

**Guía de inicio para redes virtuales**

**¿Qué es Azure Virtual Network?**

Azure Virtual Network (VNet) es el bloque de creación fundamental de una red privada en Azure. VNet permite muchos tipos de recursos de Azure, como Azure Virtual Machines (máquinas virtuales), para comunicarse de forma segura entre usuarios, con Internet y con las redes locales. VNet es similar a una red tradicional que funcionaría en su propio centro de datos, pero aporta las ventajas adicionales de la infraestructura de Azure, como la escala, la disponibilidad y el aislamiento.

**Razones para usar una red virtual de Azure**

Una red virtual de Azure permite que los recursos de Azure se comuniquen de forma segura entre ellos, con Internet y con redes locales. Entre los escenarios clave que se pueden realizar con una red virtual se incluyen los siguientes: la comunicación de los recursos de Azure con Internet, la comunicación entre los recursos de Azure, la comunicación con los recursos locales, el filtrado del tráfico de red, el enrutamiento del tráfico de red y la integración con los servicios de Azure.

**Comunicación con internet**

De manera predeterminada, todos los recursos de una red virtual tienen comunicación de salida hacia Internet. Para comunicarse con un recurso entrante, asígnele una dirección IP pública o un equilibrador de carga público. También puede usar la dirección IP pública o el equilibrador de carga público para administrar las conexiones salientes. Para más información sobre las conexiones salientes en Azure, consulte [Conexiones salientes](https://learn.microsoft.com/es-es/azure/load-balancer/load-balancer-outbound-connections), [Direcciones IP públicas](https://learn.microsoft.com/es-es/azure/virtual-network/ip-services/virtual-network-public-ip-address) y [Equilibrador de carga](https://learn.microsoft.com/es-es/azure/load-balancer/load-balancer-overview).

**Comunicación entre recursos de Azure**

Los recursos de Azure se comunican de manera segura entre sí de una de las maneras siguientes:

* **Mediante una red virtual**: tanto las máquinas virtuales como otros tipos de recursos de Azure se pueden implementar en una red virtual, como Azure App Service Environment, Azure Kubernetes Service (AKS) y Azure Virtual Machine Scale Sets. Para ver una lista completa de los recursos de Azure que puede implementar en una red virtual, consulte [Integración de red virtual para los servicios de Azure](https://learn.microsoft.com/es-es/azure/virtual-network/virtual-network-for-azure-services).
* **Mediante un punto de conexión de servicio de red virtual**: extienda el espacio de direcciones privadas de la red virtual y la identidad de la red virtual a los recursos del servicio de Azure, como cuentas de Azure Storage y Azure SQL Database, mediante una conexión directa. Los puntos de conexión de los servicios permiten proteger los recursos críticos de los servicios de Azure únicamente en una red virtual. Para más información, consulte [Puntos de conexión de servicio de red virtual](https://learn.microsoft.com/es-es/azure/virtual-network/virtual-network-service-endpoints-overview).
* **Mediante emparejamiento de VNet**: Las redes virtuales se pueden conectar entre sí, lo que permite que los recursos de cualquiera de ellas se comuniquen entre sí mediante el emparejamiento de red virtual. Las redes virtuales que conecte pueden estar en la misma región de Azure o en regiones distintas. Para más información, consulte [Emparejamiento de redes virtuales de Azure](https://learn.microsoft.com/es-es/azure/virtual-network/virtual-network-peering-overview).

**Comunicación con recursos locales**

Puede conectar los equipos y redes locales a una red virtual mediante cualquiera de las opciones siguientes:

* **Red privada virtual (VPN) de punto a sitio**: se establece entre una red virtual y un equipo individual de la red. Cada equipo que desea establecer conectividad con una red virtual debe configurar su conexión. Este tipo de conexión es muy útil cuando se está comenzando con Azure, o para los desarrolladores, porque requiere poco o ningún cambio en la red existente. La comunicación entre el equipo y una red virtual se envía mediante un túnel cifrado a través de internet. Para más información, consulte [VPN de punto a sitio](https://learn.microsoft.com/es-es/azure/vpn-gateway/point-to-site-about?toc=/azure/virtual-network/toc.json).
* **VPN de sitio a sitio**: se establece entre un dispositivo VPN local y una instancia de Azure VPN Gateway que está implementada en una red virtual. Este tipo de conexión permite que cualquier recurso local que autorice acceda a una red virtual. La comunicación entre un dispositivo VPN local y una puerta de enlace de VPN de Azure se envía mediante un túnel cifrado a través de internet. Para más información, consulte [VPN de sitio a sitio](https://learn.microsoft.com/es-es/azure/vpn-gateway/design?toc=/azure/virtual-network/toc.json#s2smulti).
* **Azure ExpressRoute:** se establece entre la red y Azure, mediante un asociado de ExpressRoute. Esta conexión es privada. El tráfico no pasa por Internet. Para más información, consulte [ExpressRoute](https://learn.microsoft.com/es-es/azure/expressroute/expressroute-introduction?toc=/azure/virtual-network/toc.json).

**Filtrado del tráfico de red**

Puede filtrar el tráfico de red entre subredes mediante una o ambas de las siguientes opciones:

* **Grupos de seguridad de red:** los grupos de seguridad de red y los grupos de seguridad de aplicaciones pueden contener varias reglas de seguridad de entrada y salida que le permiten filtrar el tráfico que llega y sale de los recursos por dirección IP, puerto y protocolo de origen y destino. Para más información, vea [grupos de seguridad de red](https://learn.microsoft.com/es-es/azure/virtual-network/network-security-groups-overview#network-security-groups) y [grupos de seguridad de aplicaciones](https://learn.microsoft.com/es-es/azure/virtual-network/network-security-groups-overview#application-security-groups).
* **Aplicaciones virtuales de red**: una aplicación de red virtual es una máquina virtual que ejecuta una función de red, como un firewall, la optimización de WAN u otra función de red. Para ver una lista de las aplicaciones virtuales de red que se pueden implementar en una red virtual, consulte [Azure Marketplace](https://azuremarketplace.microsoft.com/marketplace/apps/category/networking?page=1&subcategories=appliances).

**Enrutado del tráfico de red**

De forma predeterminada Azure enruta el tráfico entre subredes, redes virtuales conectadas, redes locales e Internet. Puede implementar una o ambas de las siguientes opciones para reemplazar las rutas predeterminadas que crea Azure:

* **Tablas de ruta**: puede crear tablas de ruta personalizadas con las rutas que controlan a dónde se enruta el tráfico para cada subred. Más información sobre las [tablas de rutas](https://learn.microsoft.com/es-es/azure/virtual-network/virtual-networks-udr-overview#user-defined).
* **Rutas de Protocolo de puerta de enlace de borde (BGP)** : si conecta la red virtual a su red local mediante una conexión de Azure VPN Gateway o ExpressRoute, puede propagar las rutas BGP locales a sus redes virtuales. Más información sobre el uso de BGP con [Azure VPN Gateway](https://learn.microsoft.com/es-es/azure/vpn-gateway/vpn-gateway-bgp-overview?toc=/azure/virtual-network/toc.json) y [ExpressRoute](https://learn.microsoft.com/es-es/azure/expressroute/expressroute-routing?toc=/azure/virtual-network/toc.json" \l "dynamic-route-exchange).

**Integración de red virtual para los servicios de Azure**

La integración de servicios de Azure en una red virtual de Azure permite el acceso privado al servicio desde las máquinas virtuales o los recursos de proceso de la red virtual. Puede integrar los servicios de Azure en la red virtual con las siguientes opciones:

* Implementación de [instancias dedicadas del servicio](https://learn.microsoft.com/es-es/azure/virtual-network/virtual-network-for-azure-services) en una red virtual. Luego se puede acceder de forma privada a los servicios dentro de la red virtual y desde redes locales.
* Usando [Private Link](https://learn.microsoft.com/es-es/azure/private-link/private-link-overview) para acceder de forma privada a una instancia específica del servicio desde la red virtual y desde las redes locales.
* También puede acceder al servicio mediante puntos de conexión públicos si amplía una red virtual al servicio a través de los [puntos de conexión de servicio](https://learn.microsoft.com/es-es/azure/virtual-network/virtual-network-service-endpoints-overview). Los puntos de conexión de servicio permiten que los recursos de servicio se protejan en la red virtual.

**Límites de Azure VNet**

Hay ciertos límites en torno al número de recursos de Azure que puede implementar. La mayoría de los límites de redes de Azure están en los valores máximos. Sin embargo, puede [aumentar ciertos límites de red](https://learn.microsoft.com/es-es/azure/azure-portal/supportability/networking-quota-requests) como se especifica en la [página de límites de red virtual](https://learn.microsoft.com/es-es/azure/azure-resource-manager/management/azure-subscription-service-limits#networking-limits).

**Redes virtuales y zonas de disponibilidad**

Las redes virtuales y las subredes abarcan todas las zonas de disponibilidad de una región. No es necesario dividirlas por zonas de disponibilidad para dar cabida a los recursos de zona. Por ejemplo, si configura una máquina virtual de zona, no tiene que tener en cuenta la red virtual al seleccionar la zona de disponibilidad de la máquina virtual. Lo mismo sucede con otros recursos de zona.

**Precios**

No hay ningún cargo por usar Azure VNet, es gratuito. Los cargos estándar son aplicables para recursos como Virtual Machines (máquinas virtuales) y otros productos. Para más información, consulte [Precios de Virtual Network](https://azure.microsoft.com/pricing/details/virtual-network/) y la [Calculadora de precios](https://azure.microsoft.com/pricing/calculator/) de Azure.