Microsoft Azure Az104

Requisitos previos para administradores de Azure.

Azure Portal permite crear, administrar y supervisar todos los elementos, desde aplicaciones web simples hasta aplicaciones complejas en la nube en una única consola unificada.

Azure Cloud Shell es un 1hell interactivo, accesible desde el explorador, para administrar recursos de Azure. Los usuarios de Linux pueden elegir una experiencia de Bash, mientras que los de Windows pueden optar por PowerShell.

Características de Azure Cloud Shell

- Es temporal y requiere que se monte un recurso compartido de Azure Files nuevo o existente.
- Ofrece un editor de texto gráfico integrado basado en el editor Monaco Editor de código abierto.
- Se autentica automáticamente para el acceso instantáneo a los recursos.
- Se ejecuta en un host temporal que se proporciona por cada sesión y usuario.
- Agota el tiempo de espera tras 20 minutos sin actividad interactiva.
- Requiere un grupo de recursos, una cuenta de almacenamiento y un recurso compartido de archivos de Azure.
- Usa el mismo recurso compartido de archivos de Azure para Bash y para PowerShell.
- Se asigna a un equipo por cuenta de usuario.
- Conserva $HOME con una imagen de 5 GB en el recurso compartido de archivos.
- Los permisos se establecen como usuario de Linux normal en Bash.

Azure PowerShell es un módulo que se agrega a Windows PowerShell o PowerShell Core, y que permite conectarse a la suscripción de Azure y administrar los recursos. Azure PowerShell requiere PowerShell para funcionar.

La CLI de Azure es un programa de línea de comandos para conectarse a Azure y ejecutar comandos administrativos en recursos de Azure. Se ejecuta en Linux, macOS y Window.

Azure Resource Manager es el servicio de implementación y administración para Azure. Proporciona una capa de administración que le permite crear, actualizar y eliminar recursos de la cuenta de Azure. Se usan las características de administración, como el control de acceso, la auditoría y las etiquetas, para proteger y organizar los recursos después de la implementación.

Los bloqueos de Resource Manager permiten que las organizaciones coloquen una estructura que impida la eliminación accidental de recursos en Azure.

Hay dos tipos de bloqueos de recursos.

- **Bloqueos de solo lectura**, que evitan cualquier cambio en el recurso.
- **Bloqueos de eliminación**, que evitan la eliminación.

Los recursos solo pueden estar en un grupo de recursos.

Una **plantilla de Resource Manager** define con exactitud todos los recursos de Resource Manager de una implementación. Una plantilla de Resource Manager se puede implementar en un grupo de recursos con una sola operación.

Las plantillas de Resource Manager se escriben en JSON, lo que permite expresar los datos almacenados como un objeto (como una máquina virtual) en texto. **Un documento JSON** es, básicamente, una colección de pares clave-valor. Cada clave es una cadena, cuyo valor puede ser lo siguiente:

- Una cadena
- Un número
- Una expresión booleana.
- Una lista de valores.
- Un objeto (que es una colección de otros pares clave-valor).

Azure Bicep es un lenguaje específico de dominio (DSL) que usa una sintaxis declarativa para implementar recursos de Azure. Brinda sintaxis concisa, seguridad de tipos confiable y compatibilidad con la reutilización de código. **La transpilación** es el proceso de convertir el código fuente escrito de un lenguaje a otro.

Un cmdlet es un comando que manipula una sola característica. El término **cmdlet** pretende implicar que es un "comando pequeño". **Az** es el nombre formal del módulo de Azure PowerShell, que contiene cmdlets para trabajar con las características de Azure. Contiene cientos de cmdlets que le permiten controlar casi cualquier aspecto de todos los recursos de Azure. **Un script de PowerShell** es un archivo de texto que contiene comandos y construcciones de control. Los comandos son invocaciones de los cmdlets. **Las construcciones de control** son características de programación como bucles, variables, parámetros, comentarios, etc., proporcionadas por PowerShell.

La *infraestructura como código* le permite describir, mediante código, la infraestructura que necesita para la aplicación. **Con la infraestructura** como código, puede mantener en un repositorio de código central el código de la aplicación y todo lo que necesita para implementarla. Las ventajas de la infraestructura como código son las siguientes:

- Configuraciones coherentes
- Escalabilidad mejorada
- Implementaciones más rápidas
- Mejor rastreabilidad

Las plantillas de ARM son archivos de notación de objetos JavaScript (JSON) que definen la infraestructura y la configuración de la implementación. La plantilla usa una ***sintaxis declarativa***. **La sintaxis declarativa** es una forma de crear la estructura y los elementos que describen el aspecto que tendrán los recursos sin describir su flujo de control. La sintaxis declarativa es diferente de la ***sintaxis imperativa***, en la que se usan comandos que el equipo debe ejecutar. El scripting imperativo se centra en especificar cada paso de la implementación de los recursos. **Los elementos de una plantilla de Azure Resource Manager** son*: schema, contentVersion, apiProfile, parameters, variables, functions, resources y output*.

Azure Compute es un servicio de informática a petición para ejecutar aplicaciones basadas en la nube. Se proporcionan recursos informáticos como discos, procesadores, memoria, redes y sistemas operativos. **Las máquinas virtuales** son emulaciones de software de equipos físicos. Incluyen un procesador virtual, memoria, almacenamiento y recursos de red. **Virtual Machines** proporciona infraestructura como servicio **(IaaS)** y se puede usar de maneras diferentes. **Los conjuntos de escalado de máquinas virtuales** son un recurso de Azure Compute que puede usar para implementar y administrar un conjunto de máquinas virtuales idénticas. **Container Instances** y **Azure Kubernetes Service** son recursos de Azure Compute que puede usar para implementar contenedores y administrarlos. Los contenedores son entornos de aplicación ligeros y virtualizados. **Azure App Service** puede compilar, implementar y escalar de forma rápida aplicaciones de API, móviles y web de nivel empresarial que se pueden ejecutar en cualquier plataforma. **App Service** es una oferta de plataforma como servicio

(PaaS). Azure Functions es una opción ideal si le preocupa solo el código que ejecuta el servicio y no la infraestructura o la plataforma subyacente.

Las máquinas virtuales son una opción ideal cuando se necesita lo siguiente:

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

Azure Batch permite trabajo por lotes paralelos a gran escala y de informática de alto rendimiento (HPC) con la capacidad de escalar a decenas, cientos o miles de máquinas virtuales.

Azure Container Instances ofrece la forma más rápida y sencilla de ejecutar un contenedor en Azure, sin tener que administrar ninguna máquina virtual o adoptar ningún servicio adicional. Es una oferta de plataforma como servicio (PaaS) que permite cargar los contenedores, que se ejecutan automáticamente.

Azure Virtual Desktop es un servicio de virtualización de escritorios y aplicaciones que se ejecuta en la nube. Permite que los usuarios usen una versión hospedada en la nube de Windows desde cualquier ubicación. Azure Virtual Desktop funciona en dispositivos como Windows, Mac, iOS, Android y Linux

Azure IoT Hub es un servicio administrado hospedado en la nube que actúa como centro de mensajes centralizado para la comunicación bidireccional entre la aplicación de IoT y los dispositivos que administra.

Azure IoT Central se basa en IoT Hub y agrega un panel que le permite conectar, supervisar y administrar sus dispositivos de IoT.

Azure Sphere crea una solución de IoT de un extremo a otro de alta seguridad para los clientes que lo abarca todo, desde el hardware y el sistema operativo del dispositivo hasta el método seguro para enviar mensajes desde el dispositivo al centro de mensajes.

Azure Security Center es un servicio de supervisión que proporciona visibilidad del nivel de seguridad en todos los servicios, tanto en Azure como en el entorno local. El término *nivel de seguridad* se refiere a las directivas y a los controles de ciberseguridad, así como a la predicción, la prevención y la respuesta a las amenazas de seguridad.

Security Center puede:

- Supervisar la configuración de seguridad en las cargas de trabajo locales y en la nube.
- Aplicar automáticamente la configuración de seguridad necesaria a los nuevos recursos a medida que se publican en línea.
- Proporcionar recomendaciones de seguridad basadas en las configuraciones, los recursos y las redes actuales.
- Supervisar de forma continua los recursos y realizar valoraciones de seguridad automáticas para identificar posibles vulnerabilidades antes de que alguien las aproveche.
- Usar el aprendizaje automático para detectar y bloquear la instalación de malware en las máquinas virtuales (VM) y otros recursos. También puede usar *controles de aplicaciones adaptables* para definir reglas que indiquen las aplicaciones permitidas a fin de garantizar que solo se puedan ejecutar las aplicaciones permitidas.
- Detectar y analizar posibles ataques entrantes e investigar amenazas y otras actividades posteriores a una brecha que pudieran haberse producido.
- Proporcionar control de acceso Just-in-Time a los puertos de red. Esto reduce la superficie expuesta a ataques al garantizar que la red solo permite el tráfico necesario en el momento en que se necesita.

La puntuación de seguridad es una medida del nivel de seguridad de una organización. Se basa en el porcentaje de controles de seguridad que se satisfacen.

Azure Sentinel es el sistema SIEM basado en la nube de Microsoft. Usa análisis de seguridad inteligente y análisis de amenazas.

Azure Sentinel permite:

- **Recopilación de datos en la nube a gran escala** Recopile datos de todos los usuarios, dispositivos, aplicaciones e infraestructura, tanto locales como de varias nubes.
- **Detección de amenazas no detectadas anteriormente** Minimice los falsos positivos mediante el análisis y la inteligencia sobre amenazas completos de Microsoft.
- **Investigación de amenazas con inteligencia artificial** Examine actividades sospechosas a gran escala y saque provecho de los años de experiencia en el campo de la ciberseguridad de Microsoft.
- **Respuesta rápida a los incidentes** Use la orquestación y la automatización de tareas comunes integradas.

Azure Key Vault es un servicio en la nube centralizado para almacenar los secretos de la aplicación en una única ubicación central. Proporciona un acceso seguro a la información confidencial mediante capacidades de control de acceso y registro.

Azure Key Vault puede ayudar a:

- **Administración de secretos** Puede usar Key Vault para almacenar de forma segura y controlar exhaustivamente el acceso a tokens, contraseñas, certificados, claves de API y otros secretos.
- **Administración de claves de cifrado** Puede usar Key Vault como solución de administración de claves. Key Vault facilita la creación y el control de las claves de cifrado que se emplean para cifrar los datos.
- **Administración de certificados SSL/TLS** Key Vault permite aprovisionar, administrar e implementar los certificados públicos y privados de Capa de sockets seguros/Seguridad de la capa de transporte (SSL/TLS) de los recursos de Azure y los recursos internos.
- **Almacenamiento de secretos basado en módulos de seguridad de hardware(HSMs)** Estas claves y secretos se pueden proteger mediante software o con dispositivos HSM validados por FIPS 140-2 de nivel 2.

Azure Dedicated Host proporciona servidores físicos dedicados para hospedar las máquinas virtuales de Azure para Windows y Linux.

La autenticación es el proceso de establecimiento de la identidad de una persona o servicio que quiere acceder a un recurso. Implica el acto de solicitar a un usuario credenciales legítimas y proporciona la base para la creación de una entidad de seguridad para el control de identidad y de acceso. Determina si el usuario es quien dicen ser. La autenticación establece la identidad del usuario, pero **la autorización** es el proceso de establecer el nivel de acceso que tiene una persona o un servicio autenticados. Especifica a qué datos puede acceder y qué puede hacer con ellos.

Azure Active Directory (Azure AD) proporciona servicios de identidad que permiten a los usuarios iniciar sesión y acceder tanto a las aplicaciones en la nube de Microsoft como a las que desarrolle personalmente. **Active Directory** ejecutado en Windows Server proporciona un servicio de administración de acceso e identidades administrado por su propia organización. **Azure AD** es un servicio de administración de acceso e identidades basado en la nube de Microsoft.

El inicio de sesión (SSO) único permite a los usuarios iniciar sesión una vez y utilizar esa credencial para acceder a varios recursos y aplicaciones de distintos proveedores.

Azure AD Connect sincroniza las identidades de usuario entre la instalación local de Active Directory y Azure AD.

La *autenticación multifactor* es un proceso en el que durante el inicio de sesión de un usuario se le solicita una forma adicional de identificación.

Estos elementos se dividen en tres categorías:

Algo que el usuario conoce

Algo que el usuario tiene

Algo que el usuario es

Azure AD Multi-Factor Authentication es un servicio de Microsoft que proporciona funcionalidades de autenticación multifactor.

El acceso condicional es una herramienta que usa Azure Active Directory para permitir (o denegar) el acceso a los recursos en función de *señales* de identidad. Estas señales incluyen quién es el usuario, dónde se encuentra y desde qué dispositivo solicita el acceso.

La Calculadora de TCO le ayuda a calcular los costos que se ahorra al hacer funcionar la solución en Azure con el tiempo, en lugar de hacerlo en el centro de datos local.

Administración de identidades y gobernanza en Azure.

Azure Active Directory (Azure AD) es el servicio de administración de identidades y directorios basado en la nube multiinquilino de Microsoft.

Características de Azure AD

Característica de Azure AD	Descripción
Acceso mediante inicio de sesión único (SSO)	Azure AD proporciona un inicio de sesión único (SSO) seguro en las aplicaciones web en la nube y en las aplicaciones locales. Los usuarios pueden iniciar sesión con el mismo conjunto de credenciales para acceder a todas sus aplicaciones.
Compatibilidad con dispositivos omnipresente	Azure AD funciona con dispositivos iOS, macOS, Android y Windows, y ofrece una experiencia común en todos los dispositivos. Los usuarios pueden iniciar aplicaciones desde un panel de acceso personalizado basado en web, una aplicación móvil, Microsoft 365 o portales de empresa personalizados con sus credenciales de trabajo existentes.
Acceso remoto seguro	Azure AD permite el acceso remoto seguro para aplicaciones web locales. El acceso seguro puede incluir la autenticación multifactor (MFA), las directivas de acceso condicional y la administración de acceso basada en grupos. Los usuarios pueden acceder a aplicaciones web locales desde cualquier lugar, incluido desde el mismo portal.
Extensibilidad a la nube	Azure AD puede ampliarse a la nube para ayudarle a administrar un conjunto coherente de usuarios, grupos, contraseñas y dispositivos en todos los entornos.
Protección de datos confidenciales	Azure AD ofrece capacidades únicas de protección de identidades para proteger los datos confidenciales y las aplicaciones. Los administradores pueden supervisar si hay actividad de inicio de sesión sospechosa y posibles vulnerabilidades en una vista consolidada de usuarios y recursos en el directorio.
Soporte mediante autoservicio	Azure AD permite delegar tareas a los empleados de la empresa que, de lo contrario, pueden completar los administradores con privilegios de acceso más elevados. Proporcionar acceso a aplicaciones de autoservicio y administración de contraseñas mediante pasos de comprobación puede reducir las llamadas al departamento de soporte técnico y mejorar la seguridad.

Conceptos de Azure AD

Concepto de Azure AD	Descripción
Identidad	Una *identidad* es un objeto que se puede autenticar. La identidad puede ser un usuario con un nombre de usuario y una contraseña. Las identidades también pueden ser aplicaciones u otros servidores que requieren autenticación mediante certificados o claves secretas. Azure AD es el producto subyacente que proporciona el servicio de identidad.
Cuenta	Una *cuenta* es una identidad que tiene datos asociados. Para tener una cuenta, primero debe tener una identidad válida. No puede tener una cuenta sin una identidad.
Cuenta de Azure AD	Una *cuenta de Azure AD* es una identidad que se crea mediante Azure AD u otro servicio en la nube de Microsoft, como Microsoft 365. Las identidades se almacenan en Azure AD y pueden acceder a ellas las suscripciones de servicio en la nube de su organización. La cuenta de Azure AD también se denomina *cuenta profesional o educativa*.
Inquilino (directorio) de Azure	Un *inquilino* de Azure es una instancia única, dedicada y de confianza de Azure AD. Cada inquilino (también denominado *directorio*) representa una sola organización. Cuando su organización se registra a una suscripción de servicio en la nube de Microsoft, automáticamente se crea un nuevo inquilino. Dado que cada inquilino es una instancia dedicada y de confianza de Azure AD, puede crear varios inquilinos o instancias.
Suscripción de Azure	Una suscripción de Azure se usa para pagar los servicios en la nube de Azure. Una suscripción está vinculada a una tarjeta de crédito. Cada suscripción se une a un único inquilino. Puede tener varias suscripciones.

- **Solución de identidad**: AD DS es principalmente un servicio de directorio, mientras que Azure AD es una solución de identidad completa. Azure AD está diseñado para aplicaciones basadas en Internet que usan comunicaciones HTTP y HTTPS. Las características y capacidades de Azure AD admiten la administración segura de identidades de destino.
- **Consultas de la API de REST**: Azure AD se basa en los protocolos HTTP y HTTPS. Los inquilinos de Azure AD no se pueden consultar mediante LDAP. Azure AD usa la API de REST sobre HTTP y HTTPS.
- **Protocolos de comunicación**: dado que Azure AD se basa en HTTP y HTTPS, no usa la autenticación Kerberos. Azure AD implementa los protocolos HTTP y HTTPS, como SAML, WS-Federation y OpenID Connect para la autenticación, así como Oauth para la autorización.
- **Servicios de federación**: Azure AD incluye servicios de federación y muchos servicios de terceros (como Facebook).
- **Estructura plana**: los usuarios y grupos de Azure AD se crean en una estructura plana. No hay unidades organizativas (UO) ni objetos de directiva de grupo (GPO).

- **Servicio administrado**: Azure AD es un servicio administrado. Solo se administran los usuarios, los grupos y las directivas. Si implementa AD DS con máquinas virtuales mediante Azure, administra muchas otras tareas, como la implementación, la configuración, las máquinas virtuales, la aplicación de revisiones y otros procesos de back-end.

Azure Active Directory Free

La edición Gratis proporciona administración de usuarios y grupos, sincronización de directorios locales e informes básicos. El acceso con inicio de sesión único se admite en Azure, Microsoft 365 y muchas aplicaciones SaaS populares.

Aplicaciones de Microsoft 365 de Azure Active Directory

Esta edición se incluye con Microsoft 365. Además de las características de la edición Gratis, esta edición proporciona administración de identidades y acceso para aplicaciones de Microsoft 365. La compatibilidad adicional incluye personalización de marca, MFA, administración de acceso a grupos y autoservicio de restablecimiento de contraseña para los usuarios en la nube.

Azure Active Directory Premium P1

Además de las características de la edición Gratis, la edición Premium P1 permite a los usuarios de entornos híbridos acceder a recursos locales y en la nube. Esta edición admite la administración avanzada, como los grupos dinámicos, la administración de grupos de autoservicio y capacidades de escritura diferida en la nube. La edición P1 también incluye Microsoft Identity Manager, un conjunto de administración de identidades y acceso local. Las características adicionales de la edición P1 permiten el autoservicio de restablecimiento de contraseña para los usuarios locales.

Azure Active Directory Premium P2

Además de incluir las características de las ediciones Gratis y P1, la edición Premium P2 ofrece Azure AD Identity Protection para facilitar el acceso condicional basado en riesgos a las aplicaciones y a los datos críticos de la empresa. Privileged Identity Management se incluye para descubrir, restringir y supervisar a los administradores y su acceso a los recursos, y proporcionar acceso Just-in-Time cuando sea necesario.

- **La característica de unión a Azure AD** funciona con SSO para proporcionar acceso a aplicaciones y recursos de la organización, así como simplificar las implementaciones de dispositivos de trabajo Windows.
- **Tenga en cuenta las opciones de conexión**. Conecte el dispositivo a Azure AD de una de estas dos maneras:
    - **Registre** el dispositivo a Azure AD para poder administrar la identidad del dispositivo. El registro de dispositivos de Azure AD proporciona una identidad al dispositivo que se utiliza para autenticarlo cuando el usuario inicia sesión en Azure AD. Puede utilizar esta identidad para habilitar o deshabilitar el dispositivo.
    - **Únase** al dispositivo, que es una extensión del registro de un dispositivo. La unión ofrece las ventajas del registro, y también cambia el estado local del dispositivo. El cambio del estado local permite a los usuarios iniciar sesión en un dispositivo mediante una cuenta profesional o educativa en lugar de con una cuenta personal.

La característica de **autoservicio de restablecimiento de contraseña** (SSPR) de Azure Active Directory le permite dar a los usuarios la posibilidad de omitir el departamento de soporte técnico y restablecer sus propias contraseñas

Azure Active Directory (Azure AD) admite tres tipos de cuentas de usuario: Identidad en la nube, Identidad sincronizada con Directory y Usuario invitado.

El administrador puede **crear** un usuario dentro de la organización o **invitar** a un usuario invitado para proporcionarle acceso a los recursos de la organización. **Solo los administradores globales** o los administradores de usuarios tienen privilegios para crear y eliminar cuentas de usuario en Azure Portal.

Los **grupos de seguridad** se usan para administrar el acceso de miembros y equipos a los recursos compartidos de un grupo de usuarios. Los **grupos de Microsoft 365** proporcionan oportunidades de colaboración. Los miembros del grupo tienen acceso a un buzón, un calendario, archivos, un sitio de SharePoint y muchos más recursos compartidos

Asignado Agregue usuarios específicos como miembros de un grupo, donde cada usuario puede tener permisos únicos.

Usuario dinámico Use reglas de pertenencia dinámicas para agregar y quitar miembros de un grupo automáticamente. Cuando los atributos de un miembro cambian, Azure revisa las reglas de grupos dinámicos del directorio.

Si los atributos del miembro cumplen los requisitos de la regla, el miembro se agrega al grupo.

Si los atributos del miembro ya no cumplen los requisitos de la regla, el miembro se elimina.

Dispositivo dinámico (Solo para grupos de seguridad) Aplique reglas de grupos dinámicos para agregar y quitar automáticamente dispositivos en grupos de seguridad.

Si los atributos de un dispositivo cambian, Azure revisa las reglas de grupos dinámicos del directorio. Si los atributos de un dispositivo cumplen los requisitos de la regla, el dispositivo se agrega al grupo de seguridad.

Si los atributos del dispositivo ya no cumplen los requisitos de la regla, el dispositivo se elimina.

Una región es un área geográfica del planeta que contiene al menos un centros de datos, aunque podrían ser varios. Los centros de datos son cercanos y están conectados mediante una red de baja latencia.

Característica	Descripción
Aislamiento físico	Azure prefiere al menos 500 km (aproximadamente) de separación entre centros de datos en un par regional. Este principio no es práctico ni posible en todas las zonas geográficas. La separación del centro de datos físico reduce la probabilidad de que los desastres naturales, los disturbios civiles, los cortes del suministro eléctrico o las interrupciones de la red física afecten simultáneamente a ambas regiones.
Replicación proporcionada por la plataforma	Algunos servicios, como el almacenamiento con redundancia geográfica, proporcionan replicación automática a la región emparejada.
Orden de recuperación de las regiones	Durante una interrupción amplia, tiene prioridad la recuperación de una región de cada par. Se garantiza que, si las aplicaciones se implementan en regiones emparejadas, se dará prioridad a la recuperación de una de las regiones.
Actualizaciones secuenciales	Las actualizaciones del sistema de Azure que estén previstas se implementan en las regiones emparejadas de forma secuencial, no a la vez. La implementación gradual minimiza el tiempo de inactividad, los errores y los errores lógicos en el caso excepcional de que una actualización sea incorrecta.
Residencia de datos	Las regiones residen dentro de la misma geografía que su conjunto habilitado (excepto las de Sur de Brasil y Singapur).

Una suscripción de Azure es una unidad lógica de servicios de Azure que está vinculada a una cuenta de Azure. **Una cuenta de Azure** es una identidad en Azure Active Directory (Azure AD) o en un directorio de confianza para Azure AD, como una cuenta profesional o académica. Todos los servicios en la nube de Azure pertenecen a una suscripción. **Microsoft Cost Management** proporciona compatibilidad con las tareas de facturación administrativa y le ayuda a administrar el acceso de facturación a los costos.

Las etiquetas son elementos de metadatos que se aplican a los recursos de Azure. Son pares clave-valor que le ayudan a identificar los recursos en función de la configuración que sean relevantes para su organización. Las etiquetas son útiles para ordenar, buscar, administrar y realizar análisis en los recursos.

El control de acceso basado en rol (RBAC) ayuda a administrar quién puede acceder a los recursos de Azure, qué pueden hacer con esos recursos y a qué áreas pueden acceder.

RBAC de Azure es un sistema de autorización basado en Azure Resource Manager que proporciona administración pormenorizada del acceso a los recursos de Azure.

- **Entidad de seguridad**. Objeto que representa un elemento que solicita acceso a los recursos. Ejemplos: usuario, grupo, entidad de servicio o identidad administrada
- **Definición de roles**. Colección de permisos en la que se enumeran las operaciones que se pueden realizar. Ejemplos: Lector, Colaborador, Propietario o Administrador de acceso de usuario
- **Ámbito**. Límite para el nivel de acceso solicitado. Ejemplos: grupo de administración, suscripción, grupo de recursos o recurso
- **Asignación**. Asociación de una definición de roles a una entidad de seguridad en un ámbito determinado. Los usuarios pueden conceder el acceso descrito en una definición de roles mediante la creación de una asignación. Actualmente, las asignaciones de denegación son de solo lectura y únicamente Azure puede establecerlas.

Cada rol es un conjunto de propiedades definido en un archivo JSON.

Una asignación de roles es el proceso de establecer el ámbito de una definición de roles para un usuario, un grupo, una entidad de servicio o identidad administrada. El propósito de la asignación de roles es conceder acceso. El acceso se revoca quitando una asignación de roles. Un recurso hereda las asignaciones de roles de su recurso principal

Roles RBAC de Azure

Administrar el acceso a los recursos de Azure.

El ámbito se puede especificar en varios niveles (grupo de administración, suscripción, grupo de recursos o recurso).

Se puede acceder a la información de roles en Azure Portal, la CLI de Azure, Azure PowerShell, en las plantillas de Azure Resource Manager y en la API REST.

Roles de Azure AD

Administrar el acceso a los recursos de Azure Active Directory.

El ámbito está en el nivel de inquilino.

Se puede acceder a la información de roles en el portal de administración de Azure, el portal de administración de Microsoft 365, Microsoft Graph, Azure AD y PowerShell.

Los roles de administrador de Azure AD se utilizan para administrar recursos en Azure AD como usuarios, grupos y dominios. **Los roles de Azure RBAC** proporcionan una administración de acceso más detallada a los recursos de Azure. Existen cuatro roles integrados fundamentales:

- **Propietario**. Tiene acceso total a todos los recursos, incluido el derecho a delegar este acceso a otros. Al administrador de servicios y a los coadministradores se les asigna el rol Propietario en el ámbito de la suscripción.
- **Colaborador**. Puede crear y administrar todos los tipos de recursos de Azure, pero no puede conceder acceso a otros.
- **Lector**. Puede ver los recursos existentes de Azure.
- **Administrador de acceso de usuario**. Permite administrar el acceso de usuario a los recursos de Azure.

Una cuenta de usuario miembro es un miembro nativo de la organización de Azure AD que tiene un conjunto de permisos predeterminados, como poder administrar su información de perfil. **El rol de usuario miembro** está pensado para aquellos usuarios que se consideran internos de una organización y que son miembros de la organización de Azure AD**.**

Los usuarios invitados tienen permisos de organización de Azure AD restringidos. Cuando invitamos a alguien a colaborar en nuestra organización, lo que haremos será agregarlo a la organización de Azure AD como usuario invitado.

Azure AD ayuda a proporcionar derechos de acceso a un solo usuario o a un grupo de usuarios entero. Existen diferentes maneras de asignar derechos de acceso:

- **Asignación directa**: asigne a un usuario los derechos de acceso que necesite asignándole directamente un rol que tenga esos derechos de acceso.
- **Asignación de grupos**: asigne a un grupo los derechos de acceso que necesite. Los miembros del grupo heredarán dichos derechos.
- **Asignación basada en reglas**: use reglas para determinar la pertenencia a un grupo en función de las propiedades de usuario o de dispositivo. Para que la pertenencia a un grupo de una cuenta de usuario o de un dispositivo sea válida, el usuario o el dispositivo en cuestión deben cumplir las reglas.

Azure Active Directory (Azure AD) de negocio a negocio (B2B) permite agregar personas de otras empresas al inquilino de Azure AD como usuarios invitados.

El control de acceso basado en rol de Azure (Azure RBAC) es un sistema de autorización de Azure que ayuda a administrar quién tiene acceso a los recursos de Azure, qué puede hacer con esos recursos y a qué áreas puede acceder. **El control de acceso basado en rol de Azure (Azure RBAC)** es un sistema de autorización integrado en Azure Resource Manager que proporciona administración de acceso específico a los recursos de Azure. Con Azure RBAC, puede conceder el acceso que los usuarios necesitan para realizar sus trabajos.

Una **entidad de seguridad** es simplemente un nombre extravagante para un usuario, un grupo o una aplicación a los que quiere conceder acceso. Una **definición de roles** es una recopilación de permisos. Una **asignación de roles** es el proceso de enlazar un rol a una entidad de servicio en un ámbito determinado con el fin de conceder acceso. **Azure RBAC** es un modelo de permiso. Lo que significa que, cuando se le asigna un rol, Azure RBAC le permite realizar determinadas acciones, como leer, escribir o eliminar.

El orden de herencia para el ámbito es grupo de administración, suscripción, grupo de recursos, recurso. Por ejemplo, si ha asignado el rol Colaborador a un grupo en el nivel del ámbito de la suscripción, todos los recursos y grupos de recursos heredarán dicho rol.

El autoservicio de restablecimiento de contraseña (**SSPR**) de Azure Active Directory (Azure AD) ofrece a los usuarios la posibilidad de cambiar o restablecer su contraseña sin necesidad de que intervenga el administrador o el departamento de soporte técnico.

En el portal de restablecimiento se llevan a cabo estos pasos:

1. **Localización**: El portal comprueba la configuración regional del explorador y representa la página SSPR en el idioma correspondiente.
2. **Comprobación**: el usuario escribe su nombre de usuario y pasa un captcha para garantizar que es un usuario, y no un robot.
3. **Autenticación**: el usuario escribe los datos necesarios para autenticar su identidad; por ejemplo, podría escribir un código o responder preguntas de seguridad.
4. **Restablecimiento de contraseña**: Si el usuario pasa las pruebas de autenticación, puede escribir una nueva contraseña y confirmarla.
5. **Notificación**: se envía un mensaje al usuario para confirmar el restablecimiento.

Hay tres opciones de configuración en la propiedad **Se habilitó el restablecimiento de contraseña del autoservicio**:

- **Deshabilitado**: ningún usuario de la organización de Azure AD puede usar SSPR. Este es el valor predeterminado.
- **Habilitado**: todos los usuarios de la organización de Azure AD pueden usar SSPR.
- **Seleccionado**: solo los miembros del grupo de seguridad especificado pueden usar SSPR.

Implementación y administración del almacenamiento en Azure.

Azure Storage es la solución de almacenamiento de Microsoft para los escenarios modernos de almacenamiento de datos. Azure Storage ofrece un almacén de objetos que se puede escalar de forma masiva destinado a objetos de datos, un servicio de sistema de archivos para la nube, un almacén de mensajería para mensajería confiable y un almacén NoSQL. Azure Storage se caracteriza por ofrecer lo siguiente:

- **Duradero y altamente disponible**. La redundancia garantiza que los datos estén seguros durante errores de hardware transitorios. Puede replicar datos entre centros de datos o regiones geográficas para obtener protección frente a catástrofes locales o desastres naturales. Los datos replicados siguen teniendo una alta disponibilidad en caso de una interrupción inesperada.
- **Seguro**. El servicio cifra todos los datos escritos en Azure Storage. Azure Storage proporciona un control pormenorizado sobre quién tiene acceso a los datos.
- **Escalable**. Azure Storage está diseñado para poderse escalar de forma masiva para satisfacer las necesidades de rendimiento y almacenamiento de datos de las aplicaciones de hoy en día.
- **Administrado**. Microsoft Azure controla automáticamente el mantenimiento, las actualizaciones y los problemas críticos del hardware.
- **Accesible**. Es posible acceder a los datos de Azure Storage desde cualquier parte del mundo a través de HTTP o HTTPS. Microsoft proporciona SDK para Azure Storage en diversos lenguajes: .NET, Java, Node.js, Python, PHP, Ruby, Go y API REST

- **Azure Storage** es un servicio que puede usar para almacenar archivos, mensajes, tablas y otros tipos de información. Azure Storage se usa para aplicaciones como recursos compartidos de archivos. En general, puede englobar Azure Storage en tres categorías:

- **Almacenamiento para máquinas virtuales**. El almacenamiento de una máquina virtual incluye discos y archivos. Los discos son almacenamiento en bloque persistente para máquinas virtuales de IaaS de Azure. Los archivos son recursos compartidos de archivos totalmente administrados en la nube.

- **Datos no estructurados**. Los datos no estructurados incluyen blobs y Data Lake Store. Los blobs son un almacén de objetos en la nube basado en REST y altamente escalable. Data Lake Store es el Sistema de archivos distribuido Hadoop (HDFS) como servicio.

- **Datos estructurados**. Los datos estructurados incluyen tablas, Cosmos DB y Azure SQL DB. Las tablas son un almacén NoSQL de escalado automático de clave-valor. Cosmos DB es un servicio de base de datos distribuido globalmente. Azure SQL DB es una base de datos como servicio totalmente administrada que se basa en SQL.

Azure Storage incluye estos servicios de datos, a los que se accede mediante una cuenta de almacenamiento.

- **Contenedores de Azure (blobs)**: almacén de objetos que se puede escalar de forma masiva para datos de texto y binarios.
- **Azure Files**: recursos compartidos de archivos administrados para implementaciones locales y en la nube.
- **Colas de Azure**: un almacén de mensajería para mensajería confiable entre componentes de aplicación.
- **Tablas de Azure**: un almacén NoSQL para el almacenamiento sin esquema de datos estructurados.

Azure Blob Storage es la solución de almacenamiento de objetos de Microsoft para la nube. Blob Storage está optimizado para el almacenamiento de cantidades masivas de datos no estructurados, como texto o datos binarios. Blob Storage resulta muy conveniente para lo siguiente:

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

Azure Files le permite configurar recursos compartidos de archivos de red de alta disponibilidad. Se puede acceder a los recursos compartidos mediante el protocolo de Bloque de mensajes del servidor (SMB) y el protocolo Network File System (NFS).

El servicio **Azure Queue** se utiliza para almacenar y recuperar mensajes. Los mensajes de la cola pueden tener un tamaño de hasta 64 KB y una cola contener millones de mensajes. Las colas se usan para almacenar listas de mensajes y procesarlas de forma asincrónica. **Azure Table Storage** ahora forma parte de Azure Cosmos DB. Además del servicio Azure Table Storage existente, hay una nueva Table API de Azure Cosmos DB que ofrece tablas con rendimiento optimizado, distribución global e índices secundarios automáticos. El almacenamiento en tablas es ideal para almacenar datos estructurados y no relacionales.

Cuenta de almacenamiento	Uso recomendado
De uso general estándar, v2	La mayoría de los escenarios incluyen Blob, File, Queue, Table y Data Lake Storage.
Blobs en bloques Premium	Escenarios de blob en bloques con altas tasas de transacciones, o bien escenarios que usan objetos más pequeños o que requieren una latencia de almacenamiento constantemente baja.
Recursos compartidos de archivos Prémium	Aplicaciones de recursos compartidos de archivos de alto rendimiento o empresariales.
Blobs en páginas Premium	Escenarios de blobs en páginas de alto rendimiento prémium.

Los datos de la cuenta de almacenamiento de Azure se replican siempre para garantizar su durabilidad y alta disponibilidad. La replicación de Azure Storage copia sus datos para que estén protegidos ante eventos tanto planeados como no. **La replicación** garantiza que la cuenta de almacenamiento cumpla el contrato de nivel de servicio (SLA) para Storage, incluso en caso de errores.

LRS es la **opción de replicación de costo más bajo** y ofrece la menor durabilidad en comparación con otras opciones. Si se produce un desastre en el nivel de centro de datos (por ejemplo, un incendio o una inundación), **es posible que todas las réplicas se pierdan o que no se puedan recuperar**.

El almacenamiento con redundancia de zona (ZRS) replica los datos de manera sincrónica en tres clústeres de almacenamiento en una sola región. Cada clúster de almacenamiento está separado físicamente de los demás y reside en su propia zona de disponibilidad.

El almacenamiento con redundancia geográfica **(GRS) replica los datos en una región secundaria**.GRS proporciona un mayor nivel de durabilidad **incluso en caso de interrupción regional**. GRS está diseñado para proporcionar al menos 99,9999999999999999 % **(16 nueves) de durabilidad**.

El almacenamiento con redundancia de zona geográfica **(GZRS) combina la alta disponibilidad del almacenamiento con redundancia de zona y la protección frente a interrupciones regionales que proporciona el almacenamiento con redundancia geográfica**. Los datos de una cuenta de almacenamiento de GZRS se replican en las zonas de disponibilidad de Azure en la región primaria y también en una región geográfica secundaria para la protección frente a desastres regionales.

Almacenamiento de blobs de Azure es un servicio que almacena datos no estructurados en la nube como objetos o blobs. El Almacenamiento de blobs puede almacenar cualquier tipo de datos binarios o texto, como un documento, un archivo multimedia o un instalador de aplicación. El Almacenamiento de blobs a veces se conoce como "almacenamiento de objetos".

El almacenamiento de blobs suele usarse para realizar las siguientes tareas:

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

Blob Storage ofrece tres tipos de recursos:

- La cuenta de almacenamiento
- Contenedores en la cuenta de almacenamiento
- Blobs en un contenedor

Los contenedores proporcionan una agrupación de un conjunto de blobs. Todos los blobs deben estar en un contenedor.

- Use **Privado** para asegurarse de que no haya ningún acceso anónimo al contenedor o a los blobs.
- Use **Blob** para permitir el acceso de lectura público anónimo solo a los blobs.
- Use **Contenedor** para permitir el acceso de lista y de lectura público anónimo a todo el contenedor, incluidos los blobs.

Azure Storage proporciona diferentes opciones para acceder a los datos de blobs en bloques, en función de patrones de uso.

Frecuente. El nivel de acceso frecuente está optimizado para el acceso habitual a objetos de la cuenta de almacenamiento.

Esporádico. El nivel de acceso esporádico está optimizado para almacenar grandes cantidades de datos a los que se accede con poca frecuencia y que llevan guardados al menos 30 días.

Archivo. Este nivel está destinado a los datos que pueden tolerar varias horas de latencia de recuperación y que permanecerán en el nivel de almacenamiento de archivo durante un mínimo de 180 días.

Un **blob** puede ser un archivo de cualquier tipo y tamaño. Azure Storage ofrece tres tipos de blobs: blobs *en* ***bloques***, blobs *en* ***páginas*** y blobs *en* ***anexos***.

- **Los blobs en bloques (valor predeterminado)** constan de bloques de datos ensamblados para crear un blob. En la mayoría de los escenarios en los que se usa Blog Storage se emplean blobs en bloques. Resultan ideales para almacenar datos de texto y binarios en la nube, como archivos, imágenes y vídeos.
- Los **blobs en anexos** son como blobs en bloques, ya que están compuestos por bloques, pero están optimizados para operaciones de anexión, por lo que resultan útiles en escenarios de registro.
- Los **blobs en páginas** pueden tener un tamaño de hasta 8 TB y son más eficaces para operaciones frecuentes de lectura y escritura. Azure Virtual Machines usa blobs en páginas como discos de sistema operativo y de datos.

Existen varios métodos para cargar datos en el almacenamiento de blobs, incluidos los siguientes:

- **AzCopy** es una herramienta de línea de comandos fácil de usar para Windows y Linux que realiza operaciones de copia con Blob Storage en ambas direcciones, entre contenedores o entre cuentas de almacenamiento.
- La **Biblioteca de movimiento de datos de Azure Storage** es una biblioteca de .NET para mover datos entre los servicios de Azure Storage. La utilidad AzCopy está creada con la Biblioteca de movimiento de datos.
- **Azure Data Factory** admite operaciones de copia de datos con Blob Storage en ambas direcciones mediante el uso de una clave de cuenta, una firma de acceso compartido, una entidad de servicio o identidades administradas paras las autenticaciones de recursos de Azure.
- **Blobfuse** es un controlador de sistema de archivos virtual para Azure Blob Storage. Puede usar blobfuse para acceder a los datos

de blob de bloque existentes en la cuenta de Storage a través del sistema de archivos de Linux.
- **Azure Data Box Disk** es un servicio para transferir datos locales al almacenamiento de blobs cuando los grandes conjuntos de datos o las restricciones de red hacen que la carga de datos a través del cable no sea realista. Puede usar discos de Azure Data Box para solicitar discos de estado sólido (SSD) a Microsoft. A continuación, puede copiar los datos en esos discos y enviarlos de vuelta a Microsoft para su carga en Blob Storage.
- El servicio **Azure Import/Export** proporciona una forma de exportar grandes cantidades de datos de la cuenta de almacenamiento a las unidades de disco duro que usted proporcione y que Microsoft después le devolverá con los datos.

Todas las solicitudes realizadas en un recurso protegido en Blob, File, Queue o Table service deben estar autorizadas.

- **Azure Active Directory (Azure AD)** . Azure AD es un servicio de administración de acceso e identidades basado en la nube de Microsoft. Con Azure AD, puede asignar acceso específico a usuarios, grupos o aplicaciones a través del control de acceso basado en rol (RBAC).
- **Clave compartida**. La autorización de clave compartida se basa en las claves de acceso de la cuenta y otros parámetros para generar una cadena de firma cifrada que se pasará en la solicitud en el encabezado de autorización.
- **Firmas de acceso compartido**. Las firmas de acceso compartido (SAS) delegan el acceso a un recurso determinado de la cuenta con los permisos especificados y durante un intervalo de tiempo especificado.
- **Acceso anónimo a contenedores y blobs**. Opcionalmente, puede hacer que los recursos de blobs se hagan públicos en los contenedores o blobs. Cualquier usuario puede acceder a un contenedor o blob público para consultarlo de forma anónima. Las solicitudes de lectura para contenedores y blobs públicos no requieren autorización.

Una Firma de acceso compartido (SAS) es un URI que concede derechos de acceso restringidos a recursos de Azure Storage. Una SAS es una forma segura de compartir los recursos de almacenamiento sin poner en peligro las claves de cuenta. SAS proporciona tanto control de **nivel de cuenta** como de **nivel de servicio**.

Una Firma de acceso compartido (SAS) ofrece acceso delegado seguro a los recursos en la cuenta de almacenamiento. Con una SAS, tiene control granular sobre la forma en que un cliente puede tener acceso a los datos. Por ejemplo:

- A qué recursos puede acceder el cliente.
- Qué permisos tienen para esos recursos.
- Cuánto tiempo es válida la SAS.

Azure Storage admite tres tipos de firmas de acceso compartido:

- SAS de delegación de usuarios
- SAS de servicio
- SAS de cuenta

Una **SAS de delegación de usuarios** está protegida con credenciales de Azure Active Directory (Azure AD) y también con los permisos especificados para la SAS. Una SAS de delegación de usuarios solo se aplica a Blob Storage.

Una **SAS de servicio** está protegida con la clave de cuenta de almacenamiento. Una SAS de servicio administra el acceso a un recurso en solo uno de los servicios de Azure Storage: Blob Storage, Queue Storage, Table Storage o Azure Files.

Una **SAS de cuenta** está protegida con la clave de cuenta de almacenamiento. SAS de cuenta delega el acceso a los recursos en uno o varios de los servicios de almacenamiento.

El URI consta del URI del recurso de almacenamiento y el token de SAS.

El **token de SAS** es una cadena que se genera del lado cliente, por ejemplo, mediante una de las bibliotecas cliente de Azure Storage.

Azure **Storage Service Encryption** (SSE) para datos en reposo protege sus datos asegurándose de cumplir con los compromisos de seguridad y cumplimiento de la organización.

SSE cifra automáticamente los datos antes de guardarlos en discos administrados por Azure, Azure Blob, Queue, Table Storage o Azure Files y descifra los datos antes de la recuperación. **Azure Key Vault** puede administrar las claves de cifrado. Puede crear sus propias claves de cifrado y almacenarlas en un almacén de claves, o puede usar las API de Azure Key Vault para generar las claves de cifrado.

Azure Files ofrece recursos compartidos de archivos totalmente administrados en la nube a los que se puede acceder mediante el protocolo estándar del sector Bloque de mensajes del servidor (SMB). Los recursos compartidos de Azure Files se pueden montar simultáneamente en implementaciones de Windows, Linux y macOS en la nube o locales. *Usa el protocolo SMB que comunica a través del puerto TCP 445.* **Azure Files** proporciona la funcionalidad de tomar instantáneas de recurso compartido de recursos compartidos de archivos. Las instantáneas de recursos compartidos capturan una copia de solo lectura de un momento dado de los datos.

Use **Azure File Sync** para centralizar los recursos compartidos de archivos de su organización en Azure Files sin renunciar a la flexibilidad, el rendimiento y la compatibilidad de un servidor de archivos local.

La nube por niveles es una característica opcional de Azure File Sync por la que los archivos a los que se tiene acceso con frecuencia se almacenan en caché localmente en el servidor mientras que todos los demás archivos se organizan en niveles en Azure Files, según la configuración de directiva.

Servicio de sincronización de almacenamiento. El servicio de sincronización de almacenamiento es el recurso de nivel superior de Azure para Azure File Sync. El recurso de este servicio es un elemento del mismo nivel del recurso de la cuenta de almacenamiento y también se puede implementar en grupos de recursos de Azure.

Grupo de sincronización. Un grupo de sincronización define la topología de sincronización de un conjunto de archivos. Los puntos de conexión dentro de un grupo de sincronización se mantienen sincronizados entre sí.

Servidor registrado. El objeto de servidor registrado representa una relación de confianza entre el servidor (o clúster) y el servicio de sincronización de almacenamiento.

Agente de Azure File Sync. El agente de Azure File Sync es un paquete descargable que permite la sincronización de Windows Server con un recurso compartido de archivos de Azure. El agente de Azure File Sync consta de tres componentes principales:

- FileSyncSvc.exe: servicio de Windows en segundo plano responsable de supervisar los cambios en los puntos de conexión de servidor y de iniciar las sesiones de sincronización en Azure.
- StorageSync.sys: el filtro del sistema de archivos de Azure File Sync, responsable de apilar los archivos en Azure Files (cuando está habilitada la característica de niveles de la nube).
- Cmdlets de administración de PowerShell: cmdlets de PowerShell para la interacción con el proveedor de recursos de Azure Microsoft.StorageSync.

Punto de conexión de servidor. Un punto de conexión de servidor representa una ubicación específica en un servidor registrado, como una carpeta en un volumen de servidor.

Punto de conexión de nube. Un punto de conexión de nube es un recurso compartido de archivos de Azure que forma parte de un grupo de sincronización.

Explorador de Azure Storage es una aplicación independiente que facilita el trabajo con los datos de Azure Storage en Windows, macOS y Linux. Con Explorador de Storage, puede acceder a varias cuentas y suscripciones y administrar todo el contenido de almacenamiento.

El servicio **Azure Import/Export** se usa para importar de forma segura grandes cantidades de datos a Azure Blob Storage y Azure Files mediante el envío de unidades de disco a un centro de datos de Azure.

Entre los escenarios en los que esto resultaría útil, se incluyen los siguientes:

- **Migración de datos a la nube**. mueva rápidamente grandes cantidades de datos a Azure de manera rápida y rentable.
- **Distribución de contenido**. envíe rápidamente datos a los sitios de cliente.
- **Copia de seguridad**. Realice copias de seguridad de los datos locales para almacenarlos en Azure Blob Storage.
- **Recuperación de datos**. Recupere una gran cantidad de datos almacenados en Blob Storage y recíbalos en su ubicación local.

La **herramienta Import/Export de Azure** es el recurso de preparación y reparación de unidades de disco que puede utilizar con el servicio Microsoft Azure Import/Export.

AzCopy v10 es la utilidad de línea de comandos de última generación para copiar datos desde y hacia Microsoft Azure Blob y File Storage, y ofrece una interfaz de la línea de comandos rediseñada y una nueva arquitectura para transferencias de datos confiables y de alto rendimiento.

Una **cuenta de almacenamiento** es un contenedor que agrupa un conjunto de servicios de almacenamiento de Azure. En las cuentas de almacenamiento solo se pueden incluir servicios de datos de Azure Storage (Azure Blobs, Azure Files, Azure Queues y Azure Tables).

El **modelo de implementación es** el sistema que Azure utiliza para organizar los recursos. El modelo define la API que se usa para crear, configurar y administrar esos recursos. Azure proporciona dos modelos de implementación:

- **Resource Manager**: modelo actual que usa Azure Resource Manager API.
- **Clásico**: oferta heredada que usa Azure Service Management API.

El **tipo de cuenta de almacenamiento** es un conjunto de directivas que determina los servicios de datos que se pueden incluir en la cuenta y el precio de estos. Existen tres tipos de cuentas de almacenamiento:

- **StorageV2 (v2 de uso general)**: oferta actual, compatible con todos los tipos de almacenamiento y las características más recientes.
- **Storage (uso general v1)**: tipo heredado que admite todos los tipos de almacenamiento, pero es posible que no todas las características.
- **Blob Storage**: tipo heredado que solo permite blobs en bloques y blobs en anexos.

El acceso público también se conoce como acceso de lectura público anónimo para contenedores y blobs.

Hay dos configuraciones independientes que afectan al acceso público:

- **Cuenta de almacenamiento.** Configure la cuenta de almacenamiento para permitir el acceso público mediante el establecimiento de la propiedad *AllowBlobPublicAccess*. Cuando se establece en true, los datos de blob solo están disponibles para el acceso público si también se establece la configuración de acceso público del contenedor.
- **Contenedor.** Solo puede habilitar el acceso anónimo si este se ha permitido para la cuenta de almacenamiento. Un contenedor tiene dos opciones de acceso público posibles: *acceso de lectura público para blobs* o *acceso de lectura público para un contenedor y sus blobs*.

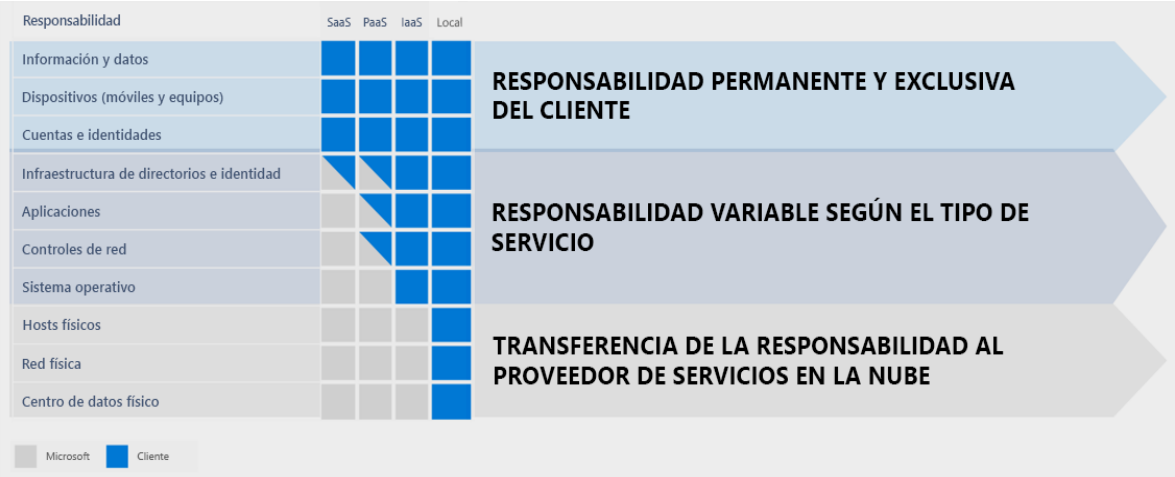
Explorador de Azure Storage puede acceder a muchos tipos de datos diferentes de servicios como los siguientes:

- **Azure Blob Storage**. Blob Storage se utiliza para almacenar datos no estructurados como un objeto binario grande (blob).
- **Azure Table Storage**. Table Storage se usa para almacenar datos NoSQL y semiestructurados.
- **Azure Queue Storage**. Queue Storage se usa para almacenar mensajes en una cola, que las aplicaciones pueden procesar y a los que pueden acceder mediante llamadas HTTP(S).
- **Azure Files**. Azure Files es un servicio de uso compartido de archivos que permite el acceso a través del protocolo Bloque de mensajes del servidor, similar a los servidores de archivos tradicionales.
- **Azure Data Lake Storage**. Azure Data Lake, basado en Apache Hadoop, se ha diseñado para grandes volúmenes de datos y puede almacenar datos estructurados y no estructurados. Azure Data Lake Storage Gen1 es un servicio dedicado. Azure Data Lake Storage Gen2 es Azure Blob Storage con la característica de espacio de nombres jerárquico habilitada en la cuenta.

Azure Data Lake Storage sirve para almacenar y analizar grandes conjuntos de datos. Admite cargas de trabajo de datos de gran tamaño y es muy adecuado para capturar datos de cualquier tipo o tamaño, y a cualquier velocidad.

La aplicación de CRM es un sistema complejo que almacena datos en Azure Storage y Azure Data Lake Storage.

Implementación y administración de recursos de procesos de Azure



Las redes virtuales se usan en Azure para proporcionar conectividad privada entre Azure Virtual Machines y otros servicios de Azure. Las máquinas virtuales y servicios que forman parte de la misma red virtual tienen acceso mutuo.

El nombre de la máquina virtual se usa como nombre del equipo, que está configurado como parte del sistema operativo. Puede especificar un nombre de hasta 15 caracteres en una máquina virtual Windows y hasta 64 caracteres en una máquina virtual Linux.

Las opciones de carga de trabajo se clasifican como se indica a continuación en Azure:

Tipo	Uso de ejemplo
Uso general	Uso equilibrado de la CPU en proporción de memoria. Ideal para desarrollo y pruebas, bases de datos pequeñas o medianas, y servidores web de tráfico bajo o medio.
Proceso optimizado	Uso elevado de la CPU en proporción de memoria. Bueno para servidores web de tráfico medio, aplicaciones de red, procesos por lotes y servidores de aplicaciones.
Memoria optimizada	Memoria alta en proporción de CPU. Excelente para servidores de bases de datos relacionales, memorias caché de capacidad media o grande y análisis en memoria.
Almacenamiento optimizado	Máquina virtual con alto rendimiento de disco y de E/S, idónea para macrodatos, bases de datos SQL y NoSQL, almacenamiento de datos y bases de datos transaccionales grandes.
GPU	Máquinas virtuales especializadas específicas para la representación de gráficos pesados y la edición de vídeo, así como para el entrenamiento e inferencia de modelos (ND) con aprendizaje profundo. Están disponibles con uno o varios GPU.
Informática de alto rendimiento	Nuestras máquinas virtuales de CPU más rápidas y eficaces con interfaces de red de alto rendimiento opcionales (RDMA).

Todas las máquinas virtuales de Azure tienen, como mínimo, **dos discos**: un disco del sistema operativo Windows (en el caso de máquinas virtuales Windows) y un disco temporal, todos los discos se almacenan como discos duros virtuales. Los datos del disco temporal pueden perderse durante un evento de mantenimiento o cuando vuelva a implementar una máquina virtual.

Un disco de datos es un disco administrado que se asocia a una máquina virtual para almacenar datos de aplicaciones u otros datos que necesita mantener. Los discos de datos se registran como unidades SCSI y se etiquetan con una letra elegida por usted.

Azure Premium Storage ofrece soporte de disco de alto rendimiento y latencia baja para máquinas virtuales (VM) con cargas de trabajo intensivas de entrada/salida (E/S).

Azure ofrece dos maneras de crear discos de Premium Storage para las VM:

El método original es usar discos no administrados. En un **disco no administrado**, administra las cuentas de almacenamiento que utiliza para almacenar los archivos del disco duro virtual (VHD) que se corresponden con los discos de VM. Los archivos VHD se almacenan como blobs de páginas en las

Un disco administrado por Azure es un disco duro virtual (VHD). Se puede considerar como un disco físico en un servidor en el entorno local, pero virtualizado. Los discos administrados de Azure se almacenan como blobs en páginas, que son un objeto de almacenamiento de E/S aleatorio en Azure. Llamamos a administrados a estos discos porque es una abstracción sobre los blobs en páginas, los contenedores de blobs y las cuentas de almacenamiento de Azure. Con los discos administrados, lo único que debe hacer es aprovisionar el disco y Azure se encarga del resto.

Azure Bastion es un nuevo servicio PaaS totalmente administrado por la plataforma que se aprovisiona en redes virtuales. Proporciona una conexión RDP/SSH segura e ininterrumpida a las máquinas virtuales directamente en Azure Portal a través de SSL. Cuando se conecta a través de Azure Bastion, las máquinas virtuales no necesitan una dirección IP pública. Bastión proporciona conectividad segura de RDP y SSH a todas las máquinas virtuales en la red virtual en la que se está aprovisionando.

Protocolo de escritorio remoto (RDP) permite establecer una sesión de interfaz gráfica de usuario (GUI) en una máquina virtual de Azure que ejecute cualquier versión compatible de Windows. Puerto TCP 3389

Administración remota de Windows (WinRM) permite establecer una sesión de línea de comandos en una máquina virtual de Azure que ejecute cualquier versión compatible de Windows. También puede usar WinRM para ejecutar scripts de Windows PowerShell que no sean interactivos. Puerto TCP 5986

SSH es un protocolo de conexión cifrada que permite inicios de sesión seguros a través de conexiones no seguras. SSH es el protocolo de conexión predeterminado de las máquinas virtuales Linux hospedadas en Azure.

SSH es con un par de claves públicas y privadas, a las que también se las conoce como claves SSH.

- La **clave pública** se coloca en la máquina virtual Linux o en cualquier otro servicio que se quiera usar con una criptografía de clave pública.
- La **clave privada** permanece en el sistema local. Esta clave se debe proteger, por lo que no se debe compartir.

Azure requiere al menos una longitud de clave de 2048 bits y el formato SSH-RSA para las claves públicas y privadas.

Hay tres escenarios que pueden afectar a la máquina virtual de Azure: mantenimiento de hardware no planeado, tiempo de inactividad inesperado y mantenimiento planeado.

Se produce un evento de **Mantenimiento de hardware no planeado** cuando la plataforma Azure predice que el hardware o cualquier componente de plataforma asociado a una máquina física está a punto de producir un error. Cuando la plataforma predice un error, emitirá un evento de mantenimiento de hardware no planeado. Azure usa tecnología de migración en vivo para migrar las máquinas virtuales del hardware en el que se producen errores a una máquina física en buen estado. Migración en vivo es una operación de conservación de máquinas virtuales que solo pausa la máquina virtual durante un breve periodo de tiempo, pero el rendimiento podría reducirse antes o después del evento.

El **tiempo de inactividad inesperado** ocurre cuando en el hardware o en la infraestructura física de la máquina virtual se produce un error de forma imprevista. El tiempo de inactividad inesperado puede incluir errores de la red local, errores de los discos locales u otros errores de nivel de bastidor. Cuando se detecta, la plataforma Azure migra (recupera) automáticamente la máquina virtual a una máquina física en buen estado en el mismo centro de datos. Durante el procedimiento de recuperación, las máquinas virtuales experimentan tiempos de inactividad (reinicio) y, en algunos casos, pérdidas de la unidad temporal.

Los eventos de **mantenimiento planeado** son actualizaciones periódicas que realiza Microsoft en la plataforma Azure subyacente para mejorar en general la fiabilidad, el rendimiento y la seguridad de la infraestructura de la plataforma sobre las que se ejecutan las máquinas virtuales. La mayoría de estas actualizaciones se realizan sin que las máquinas virtuales ni los servicios en la nube resulten afectados.

Un **conjunto de disponibilidad** es una característica lógica que sirve para asegurarse de que un grupo de máquinas virtuales relacionadas se implementa a fin de que no estén todas sujetas a un único punto de error y no se actualicen a la vez durante una actualización del sistema operativo del host en el centro de datos. Las máquinas virtuales colocadas en un conjunto de disponibilidad deben realizar un conjunto de funcionalidades idéntico y tener el mismo software instalado.

Acuerdos de Nivel de Servicios (SLA):

- Para todas las máquinas virtuales que tengan dos o más instancias implementadas en dos o más zonas de disponibilidad en la misma región de Azure, garantizamos que tendrá conectividad de máquina virtual con al menos una instancia el 99,99 % del tiempo, como mínimo.
- Para todas las máquinas virtuales que tengan dos o más instancias implementadas en el mismo conjunto de disponibilidad, garantizamos que tendrá conectividad de máquina virtual con al menos una instancia el 99,95 % del tiempo, como mínimo.
- Para todas las máquinas virtuales que usen almacenamiento Premium para todos los discos de sistema operativo y de datos, garantizamos una conectividad de la máquina virtual de al menos el 99,9 %.

Los dominios de actualización y los dominios de error permiten a Azure mantener una alta disponibilidad y tolerancia a errores al implementar y actualizar aplicaciones. Cada máquina virtual de un conjunto de disponibilidad se coloca en un dominio de actualización y un dominio de error.

Un **dominio de actualización (UD)** es un grupo de nodos que se actualizan en conjunto durante el proceso de actualización de un servicio (lanzamiento). Un dominio de actualización permite a Azure realizar actualizaciones incrementales o graduales en una implementación.

Un **dominio de error (FD)** es un grupo de nodos que representan una unidad física de error. Un dominio de error define un grupo de máquinas virtuales que comparte un conjunto común de hardware, conmutadores, que a su vez comparten un único punto de error.

Una zona de disponibilidad de una región de Azure es una combinación de un dominio de error y un dominio de actualización. Por ejemplo, si crea tres o más máquinas virtuales en tres zonas de una región de Azure, las máquinas virtuales se distribuyen eficazmente en tres dominios de error y tres dominios de actualización.

- Las zonas de disponibilidad son ubicaciones físicas exclusivas dentro de una región de Azure.
- Cada zona de disponibilidad consta de uno o varios centros de datos equipados con alimentación, refrigeración y redes independientes.
- Para garantizar la resistencia, hay tres zonas independientes como mínimo en todas las regiones habilitadas.
- La separación física de las zonas de disponibilidad dentro de una región protege las aplicaciones y los datos frente a los errores del centro de datos.
- Los servicios con redundancia de zona replican las aplicaciones y los datos entre zonas de disponibilidad para protegerlos frente a puntos de error únicos.
- Con las zonas de disponibilidad, Azure ofrece el mejor Acuerdo de Nivel de Servicio del sector de tiempo de actividad de máquina virtual, con un 99,99 %.

Los servicios de Azure que admiten zonas de disponibilidad se dividen en dos categorías:

- **Servicios de zona**. Ancla el recurso a una zona específica (por ejemplo, máquinas virtuales, discos administrados o direcciones IP estándar).
- **Servicios con redundancia de zona**. La plataforma se replica automáticamente entre zonas (por ejemplo, almacenamiento con redundancia de zona, SQL Database).

El escalado vertical, también conocido como escalar y reducir verticalmente, significa aumentar o disminuir los tamaños de las máquinas virtuales como respuesta a una carga de trabajo. El escalado vertical hace que las máquinas virtuales sean más eficaces (escalar verticalmente) o menos (reducir verticalmente). El escalado vertical puede resultar útil cuando:

- Un servicio integrado en máquinas virtuales se está infrautilizando (por ejemplo, los fines de semana). Reducir el tamaño de la máquina virtual puede disminuir los costos mensuales.
- Aumentar el tamaño de la máquina virtual para hacer frente a una mayor demanda sin crear máquinas virtuales adicionales.

En el **escalado horizontal**, también conocido como escalar horizontalmente y reducir horizontalmente, se modifica el número de máquinas virtuales según la carga de trabajo. En este caso, hay un aumento (escalado horizontal) o una disminución (reducción horizontal) en el número de instancias de máquina virtual. **Los conjuntos de escalado** de máquinas virtuales son un recurso de Azure Compute que se puede usar para implementar y administrar un conjunto de máquinas virtuales **idénticas**. Con todas las máquinas virtuales configuradas de la misma manera, los conjuntos de escalado de máquinas virtuales están diseñados para admitir el escalado automático verdadero. Los conjuntos de escalado admiten hasta 1000 instancias de máquina virtual. Si crea y carga sus propias imágenes de máquina virtual personalizadas, el límite es 600 instancias.

Las extensiones de máquina virtual de Azure son aplicaciones pequeñas que realizan tareas de automatización y configuración posteriores a la implementación en máquinas virtuales de Azure. hay varias maneras de automatizar las tareas de creación, mantenimiento y eliminación de máquinas virtuales. Uno de los métodos es usar una **extensión** de máquina virtual.

La extensión de script puede realizar tareas sencillas, como detener la máquina virtual o instalar un componente de software, pero el script podría ser más complejo y realizar una serie de tareas.

Desired State Configuration (DSC) es una plataforma de administración en Windows PowerShell. DSC permite implementar y administrar datos de configuración para servicios de software y administrar el entorno en el que se ejecutan estos servicios. DSC se centra en la creación de *configuraciones*. **Una configuración** es un script fácil de leer que describe un entorno compuesto por equipos (nodos) con características específicas. Las extensiones de script personalizado tienen 90 minutos para ejecutarse. Si la implementación supera este tiempo, se marca como tiempo de expiración.

Un plan de App Service define un conjunto de recursos de proceso para que una aplicación web se ejecute.

- **Básico**. El plan de servicio Básico está diseñado para aplicaciones que tienen requisitos de tráfico más bajos y no necesitan características avanzadas de escalado automático ni administración del tráfico. Los precios se basarán en el tamaño y el número de instancias que ejecute. La compatibilidad integrada con el equilibrio de carga de red distribuye automáticamente el tráfico entre instancias. El plan de servicio Básico con entornos en tiempo de ejecución de Linux admite Web App for Containers.
- **Estándar**. El plan de servicio Estándar está diseñado para ejecutar cargas de trabajo de producción. Los precios se basarán en el tamaño y el número de instancias que ejecute. La compatibilidad integrada con el equilibrio de carga de red distribuye automáticamente el tráfico entre instancias. El plan Estándar incluye un escalado automático que puede ajustar automáticamente el número de instancias de máquina virtual que se ejecutan para satisfacer sus necesidades de tráfico. El plan de servicio Estándar con entornos en tiempo de ejecución de Linux admite Web App for Containers.
- **Premium**. El plan de servicio Premium está diseñado para proporcionar un rendimiento mejorado para las aplicaciones de producción. El plan Premium actualizado, Premium v2, incluye máquinas virtuales de la serie Dv2 con procesadores más rápidos, almacenamiento SSD y doble relación memoria-núcleo en comparación con el plan Estándar. El nuevo plan Premium permite también una escala mayor con un número más alto de instancias, al tiempo que proporciona toda la funcionalidad avanzada del plan Estándar. La primera generación del plan Premium sigue estando disponible para las necesidades de escalado de los clientes existentes.
- **Aislada**. El plan de servicio Aislado está diseñado para ejecutar cargas de trabajo de misión crítica que son necesarias para ejecutarse en una red virtual. El plan Aislado permite a los clientes ejecutar sus aplicaciones en un entorno privado dedicado en un centro de datos de Azure mediante máquinas virtuales de la serie Dv2 con procesadores más rápidos, almacenamiento SSD y el doble de la relación memoria-núcleo en comparación con el plan Estándar. El entorno privado que se usa con un plan Aislado se denomina App Service Environment. El plan se puede escalar a 100 instancias con más disponibles a petición.

Escalado vertical: obtenga más CPU, memoria, espacio en disco y características adicionales como máquinas virtuales exclusivas, dominios y certificados personalizados, espacios de ensayo, auto escala y mucho más. Para escalar verticalmente, se cambia el plan de tarifa del plan de App Service al que pertenece la aplicación.

Escalado horizontal: se aumenta el número de instancias de máquina virtual que ejecutan la aplicación. Se puede escalar horizontalmente hasta un máximo de 30 instancias, según el plan de tarifa. Entornos de App Service en el nivel Aislado aumenta aún más el recuento de escalado horizontal a 100 instancias. El recuento de instancias de escalado se puede configurar manual o automáticamente (escalado automático). El escalado automático se basa en reglas y programaciones predefinidas.

- **Basado en métricas**. Las reglas basadas en métricas miden la carga de la aplicación y agregan o quitan máquinas virtuales en función de ella. Por ejemplo, realice esta acción cuando el uso de la CPU sea superior al 50 %. Algunos ejemplos de métricas son el tiempo de la CPU, el tiempo medio de respuesta y las solicitudes.

- **Basado en tiempo**. Las reglas basadas en tiempo (basadas en la programación) le permiten realizar un escalado cuando ve los patrones de tiempo de la carga y quiere realizar un escalado antes de que se produzca un posible aumento o disminución de la carga. Por ejemplo, puede desencadenar un webhook todos los sábados a las 8:00 en una zona horaria determinada.

Configuración de Azure App Services

Azure App Service es un servicio basado en HTTP para hospedar aplicaciones web. Puede desarrollar en su lenguaje favorito. Las aplicaciones se ejecutan y escalan fácilmente en los entornos Windows y Linux.

- **Siempre activada** mantenga cargada la aplicación, incluso cuando no hay tráfico. Esto es necesario en los WebJobs continuos o WebJobs que se desencadenan mediante una expresión CRON.
- **Afinidad ARR**. en una implementación de varias instancias, asegúrese de que el cliente esté enrutado a la misma instancia de la vida de la sesión.
- **Cadenas de conexión**. Las cadenas de conexión se cifran en reposo y transmiten a través de un canal cifrado.

La implementación automatizada, o **la integración continua**, es un proceso que se usa para insertar nuevas características y correcciones de errores en un patrón repetitivo y rápido con un impacto mínimo en los usuarios finales. Azure admite la implementación automatizada directamente desde varios orígenes. Están disponibles las opciones siguientes:

- **Azure DevOps**: Puede insertar el código en Azure DevOps (anteriormente conocido como Visual Studio Team Services), compilar el código en la nube, ejecutar las pruebas, generar una versión a partir del código y, por último, insertar el código en una aplicación web de Azure.
- **GitHub**: Azure admite la implementación automatizada directamente desde GitHub. Cuando conecte el repositorio de GitHub con Azure para la implementación automatizada, cualquier cambio que inserte en la rama de producción en GitHub se implementará de forma automática.
- **Bitbucket**: con sus similitudes con GitHub, puede configurar una implementación automatizada con Bitbucket.

Un registro A (de "Address", dirección) asigna un nombre de dominio a una dirección IP. **Un registro** CNAME (de "Canonical Name", nombre canónico) asigna un nombre de dominio a otro nombre de dominio. DNS usa el segundo nombre para buscar la dirección.

Application Insights es una característica de Azure Monitor que supervisa las aplicaciones activas. Detectará automáticamente anomalías en el rendimiento e incluye eficaces herramientas de análisis que le ayudan a diagnosticar problemas y a saber lo que hacen realmente los usuarios con la aplicación.

Application Insights está dirigido al equipo de desarrollo y sirve ayudarle a conocer el rendimiento de una aplicación y cómo se utiliza. Supervisa:

- **Tasas de solicitud, tiempos de respuesta y tasas de error** - Averigüe qué páginas que son las más conocidas, en qué momento del día y dónde están los usuarios. Vea qué páginas presentan mejor rendimiento. Si los tiempos de respuesta y las tasas de error aumentan cuando hay más solicitudes, quizás tiene un problema de recursos.
- **Tasas de dependencia, tiempos de respuesta y tasa de error** - Averigüe si los servicios externos le ralentizan.
- **Excepciones**: - Analice las estadísticas agregadas o seleccione instancias concretas y profundice en el seguimiento de la pila y las

solicitudes relacionadas. Se notifican tanto las excepciones de servidor como las de explorador.

- **Vistas de página y rendimiento de carga** - Notificados por los exploradores de los usuarios.
- **Número de usuarios y sesiones**.
- **Contadores de rendimiento** de las máquinas de servidor de Windows o Linux, como CPU, memoria y uso de la red.
- **Diagnóstico de host** de Docker o Azure.
- **Registros de seguimiento de diagnóstico** de la aplicación - De esta forma puede correlacionar eventos de seguimiento con las solicitudes.
- **Métricas y eventos personalizados** que usted mismo escribe en el código de cliente o servidor para realizar un seguimiento de eventos empresariales, como artículos vendidos o partidas ganadas.

Característica	Contenedores	Máquinas virtuales
Aislamiento	Normalmente, proporciona aislamiento ligero del host y otros contenedores, pero no proporciona un límite de seguridad tan sólido como el de una máquina virtual.	Proporciona un aislamiento completo del sistema operativo host y de otras máquinas virtuales. Esto resulta útil cuando es crítico tener un límite de seguridad fuerte, como el hospedaje de aplicaciones de compañías competidoras en el mismo servidor o clúster.
Sistema operativo	Ejecuta la parte del modo de usuario de un sistema operativo y se puede personalizar para que contenga solo los servicios necesarios para la aplicación, con menos recursos del sistema.	Ejecuta un sistema operativo completo incluido el kernel, lo que requiere más recursos del sistema (CPU, memoria y almacenamiento).
Implementación	Implementa contenedores individuales mediante Docker a través de la línea de comandos; implementa varios contenedores con un orquestador como Azure Kubernetes Service.	Implementa máquinas virtuales individuales mediante Windows Admin Center o el administrador de Hyper-V; implementa varias máquinas virtuales mediante PowerShell o System Center Virtual Machine Manager.
Almacenamiento persistente	Usa discos de Azure para el almacenamiento local para un solo nodo o Azure Files (recursos compartidos de SMB) para el almacenamiento compartido por varios nodos o servidores.	Usa un disco duro virtual (VHD) para el almacenamiento local de una sola máquina virtual o un recurso compartido de archivos SMB para el almacenamiento compartido por varios servidores.
Tolerancia a errores	Si se produce un error en un nodo del clúster, el orquestador vuelve a crear rápidamente los contenedores que se ejecutan en él en otro nodo del clúster.	Las máquinas virtuales pueden conmutar por error a otro servidor de un clúster, reiniciando el sistema operativo de la máquina virtual en el nuevo servidor.

Azure Container Instances es una solución excelente para cualquier escenario que pueda funcionar en contenedores aislados. Esto incluye aplicaciones simples, automatización de tareas y trabajos de compilación.

Azure Container Instances ofrece la forma más rápida y sencilla de ejecutar un contenedor en Azure, sin tener que administrar ninguna máquina virtual y sin necesidad de adoptar un servicio de nivel superior. Azure Container Instances es una excelente solución para cualquier escenario que pueda funcionar en contenedores aislados, incluidas las aplicaciones simples, la automatización de tareas y los trabajos de compilación.

El recurso de nivel **superior de Azure Container Instances** es el grupo de contenedores. **Un grupo de contenedores** es una colección de contenedores que se programan en la misma máquina host. Los contenedores de un grupo

comparten un ciclo de vida, los recursos, la red local y los volúmenes de almacenamiento.

Docker es una plataforma que permite a los desarrolladores hospedar aplicaciones en un contenedor. **Un contenedor** es básicamente un paquete independiente que contiene todo lo necesario para ejecutar un componente de software. El paquete incluye lo siguiente:

- Código ejecutable de la aplicación.
- Entorno en tiempo de ejecución (como .NET Core).
- Herramientas del sistema.
- Configuración.

- **Contenedor**. Un contenedor es una instancia de una imagen de Docker. Representa la ejecución de una sola aplicación, proceso o servicio. Está formado por el contenido de una imagen de Docker, un entorno de ejecución y un conjunto estándar de instrucciones. Al escalar un servicio, crea varias instancias de un contenedor a partir de la misma imagen. O bien, un proceso por lotes puede crear varios contenedores a partir de la misma imagen y pasar parámetros diferentes a cada instancia.
- **Imagen de contenedor**. Un imagen de contenedor hace referencia a un paquete con todas las dependencias y la información necesarias para crear un contenedor. Las dependencias incluyen marcos de trabajo y la configuración de implementación y ejecución que usa un entorno de ejecución de contenedor. Normalmente, una imagen se deriva de varias imágenes base que son capas que se apilan unas encima de otras para formar el sistema de archivos del contenedor. Una vez que se crea una imagen, esta es inmutable.
- **Build**. La compilación hace referencia a la acción de crear una imagen de contenedor en función de la información y el contexto que proporciona Dockerfile. La compilación también incluye cualquier otro archivo que se necesite. Las imágenes se compilan mediante el comando de compilación de Docker.
- **Incorporación de cambios**. La incorporación de cambios hace referencia al proceso de descarga de una imagen de contenedor desde un registro de contenedor.
- **Envío de cambios**. El envío de cambios hace referencia al proceso de carga de una imagen de contenedor en un registro de contenedor.
- **Dockerfile**. Dockerfile hace referencia a un archivo de texto que contiene instrucciones sobre cómo crear una imagen de Docker. Dockerfile es como un script por lotes. La primera línea identifica la imagen base. El resto del archivo incluye las acciones de compilación.

- Los **grupos** son grupos de nodos con configuraciones idénticas.
- Los **nodos** son máquinas virtuales individuales que se ejecutan en aplicaciones contenedorizadas.
- Los **pods** son una única instancia de una aplicación. Un pod puede contener varios contenedores.
- Un **contenedor** es una imagen ejecutable portable y ligera que contiene el software y todas sus dependencias.
- Una **implementación** contiene uno o más pods idénticos administrados por Kubernetes.
- Un **manifiesto** es el archivo YAML que permite describir una implementación.

Kubernetes usa servicios para agrupar lógicamente un conjunto de pods y proporcionar conectividad de red. Están disponibles los siguientes tipos de servicio:

- **Dirección IP de clúster**: crea una dirección IP interna para su uso dentro del clúster de AKS. Es útil solo para aplicaciones internas que admiten otras cargas de trabajo dentro del clúster.
- **NodePort**: crea una asignación de puerto en el nodo subyacente que permite que se pueda acceder a la aplicación directamente con la dirección IP del nodo y el puerto.
- **LoadBalancer**: crea un recurso de equilibrador de carga de Azure, configura una dirección IP externa y conecta los pods solicitados al grupo de back-end del equilibrador de carga. Para permitir que el tráfico de los clientes llegue a la aplicación, se crean las reglas de equilibrio de carga en los puertos deseados.
- **ExternalName**: crea una entrada DNS específica para facilitar el acceso a la aplicación.

Un clúster de Kubernetes se divide en dos componentes:

- **Nodos administrados por Azure**, que proporcionan los principales servicios de Kubernetes y la orquestación de las cargas de trabajo de aplicaciones.
- **Nodos administrados por el cliente** que ejecutan las cargas de trabajo de las aplicaciones.

Un ***clúster de AKS*** contiene al menos un nodo (Máquinas virtuales de Azure) que ejecuta los componentes del nodo de Kubernetes y el entorno de ejecución del contenedor.

- El *kubelet* es el agente de Kubernetes que procesa las solicitudes de orquestación del nodo administrado por Azure y la programación de la ejecución de los contenedores solicitados.
- Las redes virtuales se controlan mediante *kube-proxy* en cada nodo. El proxy enruta el tráfico de red y administra las direcciones IP para los servicios y los pods.
- El *entorno de ejecución del contenedor* es el componente que permite que las aplicaciones en contenedor ejecuten recursos adicionales e interactúen con ellos, como la red virtual y el almacenamiento.

Un pod es un recurso lógico, pero el contenedor o los contenedores se refieren al lugar donde se ejecutan las cargas de trabajo de la aplicación. Los pods suelen ser recursos efímeros y descartables.

Un *volumen* representa una manera de almacenar, recuperar y conservar datos entre pods y durante el ciclo de vida de la aplicación. **Un *volumen persistente*** es un recurso de almacenamiento creado y administrado por la API de Kubernetes, que puede existir más allá de la duración de un pod individual.

Diferencias entre los discos no administrados y administrados

Con los discos no administrados, es el responsable de las cuentas de almacenamiento que contienen los discos duros virtuales correspondientes a los discos de máquina virtual. Las tarifas de la cuenta de almacenamiento que se pagan dependen de la cantidad de espacio que se use. Una cuenta de almacenamiento tiene un límite fijo de 20 000 operaciones de E/S por segundo, lo que significa admite 40 discos duros virtuales estándar a máxima potencia. Si tiene que escalar horizontalmente, necesitará más de una cuenta de almacenamiento, lo que puede complicar las cosas.

Los discos administrados son el modelo de almacenamiento en disco más reciente y el recomendado. Solucionan de forma elegante la complejidad de los discos no administrados al pasar a Azure la carga de administrar las cuentas de almacenamiento. Especifique el tipo (Premium o Estándar) y tamaño del disco, y Azure creará y administrará tanto el disco *como* el almacenamiento que use. No tiene que preocuparse por los límites de la cuenta de almacenamiento, lo que facilita el escalado horizontal.

Los grupos de seguridad de red (NSG) son la principal herramienta para aplicar y controlar las reglas de tráfico de red en el nivel de red. Los grupos de seguridad de red son una capa de seguridad opcional que proporciona un firewall de software gracias al filtrado del tráfico entrante y saliente de la red virtual.

State Configuration de Azure Automation se usa para asegurarse de que las máquinas virtuales (VM) de un clúster se encuentren en un estado coherente con el mismo software instalado y las misma configuraciones.
State Configuration de Azure Automation es un servicio de Azure basado en PowerShell. Permite implementar de forma coherente, supervisar de manera confiable y actualizar automáticamente el estado deseado de todos los recursos.

DSC de PowerShell es una plataforma de administración declarativa que usa State Configuration de Azure Automation para configurar, implementar y controlar sistemas.

El administrador de configuración local (LCM) es un componente de Windows Management Framework (WMF) de un sistema operativo Windows. El LCM es responsable de actualizar el estado de un nodo, como una máquina virtual, para que coincida con el estado deseado. Cada vez que se ejecuta el LCM, completa los pasos siguientes:

1. **Get**: obtiene el estado actual del nodo.
2. **Test**: compara el estado actual de un nodo con el estado deseado mediante un script DSC compilado (archivo .mof).
3. **Set**: actualiza el nodo para que coincida con el estado deseado que se describe en el archivo .mof.

Modo de inserción: un administrador envía o *inserta* de forma manual las configuraciones en los nodos. El LCM se asegura de que el estado de cada nodo coincida con el que especifica la configuración.

Modo de extracción: un *servidor de extracción* contiene la información de configuración. El LCM de cada nodo sondea el servidor de extracción a intervalos regulares, de forma predeterminada cada 15 minutos, para obtener los detalles de configuración más recientes.

Configuración y administración de redes virtuales para administradores de Azure

Azure Virtual Network es una representación de su propia red en la nube. Es un aislamiento lógico de la nube de Azure dedicada a su suscripción. Puede usar las redes virtuales para aprovisionar y administrar redes privadas virtuales (VPN) en Azure y, opcionalmente, vincular las redes virtuales con otras redes virtuales en Azure o con sus infraestructura de TI local para crear soluciones híbridas o entre entornos. **Azure Virtual Network** es el bloque de creación básico de una red privada en Azure. Una red virtual permite que muchos tipos de recursos de Azure, como Azure Virtual Machines, se comuniquen de forma segura entre sí, con Internet y con redes locales.

El direccionamiento IP de Azure es fundamental para garantizar que los recursos sean accesibles. Las direcciones IP privadas se usan para la comunicación entre los recursos de Azure. Las IP públicas permiten que los recursos de Azure sean accesibles directamente desde Internet.

Las redes virtuales se pueden usar de muchas formas.

- **Creación de una red virtual dedicada solo en la nube privada**. A veces no necesita una configuración entre entornos para su solución. Cuando se crea una red virtual, los servicios y las máquinas virtuales de la red virtual pueden comunicarse de forma directa y segura entre ellas en la nube. Aun así, puede configurar conexiones de punto de conexión para las máquinas virtuales y los servicios que requieren la comunicación con Internet, como parte de la solución.
- **Ampliación segura del centro de datos con redes virtuales**. Puede crear VPN de sitio a sitio (S2S) tradicionales para escalar la capacidad del centro de datos de forma segura. Las redes virtuales de sitio a sitio (S2S) usan IPSEC para proporcionar una conexión segura entre la puerta de enlace VPN corporativa y Azure.
- **Habilitación de escenarios de nube híbrida**. Las redes virtuales proporcionan la flexibilidad para admitir una variedad de escenarios de nube híbrida. Puede conectar de forma segura aplicaciones basadas en la nube a cualquier tipo de sistema local como grandes sistemas y sistemas Unix.

Una red virtual se puede segmentar en una o más subredes. Las subredes proporcionan divisiones lógicas dentro de la red. Las subredes pueden ayudar a mejorar la seguridad, aumentar el rendimiento y facilitar la administración de la red. Cada subred contiene un intervalo de direcciones IP que están dentro del espacio de direcciones de la red virtual. El espacio de direcciones debe especificarse mediante notación de Enrutamiento de interdominios sin clases (CIDR).

- x.x.x.0: Dirección de red
- x.x.x.1: Reservado por Azure para la puerta de enlace predeterminada
- x.x.x.2, x.x.x.3: Reservado por Azure para asignar las direcciones IP de Azure DNS al espacio de red virtual
- x.x.x.255: Dirección de difusión de red

Instancias de Private Link. Azure Private Link proporciona conectividad privada desde una red virtual a la plataforma como servicio (PaaS) de Azure, propiedad del cliente o servicios de asociados de Microsoft.

Puede asignar direcciones IP a los recursos de Azure para que se comuniquen con otros recursos de Azure, la red local e Internet. Hay dos tipos de direcciones IP en Azure: públicas y privadas.

- **Direcciones IP privadas**: se usan para la comunicación dentro de una red virtual (VNet) de Azure y en la red local, cuando se usa una puerta de enlace de VPN o un circuito ExpressRoute para ampliar la red a Azure.
- **Direcciones IP públicas**: se usan para la comunicación con Internet, incluidos los servicios de acceso público de Azure.

Las direcciones IP también se pueden asignar de forma **estática** o **dinámica**. Las direcciones IP estáticas no cambian y son más recomendables para determinadas situaciones, como las siguientes:

- Resolución de nombres DNS, donde un cambio en la dirección IP requeriría actualizar los registros de host

- Modelos de seguridad basados en direcciones IP que requieren que las aplicaciones o servicios tengan una dirección IP estática
- Certificados TLS/SSL vinculados a una dirección IP.
- Reglas de firewall que permiten o deniegan el tráfico mediante intervalos de direcciones IP
- Máquinas virtuales basadas en roles, como controladores de dominio y servidores DNS

Hay dos tipos de asignaciones de direcciones IP.

- **Dinámica**. las direcciones dinámicas se asignan solo después de que una dirección IP pública se asocia a un recurso de Azure y el recurso se inicia por primera vez. Las direcciones dinámicas pueden cambiar si se asignan a un recurso, como una máquina virtual, y la máquina virtual se detiene (desasigna) y luego se reinicia. La dirección sigue siendo la misma si la máquina virtual se reinicia o se detiene (pero no se desasigna). Las direcciones dinámicas se liberan cuando un recurso de dirección IP pública se desasocia de un recurso.
- **Estática**. las direcciones estáticas se asignan cuando se crea la dirección IP pública. Las direcciones estáticas no se liberan hasta que se elimina un recurso de dirección IP pública. Si la dirección no está asociada a un recurso, puede cambiar el método de asignación después de crear la dirección. Si la dirección está asociada a un recurso, es posible que no pueda cambiar el método de asignación. Si selecciona IPv6 como la versión de dirección IP, el método de asignación debe ser Dinámica para el SKU básico. Las direcciones de SKU estándar son estáticas tanto para IPv4 como para IPv6.

SKU de dirección

Al crear una dirección IP pública, puede elegir una opción de SKU **Básica** o **Estándar**. La elección de la SKU afecta al método de asignación de IP, la seguridad, los recursos disponibles y la redundancia. Esta tabla resume las diferencias.

Característica	SKU básica	SKU estándar
Asignación IP	Estático o dinámico	estática
Seguridad	Abierta de forma predeterminada	Segura de forma predeterminada y cerrada al tráfico de entrada
Recursos	Interfaces de red, instancias de VPN Gateway, instancias de Application Gateway y equilibradores de carga orientados a Internet	Interfaces de red o equilibradores de carga estándar públicos
Redundancia	Sin redundancia de zona	Redundancia de zona de forma predeterminada

Se asigna una dirección IP privada del intervalo de direcciones de la subred de la red virtual en la que se implementa un recurso.

- **Dinámica**. Azure asigna la siguiente dirección IP sin asignar o no reservada disponible en el intervalo de direcciones de la subred. Por ejemplo, Azure asigna 10.0.0.10 a un nuevo recurso, si las direcciones 10.0.0.4 a 10.0.0.9 ya están asignadas a otros. Este es el método de asignación predeterminado.
- **Estática**. seleccione y asigne cualquier dirección IP sin asignar o no reservada en el intervalo de direcciones de la subred. Por ejemplo, si el intervalo de direcciones de una subred es 10.0.0.0/16 y las direcciones 10.0.0.4 a 10.0.0.9 ya están asignadas a otros recursos, puede asignar cualquier dirección entre 10.0.0.10 y 10.0.255.254.

Un grupo de seguridad de red contiene reglas de seguridad que permiten o deniegan el tráfico de red entrante o saliente. Un NSG se puede asociar a una subred o a una interfaz de red. Además, se puede asociar varias veces. **Las reglas** de seguridad de grupos de seguridad de red permiten filtrar el tipo de tráfico de red que puede fluir dentro y fuera de las interfaces de red y las subredes de redes virtuales.

Hay tres reglas de seguridad de entrada predeterminadas. Las reglas deniegan todo el tráfico de entrada, excepto desde la red virtual y los equilibradores de carga de Azure.

AllowVnetInBround

AllowAzureLoadBalancerInBround

DenyAllInBround

Hay tres reglas de seguridad de salida predeterminadas. Las reglas solo permiten el tráfico de salida a Internet y a la red virtual.

AllowVnetOutBround

AllowInternetOutBround

DenyAllOutBround

Los grupos de seguridad de aplicaciones le permiten configurar la seguridad de red como una extensión natural de la estructura de una aplicación, lo que le permite agrupar máquinas virtuales y directivas de seguridad de red basadas en esos grupos. Los ASG funcionan de la misma manera que los NSG, pero proporcionan una manera centrada en la aplicación de examinar la infraestructura. Las máquinas virtuales se conectan al ASG, que después se usa como origen o destino en las reglas de NSG.

Esta configuración tiene varias ventajas:

- Para la configuración no se necesitan direcciones IP específicas. Sería difícil especificar direcciones IP debido al número de servidores y porque las direcciones IP podrían cambiar. Tampoco necesita organizar los servidores en una subred específica.
- Esta configuración no necesita varios conjuntos de reglas. No tiene que crear una regla independiente para cada máquina virtual. Puede aplicar dinámicamente nuevas reglas al ASG. Las nuevas

reglas de seguridad se aplican automáticamente a todas las máquinas virtuales del grupo de seguridad de aplicaciones.
- La configuración es fácil de mantener y comprender, ya que se basa en el uso de la carga de trabajo.

El proceso de aislar y proteger los recursos de red en Azure es muy importante para el trabajo. Los grupos de seguridad de red protegen redes virtuales mediante la creación de reglas para controlar el tráfico de red.

Azure Firewall es un servicio de seguridad de red administrado y basado en la nube que protege los recursos de Azure Virtual Network. Se trata de un firewall como servicio con estado completo que incorpora alta disponibilidad y escalabilidad a la nube sin restricciones. **Azure** Firewall usa una dirección IP pública estática para los recursos de red virtual, que permite que los firewall externos identifiquen el tráfico procedente de la red virtual. El servicio está totalmente integrado con Azure Monitor para los registros y análisis.

- **Alta disponibilidad integrada**. La alta disponibilidad está integrada, por lo que no se requieren equilibradores de carga adicionales. No es necesario que configure nada.
- **Zonas de disponibilidad**. Azure Firewall se puede configurar durante la implementación para abarcar varias zonas de disponibilidad y aumentar la disponibilidad.
- **Escalabilidad en la nube sin restricciones**. Azure Firewall puede escalarse verticalmente todo lo que sea necesario para acoger los flujos de tráfico de red cambiantes, por lo que no es necesario elaborar un presupuesto para el tráfico en su momento álgido.
- **Reglas de filtrado de FQDN de aplicación**. Puede limitar el tráfico HTTP/S o el tráfico de Azure SQL saliente a una lista especificada de nombres de dominio completos (FQDN) que incluye caracteres comodín.
- **Reglas de filtrado de tráfico de red**. Puede crear centralmente reglas de filtrado de red para permitir o denegar por dirección IP de origen y destino, puerto y protocolo. Azure Firewall tiene estado completo, de modo que puede distinguir los paquetes legítimos de diferentes tipos de conexiones. Las reglas se aplican y se registran en varias suscripciones y redes virtuales.
- **Información sobre amenazas**. El filtrado basado en inteligencia sobre amenazas puede habilitarse para que el firewall alerte y deniegue el tráfico desde y hacia los dominios y las direcciones IP malintencionados. La direcciones IP y los dominios proceden de la fuente Inteligencia sobre amenazas de Microsoft.
- **Varias direcciones IP públicas**. Puede asociar varias direcciones IP públicas al firewall.

Al implementar un firewall, se recomienda usar una topología en estrella tipo **hub-and-spoke**.

- El *centro* es una red virtual en Azure que actúa como punto central de conectividad para la red local.
- Los *radios* son redes virtuales que se emparejan con el centro y que se pueden usar para aislar las cargas de trabajo.
- El tráfico fluye entre el centro de datos local y el concentrador a través de una conexión a ExpressRoute o a VPN Gateway.

Hay tres tipos de reglas que puede configurar en Azure Firewall:

Reglas NAT. La traducción de direcciones de red de destino (DNAT) de Azure Firewall se puede configurar para traducir y filtrar el tráfico que entra a las subredes. Todas las reglas de la colección de reglas NAT pueden usarse para traducir la dirección IP y el puerto públicos del firewall a una dirección IP y puerto privados.

Reglas de Red. Cualquier tráfico que no sea HTTP/S que pueda fluir a través del firewall debe tener una regla de red. Por ejemplo, si los recursos de una subred deben comunicarse con los recursos de otra subred, configuraría una regla de red del origen al destino.

Reglas de Aplicación. Las reglas de aplicación definen los nombres de dominio completo (FQDN) a los que se puede acceder desde una subred. Por ejemplo, especifique el tráfico de red de Windows Update a través del firewall.

Azure Firewall actúa como barrera entre la red virtual de Azure e Internet. Azure Firewall examina todo el tráfico entrante y saliente. Azure Firewall usa inteligencia sobre amenazas, reglas y otras configuraciones de directiva para permitir el tráfico legítimo y denegar el que supone una amenaza o es desconocido.

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

- Debe ser un administrador global para realizar tareas de administración de dominios. El administrador global es el usuario que creó la suscripción.
- Los nombres de dominio en Azure AD son únicos globalmente. Cuando un directorio de Azure AD ha comprobado un nombre de dominio, no pueden usar ese nombre otros directorios.
- Para que Azure AD pueda usar un nombre de dominio personalizado, dicho nombre debe agregarse al directorio y comprobarse.

Azure DNS proporciona un servicio DNS seguro y confiable para administrar y resolver los nombres de dominio de una red virtual sin necesidad de agregar una solución DNS personalizada.

Es importante comprender la diferencia entre los conjuntos de registros de DNS y los registros DNS individuales. Un conjunto de registros es una colección de registros de una zona con el mismo nombre y el mismo tipo. Los conjuntos de registros de tipo **CNAME** pueden contener, como máximo, un registro.

El **registro A o AAAA** asigna una dirección IP a un dominio. Varias direcciones IP se denominan conjunto de registros.

DNS privado de Azure permite administrar y resolver nombres de dominio en una red virtual sin agregar una solución DNS personalizada.

Azure DNS hospeda los dominios registrados. Los administradores pueden controlar y configurar los registros de dominio, como A, CNAME o MX, y configurar registros de alias.

El emparejamiento de red virtual conecta redes virtuales en una topología en estrella tipo hub-and-spoke. El emparejamiento de red virtual es rentable y fácil de configurar.

Existen dos tipos de emparejamiento de red virtual:

- El **emparejamiento de red virtual regional** conecta redes virtuales de Azure de la misma región.
- El **emparejamiento de VNet** conecta redes virtuales de Azure de regiones diferentes. Al crear un emparejamiento global, las redes virtuales emparejadas pueden existir en cualquier región de la nube pública de Azure, pero no en las regiones de la nube de Government. Solo se pueden emparejar redes virtuales de la misma región que existan en regiones de la nube de Azure Government.

Cuando las redes virtuales están emparejadas, puede configurar una instancia de VPN Gateway en la red virtual emparejada como punto de tránsito. En este caso, una red virtual emparejada usa la puerta de enlace remota para obtener acceso a otros recursos. Una red virtual no puede tener más de una puerta de enlace. Se admite el tránsito de puerta de enlace tanto para el emparejamiento de VNet como para el emparejamiento de VNet global. Cuando se permite el tránsito de puerta de enlace, la red virtual puede comunicarse con recursos de fuera del emparejamiento. Por ejemplo, la puerta de enlace de subred podría hacer lo siguiente:

- Usar una VPN de sitio a sitio para conectarse a una red local.
- Usar una conexión de red virtual a red virtual a otra red virtual.
- Usar una VPN de punto a sitio para conectarse a un cliente.

El emparejamiento de red virtual no es transitivo. Al establecer el emparejamiento de red virtual entre VNet1 y VNet2 y entre VNet2 y VNet3, las funcionalidades de emparejamiento de red virtual no se aplican entre VNet1 y VNet3. Aun así, puede configurar rutas definidas por el usuario y encadenamiento de servicios para proporcionar transitividad.

Al implementar redes en estrella tipo hub-and-spoke, la red virtual de concentrador puede hospedar componentes de la infraestructura, como la aplicación virtual de red o una instancia de VPN Gateway. Todas las redes virtuales de radio se pueden emparejar con la red virtual de concentrador. El tráfico puede fluir por las aplicaciones virtuales de red o puertas de enlace de VPN que se ejecutan en la red virtual de concentrador.

El emparejamiento de red virtual permite que el próximo salto de una ruta definida por el usuario sea la dirección IP de una máquina virtual de la red virtual emparejada o en una puerta de enlace de VPN.

El encadenamiento de servicios permite definir rutas de usuario. Dichas rutas dirigen el tráfico de una red virtual a una aplicación virtual, o bien a una puerta de enlace de red virtual.

Estado del emparejamiento de red virtual:

- **Iniciado**: cuando se crea el emparejamiento a la segunda red virtual desde la primera, el estado de emparejamiento es Iniciado.
- **Conectado**: cuando se crea el emparejamiento desde la segunda red virtual a la primera, el estado de emparejamiento es Conectado. El emparejamiento no se habrá establecido correctamente mientras el estado de ambos emparejamientos de red virtual no sea Conectado.

El tránsito de puerta de enlace permite que las redes virtuales emparejadas compartan la puerta de enlace y obtengan acceso a los recursos.

VPN Gateway es un tipo específico de puerta de enlace de red virtual que se usa para enviar tráfico cifrado entre una red virtual de Azure y una ubicación local a través de la red pública de Internet. También puede usar una instancia de VPN Gateway para enviar tráfico cifrado entre las redes virtuales de Azure a través de la red de Microsoft. Cada red virtual solo puede tener una instancia de VPN Gateway.

- Las conexiones **de sitio a sitio** conectan los centros de datos locales a redes virtuales de Azure.
- Las conexiones **de red virtual a red virtual** conectan redes virtuales de Azure (personalizadas).
- Las conexiones **de punto a sitio** conectan los dispositivos individuales a redes virtuales de Azure.

Una puerta de enlace de red virtual se compone de dos o más máquinas virtuales que se implementan en una subred específica llamada subred de la puerta de enlace. Las máquinas virtuales de puerta de enlace de red virtual contienen tablas de enrutamiento y ejecutan servicios específicos de puerta de enlace.

Tipos de VPN:

- **VPN basadas en rutas**. Las VPN basadas en enrutamiento utilizan *rutas* en la dirección IP de reenvío o en la tabla de enrutamiento para dirigir los paquetes a sus interfaces de túnel correspondientes. A continuación, las interfaces de túnel cifran o descifran los paquetes dentro y fuera de los túneles. La directiva (o el selector de tráfico) para las VPN basadas en rutas se configura como conectividad de tipo cualquiera a cualquier (o caracteres comodín).
- **VPN basadas en directivas**. Las VPN basadas en directivas cifran y dirigen los paquetes a través de túneles de IPsec basados en las directivas de IPsec configuradas con las combinaciones de prefijos de dirección entre su red local y la red virtual de Azure. La directiva (o el selector de tráfico) se define como una lista de acceso en la configuración del dispositivo VPN

Puerta de enlace de VPN local:

Para configurar el dispositivo VPN, necesitará lo siguiente:

- **Una clave compartida**. Es la misma clave compartida que se especifica al crear la conexión VPN.
- **La IP pública de la puerta de enlace de VPN**. La dirección IP puede ser nueva o existente.

Cada instancia de Azure VPN Gateway consta de dos instancias en una configuración **activa-en espera**. Cuando están en una configuración activa-activa, el tráfico desde la red virtual de Azure hasta su red local se enrutará mediante ambos túneles simultáneamente. El mismo flujo TCP o UDP siempre atravesará el mismo túnel o ruta de acceso, a menos que se produzca un evento de mantenimiento en una de las instancias.

Azure ExpressRoute permite extender las redes locales a la nube de Microsoft. Un proveedor de conectividad facilita la conexión. Con ExpressRoute, se pueden establecer conexiones con servicios en la nube de Microsoft, como Microsoft Azure, Microsoft 365 y CRM Online. **Azure ExpressRoute** permite crear conexiones privadas entre los centros de datos de Azure y la infraestructura de su entorno local o de coubicación. Las conexiones ExpressRoute no usan la red de Internet pública y ofrecen más confiabilidad, velocidad, seguridad y una menor latencia que las conexiones a Internet habituales.

ExpressRoute ofrece una conexión rápida y fiable a Azure con anchos de banda de hasta 100 Gbps. Las conexiones de ExpressRoute permiten el acceso a los servicios de Microsoft Azure y Microsoft 365, así como a Microsoft Dynamics 365. Microsoft 365 se creó para poder acceder a él de forma segura y fiable mediante Internet, por lo que ExpressRoute requiere la autorización de Microsoft.

ExpressRoute es una conexión privada directa desde la WAN (no a través de Internet) a servicios Microsoft, incluido Azure. El tráfico VPN de sitio a sitio viaja cifrado a través de la red pública de Internet. Poder configurar las conexiones VPN de sitio a sitio y ExpressRoute para la misma red virtual tiene varias ventajas.

Cree una conexión entre su red local y la nube de Microsoft de tres formas diferentes: coubicación en un intercambio en la nube, conexión Ethernet de punto a punto y conexión universal (IPVPN).

Coubicación en un intercambio en la nube. Si está colocado en la misma instalación con un intercambio en la nube, solicite conexiones cruzadas virtuales a la nube de Microsoft mediante el intercambio de Ethernet del proveedor de la coubicación.

Conexiones de Ethernet de punto a punto. Los centros de datos locales o las oficinas se conectan a la nube de Microsoft mediante vínculos Ethernet de punto a punto. Los proveedores de Ethernet de punto a punto ofrecen conexiones de nivel 2 o de nivel 3 administradas entre el sitio y la nube de Microsoft.

Redes de conectividad universal (IPVPN). Integre la WAN con la nube de Microsoft. Los proveedores de IPVPN, normalmente, de VPN de conmutación de etiquetas multiprotocolo (MPLS), ofrecen conectividad universal entre las sucursales y los centros de datos. La nube de Microsoft puede estar conectada a la WAN de forma que parezca otra sucursal más. Los proveedores de WAN normalmente ofrecen una conectividad de nivel 3 administrada.

Connection	Servicios de Azure admitidos	Anchos de banda	Protocolos	Caso de uso típico
Red virtual de punto a sitio	Servicios de IaaS de Azure, Azure Virtual Machines	Se basa en la SKU de puerta de enlace	Activo/pasivo	Entornos de laboratorio, desarrollo y prueba para servicios en la nube y máquinas virtuales.
Red virtual de sitio a sitio	Servicios de IaaS de Azure, Azure Virtual Machines	Agregación típica de < 1 Gbps	Activo-pasivo, activo-activo	Entornos de laboratorio, desarrollo y prueba. Cargas de trabajo de producción a pequeña escala y máquinas virtuales.
ExpressRoute	Servicios de IaaS y PaaS de Azure, servicios de Microsoft 365	Desde 50 Mbps hasta 100 Gbps	Activo/activo	Cargas de trabajo críticas y de clase empresarial. Soluciones de macrodatos.

Azure Virtual WAN es un servicio de redes que ofrece conectividad entre ramas automatizada y optimizada a y mediante Azure. Las regiones de Azure sirven como centros que se pueden elegir para conectar las distintas ramas. La red troncal de Azure se usa para conectar sucursales y disfrutar de conectividad de sucursal a red virtual. Hay una lista de asociados que admiten la automatización de la conectividad con la VPN de Azure Virtual WAN. La conectividad con las redes virtuales de Azure se establece mediante el uso de conexiones de red virtual. La arquitectura de red de tránsito global se basa en un modelo de conectividad de concentrador y radio. El "centro de conectividad" de la red que se hospeda en la nube permite la conectividad transitiva entre puntos de conexión que pueden estar distribuidos en distintos tipos de "radios".

Ventajas de Virtual WAN

- **Soluciones de conectividad integrada en un modelo de concentrador y radio**. Configuración de sitio a sitio automatizada y conectividad entre sitios locales y un centro de Azure.
- **Instalación y configuración automatizadas de radio**. conecte sin problemas las cargas de trabajo y las redes virtuales al centro de Azure.
- **Solución intuitiva de problemas**. puede ver el flujo de un extremo a otro dentro de Azure y usar esta información para realizar las acciones necesarias.

Tipos de Virtual WAN

Existen dos tipos de WAN virtuales: Básico y Estándar.

Tipo de Virtual WAN	Tipo de centro de conectividad	Configuraciones disponibles
Basic	Básico	Solo VPN de sitio a sitio
Estándar	Estándar	ExpressRoute, VPN de usuario (P2S). VPN (de sitio a sitio), tránsito entre centros de conectividad y de red virtual a red virtual mediante el centro de conectividad virtual.

Azure ExpressRoute se puede usar para conectar las redes locales a la infraestructura en la nube de Microsoft. ExpressRoute funciona con un proveedor de conectividad aprobado para establecer las conexiones a través de un circuito dedicado.

Azure Virtual WAN también se puede usar para establecer conexiones de red. Azure Virtual WAN proporciona conectividad universal, enrutamiento personalizado y seguridad.

Azure usa **rutas del sistema** para dirigir el tráfico de red entre máquinas virtuales, redes locales e Internet. Estas rutas del sistema administran las siguientes situaciones:

- Tráfico entre máquinas virtuales de la misma subred
- Tráfico entre máquinas virtuales de subredes diferentes de la misma red virtual
- Flujo de datos de máquinas virtuales a Internet

Las UDR controlan el tráfico de red mediante la definición de rutas que especifican el próximo salto del flujo de tráfico. El salto puede ser una puerta de enlace de red virtual, una red virtual, Internet o una aplicación virtual.

Un punto de conexión de servicio de red virtual proporciona la identidad de la red virtual al servicio de Azure. Una vez que los puntos de conexión de servicio se habilitan en la red virtual, puede proteger los recursos de servicio de Azure en la red virtual mediante la incorporación de una regla de red virtual a los recursos.

Usos de punto de conexión de servicio:

- **Seguridad mejorada para los recursos de servicio de Azure**. El espacio de direcciones privadas de red virtual se puede estar solapando y, por tanto, no se puede usar para identificar de forma única el tráfico que se origina en la red virtual. Los puntos de conexión de servicio protegen los recursos de los servicios de Azure en la red virtual al ampliar la identidad de la red virtual al servicio. Cuando los puntos de conexión de servicio están habilitados en la red virtual, los recursos de los servicios de Azure se protegen en la red virtual mediante la adición de una regla de red virtual. Esta regla mejora la seguridad, ya que elimina totalmente el acceso público de Internet a los recursos y solo permite el tráfico que procede de la red virtual.
- **Enrutamiento óptimo para el tráfico del servicio de Azure desde la red virtual**. en la actualidad, las rutas de la red virtual que fuerzan el tráfico de Internet a las aplicaciones virtuales o locales, conocidas como tunelización forzada, también fuerzan el tráfico del servicio de Azure para realizar la misma ruta que el tráfico de Internet. Los puntos de conexión de servicio proporcionan un enrutamiento óptimo al tráfico de Azure.
- **Los puntos de conexión siempre llevan el tráfico del servicio directamente de la red virtual al servicio en la red troncal de Microsoft Azure**. Mantener el tráfico en la red troncal de Azure permite seguir auditando y supervisando el tráfico saliente de Internet desde las redes virtuales, a través de la tunelización forzada, sin que afecte al tráfico del servicio. Obtenga más información sobre las rutas definidas por el usuario y la tunelización forzada.
- **Facilidad de configuración con menos sobrecarga de administración**. ya no necesita direcciones IP públicas y reservadas en sus redes virtuales para proteger los recursos de Azure a través de una dirección IP del firewall. No hay ningún dispositivo NAT o de puerta de enlace necesario para configurar los puntos de conexión de servicio. Los puntos de conexión de servicio se configuran mediante la subred. No hay sobrecarga adicional para mantener los puntos de conexión.

Azure Storage. disponibilidad general en todas las regiones de Azure. Este punto de conexión proporciona al tráfico una ruta óptima hasta el servicio de Azure Storage. Cada cuenta de almacenamiento admite hasta 100 reglas de red virtual.

Azure SQL Database y Azure SQL Data Warehouse. disponibilidad general en todas las regiones de Azure. Una característica de seguridad de firewall controla si el servidor de bases de datos únicas y del grupo elástico de Azure SQL Database o de las bases de datos de SQL Database Warehouse acepta las comunicaciones que se envían desde subredes específicas de redes virtuales.

Servidor de Azure Database for PostgreSQL y MySQL. disponibilidad general en las regiones de Azure en las que el servicio de base de datos esté disponible. Las reglas y los puntos de conexión de servicios de red virtual (VNet) amplían el espacio de direcciones privadas de una red virtual al servidor de Azure Database for PostgreSQL y de MySQL.

Azure Cosmos DB. disponibilidad general en todas las regiones de Azure. Puede configurar la cuenta de Azure Cosmos para permitir el acceso solo desde una subred específica de la red virtual (VNET). Si habilita el punto de conexión de servicio para acceder a Azure Cosmos DB en la subred de una red virtual, el tráfico de esa subred se envía a Azure Cosmos DB con la identidad de la subred y la red virtual. Una vez habilitado el punto de conexión de servicio de Azure Cosmos DB, puede limitar el acceso a la subred agregándola a la cuenta de Azure Cosmos.

Azure Key Vault disponibilidad general en todas las regiones de Azure. Los puntos de conexión de servicio de red virtual para Azure Key Vault permiten restringir el acceso a una red virtual especificada. También permiten restringir el acceso a una lista de intervalos de direcciones IPv4 (protocolo de Internet, versión 4). A todos los usuarios que se conecten a su almacén de claves desde fuera de esos orígenes se les negará el acceso.

Azure Service Bus y Azure Event Hubs. disponibilidad general en todas las regiones de Azure. La integración de Service Bus con los puntos de conexión de servicio de una red virtual (VNet) permite el acceso seguro a las funcionalidades de mensajería de cargas de trabajo como las de máquinas virtuales que están enlazadas a redes virtuales, con una ruta de acceso del tráfico de red que está protegida en ambos extremos.

Azure Private Link proporciona conectividad privada desde una red virtual a la plataforma como servicio (PaaS) de Azure, propiedad del cliente o servicios de asociados de Microsoft. Simplifica la arquitectura de red y protege la conexión entre los puntos de conexión de Azure mediante la eliminación de la exposición de los datos a la red pública de Internet.

- **Conectividad privada a los servicios de Azure**. El tráfico permanece en la red de Microsoft, sin acceso a la red pública de Internet. Conéctese de forma privada a los servicios que se ejecutan en otras regiones de Azure. Private Link es global y no tiene restricciones regionales.
- **Integración con redes locales y emparejadas**. Acceda a puntos de conexión privados mediante el emparejamiento privado o túneles VPN desde redes virtuales locales o emparejadas. Microsoft hospeda el tráfico, por lo que no es necesario configurar el emparejamiento público ni usar Internet para migrar las cargas de trabajo a la nube.
- **Protección contra la filtración de datos de recursos de Azure**. Use Private Link para asignar puntos de conexión privados a recursos de PaaS de Azure. Cuando se produce un incidente de seguridad en la red, solo se podrá acceder al recurso asignado, lo que elimina la amenaza de filtración de datos.
- **Servicios entregados directamente a las redes virtuales de los clientes**. Consuma de forma privada servicios de PaaS de Azure, de asociados de Microsoft y los suyos propios en sus redes virtuales en Azure. Private Link funciona entre inquilinos de Azure Active Directory (Azure AD) para ayudar a unificar la experiencia entre los servicios. Envíe, apruebe o rechace solicitudes directamente, sin permisos ni controles de acceso basados en roles.

Use Private Link para llevar los servicios entregados en Azure a la red virtual privada mediante su asignación a un punto de conexión privado. También puede ofrecer sus propios servicios de forma privada en las redes virtuales de los clientes. Todo el tráfico dirigido al servicio se puede enrutar mediante el punto de conexión privado, por lo que no se necesita ninguna puerta de enlace, dispositivos NAT, conexiones de ExpressRoute o VPN ni direcciones IP públicas. Private Link mantiene el tráfico en la red global de Microsoft.

Azure Load Balancer ofrece alta disponibilidad y rendimiento de la red para sus aplicaciones. El equilibrador de carga distribuye el tráfico de entrada a los recursos de back-end mediante reglas de equilibrio de carga y sondeos de estado.

- Las reglas de equilibrio de carga determinan cómo se distribuye el tráfico al back-end.
- Los sondeos de estado garantizan que los recursos del back-end son correctos.

El equilibrador de carga puede usarse en escenarios de entrada y de salida y escala hasta millones de flujos de aplicaciones TCP y UDP.

Existen dos tipos de equilibradores de carga: **públicos** e **internos**.

El equilibrador de carga público asigna la dirección IP pública y el número de puerto del tráfico de entrada a la dirección IP privada y el número de puerto de la máquina virtual. También se proporciona asignación para el tráfico de respuesta de la máquina virtual. Al aplicar reglas de equilibrio de carga, puede distribuir tipos específicos de tráfico en varias máquinas virtuales o servicios. Por ejemplo, puede distribuir la carga de tráfico de solicitudes web de entrada entre varios servidores web.

Los equilibradores de carga internos dirigen el tráfico a los recursos que están dentro de una red virtual o que usan una VPN para acceder a la infraestructura de Azure. Las direcciones IP de front-end y las redes virtuales no se exponen nunca directamente a un punto de conexión de Internet. Las aplicaciones de línea de negocio internas se ejecutan en Azure y se accede a ellas desde Azure o desde recursos locales. Por ejemplo, un equilibrador de carga interno podría recibir solicitudes de base de datos que necesitan distribuirse a servidores SQL de back-end.

El equilibrador de carga interno permite los siguientes tipos de equilibrio de carga:

- **En una red virtual**. equilibrio de carga entre las máquinas virtuales de la red virtual y un conjunto de máquinas virtuales que residen en la misma red virtual.
- **En una red virtual entre entornos locales**. equilibrio de carga entre los equipos locales y un conjunto de máquinas virtuales que residen en la misma red virtual.
- **En aplicaciones de niveles múltiples**. equilibrio de carga para aplicaciones de niveles múltiples accesibles desde Internet, a cuyos niveles de back-end no se puede acceder desde Internet. Los niveles de back-end requieren un equilibrio de carga del tráfico desde el nivel accesible desde Internet.

- **En aplicaciones de línea de negocio**. equilibrio de carga para las aplicaciones de línea de negocio hospedadas en Azure sin requerir hardware ni software adicional de equilibrador de carga. Este escenario incluye servidores locales que se encuentran en el conjunto de equipos de cuyo tráfico se va a equilibrar la carga.

Standard Load Balancer es el nuevo producto de equilibrador de carga con un conjunto de características ampliado y más pormenorizado que el equilibrador de carga básico. Se trata de un superconjunto del equilibrador de carga básico.

Funcionalidades

Característica	SKU básica	SKU estándar
Grupos back-end	Hasta 300 instancias	Hasta 1000 instancias
Sondeos de estado	HTTP, TCP	HTTPS, HTTP y TCP
Zonas de disponibilidad	No disponible	Servidores front-end con redundancia de zona y zonales para el tráfico de entrada y salida.
Varios front-ends	Solo de entrada	Entrada y salida
Seguro de forma predeterminada	Abrir de forma predeterminada. NSG opcional.	Cerrado a flujos de entrada, a menos que lo permita un NSG. Se permite el tráfico interno desde la red virtual al equilibrador de carga interno.
Contrato de nivel de servicio	No disponible	99,99 %

Para distribuir el tráfico, un grupo de direcciones de back-end contiene las direcciones IP de las tarjetas de interfaz de red (NIC) virtuales conectadas al equilibrador de carga. La forma en que se configura el grupo de back-end depende de si se usa la SKU estándar o básica.

	SKU estándar	SKU básica
Puntos de conexión del grupo de back-end	Todas las máquinas virtuales de una red virtual. Esto incluye una combinación de máquinas virtuales, conjuntos de disponibilidad y conjuntos de escalado de máquinas virtuales.	Máquinas virtuales en un único conjunto de disponibilidad o conjunto de escalado de máquinas virtuales.

Los grupos de back-end se configuran en la hoja Grupo de back-end. En el caso de la SKU estándar, puede conectarse a un conjunto de disponibilidad, una sola máquina virtual o un conjunto de escalado de máquinas virtuales.

Una regla del equilibrador de carga define cómo se distribuye el tráfico al grupo de back-end. La regla asigna una combinación dada de dirección IP de front-end y puerto a una combinación de direcciones IP de back-end y puerto.

Azure Load Balancer distribuye el tráfico de red equitativamente entre varias instancias de máquina virtual. El equilibrador de carga usa un hash de cinco tuplas (IP de origen, puerto de origen, IP de destino, puerto de destino y tipo de protocolo) para asignar el tráfico a los servidores disponibles. Dicho algoritmo solo proporciona adherencia dentro de una sesión de transporte.

La persistencia de la sesión especifica cómo se debe controlar el tráfico de un cliente. El comportamiento predeterminado (Ninguno) es que cualquier máquina virtual puede controlar las solicitudes sucesivas de un cliente. Puede cambiar este comportamiento.

- **Ninguno (valor predeterminado)** especifica que cualquier máquina virtual puede controlar la solicitud.
- **IP de cliente**: especifica que la misma máquina virtual controlará las solicitudes sucesivas de la misma dirección IP de cliente.
- **IP y protocolo del cliente** especifica que la misma máquina virtual controlará las solicitudes sucesivas de la misma combinación de dirección IP y protocolo del cliente.

El equilibrador de carga usa un hash de cinco tuplas (IP de origen, puerto de origen, IP de destino, puerto de destino y tipo de protocolo) para asignar el tráfico a los servidores disponibles.

El sondeo de estado permite al equilibrador de carga supervisar el estado de la aplicación. El sondeo de estado agrega o quita de forma dinámica las máquinas virtuales de la rotación del equilibrador de carga en base a su respuesta a las comprobaciones de estado. Cuando un sondeo no responde, el equilibrador de carga deja de enviar nuevas conexiones a las instancias incorrectas.

Hay dos maneras principales de configurar sondeos de estado **HTTP** y **TCP**:

Sondeo HTTP personalizado. El equilibrador de carga sondea periódicamente el punto de conexión (de forma predeterminada, cada 15 segundos). La instancia es correcta si responde con HTTP 200 antes de que finalice el tiempo de espera (el valor predeterminado es 31 segundos). Cualquier estado distinto de HTTP 200 hace que se produzca un error en el sondeo. Puede especificar el puerto (Puerto), el URI para solicitar el estado de mantenimiento del back-end (URI), la cantidad de tiempo entre los intentos de sondeo (Intervalo) y el número de errores que deben producirse para que la instancia se considere incorrecta (Umbral incorrecto).

Sondeo TCP personalizado. Este sondeo se basa en el establecimiento de una sesión TCP correcta en un puerto de sondeo definido. Si existe el agente de escucha especificado en la máquina virtual, el sondeo se realizará correctamente. Si se rechaza la conexión, se producirá un error en el sondeo. Puede especificar el puerto, el intervalo y el umbral incorrecto.

Application Gateway proporciona funcionalidades de equilibrio de carga y enrutamiento de aplicaciones en varios sitios web. Hay varios métodos de enrutamiento disponibles, incluido el enrutamiento basado en rutas de acceso. Además, Application Gateway incluye una instancia de Web Application Firewall con características de seguridad integradas.

Application Gateway administra las solicitudes que las aplicaciones cliente envían a una aplicación web.

Application Gateway utiliza el enrutamiento de niveles de aplicación. El enrutamiento de niveles de aplicación conduce el tráfico a un grupo de servidores web a partir de la dirección URL de una solicitud. El grupo back-end puede estar compuesto de máquinas virtuales de Azure, conjuntos de escalado de máquinas virtuales de Azure, Azure App Service e incluso servidores locales.

Application Gateway utiliza el mecanismo round robin para enviar solicitudes de equilibrio de carga a los servidores de cada grupo back-end. Application Gateway proporciona la permanencia de sesión. Utilice la permanencia de sesión para garantizar que las solicitudes de cliente de una misma sesión se enrutan al mismo servidor back-end.

Hay dos métodos principales de enrutamiento de tráfico: enrutamiento basado en rutas de acceso y enrutamiento de varios sitios:

El enrutamiento basado en rutas de acceso envía solicitudes con distintas rutas de acceso de URL a distintos grupos de servidores back-end. Por ejemplo, podría dirigir las solicitudes con la ruta /video/* a un grupo de servidores backend que contenga servidores que están optimizados para controlar el streaming de vídeo y dirigir las solicitudes de /images/* a un grupo de servidores que administran la recuperación de imágenes.

El enrutamiento de varios sitios configura más de una aplicación web en la misma instancia de Application Gateway. En una configuración de varios sitios, hay que registrar varios nombres de DNS (CNAME) para la dirección IP de Application Gateway, especificando el nombre de cada sitio. Application Gateway usa agentes de escucha independientes para esperar por las solicitudes de cada sitio. Cada agente de escucha pasa la solicitud a otra regla, que puede enrutar las solicitudes a servidores en otro grupo de servidores back-end.

Las configuraciones de varios sitios son útiles para admitir aplicaciones de varios inquilinos, donde cada inquilino tiene su propio conjunto de máquinas virtuales u otros recursos que hospedan una aplicación web.

Application Gateway tiene una serie de componentes que se combinan para enrutar las solicitudes a un grupo de servidores web y para comprobar el estado de dichos servidores web.

Dirección IP de front-end. Las solicitudes de cliente se reciben a través de una dirección IP de front-end. Puede configurar Application Gateway para que tenga una dirección IP pública, privada o ambas. Application Gateway no puede tener más de una dirección IP pública y una privada.

Agentes de escucha. Application Gateway usa uno o varios agentes de escucha para recibir las solicitudes entrantes. Un agente de escucha acepta el tráfico que llega a una combinación especificada de protocolo, puerto, host y dirección IP. Cada agente de escucha enruta las solicitudes a un grupo de servidores back-end siguiendo las reglas de enrutamiento que especifique. Un agente de escucha puede ser básico o multisitio. Un agente de escucha básico solo enruta una solicitud según la ruta de acceso de la dirección URL. Un agente de escucha multisitio también puede enrutar las solicitudes mediante el elemento de nombre de host de la dirección URL.

Reglas de enrutamiento. Una regla de enrutamiento enlaza un agente de escucha a los grupos de servidores back-end. Una regla especifica cómo interpretar los elementos de nombre de host y ruta de la dirección URL de una solicitud y, después, dirigir la solicitud al grupo de servidores back-end adecuado. Una regla de enrutamiento también tiene un conjunto de configuración de HTTP asociado.

Grupos de servidores back-end. Un grupo de servidores back-end hace referencia a una colección de servidores web. Al configurar el grupo, proporciona la dirección IP de cada servidor web y el puerto en el que escucha las solicitudes. Cada grupo puede especificar un conjunto fijo de máquinas virtuales, un conjunto de escalado de máquinas virtuales, una aplicación hospedada por Azure App Services o una colección de servidores locales. Cada grupo de servidores back-end tiene un equilibrador de carga asociado que distribuye el trabajo en el grupo.

Firewall de aplicaciones web. El firewall de aplicaciones web (WAF) es un componente opcional que controla las solicitudes entrantes antes de que lleguen a un agente de escucha. El firewall de aplicaciones web comprueba cada solicitud en busca de muchos riesgos comunes, según la Open Web Application Security Project (OWASP). Entre las amenazas habituales se encuentran la inyección de código SQL, los scripts entre sitios, la inyección de comandos, el contrabando de solicitudes HTTP, la división de respuestas HTTP, la inclusión remota de archivos, los bots, los rastreadores y los escáneres, y las anomalías e infracciones del protocolo HTTP.

Sondeos de estado. Los sondeos de estado determinan qué servidores están disponibles para el equilibrio de carga en un grupo back-end. Application Gateway usa un sondeo de estado para enviar una solicitud a un servidor. Cuando el servidor devuelve una respuesta HTTP con un código de estado entre 200 y 399, se considera que el servidor está en buen estado.

Si no configura un sondeo de estado, Application Gateway crea un sondeo predeterminado que espera 30 segundos antes de decidir que un servidor no está disponible.

Un diseño típico de red local incluye estos componentes:

- Enrutadores
- Firewalls
- Conmutadores
- Segmentación de red

En el diagrama se muestra una versión simplificada de una red local típica. En los enrutadores orientados al proveedor de acceso a Internet (ISP), tiene direcciones IP públicas que el tráfico saliente de Internet usa como origen. Estas direcciones también se usan para el tráfico entrante a través de Internet. Es posible que el ISP le emita un bloque de direcciones IP para asignarlas a los dispositivos, o bien puede tener un bloque propio de direcciones IP públicas que la organización posee y controla. Puede asignar estas direcciones a sistemas que le gustaría que fueran accesibles desde Internet, como los servidores web.

La red perimetral y la zona interna tienen direcciones IP privadas. En la red perimetral y en la zona interna, las direcciones IP asignadas a estos dispositivos no son accesibles a través de Internet. El administrador tiene control total sobre la asignación de direcciones IP, la resolución de nombres, la configuración de seguridad y las reglas de seguridad. Hay tres intervalos de direcciones IP no enrutables diseñados para redes internas que no se enviarán a través de enrutadores de Internet:

- 10.0.0.0 a 10.255.255.255
- 172.16.0.0 a 172.31.255.255
- De 192.168.0.0 a 192.168.255.255

El administrador puede agregar o quitar subredes locales para dar cabida a los dispositivos y servicios de red. El número de subredes y direcciones IP que puede tener en la red local depende del enrutamiento de interdominios sin clases (CIDR) para el bloque de direcciones IP.

Un diseño de red de Azure típico normalmente incluye estos componentes:

- Redes virtuales
- Subredes
- Grupos de seguridad de red
- Firewalls
- Equilibradores de carga

La red de Azure no sigue el típico diseño de una red jerárquica local. La red de Azure ofrece la posibilidad de escalar y reducir verticalmente la infraestructura en función de la demanda. El aprovisionamiento en la red de Azure se produce en cuestión de segundos. No hay dispositivos de hardware como enrutadores o conmutadores. Toda la infraestructura es virtual y se puede segmentar en fragmentos que se adaptan a sus necesidades.

Una red virtual es la red en la nube. Puede dividir la red virtual en varias subredes. Cada subred tiene una parte del espacio de direcciones IP asignada a la red virtual. Puede agregar, quitar, expandir o contraer una subred si no hay máquinas virtuales ni servicios implementados en ella.

En Azure, puede usar dos tipos de direcciones IP:

- **Direcciones IP públicas**
- **Direcciones IP privadas**

Los dos tipos de direcciones IP se pueden asignar de una de estas dos maneras:

- **Dinámica**
- **Estática**

Use una dirección IP pública para los servicios de acceso público. Una dirección pública puede ser estática o dinámica. Una dirección IP pública puede estar asignada a una máquina virtual, un equilibrador de carga accesible desde Internet, una puerta de enlace de VPN o una puerta de enlace de aplicaciones.

- A las **direcciones IP públicas dinámicas** se les asignan direcciones que pueden cambiar durante la vida útil del recurso de Azure. La dirección IP dinámica se asigna cuando se crea una máquina virtual o se inicia una máquina virtual. La dirección IP se libera cuando se detiene o se elimina la máquina virtual. En cada región de Azure, las direcciones IP públicas se asignan desde un grupo de direcciones únicas. El método de asignación predeterminado es dinámico.

- A las **direcciones IP públicas estáticas** se les asignan direcciones que no cambiarán durante la vida útil del recurso de Azure. Para asegurarse de que la dirección IP del recurso no cambia, puede establecer el método de asignación en estático. En este caso, se asigna una dirección IP inmediatamente y solo se libera cuando se elimina el recurso o se cambia el método de asignación IP a dinámico.

Para las direcciones IP públicas, hay dos SKU entre las que elegir: **básica** y **estándar**. Todas las direcciones IP públicas creadas antes de la introducción de SKU son direcciones IP públicas de SKU básica. Con la introducción de SKU, puede elegir la escala, las características y los precios para equilibrar la carga del tráfico de Internet.

Tanto las SKU básicas como las estándar:

- Tienen un tiempo de espera de inactividad de flujo originado de entrada predeterminado de 4 minutos, que se puede ajustar hasta 30 minutos.
- Tienen un tiempo de espera de inactividad de flujo originado de salida fijo de 4 minutos.

SKU Básico

Las direcciones IP públicas básicas se pueden asignar mediante métodos de asignación estáticos o dinámicos. Las direcciones IP públicas básicas se pueden asignar a cualquier recurso de Azure al que se pueda asignar una dirección IP pública. Esto incluye las interfaces de red, las puertas de enlace de VPN y aplicación, y los equilibradores de carga accesibles desde Internet.

De manera predeterminada, las direcciones IP de SKU básica:

- Están abiertas. Se recomienda el uso de grupos de seguridad de red, pero es opcional para restringir el tráfico de entrada o de salida.
- Están disponibles solo para el tráfico de entrada.
- Están disponibles cuando se usa Instance Metadata Service (IMDS).
- No admiten las zonas de disponibilidad.
- No admiten las preferencias de enrutamiento.

SKU Estándar

De manera predeterminada, las direcciones IP de SKU estándar:

- Usan siempre la asignación estática.
- Son seguras y, por tanto, se cierran al tráfico de entrada. Debe habilitar el tráfico de entrada mediante un grupo de seguridad de red.
- Tienen redundancia de zona y, opcionalmente, pueden ser zonales (se pueden crear como zonales y garantizadas en una zona de disponibilidad específica).
- Se pueden asignar a interfaces de red, equilibradores de carga públicos estándar y puertas de enlace de aplicaciones o de VPN.
- Se puede usar con la preferencia de enrutamiento para permitir un control más detallado de cómo se enruta el tráfico entre Azure e Internet.
- Se pueden usar como IP de front-end de difusión por proximidad para los equilibradores de carga entre regiones.

un **prefijo de dirección IP pública** es un intervalo estático y reservado de direcciones IP públicas. Azure asigna una dirección IP de un grupo de direcciones disponibles que es única para cada región de cada nube de Azure. Al definir un prefijo de dirección IP pública, las direcciones IP públicas asociadas se asignan desde un grupo para una región de Azure.

Puede crear un prefijo de dirección IP pública, especifique un nombre y un tamaño de prefijo. El tamaño del prefijo es el número de direcciones reservadas disponibles para su uso.

- Los prefijos de dirección IP pública constan de direcciones IPv4 o IPv6.
- Puede usar tecnología como Azure Traffic Manager para equilibrar las instancias específicas de cada región.
- Las direcciones IP públicas propias no se pueden trasladar de redes locales a Azure.
- No puede especificar direcciones al crear un prefijo, ya que las asigna Azure. Una vez creado el prefijo, las direcciones IP se fijan en un intervalo contiguo.
- Las direcciones IP públicas no se pueden cambiar entre regiones; todas son específicas de la región.

Las direcciones IP privadas se usan para la comunicación dentro de una instancia de Azure Virtual Network, incluidas las redes virtuales y las redes locales. Las direcciones IP privadas se pueden establecer en dinámicas (concesión de DHCP) o estáticas (reserva de DHCP).

Las **direcciones IP privadas dinámicas** se asignan a través de una concesión de DHCP y pueden cambiar durante la vida útil del recurso de Azure.

Las **direcciones IP privadas estáticas** se asignan a través de una reserva de DHCP y no cambian durante la vida útil del recurso de Azure. Se conservan si se detiene o se cancela la asignación de un recurso.

Las direcciones IP privadas reservadas por Internet Assigned Numbers Authority (IANA) se eligen en función de los requisitos de red:

- 10.0.0.0/8
- 172.16.0.0/12
- 192.168.0.0/16

Una subred es un intervalo de direcciones IP dentro de la red virtual. Puede dividir una red virtual en varias subredes. Cada subred debe tener un intervalo de direcciones único, que se especifica en el formato de enrutamiento de interdominios sin clases (CIDR). CIDR es una manera de representar un bloque de direcciones IP de red. Un CIDR IPv4, especificado como parte de la dirección IP, muestra la longitud del prefijo de red.

En las redes virtuales de Azure, las direcciones IP se pueden asignar a los tipos de recursos siguientes:

- Interfaces de red de máquinas virtuales
- Equilibradores de carga
- Puertas de enlace de aplicaciones

Los dos tipos de conexiones de emparejamiento se crean de la misma manera:

- El **emparejamiento de red virtual** conecta las redes virtuales en la misma región de Azure, por ejemplo, dos redes virtuales en Norte de Europa.
- El **emparejamiento de red virtual global** conecta las redes virtuales que están en regiones de Azure distintas, por ejemplo, una red virtual en Norte de Europa y otra en Oeste de Europa.

El emparejamiento de redes virtuales requiere conexiones similares en cada red virtual. Las conexiones recíprocas proporcionan esta funcionalidad.

El emparejamiento de redes virtuales es no **transitivo**. Solo las redes virtuales emparejadas directamente se pueden comunicar entre sí. Las redes virtuales no se pueden comunicar con las del mismo nivel de sus redes del mismo nivel.

El emparejamiento de redes virtuales es la forma menos compleja de conectar redes virtuales conjuntamente. Otros métodos se centran principalmente en la conectividad entre redes locales y de Azure en lugar de las conexiones entre las redes virtuales.

Las redes virtuales que se conectan a un circuito ExpressRoute forman parte del mismo dominio de enrutamiento y se pueden comunicar entre sí. Las conexiones ExpressRoute no pasan por la red pública de Internet, por lo que las comunicaciones con los servicios de Azure son tan seguras como sea posible.

Azure DNS es un servicio de hospedaje para dominios DNS que ofrece resolución de nombres mediante la infraestructura de Microsoft Azure.

DNS (sistema de nombres de dominio) es un protocolo que se encuentra dentro del estándar TCP/IP. DNS tiene un rol esencial de convertir los nombres de dominio legibles (por ejemplo: `www.wideworldimports.com`) en una dirección de protocolo IP conocida.

Un servidor DNS desempeña una de las dos funciones principales:

- Mantiene una memoria caché local de nombres de dominio usados recientemente y sus direcciones IP. Esta memoria caché proporciona una respuesta más rápida a una solicitud de búsqueda en un dominio local. Si el servidor DNS no encuentra el dominio solicitado, pasa la solicitud a otro servidor DNS. Este proceso se repite en cada servidor DNS hasta que se encuentra una coincidencia o hasta que se agota el tiempo de espera de la búsqueda.
- Mantiene la base de datos de pares clave-valor de las direcciones IP y cualquier host o subdominio sobre el que el servidor DNS tiene autoridad. Esta función se suele asociar al correo, la Web y otros servicios de dominio de Internet.

Hay dos estándares de dirección IP: IPv4 e IPv6.

- **IPv4** se compone de cuatro conjuntos de números, en el intervalo de 0 a 255, separados por un punto. Ejemplo: 127.0.0.1. En la

actualidad, IPv4 es el estándar que se usa con más frecuencia. Sin embargo, con el aumento de los dispositivos IoT, el estándar IPv4 no podrá mantenerse.
- **IPv6** es un estándar relativamente nuevo y acabará reemplazando al estándar IPv4. Está formado por ocho grupos de números hexadecimales, separados por dos puntos. Ejemplo: fe80:11a1:ac15:e9gf:e884:edb0:ddee:fea3.

La información de configuración del servidor DNS se almacena en forma de archivo dentro de una zona del servidor DNS. Cada archivo se denomina registro. Los siguientes tipos de registro son los que se crean y usan más a menudo:

- **A** es el registro host y es el tipo de registro DNS más habitual. Asigna el nombre de dominio o de host a la dirección IP.
- **CNAME** es un registro de nombre canónico que se usa para asignar un alias de un nombre de dominio a otro. Si tuviera nombres de dominio diferentes a los que ha tenido acceso el mismo sitio web, usaría CNAME.
- **MX** es el registro de intercambio de correo. Asigna solicitudes de correo al servidor de correo electrónico, tanto si están hospedadas en el entorno local como en la nube.
- **TXT** es el registro de texto. Sirve para asociar cadenas de texto a un nombre de dominio. Azure y Microsoft 365 usan registros TXT para comprobar la propiedad del dominio.

Por otro lado, existen también los siguientes tipos de registro:

- Caracteres comodín
- CAA (entidad de certificación)
- NS (servidor de nombres)
- SOA (inicio de autoridad)
- SPF (marco de directivas de remitente)
- SRV (ubicaciones de servidor)

Los registros SOA y NS se crean automáticamente al crear una zona DNS con Azure DNS.

Azure DNS le permite hospedar y administrar sus dominios usando una infraestructura de servidor de nombres distribuida globalmente. Le permite administrar todos sus dominios con sus credenciales de Azure existentes. **Azure DNS** le permite hospedar sus registros DNS de sus dominios en la infraestructura de Azure. Con Azure DNS puede usar las mismas credenciales, API, herramientas y facturación que con los demás servicios de Azure.

Azure DNS actúa como SOA del dominio.

Azure DNS se basa en el servicio Azure Resource Manager, el cual ofrece las siguientes ventajas:

- Seguridad mejorada
- Facilidad de uso
- Dominios de DNS privados
- Conjuntos de registros de alias

Azure DNS puede administrar registros DNS para sus servicios de Azure y proporcionar DNS para sus recursos externos. Azure DNS usa las mismas credenciales de Azure, el mismo contrato de soporte técnico y la misma facturación que los demás servicios de Azure.

Azure DNS controla la conversión de nombres de dominio externos en una dirección IP. Azure DNS le permite crear zonas privadas. Estas proporcionan la resolución de nombres para las máquinas virtuales (VM) dentro de una red virtual, y entre redes virtuales, sin tener que crear una solución DNS personalizada. De esta forma puede usar sus propios nombres de dominio personalizados en lugar de los nombres proporcionados por Azure.

Para publicar una zona DNS privada en la red virtual, debe especificar la lista de redes virtuales que pueden resolver registros dentro de la zona.

Las zonas DNS privadas ofrecen las ventajas siguientes:

- No es necesario invertir en una solución DNS. Las zonas DNS se admiten como parte de la infraestructura de Azure.
- Se admiten todos los tipos de registros DNS: D, CNAME, TXT, MX, SOA, AAAA, PTR y SVR.
- Los nombres de host de las máquinas virtuales de su red virtual se mantienen automáticamente.
- La compatibilidad con DNS de horizonte dividido permite que el mismo nombre de dominio exista en zonas públicas y privadas. Se resuelve en el dominio correcto en función de la ubicación de la solicitud de origen.

El conjunto de registros de alias es compatible con los siguientes tipos de registro DNS:

- A
- AAAA
- CNAME

El dominio de vértice representa el nivel más alto del dominio. El dominio de vértice también se conoce como *vértice de zona* o *vértice raíz*. Suele representarse con el símbolo "@" en los registros de la zona DNS.

Los registros de alias de Azure permiten que un dominio de vértice de zona haga referencia a otros recursos de Azure desde la zona DNS.

El registro de alias de Azure puede apuntar a los siguientes recursos de Azure:

- Un perfil de Traffic Manager.
- Puntos de conexión de Azure Content Delivery Network.
- Un recurso de IP pública.
- Un perfil de puerta principal.

El conjunto de registros de alias es compatible con los siguientes tipos de registro de zona DNS:

- **A:** el registro de asignación de nombres de dominio IPv4.
- **AAAA:** el registro de asignación de nombres de dominio IPv6.
- **CNAME:** el alias del dominio, que se vincula al registro A.

El tráfico de red en Azure se enruta automáticamente entre las redes locales, las redes virtuales y las subredes de Azure. Este enrutamiento se controla mediante rutas del sistema, que se asignan de forma predeterminada a cada subred de una red virtual. Con estas rutas del sistema, cualquier máquina virtual de Azure que se implemente en una red virtual se puede comunicar con cualquier otra de la red. También se puede tener acceso a estas máquinas virtuales desde el entorno local a través de una red híbrida o de Internet.

La ruta de acceso puede ser uno de los tipos de salto siguientes:

- **Red virtual**: se crea una ruta en el prefijo de dirección. El prefijo representa cada intervalo de direcciones creado en el nivel de red virtual. Si se especifican varios intervalos de direcciones, se crean varias rutas para cada uno.
- **Internet**: la ruta predeterminada del sistema 0.0.0.0/0 enruta cualquier intervalo de direcciones a Internet, a menos que se reemplace la ruta predeterminada de Azure por una ruta personalizada.
- **Ninguno**: todo el tráfico enrutado a este tipo de salto se omite y no se enruta fuera de la subred. De forma predeterminada, se crean los siguientes prefijos de dirección privada IPv4: 10.0.0.0/8, 172.16.0.0/12 y 192.168.0.0/16. También se agrega el prefijo 100.64.0.0/10 para un espacio de direcciones compartido. Ninguno de estos intervalos de direcciones se puede enrutar globalmente.

Dentro de Azure hay otras rutas del sistema. Azure creará estas rutas si se habilitan las funcionalidades siguientes:

- Emparejamiento de redes virtuales
- Encadenamiento de servicios
- Puerta de enlace de red virtual
- Puntos de conexión de servicio de red virtual

El emparejamiento de redes virtuales y **el encadenamiento de servicios** permiten que las redes virtuales de Azure se conecten entre sí. Con esta conexión, las máquinas virtuales se pueden comunicar entre sí dentro de la misma región o entre regiones. Esta comunicación, a su vez, crea más rutas dentro de la tabla de rutas predeterminada. El encadenamiento de servicios permite reemplazar estas rutas mediante la creación de rutas definidas por el usuario entre redes emparejadas.

Use una **puerta de enlace de red virtual** para enviar tráfico cifrado entre Azure y el entorno local a través de Internet, así como para enviar tráfico cifrado entre redes de Azure. Una puerta de enlace de red virtual contiene tablas de enrutamiento y servicios de puerta de enlace.

Los puntos de conexión de red virtual amplían el espacio de direcciones privadas en Azure proporcionando una conexión directa a los recursos de Azure. Este conexión restringe el flujo de tráfico: las máquinas virtuales de Azure pueden acceder a la cuenta de almacenamiento directamente desde el espacio de direcciones privadas y denegar el acceso desde una máquina virtual pública.

Las rutas del sistema podrían facilitar la tarea de poner rápidamente en marcha el entorno, pero hay muchos escenarios en los que preferirá tener un control más estrecho del flujo de tráfico dentro de la red. Por ejemplo, es posible que quiera enrutar el tráfico a través de una NVA o de un firewall. Este control es posible con las rutas personalizadas.

Una ruta definida por el usuario se puede usar para reemplazar las rutas predeterminadas del sistema para que el tráfico se pueda enrutar a través de firewalls o aplicaciones virtuales de red.

Al crear rutas definidas por el usuario, se pueden especificar estos tipos de próximo salto:

- **Aplicación virtual**: suele ser un dispositivo de firewall que se usa para analizar o filtrar el tráfico que entra o sale de la red. Puede especificar la dirección IP privada de una NIC conectada a una máquina virtual para que se pueda habilitar el reenvío IP. O bien, puede proporcionar la dirección IP privada de un equilibrador de carga interno.
- **Puerta de enlace de red virtual**: se usa para indicar cuándo quiere que las rutas para una dirección específica se enruten a una puerta de enlace de red virtual. La puerta de enlace de red virtual se especifica como VPN para el tipo de próximo salto.
- **Red virtual**: se usa para reemplazar la ruta predeterminada del sistema en una red virtual.
- **Internet**: se usa para enrutar el tráfico a un prefijo de dirección especificado que se enruta a Internet.
- **Ninguno**: se usa para quitar el tráfico enviado a un prefijo de dirección especificado.

Una puerta de enlace de red en la red local puede intercambiar rutas con una puerta de enlace de red virtual en Azure mediante el Protocolo de puerta de enlace de borde (BGP). **BGP(Border Gateway Protocol)** es el protocolo de enrutamiento estándar que se usa habitualmente para el intercambio de enrutamiento e información entre dos o más redes. BGP se usa para transferir datos e información entre diferentes puertas de enlace de host en Internet o entre sistemas autónomos.

El **BGP** es un protocolo de puerta de enlace exterior (EGP) que se utiliza para intercambiar información de enrutamiento entre enrutadores en diferentes sistemas autónomos (AS). La información de enrutamiento del BGP incluye la ruta completa a cada destino. El BGP utiliza la información de enrutamiento para mantener una base de datos de información de accesibilidad de red, que intercambia con otros sistemas BGP. El BGP utiliza la información de accesibilidad de la red para construir un gráfico de conectividad del AS, lo que permite al BGP eliminar bucles de enrutamiento y aplicar decisiones de política en el nivel del AS.

Si hay varias rutas disponibles en una tabla de rutas, Azure usa la ruta con la coincidencia de prefijo más larga. Por ejemplo, si un mensaje se envía a la dirección IP 10.0.0.2, pero hay dos rutas disponibles con los prefijos 10.0.0.0/16 y 10.0.0.0/24, Azure selecciona la ruta con el prefijo 10.0.0.0/24 porque es más específica.

Cuanto más largo sea el prefijo de ruta, más corta será la lista de direcciones IP disponibles a través de ese prefijo. Cuando se usan prefijos más largos, el algoritmo de enrutamiento puede seleccionar la dirección deseada más rápidamente.

Si hay varias rutas con el mismo prefijo de dirección, Azure selecciona la ruta según el tipo, con el orden de prioridad siguiente:

1. Rutas definidas por el usuario
2. Rutas BGP
3. Rutas del sistema

Una aplicación virtual de red (NVA) es una aplicación virtual que se compone de varias capas como las siguientes:

- un firewall
- un optimizador de WAN
- controladores de entrega de aplicaciones
- enrutadores
- equilibradores de carga
- IDS/IPS
- proxies

Las aplicaciones virtuales de red (NVA) son máquinas virtuales que controlan el flujo del tráfico de red mediante el control del enrutamiento. Se suelen usar para administrar el flujo de tráfico desde un entorno de red perimetral a otras redes o subredes.

En la mayoría de los entornos, las rutas predeterminadas del sistema ya definidas por Azure son suficientes para poner en marcha los entornos. En ciertos casos, hay que crear una tabla de enrutamiento y agregar rutas personalizadas. Algunos ejemplos son:

- Acceso a Internet a través de una red local con tunelización forzada
- Uso de aplicaciones virtuales para controlar el flujo de tráfico

Azure Load Balancer es un servicio que se puede usar para distribuir el tráfico entre varias máquinas virtuales. Use Load Balancer para escalar las aplicaciones y crear alta disponibilidad para las máquinas virtuales y los servicios. **El equilibrador de carga** usa un algoritmo de distribución basado en hash. De forma predeterminada, se usa un **hash 5-tupla** para asignar el tráfico a los servidores disponibles. El hash se compone de los elementos siguientes:

- **IP de origen**: dirección IP del cliente que realiza la solicitud.
- **Puerto de origen**: puerto del cliente que realiza la solicitud.
- **IP de destino**: IP de destino de la solicitud.
- **Puerto de destino**: puerto de destino de la solicitud.
- **Tipo de protocolo**: el tipo de protocolo especificado, TCP o UDP

Con Load Balancer, puede usar conjuntos de disponibilidad y zonas de disponibilidad para garantizar que las máquinas virtuales estén siempre disponibles:

Configuración	Acuerdo de Nivel de Servicio (SLA)	Información
Conjunto de disponibilidad	99,95 %	Protección contra errores de hardware en centros de datos
Zona de disponibilidad	99,99 %	Protección contra errores en todo el centro de datos

Un conjunto de disponibilidad es una agrupación lógica que se usa para aislar los recursos de máquina virtual entre sí cuando se implementan. Azure garantiza que las máquinas virtuales colocadas en un conjunto de disponibilidad se ejecuten en varios servidores físicos, grupos de proceso, unidades de almacenamiento y conmutadores de red. Los conjuntos de disponibilidad son esenciales para la creación de soluciones en la nube confiables.

Una zona de disponibilidad ofrece grupos de uno o varios centros de datos con alimentación, refrigeración y redes independientes. Las máquinas virtuales de una zona de disponibilidad se colocan en otras ubicaciones físicas dentro de la misma región.

Al crear un equilibrador de carga en Azure, hay dos productos disponibles: equilibradores de **carga básicos** y equilibradores de **carga estándar**.

Los equilibradores de carga básicos permiten realizar lo siguiente:

- Reenvío de puertos
- Reconfiguración automática
- Sondeos de estado
- Conexiones de salida a través de la traducción de direcciones de red de origen (SNAT)
- Diagnóstico a través de Azure Log Analytics para equilibradores de carga de acceso público

Los equilibradores de carga estándar admiten todas las características de los equilibradores de carga básicos. También permiten:

- Sondeos de estado HTTPS
- Zonas de disponibilidad
- Diagnóstico a través de Azure Monitor, para métricas multidimensionales
- Puertos de alta disponibilidad
- Reglas de salida
- Acuerdo de Nivel de Servicio (SLA) garantizado (99,99 % para dos o más máquinas virtuales)

Un equilibrador de carga externo funciona distribuyendo el tráfico de cliente entre varias máquinas virtuales y permite el tráfico desde Internet. Es posible que el tráfico proceda de exploradores, aplicaciones móviles u otros orígenes.

Un equilibrador de carga interno distribuye una carga desde los recursos internos de Azure a otros recursos de Azure. Por ejemplo, si tiene servidores web front-end en los que se tiene que llamar a la lógica de negocios hospedada en varios servidores de nivel intermedio, puede distribuir esa carga de manera uniforme mediante un equilibrador de carga interno.

Un equilibrador de carga público asigna la dirección IP pública y el número de puerto del tráfico de entrada a la dirección IP privada y el número de puerto de una máquina virtual del grupo de back-end. Las respuestas se devuelven después al cliente. Al aplicar reglas de equilibrio de carga, se distribuyen tipos específicos de tráfico en varios servicios o máquinas virtuales.

Azure Load Balancer distribuye el tráfico de red equitativamente entre varias instancias de máquina virtual. Los modos de distribución siguientes también son posibles si se requiere otro comportamiento:

- **Hash de cinco tuplas**. El modo de distribución predeterminado de Load Balancer es un hash de cinco tuplas. La tupla se compone de la IP de origen, el puerto de origen, la IP de destino, el puerto de destino y el tipo de protocolo. Como el puerto de origen se incluye en el hash y cambia para cada sesión, es posible que los clientes se dirijan a una máquina virtual diferente en cada sesión.

- **Afinidad de IP de origen**. Este modo de distribución también se conoce como ***afinidad de sesión*** o ***afinidad de IP del cliente***. Para asignar el tráfico a los servidores disponibles, el modo de afinidad de dirección IP de origen usa un hash de dos tuplas (de la dirección IP de origen y la de destino), o bien uno de tres tuplas (de la dirección IP de origen, la de destino y el tipo de protocolo). El hash garantiza que las solicitudes de un cliente determinado se envían siempre a la misma máquina virtual detrás del equilibrador de carga.

Puede configurar un equilibrador de carga interno prácticamente de la misma manera que un equilibrador de carga externo, pero con estas diferencias:

- Al crear el equilibrador de carga, seleccione **Interno** para **Tipo**. Cuando se elige esta opción, la dirección IP de front-end del equilibrador de carga no se expone a Internet.
- Asigne una dirección IP privada al front-end del equilibrador de carga en lugar de una dirección IP pública.
- Coloque el equilibrador de carga en la red virtual protegida que contiene las máquinas virtuales que quiere que controlen las solicitudes.

Supervisión y copia de seguridad de recursos de Azure

Azure Backup es el servicio de Azure que puede usar para hacer una copia de seguridad de los datos (protegerlos) y restaurarlos en Microsoft Cloud. Reemplaza su solución de copia de seguridad local o remota existente por una solución confiable, segura y rentable basada en la nube.

Azure Backup ofrece dos tipos de replicación para mantener la alta disponibilidad de los datos o del almacenamiento.

- **El almacenamiento con redundancia local (LRS)** replica los datos tres veces (crea tres copias de los datos) en una unidad de escalado de almacenamiento de un centro de datos. Todas las copias de los datos se encuentran en la misma región. LRS es una opción de bajo costo para proteger los datos contra errores de hardware local.
- **El almacenamiento con redundancia geográfica (GRS)** es el valor predeterminado y la opción de replicación recomienda. GRS replica los datos en una región secundaria (a cientos de kilómetros de la ubicación principal de los datos de origen). GRS cuesta más que LRS, pero proporciona un mayor nivel de durabilidad de los datos, incluso si hay una interrupción regional.

Azure Backup tiene un límite de 9999 puntos de recuperación por instancia protegida.

El Centro de copias de seguridad proporciona una experiencia única de administración unificada en Azure para que las empresas controlen, supervisen, operen y analicen las copias de seguridad a gran escala. Como tal, es coherente con las experiencias de administración nativas de Azure.

Entre algunas de las ventajas principales del Centro de copias de seguridad se incluyen:

- **Panel único para administrar copias de seguridad**. El Centro de copias de seguridad está diseñado para funcionar bien en entornos de Azure grandes y distribuidos. Puede usar el Centro de copias de seguridad para administrar de forma eficaz las copias de seguridad que abarcan varios tipos de cargas de trabajo, almacenes, suscripciones, regiones e inquilinos.
- **Administración centrada en orígenes de datos**. El Centro de copias de seguridad proporciona vistas y filtros que se centran en los orígenes de datos de los que se realiza la copia de seguridad. Orígenes de datos como máquinas virtuales y bases de datos. Esta característica permite que un propietario de recursos o un

administrador de copia de seguridad administren elementos de copia de seguridad en distintos almacenes. El administrador también puede filtrar las vistas por propiedades específicas del origen de datos. Estas propiedades incluyen la suscripción al origen de datos, así como el grupo de recursos y las etiquetas de este origen de datos.

- **Experiencias conectadas**. El Centro de copias de seguridad proporciona integraciones nativas a los servicios de Azure existentes que permiten la administración a gran escala. Por ejemplo, el Centro de copias de seguridad usa la experiencia de Azure Policy para ayudarle a controlar las copias de seguridad. Usa los libros de Azure y los registros de Azure Monitor para ayudarle a ver informes detallados sobre las copias de seguridad. Por lo tanto, no es necesario conocer los nuevos principios para usar las diversas características que ofrece el Centro de copias de seguridad. También puede detectar recursos de la comunidad desde el Centro de copias de seguridad.

El **almacén de Recovery Services** es una entidad de almacenamiento de Azure que aloja datos. Los almacenes de Recovery Services almacenan datos de copia de seguridad de varios servicios de Azure, como máquinas virtuales de IaaS (Linux o Windows), y bases de datos de Azure SQL. Los almacenes de Recovery Services admiten System Center DPM, Windows Server y Azure Backup Server, entre otros.

Dentro de una suscripción de Azure, puede crear hasta 25 almacenes de Recovery Services por región.

Azure Backup para archivos y carpetas se basa en el agente **de Microsoft Azure Recovery Services (MARS)** que se va a instalar en el cliente o servidor de Windows.

El agente de **MARS** es un agente completo que tiene muchas características.

- Copia de seguridad de archivos y carpetas en el sistema operativo Windows físico o virtual (las máquinas virtuales pueden estar en el entorno local o en Azure).
- No se necesita ningún servidor de copia de seguridad independiente.
- No es compatible con la aplicación; restauración solo a nivel de archivo, carpeta y volumen.
- Copia de seguridad y restauración de contenido.

La copia de seguridad de recursos compartidos de archivos de Azure es una solución de copia de seguridad nativa basada en la nube que protege los datos en la nube. Azure Backup elimina la sobrecarga de mantenimiento adicional implicada en las soluciones de copia de seguridad locales.

Azure Backup. Para realizar copias de seguridad de máquinas virtuales de Azure que ejecutan cargas de trabajo de producción, use Azure Backup. Azure Backup admite las copias de seguridad coherentes con la aplicación para máquinas virtuales Windows y Linux. Azure Backup crea puntos de recuperación que se almacenan en almacenes de recuperación con redundancia geográfica. Cuando se realiza una restauración desde un punto de recuperación, se puede restaurar toda una máquina virtual o solo determinados archivos.

Azure Site Recovery. Azure Site Recovery protege las máquinas virtuales ante desastres graves en los que toda una región experimente una interrupción debido a un desastre natural importante o a una interrupción del servicio generalizada. Puede configurar Azure Site Recovery para las VM de modo que pueda recuperar la aplicación con un solo clic en cuestión de minutos. Puede replicar en la región de Azure que elija.

Instantáneas de disco administrado. En entornos de desarrollo y prueba, las instantáneas proporcionan una opción rápida y sencilla para realizar copias de seguridad de máquinas virtuales que usan Managed Disks. Una instantánea de disco administrado es una copia completa de solo lectura de un disco administrado que, de forma predeterminada, se almacena como disco administrado estándar. Con las instantáneas, puede realizar una copia de seguridad de sus discos administrados en cualquier momento.

Imágenes. Los discos administrados también admiten la creación de una imagen personalizada administrada. Puede crear una imagen desde un disco duro virtual personalizado en una cuenta de almacenamiento, o bien directamente desde una máquina virtual generalizada (con Sysprep). Este proceso captura una imagen única. Esta imagen contiene todos los discos administrados asociados con una máquina virtual, lo que incluye tanto el disco de datos como el del sistema operativo.

Es importante comprender la diferencia entre imágenes e instantáneas. Con los discos administrados, es posible tomar una imagen de una máquina virtual generalizada que se ha desasignado. Esta imagen incluye todos los discos asociados a la máquina virtual. La imagen se puede usar para crear una máquina virtual e incluye todos los discos.

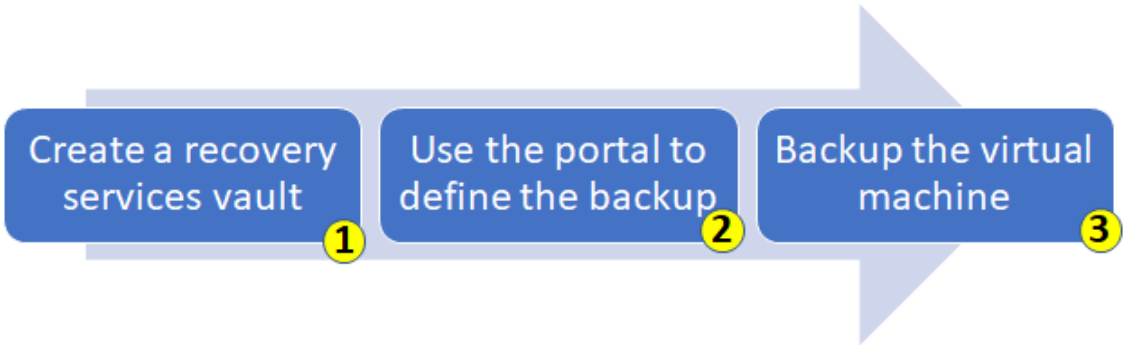
- **Una instantánea** es una copia de un disco en el momento dado en que se toma. Se aplica solo a un disco. Si tiene una máquina virtual con un solo disco (el del sistema operativo), puede tomar una instantánea o una imagen de él y crear una máquina virtual a partir de cualquiera de ellas.
- **Una instantánea** no tiene información sobre ningún disco, excepto el que contiene. Como consecuencia, resulta problemático usarla en escenarios que requieren la coordinación de varios discos, como la creación de bandas. Las instantáneas deben poderse coordinar entre sí y esta funcionalidad no se admite actualmente.

Un trabajo de copia de seguridad de Azure consta de dos fases. En primer lugar, se toma una instantánea de máquina virtual. En segundo lugar, la instantánea de máquina virtual se transfiere al almacén de Azure Recovery Services.

Un punto de recuperación se considera creado solo después de que se completen ambos pasos. Como parte de la actualización, se crea un punto de recuperación en cuanto finaliza la instantánea. Este punto de recuperación se usa para realizar una restauración.

El almacén de Recovery Services es una entidad de almacenamiento de Azure que aloja datos. Normalmente, los datos son copias de datos o información de configuración de máquinas virtuales (VM), cargas de trabajo, servidores o estaciones de trabajo.

La copia de seguridad de máquinas virtuales de Azure con Azure Backup es fácil y sigue un proceso sencillo.



1. **Cree un almacén de Recovery Services**. Para hacer una copia de seguridad de los archivos y las carpetas, tiene que crear un almacén de Recovery Services en la región donde desea almacenar los datos. También debe determinar cómo quiere que se replique el almacenamiento, ya sea con redundancia geográfica (valor predeterminado) o con redundancia local. De forma predeterminada, el almacén tiene almacenamiento con redundancia geográfica. Si usa Azure como punto de conexión del almacenamiento de copia de seguridad principal, use el almacenamiento con redundancia geográfica predeterminado. Si usa Azure como punto de conexión del almacenamiento de copia de seguridad no principal, elija un almacenamiento con redundancia local, ya que ello reducirá el costo de almacenamiento de datos en Azure.
2. **Use Azure Portal para definir la copia de seguridad**. Proteja sus datos tomando instantáneas de sus datos a intervalos definidos. Estas instantáneas se denominan puntos de recuperación y se almacenan en almacenes de Servicios de recuperación. Cuando es necesario reparar o volver a generar una máquina virtual, puede restaurar la máquina virtual desde cualquiera de los puntos de recuperación guardados. Una directiva de copia de seguridad define una matriz del momento en que se toman las instantáneas de datos y cuánto tiempo se retienen las instantáneas. Al definir una directiva para la copia de seguridad de una máquina virtual, puede desencadenar un trabajo de copia de seguridad una vez al día.
3. **Realice una copia de seguridad de la máquina virtual**. El agente de máquina virtual de Azure se debe instalar en la máquina virtual de Azure para que funcione la extensión de copia de seguridad. Sin embargo, si la máquina virtual se creó desde la galería de Azure, el agente de máquina virtual ya está presente en la máquina virtual. Las máquinas virtuales que se migran desde centros de datos locales no tienen instalado el agente de máquina virtual. En ese caso, el agente de máquina virtual debe instalarse explícitamente.

Componente	Ventajas	Límites	¿Qué se protege?	¿Dónde se almacenan las copias de seguridad?
Agente de Azure Backup (MARS)	Copia de seguridad de archivos y carpetas en el sistema operativo físico o virtual de Windows; no se requiere ningún servidor de copia de seguridad independiente	Copia de seguridad tres veces al día; no tiene en cuenta la aplicación; solo restauración de archivos, carpetas y volúmenes; sin compatibilidad con Linux	Archivos y carpetas	Almacén de Recovery Services
Servidor de Azure Backup (MABS)	Instantáneas que tienen en cuenta la aplicación; flexibilidad total de cuándo realizar las copias de seguridad; granularidad de recuperación; compatibilidad con Linux en máquinas virtuales de Hyper-V y VMware; copia de seguridad y restauración de máquinas virtuales de VMware, no requiere licencia de System Center	No se puede realizar una copia de seguridad de las cargas de trabajo de Oracle; esto siempre requiere una suscripción de Azure activa; no se admite la copia de seguridad en cinta	Archivos, carpetas, volúmenes, máquinas virtuales, aplicaciones y cargas de trabajo	Almacén de Recovery Services, disco conectado localmente

Azure Storage ofrece la posibilidad de eliminar temporalmente objetos de blob, con el fin de que pueda recuperar más fácilmente los datos cuando una aplicación u otro usuario de la cuenta de almacenamiento los hayan modificado o eliminado por error. La eliminación temporal de máquinas virtuales protege las copias de seguridad de las máquinas virtuales de una eliminación imprevista. Incluso después de que se eliminen **las copias de seguridad, se conservan en estado de eliminación temporal durante 14 días adicionales.**

Azure Monitor es un servicio de Azure que proporciona supervisión del rendimiento y la disponibilidad para aplicaciones y servicios en Azure, en otros entornos en la nube o en el entorno local.

- **Supervise y visualice las métricas**. Las métricas son valores numéricos que están disponibles en los recursos de Azure y que le ayudan a comprender el estado, el funcionamiento y el rendimiento de su sistema.
- **Consulte y analice los registros**. Los registros hacen referencia a los registros de actividad, los de diagnóstico y la telemetría de las soluciones de supervisión; las consultas de análisis ayudan con la solución de problemas y las visualizaciones.
- **Configure alertas y acciones**: Las alertas le informan de condiciones críticas y pueden realizar acciones correctivas automatizadas según los desencadenadores de métricas o registros.

La supervisión es la acción de recopilar y analizar datos. Los datos se pueden usar para determinar el rendimiento, el estado y la disponibilidad de la aplicación empresarial y de los recursos de los que esta depende.

Una estrategia de supervisión eficaz le ayuda a comprender el funcionamiento detallado de los componentes de la aplicación. La supervisión también le ayuda a aumentar su tiempo de actividad, ya que se le envían notificaciones de los errores críticos. Tras ello, puede resolver los problemas antes de que se vuelvan graves.

Todos los datos recopilados por Azure Monitor pueden clasificarse como uno de los dos tipos fundamentales: **métricas** y **registros**.

- Las **métricas** son valores numéricos que describen algún aspecto de un sistema en un momento dado. Las métricas son ligeras y capaces de admitir escenarios de tiempo casi real.
- Los **registros** contienen distintos tipos de datos organizados en grupos de registros, donde cada tipo tiene diferentes conjuntos de propiedades. Los datos, como los eventos y los seguimientos, se almacenan como registros junto con los datos de rendimiento para poder analizarlos de forma combinada.

Para muchos recursos de Azure, los datos que recopila Azure Monitor se muestran en la página Información general Azure Portal. Por ejemplo, las máquinas virtuales tienen varios gráficos en los que se muestran métricas de rendimiento.

Los datos de registro recopilados por Azure Monitor se guardan en Log Analytics, que cuenta con un lenguaje de consulta avanzado para poder recuperar, consolidar y analizar rápidamente los datos recopilados. Puede crear y probar consultas con la página de Log Analytics en Azure Portal.

Azure Monitor puede recopilar datos de diversos orígenes. Puede pensar en supervisar datos para las aplicaciones en niveles que abarcan desde la aplicación hasta el sistema operativo y los servicios en los que se basa, pasando por la propia plataforma. Azure Monitor recopila datos de cada uno de los siguientes niveles:

- **Datos de supervisión de aplicaciones:** datos sobre el rendimiento y la funcionalidad del código que ha escrito, independientemente de la plataforma.
- **Datos de supervisión del sistema operativo invitado:** datos sobre el sistema operativo en el que se ejecuta la aplicación. La aplicación se puede ejecutar en Azure, en otra nube o en el entorno local.
- **Datos de supervisión de recursos de Azure:** datos acerca del funcionamiento de un recurso de Azure.
- **Datos de supervisión de la suscripción de Azure:** datos sobre el funcionamiento y la administración de una suscripción de Azure, así como sobre el estado y el funcionamiento del propio Azure.
- **Datos de supervisión del inquilino de Azure:** datos sobre el funcionamiento de los servicios de Azure en el nivel del inquilino, como Azure Active Directory.

El registro de actividad de Azure es un registro de suscripción que proporciona información sobre los eventos de nivel de suscripción que se han producido en Azure. Esta incluye un rango de datos, desde datos operativos de Azure Resource Manager hasta actualizaciones en eventos de Estado del servicio. Los registros de actividad se conservan 90 días.

Características de Eventos:

- **Administrativos**. Esta categoría contiene el registro de todas las operaciones de creación, actualización, eliminación y acción realizadas a través de Resource Manager. Entre los ejemplos de los tipos de eventos que observaría en esta categoría, se incluyen "crear máquina virtual" y "eliminar grupo de seguridad de red". La categoría Administrativo también incluye los cambios realizados en el control de acceso basado en roles de una suscripción.
- **Estado del servicio**. Esta categoría contiene el registro de los incidentes de estado del servicio que se han producido en Azure. Un ejemplo del tipo de evento que observaría en esta categoría es "SQL Azure en el Este de EE. UU. está experimentando tiempo de inactividad".Los eventos de estado del servicio pueden ser de seis variedades: Acción requerida, Recuperación asistida, Incidente, Mantenimiento, Información o Seguridad.
- **Estado de los recursos**. Esta categoría contiene el registro de los eventos de estado del servicio que se han producido en los recursos de Azure. Un ejemplo del tipo de evento que vería en esta categoría es "Estado de mantenimiento de la máquina virtual cambiado a no disponible". Los eventos de mantenimiento de recursos pueden representar uno de los cuatro estados de mantenimiento: Disponible, No disponible, Degradado y Desconocido.
- **Alerta**. Esta categoría contiene el registro de todas las activaciones de alertas de Azure. Un ejemplo del tipo de evento que vería en esta categoría es "CPU % on myVM has been over 80 for the past 5 minutes" (El porcentaje de CPU en myVM ha sido superior al 80 % durante los últimos 5 minutos).
- **Escalabilidad automática**. Esta categoría contiene el registro de los eventos relacionados con el funcionamiento del motor de escalado automático en función de cualquier configuración de escalado automático que haya definido en la suscripción. Un ejemplo del tipo de evento que vería en esta categoría es "Autoscale scale up action failed" (No se ha podido completar la acción de escalado automático vertical).
- **Recomendación**. Esta categoría contiene eventos de recomendación de determinados tipos de recursos, como sitios web y servidores SQL Server. Estos eventos ofrecen recomendaciones para usar mejor los recursos.

- **Seguridad**. Esta categoría contiene el registro de todas las alertas que ha generado Azure Defender para servidores. Un ejemplo del tipo de evento que vería en esta categoría es "Suspicious double extension file executed" (Se ha ejecutado un archivo de extensión doble sospechoso).
- **Directiva**. Esta categoría contiene registros de todas las operaciones de acción de efecto realizadas por Azure Policy. Algunos ejemplos de los tipos de eventos que podrían aparecer en esta categoría son Auditoría y Denegación.

La experiencia de supervisión de alertas tiene muchas ventajas.

- **Mejor sistema de notificaciones**. todas las nuevas alertas usan grupos de acciones, que se denominan grupos de notificaciones y acciones que pueden reutilizarse en varias alertas.
- **Experiencia de creación unificada**. La creación de todas las alertas para las métricas, los registros y el registro de actividad en Azure Monitor, Log Analytics y Application Insights está disponible desde un solo lugar.
- **Vea las alertas de Log Analytics en Azure Portal**. Ahora también puede observar las alertas de Log Analytics en su suscripción. Anteriormente, estas se encontraban en un portal independiente.
- **Separación de alertas desencadenadas y las reglas de alertas**. Las reglas de alertas (la definición de la condición que desencadena una alerta) y las alertas desencadenadas (una instancia de la activación de la regla de alertas) están diferenciadas, por lo que las vistas operativas y de configuración son independientes.
- **Mejor flujo de trabajo**. La nueva experiencia de creación de alertas guía al usuario por el proceso de configuración de una regla de alertas, lo que facilita la detección de las condiciones correctas para que se active una alerta.

Estados de alerta:

State	Descripción
Nuevo	Se ha detectado la incidencia y todavía no se ha revisado.
Confirmado	Un administrador revisó la alerta y empezó a trabajar en ella.
Closed	Se resolvió el problema. Después de cerrar una alerta, puede volver a abrirla mediante el cambio a otro estado.

Las alertas constan de reglas de alertas, grupos de acciones y condiciones de supervisión.

Los atributos clave de las reglas de alertas son:

- **Recurso de destino**: define el ámbito y las señales disponibles para las alertas. Un destino puede ser cualquier recurso de Azure. Destinos de ejemplo: una máquina virtual, una cuenta de almacenamiento, un conjunto de escalado de máquinas virtuales, un área de trabajo de Log Analytics o un recurso de Application Insights. Para determinados recursos (por ejemplo, Virtual Machines), puede especificar varios recursos como destino de la regla de alertas.
- **Señal**: las señales las emite el recurso de destino y pueden ser de varios tipos. Métrica, registro de actividad, Application Insights y registro.
- **Criterios**: los criterios son una combinación de señal y de lógica aplicada en un recurso de destino. Ejemplos: * porcentaje de CPU: 70 %; tiempo de respuesta del servidor: 4 ms; y recuento de resultados de una consulta de registro: 100.
- **Nombre de la alerta**: nombre específico de la regla de alertas configurada por el usuario.
- **Descripción de la alerta**: descripción de la regla de alertas configurada por el usuario.
- **Gravedad**: gravedad de la alerta, una vez que se cumplen los criterios especificados en la regla de alertas. La gravedad puede tener un valor entre 0 y 4.
- **Acción**: una acción específica llevada a cabo al desencadenarse la alerta.

Un grupo de acciones es una colección de las preferencias de notificación que el propietario de una suscripción de Azure define. Las alertas de Azure Monitor y Service Health usan grupos de acciones para notificar a los usuarios que se ha desencadenado una alerta.

Las **notificaciones** configuran el método con el que se notificará a los usuarios cuando se desencadene el grupo de acciones.

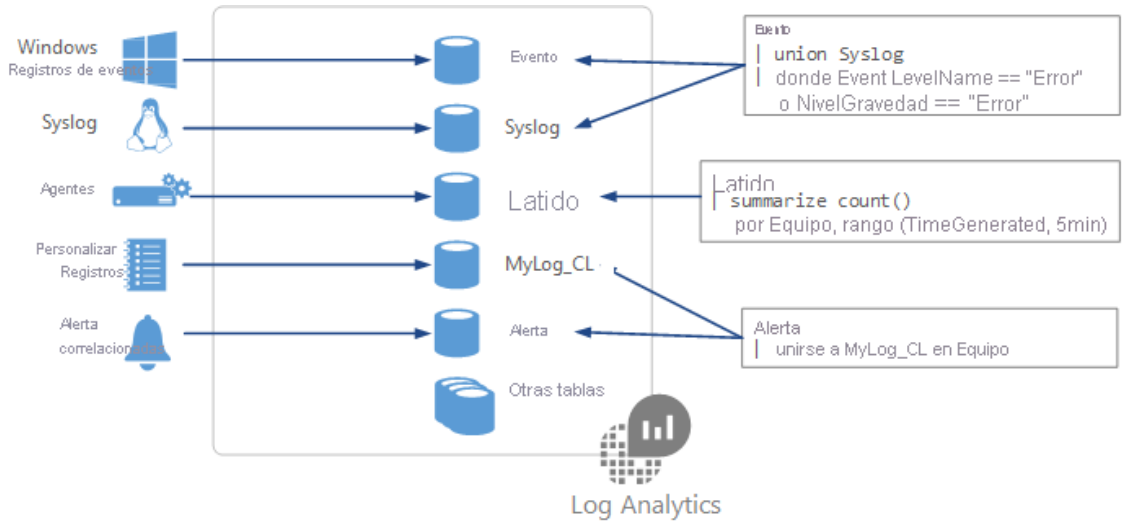
- **Rol de Azure Resource Manager de correo electrónico:** envíe un correo electrónico a los miembros del rol de la suscripción. El correo electrónico solo se enviará a los miembros usuarios de Azure AD del rol. No se enviará correo electrónico a grupos de Azure AD ni entidades de servicio.
- **Correo electrónico, mensaje SMS, notificación de inserción o voz**: especifique cualquier acción de correo electrónico, SMS, notificación de inserción o voz.

En **Acciones** se configura el método en el que se realizan las acciones cuando se desencadena el grupo de acciones.

- **Runbook de Automation**: un runbook de Automation permite definir, compilar, organizar y administrar flujos de trabajo que admiten procesos operativos de red y sistema, así como informar sobre ellos. Un flujo de trabajo de runbook puede llegar a interactuar con todos los tipos de elementos de infraestructura, como aplicaciones, bases de datos y hardware.
- **Azure Functions:** Azure Functions es un servicio de proceso sin servidor que le permite ejecutar código desencadenado por eventos sin tener que aprovisionar o administrar explícitamente la infraestructura.
- **ITSM:**: permite conectar Azure y un producto o servicio compatible de Administración de servicios de TI (ITSM). Esto requiere una conexión de ITSM.
- **Logic Apps:**: Logic Apps conecta las aplicaciones y los servicios críticos para la empresa mediante la automatización de los flujos de trabajo.
- **Webhook**: un webhook es un punto de conexión HTTPS o HTTP que permite a las aplicaciones externas comunicarse con el sistema.

Log Analytics es un servicio que le ayuda a recopilar y analizar los datos generados por los recursos en los entornos locales o de nube. Es una herramienta de Azure Portal que se usa para editar y ejecutar consultas de registro con datos de registros de Azure Monitor.

Algunas tablas de consulta comunes son Evento, Syslog, Latido y Alerta.



Network Watcher proporciona herramientas para **supervisar**, **diagnosticar**, ver las **métricas** y habilitar o deshabilitar **registros** de recursos en una red virtual de Azure. Network Watcher es un servicio regional que permite supervisar y diagnosticar las condiciones en un nivel de escenario de red.

- **Automatización de la supervisión de la red remota con captura de paquetes.** Supervise y diagnostique problemas de red sin iniciar sesión en las máquinas virtuales (VM) mediante Network Watcher. Desencadene la captura de paquetes mediante el establecimiento de alertas y obtenga acceso a información de rendimiento en tiempo real en el ámbito de paquete. Cuando observe un problema, puede investigar en detalle para obtener mejores diagnósticos.
- **Obtenga información detallada sobre el tráfico de la red mediante registros de flujo**. Conozca al detalle el patrón de tráfico de red mediante los registros de flujo del grupo de seguridad de red. La información proporcionada por los registros de flujo le ayuda a recopilar datos para el cumplimiento, la auditoría y la supervisión de su perfil de seguridad de red.
- **Diagnostique problemas de conectividad VPN**. Network Watcher le ofrece la posibilidad de diagnosticar los problemas más comunes de las conexiones y VPN Gateway. Esto no solo le permite identificar el problema, sino también usar los registros detallados creados para ampliar la investigación.

Comprobación del flujo de IP: diagnostique rápidamente problemas de conectividad desde o hacia Internet, y desde o hacia el entorno local. Por ejemplo, confirme si una

regla de seguridad bloquea el tráfico de entrada o de salida hacia una máquina virtual o desde ella. La comprobación del flujo de IP es ideal para asegurarse de que las reglas de seguridad se apliquen correctamente. Cuando se usa para solucionar problemas, si la comprobación del flujo de IP no muestra un problema, tendrá que explorar otras áreas, como las restricciones de firewall.

Próximo salto: sirve para determinar si el tráfico se dirige al destino previsto mediante la representación del próximo salto. Esto le ayudará a determinar si el enrutamiento de la red está configurado correctamente. La funcionalidad Próximo salto también devuelve la tabla de ruta asociada con el próximo salto. Si la ruta se define como una ruta definida por el usuario, se devolverá esa ruta. De lo contrario, la funcionalidad devolverá Ruta de sistema. En función de la situación, el próximo salto podría ser Internet, Aplicación virtual, Puerta de enlace de red virtual, Red virtual local, Emparejamiento de VNet o Ninguno. "Ninguno" le permite saber que, aunque puede haber una ruta del sistema válida al destino, no hay ningún próximo salto para enrutar el tráfico al destino. Cuando se crea una red virtual, Azure crea varias rutas de salida predeterminadas para el tráfico de red. El tráfico saliente de todos los recursos, como las máquinas virtuales, implementados en una red virtual, se enruta por las rutas predeterminadas de Azure. Puede invalidar las rutas predeterminadas de Azure o crear rutas adicionales.

Diagnóstico de VPN: solución de problemas de puertas de enlace y conexiones. "Diagnóstico de VPN" devuelve una gran cantidad de información. La información de resumen está disponible en el portal y en los archivos de registro se proporciona información más detallada. Los archivos de registro se almacenan en una cuenta de almacenamiento e incluyen aspectos como estadísticas de conexión, información de CPU y memoria, errores de seguridad de IKE, eliminaciones de paquetes y búferes y eventos.

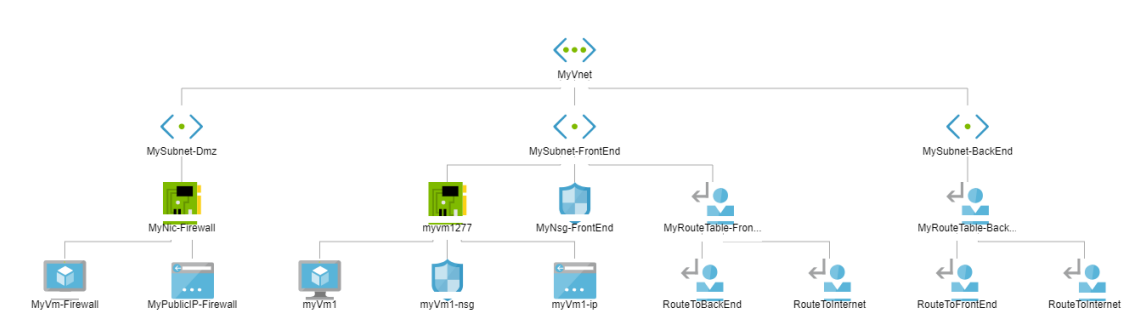
Registros de flujos de NSG: los registros de flujos de grupo de seguridad de red asignan el tráfico IP por medio de un grupo de seguridad de red. Estas funcionalidades se pueden usar en la auditoría y el cumplimiento de la seguridad. Puede definir un conjunto prescriptivo de reglas de seguridad como modelo para la gobernanza de la seguridad de su organización. Una auditoría periódica del cumplimiento puede implementarse de forma programática al comparar las reglas preceptivas con las reglas vigentes para cada una de las máquinas virtuales en la red.

Solución de problemas de conexión. Solución de problemas de conexión de Network Watcher es una adición reciente al conjunto de herramientas y funcionalidades de red de Network Watcher. Solución de problemas de conexión permite solucionar problemas de conectividad y rendimiento de red en Azure.

Objetivo de la comprobación del flujo de IP: comprueba si se permite o deniega un paquete hacia o desde una máquina virtual. Por ejemplo, confirme si una regla de seguridad bloquea el tráfico de entrada o de salida hacia una máquina virtual o desde ella. La comprobación del flujo de IP es ideal para asegurarse de que las reglas de seguridad se apliquen correctamente. Cuando se usa para solucionar problemas, si la comprobación del flujo de IP no muestra un problema, tendrá que explorar otras áreas, como las restricciones de firewall.

Objetivo del próximo salto: determinar si el tráfico se dirige al destino previsto. La información del próximo salto le ayudará a determinar si el enrutamiento de red está configurado correctamente.

La funcionalidad Topología de Network Watcher le permite generar un diagrama visual de los recursos de una red virtual y las relaciones existentes entre los recursos. En la imagen siguiente se muestra un diagrama de topología de ejemplo de una red virtual que tiene tres subredes, dos máquinas virtuales, interfaces de red, direcciones IP públicas, grupos de seguridad de red, tablas de rutas y las relaciones entre los recursos:



La herramienta Topología genera una presentación gráfica de la red virtual de Azure, sus recursos, sus interconexiones y sus relaciones entre sí.

Azure Monitor es una herramienta eficaz de análisis y creación de informes. Úsela para obtener información sobre el comportamiento y la ejecución de su entorno y sus aplicaciones. De este modo, podrá responder de forma proactiva a los errores del sistema.

Azure Monitor recibe datos de recursos de destino, como aplicaciones, sistemas operativos, recursos de Azure, suscripciones a Azure e inquilinos de Azure. La naturaleza del recurso define los tipos de datos que están disponibles. Un tipo de datos será una *métrica*, un *registro*, o bien una métrica y un registro:

- Los tipos de datos basados en ***métricas*** se centran en los valores numéricos que dependen del tiempo y que representan algún aspecto del recurso de destino.
- Los tipos de datos basados en ***registros*** se centran en la consulta de los datos de contenido en archivos de registro estructurados y basados en registros que son pertinentes para el recurso de destino.

- Las alertas de **métricas** proporcionan un desencadenador de alertas para cuando se supera un umbral especificado. Por ejemplo, una alerta de métrica puede notificarle cuando el uso de CPU sea superior al 95 %.
- Las alertas de **registro de actividad** le notifican cuando los recursos de Azure cambian de estado. Por ejemplo, una alerta del registro de actividad puede recibir una notificación cuando se elimina un recurso.
- Las alertas de **registro** se basan en las cosas escritas en los archivos de registro. Por ejemplo, una alerta de registro puede notificarle cuando un servidor web haya devuelto varias respuestas 404 o 500.

- **RECURSO**
  - El *recurso de destino* que se usará para la regla de alertas. Es posible asignar varios recursos de destino a una única regla de alertas. El tipo de recurso definirá los tipos de señales disponibles.
- **CONDICIÓN**
  - El *tipo de señal* que se va a usar para evaluar la regla. El tipo de señal puede ser una métrica, un registro de actividad o de registros. Hay otros, pero no se tratan en este módulo.
  - La *lógica de alerta* aplicada a los datos proporcionados a través del tipo de señal. La estructura de la lógica de alerta cambiará en función del tipo de señal.
- **ACCIONES**
  - La *acción*, como el envío de un correo electrónico, el envío de un mensaje SMS o el uso de un webhook.
  - Un *grupo de acciones*, que normalmente contiene un conjunto único de destinatarios para la acción.

- **DETALLES DE ALERTAS**
    - Un *nombre de alerta* y una *descripción de alerta* que deben especificar el propósito de la alerta.
    - La *gravedad* de la alerta si los criterios o la prueba de lógica tienen una evaluación true. Los cinco niveles de gravedad son:
        - **0**: Crítico
        - **1**: Error
        - **2**: Advertencia
        - **3**: Informativo
        - **4**: Detallado

En Azure Monitor, puede usar las alertas de métricas para realizar una supervisión periódica del umbral de los recursos de Azure. Azure Monitor ejecuta las condiciones del desencadenador de alertas de métricas a intervalos regulares. Cuando la evaluación es verdadera, Azure Monitor envía una notificación. Las alertas de métricas tienen estado y Azure Monitor solo enviará una notificación cuando se cumplan las condiciones de requisitos previos.

Las alertas de métricas estáticas se basan en las condiciones y los umbrales estáticos simples que define. Con las métricas estáticas, debe especificar el umbral que se usará para desencadenar la alerta o la notificación.

Las alertas de métricas dinámicas usan herramientas de aprendizaje automático que proporciona Azure para mejorar automáticamente la precisión de los umbrales definidos por la regla inicial.

No hay ningún umbral estricto en las métricas dinámicas. Sin embargo, deberá definir dos parámetros más:

- El ***período de retroceso*** define el número de períodos anteriores que deben evaluarse.
- El ***número de infracciones*** expresa cuántas veces tiene que desviarse la condición lógica del comportamiento esperado antes de que la regla de alertas desencadene una notificación.

Las alertas de registro usan los datos de registro para evaluar la lógica de la regla y, si es necesario, desencadenan una alerta. Estos datos pueden proceder de cualquier recurso de Azure, como registros de servidor, registros de servidor de aplicaciones o registros de aplicaciones.

Cada alerta de registro tiene una regla de búsqueda asociada. Estas reglas están compuestas por los siguientes elementos:

- **Consulta de registro**: consulta que se ejecuta cada vez que se activa la regla de alertas.
- **Período de tiempo**: intervalo de tiempo para la consulta.
- **Frecuencia**: frecuencia con la que se debe ejecutar la consulta.
- **Umbral**: punto desencadenante para crear una alerta.

Los resultados de la búsqueda de registros son de dos tipos: número de registros o medición de métricas.

Las alertas de registro de actividad le permiten recibir notificaciones cuando se produce un evento específico en algún recurso de Azure. Por ejemplo, puede recibir una notificación cuando alguien cree una máquina virtual nueva en una suscripción. Un registro de actividad también puede incluir alertas para el estado del servicio de Azure.

Las *alertas de métricas* son ideales para supervisar las infracciones de umbral o detectar tendencias; **las *alertas de registro*** permiten una mayor supervisión analítica de los datos históricos.

Hay dos tipos de alertas de registro de actividad:

- **Operaciones específicas**: se aplica a los recursos de la suscripción a Azure y, a menudo, tiene un ámbito con recursos específicos o un grupo de recursos. Utilizará este tipo cuando necesite recibir una alerta que informe de un cambio en un aspecto de su suscripción.

- **Eventos de estado del servicio**: incluyen la notificación de incidentes y el mantenimiento de los recursos de destino.

Los grupos inteligentes son una característica automática de Azure Monitor. Mediante el uso de algoritmos de aprendizaje automático, Azure Monitor agrupa las alertas en función de su repetición o similitud. Los grupos inteligentes le permiten dirigir un grupo de alertas en lugar de alertas individuales.

Azure Monitor es un servicio para recopilar y analizar datos de telemetría. Ayuda a obtener el máximo rendimiento y disponibilidad para las aplicaciones en la nube, así como para los recursos y las aplicaciones locales. Muestra el rendimiento de las aplicaciones e identifica todos los problemas que puedan tener.

Azure Monitor recopila dos tipos fundamentales de datos: **métricas** y **registros**. Las métricas indican cuál es el rendimiento de un recurso y qué otros recursos consume. Los registros contienen registros que indican cuándo se crean o modifican los recursos.

Los registros contienen información con marca de tiempo de los cambios realizados en los recursos. El tipo de información registrada varía según el origen del registro. Los datos de registro se organizan en registros, con diferentes conjuntos de propiedades para cada tipo de registro. Los registros pueden incluir valores numéricos como métricas de Azure Monitor, pero la mayoría incluyen datos de texto, en lugar de valores numéricos.

El tipo más común de entrada de registro realiza el registro de un evento. Los eventos pueden producirse esporádicamente, en lugar de a intervalos fijos o según una programación concreta. Los eventos se crean mediante aplicaciones y servicios, que proporcionan el contexto para los eventos.

Las métricas son valores numéricos que describen algunos aspectos de un sistema en un momento dado. Azure Monitor puede capturar métricas en tiempo casi real. Las métricas se recopilan a intervalos regulares y son útiles para las alertas debido a su muestreo frecuente. Puede usar diversos algoritmos para comparar una métrica con otras y observar las tendencias a lo largo del tiempo.

Kusto Query Language es una herramienta eficaz para explorar los datos y detectar patrones, identificar anomalías y valores atípicos, crear modelos estadísticos y mucho más. **Una consulta de Kusto** es una solicitud de solo lectura para procesar los datos y devolver resultados. La solicitud se indica en texto sin formato, mediante un modelo de flujo de datos fácil de leer, crear y automatizar.

Los registros de Azure Monitor recopilan y organizan los datos de registro generados a partir de los recursos de Azure. Los datos de registro se almacenan en un área de trabajo de Log Analytics. Los datos que se encuentran en el área de trabajo se pueden consultar para obtener análisis de tendencias, informes y alertas.

Azure Monitor - VM Insights es una característica de Azure Monitor que se basa en los registros de Azure Monitor. Azure Monitor - VM Insights usa una tabla denominada "InsightsMetrics". Con esa tabla, los administradores pueden consultar el rendimiento y el uso de las máquinas virtuales.

Azure Monitor captura datos de supervisión de los orígenes siguientes:

- Application
- SO invitado
- Recursos de Azure
- Suscripciones de Azure
- Inquilino de Azure

Los datos recopilados por Azure Monitor se componen de métricas (métricas de Azure Monitor) y registros (registros de Azure Monitor). Las métricas de Azure Monitor son valores numéricos ligeros que se almacenan en una base de datos de serie temporal que se puede usar para las alertas casi en tiempo real. Algunos ejemplos de métricas capturadas son los porcentajes de IOPS y los ciclos de CPU.

Característica	Descripción	Notas
Modo de acceso	Implica el modo en que los usuarios acceden a un área de trabajo de Log Analytics, además de definir el ámbito.	Hay dos opciones. *Contexto del área de trabajo*: proporciona acceso a todos los registros de un área de trabajo donde se asigna el permiso. Las consultas se limitan a todos los datos de todas las tablas. *Contexto del recurso*: proporciona acceso para ver los registros de los recursos de todas las tablas a las que tiene acceso. El ámbito de las consultas solo se limita a los datos asociados a dicho recurso.
Modo de control de acceso	Define cómo funcionan los permisos en cualquier área de trabajo de Log Analytics determinada.	*Requerir permisos del área de trabajo* significa que un usuario tendría acceso a todos los datos de cualquier tabla en la que se hayan definido permisos, lo cual no permite el control de acceso basado en roles (RBAC) granular. *Usar permisos de recurso o de área de trabajo* permite un RBAC granular, ya que los usuarios solo pueden ver los datos de registro de los recursos que se les permite ver. Los permisos se pueden aplicar a un individuo o a grupos de usuarios para el área de trabajo o el recurso.
RBAC de nivel de tabla	Proporciona un mecanismo para definir un control de datos más granular dentro de un área de trabajo de Log Analytics con otros permisos que se enumeran en la tabla.	Esta característica permite que un administrador defina qué tipos de datos específicos son accesibles para un conjunto de usuarios. La configuración de RBAC de nivel de tabla requiere que los roles personalizados de Azure concedan o denieguen el acceso a tablas específicas. Estos roles se aplican a las áreas de trabajo de Log Analytics, con los modos de acceso de contexto de área de trabajo o de contexto del recurso configurados.

Agente	Descripción	Notas
Agente de Azure Monitor	Recopila datos de supervisión de sistemas operativos invitados en máquinas virtuales y entrega datos a métricas o registros de Azure Monitor.	Con el tiempo, este agente reemplazará al agente de Log Analytics y a la extensión de diagnóstico de Azure que se enumeran a continuación. Aunque este agente agrega nuevas funcionalidades, no admite todos los escenarios de supervisión que cubren los agentes anteriores. Antes de cambiar al agente de Azure Monitor, es necesario comprender las contrapartidas.
Agente de Log Analytics	Recopila registros y datos de rendimiento de las máquinas virtuales en Azure, en otras nubes o en el entorno local.	Permite la incorporación de Azure Monitor - VM Insights, Microsoft Defender for Cloud y Microsoft Sentinel. El agente también funciona con cuentas de Azure Automation para incorporar Azure Update Management y State Configuration de Azure Automation, junto con Seguimiento de cambios e inventario de Azure Automation.
Extensión de Diagnósticos de Azure	Permite a los clientes recibir datos adicionales de los sistemas operativos invitados y las cargas de trabajo que se encuentran en recursos de proceso.	Los datos que se capturan principalmente con esta extensión se enviarán a las métricas de Azure Monitor. Si es necesario, también se pueden enviar estos datos a una herramienta de terceros mediante Azure Event Hubs o a Azure Storage para archivarlos. También puede recopilar diagnósticos de arranque, lo que ayuda a las investigaciones de problemas de arranque de máquinas virtuales.
Dependency Agent	Recopila datos detectados sobre determinados procesos que se ejecutan en máquinas virtuales.	Asigna todas las dependencias entre máquinas virtuales y cualquier dependencia de procesos externos.

El *esquema* es una serie de tablas agrupadas de forma lógica. El esquema permite comprender fácilmente cómo Log Analytics almacena los datos. El esquema se muestra en el *panel de esquema* ubicado en el extremo izquierdo de un área de trabajo de Log Analytics. El esquema es útil cuando se elaboran consultas.