puede utilizar Blueprints para configurar grupos de recursos dentro de las suscripciones.
- Configure varios entornos dentro del mismo entorno compartido, cuando asigna un Blueprint a una suscripción.

## Fuentes:

<https://docs.microsoft.com/en-us/azure/governance/blueprints/overview>

<https://azure.microsoft.com/en-us/services/blueprints/>



#### Administrador de cumplimiento de Azure

- Un panel y una herramienta de supervisión que resume la protección de datos, la puntuación de cumplimiento y las recomendaciones.
- Le permite asignar, rastrear y registrar el cumplimiento y las actividades relacionadas con la evaluación. Recomendaciones para regulaciones de la industria: **GDPR, ISO, y NIST**
- Puede cargar y administrar artefactos o pruebas en un repositorio seguro.

#### Fuentes:

<https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/govern/policy-compliance/regulatory-compliance>

<https://docs.microsoft.com/en-us/microsoft-365/compliance/meet-data-protection-and-regulatory-reqs-usingmicrosoft-cloud>



## Azure RBAC

- Un servicio de control de acceso basado en roles para administrar el acceso de los usuarios a los recursos de Azure, incluido lo que pueden hacer con esos recursos y las áreas a las que pueden acceder.
- Es un sistema de autorización basado en **Administrador de recursos de Azure**, que proporciona una gestión de acceso precisa de los recursos de Azure.

### Conceptos

- Un rol La asignación se compone del principal de seguridad, la definición de funciones y el alcance.
  - **Director de seguridad** - un objeto que representa un usuario, grupo, entidad de servicio e identidad administrada que solicita acceso a los recursos de Azure.
  - **Definición de rol** - una lista de permisos que se pueden realizar, como leer, escribir y eliminar.
  - **Alcance** - conjunto de recursos a los que se aplica el acceso.
- Adjuntar una definición de rol a un usuario, grupo, entidad de servicio e identidad administrada para otorgar acceso a un ámbito particular se llama **asignación de roles**.
- Puede adjuntar múltiples asignaciones de roles ya que RBAC es un modelo aditivo. Azure RBAC admite asignaciones tanto para permitir como para denegar.

### Roles

- Azur Roles: Azure RBAC tiene más de 70 roles integrados. Los siguientes son los cuatro roles fundamentales de Azure: Propietario
  - 
  - Contribuyente
  - Lector
  - Administrador de acceso de usuario
- Azur Roles de AD: brinde acceso para administrar los recursos de Azure AD en un directorio como crear usuarios, asignar roles administrativos a otros, administrar licencias, restablecer contraseñas y administrar dominios.

Roles de Azure	Roles de Azure AD
Administre el acceso a los recursos de Azure.	Administre el acceso a los recursos de Azure Active Directory (Active AD).
Admite roles personalizados.	Admite roles personalizados.
El alcance se puede especificar en varios niveles (grupo de administración, suscripción, grupo de recursos, recurso).	El alcance es solo a nivel de inquilino.



Se puede acceder a la información de roles a través de Azure Portal, CLI, PowerShell, plantillas de Resource Manager y API REST.	Se puede acceder a la información del rol a través del Portal de administración de Azure, el Centro de administración de Microsoft 365, Microsoft Graph y Azure AD PowerShell.
--	--

#### Mejores prácticas

- Use Azure RBAC para separar las tareas dentro de su equipo y otorgue solo el acceso que necesitan sus usuarios.
- Limite el número de propietarios de suscripciones (*máximo de 3*) para reducir el potencial de incumplimiento por parte de un propietario comprometido.
- Puede usar Azure AD PIM para proteger cuentas privilegiadas de ciberataques malintencionados.

#### Fuente:

<https://docs.microsoft.com/en-us/azure/role-based-access-control/overview>



## SOLUCIONES

### Azure Internet de las cosas (IoT)

- Un servicio que le permite conectar, monitorear y controlar uno o más dispositivos de IoT que pueden comunicarse con servicios de back-end alojados en la nube.

#### Azur IoT Hub

- Una solución PaaS que proporciona un control completo sobre la recopilación y el procesamiento de datos de IoT.
- Para crear una solución completa de un extremo a otro, puede integrar IoT Hub con otros servicios de Azure.
  - Cuadrícula de eventos de Azure
  - Aplicaciones de Azure Logic
  - Aprendizaje automático de Azure
  - Azure Stream Analytics
- La integración del enruteamiento de mensajes lo ayuda automáticamente a responder a un cambio de estado informado por el dispositivo. Puede usar el escalado de IoT Hub si se está acercando al límite de mensajes en su IoT Hub.

#### Azur IoT Central

- Una solución SaaS que proporciona una colección de plantillas de aplicaciones específicas de la industria.
- Puede crear su propia plantilla de dispositivo para definir las características y el comportamiento de un dispositivo. Configure paneles personalizados para monitorear el estado y la telemetría de su dispositivo. Cree reglas personalizadas cuando la telemetría del dispositivo cruce un umbral específico.
- Puede aplicar actualizaciones individuales o masivas creando trabajos.

#### Azur Esfera

- Una solución de seguridad de IoT que lo ayuda a proteger sus datos, privacidad e infraestructura. Componentes:
  - Chip Azure Sphere: una unidad de microcontrolador que proporciona capacidades de procesamiento en tiempo real.
  - Azure Sphere OS: un sistema operativo basado en Linux que se ejecuta en un chip Azure Sphere.
  - Servicio de seguridad Azure Sphere: admite autenticación basada en certificados, actualizaciones automáticas de software e informes de errores. De forma predeterminada, los datos se cifran en reposo.
- Los dispositivos Azure Sphere pueden ejecutarse en dos tipos de aplicaciones:
  - Aplicaciones de alto nivel para contenedores.
  - Aplicaciones con capacidad en tiempo real (RTApps) para metales desnudos.

#### Azur Productos de IoT

- Los aceleradores de soluciones de Azure IoT le permiten personalizar plantillas de soluciones para escenarios comunes de IoT. Azure IoT Edge le permite implementar análisis en la nube y lógica empresarial personalizada de forma local en dispositivos de borde de IoT.
- Cree gráficos de conocimiento basados en modelos digitales de entornos completos con Azure Digital Twins.



- Si necesita monitorear, analizar y visualizar sus datos de IoT en tiempo real, puede usar Azure Time Series Insights.
- Un sistema operativo en tiempo real para dispositivos IoT, con tecnología de MCU, se llama Azure RTOS. Azure SQL Edge es un motor de base de datos SQL optimizado para implementaciones de IoT e IoT Edge.

**Fuentes:**

<https://docs.microsoft.com/en-us/azure/iot-hub/about-iot-hub>

<https://docs.microsoft.com/en-us/azure/iot-central/core/overview-iot -central>

<https://azure.microsoft.com/en-us/product-categories/iot/>



## Azure Big Data

- Un servicio para almacenar y procesar grandes cantidades de conjuntos de datos. Utilizar **Análisis de Azure Data Lake** para escribir consultas que lo ayuden a transformar sus datos y extraer información valiosa.
  - Ofrece escalado dinámico y paralelismo de datos.
  - Puede integrar Data Lake Analytics con Active Directory para administrar los permisos de los usuarios. Cree clústeres de
- big data para Hadoop, Spark y Kafka con **Azure HDInsight**.
  - Reduzca los costos aumentando y reduciendo sus cargas de trabajo.
  - Supervise todos sus clústeres con Azure Monitor.
- **Azure Databricks** se basa en las capacidades de Apache Spark que proporcionan un espacio de trabajo interactivo y flujos de trabajo optimizados.
  - Le permite leer datos de varias fuentes y utilizar Spark para crear conocimientos innovadores.
- **Análisis de Azure Synapse** es un servicio de almacenamiento de datos y análisis de big data.
  - Le permite ingerir, preparar, administrar y entregar datos para las necesidades de BI y ML.

### Notas del examen AZ-900:

Azure Synapse Analytics se conocía anteriormente como *Almacén de datos SQL de Azure*. Incluye pool SQL como solución de almacenamiento de datos. Esta plataforma también combina exploración de datos, ingestión, transformación, preparación y una capa de análisis de servicio.

- Puedes usar **Azure Event Hubs** para el servicio de transmisión de big data e ingestión de eventos.
  - Le permite recibir y procesar millones de eventos por segundo.
- **Azure Stream Analytics** le proporciona análisis en tiempo real y un motor de procesamiento de eventos complejo.
  - Analice y procese simultáneamente grandes volúmenes de datos de transmisión de múltiples fuentes.

### Fuentes:

<https://docs.microsoft.com/en-us/azure/data-lake-analytics/data-lake-analytics-overview>

<https://docs.microsoft.com/en-us/azure/hdinsight/hdinsight-overview>

<https://docs.microsoft.com/en-us/azure/databricks/scenarios/what-is-azure-databricks>

<https://docs.microsoft.com/en-us/azure/synapse-analytics/sql-data-warehouse/sql-data-warehouse-overviewwhat-is>

<https://docs.microsoft.com/en-us/azure/event-hubs/event-hubs-about>

<https://docs.microsoft.com/en-us/azure/stream-analytics/stream-analytics-introduction>



## Aprendizaje automático de Azure

- Un servicio para entrenar, implementar, automatizar, administrar y rastrear modelos de aprendizaje automático. Ofertas de Azure ML Básico y Empresa ediciones.
- Puedes usar **Azure ML SDK para Python**, **Azure ML Studio**, y **ML CLI** para gestionar sus modelos desplegados. Puede automatizar y acelerar el ciclo de vida del AA mediante **MLOps**.
- 
- Azure ML **diseñador** le permite conectar visualmente (arrastrar y soltar) conjuntos de datos y módulos sin escribir ningún código.
- ML **oleoductos** proporcionan un flujo de trabajo lógico completo y una secuencia ordenada de pasos.
- **AutoML** utiliza la métrica de destino que específicas para entrenar y ajustar un modelo.
- **Servicios cognitivos de Azure** permite a los desarrolladores crear aplicaciones cognitivas inteligentes sin tener habilidades de inteligencia artificial o ciencia de datos. Las siguientes son las API de REST cognitiva de Azure que puede usar:
  - API de visión, habla, lenguaje, búsqueda y decisión.

## Azur Servicio de bot

- Cree un bot que utilice el lenguaje natural y las capacidades del habla para comunicarse con sus usuarios. Puede integrar Bot Service
- a través de múltiples canales de comunicación como Microsoft Teams, Slack y Facebook Messenger.
- Utilice Bot Framework Composer si necesita un lienzo de edición visual para los flujos de conversación.
- Con Bot Framework SDK, puede crear un bot que use el habla, comprenda el lenguaje natural y maneje preguntas y respuestas.

## Fuentes:

<https://docs.microsoft.com/en-us/azure/machine-learning/overview-what-is-azure-ml>

<https://azure.microsoft.com/en-us/services/machine-learning/>



## Azure sin servidor

- Le permite crear aplicaciones sin administrar la infraestructura.

### Azur Funciones

- Le permite ejecutar un pequeño fragmento de código para realizar una tarea. Se
- realiza una única tarea para cada invocación.
- Idiomas admitidos: C #, Java, JavaScript, Python y PowerShell
- Puede ejecutar su código según las solicitudes HTTP o programar cuándo se ejecuta su función. Solo se le cobra por el tiempo que ejecuta su código.

### Azur Aplicaciones lógicas

- Le permite automatizar sus flujos de trabajo sin escribir una sola línea de código. Cree su flujo de trabajo con un
- diseñador de aplicaciones lógicas.
- Componentes:
  - **Flujo de trabajo** le ayuda a crear una serie de pasos para su aplicación lógica.
  - **Conectores gestionados** le permiten acceder a sus datos y trabajar con ellos.
  - **Desencadenar** es el primer paso para ejecutar su aplicación lógica.
  - **Comportamiento** son pasos que ocurren después del disparador y realizan tareas en el flujo de trabajo de su aplicación lógica.
- **Paquete de integración empresarial** le permite crear un flujo de trabajo de integración empresarial automatizado y escalable.

### Azur Cuadrícula de eventos

- Una red para enrutar eventos entre aplicaciones Enrutar eventos
- personalizados a diferentes puntos finales. Componentes:
  - **Eventos** - La información que sucedió en el sistema.
  - **Fuentes de eventos** - De donde viene el evento.
  - **Temas** - Proporciona un punto final al que el editor envía eventos.
  - **Suscripciones a eventos** - Filtra los eventos que te envían.
  - **Controladores de eventos** - El servicio que procesará el evento.
- Debe proporcionar un token SAS o autenticación de clave antes de publicar un tema.

### Fuentes:

<https://docs.microsoft.com/en-us/azure/azure-functions/functions-overview>

<https://docs.microsoft.com/en-us/azure/logic-apps/logic-apps-overview>

<https://docs.microsoft.com/en-us/azure/event-grid/overview>



## Azure DevOps

- Un servicio que ofrece un conjunto de herramientas para planificar, construir e implementar aplicaciones.

### Características

- **Azur Tableros**
  - Le permite realizar un seguimiento de las características, historias de usuarios, tareas y errores asociados con su proyecto.
  - También puede personalizar sus paneles y realizar un seguimiento del progreso fácilmente durante el ciclo de vida de su proyecto.
- **Azur Oleoductos**
  - Un servicio de CI / CD que le ayuda a crear y probar su código automáticamente. Le permite implementar sus códigos en múltiples objetivos al mismo tiempo.
- **Azur Reposiciones**
  - Almacene y administre sus códigos utilizando un conjunto de herramientas de control de versiones.
  - Admite un sistema de control de versiones para realizar un seguimiento de cada cambio que realizó en su código.
- **Azur Planes de prueba**
  - Una solución de gestión de pruebas que admite la trazabilidad de un extremo a otro. Ejecute pruebas simultáneamente utilizando sesiones de prueba exploratorias.
- **Azur Artefactos**
  - Le permite crear, alojar y compartir su código / paquetes con su equipo u otra organización. Puede compartir su código almacenando paquetes Maven, npm, NuGet y Python juntos.

### Azur Laboratorios DevTest

- Un espacio aislado de autoservicio que le ayuda a crear entornos de desarrollo y pruebas.
- Puede aprovisionar rápidamente diferentes entornos mediante el uso de artefactos y plantillas reutilizables.
- También tiene una función de administración de costos para rastrear sus VM y recursos PaaS para mantenerse dentro del presupuesto asignado.

### Acciones de GitHub para Azure

- Automatiza los flujos de trabajo de desarrollo de software.
- UN **flujo de trabajo** le permite crear, probar, empaquetar, lanzar e implementar proyectos en Azure.
- Cada flujo de trabajo se compone de acciones individuales que se ejecutan después de un evento en particular. Estas **comportamiento** se definen en archivos YAML.
- Puede encontrar todas las acciones disponibles en Marketplace for GitHub Actions for Azure.

### Fuentes:

<https://docs.microsoft.com/en-us/azure/devops/user-guide/what-is-azure-devops?view=azure-devops>

<https://azure.microsoft.com/en-us/services / devops />



## OTRAS NOTAS AZURAS

### Bus de servicio de Azure

- Un servicio de intermediario de mensajes totalmente gestionado.
- Le permite desacoplar aplicaciones y servicios.
- Proporciona una plataforma confiable y segura para datos asincrónicos y transferencia de estado.
- Le permite enviar mensajes a varios suscriptores y distribuir mensajes en forma de abanico a los sistemas posteriores.

### Características

- **Sesiones de mensajes** para implementar primero en entrar, primero en salir (FIFO) y patrones de solicitud-respuesta para asegurar el orden de los mensajes en la cola.
- **Reenvío automático** le permite eliminar mensajes de una cola o suscripción y transferirlos a una cola o tema diferente (*debe estar en el mismo espacio de nombres*).
- Una cola de mensajes no entregados contiene los mensajes que no se pueden entregar a ningún receptor.
- Admite una entrega programada de mensajes.
- Puede apartar un mensaje usando **aplazamiento del mensaje**.
- Con **procesamiento por lotes del lado del cliente**, puede retrasar el envío de mensajes durante un cierto período de tiempo.
- **Autodelete en inactivo** le permite establecer un intervalo de inactividad para eliminar automáticamente una cola. Cinco minutos es la duración mínima.
- **Detección de duplicados** le permite reenviar el mismo mensaje y descartar cualquier copia duplicada.
- Puede continuar la operación de su entorno en una región o centro de datos diferente con **recuperación ante desastres geográficos**.

### Componentes

- Un contenedor para todos los componentes de mensajería se denomina **espacio de nombres**.
- Envías y recibes mensajes de **colas** (*comunicación punto a punto*).
- Se admiten varias colas y temas en un solo espacio de nombres, y los espacios de nombres a menudo sirven como contenedores de aplicaciones.
- **Temas** también le permite enviar y recibir mensajes y se utiliza principalmente en escenarios de publicación / suscripción. Contiene múltiples suscripciones independientes llamadas **entidades**.
- Para filtrar mensajes específicos, puede usar reglas y filtros para definir condiciones que desencadenan acciones opcionales.

### Seguridad

- **Firmas de acceso compartido (SAS)** protege el acceso a Service Bus según las reglas de autorización.
- Puede autenticar y autorizar una aplicación para acceder a entidades de Service Bus, como colas, temas, suscripciones y filtros mediante **Azure AD**.



- Crea una identidad de seguridad usando **Identidades administradas para recursos de Azure** y asociar esa identidad con roles de control de acceso para otorgar permisos personalizados para acceder a recursos específicos de Azure.

#### Precios

- Se le cobrará en función de lo siguiente:
  - El número de operaciones
  - La cantidad de conexiones AMQP o llamadas HTTP
- Para las conexiones híbridas, se le cobra en función del número de oyentes.
- Con las retransmisiones de Windows Communication Foundation (WCF), se le cobra según el volumen de mensajes y las horas de retransmisión.

#### Fuentes:

<https://azure.microsoft.com/en-us/services/service-bus/>

<https://docs.microsoft.com/en-us/azure/service-bus-messaging/service-bus-messaging-overview>



## COMPARACIÓN DE SERVICIOS AZURE

### Azure Virtual Machines vs aplicación web

	Máquina virtual de Azure	Aplicación web de Azure
Descripción	Infraestructura como servicio, si necesita tener un control total sobre su computación ambiente.	Plataforma como servicio, te permite integrar la aplicación sin gestionando el subyacente infraestructura.
Desplegar	Utiliza una imagen del sistema operativo.	Utiliza una pila en tiempo de ejecución.
Administración del Estado	Con estado o sin estado	Apátrida
Ajuste de escala automático	Debe usar conjuntos de escalado de VM para admitir el ajuste de escala automático en máquinas virtuales.	El ajuste de escala automático es un servicio integrado en App Service.
Límite de escala	1000 nodos por juego de básculas para imagen de plataforma y 600 nodos 20 instancias y 100 con aplicación por escala imagen	Entorno de servicio
Distribución del tráfico	Distribuir lo entrante tráfico de red con el equilibrador de carga de Azure.	El equilibrio de carga está integrado en App Service.
Estilos de arquitectura	La arquitectura soportada los estilos son N-Tier y Web-Queue-Worker.	Los estilos de arquitectura admitidos son N-Tier y Big Compute (HPC).



## Azure Container Instances (ACI) frente a Azure Kubernetes Service (AKS)

	ACI	AKS
<b>Descripción</b>	Ejecute contenedores sin administrar servidores.	Organice y gestione múltiples imágenes y aplicaciones de contenedores.
<b>Despliegue</b>	Para aplicaciones impulsadas por eventos, implemente rápidamente desde su contenedor canalizaciones de desarrollo, ejecutar el procesamiento de datos y crear trabajos.	Utiliza clústeres y pods para escalar e implementar aplicaciones.
<b>Aplicaciones web (Monolítico)</b>	si	si
<b>Aplicaciones de N-Tier (Servicios)</b>	si	si
<b>Nativo de la nube (Microservicios)</b>	si	Sí, recomendado para contenedores de Linux
<b>Lote / Trabajos (Antecedentes Tareas)</b>	si	si
<b>Casos de uso</b>	<ul style="list-style-type: none"><li>● Escenarios de desarrollo / prueba</li><li>● Automatización de tareas</li><li>● Agentes de CI / CD</li><li>● Lote a pequeña escala</li><li>● Procesando</li><li>● Aplicaciones web simples</li></ul>	<ul style="list-style-type: none"><li>● Contenedores y aplicación portabilidad de la configuración</li><li>● Le permite seleccionar la cantidad de hosts, tamaño y herramientas de orquestador</li><li>● Transferir cargas de trabajo de contenedores a la nube sin cambiar tu corriente</li><li>● Prácticas de manejo.</li></ul>
<b>Diferencia mayor</b>	Debe usar AKS si necesita una orquestación completa de contenedores, como el descubrimiento de servicios en varios contenedores, el escalado automático y las actualizaciones de aplicaciones coordinadas.	



#### Azure Functions frente a Logic Apps frente a Event Grid

	Funciones	Aplicaciones lógicas	Cuadrícula de eventos
Servicio	Computación sin servidor	Flujos de trabajo sin servidor	Eventos sin servidor
Descripción	Ejecute un pequeño fragmento de código para realizar una tarea	Automatiza tus flujos de trabajo sin escribir una sola línea de código.	Enrute eventos personalizados a diferentes puntos finales.
Características	<ul style="list-style-type: none"><li>• Sin servidor aplicaciones</li><li>• Elección de idioma</li><li>• Trae tu propio dependencias</li><li>• Integrado seguridad</li><li>• Flexible desarrollo herramientas</li><li>• Con estado sin servidor arquitectura</li></ul>	<ul style="list-style-type: none"><li>• Integrado y gestionado conectores</li><li>• Controla tus flujos de trabajo</li><li>• Administrar o manipular datos</li><li>• Aplicación, datos y sistema integración</li><li>• Empresa solicitud integración</li><li>• B2B comunicación en la nube o En las instalaciones</li></ul>	<ul style="list-style-type: none"><li>• Filtrado avanzado</li><li>• Abanico a múltiple puntos finales</li><li>• Apoyos alto volumen cargas de trabajo</li><li>• Eventos integrados</li><li>• Eventos personalizados</li></ul>
Desarrollo	Código primero	Diseñador- primero	Fuente de evento y Manipuladores
Caso de uso	Procesamiento de Big Data, referencia de microservicios y arquitectura de vanguardia, y sistemas con prefabricados conectores. mensajería sin servidor	Conecte el legado, lo moderno, y sistemas con prefabricados conectores.	Aplicación sin servidor arquitecturas, Operaciones Automatización y Integración de aplicaciones
Precios	Solo se le cobra por código.	Se le ejecuta su el tiempo que ejecuta su ejecución de disparadores, acción y conectores.	Se le cobrará por cada operación, como eventos de ingreso, avanzado partidos, entrega intentos, y gestión de llamadas.



#### Conjunto de escala de Azure frente a conjunto de disponibilidad

	Conjunto de escala	Conjunto de disponibilidad
<b>Descripción</b>	Un grupo de máquinas virtuales con configuración idéntica distribuidas en dominios de falla.	Un grupo de máquinas virtuales discretas distribuidas en dominios de fallas.
<b>Cargas de trabajo</b>	Utilice Scale Set para cargas de trabajo impredecibles (autoescala).	Utilice el conjunto de disponibilidad para cargas de trabajo predecibles.
<b>Dominio predeterminado</b>	Tiene 5 dominios de falla y 5 actualizaciones. Tiene 3 dominios predeterminada	de falla y 5 dominios de actualización de forma dominios por defecto
<b>Configuración</b>	Las máquinas virtuales se crean a partir de la misma imagen y configuración.	Las máquinas virtuales se crean a partir de diferentes imágenes y configuraciones.
<b>Distribución</b>	Los conjuntos de escalado de máquinas virtuales se pueden distribuir en un solo centro de datos o en varios datos distribuidos dentro de un centro de datos.	Las máquinas virtuales son automáticamente distribuidas entre los centros de datos.
<b>Cantidad de VM</b>	Los conjuntos de escalas pueden aumentar el número de máquinas virtuales en función del conjunto de disponibilidad cuando se solicita.	Solo puedes agregar una máquina virtual al conjunto de disponibilidad cuando se solicita.
<b>Precios</b>	Los juegos de básculas no tienen cargo adicional. Solo paga por los recursos informáticos.	El conjunto de disponibilidad no tiene cargo adicional. Solo paga por los recursos informáticos.



#### Azure Blob vs disco vs almacenamiento de archivos

	Almacenamiento de blobs	Almacenamiento de disco	Almacenamiento de archivos
<b>Tipo de almacenamiento</b>	Almacenamiento de objetos para almacenar todo tipo de formatos de datos. máquinas.	Almacenamiento en bloque para el sistema de archivos virtual en todo las máquinas.	
<b>Almacenamiento máximo Talla</b>	Igual que el máximo cuenta de almacenamiento capacidad	65.536 GiB para ultra disco 32.767 GiB para estándar y unidades premium	Escale hasta 100 TiB
<b>Tamaño máximo de archivo</b>	190,7 TiB para blob en bloque Equivalente al 195 GiB para agregar el tamaño máximo de blob de sus volúmenes 8 TiB para blob de página		4 TiB para un solo archivo
<b>Actuación (Rendimiento)</b>	500 solicitudes por segundo Hasta blob	2000 MBps por para un solo disco.	6,204 MiB / s para salida 4.136 MiB / s para el ingreso
<b>Datos Accediendo</b>	Se puede acceder a los objetos Una sola HTTP.	Una máquina virtual a través de HTTP / en una sola AZ.	Comparta sus archivos de forma local o en la nube.
<b>Cifrado Métodos</b>	Cifre sus datos con Azure SSE (AES de 256 bits)	SSE por servicio de almacenamiento y ADE para SO y discos de datos.	Cifre sus datos con Azure SSE (AES de 256 bits)
<b>Copia de seguridad y Restauracion</b>	Control de versiones, instantáneas y replicación de objetos	Puede realizar una copia de seguridad de sus discos administrados en cualquier momento mediante instantáneas.	Utiliza archivo compartido instantáneas
<b>Precios</b>	Se le factura en función de los datos almacenados por mes, operaciones realizado, transferencia de datos, de redundancia.	Usted paga por el tamaño del disco, los GiB aprovisionados por instantáneas y el número de mes y el número de transacciones. y	Pagas por el número de servidores conectados al punto final de la nube.
<b>Casos de uso</b>	Sitio web estático, medios y archivos de registro, copias de seguridad, cargas de trabajo analíticas	Volúmenes de arranque y intensivo en transacciones cargas de trabajo	Ubicación central de sus archivos, registros de seguimiento y aplicaciones



Almacenamiento con redundancia local (LRS) frente a almacenamiento con redundancia de zona (ZRS) frente a (GRS)

	Localmente redundante Almacenamiento (LRS)	Zona redundante Almacenamiento (ZRS)	Almacenamiento con redundancia geográfica (GRS)
Replicación	Replica sus datos 3 veces en una sola ubicación física sincrónicamente en el región primaria.	Replica tus datos en 3 Azure Zonas de disponibilidad sincrónicamente en el región primaria	Replica sus datos en su cuenta de almacenamiento a una región secundaria
Redundancia	Bajo	Moderar	Alto
Costo	Proporciona lo mínimo replicación cara opción	Cuesta más que LRS pero proporciona mayor disponibilidad	Cuesta más que ZRS pero ofrece disponibilidad en caso de cortes regionales
Porcentaje de durabilidad de Al menos objetos sobre un determinado año	Al menos 99,99999999% (11 9's)	Al menos 99,999999999% (12 9's)	Al menos 99,9999999999999% (16 9)
SLA de disponibilidad para leer solicitudes	Al menos 99,9% (99% para Al menos frío)	99,9% (99% para el nivel de acceso genial)	Al menos el 99,9% (99% para el nivel de acceso frío) para GRS  Al menos el 99,99% (99,9% para el nivel de acceso frío) para RA-GRS
SLA de disponibilidad para escribir solicitudes	Al menos 99,9% (99% para Al menos frío)	99,9% (99% para Al menos 99,9% (99% para el nivel de acceso frío) nivel de acceso genial)	99,9% (99% para el nivel de acceso genial)
¿Disponible si un nodo se cayó dentro de un centro de datos?	sí	sí	sí
Disponible si todo el centro de datos (zonal o no zonal) fue abajo?	No	sí	sí



Disponible en interrupción en toda la región en No la región primaria?		No	sí
Tiene acceso de lectura a la región secundaria si la región principal no está disponible?	No	No	sí
Almacenamiento compatible tipos de cuenta	V2 de uso general V1 de uso general Almacenamiento de blobs en bloque Almacenamiento de blobs Almacenamiento de archivos	V2 de uso general Almacenamiento de blobs en bloque Almacenamiento de archivos	V2 de uso general V1 de uso general Almacenamiento de blobs



#### Azure Load Balancer frente a App Gateway frente a Traffic Manager

	Balanceador de carga	Puerta de enlace de la aplicación	Gerente de tráfico
<b>Servicio</b>	Equilibrador de carga de red.	Balanceador de carga de tráfico web.	Carga de tráfico basada en DNS balancín.
<b>Red Protocolos</b>	Capa 4 (TCP o UDP)	Capa 7 (HTTP / HTTPS)	Capa 7 (DNS)
<b>Características</b>	Equilibrador de carga interno y público	Terminación SSL / TLS y sesión basada en cookies a affinidad	Métodos de enrutamiento de tráfico, Perfil del gestor de tráfico, monitoreo de endpoint opciones
<b>Enrutamiento</b>	Origen / Destino (IP y Puerto) y Protocolo	Ruta URI o encabezados de host	Ofrece varias rutas métodos como: Prioridad, ponderada, Actuación, Geográfico, multivalor y subred
<b>Seguridad</b>	Integrar Azure Firewall con Standard LB.	Perfil del administrador de tráfico de Web	Use candados para proteger su Application Firewall.



#### Grupo de seguridad de red (NSG) frente al grupo de seguridad de aplicaciones

	Grupo de seguridad de red	Grupo de seguridad de aplicaciones
Descripción	Se utiliza un grupo de seguridad de red para hacer cumplir y controlar el tráfico de la red.	Un grupo de seguridad de la aplicación es una referencia de objeto dentro de un NSG.
Características	Controla el tráfico entrante y saliente a nivel de subred.	Controla el tráfico entrante y saliente a nivel de interfaz de red.
Reglas	Las reglas se aplican a todos los recursos de la subred asociada.	Las reglas se aplican a todos los ASG en la misma red virtual.
Dirección	Tiene reglas separadas para el tráfico entrante y saliente.	Tiene reglas separadas para el tráfico entrante y saliente.
Límites	NSG tiene un límite de 1000 reglas.	Los ASG que se pueden especificar dentro de todas las reglas de seguridad de un NSG tienen un límite de 100 reglas.
Acción	Apoyos PERMITIR y NEGAR reglas.	Apoyos PERMITIR y NEGAR reglas.
Restricciones	No puede especificar varias direcciones IP ni rangos de direcciones IP en el NSG creado por el modelo de implementación clásico.	No se le permite especificar varios ASG en el origen o el destino.



#### Centro de seguridad de Azure frente a Sentinel

	Centro de seguridad de Azure	Centinela azur
Descripción	Seguridad de la infraestructura unificada sistema de gestión	Servicio de inteligencia de amenazas y análisis de seguridad inteligente.
Categoría	Gestión de la postura de seguridad en la nube (CSPM) / Plataforma de protección de cargas de trabajo en la nube (CWPP)	Gestión de eventos de información de seguridad (SIEM) / Orquestación de seguridad Respuesta automatizada (SOAR)
Función	Proporciona alertas de seguridad, puntuaciones, evaluación de vulnerabilidades, recomendaciones, postura de seguridad, caza proactiva y respuesta a amenazas. administración.	Proporciona detección de alertas, visibilidad de amenazas, respuesta a amenazas.
Características	<ul style="list-style-type: none"><li>• ATP de Microsoft Defender</li><li>• Integración</li><li>• Mapa de red</li><li>• Comportamiento de la máquina virtual</li><li>• Analítica</li><li>• Fortalecimiento de la red adaptable</li><li>• Cumplimiento normativo</li><li>• tablero e informes</li><li>• Faltan parches del sistema operativo</li><li>• evaluación</li><li>• Configuraciones erróneas de seguridad</li><li>• evaluación</li><li>• Evaluación de protección de endpoints</li><li>• Evaluación de cifrado de disco</li><li>• Vulnerabilidad de terceros</li><li>• evaluación</li><li>• Evaluación de la seguridad de la red</li></ul>	<ul style="list-style-type: none"><li>• Reglas de análisis personalizadas</li><li>• Vista de varios espacios de trabajo</li><li>• Libros de trabajo de Azure Monitor</li><li>• Integración</li><li>• Libro de jugadas de seguridad</li><li>• Gráfico de investigación</li><li>• Herramientas de búsqueda y consulta de caza</li></ul>
Proporciona seguridad ¿Recomendación?	si	No
Respuesta a amenazas administración	Manual	Automatizado
Integración	Puede utilizar Azure Security Center para proporcionar a Azure Sentinel más información para identificar, investigar y remediar amenazas.	



#### Azure Policy frente al control de acceso basado en roles de Azure (RBAC)

	Política de Azure	Control de acceso basado en roles (RBAC)
<b>Descripción</b>	Asegúrese de que los recursos cumplan con el sistema de autorización para proporcionar un conjunto de reglas.	controles de acceso de grano fino.
<b>Atención</b>	La política se centra en las propiedades de recursos.	RBAC se centra en qué recursos los usuarios pueden acceder.
<b>Implementación</b>	Usted especifica un conjunto de reglas para evitar que sobreaprovisionan recursos.	conceda permiso sobre qué usuarios puede crear.
<b>Acceso predeterminado</b>	De forma predeterminada, las reglas se establecen en PERMITIR.	De forma predeterminada, se deniega todo el acceso.
<b>Alcance</b>	Política dentro del grupo de recursos o suscripción.	Otorgue acceso a usuarios o grupos dentro de una suscripción.
<b>Integración</b>	Ambos servicios funcionan de la mano para proporcionar gobernanza en su entorno.	



## SERVICIOS AWS vs AZURE

Para ayudarlo a conocer los diferentes servicios de Microsoft Azure, hemos creado este **Comparación de servicios AWS vs Azure**. Si ya tiene experiencia en AWS (o computación en la nube en general), ya sea a través de experiencia laboral o certificaciones de AWS, entonces no tendrá dificultades para aprender Microsoft Azure.

A continuación, se muestran los servicios relacionados de AWS y Azure según la función y las capacidades. Cada servicio de AWS de esta lista tiene un servicio similar en Azure.



## Calcular

Amazon EC2 frente a la máquina virtual de Azure

TD Tutorials Dojo	Amazon EC2	Azure VM
<b>Description</b>	A virtual server that supports both Linux and Windows operating systems.	A Linux-based / Windows-based virtual server that you can provision.
<b>Configurations</b>	EC2 configurations are called <b>instance types</b> .	Virtual machine configurations are called <b>VM series</b>
<b>Images</b>	AMI or operating systems are stored in a root volume.	<b>VM images</b> or operating systems are stored in an OS disk.
<b>OS Volumes</b>	Root volume type: General Purpose SSD (gp2), Provisioned IOPS SSD (io1 and io2), and Magnetic (standard)	OS disk type: Standard HDD, Standard SSD, and Premium SSD
<b>Storage Volumes</b>	Persistent storage volumes for your data using <b>Elastic Block Storage volumes</b> .	Persistent storage volumes for your data using <b>Azure Disk</b> .
<b>Encryption</b>	Encrypt EBS volumes with <b>AWS KMS</b> .	Encrypt OS and data disks with <b>Azure SSE</b> .
<b>Script</b>	Add a script that will be run on an instance boot called <b>user-data</b> .	Add a script that will be run into the virtual machine while it is being provisioned called <b>custom data</b> .
<b>Security</b>	<b>Security group</b> enables you to create security rules to allow the traffic going to your instances.	<b>NIC network security group</b> enables you to create security rules to allow or deny the traffic going to your virtual machine.
<b>Monitoring</b>	Monitor the performance of your EC2 instances with <b>Amazon CloudWatch</b> .	Monitor the performance of your virtual machines with <b>Azure Monitor</b> .
<b>Network</b>	All EC2 instances are launched in an isolated network called <b>VPC</b> .	All virtual machines are launched in an isolated network called <b>VNet</b> .



---

#### Comparación de otros servicios informáticos

- **Lote de AWS y Lote Azure** - suministre decenas, cientos o miles de recursos informáticos según los requisitos del trabajo.
- **Escalado automático de AWS y Conjuntos de escalas de máquinas virtuales de Azure**: aumente o disminuya el número de sus recursos a medida que cambia la demanda.
- **AWS Lambda y Funciones de Azure**: una plataforma informática sin servidor para ejecutar código en respuesta a eventos.
- **Amazon ECS, AWS Fargate, y Instancias de contenedor de Azure**: ejecutar aplicaciones en contenedores sin administrar ningún servidor.
- **Amazon ECR y Registro de contenedores de Azure**: un repositorio para almacenar y administrar imágenes de contenedores.
- **Amazon EKS y Servicio Azure Kubernetes**: Simplifique la gestión de sus aplicaciones en contenedores en un grupo de nodos.



## Almacenamiento

### Amazon S3 frente a Azure Blob

TD Tutorials Dojo	Amazon S3	Azure Blob
<b>Description</b>	Object storage service of AWS	Object storage service of Azure.
<b>Components</b>	S3 is composed of <b>buckets</b> and <b>objects</b> .	Blob storage resources: <b>Storage Account</b> , <b>Container</b> , and <b>Blob</b>
<b>Max File Size</b>	The maximum file size for each object is 5 TB.	The maximum file size for each blob: Block (190.7 TiB), Append (195 GiB), and Page (8 TiB).
<b>Max Storage Size</b>	Bucket capacity is virtually unlimited.	Single blob container size is the same as the maximum storage account capacity.
<b>Tiers</b>	S3 tiers: Standard, Standard-IA, One Zone-IA, Intelligent-Tiering, Glacier, and Glacier Deep Archive	Blob tiers: Hot, Cool, and Archive.
<b>Durability</b>	Data durability across multi-AZ is 11 9's.	Data durability across LRS (11 9's), ZRS (12 9's), GRS, and RA-GRS (16 9's).
<b>Replication</b>	Copy objects across S3 buckets in different AWS Regions using <b>Cross-Region Replication</b> .	Copy block blobs between a source and destination account using <b>Object Replication</b> .
<b>CDN</b>	Cache content from a static website with <b>Amazon CloudFront</b> .	Cache content from a static website with <b>Azure CDN</b> .
<b>Encryption</b>	Encrypt objects using Client-Side and Server-Side Encryption.	Encrypt storage account using Microsoft- and Customer-managed keys.
<b>Endpoint</b>	Endpoint: <tutorialdojo>.s3.<region>.amazonaws.com	Endpoint: <tutorialdojo>.blob.core.windows.net

### Comparación de otros servicios de almacenamiento

- **Amazon EBS y Disco de Azure** - un almacenamiento en disco para almacenar sus datos y sistema operativo.
- **Amazon EFS y Archivos de Azure** - cree y configure sistemas de archivos y comparta sus archivos a través de múltiples recursos.
- **AWS Storage Gateway y Azure StorSimple** - Simplifique la gestión del almacenamiento mediante el uso de una solución de almacenamiento en la nube híbrida.
- **Familia de nieve de AWS y Cuadro de datos de Azure** - transfiera petabytes y exabytes de datos a la nube.



## Bases de datos

### Amazon RDS frente a Azure SQL

TD Tutorials Dojo	Amazon RDS	Azure SQL
<b>Description</b>	Configure and scale a relational database in the cloud.	Fully managed and intelligent relational database in the cloud.
<b>DB Engines</b>	Database engines: Amazon Aurora, PostgreSQL, MySQL, Oracle, MariaDB, and Microsoft SQL Server	Database Engine: Microsoft SQL Server
<b>Serverless</b>	The serverless database is called <b>Amazon Aurora Serverless</b> .	The serverless database is called <b>Azure SQL Database serverless</b> .
<b>Templates</b>	DB templates are Free Tier, Dev/Test, and Production.	DB templates are Basic, Standard, and Premium.
<b>Performance</b>	DB performance: Standard, Memory-Optimized, and Burstable Classes	DB performance: General Purpose, Hyperscale, and Business Critical
<b>High Availability</b>	Eliminate a single point of failure with <b>Multi-AZ deployment</b> .	Eliminate a single point of failure with <b>zone redundant configuration</b> .
<b>Secondary DB</b>	Create readable secondary databases in the same or different regions with <b>read replicas</b> .	Create readable secondary databases in the same or different regions with <b>active geo-replication</b> .
<b>Backup</b>	Automated backups retention period up to 35 days.	Automated backups retention period up to 35 days.
<b>Monitoring</b>	Monitor the metrics of your database with <b>Amazon CloudWatch</b> .	Monitor the metrics of your database with <b>Azure Monitor</b> .
<b>Endpoint</b>	Endpoint: rds.<region>.amazonaws.com	Endpoint: <server_name>.database.windows.net



---

Comparación de otros servicios de bases de datos

- **Amazon DynamoDB y Azure Cosmos DB** - un modelo de base de datos para almacenes de documentos y valores-clave.
- **Amazon Redshift y Análisis de Azure Synapse**: un servicio de almacenamiento de datos en la nube utilizado para herramientas de análisis e inteligencia empresarial.
- **Amazon ElastiCache y Azure Cache para Redis**: un servicio de almacenamiento en caché basado en memoria para mejorar el rendimiento de su base de datos existente.
- **AWS DMS y Azure DMS**: Automatice la migración de sus datos desde múltiples bases de datos.



## Redes

Amazon VPC frente a Azure VNet

TD Tutorials Dojo	Amazon VPC	Azure VNet
<b>Description</b>	A virtual network service in AWS where you can launch your resources.	An isolated network service in Azure to run your VMs and applications.
<b>Default</b>	Default VPC in each region.	Default VNet is not existing.
<b>Reserved IP address</b>	AWS reserves 5 IP addresses within each subnet.	Azure reserves 5 IP addresses within each subnet.
<b>Subnets</b>	Subnets are from /28 to /16.	Subnets are from /29 to /8.
<b>Subnet Types</b>	Subnets types: Private, Public and VPN-only	Subnets types: Private, Public and Gateway
<b>Static IP address</b>	You can assign a static IPv4 to your resources with <b>Elastic IP addresses</b> .	You can assign a static IPv4 and IPv6 address to your resources.
<b>Security</b>	Secure your network using <b>NACLs</b> and <b>Security Groups</b> .	Secure your network using <b>NSGs</b> and <b>ASGs</b> .
<b>Gateways</b>	Types of gateways: Internet Gateway, Egress-only, NAT Gateway, Virtual Private Gateway, and Customer Gateway	Types of gateways: VPN Gateway and ExpressRoute Gateway
<b>Route Table</b>	By default, subnets are automatically associated with the main route table.	Route tables are not automatically associated with your subnets.
<b>Peering</b>	A <b>VPC peering</b> enables communication between two VPCs.	A <b>VNet peering</b> enables the communication between virtual networks.

Comparación de otros servicios de red

- **Puerta de enlace VPN de AWS y Puerta de enlace de VPN de Azure:** conexión segura desde su red local a su red privada en la nube.
- **Ruta Amazónica 53 y DNS de Azure** - le ayuda a administrar sus registros DNS.



- **AWS Direct Connect y Azure ExpressRoute** - conexión privada dedicada entre el proveedor de la nube y su centro de datos.
- **Amazon ELB: NLB y Equilibrador de carga de Azure**: equilibrador de carga de capa 4 para protocolos TCP y UDP.
- **Amazon ELB: ALB y Puerta de enlace de aplicaciones de Azure**: equilibrador de carga para el tráfico de capa 7 (terminación SSL, permanencia de cookies y enrutamiento por turnos).



## Seguridad e Identidad

### AWS Identity & Access Management (IAM) frente a Azure Active Directory y RBAC

Tutorials Dojo	AWS IAM	Azure AD & RBAC
<b>Description</b>	Create and manage users, groups, roles, and policies in your account.	Create users and groups with <b>Azure Active Directory</b> .
<b>MFA</b>	Secure your account by activating MFA.	Secure your account by activating MFA in Azure AD.
<b>Groups</b>	IAM groups allow you to organize a large number of IAM users.	Azure AD allows you to assign a large number of users to groups.
<b>Roles</b>	Delegate administrator roles using <b>identity-based policies</b> .	Delegate administrator roles using Azure AD.
<b>Access</b>	Access resources only in the AWS console	Azure AD supports <b>hybrid identity</b> to access resources in the cloud or on-premises.
<b>Monitoring</b>	Monitor the status of your user accounts with a <b>credential report</b> .	Monitor the security and usage patterns of your environment with <b>Azure AD reports and monitoring</b> .
<b>Domain</b>	Unique account sign-in page URL: <code>https://&lt;My_AWS_Account_ID&gt;.signin.aws.amazon.com/console/</code>	The domain name of Azure AD tenant: <code>&lt;Azure_Tenant&gt;.onmicrosoft.com</code>
<b>Permission</b>	Grant users temporary permission using <b>IAM roles</b> .	<b>RBAC</b> enables you to grant users certain roles to access specific resources.
<b>Policy</b>	A collection of permissions written in JSON is called <b>IAM policies</b> .	A collection of permissions written in JSON is called <b>role definition</b> in RBAC.
<b>Multiple roles</b>	You can assign multiple permissions to an IAM user.	You can assign multiple roles to a resource group with RBAC.

### Comparación de otros servicios de seguridad e identidad

- **AWS WAF y Azure WAF en Application Gateway:** protege las aplicaciones web de exploits y vulnerabilidades comunes.



- **Escudo de AWS y Protección contra DDoS de Azure:** proteja sus recursos de ataques de denegación de servicio.
- **AWS KMS y Azure Key Vault** - crear y administrar las claves utilizadas para cifrar sus datos.
- **Asesor de confianza de AWS y Asesor de Azure** - proporciona recomendaciones sobre excelencia operativa, seguridad, rendimiento, confiabilidad y costo.

**Fuentes:**

<https://aws.amazon.com/>

<https://docs.microsoft.com/en-us/azure/architecture/aws-professional/>



## OBSERVACIONES FINALES

Si es un estudiante o una persona no técnica que quiere dedicarse a la industria de la TI, la computación en la nube es una de las habilidades más solicitadas que lo ayudará a convertirse en un candidato competitivo. Microsoft Azure es uno de los principales proveedores de servicios en la nube que puede ayudarlo a crear, implementar y administrar aplicaciones rápidamente. La creación de nuevas soluciones para startups para empresas empresariales requiere habilidades y conocimientos. Dado que se trata de una tecnología emergente, muchas personas aspiran a obtener la certificación Microsoft Azure. Estas certificaciones son inversiones en usted y también para mejorar sus habilidades. Todos en la comunidad reconocen las certificaciones de Microsoft.

En Tutorials Dojo estamos dedicados a ayudarlo a mejorar sus habilidades y su carrera. Tenemos varias colecciones de blogs técnicos, guías, hojas de trucos y exámenes de práctica que se actualizan constantemente en función de nuestras experiencias y los comentarios de nuestros estudiantes. Si se está preparando en su viaje para obtener la certificación AZ-900, proporcionamos contenido valioso para lograr los resultados que desea.

Si está leyendo esto en este momento, nos complace ayudarlo en su viaje hacia la nube. Gracias por elegir Tutorials Dojo, y esperamos que continúe apoyándonos. Si desea validar lo que ha aprendido hasta ahora, ahora es un buen momento para consultar nuestra [Exámenes de práctica de conceptos básicos de Microsoft Azure AZ-900](#). También puede probar la versión de [muestra gratuita de nuestro curso de prueba de práctica completo Aquí](#). También le deseamos lo mejor en sus futuros exámenes de certificación de Azure.

Buena suerte en tu examen y esperamos verte en nuestros otros cursos de prueba de práctica.

## SOBRE LOS AUTORES



### Jon Bonso

Nacido y criado en Filipinas, Jon es el cofundador de [Tutoriales Dojo](#). Ahora con sede en Sydney, Australia, tiene más de una década de experiencia diversificada en banca, servicios financieros y telecomunicaciones. Tiene 8 veces la certificación AWS y ha trabajado con varios servicios en la nube como Google Cloud y Microsoft Azure. Jon es un apasionado de lo que hace y dedica mucho tiempo a crear cursos educativos. Ha impartido seminarios de TI en diferentes universidades de Filipinas de forma gratuita y ha lanzado sitios web educativos con su propio dinero y sin ningún tipo de financiación externa.



### Gerome Pagatpatan

Gerome está certificado en AWS, Azure y Oracle. Después de graduarse de la universidad con un título en Ingeniería Electrónica, decidió dedicarse al campo de la Tecnología de la Información a través del autoestudio. Es un apasionado de la educación y ahora le toca a él compartir sus conocimientos, experiencias y pasión por la computación en la nube.