**Introducción**

**Escenario**

Azure DNS es un servicio de hospedaje que permite administrar dominios DNS mediante la infraestructura de Microsoft Azure.

Supongamos que su empresa obtiene un nombre de dominio personalizado para un nuevo sitio web. Usted necesita usar Azure DNS para administrar este dominio.

El objetivo de este módulo es proporcionar información sobre cómo usar Azure DNS.

**Aptitudes evaluadas**

La configuración de Azure DNS forma parte del [examen AZ-104: Administrador de Microsoft Azure](https://learn.microsoft.com/es-es/learn/certifications/exams/az-104).

**Objetivos de aprendizaje**

En este módulo aprenderá a:

* Identificar las características y los casos de uso de dominios, dominios personalizados y zonas privadas
* Comprobar nombres de dominio personalizados mediante registros DNS
* Implementar zonas DNS, la delegación DNS y conjuntos de registros de DNS

**Requisitos previos**

* Familiaridad con DNS, incluidos los conjuntos de registros, la delegación y las zonas.

**Identificación de dominios y dominios personalizados**

Azure DNS permite hospedar los dominios DNS en Azure y acceder a la resolución de nombres de los dominios mediante la infraestructura de Microsoft Azure. Puede configurar y administrar los dominios personalizados con Azure DNS en Azure Portal. Al acceder a los dominios en Azure, puede usar sus mismas credenciales, contratos de soporte técnico y preferencias de facturación que con los demás servicios de Azure.

Antes de empezar a usar Azure DNS para hospedar registros DNS de los dominios, hay algunos conceptos importantes que se deben revisar.

**Aspectos que saber sobre los nombres de dominio en Azure**

Vamos a analizar cómo se implementa un *nombre de dominio inicial* y *nombres de dominio personalizados* en Azure.

* Al crear una suscripción de Azure, Azure crea automáticamente un dominio de Microsoft Entra para su suscripción.

**Nota**

Debe ser un administrador global para realizar tareas de administración de dominios. El administrador global es el usuario que creó la suscripción.

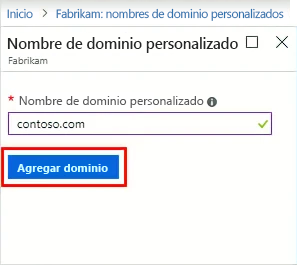
* Azure emplea un **nombre de dominio inicial** en la instancia de dominio inicial.

El nombre de dominio inicial sigue el formato <Your Domain Name>, seguido de .onmicrosoft.com. Por ejemplo, yourdomainname.onmicrosoft.com.

* El propósito de un nombre de **dominio personalizado** es proporcionar una forma simplificada del nombre de dominio para dar cabida a usuarios o tareas específicos.

Las organizaciones suelen implementar nombres de dominio personalizados para permitir que los usuarios accedan a su dominio mediante credenciales con las que están familiarizados.

Considere el dominio de Microsoft Entra incorporado al administrador de Azure. Azure crea el nombre de dominio inicial para la instancia de Microsoft Entra como azureadminincorg.onmicrosoft.com. Un nombre de dominio personalizado de la instancia podría ser azureadmininc.org.



* El nombre de dominio inicial está pensado para usarse hasta que el nombre de dominio personalizado se *verifique*.
* Para que Microsoft Entra ID pueda usar un nombre de dominio personalizado, dicho nombre debe agregarse al directorio y comprobarse.
* El nombre de dominio inicial no se puede cambiar ni eliminar, pero sí se puede agregar un nombre de dominio personalizado enrutable que se pueda controlar.
* En Microsoft Entra ID, los **nombres de dominio deben ser únicos globalmente**. Cuando un directorio de Microsoft Entra ha verificado un nombre de dominio específico, el resto de Microsoft Entra no podrá usar ese nombre.

**Comprobación de nombres de dominio personalizados**

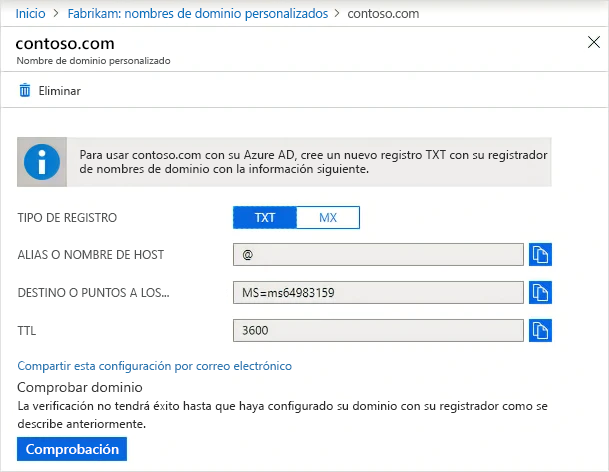
Cuando un administrador agrega un nombre de dominio personalizado a una instancia de Microsoft Entra, el nombre de dominio personalizado inicialmente se encuentra en un estado *no comprobado*. Microsoft Entra ID no permitirá que ningún recurso de directorio use un nombre de dominio personalizado sin comprobar.

Para poder usar un nombre de dominio personalizado para la instancia de Microsoft Entra, se debe *comprobar* el nombre de dominio personalizado.

**Comprobación del nombre de dominio personalizado**

Después de agregar un nombre de dominio personalizado para la instancia de Microsoft Entra en Azure Portal, debe comprobar la titularidad del nombre de dominio personalizado.

Para iniciar el proceso de comprobación, agregue un **registro DNS** para el nombre de dominio personalizado. El tipo de registro DNS puede ser MX o TXT, como se muestra en la imagen siguiente:



El registro MX (o *Intercambio de correo*) enumera los servidores de intercambio de correo que aceptan correo electrónico para su dominio. El registro TXT (o *Texto*) indica texto legible o datos legibles por máquina sobre el dominio. Estos tipos de registro se definen en [RFC 1035](https://datatracker.ietf.org/doc/html/rfc1035#page-12).

Después de agregar un registro DNS al nombre de dominio personalizado, Azure consulta el dominio DNS para comprobar que el registro DNS está presente.

**Nota**

El proceso de comprobación de Azure puede tardar varios minutos o horas.

Después de que Azure compruebe la presencia del registro DNS para el nombre de dominio personalizado, Azure agrega el nuevo nombre de dominio personalizado a la suscripción para la instancia de Microsoft Entra.

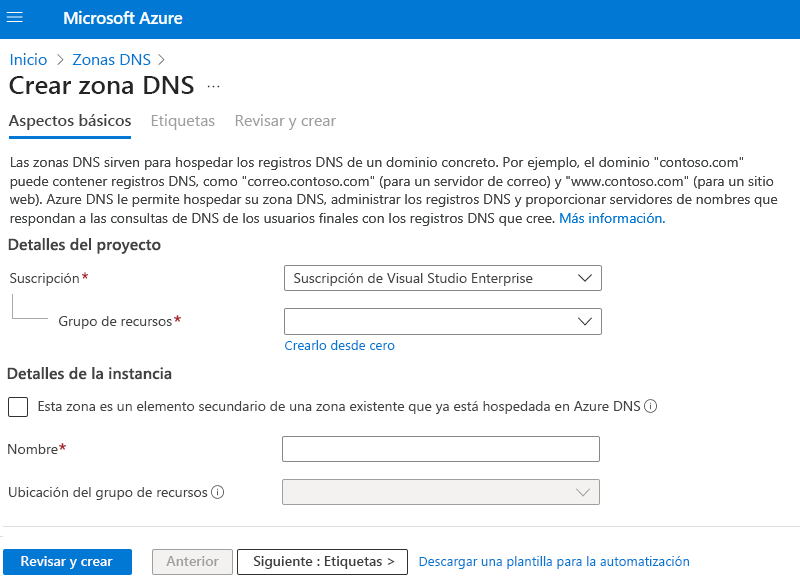
**Creación de zonas de Azure DNS**

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.

Una **zona DNS** de Azure hospeda los registros DNS de un dominio. Para iniciar el hospedaje de su dominio en Azure DNS, debe crear una zona DNS para ese nombre de dominio. Cada registro DNS del dominio se crea luego en esta zona DNS.

**Aspectos que saber sobre las zonas DNS**

Una zona DNS se puede agregar en Azure Portal, como se muestra en la siguiente imagen. Para crear una zona DNS se necesitan varias opciones de configuración. En el portal, especifique el nombre de la zona DNS, el número de registros, el grupo de recursos, la ubicación de la zona, la suscripción asociada y los servidores de nombres DNS.



Dedique un momento a revisar algunas características importantes sobre las zonas DNS.

* El nombre de una zona DNS debe ser único dentro de un grupo de recursos.

Al proporcionar un nombre único en la creación de una zona DNS, Azure garantiza que la zona DNS aún no existe en el grupo de recursos.

* Puede haber varias zonas DNS con el mismo nombre, pero deben estar en grupos de recursos diferentes o en suscripciones de Azure distintas.
* Cuando varias zonas DNS comparten el mismo nombre, cada instancia de zona DNS se asigna a una dirección de servidor de nombres DNS diferente.
* El dominio raíz o principal se registra en el registrador y luego apunta a Azure DNS.
* Los dominios secundarios se registran directamente en Azure DNS.

**Sugerencia**

No tiene que poseer un nombre de dominio para crear una zona DNS con dicho nombre de dominio en Azure DNS. Aun así, debe ser el propietario del dominio para configurarlo.

**Delegación de dominios DNS**

Para delegar su dominio a Azure DNS, debe identificar los servidores DNS de la zona DNS. Cada vez que se crea una zona DNS, Azure DNS asigna servidores DNS de un grupo. Una vez asignados los servidores DNS, Azure DNS crea automáticamente registros autoritativos NS (o *servidor de nombres*) en la zona DNS.

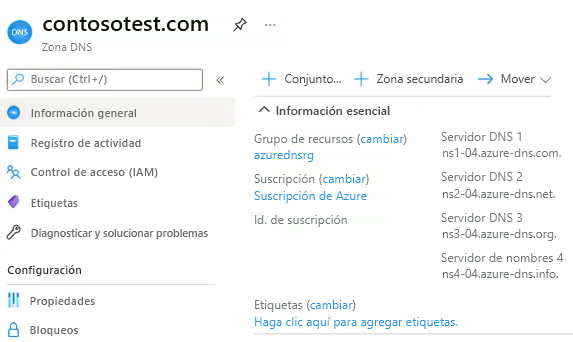
El proceso de delegación del dominio conlleva varios pasos:

1. Identificar los servidores DNS
2. Actualizar el dominio primario
3. Delegar los subdominios (opcional)

**Cómo localizar los servidores DNS**

La manera más fácil de localizar los servidores DNS asignados a su zona DNS es mediante Azure Portal.

Echemos un vistazo a nuestro ejemplo de dominio de Microsoft Entra incorporado al administrador de Azure. En una unidad anterior, definimos un nombre de dominio personalizado para la instancia de ejemplo como azureadmininc.org. En Azure Portal, podemos examinar el dominio personalizado y ver que Azure asignó cuatro servidores DNS a la zona DNS para el dominio: ns1-02.azure-dns.com., ns2-02.azure-dns.net., ns3-02.azure-dns.org. y ns4-02.azure-dns.info..



**Cómo actualizar el dominio primario**

Una vez que la zona DNS se ha creado y los servidores DNS se pueden identificar, debe actualizar el dominio principal.

Cada registrador dispone de sus propias herramientas de administración de DNS para administrar los registros de servidores DNS de un dominio. El término *registrador* hace referencia a un registrador de dominios de terceros, que es la empresa donde registró su dominio.

El siguiente es un proceso básico que se puede seguir para actualizar la información del dominio primario con el registrador:

1. Vaya a la página de administración de DNS del registrador.
2. Localice los registros NS existentes de su dominio primario
3. Reemplace los registros NS existentes por los registros NS que Azure DNS ha creado para el dominio.

**Aspectos que tener en cuenta al trabajar con registros NS**

Hay varias consideraciones importantes que se deben tener en cuenta al trabajar con los registros NS y los servidores DNS de una zona DNS.

* Al copiar un registro NS (una dirección de servidor DNS), asegúrese de incluir el punto final (.) de la dirección. Este punto final indica el final de un nombre de dominio completo, como ns1-02.azure-dns.com. y ns3-02.azure-dns.org..
* Para delegar el dominio a Azure DNS, debe usar los nombres exactos de los servidores DNS creados por Azure DNS.
* Se recomienda copiar siempre **todos** los registros NS de servidor DNS del dominio en el dominio primario, independientemente del nombre de dominio real. En nuestro escenario de ejemplo, supongamos que no esperamos tráfico en el servidor DNS ns4-02.azure-dns.info.. Aunque no esperamos tráfico en esta dirección de servidor DNS, el procedimiento recomendado es copiar también este registro NS en el dominio primario con el registrador, junto con las demás direcciones del servidor DNS.

**Cómo delegar subdominios**

Para delegar un subdominio del dominio en Azure DNS, configure una zona DNS secundaria independiente.

Vamos a considerar nuestro ejemplo de dominio de Microsoft Entra incorporado al administrador de Azure. Hemos creado el nombre de dominio personalizado azureadmininc.org para la instancia. Podemos configurar una zona DNS secundaria aparte para el dominio personalizado para admitir asociados de la organización, como partners.azureadmininc.org.

Los pasos de configuración para delegar una zona DNS secundaria son similares al proceso de delegación típico. La principal diferencia es que no hay que trabajar con el registrador para delegar un subdominio. La zona DNS secundaria se delega en Azure Portal.

Estos son los pasos para delegar un subdominio:

1. Vaya a la zona DNS primaria del dominio en Azure Portal.
2. Localice los registros NS existentes de su dominio primario
3. Cree registros NS para la zona DNS secundaria (subdominio).

**Nota**

Las zonas DNS principal y secundaria pueden estar en el mismo grupo de recursos o en otro.

En nuestro ejemplo, observe que el nombre del servidor de registros NS de la zona DNS secundaria es el mismo que el de la zona DNS primaria, azureadmininc.com. La única diferencia que distingue al subdominio es la incorporación de la palabra clave *partners* con el punto de separación (.).

**Adición de conjuntos de registros de DNS**

Es importante comprender la diferencia entre **conjuntos de registros de DNS** y registros DNS individuales. Un conjunto de registros DNS (también denominado *conjunto de registros de recursos*) es una colección de registros en una zona DNS.

Los conjuntos de registros se definen en Azure Portal. Las opciones de configuración dependen del tipo de registro del conjunto que se va a crear.

Supongamos que decide crear un conjunto de registros A (o *registro de direcciones*) para identificar las direcciones IP asociadas al dominio. Para crear los registros A, debe proporcionar el TTL (período de vida) y las direcciones IP. El valor de TTL especifica durante cuánto tiempo los clientes almacenan cada registro en caché.



**Aspectos que saber sobre los conjuntos de registros de DNS**

Vamos a examinar algunas características de los conjuntos de registros de DNS.

* Todos los registros de un conjunto de registros de DNS deben tener el mismo nombre y el mismo tipo de registro.

Veamos el siguiente ejemplo en el que tenemos dos registros en un conjunto de registros. Todos los registros tienen el mismo nombre, www.contoso.com.. Todos los registros tienen el mismo tipo de registro, A. Cada registro del conjunto tiene un valor diferente. En este caso, cada registro proporciona una dirección IP diferente.

www.contoso.com. 3600 IN A 134.170.185.46

www.contoso.com. 3600 IN A 134.170.188.221

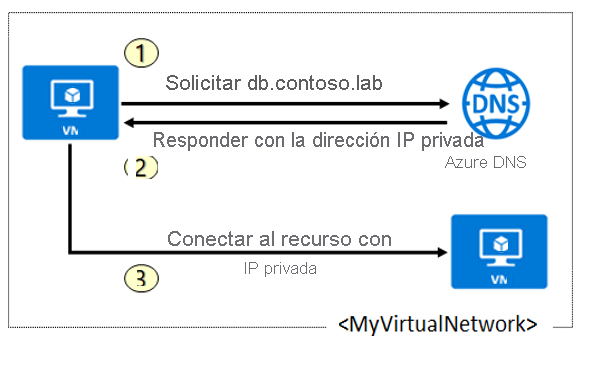
* Un conjunto de registros de DNS no puede contener dos registros idénticos.
* Un conjunto de registros de tipo CNAME puede contener solamente un registro.

Un registro CNAME (o *registro de nombre canónico*) proporciona un alias de un nombre de dominio a otro. Este registro se usa para proporcionar otro nombre para el dominio. La operación DNS lookup trata de encontrar el dominio reintentando la operación lookup con el otro nombre especificado en el registro CNAME.

* Puede crear un conjunto de registros que no tenga ningún registro. Este conjunto se denomina *conjunto de registros vacío*.
* Si tiene un conjunto de registros vacío para el dominio, este conjunto no aparece en los servidores DNS de Azure.

**Planeamiento de zonas del DNS privado de Azure**

Las zonas de DNS privado de Azure se pueden crear con sus propios nombres de dominio personalizados en lugar de los nombres proporcionados por Azure. Con sus propios nombres de dominio personalizados puede adaptar la arquitectura de red virtual para satisfacer mejor las necesidades de su organización. Obtiene la resolución de nombres para las máquinas virtuales dentro de una red virtual y entre redes virtuales. Puede configurar nombres de zonas DNS con una vista de *horizonte dividido* que permite que una zona DNS privada y otra pública compartan el mismo nombre de dominio.



**Aspectos que se deben conocer sobre las ventajas del DNS privado de Azure**

Hay muchas ventajas al implementar el DNS privado de Azure para el dominio.

| **Prestación** | **Descripción** |
| --- | --- |
| **No se requiere ninguna solución DNS personalizada** | Anteriormente, muchos clientes crearon soluciones DNS personalizadas para administrar zonas DNS en su red virtual. Ahora puede llevar a cabo la administración de las zonas DNS mediante la infraestructura nativa de Azure. El DNS privado de Azure elimina la carga que supone crear y administrar soluciones DNS personalizadas. |
| **Compatibilidad con tipos de registros DNS comunes** | El DNS privado de Azure admite todos los tipos de registros DNS comunes, incluidos A, AAAA, CNAME, MX, PTR, SOA, SRV y TXT. |
| **Administración automática de registros de nombres de host** | Además de hospedar los registros de DNS personalizados, el DNS privado de Azure mantiene automáticamente los registros de nombres de host de las máquinas virtuales en las redes virtuales especificadas. En este escenario, puede optimizar los nombres de dominio usados sin necesidad de crear soluciones DNS personalizadas ni de modificar aplicaciones. |
| **Resolución de nombres de host entre redes virtuales** | A diferencia de los nombres de host proporcionados por Azure, las zonas DNS de Azure privadas pueden compartirse entre redes virtuales. Esta funcionalidad simplifica los escenarios de detección de servicios y de distintas redes, como el emparejamiento de red virtual. |
| **Experiencia del usuario y herramientas familiares** | Para reducir la curva de aprendizaje, el DNS privado de Azure usa herramientas de Azure DNS establecidas, incluidas PowerShell, plantillas de Azure Resource Manager (ARM) y la API REST. |
| **Compatibilidad con DNS de horizonte dividido** | Con el DNS privado de Azure, puede crear zonas con el mismo nombre que se resuelve en diferentes respuestas desde dentro de una red virtual y desde la red pública de Internet. Un escenario típico de DNS de horizonte dividido es proporcionar una versión dedicada de un servicio para usarla dentro de la red virtual. |
| **Compatibilidad con regiones de Azure** | Las zonas de DNS privado de Azure están disponible en todas las regiones de Azure de la nube pública de Azure. |

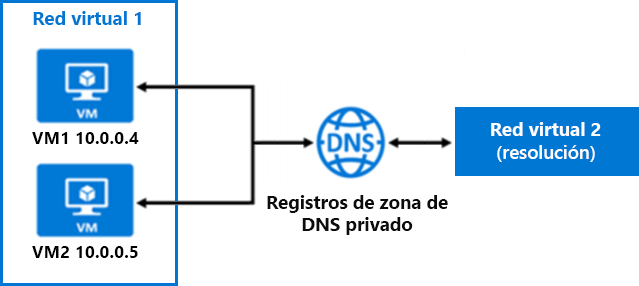
En la sección siguiente, revisaremos algunos escenarios de implementación comunes para el DNS privado de Azure.

**Revisión de escenarios de zona del DNS privado de Azure**

Vamos a revisar algunos escenarios comunes para implementar registros de zona de DNS privado de Azure.

**Escenario 1: Resolución de nombres con ámbito de una única red virtual**

El primer escenario consta de redes virtuales y recursos en Azure que incluyen máquinas virtuales. Los recursos deben resolverse desde dentro de la red virtual mediante un nombre de dominio específico (o zona DNS). La resolución de nombres debe ser privada y no ser accesible desde Internet. El escenario requiere que Azure registre automáticamente las máquinas virtuales dentro de la red virtual en la zona DNS.



Vamos a examinar los detalles de este escenario:

* La red virtual 1 contiene dos máquinas virtuales: VM1 y VM2. VM1 y VM2 tienen una dirección IP privada.
* Cuando se crea una dirección de zona de DNS privado de Azure (como contoso.lab) y se vincula a la red virtual 1, Azure DNS crea automáticamente dos registros A en la zona DNS si el **registro automático** está habilitado en la configuración del vínculo.
* En este escenario, Azure DNS usa solo la Red virtual 2 para resolver consultas de nombre de dominio (o zona DNS).

Las consultas de Azure DNS de VM1 en la Red virtual 1 para resolver la dirección VM2.contoso.lab reciben una respuesta de Azure DNS que contiene la dirección IP privada de VM2 (10.0.0.5).

* Una consulta de DNS inversa (PTR) de la dirección IP privada de VM1 (10.0.0.4) emitida desde VM2 recibirá una respuesta de Azure DNS que contiene el FQDN de VM1, según lo previsto.

**Escenario 2: Resolución de nombres para varias redes**

El segundo escenario implica la resolución de nombres en varias redes virtuales, que probablemente es el uso más común para las zonas de DNS privado de Azure. Este escenario consta de dos redes virtuales. Una red se centra en el registro de los registros de zona de DNS privado de Azure y la otra admite la resolución de nombres.



Estos son los detalles de esta configuración:

* La red virtual 1 se designa para el *registro*. La red virtual 2 se designa para la *resolución de nombres*.
* La estrategia de diseño es que ambas redes virtuales compartan la dirección de zona DNS común, contoso.lab.
* Las redes virtuales de resolución y registro están vinculadas a la zona DNS común.
* Los registros de zona de DNS privado de Azure para las máquinas virtuales de la Red virtual 1 (registro) se crean automáticamente.
* En el caso de las máquinas virtuales de la Red virtual 2 (resolución), los registros de zona de DNS privado de Azure se pueden crear manualmente.
* En este escenario, Azure DNS usa ambas redes virtuales para resolver consultas de nombres de dominio.

Una consulta de Azure DNS de una máquina virtual en la Red virtual 2 (resolución) para una máquina virtual de la Red virtual 1 (registro) recibe una respuesta de Azure DNS que contiene la dirección IP privada de la máquina virtual.

* Las consultas de DNS inverso tienen como ámbito la misma red virtual.
  + Una consulta de DNS inverso (PTR) de una máquina virtual en la Red virtual 2 (resolución) para una máquina virtual de la Red virtual 1 (registro) recibe una respuesta de Azure DNS que contiene NXDOMAIN de la máquina virtual. NXDOMAIN es un mensaje de error que indica que el dominio consultado no existe.
  + Una consulta de DNS inverso (PTR) de una máquina virtual en la Red virtual 1 (registro) para una máquina virtual también en la Red virtual 1 recibe el FQDN de la máquina virtual.

**Comprobación de conocimiento**

Su organización quiere usar Azure DNS para administrar el dominio personalizado para un nuevo sitio web de la empresa. Está trabajando en el plan de implementación de las zonas DNS, la delegación DNS y los conjuntos de registros DNS.

* El equipo de TI quiere saber si hay ventajas al usar DNS privado de Azure.
* El equipo de administración necesita información sobre cómo asignar registros DNS a direcciones IP.

**Responda a las siguientes preguntas**

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

Principio del formulario

**1. ¿Qué resumen describe mejor el propósito principal de Azure DNS?**

1. Azure DNS administra la seguridad y el acceso al sitio web.
2. Azure DNS administra y hospeda el dominio registrado para un sitio web y sus registros asociados.
3. Azure DNS registra nuevos nombres de dominio, por lo que no es necesario usar un registrador de dominios.

**2. ¿Qué tipo de registro de DNS puede asignar una o varias direcciones IP en un solo dominio?**

1. CNAME
2. SOA
3. A o AAAA

**3. ¿Cuál de los escenarios siguientes admite el DNS privado de Azure?**

1. Las organizaciones administran y resuelven nombres de dominio en una red virtual sin agregar una solución DNS personalizada.
2. Las organizaciones administran y resuelven nombres de dominio en una red virtual mediante la adición de una solución DNS personalizada.
3. Las organizaciones administran nombres de dominio en otras organizaciones.
4. B
5. C
6. A

Final del formulario

**Resumen y recursos**

En este módulo, ha conocido Azure DNS. Ha aprendido a identificar las características y los casos de uso de dominios, dominios personalizados y zonas privadas. También ha aprendido a comprobar nombres de dominio personalizados mediante registros DNS e implementar zonas DNS, delegación y conjuntos de registros.

Las principales conclusiones de este módulo son:

* Azure DNS es un servicio de hospedaje que permite administrar dominios DNS mediante la infraestructura de Microsoft Azure.
* También puede comprobar nombres de dominio personalizados mediante registros DNS e implementar zonas DNS, delegación y conjuntos de registros.
* Azure DNS es un servicio DNS confiable y seguro que elimina la necesidad de una solución DNS personalizada en una red virtual.
* Las zonas de DNS privado ofrecen más flexibilidad en el diseño de la arquitectura de red virtual y proporcionan resolución de nombres entre redes virtuales.