**Introducción**

Este módulo se centra en dotar a los administradores con los conocimientos y aptitudes necesarios para planear e implementar medidas de seguridad sólidas para el acceso privado a los recursos de Azure, proteger los datos confidenciales y mejorar la integridad de la red.

**Escenario**

Imagine que es un especialista en seguridad de Azure responsable de proteger el acceso a los recursos de Azure en entornos corporativos. Su organización confía en los servicios de Azure para la gestión de aplicaciones y datos críticos, y debe asegurarse de que el acceso esté restringido a usuarios autorizados, al mismo tiempo que mantiene altos niveles de seguridad.

**Objetivos de aprendizaje**

Al final de este módulo, los participantes podrán:

* Planee e implemente estrategias de seguridad para el acceso privado a los recursos de Azure, protegiendo datos confidenciales y recursos.
* Utilice eficazmente puntos de conexión de servicio de red virtual para proteger el acceso a los servicios de Azure.
* Planee e implemente puntos de conexión privados para habilitar la conectividad de red privada con los servicios de Azure.
* Cree y administre servicios de Private Link para exponer recursos de forma segura a los consumidores.
* Integre Azure App Service y Azure Functions con redes virtuales para mejorar la seguridad y el aislamiento.
* Configure las opciones de seguridad de red para instancias de App Service Environment (ASE) para proteger las aplicaciones web.
* Establezca configuraciones de seguridad de red para Azure SQL Managed Instance para proteger las bases de datos y el acceso a los datos.

**Objetivos**

El módulo tiene como objetivo proveer a los participantes de los conocimientos y aptitudes necesarios para diseñar, implementar y administrar estrategias de seguridad completas de acceso privado a los recursos de Azure. Los participantes podrán proteger eficazmente datos críticos y aplicaciones, garantizando que solo los usuarios y sistemas autorizados puedan acceder a ellos, preservando la integridad del entorno de red de Azure.

**Planeamiento e implementación de puntos de conexión de servicio de red virtual**

El punto de conexión de servicio de red virtual (VNet) proporciona conectividad directa y segura con los servicios de Azure por medio de una ruta optimizada a través de la red troncal de Azure. Los puntos de conexión permiten proteger los recursos de servicio de Azure críticos únicamente para las redes virtuales. Los puntos de conexión de servicio permiten a las direcciones IP privadas de la red virtual alcanzar el punto de conexión de un servicio de Azure sin necesidad de una dirección IP pública en la red virtual.

Los puntos de conexión de servicio están disponibles para los servicios y las regiones siguientes de Azure. El recurso *Microsoft.\** está entre paréntesis. Habilítelo desde la subred mientras configura los puntos de conexión del servicio:

**Disponibilidad general**

* Azure Storage (*Microsoft.Storage*): Disponibilidad general en todas las regiones de Azure.
* Puntos de conexión de servicio entre regiones de Azure Storage (*Microsoft.Storage.Global*): Disponibilidad general en todas las regiones de Azure.
* Azure SQL Database (*Microsoft.Sql*): Disponibilidad general en todas las regiones de Azure.
* Azure Synapse Analytics (*Microsoft.Sql*): Disponible con carácter general en todas las regiones de Azure para grupos de SQL dedicados (anteriormente, SQL DW).
* Servidor de Azure Database for PostgreSQL (*Microsoft.Sql*): Disponibilidad general en las regiones de Azure en las que el servicio de base de datos esté disponible.
* Servidor de Azure Database for MySQL (*Microsoft.Sql*): Disponibilidad general en las regiones de Azure en las que el servicio de base de datos esté disponible.
* Azure Database for MariaDB (*Microsoft.Sql*): Disponibilidad general en las regiones de Azure en las que el servicio de base de datos esté disponible.
* Azure Cosmos DB (*Microsoft.AzureCosmosDB*): Disponibilidad general en todas las regiones de Azure.
* Azure Key Vault (*Microsoft.KeyVault*): Disponibilidad general en todas las regiones de Azure.
* Azure Service Bus (*Microsoft.ServiceBus*): Disponibilidad general en todas las regiones de Azure.
* Azure Event Hubs (*Microsoft.EventHub*): Disponibilidad general en todas las regiones de Azure.
* Azure Data Lake Store Gen 1 (*Microsoft.AzureActiveDirectory*): Disponible con carácter general en todas las regiones de Azure donde ADLS Gen1 esté disponible.
* Azure App Service (*Microsoft.Web*): Disponible con carácter general en todas las regiones de Azure en las que App Service esté disponible.
* Azure Cognitive Services (*Microsoft.CognitiveServices*): Disponible con carácter general en todas las regiones de Azure en las que los servicios de Azure AI estén disponibles.

**Ventajas principales**

Los puntos de conexión de servicio proporcionan las siguientes ventajas:

* **Seguridad mejorada para los recursos de servicio de Azure**: Los espacios de direcciones privadas de una red virtual pueden superponerse. No se pueden usar espacios superpuestos para identificar de forma exclusiva el tráfico que parte de una red virtual. Los puntos de conexión de servicio permiten proteger los recursos de los servicios de Azure en la red virtual al ampliar la identidad de la red virtual al servicio. Una vez que habilita puntos de conexión de servicio en su red virtual, puede agregar una regla de red virtual para proteger los recursos de los servicios de Azure en la red virtual. La adición de la regla proporciona una mayor 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**: hoy, las rutas de la red virtual que fuerzan el tráfico de Internet a las aplicaciones virtuales o locales también fuerzan al tráfico del servicio de Azure a que realice 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. Para más información sobre las rutas definidas por el usuario y la tunelización forzada, consulte Enrutamiento del tráfico de redes virtuales de Azure.

* **Fácil de configurar 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 de traducción de direcciones de red (NAT) o de puerta de enlace necesario para configurar los puntos de conexión de servicio. Estos se pueden configurar con una selección individual en una subred. El mantenimiento de los puntos de conexión no supone una sobrecarga adicional.

**Limitaciones**

* Esta característica solo está disponible en las redes virtuales implementadas con el modelo de implementación de Azure Resource Manager.
* Los puntos de conexión están habilitados en subredes configuradas en redes virtuales de Azure. No se pueden usar los puntos de conexión para el tráfico desde los servicios locales a los servicios de Azure. Para obtener más información, consulte Protección del acceso a servicios de Azure desde el entorno local.
* Para Azure SQL, un punto de conexión de servicio solo se aplica al tráfico del servicio de Azure dentro de la región de una red virtual.
* En el caso de Azure Data Lake Storage (ADLS) Gen 1, la funcionalidad de integración de red virtual solo está disponible para las redes sociales que se encuentran dentro de la misma región. Tenga también en cuenta que la integración de la red virtual en ADLS Gen1 usa la seguridad del punto de conexión de servicio de red virtual entre la red virtual y Azure Active Directory (Azure AD) para generar notificaciones de seguridad adicionales en el token de acceso. Estas notificaciones se usan entonces para autenticar la red virtual en la cuenta de Data Lake Storage Gen1 y permitir el acceso. La etiqueta Microsoft.AzureActiveDirectory que aparece debajo de los servicios que admiten puntos de conexión de servicios se usa solo para admitir puntos de conexión de servicios en ADLS Gen 1. Azure AD no admite puntos de conexión de servicio de forma nativa. Para más información acerca de la integración de redes virtuales en Azure Data Lake Store Gen 1, consulte Seguridad de red en Azure Data Lake Storage Gen1.
* Una red virtual se puede asociar a hasta 200 suscripciones y regiones diferentes por cada servicio admitido con reglas de red virtual activas configuradas.

**Protección de servicios de Azure en redes virtuales**

* Un punto de conexión de servicio de red virtual proporciona la identidad de la red virtual al servicio de Azure. Una vez que habilita puntos de conexión de servicio en su red virtual, puede agregar una regla de red virtual para proteger los recursos de los servicios de Azure en la red virtual.
* Actualmente, el tráfico del servicio de Azure desde una red virtual usa direcciones IP públicas como direcciones IP de origen. Con los puntos de conexión de servicio, el tráfico del servicio cambia para usar direcciones privadas de red virtual como la direcciones IP de origen al acceder al servicio de Azure desde una red virtual. Este modificador permite acceder a los servicios sin necesidad de direcciones IP públicas y reservadas utilizadas en los firewalls IP.

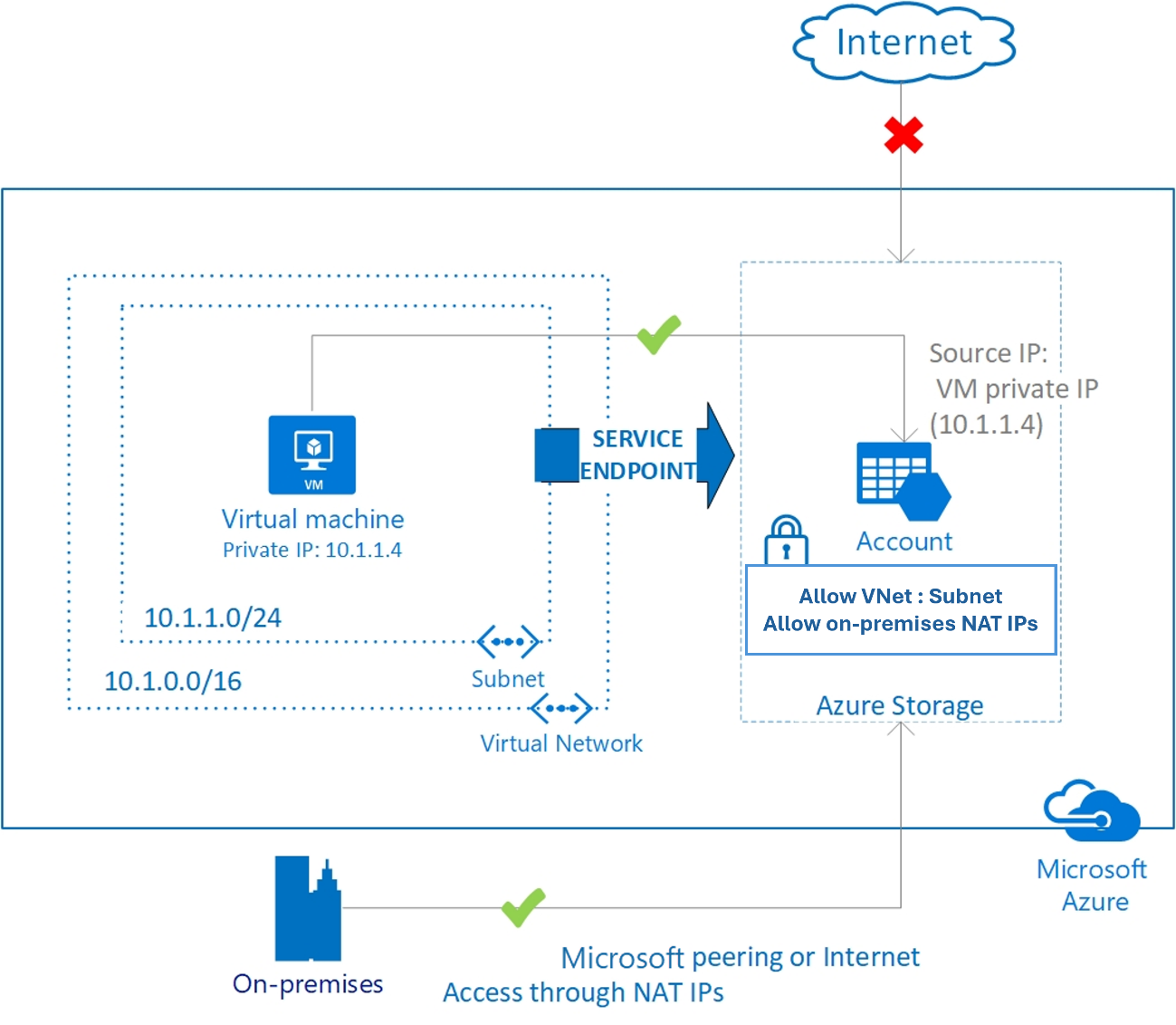
**Nota**

Con los puntos de conexión de servicio, las direcciones IP de origen de las máquinas virtuales en la subred para el tráfico de servicio pasan de utilizar direcciones IPv4 públicas a utilizar direcciones IPv4 privadas. Las reglas existentes de firewall de servicio de Azure que utilizan direcciones IP públicas Azure dejarán de funcionar con este cambio. Asegúrese de que las reglas de firewall del servicio de Azure permiten este cambio antes de configurar los puntos de conexión de servicio. También es posible que experimente una interrupción temporal del tráfico de servicio desde esta subred mientras configura los puntos de conexión de servicio.

**Protección del acceso de servicio de Azure desde el entorno local**

De forma predeterminada, a los recursos de los servicios de Azure protegidos en las redes virtuales no se puede acceder desde redes locales. Si quiere permitir el tráfico desde el entorno local, también debe permitir las direcciones IP públicas (normalmente NAT) desde el entorno local o ExpressRoute. Estas direcciones IP se pueden agregar mediante la configuración del firewall de IP para los recursos de los servicios de Azure.

ExpressRoute: Si usa ExpressRoute para el emparejamiento público o el emparejamiento de Microsoft desde un entorno local, tendrá que identificar las direcciones IP de NAT que va a usar. En el caso del emparejamiento público, cada circuito ExpressRoute usa de forma predeterminada dos direcciones IP de NAT que se aplican al tráfico del servicio de Azure cuando entra en la red troncal de Microsoft Azure. En el caso del emparejamiento de Microsoft, las direcciones IP de NAT que se utilizan las proporcionan el cliente o el proveedor de servicios. Para permitir el acceso a los recursos de servicio, tiene que permitir estas direcciones IP públicas en la configuración del firewall de IP de recursos. Para encontrar las direcciones de IP de circuito de ExpressRoute de los pares públicos, abra una incidencia de soporte técnico con ExpressRoute a través de Azure Portal.



**Configuración**

* Configure los puntos de conexión de servicio en una subred de una red virtual. Los puntos de conexión funcionan con cualquier tipo de instancias de proceso que se ejecute en esa subred.
* Puede configurar varios puntos de conexión de servicio para todos los servicios de Azure admitidos (por ejemplo, Azure Storage o Azure SQL Database) en una subred.
* Para Azure SQL Database, las redes virtuales deben estar en la misma región que el recurso de servicio de Azure. En el caso de los restantes servicios, los recursos de servicio de Azure se pueden proteger en las redes virtuales de cualquier región.
* La red virtual donde se ha configurado el punto de conexión puede estar en la misma suscripción o en otra distinta del recurso de servicio de Azure.
* Para los servicios compatibles, puede proteger los nuevos recursos o los recursos existentes a las redes virtuales con puntos de conexión de servicio.

**Consideraciones**

* Después de habilitar un punto de conexión de servicio, las direcciones IP de origen pasan de utilizar las direcciones IPv4 públicas a usar su dirección IPv4 privada, cuando se comunican con el servicio desde dicha subred. Las conexiones TCP abiertas existentes en el servicio se cierran durante este cambio. Asegúrese de que no se esté ejecutando ninguna tarea crítica al habilitar o deshabilitar un punto de conexión de servicio en un servicio para una subred. Además, asegúrese de que las aplicaciones pueden conectarse automáticamente a los servicios de Azure después del cambio de dirección IP.

El cambio de dirección IP solo afecta el tráfico del servicio desde la red virtual. No afecta a ningún otro tráfico entrante o saliente de las direcciones IPv4 públicas asignadas a las máquinas virtuales. Para los servicios de Azure, si tiene reglas de firewall existentes que usan direcciones IP públicas de Azure, estas reglas dejan de funcionar con el cambio a las direcciones privadas de red virtual.

* Con los puntos de conexión de servicio, las entradas DNS para los servicios de Azure permanecen tal cual en la actualidad y siguen resolviendo las direcciones IP públicas asignadas al servicio de Azure.
* Grupos de seguridad de red (NSG) con puntos de conexión de servicio:
  + De forma predeterminada, los grupos de seguridad de red no solo permiten el tráfico de Internet saliente, sino también el tráfico de su red virtual a los servicios de Azure. Este tráfico sigue funcionando con puntos de conexión de servicio tal cual.
  + Si desea denegar todo el tráfico de Internet saliente y permitir únicamente el tráfico a servicios de Azure concretos, puede hacerlo mediante las etiquetas de servicio de sus grupos de seguridad de red. Puede especificar los servicios de Azure compatibles como destino en las reglas de grupos de seguridad de red y Azure también proporciona el mantenimiento de las direcciones IP subyacentes en cada etiqueta.

**Escenarios**

* **Redes virtuales emparejadas, conectadas o múltiples**: para proteger los servicios de Azure de varias subredes dentro de una red virtual o entre varias redes virtuales, puede habilitar los puntos de conexión de servicio en cada una de las subredes de manera independiente y proteger los recursos del servicio de Azure a todas las subredes.
* **Filtrado de tráfico saliente desde una red virtual a los servicios de Azure**: Si desea inspeccionar o filtrar el tráfico enviado a un servicio de Azure desde una red virtual, puede implementar una aplicación virtual de red dentro de la red virtual. Después, puede aplicar los puntos de conexión de servicio a la subred donde se implementa la aplicación virtual de red y se protegen los recursos de servicio de Azure solo para esta subred. Este escenario puede resultar útil si desea usar el filtrado de la aplicación virtual de red para restringir el acceso de los servicios de Azure desde la red virtual solo a recursos concretos de Azure. Para más información, consulte el artículo sobre la salida con las aplicaciones de redes virtuales.
* **Protección de recursos de Azure con los servicios implementados directamente en redes virtuales**: puede implementar directamente varios servicios de Azure en subredes concretas de una red virtual. Puede proteger los recursos de servicio de Azure para subredes de servicio administrado mediante la configuración de un punto de conexión de servicio en la subred de servicio administrada.
* **Tráfico de disco procedente de una máquina virtual de Azure**: el tráfico de disco de máquina virtual, tanto en discos administrados como no administrados, no resulta afectado por los puntos de conexión de servicio que enrutan los cambios en Azure Storage. Este tráfico no solo incluye la E/S de disco, sino también el montaje y desmontaje. Puede limitar el acceso de REST a los blobs en páginas para determinadas redes mediante puntos de conexión de servicio y reglas de red de Azure Storage.

**Registro y solución de problemas**

Una vez que configure los puntos de conexión de servicio en un servicio concreto, asegúrese de que la ruta del punto de conexión de servicio está en vigor de la forma siguiente:

* Valide la dirección IP de origen de todas las solicitudes de servicio en los diagnósticos del servicio. Todas las nuevas solicitudes con puntos de conexión de servicio muestran la dirección IP de origen de la solicitud como la dirección de red virtual privada, asignada al cliente que realiza la solicitud desde la red virtual. Sin el punto de conexión, la dirección es una dirección IP pública de Azure.
* Visualice las rutas eficaces en cualquier interfaz de red de una subred. La ruta al servicio:
  + Muestra una ruta predeterminada más específica a los intervalos de prefijos de la dirección de cada servicio
  + Tiene una clase nextHopType de *VirtualNetworkServiceEndpoint*
  + Indica que está en vigor una conexión más directa al servicio, en comparación con cualquier ruta de tunelización forzada

**Nota**

Las rutas del punto de conexión de servicio invalidan las rutas BGP para la coincidencia del prefijo de dirección de un servicio de Azure.

**Aprovisionamiento**

Un usuario con acceso de escritura a una red virtual puede configurar puntos de conexión de servicio en redes virtuales de forma independiente. Para proteger los recursos de los servicios de Azure en una red virtual, el usuario debe tener permiso en *Microsoft.Network/virtualNetworks/subnets/joinViaServiceEndpoint/action* para las subredes agregadas. Los roles de administrador de servicios integrados incluyen este permiso de manera predeterminada. El permiso se puede modificar mediante la creación de roles personalizados.

Las redes virtuales y los recursos de servicio de Azure pueden encontrarse en la misma o en diferentes suscripciones. Algunos servicios de Azure (no todos), como Azure Storage y Azure Key Vault, también admiten puntos de conexión de servicio en distintos inquilinos de Active Directory (AD). Esto significa que la red virtual y el recurso del servicio de Azure pueden estar en distintos inquilinos de Active Directory (AD).

**Directivas de punto de conexión de servicio de una red virtual**

Las directivas de punto de conexión de servicio de una red virtual permiten filtrar el tráfico de la red virtual a los servicios de Azure. Este filtro solo permite determinados recursos de servicio de Azure a través de puntos de conexión de servicio. Las directivas de punto de conexión de servicio ofrecen un control de acceso pormenorizado para el tráfico de red virtual a los servicios de Azure.

**Planeamiento e implementación de puntos de conexión privados**

Un punto de conexión privado es una interfaz de red que usa una dirección IP privada de la red virtual. Esta interfaz de red le conecta de forma privada y segura a un servicio con la tecnología de Azure Private Link. Al habilitar un punto de conexión privado, incorpora el servicio a la red virtual.

El servicio podría ser un servicio de Azure como:

* Azure Storage
* Azure Cosmos DB
* Azure SQL Database
* Su propio servicio mediante el servicio Private Link.

**Nota**

Solo se pueden crear puntos de conexión privados en una cuenta de almacenamiento De uso general v2 (GPv2).

**Seguridad de red de los puntos de conexión privados**

Cuando se usan puntos de conexión privados, el tráfico se protege en un recurso de vínculo privado. La plataforma valida las conexiones de red y solo permite las que llegan al recurso de vínculo privado especificado. Para acceder a más subrecursos dentro del mismo servicio Azure, se necesitan más puntos de conexión privados con sus correspondientes destinos. En el caso de Azure Storage, por ejemplo, se necesitarán puntos de conexión privados independientes para acceder a los subrecursos archivo y blob.

Los puntos de conexión privados proporcionan una dirección IP de acceso privado para el servicio de Azure, pero no restringen necesariamente el acceso de red pública al servicio. Sin embargo, todos los demás servicios de Azure requieren controles de acceso adicionales. Estos controles proporcionan una capa de seguridad de red adicional a los recursos, que ofrece protección para evitar el acceso al servicio de Azure asociado con el recurso de vínculo privado.

Los puntos de conexión privados admiten directivas de red. Las directivas de red permiten la compatibilidad con grupos de seguridad de red (NSG), rutas definidas por el usuario (UDR) y grupos de seguridad de aplicaciones (ASG). Para más información sobre la habilitación de directivas de red para un punto de conexión privado, consulte Administración de directivas de red para puntos de conexión privados.

A través de una conexión de punto de conexión privado, el propietario de un recurso de vínculo privado puede:

* Revisar todos los detalles de la conexión del punto de conexión privado.
* Aprobar una conexión de punto de conexión privado. El punto de conexión privado correspondiente está habilitado para enviar tráfico al recurso de vínculo privado.
* Rechazar una conexión de punto de conexión privado. El punto de conexión privado correspondiente se actualiza para reflejar el estado.
* Eliminar una conexión de punto de conexión privado en cualquier estado. El punto de conexión privado correspondiente se actualiza con un estado desconectado para reflejar la acción. El propietario del punto de conexión privado solo puede eliminar el recurso en este momento.

**Conexión mediante un alias**

Un alias es un moniker único que se genera cuando el propietario de un servicio crea un servicio de vínculo privado detrás de un equilibrador de carga estándar. Los propietarios de servicios pueden compartir este alias sin conexión con los consumidores del servicio.

Los consumidores pueden solicitar una conexión al servicio de vínculo privado mediante el URI de recurso o el alias. Para conectarse mediante el alias, cree un punto de conexión privado mediante el método de aprobación de conexión manual. Para usar el método de aprobación de conexión manual, establezca el parámetro de solicitud manual en True durante el flujo de creación del punto de conexión privado.

**Configuración de DNS**

La configuración de DNS que se usa para conectarse a un recurso de vínculo privado es importante. Es posible que los servicios de Azure existentes ya tengan una configuración de DNS que puede usar al conectarse a través de un punto de conexión público. Para conectarse al mismo servicio a través de un punto de conexión privado, se requieren configuraciones DNS independientes, a menudo configuradas a través de zonas DNS privadas. Asegúrese de que la configuración de DNS sea correcta cuando use el nombre de dominio completo (FQDN) para la conexión. La configuración debe resolver la dirección IP privada del punto de conexión privado.

La interfaz de red asociada al punto de conexión privado contiene la información necesaria para configurar DNS. La información incluye el FQDN y las direcciones IP privadas del recurso de vínculo privado.

**Limitaciones**

En la siguiente información se enumeran las limitaciones conocidas para el uso de puntos de conexión privados:

**Dirección IP estática**

| **Limitación** | **Descripción** |
| --- | --- |
| Actualmente no se admite la configuración de direcciones IP estáticas. | Azure Kubernetes Service (AKS) Azure Application Gateway HD Insight Almacenes de Recovery Services Servicios de Private Link de terceros |

**Grupo de seguridad de red**

| **Limitación** | **Descripción** |
| --- | --- |
| Las rutas vigentes y las reglas de seguridad no están disponibles para la interfaz de red del punto de conexión privado. | Las rutas vigentes y las reglas de seguridad no se mostrarán para la NIC del punto de conexión privado en Azure Portal. |
| Registros de flujo de NSG no admitidos. | Los registros de flujo de NSG no están disponibles para el tráfico entrante destinado a un punto de conexión privado. |
| No más de 50 miembros en un grupo de seguridad de aplicaciones. | Cincuenta es el número de configuraciones de IP que se pueden asociar a cada ASG respectivo que está asociado al NSG en la subred del punto de conexión privado. Los errores de conexión pueden producirse con más de 50 miembros. |
| Los intervalos de puertos de destino admiten hasta un factor de 250 000. | Los intervalos de puertos de destino se admiten como una multiplicación SourceAddressPrefixes, DestinationAddressPrefixes y DestinationPortRanges.  Regla de entrada de ejemplo: Un origen \* un destino \* 4K portRanges = 4K Válido 10 orígenes \* 10 destinos \* 10 portRanges = 1 K Válido 50 orígenes \* 50 destinos \* 50 portRanges = 125 K Válido 50 orígenes \* 50 destinos \* 100 portRanges = 250 K Válido 100 orígenes \* 100 destinos \* 100 portRanges = 1M No válido, el NSG tiene demasiados orígenes, destinos o puertos. |
| El filtrado de puertos de origen se interpreta como \* | El filtrado de puertos de origen no se usa activamente como escenario válido de filtrado de tráfico para el tráfico que está destinado a un punto de conexión privado. |
| Característica no disponible en determinadas regiones. | Actualmente no está disponible en las siguientes regiones: Oeste de la India Centro de Australia 2 Oeste de Sudáfrica Sudeste de Brasil Todas las regiones de Azure Government Todas las regiones de China |

**Consideraciones sobre el grupo de seguridad de red**

* El tráfico saliente denegado desde un punto de conexión privado no es un escenario válido, ya que el proveedor de servicios no puede originar el tráfico.
* Es posible que los siguientes servicios necesiten que todos los puertos de destino estén abiertos cuando usen un punto de conexión privado y agreguen filtros de seguridad de NSG:  
  + Azure Cosmos DB

**UDR**

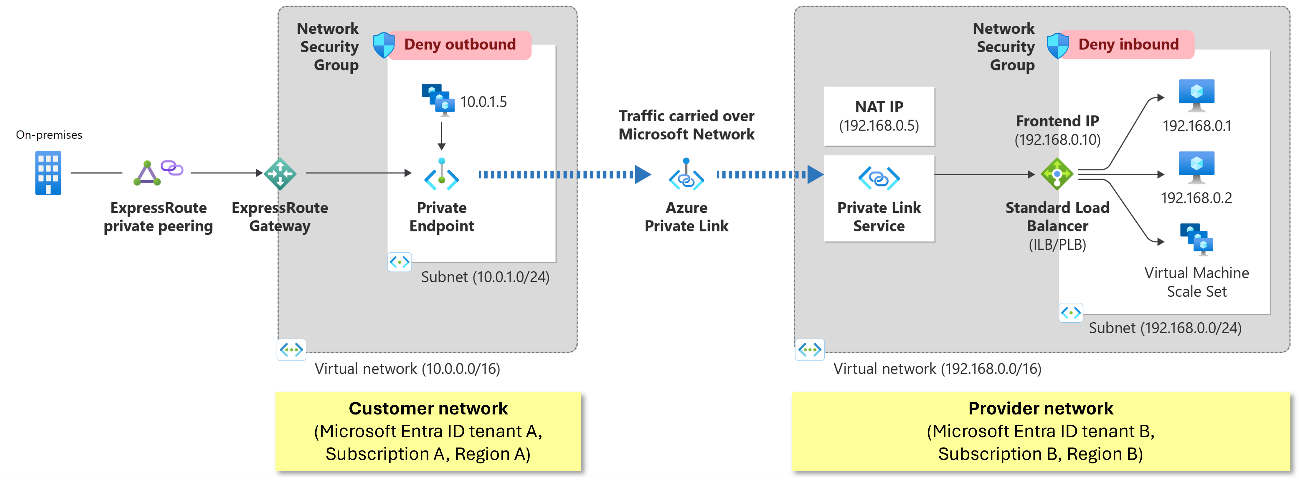
| **Limitación** | **Descripción** |
| --- | --- |
| SNAT siempre se recomienda. | Debido a la naturaleza variable del plano de datos del punto de conexión privado, se recomienda usar el tráfico SNAT que esté destinado a un punto de conexión privado para asegurarse de que se respeta el tráfico devuelto. |
| Característica no disponible en determinadas regiones. | Actualmente no está disponible en las siguientes regiones: Oeste de la India Centro de Australia 2 Oeste de Sudáfrica Sudeste de Brasil |

**Grupo de seguridad de aplicaciones**

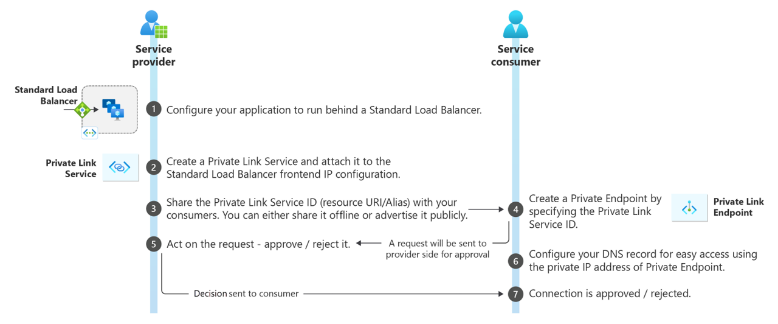
| **Limitación** | **Descripción** |
| --- | --- |
| Característica no disponible en determinadas regiones. | Actualmente no está disponible en las siguientes regiones: Oeste de la India Centro de Australia 2 Oeste de Sudáfrica Sudeste de Brasil |

**Planeamiento e implementación de servicios de Private Link**

El servicio Azure Private Link es la referencia a su propio servicio que usa la tecnología de Azure Private Link. El servicio que se ejecuta de forma subyacente a Azure Standard Load Balancer se puede habilitar para el acceso a Private Link de modo que los consumidores del servicio puedan tener acceso a este de forma privada desde sus propias redes virtuales. Sus clientes pueden crear un punto de conexión privado dentro de su red virtual y asignarlo a este servicio. En este ejemplo se explican los conceptos relacionados con el lado del proveedor de servicios.



**Flujo de trabajo**



**Creación de su servicio Private Link**

Configure su aplicación para ejecutarla de forma subyacente a una instancia de Standard Load Balancer en su red virtual. Si ya tiene su aplicación configurada de forma subyacente a una instancia de Standard Load Balancer, puede omitir este paso.

Cree un servicio Private Link que haga referencia al equilibrador de carga anterior. En el proceso de selección del equilibrador de carga, elija la configuración de IP de front-end donde desea recibir el tráfico. Elija una subred para las direcciones IP de NAT del servicio Private Link. Se recomienda tener al menos ocho direcciones IP de NAT disponibles en la subred. Todo el tráfico de consumidor parecerá originarse en este grupo de direcciones IP privadas del proveedor de servicios. Elija las propiedades o la configuración adecuadas para el servicio Private Link.

**Uso compartido del servicio**

Una vez creado un servicio Private Link, Azure generará un moniker con nombre único global llamado alias basado en el nombre que proporcione para el servicio. Puede compartir el alias o el URI del recurso del servicio con sus clientes sin conexión. Los consumidores pueden iniciar una conexión de Private Link mediante el alias o el URI del recurso.

**Administración de sus solicitudes de conexión**

Después de que un consumidor inicie una conexión, el proveedor de servicios puede aceptar o rechazar la solicitud de conexión. Todas las solicitudes de conexión se mostrarán en la propiedad privateendpointconnections del servicio Private Link.

**Eliminación del servicio**

Si ya no se usa el servicio Private Link, puede eliminarlo. Pero, antes de eliminarlo, asegúrese de que no haya ninguna conexión de punto de conexión privado asociada a él. Puede rechazar todas las conexiones y eliminar el servicio.

**Propiedades**

Un servicio Private Link especifica las siguientes propiedades:

| **Propiedad** | **Explicación** |
| --- | --- |
| Estado de aprovisionamiento (provisioningState) | Una propiedad de solo lectura que muestra el estado de aprovisionamiento actual del servicio Private Link. Los estados de aprovisionamiento aplicables son: Eliminando, Error,Correcto,\* Actualizando. Si el estado de aprovisionamiento es Correcto, ha aprovisionado correctamente su servicio Private Link. |
| Alias (alias) | Alias es una cadena de solo lectura única global para su servicio. Le ayuda a enmascarar los datos del cliente para su servicio y, al mismo tiempo, crea un nombre fácil de compartir para este. Al crear un servicio Private Link, Azure genera el alias para su servicio, el cual puede compartir con sus clientes. Sus clientes pueden usar este alias para solicitar una conexión a su servicio. |
| Visibilidad (visibility) | Visibilidad es la propiedad que controla la configuración de exposición para su servicio Private Link. Los proveedores de servicios pueden elegir limitar la exposición a su servicio a suscripciones con permisos de control de acceso basado en roles de Azure. También se puede usar un conjunto restringido de suscripciones para limitar la exposición. |
| Aprobación automática (autoApproval) | Aprobación automática controla el acceso automatizado al servicio Private Link. Las suscripciones especificadas en la lista de aprobación automática se aprueban automáticamente al solicitarse una conexión desde puntos de conexión privados de esas suscripciones. |
| Configuración de IP de front-end de Load Balancer (loadBalancerFrontendIpConfigurations) | El servicio Private Link está asociado a la dirección IP de front-end de una instancia de Standard Load Balancer. Todo el tráfico destinado al servicio alcanzará el front-end de SLB. Puede configurar las reglas de SLB para dirigir este tráfico a grupos de back-end adecuados donde se ejecutan sus aplicaciones. Las configuraciones de IP de front-end de Load Balancer son distintas de las configuraciones de IP de NAT. |
| Configuración de IP de NAT (ipConfigurations) | Esta propiedad hace referencia a la configuración de IP de NAT (traducción de direcciones de red) para el servicio Private Link. La IP de NAT se puede elegir desde cualquier subred de la red virtual de un proveedor de servicios. El servicio Private Link realiza traducciones de direcciones de red del lado del destino en el tráfico de Private Link. Este NAT garantiza que no haya ningún conflicto de IP entre el espacio de direcciones de origen (lado del consumidor) y destino (proveedor de servicios). En el lado del proveedor de servicios o de destino, la dirección IP NAT se muestra como IP de origen para todos los paquetes recibidos por el servicio. La dirección IP de destino se muestra para todos los paquetes enviados por el servicio. |
| Conexiones de punto de conexión privado (privateEndpointConnections) | Esta propiedad muestra los puntos de conexión privados que se conectan al servicio Private Link. Varios puntos de conexión privados pueden conectarse al mismo servicio Private Link y el proveedor de servicios puede controlar el estado para los puntos de conexión privados individuales. |
| Proxy TCP V2 (EnableProxyProtocol) | Esta propiedad permite al proveedor de servicios utilizar el proxy TCP v2 para recuperar información de conexión sobre el consumidor del servicio. El proveedor de servicios es responsable de preparar las configuraciones del receptor para que este pueda analizar el encabezado del protocolo de proxy v2. |

**Detalles**

Se puede acceder al servicio Private Link desde puntos de conexión privados aprobados en cualquier región pública. Se puede acceder al punto de conexión privado desde la misma red virtual y las redes virtuales emparejadas regionalmente. Se puede alcanzar el punto de conexión privado desde redes virtuales emparejadas a nivel global mediante conexiones VPN o ExpressRoute privadas.

Al crear un servicio Private Link, se crea una interfaz de red para el ciclo de vida del recurso. El cliente no puede administrar esta interfaz.

El servicio Private Link debe implementarse en la misma región que la red virtual y Standard Load Balancer.

Se puede acceder a un solo servicio Private Link desde varios puntos de conexión privados pertenecientes a diferentes redes virtuales, suscripciones o inquilinos de Active Directory. La conexión se establece a través de un flujo de trabajo de conexión.

Pueden crearse varios servicios Private Link en la misma instancia de Standard Load Balancer mediante diferentes configuraciones de IP de front-end. Existen límites en cuanto al número de servicios Private Link que puede crear por Standard Load Balancer y por suscripción. Para más información, consulte el artículo acerca de los límites de Azure.

El servicio Private Link puede tener más de una configuración de IP de NAT vinculada a él. Elegir más de una configuración de IP de NAT puede ayudar a los proveedores de servicios a escalar. Actualmente, los proveedores de servicios pueden asignar hasta ocho direcciones de IP de NAT por servicio Private Link. Con cada dirección IP de NAT, puede asignar más puertos para sus conexiones TCP y, por tanto, escalar horizontalmente. Tras agregar varias direcciones IP de NAT a un servicio Private Link, no puede eliminar las direcciones IP de NAT. Esta restricción se establece para garantizar que las conexiones activas no se vean afectadas durante la eliminación de las direcciones IP de NAT.

**Alias**

Alias es un nombre único global para el servicio. Le ayuda a enmascarar los datos del cliente para su servicio y, al mismo tiempo, crea un nombre fácil de compartir para este. Al crear un servicio Private Link, Azure genera un alias para su servicio, el cual puede compartir con sus clientes. Sus clientes pueden usar este alias para solicitar una conexión a su servicio.

El alias consta de tres partes: *Prefix.GUID.Suffix*

* Prefix es el nombre del servicio. Puede elegir su propio prefijo. Tras crear "**Alias**", no puede cambiarlo, de modo que seleccione su prefijo adecuadamente.
* La plataforma proporcionará GUID. Este GUID (identificador único global) hace que el nombre sea único globalmente.
* Azure anexa Suffix: *region*.azure.privatelinkservice
* Alias completo: *Prefix. {GUID}.region*.azure.privatelinkservice

**Exposición del servicio de control**

El servicio Private Link le proporciona tres opciones en el valor Visibilidad para controlar la exposición del servicio. La configuración de visibilidad determina si un consumidor se puede conectar al servicio. Estas son las opciones de configuración de visibilidad, desde las más restrictivas a las menos restrictivas:

* **Solo control de acceso basado en rol**: si el servicio es para consumo privado desde diferentes redes virtuales de su propiedad, use control de acceso dentro de las suscripciones que están asociadas al mismo inquilino de Active Directory. La visibilidad entre inquilinos se permite mediante el control de acceso basado en rol.
* **Restringido por suscripción**: si el servicio se consumirá en distintos inquilinos, puede restringir la exposición a un conjunto limitado de suscripciones en las que confíe. Las autorizaciones se pueden aprobar previamente.
* **Cualquier usuario con su alias**: si quiere que el servicio sea público y permitir que cualquier usuario con su alias de servicio Private Link solicite una conexión, seleccione esta opción.

**Acceso al servicio de control**

Los consumidores con exposición controlada por la configuración de visibilidad a su servicio Private Link pueden crear un punto de conexión privado en sus redes virtuales y solicitar una conexión a su servicio Private Link. La conexión de punto de conexión privado se crearán en un estado **Pendiente** del objeto de servicio Private Link. El proveedor de servicios es responsable de actuar en la solicitud de conexión. Puede aprobar la conexión, rechazarla o eliminarla. Solo las conexiones que se aprueban pueden enviar tráfico al servicio Private Link.

La acción de aprobar las conexiones se puede automatizar mediante la propiedad de aprobación automática del servicio Private Link. La aprobación automática es la capacidad de los proveedores de servicios de aprobar de forma previa un conjunto de suscripciones para el acceso automatizado a su servicio. Los clientes tendrán que compartir sus suscripciones sin conexión para que los proveedores de servicios se agreguen a la lista de aprobación automática. La aprobación automática es un subconjunto de la matriz de visibilidad.

La visibilidad controla la configuración de exposición, mientras que la aprobación automática controla la configuración de aprobación para su servicio. Si un cliente solicita una conexión desde una suscripción en la lista de aprobación automática, la conexión se aprobará automáticamente y se establecerá. No es necesario que los proveedores de servicios aprueben manualmente la solicitud. Si un cliente solicita una conexión desde una suscripción en la matriz de visibilidad y no en la de aprobación automática, el proveedor de servicios recibirá la solicitud. El proveedor de servicios debe aprobar manualmente las conexiones.

**Cómo obtener información de conexión mediante el proxy TCP V2**

En el servicio de hipervínculo privado, la dirección IP de origen de los paquetes procedentes de un punto de conexión privado es traducida a dirección de red (NAT) en el lado del proveedor de servicios mediante la dirección IP NAT asignada desde la red virtual del proveedor. Las aplicaciones reciben la dirección IP NAT asignada en lugar de la dirección IP de origen real de los consumidores del servicio. Si la aplicación necesita una dirección IP de origen real del lado del consumidor, se puede habilitar el protocolo de proxy en el servicio y recuperar la información a partir del encabezado del protocolo de proxy. Además de la dirección IP de origen, el encabezado del protocolo de proxy también incluye el LinkID del punto de conexión privado. Combinar la dirección IP de origen con el LinkID puede ayudar a los proveedores de servicios a identificar de forma única a sus consumidores.

Esta información se codifica mediante un vector tipo-longitud-valor (TLV) personalizado como se indica a continuación:

Detalles personalizados de longitud y valor de tipo:

| **Campo** | **Longitud (octetos)** | **Descripción** |
| --- | --- | --- |
| Tipo | 1 | PP2\_TYPE\_AZURE (0xEE) |
| Length | 2 | Longitud del valor |
| Value | 1 | PP2\_SUBTYPE\_AZURE\_PRIVATEENDPOINT\_LINKID (0x01) |
|  | 4 | UINT32 (4 bytes) que representan el LINKID del punto de conexión privado. Codificado en formato little endian. |

**Nota**

El proveedor de servicios es responsable de asegurarse de que el servicio que está detrás del equilibrador de carga estándar está configurado para analizar el encabezado del protocolo de proxy según la especificación cuando el protocolo de proxy está habilitado en el servicio de vínculo privado. Se producirá un error en la solicitud si la configuración del protocolo de proxy está habilitada en el servicio de vínculo privado pero el servicio del proveedor de servicios no está configurado para analizar el encabezado. Se producirá un error en la solicitud si el servicio del proveedor de servicios espera un encabezado de protocolo de proxy mientras la configuración no está habilitada en el servicio de vínculo privado. Una vez habilitada la configuración del protocolo de proxy, el encabezado del protocolo de proxy también se incluirá en los sondeos de estado HTTP/TCP desde el host hasta las máquinas virtuales de back-end. La información del cliente no está incluida en el encabezado.

El valor correspondiente de LINKID que forma parte del protocolo PROXYv2 (TLV) se puede encontrar en PrivateEndpointConnection como propiedad linkIdentifier.

**Limitaciones**

A continuación se muestran las limitaciones conocidas al usar el servicio Private Link:

* Solo se admite en Standard Load Balancer. No se admite en la instancia básica de Load Balancer.
* Solo se admite en Standard Load Balancer donde el grupo de back-end se configura mediante NIC. No se admite en Standard Load Balancer donde la dirección IP configura el grupo de back-end.
* Solo admite el tráfico IPv4
* Solo admite el tráfico TCP y UDP
* El servicio Private Link tiene un tiempo de espera de inactividad de unos 5 minutos (300 segundos). Para evitar alcanzar este límite, las aplicaciones que se conectan a través del servicio Private Link deben usar Keepalives TCP con un valor inferior a ese tiempo.

**Planeamiento e implementación de la integración de red de Azure App Service y Azure Functions**

Con Azure Virtual Network, puede colocar cualquier recurso de Azure en una red que se pueda enrutar distinta de Internet. La característica de integración de red virtual de App Service permite a las aplicaciones acceder a los recursos de una red virtual o mediante esta.

App Service tiene dos variantes:

* Los planes de tarifa de proceso dedicados, que incluyen los niveles Básico, Estándar, Premium, Premium v2 y Premium v3.
* App Service Environment que se implementa directamente en la red virtual con una infraestructura de soporte técnico dedicada y usa los planes de tarifa Aislado y Aislado v2.

La característica de integración en red virtual se usa en planes de tarifa de proceso dedicado de Azure App Service. Si la aplicación está en una instancia de App Service Environment, ya está integrada con una red virtual y no le exige que configure la característica de integración de red virtual para acceder a recursos de la misma red virtual.

Integración con red virtual proporciona a la aplicación acceso a los recursos de la red virtual, pero no concede acceso privado de entrada a la aplicación desde esa red virtual. El acceso privado a sitios se refiere a que solo se puede acceder a la aplicación desde una red privada; por ejemplo, desde dentro de una red virtual de Azure. Integración de Virtual Network solo se usa para realizar llamadas salientes de la aplicación a la red virtual.

La característica de integración de red virtual:

* Necesita un plan de precios Básico o Estándar admitido, Premium, Premium v2, Premium v3 o Elástico Premium de App Service.
* Es compatible con TCP y UDP.
* Funciona con aplicaciones de App Service, de funciones y lógicas.

Hay algunos aspectos que la integración de red virtual no admite, como:

* Montar una unidad.
* Unión al dominio de Windows Server Active Directory.
* NetBIOS.

La integración de red virtual admite la conexión a una red virtual en la misma región. El uso de la integración de red virtual habilita a la aplicación para acceder a:

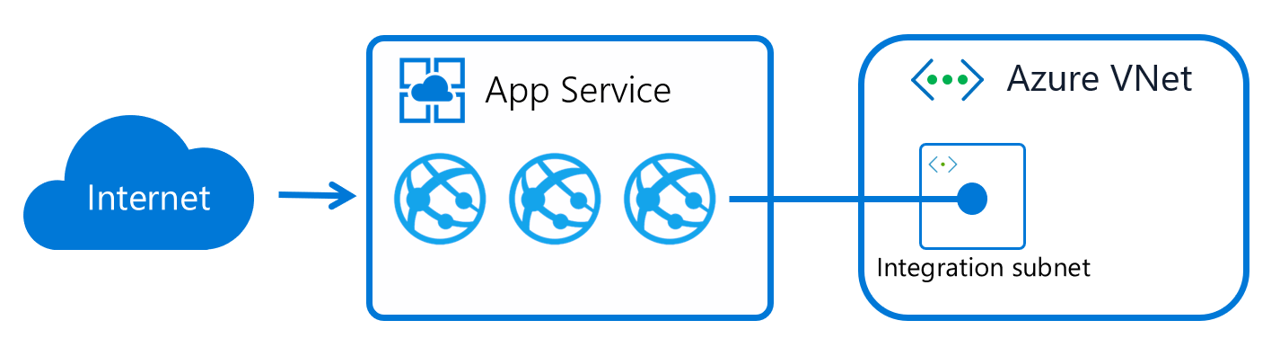
* Recursos de la red virtual con la que está conectado.
* Los recursos de las redes virtuales emparejadas con la red virtual con la que se integra la aplicación incluyen conexiones de emparejamiento global.
* Recursos de diferentes conexiones de Azure ExpressRoute.
* Servicios protegidos mediante puntos de conexión de servicio
* Servicios habilitados para puntos de conexión privados

Cuando usa la integración de red virtual, puede utilizar las siguientes características de redes de Azure:

* Grupos de seguridad de red (NSG) : el tráfico saliente se puede bloquear con un grupo de seguridad de red que se encuentre en la subred de integración. Las reglas de entrada no se aplican, ya que la integración de red virtual no se puede usar para proporcionar acceso de entrada a la aplicación.
* Tablas de enrutamiento (UDR) : puede colocar una tabla de enrutamiento en la subred de integración para enviar el tráfico de salida donde quiera.
* Puerta de enlace NAT: Puede usar la puerta de enlace NAT para obtener una dirección IP de salida dedicada y mitigar el agotamiento de puertos SNAT.

**Cómo funciona la integración de red virtual**

Las aplicaciones en App Service se hospedan en roles de trabajo. La integración de red virtual funciona montando interfaces virtuales en los roles de trabajo con las direcciones de la subred delegada. Las interfaces virtuales utilizadas no son recursos a los que los clientes tengan acceso directo. Dado que la dirección de origen se encuentra en la red virtual, puede tener acceso a la mayoría de elementos en la red virtual o a través de ella, como haría una máquina virtual en la red virtual.



Cuando la integración de red virtual está habilitada, la aplicación realiza llamadas salientes a través de la red virtual. Las direcciones salientes que se muestran en el portal de propiedades de la aplicación siguen siendo las direcciones usadas por la aplicación. Pero si la llamada saliente es a una máquina virtual o un punto de conexión privado en la red virtual de integración o en la red virtual emparejada, la dirección saliente es una dirección de la subred de integración. La dirección IP privada asignada a la instancia se expone por medio de la variable de entorno, WEBSITE\_PRIVATE\_IP.

Si todo el enrutamiento de tráfico está habilitado, todo el tráfico saliente se envía a la red virtual. Si no está habilitado todo el enrutamiento del tráfico, solo se envía a la red virtual el tráfico privado (RFC1918) y los puntos de conexión de servicio configurados en la subred de integración. El tráfico saliente a Internet se enruta directamente desde la aplicación.

Para los planes de Windows App Service, la característica de integración de red virtual es compatible con dos interfaces virtuales por trabajo. Dos interfaces virtuales por trabajo quiere decir dos integraciones de redes virtuales por plan de App Service. Es decir, un plan de Windows App Service puede tener integraciones de red virtual con hasta dos subredes o redes virtuales. Las aplicaciones del mismo plan de App Service solo pueden usar una de las integraciones de red virtual en una subred específica, lo que significa que una aplicación solo puede tener una integración de red virtual en un momento dado. Los planes de App Service de Linux solo admiten una integración de red virtual por plan.

**Requisitos de subred**

La integración de red virtual depende de una subred dedicada. Al crear una subred, la subred de Azure consume cinco direcciones IP desde el inicio. Se usa una dirección de la subred de integración para cada instancia del plan de App Service. Si escala la aplicación a cuatro instancias, se usan cuatro direcciones.

Al escalar o reducir verticalmente el número de instancias, el espacio de direcciones necesario se duplica durante un breve período de tiempo. La operación de escalado agrega el mismo número de nuevas instancias y, después, elimina las instancias existentes. La operación de escalada afecta a las instancias admitidas reales y disponibles para un tamaño de subred determinado. Las actualizaciones de la plataforma necesitan direcciones IP gratuitas para asegurarse de que las actualizaciones pueden producirse sin interrupciones en el tráfico saliente. Por último, después de escalar verticalmente, reducir verticalmente o reducir verticalmente las operaciones, puede haber un breve período de tiempo antes de que se libere la dirección IP.

Como el tamaño de la subred no se puede cambiar después de la asignación, use una subred lo suficientemente grande como para dar cabida a cualquier escala que pueda alcanzar la aplicación. También debe reservar direcciones IP para las actualizaciones de la plataforma. Para evitar problemas con la capacidad de la subred, debe usar /26 con 64 direcciones. Cuando crea subredes en Azure Portal como parte de la integración con la red virtual, se requiere un tamaño mínimo de /27. Si la subred ya existe antes de realizar la integración a través del portal, puede usar una subred /28.

**Nota**

Los contenedores de Windows usan una dirección IP adicional por aplicación para cada instancia de plan de App Service; debe ajustar el tamaño de la subred según corresponda. Si tiene, por ejemplo, 10 instancias de planes de App Service con contenedores de Windows con 4 aplicaciones en ejecución, necesitará 50 direcciones IP, y direcciones adicionales para admitir el escalado horizontal (entrada o salida).

Cálculo de ejemplo:

Para cada instancia de plan de App Service, necesita:

* 4 aplicaciones de contenedor Windows = 4 direcciones IP
* 1 dirección IP por instancia de plan de App Service
* 4 + 1 = 5 direcciones IP

Para 10 instancias:

* 5 x 10 = 50 direcciones IP por plan de App Service

Puesto que tiene 1 plane de App Service, 1 x 50 = 50 direcciones IP.

Si quiere que las aplicaciones de otro plan se comuniquen con una red virtual a la que ya están conectadas aplicaciones de otro plan, seleccione una subred distinta a la usada por la característica de integración de red virtual ya existente.

**Permisos**

Debe tener al menos los siguientes permisos de control de acceso basado en roles en la subred o en un nivel superior para configurar la integración de red virtual a través de Azure Portal, la CLI o al establecer la propiedad virtualNetworkSubnetId del sitio directamente:

| **Acción** | **Descripción** |
| --- | --- |
| Microsoft.Network/virtualNetworks/read | Leer la definición de red virtual. |
| Microsoft.Network/virtualNetworks/subnets/read | Leer una definición de subred de red virtual. |
| Microsoft.Network/virtualNetworks/subnets/join/action | Se une a una red virtual |

**Rutas**

Puede controlar qué tráfico pasa a través de la integración de red virtual. Hay tres tipos de enrutamiento que se deben tener en cuenta al configurar la integración de red virtual. El enrutamiento de aplicaciones define qué tráfico se enruta desde la aplicación y hacia la red virtual. El enrutamiento de configuración afecta las operaciones que ocurren antes o durante el inicio de su aplicación. Algunos ejemplos son la extracción de imágenes de contenedor y la configuración de la aplicación con la referencia de Key Vault. El enrutamiento de red es la capacidad de controlar cómo se enrutan tanto el tráfico de aplicaciones como el de configuración desde su red virtual y hacia afuera.

Mediante las opciones de enrutamiento de aplicaciones o enrutamiento de configuraciones, puede configurar el tráfico que se envía mediante la integración de la red virtual. El tráfico solo está sujeto al enrutamiento de red si se envía a través de la integración de red virtual.

**Enrutamiento de aplicaciones**

El enrutamiento de aplicaciones se aplica al tráfico que se envía desde la aplicación después de que se haya iniciado. Consulte enrutamiento de configuración para el tráfico durante el startup. Al configurar el enrutamiento de aplicaciones, puede enrutar todo el tráfico o solo el tráfico privado (también conocido como tráfico RFC1918) a su red virtual. Este comportamiento se configura mediante el valor de tráfico saliente de Internet. Si el enrutamiento de tráfico saliente de Internet está deshabilitado, la aplicación solo enruta el tráfico privado a la red virtual. Si quiere enrutar todo el tráfico de la aplicación saliente a la red virtual, asegúrese de que el tráfico saliente de Internet esté habilitado.

Solo el tráfico configurado en el enrutamiento de aplicaciones o de la configuración está sujeto a los NSG y UDR que se aplican a la subred de integración.

Cuando se habilita el enrutamiento del tráfico saliente de Internet, la dirección de origen del tráfico saliente de la aplicación sigue siendo una de las direcciones IP que se enumeran en las propiedades de la aplicación. Si enruta el tráfico a través de un firewall o de una puerta de enlace NAT, la dirección IP de origen se origina en este servicio.

**Nota**

La conectividad SMTP saliente (puerto 25) es compatible con App Service cuando el tráfico SMTP se enruta mediante la integración de red virtual. La compatibilidad viene determinada por una configuración en la suscripción donde se implementa la red virtual. Para redes virtuales o subredes que se hayan creado antes de la 1. En agosto de 2022 debe iniciar un cambio de configuración temporal en la red virtual o subred para que la configuración se sincronice desde la suscripción. Un ejemplo sería agregar una subred temporal, asociar o desasociar temporalmente un grupo de seguridad de red o configurar un punto de conexión de servicio temporalmente. Para obtener más información, consulte Solución de problemas de conectividad SMTP salientes en Azure

**Enrutamiento de la configuración**

Cuando use la integración de red virtual, puede configurar cómo se administran las diferentes partes del tráfico de configuración. De forma predeterminada, el tráfico de configuración pasa directamente a través de la ruta pública, pero para los componentes individuales mencionados, puede configurarlo activamente para que se enruta a través de la integración de red virtual.

**Recurso compartido de contenido**

Traer su propio almacenamiento para el contenido se usa a menudo en las funciones, donde el recurso compartido de contenido se configura como parte de la aplicación de funciones.

Para enrutar el tráfico de recursos compartidos de contenido a través de la integración de redes virtuales, debe asegurarse de que la configuración de enrutamiento está definida.

Además de configurar el enrutamiento, también debe asegurarse de que cualquier firewall o grupo de seguridad de red configurado en el tráfico desde la subred permite que llegue tráfico a los puertos 443 y 445.

**Extracción de una imagen de contenedor**

Si se usan contenedores personalizados, se puede extraer el contenedor a través de la integración de red virtual. Para enrutar el tráfico de extracción de contenedores a través de la integración de redes virtuales, debe asegurarse de que la configuración de enrutamiento está definida.

**Copia de seguridad y restauración**

App Service tiene una copia de seguridad o restauración integrada, pero si quiere realizar una copia de seguridad en una cuenta de almacenamiento propia, puede usar la característica de copia de seguridad y restauración personalizada. Si quiere enrutar el tráfico a la cuenta de almacenamiento mediante la integración de red virtual, debe establecer la configuración de ruta. No se admite la copia de seguridad de la base de datos mediante la integración de la red virtual.

**Configuración de la aplicación mediante referencias de Key Vault**

La configuración de la aplicación mediante referencias de Key Vault intenta obtener secretos a través de la ruta pública. Si la instancia de Key Vault bloquea el tráfico público y la aplicación usa la integración de red virtual, se intenta obtener los secretos mediante la integración de red virtual.

* Actualmente no se admite la configuración de certificados SSL/TLS desde almacenes de claves privados
* Actualmente no se admiten los registros de App Service en cuentas de almacenamiento privadas. Se recomienda usar registro de diagnóstico y permitir servicios de confianza para la cuenta de almacenamiento.

**Enrutamiento de red**

Las tablas de rutas se pueden usar para enrutar el tráfico saliente de la aplicación sin restricciones. Los destinos más habituales suelen ser puertas de enlace o dispositivos de firewall. También puede usar un grupo de seguridad de red (NSG) para bloquear el tráfico saliente a los recursos de la red virtual o Internet. Un grupo de seguridad de red que se aplique a la subred de integración está en vigor, con independencia de las tablas de enrutamiento aplicadas a la subred de integración.

Las tablas de rutas y los grupos de seguridad de red solo se aplican al tráfico enrutado a través de la integración de red virtual. Consulte Enrutamiento de aplicaciones y Enrutamiento de la configuración para más información. Las rutas no se aplican a las respuestas que vengan de solicitudes de aplicaciones de entrada y las reglas de entrada en un NSG no tienen efecto en la aplicación. La integración de red virtual solo afecta al tráfico saliente de la aplicación. Para controlar el trafico de entrada a la aplicación, use la característica restricciones de acceso o los puntos de conexión privados.

Al configurar los grupos de seguridad de red o las tablas de rutas que afectan al tráfico saliente, debe asegurarse de tener en cuenta las dependencias de la aplicación. Las dependencias de la aplicación incluyen puntos de conexión que la aplicación necesita durante el tiempo de ejecución. Además de las API y los servicios a los que llama la aplicación, estos puntos de conexión también podrían ser puntos de conexión derivados, como los puntos de conexión de comprobación de la lista de revocación de certificados (CRL) y el punto de conexión de identidad o autenticación, por ejemplo, Microsoft Entra ID. Si usa la implementación continua en App Service, es posible que también deba permitir puntos de conexión en función del tipo y el idioma. Específicamente para la implementación continua de Linux es necesario permitir oryx-cdn.microsoft.io:443. Para Python, también se debe permitir files.pythonhosted.org, pypi.org.

Si quiere enrutar el tráfico saliente del entorno local, puede utilizar una tabla de rutas para enviarlo a la puerta de enlace de ExpressRoute. Si no enruta el tráfico a una puerta de enlace, establezca las rutas en la red externa para poder enviar de vuelta las respuestas. Las rutas del Protocolo de puerta de enlace de borde (BGP) también afectan al tráfico de la aplicación. Si tiene rutas de BGP cuyo origen es algo similar a una puerta de enlace de ExpressRoute, el tráfico de salida de la aplicación se verá afectado. De forma similar a las rutas definidas por el usuario, las rutas BGP afectan al tráfico según la configuración del ámbito de enrutamiento.

**Puntos de conexión del servicio**

La integración de red virtual le permite acceder a los servicios de Azure que están protegidos con puntos de conexión de servicio. Para acceder a un servicio protegido por puntos de conexión de servicio, siga estos pasos:

1. Configure la integración de red virtual con su aplicación web para conectarse a una subred específica para la integración.
2. Vaya al servicio de destino y configure los puntos de conexión de servicio en la subred de integración.

**Puntos de conexión privados**

Si quiere realizar llamadas a puntos de conexión privados, asegúrese de que las búsquedas de DNS se resuelvan en el punto de conexión privado. Puede aplicar este comportamiento de una de las siguientes formas:

* Realizar la integración con zonas privadas de Azure DNS. Si la red virtual no tiene un servidor DNS personalizado, esta integración se lleva a cabo automáticamente cuando las zonas están vinculadas a ella.
* Administrar el punto de conexión privado en el servidor DNS que usa la aplicación. Para administrar la configuración, debe conocer la dirección IP del punto de conexión privado. A continuación, señale el punto de conexión al que está intentando llegar a esa dirección mediante un registro A.
* Configurar su propio servidor DNS para reenviarlo a zonas privadas de Azure DNS.

**Zonas privadas de Azure DNS**

Cuando la aplicación esté integrada con la red virtual, usará el mismo servidor DNS con que está configurada la red virtual. Si no se especifica ningún DNS personalizado, usa el DNS predeterminado de Azure y las zonas privadas vinculadas a la red virtual.

**Limitaciones**

Existen algunas limitaciones cuando se usa la integración de red virtual:

* La característica está disponible en todas las implementaciones de App Service en Premium V2 y Premium V3. También está disponible en los niveles Básico y Estándar, pero solo desde las implementaciones de App Service más recientes. Si está en una implementación anterior, solo puede usar la característica desde un plan de App Service Premium v2. Si quiere asegurarse de que puede usar esta función en un plan Básico o Estándar de App Service, cree su propia aplicación en un plan de App Service Premium V3. Esos planes solo se admiten en las implementaciones más recientes. Si quiere, puede reducir verticalmente después de crear el plan.
* La característica no está disponible para las aplicaciones de plan aislado en una instancia de App Service Environment.
* No puede acceder a los recursos a través de conexiones de emparejamiento con redes virtuales clásicas.
* La característica requiere una subred sin usar que sea un bloque IPv4 /28 o mayor en una red virtual de Azure Resource Manager.
* Tanto la aplicación como la red virtual deben estar en la misma región.
* La red virtual de integración no puede tener espacios de direcciones IPv6 definidos.
* La subred de integración no puede tener habilitadas las directivas de punto de conexión de servicio.
* La subred de integración solo puede usarla un plan de App Service.
* No se pueden eliminar redes virtuales que tengan aplicaciones integradas. Quite la integración antes de eliminar la red virtual.
* No puede tener más de dos integraciones de red virtual por plan de Windows App Service. No puede tener más de una integración de red virtual por plan de App Service de Linux. Varias aplicaciones del mismo plan de App Service pueden usar la misma integración con redes virtuales.
* No se puede cambiar la suscripción de una aplicación o de un plan mientras haya una aplicación que use la integración de red virtual.

**Acceso a recursos locales**

No se requiere ninguna configuración adicional para que la característica de integración de red virtual acceda a través de la red virtual a los recursos locales. Basta con conectar la red virtual a los recursos locales usando ExpressRoute o una VPN de sitio a sitio.

**Emparejamiento**

Si usa el emparejamiento con la integración de red virtual, no es necesario realizar más configuraciones.

**Administración de integración de red virtual**

La conexión y la desconexión con una red virtual tiene lugar en el nivel de la aplicación. Las operaciones que pueden afectar a la integración de red virtual en varias aplicaciones se encuentran en un nivel del plan de App Service. En la aplicación, en **Redes**, **Portal de integración con redes virtuales**, es posible obtener detalles sobre la red virtual. Encontrará información similar en el nivel del plan de App Service en **Plan de App Service**, **Redes**, **Portal de integración de redes virtuales**.

En la vista de la aplicación de la instancia de integración de red virtual, puede desconectar la aplicación de la red virtual y configurar el enrutamiento de aplicaciones. Para desconectar la aplicación de una red virtual, seleccione **Desconectar**. La aplicación se reinicia cuando se desconecte de una red virtual. La desconexión no cambia la red virtual. La subred no se ha quitado. Si después desea eliminar la red virtual, primero debe desconectar la aplicación de la red virtual.

La dirección IP privada asignada a la instancia se expone por medio de la variable de entorno, WEBSITE\_PRIVATE\_IP. La interfaz de usuario de la consola de Kudu también muestra la lista de variables de entorno disponibles para la aplicación web. Esta dirección IP se asigna desde el intervalo de direcciones de la subred integrada. Esta es la dirección IP que usa la aplicación web para conectarse a los recursos a través de la red virtual de Azure.

**Nota**

El valor de WEBSITE\_PRIVATE\_IP va a cambiar. Sin embargo, será una IP del intervalo de direcciones de la subred de integración, por lo que va a tener que permitir el acceso desde el intervalo de direcciones completo.

**Eliminación del plan o de la aplicación de App Service antes de desconectar la integración de red**

Si eliminó la aplicación o el plan de App Service sin desconectar primero la integración de red virtual, no puede realizar ninguna operación de actualización o eliminación en la red virtual o subred que se usó para la integración con el recurso eliminado. Una delegación de subred "Microsoft.Web/serverFarms" permanece asignada a la subred y evita las operaciones de actualización o eliminación.

Para actualizar o eliminar la subred o la red virtual de nuevo, debe volver a crear la integración de red virtual y, después, desconectarla:

1. Vuelva a crear el plan y la aplicación de App Service (es obligatorio usar exactamente el mismo nombre de aplicación web que antes).
2. Vaya a Redes en la aplicación, en Azure Portal, y configure la integración de red virtual.
3. Una vez configurada la integración de red virtual, seleccione el botón "Desconectar".
4. Elimine el plan o la aplicación de App Service.
5. Actualice o elimine la subred o red virtual.

**Planeamiento e implementación de configuraciones de seguridad de red de una instancia de App Service Environment (ASE)**

Recuerde estas consideraciones clave al planear e implementar configuraciones de seguridad de red para un ASE:

**Implementación de la integración de red virtual regional:**

* Use la característica de integración de red virtual para implementar servicios en una instancia privada de Azure Virtual Network (VNet).
* Benefíciese de una dirección IP estable para las comunicaciones salientes con el fin de habilitar la lista de permitidos en función de las direcciones IP.
* Implemente App Service en el plan de tarifa Aislado directamente en una subred dentro de Azure Virtual Network.

**Optimización de los grupos de seguridad de red (NSG):**

* Aproveche la eficacia de los grupos de seguridad de red para administrar el tráfico, el bloqueo y permitir flujos entrantes y salientes según sea necesario.
* Asegúrese de que las reglas de permiso explícitas se agreguen a los grupos de seguridad de red, teniendo en cuenta la regla de denegación implícita predeterminada.

**Mejora de la seguridad con Azure Private Link:**

* Adopte puntos de conexión privados para Azure Web Apps, lo que garantiza que los clientes de la red privada puedan interactuar de forma segura con las aplicaciones a través de Private Link.
* Use puntos de conexión privados para simplificar el tráfico entrante a la aplicación web mientras administra los flujos salientes mediante la característica de integración de red virtual.

**Limitación de la exposición de la red pública:**

* Deshabilite activamente el acceso a la red pública mediante reglas de filtrado de ACL de IP, puntos de conexión privados o mediante la modificación de la propiedad publicNetworkAccess.

**Integración de DDoS Protection:**

* Actualice la red virtual vinculada al firewall de aplicaciones web de App Service con DDoS Protection Estándar, lo que mejora las medidas de seguridad frente a posibles ataques DDoS.

**Implementación y ajuste del firewall de aplicaciones web (WAF):**

* Asegúrese de que el tráfico se enruta a través de una instancia de Azure Application Gateway habilitada para WAF o Azure Front Door.
* Use una combinación de restricciones de acceso, puntos de conexión de servicio y puntos de conexión privados para bloquear el acceso, impidiendo cualquier omisión del WAF.

**Planeamiento e implementación de configuraciones de seguridad de red de una instancia de Azure SQL Managed Instance**

Al planear e implementar configuraciones de seguridad de red para Azure SQL Managed Instance, siga esta línea de base:

**1. Integración de la red virtual:**

* Incorpore SQL Managed Instance a la red virtual privada (VNet) de un cliente y confíe en direcciones IP privadas, evitando direcciones IP públicas a menos que sea necesario.
* Referencia: Uso de reglas y puntos de conexión de servicio de red virtual para servidores de Azure SQL Database.

**2. Aprovechamiento de la compatibilidad con grupos de seguridad de red (NSG):**

* Emplee etiquetas de servicio de Azure Virtual Network para definir controles de acceso en grupos de seguridad de red o Azure Firewall adaptados a los recursos de Azure SQL.
* Para una conectividad sin problemas con Azure SQL Database, especialmente cuando se usan puntos de conexión de servicio, asegúrese de que los NSG están abiertos a direcciones IP de Azure SQL Database.
* Referencia: Uso de reglas y puntos de conexión de servicio de red virtual para servidores de Azure SQL Database.

**3. Implementación de Azure Private Link:**

* Configure puntos de conexión privados para recursos de Azure compatibles con la característica Private Link, que establece un punto de acceso dedicado para estos recursos.
* Referencia: Azure Private Link para Azure SQL Database y Azure Synapse Analytics.

**4. Deshabilitación del acceso directo a la red pública:**

* El acceso a la red pública se admite y se habilita de forma predeterminada, pero para mejorar la seguridad, considere la posibilidad de deshabilitar esta característica.
* Referencia: Configuración de la conectividad de Azure SQL.

**5. Supervisión de Microsoft Defender for Cloud:**

* Habilite Microsoft Defender para supervisar y proteger continuamente Azure SQL Managed Instance.

**6. Siga las recomendaciones de Azure Policy:**

* Deshabilite el acceso a la red pública en Azure SQL Managed Instance para asegurarse de que el acceso solo está dentro de sus redes virtuales o a través de puntos de conexión privados.
* Habilite las conexiones de punto de conexión privado para fortalecer la comunicación segura con Azure SQL Database.
* Desactive la propiedad de acceso a la red pública en Azure SQL Database para aplicar el acceso solo desde un punto de conexión privado.

**Prueba de conocimientos**

Elija la mejor respuesta para cada una de las preguntas. Después, seleccione **Comprobar las respuestas**.

**Comprobación de conocimientos**

Principio del formulario

**1. ¿Cuál es el propósito de Azure App Service?**

1. Proporcionar almacenamiento adicional para máquinas virtuales
2. Habilitar el escalado automático de redes virtuales
3. Hospedar aplicaciones web y móviles

**2. Una empresa quiere enrutar el tráfico de sus contenedores personalizados a través de la integración de red virtual. ¿Qué deben asegurarse de que está configurado además de la configuración de enrutamiento?**

1. La copia de seguridad de la base de datos se admite a través de la integración de red virtual.
2. Un Firewall o grupo de seguridad de red configurado en el tráfico desde la subred permiten el tráfico al puerto 80 y 443.
3. Cualquier firewall o grupo de seguridad de red configurado en el tráfico desde la subred permiten el tráfico al puerto 443 y 445.

**3. Una empresa quiere implementar una aplicación web en Azure. Quieren asegurarse de que la aplicación es de alta disponibilidad y pueden controlar picos repentinos en el tráfico. ¿Cuál de los siguientes servicios de Azure debe usar?**

1. Azure Virtual Machines
2. Azure Functions
3. Azure App Service

**4. Una empresa quiere crear un servicio Private Link en Azure. ¿Cuál es la finalidad de un alias en un servicio Private Link?**

1. Restringir el acceso al servicio a un conjunto limitado de suscripciones de confianza.
2. Restringir el acceso al servicio solo en función del control de acceso basado en roles.
3. Proporcionar un nombre único global para el servicio que se puede compartir con los clientes y usar a fin de solicitar una conexión al servicio.

**5. Una empresa quiere conectarse de forma segura a un servicio de Azure mediante una dirección IP privada. ¿Cuál de las siguientes opciones debería usar?**

1. Interfaz de red virtual
2. Punto de conexión público
3. Punto de conexión privado
4. C
5. C
6. C
7. C
8. C

Final del formulario

**Resumen**

En este módulo, aprendió a planear e implementar una estrategia de seguridad sólida para el acceso privado a los recursos de Azure, incluyendo el uso de puntos de conexión de servicio de red virtual, puntos de conexión privados, servicios de Private Link, la integración de red para Azure App Service y Azure Functions, así como configuraciones de seguridad de red para entornos de App Service Environment (ASE) e instancias de Azure SQL Managed Instance para proteger datos confidenciales y recursos.