

Contents

Documentación de Load Balancer

Información general

- ¿Qué es Azure Load Balancer?

Guías de inicio rápido

- Creación de un equilibrador de carga público: Azure Portal

- Creación de un equilibrador de carga público: PowerShell

- Creación de un equilibrador de carga público: CLI de Azure

- Creación de un equilibrador de carga público: plantilla de Resource Manager

- Creación de un equilibrador de carga interno: Azure Portal

- Creación de un equilibrador de carga interno: PowerShell

- Creación de un equilibrador de carga interno: CLI de Azure

- Creación de un equilibrador de carga interno: plantilla de Resource Manager

Tutoriales

- Equilibrio de carga de máquinas virtuales entre zonas de disponibilidad

- Equilibrio de carga de máquinas virtuales en una zona de disponibilidad específica

- Configuración del reenvío de puertos de Load Balancer

Ejemplos

- Azure CLI

- Azure PowerShell

Conceptos

- Componentes

- Conceptos

- SKU

- Supervisión del estado

 - Sondeos de estado

 - Diagnósticos y métrica de Load Balancer estándar

 - Registros de Azure Monitor para Load Balancer básico

 - Obtención de métricas de Load Balancer con REST

- Puertos de alta disponibilidad

Varios servidores front-end

Conexiones de salida

Restablecimiento de TCP en tiempo de espera de inactividad

Load Balancer Estándar y zonas de disponibilidad

Controles de seguridad integrados

Administración de grupos de back-end

Standard Load Balancer y Virtual Machine Scale Sets

Procedimientos

Configuración del portal

Conjuntos de escalado de máquinas virtuales

- Uso con una instancia de Azure Load Balancer (Azure Portal)

- Uso con una instancia de Azure Load Balancer (PowerShell)

- Uso con una instancia de Azure Load Balancer (CLI)

Actualización de la versión Básico de Load Balancer a Standard Load Balancer

- Actualización de la versión Básico de un equilibrador de carga público

- Actualización de un equilibrador de carga interno: no se requiere conexión de salida

- Actualización de un equilibrador de carga interno: se requiere conexión de salida

Creación de Load Balancer público con IPv6

- Azure CLI

- Azure PowerShell

- Plantilla del Administrador de recursos de Azure

Configuración del tiempo de espera de inactividad TCP del equilibrador de carga

Configuración del modo de distribución de Load Balancer

Uso de varias configuraciones de IP

- Portal

- Azure CLI

- Azure PowerShell

Traslado entre regiones

- Equilibrador de carga público: Azure Portal

- Equilibrador de carga público: PowerShell

- Equilibrador de carga público: Azure Portal

- Equilibrador de carga interno: PowerShell

[Configuración del equilibrador de carga solo de salida](#)

[Solución de problemas](#)

[Solución de problemas de Azure Load Balancer](#)

[Solución de errores de implementación comunes](#)

[Solución de problemas comunes de la conexión saliente](#)

[Solución de problemas de estado y disponibilidad de entrada de los recursos](#)

[Referencia](#)

[Ejemplos de código](#)

[Azure PowerShell](#)

[Azure CLI](#)

[.NET](#)

[Java](#)

[Node.js](#)

[Ruby](#)

[Python](#)

[REST](#)

[Plantilla de Resource Manager](#)

[Recursos](#)

[Desarrollo de aptitudes con Microsoft Learn](#)

[Azure Roadmap](#)

[Comentarios sobre Azure Load Balancer](#)

[Precios](#)

[Calculadora de precios](#)

[Actualizaciones del producto](#)

[Preguntas más frecuentes](#)

¿Qué es Azure Load Balancer?

23/09/2020 • 7 minutes to read • [Edit Online](#)

El *equilibrio de carga* hace referencia a la distribución uniforme de la carga (el tráfico de red entrante) en un grupo de recursos o servidores de back-end.

Azure Load Balancer opera en la capa cuatro del modelo de interconexión de sistema abierto (OSI). Es el único punto de contacto de los clientes. Load Balancer distribuye flujos de entrada que llegan al front-end del equilibrador de carga a las instancias del grupo de servidores back-end. Estos flujos están de acuerdo con las reglas de equilibrio de carga y los sondeos de estado configurados. Las instancias del grupo de back-end pueden ser instancias de Azure Virtual Machines o de un conjunto de escalado de máquinas virtuales.

Un **equilibrador de carga público** puede proporcionar conexiones de salida para máquinas virtuales dentro de la red virtual. Estas conexiones se realizan mediante la traducción de sus direcciones IP privadas a direcciones IP públicas. Las instancias públicas de Load Balancer se usan para equilibrar la carga del tráfico de Internet en las máquinas virtuales.

Un **equilibrador de carga interno (o privado)** se usa cuando se necesitan direcciones IP privadas solo en el front-end. Los equilibradores de carga internos se usan para equilibrar la carga del tráfico dentro de una red virtual. También se puede acceder a un servidor front-end del equilibrador de carga desde una red local en un escenario híbrido.

Ilustración: Equilibrar las aplicaciones de niveles múltiples mediante Load Balancer público e interno

Para más información sobre los componentes individuales de Load Balancer, consulte [Componentes de Azure Load Balancer](#).

Uso de Azure Load Balancer

Con Standard Load Balancer, puede escalar las aplicaciones y crear servicios con alta disponibilidad. Load Balancer admite escenarios de entrada y salida. Una instancia de Load Balancer proporciona baja latencia y alto rendimiento, y puede escalar hasta millones de flujos para todas las aplicaciones TCP y UDP.

Entre los escenarios clave que puede realizar con Standard Load Balancer se incluyen:

- Equilibrio de carga del tráfico **interno** y **externo** a las máquinas virtuales de Azure.
- Aumento de la disponibilidad mediante la distribución de recursos **en zonas** y **a través de ellas** .
- Configuración de la **conectividad de salida** para máquinas virtuales de Azure.
- Uso de **sondeos de estado** para supervisar los recursos con equilibrio de carga.
- Empleo del **desvío de puertos** para acceder a las máquinas virtuales de una red virtual mediante la dirección IP pública y el puerto.
- Habilitación de la compatibilidad con el **equilibrio de carga** de **IPv6** .
- Standard Load Balancer proporciona métricas multidimensionales mediante [Azure Monitor](#). Estas métricas se pueden filtrar, agrupar y desglosar para una dimensión determinada. Proporcionan una perspectiva actual e histórica del rendimiento y el mantenimiento del servicio. También se admite Resource Health. Consulte [Diagnósticos de Standard Load Balancer](#) para más información.

- Servicios de equilibrio de carga en [varios puertos, varias direcciones IP, o en ambos](#) .
- Desplazamiento de los recursos [internos](#) y [externos](#) del equilibrador de carga por las regiones de Azure.
- Equilibrio de carga del flujo de TCP y UDP en todos los puertos simultáneamente mediante los [puertos de alta disponibilidad](#) .

Seguro de forma predeterminada

Standard Load Balancer se basa en el modelo de seguridad de red de confianza cero en su núcleo. Standard Load Balancer es seguro de forma predeterminada y forma parte de la red virtual. La red virtual es una red privada y aislada. Esto significa que las instancias de Standard Load Balancer y las direcciones IP públicas estándar se cierran en los flujos de entrada a menos que los abran los grupos de seguridad de red. Los grupos de seguridad de red se usan para permitir explícitamente el tráfico admitido. Si no tiene ningún grupo de seguridad de red en una subred o NIC del recurso de máquina virtual, no se permitirá que el tráfico llegue a este recurso. Para aprender más sobre los NSG y cómo aplicarlos en su caso, vea [Grupos de seguridad de red](#). Load Balancer Básico está abierto a Internet de forma predeterminada. Además, Load Balancer no almacena datos de los clientes.

Precios y contrato de nivel de servicio

Para más información sobre los precios de Standard Load Balancer, consulte [Precios de Load Balancer](#). Load Balancer Básico se ofrece sin cargo. Consulte [Acuerdo de Nivel de Servicio para Load Balancer](#). Load Balancer Básico no tiene Acuerdo de Nivel de Servicio.

Novedades

Suscríbase a la fuente RSS y vea las actualizaciones más recientes de las características de Azure Load Balancer en la página [Actualizaciones de Azure](#).

Pasos siguientes

Consulte [Actualización de la versión Básico de un equilibrador de carga](#) para actualizar a la versión Estándar.

Consulte el artículo sobre cómo [crear una instancia de Standard Load Balancer pública](#) para empezar a usar un equilibrador de carga.

Para más información acerca de las limitaciones y los componentes de Azure Load Balancer, consulte [Componentes de Azure Load Balancer](#) y [Conceptos de Azure Load Balancer](#)

Si desea ver una comparación de las distintas opciones de equilibrio de carga de Azure, consulte [Información general sobre las opciones de equilibrio de carga en Azure](#).

Inicio rápido: Uso de Azure Portal para crear un equilibrador de carga público para equilibrar la carga de máquinas virtuales

23/09/2020 • 32 minutes to read • [Edit Online](#)

Comience a usar Azure Load Balancer mediante Azure Portal para crear un equilibrador de carga público y tres máquinas virtuales.

Requisitos previos

- Una cuenta de Azure con una suscripción activa. [Cree una cuenta gratuita](#).

Inicio de sesión en Azure

Inicie sesión en Azure Portal en <https://portal.azure.com>.

- [SKU Estándar](#)
- [SKU básica](#)

NOTE

Se recomienda usar la SKU Estándar de Load Balancer para las cargas de trabajo de producción. Para más información sobre las SKU, consulte [SKU de Azure Load Balancer](#).

En esta sección, va a crear un equilibrador de carga que equilibra la carga de las máquinas virtuales.

Cuando se crea una instancia pública de Load Balancer, también se debe crear una nueva dirección IP pública que se configura como front-end (llamada **LoadBalancerFrontend** de forma predeterminada) para dicha instancia.

1. En la parte superior izquierda de la pantalla, seleccione **Crear un recurso** > **Redes** > **Load Balancer**.
2. En la pestaña **Conceptos básicos** de la página **Crear equilibrador de carga**, escriba o seleccione la siguiente información:

CONFIGURACIÓN	VALUE
Subscription	Seleccione su suscripción.
Resource group	Seleccione Crear nuevo y escriba MyResourceGroupLB en el cuadro de texto.
Nombre	Escriba myLoadBalancer .
Region	Seleccione Oeste de Europa .
Tipo	Seleccione Público .
SKU	Seleccione Estándar .

CONFIGURACIÓN	VALUE
Dirección IP pública	Seleccione Crear nuevo . Si tiene una dirección IP pública que le gustaría usar, seleccione Utilizar existente .
Nombre de la dirección IP pública	Escriba myPublicIP en el cuadro de texto.
Zona de disponibilidad	Seleccione Con redundancia de zona para crear un equilibrador de carga resistente. Para crear una instancia de Load Balancer de zona, seleccione una zona específica entre 1, 2 o 3.
Adición de una dirección IPv6 pública	así que seleccione No . Para más información sobre las direcciones IPv6 y el equilibrador de carga, consulte ¿Qué es IPv6 para Azure Virtual Network?

- Acepte los valores predeterminados en los demás valores y seleccione **Revisar y crear**.
- En la pestaña **Revisar + crear**, seleccione **Crear**.

Microsoft Azure

Buscar recursos, servicios y documentos

Inicio > Nuevo > Crear equilibrador de carga

Crear equilibrador de carga

Conceptos básicos Etiquetas Revisar y crear

Azure Load Balancer es un equilibrador de carga de capa 4 que distribuye el tráfico entrante entre las instancias de máquina virtual correctas. Los equilibradores de carga usan un algoritmo de distribución basado en hash. De forma predeterminada, usa el hash 5-tupla (IP de origen, puerto de origen, IP de destino, puerto de destino y tipo de protocolo) para asignar el tráfico a los servidores disponibles. Los equilibradores de carga pueden ser accesibles desde Internet, a través de direcciones IP públicas, o bien internos, a los que solo se puede acceder desde una red virtual. Los equilibradores de carga de Azure también son compatibles con la traducción de direcciones de red (NAT) para enrutar el tráfico entre las direcciones IP públicas y privadas. [Obtenga más información.](#)

DETALLES DEL PROYECTO

* Suscripción: suscripción

* Grupo de recursos: (Nuevo) myLoadBalancerSLB [Crear nuevo](#)

DETALLES DE INSTANCIA

* Nombre: myLoadBalancer ✓

* Región: Oeste de Europa

* Tipo: ☐ Interno ☒ Público

* SKU: ☐ Básico ☒ Estándar

DIRECCIÓN IP PÚBLICA

* Dirección IP pública: ☒ Crear nuevo ☐ Usar existente

* Nombre de dirección IP pública: myPublicIP ✓

SKU de la dirección IP pública: Estándar

* Asignación: ☐ Dinámico ☒ Contenido

* Zona de disponibilidad: Con redundancia de zona

[Revisar y crear](#) Anterior [Siguiente: Etiquetas >](#) [Descargar una plantilla para la automatización](#)

Creación de recursos del equilibrador de carga

En esta sección, va a configurar:

- Las opciones del equilibrador de carga para un grupo de direcciones de back-end.
- Un sondeo de estado.
- Una regla de equilibrador de carga.

Creación de un grupo de back-end

Un grupo de direcciones de back-end contiene las direcciones IP de las tarjetas de interfaz de red virtuales conectadas al equilibrador de carga.

Cree el grupo de direcciones de back-end **myBackendPool** para incluir máquinas virtuales para el tráfico de Internet de equilibrio de carga.

1. Seleccione **Todos los servicios** en el menú de la izquierda, **Todos los recursos** y, después, en la lista de recursos, **myLoadBalancer**.
2. En **Configuración**, seleccione **Grupos de back-end** y, a continuación, seleccione **Agregar**.
3. En la página **Agregar un grupo back-end**, en nombre, escriba **myBackEndPool**, como el nombre del grupo de back-end y, a continuación, seleccione **Aceptar**.

Creación de un sondeo de estado

El equilibrador de carga supervisa el estado de la aplicación con un sondeo de estado.

El sondeo de estado agrega o quita las máquinas virtuales del equilibrador de carga a partir de su respuesta a las comprobaciones de estado.

Cree un sondeo de mantenimiento llamado **myHealthProbe** para supervisar el mantenimiento de las máquinas virtuales.

1. Seleccione **Todos los servicios** en el menú de la izquierda, **Todos los recursos** y, después, en la lista de recursos, **myLoadBalancer**.
2. En **Configuración**, seleccione **Sondeos de estado** y, a continuación, seleccione **Agregar**.

CONFIGURACIÓN	VALUE
Nombre	Escriba myHealthProbe .
Protocolo	Seleccione HTTP .
Port	Escriba 80 .
Intervalo	Escriba 15 como número de Intervalo , en segundos, entre los intentos de sondeo.
Umbral incorrecto	Seleccione 2 como número de Umbral incorrecto o errores de sondeo consecutivos que deben producirse para que una máquina virtual se considere que no funciona de manera correcta.

3. Deje el resto de valores predeterminados y seleccione **Aceptar**.

Creación de una regla de equilibrador de carga

Las reglas de equilibrador de carga se utilizan para definir cómo se distribuye el tráfico a las máquinas virtuales. Defina la configuración IP del front-end para el tráfico entrante y el grupo de direcciones IP de back-end para

recibir el tráfico. Los puertos de origen y de destino se definen en la regla.

En esta sección va a crear una regla de equilibrador de carga:

- Llamada **myHTTPRule**.
 - En el front-end llamado **LoadBalancerFrontEnd**.
 - A la escucha en el **puerto 80**.
 - Dirige el tráfico con equilibrio de carga al back-end llamado **myBackendPool** en el **puerto 80**.
1. Seleccione **Todos los servicios** en el menú de la izquierda, **Todos los recursos** y, después, en la lista de recursos, **myLoadBalancer**.
 2. En **Configuración**, seleccione **Reglas de equilibrio de carga** y, a continuación, seleccione **Agregar**.
 3. Use estos valores para configurar la regla de equilibrio de carga:

CONFIGURACIÓN	VALUE
Nombre	Escriba myHTTPRule .
Versión de la dirección IP	Seleccione IPv4 .
Dirección IP del front-end	Seleccione LoadBalancerFrontEnd .
Protocolo	seleccione TCP .
Port	Escriba 80 .
Puerto back-end	Escriba 80 .
Grupo back-end	Seleccione MyBackendPool .
Sondeo de mantenimiento	Seleccione myHealthProbe .
Creación de reglas de salida implícitas	así que seleccione No .

4. Deje el resto de valores predeterminados y después seleccione **Aceptar**.

Creación de servidores back-end

En esta sección:

- Cree una red virtual.
- Creará tres máquinas virtuales para el grupo de back-end del equilibrador de carga.
- Instalará IIS en las máquinas virtuales para probar el equilibrador de carga.

Crear la red virtual

En esta sección, creará una red virtual y una subred.

1. En la parte superior izquierda de la pantalla, seleccione **Crear un recurso > Redes > Red virtual** o busque **Red virtual** en el cuadro de búsqueda.
2. En **Crear red virtual**, escriba o seleccione esta información en la pestaña **Conceptos básicos**:

CONFIGURACIÓN	VALOR
Detalles del proyecto	
Suscripción	Selección de su suscripción a Azure
Grupo de recursos	Seleccione myResourceGroupLB .
Detalles de instancia	
Nombre	Escriba myVNet .
Region	Seleccione Oeste de Europa .

3. Seleccione la pestaña **Direcciones IP** o el botón **Siguiente: Direcciones IP** situado en la parte inferior de la página.

4. En la pestaña **Direcciones IP**, especifique esta información:

CONFIGURACIÓN	VALUE
Espacio de direcciones IPv4	Escriba 10.1.0.0/16 .

5. En **Nombre de subred**, seleccione la palabra **predeterminada**.

6. En **Editar subred**, especifique esta información:

CONFIGURACIÓN	VALUE
Nombre de subred	Escriba myBackendSubnet .
Intervalo de direcciones de subred	Escriba 10.1.0.0/24 .

7. Seleccione **Guardar**.

8. Seleccione la pestaña **Seguridad**.

9. En **BastionHost**, seleccione **Habilitar**. Escriba esta información:

CONFIGURACIÓN	VALUE
Nombre del bastión	Escriba myBastionHost .
Espacio de direcciones de AzureBastionSubnet	Escriba 10.1.1.0/24 .
Dirección IP pública	Seleccione Crear nuevo . En Nombre , escriba myBastionIP . Seleccione Aceptar .

10. Seleccione la pestaña **Revisar y crear** o el botón **Revisar y crear**.

11. Seleccione **Crear**.

Creación de máquinas virtuales

En esta sección, creará tres máquinas virtuales (**myVM1**, **myVM2** y **myVM3**) en tres zonas diferentes (**Zona 1**, **Zona 2** y **Zona 3**).

Estas máquinas virtuales se agregan al grupo de back-end del equilibrador de carga que se creó anteriormente.

1. En la parte superior izquierda de Azure Portal, seleccione **Crear un recurso** > **Proceso** > **Máquina virtual**.
2. En **Crear una máquina virtual**, escriba o seleccione los valores en la pestaña **Básico**:

CONFIGURACIÓN	VALUE
Detalles del proyecto	
Suscripción	Selección de su suscripción a Azure
Grupo de recursos	Seleccione myResourceGroupLB .
Detalles de instancia	
Nombre de la máquina virtual	Escriba myVM1 .
Region	Seleccione Oeste de Europa .
Opciones de disponibilidad	Seleccione Zonas de disponibilidad .
Zona de disponibilidad	Seleccione 1 .
Imagen	Seleccione Windows Server 2019 Datacenter .
Instancia de Azure Spot	Seleccione No .
Size	Elija el tamaño de la máquina virtual o acepte la configuración predeterminada.
Cuenta de administrador	
Nombre de usuario	Escriba un nombre de usuario.
Contraseña	Escriba una contraseña.
Confirmar contraseña	Vuelva a escribir la contraseña.
Reglas de puerto de entrada	
Puertos de entrada públicos	Seleccione Ninguno .

3. Seleccione la pestaña **Redes** o seleccione **Siguiente: Discos** y, después, **Siguiente: Redes**.
4. En la pestaña **Redes**, seleccione o escriba:

CONFIGURACIÓN	VALUE
Interfaz de red	
Virtual network	myVNet

CONFIGURACIÓN	VALUE
Subnet	myBackendSubnet
Dirección IP pública	Seleccione Ninguno .
Grupo de seguridad de red de NIC	Seleccione Avanzado .
Configuración del grupo de seguridad de red	Seleccione Crear nuevo . En la página Crear grupo de seguridad de red , escriba myNSG en Nombre . En Reglas de entrada , seleccione +Agregar una regla de entrada . En Intervalos de puertos de destino , escriba 80 . En Prioridad , escriba 100 . En Nombre , escriba myHTTPRule . Seleccione Agregar . Seleccione Aceptar .
Equilibrio de carga	
¿Quiere colocar esta máquina virtual como subyacente respecto a una solución de equilibrio de carga existente?	Seleccione Sí .
Configuración de equilibrio de carga	
Opciones de equilibrio de carga	Seleccione Equilibrio de carga de Azure .
Seleccionar un equilibrador de carga	Seleccione myLoadBalancer .
Seleccionar un grupo de back-end	Seleccione MyBackendPool .

5. Seleccione la pestaña **Administración** o seleccione **Siguiente > Administración**.

6. En la pestaña **Administración**, seleccione o escriba:

CONFIGURACIÓN	VALUE
Supervisión	
Diagnósticos de arranque	Seleccione Desactivado .

7. Seleccione **Revisar + crear**.

8. Revise la configuración y, a continuación, seleccione **Crear**.

9. Siga los pasos 1 a 8 para crear dos máquinas virtuales adicionales con los siguientes valores y todos los demás valores deben coincidir con los de **myVM1**:

CONFIGURACIÓN	VM 2	VM 3
Nombre	myVM2	myVM3
Zona de disponibilidad	2	3

CONFIGURACIÓN	VM 2	VM 3
Grupo de seguridad de red	Seleccione el grupo myNSG existente.	Seleccione el grupo myNSG existente.

Creación de la configuración de regla de salida

Las reglas de salida del equilibrador de carga configuran SNAT saliente para las máquinas virtuales del grupo de back-end.

Para más información sobre las conexiones salientes, consulte [Conexiones salientes en Azure](#).

Creación de una regla de salida

1. Seleccione **Todos los servicios** en el menú de la izquierda, **Todos los recursos** y, después, en la lista de recursos, **myLoadBalancer**.
2. En **Configuración**, seleccione **Reglas de salida** y, a continuación, seleccione **Agregar**.
3. Use estos valores para configurar las reglas de salida:

CONFIGURACIÓN	VALUE
Nombre	Escriba myOutboundRule .
Dirección IP del front-end	<p>Seleccione Crear nuevo.</p> <p>En Nombre, escriba LoadBalancerFrontEndOutbound.</p> <p>Seleccione Dirección IP o Prefijo IP.</p> <p>Seleccione Crear nuevo en Dirección IP pública o Prefijo de dirección IP pública.</p> <p>En Nombre, escriba myPublicIPOutbound o myPublicIPPrefixOutbound.</p> <p>Seleccione Agregar.</p>
Tiempo de espera de inactividad (minutos)	Mueva el control deslizante a 15 minutos .
Restablecimiento de TCP	Seleccione Habilitado .
Grupo back-end	<p>Seleccione Crear nuevo.</p> <p>Escriba myBackendPoolOutbound en Name.</p> <p>Seleccione Agregar.</p>
Asignación de puertos: > Asignación de puertos	Seleccione Elegir manualmente el número de puertos de salida .
Puertos de salida: > Elegir por	Seleccione Puertos por instancia .
Puertos de salida -> Puertos por instancia	Escriba 10000 .

4. Seleccione **Agregar**.

Adición de máquinas virtuales al grupo de salida

1. Seleccione **Todos los servicios** en el menú de la izquierda, **Todos los recursos** y, después, en la lista de recursos, **myLoadBalancer**.
2. En **Configuración**, seleccione **Grupos de back-end**.

3. Seleccione **myBackendPoolOutbound**.
4. En **Red virtual**, seleccione **myVNet**.
5. En **Máquinas virtuales**, seleccione + **Agregar**.
6. Active las casillas situadas junto a **myVM1**, **myVM2** y **myVM3**.
7. Seleccione **Agregar**.
8. Seleccione **Guardar**.

Instalación de IIS

1. Seleccione **Todos los servicios** en el menú de la izquierda, seleccione **Todos los recursos** y, después, en la lista de recursos, seleccione **myVM1**, que se encuentra en el grupo de recursos **myResourceGroupLB**.
2. En la página **Introducción**, seleccione **Conectar** y después **Instancia de Bastion**.
3. Escriba el nombre de usuario y la contraseña especificados durante la creación de la máquina virtual.
4. Seleccione **Conectar**.
5. En el escritorio del servidor, vaya a **Herramientas administrativas de Windows > Windows PowerShell**.
6. Ejecute los siguientes comandos en la ventana de PowerShell para:
 - Instalar el servidor IIS
 - Eliminar el archivo predeterminado iisstart.htm
 - Agregue un nuevo archivo iisstart.htm que muestre el nombre de la máquina virtual:

```
# install IIS server role
Install-WindowsFeature -name Web-Server -IncludeManagementTools

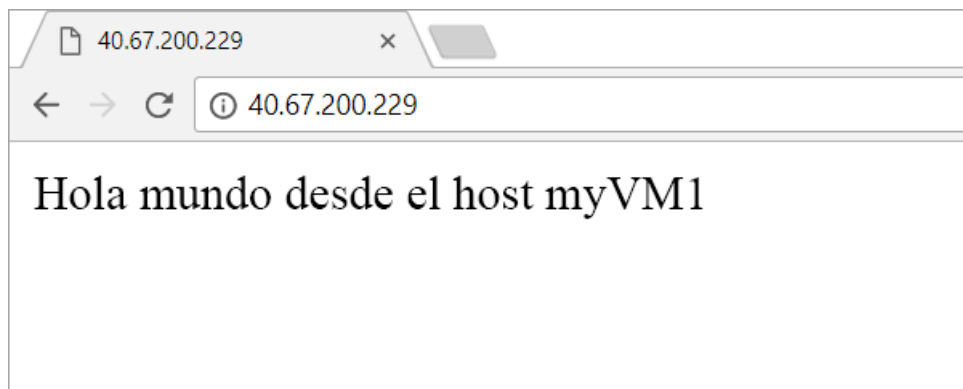
# remove default htm file
remove-item C:\inetpub\wwwroot\iisstart.htm

# Add a new htm file that displays server name
Add-Content -Path "C:\inetpub\wwwroot\iisstart.htm" -Value $("Hello World from " + $env:computername)
```

7. Cierre la sesión de Bastion con **myVM1**.
8. Repita los pasos 1 a 6 para instalar IIS y el archivo iisstart.htm actualizado en **myVM2** y **myVM3**.

Prueba del equilibrador de carga

1. Busque la dirección IP pública de Load Balancer en la pantalla **Información general**. Seleccione **Todos los servicios** en el menú de la izquierda, **Todos los recursos** y, después, **myPublicIP**.
2. Copie la dirección IP pública y péguela en la barra de direcciones del explorador. La página predeterminada del servidor web de IIS se muestra en el explorador.



Para ver el tráfico distribuido por Load Balancer entre las tres máquinas virtuales, puede personalizar la página predeterminada de cada servidor web IIS de las máquinas virtuales y luego forzar una actualización del explorador web desde el equipo cliente.

Limpieza de recursos

Cuando no los necesite, elimine el grupo de recursos, la instancia de Load Balancer y todos los recursos relacionados. Para ello, seleccione el grupo de recursos **myResourceGroupLB**, que contiene los recursos y, a continuación, seleccione **Eliminar**.

Pasos siguientes

En esta guía de inicio rápido:

- Ha creado una instancia Estándar o Básica de Azure Load Balancer.
- Ha conectado 3 máquinas virtuales al equilibrador de carga.
- Ha configurado la regla de tráfico del equilibrador de carga, el sondeo de estado y, a continuación, ha probado el equilibrador de carga.

Para más información sobre Azure Load Balancer, consulte [¿Qué es Azure Load Balancer?](#) y [Preguntas frecuentes de Load Balancer](#).

Más información sobre [Load Balancer y zonas de disponibilidad](#).

Inicio rápido: Creación de un equilibrador de carga público para equilibrar la carga de las VM con Azure PowerShell

23/09/2020 • 37 minutes to read • [Edit Online](#)

Comience a usar Azure Load Balancer mediante Azure PowerShell para crear un equilibrador de carga público y tres máquinas virtuales.

Requisitos previos

- Una cuenta de Azure con una suscripción activa. [Cree una cuenta gratuita](#).
- Azure PowerShell instalado localmente o Azure Cloud Shell




NOTE

Este artículo se ha actualizado para usar el nuevo módulo Az de Azure PowerShell. Aún puede usar el módulo de AzureRM que continuará recibiendo correcciones de errores hasta diciembre de 2020 como mínimo. Para más información acerca del nuevo módulo Az y la compatibilidad con AzureRM, consulte [Introducing the new Azure PowerShell Az module](#) (Presentación del nuevo módulo Az de Azure PowerShell). Para obtener instrucciones sobre la instalación del módulo Az, consulte [Instalación de Azure PowerShell](#).

Uso de Azure Cloud Shell

En Azure se hospeda Azure Cloud Shell, un entorno de shell interactivo que puede utilizar mediante el explorador. Puede usar Bash o PowerShell con Cloud Shell para trabajar con los servicios de Azure. Puede usar los comandos preinstalados de Cloud Shell para ejecutar el código de este artículo sin tener que instalar nada en su entorno local.

Para iniciar Azure Cloud Shell:

OPCIÓN	EJEMPLO O VÍNCULO
Seleccione Pruébalo en la esquina superior derecha de un bloque de código. Solo con seleccionar Pruébalo no se copia automáticamente el código en Cloud Shell.	
Vaya a https://shell.azure.com o seleccione el botón Iniciar Cloud Shell para abrir Cloud Shell en el explorador.	
Seleccione el botón Cloud Shell en la barra de menús de la esquina superior derecha de Azure Portal .	

Para ejecutar el código de este artículo en Azure Cloud Shell:

1. Inicie Cloud Shell.
2. Seleccione el botón **Copiar** de un bloque de código para copiar el código.
3. Pegue el código en la sesión de Cloud Shell. Para ello, seleccione **Ctrl+Mayús+V** en Windows y Linux, o bien seleccione **Cmd+Mayús+V** en macOS.

4. Seleccione **Entrar** para ejecutar el código.

Si decide instalar y usar PowerShell de forma local, para realizar los pasos de este artículo necesita la versión 5.4.1 del módulo de Azure PowerShell o cualquier versión posterior. Ejecute `Get-Module -ListAvailable Az` para buscar la versión instalada. Si necesita actualizarla, consulte [Instalación del módulo de Azure PowerShell](#). Si PowerShell se ejecuta localmente, también debe ejecutar `Connect-AzAccount` para crear una conexión con Azure.

Crear un grupo de recursos

Un grupo de recursos de Azure es un contenedor lógico en el que se implementan y se administran los recursos de Azure.

Cree un grupo de recursos con [New-AzResourceGroup](#):

- Denominado **myResourceGroupLB**.
- En la ubicación **eastus**.

```
## Variables for the command ##
$rg = 'MyResourceGroupLB'
$loc = 'eastus'

New-AzResourceGroup -Name $rg -Location $loc
```

- [SKU Estándar](#)
- [SKU básica](#)

NOTE

Se recomienda usar la SKU Estándar de Load Balancer para las cargas de trabajo de producción. Para más información sobre las SKU, consulte [SKU de Azure Load Balancer](#).

Crear una dirección IP pública

Para obtener acceso a la aplicación web en Internet, necesita una dirección IP pública para el equilibrador de carga.

Use [New-AzPublicIpAddress](#) para:

- Crear una dirección IP pública con redundancia de zona estándar denominada **myPublicIP**.
- En **myResourceGroupLB**.

```
## Variables for the command ##
$rg = 'MyResourceGroupLB'
$loc = 'eastus'
$pubIP = 'myPublicIP'
$sku = 'Standard'
$all = 'static'

$publicIp =
New-AzPublicIpAddress -ResourceGroupName $rg -Name $pubIP -Location $loc -AllocationMethod $all -SKU $sku
```

Para crear una dirección IP pública de zona en la zona 1, utilice el comando siguiente.

```
## Variables for the command ##
$rg = 'MyResourceGroupLB'
$loc = 'eastus'
$pubIP = 'myPublicIP'
$sku = 'Standard'
$all = 'static'

$publicIp =
New-AzPublicIpAddress -ResourceGroupName $rg -Name $pubIP -Location $loc -AllocationMethod $all -SKU $sku -
zone 1
```

Creación de un equilibrador de carga estándar

En esta sección se detalla cómo se pueden crear y configurar los componentes siguientes del equilibrador de carga:

- Un grupo de direcciones IP de front-end que recibe el tráfico de red entrante en el equilibrador de carga.
- Un grupo de direcciones IP de back-end al que el grupo de servidores front-end envía el tráfico de red de carga equilibrada.
- Un sondeo de estado que determina el estado de las instancias de máquina virtual de back-end.
- Una regla de equilibrador de carga que define cómo se distribuye el tráfico a las VM.

Creación de la dirección IP de front-end

Cree una dirección IP de front-end con [New-AzLoadBalancerFrontendIpConfig](#):

- Denominada **mi FrontEnd**.
- Conectada a la dirección IP pública **myPublicIP**.

```
## Variables for the commands ##
$fe = 'myFrontEnd'
$rg = 'MyResourceGroupLB'
$loc = 'eastus'
$pubIP = 'myPublicIP'

$publicIp =
Get-AzPublicIpAddress -Name $pubIP -ResourceGroupName $rg

$feip =
New-AzLoadBalancerFrontendIpConfig -Name $fe -PublicIpAddress $publicIp
```

Configuración del grupo de direcciones de back-end

Cree un grupo de direcciones de back-end con [New-AzLoadBalancerBackendAddressPoolConfig](#):

- Denominado **myBackEndPool**.
- En el resto de los pasos, las máquinas virtuales se conectan a este grupo back-end.

```
## Variable for the command ##
$be = 'myBackEndPool'

$bepool =
New-AzLoadBalancerBackendAddressPoolConfig -Name $be
```

Creación del sondeo de estado

Los sondeos de estado comprueban todas las instancias de máquina virtual para asegurarse de que pueden enviar tráfico de red.

Una máquina virtual con una comprobación de sondeo con errores se quita del equilibrador de carga. La máquina

virtual se agrega de nuevo al equilibrador de carga cuando se resuelve el error.

Cree un sondeo de estado con [Add-AzLoadBalancerProbeConfig](#):

- Supervisa el estado de las máquinas virtuales.
- Denominado **myHealthProbe**.
- Protocolo TCP.
- **Puerto 80** de supervisión.

```
## Variables for the command ##
$hp = 'myHealthProbe'
$pro = 'http'
$port = '80'
$int = '360'
$cnt = '5'

$probe =
New-AzLoadBalancerProbeConfig -Name $hp -Protocol $pro -Port $port -RequestPath / -IntervalInSeconds $int -
ProbeCount $cnt
```

Creación de la regla de equilibrador de carga

Una regla de equilibrador de carga define:

- La configuración de IP del front-end para el tráfico entrante.
- El grupo de IP de back-end para recibir el tráfico.
- Los puertos de origen y de destino requeridos.

Cree una regla del equilibrador de carga con [Add-AzLoadBalancerRuleConfig](#):

- Denominada **myHTTPRule**.
- Que escuche en el **puerto 80** en el grupo de front-end **myFrontEnd**.
- Que envíe el tráfico de red con equilibrio de carga al grupo de direcciones de back-end **myBackEndPool** a través del **Puerto 80**.
- Mediante el sondeo de estado **myHealthProbe**.
- Protocolo TCP.

```
## Variables for the command ##
$lbr = 'myHTTPRule'
$pro = 'tcp'
$port = '80'

## $feip and $bePool are the variables from previous steps. ##

$rule =
New-AzLoadBalancerRuleConfig -Name $lbr -Protocol $pro -Probe $probe -FrontendPort $port -BackendPort $port -
FrontendIpConfiguration $feip -BackendAddressPool $bePool -DisableOutboundSNAT
```

Creación de un recurso de equilibrador de carga

Cree un equilibrador de carga público con [New-AzLoadBalancer](#):

- Denominado **myLoadBalancer**.
- En **eastus**.
- En el grupo de recursos **myResourceGroupLB**.

```
## Variables for the command ##
$lb = 'myLoadBalancer'
$rg = 'myResourceGroupLB'
$loc = 'eastus'
$sku = 'Standard'

## $feip, $bepool, $probe, $rule are variables with configuration information from previous steps. ##

$lb =
New-AzLoadBalancer -ResourceGroupName $rg -Name $lb -SKU $sku -Location $loc -FrontendIpConfiguration $feip -
BackendAddressPool $bepool -Probe $probe -LoadBalancingRule $rule
```

Configurar la red virtual

Antes de implementar las VM y probar el equilibrador de carga, cree los recursos de red virtual auxiliares.

Creación de una red virtual

Cree una red virtual con [New-AzVirtualNetwork](#):

- Denominada **myVNet**.
- En el grupo de recursos **myResourceGroupLB**.
- Subred denominada **MyBackendSubnet**.
- Red virtual **10.0.0.0/16**.
- Subred **10.0.0.0/24**.

```
## Variables for the command ##
$rg = 'myResourceGroupLB'
$loc = 'eastus'
$sub = 'myBackendSubnet'
$spfx = '10.0.0.0/24'
$vnrm = 'myVNet'
$vpfx = '10.0.0.0/16'

## Create backend subnet config ##
$subnetConfig =
New-AzVirtualNetworkSubnetConfig -Name $sub -AddressPrefix $spfx

## Create the virtual network ##
$vnet =
New-AzVirtualNetwork -ResourceGroupName $rg -Location $loc -Name $vnrm -AddressPrefix $vpfx -Subnet
$subnetConfig
```

Creación de un grupo de seguridad de red

Cree un grupo de seguridad de red para definir las conexiones entrantes a la red virtual.

Creación de una regla de grupo de seguridad de red para el puerto 80

Cree una regla de grupo de seguridad de red con [New-AzNetworkSecurityRuleConfig](#):

- Denominada **myNSGRuleHTTP**.
- Descripción de **Allow HTTP**.
- Acceso de **Allow**.
- Protocolo **(*)**.
- Dirección **Inbound**.
- Prioridad **2000**.
- Origen de **Internet**.
- Intervalo de puertos de origen de **(*)**.

- Prefijo de dirección de destino (*) .
- Puerto de destino 80.

```
## Variables for command ##
$nm = 'myNSGRuleHTTP'
$des = 'Allow HTTP'
$acc = 'Allow'
$pro = '*'
$dir = 'Inbound'
$pri = '2000'
$spfx = 'Internet'
$spr = '*'
$dpr = '*'

$rule1 =
New-AzNetworkSecurityRuleConfig -Name $nm -Description $des -Access $acc -Protocol $pro -Direction $dir -
Priority $pri -SourceAddressPrefix $spfx -SourcePortRange $spr -DestinationAddressPrefix $dpr -
DestinationPortRange $dpr
```

Crear un grupo de seguridad de red

Cree un grupo de seguridad de red con [New-AzNetworkSecurityGroup](#):

- Denominado **myNSG**.
- En el grupo de recursos **myResourceGroupLB**.
- En la ubicación **eastus**.
- Con las reglas de seguridad creadas en los pasos anteriores almacenadas en una variable.

```
## Variables for command ##
$rg = 'myResourceGroupLB'
$loc = 'eastus'
$nmn = 'myNSG'

## $rule1 contains configuration information from the previous steps. ##
$nsg =
New-AzNetworkSecurityGroup -ResourceGroupName $rg -Location $loc -Name $nmn -SecurityRules $rule1
```

Creación de interfaces de red

Cree tres interfaces de red con [New-AzNetworkInterface](#):

VM 1

- Denominada **myNicVM1**.
- En el grupo de recursos **myResourceGroupLB**.
- En la ubicación **eastus**.
- En la red virtual **myVNet**.
- En la subred **myBackendSubnet**.
- En el grupo de seguridad de red **myNSG**.
- Conectada al equilibrador de carga **myLoadBalancer** en **myBackEndPool**.

```
## Variables for command ##
$rg = 'myResourceGroupLB'
$loc = 'eastus'
$nic1 = 'myNicVM1'
$vnt = 'myVNet'
$lb = 'myLoadBalancer'
$ngn = 'myNSG'

## Command to get virtual network configuration. ##
$vnet =
Get-AzVirtualNetwork -Name $vnt -ResourceGroupName $rg

## Command to get load balancer configuration
$bepool =
Get-AzLoadBalancer -Name $lb -ResourceGroupName $rg | Get-AzLoadBalancerBackendAddressPoolConfig

## Command to get network security group configuration ##
$nsg =
Get-AzNetworkSecurityGroup -Name $ngn -ResourceGroupName $rg

## Command to create network interface for VM1 ##
$nicVM1 =
New-AzNetworkInterface -ResourceGroupName $rg -Location $loc -Name $nic1 -LoadBalancerBackendAddressPool
$bepool -NetworkSecurityGroup $nsg -Subnet $vnet.Subnets[0]
```

VM 2

- Denominada **myNicVM2**.
- En el grupo de recursos **myResourceGroupLB**.
- En la ubicación **eastus**.
- En la red virtual **myVNet**.
- En la subred **myBackendSubnet**.
- En el grupo de seguridad de red **myNSG**.
- Conectada al equilibrador de carga **myLoadBalancer** en **myBackEndPool**.

```
## Variables for command ##
$rg = 'myResourceGroupLB'
$loc = 'eastus'
$nic2 = 'myNicVM2'
$vnt = 'myVNet'
$lb = 'myLoadBalancer'
$ngn = 'myNSG'

## Command to get virtual network configuration. ##
$vnet =
Get-AzVirtualNetwork -Name $vnt -ResourceGroupName $rg

## Command to get load balancer configuration
$bepool =
Get-AzLoadBalancer -Name $lb -ResourceGroupName $rg | Get-AzLoadBalancerBackendAddressPoolConfig

## Command to get network security group configuration ##
$nsg =
Get-AzNetworkSecurityGroup -Name $ngn -ResourceGroupName $rg

## Command to create network interface for VM2 ##
$nicVM2 =
New-AzNetworkInterface -ResourceGroupName $rg -Location $loc -Name $nic2 -LoadBalancerBackendAddressPool
$bepool -NetworkSecurityGroup $nsg -Subnet $vnet.Subnets[0]
```

VM 3

- Denominada **myNicVM3**.

- En el grupo de recursos **myResourceGroupLB**.
- En la ubicación **eastus**.
- En la red virtual **myVNet**.
- En la subred **myBackendSubnet**.
- En el grupo de seguridad de red **myNSG**.
- Conectada al equilibrador de carga **myLoadBalancer** en **myBackEndPool**.

```
## Variables for command ##
$rg = 'myResourceGroupLB'
$loc = 'eastus'
$nic3 = 'myNicVM3'
$vnt = 'myVNet'
$lb = 'myLoadBalancer'
$ngn = 'myNSG'

## Command to get virtual network configuration. ##
$vnet =
Get-AzVirtualNetwork -Name $vnt -ResourceGroupName $rg

## Command to get load balancer configuration
$bepool =
Get-AzLoadBalancer -Name $lb -ResourceGroupName $rg | Get-AzLoadBalancerBackendAddressPoolConfig

## Command to get network security group configuration ##
$nsg =
Get-AzNetworkSecurityGroup -Name $ngn -ResourceGroupName $rg

## Command to create network interface for VM3 ##
$nicVM3 =
New-AzNetworkInterface -ResourceGroupName $rg -Location $loc -Name $nic3 -LoadBalancerBackendAddressPool
$bepool -NetworkSecurityGroup $nsg -Subnet $vnet.Subnets[0]
```

Creación de máquinas virtuales

Establezca un nombre de usuario de administrador y una contraseña para las máquinas virtuales con [Get-Credential](#):

```
$cred = Get-Credential
```

Cree las máquinas virtuales con:

- [New-AzVM](#)
- [New-AzVMConfig](#)
- [Set-AzVMOperatingSystem](#)
- [Set-AzVMSourceImage](#)
- [Add-AzVMNetworkInterface](#)

VM1

- Denominada **myVM1**.
- En el grupo de recursos **myResourceGroupLB**.
- Conectada a la interfaz de red **myNicVM1**.
- Conectada al equilibrador de carga **myLoadBalancer**.
- En **Zona 1**.
- En la ubicación **eastus**.

```
## Variables used for command. ##
$rg = 'myResourceGroupLB'
$vm = 'myVM1'
$siz = 'Standard_DS1_v2'
$pub = 'MicrosoftWindowsServer'
$off = 'WindowsServer'
$sku = '2019-Datacenter'
$ver = 'latest'
$zn = '1'
$loc = 'eastus'

## Create a virtual machine configuration. $cred and $nicVM1 are variables with configuration from the
previous steps. ##

$vmConfig =
New-AzVMConfig -VMName $vm -VMSize $siz | Set-AzVMOperatingSystem -Windows -ComputerName $vm -Credential $cred
| Set-AzVMSourceImage -PublisherName $pub -Offer WindowsServer -Skus $sku -Version $ver | Add-
AzVMNetworkInterface -Id $nicVM1.Id

## Create the virtual machine ##
New-AzVM -ResourceGroupName $rg -Zone $zn -Location $loc -VM $vmConfig
```

VM2

- Denominada **myVM2**.
- En el grupo de recursos **myResourceGroupLB**.
- Conectada a la interfaz de red **myNicVM2**.
- Conectada al equilibrador de carga **myLoadBalancer**.
- En **Zona 2**.
- En la ubicación **eastus**.

```
## Variables used for command. ##
$rg = 'myResourceGroupLB'
$vm = 'myVM2'
$siz = 'Standard_DS1_v2'
$pub = 'MicrosoftWindowsServer'
$off = 'WindowsServer'
$sku = '2019-Datacenter'
$ver = 'latest'
$zn = '2'
$loc = 'eastus'

## Create a virtual machine configuration. $cred and $nicVM2 are variables with configuration from the
previous steps. ##

$vmConfig =
New-AzVMConfig -VMName $vm -VMSize $siz | Set-AzVMOperatingSystem -Windows -ComputerName $vm -Credential $cred
| Set-AzVMSourceImage -PublisherName $pub -Offer WindowsServer -Skus $sku -Version $ver | Add-
AzVMNetworkInterface -Id $nicVM2.Id

## Create the virtual machine ##
New-AzVM -ResourceGroupName $rg -Zone $zn -Location $loc -VM $vmConfig
```

VM3

- Denominada **myVM3**.
- En el grupo de recursos **myResourceGroupLB**.
- Conectada a la interfaz de red **myNicVM3**.
- Conectada al equilibrador de carga **myLoadBalancer**.
- En **Zona 3**.
- En la ubicación **eastus**.


```
## Variables used for command. ##
$rg = 'myResourceGroupLB'
$vm = 'myVM3'
$siz = 'Standard_DS1_v2'
$pub = 'MicrosoftWindowsServer'
$off = 'WindowsServer'
$sku = '2019-Datacenter'
$ver = 'latest'
$zn = '3'
$loc = 'eastus'

## Create a virtual machine configuration. $cred and $nicVM3 are variables with configuration from the
previous steps. ##

$vmConfig =
New-AzVMConfig -VMName $vm -VMSize $siz | Set-AzVMOperatingSystem -Windows -ComputerName $vm -Credential $cred
| Set-AzVMSourceImage -PublisherName $pub -Offer WindowsServer -Skus $sku -Version $ver | Add-
AzVMNetworkInterface -Id $nicVM3.Id

## Create the virtual machine ##
New-AzVM -ResourceGroupName $rg -Zone $zn -Location $loc -VM $vmConfig
```

Creación de la configuración de regla de salida

Las reglas de salida del equilibrador de carga configuran la traducción de direcciones de red (SNAT) saliente para las VM del grupo de back-end.

Para obtener más información sobre las conexiones salientes, consulte [Conexiones salientes en Azure](#).

Creación de una dirección IP pública de salida

Use [New-AzPublicIpAddress](#) para:

- Cree una dirección IP pública con redundancia de zona estándar denominada **myPublicIPOutbound**.
- En **myResourceGroupLB**.

```
## Variables for the command ##
$rg = 'MyResourceGroupLB'
$loc = 'eastus'
$pubIP = 'myPublicIPOutbound'
$sku = 'Standard'
$all = 'static'

$publicIp =
New-AzPublicIpAddress -ResourceGroupName $rg -Name $pubIP -Location $loc -AllocationMethod $all -SKU $sku
```

Para crear una dirección IP pública de zona en la zona 1, utilice el comando siguiente.

```
## Variables for the command ##
$rg = 'MyResourceGroupLB'
$loc = 'eastus'
$pubIP = 'myPublicIPOutbound'
$sku = 'Standard'
$all = 'static'

$publicIp =
New-AzPublicIpAddress -ResourceGroupName $rg -Name $pubIP -Location $loc -AllocationMethod $all -SKU $sku -
zone 1
```

Creación de una configuración de direcciones IP de front-end de salida

Cree una nueva configuración de IP de front-end con [Add-AzLoadBalancerFrontendIPConfig](#):

- Denominada **myFrontEndOutbound**.
- Asociada a la dirección IP pública **myPublicIPOutbound**.

```
## Variables for the command ##
$fen = 'myFrontEndOutbound'
$lbn = 'myLoadBalancer'

## Get the load balancer configuration and apply the frontend config##
Get-AzLoadBalancer -Name $lbn -ResourceGroupName $rg | Add-AzLoadBalancerFrontendIPConfig -Name $fen -
PublicIpAddress $publicIP | Set-AzLoadBalancer
```

Creación del grupo de salida

Cree un nuevo grupo de salida con [Add-AzLoadBalancerBackendAddressPoolConfig](#).

Aplique el grupo y la dirección IP de front-end al equilibrador de carga con [Set-AzLoadBalancer](#):

- Denominado **myBackendPoolOutbound**.

```
## Variables for the command ##
$ben = 'myBackEndPoolOutbound'
$lbn = 'myLoadBalancer'
$rg = 'myResourceGroupLB'

## Get the load balancer configuration and create the outbound backend address pool##
Get-AzLoadBalancer -Name $lbn -ResourceGroupName $rg | Add-AzLoadBalancerBackendAddressPoolConfig -Name $ben |
Set-AzLoadBalancer
```

Creación de una regla de salida y aplicación en el equilibrador de carga

Cree una nueva regla de salida para el grupo de back-end de salida con [Add-AzLoadBalancerOutboundRuleConfig](#).

Aplique la regla en el equilibrador de carga con [Set-AzLoadBalancer](#):

- Denominada **myOutboundRule**.
- Asociada al equilibrador de carga **myLoadBalancer**.
- Asociada al front-end **myFrontEndOutbound**.
- Protocolo **All**.
- Tiempo de espera de inactividad de **15**.
- **10000** puertos de salida.
- Asociada al grupo de back-end **myBackEndPoolOutbound**.
- En el grupo de recursos **myResourceGroupLB**.

```
## Variables for the commands ##
$rg = 'myResourceGroupLB'
$lbn = 'myLoadBalancer'
$brn = 'myOutboundRule'
$pro = 'All'
$idl = '15'
$por = '10000'

## Get the load balancer configuration ##
$lb =
Get-AzLoadBalancer -Name $lbn -ResourceGroupName $rg

## Apply the outbound rule configuration to the load balancer. ##
$lb | Add-AzLoadBalancerOutBoundRuleConfig -Name $brn -FrontendIPConfiguration $lb.FrontendIpConfigurations[1]
-BackendAddressPool $lb.BackendAddressPools[1] -Protocol $pro -IdleTimeoutInMinutes $idl -
AllocatedOutboundPort $por | Set-AzLoadBalancer
```

Adición de máquinas virtuales al grupo de salida

Agregue las interfaces de red de máquina virtual al grupo de salida del equilibrador de carga con [Add-AzNetworkInterfaceConfig](#):

VM1

- En el grupo de direcciones de back-end **myBackEndPoolOutbound**.
- En el grupo de recursos **myResourceGroupLB**.
- Asociada a la interfaz de red **myNicVM1** e **ipconfig1**.
- Asociada al equilibrador de carga **myLoadBalancer**.

```
## Variables for the commands ##
$rg = 'myResourceGroupLB'
$lbn = 'myLoadBalancer'
$bep = 'myBackEndPoolOutbound'
$nic1 = 'myNicVM1'
$ipc = 'ipconfig1'

## Get the load balancer configuration ##
$lb =
Get-AzLoadBalancer -Name $lbn -ResourceGroupName $rg

## Get the network interface configuration ##
$nic =
Get-AzNetworkInterface -Name $nic1 -ResourceGroupName $rg

## Apply the backend to the network interface ##
$nic | Set-AzNetworkInterfaceIpConfig -Name $ipc -LoadBalancerBackendAddressPoolId
$lb.BackendAddressPools[0].id,$lb.BackendAddressPools[1].id | Set-AzNetworkInterface
```

VM2

- En el grupo de direcciones de back-end **myBackEndPoolOutbound**.
- En el grupo de recursos **myResourceGroupLB**.
- Asociada a la interfaz de red **myNicVM2** e **ipconfig1**.
- Asociada al equilibrador de carga **myLoadBalancer**.

```
## Variables for the commands ##
$rg = 'myResourceGroupLB'
$lbn = 'myLoadBalancer'
$bep = 'myBackEndPoolOutbound'
$nic2 = 'myNicVM2'
$ipc = 'ipconfig1'

## Get the load balancer configuration ##
$lb =
Get-AzLoadBalancer -Name $lbn -ResourceGroupName $rg

## Get the network interface configuration ##
$nic =
Get-AzNetworkInterface -Name $nic2 -ResourceGroupName $rg

## Apply the backend to the network interface ##
$nic | Set-AzNetworkInterfaceIpConfig -Name $ipc -LoadBalancerBackendAddressPoolId
$lb.BackendAddressPools[0].id,$lb.BackendAddressPools[1].id | Set-AzNetworkInterface
```

VM3

- En el grupo de direcciones de back-end **myBackEndPoolOutbound**.
- En el grupo de recursos **myResourceGroupLB**.
- Asociada a la interfaz de red **myNicVM3** e **ipconfig1**.
- Asociada al equilibrador de carga **myLoadBalancer**.

```
## Variables for the commands ##
$rg = 'myResourceGroupLB'
$lbn = 'myLoadBalancer'
$bep = 'myBackEndPoolOutbound'
$nic3 = 'myNicVM3'
$ipc = 'ipconfig1'

## Get the load balancer configuration ##
$lb =
Get-AzLoadBalancer -Name $lbn -ResourceGroupName $rg

## Get the network interface configuration ##
$nic =
Get-AzNetworkInterface -Name $nic3 -ResourceGroupName $rg

## Apply the backend to the network interface ##
$nic | Set-AzNetworkInterfaceIpConfig -Name $ipc -LoadBalancerBackendAddressPoolId
$lb.BackendAddressPools[0].id,$lb.BackendAddressPools[1].id | Set-AzNetworkInterface
```

Instalación de IIS

Use [Set-AzVMExtension](#) para instalar la extensión de script personalizado.

La extensión ejecuta Add-WindowsFeature Web-Server de PowerShell para instalar el servidor web IIS y después actualiza la página Default.htm para mostrar el nombre de host de la máquina virtual:

VM1

```
## Variables for command. ##
$rg = 'myResourceGroupLB'
$enm = 'IIS'
$vmn = 'myVM1'
$loc = 'eastus'
$pub = 'Microsoft.Compute'
$ext = 'CustomScriptExtension'
$typ = '1.8'

Set-AzVMExtension -ResourceGroupName $rg -ExtensionName $enm -VMName $vmn -Location $loc -Publisher $pub -
ExtensionType $ext -TypeHandlerVersion $typ -SettingString '{"commandToExecute":"powershell Add-WindowsFeature
Web-Server; powershell Add-Content -Path `C:\\inetpub\\wwwroot\\Default.htm\" -Value $($env:computername)}'
```

VM2

```
## Variables for command. ##
$rg = 'myResourceGroupLB'
$enm = 'IIS'
$vmn = 'myVM2'
$loc = 'eastus'
$pub = 'Microsoft.Compute'
$ext = 'CustomScriptExtension'
$typ = '1.8'

Set-AzVMExtension -ResourceGroupName $rg -ExtensionName $enm -VMName $vmn -Location $loc -Publisher $pub -
ExtensionType $ext -TypeHandlerVersion $typ -SettingString '{"commandToExecute":"powershell Add-WindowsFeature
Web-Server; powershell Add-Content -Path `C:\\inetpub\\wwwroot\\Default.htm\" -Value $($env:computername)}'
```

VM3

```
## Variables for command. ##
$rg = 'myResourceGroupLB'
$enm = 'IIS'
$vmn = 'myVM3'
$loc = 'eastus'
$pub = 'Microsoft.Compute'
$ext = 'CustomScriptExtension'
$typ = '1.8'

Set-AzVMExtension -ResourceGroupName $rg -ExtensionName $enm -VMName $vmn -Location $loc -Publisher $pub -
ExtensionType $ext -TypeHandlerVersion $typ -SettingString '{"commandToExecute":"powershell Add-WindowsFeature
Web-Server; powershell Add-Content -Path `C:\\inetpub\\wwwroot\\Default.htm\" -Value $($env:computername)}'
```

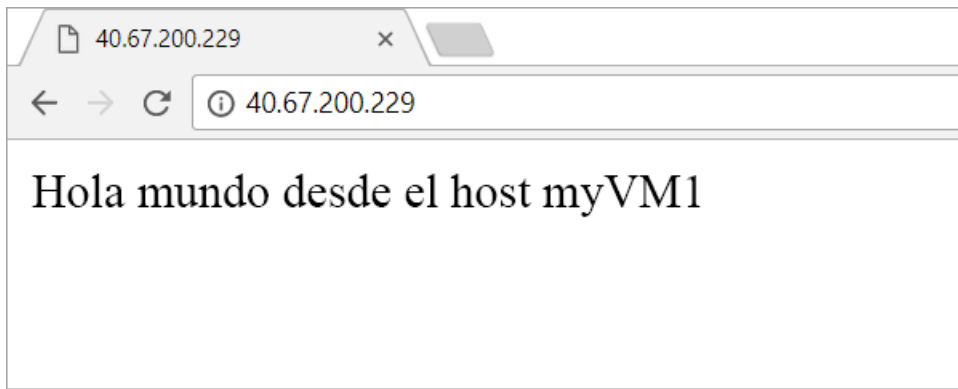
Prueba del equilibrador de carga

Use [Get-AzPublicIpAddress](#) para obtener la dirección IP pública del equilibrador de carga:

```
## Variables for command. ##
$rg = 'myResourceGroupLB'
$ipn = 'myPublicIP'

Get-AzPublicIpAddress -ResourceGroupName $rg -Name $ipn | select IPAddress
```

Copie la dirección IP pública y péguela en la barra de direcciones del explorador. La página predeterminada del servidor web de IIS se muestra en el explorador.



Para ver el tráfico distribuido por Load Balancer entre las tres máquinas virtuales, puede personalizar la página predeterminada de cada servidor web IIS de las máquinas virtuales y luego forzar una actualización del explorador web desde el equipo cliente.

Limpieza de recursos

Cuando ya no los necesite, puede usar el comando [Remove-AzResourceGroup](#) para quitar el grupo de recursos, el equilibrador de carga y el resto de los recursos.

```
## Variable for command. ##  
$rg = 'myResourceGroupLB'  
  
Remove-AzResourceGroup -Name $rg
```

Pasos siguientes

En esta guía de inicio rápido

- Creó un equilibrador de carga público básico o estándar.
- Conectó máquinas virtuales.
- Configuró la regla de tráfico del equilibrador de carga y el sondeo de estado.
- Probó el equilibrador de carga.

Para más información sobre Azure Load Balancer, consulte [¿Qué es Azure Load Balancer?](#) y [Preguntas frecuentes de Load Balancer](#).

- Más información sobre [Load Balancer y zonas de disponibilidad](#).

Inicio rápido: Creación de un equilibrador de carga público para equilibrar la carga de las VM con la CLI de Azure

23/09/2020 • 33 minutes to read • [Edit Online](#)

Comience a usar Azure Load Balancer con la CLI de Azure para crear un equilibrador de carga público y tres máquinas virtuales.




Requisitos previos

- Una cuenta de Azure con una suscripción activa. [Cree una cuenta gratuita](#).
- CLI de Azure instalada localmente o Azure Cloud Shell

Uso de Azure Cloud Shell

En Azure se hospeda Azure Cloud Shell, un entorno de shell interactivo que puede utilizar mediante el explorador. Puede usar Bash o PowerShell con Cloud Shell para trabajar con los servicios de Azure. Puede usar los comandos preinstalados de Cloud Shell para ejecutar el código de este artículo sin tener que instalar nada en su entorno local.

Para iniciar Azure Cloud Shell:

OPCIÓN	EJEMPLO O VÍNCULO
Seleccione Pruébalo en la esquina superior derecha de un bloque de código. Solo con seleccionar Pruébalo no se copia automáticamente el código en Cloud Shell.	
Vaya a https://shell.azure.com o seleccione el botón Iniciar Cloud Shell para abrir Cloud Shell en el explorador.	
Seleccione el botón Cloud Shell en la barra de menús de la esquina superior derecha de Azure Portal .	

Para ejecutar el código de este artículo en Azure Cloud Shell:

1. Inicie Cloud Shell.
2. Seleccione el botón **Copiar** de un bloque de código para copiar el código.
3. Pegue el código en la sesión de Cloud Shell. Para ello, seleccione **Ctrl+Mayús+V** en Windows y Linux, o bien seleccione **Cmd+Mayús+V** en macOS.
4. Seleccione **Entrar** para ejecutar el código.

Si decide instalar y usar la CLI localmente, para esta guía de inicio rápido se necesita la versión 2.0.28 de la CLI de Azure o una versión posterior. Para encontrar la versión, ejecute `az --version`. Si necesita instalarla o actualizarla, consulte [Instalación de la CLI de Azure](#).

Crear un grupo de recursos

Un grupo de recursos de Azure es un contenedor lógico en el que se implementan y se administran los recursos de Azure.

Cree un grupo de recursos con [az group create](#):

- Denominado **myResourceGroupLB**.
- En la ubicación **eastus**.

```
az group create \  
  --name myResourceGroupLB \  
  --location eastus
```

- [SKU Estándar](#)
- [SKU básica](#)

NOTE

Se recomienda usar la SKU Estándar de Load Balancer para las cargas de trabajo de producción. Para más información sobre las SKU, consulte [SKU de Azure Load Balancer](#).

Configurar la red virtual

Antes de implementar las VM y probar el equilibrador de carga, cree los recursos de red virtual auxiliares.

Creación de una red virtual

Cree una red virtual con [az network vnet create](#):

- Denominada **myVNet**.
- Con el prefijo de dirección **10.1.0.0/16**.
- Subred denominada **MyBackendSubnet**.
- Con el prefijo de subred **10.1.0.0/24**.
- En el grupo de recursos **myResourceGroupLB**.
- Ubicación de **eastus**.

```
az network vnet create \  
  --resource-group myResourceGroupLB \  
  --location eastus \  
  --name myVNet \  
  --address-prefixes 10.1.0.0/16 \  
  --subnet-name myBackendSubnet \  
  --subnet-prefixes 10.1.0.0/24
```

Crear un grupo de seguridad de red

En el caso de un equilibrador de carga estándar, las VM de la dirección de back-end deben tener interfaces de red que pertenezcan a un grupo de seguridad de red.

Cree un grupo de seguridad de red con [az network nsg create](#):

- Denominado **myNSG**.
- En el grupo de recursos **myResourceGroupLB**.


```
az network nsg create \  
  --resource-group myResourceGroupLB \  
  --name myNSG
```

Creación de una regla de grupo de seguridad de red

Cree una regla de grupo de seguridad de red con el [az network nsg rule create](#):

- Denominada **myNSGRuleHTTP**.
- En el grupo de seguridad de red que creó en el paso anterior, **myNSG**.
- En el grupo de recursos **myResourceGroupLB**.
- Protocolo (*) .
- Dirección **Inbound**.
- Origen (*) .
- Destino: (*) .
- Puerto de destino **80**.
- Acceso: **Allow**.
- Prioridad **200**.

```
az network nsg rule create \  
  --resource-group myResourceGroupLB \  
  --nsg-name myNSG \  
  --name myNSGRuleHTTP \  
  --protocol '*' \  
  --direction inbound \  
  --source-address-prefix '*' \  
  --source-port-range '*' \  
  --destination-address-prefix '*' \  
  --destination-port-range 80 \  
  --access allow \  
  --priority 200
```

Creación de interfaces de red para las máquinas virtuales

Cree tres interfaces de red con [az network nic create](#):

VM1

- Denominada **myNicVM1**.
- En el grupo de recursos **myResourceGroupLB**.
- En la red virtual **myVNet**.
- En la subred **myBackendSubnet**.
- En el grupo de seguridad de red **myNSG**.

```
az network nic create \  
  --resource-group myResourceGroupLB \  
  --name myNicVM1 \  
  --vnet-name myVNet \  
  --subnet myBackEndSubnet \  
  --network-security-group myNSG
```

VM2

- Denominada **myNicVM2**.
- En el grupo de recursos **myResourceGroupLB**.
- En la red virtual **myVNet**.

- En la subred **myBackendSubnet**.

```
az network nic create \  
  --resource-group myResourceGroupLB \  
  --name myNicVM2 \  
  --vnet-name myVnet \  
  --subnet myBackEndSubnet \  
  --network-security-group myNSG
```

VM3

- Denominada **myNicVM3**.
- En el grupo de recursos **myResourceGroupLB**.
- En la red virtual **myVNet**.
- En la subred **myBackendSubnet**.
- En el grupo de seguridad de red **myNSG**.

```
az network nic create \  
  --resource-group myResourceGroupLB \  
  --name myNicVM3 \  
  --vnet-name myVnet \  
  --subnet myBackEndSubnet \  
  --network-security-group myNSG
```

Creación de servidores back-end

En esta sección, creará:

- Un archivo de configuración de nube denominado **cloud-init.txt** para la configuración del servidor.
- Tres máquinas virtuales que se usarán como servidores back-end para el equilibrador de carga.

Creación del archivo de configuración cloud-init

Use un archivo de configuración cloud-init para instalar NGINX y ejecutar una aplicación Node.js "Hola mundo" en una máquina virtual Linux.

En el shell actual, cree un archivo denominado cloud-init.txt. Copie el siguiente fragmento de código y péguelo en el shell. Asegúrese de copiar correctamente todo el archivo cloud-init, especialmente la primera línea:

```
#cloud-config
package_upgrade: true
packages:
- nginx
- nodejs
- npm
write_files:
- owner: www-data:www-data
- path: /etc/nginx/sites-available/default
  content: |
    server {
      listen 80;
      location / {
        proxy_pass http://localhost:3000;
        proxy_http_version 1.1;
        proxy_set_header Upgrade $http_upgrade;
        proxy_set_header Connection keep-alive;
        proxy_set_header Host $host;
        proxy_cache_bypass $http_upgrade;
      }
    }
- owner: azureuser:azureuser
- path: /home/azureuser/myapp/index.js
  content: |
    var express = require('express')
    var app = express()
    var os = require('os');
    app.get('/', function (req, res) {
      res.send('Hello World from host ' + os.hostname() + '!!')
    })
    app.listen(3000, function () {
      console.log('Hello world app listening on port 3000!')
    })
runcmd:
- service nginx restart
- cd "/home/azureuser/myapp"
- npm init
- npm install express -y
- nodejs index.js
```

Creación de máquinas virtuales

Cree las máquinas virtuales con [az vm create](#):

VM1

- Denominada **myVM1**.
- En el grupo de recursos **myResourceGroupLB**.
- Conectada a la interfaz de red **myNicVM1**.
- Imagen de máquina virtual **UbuntuLTS**.
- Archivo de configuración **cloud-init.txt** creado en el paso anterior.
- En **Zona 1**.

```
az vm create \
  --resource-group myResourceGroupLB \
  --name myVM1 \
  --nics myNicVM1 \
  --image UbuntuLTS \
  --generate-ssh-keys \
  --custom-data cloud-init.txt \
  --zone 1 \
  --no-wait
```

VM2

- Denominada **myVM2**.
- En el grupo de recursos **myResourceGroupLB**.
- Conectada a la interfaz de red **myNicVM2**.
- Imagen de máquina virtual **UbuntuLTS**.
- Archivo de configuración **cloud-init.txt** creado en el paso anterior.
- En **Zona 2**.

```
az vm create \
  --resource-group myResourceGroupLB \
  --name myVM2 \
  --nics myNicVM2 \
  --image UbuntuLTS \
  --generate-ssh-keys \
  --custom-data cloud-init.txt \
  --zone 2 \
  --no-wait
```

VM3

- Denominada **myVM3**.
- En el grupo de recursos **myResourceGroupLB**.
- Conectada a la interfaz de red **myNicVM3**.
- Imagen de máquina virtual **UbuntuLTS**.
- Archivo de configuración **cloud-init.txt** creado en el paso anterior.
- En **Zona 3**.

```
az vm create \
  --resource-group myResourceGroupLB \
  --name myVM3 \
  --nics myNicVM3 \
  --image UbuntuLTS \
  --generate-ssh-keys \
  --custom-data cloud-init.txt \
  --zone 3 \
  --no-wait
```

Puede que las VM tarden unos minutos en implementarse.

Crear una dirección IP pública

Para obtener acceso a la aplicación web en Internet, necesita una dirección IP pública para el equilibrador de carga.

Use [az network public-ip create](#) para:

- Crear una dirección IP pública con redundancia de zona estándar denominada **myPublicIP**.
- En **myResourceGroupLB**.

```
az network public-ip create \
  --resource-group myResourceGroupLB \
  --name myPublicIP \
  --sku Standard
```

Para crear una dirección IP pública con redundancia de zona en la Zona 1:

```
az network public-ip create \  
  --resource-group myResourceGroupLB \  
  --name myPublicIP \  
  --sku Standard \  
  --zone 1
```

Creación de un equilibrador de carga estándar

En esta sección se detalla cómo se pueden crear y configurar los componentes siguientes del equilibrador de carga:

- Un grupo de direcciones IP de front-end que recibe el tráfico de red entrante en el equilibrador de carga.
- Un grupo de direcciones IP de back-end al que el grupo de servidores front-end envía el tráfico de red de carga equilibrada.
- Un sondeo de estado que determina el estado de las instancias de máquina virtual de back-end.
- Una regla de equilibrador de carga que define cómo se distribuye el tráfico a las VM.

Creación del recurso del equilibrador de carga

Cree un equilibrador de carga público con [az network lb create](#):

- Denominado **myLoadBalancer**.
- Un grupo de front-end denominado **MyFrontEnd**.
- Un grupo de back-end denominado **myBackEndPool**
- Asociado a la dirección IP pública **myPublicIP** que creó en el paso anterior.

```
az network lb create \  
  --resource-group myResourceGroupLB \  
  --name myLoadBalancer \  
  --sku Standard \  
  --public-ip-address myPublicIP \  
  --frontend-ip-name myFrontEnd \  
  --backend-pool-name myBackEndPool
```

Creación del sondeo de estado

Los sondeos de estado comprueban todas las instancias de máquina virtual para asegurarse de que pueden enviar tráfico de red.

Una máquina virtual con una comprobación de sondeo con errores se quita del equilibrador de carga. La máquina virtual se agrega de nuevo al equilibrador de carga cuando se resuelve el error.

Cree un sondeo de estado con [az network lb probe create](#):

- Supervisa el estado de las máquinas virtuales.
- Denominado **myHealthProbe**.
- Protocolo TCP.
- **Puerto 80** de supervisión.

```
az network lb probe create \  
  --resource-group myResourceGroupLB \  
  --lb-name myLoadBalancer \  
  --name myHealthProbe \  
  --protocol tcp \  
  --port 80
```

Creación de la regla de equilibrador de carga

Una regla de equilibrador de carga define:

- La configuración de IP del front-end para el tráfico entrante.
- El grupo de IP de back-end para recibir el tráfico.
- Los puertos de origen y de destino requeridos.

Cree una regla de equilibrador de carga con [az network lb rule create](#):

- Denominada **myHTTPRule**.
- Que escuche en el **puerto 80** en el grupo de front-end **myFrontEnd**.
- Que envíe el tráfico de red con equilibrio de carga al grupo de direcciones de back-end **myBackEndPool** a través del **Puerto 80**.
- Mediante el sondeo de estado **myHealthProbe**.
- Protocolo **TCP**.
- Habilite la traducción de direcciones de red de origen (SNAT) de salida mediante la dirección IP de front-end.

```
az network lb rule create \  
  --resource-group myResourceGroupLB \  
  --lb-name myLoadBalancer \  
  --name myHTTPRule \  
  --protocol tcp \  
  --frontend-port 80 \  
  --backend-port 80 \  
  --frontend-ip-name myFrontEnd \  
  --backend-pool-name myBackEndPool \  
  --probe-name myHealthProbe \  
  --disable-outbound-snat true
```

Adición de máquinas virtuales al grupo de back-end del equilibrador de carga

Agregue las máquinas virtuales al grupo de back-end con [az network nic ip-config address-pool add](#):

VM1

- En el grupo de direcciones de back-end **myBackEndPool**.
- En el grupo de recursos **myResourceGroupLB**.
- Asociada a la interfaz de red **myNicVM1** e **ipconfig1**.
- Asociada al equilibrador de carga **myLoadBalancer**.

```
az network nic ip-config address-pool add \  
  --address-pool myBackendPool \  
  --ip-config-name ipconfig1 \  
  --nic-name myNicVM1 \  
  --resource-group myResourceGroupLB \  
  --lb-name myLoadBalancer
```

VM2

- En el grupo de direcciones de back-end **myBackEndPool**.
- En el grupo de recursos **myResourceGroupLB**.
- Asociada a la interfaz de red **myNicVM2** e **ipconfig1**.
- Asociada al equilibrador de carga **myLoadBalancer**.

```
az network nic ip-config address-pool add \  
  --address-pool myBackendPool \  
  --ip-config-name ipconfig1 \  
  --nic-name myNicVM2 \  
  --resource-group myResourceGroupLB \  
  --lb-name myLoadBalancer
```

VM3

- En el grupo de direcciones de back-end **myBackendPool**.
- En el grupo de recursos **myResourceGroupLB**.
- Asociada a la interfaz de red **myNicVM3** e **ipconfig1**.
- Asociada al equilibrador de carga **myLoadBalancer**.

```
az network nic ip-config address-pool add \  
  --address-pool myBackendPool \  
  --ip-config-name ipconfig1 \  
  --nic-name myNicVM3 \  
  --resource-group myResourceGroupLB \  
  --lb-name myLoadBalancer
```

Creación de la configuración de regla de salida

Las reglas de salida del equilibrador de carga configuran SNAT saliente para las máquinas virtuales del grupo de back-end.

Para obtener más información sobre las conexiones salientes, consulte [Conexiones salientes en Azure](#).

Cree una dirección IP pública de salida o un prefijo de dirección IP pública.

Use [az network public-ip create](#) para crear una única dirección IP para la conectividad saliente.

Use [az network public-ip prefix create](#) para crear un prefijo de dirección IP pública para la conectividad saliente.

Para obtener más información sobre el escalado de NAT de salida y la conectividad de salida, consulte [NAT de salida de escala con varias direcciones IP](#).

Dirección IP pública

- Denominada **myPublicIPOutbound**.
- En **myResourceGroupLB**.

```
az network public-ip create \  
  --resource-group myResourceGroupLB \  
  --name myPublicIPOutbound \  
  --sku Standard
```

Para crear una dirección IP pública con redundancia de zona en la Zona 1:

```
az network public-ip create \  
  --resource-group myResourceGroupLB \  
  --name myPublicIPOutbound \  
  --sku Standard \  
  --zone 1
```

Prefijo de IP pública

- Denominada **myPublicIPPrefixOutbound**.
- En **myResourceGroupLB**.

- Longitud del prefijo de 28.

```
az network public-ip prefix create \  
  --resource-group myResourceGroupLB \  
  --name myPublicIPPrefixOutbound \  
  --length 28
```

Para crear un prefijo de dirección IP pública con redundancia de zona en la Zona 1:

```
az network public-ip prefix create \  
  --resource-group myResourceGroupLB \  
  --name myPublicIPPrefixOutbound \  
  --length 28 \  
  --zone 1
```

Creación de una configuración de direcciones IP de front-end de salida

Cree una nueva configuración de IP de front-end con [az network lb frontend-ip create](#):

Seleccione los comandos de dirección IP pública o prefijo de dirección IP pública según la decisión del paso anterior.

Dirección IP pública

- Denominada **myFrontEndOutbound**.
- En el grupo de recursos **myResourceGroupLB**.
- Asociada a la dirección IP pública **myPublicIPOutbound**.
- Asociada al equilibrador de carga **myLoadBalancer**.

```
az network lb frontend-ip create \  
  --resource-group myResourceGroupLB \  
  --name myFrontEndOutbound \  
  --lb-name myLoadBalancer \  
  --public-ip-address myPublicIPOutbound
```

Prefijo de IP pública

- Denominada **myFrontEndOutbound**.
- En el grupo de recursos **myResourceGroupLB**.
- Asociado al prefijo de dirección IP pública **myPublicIPPrefixOutbound**.
- Asociada al equilibrador de carga **myLoadBalancer**.

```
az network lb frontend-ip create \  
  --resource-group myResourceGroupLB \  
  --name myFrontEndOutbound \  
  --lb-name myLoadBalancer \  
  --public-ip-prefix myPublicIPPrefixOutbound
```

Creación del grupo de salida

Cree un nuevo grupo de salida con [az network lb address-pools create](#):

- Denominado **myBackendPoolOutbound**.
- En el grupo de recursos **myResourceGroupLB**.
- Asociada al equilibrador de carga **myLoadBalancer**.


```
az network lb address-pool create \  
  --resource-group myResourceGroupLB \  
  --lb-name myLoadBalancer \  
  --name myBackendPoolOutbound
```

Creación de una regla de salida

Cree una nueva regla de salida para el grupo de back-end de salida con [az network lb outbound-rule create](#):

- Denominada **myOutboundRule**.
- En el grupo de recursos **myResourceGroupLB**.
- Asociada al equilibrador de carga **myLoadBalancer**.
- Asociada al front-end **myFrontEndOutbound**.
- Protocolo **All**.
- Tiempo de espera de inactividad de **15**.
- **10000** puertos de salida.
- Asociada al grupo de back-end **myBackEndPoolOutbound**.

```
az network lb outbound-rule create \  
  --resource-group myResourceGroupLB \  
  --lb-name myLoadBalancer \  
  --name myOutboundRule \  
  --frontend-ip-configs myFrontEndOutbound \  
  --protocol All \  
  --idle-timeout 15 \  
  --outbound-ports 10000 \  
  --address-pool myBackEndPoolOutbound
```

Adición de máquinas virtuales al grupo de salida

Agregue las máquinas virtuales al grupo de salida con [az network nic ip-config address-pool add](#):

VM1

- En el grupo de direcciones de back-end **myBackEndPoolOutbound**.
- En el grupo de recursos **myResourceGroupLB**.
- Asociada a la interfaz de red **myNicVM1** e **ipconfig1**.
- Asociada al equilibrador de carga **myLoadBalancer**.

```
az network nic ip-config address-pool add \  
  --address-pool myBackendPoolOutbound \  
  --ip-config-name ipconfig1 \  
  --nic-name myNicVM1 \  
  --resource-group myResourceGroupLB \  
  --lb-name myLoadBalancer
```

VM2

- En el grupo de direcciones de back-end **myBackEndPoolOutbound**.
- En el grupo de recursos **myResourceGroupLB**.
- Asociada a la interfaz de red **myNicVM2** e **ipconfig1**.
- Asociada al equilibrador de carga **myLoadBalancer**.

```
az network nic ip-config address-pool add \  
  --address-pool myBackendPoolOutbound \  
  --ip-config-name ipconfig1 \  
  --nic-name myNicVM2 \  
  --resource-group myResourceGroupLB \  
  --lb-name myLoadBalancer
```

VM3

- En el grupo de direcciones de back-end **myBackendPoolOutbound**.
- En el grupo de recursos **myResourceGroupLB**.
- Asociada a la interfaz de red **myNicVM3** e **ipconfig1**.
- Asociada al equilibrador de carga **myLoadBalancer**.

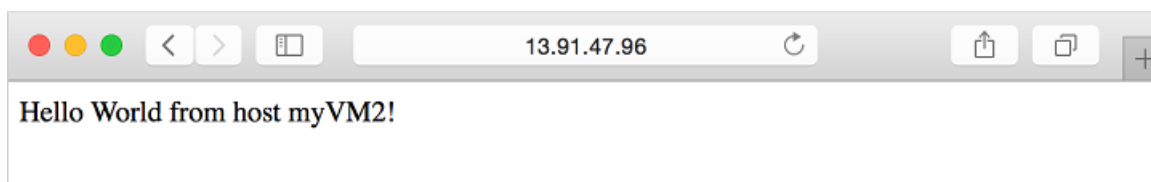
```
az network nic ip-config address-pool add \  
  --address-pool myBackendPoolOutbound \  
  --ip-config-name ipconfig1 \  
  --nic-name myNicVM3 \  
  --resource-group myResourceGroupLB \  
  --lb-name myLoadBalancer
```

Prueba del equilibrador de carga

Para obtener la dirección IP pública del equilibrador de carga, use [az network public-ip show](#).

Copie la dirección IP pública y péguela en la barra de direcciones del explorador.

```
az network public-ip show \  
  --resource-group myResourceGroupLB \  
  --name myPublicIP \  
  --query [ipAddress] \  
  --output tsv
```



Limpieza de recursos

Cuando ya no se necesiten, use el comando [az group delete](#) para quitar el grupo de recursos, el equilibrador de carga y todos los recursos relacionados.

```
az group delete \  
  --name myResourceGroupLB
```

Pasos siguientes

En esta guía de inicio rápido

- Creó un equilibrador de carga estándar o público.
- Conectó máquinas virtuales.
- Configuró la regla de tráfico del equilibrador de carga y el sondeo de estado.
- Probó el equilibrador de carga.

Para más información sobre Azure Load Balancer, consulte [¿Qué es Azure Load Balancer?](#) y [Preguntas frecuentes de Load Balancer](#).

Más información sobre [Load Balancer y zonas de disponibilidad](#).

Inicio rápido: Creación de una instancia de Load Balancer para equilibrar la carga de las máquinas virtuales con una plantilla de Resource Manager

23/09/2020 • 10 minutes to read • [Edit Online](#)

El equilibrio de carga proporciona un mayor nivel de disponibilidad y escala, ya que distribuye las solicitudes entrantes entre varias máquinas virtuales. En este inicio rápido se muestra cómo implementar una plantilla de Azure Resource Manager que crea una instancia de Standard Load Balancer para cargar máquinas virtuales de equilibrio de carga. El uso de una plantilla de Resource Manager requiere menos pasos que otros métodos de implementación.

Una [plantilla de Resource Manager](#) es un archivo de notación de objetos JavaScript (JSON) que define la infraestructura y la configuración del proyecto. La plantilla usa sintaxis declarativa, lo que permite establecer lo que pretende implementar sin tener que escribir la secuencia de comandos de programación para crearla.

Si su entorno cumple los requisitos previos y está familiarizado con el uso de plantillas de Resource Manager, seleccione el botón **Implementar en Azure**. La plantilla se abrirá en Azure Portal.

Requisitos previos

Si no tiene una suscripción a Azure, cree una [cuenta gratuita](#) antes de empezar.

Revisión de la plantilla

La plantilla usada en este inicio rápido forma parte de las [plantillas de inicio rápido de Azure](#).

Load Balancer y las SKU de IP públicas deben coincidir. Cuando se crea una instancia de Standard Load Balancer, también se debe crear una nueva dirección IP pública estándar que se configura como front-end para dicha instancia. Si desea crear una instancia de Load Balancer Básico, use [esta plantilla](#). Microsoft recomienda usar la SKU estándar para cargas de trabajo de producción.

```
{
  "$schema": "https://schema.management.azure.com/schemas/2019-04-01/deploymentTemplate.json#",
  "contentVersion": "1.0.0.0",
  "parameters": {
    "projectName": {
      "type": "string",
      "metadata": {
        "description": "Specifies a project name that is used for generating resource names."
      }
    },
    "location": {
      "type": "string",
      "defaultValue": "[resourceGroup().location]",
      "metadata": {
        "description": "Specifies the location for all of the resources created by this template."
      }
    },
    "adminUsername": {
      "type": "string",
      "metadata": {
        "description": "Specifies the virtual machine administrator username."
      }
    }
  }
}
```

```

    }
  },
  "adminPassword": {
    "type": "securestring",
    "metadata": {
      "description": "Specifies the virtual machine administrator password."
    }
  },
  "vmSize": {
    "type": "string",
    "defaultValue": "Standard_DS1_v2",
    "metadata": {
      "description": "Size of the virtual machine"
    }
  }
},
"variables": {
  "lbName": "[concat(parameters('projectName'), '-lb')]",
  "lbSkuName": "Standard",
  "lbPublicIpAddressName": "[concat(parameters('projectName'), '-lbPublicIP')]",
  "lbFrontEndName": "LoadBalancerFrontEnd",
  "lbBackendPoolName": "LoadBalancerBackEndPool",
  "lbProbeName": "loadBalancerHealthProbe",
  "nsgName": "[concat(parameters('projectName'), '-nsg')]",
  "vNetName": "[concat(parameters('projectName'), '-vnet')]",
  "vNetAddressPrefix": "10.0.1.0/24",
  "vNetSubnetName": "BackendSubnet",
  "vNetSubnetAddressPrefix": "10.0.1.0/24",
  "vmStorageAccountType": "Premium_LRS"
},
"resources": [
  {
    "type": "Microsoft.Network/loadBalancers",
    "apiVersion": "2020-05-01",
    "name": "[variables('lbName')]",
    "location": "[parameters('location')]",
    "sku": {
      "name": "[variables('lbSkuName')]"
    },
    "dependsOn": [
      "[resourceId('Microsoft.Network/publicIPAddresses', variables('lbPublicIpAddressName'))]"
    ],
    "properties": {
      "frontendIPConfigurations": [
        {
          "name": "[variables('lbFrontEndName')]",
          "properties": {
            "publicIPAddress": {
              "id": "[resourceId('Microsoft.Network/publicIPAddresses', variables('lbPublicIpAddressName'))]"
            }
          }
        }
      ],
      "backendAddressPools": [
        {
          "name": "[variables('lbBackendPoolName')]"
        }
      ],
      "loadBalancingRules": [
        {
          "name": "HTTPLBRule",
          "properties": {
            "frontendIPConfiguration": {
              "id": "[resourceId('Microsoft.Network/loadBalancers/frontendIPConfigurations', variables('lbName'), variables('lbFrontEndName'))]"
            },
            "backendAddressPool": {
              "id": "[resourceId('Microsoft.Network/loadBalancers/backendAddressPools', variables('lbName'), variables('lbBackendPoolName'))]"
            }
          }
        }
      ]
    }
  }
]

```

```

    },
    "frontendPort": 80,
    "backendPort": 80,
    "enableFloatingIP": false,
    "idleTimeoutInMinutes": 4,
    "protocol": "Tcp",
    "enableTcpReset": false,
    "loadDistribution": "Default",
    "disableOutboundSnat": false,
    "probe": {
      "id": "[resourceId('Microsoft.Network/loadBalancers/probes', variables('lbName'),
variables('lbProbeName'))]"
    }
  }
},
"probes": [
  {
    "name": "[variables('lbProbeName')]",
    "properties": {
      "protocol": "Http",
      "port": 80,
      "requestPath": "/",
      "intervalInSeconds": 5,
      "numberOfProbes": 2
    }
  }
]
},
{
  "type": "Microsoft.Network/publicIPAddresses",
  "apiVersion": "2020-05-01",
  "name": "[variables('lbPublicIPAddressName')]",
  "location": "[parameters('location')]",
  "sku": {
    "name": "[variables('lbSkuName')]"
  },
  "properties": {
    "publicIPAddressVersion": "IPv4",
    "publicIPAllocationMethod": "Static"
  }
},
{
  "type": "Microsoft.Network/networkSecurityGroups",
  "apiVersion": "2020-05-01",
  "name": "[variables('nsgName')]",
  "location": "[parameters('location')]",
  "properties": {
    "securityRules": [
      {
        "name": "AllowHTTPInbound",
        "properties": {
          "protocol": "*",
          "sourcePortRange": "*",
          "destinationPortRange": "80",
          "sourceAddressPrefix": "Internet",
          "destinationAddressPrefix": "*",
          "access": "Allow",
          "priority": 100,
          "direction": "Inbound"
        }
      },
      {
        "name": "default-allow-rdp",
        "properties": {
          "priority": 1000,
          "protocol": "TCP",
          "access": "Allow",

```

```

        "direction": "Inbound",
        "sourceAddressPrefix": "*",
        "sourcePortRange": "*",
        "destinationAddressPrefix": "*",
        "destinationPortRange": "3389"
    }
}
]
}
},
{
    "type": "Microsoft.Network/virtualNetworks",
    "apiVersion": "2020-05-01",
    "name": "[variables('vNetName')]",
    "location": "[parameters('location')]",
    "properties": {
        "addressSpace": {
            "addressPrefixes": [
                "[variables('vNetAddressPrefix')]"
            ]
        },
        "subnets": [
            {
                "name": "[variables('vNetSubnetName')]",
                "properties": {
                    "addressPrefix": "[variables('vNetSubnetAddressPrefix')]"
                }
            }
        ]
    }
},
{
    "type": "Microsoft.Compute/virtualMachines",
    "apiVersion": "2019-12-01",
    "name": "[concat(parameters('projectName'), '-vm', copyIndex(1))]",
    "location": "[parameters('location')]",
    "zones": [
        "[copyIndex(1)]"
    ],
    "copy": {
        "name": "vmCopy",
        "count": 3
    },
    "dependsOn": [
        "networkInterfaceCopy"
    ],
    "properties": {
        "hardwareProfile": {
            "vmSize": "[parameters('vmSize')]"
        },
        "storageProfile": {
            "imageReference": {
                "publisher": "MicrosoftWindowsServer",
                "offer": "WindowsServer",
                "sku": "2019-Datacenter",
                "version": "latest"
            },
            "osDisk": {
                "createOption": "fromImage",
                "managedDisk": {
                    "storageAccountType": "[variables('vmStorageAccountType')]"
                }
            }
        },
        "networkProfile": {
            "networkInterfaces": [
                {
                    "id": "[resourceId('Microsoft.Network/networkInterfaces', concat(parameters('projectName'), '-vm',
copyIndex(1), '-networkInterface'))]"

```

```

copyIndex(1), '-networkInterface')]]
    }
  ]
},
"osProfile": {
  "computerName": "[concat(parameters('projectName'), '-vm', copyIndex(1))]",
  "adminUsername": "[parameters('adminUsername')]",
  "adminPassword": "[parameters('adminPassword')]",
  "windowsConfiguration": {
    "enableAutomaticUpdates": true,
    "provisionVmAgent": true
  }
}
}
},
{
  "type": "Microsoft.Network/publicIPAddresses",
  "apiVersion": "2020-05-01",
  "name": "[concat(parameters('projectName'), '-vm', copyIndex(1), '-publicIp')]",
  "location": "[parameters('location')]",
  "sku": {
    "name": "Standard"
  },
  "copy": {
    "name": "publicIpAddressCopy",
    "count": 3
  },
  "properties": {
    "publicIpAddressVersion": "IPv4",
    "publicIPAllocationMethod": "Static"
  }
},
{
  "type": "Microsoft.Network/networkInterfaces",
  "apiVersion": "2020-05-01",
  "name": "[concat(parameters('projectName'), '-vm', copyIndex(1), '-networkInterface')]",
  "location": "[parameters('location')]",
  "copy": {
    "name": "networkInterfaceCopy",
    "count": 3
  },
  "dependsOn": [
    "[resourceId('Microsoft.Network/virtualNetworks/', variables('vNetName'))]",
    "[resourceId('Microsoft.Network/loadBalancers/', variables('lbName'))]",
    "[resourceId('Microsoft.Network/networkSecurityGroups/', variables('nsgName'))]",
    "publicIpAddressCopy"
  ],
  "properties": {
    "ipConfigurations": [
      {
        "name": "ipconfig1",
        "properties": {
          "privateIPAllocationMethod": "Dynamic",
          "subnet": {
            "id": "[resourceId('Microsoft.Network/virtualNetworks/subnets', variables('vNetName'),
variables('vNetSubnetName'))]"
          },
          "publicIpAddress": {
            "id": "[resourceId('Microsoft.Network/publicIpAddresses', concat(parameters('projectName'), '-
vm', copyIndex(1), '-publicIp'))]"
          },
          "loadBalancerBackendAddressPools": [
            {
              "id": "[resourceId('Microsoft.Network/loadBalancers/backendAddressPools',
variables('lbName'), variables('lbBackendPoolName'))]"
            }
          ]
        }
      }
    ]
  }
}
}
}

```



```

    },
    "networkSecurityGroup": {
      "id": "[resourceId('Microsoft.Network/networkSecurityGroups', variables('nsgName'))]"
    }
  },
  {
    "type": "Microsoft.Compute/virtualMachines/extensions",
    "apiVersion": "2019-12-01",
    "name": "[concat(parameters('projectName'), '-vm', copyIndex(1), '/', 'InstallWebServer')]",
    "location": "[parameters('location')]",
    "copy": {
      "name": "extensionCopy",
      "count": 3
    },
    "dependsOn": [
      "vmCopy"
    ],
    "properties": {
      "publisher": "Microsoft.Compute",
      "type": "CustomScriptExtension",
      "typeHandlerVersion": "1.7",
      "autoUpgradeMinorVersion": true,
      "settings": {
        "commandToExecute": "powershell.exe Install-WindowsFeature -name Web-Server -IncludeManagementTools
&& powershell.exe remove-item 'C:\\inetpub\\wwwroot\\iisstart.htm' && powershell.exe Add-Content -Path
'C:\\inetpub\\wwwroot\\iisstart.htm' -Value $('Hello World from ' + $env:computername)"
      }
    }
  }
}
]
}

```

En la plantilla se han definido varios recursos de Azure:

- [Microsoft.Network/loadBalancers](#)
- [Microsoft.Network/publicIPAddresses](#): para el equilibrador de carga y para cada una de las tres máquinas virtuales.
- [Microsoft.Network/networkSecurityGroups](#)
- [Microsoft.Network/virtualNetworks](#)
- [Microsoft.Compute/virtualMachines](#) (3 de ellas)
- [Microsoft.Network/networkInterfaces](#) (3 de ellas)
- [Microsoft.Compute/virtualMachine/extensions](#) (3 de ellas): se usan para configurar los IIS y las páginas web.

Para encontrar más plantillas relacionadas con Azure Load Balancer, consulte [Plantillas de inicio rápido de Azure](#).

Implementación de la plantilla

1. Seleccione **Try It** (Probarlo) en el bloque de código siguiente para abrir Azure Cloud Shell y siga las instrucciones para iniciar sesión en Azure.

```

$projectName = Read-Host -Prompt "Enter a project name with 12 or less letters or numbers that is used
to generate Azure resource names"
$location = Read-Host -Prompt "Enter the location (i.e. centralus)"
$adminUserName = Read-Host -Prompt "Enter the virtual machine administrator account name"
$adminPassword = Read-Host -Prompt "Enter the virtual machine administrator password" -AsSecureString

$resourceGroupName = "${projectName}rg"
$templateUri = "https://raw.githubusercontent.com/Azure/azure-quickstart-templates/master/101-load-
balancer-standard-create/azuredeploy.json"

New-AzResourceGroup -Name $resourceGroupName -Location $location
New-AzResourceGroupDeployment -ResourceGroupName $resourceGroupName -TemplateUri $templateUri -
projectName $projectName -location $location -adminUsername $adminUsername -adminPassword $adminPassword

Write-Host "Press [ENTER] to continue."

```

Espere hasta que vea el aviso de la consola.

2. Seleccione **Copiar** en el bloque de código anterior para copiar el script de PowerShell.
3. Haga clic con el botón derecho en el panel de consola del shell y, a continuación, seleccione **Pegar**.
4. Escriba los valores.

La implementación de plantilla crea tres zonas de disponibilidad. Las zonas de disponibilidad se admiten solo en [determinadas regiones](#). Use alguna de las regiones admitidas. Si no está seguro, escriba **centralus**.

El nombre del grupo de recursos es el nombre del proyecto con **rg** anexo. Necesitará el nombre del grupo de recursos en la sección siguiente.

Tardará unos 10 minutos en implementar la plantilla. Al finalizar, la salida es parecida a esta:

```

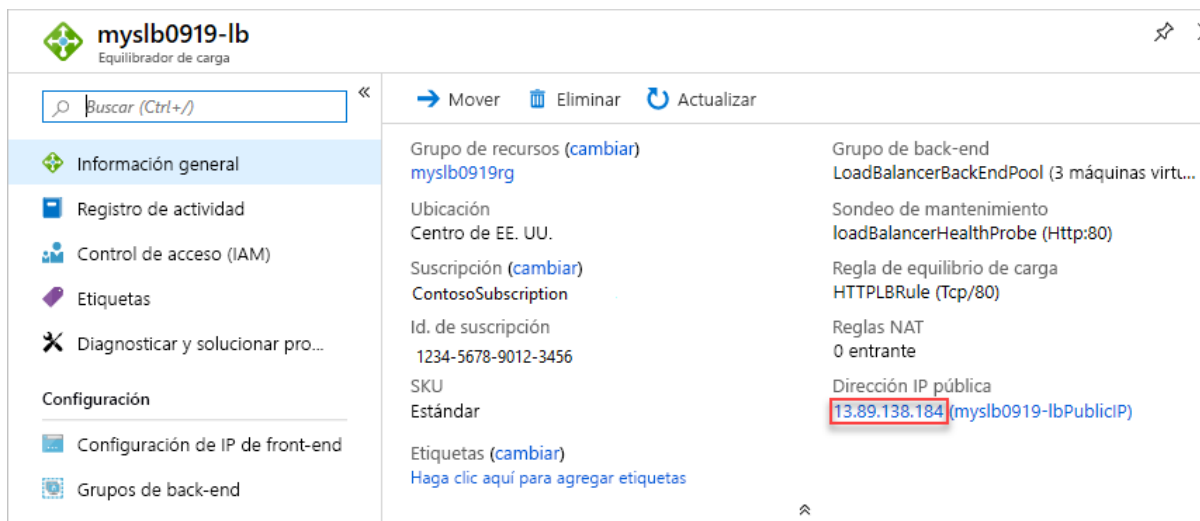
DeploymentName      : azuredeploy
ResourceGroupName  : myslb0919rg
ProvisioningState   : Succeeded
Timestamp          : 9/19/19 2:17:47 PM
Mode               : Incremental
TemplateLink       :
Uri                : https://raw.githubusercontent.com/Azure/azure-quickstart-templates/master/
ContentVersion     : 1.0.0.0
Parameters         :
Name               Type               Value
-----
projectName        String              myslb0919
location           String              centralus
adminUsername      String              jgao
adminPassword      SecureString

```

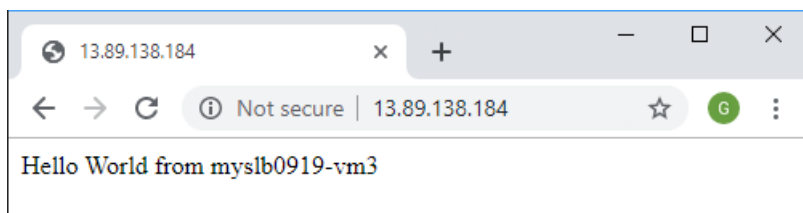
Azure PowerShell se usa para implementar la plantilla. Además de Azure PowerShell, también puede usar Azure Portal, la CLI de Azure y API REST. Para obtener información sobre otros métodos de implementación, consulte [Implementación de plantillas](#).

Revisión de los recursos implementados

1. Inicie sesión en [Azure Portal](#).
2. Seleccione **Grupos de recursos** en el panel izquierdo.
3. Seleccione el grupo de recursos que creó en la sección anterior. El nombre del grupo de recursos predeterminado es el nombre del proyecto con **rg** anexo.
4. Seleccione el equilibrador de carga. Su nombre predeterminado es el nombre del proyecto con **-lb** anexo.
5. Copie solo la parte de la dirección IP pública y, luego, péguela en la barra de direcciones del explorador.



El explorador muestra la página predeterminada del servidor web de Internet Information Services (IIS).



Para ver cómo Load Balancer distribuye el tráfico entre las tres máquinas virtuales, puede forzar una actualización del explorador web desde la máquina cliente.

Limpieza de recursos

Cuando no los necesite, elimine el grupo de recursos, el equilibrador de carga y todos los recursos relacionados. Para ello, vaya a Azure Portal, seleccione el grupo de recursos que contiene el equilibrador de carga y, luego, seleccione **Eliminar grupo de recursos**.

Pasos siguientes

En esta guía de inicio rápido, ha creado una instancia de Standard Load Balancer, le ha asociado máquinas virtuales, ha configurado la regla de tráfico de Load Balancer, ha realizado un sondeo de estado y, después, ha probado la instancia de Load Balancer.

Para más información, continúe con los tutoriales para Load Balancer.

[Tutoriales de Azure Load Balancer](#)

Inicio rápido: Creación de un equilibrador de carga interno para equilibrar la carga de las máquinas virtuales mediante Azure Portal

23/09/2020 • 32 minutes to read • [Edit Online](#)

Para empezar a usar Azure Load Balancer diríjase a Azure Portal para crear un equilibrador de carga interno y dos máquinas virtuales.

Requisitos previos

- Una cuenta de Azure con una suscripción activa. [Cree una cuenta gratuita](#).

Inicio de sesión en Azure

Inicie sesión en Azure Portal en <https://portal.azure.com>.

- [SKU Estándar](#)
- [SKU básica](#)

NOTE

Se recomienda usar la SKU Estándar de Load Balancer para las cargas de trabajo de producción. Para más información sobre las SKU, consulte [SKU de Azure Load Balancer](#).

En esta sección, va a crear un equilibrador de carga que equilibra la carga de las máquinas virtuales.

Puede crear un equilibrador de carga público o interno.

Cuando se crea un equilibrador de carga interno, se configura una red virtual como red para el equilibrador de carga.

Una dirección IP privada de la red virtual se configura como front-end (denominado **LoadBalancerFrontend** de manera predeterminada) para el equilibrador de carga.

La dirección IP de front-end puede ser **estática** o **dinámica**.

Crear la red virtual

En esta sección, creará una red virtual y una subred.

1. En la parte superior izquierda de la pantalla, seleccione **Crear un recurso** > **Redes** > **Red virtual** o busque **Red virtual** en el cuadro de búsqueda.
2. En **Crear red virtual**, escriba o seleccione esta información en la pestaña **Conceptos básicos**:

CONFIGURACIÓN	VALOR
Detalles del proyecto	
Suscripción	Selección de su suscripción a Azure

CONFIGURACIÓN	VALOR
Grupo de recursos	Seleccione myResourceGroupLB .
Detalles de instancia	
Nombre	Escriba myVNet .
Region	Seleccione Oeste de Europa .

3. Seleccione la pestaña **Direcciones IP** o el botón **Siguiente: Direcciones IP** situado en la parte inferior de la página.

4. En la pestaña **Direcciones IP**, especifique esta información:

CONFIGURACIÓN	VALUE
Espacio de direcciones IPv4	Escriba 10.1.0.0/16 .

5. En **Nombre de subred**, seleccione la palabra **predeterminada**.

6. En **Editar subred**, especifique esta información:

CONFIGURACIÓN	VALUE
Nombre de subred	Escriba myBackendSubnet .
Intervalo de direcciones de subred	Escriba 10.1.0.0/24 .

7. Seleccione **Guardar**.

8. Seleccione la pestaña **Seguridad**.

9. En **BastionHost**, seleccione **Habilitar**. Escriba esta información:

CONFIGURACIÓN	VALUE
Nombre del bastión	Escriba myBastionHost .
Espacio de direcciones de AzureBastionSubnet	Escriba 10.1.1.0/24 .
Dirección IP pública	Seleccione Crear nuevo . En Nombre , escriba myBastionIP . Seleccione Aceptar .

10. Seleccione la pestaña **Revisar y crear** o el botón **Revisar y crear**.

11. Seleccione **Crear**.

Creación de un equilibrador de carga

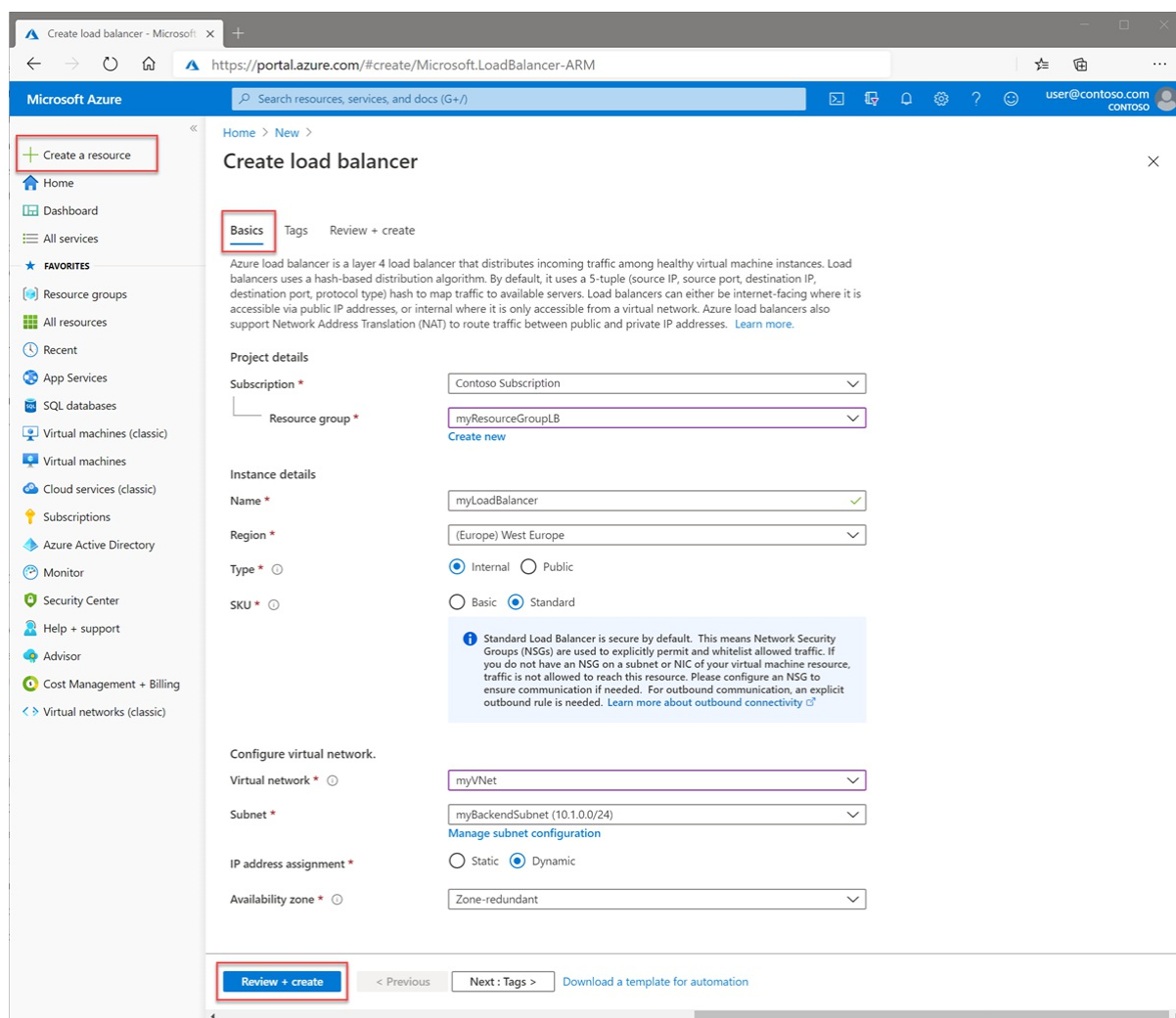
1. En la parte superior izquierda de la pantalla, seleccione **Crear un recurso** > **Redes** > **Load Balancer**.

2. En la pestaña **Conceptos básicos** de la página **Crear equilibrador de carga**, escriba o seleccione la

siguiente información:

CONFIGURACIÓN	VALUE
Suscripción	Seleccione su suscripción.
Resource group	Seleccione myResourceGroupLB , que creó en el paso anterior.
Nombre	Escriba myLoadBalancer .
Region	Seleccione Oeste de Europa .
Tipo	seleccione Interno .
SKU	Seleccione Estándar .
Virtual network	Seleccione myVNet , que creó en el paso anterior.
Subnet	Seleccione myBackendSubnet , que creó en el paso anterior.
Asignación de dirección IP	seleccione Dinámico .
Zona de disponibilidad	Seleccione Con redundancia de zona .

3. Acepte los valores predeterminados en los demás valores y seleccione **Revisar y crear**.
4. En la pestaña **Revisar + crear**, seleccione **Crear**.



Creación de recursos del equilibrador de carga

En esta sección, va a configurar:

- Las opciones del equilibrador de carga para un grupo de direcciones de back-end.
- Un sondeo de estado.
- Una regla de equilibrador de carga.

Creación de un grupo de back-end

Un grupo de direcciones de back-end contiene las direcciones IP de las tarjetas de interfaz de red virtuales conectadas al equilibrador de carga.

Cree el grupo de direcciones de back-end **myBackendPool** para incluir máquinas virtuales para el tráfico de Internet de equilibrio de carga.

1. Seleccione **Todos los servicios** en el menú de la izquierda, **Todos los recursos** y, después, en la lista de recursos, **myLoadBalancer**.
2. En **Configuración**, seleccione **Grupos de back-end** y, a continuación, seleccione **Agregar**.
3. En la página **Agregar un grupo back-end**, en nombre, escriba **myBackEndPool**, como el nombre del grupo de back-end y, a continuación, seleccione **Aceptar**.

Creación de un sondeo de estado

El equilibrador de carga supervisa el estado de la aplicación con un sondeo de estado.

El sondeo de estado agrega o quita las máquinas virtuales del equilibrador de carga a partir de su respuesta a las comprobaciones de estado.

Cree un sondeo de mantenimiento llamado **myHealthProbe** para supervisar el mantenimiento de las máquinas virtuales.

1. Seleccione **Todos los servicios** en el menú de la izquierda, **Todos los recursos** y, después, en la lista de recursos, **myLoadBalancer**.
2. En **Configuración**, seleccione **Sondeos de estado** y, a continuación, seleccione **Agregar**.

CONFIGURACIÓN	VALUE
Nombre	Escriba myHealthProbe .
Protocolo	Seleccione HTTP .
Port	Escriba 80 .
Intervalo	Escriba 15 como número de Intervalo , en segundos, entre los intentos de sondeo.
Umbral incorrecto	Seleccione 2 como número de Umbral incorrecto o errores de sondeo consecutivos que deben producirse para que una máquina virtual se considere que no funciona de manera correcta.

3. Deje el resto de valores predeterminados y seleccione **Aceptar**.

Creación de una regla de equilibrador de carga

Las reglas de equilibrador de carga se utilizan para definir cómo se distribuye el tráfico a las máquinas virtuales. Defina la configuración IP del front-end para el tráfico entrante y el grupo de direcciones IP de back-end para recibir el tráfico. Los puertos de origen y de destino se definen en la regla.

En esta sección va a crear una regla de equilibrador de carga:

- Llamada **myHTTPRule**.
- En el front-end llamado **LoadBalancerFrontEnd**.
- A la escucha en el **puerto 80**.
- Dirige el tráfico con equilibrio de carga al back-end llamado **myBackendPool** en el **puerto 80**.

1. Seleccione **Todos los servicios** en el menú de la izquierda, **Todos los recursos** y, después, en la lista de recursos, **myLoadBalancer**.
2. En **Configuración**, seleccione **Reglas de equilibrio de carga** y, a continuación, seleccione **Agregar**.
3. Use estos valores para configurar la regla de equilibrio de carga:

CONFIGURACIÓN	VALUE
Nombre	Escriba myHTTPRule .
Versión de la dirección IP	Seleccione IPv4 .
Dirección IP del front-end	Seleccione LoadBalancerFrontEnd .
Protocolo	seleccione TCP .

CONFIGURACIÓN	VALUE
Port	Escriba 80 .
Puerto back-end	Escriba 80 .
Grupo back-end	Seleccione MyBackendPool .
Sondeo de mantenimiento	Seleccione myHealthProbe .
Creación de reglas de salida implícitas	así que seleccione No .

4. Deje el resto de valores predeterminados y después seleccione **Aceptar**.

NOTE

Las máquinas virtuales del grupo de back-end no tendrán conectividad de salida a Internet con esta configuración. Para más información acerca de cómo proporcionar conectividad de salida, consulte:

[Conexiones salientes en Azure](#)

Opciones para proporcionar conectividad:

[Configuración del equilibrador de carga solo de salida](#)

[¿Qué es NAT de Virtual Network?](#)

Creación de servidores back-end

En esta sección:

- Creará dos máquinas virtuales para el grupo de back-end del equilibrador de carga.
- Instalará IIS en las máquinas virtuales para probar el equilibrador de carga.

Creación de máquinas virtuales

En esta sección, creará dos máquinas virtuales (**myVM1** y **myVM2**) con una dirección IP pública estándar en dos zonas (**Zona 1** y **Zona 2**).

Estas máquinas virtuales se agregan al grupo de back-end del equilibrador de carga que se creó anteriormente.

1. En la parte superior izquierda de Azure Portal, seleccione **Crear un recurso** > **Proceso** > **Máquina virtual**.
2. En **Crear una máquina virtual**, escriba o seleccione los valores en la pestaña **Básico**:

CONFIGURACIÓN	VALUE
Detalles del proyecto	
Suscripción	Selección de su suscripción a Azure
Grupo de recursos	Seleccione myResourceGroupLB .
Detalles de instancia	
Nombre de la máquina virtual	Escriba myVM1 .
Region	Seleccione Oeste de Europa .

CONFIGURACIÓN	VALUE
Opciones de disponibilidad	Seleccione Zonas de disponibilidad .
Zona de disponibilidad	Seleccione 1 .
Imagen	Seleccione Windows Server 2019 Datacenter .
Instancia de Azure Spot	Seleccione No .
Size	Elija el tamaño de la máquina virtual o acepte la configuración predeterminada.
Cuenta de administrador	
Nombre de usuario	Escriba un nombre de usuario.
Contraseña	Escriba una contraseña.
Confirmar contraseña	Vuelva a escribir la contraseña.

3. Seleccione la pestaña **Redes** o seleccione **Siguiente: Discos** y, después, **Siguiente: Redes**.

4. En la pestaña **Redes**, seleccione o escriba:

CONFIGURACIÓN	VALUE
Interfaz de red	
Virtual network	myVNet
Subnet	myBackendSubnet
Dirección IP pública	Acepte el valor predeterminado de myVM-ip . La dirección IP será automáticamente una dirección IP de la SKU estándar en la Zona 1.
Grupo de seguridad de red de NIC	Seleccione Avanzado .
Configuración del grupo de seguridad de red	Seleccione Crear nuevo . En la página Crear grupo de seguridad de red , escriba myNSG en Nombre . Seleccione Aceptar .
Equilibrio de carga	
¿Quiere colocar esta máquina virtual como subyacente respecto a una solución de equilibrio de carga existente?	Seleccione Sí .
Configuración de equilibrio de carga	
Opciones de equilibrio de carga	Seleccione Equilibrio de carga de Azure .
Seleccionar un equilibrador de carga	Seleccione myLoadBalancer .

CONFIGURACIÓN	VALUE
Seleccionar un grupo de back-end	Seleccione MyBackendPool .

5. Seleccione la pestaña **Administración** o seleccione **Siguiente > Administración**.

6. En la pestaña **Administración**, seleccione o escriba:

CONFIGURACIÓN	VALUE
Supervisión	
Diagnósticos de arranque	Seleccione Desactivado .

7. Seleccione **Revisar + crear**.

8. Revise la configuración y, a continuación, seleccione **Crear**.

9. Siga los pasos 1 a 8 para crear otra máquina virtual con los siguientes valores, mientras que el resto de la configuración es la misma que la de la máquina virtual **myVM1**:

CONFIGURACIÓN	VM 2
Nombre	myVM2
Zona de disponibilidad	2
Grupo de seguridad de red	Seleccione el grupo myNSG existente.

Creación de una máquina virtual de prueba

En esta sección va a crear una máquina virtual denominada **myTestVM**. Esta máquina virtual se usará para probar la configuración del equilibrador de carga.

1. En la parte superior izquierda de Azure Portal, seleccione **Crear un recurso > Proceso > Máquina virtual**.

2. En **Crear una máquina virtual**, escriba o seleccione los valores en la pestaña **Básico**:

CONFIGURACIÓN	VALUE
Detalles del proyecto	
Suscripción	Selección de su suscripción a Azure
Grupo de recursos	Seleccione myResourceGroupLB .
Detalles de instancia	
Nombre de la máquina virtual	Escriba myTestVM
Region	Seleccione Oeste de Europa .

CONFIGURACIÓN	VALUE
Opciones de disponibilidad	Seleccione No se requiere redundancia de la infraestructura
Imagen	Seleccione Windows Server 2019 Datacenter .
Instancia de Azure Spot	Seleccione No .
Size	Elija el tamaño de la máquina virtual o acepte la configuración predeterminada.
Cuenta de administrador	
Nombre de usuario	Escriba un nombre de usuario.
Contraseña	Escriba una contraseña.
Confirmar contraseña	Vuelva a escribir la contraseña.

3. Seleccione la pestaña **Redes** o seleccione **Siguiente: Discos** y, después, **Siguiente: Redes**.

4. En la pestaña **Redes**, seleccione o escriba:

CONFIGURACIÓN	VALUE
Interfaz de red	
Virtual network	myVNet
Subnet	myBackendSubnet
Dirección IP pública	Seleccione Ninguno .
Grupo de seguridad de red de NIC	Seleccione Avanzado .
Configuración del grupo de seguridad de red	Seleccione MyNSG , que creó en el paso anterior.

5. Seleccione la pestaña **Administración** o seleccione **Siguiente > Administración**.

6. En la pestaña **Administración**, seleccione o escriba:

CONFIGURACIÓN	VALUE
Supervisión	
Diagnósticos de arranque	Seleccione Desactivado .

7. Seleccione **Revisar + crear**.

8. Revise la configuración y, a continuación, seleccione **Crear**.

Instalación de IIS

1. Seleccione **Todos los servicios** en el menú de la izquierda, seleccione **Todos los recursos** y, después, en

la lista de recursos, seleccione **myVM1**, que se encuentra en el grupo de recursos **myResourceGroupLB**.

2. En la página **Introducción**, seleccione **Conectar** y después **Instancia de Bastion**.
3. Escriba el nombre de usuario y la contraseña especificados durante la creación de la máquina virtual.
4. Seleccione **Conectar**.
5. En el escritorio del servidor, vaya a **Herramientas administrativas de Windows > Windows PowerShell**.
6. Ejecute los siguientes comandos en la ventana de PowerShell para:
 - Instalar el servidor IIS
 - Eliminar el archivo predeterminado iisstart.htm
 - Agregue un nuevo archivo iisstart.htm que muestre el nombre de la máquina virtual:

```
# install IIS server role
Install-WindowsFeature -name Web-Server -IncludeManagementTools

# remove default htm file
remove-item C:\inetpub\wwwroot\iisstart.htm

# Add a new htm file that displays server name
Add-Content -Path "C:\inetpub\wwwroot\iisstart.htm" -Value $("Hello World from " + $env:computername)
```

7. Cierre la sesión de Bastion con **myVM1**.
8. Repita los pasos 1 a 6 para instalar IIS y el archivo iisstart.htm actualizado en **myVM2**.

Prueba del equilibrador de carga

1. Busque la dirección IP privada del equilibrador de carga en la pantalla **Información general**. Seleccione **Todos los servicios** en el menú de la izquierda, **Todos los recursos** y, después, **myLoadBalancer**.
2. Tome nota o copie la dirección que encontrará junto a **Dirección IP privada**, en la pestaña **Información general** de **myLoadBalancer**.
3. Seleccione **Todos los servicios** en el menú de la izquierda, seleccione **Todos los recursos** y, después, en la lista de recursos, seleccione **myTestVM**, que se encuentra en el grupo de recursos **myResourceGroupLB**.
4. En la página **Introducción**, seleccione **Conectar** y después **Instancia de Bastion**.
5. Escriba el nombre de usuario y la contraseña especificados durante la creación de la máquina virtual.
6. Abra **Internet Explorer** en **myTestVM**.
7. Escriba la dirección IP del paso anterior en la barra de direcciones del explorador. La página predeterminada del servidor web de IIS se muestra en el explorador.



Hello World from myVM1

Para ver el tráfico distribuido por Load Balancer entre las tres máquinas virtuales, puede personalizar la página predeterminada de cada servidor web IIS de las máquinas virtuales y luego forzar una actualización del explorador web desde el equipo cliente.

Limpieza de recursos

Cuando no los necesite, elimine el grupo de recursos, la instancia de Load Balancer y todos los recursos relacionados. Para ello, seleccione el grupo de recursos **myResourceGroupLB**, que contiene los recursos y, a continuación, seleccione **Eliminar**.

Pasos siguientes

En esta guía de inicio rápido:

- Ha creado un equilibrador de carga Básico o Estándar en Azure.
- Ha conectado dos máquinas virtuales al equilibrador de carga.
- Ha configurado la regla de tráfico del equilibrador de carga, el sondeo de estado y, a continuación, ha probado el equilibrador de carga.

Para más información sobre Azure Load Balancer, consulte [¿Qué es Azure Load Balancer?](#) y [Preguntas frecuentes de Load Balancer](#).

- Más información sobre [Load Balancer y zonas de disponibilidad](#).
- Más información acerca de [Azure Bastion](#).

Inicio rápido: Creación de un equilibrador de carga interno para equilibrar la carga de las máquinas virtuales mediante Azure PowerShell

23/09/2020 • 33 minutes to read • [Edit Online](#)

Para empezar a usar Azure Load Balancer diríjase a Azure PowerShell para crear un equilibrador de carga interno y dos máquinas virtuales.

Requisitos previos

- Una cuenta de Azure con una suscripción activa. [Cree una cuenta gratuita](#).
- Azure PowerShell instalado localmente o Azure Cloud Shell




NOTE

Este artículo se ha actualizado para usar el nuevo módulo Az de Azure PowerShell. Aún puede usar el módulo de AzureRM que continuará recibiendo correcciones de errores hasta diciembre de 2020 como mínimo. Para más información acerca del nuevo módulo Az y la compatibilidad con AzureRM, consulte [Introducing the new Azure PowerShell Az module](#) (Presentación del nuevo módulo Az de Azure PowerShell). Para obtener instrucciones sobre la instalación del módulo Az, consulte [Instalación de Azure PowerShell](#).

Uso de Azure Cloud Shell

En Azure se hospeda Azure Cloud Shell, un entorno de shell interactivo que puede utilizar mediante el explorador. Puede usar Bash o PowerShell con Cloud Shell para trabajar con los servicios de Azure. Puede usar los comandos preinstalados de Cloud Shell para ejecutar el código de este artículo sin tener que instalar nada en su entorno local.

Para iniciar Azure Cloud Shell:

OPCIÓN	EJEMPLO O VÍNCULO
Seleccione Pruébalo en la esquina superior derecha de un bloque de código. Solo con seleccionar Pruébalo no se copia automáticamente el código en Cloud Shell.	
Vaya a https://shell.azure.com o seleccione el botón Iniciar Cloud Shell para abrir Cloud Shell en el explorador.	
Seleccione el botón Cloud Shell en la barra de menús de la esquina superior derecha de Azure Portal .	

Para ejecutar el código de este artículo en Azure Cloud Shell:

1. Inicie Cloud Shell.
2. Seleccione el botón **Copiar** de un bloque de código para copiar el código.
3. Pegue el código en la sesión de Cloud Shell. Para ello, seleccione **Ctrl+Mayús+V** en Windows y Linux, o bien seleccione **Cmd+Mayús+V** en macOS.

4. Seleccione **Entrar** para ejecutar el código.

Si decide instalar y usar PowerShell de forma local, para realizar los pasos de este artículo necesita la versión 5.4.1 del módulo de Azure PowerShell o cualquier versión posterior. Ejecute `Get-Module -ListAvailable Az` para buscar la versión instalada. Si necesita actualizarla, consulte [Instalación del módulo de Azure PowerShell](#). Si PowerShell se ejecuta localmente, también debe ejecutar `Connect-AzAccount` para crear una conexión con Azure.

Crear un grupo de recursos

Un grupo de recursos de Azure es un contenedor lógico en el que se implementan y se administran los recursos de Azure.

Cree un grupo de recursos con `New-AzResourceGroup`:

- Denominado **myResourceGroupLB**.
- En la ubicación **eastus**.

```
## Variables for the command ##
$rg = 'MyResourceGroupLB'
$loc = 'eastus'

New-AzResourceGroup -Name $rg -Location $loc
```

- [SKU Estándar](#)
- [SKU básica](#)

NOTE

Se recomienda usar la SKU Estándar de Load Balancer para las cargas de trabajo de producción. Para más información sobre las SKU, consulte [SKU de Azure Load Balancer](#).

Configurar la red virtual

Antes de implementar las VM y probar el equilibrador de carga, cree los recursos de red virtual auxiliares.

Creación de una red virtual y un host de Azure Bastion

Cree una red virtual con `New-AzVirtualNetwork`:

- Denominada **myVNet**.
- En el grupo de recursos **myResourceGroupLB**.
- Subred denominada **MyBackendSubnet**.
- Red virtual **10.0.0.0/16**.
- Subred **10.0.0.0/24**.
- Subred llamada **AzureBastionSubnet**.
- Subred **10.0.1.0/24**.


```
## Variables for the command ##
$rg = 'myResourceGroupLB'
$loc = 'eastus'
$sub = 'myBackendSubnet'
$spfx = '10.0.0.0/24'
$vnrm = 'myVNet'
$vpfx = '10.0.0.0/16'
$bssub = 'AzureBastionSubnet'
$bpfx = '10.0.1.0/24'

## Create backend subnet config ##
$subnetConfig =
New-AzVirtualNetworkSubnetConfig -Name $sub -AddressPrefix $spfx

## Create Azure Bastion subnet
$bassubConfig =
New-AzVirtualNetworkSubnetConfig -Name $bssub -AddressPrefix $bpfx

## Create the virtual network ##
$vnrm =
New-AzVirtualNetwork -ResourceGroupName $rg -Location $loc -Name $vnrm -AddressPrefix $vpfx -Subnet
$subnetConfig,$bassubConfig
```

Creación de una dirección IP pública para un host de Azure Bastion

Use [New-AzPublicIpAddress](#) para crear una dirección IP pública para el host bastión:

- Se denomina **myPublicIPBastion**.
- En el grupo de recursos **myResourceGroupLB**.
- En la ubicación **eastus**.
- Método de asignación **estático**.
- SKU **Standard**.

```
## Variables for the command ##
$rg = 'myResourceGroupLB'
$loc = 'eastus'
$ipn = 'myPublicIPBastion'
$all = 'static'
$sku = 'standard'

$publicip =
New-AzPublicIpAddress -ResourceGroupName $rg -Location $loc -Name $ipn -AllocationMethod $all -Sku $sku
```

Creación de un host de Azure Bastion

Use [New-AzBastion](#) para crear un host bastión:

- Se denomina **myBastion**.
- En el grupo de recursos **myResourceGroupLB**.
- En la red virtual **myVNet**.
- Asociada a la dirección IP pública **myPublicIPBastion**.

```
## Variables for the commands ##
$rg = 'myResourceGroupLB'
$nmn = 'myBastion'

## Command to create bastion host. $vnrm and $publicip are from the previous steps ##
New-AzBastion -ResourceGroupName $rg -Name $nmn -PublicIpAddress $publicip -VirtualNetwork $vnrm
```

El host de Azure Bastion tarda unos minutos en implementarse.

Creación de un grupo de seguridad de red

Cree un grupo de seguridad de red para definir las conexiones entrantes a la red virtual.

Creación de una regla de grupo de seguridad de red para el puerto 80

Cree una regla de grupo de seguridad de red con [New-AzNetworkSecurityRuleConfig](#):

- Denominada **myNSGRuleHTTP**.
- Descripción de **Allow HTTP**.
- Acceso de **Allow**.
- Protocolo **(*)**.
- Dirección **Inbound**.
- Prioridad **2000**.
- Origen de **Internet**.
- Intervalo de puertos de origen de **(*)**.
- Prefijo de dirección de destino **(*)**.
- Puerto de destino **80**.

```
## Variables for command ##
$rmn = 'myNSGRuleHTTP'
$des = 'Allow HTTP'
$acc = 'Allow'
$pro = '*'
$dir = 'Inbound'
$pri = '2000'
$spfx = 'Internet'
$spr = '*'
$dpr = '80'

$rule1 =
New-AzNetworkSecurityRuleConfig -Name $rmn -Description $des -Access $acc -Protocol $pro -Direction $dir -
Priority $pri -SourceAddressPrefix $spfx -SourcePortRange $spr -DestinationAddressPrefix $dpfx -
DestinationPortRange $dpr
```

Crear un grupo de seguridad de red

Cree un grupo de seguridad de red con [New-AzNetworkSecurityGroup](#):

- Denominado **myNSG**.
- En el grupo de recursos **myResourceGroupLB**.
- En la ubicación **eastus**.
- Con las reglas de seguridad creadas en los pasos anteriores almacenadas en una variable.

```
## Variables for command ##
$rg = 'myResourceGroupLB'
$loc = 'eastus'
$nmn = 'myNSG'

## $rule1 contains configuration information from the previous steps. ##
$nsg =
New-AzNetworkSecurityGroup -ResourceGroupName $rg -Location $loc -Name $nmn -SecurityRules $rule1
```

Creación de un equilibrador de carga estándar

En esta sección se detalla cómo se pueden crear y configurar los componentes siguientes del equilibrador de carga:

- Un grupo de direcciones IP de front-end que recibe el tráfico de red entrante en el equilibrador de carga.
- Un grupo de direcciones IP de back-end al que el grupo de servidores front-end envía el tráfico de red de carga equilibrada.
- Un sondeo de estado que determina el estado de las instancias de máquina virtual de back-end.
- Una regla de equilibrador de carga que define cómo se distribuye el tráfico a las VM.

Creación de la dirección IP de front-end

Cree una dirección IP de front-end con [New-AzLoadBalancerFrontendIpConfig](#):

- Denominada **mi FrontEnd**.
- Dirección IP privada de **10.0.0.4**.

```
## Variables for the commands ##
$fe = 'myFrontEnd'
$rg = 'MyResourceGroupLB'
$ip = '10.0.0.4'

## Command to create frontend configuration. The variable $vnet is from the previous commands. ##
$feip =
New-AzLoadBalancerFrontendIpConfig -Name $fe -PrivateIpAddress $ip -SubnetId $vnet.subnets[0].Id
```

Configuración del grupo de direcciones de back-end

Cree un grupo de direcciones de back-end con [New-AzLoadBalancerBackendAddressPoolConfig](#):

- Denominado **myBackEndPool**.
- En el resto de los pasos, las máquinas virtuales se conectan a este grupo back-end.

```
## Variable for the command ##
$be = 'myBackEndPool'

$bepool =
New-AzLoadBalancerBackendAddressPoolConfig -Name $be
```

Creación del sondeo de estado

Los sondeos de estado comprueban todas las instancias de máquina virtual para asegurarse de que pueden enviar tráfico de red.

Una máquina virtual con una comprobación de sondeo con errores se quita del equilibrador de carga. La máquina virtual se agrega de nuevo al equilibrador de carga cuando se resuelve el error.

Cree un sondeo de estado con [Add-AzLoadBalancerProbeConfig](#):

- Supervisa el estado de las máquinas virtuales.
- Denominado **myHealthProbe**.
- Protocolo **TCP**.
- **Puerto 80** de supervisión.

```
## Variables for the command ##
$hp = 'myHealthProbe'
$pro = 'http'
$port = '80'
$int = '360'
$cnt = '5'

$probe =
New-AzLoadBalancerProbeConfig -Name $hp -Protocol $pro -Port $port -RequestPath / -IntervalInSeconds $int -
ProbeCount $cnt
```

Creación de la regla de equilibrador de carga

Una regla de equilibrador de carga define:

- La configuración de IP del front-end para el tráfico entrante.
- El grupo de IP de back-end para recibir el tráfico.
- Los puertos de origen y de destino requeridos.

Cree una regla del equilibrador de carga con [Add-AzLoadBalancerRuleConfig](#):

- Denominada **myHTTPRule**.
- Que escuche en el **puerto 80** en el grupo de front-end **myFrontEnd**.
- Que envíe el tráfico de red con equilibrio de carga al grupo de direcciones de back-end **myBackEndPool** a través del **Puerto 80**.
- Mediante el sondeo de estado **myHealthProbe**.
- Protocolo TCP.

```
## Variables for the command ##
$lbr = 'myHTTPRule'
$pro = 'tcp'
$port = '80'

## $feip and $bePool are the variables from previous steps. ##

$rule =
New-AzLoadBalancerRuleConfig -Name $lbr -Protocol $pro -Probe $probe -FrontendPort $port -BackendPort $port -
FrontendIpConfiguration $feip -BackendAddressPool $bePool -DisableOutboundSNAT
```

NOTE

Las máquinas virtuales del grupo de back-end no tendrán conectividad de salida a Internet con esta configuración. Para más información acerca de cómo proporcionar conectividad de salida, consulte:

[Conexiones salientes en Azure](#)

Opciones para proporcionar conectividad:

[Configuración del equilibrador de carga solo de salida](#)

[¿Qué es NAT de Virtual Network?](#)

Creación de un recurso de equilibrador de carga

Cree un equilibrador de carga interno con [New-AzLoadBalancer](#):

- Denominado **myLoadBalancer**.
- En **eastus**.
- En el grupo de recursos **myResourceGroupLB**.

```
## Variables for the command ##
$lb = 'myLoadBalancer'
$rg = 'myResourceGroupLB'
$loc = 'eastus'
$sku = 'Standard'

## $feip, $bepool, $probe, $rule are variables with configuration information from previous steps. ##

$lb =
New-AzLoadBalancer -ResourceGroupName $rg -Name $lb -SKU $sku -Location $loc -FrontendIpConfiguration $feip -
BackendAddressPool $bepool -Probe $probe -LoadBalancingRule $rule
```

Creación de interfaces de red

Cree tres interfaces de red con [New-AzNetworkInterface](#):

VM 1

- Denominada **myNicVM1**.
- En el grupo de recursos **myResourceGroupLB**.
- En la ubicación **eastus**.
- En la red virtual **myVNet**.
- En la subred **myBackendSubnet**.
- En el grupo de seguridad de red **myNSG**.
- Conectada al equilibrador de carga **myLoadBalancer** en **myBackEndPool**.

```
## Variables for command ##
$rg = 'myResourceGroupLB'
$loc = 'eastus'
$nic1 = 'myNicVM1'
$vnt = 'myVNet'
$lb = 'myLoadBalancer'
$ngn = 'myNSG'

## Command to get virtual network configuration. ##
$vnet =
Get-AzVirtualNetwork -Name $vnt -ResourceGroupName $rg

## Command to get load balancer configuration
$bepool =
Get-AzLoadBalancer -Name $lb -ResourceGroupName $rg | Get-AzLoadBalancerBackendAddressPoolConfig

## Command to get network security group configuration ##
$nsg =
Get-AzNetworkSecurityGroup -Name $ngn -ResourceGroupName $rg

## Command to create network interface for VM1 ##
$nicVM1 =
New-AzNetworkInterface -ResourceGroupName $rg -Location $loc -Name $nic1 -LoadBalancerBackendAddressPool
$bepool -NetworkSecurityGroup $nsg -Subnet $vnet.Subnets[0]
```

VM 2

- Denominada **myNicVM2**.
- En el grupo de recursos **myResourceGroupLB**.
- En la ubicación **eastus**.
- En la red virtual **myVNet**.
- En la subred **myBackendSubnet**.
- En el grupo de seguridad de red **myNSG**.
- Conectada al equilibrador de carga **myLoadBalancer** en **myBackEndPool**.

```
## Variables for command ##
$rg = 'myResourceGroupLB'
$loc = 'eastus'
$nic2 = 'myNicVM2'
$vn1 = 'myVNet'
$lb = 'myLoadBalancer'
$ngn = 'myNSG'

## Command to get virtual network configuration. ##
$vn1 =
Get-AzVirtualNetwork -Name $vn1 -ResourceGroupName $rg

## Command to get load balancer configuration
$bepool =
Get-AzLoadBalancer -Name $lb -ResourceGroupName $rg | Get-AzLoadBalancerBackendAddressPoolConfig

## Command to get network security group configuration ##
$nsg =
Get-AzNetworkSecurityGroup -Name $ngn -ResourceGroupName $rg

## Command to create network interface for VM2 ##
$nicVM2 =
New-AzNetworkInterface -ResourceGroupName $rg -Location $loc -Name $nic2 -LoadBalancerBackendAddressPool
$bepool -NetworkSecurityGroup $nsg -Subnet $vn1.Subnets[0]
```

Creación de máquinas virtuales

Establezca un nombre de usuario de administrador y una contraseña para las máquinas virtuales con [Get-Credential](#):

```
$cred = Get-Credential
```

Cree las máquinas virtuales con:

- [New-AzVM](#)
- [New-AzVMConfig](#)
- [Set-AzVMOperatingSystem](#)
- [Set-AzVMSourceImage](#)
- [Add-AzVMNetworkInterface](#)

VM1

- Denominada **myVM1**.
- En el grupo de recursos **myResourceGroupLB**.
- Conectada a la interfaz de red **myNicVM1**.
- Conectada al equilibrador de carga **myLoadBalancer**.
- En **Zona 1**.
- En la ubicación **eastus**.

```
## Variables used for command. ##
$rg = 'myResourceGroupLB'
$vm = 'myVM1'
$siz = 'Standard_DS1_v2'
$pub = 'MicrosoftWindowsServer'
$off = 'WindowsServer'
$sku = '2019-Datacenter'
$ver = 'latest'
$zn = '1'
$loc = 'eastus'

## Create a virtual machine configuration. $cred and $nicVM1 are variables with configuration from the previous steps. ##

$vmConfig =
New-AzVMConfig -VMName $vm -VMSize $siz | Set-AzVMOperatingSystem -Windows -ComputerName $vm -Credential $cred
| Set-AzVMSourceImage -PublisherName $pub -Offer WindowsServer -Skus $sku -Version $ver | Add-
AzVMNetworkInterface -Id $nicVM1.Id

## Create the virtual machine ##
New-AzVM -ResourceGroupName $rg -Zone $zn -Location $loc -VM $vmConfig
```

VM2

- Denominada **myVM2**.
- En el grupo de recursos **myResourceGroupLB**.
- Conectada a la interfaz de red **myNicVM2**.
- Conectada al equilibrador de carga **myLoadBalancer**.
- En **Zona 2**.
- En la ubicación **eastus**.

```
## Variables used for command. ##
$rg = 'myResourceGroupLB'
$vm = 'myVM2'
$siz = 'Standard_DS1_v2'
$pub = 'MicrosoftWindowsServer'
$off = 'WindowsServer'
$sku = '2019-Datacenter'
$ver = 'latest'
$zn = '2'
$loc = 'eastus'

## Create a virtual machine configuration. $cred and $nicVM2 are variables with configuration from the previous steps. ##

$vmConfig =
New-AzVMConfig -VMName $vm -VMSize $siz | Set-AzVMOperatingSystem -Windows -ComputerName $vm -Credential $cred
| Set-AzVMSourceImage -PublisherName $pub -Offer WindowsServer -Skus $sku -Version $ver | Add-
AzVMNetworkInterface -Id $nicVM2.Id

## Create the virtual machine ##
New-AzVM -ResourceGroupName $rg -Zone $zn -Location $loc -VM $vmConfig
```

Instalación de IIS

Use [Set-AzVMExtension](#) para instalar la extensión de script personalizado.

La extensión ejecuta Add-WindowsFeature Web-Server de PowerShell para instalar el servidor web IIS y después actualiza la página Default.htm para mostrar el nombre de host de la máquina virtual:

VM1

```
## Variables for command. ##
$rg = 'myResourceGroupLB'
$enm = 'IIS'
$vmn = 'myVM1'
$loc = 'eastus'
$pub = 'Microsoft.Compute'
$ext = 'CustomScriptExtension'
$typ = '1.8'

Set-AzVMExtension -ResourceGroupName $rg -ExtensionName $enm -VMName $vmn -Location $loc -Publisher $pub -
ExtensionType $ext -TypeHandlerVersion $typ -SettingString '{"commandToExecute":"powershell Add-WindowsFeature
Web-Server; powershell Add-Content -Path \"C:\\inetpub\\wwwroot\\Default.htm\" -Value $($env:computername)}'
```

VM2

```
## Variables for command. ##
$rg = 'myResourceGroupLB'
$enm = 'IIS'
$vmn = 'myVM2'
$loc = 'eastus'
$pub = 'Microsoft.Compute'
$ext = 'CustomScriptExtension'
$typ = '1.8'

Set-AzVMExtension -ResourceGroupName $rg -ExtensionName $enm -VMName $vmn -Location $loc -Publisher $pub -
ExtensionType $ext -TypeHandlerVersion $typ -SettingString '{"commandToExecute":"powershell Add-WindowsFeature
Web-Server; powershell Add-Content -Path \"C:\\inetpub\\wwwroot\\Default.htm\" -Value $($env:computername)}'
```

Prueba del equilibrador de carga

Creación de la interfaz de red

Cree una interfaz de red con [New-AzNetworkInterface](#):

myTestVM

- Llamada **myNicTestVM**.
- En el grupo de recursos **myResourceGroupLB**.
- En la ubicación **eastus**.
- En la red virtual **myVNet**.
- En la subred **myBackendSubnet**.
- En el grupo de seguridad de red **myNSG**.


```
## Variables for command ##
$rg = 'myResourceGroupLB'
$loc = 'eastus'
$nic1 = 'myNicTestVM'
$vnt = 'myVNet'
$ngn = 'myNSG'

## Command to get virtual network configuration. ##
$vnet =
Get-AzVirtualNetwork -Name $vnt -ResourceGroupName $rg

## Command to get network security group configuration ##
$nsrg =
Get-AzNetworkSecurityGroup -Name $ngn -ResourceGroupName $rg

## Command to create network interface for myTestVM ##
$nicTestVM =
New-AzNetworkInterface -ResourceGroupName $rg -Location $loc -Name $nic1 -NetworkSecurityGroup $nsrg -Subnet
$vnet.Subnets[0]
```

Crear máquina virtual

Establezca un nombre de usuario de administrador y una contraseña para la máquina virtual con [Get-Credential](#):

```
$cred = Get-Credential
```

Cree la máquina virtual con:

- [New-AzVM](#)
- [New-AzVMConfig](#)
- [Set-AzVMOperatingSystem](#)
- [Set-AzVMSourceImage](#)
- [Add-AzVMNetworkInterface](#)

myTestVM

- Llamada **myTestVM**.
- En el grupo de recursos **myResourceGroupLB**.
- Conectada a la interfaz de red **myNicTestVM**.
- En la ubicación **eastus**.

```
## Variables used for command. ##
$rg = 'myResourceGroupLB'
$vm = 'myTestVM'
$siz = 'Standard_DS1_v2'
$pub = 'MicrosoftWindowsServer'
$off = 'WindowsServer'
$sku = '2019-Datacenter'
$ver = 'latest'
$loc = 'eastus'

## Create a virtual machine configuration. $cred and $nicTestVM are variables with configuration from the
previous steps. ##

$vmConfig =
New-AzVMConfig -VMName $vm -VMSize $siz | Set-AzVMOperatingSystem -Windows -ComputerName $vm -Credential $cred
| Set-AzVMSourceImage -PublisherName $pub -Offer WindowsServer -Skus $sku -Version $ver | Add-
AzVMNetworkInterface -Id $nicTestVM.Id

## Create the virtual machine ##
New-AzVM -ResourceGroupName $rg -Location $loc -VM $vmConfig
```

Prueba

1. [Inicie sesión](#) en Azure Portal.
2. Busque la dirección IP privada del equilibrador de carga en la pantalla **Información general**. Seleccione **Todos los servicios** en el menú de la izquierda, **Todos los recursos** y, después, **myLoadBalancer**.
3. Tome nota o copie la dirección que encontrará junto a **Dirección IP privada**, en la pestaña **Información general** de **myLoadBalancer**.
4. Seleccione **Todos los servicios** en el menú de la izquierda, seleccione **Todos los recursos** y, después, en la lista de recursos, seleccione **myTestVM**, que se encuentra en el grupo de recursos **myResourceGroupLB**.
5. En la página **Introducción**, seleccione **Conectar** y después **Instancia de Bastion**.
6. Escriba el nombre de usuario y la contraseña especificados durante la creación de la máquina virtual.
7. Abra **Internet Explorer** en **myTestVM**.
8. Escriba la dirección IP del paso anterior en la barra de direcciones del explorador. La página predeterminada del servidor web de IIS se muestra en el explorador.



Hello World from myVM1

Para ver el tráfico distribuido por Load Balancer entre las tres máquinas virtuales, puede personalizar la página predeterminada de cada servidor web IIS de las máquinas virtuales y luego forzar una actualización del explorador

web desde el equipo cliente.

Limpieza de recursos

Cuando ya no los necesite, puede usar el comando [Remove-AzResourceGroup](#) para quitar el grupo de recursos, el equilibrador de carga y el resto de los recursos.

```
## Variable for command. ##
$rg = 'myResourceGroupLB'

Remove-AzResourceGroup -Name $rg
```

Pasos siguientes

En esta guía de inicio rápido

- Ha creado un equilibrador de carga interno Básico o Estándar
- Conectó máquinas virtuales.
- Configuró la regla de tráfico del equilibrador de carga y el sondeo de estado.
- Probó el equilibrador de carga.

Para más información sobre Azure Load Balancer, consulte [¿Qué es Azure Load Balancer?](#) y [Preguntas frecuentes de Load Balancer](#).

- Más información sobre [Load Balancer y zonas de disponibilidad](#).

Inicio rápido: Creación de un equilibrador de carga interno para equilibrar la carga de las máquinas virtuales con la CLI de Azure

23/09/2020 • 29 minutes to read • [Edit Online](#)

Comience a usar Azure Load Balancer con la CLI de Azure para crear un equilibrador de carga público y tres máquinas virtuales.



Requisitos previos

- Una cuenta de Azure con una suscripción activa. [Cree una cuenta gratuita](#).
- CLI de Azure instalada localmente o Azure Cloud Shell

Uso de Azure Cloud Shell

En Azure se hospeda Azure Cloud Shell, un entorno de shell interactivo que puede utilizar mediante el explorador. Puede usar Bash o PowerShell con Cloud Shell para trabajar con los servicios de Azure. Puede usar los comandos preinstalados de Cloud Shell para ejecutar el código de este artículo sin tener que instalar nada en su entorno local.

Para iniciar Azure Cloud Shell:

OPCIÓN	EJEMPLO O VÍNCULO
Seleccione Pruébelo en la esquina superior derecha de un bloque de código. Solo con seleccionar Pruébelo no se copia automáticamente el código en Cloud Shell.	
Vaya a https://shell.azure.com o seleccione el botón Iniciar Cloud Shell para abrir Cloud Shell en el explorador.	
Seleccione el botón Cloud Shell en la barra de menús de la esquina superior derecha de Azure Portal .	

Para ejecutar el código de este artículo en Azure Cloud Shell:

1. Inicie Cloud Shell.
2. Seleccione el botón **Copiar** de un bloque de código para copiar el código.
3. Pegue el código en la sesión de Cloud Shell. Para ello, seleccione **Ctrl+Mayús+V** en Windows y Linux, o bien seleccione **Cmd+Mayús+V** en macOS.
4. Seleccione **Entrar** para ejecutar el código.

Si decide instalar y usar la CLI localmente, para esta guía de inicio rápido se necesita la versión 2.0.28 de la CLI de Azure o una versión posterior. Para encontrar la versión, ejecute `az --version`. Si necesita instalarla o actualizarla, consulte [Instalación de la CLI de Azure](#).

Crear un grupo de recursos

Un grupo de recursos de Azure es un contenedor lógico en el que se implementan y se administran los recursos de Azure.

Cree un grupo de recursos con [az group create](#):

- Denominado **myResourceGroupLB**.
- En la ubicación **eastus**.

```
az group create \  
  --name myResourceGroupLB \  
  --location eastus
```

- [SKU Estándar](#)
- [SKU básica](#)

NOTE

Se recomienda usar la SKU Estándar de Load Balancer para las cargas de trabajo de producción. Para más información sobre las SKU, consulte [SKU de Azure Load Balancer](#).

Configurar la red virtual

Antes de implementar las máquinas virtuales y el equilibrador de carga, cree los recursos de red virtual auxiliares.

Creación de una red virtual

Cree una red virtual con [az network vnet create](#):

- Denominada **myVNet**.
- Con el prefijo de dirección **10.1.0.0/16**.
- Subred denominada **MyBackendSubnet**.
- Con el prefijo de subred **10.1.0.0/24**.
- En el grupo de recursos **myResourceGroupLB**.
- Ubicación de **eastus**.

```
az network vnet create \  
  --resource-group myResourceGroupLB \  
  --location eastus \  
  --name myVNet \  
  --address-prefixes 10.1.0.0/16 \  
  --subnet-name myBackendSubnet \  
  --subnet-prefixes 10.1.0.0/24
```

Crear un grupo de seguridad de red

En el caso de un equilibrador de carga estándar, las VM de la dirección de back-end deben tener interfaces de red que pertenezcan a un grupo de seguridad de red.

Cree un grupo de seguridad de red con [az network nsg create](#):

- Denominado **myNSG**.
- En el grupo de recursos **myResourceGroupLB**.

```
az network nsg create \  
  --resource-group myResourceGroupLB \  
  --name myNSG
```

Creación de una regla de grupo de seguridad de red

Cree una regla de grupo de seguridad de red con el [az network nsg rule create](#):

- Denominada **myNSGRuleHTTP**.
- En el grupo de seguridad de red que creó en el paso anterior, **myNSG**.
- En el grupo de recursos **myResourceGroupLB**.
- Protocolo (*) .
- Dirección **Inbound**.
- Origen (*) .
- Destino: (*) .
- Puerto de destino **80**.
- Acceso: **Allow**.
- Prioridad **200**.

```
az network nsg rule create \  
  --resource-group myResourceGroupLB \  
  --nsg-name myNSG \  
  --name myNSGRuleHTTP \  
  --protocol '*' \  
  --direction inbound \  
  --source-address-prefix '*' \  
  --source-port-range '*' \  
  --destination-address-prefix '*' \  
  --destination-port-range 80 \  
  --access allow \  
  --priority 200
```

Creación de interfaces de red para las máquinas virtuales

Cree dos interfaces de red con [az network nic create](#):

VM1

- Denominada **myNicVM1**.
- En el grupo de recursos **myResourceGroupLB**.
- En la red virtual **myVNet**.
- En la subred **myBackendSubnet**.
- En el grupo de seguridad de red **myNSG**.

```
az network nic create \  
  --resource-group myResourceGroupLB \  
  --name myNicVM1 \  
  --vnet-name myVNet \  
  --subnet myBackEndSubnet \  
  --network-security-group myNSG
```

VM2

- Denominada **myNicVM2**.
- En el grupo de recursos **myResourceGroupLB**.
- En la red virtual **myVNet**.
- En la subred **myBackendSubnet**.

- En el grupo de seguridad de red **myNSG**.

```
az network nic create \  
  --resource-group myResourceGroupLB \  
  --name myNicVM2 \  
  --vnet-name myVnet \  
  --subnet myBackEndSubnet \  
  --network-security-group myNSG
```

Creación de servidores back-end

En esta sección, creará:

- Un archivo de configuración de nube denominado **cloud-init.txt** para la configuración del servidor.
- Dos máquinas virtuales que se usarán como servidores back-end para el equilibrador de carga.

Creación del archivo de configuración cloud-init

Use un archivo de configuración cloud-init para instalar NGINX y ejecutar una aplicación Node.js "Hola mundo" en una máquina virtual Linux.

En el shell actual, cree un archivo denominado cloud-init.txt. Copie el siguiente fragmento de código y péguelo en el shell. Asegúrese de copiar correctamente todo el archivo cloud-init, especialmente la primera línea:

```
#cloud-config
package_upgrade: true
packages:
- nginx
- nodejs
- npm
write_files:
- owner: www-data:www-data
- path: /etc/nginx/sites-available/default
  content: |
    server {
      listen 80;
      location / {
        proxy_pass http://localhost:3000;
        proxy_http_version 1.1;
        proxy_set_header Upgrade $http_upgrade;
        proxy_set_header Connection keep-alive;
        proxy_set_header Host $host;
        proxy_cache_bypass $http_upgrade;
      }
    }
- owner: azureuser:azureuser
- path: /home/azureuser/myapp/index.js
  content: |
    var express = require('express')
    var app = express()
    var os = require('os');
    app.get('/', function (req, res) {
      res.send('Hello World from host ' + os.hostname() + '!!')
    })
    app.listen(3000, function () {
      console.log('Hello world app listening on port 3000!')
    })
runcmd:
- service nginx restart
- cd "/home/azureuser/myapp"
- npm init
- npm install express -y
- nodejs index.js
```

Creación de máquinas virtuales

Cree las máquinas virtuales con [az vm create](#):

VM1

- Denominada **myVM1**.
- En el grupo de recursos **myResourceGroupLB**.
- Conectada a la interfaz de red **myNicVM1**.
- Imagen de máquina virtual **UbuntuLTS**.
- Archivo de configuración **cloud-init.txt** creado en el paso anterior.
- En **Zona 1**.


```
az vm create \  
  --resource-group myResourceGroupLB \  
  --name myVM1 \  
  --nics myNicVM1 \  
  --image UbuntuLTS \  
  --admin-user azureuser \  
  --generate-ssh-keys \  
  --custom-data cloud-init.txt \  
  --zone 1 \  
  --no-wait
```

VM2

- Denominada **myVM2**.
- En el grupo de recursos **myResourceGroupLB**.
- Conectada a la interfaz de red **myNicVM2**.
- Imagen de máquina virtual **UbuntuLTS**.
- Archivo de configuración **cloud-init.txt** creado en el paso anterior.
- En **Zona 2**.

```
az vm create \  
  --resource-group myResourceGroupLB \  
  --name myVM2 \  
  --nics myNicVM2 \  
  --image UbuntuLTS \  
  --admin-user azureuser \  
  --generate-ssh-keys \  
  --custom-data cloud-init.txt \  
  --zone 2 \  
  --no-wait
```

Puede que las VM tarden unos minutos en implementarse.

Creación de un equilibrador de carga estándar

En esta sección se detalla cómo se pueden crear y configurar los componentes siguientes del equilibrador de carga:

- Un grupo de direcciones IP de front-end que recibe el tráfico de red entrante en el equilibrador de carga.
- Un grupo de direcciones IP de back-end al que el grupo de servidores front-end envía el tráfico de red de carga equilibrada.
- Un sondeo de estado que determina el estado de las instancias de máquina virtual de back-end.
- Una regla de equilibrador de carga que define cómo se distribuye el tráfico a las VM.

Creación del recurso del equilibrador de carga

Cree un equilibrador de carga público con [az network lb create](#):

- Denominado **myLoadBalancer**.
- Un grupo de front-end denominado **MyFrontEnd**.
- Un grupo de back-end denominado **myBackendPool**
- Asociado a la red virtual **myVNet**.
- Asociado a la subred de back-end **myBackendSubnet**.

```
az network lb create \  
  --resource-group myResourceGroupLB \  
  --name myLoadBalancer \  
  --sku Standard \  
  --vnet-name myVnet \  
  --subnet myBackendSubnet \  
  --frontend-ip-name myFrontEnd \  
  --backend-pool-name myBackEndPool
```

Creación del sondeo de estado

Los sondeos de estado comprueban todas las instancias de máquina virtual para asegurarse de que pueden enviar tráfico de red.

Una máquina virtual con una comprobación de sondeo con errores se quita del equilibrador de carga. La máquina virtual se agrega de nuevo al equilibrador de carga cuando se resuelve el error.

Cree un sondeo de estado con [az network lb probe create](#):

- Supervisa el estado de las máquinas virtuales.
- Denominado **myHealthProbe**.
- Protocolo **TCP**.
- **Puerto 80** de supervisión.

```
az network lb probe create \  
  --resource-group myResourceGroupLB \  
  --lb-name myLoadBalancer \  
  --name myHealthProbe \  
  --protocol tcp \  
  --port 80
```

Creación de la regla de equilibrador de carga

Una regla de equilibrador de carga define:

- La configuración de IP del front-end para el tráfico entrante.
- El grupo de IP de back-end para recibir el tráfico.
- Los puertos de origen y de destino requeridos.

Cree una regla de equilibrador de carga con [az network lb rule create](#):

- Denominada **myHTTPRule**.
- Que escuche en el **puerto 80** en el grupo de front-end **myFrontEnd**.
- Que envíe el tráfico de red con equilibrio de carga al grupo de direcciones de back-end **myBackEndPool** a través del **Puerto 80**.
- Mediante el sondeo de estado **myHealthProbe**.
- Protocolo **TCP**.
- Habilite la traducción de direcciones de red de origen (SNAT) de salida mediante la dirección IP de front-end.

```
az network lb rule create \  
  --resource-group myResourceGroupLB \  
  --lb-name myLoadBalancer \  
  --name myHTTPTRule \  
  --protocol tcp \  
  --frontend-port 80 \  
  --backend-port 80 \  
  --frontend-ip-name myFrontEnd \  
  --backend-pool-name myBackEndPool \  
  --probe-name myHealthProbe \  
  --disable-outbound-snat true
```

NOTE

Las máquinas virtuales del grupo de back-end no tendrán conectividad de salida a Internet con esta configuración. Para más información acerca de cómo proporcionar conectividad de salida, consulte:

[Conexiones salientes en Azure](#)

Opciones para proporcionar conectividad:

[Configuración del equilibrador de carga solo de salida](#)

[¿Qué es NAT de Virtual Network?](#)

Adición de máquinas virtuales al grupo de back-end del equilibrador de carga

Agregue las máquinas virtuales al grupo de back-end con [az network nic ip-config address-pool add](#):

VM1

- En el grupo de direcciones de back-end **myBackEndPool**.
- En el grupo de recursos **myResourceGroupLB**.
- Asociada a la interfaz de red **myNicVM1** e **ipconfig1**.
- Asociada al equilibrador de carga **myLoadBalancer**.

```
az network nic ip-config address-pool add \  
  --address-pool myBackEndPool \  
  --ip-config-name ipconfig1 \  
  --nic-name myNicVM1 \  
  --resource-group myResourceGroupLB \  
  --lb-name myLoadBalancer
```

VM2

- En el grupo de direcciones de back-end **myBackEndPool**.
- En el grupo de recursos **myResourceGroupLB**.
- Asociada a la interfaz de red **myNicVM2** e **ipconfig1**.
- Asociada al equilibrador de carga **myLoadBalancer**.

```
az network nic ip-config address-pool add \  
  --address-pool myBackEndPool \  
  --ip-config-name ipconfig1 \  
  --nic-name myNicVM2 \  
  --resource-group myResourceGroupLB \  
  --lb-name myLoadBalancer
```

Prueba del equilibrador de carga

Creación de una dirección IP pública de Azure Bastion

Use [az network public-ip create](#) para crear una dirección IP pública para el host bastión:

- Cree una dirección IP pública con redundancia de zona estándar llamada **myBastionIP**.
- En **myResourceGroupLB**.

```
az network public-ip create \  
  --resource-group myResourceGroupLB \  
  --name myBastionIP \  
  --sku Standard
```

Creación de una subred de Azure Bastion

Use [az network vnet subnet create](#) para crear una subred:

- Llamada **AzureBastionSubnet**.
- Con el prefijo de dirección **10.1.1.0/24**.
- En la red virtual **myVNet**.
- En el grupo de recursos **myResourceGroupLB**.

```
az network vnet subnet create \  
  --resource-group myResourceGroupLB \  
  --name AzureBastionSubnet \  
  --vnet-name myVNet \  
  --address-prefixes 10.1.1.0/24
```

Creación de un host de Azure Bastion

Use [az network bastion create](#) para crear un host bastión:

- Llamado **myBastionHost**.
- En **myResourceGroupLB**.
- Asociado a la dirección IP pública **myBastionIP**.
- Asociado a la red virtual **myVNet**.
- En la ubicación **eastus**.

```
az network bastion create \  
  --resource-group myResourceGroupLB \  
  --name myBastionHost \  
  --public-ip-address myBastionIP \  
  --vnet-name myVNet \  
  --location eastus
```

El host bastión tardará unos minutos en implementarse.

Creación de una máquina virtual de prueba

Cree la interfaz de red con [az network nic create](#):

- Llamada **myNicTestVM**.
- En el grupo de recursos **myResourceGroupLB**.
- En la red virtual **myVNet**.
- En la subred **myBackendSubnet**.
- En el grupo de seguridad de red **myNSG**.

```
az network nic create \  
  --resource-group myResourceGroupLB \  
  --name myNicTestVM \  
  --vnet-name myVNet \  
  --subnet myBackEndSubnet \  
  --network-security-group myNSG
```

Cree la máquina virtual con [az vm create](#):

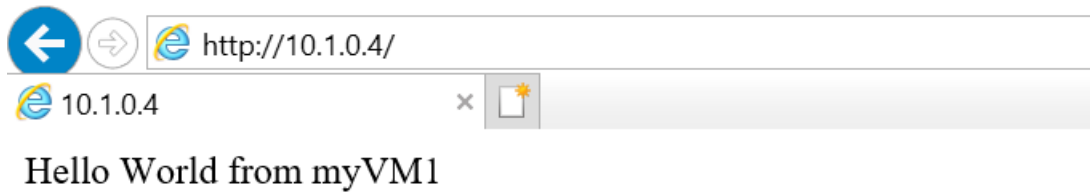
- Llamada **myTestVM**.
- En el grupo de recursos **myResourceGroupLB**.
- Conectada a la interfaz de red **myNicTestVM**.
- Con la imagen de máquina virtual **Win2019Datacenter**.
- Elija los valores de **<adminpass>** y **<adminuser>** .

```
az vm create \  
  --resource-group myResourceGroupLB \  
  --name myTestVM \  
  --nics myNicTestVM \  
  --image Win2019Datacenter \  
  --admin-username <adminuser> \  
  --admin-password <adminpass> \  
  --no-wait
```

La implementación de la máquina virtual puede tardar unos minutos.

Prueba

1. [Inicie sesión](#) en Azure Portal.
2. Busque la dirección IP privada del equilibrador de carga en la pantalla **Información general**. Seleccione **Todos los servicios** en el menú de la izquierda, **Todos los recursos** y, después, **myLoadBalancer**.
3. Tome nota o copie la dirección que encontrará junto a **Dirección IP privada**, en la pestaña **Información general** de **myLoadBalancer**.
4. Seleccione **Todos los servicios** en el menú de la izquierda, seleccione **Todos los recursos** y, después, en la lista de recursos, seleccione **myTestVM**, que se encuentra en el grupo de recursos **myResourceGroupLB**.
5. En la página **Introducción**, seleccione **Conectar** y después **Instancia de Bastion**.
6. Escriba el nombre de usuario y la contraseña especificados durante la creación de la máquina virtual.
7. Abra **Internet Explorer** en **myTestVM**.
8. Escriba la dirección IP del paso anterior en la barra de direcciones del explorador. La página predeterminada del servidor web de IIS se muestra en el explorador.



Para ver el tráfico distribuido por Load Balancer entre las tres máquinas virtuales, puede personalizar la página predeterminada de cada servidor web IIS de las máquinas virtuales y luego forzar una actualización del explorador web desde el equipo cliente.

Limpieza de recursos

Cuando ya no se necesiten, use el comando `az group delete` para quitar el grupo de recursos, el equilibrador de carga y todos los recursos relacionados.

```
az group delete \
  --name myResourceGroupLB
```

Pasos siguientes

En esta guía de inicio rápido

- Creó un equilibrador de carga estándar o público.
- Conectó máquinas virtuales.
- Configuró la regla de tráfico del equilibrador de carga y el sondeo de estado.
- Probó el equilibrador de carga.

Para más información sobre Azure Load Balancer, consulte [¿Qué es Azure Load Balancer?](#) y [Preguntas frecuentes de Load Balancer](#).

Más información sobre [Load Balancer y zonas de disponibilidad](#).

Tutorial: Equilibrio de carga de máquinas virtuales en distintas zonas de disponibilidad con Load Balancer Estándar mediante Azure Portal

23/09/2020 • 19 minutes to read • [Edit Online](#)

El equilibrio de carga proporciona un mayor nivel de disponibilidad al distribuir las solicitudes entrantes entre varias máquinas virtuales. En este tutorial, se explican los pasos necesarios para crear una instancia de Standard Load Balancer público que equilibre la carga de las máquinas virtuales entre zonas de disponibilidad. Esto le ayudará a proteger sus aplicaciones y sus datos en el caso improbable de que se produzca una pérdida o un error en la totalidad de un centro de datos. Con la redundancia de zona, aunque se produzcan errores en una o varias zonas de disponibilidad, la ruta de los datos puede mantenerse a salvo siempre que una zona de la región permanezca en buen estado. Aprenderá a:

- Crear un equilibrador de carga estándar
- Crear grupos de seguridad de red para definir las reglas de tráfico de entrada
- Crear máquinas virtuales con redundancia de zona entre diferentes zonas y atribuir las a un equilibrador de carga
- Crear un sondeo de estado de un equilibrador de carga
- Crear reglas de tráfico del equilibrador de carga
- Crear un sitio de IIS básico
- Ver un equilibrador de carga en acción

Para más información sobre cómo usar las zonas de disponibilidad con Load Balancer Estándar, consulte [Load Balancer Estándar y zonas de disponibilidad](#).

Si lo prefiere, puede realizar los pasos de este artículo con la [CLI de Azure](#).

Si no tiene una suscripción a Azure, cree una [cuenta gratuita](#) antes de empezar.

Inicio de sesión en Azure

Inicie sesión en Azure Portal en <https://portal.azure.com>.

Crear un equilibrador de carga estándar

La versión Estándar de Load Balancer solo admite direcciones IP públicas estándar. Cuando se crea una dirección IP pública nueva al crear el equilibrador de carga, se configura automáticamente como una versión de la SKU Estándar y también tiene automáticamente redundancia de zona.

1. En la parte superior izquierda de la pantalla, haga clic en **Crear un recurso** > **Redes** > **Azure Load Balancer**.
2. En la pestaña **Datos básicos** de la página **Crear equilibrador de carga**, escriba o seleccione la siguiente información, acepte los valores predeterminados del resto de la configuración y, luego, seleccione **Revisar y crear**:

CONFIGURACIÓN	VALUE
Suscripción	Seleccione su suscripción.

CONFIGURACIÓN	VALUE
Resource group	Seleccione Crear nuevo y escriba <i>MyResourceGroupLBAZ</i> en el cuadro de texto.
Nombre	<i>myLoadBalancer</i>
Region	Seleccione Oeste de Europa .
Tipo	Seleccione Público .
SKU	Seleccione Estándar .
Dirección IP pública	Seleccione Crear nuevo .
Nombre de la dirección IP pública	Escriba <i>myPublicIP</i> en el cuadro de texto.
Zona de disponibilidad	Seleccione Redundancia de zona .

Creación de servidores back-end

En esta sección, creará una red virtual y máquinas virtuales en diferentes zonas de la región. Después, instalará IIS en las máquinas virtuales para que le ayude a probar el equilibrador de carga con redundancia de zona. Por lo tanto, si se produce un error en una zona, se produce un error en el sondeo de estado de la máquina virtual en la misma zona y continúa el tráfico servido por las máquinas virtuales de las demás zonas.

Red virtual y parámetros

En los pasos de esta sección, tendrá que reemplazar los siguientes parámetros por la siguiente información:

PARÁMETRO	VALUE
<resource-group-name>	myResourceGroupLBAZ (seleccione el grupo de recursos existente)
<virtual-network-name>	myVNet
<region-name>	Oeste de Europa
<IPv4-address-space>	10.0.0.0/16
<subnet-name>	myBackendSubnet
<subnet-address-range>	10.0.0.0/24

Crear la red virtual

En esta sección, creará una red virtual y una subred.

1. En la parte superior izquierda de la pantalla, seleccione **Crear un recurso > Redes > Red virtual** o busque **Red virtual** en el cuadro de búsqueda.
2. En **Crear red virtual**, escriba o seleccione esta información en la pestaña **Conceptos básicos**:

CONFIGURACIÓN	VALOR
Detalles del proyecto	
Suscripción	Selección de su suscripción a Azure
Grupo de recursos	Seleccione Crear nuevo , escriba <resource-group-name> , seleccione Aceptar o seleccione un <resource-group-name> existente basado en parámetros.
Detalles de instancia	
Nombre	Escriba <virtual-network-name>
Region	Selección de <region-name>

3. Seleccione la pestaña **Direcciones IP** o el botón **Siguiente: Direcciones IP** situado en la parte inferior de la página.

4. En la pestaña **Direcciones IP**, especifique esta información:

CONFIGURACIÓN	VALUE
Espacio de direcciones IPv4	Escriba <IPv4-address-space>

5. En **Nombre de subred**, seleccione la palabra **predeterminada**.

6. En **Editar subred**, especifique esta información:

CONFIGURACIÓN	VALUE
Nombre de subred	Escriba <subnet-name>
Intervalo de direcciones de subred	Escriba <subnet-address-range>

7. Seleccione **Guardar**.

8. Seleccione la pestaña **Revisar y crear** o el botón **Revisar y crear**.

9. Seleccione **Crear**.

Crear un grupo de seguridad de red

Cree un grupo de seguridad de red para definir las conexiones entrantes a la red virtual.

- En la parte superior izquierda de la pantalla, haga clic en **Crear un recurso**, en el cuadro de búsqueda, escriba *Grupo de seguridad de red*, en la página del grupo de seguridad de red, haga clic en **Crear**.
- En la página **Crear grupo de seguridad de red**, escriba estos valores:
 - myNetworkSecurityGroup*: como nombre del grupo de seguridad de red.
 - myResourceGroupLBAZ*: como nombre del grupo de recursos existente.

Home > New > Marketplace > Everything > Network > Network security groups

Create network security group

* Name
myNetworkSecurityGroup ✓

* Subscription
Kumud's subscription ✓

* Resource group
☐ Create new ☒ Use existing

myResourceGroupLBAZ ✓

* Location
West Europe ✓

☐ Pin to dashboard

Create [Automation options](#)

Creación de reglas de grupo de seguridad de red

En esta sección, va a crear reglas de grupo de seguridad de red para permitir conexiones entrantes que usen HTTP y RDP mediante Azure Portal.

1. En Azure Portal, haga clic en **Todos los recursos** en el menú de la izquierda y, a continuación, busque y haga clic en **myNetworkSecurityGroup**, que se encuentra en el grupo de recursos **myResourceGroupLBAZ**.
2. En **Configuración**, haga clic en **Reglas de seguridad de entrada** y, después, en **Agregar**.
3. Especifique estos valores para la regla de seguridad de entrada llamada *myHTTPRule* para permitir que las conexiones HTTP entrantes usen el puerto 80:
 - *Etiqueta de servicio*: en **Origen**.
 - *Internet*: en **Etiqueta de servicio de origen**
 - *80*: en **Intervalos de puerto de destino**
 - *TCP*: en **Protocolo**
 - *Permitir*: en **Acción**
 - *100* en **Prioridad**
 - *myHTTPRule*: en el nombre de la regla del equilibrador de carga
 - *Allow HTTP* (Permitir HTTP): en la descripción de la regla del equilibrador de carga
4. Haga clic en **OK**.

Add inbound security rule

myNetworkSecurityGroup

Basic

* Source ⓘ

Service Tag

* Source service tag ⓘ

Internet

* Source port ranges ⓘ

*

* Destination ⓘ

Any

* Destination port ranges ⓘ

80

* Protocol

Any TCP UDP

* Action

Allow Deny

* Priority ⓘ

100

* Name

myHTTPRule

Description

Allow HTTP

OK

5. Repita los pasos 2 a 4 para crear otra regla llamada *myRDPRule* que permita una conexión RDP entrante con el puerto 3389 con los valores siguientes:

- *Etiqueta de servicio*: en Origen.
- *Internet*: en Etiqueta de servicio de origen
- *3389*: en Intervalos de puerto de destino
- *TCP*: en Protocolo
- *Permitir*: en Acción
- *200* en Prioridad

- *myRDPRule* como nombre
- *Permitir RDP* como descripción

Creación de máquinas virtuales

Cree máquinas virtuales en distintas zonas (zona 1, zona 2 y zona 3) de la región que puedan actuar como servidores back-end en el equilibrador de carga.

1. En la parte superior izquierda de la pantalla, haga clic en **Crear un recurso** > **Proceso** > **Windows Server 2016 Datacenter** y especifique estos valores para la máquina virtual:
 - *myVM1*: como el nombre de la máquina virtual.
 - *azureuser*: como nombre del usuario administrador.
 - *myResourceGroupLBAZ*: como **grupo de recursos**. Seleccione **Usar existente** y, después, seleccione *myResourceGroupLBAZ*.
2. Haga clic en **OK**.
3. Seleccione **DS1_V2** como tamaño de la máquina virtual y haga clic en **Seleccionar**.
4. Especifique estos valores para la configuración de la máquina virtual:
 - *zona 1*: para la zona en la que va a situar la máquina virtual.
 - *myVNet*: asegúrese de que se selecciona como red virtual.
 - *myBackendSubnet*: asegúrese de que se selecciona como subred.
 - *myNetworkSecurityGroup*: como nombre del grupo de seguridad de red (firewall).
5. Haga clic en **Deshabilitado** para deshabilitar los diagnósticos de arranque.
6. Haga clic en **Aceptar**, revise la configuración en la página de resumen y haga clic en **Crear**.
7. Cree una segunda máquina virtual llamada *VM2* en la Zona 2 y una tercera máquina virtual en la Zona 3, con *myVnet* como la red virtual, *myBackendSubnet* como la subred y **myNetworkSecurityGroup* como el grupo de seguridad de red mediante los pasos del 1 al 6.

Instalación de IIS en las máquinas virtuales

1. Haga clic en **Todos los recursos** en el menú de la izquierda y, después, en la lista de recursos haga clic en **myVM1**, que se encuentra en el grupo de recursos *myResourceGroupLBAZ*.
2. En la página **Información general**, haga clic en **Conectar a RDP** en la máquina virtual.
3. Inicie sesión en la máquina virtual con el nombre de usuario *azureuser*.
4. En el escritorio del servidor, vaya a **Herramientas administrativas de Windows** > **Windows PowerShell**.
5. En la ventana de PowerShell, ejecute los comandos siguientes para instalar el servidor IIS, eliminar el archivo *iisstart.htm* predeterminado y agregar uno nuevo que muestre el nombre de la máquina virtual:

```
# install IIS server role
Install-WindowsFeature -name Web-Server -IncludeManagementTools

# remove default htm file
remove-item C:\inetpub\wwwroot\iisstart.htm

# Add a new htm file that displays server name
Add-Content -Path "C:\inetpub\wwwroot\iisstart.htm" -Value $("Hello World from" + $env:computername)
```

6. Cierre la sesión de RDP con *myVM1*.
7. Repita los pasos 1 a 6 para instalar IIS y el archivo *iisstart.htm* actualizado en *myVM2* y *myVM3*.

Creación de recursos del equilibrador de carga

En esta sección, va a configurar el equilibrador de carga para un grupo de direcciones de back-end y un sondeo de mantenimiento, y a especificar el equilibrador de carga y las reglas NAT.

Creación de un grupo de direcciones de back-end

Para distribuir el tráfico a las máquinas virtuales, un grupo de direcciones de back-end contiene las direcciones IP de las tarjetas de interfaz de red (NIC) virtual conectadas al equilibrador de carga. Cree el grupo de direcciones de back-end *myBackendPool* para incluir *VM1*, *VM2* y *VM3*.

1. Haga clic en **Todos los recursos** en el menú de la izquierda y, después, haga clic en **myLoadBalancer** en la lista de recursos.
2. En **Configuración**, haga clic en **Grupos de back-end** y luego en **Agregar**.
3. En la página **Agregar grupo back-end**, realice lo siguiente:
 - En el nombre, escriba *myBackendPool* como nombre del grupo de servidores back-end.
 - Para **Red virtual**, en el menú desplegable, haga clic en **myVNet**
 - Para **Máquina virtual**, en el menú desplegable, haga clic en **myVM1**.
 - Para **Dirección IP**, en el menú desplegable, haga clic en la dirección IP de *myVM1*.
4. Haga clic en **Agregar nuevo recurso de back-end** para agregar cada máquina virtual (*myVM2* y *myVM3*) al grupo de back-end del equilibrador de carga.
5. Haga clic en **Agregar**.

Home > Resource groups > myResourceGroupLBaz > myPublicLoadBalancer - Backend pools > Add backend pool

Add backend pool

myPublicLoadBalancer

* Name
myBackendPool ✓

IP version ⓘ
IPv4

* Virtual network ⓘ
myvnet (3 VM) ▼

Name: myvm1 RG: myresourcegrouplbaz IP: 10.0.0.7 Type: Virtual machine	✕
Name: myvm2 RG: myresourcegrouplbaz IP: 10.0.0.8 Type: Virtual machine	✕

Virtual machine
myvm3 ▼

IP address
ipconfig1 (10.0.0.9) ▼

Add new backend resource

Add

6. Compruebe que la configuración del grupo de back-end del equilibrador de carga muestra las tres máquinas virtuales: *myVM1*, *myVM2* y *myVM3*.

Creación de un sondeo de estado

Para permitir que el equilibrador de carga supervise el estado de la aplicación, utilice un sondeo de estado. El sondeo de estado agrega o quita de forma dinámica las máquinas virtuales de la rotación del equilibrador de carga en base a su respuesta a las comprobaciones de estado. Cree un sondeo de estado, *myHealthProbe*, para supervisar el estado de las máquinas virtuales.

1. Haga clic en **Todos los recursos** en el menú de la izquierda y, después, haga clic en **myLoadBalancer** en la lista de recursos.

2. En **Configuración**, haga clic en **Sondeos de estado** y luego en **Agregar**.
3. Use estos valores para crear el sondeo de estado:
 - *myHealthProbe*: como nombre del sondeo de estado.
 - **HTTP**: en tipo de protocolo.
 - **80**: en número de puerto.
 - **15**: como número de **Intervalo**, en segundos, entre los intentos de sondeo.
 - **2**: como número de **Umbral incorrecto** o errores de sondeo consecutivos que deben producirse para que una máquina virtual se considere que no funciona de manera incorrecta.
4. Haga clic en **OK**.

... > MyResourceGroupLBAZ > myLoadBalancer - Health probes > Add health probe

Add health probe

myLoadBalancer

Name *

myHealthProbe ✓

Protocol ⓘ

TCP ✓

Port * ⓘ

80

Interval * ⓘ

15 ✓

seconds

Unhealthy threshold * ⓘ

2

consecutive failures

OK

Creación de una regla de equilibrador de carga

Las reglas de equilibrador de carga se utilizan para definir cómo se distribuye el tráfico a las máquinas virtuales. Se define la configuración de IP front-end para el tráfico entrante y el grupo IP de back-end para recibir el tráfico, junto con el puerto de origen y destino requeridos. Cree una regla de Load Balancer *myLoadBalancerRuleWeb* para escuchar el puerto 80 en el front-end *FrontendLoadBalancer* y enviar tráfico de red con equilibrio de carga al conjunto de direcciones back-end, *myBackEndPool*, que también usan el puerto 80.

1. Haga clic en **Todos los recursos** en el menú de la izquierda y, después, haga clic en **myLoadBalancer** en la lista de recursos.
2. En **Configuración**, haga clic en **Reglas de equilibrio de carga** y luego en **Agregar**.
3. Use estos valores para configurar la regla de equilibrio de carga:
 - *myHTTPRule*: como nombre de la regla de equilibrio de carga.

- TCP: en tipo de protocolo.
- 80: en número de puerto.
- 80: como puerto de back-end.
- *myBackendPool*: como nombre del grupo back-end.
- *myHealthProbe*: como nombre del sondeo de estado.

4. Haga clic en OK.

Home > Resource groups > myResourceGroupLBAZ > myPublicLoadBalancer - Load balancing rules > Add load balancing rule

Add load balancing rule

myPublicLoadBalancer

* Name
myHTTPRule

* IP Version
☒ IPv4 ☐ IPv6

* Frontend IP address ⓘ
40.67.218.153 (LoadBalancerFrontEnd)

Protocol
☒ TCP ☐ UDP

* Port
80

* Backend port ⓘ
80

Backend pool ⓘ
myBackendPool (3 virtual machines)

Health probe ⓘ
myHealthProbe (TCP:80)

Session persistence ⓘ
None

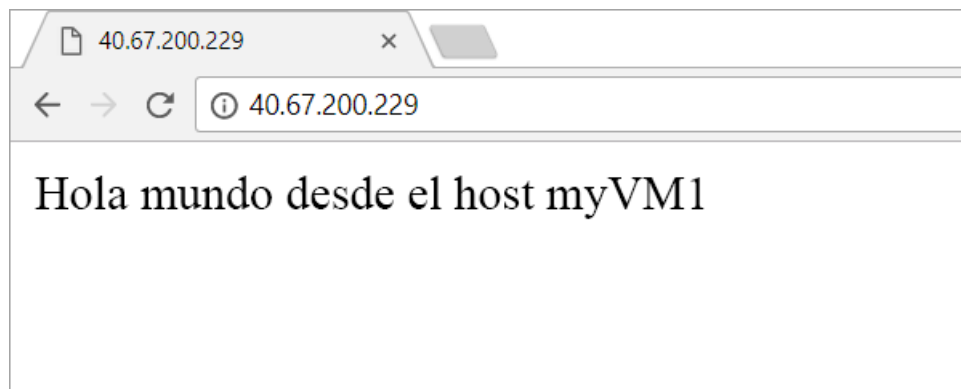
Idle timeout (minutes) ⓘ
4

Floating IP (direct server return) ⓘ
Disabled Enabled

OK

Prueba del equilibrador de carga

1. Busque la dirección IP pública de Load Balancer en la pantalla **Información general**. Haga clic en **Todos los recursos** y, después, en **myPublicIP**.
2. Copie la dirección IP pública y péguela en la barra de direcciones del explorador. La página predeterminada del servidor web de IIS se muestra en el explorador.



Para ver cómo el equilibrador de carga reparte el tráfico entre las máquinas virtuales distribuidas por la zona, puede realizar una actualización forzada del explorador web.

Limpieza de recursos

Cuando no los necesite, elimine el grupo de recursos, el equilibrador de carga y todos los recursos relacionados. Para ello, seleccione el grupo de recursos que contiene el equilibrador de carga y haga clic en **Eliminar**.

Pasos siguientes

Más información acerca de [Load Balancer Estándar](#).

Tutorial: Equilibrio de carga de máquinas virtuales en una zona de disponibilidad con Standard Load Balancer mediante Azure Portal

23/09/2020 • 18 minutes to read • [Edit Online](#)

En este tutorial se crea una instancia de [Azure Standard Load Balancer](#) pública con un front-end de zona que usa una dirección IP pública estándar mediante Azure Portal. En este escenario, puede especificar una zona determinada para las instancias de front-end y back-end para alinear la ruta de acceso a los datos y los recursos con una zona específica. Aprenderá a realizar las siguientes funciones:

- Crear una instancia de Standard Load Balancer con un front-end de zona.
- Crear grupos de seguridad de red para definir las reglas de tráfico de entrada.
- Crear máquinas virtuales de zona y conectarlas a un equilibrador de carga.
- Crear un sondeo de mantenimiento del equilibrador de carga.
- Crear reglas de tráfico del equilibrador de carga.
- Crear un sitio de Internet Information Services (IIS) básico.
- Visualizar un equilibrador de carga en acción.

Para más información sobre cómo usar las zonas de disponibilidad con Standard Load Balancer, consulte [Standard Load Balancer y Availability Zones](#).

Si lo prefiere, utilice la [CLI de Azure](#) para completar este tutorial.

Inicio de sesión en Azure

Inicie sesión en Azure Portal en <https://portal.azure.com>.

Creación de una instancia de Standard Load Balancer pública

Standard Load Balancer solo admite direcciones IP públicas estándar. Cuando se crea una dirección IP pública nueva al crear el equilibrador de carga, se configura automáticamente como una versión de la SKU Estándar. También tiene automáticamente redundancia de zona.

1. En la parte superior izquierda de la pantalla, seleccione **Crear un recurso** > **Redes** > **Load Balancer**.
2. En la pestaña **Datos básicos** de la página **Crear equilibrador de carga**, escriba o seleccione la siguiente información, acepte los valores predeterminados del resto de la configuración y, luego, seleccione **Revisar y crear**:

CONFIGURACIÓN	VALUE
Subscription	Seleccione su suscripción.
Resource group	Seleccione Crear nuevo y escriba <i>MyResourceGroupZLB</i> en el cuadro de texto.
Nombre	<i>myLoadBalancer</i>
Region	Seleccione Oeste de Europa .

CONFIGURACIÓN	VALUE
Tipo	Seleccione Público .
SKU	Seleccione Estándar .
Dirección IP pública	Seleccione Crear nuevo .
Nombre de la dirección IP pública	Escriba <i>myPublicIP</i> en el cuadro de texto.
Zona de disponibilidad	Seleccione 1 .

3. En la pestaña **Revisar y crear**, haga clic en **Crear**.

Creación de servidores back-end

En esta sección, creará una red virtual. También creará dos máquinas virtuales en la misma zona (es decir, la zona 1) para la región que desea agregar al grupo de back-end del equilibrador de carga. A continuación, se instala IIS en las máquinas virtuales para ayudar a probar el equilibrador de carga con redundancia de zona. Si se produce un error en una máquina virtual, se produce un error en el sondeo de mantenimiento de la máquina virtual en la misma zona. El tráfico continúa en otras máquinas virtuales dentro de la misma zona.

Red virtual y parámetros

En los pasos de esta sección, tendrá que reemplazar los siguientes parámetros por la siguiente información:

PARÁMETRO	VALUE
<resource-group-name>	myResourceGroupZLB (seleccione el grupo de recursos existente)
<virtual-network-name>	myVNet
<region-name>	Oeste de Europa
<IPv4-address-space>	10.0.0.0\16
<subnet-name>	myBackendSubnet
<subnet-address-range>	10.0.0.0\24

Crear la red virtual

En esta sección, creará una red virtual y una subred.

1. En la parte superior izquierda de la pantalla, seleccione **Crear un recurso > Redes > Red virtual** o busque **Red virtual** en el cuadro de búsqueda.
2. En **Crear red virtual**, escriba o seleccione esta información en la pestaña **Conceptos básicos**:

CONFIGURACIÓN	VALOR
Detalles del proyecto	

CONFIGURACIÓN	VALOR
Suscripción	Selección de su suscripción a Azure
Grupo de recursos	Seleccione Crear nuevo , escriba <resource-group-name> , seleccione Aceptar o seleccione un <resource-group-name> existente basado en parámetros.
Detalles de instancia	
Nombre	Escriba <virtual-network-name>
Region	Selección de <region-name>

3. Seleccione la pestaña **Direcciones IP** o el botón **Siguiente: Direcciones IP** situado en la parte inferior de la página.
4. En la pestaña **Direcciones IP**, especifique esta información:

CONFIGURACIÓN	VALUE
Espacio de direcciones IPv4	Escriba <IPv4-address-space>

5. En **Nombre de subred**, seleccione la palabra **predeterminada**.
6. En **Editar subred**, especifique esta información:

CONFIGURACIÓN	VALUE
Nombre de subred	Escriba <subnet-name>
Intervalo de direcciones de subred	Escriba <subnet-address-range>

7. Seleccione **Guardar**.
8. Seleccione la pestaña **Revisar y crear** o el botón **Revisar y crear**.
9. Seleccione **Crear**.

Crear un grupo de seguridad de red

1. En la parte superior izquierda de la pantalla, seleccione **Crear un recurso**. En el cuadro de búsqueda, escriba **Grupo de seguridad de red**. En la página Grupo de seguridad de red, seleccione **Crear**.
2. En la página **Crear grupo de seguridad de red**, escriba estos valores:
 - **myNetworkSecurityGroup** como nombre del grupo de seguridad de red.
 - **myResourceGroupLBAZ** como nombre del grupo de recursos existente.

Creación de reglas de NSG

En esta sección, se crean reglas de NSG para permitir conexiones entrantes que usen HTTP y Microsoft Remote Desktop Protocol (RDP) mediante Azure Portal.

1. Seleccione **Todos los recursos** en el menú de la izquierda de Azure Portal. A continuación, busque y seleccione **myNetworkSecurityGroup**. Se encuentra en el grupo de recursos **myResourceGroupZLB**.
2. En **Configuración**, seleccione **Reglas de seguridad de entrada**. A continuación, seleccione **Agregar**.
3. Especifique los siguientes valores para la regla de seguridad de entrada llamada **myHTTPRule** para permitir que las conexiones HTTP entrantes usen el puerto 80:
 - **Etiqueta de servicio** en Origen.
 - **Internet** en Etiqueta de servicio de origen.
 - **80** en Intervalos de puerto de destino.
 - **vTCP** en Protocolo.
 - **Permitir** en Acción.
 - **100** en Prioridad.
 - **myHTTPRule** en Nombre.
 - **Permitir HTTP** en Descripción.
4. Seleccione **Aceptar**.

Add inbound security rule

myNetworkSecurityGroup

Basic

* Source ⓘ

Service Tag

* Source service tag ⓘ

Internet

* Source port ranges ⓘ

*

* Destination ⓘ

Any

* Destination port ranges ⓘ

80

* Protocol

Any

TCP

UDP

* Action

Allow

Deny

* Priority ⓘ

100

* Name

myHTTPRule

Description

Allow HTTP

OK

5. Repita los pasos 2 a 4 para crear otra regla llamada **myRDPRule**. Esta regla permite una conexión RDP entrante que usa el puerto 3389, con los valores siguientes:

- **Etiqueta de servicio en Origen.**
- **Internet en Etiqueta de servicio de origen.**
- **3389 en Intervalos de puerto de destino.**
- **TCP en Protocolo.**

- Permitir en Acción.
- 200 en Prioridad.
- myRDPRule en Nombre.
- Permitir RDP en Descripción.

Add inbound security rule
myNetworkSecurityGroup

Basic

* Source ⓘ
Service Tag

* Source service tag ⓘ
Internet

* Source port ranges ⓘ
*

* Destination ⓘ
Any

* Destination port ranges ⓘ
3389

* Protocol
Any TCP UDP

* Action
Allow Deny

* Priority ⓘ
200

* Name
myRDPRule

Description
Allow RDP

OK

Creación de máquinas virtuales

- En la esquina superior izquierda de la pantalla, seleccione **Crear un recurso > Compute > Windows Server 2016 Datacenter**. Especifique estos valores para la máquina virtual:
 - **myVM1** como nombre de la máquina virtual.
 - **azureuser** como nombre del usuario administrador.
 - **myResourceGroupZLB** como **Grupo de recursos**. Seleccione **Usar existente** y, a continuación, seleccione **myResourceGroupZLB**.
- Seleccione **Aceptar**.
- Seleccione **DS1_V2** como tamaño de la máquina virtual. Elija **Seleccionar**.

- Especifique estos valores para la configuración de la máquina virtual:
 - Zona 1** como Zona de disponibilidad donde va a situar la máquina virtual.
 - myVNet**. Asegúrese de que está seleccionada como la red virtual.
 - myVM1PIP** como la dirección IP pública estándar que crea. Seleccione **Crear nuevo**. A continuación, en nombre, seleccione **myVM1PIP**. Para **Zona**, seleccione **1**. La SKU de la dirección IP es estándar de manera predeterminada.
 - myBackendSubnet**. Asegúrese de que está seleccionada como la subred.
 - myNetworkSecurityGroup** como nombre del firewall del grupo de seguridad de red existente.
- Seleccione **Deshabilitado** para deshabilitar los diagnósticos de arranque.
- Seleccione **Aceptar**. Revise la configuración en la página Resumen. Seleccione **Crear**.
- Repita los pasos 1 a 6 para crear una segunda máquina virtual, llamada **myVM2** en la Zona 1. Especifique **myVnet** como la red virtual. Especifique **myVM2PIP** como la dirección IP pública estándar. Especifique **myBackendSubnet** como la subred. Y especifique **myNetworkSecurityGroup** como el grupo de seguridad de red.

The image displays three side-by-side screenshots from the Azure portal, illustrating the configuration of a virtual machine's network settings.

- Left Screenshot (Settings):** Shows the 'Settings' page for a virtual machine. The 'High availability' section has 'Availability zone' set to '1'. The 'Network' section shows 'Virtual network' as 'myVNet', 'Subnet' as 'myBackendSubnet (10.1.0.0/24)', and 'Public IP address' as '(new) myVM1PIP'. The 'Network security group (firewall)' is set to 'myNetworkSecurityGroup'. The 'Auto-shutdown' section has 'Enable auto-shutdown' set to 'Off'. The 'Monitoring' section has 'Boot diagnostics' set to 'Disabled'. An 'OK' button is at the bottom.
- Middle Screenshot (Choose public IP address):** Shows the 'Choose public IP address' page. It displays a list of public IP addresses, with a '+ Create new' button highlighted. Below the list, it shows 'None'.
- Right Screenshot (Create public IP address):** Shows the 'Create public IP address' page. The 'Name' field is filled with 'myVM1PIP'. The 'SKU' section has 'Standard' selected. The 'Assignment' section has 'Static' selected. The 'Availability zone' section has 'Zone 1' selected. An 'OK' button is at the bottom.

Instalación de IIS en las máquinas virtuales

- Seleccione **Todos los recursos** en el menú de la izquierda. A continuación, en la lista de recursos, seleccione **myVM1**. Se encuentra en el grupo de recursos **myResourceGroupZLB**.
- En la página **Información general**, seleccione **Conectar** para conectar mediante RDP con la máquina virtual.
- Inicie sesión en la máquina virtual con el nombre de usuario y la contraseña que especificó al crear la máquina virtual. Para especificar las credenciales que especificó cuando creó la máquina virtual, tendrá que seleccionar **Más opciones**. Después, seleccione **Usar otra cuenta**. Y, a continuación, seleccione **Aceptar**. Puede recibir una advertencia de certificado durante el proceso de inicio de sesión. Seleccione **Sí** para continuar con la conexión.
- En el escritorio del servidor, vaya a **Herramientas administrativas de Windows > Windows PowerShell**.

5. En la ventana de **PowerShell**, ejecute los comandos siguientes para instalar el servidor IIS. Estos comandos también eliminan el archivo `iisstart.htm` predeterminado y, a continuación, agregan uno nuevo que muestra el nombre de la máquina virtual:

```
# install IIS server role
Install-WindowsFeature -name Web-Server -IncludeManagementTools
# remove default htm file
remove-item C:\inetpub\wwwroot\iisstart.htm
# Add a new htm file that displays server name
Add-Content -Path "C:\inetpub\wwwroot\iisstart.htm" -Value $("Hello World from" + $env:computername)
```

6. Cierre la sesión de RDP con **myVM1**.
7. Repita los pasos del 1 al 7 para instalar IIS en **myVM2**.

Creación de recursos del equilibrador de carga

En esta sección se configuran los valores del equilibrador de carga para un grupo de direcciones de back-end y un sondeo de mantenimiento. También se especifican reglas de traducción de direcciones de red y el equilibrador de carga.

Creación de un grupo de direcciones de back-end

Para distribuir el tráfico a las máquinas virtuales, un grupo de direcciones de back-end contiene las direcciones IP de las tarjetas de interfaz de red virtual conectadas al equilibrador de carga. Cree el grupo de direcciones de back-end **myBackendPool** para incluir **VM1** y **VM2**.

1. Seleccione **Todos los recursos** en el menú de la izquierda. A continuación, seleccione **myLoadBalancer** en la lista de recursos.
2. En **Configuración**, seleccione **Grupos de back-end**. A continuación, seleccione **Agregar**.
3. En la página **Agregar grupo back-end**, realice lo siguiente:
 - En el espacio para el nombre, escriba **myBackEndPool** como nombre del grupo de back-end.
 - Para **Red virtual**, en el menú desplegable, seleccione **myVNet**.
 - Para **Máquina Virtual** y **Dirección IP**, agregue **myVM1** y **myVM2** y sus direcciones IP públicas correspondientes.
4. Seleccione **Agregar**.
5. Asegúrese de que la configuración del grupo de back-end del equilibrador de carga muestra las dos máquinas virtuales, **myVM1** y **myVM2**.

Home > [Resource groups](#) > [myResourceGroupZLB](#) > [myLoadBalancer - Backend pools](#) > [myBackendPool](#)

myBackendPool

myLoadBalancer

Save Discard

Name
myBackendPool

IP version ⓘ
IPv4

* Virtual network ⓘ
myvnet (2 VM) ▼

<input type="checkbox"/>	VIRTUAL MACHINE	IP ADDRESS	
<input type="checkbox"/>	myvm1 ▼	ipconfig1 (10.1.0.6) ▼	...
	▼	▼	

Creación de un sondeo de estado

Para permitir que el equilibrador de carga supervise el estado de la aplicación, utilice un sondeo de mantenimiento. El sondeo de estado agrega o quita de forma dinámica las máquinas virtuales de la rotación del equilibrador de carga en base a su respuesta a las comprobaciones de estado. Cree un sondeo de estado, **myHealthProbe**, para supervisar el estado de las máquinas virtuales.

1. Seleccione **Todos los recursos** en el menú de la izquierda. A continuación, seleccione **myLoadBalancer** en la lista de recursos.
2. En **Configuración**, seleccione **Sondeos de estado**. A continuación, seleccione **Agregar**.
3. Use estos valores para crear el sondeo de estado:
 - **myHealthProbe** como nombre del sondeo de mantenimiento.
 - **HTTP** en tipo de protocolo.
 - **80** en número de puerto.
 - **15** como número de **Intervalo**, en segundos, entre los intentos de sondeo.
 - **2** como número de **Umbral incorrecto** o errores de sondeo consecutivos que deben producirse para que una máquina virtual se considere que no funciona de manera correcta.
4. Seleccione **Aceptar**.

... > MyResourceGroupLBAZ > myLoadBalancer - Health probes > Add health probe

Add health probe

myLoadBalancer

Name *

Protocol ⓘ

Port * ⓘ

Interval * ⓘ

seconds

Unhealthy threshold * ⓘ

consecutive failures

OK

Creación de una regla de equilibrador de carga

Una regla del equilibrador de carga define cómo se distribuye el tráfico a las máquinas virtuales. Defina la configuración de la IP de front-end para el tráfico entrante y el grupo de IP de back-end para el tráfico entrante, junto con los puertos de origen y destino requeridos. Cree una regla del equilibrador de carga llamada **myLoadBalancerRuleWeb** para escuchar en el puerto 80 en el front-end **FrontendLoadBalancer**. La regla envía tráfico de red con equilibrio de carga al grupo de direcciones de back-end **myBackendPool**, también a través del puerto 80.

1. Seleccione **Todos los recursos** en el menú de la izquierda. A continuación, seleccione **myLoadBalancer** en la lista de recursos.
2. En **Configuración**, seleccione **Reglas de equilibrio de carga**. A continuación, seleccione **Agregar**.
3. Use estos valores para configurar la regla de equilibrio de carga:
 - **myHTTPRule** como nombre de la regla de equilibrio de carga.
 - **TCP** en tipo de protocolo.
 - **80** en número de puerto.
 - **80** como puerto de back-end.
 - **myBackendPool** como nombre del grupo back-end.
 - **myHealthProbe** como nombre del sondeo de mantenimiento.
4. Seleccione **Aceptar**.

Home > Resource groups > myResourceGroupZLB > myLoadBalancer - Load balancing rules > Add load balanc

Add load balancing rule

myLoadBalancer

* Name
myHTTPRule

* IP Version
☒ IPv4 ☐ IPv6

* Frontend IP address ⓘ
40.67.200.229 (LoadBalancerFrontEnd) ▼

Protocol
☒ TCP ☐ UDP

* Port
80

* Backend port ⓘ
80

Backend pool ⓘ
myBackendPool (2 virtual machines) ▼

Health probe ⓘ
myHealthProbe (TCP:80) ▼

Session persistence ⓘ
None ▼

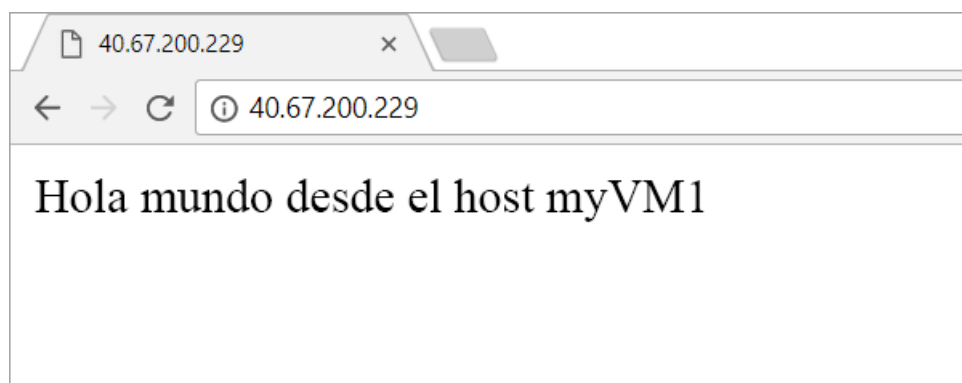
Idle timeout (minutes) ⓘ
 4

Floating IP (direct server return) ⓘ

OK

Prueba del equilibrador de carga

1. Busque la dirección IP pública de Load Balancer en la pantalla **Información general**. Seleccione **Todos los recursos**. A continuación, seleccione **myPublicIP**.
2. Copie la dirección IP pública. A continuación, péguela en la barra de direcciones del explorador. La página predeterminada que incluye el nombre de la página del servidor web se muestra en el explorador.



3. Para ver el equilibrador de carga en acción, fuerce la detención de la máquina virtual que se muestra.
Actualice el explorador para ver el otro nombre de servidor que aparece en el explorador.

Limpieza de recursos

Cuando ya no los necesite, elimine el grupo de recursos, el equilibrador de carga y todos los recursos relacionados. Seleccione el grupo de recursos que contiene el equilibrador de carga. A continuación, seleccione **Eliminar**.

Pasos siguientes

- Más información acerca de [Load Balancer Estándar](#).
- [Equilibrio de carga de máquinas virtuales entre zonas de disponibilidad](#).

Tutorial: Configuración del enrutamiento de puerto en Azure Load Balancer mediante Azure Portal

23/09/2020 • 24 minutes to read • [Edit Online](#)

El enrutamiento de puerto le permite conectarse a máquinas virtuales (VM) en una red virtual de Azure con el uso de un número de puerto y una dirección IP pública de Azure Load Balancer.

En este tutorial, se va a configurar el enrutamiento de puerto en Azure Load Balancer. Aprenderá a:

- Crear un equilibrador de carga estándar público para equilibrar el tráfico de red a través de las máquinas virtuales.
- Crear una red virtual y máquinas virtuales con una regla de grupo de seguridad de red (NSG).
- Agregar las máquinas virtuales al grupo de direcciones de back-end del equilibrador de carga.
- Crear un sondeo de mantenimiento del equilibrador de carga y reglas de tráfico.
- Crear reglas de enrutamiento de puerto de entrada del equilibrador de carga.
- Instalar y configurar IIS en las máquinas virtuales para ver el equilibrio de carga y el enrutamiento de puerto en acción.

Si no tiene una suscripción a Azure, cree una [cuenta gratuita](#) antes de empezar.

Para realizar todos los pasos de este tutorial, inicie sesión en Azure Portal en <https://portal.azure.com>.

Creación de un equilibrador de carga estándar

En primer lugar, cree un equilibrador de carga estándar público que pueda equilibrar la carga de tráfico a través de las máquinas virtuales. Un equilibrador de carga estándar solo admite una dirección IP pública estándar. Cuando se crea un equilibrador de carga estándar, también se crea una dirección IP pública estándar, que se configura como el front-end de equilibrador de carga y se denomina **LoadBalancerFrontEnd** de manera predeterminada.

1. En la parte superior izquierda de la pantalla, haga clic en **Crear un recurso > Redes > Azure Load Balancer**.
2. En la pestaña **Datos básicos** de la página **Crear equilibrador de carga**, escriba o seleccione la siguiente información, acepte los valores predeterminados del resto de la configuración y, luego, seleccione **Revisar y crear**:

CONFIGURACIÓN	VALUE
Subscription	Seleccione su suscripción.
Resource group	Seleccione Crear nuevo y escriba <i>MyResourceGroupLB</i> en el cuadro de texto.
Nombre	<i>myLoadBalancer</i>
Region	Seleccione Oeste de Europa .
Tipo	Seleccione Público .
SKU	Seleccione Estándar .

CONFIGURACIÓN	VALUE
Dirección IP pública	Seleccione Crear nuevo .
Nombre de la dirección IP pública	Escriba <i>myPublicIP</i> en el cuadro de texto.
Zona de disponibilidad	Seleccione Redundancia de zona .

NOTE

Asegúrese de crear el equilibrador de carga y todos los recursos para él en una ubicación compatible con Availability Zones. Para más información, vea [Regiones que admiten Availability Zones](#).

- En la pestaña **Revisar y crear**, haga clic en **Crear**.

Creación y configuración de servidores back-end

Cree una red virtual con dos máquinas virtuales y agréguelas al grupo de back-end del equilibrador de carga.

Red virtual y parámetros

En los pasos de esta sección, tendrá que reemplazar los siguientes parámetros por la siguiente información:

PARÁMETRO	VALUE
<resource-group-name>	myResourceGroupLB (seleccione el grupo de recursos existente)
<virtual-network-name>	myVNet
<region-name>	Oeste de Europa
<IPv4-address-space>	10.3.0.0\16
<subnet-name>	myBackendSubnet
<subnet-address-range>	10.3.0.0\24

Crear la red virtual

En esta sección, creará una red virtual y una subred.

- En la parte superior izquierda de la pantalla, seleccione **Crear un recurso** > **Redes** > **Red virtual** o busque **Red virtual** en el cuadro de búsqueda.
- En **Crear red virtual**, escriba o seleccione esta información en la pestaña **Conceptos básicos**:

CONFIGURACIÓN	VALOR
Detalles del proyecto	
Suscripción	Selección de su suscripción a Azure

CONFIGURACIÓN	VALOR
Grupo de recursos	Seleccione Crear nuevo , escriba <resource-group-name> , seleccione Aceptar o seleccione un <resource-group-name> existente basado en parámetros.
Detalles de instancia	
Nombre	Escriba <virtual-network-name>
Region	Selección de <region-name>

3. Seleccione la pestaña **Direcciones IP** o el botón **Siguiente: Direcciones IP** situado en la parte inferior de la página.

4. En la pestaña **Direcciones IP**, especifique esta información:

CONFIGURACIÓN	VALUE
Espacio de direcciones IPv4	Escriba <IPv4-address-space>

5. En **Nombre de subred**, seleccione la palabra **predeterminada**.

6. En **Editar subred**, especifique esta información:

CONFIGURACIÓN	VALUE
Nombre de subred	Escriba <subnet-name>
Intervalo de direcciones de subred	Escriba <subnet-address-range>

7. Seleccione **Guardar**.

8. Seleccione la pestaña **Revisar y crear** o el botón **Revisar y crear**.

9. Seleccione **Crear**.

Crear máquinas virtuales y agregarlas al grupo de back-end del equilibrador de carga

1. En la parte superior izquierda del portal, seleccione **Crear un recurso > Proceso > Windows Server 2016 Datacenter**.

2. En **Crear una máquina virtual**, escriba o seleccione los valores siguientes en la pestaña **Básico**:

- **Suscripción > Grupo de recursos**: despliegue y seleccione **MyResourceGroupLB**.
- **Nombre de la máquina virtual**: escriba *MyVM1*.
- **Región**: Seleccione **Oeste de Europa**.
- **Nombre de usuario**: escriba *azureuser*.
- **Contraseña**: escriba *Azure1234567*. Vuelva a escribir la contraseña en el campo **Confirmar contraseña**.

3. Seleccione la pestaña **Redes** o seleccione **Siguiente: Discos** y, después, **Siguiente: Redes**.

Asegúrese de que está seleccionado lo siguiente:

- **Red virtual**: **MyVNet**
- **Subred**: **MyBackendSubnet**

4. En **IP pública**, seleccione **Crear nueva**, seleccione **Estándar** en la página **Crear dirección IP pública** y,

después, seleccione **Aceptar**.

5. En **Grupo de seguridad de red**, seleccione **Avanzado** para crear un grupo de seguridad de red (NSG), un tipo de firewall.
 - a. En el campo **Configurar grupo de seguridad de red**, seleccione **Crear nuevo**.
 - b. Escriba *MyNetworkSecurityGroup* y seleccione **Aceptar**.

NOTE

Observe que, de forma predeterminada, el NSG ya tiene una regla de entrada para abrir el puerto 3389, el puerto de escritorio remoto (RDP).

6. Agregue la máquina virtual a un grupo de back-end de equilibrador de carga que cree:
 - a. En **EQUILIBRIO DE CARGA > Place this virtual machine behind an existing load balancing solution?** (¿Colocar esta máquina virtual detrás de una solución de equilibrio de carga existente?), seleccione **Sí**.
 - b. En **Opciones de equilibrio de carga**, seleccione **Azure Load Balancer** en el menú desplegable.
 - c. En **Select a load balancer** (Seleccionar un equilibrador de carga), seleccione **MyLoadBalancer** en el menú desplegable.
 - d. En **Select a backend pool** (Seleccionar un grupo de back-end), seleccione **Crear nuevo**, escriba *MyBackendPool* y seleccione **Crear**.

Create a virtual machine	Create public IP address
<div>Basics Disks Networking Management Guest config Tags Review + create</div> <p>Configure a new or existing virtual network for your VM as well as how your VM will be accessed on the virtual network. Learn more</p> <p>NETWORK INTERFACE</p> <p>When creating a virtual machine, a network interface will be created for you.</p> <p>* Virtual network MyVNet Create new</p> <p>* Subnet MyBackendSubnet (10.3.0.0/24) Manage subnet configuration</p> <p>Public IP (new) MyVM1-ip Create new</p> <p>Network security group Basic <input type="radio"/> Advanced <input checked="" type="radio"/></p> <p>Configure network security group MyNetworkSecurityGroup Create new</p> <p>Accelerated networking On <input type="radio"/> Off <input checked="" type="radio"/> <small>The selected VM size does not support accelerated networking.</small></p> <p>LOAD BALANCING</p> <p>You can place this virtual machine in the backend pool of an existing Azure load balancing solution. Learn more</p> <p>Place this virtual machine behind an existing load balancing solution? Yes <input checked="" type="radio"/> No <input type="radio"/></p> <p>LOAD BALANCING SETTINGS</p> <ul style="list-style-type: none">Application Gateway is a web traffic, Layer 7 load balancer with URL-based routing, SSL termination, session persistence, and web application firewall. About Application GatewayAzure Load Balancer supports all TCP/UDP network traffic, port-forwarding, and outbound flows. About Azure Load Balancer <p>* Load balancing options Azure load balancer</p> <p>* Select a load balancer MyLoadBalancer</p> <p>* Select a backend pool MyBackendPool Create new</p>	<p>* Name MyVM1-ip</p> <p>SKU Basic <input type="radio"/> Standard <input checked="" type="radio"/></p> <p>Assignment Static <input checked="" type="radio"/></p> <p>Availability zone Zone-redundant</p> <p>OK</p>

7. Seleccione la pestaña **Administración** o seleccione **Siguiente > Administración**. En **Supervisión**, establezca **Diagnósticos de arranque** en **Desactivado**.
8. Seleccione **Revisar + crear**.

9. Revise la configuración y, cuando la validación sea correcta, seleccione **Crear**.
10. Siga los pasos para crear una segunda máquina virtual llamada *MyVM2*, con todos los demás valores igual a *MyVM1*.

En **Grupo de seguridad de red**, después de seleccionar **Avanzado**, seleccione en el menú desplegable el grupo **MyNetworkSecurityGroup** que ya ha creado.

En **Select a backend pool** (Seleccionar un grupo de back-end), asegúrese de que **MyBackendPool** está seleccionado.


Creación de una regla de NSG para las máquinas virtuales

Cree una regla de grupo de seguridad de red (NSG) para que las máquinas virtuales permitan conexiones entrantes de Internet (HTTP).


NOTE

De forma predeterminada, el NSG ya tiene una regla que abre el puerto 3389, el puerto de escritorio remoto (RDP).

1. Seleccione **Todos los recursos** en el menú izquierdo. En la lista de recursos, seleccione **MyNetworkSecurityGroup** en el grupo de recursos **MyResourceGroupLB**.
2. En **Configuración**, seleccione **Reglas de seguridad de entrada** y, a continuación, seleccione **Agregar**.
3. En el cuadro de diálogo **Agregar regla de seguridad de entrada**, escriba o seleccione lo siguiente:
 - **Origen**: seleccione **Etiqueta de servicio**.
 - **Etiqueta de servicio de origen**: seleccione **Internet**.
 - **Intervalos de puerto de destino**: escriba *80*.
 - **Protocolo**: seleccione **TCP**.
 - **Acción**: seleccione **Permitir**.
 - **Prioridad**: escriba *100*.
 - **Nombre**: escriba *MyHTTPRule*.
 - **Descripción**: escriba *Permitir HTTP*.
4. Seleccione **Agregar**.


Add inbound security rule
✕

MyNetworkSecurityGroup


 Basic

* Source ⓘ

Service Tag

* Source service tag ⓘ

Internet

* Source port ranges ⓘ

*

* Destination ⓘ

Any

* Destination port ranges ⓘ

80

* Protocol

Any TCP UDP

* Action

Allow Deny

* Priority ⓘ

100

* Name

MyHTTPRule

Description

Allow HTTP

Add

Creación de recursos del equilibrador de carga

En esta sección, va a inspeccionar el grupo de back-end del equilibrador de carga y a configurar reglas de tráfico y sondeo de mantenimiento de un equilibrador de carga.

Visualización del grupo de direcciones de back-end

Para distribuir el tráfico a las máquinas virtuales, el equilibrador de carga usa un grupo de direcciones de back-end que contiene las direcciones IP de las interfaces de red virtual (NIC) conectadas al equilibrador de carga.

Se ha creado el grupo de back-end del equilibrador de carga y se han agregado máquinas virtuales a él cuando se crearon las máquinas virtuales. También puede crear grupos de back-end y agregar o quitar máquinas virtuales en la página de **Grupos de back-end** del equilibrador de carga.

1. Seleccione **Todos los recursos** en el menú de la izquierda y, a continuación, en la lista de recursos seleccione **MyLoadBalancer**.
2. En **Configuración**, seleccione **Grupos de back-end**.
3. En la página **Grupos back-end**, expanda **MyBackendPool** y asegúrese de que aparecen ambas máquinas **VM1** y **VM2**.
4. Seleccione **MyBackendPool**.

En la página **MyBackendPool**, en **MÁQUINA VIRTUAL** y **DIRECCIÓN IP**, puede agregar las máquinas virtuales disponibles al grupo o quitarlas.

Puede crear grupos de back-end; para ello, seleccione **Agregar** en la página **Grupos de back-end**.

Creación de un sondeo de estado

Para permitir que el equilibrador de carga supervise el mantenimiento de la máquina virtual, utilice un sondeo de mantenimiento. El sondeo de estado agrega o quita de forma dinámica las máquinas virtuales de la rotación del equilibrador de carga en base a su respuesta a las comprobaciones de estado.

1. Seleccione **Todos los recursos** en el menú de la izquierda y, a continuación, en la lista de recursos seleccione **MyLoadBalancer**.
2. En **Configuración**, seleccione **Sondeos de mantenimiento** y, a continuación, seleccione **Agregar**.
3. En la página **Agregar sondeo de mantenimiento**, escriba o seleccione los siguientes valores:
 - **Name:** escriba *MyHealthProbe*.
 - **Protocolo:** en la lista desplegable, seleccione **HTTP**.
 - **Puerto:** escriba *80*.
 - **Ruta de acceso:** acepte /para el identificador URI predeterminado. Puede reemplazar este valor por cualquier otro identificador URI.
 - **Intervalo:** escriba *15*. El valor Intervalo es el número de segundos entre los intentos de sondeo.
 - **Umbral incorrecto:** escriba *2*. Este valor es el número de errores de sondeo consecutivos que tienen que producirse para que se considere que una máquina virtual no funciona correctamente.
4. Seleccione **Aceptar**.

Add health probe

MyLoadBalancer

* Name
MyHealthProbe ✓

IP version
IPv4

Protocol ⓘ
HTTP ✓

* Port ⓘ
80

* Path ⓘ
/

* Interval ⓘ
15 ✓
seconds

* Unhealthy threshold ⓘ
2
consecutive failures

OK

Creación de una regla de equilibrador de carga

Una regla del equilibrador de carga define cómo se distribuye el tráfico a las máquinas virtuales. La regla define la configuración IP de front-end para el tráfico entrante y el grupo de direcciones IP de back-end para recibir el tráfico y los puertos de origen y destino requeridos.

La regla del equilibrador de carga llamada **MyLoadBalancerRule** escucha en el puerto 80 en el front-end **LoadBalancerFrontEnd**. La regla envía el tráfico de red al grupo de direcciones de back-end **MyBackendPool**, también a través del puerto 80.

1. Seleccione **Todos los recursos** en el menú de la izquierda y, a continuación, en la lista de recursos seleccione **MyLoadBalancer**.
2. En **Configuración**, seleccione **Reglas de equilibrio de carga** y, a continuación, seleccione **Agregar**.
3. En la página **Agregar regla de equilibrio de carga**, escriba o seleccione los valores siguientes:
 - **Name:** escriba *MyLoadBalancerRule*.
 - **Protocolo:** seleccione TCP.
 - **Puerto:** escriba *80*.
 - **Puerto back-end:** escriba *80*.
 - **Grupo de back-end:** seleccione **MyBackendPool**.
 - **Sondeo de mantenimiento:** seleccione **MyHealthProbe**.
4. Seleccione **Aceptar**.

Add load balancing rule

MyLoadBalancer

* Name
MyLoadBalancerRule ✓

* IP Version
☒ IPv4 ☐ IPv6

* Frontend IP address ⓘ
40.67.218.235 (LoadBalancerFrontEnd) ▼

Protocol
☒ TCP ☐ UDP

* Port
80

* Backend port ⓘ
80

Backend pool ⓘ
MyBackendPool (2 virtual machines) ▼

Health probe ⓘ
MyHealthProbe (HTTP:80) ▼

Session persistence ⓘ
None ▼

Idle timeout (minutes) ⓘ
 4

Floating IP (direct server return) ⓘ

OK

Creación de una regla de enrutamiento de puerto NAT de entrada

Cree una regla de traducción de direcciones de red (NAT) de entrada del equilibrador de carga para enrutar el tráfico desde un puerto específico de la dirección IP front-end a un puerto específico de una máquina virtual back-

end.

1. Seleccione **Todos los recursos** en el menú de la izquierda y, después, en la lista de recursos seleccione **MyLoadBalancer**.
2. En **Configuración**, seleccione **Reglas NAT de entrada** y, después, seleccione **Agregar**.
3. En la página **Agregar regla NAT de entrada**, escriba o seleccione los valores siguientes:
 - **Name**: escriba *MyNATRuleVM1*.
 - **Puerto**: escriba *4221*.
 - **Máquina virtual de destino**: seleccione **MyVM1** en la lista desplegable.
 - **Configuración de IP de red**: seleccione **ipconfig1** en la lista desplegable.
 - **Asignación de puertos**: seleccione **Personalizada**.
 - **Puerto de destino**: escriba *3389*.
4. Seleccione **Aceptar**.
5. Repita los pasos para agregar una regla NAT de entrada denominada *MyNATRuleVM2*, con **Puerto**: *4222* y **Máquina virtual de destino**: **MyVM2**.

Prueba del equilibrador de carga

En esta sección, se instalará Internet Information Services (IIS) en los servidores back-end y se personalizará la página web predeterminada para mostrar el nombre de la máquina. Después, se usará la dirección IP pública del equilibrador de carga para probar el equilibrador de carga.

Cada máquina virtual de back-end sirve una versión diferente de la página web IIS predeterminada, de esta forma puede ver como el equilibrador de carga distribuye las solicitudes entre las dos máquinas virtuales.

Conexión a las máquinas virtuales con RDP

Conéctese a cada máquina virtual con Escritorio remoto (RDP).

1. En el portal, seleccione **Todos los recursos** en el menú izquierdo. En la lista de recursos, seleccione cada máquina virtual en el grupo de recursos **MyResourceGroupLB**.
2. En la página **Información general**, seleccione **Conectar** y, a continuación, seleccione **Descargar archivo RDP**.
3. Abra el archivo RDP que descargó y seleccione **Conectar**.
4. En la pantalla Seguridad de Windows, seleccione **Más opciones** y, después, **Usar otra cuenta**.

Escriba el nombre de usuario *azureuser* y la contraseña *Azure1234567* y seleccione **Aceptar**.
5. Responda **Sí** a cualquier solicitud de certificado.

El escritorio de la máquina virtual se abre en una nueva ventana.

Instalar IIS y reemplazar la página web predeterminada de IIS

Use PowerShell para instalar IIS y reemplazar la página web predeterminada de IIS por una página en la que se muestre el nombre de la máquina virtual.

1. Iniciar **Windows PowerShell** en MyVM1 y MyVM2 desde el menú **Inicio**.
2. Ejecute los comandos siguientes para instalar IIS y reemplazar la página web predeterminada de IIS:

```
# Install IIS
Install-WindowsFeature -name Web-Server -IncludeManagementTools

# Remove default htm file
remove-item C:\inetpub\wwwroot\iisstart.htm

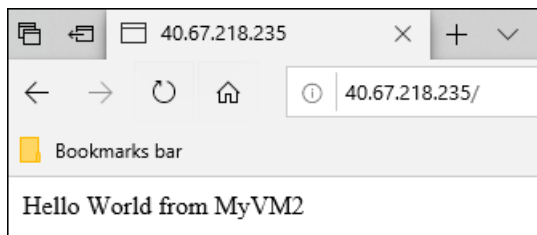
#Add custom htm file that displays server name
Add-Content -Path "C:\inetpub\wwwroot\iisstart.htm" -Value $("Hello World from " + $env:computername)
```

3. Cierre las conexiones RDP con MyVM1 y MyVM2 seleccionando **Desconectar**. No apague las máquinas virtuales.

Prueba del equilibrio de carga

1. En el portal, en la página **Información general** de **MyLoadBalancer**, copie la dirección IP pública en **Dirección IP pública**. Mantenga el puntero sobre la dirección y seleccione el icono **Copiar** para copiarlo. En este ejemplo, es **40.67.218.235**.
2. Pegue o escriba la dirección IP pública del equilibrador de carga (**40.67.218.235**) en la barra de direcciones del explorador de Internet.

La página predeterminada del servidor web de IIS personalizada aparece en el explorador. El mensaje que aparece será **Hola mundo de MyVM1**, u **Hola mundo de MyVM2**.



3. Actualice el explorador para ver cómo el equilibrador de carga distribuye el tráfico entre máquinas virtuales. A veces aparece la página **MyVM1** y otras es la página **MyVM2** la que aparece, ya que el equilibrador de carga distribuye las solicitudes a cada máquina virtual de back-end.

NOTE

Puede que deba borrar la caché del explorador o abrir una nueva ventana del explorador entre intentos.

Comprobación del reenvío de puertos

Con el enrutamiento de puerto, puede remitir el escritorio remoto a una máquina virtual back-end con la dirección IP del equilibrador de carga y el valor del puerto de front-end definidos en la regla NAT.

1. En el portal, en la página **Información general** de **MyLoadBalancer**, copie su dirección IP pública. Mantenga el puntero sobre la dirección y seleccione el icono **Copiar** para copiarlo. En este ejemplo, es **40.67.218.235**.
2. Abra un símbolo del sistema y use el siguiente comando para crear una sesión de escritorio remoto con MyVM2, utilizando la dirección IP pública del equilibrador de carga y el puerto de front-end que definió en la regla NAT de la máquina virtual.

```
mstsc /v:40.67.218.235:4222
```

3. Abra el archivo RDP descargado y seleccione **Conectar**.

4. En la pantalla Seguridad de Windows, seleccione **Más opciones** y, después, **Usar otra cuenta**.

Escriba el nombre de usuario *azureuser* y la contraseña *Azure1234567* y seleccione **Aceptar**.

5. Responda **Sí** a cualquier solicitud de certificado.

El escritorio de MyVM2 se abre en una nueva ventana.

La conexión RDP se realiza correctamente, porque la regla NAT entrante **MyNATRuleVM2** dirige el tráfico del puerto de front-end del equilibrador de carga 4222 al puerto de MyVM2 3389 (puerto RDP).

Limpieza de recursos

Para eliminar el equilibrador de carga y todos los recursos relacionados cuando ya no los necesite, abra el grupo de recursos **MyResourceGroupLB** y seleccione **Eliminar grupo de recursos**.

Pasos siguientes

En este tutorial, ha creado un equilibrador de carga público estándar. Ha creado y configurado los recursos de red, servidores back-end, un sondeo de mantenimiento y las reglas para el equilibrador de carga. Ha instalado IIS en las máquinas virtuales de back-end y ha utilizado la dirección IP pública del equilibrador de carga para probar el equilibrador de carga. Ha configurado y probado el enrutamiento de puerto desde un puerto específico del equilibrador de carga a un puerto de la máquina virtual de back-end.

Para más información sobre Azure Load Balancer, consulte otros tutoriales sobre Load Balancer.

[Tutoriales de Azure Load Balancer](#)

Ejemplos de la CLI de Azure para Load Balancer

23/09/2020 • 2 minutes to read • [Edit Online](#)

En la tabla siguiente se incluyen vínculos a scripts de Bash creados con la CLI de Azure.

- [Equilibrio de carga del tráfico a las máquinas virtuales para conseguir alta disponibilidad](#)

Crea varias máquinas virtuales de alta disponibilidad y una configuración de equilibrio de carga.

- [Equilibrio de carga de máquinas virtuales en distintas zonas de disponibilidad](#)

Crea tres máquinas virtuales en zonas de disponibilidad diferentes dentro de una región y una instancia de Standard Load Balancer con una dirección IP de front-end con redundancia de zona. Esta configuración del equilibrador de carga le ayudará a proteger sus aplicaciones y sus datos en el caso improbable de que se produzca una pérdida o un error en todo el centro de datos.

- [Equilibrio de carga de máquinas virtuales en una zona de disponibilidad específica](#)

Crea tres máquinas virtuales, una instancia de Standard Load Balancer con la dirección IP de front-end de zona que ayuda a alinear la ruta de acceso a los datos y los recursos en una sola zona de una región específica.

- [Equilibrio de carga entre varios sitios web en máquinas virtuales](#)

Creación de dos máquinas virtuales con varias configuraciones de IP, unidas a un conjunto de disponibilidad de Azure, accesibles a través de una instancia de Azure Load Balancer.

Ejemplos de Azure PowerShell para Load Balancer

23/09/2020 • 2 minutes to read • [Edit Online](#)

En la tabla siguiente se incluyen vínculos a scripts creados con Azure PowerShell.

SCRIPT	DESCRIPCIÓN
Equilibrio de carga del tráfico a las máquinas virtuales para conseguir alta disponibilidad	Crea varias máquinas virtuales de alta disponibilidad y una configuración de equilibrio de carga.
Equilibrio de carga entre varios sitios web en máquinas virtuales	Creación de dos máquinas virtuales con varias configuraciones de IP, unidas a un conjunto de disponibilidad de Azure, accesibles a través de una instancia de Azure Load Balancer.

Componentes de Azure Load Balancer

23/09/2020 • 10 minutes to read • [Edit Online](#)

Azure Load Balancer incluye algunos componentes clave. Puede configurar esos componentes en su suscripción mediante:

- Azure portal
- Azure CLI
- Azure PowerShell
- Plantillas de Resource Manager

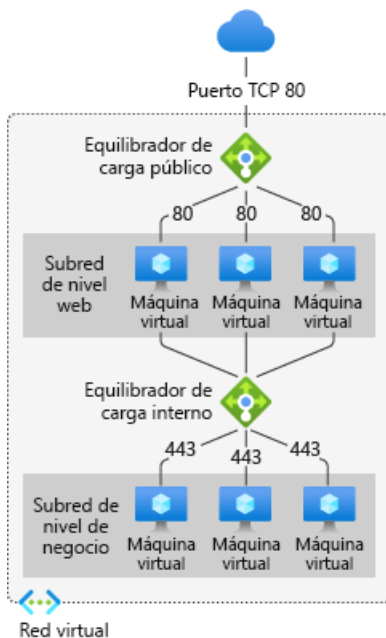
Configuración de direcciones IP de front-end

La dirección IP de Azure Load Balancer. Es el punto de contacto de los clientes. Estas direcciones IP pueden ser:

- Dirección IP pública
- Dirección IP privada

La naturaleza de la dirección IP determina el **tipo** de equilibrador de carga creado. Si se selecciona una dirección IP privada, se crea un equilibrador de carga interno. Si se selecciona una dirección IP pública, se crea un equilibrador de carga público.

	EQUILIBRADOR DE CARGA PÚBLICO	EQUILIBRADOR DE CARGA INTERNO
Configuración de direcciones IP de front-end	Dirección IP pública	Dirección IP privada
Descripción	Los equilibradores de carga públicos asignan la IP pública y el puerto de tráfico entrante a la IP privada y al puerto de la máquina virtual. El equilibrador de carga asigna el tráfico de la otra manera en torno al tráfico de respuesta de la máquina virtual. Puede distribuir determinados tipos de tráfico entre varias máquinas virtuales o servicios aplicando reglas de equilibrio de carga. Por ejemplo, puede distribuir la carga del tráfico de solicitudes web entre varios servidores web.	Un equilibrador de carga interno distribuye el tráfico a los recursos que se encuentran en una red virtual. Azure restringe el acceso a las direcciones IP de front-end de una red virtual que tienen equilibrio de carga. Las direcciones IP de front-end y las redes virtuales no se exponen nunca directamente a un punto de conexión de Internet. Las aplicaciones de línea de negocio internas se ejecutan en Azure y se accede a ellas desde Azure o desde recursos locales.
SKU compatibles	Básico y Estándar	Básico y Estándar



Load Balancer puede tener varias direcciones IP de front-end. Obtenga más información acerca del uso de [varios front-end](#).

Grupo back-end

El grupo de máquinas virtuales o instancias de un conjunto de escalado de máquinas virtuales que van a atender la solicitud entrante. Para escalar de forma rentable, con el fin de satisfacer grandes volúmenes de instrucciones para el procesamiento de tráfico entrante, generalmente se recomienda agregar más instancias al grupo de back-end.

El equilibrador de carga se reconfigura al instante de forma automática mediante el escalado o la reducción vertical de instancias. Si se agregan o quitan máquinas virtuales del grupo de servidores back-end, el equilibrador de carga se vuelve a configurar sin operaciones adicionales. El ámbito del grupo de back-end es cualquier máquina virtual de la red virtual.

A la hora de considerar cómo diseñar el grupo de back-end, diseñe el menor número de recursos individuales del grupo de back-end para optimizar la duración de las operaciones de administración. No hay ninguna diferencia en el rendimiento o la escala del plano de los datos.

Sondeos de estado

Los sondeos de estado se usan para determinar el estado de mantenimiento de las instancias del grupo de back-end. Durante la creación del equilibrador de carga, configure un sondeo de estado para que lo use el equilibrador de carga. Este sondeo de estado determinará si una instancia está en buen estado y puede recibir tráfico.

Puede definir el umbral incorrecto de los sondeos de estado. Si un sondeo no responde, Azure Load Balancer deja de enviar nuevas conexiones a las instancias incorrectas. Un error de sondeo no afecta a las conexiones existentes. La conexión continúa hasta que la aplicación:

- Finaliza el flujo.
- Se produce el tiempo de espera de inactividad.
- La máquina virtual se apaga.

Load Balancer proporciona diferentes tipos de sondeo de estado para los puntos de conexión: TCP, HTTP y HTTPS. [Obtenga más información sobre los sondeos de estado de Load Balancer](#).

La versión Básico de Load Balancer no admite sondeos HTTPS. Además, cierra todas las conexiones TCP (incluidas las conexiones establecidas).

Reglas de equilibrio de carga

Las reglas de Load Balancer se usan para definir cómo se distribuye el tráfico entrante a **todas** las instancias del grupo de back-end. Las reglas de equilibrio de carga asignan una configuración de dirección IP de front-end y un puerto dados a varios puertos y direcciones IP de back-end.

Por ejemplo, use una regla de equilibrio de carga para el puerto 80, a fin de enrutar el tráfico de la dirección IP de front-end al puerto 80 de las instancias de back-end.

Ilustración: Reglas de equilibrio de carga

Puertos de alta disponibilidad

Regla de equilibrador de carga configurada con "protocol - all and port - 0" .

Permite proporcionar una única regla para equilibrar la carga de todos los flujos TCP y UDP que llegan a todos los puertos de una instancia interna de Standard Load Balancer.

La decisión de equilibrio de carga se toma por cada flujo. Esta acción se basa en la siguiente conexión de tupla de cinco elementos:

1. dirección IP de origen
2. puerto de origen
3. dirección IP de destino
4. puerto de destino
5. protocol

Las reglas de equilibrio de carga de puertos de alta disponibilidad le ayudan a la hora de usar escenarios críticos como aquellos con alta disponibilidad y escalabilidad para dispositivos virtuales de red (NVA) que estén en redes virtuales. La característica puede ayudar cuando hay que equilibrar la carga de un gran número de puertos.

Ilustración: Reglas de puertos de alta disponibilidad

Más información sobre los [puertos de alta disponibilidad](#)

Reglas NAT de entrada

Una regla NAT de entrada reenvía el tráfico entrante enviado a la combinación de dirección IP y puerto de front-end. El tráfico se envía a una máquina virtual o instancia **específica** en el grupo de back-end. El reenvío de puertos se realiza mediante la misma distribución basada en hash que el equilibrio de carga.

Por ejemplo, se desea que las sesiones de Secure Shell (SSH) o del Protocolo de escritorio remoto (RDP) separen las instancias de máquina virtual en un grupo de back-end. Se pueden asignar varios puntos de conexión internos a puertos de la misma dirección IP de front-end. Las direcciones IP de front-end se pueden usar para administrar de forma remota máquinas virtuales sin un jumpbox adicional.

Ilustración: Reglas NAT de entrada

Las reglas NAT de entrada en el contexto de Virtual Machine Scale Sets son grupos de NAT de entrada. Más información sobre los [componentes de Load Balancer y el conjunto de escalado de máquinas virtuales](#)

Reglas de salida

Una regla de salida configura una traducción de direcciones de red (NAT) de salida para todas las máquinas virtuales o instancias identificadas por el grupo de back-end. Esta regla permite que las instancias del back-end se comuniquen (saliente) con Internet u otros puntos de conexión.

Obtenga más información sobre las [conexiones y reglas de salida](#).

Load Balancer Básico no admite reglas de salida.

Pasos siguientes

- Consulte el artículo sobre cómo [crear una instancia de Standard Load Balancer pública](#) para empezar a usar un equilibrador de carga.
- Más información sobre [Azure Load Balancer](#).
- Información sobre las [direcciones IP públicas](#)
- Información sobre las [direcciones IP privadas](#)
- Más información en [Standard Load Balancer y Availability Zones](#).
- Más información acerca de los [diagnósticos de Load Balancer Estándar](#).
- Obtenga información sobre el [restablecimiento de TCP en estado inactivo](#).
- Más información acerca de [Standard Load Balancer con reglas de equilibrio de carga para puertos HA](#).
- Más información sobre los [grupos de seguridad de red](#).
- Más información sobre los [límites de Load Balancer](#).
- Información sobre el uso del [reenvío de puertos](#).

Conceptos de Azure Load Balancer

23/09/2020 • 14 minutes to read • [Edit Online](#)

Load Balancer proporciona varias funcionalidades para las aplicaciones UDP y TCP.

Algoritmo de equilibrio de carga

Se puede crear una regla de equilibrio de carga para distribuir el tráfico del front-end a un grupo del back-end. Azure Load Balancer usa un algoritmo hash para la distribución de los flujos (no bytes) entrantes. Load Balancer reescribe los encabezados de los flujos en las instancias del grupo del back-end. Un servidor está disponible para recibir nuevos flujos cuando el sondeo de estado indica un punto de conexión de back-end correcto.

De forma predeterminada, Load Balancer usa un hash de tupla de cinco elementos.

El hash incluye:

- Dirección IP de origen
- Puerto de origen
- Dirección IP de destino
- Puerto de destino
- Número de protocolo IP para asignar flujos a servidores disponibles

La afinidad con una dirección IP de origen se crea mediante un hash de tuplas de dos o tres elementos. Todos los paquetes del mismo flujo de paquetes llegan a la misma instancia detrás del front-end con equilibrio de carga.

El puerto de origen cambia cuando un cliente inicia un nuevo flujo desde Cuando el cliente inicia un nuevo flujo desde la misma dirección IP de origen. En consecuencia, el hash de tupla de cinco elementos puede hacer que el tráfico vaya a otro punto de conexión de back-end. Para más información, consulte [Configurar el modo de distribución para Azure Load Balancer](#).

En la siguiente imagen se muestra la distribución basada en hash:

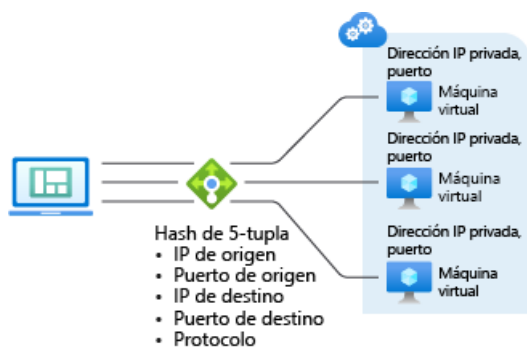


Ilustración: distribución basada en hash

Independencia y transparencia de aplicaciones

Load Balancer no interactúa directamente con TCP ni UDP ni con la capa de aplicación. Se puede admitir cualquier escenario de aplicación TCP o UDP. Load Balancer no cierra ni origina flujos, ni interactúa con la carga del flujo. Load Balancer no proporciona la funcionalidad de puerta de enlace de la capa de aplicación. Los protocolos de enlace de protocolo siempre se producen directamente entre el cliente y la instancia del grupo de back-end. Una respuesta a un flujo de entrada siempre es una respuesta de una máquina virtual. Cuando llega el flujo a la máquina virtual, también se conserva la dirección IP de origen original.

- A cada punto de conexión le responde una máquina virtual. Por ejemplo, un protocolo de enlace TCP se realiza entre el cliente y la máquina virtual de back-end seleccionada. Una respuesta a una solicitud a un front-end es una respuesta generada por una máquina virtual de back-end. Cuando se valida correctamente la conectividad con un front-end, se valida la conectividad de un extremo a otro con al menos una máquina virtual de back-end.
- Las cargas útiles de las aplicaciones son transparentes para Load Balancer. Se puede admitir cualquier aplicación UDP o TCP.
- Como Load Balancer no interactúa con la carga de TCP y proporciona descarga de TLS, puede crear escenarios cifrados completos. Con Load Balancer se obtiene una mayor escalabilidad horizontal de las aplicaciones TLS, ya que la conexión TLS finaliza en la propia máquina virtual. Por ejemplo, la capacidad para claves de sesión TLS solo está limitada por el tipo y número de máquinas virtuales que se agregan al grupo de servidores back-end.

Conexiones de salida

Los flujos del grupo de back-end a direcciones IP públicas se asignan al front-end. Azure traduce las conexiones salientes a la dirección IP pública del front-end a través de la regla de salida de equilibrio de carga. Esta configuración tiene las siguientes ventajas. Actualización sencilla y recuperación ante desastres de servicios, ya que el front-end se puede asignar dinámicamente a otra instancia del servicio. Facilita la administración de la lista de control de acceso (ACL). Las ACL que se expresan como direcciones IP de front-end no cambian a medida que los servicios se escalan o bajan horizontalmente o se vuelve a implementar. La traducción de las conexiones salientes a un número menor de direcciones IP que las máquinas reduce la carga de la implementación de listas de destinatarios seguras. Para más información sobre la traducción de direcciones de red de origen (SNAT) y Azure Load Balancer, consulte [SNAT y Azure Load Balancer](#).

Zonas de disponibilidad

Standard Load Balancer admite otras funcionalidades en las regiones donde Availability Zones está disponible. Las configuraciones de Availability Zones están disponibles para ambos tipos de instancias de Standard Load Balancer, públicas e internas. Un front-end con redundancia de zona sobrevive a los errores de la zona mediante una infraestructura dedicada en todas las zonas al mismo tiempo. Además, puede garantizar un front-end en una zona específica. Un front-end zonal es atendido por una infraestructura dedicada en una zona individual. El equilibrio de carga entre zonas está disponible para el grupo de back-end. Cualquier recurso de máquina virtual de una red virtual puede formar parte de un grupo de back-end. Basic Load Balancer no admite zonas. Revise la [explicación detallada de las capacidades relacionadas con las zonas de disponibilidad](#) y la [introducción a las zonas de seguridad](#) para más información.

Puertos de alta disponibilidad

Puede configurar reglas de equilibrio de carga en puertos de alta disponibilidad para que una aplicación sea escalable y muy confiable. Estas reglas proporcionan un equilibrio de carga por flujo a los puertos transitorios de la IP del front-end del equilibrador de carga interno. La característica es útil cuando no es práctico o no se desea especificar puertos individuales. Una regla de puertos de alta disponibilidad le permite crear $n+1$ escenarios de activo-pasivo o activo-activo. Estos escenarios son para aplicaciones virtuales de red y cualquier aplicación, lo que requiere grandes rangos de puertos de entrada. Se puede usar un sondeo de mantenimiento para determinar qué back-ends deberían recibir nuevos flujos. Puede usar un grupo de seguridad de red para emular un escenario de intervalo de puertos. Basic Load Balancer no admite puertos de alta disponibilidad. Consulte la [explicación detallada sobre los puertos HA](#).

Varios servidores front-end

Load Balancer admite varias reglas con varios front-ends. Standard Load Balancer amplía esta funcionalidad a los escenarios de salida. Las reglas de salida son lo opuesto a las de entrada. La regla de salida crea una asociación para las conexiones de salida. Standard Load Balancer usa todos los front-ends asociados a un recurso de máquina

virtual mediante una regla de equilibrio de carga. Además, un parámetro en la red de equilibrio de carga permite suprimir una red de equilibrio de carga para la conectividad de salida, lo que permite elegir front-ends específicos o, incluso, ninguno. Para la comparación, Basic Load Balancer selecciona un solo front-end de forma aleatoria. No hay ninguna capacidad que controle qué front-end se ha seleccionado.

Dirección IP flotante

Algunos escenarios de aplicación prefieren o requieren que varias instancias de la aplicación usen el mismo puerto en una sola máquina virtual en el grupo back-end. Entre los ejemplos comunes de reutilización de puertos se incluyen la agrupación en clústeres para alta disponibilidad, dispositivos de red virtuales y la exposición de varios puntos de conexión TLS sin volver a cifrar. Si desea reutilizar el puerto back-end en varias reglas, debe habilitar la IP flotante en la definición de la regla.

La **IP flotante** es el término de Azure para referirse a una parte de lo que se conoce como Direct Server Return (DSR). DSR consta de dos partes:

- Topología de flujo
- Esquema de asignación de direcciones IP

En un nivel de plataforma, Azure Load Balancer siempre funciona en una topología de flujo DSR independientemente de si la dirección IP flotante está habilitada o no. Esto significa que la parte de salida de un flujo siempre se reescribe correctamente para que se dirija de nuevo al origen. Sin una IP flotante, Azure expone un esquema de asignación de direcciones IP de equilibrio para facilitar el uso (la IP de las instancias de máquina virtual). Habilitar la dirección IP flotante cambia el esquema de asignación de direcciones IP a la IP de servidor front-end del equilibrador de carga para permitir una flexibilidad adicional. Obtenga más información [aquí](#).

Limitaciones

- La IP flotante no se admite actualmente en las configuraciones de IP secundarias para los escenarios de equilibrio de carga internos.
- Una regla de equilibrador de carga no puede abarcar dos redes virtuales. Los front-end y sus instancias de back-end deben estar ubicados en la misma red virtual.
- A los roles de trabajo web sin una red virtual y otros servicios de plataforma de Microsoft solo se puede acceder desde instancias que estén detrás de una instancia interna de Standard Load Balancer. No dependa de esta accesibilidad, ya que tanto el propio servicio como la plataforma subyacente pueden cambiar sin previo aviso. Si se requiere conectividad saliente al usar una instancia interna de Standard Load Balancer, se debe configurar la [conectividad saliente](#).
- Load Balancer proporciona equilibrio de carga y reenvío de puertos para protocolos TCP o UDP concretos. Las reglas de equilibrio de carga y las reglas NAT de entrada admiten TCP y UDP, pero no otros protocolos IP, incluido ICMP.
- No se generará el flujo saliente de una máquina virtual del back-end a un front-end de un equilibrador de carga interno.
- No se admite el reenvío de fragmentos IP en reglas de equilibrio de carga. No se admite la fragmentación IP de paquetes UDP y TCP en reglas de equilibrio de carga. Las reglas de equilibrio de carga de los puertos de alta disponibilidad se pueden usar para reenviar fragmentos de IP existentes. Para más información, consulte [Información general sobre los puertos de alta disponibilidad](#).

Pasos siguientes

- Consulte [Creación de una instancia de Standard Load Balancer](#) para empezar a usar una instancia de Load Balancer: crear una, crear máquinas virtuales con una extensión de IIS personalizada instalada y equilibrar la

carga de la aplicación web entre las máquinas virtuales.

- Información sobre [Conexiones salientes de Azure Load Balancer](#).
- Más información sobre [Azure Load Balancer](#).
- Más información sobre [sondeos de mantenimiento](#).
- Más información acerca de los [diagnósticos de Load Balancer Estándar](#).
- Más información sobre los [grupos de seguridad de red](#).

SKU de Azure Load Balancer

23/09/2020 • 4 minutes to read • [Edit Online](#)

Azure Load Balancer tiene dos SKU.

Comparación de SKU

Load balancer admite SKU estándar y básicas. Estas SKU difieren en la escala, las características y los precios del escenario. Cualquier escenario que sea posible con Basic Load Balancer se puede crear con Standard Load Balancer.

Para comparar y comprender las diferencias, consulte la siguiente tabla. Para más información, consulte [Información general sobre Standard Load Balancer de Azure](#).

NOTE

Microsoft recomienda Standard Load Balancer. Las máquinas virtuales independientes, los conjuntos de disponibilidad y los conjuntos de escalado de máquinas virtuales solo se pueden conectar a una SKU, nunca a ambas. Las SKU de Load Balancer y de la IP pública deben coincidir cuando se usan con direcciones IP públicas. Las SKU de Load Balancer y de la IP pública no son mutables.

	STANDARD LOAD BALANCER	VERSIÓN BÁSICO DE LOAD BALANCER
Tamaño de grupo de back-end	Admite hasta 1000 instancias.	Admite hasta 300 instancias.
Puntos de conexión del grupo de back-end	Todas las máquinas virtuales o conjuntos de escalado de máquinas virtuales de una red virtual individual.	Máquinas virtuales en un único conjunto de disponibilidad o conjunto de escalado de máquinas virtuales.
Sondeos de estado	TCP, HTTP, HTTPS	TCP, HTTP
Comportamiento del sondeo de mantenimiento	Las conexiones TCP permanecen activas en el sondeo de la instancia y en todos los sondeos.	Las conexiones TCP permanecen activas en un sondeo de instancia. Todas las conexiones TCP terminan cuando todos los sondeos están inactivos.
Zonas de disponibilidad	Servidores front-end con redundancia de zona y zonales para el tráfico de entrada y salida.	No disponible
Diagnóstico	Métricas multidimensionales de Azure Monitor	Registros de Azure Monitor
Puertos de alta disponibilidad	Disponibles para el equilibrador de carga interno	No disponible

	STANDARD LOAD BALANCER	VERSIÓN BÁSICO DE LOAD BALANCER
Seguro de forma predeterminada	Cerrado a los flujos de entrada, a menos que lo permita un grupo de seguridad de red. Se permite el tráfico interno desde la red virtual al equilibrador de carga interno.	Abrir de forma predeterminada. Grupo de seguridad de red opcional.
Reglas de salida	Configuración declarativa de NAT de salida	No disponible
Restablecimiento de TCP en tiempo de espera de inactividad	Disponible en cualquier regla	No disponible
Varios servidores front-end	Entrada y salida	Solo de entrada
Operaciones de administración	La mayoría de las operaciones en menos de 30 segundos	Normalmente, entre 60 y 90 segundos
Acuerdo de Nivel de Servicio	99.99%	No disponible

Para más información, consulte [Límites del equilibrador de carga](#). Para más información de Load Balancer Estándar, consulte los artículos de [introducción](#), [precios](#) y [Acuerdo de Nivel de Servicio](#).

Limitaciones

- Las SKU no son mutables. No se puede cambiar la SKU de un recurso existente.
- Un recurso de máquina virtual independiente, un recurso de conjunto de disponibilidad o un recurso de conjunto de escalado de máquinas virtuales puede hacer referencia únicamente a una SKU, nunca a ambas.
- Las [operaciones de traslado de suscripción](#) no se admiten en Standard Load Balancer ni en los recursos de direcciones IP públicas estándar.

Pasos siguientes

- Consulte el artículo sobre cómo [crear una instancia de Standard Load Balancer pública](#) para empezar a usar un equilibrador de carga.
- Más información en [Standard Load Balancer y Availability Zones](#).
- Más información sobre [sondeos de mantenimiento](#).
- Más información acerca de cómo usar [Load Balancer para conexiones salientes](#).
- Más información acerca de [Standard Load Balancer con reglas de equilibrio de carga para puertos HA](#).
- Más información sobre los [grupos de seguridad de red](#).

Sondeos de estado de Load Balancer

23/09/2020 • 33 minutes to read • [Edit Online](#)

Al usar reglas de equilibrio de carga con Azure Load Balancer, debe especificar un sondeo de estado para permitir que Load Balancer detecte el estado del punto de conexión de back-end. La configuración del sondeo de estado y las respuestas de sondeo determinan qué instancias del grupo de back-end recibirán nuevos flujos. Puede usar los sondeos de estado para detectar el error de una aplicación en un punto de conexión de back-end. También se puede generar una respuesta personalizada para un sondeo de estado y usar el sondeo de estado para el control de flujo con el fin de administrar la carga o el tiempo de inactividad planeado. Cuando se genera un error en el sondeo de estado, Load Balancer deja de enviar nuevos flujos a la instancia con estado incorrecto respectiva. La conectividad saliente no se ve afectada, solo se ve afectada la conectividad entrante.

Los sondeos de estado admiten varios protocolos. La disponibilidad de un protocolo específico de sondeo de estado varía en función de la SKU de Load Balancer. Además, el comportamiento del servicio varía según la SKU de Load Balancer, como se muestra en esta tabla:

	SKU ESTÁNDAR	SKU BÁSICO
Tipos de sondeo	TCP, HTTP, HTTPS	TCP, HTTP
Comportamiento de sondeo inactivo	Todos los sondeos inactivos y todos los flujos TCP continúan.	Todos los sondeos inactivos y todos los flujos TCP expiran.

IMPORTANT

Revise este documento en su totalidad, incluidas las [instrucciones de diseño importantes](#) que se indican a continuación para crear un servicio confiable.

IMPORTANT

Los sondeos de estado de Load Balancer parten de la dirección IP 168.63.129.16 y no se deben bloquear para que los sondeos marquen la instancia como activa. Para más información, consulte el apartado [Probe source IP address](#) (Dirección IP de origen de sondeo).

IMPORTANT

Independientemente del umbral de tiempo de espera configurado, los sondeos de estado del equilibrador de carga HTTP o HTTPS comprobarán automáticamente una instancia si el servidor devuelve cualquier código de estado que no sea HTTP 200 u OK o si la conexión se termina a través del restablecimiento de TCP.

Configuración de sondeo

La configuración del sondeo de estado se compone de los siguientes elementos:

- Duración del intervalo entre sondeos
- Número de respuestas de sondeo que han de observarse antes de que el sondeo pase a un estado diferente
- Protocolo del sondeo
- Puerto del sondeo

- Ruta de acceso HTTP que se va a usar para HTTP GET al utilizar sondeos HTTP(S)

NOTE

No se requiere una definición de sondeo ni se comprueba cuando se usa Azure PowerShell, la CLI de Azure, plantillas o una API. Las pruebas de validación de sondeos solo se realizan cuando se usa Azure Portal.

Descripción de la señal de aplicación, detección de la señal y reacción de la plataforma

El número de respuestas de sondeo se aplica a:

- el número de sondeos correctos que permiten que una instancia se marque como activa y
- el número de sondeos con tiempo de espera expirado que hacen que una instancia se marque como inactiva.

Los valores de intervalo y tiempo de espera especificados determinan si una instancia se marca como activa o inactiva. La duración del intervalo multiplicado por el número de respuestas de sondeo determina el período durante el cual se deben detectar las respuestas de sondeo. El servicio reaccionará después de que se hayan logrado los sondeos necesarios.

Se puede ilustrar mejor el comportamiento con un ejemplo. Si ha establecido el número de respuestas de sondeo en 2 y el intervalo en 5 segundos, esto significa que se deben observar dos errores de tiempo de espera expirado de sondeo en un intervalo de 10 segundos. Dado que la hora a la que se envía un sondeo no está sincronizada cuando la aplicación puede cambiar de estado, se puede enlazar el tiempo con la detección mediante dos escenarios:

1. Si la aplicación comienza a producir una respuesta de sondeo con tiempo de espera expirado justo antes de que llegue el primer sondeo, la detección de estos eventos tardará 10 segundos (intervalos de 2 x 5 segundos) más lo que tarda la aplicación en empezar a señalar un error de tiempo de espera expirado cuando llega el primer sondeo. Puede suponer que esta detección tarda algo más de 10 segundos.
2. Si la aplicación comienza a producir una respuesta de sondeo con tiempo de espera expirado justo después de que llegue el primer sondeo, la detección de estos eventos no comenzará hasta que llegue el siguiente sondeo (con el tiempo de espera expirado) más otros 10 segundos (intervalos de 2 x 5 segundos). Puede suponer que esta detección tarda poco menos de 15 segundos.

En este ejemplo, una vez que se ha producido la detección, la plataforma tarda una pequeña cantidad de tiempo en reaccionar a este cambio. Esto significa que, dependiendo de:

1. el momento en que la aplicación empieza a cambiar de estado,
2. el momento en que se detecta este cambio y se cumplen los criterios necesarios (número de sondeos enviados en el intervalo especificado) y
3. el momento en que la detección se haya comunicado a través de la plataforma,

puede asumir que la reacción a un sondeo con tiempo de espera expirado tardará entre poco más de 10 segundos como mínimo y algo más de 15 segundos como máximo en reaccionar ante un cambio en la señal de la aplicación. Este ejemplo tiene como fin ilustrar lo que está teniendo lugar; no obstante, no es posible predecir una duración exacta aparte de la orientación aproximada que se acaba de mostrar.

NOTE

El sondeo de estado comprobará todas las instancias en ejecución en el grupo de back-end. Si se detiene una instancia, no se sondeará hasta que se haya iniciado de nuevo.

Tipos de sondeo

El protocolo que usa el sondeo de estado puede configurarse con una de las siguientes opciones:

- [Agentes de escucha TCP](#)
- [Puntos de conexión HTTP](#)
- [Puntos de conexión HTTPS](#)

Los protocolos disponibles dependen de la SKU de Load Balancer usada:

	TCP	HTTP	HTTPS
SKU estándar	✓	✓	✓
SKU básica	✓	✓	✗

Sondeo TCP

Los sondeos TCP inician una conexión mediante la realización de un protocolo de enlace TCP abierto de tres vías con el puerto definido. Los sondeos TCP terminan una conexión con un protocolo de enlace TCP cerrado de cuatro vías.

El intervalo de sondeo mínimo es de 5 segundos y el número mínimo de respuestas incorrectas es 2. La duración total de todos los intervalos no puede superar los 120 segundos.

Un sondeo TCP genera un error cuando:

- El agente de escucha TCP de la instancia no responde durante el período de tiempo de expiración. El sondeo se marca como inactivo en función del número de solicitudes de sondeo con tiempo de espera expirado, que se configuraron para quedarse sin respuesta antes de marcar el sondeo como inactivo.
- El sondeo recibe un restablecimiento de TCP de la instancia.

A continuación se muestra cómo puede expresar este tipo de configuración de sondeo en una plantilla de Resource Manager:

```
{
  "name": "tcp",
  "properties": {
    "protocol": "Tcp",
    "port": 1234,
    "intervalInSeconds": 5,
    "numberOfProbes": 2
  },
}
```

Sondeo HTTP/HTTPS

NOTE

El sondeo HTTPS solo está disponible para [Standard Load Balancer](#).

Los sondeos HTTP y HTTPS se basan en el sondeo TCP y emiten una solicitud HTTP GET con la ruta de acceso especificada. Ambos sondeos admiten rutas de acceso relativas para la solicitud HTTP GET. Los sondeos HTTPS son lo mismo que los sondeos de HTTP con un contenedor de Seguridad de la capa de transporte (TLS, conocida anteriormente como SSL) añadido. El sondeo de estado se marca cuando la instancia responde con un código de estado 200 de HTTP dentro del período de tiempo de espera. De forma predeterminada, el sondeo de estado intenta comprobar cada 15 segundos el puerto de sondeo de estado configurado. El intervalo de sondeo mínimo es 5 segundos. La duración total de todos los intervalos no puede superar los 120 segundos.

Los sondeos HTTP/HTTPS también pueden ser útiles para implementar su propia lógica para quitar instancias de la rotación del equilibrador de carga si el puerto de sondeo es también el agente de escucha para el propio servicio. Por ejemplo, podría decidir quitar una instancia si está por encima del 90 % de la CPU y devolver un estado que no es 200.

NOTE

El sondeo HTTPS requiere el uso de certificados basados en que tienen un hash de firma mínimo de SHA256 en toda la cadena.

Si usa Cloud Services y tiene roles web que utilizan w3wp.exe, también obtiene una supervisión automática de su sitio web. Los errores en el código del sitio web devuelven un estado distinto de 200 para el sondeo del equilibrador de carga.

Un sondeo HTTP / HTTPS genera un error cuando:

- El punto de conexión de sondeo devuelve un código HTTP de respuesta distinto de 200 (por ejemplo, 403, 404 o 500). Esto marcará el sondeo de estado como inactivo de forma inmediata.
- El punto de conexión de sondeo no responde durante el intervalo de sondeo mínimo y un período de tiempo de espera de 30 segundos. Es posible que no se respondan varias solicitudes de sondeo antes de que el sondeo se marque como que no se está ejecutando, hasta que se haya alcanzado la suma de todos los intervalos de tiempo de espera.
- El punto de conexión de sondeo cierra la conexión mediante TCP Reset.

A continuación se muestra cómo puede expresar este tipo de configuración de sondeo en una plantilla de Resource Manager:

```
{
  "name": "http",
  "properties": {
    "protocol": "Http",
    "port": 80,
    "requestPath": "/",
    "intervalInSeconds": 5,
    "numberOfProbes": 2
  },
}
```

```
{
  "name": "https",
  "properties": {
    "protocol": "Https",
    "port": 443,
    "requestPath": "/",
    "intervalInSeconds": 5,
    "numberOfProbes": 2
  },
}
```

Sondeo de agente invitado (solo clásico)

Los roles del servicio en la nube (roles de trabajo y roles web) usan un agente invitado para la supervisión del sondeo de forma predeterminada. Un sondeo de agente invitado es una configuración de último recurso. Use siempre un sondeo de estado de forma explícita con un sondeo TCP o HTTP. Un sondeo del agente invitado no es tan eficaz como LOS sondeos definidos explícitamente en los escenarios de la mayor parte de las aplicaciones.

Un sondeo del agente invitado es una comprobación del agente invitado dentro de la máquina virtual. A continuación, escucha y responde con una respuesta HTTP 200 OK solo cuando la instancia está en estado Preparado. (Otros estados son Ocupado, Reciclado o Deteniendo).

Para obtener más información, consulte [Configuring the service definition file \(csdef\) for health probes](#) (Configuración del archivo de definición de servicio (csdef) para los sondeos de estado) o [Get started by creating a public load balancer for cloud services](#) (Introducción a la creación de un equilibrador de carga público para servicios en la nube).

Si el agente invitado no responde con HTTP 200 OK, el equilibrador de carga marca la instancia como sin respuesta. y deja de enviar flujos a dicha instancia. El equilibrador de carga sigue comprobando la instancia.

Si el agente invitado responde con un HTTP 200, el equilibrador de carga vuelve a enviar nuevos flujos a dicha instancia.

Cuando se usa un rol web, el código de sitio web normalmente se ejecuta en w3wp.exe, que no está supervisado por el agente invitado ni el tejido de Azure. Los errores en w3wp.exe (por ejemplo, las respuestas de HTTP 500) no se notifican al agente invitado. Por lo tanto, el equilibrador de carga no toma esa instancia fuera de la rotación.

Comportamiento del sondeo activo

Los sondeos de estado TCP, HTTP y HTTPS se consideran en buen estado y marcan el punto de conexión de back-end como tal en los casos siguientes:

- El sondeo de estado es correcto después de arrancar la máquina virtual.
- Se ha obtenido el número especificado de sondeos necesarios para marcar el punto de conexión de back-end como en buen estado.

Cualquier punto de conexión de back-end que haya logrado un estado correcto se considera apto para recibir nuevos flujos.

NOTE

Si el sondeo de estado fluctúa, el equilibrador de carga espera más tiempo antes de volver a poner el punto de conexión de back-end en buen estado. Este tiempo de espera adicional protege el usuario y la infraestructura y es una directiva intencionada.

Comportamiento de sondeo inactivo

Conexiones TCP

Se realizarán nuevas conexiones TCP correctamente al punto de conexión de back-end en buen estado.

Si se produce un error en el sondeo de estado de un punto de conexión de back-end, las conexiones TCP establecidas con él continúan.

Si se produce algún error en todos los sondeos de todas las instancias de un grupo de back-end, no se enviarán flujos nuevos a dicho grupo. Standard Load Balancer permitirá que los flujos de TCP establecidos continúen. Basic Load Balancer terminará todos los flujos de TCP existente en el grupo de back-end.

Load Balancer es un servicio intermedio (no termina las conexiones TCP) y el flujo siempre se produce entre el cliente y el sistema operativo invitado y la aplicación de la máquina virtual. Un grupo con todos los sondeos inactivos provocará que un front-end no responda a los intentos de apertura de una conexión TCP (SYN), ya que no hay ningún punto de conexión de back-end en buen estado que reciba el flujo y responda con SYN-ACK.

Datagramas UDP

Los datagramas UDP se entregarán a los puntos de conexión de back-end correctos.

UDP no tiene conexión y no hay ningún estado de flujo que realice el seguimiento para UDP. Si se produce un error en el sondeo de estado de un punto de conexión de back-end, los flujos UDP existentes se mueven a otra instancia en buen estado del grupo de back-end.

Si se produce un error en todos los sondeos de todas las instancias de un grupo de back-end, los flujos UDP terminarán para las instancias de Basic Load Balancer y Standard Load Balancer.

Dirección IP de origen del sondeo

Load Balancer usa un servicio de sondeo distribuido para su modelo de mantenimiento interno. El servicio de sondeos reside en todos los host donde residan las máquinas virtuales y se puede programar a petición para generar sondeos de estado por cada configuración de cliente. El tráfico del sondeo de estado se realiza directamente entre el servicio de sondeos que genera el sondeo de estado y la máquina virtual del cliente. Todos los sondeos de Load Balancer tienen como origen la dirección IP 168.63.129.16. Puede usar el espacio de direcciones IP dentro de una red virtual que no sea el espacio RFC1918. El uso de una dirección IP propiedad de Microsoft reservada de forma global reduce la posibilidad de un conflicto de dirección IP con el espacio de direcciones IP que se usa dentro de la red virtual. Esta dirección IP es la misma en todas las regiones y no cambia, y no supone un riesgo de seguridad porque solo el componente de la plataforma interna de Azure puede originar un paquete desde esta dirección IP.

La etiqueta del servicio AzureLoadBalancer identifica esta dirección IP de origen en los [grupos de seguridad de red](#) y permite el tráfico de sondeo de estado de forma predeterminada.

Además de los sondeos de estado de Load Balancer, en las [operaciones siguientes se usa esta dirección IP](#):

- Permite al agente de VM comunicarse con la plataforma para indicar que se encuentra en estado "Listo"
- Permite la comunicación con el servidor virtual de DNS para proporcionar resolución de nombres filtrada a los clientes que no definen servidores DNS personalizados. Este filtro garantiza que los clientes solo pueden resolver los nombres de host de su implementación.
- Permite que la máquina virtual obtenga una dirección IP dinámica desde el servicio DHCP en Azure.

Instrucciones de diseño

Los sondeos de estado se usan para hacer que el servicio sea resistente y se pueda escalar. Una configuración o un patrón de diseño incorrectos pueden afectar a la disponibilidad y escalabilidad del servicio. Revise todo el documento y tenga en cuenta el impacto en su escenario es cuando esta respuesta de sondeo se marca como inactiva o activa, y cómo afecta a la disponibilidad del escenario de la aplicación.

Al diseñar el modelo de mantenimiento de la aplicación, debe sondear un puerto en un punto de conexión de back-end que refleje el estado de esa instancia y el servicio de aplicación que se va a proporcionar. El puerto de la aplicación y el puerto de sondeo no deben ser el mismo. En algunos escenarios, puede ser conveniente que el puerto de sondeo sea diferente al que la aplicación usa para proporcionar el servicio.

En ocasiones, puede ser útil que la aplicación genere una respuesta de sondeo de estado no solo para detectar el estado de la aplicación, sino también para señalar directamente a Load Balancer si la instancia debe recibir flujos nuevos o no. Puede manipular la respuesta de sondeo para permitir que la aplicación cree contrapresión y limite la entrega de los flujos nuevos a una instancia si provoca un problema en el sondeo de estado, o bien prepara el mantenimiento de la aplicación e inicia el vaciado del escenario. Cuando se usa Standard Load Balancer, una [señal de sondeo inactivo](#) siempre permitirá que los flujos TCP continúen hasta el tiempo de espera de inactividad o el cierre de la conexión.

En el caso del equilibrio de carga de UDP, debe generar una señal de sondeo de estado personalizada desde el punto de conexión de back-end y usar un sondeo de estado TCP, HTTP o HTTPS destinado al agente de escucha correspondiente para reflejar el estado de la aplicación de UDP.

Si se usan [reglas de equilibrio de carga de puertos de alta disponibilidad](#) con [Standard Load Balancer](#), todos los puertos tienen la carga equilibrada y una sola respuesta del sondeo de estado tiene que reflejar el estado de toda la instancia.

No se debe traducir ni conectar mediante proxy un sondeo de estado a través de la instancia que recibe el

sondeo de estado con otra instancia de la red virtual, porque se podrían provocar errores en cascada en el escenario. Considere el escenario siguiente: un conjunto de aplicaciones de terceros se implementa en el grupo de back-end de un recurso de Load Balancer para proporcionar escalabilidad y redundancia para los dispositivos, y el sondeo de estado se configura para sondear un puerto que la aplicación de terceros redirige mediante un proxy o traduce a otras máquinas virtuales detrás del dispositivo. Si se sondea el mismo puerto que se usa para traducir o redirigir mediante un proxy a las otras máquinas virtuales detrás de la aplicación, cualquier respuesta de sondeo de una sola máquina virtual detrás de la aplicación marcará el propio dispositivo como inactivo. Esta configuración puede provocar un error en cascada del escenario completo de la aplicación a consecuencia de un punto de conexión de back-end único detrás del dispositivo. El desencadenador puede ser un error de sondeo intermitente que provocará que Load Balancer marque como inactivo el destino original (la instancia de la aplicación) y, a su vez, puede deshabilitar el escenario de toda la aplicación. En su lugar, sondee el estado del propio dispositivo. La selección del sondeo para determinar la señal de estado es una consideración importante para los escenarios de aplicaciones de red virtual (NVA) y debe consultar con su proveedor de aplicaciones cuál es la señal de estado adecuada para esos escenarios.

Si en las directivas de firewall no se permite la [dirección IP de origen](#) del sondeo, se producirá un error en el sondeo de estado, ya que no puede acceder a la instancia. A su vez, Load Balancer marcará la instancia como inactiva debido al error del sondeo de estado. Esta configuración incorrecta puede producir un error en el escenario de aplicación con equilibrio de carga.

Para que el sondeo de estado de Load Balancer marque la instancia como activa, se **debe** permitir esta dirección IP en todos los [grupos de seguridad de red](#) de Azure y en las directivas de firewall locales. De forma predeterminada, todos los grupos de seguridad de red incluyen la [etiqueta de servicio](#) AzureLoadBalancer para permitir el tráfico de sondeo de estado.

Si quiere probar un error de un sondeo de mantenimiento o marcar como inactiva una instancia individual, puede usar un [grupo de seguridad de red](#) para bloquear de forma explícita el sondeo de mantenimiento (puerto de destino o [dirección IP de origen](#)) y simular el error del sondeo.

No configure la red virtual con el intervalo de direcciones IP propiedad de Microsoft que contiene 168.63.129.16. Esas configuraciones entrarán en conflicto con la dirección IP del sondeo de estado y pueden provocar un error en el escenario.

Si tiene varias interfaces en la máquina virtual, es preciso que se asegure de que responde al sondeo en la interfaz en que lo recibió. Es posible que tenga que traducir la dirección de red de origen de esta dirección en la máquina virtual para cada interfaz.

No habilite [las marcas de tiempo TCP](#). Habilitar las marcas de tiempo TCP puede hacer que se produzca un error en los sondeos de estado debido a que la pila TCP del sistema operativo invitado de la máquina virtual quita los paquetes TCP y, como resultado, Load Balancer marca como inactivo el punto de conexión correspondiente. Normalmente, las marcas de tiempo TCP están habilitadas de forma predeterminada en las imágenes de máquina virtual con seguridad reforzada y se deben deshabilitar.

Supervisión

[Standard Load Balancer](#), tanto público como interno, expone el estado del sondeo de estado por punto de conexión y punto de conexión de back-end como métricas multidimensionales mediante Azure Monitor. Otros servicios de Azure o aplicaciones de asociados pueden usar estas métricas.

La instancia pública básica de Load Balancer expone el estado del sondeo de estado resumido por grupo de back-end mediante registros de Azure Monitor. Los registros de Azure Monitor no están disponible para las instancias internas básicas de Load Balancer. Puede usar los [registros de Azure Monitor](#) para comprobar el estado del sondeo de estado y el número de sondeos del equilibrador de carga público. El registro se puede utilizar con Power BI o con Azure Operational Insights para proporcionar estadísticas del estado de mantenimiento del equilibrador de carga.

Limitaciones

- Los sondeos HTTPS no admiten la autenticación mutua con un certificado de cliente.
- Debe asumir que se producirá un error en los sondeos de estado cuando se habiliten las marcas de tiempo TCP.

Pasos siguientes

- Más información sobre [Load Balancer Estándar](#)
- [Empiece a crear un equilibrador de carga público en Resource Manager mediante Azure PowerShell](#)
- [API REST para los sondeos de estado](#)
- Solicite nuevas capacidades de sondeo de estado con [Uservice de Load Balancer](#)

Diagnóstico de Standard Load Balancer con métricas, alertas y estado de los recursos

23/09/2020 • 30 minutes to read • [Edit Online](#)

Azure Standard Load Balancer proporciona las siguientes funcionalidades de diagnóstico:

- **Métricas y alertas multidimensionales:** Proporciona funcionalidades de diagnóstico multidimensionales para configuraciones de Standard Load Balancer mediante [Azure Monitor](#). Puede supervisar, administrar y solucionar problemas con los recursos del equilibrador de carga estándar.
- **Estado de los recursos:** el estado de Resource Health de su instancia de Load Balancer está disponible en la página Resource Health de Monitor. Esta comprobación automática le informa de la disponibilidad actual del recurso de Load Balancer.

En este artículo se proporciona una introducción a estas funcionalidades y maneras de usarlas con Load Balancer Estándar.

Métricas multidimensionales

Azure Load Balancer proporciona métricas multidimensionales en la página Métricas de Azure de Azure Portal y le ayuda a obtener información detallada de diagnóstico en tiempo real sobre los recursos del equilibrador de carga.

Las distintas configuraciones de Load Balancer Estándar proporcionan las siguientes métricas:

MÉTRICA	TIPO DE RECURSO	DESCRIPCIÓN	AGREGACIÓN RECOMENDADA
Disponibilidad de la ruta de acceso de datos	Equilibrador de carga interno y público	Load Balancer Estándar usa continuamente la ruta de acceso a los datos desde una región hasta el servidor front-end del equilibrador de carga y, finalmente, hasta la pila de SDN que respalda la máquina virtual. Siempre que permanezcan las instancias correctas, la medida sigue la misma ruta de acceso que el tráfico con equilibrio de carga de las aplicaciones. También se valida la ruta de acceso a los datos que usan los clientes. La medida es invisible para la aplicación y no interfiere con otras operaciones.	Average

MÉTRICA	TIPO DE RECURSO	DESCRIPCIÓN	AGREGACIÓN RECOMENDADA
Estado del sondeo de mantenimiento	Equilibrador de carga interno y público	Load Balancer Estándar usa un servicio de sondeo de mantenimiento distribuido que supervisa el mantenimiento del punto de conexión de la aplicación de acuerdo con la configuración. Esta métrica proporciona una vista agregada o filtrada por punto de conexión de cada punto de conexión de instancia del grupo del equilibrador de carga. Puede ver cómo Load Balancer observa el estado de su aplicación según se indica en la configuración de sondeo de estado.	Average
Paquetes SYN (sincronizar)	Equilibrador de carga interno y público	Load Balancer Estándar no finaliza las conexiones de Protocolo de control de transmisión (TCP) ni interactúa con los flujos de paquetes TCP o UDP. Los flujos y los protocolos de enlace son siempre entre el origen y la instancia de máquina virtual. Para solucionar mejor los escenarios de protocolo TCP, puede hacer uso de estos contadores de paquetes SYN para saber el número de intentos de conexión TCP realizados. La métrica indica el número de paquetes TCP SYN recibidos.	Average

MÉTRICA	TIPO DE RECURSO	DESCRIPCIÓN	AGREGACIÓN RECOMENDADA
Conexiones SNAT	Equilibrador de carga público	Load Balancer Estándar informa del número de flujos salientes enmascarados en el servidor front-end de dirección IP pública. Los puertos de traducción de direcciones de red de origen (SNAT) son un recurso agotable. Esta métrica puede proporcionar una indicación de la dependencia que su aplicación tiene de SNAT en los flujos salientes originados. Los contadores de los flujos de salida de SNAT que se realizaron con éxito y los que tuvieron algún error se notifican y se pueden utilizar para solucionar problemas y comprender el estado de los flujos de salida.	Average
Puertos SNAT asignados	Equilibrador de carga público	Standard Load Balancer informa del número de puertos SNAT asignados por instancia de back-end.	Average
Puertos SNAT usados	Equilibrador de carga público	Standard Load Balancer informa del número de puertos SNAT usados por instancia de back-end.	Average
Contadores de bytes	Equilibrador de carga interno y público	Load Balancer Estándar informa de los datos procesados por front-end. Es posible que observe que los bytes no se distribuyen equitativamente entre las instancias de back-end. Se espera que el algoritmo de Azure Load Balancer se base en flujos.	Average
Contadores de paquetes	Equilibrador de carga interno y público	Load Balancer Estándar informa de los paquetes procesados por front-end.	Average

NOTE

Cuando se usa la distribución del tráfico de un equilibrador de carga interno a través de una NVA o un paquete SYN de firewall, las métricas del contador de bytes y del contador de paquetes no están disponibles y se mostrarán como cero.

Visualización de las métricas del equilibrador de carga en Azure Portal

Azure Portal expone las métricas del equilibrador de carga en la página Métricas, que está disponible en la

página de recursos del equilibrador de carga de un recurso específico y también en la página de Azure Monitor.

Para ver las métricas de los recursos de Load Balancer Estándar:

1. Vaya a la página Métricas y realice una de las siguientes acciones:
 - En la página de recursos de equilibrador de carga, seleccione el tipo de métrica en la lista desplegable.
 - En la página de Azure Monitor, seleccione el recurso del equilibrador de carga.
2. Configure el tipo de agregación de métricas adecuado.
3. Opcionalmente, configure el filtrado y la agrupación necesarios.
4. Opcionalmente, configure el intervalo y la agregación de tiempo. La hora se muestra en UTC de forma predeterminada.

NOTE

La agregación de tiempo es importante cuando se interpretan ciertas métricas, ya que los datos se muestrean una vez cada minuto. Si la agregación de tiempo se establece en cinco minutos y se usa el tipo de agregación de métricas Suma en métricas como la de asignación de SNAT, el gráfico mostrará cinco veces el total de puertos SNAT asignados.

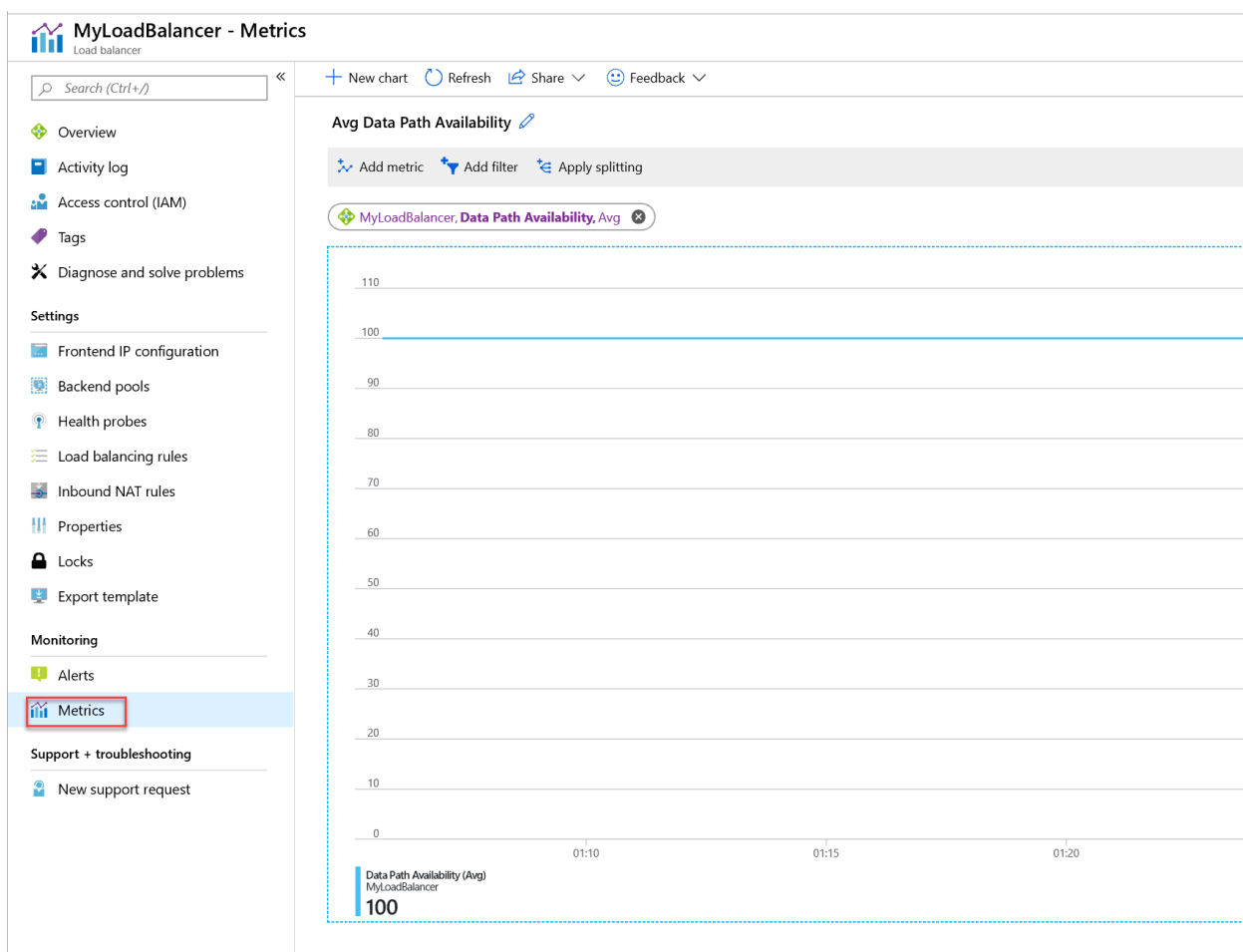


Ilustración: Métrica de disponibilidad de la ruta de acceso de datos para Standard Load Balancer

Recuperación de las métricas multidimensionales mediante programación con API

Para obtener orientación de API para recuperar las definiciones y los valores de las métricas multidimensionales, consulte el [tutorial sobre la API REST de supervisión de Azure](#). Estas métricas se pueden escribir en una cuenta de almacenamiento solo a través de la opción "Todas las métricas".

Configuración de alertas para métricas multidimensionales

Azure Standard Load Balancer admite alertas configurables fácilmente para métricas multidimensionales. Configure umbrales personalizados para que métricas específicas desencadenen alertas con distintos niveles de

gravedad para habilitar una experiencia de supervisión de recursos sin contacto.

Para configurar alertas:

1. Vaya a la subhoja de la alerta del equilibrador de carga.
2. Creación de una nueva regla de alertas
 - a. Configuración de la condición de alerta
 - b. (Opcional) Adición de un grupo de acciones para la reparación automatizada
 - c. Asigne la gravedad de la alerta, el nombre y la descripción que habilitan una reacción intuitiva.

NOTE

La ventana de configuración de la condición de alerta mostrará la serie temporal para el historial de señales. Hay una opción para filtrar esta serie temporal por dimensiones, como la dirección IP de back-end. Esto filtrará el gráfico de la serie temporal, pero **no** la propia alerta. No puede configurar alertas para direcciones IP de back-end específicas.

Escenarios comunes de diagnóstico y vistas recomendadas

¿Está lista y disponible la ruta de acceso de datos para mi front-end de Load Balancer?

► Expanda

¿Responden las instancias de back-end de mi Load Balancer a los sondeos?

► Expanda

¿Cómo se comprueban las estadísticas de conexión saliente?

► Expanda

¿Cómo se comprueba el uso y asignación de puertos SNAT?

► Expanda

¿Cómo se comprueban los intentos de conexión entrantes y salientes de mi servicio?

► Expanda

¿Cómo se comprueba el consumo de ancho de banda de la red?

► Expanda

¿Cómo se diagnostica la implementación de Load Balancer?

► Expanda

Estado de mantenimiento de los recursos

El estado de mantenimiento de los recursos de Load Balancer Estándar se expone en **Mantenimiento de los recursos**, en **Supervisar > Estado del servicio**.

Para ver el mantenimiento de los recursos públicos de Load Balancer Estándar:

1. Seleccione **Monitor > Service Health**.

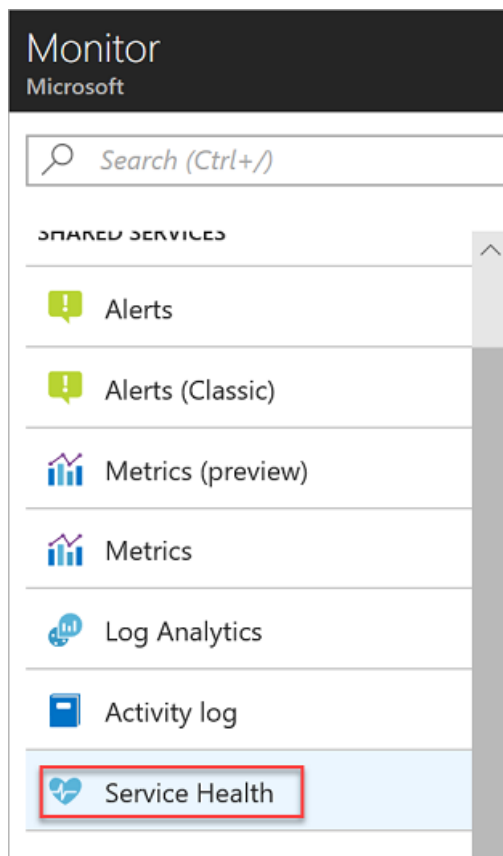


Ilustración: Vínculo de Service Health en Azure Monitor

2. Seleccione **Resource Health** y asegúrese de que **Id. de suscripción** y **Resource Type = Load Balancer** (Tipo de recurso = Load Balancer) están seleccionados.

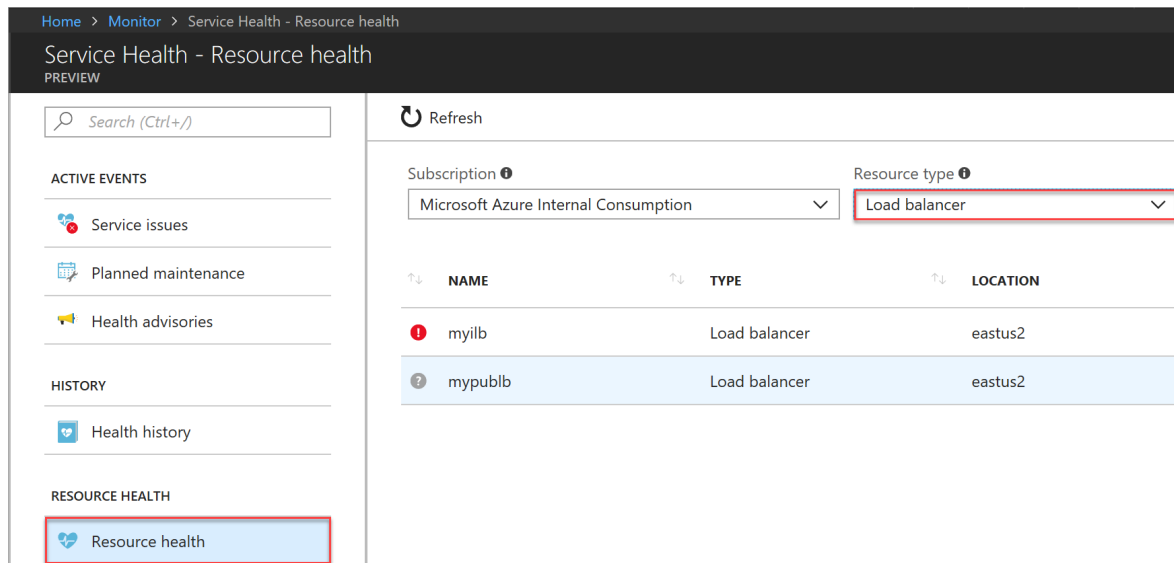


Ilustración: Selección de un recurso para ver su mantenimiento

3. Haga clic en el recurso de Load Balancer de la lista para ver sus datos históricos de estado de mantenimiento.

RESOURCE HEALTH

✔ Available

There aren't any known Azure platform problems affecting this Load Balancer [More details](#)

RECENT ACTIVITY

Activity for the past 24 hours

0 failed deployments | 0 role assignments | 0 errors | 0 alerts fired | [See all activity](#)

SOLUTIONS TO COMMON PROBLEMS

> My Load Balanced VMs are not receiving traffic

> VMs behind Load Balancer (LB) not responding to requests

> ADFS & SharePoint connections fail behind Load Balancer over VPN

> My issue is not listed

CONTACT MICROSOFT SUPPORT

If you need assistance solving your issue, please open a [support request](#)

Ilustración: Vista del mantenimiento de los recursos de Load Balancer

La descripción genérica del estado de mantenimiento de los recursos está disponible en la [documentación de RHC](#). En la tabla siguiente se enumeran los estados específicos de Azure Load Balancer:

ESTADO DE MANTENIMIENTO DE LOS RECURSOS	DESCRIPCIÓN
Disponible	El recurso de Standard Load Balancer está listo y disponible.
Degradado	El equilibrador de carga estándar tiene eventos iniciados por el usuario o la plataforma que afectan al rendimiento. La métrica de disponibilidad de la ruta de acceso a los datos ha informado un mantenimiento de menos del 90 %, pero superior que el 25 % durante al menos dos minutos. Experimentará un impacto entre moderado y grave en el rendimiento. [Siga la guía de solución de problemas de disponibilidad de la ruta de acceso a los datos] para determinar si hay eventos iniciados por el usuario que provoquen un impacto en la disponibilidad.
No disponible	El recurso de Standard Load Balancer público no es correcto. La métrica de disponibilidad de la ruta de acceso a los datos ha informado un mantenimiento de menos del 25 % durante al menos dos minutos. Experimentará un impacto significativo en el rendimiento o falta de disponibilidad para la conectividad entrante. Puede haber eventos de usuario o plataforma que generan la falta de disponibilidad. [Siga la guía de solución de problemas de disponibilidad de la ruta de acceso a los datos] para determinar si hay eventos iniciados por el usuario que afecten a la disponibilidad.

ESTADO DE MANTENIMIENTO DE LOS RECURSOS	DESCRIPCIÓN
Unknown	El estado de mantenimiento de recurso del recurso de Standard Load Balancer no se ha actualizado todavía o no ha recibido la información de disponibilidad de la ruta de acceso a los datos durante los últimos 10 minutos. Este estado debe ser transitorio y reflejará el estado correcto en cuanto se reciban dichos datos.

Pasos siguientes

- Más información acerca de [Load Balancer Estándar](#).
- Más información sobre la [conectividad saliente de Load Balancer](#).
- Más información acerca de [Azure Monitor](#).
- Obtenga información sobre la [API REST de Azure Monitor](#) y [cómo recuperar las métricas a través de la API REST](#).

Registros de Azure Monitor para el equilibrador de carga básica público

23/09/2020 • 13 minutes to read • [Edit Online](#)

Puede usar diferentes tipos de registros en Azure para administrar y solucionar problemas de Basic Load Balancer. Se puede acceder a algunos de estos registros a través del portal. Los registros se pueden transmitir a un centro de eventos o a un área de trabajo de Log Analytics. Se pueden extraer todos los registros desde Azure Blob Storage y visualizarse en distintas herramientas, como Excel y Power BI. Puede obtener más información acerca de los diferentes tipos de registros en la lista siguiente.

- **Registros de actividad:** Puede usar [Visualización de registros de actividad para supervisar acciones sobre recursos](#) para ver toda la actividad que se está enviando a las suscripciones de Azure y sus estados. Los registros de actividad están habilitados de manera predeterminada y se pueden ver en Azure Portal.
- **Registro de eventos de alerta:** puede utilizar este registro para las alertas generadas por el equilibrador de carga. El estado del equilibrador de carga se recopila cada cinco minutos. Este registro se escribe solo si se produce un evento de alerta del equilibrador de carga.
- **Registro de sondeo de estado:** puede utilizar este registro para ver los problemas detectados por el sondeo de estado, como el número de instancias en el grupo back-end que no reciben las solicitudes del equilibrador de carga debido a errores de sondeo de estado. Este registro se escribe cuando se produce un cambio en el estatus del sondeo de estado.

IMPORTANT

Los registros de eventos de sondeo de estado no funcionan en la actualidad y aparecen listados en los [problemas conocidos de Azure Load Balancer](#). Los registros solo están disponibles para los recursos implementados en el modelo de implementación del Administrador de recursos. No puede usar los registros de recursos del modelo de implementación clásica. Para más información sobre estos modelos de implementación, consulte [Understanding Resource Manager deployment and classic deployment](#) (Descripción de la implementación de Resource Manager y la implementación clásica).

Habilitar registro

El registro de actividades se habilita automáticamente para todos los recursos de Resource Manager. Habilite el registro de eventos y de sondeos de estado para iniciar la recopilación de los datos disponibles a través de esos registros. Para habilitar el registro, realice los siguientes pasos.

Inicie sesión en [Azure Portal](#). Si aún no tiene un equilibrador de carga, [cree uno](#) antes de continuar.

1. En el portal, haga clic en **Grupos de recursos**.
2. Seleccione el grupo de recursos **<resource-group-name>** donde esté el equilibrador de carga.
3. Seleccione el equilibrador de carga.
4. Seleccione **Registro de actividades > Configuración de diagnóstico**.
5. En el panel **Configuración de diagnóstico**, en **Configuración de diagnóstico**, seleccione **+ Agregar configuración de diagnóstico**.
6. En el panel de creación **Configuración de diagnóstico**, escriba **myLBdiagnostics** en el campo **Nombre**.

7. Tiene tres opciones para la **Configuración de diagnóstico**. Puede elegir una, dos o las tres y configurar cada una de ellas según sus requisitos:

- **Archivar en una cuenta de almacenamiento**
- **Transmisión a un centro de eventos**
- **Enviar a Log Analytics**

Archivar en una cuenta de almacenamiento

Necesitará una cuenta de almacenamiento ya creada para este proceso. Para crear una cuenta de almacenamiento, consulte [Creación de una cuenta de almacenamiento](#).

- Active la casilla junto a **Archivar en una cuenta de almacenamiento**.
- Seleccione **Configurar** para abrir el panel **Selección de una cuenta de almacenamiento**.
- Seleccione la **Suscripción** donde se creó la cuenta de almacenamiento en el cuadro desplegable.
- Seleccione el nombre de la cuenta de almacenamiento en **Cuenta de almacenamiento** en el cuadro desplegable.
- Seleccione **Aceptar**.

Transmitir a un centro de eventos

Necesitará un centro de eventos ya creado para este proceso. Para crear un centro de eventos, consulte [Inicio rápido: Creación de un centro de eventos mediante Azure Portal](#).

- Active la casilla situada junto a **Transmitir a un centro de eventos**.
- Seleccione **Configurar** para abrir el panel **Select event hub** (Selección del centro de eventos).
- Seleccione la **Suscripción** donde se creó el centro de eventos en el cuadro desplegable.
- Seleccione el **espacio de nombres del centro de eventos** en el cuadro desplegable.
- Seleccione el **nombre de la directiva del centro de eventos** en el cuadro desplegable.
- Seleccione **Aceptar**.

Enviar a Log Analytics

Deberá tener un área de trabajo de Log Analytics creada y configurada para este proceso. Para crear un área de trabajo de Log Analytics, consulte [Creación de un área de trabajo de Log Analytics en Azure Portal](#).

- Active la casilla junto a **Enviar a Log Analytics**.
- Seleccione la **Suscripción** donde se encuentra el área de trabajo de Log Analytics en el cuadro desplegable.
- Seleccione el **área de trabajo de Log Analytics** en el cuadro desplegable.

8. En la sección **LOG** del panel **Configuración de diagnóstico**, active la casilla junto a:

- **LoadBalancerAlertEvent**
- **LoadBalancerProbeHealthStatus**

9. En la sección **METRIC** del panel **Configuración de diagnóstico**, active la casilla junto a:

- **AllMetrics**
11. Compruebe que todo esté correcto y haga clic en **Guardar** en la parte superior del panel de creación de **Configuración de diagnóstico**.

Registro de actividades

El registro de actividad se genera de manera predeterminada. Los registros se conservan durante 90 días en el almacén de registros de eventos de Azure. Obtenga más información sobre estos registros en el artículo [Visualización de registros de actividad para supervisar acciones sobre recursos](#).

Archivado en los registros de la cuenta de almacenamiento

Registro de eventos de alerta

Este registro solo se genera si lo habilitó para cada uno de los equilibradores de carga. Los eventos se registran en formato JSON y se almacenan en la cuenta de almacenamiento que especificó cuando habilitó el registro. El ejemplo siguiente es de un evento.

```
{
  "time": "2016-01-26T10:37:46.6024215Z",
  "systemId": "32077926-b9c4-42fb-94c1-762e528b5b27",
  "category": "LoadBalancerAlertEvent",
  "resourceId": "/SUBSCRIPTIONS/XXXXXXXXXXXXXXXX-XXXX-XXXX-XXXXXXXX/RESOURCEGROUPS/RG7/PROVIDERS/MICROSOFT.NETWORK/LOADBALANCERS/WWEBLB",
  "operationName": "LoadBalancerProbeHealthStatus",
  "properties": {
    "eventName": "Resource Limits Hit",
    "eventDescription": "Ports exhausted",
    "eventProperties": {
      "public ip address": "40.117.227.32"
    }
  }
}
```

El resultado de JSON muestra la propiedad *eventname* que describirá el motivo de creación de una alerta por parte del equilibrador de carga. En este caso, la alerta generada se debió al agotamiento de puertos TCP causado por los límites de IP NAT de origen (SNAT).

Registro de sondeo de estado

Este registro solo se genera si lo habilitó para cada uno de los equilibradores de carga, tal como se indicó anteriormente. Los datos se almacenan en la cuenta de almacenamiento que especificó cuando habilitó el registro. Se crea un contenedor denominado "insights-logs-loadbalancerprobehealthstatus" y se registran los datos siguientes:

```
{
  "records": [
    {
      "time": "2016-01-26T10:37:46.6024215Z",
      "systemId": "32077926-b9c4-42fb-94c1-762e528b5b27",
      "category": "LoadBalancerProbeHealthStatus",
      "resourceId": "/SUBSCRIPTIONS/XXXXXXXXXXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXX/RESOURCEGROUPS/RG7/PROVIDERS/MICROSOFT.NETWORK/LOADBALANCERS/WWEBLB",
      "operationName": "LoadBalancerProbeHealthStatus",
      "properties": {
        "publicIpAddress": "40.83.190.158",
        "port": "81",
        "totalDipCount": 2,
        "dipDownCount": 1,
        "healthPercentage": 50.000000
      }
    },
    {
      "time": "2016-01-26T10:37:46.6024215Z",
      "systemId": "32077926-b9c4-42fb-94c1-762e528b5b27",
      "category": "LoadBalancerProbeHealthStatus",
      "resourceId": "/SUBSCRIPTIONS/XXXXXXXXXXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXX/RESOURCEGROUPS/RG7/PROVIDERS/MICROSOFT.NETWORK/LOADBALANCERS/WWEBLB",
      "operationName": "LoadBalancerProbeHealthStatus",
      "properties": {
        "publicIpAddress": "40.83.190.158",
        "port": "81",
        "totalDipCount": 2,
        "dipDownCount": 0,
        "healthPercentage": 100.000000
      }
    }
  ]
}
```

El resultado JSON muestra en el campo de propiedades la información básica del estado de mantenimiento del sondeo. La propiedad *dipDownCount* muestra el número total de instancias en el back-end que no están recibiendo tráfico de red debido a las respuestas de sondeo con error.

Visualización y análisis del registro de actividades

Puede ver y analizar los datos del registro de actividades mediante el uso de cualquiera de los métodos siguientes:

- **Herramientas de Azure:** puede recuperar información de los registros de actividad mediante Azure PowerShell, la interfaz de la línea de comandos (CLI) de Azure, la API REST de Azure o Azure Portal. En el artículo [Operaciones de auditoría con el Administrador de recursos](#) se detallan instrucciones paso a paso de cada método.
- **Power BI:** si todavía no tiene una cuenta de [Power BI](https://.microsoft.com/pricing), puede probarlo gratis. Con el [paquete de contenido de los registros de auditoría de Azure para Power BI](https://.microsoft.com/documentation/-content-pack-azure-audit-logs) puede analizar los datos con los paneles preconfigurados o puede personalizar las vistas para que se adapten a sus necesidades.

Visualización y análisis del registro de eventos y de sondeos de estado

Conéctese a la cuenta de almacenamiento y recupere las entradas del registro JSON para los registros de eventos y de sondeos de estado. Cuando descargue los archivos JSON, se pueden convertir a CSV y consultarlos en Excel, Power BI o cualquier otra herramienta de visualización de datos.

TIP

Si está familiarizado con Visual Studio y con los conceptos básicos de cambio de los valores de constantes y variables de C#, puede usar las [herramientas convertidoras de registros](#) que encontrará en GitHub.

Transmitir a un centro de eventos

Cuando se transmite información de diagnóstico a un centro de eventos, se puede usar para el análisis de registros centralizado en una herramienta SIEM de terceros con la integración de Azure Monitor. Para más información, consulte [Transmisión de datos de supervisión de Azure a un centro de eventos](#).

Enviar a Log Analytics

Los recursos de Azure pueden hacer que su información de diagnóstico se envíe directamente a un área de trabajo de Log Analytics, donde se pueden ejecutar consultas complejas en la información para la solución de problemas y el análisis. Para más información, consulte [Recopilación de registros de recursos de Azure en el área de trabajo de Log Analytics en Azure Monitor](#)

Pasos siguientes

[Descripción de los sondeos del equilibrador de carga](#)

Obtención de métricas de utilización de Load Balancer con la API de REST

23/09/2020 • 2 minutes to read • [Edit Online](#)

Recopile el número de bytes procesados por una instancia de [Standard Load Balancer](#) durante un intervalo de tiempo mediante la [API de REST de Azure](#).

La documentación de referencia completa y ejemplos adicionales para la API de REST están disponibles en [Azure Monitor REST reference](#) (Referencia de REST de Azure Monitor).

Compilar la solicitud

Utilice la siguiente solicitud GET para recopilar la [métrica de ByteCount](#) desde un servicio Standard Load Balancer.

```
GET
https://management.azure.com/subscriptions/{subscriptionId}/resourceGroups/{resourceGroupName}/providers/Microsoft.Network/loadBalancers/{loadBalancerName}/providers/microsoft.insights/metrics?api-version=2018-01-01&metricnames=ByteCount&timespan=2018-06-05T03:00:00Z/2018-06-07T03:00:00Z
```

Encabezados de solicitud

Los siguientes encabezados son obligatorios:

ENCABEZADO DE SOLICITUD	DESCRIPCIÓN
<i>Content-Type:</i>	Necesario. Establézcalo en <code>application/json</code> .
<i>Authorization:</i>	Necesario. Establézcalo en un token de acceso <code>Bearer</code> válido.

Parámetros del identificador URI

NOMBRE	DESCRIPCIÓN
subscriptionId	El id. de suscripción que identifica una suscripción de Azure. Si tiene varias suscripciones, consulte Trabajo con varias suscripciones .
resourceGroupName	Nombre del grupo de recursos que contiene el recurso. Puede obtener este valor en la API de Azure Resource Manager, la CLI o en Azure Portal.
loadBalancerName	El nombre de Azure Load Balancer.
metric names	Lista separada por comas de métricas válidas de Load Balancer .
api-version	La versión de API que se usará para la solicitud. En este documento se describe la versión <code>2018-01-01</code> de la API que se incluye en la dirección URL anterior.

NOMBRE	DESCRIPCIÓN
timespan	El intervalo de tiempo de la consulta. Es una cadena con el siguiente formato <code>startDateTime_ISO/endDateTime_ISO</code> . Este parámetro opcional se establece para devolver los datos recopilados durante un día en el ejemplo.

Cuerpo de la solicitud

No se necesita ningún cuerpo de solicitud para esta operación.

Control de la respuesta

Cuando la lista de valores de métricas se devuelve correctamente, se devuelve el código de estado 200. Una lista completa de códigos de error está disponible en la [documentación de referencia](#).

Respuesta de ejemplo

```
{
  "cost": 0,
  "timespan": "2018-06-05T03:00:00Z/2018-06-07T03:00:00Z",
  "interval": "PT1M",
  "value": [
    {
      "id":
"/subscriptions/{subscriptionId}/resourceGroups/{resourceGroupName}/providers/Microsoft.Network/loadBalancers/{loadBalancerName}/providers/Microsoft.Insights/metrics/ByteCount",
      "type": "Microsoft.Insights/metrics",
      "name": {
        "value": "ByteCount",
        "localizedValue": "Byte Count"
      },
      "unit": "Count",
      "timeseries": [
        {
          "metadatavalues": [],
          "data": [
            {
              "timeStamp": "2018-06-06T17:24:00Z",
              "total": 1067921034.0
            },
            {
              "timeStamp": "2018-06-06T17:25:00Z",
              "total": 0.0
            },
            {
              "timeStamp": "2018-06-06T17:26:00Z",
              "total": 3781344.0
            }
          ]
        }
      ]
    }
  ]
},
"namespace": "Microsoft.Network/loadBalancers",
"resourceregion": "eastus"
}
```

Introducción a los puertos de alta disponibilidad

23/09/2020 • 11 minutes to read • [Edit Online](#)

Azure Load Balancer Estándar le ayuda a equilibrar la carga de los flujos TCP y UDP en todos los puertos a la vez cuando se usa un equilibrador de carga interno.

Una regla de equilibrio de carga de puertos de alta disponibilidad (HA) es una variante de una regla de equilibrio de carga configurada en una instancia interna de Standard Load Balancer. Puede simplificar el uso de un equilibrador de carga si proporciona una única regla para equilibrar la carga de todos los flujos TCP y UDP que llegan a todos los puertos de una instancia interna de Load Balancer Estándar. La decisión de equilibrio de carga se toma por cada flujo. Esta decisión se toma en función de la conexión de cinco tuplas siguiente: dirección IP de origen, puerto de origen, dirección IP de destino, puerto de destino y protocolo.

Las reglas de equilibrio de carga de puertos de alta disponibilidad le ayudan a la hora de usar escenarios críticos como aquellos con alta disponibilidad y escalabilidad para dispositivos virtuales de red (NVA) que estén en redes virtuales. La característica también ayuda cuando hay que equilibrar la carga de un gran número de puertos.

Las reglas de equilibrio de carga de puertos de alta disponibilidad se configuran al establecer los puertos de front-end y back-end en **0** y el protocolo en **Todos**. Es entonces cuando el equilibrador de carga interno equilibra todos los flujos TCP y UDP, independientemente del número de puerto.

¿Por qué usar puertos de alta disponibilidad?

Dispositivos virtuales de red

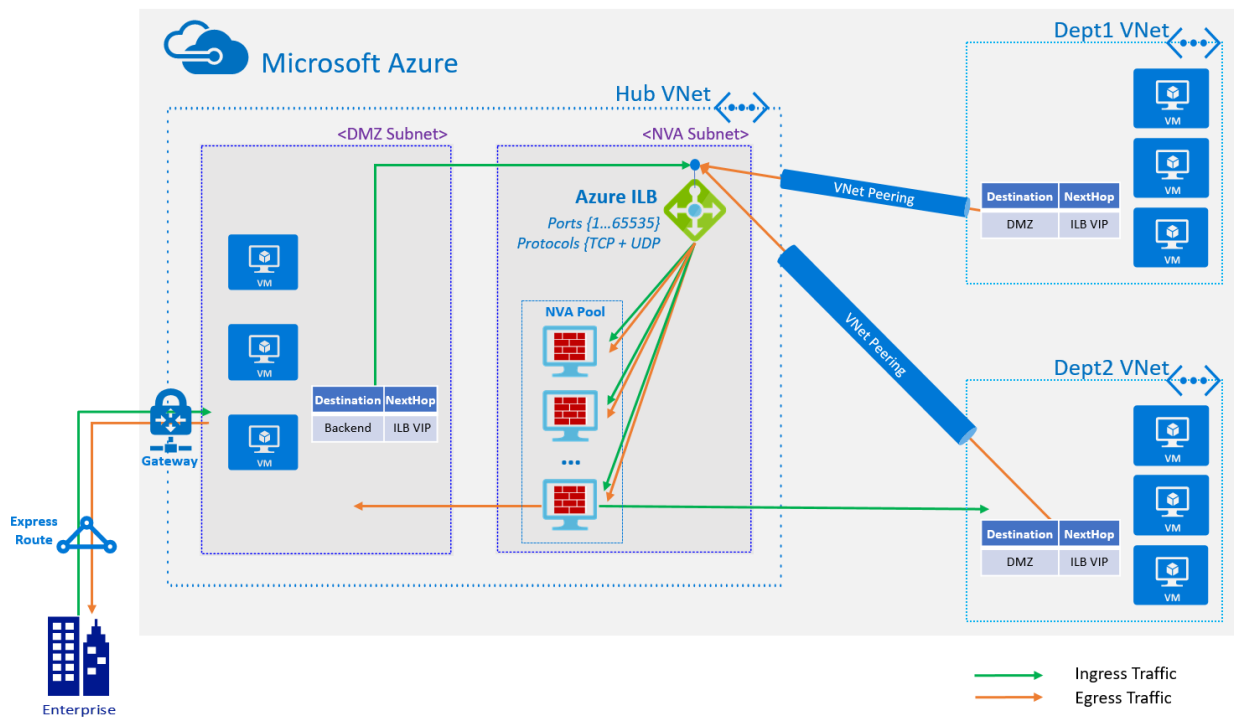
Puede usar dispositivos virtuales de red (NVA) para proteger la carga de trabajo de Azure frente a varios tipos de amenazas de seguridad. Cuando se usan NVA en estos escenarios, deben ser confiables y de alta disponibilidad y escalar horizontalmente a petición.

Puede lograr estos objetivos si agrega instancias de NVA al grupo de back-end del equilibrador de carga interno y configura una regla de equilibrador de carga en puertos de alta disponibilidad.

En los escenarios de HA de NVA, los puertos de alta disponibilidad proporcionan las siguientes ventajas:

- Proporcionan conmutación por error rápida para instancias en buen estado con sondeos de estado por instancia
- Garantizan un mayor rendimiento con escalado horizontal para instancias n -activas
- Proporcionan escenarios n -activos y activo-pasivos
- Eliminan la necesidad de usar soluciones complejas, como los nodos de Apache ZooKeeper, para la supervisión de dispositivos

En el diagrama siguiente se muestra una implementación de la red virtual de tipo hub-and-spoke. Los radios dirigen su tráfico a la red virtual del concentrador y a través de los NVA, antes de abandonar el espacio de confianza. Los NVA están detrás de una instancia interna de Load Balancer estándar con una configuración de puertos de alta disponibilidad. En consecuencia, se puede procesar y reenviar todo el tráfico. Cuando se configura como se muestra en el diagrama siguiente, una regla de equilibrio de carga de puertos de alta disponibilidad proporciona además simetría de flujo para el tráfico de entrada y salida.



NOTE

Si va a usar NVA, confirme con su proveedor cómo aprovechar mejor los puertos de alta disponibilidad y cuáles son los escenarios admitidos.

Equilibrado de carga de un gran número de puertos

También puede usar puertos de alta disponibilidad para aplicaciones que requieran equilibrar la carga de un gran número de puertos. Igualmente, puede simplificar estos escenarios mediante una instancia interna de [Load Balancer estándar](#) con puertos de alta disponibilidad. Una regla de equilibrio de carga única sustituye a varias reglas individuales de equilibrio de carga, una por cada puerto.

Disponibilidad en regiones

La característica de puertos de alta disponibilidad está disponible en todas las regiones globales de Azure.

Configuraciones admitidas

Una configuración de puertos HA con una única dirección IP no flotante (sin Direct Server Return) en una instancia interna de Load Balancer Estándar

Esta es una configuración básica de puertos HA. Para configurar una regla de equilibrio de carga de puertos HA en una sola dirección IP de front-end, haga lo siguiente:

1. Al configurar Load Balancer Estándar, active la casilla **Puertos HA** en la configuración de reglas de equilibrador de carga.
2. En **IP flotante**, seleccione **Deshabilitado**.

Esta configuración no permite ninguna otra configuración de reglas de equilibrio de carga en el equilibrador de carga actual. Tampoco permite ninguna otra configuración del equilibrador de carga interno para el conjunto especificado de instancias de back-end.

Pero, además de esta regla de puertos HA, puede configurar una instancia pública de Load Balancer Estándar para las instancias de back-end.

Una configuración de puertos HA con una única dirección IP flotante (Direct Server Return) en una instancia interna de Load Balancer Estándar

De igual forma, puede configurar el equilibrador de carga para usar una regla de equilibrio de carga con **Puerto HA** con un único front-end si establece **IP flotante** en **Habilitado**.

Esta configuración permite agregar más reglas de equilibrio de carga con IP flotante o un equilibrador de carga público. Pero no puede usar una configuración de equilibrio de carga de puertos HA con IP no flotante encima de esta configuración.

Varias configuraciones de puertos HA en una instancia interna de Load Balancer Estándar

Si el escenario requiere que configure más de un front-end de puertos HA para el mismo grupo de back-end, puede hacer lo siguiente:

- Configure más de una dirección IP privada de front-end para un único recurso interno Load Balancer Standard.
- Configure varias reglas de equilibrio de carga, donde cada una tenga seleccionada una única dirección IP de front-end.
- Seleccione la opción **Puertos HA** y establezca **IP flotante** en **Habilitado** en todas las reglas de equilibrio de carga.

Un equilibrador de carga interno con puertos HA y un equilibrador de carga público en la misma instancia de back-end

Puede configurar *un* recurso de una instancia pública de Load Balancer estándar para los recursos de back-end, junto con una única instancia interna de Load Balancer estándar con puertos HA.

Limitaciones

- Las reglas de equilibrio de carga de puertos de alta disponibilidad solo están disponibles para la instancia interna de Standard Load Balancer.
- **No** se admite la combinación de una regla de equilibrio de carga de puertos de alta disponibilidad y una regla de equilibrio de carga de puertos que no son de alta disponibilidad que apunta a las mismas configuraciones IP de back-end admitidas en una única configuración IP de front-end, salvo que ambas tengan habilitada la IP flotante.
- Los fragmentos IP existentes se reenviarán mediante reglas de equilibrio de carga de puertos de alta disponibilidad al mismo destino que el primer paquete. No se admite la fragmentación de IP en un paquete UDP o TCP.
- La simetría de flujo (principalmente en escenarios de NVA) se admite con instancias de back-end y una NIC única (y una sola configuración de IP), solo si se usa como se muestra en el diagrama anterior y mediante reglas de equilibrio de carga de los puertos de alta disponibilidad. No se proporciona para ningún otro escenario. Esto significa que dos o más recursos de Load Balancer y sus respectivas reglas toman decisiones independientes y nunca se coordinan. Consulte la descripción y el diagrama de los [dispositivos virtuales de red](#). Si usa varias NIC o sitúa la aplicación virtual de red entre una instancia pública y una privada de Load Balancer, la simetría de flujo no está disponible. Para solucionar este problema, puede alterar el origen del primer paquete del flujo de entrada a la IP de la aplicación para permitir que las respuestas lleguen a la misma NVA. Sin embargo, se recomienda encarecidamente utilizar una sola NIC y la arquitectura de referencia que se ha mostrado en el diagrama anterior.

Pasos siguientes

- [Aprenda a configurar los puertos de alta disponibilidad para su ILB mediante Azure Portal, PowerShell, la CLI o plantillas.](#)
- [Más información sobre Load Balancer estándar](#)

Varios servidores front-end para Azure Load Balancer

23/09/2020 • 15 minutes to read • [Edit Online](#)

Azure Load Balancer permite utilizar servicios de equilibrio de carga en varios puertos, varias direcciones IP, o en ambos. Puede usar las definiciones de equilibrador de carga públicas e internas para flujos de equilibrio de carga entre un conjunto de máquinas virtuales.

En este artículo se describen los fundamentos de esta capacidad, los conceptos importantes y las restricciones. Si solo desea exponer los servicios en una dirección IP, puede encontrar instrucciones simplificadas para configuraciones [públicas](#) o [internas](#) del equilibrador de carga. Agregar varios servidores front-end es una acción incremental de la configuración de un único front-end. Mediante los conceptos de este artículo, puede expandir una configuración simplificada en cualquier momento.

Al definir un Azure Load Balancer, las configuraciones de un grupo de servidores front-end y back-end están conectadas con reglas. El sondeo de estado a que hace referencia la regla se utiliza para determinar cómo se envían nuevos flujos a un nodo en el grupo de back-end. El front-end (también llamada VIP) se define mediante una tupla de 3 elementos formada por una dirección IP (pública o interna), un protocolo de transporte (UDP o TCP) y un número de puerto de la regla de equilibrio de carga. El grupo de servidores back-end es una colección de configuraciones de IP de máquinas virtuales (parte del recurso NIC) que hace referencia al grupo de servidores back-end de Load Balancer.

La tabla siguiente contiene algunas configuraciones de front-end de ejemplo:

FRONT-END	DIRECCIÓN IP	PROTOCOL	PORT
1	65.52.0.1	TCP	80
2	65.52.0.1	TCP	8080
3	65.52.0.1	UDP	80
4	65.52.0.2	TCP	80

En la tabla se muestran cuatro front-end diferentes. Los servidores front-end 1, 2 y 3 son un único servidor front-end con varias reglas. Se utiliza la misma dirección IP, pero el puerto o el protocolo es diferente para cada front-end. Los servidores front-end 1 y 4 son un ejemplo de varios servidores front-end, donde el mismo protocolo y puerto de front-end se reutilizan entre varios servidores front-end.

Azure Load Balancer proporciona flexibilidad para definir las reglas de equilibrio de carga. Una regla declara cómo se asigna una dirección y el puerto en el front-end a la dirección de destino y al puerto en el back-end. El hecho de que los puertos back-end se reutilicen o no a través de las reglas depende del tipo de regla. Cada tipo de regla tiene requisitos específicos que pueden afectar al diseño del sondeo y a la configuración del host. Existen dos tipos de reglas:

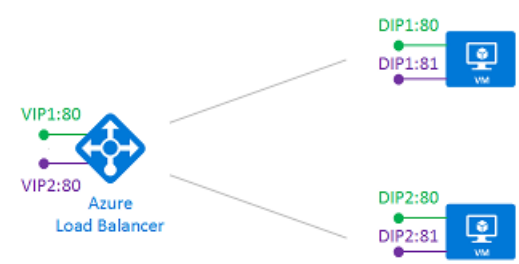
1. La regla predeterminada sin la reutilización de un puerto back-end
2. La regla de dirección IP flotante donde se reutilizan puertos back-end

Azure Load Balancer permite combinar ambos tipos de regla en la misma configuración de equilibrador de carga. El equilibrador de carga puede utilizarlos simultáneamente para una máquina virtual determinada, o

cualquier combinación, siempre y cuando se cumplan las restricciones de la regla. El tipo de regla que elija depende de los requisitos de la aplicación y la complejidad de la compatibilidad con dicha configuración. Debe evaluar qué tipos de reglas son mejores para su escenario.

Se analizan aún más estos escenarios empezando con el comportamiento predeterminado.

Tipo de regla 1: No reutilización de puerto back-end



En este escenario, los servidores front-end están configurados del modo siguiente:

FRONT-END	DIRECCIÓN IP	PROTOCOL	PORT
<div>1</div>	65.52.0.1	TCP	80
<div>2</div>	65.52.0.2	TCP	80

La DIP es el destino del flujo de entrada. En el grupo back-end, cada máquina virtual expone el servicio deseado en un puerto único en una DIP. Este servicio está asociado con el front-end a través de una definición de regla.

Se definen dos reglas:

REGLA	ASIGNACIÓN DE FRONT-END	PARA GRUPO BACK-END
1	<div>Frontend1:80</div>	<div>DIP1:80, DIP2:80</div>
2	<div>Frontend2:80</div>	<div>DIP1:81, DIP2:81</div>

La asignación completa en Azure Load Balancer ahora se realiza como sigue:

REGLA	DIRECCIÓN IP DEL FRONT-END	PROTOCOL	PORT	DESTINATION	PORT
<div>1</div>	65.52.0.1	TCP	80	Dirección IP de DIP	80
<div>2</div>	65.52.0.2	TCP	80	Dirección IP de DIP	81

Cada regla debe generar un flujo con una combinación única de dirección IP de destino y puerto de destino. Al variar el puerto de destino del flujo, varias reglas pueden entregar flujos en la misma DIP en puertos diferentes.

Los sondeos de estado siempre se dirigen a la DIP de una máquina virtual. Debe asegurarse de que el sondeo refleja el estado de la máquina virtual.

Tipo de regla 2: reutilización de puerto back-end mediante IP flotante

Azure Load Balancer ofrece la flexibilidad de reutilizar el puerto front-end en varios servidores front-end con independencia del tipo de regla usado. Además, algunos escenarios de aplicación prefieren o requieren que

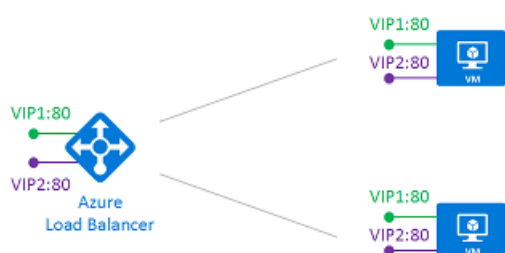
varias instancias de la aplicación usen el mismo puerto en una sola máquina virtual en el grupo back-end. Entre los ejemplos comunes de reutilización de puertos se incluyen la agrupación en clústeres para alta disponibilidad, dispositivos de red virtuales y la exposición de varios puntos de conexión TLS sin volver a cifrar.

Si desea reutilizar el puerto back-end en varias reglas, debe habilitar la IP flotante en la definición de la regla.

La "IP flotante" es el término de Azure para referirse a una parte de lo que se conoce como Direct Server Return (DSR). DSR consta de dos partes: una topología de flujo y un esquema de asignación de direcciones IP. En un nivel de plataforma, Azure Load Balancer siempre funciona en una topología de flujo DSR independientemente de si la dirección IP flotante está habilitada o no. Esto significa que la parte de salida de un flujo siempre se reescribe correctamente para que se dirija de nuevo al origen.

Con el tipo de regla predeterminada, Azure expone un esquema de asignación de direcciones IP de equilibrio de carga tradicional a efectos de facilitar el uso. Habilitar la dirección IP flotante cambia el esquema de asignación de direcciones IP para permitir una flexibilidad adicional, como se explica a continuación.

En el siguiente diagrama, se ilustra esta configuración:



En este escenario, cada máquina virtual del grupo back-end tiene tres interfaces de red:

- DIP: una NIC virtual asociada a la máquina virtual (configuración IP del recurso NIC de Azure)
- Frontend 1: una interfaz de bucle invertido en el sistema operativo invitado que se configura con la dirección IP de Frontend 1
- Frontend 2: una interfaz de bucle invertido en el sistema operativo invitado que se configura con la dirección IP de Frontend 2

Para cada máquina virtual del grupo de back-end, ejecute los siguientes comandos en un símbolo del sistema de Windows.

Para obtener la lista de nombres de interfaz que tiene en la máquina virtual, escriba este comando:

```
netsh interface show interface
```

En el caso de la NIC de VM (administrado por Azure), escriba este comando:

```
netsh interface ipv4 set interface "interfacename" weakhostreceive=enabled
```

(reemplace interfacename por el nombre de esta interfaz).

Para cada interfaz de bucle invertido que agregue, repita estos comandos:

```
netsh interface ipv4 set interface "interfacename" weakhostreceive=enabled
```

(reemplace interfacename por el nombre de esta interfaz de bucle invertido).



```
netsh interface ipv4 set interface "interfacename" weakhostsend=enabled
```


(reemplace interfacename por el nombre de esta interfaz de bucle invertido).





IMPORTANT

La configuración de las interfaces de bucle invertido se ejecuta en el sistema operativo invitado. Esta configuración no se ejecuta ni administra en Azure. Sin esta configuración, las reglas no funcionarán. Las definiciones de sondeo de mantenimiento usan la DIP de la máquina virtual en lugar de la interfaz de bucle invertido que representa el front-end de DSR. Por lo tanto, el servicio debe proporcionar respuestas de sondeo en un puerto DIP que reflejen el estado del servicio ofrecido en la interfaz de bucle invertido que representa el front-end de DSR.



Se asume que la configuración front-end es la misma que en el escenario anterior:

FRONT-END	DIRECCIÓN IP	PROTOCOL	PORT
 1	65.52.0.1	TCP	80
 2	65.52.0.2	TCP	80

Se definen dos reglas:

REGLA	FRONT-END	ASIGNAR A GRUPO DE SERVIDORES BACK-END
1	 Frontend1:80	 Frontend1:80 (en VM1 y VM2)
2	 Frontend2:80	 Frontend2:80 (en VM1 y VM2)

En la tabla siguiente se muestra la asignación completa en el equilibrador de carga:

REGLA	DIRECCIÓN IP DEL FRONT-END	PROTOCOL	PORT	DESTINATION	PORT
 1	65.52.0.1	TCP	80	igual que el front-end (65.52.0.1)	igual que el front-end (80)
 2	65.52.0.2	TCP	80	igual que el front-end (65.52.0.2)	igual que el front-end (80)

El destino del flujo de entrada es la dirección IP de front-end en la interfaz de bucle invertido de la máquina virtual. Cada regla debe generar un flujo con una combinación única de dirección IP de destino y puerto de destino. Al variar la dirección IP de destino del flujo, se puede reutilizar el puerto en la misma máquina virtual. El servicio se expone al equilibrador de carga mediante su enlace a la dirección IP del front-end y al puerto de la interfaz de bucle invertido correspondiente.

Observe que este ejemplo no cambia el puerto de destino. Aunque se trata de un escenario de IP flotante, Azure Load Balancer también admite la definición de una regla para volver a escribir el puerto de destino back-end y para que sea diferente del puerto de destino front-end.

El tipo de regla de dirección IP flotante es el fundamento de varios modelos de configuración del equilibrador de carga. Un ejemplo que está disponible actualmente es la configuración [SQL AlwaysOn con varios agentes de escucha](#) . Con el tiempo, se documentarán varios de estos escenarios.

Limitaciones

- Solo se admiten configuraciones de varios servidores front-end con máquinas virtuales de IaaS.
- Con la regla de dirección IP flotante, la aplicación debe utilizar la configuración IP principal para los flujos SNAT salientes. Si la aplicación se enlaza a la dirección IP del front-end configurada en la interfaz de bucle invertido en el sistema operativo invitado, entonces el SNAT saliente de Azure no está disponible para volver a escribir el flujo de salida y, por tanto, se produce un error en el flujo. Revise los [escenarios salientes](#).
- Las direcciones IP públicas repercuten en la facturación. Para obtener más información, vea [Precios de las direcciones IP](#)
- Se aplican los límites de suscripción. Para más información, vea los [límites de servicio](#) .

Pasos siguientes

- Revise [Conexiones salientes](#) para entender el impacto de varios front-ends en el comportamiento de conexión de salida.

Conexiones salientes en Azure

23/09/2020 • 35 minutes to read • [Edit Online](#)

Azure Load Balancer proporciona conectividad saliente mediante varios mecanismos. En este artículo se describen los escenarios y cómo administrarlos. Si tiene problemas con la conectividad saliente a través de Azure Load Balancer, vea la [guía de solución de problemas para conexiones salientes](#).

NOTE

En este artículo se describen las implementaciones de Resource Manager. Microsoft recomienda Resource Manager para las cargas de trabajo de producción.

Terminología

TÉRMINO	PROTOCOLOS APLICABLES	DETALLES
Traducción de direcciones de red de origen (SNAT)	TCP, UDP	En una implementación de Azure es posible comunicarse con puntos de conexión externos a Azure en el espacio de direcciones IP públicas. Cuando una instancia inicia un flujo de salida a un destino del espacio de direcciones IP públicas, Azure asigna dinámicamente la dirección IP privada a una dirección IP pública. Una vez creada esta asignación, el tráfico de retorno de este flujo originado de salida también puede comunicarse con la dirección IP privada donde se originó el flujo. Azure usa la traducción de direcciones de red de origen (SNAT) para realizar esta función.

TÉRMINO	PROTOCOLOS APLICABLES	DETALLES
Arquitectura de redes de sistemas de enmascaramiento de puertos (PAT)	TCP, UDP	<p>Cuando se enmascaran varias direcciones IP privadas detrás de una única dirección IP pública, Azure usa la traducción de direcciones de puerto (PAT) para ocultar o enmascarar las direcciones IP privadas. En PAT se usan puertos efímeros y se asignan previamente en función del tamaño del grupo. Cuando un recurso de Load Balancer público está asociado con instancias de máquina virtual, que no tienen direcciones IP públicas dedicadas, se reescribe cada origen de conexión saliente. El origen se reescribe del espacio de direcciones IP privadas de la red virtual a la dirección IP pública de servidor front-end del equilibrador de carga. En el espacio de direcciones IP públicas, la tupla de cinco elementos del flujo (dirección IP de origen, puerto de origen, protocolo de transporte IP, dirección IP de destino, puerto de destino) debe ser única. SNAT de enmascaramiento de puertos se puede usar con los protocolos IP UDP o TCP. Para conseguir esto, se usan puertos efímeros (puertos SNAT) después de volver a escribir la dirección IP de origen privada, dado que varios flujos se originan desde una única dirección IP pública. El algoritmo SNAT de enmascaramiento de puertos asigna los puertos SNAT de forma diferente para UDP que para TCP.</p>

TÉRMINO	PROTOCOLOS APLICABLES	DETALLES
Puertos SNAT	TCP	Los puertos SNAT son puertos efímeros disponibles para una determinada dirección IP de origen pública. Se consume un puerto SNAT por cada flujo a una combinación única de dirección IP y puerto de destino. En el caso de varios flujos TCP a la misma dirección IP, puerto y protocolo de destino, cada flujo TCP consume un solo puerto SNAT. Esto garantiza que los flujos son únicos si se han originado desde la misma dirección IP pública y se dirigen a la misma dirección IP, puerto y protocolo de destino. Si hay varios flujos, cada uno de ellos dirigido a una dirección IP, un puerto y un protocolo de destino diferentes, se comparte un solo puerto SNAT. La dirección IP, el puerto y el protocolo de destino hacen que los flujos sean únicos, sin necesidad de usar puertos de origen adicionales para distinguirlos en el espacio de direcciones IP públicas.
Puertos SNAT	UDP	Los puertos UDP SNAT se administran mediante un algoritmo diferente que los puertos TCP SNAT. Load Balancer utiliza un algoritmo que se conoce como "NAT de cono restringido de puertos" para UDP. Se consume un puerto SNAT por cada flujo, con independencia de la combinación de dirección IP y puerto de destino.
Agotamiento	-	Cuando se agotan los recursos de los puertos SNAT, los flujos de salida generan errores hasta que los flujos ya existentes liberan puertos SNAT. Load Balancer reclama puertos SNAT cuando el flujo se cierra y usa un tiempo de espera de inactividad de 4 minutos para reclamar puertos SNAT de los flujos inactivos. Los puertos UDP SNAT suelen agotarse mucho más rápidamente que los puertos TCP SNAT debido a la diferencia en el algoritmo utilizado. Debe tener presente esta diferencia al realizar pruebas de diseño y escalado.

TÉRMINO	PROTOCOLOS APLICABLES	DETALLES
Comportamiento de liberación de puertos SNAT	TCP	Si tanto el cliente como el servidor envían FIN/ACK, el puerto SNAT se liberará después de 240 segundos. Si se ve un RST, el puerto SNAT se liberará después de 15 segundos. Si se agotó el tiempo de expiración, el puerto se libera.
Comportamiento de liberación de puertos SNAT	UDP	Si se agotó el tiempo de expiración, el puerto se libera.
Reutilización del puerto SNAT	TCP, UDP	Una vez que se ha liberado un puerto, está disponible para reutilizarse según sea necesario. Puede pensar en los puertos SNAT como una secuencia del menor al mayor disponibles para un escenario determinado. El primer puerto SNAT disponible se usa para las nuevas conexiones.

Algoritmo de asignación de puertos

Azure usa un algoritmo para determinar el número de puertos SNAT asignados previamente disponibles en función del tamaño del grupo de back-end cuando se usa PAT. Para cada dirección IP pública asociada a un equilibrador de carga, hay 64 000 puertos disponibles como puertos SNAT para cada protocolo de transporte IP. Está preasignado el mismo número de puertos SNAT para UDP y TCP respectivamente, y se consumen independiente para cada protocolo de transporte de IP. Aunque la utilización del puerto SNAT varía en función de que el flujo sea UDP o TCP. Cuando se crean flujos de salida, estos puertos se consumen de forma dinámica (hasta el límite asignado previamente) y se liberan cuando el flujo se cierra o se producen [tiempos de espera de inactividad](#). Solo se consumen puertos si es necesario que los flujos sean únicos.

Puertos SNAT predeterminados asignados

En la tabla siguiente se muestran las asignaciones previas de puertos SNAT para los niveles de tamaño de grupo de servidores back-end:

TAMAÑO DEL GRUPO (INSTANCIAS DE MÁQUINA VIRTUAL)	PUERTOS SNAT ASIGNADOS PREVIAMENTE POR CONFIGURACIÓN IP
1-50	1024
51-100	512
101-200	256
201-400	128
401-800	64
801-1000	32

El cambio del tamaño del grupo de back-end puede afectar a algunos de los flujos establecidos:

- Si el tamaño del grupo de servidores back-end aumenta y pasa al siguiente nivel, la mitad de los

puertos SNAT previamente asignados se reclaman durante la transición al siguiente nivel más grande del grupo de servidores back-end. Los flujos que están asociados a un puerto SNAT reclamado agotan el tiempo de espera y deben restablecerse. Si se intenta un nuevo flujo, el flujo se inicia inmediatamente siempre y cuando los puertos asignados previamente estén disponibles.

- Si el tamaño del grupo de servidores back-end se reduce y pasa a un nivel inferior, aumenta el número de puertos SNAT disponibles. En este caso, los puertos SNAT asignados existentes y sus flujos respectivos no se ven afectados.

Información general sobre el escenario de conexiones salientes

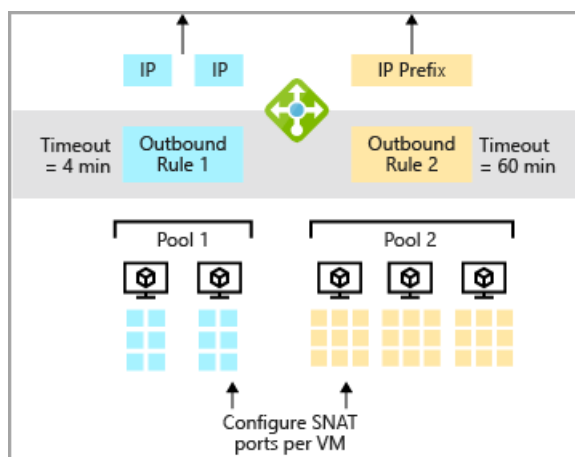
ESCENARIO	MÉTODO	PROTOCOLOS IP	DESCRIPCIÓN
1. Máquina virtual con un dirección IP pública (con o sin Azure Load Balancer)	SNAT, no se usa el enmascaramiento de puertos	TCP, UDP, ICMP, ESP	Azure usa la dirección IP pública asignada a la configuración IP de la NIC de la instancia para todos los flujos de salida. La instancia tiene disponibles todos los puertos efímeros. Es irrelevante si la máquina virtual es de carga equilibrada o no. Este escenario tiene prioridad sobre las demás. Una dirección IP pública asignada a una máquina virtual es una relación 1:1 (en lugar de 1:muchos) y se implementa como NAT de 1:1 sin estado.

ESCENARIO	MÉTODO	PROTOCOLOS IP	DESCRIPCIÓN
2. Load Balancer público asociado a una máquina virtual (ninguna dirección IP pública en la instancia o máquina virtual)	SNAT con enmascaramiento de puertos (PAT) mediante los servidores front-end de Load Balancer	TCP, UDP	<p>En este escenario, el recurso Load Balancer se debe configurar con una regla de equilibrador de carga que cree un vínculo entre el front-end de dirección IP pública y el grupo de back-end. Si no configura esta regla, el comportamiento es el que se describe en el escenario 3. No es necesario que la regla tenga un agente de escucha en funcionamiento en el grupo de servidores back-end o que el sondeo de mantenimiento sea correcto. Cuando la máquina virtual crea un flujo de salida, Azure traduce la dirección IP de origen privada del flujo de salida en la dirección IP pública del front-end público de Load Balancer a través de SNAT. Para distinguir los flujos individuales que se originan en la máquina virtual, se usan puertos efímeros de la dirección IP pública de front-end del equilibrador de carga. Cuando se crean flujos de salida, SNAT usa dinámicamente los puertos efímeros asignados previamente. En este contexto, los puertos efímeros usados para SNAT se conocen como puertos SNAT. Los puertos SNAT se asignan previamente, como se describe en la tabla de puertos SNAT asignados predeterminados.</p>

ESCENARIO	MÉTODO	PROTOCOLOS IP	DESCRIPCIÓN
3. Máquina virtual (sin Load Balancer, sin dirección IP pública) o máquina virtual asociada con Load Balancer interno básico	SNAT con enmascaramiento de puertos (PAT)	TCP, UDP	Cuando la máquina virtual crea un flujo de salida, Azure traduce la dirección IP de origen privado del flujo de salida en una dirección IP de origen público. Esta dirección IP pública no es configurable , no se puede reservar y no cuenta para el límite de recursos de IP pública de la suscripción. Si vuelve a implementar la máquina virtual, el conjunto de disponibilidad o el conjunto de escalado de máquinas virtuales, esta dirección IP pública se publicará y se solicitará una nueva dirección IP pública. No use este escenario para direcciones IP permitidas. En su lugar, use el escenario 1 o 2 donde se declara explícitamente el comportamiento de salida. Los puertos SNAT se asignan previamente, como se describe en la tabla de puertos SNAT asignados predeterminados .

Reglas de salida

Las reglas de salida simplifican la configuración de la traducción de direcciones de red públicas de salida de [Standard Load Balancer](#). Tiene control declarativo completo sobre la conectividad de salida para escalar y ajustar esta conectividad según sus necesidades específicas. En esta sección se expande el escenario 2 (B) descrito anteriormente.



Con las reglas de salida, puede usar Load Balancer para definir la NAT de salida desde cero. También puede escalar y ajustar el comportamiento de la NAT de salida existente.

Las reglas de salida permiten controlar:

- qué máquinas virtuales se deben traducir para qué direcciones IP públicas.
- cómo se deben asignar los puertos de SNAT de salida.
- para qué protocolos se proporciona traducción de salida.
- qué duración se debe usar para el tiempo de espera de inactividad de conexión (de 4 a 120 minutos).
- si quiere enviar un restablecimiento de TCP en caso de tiempo de espera de inactividad.
- protocolos de transporte TCP y UDP con una sola regla

Definición de la regla de salida

Como sucede con el resto de reglas de Load Balancer, las de salida siguen la misma sintaxis conocida que las reglas de NAT de entrada y de equilibrio de carga: **front-end + parámetros + grupo de back-end**. Una regla de salida configura una NAT de salida para *todas las máquinas virtuales identificadas por el grupo de back-end* que se deben traducir para el *front-end*. Los *parámetros* proporcionan un control más preciso sobre el algoritmo de NAT de salida.

NAT de salida de escala con varias direcciones IP

Cada dirección IP adicional que proporciona un front-end ofrece 64 000 puertos efímeros adicionales que Load Balancer puede usar como puertos SNAT. Puede usar varias direcciones IP para planear escenarios de gran escala y puede usar reglas de salida para mitigar los patrones con tendencia a [agotamiento de SNAT](#).

También puede usar un [prefijo de IP pública](#) directamente con una regla de salida. El uso de un prefijo de dirección IP pública proporciona un escalado más fácil y una creación simplificada de listas de permitidos para los flujos que se originan en la implementación de Azure. Puede configurar una configuración de IP de front-end en el recurso de Load Balancer para hacer referencia directamente a un prefijo de dirección IP pública. Esto permite el control exclusivo de Load Balancer sobre el prefijo IP público y la regla de salida usará automáticamente todas las direcciones IP públicas que contiene el prefijo de IP pública para las conexiones de salida. Cada una de las direcciones IP dentro del prefijo de IP pública proporciona 64 000 puertos efímeros adicionales por dirección IP que Load Balancer puede usar como puertos SNAT.

Tiempo de espera de inactividad de flujo de salida y restablecimiento de TCP

Las reglas de salida proporcionan un parámetro de configuración para controlar el tiempo de espera de inactividad del flujo de salida y que se corresponda con las necesidades de su aplicación. El tiempo de espera de inactividad de salida predeterminado es de 4 minutos. Puede aprender a [configurar tiempos de espera de inactividad](#). De forma predeterminada, Load Balancer anula el flujo en silencio cuando se alcanza el tiempo de espera de inactividad de salida. Con el parámetro `enableTCPReset`, puede habilitar un comportamiento de la aplicación más predecible y controlar si se debe enviar un restablecimiento de TCP bidireccional (TCP RST) al agotarse el tiempo de espera de inactividad de salida. Revise [Restablecimiento de TCP al agotarse el tiempo de espera de inactividad](#) para obtener detalles como la disponibilidad por regiones.

Impedir la conectividad saliente

Las reglas de equilibrio de carga proporcionan programación automática de NAT de salida. Sin embargo, algunos escenarios requieren que deshabilite la programación automática de NAT de salida por parte de la regla de equilibrio de carga para permitirle controlar o refinar el comportamiento, o bien mejoran al hacerlo.

Puede usar este parámetro de dos maneras:

1. Supresión opcional del uso de la dirección IP de entrada para SNAT de salida mediante la deshabilitación de SNAT de salida para una regla de equilibrio de carga
2. Ajuste los parámetros de SNAT de salida de una dirección IP que se usa para el tráfico de entrada

y salida al mismo tiempo. La programación de NAT de salida automática debe deshabilitarse para permitir que una regla de salida tome el control. Por ejemplo, para cambiar la asignación de puertos SNAT de una dirección que también se usa para la entrada, el parámetro `disableOutboundSnat` se debe establecer en true. Si intenta usar una regla de salida para volver a definir los parámetros de una dirección IP que también se usa para la entrada y no ha liberado la programación de NAT saliente de la regla de equilibrio de carga, se producirá un error en la operación para configurar una regla de salida.

IMPORTANT

La máquina virtual no tendrá conectividad de salida si este parámetro se establece en true y no tiene una regla de salida para definir la conectividad de salida. Algunas operaciones de la VM o la aplicación pueden depender de la conectividad de salida disponible. Asegúrese de comprender las dependencias del escenario y de haber considerado el impacto de hacer este cambio.

En ocasiones, no es aconsejable permitir que una máquina virtual cree un flujo de salida. O bien, puede que exista un requisito para administrar a qué destinos se puede llegar con los flujos de salida o qué destinos pueden comenzar los flujos de entrada. En este caso, puede usar los [grupos de seguridad de red](#) para administrar los destinos a los que puede llegar la máquina virtual. También puede usar los NSG para administrar qué destino público puede iniciar los flujos de entrada.

Cuando aplique un grupo de seguridad de red a una máquina virtual de carga equilibrada, preste atención a las [etiquetas de servicio](#) y a las [reglas de seguridad predeterminadas](#). Debe asegurarse de que la máquina virtual puede recibir solicitudes de sondeo de mantenimiento desde Azure Load Balancer.

Si un grupo de seguridad de red bloquea las solicitudes de sondeo de mantenimiento de la etiqueta predeterminada AZURE_LOADBALANCER, se producirá un error en el sondeo de mantenimiento de la máquina virtual y esta se marca como inactiva. Load Balancer dejará de enviar nuevos flujos a esa máquina virtual.

Escenarios con reglas de salida

#	ESCENARIO	DETALLES
---	-----------	----------

#	ESCENARIO	DETALLES
I	Limpieza de las conexiones de salida en un conjunto específico de direcciones IP públicas	<p>Puede usar una regla de salida para limpiar las conexiones de salida para que parezca que se originan en un conjunto concreto de direcciones IP públicas a fin de facilitar los escenarios de creación de listas de permitidos. Esta dirección IP pública de origen puede ser la misma que usa una regla de equilibrio de carga u otro conjunto de direcciones IP públicas distinto del que usa la regla de equilibrio de carga.</p> <ol style="list-style-type: none"> 1. Cree un prefijo IP público (o direcciones IP públicas a partir de un prefijo de IP pública). 2. Cree una instancia pública de Standard Load Balancer. 3. Cree servidores front-end que hagan referencia al prefijo de IP pública (o direcciones IP públicas) que quiera usar. 4. Reutilice un grupo de back-end o cree uno, y coloque las VM en un grupo de back-end de la instancia pública de Load Balancer. 5. Configure una regla de salida en la instancia pública de Load Balancer para programar una NAT de salida para estas VM mediante los front-end. Si no quiere usar la regla de equilibrio de carga para la salida, debe deshabilitar la SNAT de salida en la regla de equilibrio de carga.

#	ESCENARIO	DETALLES
II	Modificación de la asignación de puertos SNAT	<p>Puede utilizar reglas de salida para ajustar la asignación de puertos de SNAT automática basada en el tamaño del grupo de back-end. Por ejemplo, si tiene dos máquinas virtuales que comparten una única dirección IP pública de NAT de salida, puede aumentar el número de puertos SNAT asignados a de los 1024 puertos predeterminados si experimenta agotamiento de SNAT. Cada dirección IP pública puede contribuir hasta a 64 000 puertos efímeros. Si configura una regla de salida con un único front-end de dirección IP pública, puede distribuir un total de 64 000 puertos SNAT a VM del grupo de back-end. Para dos VM, se puede asignar un máximo de 32 000 puertos SNAT con una regla de salida ($2 \times 32\,000 = 64\,000$). Puede usar reglas de salida para ajustar los puertos SNAT asignados de forma predeterminada. Puede asignar más o menos puertos SNAT de los que proporciona la asignación predeterminada. Cada dirección IP pública de todos los front-end de una regla de salida aporta hasta 64 000 puertos efímeros para usarlos como puertos SNAT. Load Balancer asigna puertos SNAT en múltiplos de 8. Si proporciona un valor que no se puede dividir por 8, se rechaza la operación de configuración. Si intenta asignar más puertos SNAT de los disponibles en función del número de direcciones IP públicas, se rechaza la operación de configuración. Por ejemplo, si asigna 10 000 puertos por VM y 7 VM de un grupo de back-end tienen que compartir una única dirección IP pública, la configuración se rechaza ($7 \times 10\,000$ puertos SNAT > 64 000 puertos SNAT). Puede agregar más direcciones IP públicas al front-end de la regla de salida para habilitar el escenario. Puede volver a la asignación de puertos SNAT predeterminada basada en el tamaño del grupo de back-end si especifica 0 como el número de puertos. En ese caso, las primeras 50 instancias de máquina virtual obtendrán 1024 puertos, las instancias de máquina virtual de la 51 a la 100 obtendrán 512 y así sucesivamente según la tabla.</p>

#	ESCENARIO	DETALLES
III	Habilitación de solo la salida	Puede usar una instancia pública de Standard Load Balancer para proporcionar NAT de salida para un grupo de VM. En este escenario, puede usar una sola regla de salida, sin necesidad de reglas adicionales.
IV	NAT de salida solo para VM (no de entrada)	Defina una instancia pública de Standard Load Balancer, coloque las VM en el grupo de back-end y configure una regla de salida para programar la NAT de salida y limpiar las conexiones de salida para que se originen desde una dirección IP pública específica. También puede usar un prefijo IP público para simplificar la inclusión del origen de las conexiones de salida en una lista blanca. 1. Cree una instancia pública de Standard Load Balancer. 2. Cree un grupo de back-end y coloque las VM en un grupo de back-end de la instancia pública de Load Balancer. 3. Configure una regla de salida en la instancia pública de Load Balancer para programar una NAT de salida para estas VM.
V	NAT de salida para escenarios internos de Standard Load Balancer	Cuando se usa una instancia de Standard Load Balancer, la NAT de salida no está disponible hasta que la conectividad de salida se haya declarado explícitamente. Puede definir la conectividad de salida utilizando una regla de salida para crear conectividad de salida para las máquinas virtuales detrás de una instancia interna de Standard Load Balancer con los pasos siguientes: 1. Cree una instancia pública de Standard Load Balancer. 2. Cree un grupo de back-end y coloque las máquinas virtuales en un grupo de back-end de la instancia pública de Load Balancer además de la instancia interna de Load Balancer. 3. Configure una regla de salida en la instancia pública de Load Balancer para programar una NAT de salida para estas VM. Para más detalles sobre este escenario, consulte este ejemplo .

#	ESCENARIO	DETALLES
VI	Habilitar los protocolos TCP y UDP para NAT de salida con una instancia pública de Standard Load Balancer	<p>Cuando se usa una instancia pública de Standard Load Balancer, la programación de NAT de salida automática proporcionada coincide con el protocolo de transporte de la regla de equilibrio de carga. 1. Deshabilite la SNAT de salida en la regla de equilibrio de carga. 2. Configure una regla de salida en la misma instancia de Load Balancer. 3. Vuelva a usar el grupo de back-end que usó para sus VM. 4. Especifique "protocol": "All" como parte de la regla de salida. Si solo se usan reglas de NAT entrantes, no se proporciona ninguna NAT de salida.</p> <p>1. Coloque las VM en un grupo de back-end. 2. Defina una o varias configuraciones de IP de front-end con direcciones IP públicas o un prefijo de IP pública. 3. Configure una regla de salida en la misma instancia de Load Balancer. 4. Especifique "protocol": "All" como parte de la regla de salida.</p>

Limitaciones

- El número máximo de puertos efímeros posibles por dirección IP de front-end es 64 000.
- El intervalo de tiempo de espera de inactividad de salida que puede configurar oscila entre 4 y 120 minutos (de 240 a 7200 segundos).
- Load Balancer no es compatible con ICMP para NAT de salida.
- Las reglas de salida solo se pueden aplicar a la configuración de IP principal de una NIC. No se puede crear una regla de salida para la dirección IP secundaria de una máquina virtual o NVA. Se admiten varias NIC.
- Solo se puede acceder a los roles de trabajo web sin una red virtual y otros servicios de plataforma de Microsoft si se usa un equilibrador de carga estándar debido a un efecto secundario del funcionamiento de los servicios previos a la red virtual y otros servicios de plataforma. No dependa de este efecto secundario, porque el propio servicio o la plataforma subyacente pueden cambiar sin previo aviso. Siempre debe pensar que necesita crear conectividad de salida de manera explícita si lo desea al usar solo un equilibrador de carga estándar interno. El escenario 3 que se describe en este artículo no está disponible.

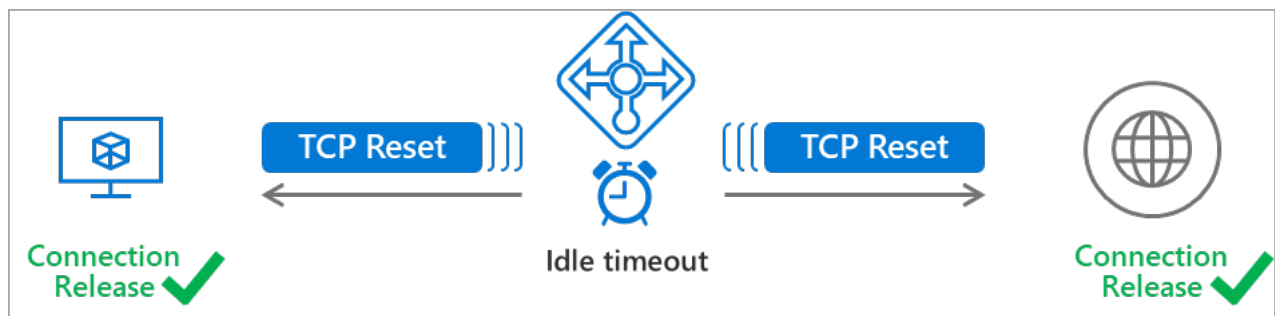
Pasos siguientes

- Más información acerca de [Load Balancer Estándar](#).
- Vea las [preguntas más frecuentes sobre Azure Load Balancer](#).
- Obtenga más información sobre las [reglas de salida](#) para la instancia pública de Load Balancer estándar.
- Más información acerca de [Load Balancer](#).
- Más información sobre los [grupos de seguridad de red](#).
- Aprenda sobre las demás [funcionalidades de red](#) clave en Azure.

Load Balancer con restablecimiento de TCP inactivo

23/09/2020 • 4 minutes to read • [Edit Online](#)

Puede usar [Standard Load Balancer](#) para crear un comportamiento de aplicación más predecible para los escenarios si habilita el restablecimiento de TCP inactivo para una regla determinada. El comportamiento predeterminado de Load Balancer es descartar silenciosamente los flujos cuando se alcanza el tiempo de inactividad de un flujo. Si habilita esta característica, Load Balancer enviará restablecimientos de TCP bidireccionales (paquete TCP RST) cuando se agote el tiempo de espera de inactividad. Esto le informará a los puntos de conexión de la aplicación que el tiempo de espera se agotó y ya no se puede usar. De ser necesario, los puntos de conexión pueden establecer una conexión nueva inmediatamente.



Puede cambiar este comportamiento predeterminado y habilitar el envío de restablecimientos de TCP al agotarse el tiempo de espera de inactividad en las reglas NAT de entrada, en las reglas de equilibrio de carga y en las [reglas de salida](#). Cuando se habilita en cada regla, Load Balancer envía restablecimientos TCP bidireccionales (paquetes RST de TCP) tanto a los puntos de conexión del cliente como a los del servidor en el momento en que se agota el tiempo de espera de inactividad para todos los flujos que correspondan.

Los puntos de conexión que reciben los paquetes RST de TCP cierran inmediatamente el socket correspondiente. De este modo, se proporciona una notificación inmediata a los puntos de conexión para indicar que se ha liberado la conexión y cualquier comunicación posterior en la misma conexión TCP generará un error. Las aplicaciones pueden purgar las conexiones cuando el socket se cierra y restablecer las conexiones según sea necesario sin tener que esperar que la conexión TCP, finalmente, agote el tiempo de espera.

En muchos escenarios, esto puede evitar que haya que enviar paquetes keepalive de TCP (o en la capa de la aplicación) para actualizar el tiempo de inactividad de un flujo.

Si la duración de la inactividad supera la permitida por la configuración o la aplicación muestra un comportamiento no deseado con los restablecimientos de TCP habilitados, es posible que siga teniendo que usar paquetes keepalive de TCP (o de la capa de la aplicación) para supervisar el estado de las conexiones TCP. Además, los paquetes keepalive también pueden seguir siendo útiles cuando la conexión atraviesa un proxy en algún lugar de la ruta de acceso, especialmente en el caso de los paquetes keepalive de la capa de la aplicación.

Examine con cuidado todo el escenario completo para decidir si le beneficia habilitar los restablecimientos de TCP y ajustar el tiempo de espera de inactividad, y si es posible que se requieran pasos adicionales para garantizar el comportamiento deseado de la aplicación.

Habilitación del restablecimiento de TCP al agotarse el tiempo de espera de inactividad

Con la API versión 2018-07-01, puede habilitar el envío de restablecimientos de TCP bidireccionales al agotarse el tiempo de espera de inactividad en cada regla:


```
"loadBalancingRules": [  
  {  
    "enableTcpReset": true | false,  
  }  
]
```

```
"inboundNatRules": [  
  {  
    "enableTcpReset": true | false,  
  }  
]
```

```
"outboundRules": [  
  {  
    "enableTcpReset": true | false,  
  }  
]
```

Disponibilidad en regiones

Disponible en todas las regiones.

Limitaciones

- TCP RST solo se envía durante la conexión TCP en el estado ESTABLECIDO.

Pasos siguientes

- Más información sobre [Standard Load Balancer](#).
- Más información sobre [reglas de salida](#).
- [Configurar TCP RST en tiempo de espera de inactividad](#)

Load Balancer Estándar y zonas de disponibilidad

23/09/2020 • 19 minutes to read • [Edit Online](#)

Azure Standard Load Balancer admite escenarios de zonas de disponibilidad. Puede usar Standard Load Balancer para aumentar la disponibilidad en todo el escenario mediante la alineación de recursos con zonas y su distribución entre ellas. Las zonas de disponibilidad, combinadas con Standard Load Balancer, son un conjunto de características ampliable y flexible que posibilita la creación de diferentes escenarios. Revise este documento para conocer estos [conceptos](#) y la [guía de diseño](#) de un escenario básico.

Conceptos de las zonas de disponibilidad aplicados a Load Balancer

Un equilibrador de carga hereda la configuración de zona de sus componentes:

- Front-end
- Reglas
- Definición de grupo de back-end

En el contexto de las zonas de disponibilidad, el comportamiento y las propiedades de una regla de equilibrador de carga se describen como con redundancia de zona o zonales. En el contexto del equilibrador de carga, con redundancia de zona siempre significa **varias zonas** y zonal significa aislar el servicio para una **sola zona**. Una instancia de Azure Load Balancer tiene dos tipos: pública e interna. Ambos tipos de equilibrador de carga admiten la redundancia de zona y la implementación zonal. Además, ambos pueden dirigir el tráfico entre las zonas según sea necesario.

Front-end

Un front-end de equilibrador de carga es una configuración de IP de front-end que hace referencia a una dirección IP pública o privada dentro de la subred de una red virtual. Conformar el punto de conexión con equilibrio de carga en el que se expone su servicio.

Un recurso de equilibrador de carga puede contener reglas con front-end zonales y con redundancia de zona al mismo tiempo. Cuando se garantiza una dirección IP pública o privada para una zona, no se puede modificar la zonalidad (o la ausencia de zonalidad). Para cambiar u omitir la zonalidad de un front-end con dirección IP pública o privada, vuelva a crear la dirección IP en la zona que corresponda.

Las zonas de disponibilidad no cambian las restricciones para varios servidores front-end. Revise el artículo [varios servidores front-end para Load Balancer](#) para obtener más información sobre esta funcionalidad.

Redundancia de zona

En una región con zonas de disponibilidad, un front-end de Standard Load Balancer tiene redundancia de zona. Varias zonas pueden servir como entrada o salida en una región. El tráfico se sirve mediante una dirección IP única. No son necesarios esquemas de redundancia de DNS.

Una única dirección IP de servidor front-end sobrevivirá a los errores de zona. Se puede usar la IP de front-end para llegar a todos los miembros del grupo de back-end (no afectados), independientemente de la zona. Se puede producir un error en una o más zonas de disponibilidad y la ruta de acceso de datos sobrevive siempre que una zona de la región permanezca correcta.

La dirección IP del front-end se suministra a la vez en varias implementaciones de infraestructura independientes de varias zonas de disponibilidad. Los reintentos o el restablecimiento se realizarán correctamente en otras zonas a las que no haya afectado por el error de zona.

Ilustración: Equilibrador de carga con redundancia de zona

Zonal

Puede optar por tener un front-end garantizado para una sola zona, que se conoce como un *front-end zonal*. Este escenario significa que cualquier flujo de entrada o de salida es atendido por una sola zona en una región. El front-end comparte destino con el estado de la zona. La ruta de acceso de datos no se ve afectada por errores en zonas distintas a la garantizada. Puede utilizar front-end zonales para exponer una dirección IP por cada zona de disponibilidad.

Además, se admite el uso de servidores front-end zonales directamente para puntos de conexión con equilibrio de carga dentro de cada zona. Puede usar esta configuración para exponer puntos de conexión con equilibrio de carga por zona para supervisar de forma individual cada zona. En el caso de los puntos de conexión públicos, puede integrarlos con un producto de equilibrio de carga de DNS como [Traffic Manager](#) y usar un nombre DNS único.

Ilustración: Equilibrador de carga con redundancia de zona

Si desea combinar estos conceptos (con redundancia de zona y zonal para el mismo back-end), consulte [varios front-end en Azure Load Balancer](#).

En el caso de un servidor front-end de equilibrador de carga público, se agrega un parámetro de **zonas** a la dirección IP pública. La configuración IP del servidor front-end que usa la regla correspondiente hace referencia a esta dirección IP pública.

En el caso de un servidor front-end de equilibrador de carga interno, se agrega un parámetro de **zonas** a la configuración IP del front-end del recurso de equilibrador de carga interno. Un servidor front-end zonal garantiza una dirección IP en una subred a una zona específica.

Back-end

Azure Load Balancer funciona con instancias de máquinas virtuales. Estas pueden ser independientes, conjuntos de disponibilidad o conjuntos de escalado de máquinas virtuales. Cualquier máquina virtual de una red virtual única puede formar parte del grupo de back-end, independientemente de la zona a la que esté asignada la máquina virtual.

Para alinear y garantizar el front-end y el back-end con una sola zona, basta con colocar las máquinas virtuales dentro de la misma zona en el grupo de back-end correspondiente.

Para ubicar las máquinas virtuales a través de varias zonas, coloque las máquinas virtuales de varias zonas en el mismo grupo de back-end.

Cuando use conjuntos de escalado de máquinas virtuales, ubique uno o más conjuntos de escalado de máquinas virtuales en el mismo grupo de back-end. Los conjuntos de escalado pueden estar en una o varias zonas.

Conexiones de salida

La redundancia de zona y la zonalidad se aplican a las [conexiones salientes](#). Todas las zonas proporcionan una dirección IP pública con redundancia de zona para las conexiones salientes. Una dirección IP pública zonal solo sirve en la zona en la que está asignada.

Las asignaciones del puerto SNAT de conexión saliente sobreviven a los errores de zona y el escenario seguirá proporcionando conectividad SNAT saliente si no se ve afectado por un error de zona. Los errores de

zona pueden requerir que las conexiones se vuelvan a establecerse para escenarios con redundancia de zona si una zona afectada sirvió el tráfico. Los flujos en zonas distintas de las zonas afectadas no se ven afectados.

El algoritmo de asignación previa de puerto SNAT es el mismo, con o sin zonas de disponibilidad.

Sondeos de estado

Las definiciones de sondeos de mantenimiento existentes permanecen tal cual estaban sin zonas de disponibilidad. Pero hemos ampliado el modelo de mantenimiento hasta un nivel de infraestructura.

Cuando se usan servidores front-end con redundancia de zona, el equilibrador de carga expande su comprobación de estado interna. El equilibrador de carga sondea de forma independiente la disponibilidad de una máquina virtual de cada zona y cierra las rutas de acceso de las zonas en las que se produjo un error sin intervención.

Otras zonas que puedan llegar a esta máquina virtual pueden continuar sirviendo la máquina virtual desde sus front-end respectivos. Durante los eventos de error, cada zona puede tener distribuciones diferentes de nuevos flujos al proteger el mantenimiento general de su servicio.

Consideraciones de diseño

Load Balancer es flexible en el contexto de las zonas de disponibilidad. Puede optar por alinearse con zonas y por la redundancia de zona para cada regla. Una mayor disponibilidad puede suponer una mayor complejidad. Al diseñar, tenga en mente la disponibilidad para lograr un rendimiento óptimo.

Redundancia de zona

Load Balancer hace sencillo tener una dirección IP única como un front-end con redundancia de zona. Una dirección IP con redundancia de zona puede servir a un recurso zonal en cualquier zona. La IP puede sobrevivir a uno o más errores de zona siempre que una de las zonas tenga un estado correcto dentro de la región. En su lugar, un servidor front-end zonal es una reducción del servicio a una única zona y comparte el mismo destino que la zona correspondiente.

La redundancia de zona no implica una ruta de acceso de datos sin incidencias ni un plano de control; es un plano de datos. Los flujos con redundancia de zona pueden usar cualquier zona y los flujos de un cliente utilizarán todas las zonas correctas de una región. En el caso de un error de zona, los flujos de tráfico que usan zonas correctas no se ven afectados.

Los flujos de tráfico que están usando una zona en el momento en que se produce un error en esta pueden resultar afectados, pero las aplicaciones se pueden recuperar. El tráfico continúa por las zonas correctas de la región después de la retransmisión cuando Azure ha detectado el error en la zona.

Límites entre zonas

Es importante comprender que cuando un servicio cruza zonas, comparte su destino no con una, sino potencialmente con varias zonas. Como resultado, el servicio podría no aumentar su disponibilidad en implementaciones no zonales.

Cuando use zonas de disponibilidad, evite la introducción de dependencias entre zonas no deseadas que anulen las mejoras de disponibilidad. Si la aplicación contiene varios componentes críticos, asegúrese de que sobrevivan a un error de zona.

Un único componente crítico puede afectar a toda la aplicación si solo se encuentra en una zona distinta de las zonas supervivientes. Considere también la restauración de la zona y cómo se restablecerá la aplicación. Obtenga información sobre cómo responde la aplicación a los errores en algunas partes de la misma. Revise los puntos clave y úselos para las preguntas al pensar sobre su escenario concreto.

- Si la aplicación tiene dos componentes:

- Dirección IP
- Máquina virtual con disco administrado

Están configurados en las zonas 1 y 2. Cuando se produce un error en la zona 1, el servicio no sobrevive. En los escenarios zonales no se deben cruzar las zonas, a menos que entienda perfectamente que se va a crear un modo de error potencialmente perjudicial. Este escenario puede proporcionar flexibilidad.

- Si la aplicación tiene dos componentes:
 - Dirección IP
 - Máquina virtual con disco administrado

Están configurados para tener redundancia de zona y estar en la zona 1. El servicio sobrevivirá el error de la zona 2, la zona 3 o ambas, a menos que se haya producido un error en la zona 1. No obstante, perderá cierta capacidad para razonar sobre el estado del servicio si solo presta atención a la disponibilidad del servidor front-end. Considere la posibilidad de desarrollar un modelo de mantenimiento y capacidad más amplio. Podría usar los conceptos zonal y con redundancia de zona juntos para ampliar su visión y capacidad de administración.

- Si la aplicación tiene dos componentes:
 - Servidor front-end de Load Balancer con redundancia de zona
 - Conjunto de escalado de máquinas virtuales entre tres zonas

Los recursos de las zonas que no sean afectados por el error estarán disponibles. La capacidad del servicio puede disminuir durante el error. Desde una perspectiva de infraestructura, la implementación puede sobrevivir a uno o más errores de zona. En este escenario, surgen las siguientes preguntas:

- ¿Conoce la respuesta de la aplicación ante estos errores y ante una capacidad disminuida?
- ¿Necesita contar con medidas de seguridad en el servicio para forzar la conmutación por error a un par de regiones, si es necesario?
- ¿Cómo serán la supervisión, la detección y la mitigación ante este escenario? Puede usar los diagnósticos de Standard Load Balancer para aumentar la supervisión del rendimiento del servicio. Tenga en cuenta lo que está disponible y lo que puede necesitar de un aumento.
- Las zonas pueden hacer que los errores sean más fáciles de entender y contener. Un error en la zona no es diferente a otros errores en cuanto a tiempos de espera, reintentos y algoritmos de retroceso. Azure Load Balancer proporciona rutas de acceso con redundancia de zona. El equilibrador de carga intenta recuperarse rápidamente en el nivel de paquete en tiempo real. Las retransmisiones o el restablecimiento puede producirse durante la aparición de un error. Es importante comprender cómo se enfrenta la aplicación con los errores. El esquema de equilibrio de carga sobrevivirá, pero debe planear con las siguientes preguntas en mente:
 - Cuando se produce un error en una zona, ¿el servicio lo comprende? Y si se pierde el estado, ¿cómo se recuperará?
 - Cuando vuelve la disponibilidad de una zona, ¿la aplicación sabe cómo realizar una recuperación de forma segura?

Revise [los patrones de diseño en la nube de Azure](#) para mejorar la resistencia de la aplicación a los escenarios de error.

Pasos siguientes

- Aprenda más sobre [zonas de disponibilidad](#).
- Más información sobre [Load Balancer Estándar](#)

- Obtenga información sobre cómo [equilibrar la carga de las máquinas virtuales dentro de una zona con Load Balancer estándar con un front-end de zona](#)
- Obtenga información sobre cómo [equilibrar la carga de las máquinas virtuales en distintas zonas con Load Balancer estándar con un front-end con redundancia de zona](#)
- Más información sobre [los patrones de diseño en la nube de Azure](#) para mejorar la resistencia de la aplicación a los escenarios de error.

Controles de seguridad para Azure Load Balancer

23/09/2020 • 2 minutes to read • [Edit Online](#)

En este artículo se explican los controles de seguridad integrados en Azure Load Balancer.

Un control de seguridad es una cualidad o característica de un servicio de Azure que ayuda a dicho servicio a prevenir y detectar vulnerabilidades de seguridad, así como a responder a ellas.

En cada control, utilizamos "Sí" o "No" para indicar si dicho control está habilitado o no en el servicio, y "N/D" si no está disponible para el servicio. También se puede incluir una nota o un vínculo para aportar más información sobre un atributo.

Red

CONTROL DE SEGURIDAD	SÍ/NO	NOTAS
Compatibilidad con punto de conexión de servicio	N/D	
Compatibilidad con la inserción de redes virtuales	N/D	
Compatibilidad con el aislamiento de red y los firewalls	N/D	
Compatibilidad con la tunelización forzada	N/D	

Supervisión y registro

CONTROL DE SEGURIDAD	SÍ/NO	NOTAS
Compatibilidad con la supervisión de Azure (Log Analytics, Application Insights, etc.)	Sí	Consulte Registros de Azure Monitor para el equilibrador de carga básica público .
Registro y auditoría del plano de administración y de control	Sí	Consulte Registros de Azure Monitor para el equilibrador de carga básica público .
Registro y auditoría del plano de datos	N/D	

Identidad

CONTROL DE SEGURIDAD	SÍ/NO	NOTAS
Authentication	N/D	
Authorization	N/D	

Protección de los datos

CONTROL DE SEGURIDAD	SÍ/NO	NOTAS
Cifrado del lado servidor en reposo: Claves administradas por Microsoft	N/D	
Cifrado en tránsito (por ejemplo, cifrado de ExpressRoute, cifrado en la red virtual y cifrado de red virtual a red virtual)	N/D	
Cifrado del lado servidor en reposo: claves administradas por el cliente (BYOK)	N/D	
Cifrado de nivel de columna (Azure Data Services)	N/D	
Llamadas a API cifradas	Sí	A través de Azure Resource Manager .

Administración de configuración

CONTROL DE SEGURIDAD	SÍ/NO	NOTAS
Compatibilidad con la administración de configuración (control de versiones de configuración, etc.)	N/D	

Pasos siguientes

- Más información sobre los [controles de seguridad integrados en los servicios de Azure](#).

Administración de grupos de back-end

23/09/2020 • 16 minutes to read • [Edit Online](#)

El grupo de back-end es un componente esencial del equilibrador de carga. Define el grupo de recursos que atenderán el tráfico de una regla de equilibrio de carga determinada.

Hay dos formas de configurar un grupo de back-end:

- Tarjeta de interfaz de red (NIC)
- Combinación de dirección IP e identificador de recurso de red virtual

Configure el grupo de back-end por la NIC si usa máquinas virtuales y conjuntos de escalado de máquinas virtuales existentes. Este método crea el vínculo más directo entre el recurso y el grupo de back-end.

Al asignar previamente el grupo de back-end con un intervalo de direcciones IP con el que planea crear posteriormente máquinas virtuales y conjuntos de escalado de máquinas virtuales, configure el grupo de back-end por la combinación de dirección IP e identificador de red virtual.

Las secciones de configuración de este artículo se centrarán en los siguientes elementos:

- Azure PowerShell
- Azure CLI
- API DE REST
- Plantillas del Administrador de recursos de Azure

En estas secciones se proporciona información sobre cómo se estructuran los grupos de back-end para cada opción de configuración.

Configuración del grupo de back-end mediante NIC

El grupo de back-end se crea como parte de la operación del equilibrador de carga. Se usa la propiedad de configuración de dirección IP de la NIC para agregar miembros al grupo de back-end.

Los siguientes ejemplos se centran en las operaciones de creación y rellenado del grupo de back-end para resaltar este flujo de trabajo y esta relación.

NOTE

Es importante tener en cuenta que los grupos de back-end configurados mediante la interfaz de red no se pueden actualizar como parte de una operación en el grupo de back-end. Cualquier incorporación o eliminación de recursos de back-end debe realizarse en la interfaz de red del recurso.

PowerShell

Cree un nuevo grupo de back-end:

```
$resourceGroup = "myResourceGroup"
$loadBalancerName = "myLoadBalancer"
$backendPoolName = "myBackendPool"

$backendPool =
New-AzLoadBalancerBackendAddressPool -ResourceGroupName $resourceGroup -LoadBalancerName $loadBalancerName -
BackendAddressPoolName $backendPoolName
```

Cree una nueva interfaz de red y agréguela al grupo de back-end:

```
$resourceGroup = "myResourceGroup"
$loadBalancerName = "myLoadBalancer"
$backendPoolName = "myBackendPool"
$nicname = "myNic"
$location = "eastus"
$vnetname = <your-vnet-name>

$vnet =
Get-AzVirtualNetwork -Name $vnetname -ResourceGroupName $resourceGroup

$nic =
New-AzNetworkInterface -ResourceGroupName $resourceGroup -Location $location -Name $nicname -
LoadBalancerBackendAddressPool $backendPoolName -Subnet $vnet.Subnets[0]
```

Recupere la información del grupo de back-end para que el equilibrador de carga confirme que esta interfaz de red se agrega al grupo de back-end:

```
$resourceGroup = "myResourceGroup"
$loadBalancerName = "myLoadBalancer"
$backendPoolName = "myBackendPool"

$lb =
Get-AzLoadBalancer -ResourceGroupName $res
Get-AzLoadBalancerBackendAddressPool -ResourceGroupName $resourceGroup -LoadBalancerName $loadBalancerName -
BackendAddressPoolName $backendPoolName
```

Cree una nueva máquina virtual y conecte la interfaz de red para colocarla en el grupo de back-end:

```
# Create a username and password for the virtual machine
$cred = Get-Credential

# Create a virtual machine configuration
$vmname = "myVM1"
$vmsize = "Standard_DS1_v2"
$pubname = "MicrosoftWindowsServer"
$nicname = "myNic"
$off = "WindowsServer"
$sku = "2019-Datacenter"
$resourceGroup = "myResourceGroup"
$location = "eastus"

$nic =
Get-AzNetworkInterface -Name $nicname -ResourceGroupName $resourceGroup

$vmConfig =
New-AzVMConfig -VMName $vmname -VMSize $vmsize | Set-AzVMOperatingSystem -Windows -ComputerName $vmname -
Credential $cred | Set-AzVMSourceImage -PublisherName $pubname -Offer $off -Skus $sku -Version latest | Add-
AzVMNetworkInterface -Id $nic.Id

# Create a virtual machine using the configuration
$vm1 = New-AzVM -ResourceGroupName $resourceGroup -Zone 1 -Location $location -VM $vmConfig
```

CLI

Cree el grupo de back-end:

```
az network lb address-pool create \  
--resourceGroup myResourceGroup \  
--lb-name myLB \  
--name myBackendPool
```

Cree una nueva interfaz de red y agréguela al grupo de back-end:

```
az network nic create \  
--resource-group myResourceGroup \  
--name myNic \  
--vnet-name myVnet \  
--subnet mySubnet \  
--network-security-group myNetworkSecurityGroup \  
--lb-name myLB \  
--lb-address-pools myBackEndPool
```

Recupere el grupo de back-end para confirmar que la dirección IP se ha agregado correctamente:

```
az network lb address-pool show \  
--resource-group myResourceGroup \  
--lb-name myLb \  
--name myBackendPool
```

Cree una nueva máquina virtual y conecte la interfaz de red para colocarla en el grupo de back-end:

```
az vm create \  
--resource-group myResourceGroup \  
--name myVM \  
--nics myNic \  
--image UbuntuLTS \  
--admin-username azureuser \  
--generate-ssh-keys
```

API DE REST

Cree el grupo de back-end:

```
PUT https://management.azure.com/subscriptions/{subscription-id}/resourceGroups/{resource-group-name}/providers/Microsoft.Network/loadBalancers/{load-balancer-name}/backendAddressPools/{backend-pool-name}?api-version=2020-05-01
```

Cree una interfaz de red y agréguela al grupo de back-end que ha creado mediante la propiedad de configuración de direcciones IP de la interfaz de red:

```
PUT https://management.azure.com/subscriptions/{subscription-id}/resourceGroups/{resource-group-name}/providers/Microsoft.Network/networkInterfaces/{nic-name}?api-version=2020-05-01
```

Cuerpo de la solicitud JSON:

```
{
  "properties": {
    "enableAcceleratedNetworking": true,
    "ipConfigurations": [
      {
        "name": "ipconfig1",
        "properties": {
          "subnet": {
            "id": "/subscriptions/{subscription-id}/resourceGroups/{resource-group-
name}/providers/Microsoft.Network/virtualNetworks/{vnet-name}/subnets/{subnet-name}"
          },
          "loadBalancerBackendAddressPools": {
            "id": "/subscriptions/{subscription-id}/resourceGroups/{resource-group-
name}/providers/Microsoft.Network/loadBalancers/{load-balancer-name}/backendAddressPools/{backend-pool-name}"
          }
        }
      }
    ]
  },
  "location": "eastus"
}
```

Recupere la información del grupo de back-end para que el equilibrador de carga confirme que esta interfaz de red se agrega al grupo de back-end:

```
GET https://management.azure.com/subscriptions/{subscription-id}/resourceGroups/{resource-group-
name}/providers/Microsoft.Network/loadBalancers/{load-balancer-name}/backendAddressPools/{backend-pool-name}?api-
version=2020-05-01
```

Cree una máquina virtual y conecte la NIC que hace referencia al grupo de back-end:

```
PUT https://management.azure.com/subscriptions/{subscription-id}/resourceGroups/{resource-group-
name}/providers/Microsoft.Compute/virtualMachines/{vm-name}?api-version=2019-12-01
```

Cuerpo de la solicitud JSON:

```
{
  "location": "eastus",
  "properties": {
    "hardwareProfile": {
      "vmSize": "Standard_D1_v2"
    },
    "storageProfile": {
      "imageReference": {
        "sku": "2016-Datacenter",
        "publisher": "MicrosoftWindowsServer",
        "version": "latest",
        "offer": "WindowsServer"
      },
      "osDisk": {
        "caching": "ReadWrite",
        "managedDisk": {
          "storageAccountType": "Standard_LRS"
        },
        "name": "myVMosdisk",
        "createOption": "FromImage"
      }
    },
    "networkProfile": {
      "networkInterfaces": [
        {
          "id": "/subscriptions/{subscription-id}/resourceGroups/myResourceGroup/providers/Microsoft.Network/networkInterfaces/{nic-name}",
          "properties": {
            "primary": true
          }
        }
      ]
    },
    "osProfile": {
      "adminUsername": "{your-username}",
      "computerName": "myVM",
      "adminPassword": "{your-password}"
    }
  }
}
```

Plantilla de Resource Manager

Siga la [plantilla de Resource Manager de este inicio rápido](#) para implementar un equilibrador de carga y máquinas virtuales, y para agregar las máquinas virtuales al grupo de back-end a través de la interfaz de red.

Configuración del grupo de back-end por dirección IP y red virtual

En escenarios con grupos de back-end rellenos previamente, use dirección IP y red virtual.

Toda la administración del grupo de back-end se realiza directamente en el objeto de grupo de back-end, como se resalta en los ejemplos siguientes.

IMPORTANT

Esta característica se encuentra actualmente en versión preliminar y tiene las siguientes limitaciones:

- Solo se puede utilizar con el equilibrador de carga estándar.
- Límite de 100 direcciones IP en el grupo de back-end
- Los recursos de back-end deben estar en la misma red virtual que el equilibrador de carga.
- Esta característica no se admite actualmente en Azure Portal.
- Los contenedores ACI no admiten esta característica actualmente
- Los equilibradores de carga o los servicios precedidos por equilibradores de carga no se pueden colocar en el grupo de back-end del equilibrador de carga

PowerShell

Cree un nuevo grupo de back-end:

```
$resourceGroup = "myResourceGroup"
$loadBalancerName = "myLoadBalancer"
$backendPoolName = "myBackendPool"
$vnetName = "myVnet"
$location = "eastus"
$nicName = "myNic"

$backendPool = New-AzLoadBalancerBackendAddressPool -ResourceGroupName $resourceGroup -
LoadBalancerName $loadBalancerName -Name $backendPoolName
```

Actualice el grupo de back-end con una nueva dirección IP de la red virtual existente:

```
$virtualNetwork =
Get-AzVirtualNetwork -Name $vnetName -ResourceGroupName $resourceGroup

$ip1 = New-AzLoadBalancerBackendAddressConfig -IpAddress "10.0.0.5" -Name "TestVNetRef" -
VirtualNetwork $virtualNetwork

$backendPool.LoadBalancerBackendAddresses.Add($ip1)

Set-AzLoadBalancerBackendAddressPool -InputObject $backendPool
```

Recupere la información del grupo de back-end del equilibrador de carga para confirmar que las direcciones de back-end se agregan al grupo de back-end:

```
Get-AzLoadBalancerBackendAddressPool -ResourceGroupName $resourceGroup -LoadBalancerName $loadBalancerName -
Name $backendPoolName
```

Cree una interfaz de red y agréguela al grupo de back-end. Establezca la dirección IP en una de las direcciones de back-end:

```
$nic =
New-AzNetworkInterface -ResourceGroupName $resourceGroup -Location $location -Name $nicName -PrivateIpAddress
10.0.0.4 -Subnet $virtualNetwork.Subnets[0]
```

Cree una máquina virtual y conecte la NIC con una dirección IP en el grupo de back-end:

```
# Create a username and password for the virtual machine
$cred = Get-Credential

# Create a virtual machine configuration
$vmname = "myVM1"
$vmsize = "Standard_DS1_v2"
$pubname = "MicrosoftWindowsServer"
$nicname = "myNic"
$off = "WindowsServer"
$sku = "2019-Datacenter"
$resourceGroup = "myResourceGroup"
$location = "eastus"

$nic =
Get-AzNetworkInterface -Name $nicname -ResourceGroupName $resourceGroup

$vmConfig =
New-AzVMConfig -VMName $vmname -VMSize $vmsize | Set-AzVMOperatingSystem -Windows -ComputerName $vmname -
Credential $cred | Set-AzVMSourceImage -PublisherName $pubname -Offer $off -Skus $sku -Version latest | Add-
AzVMNetworkInterface -Id $nic.Id

# Create a virtual machine using the configuration
$vm1 = New-AzVM -ResourceGroupName $resourceGroup -Zone 1 -Location $location -VM $vmConfig
```

CLI

Con la CLI puede rellenar el grupo de back-end mediante parámetros de la línea de comandos o mediante un archivo de configuración de JSON.

Cree y rellene el grupo de back-end mediante parámetros de la línea de comandos:

```
az network lb address-pool create \
--resource-group myResourceGroup \
--lb-name myLB \
--name myBackendPool \
--vnet {VNET resource ID} \
--backend-address name=addr1 ip-address=10.0.0.4 \
--backend-address name=addr2 ip-address=10.0.0.5
```

Cree y rellene el grupo de back-end mediante el archivo de configuración de JSON:

```
az network lb address-pool create \
--resource-group myResourceGroup \
--lb-name myLB \
--name myBackendPool \
--vnet {VNET resource ID} \
--backend-address-config-file @config_file.json
```

Archivo de configuración de JSON:

```
[
  {
    "name": "address1",
    "virtualNetwork": "/subscriptions/{subscriptionId}/resourceGroups/{resource-group-name}/providers/Microsoft.Network/virtualNetworks/{vnet-name}",
    "ipAddress": "10.0.0.4"
  },
  {
    "name": "address2",
    "virtualNetwork": "/subscriptions/{subscriptionId}/resourceGroups/{resource-group-name}/providers/Microsoft.Network/virtualNetworks/{vnet-name}",
    "ipAddress": "10.0.0.5"
  }
]
```

Recupere la información del grupo de back-end del equilibrador de carga para confirmar que las direcciones de back-end se agregan al grupo de back-end:

```
az network lb address-pool show \
--resource-group myResourceGroup \
--lb-name MyLb \
--name MyBackendPool
```

Cree una interfaz de red y agréguela al grupo de back-end. Establezca la dirección IP en una de las direcciones de back-end:

```
az network nic create \
--resource-group myResourceGroup \
--name myNic \
--vnet-name myVnet \
--subnet mySubnet \
--network-security-group myNetworkSecurityGroup \
--lb-name myLB \
--private-ip-address 10.0.0.4
```

Cree una máquina virtual y conecte la NIC con una dirección IP en el grupo de back-end:

```
az vm create \
--resource-group myResourceGroup \
--name myVM \
--nics myNic \
--image UbuntuLTS \
--admin-username azureuser \
--generate-ssh-keys
```

API DE REST

Cree el grupo de back-end y defina las direcciones de back-end mediante una solicitud PUT de grupo de back-end. Configure las direcciones de back-end en el cuerpo JSON de la solicitud PUT por:

- Nombre de dirección
- Dirección IP
- Identificador de red virtual

```
PUT
https://management.azure.com/subscriptions/subid/resourceGroups/testrg/providers/Microsoft.Network/loadBalancer
s/lb/backendAddressPools/backend?api-version=2020-05-01
```


Cuerpo de la solicitud JSON:

```
{
  "properties": {
    "loadBalancerBackendAddresses": [
      {
        "name": "address1",
        "properties": {
          "virtualNetwork": {
            "id": "/subscriptions/{subscription-id}/resourceGroups/{resource-group-
name}/providers/Microsoft.Network/virtualNetworks/{vnet-name}"
          },
          "ipAddress": "10.0.0.4"
        }
      },
      {
        "name": "address2",
        "properties": {
          "virtualNetwork": {
            "id": "/subscriptions/{subscription-id}/resourceGroups/{resource-group-
name}/providers/Microsoft.Network/virtualNetworks/{vnet-name}"
          },
          "ipAddress": "10.0.0.5"
        }
      }
    ]
  }
}
```

Recupere la información del grupo de back-end del equilibrador de carga para confirmar que las direcciones de back-end se agregan al grupo de back-end:

```
GET https://management.azure.com/{subscription-id}/resourceGroups/{resource-group-
name}/providers/Microsoft.Network/loadBalancers/{load-balancer-name}/backendAddressPools/{backend-pool-name}?
api-version=2020-05-01
```

Cree una interfaz de red y agréguela al grupo de back-end. Establezca la dirección IP en una de las direcciones de back-end:

```
PUT https://management.azure.com/subscriptions/{subscription-id}/resourceGroups/{resource-group-
name}/providers/Microsoft.Network/networkInterfaces/{nic-name}?api-version=2020-05-01
```

Cuerpo de la solicitud JSON:

```
{
  "properties": {
    "enableAcceleratedNetworking": true,
    "ipConfigurations": [
      {
        "name": "ipconfig1",
        "properties": {
          "privateIPAddress": "10.0.0.4",
          "subnet": {
            "id": "/subscriptions/{subscription-id}/resourceGroups/{resource-group-name}/providers/Microsoft.Network/virtualNetworks/{vnet-name}/subnets/{subnet-name}"
          }
        }
      }
    ]
  },
  "location": "eastus"
}
```

Cree una máquina virtual y conecte la NIC con una dirección IP en el grupo de back-end:

```
PUT https://management.azure.com/subscriptions/{subscription-id}/resourceGroups/{resource-group-name}/providers/Microsoft.Compute/virtualMachines/{vm-name}?api-version=2019-12-01
```

Cuerpo de la solicitud JSON:

```

{
  "location": "eastus",
  "properties": {
    "hardwareProfile": {
      "vmSize": "Standard_D1_v2"
    },
    "storageProfile": {
      "imageReference": {
        "sku": "2016-Datacenter",
        "publisher": "MicrosoftWindowsServer",
        "version": "latest",
        "offer": "WindowsServer"
      },
      "osDisk": {
        "caching": "ReadWrite",
        "managedDisk": {
          "storageAccountType": "Standard_LRS"
        },
        "name": "myVMosdisk",
        "createOption": "FromImage"
      }
    },
    "networkProfile": {
      "networkInterfaces": [
        {
          "id": "/subscriptions/{subscription-id}/resourceGroups/myResourceGroup/providers/Microsoft.Network/networkInterfaces/{nic-name}",
          "properties": {
            "primary": true
          }
        }
      ]
    },
    "osProfile": {
      "adminUsername": "{your-username}",
      "computerName": "myVM",
      "adminPassword": "{your-password}"
    }
  }
}

```

Plantilla de Resource Manager

Cree el equilibrador de carga y el grupo de back-end, y rellene el grupo de back-end con las direcciones de back-end:

```

{
  "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
  "contentVersion": "1.0.0.0",
  "parameters": {
    "loadBalancers_myLB_location": {
      "type": "SecureString"
    },
    "loadBalancers_myLB_location_1": {
      "type": "SecureString"
    },
    "backendAddressPools_myBackendPool_location": {
      "type": "SecureString"
    },
    "backendAddressPools_myBackendPool_location_1": {
      "type": "SecureString"
    },
    "loadBalancers_myLB_name": {
      "defaultValue": "myLB",
      "type": "String"
    },
  },

```

```

    "virtualNetworks_myVNET_externalid": {
      "defaultValue": "/subscriptions/6bb4a28a-db84-4e8a-b1dc-fabf7bd9f0b2/resourceGroups/ErRobin4/providers/Microsoft.Network/virtualNetworks/myVNET",
      "type": "String"
    }
  },
  "variables": {},
  "resources": [
    {
      "type": "Microsoft.Network/loadBalancers",
      "apiVersion": "2020-04-01",
      "name": "[parameters('loadBalancers_myLB_name')]",
      "location": "eastus",
      "sku": {
        "name": "Standard"
      },
      "properties": {
        "frontendIPConfigurations": [
          {
            "name": "LoadBalancerFrontEnd",
            "properties": {
              "privateIPAddress": "10.0.0.7",
              "privateIPAllocationMethod": "Dynamic",
              "subnet": {
                "id": "[concat(parameters('virtualNetworks_myVNET_externalid'),
'/subnets/Subnet-1')]"
              },
              "privateIPAddressVersion": "IPv4"
            }
          }
        ],
        "backendAddressPools": [
          {
            "name": "myBackendPool",
            "properties": {
              "loadBalancerBackendAddresses": [
                {
                  "name": "addr1",
                  "properties": {
                    "ipAddress": "10.0.0.4",
                    "virtualNetwork": {
                      "location": "[parameters('loadBalancers_myLB_location')]"
                    }
                  }
                },
                {
                  "name": "addr2",
                  "properties": {
                    "ipAddress": "10.0.0.5",
                    "virtualNetwork": {
                      "location": "[parameters('loadBalancers_myLB_location_1')]"
                    }
                  }
                }
              ]
            }
          }
        ],
        "loadBalancingRules": [],
        "probes": [],
        "inboundNatRules": [],
        "outboundRules": [],
        "inboundNatPools": []
      }
    },
    {
      "type": "Microsoft.Network/loadBalancers/backendAddressPools",
      "apiVersion": "2020-04-01",
      "name": "[concat(parameters('loadBalancers_myLB_name'), '/myBackendPool')]",

```

```

        "dependsOn": [
            "[resourceId('Microsoft.Network/loadBalancers', parameters('loadBalancers_myLB_name'))]"
        ],
        "properties": {
            "loadBalancerBackendAddresses": [
                {
                    "name": "addr1",
                    "properties": {
                        "ipAddress": "10.0.0.4",
                        "virtualNetwork": {
                            "location": "[parameters('backendAddressPools_myBackendPool_location')]"
                        }
                    }
                },
                {
                    "name": "addr2",
                    "properties": {
                        "ipAddress": "10.0.0.5",
                        "virtualNetwork": {
                            "location": "[parameters('backendAddressPools_myBackendPool_location_1')]"
                        }
                    }
                }
            ]
        }
    }
}

```

Cree una máquina virtual y una interfaz de red conectada. Establezca la dirección IP de la interfaz de red en una de las direcciones de back-end:

```

{
  "$schema": "http://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json",
  "contentVersion": "1.0.0.0",
  "parameters": {
    "storageAccountName": {
      "type": "String",
      "metadata": {
        "description": "Name of storage account"
      }
    },
    "storageAccountDomain": {
      "type": "String",
      "metadata": {
        "description": "The domain of the storage account to be created."
      }
    },
    "adminUsername": {
      "type": "String",
      "metadata": {
        "description": "Admin username"
      }
    },
    "adminPassword": {
      "type": "SecureString",
      "metadata": {
        "description": "Admin password"
      }
    },
    "vmName": {
      "defaultValue": "myVM",
      "type": "String",
      "metadata": {
        "description": "Prefix to use for VM names"
      }
    }
  }
}

```

```

},
"imagePublisher": {
  "type": "String",
  "metadata": {
    "description": "Image Publisher"
  }
},
"imageOffer": {
  "defaultValue": "WindowsServer",
  "type": "String",
  "metadata": {
    "description": "Image Offer"
  }
},
"imageSKU": {
  "defaultValue": "2012-R2-Datacenter",
  "type": "String",
  "metadata": {
    "description": "Image SKU"
  }
},
"lbName": {
  "defaultValue": "myLB",
  "type": "String",
  "metadata": {
    "description": "Load Balancer name"
  }
},
"nicName": {
  "defaultValue": "nic",
  "type": "String",
  "metadata": {
    "description": "Network Interface name prefix"
  }
},
"privateIpAddress": {
  "defaultValue": "10.0.0.5",
  "type": "String",
  "metadata": {
    "description": "Private IP Address of the VM"
  }
},
"vnetName": {
  "defaultValue": "myVNET",
  "type": "String",
  "metadata": {
    "description": "VNET name"
  }
},
"vmSize": {
  "defaultValue": "Standard_A1",
  "type": "String",
  "metadata": {
    "description": "Size of the VM"
  }
},
"storageLocation": {
  "type": "String",
  "metadata": {
    "description": "Location of the Storage Account."
  }
},
"location": {
  "type": "String",
  "metadata": {
    "description": "Location to deploy all the resources in."
  }
},

```

```

"variables": {
  "networkSecurityGroupName": "networkSecurityGroup1",
  "storageAccountType": "Standard_LRS",
  "subnetName": "Subnet-1",
  "publicIPAddressType": "Static",
  "vnetID": "[resourceId('Microsoft.Network/virtualNetworks',parameters('vnetName'))]",
  "subnetRef": "[concat(variables('vnetID'),'/subnets/',variables('subnetName'))]"
},
"resources": [
  {
    "type": "Microsoft.Storage/storageAccounts",
    "apiVersion": "2015-05-01-preview",
    "name": "[parameters('storageAccountName')]",
    "location": "[parameters('storageLocation')]",
    "properties": {
      "accountType": "[variables('storageAccountType')]"
    }
  },
  {
    "type": "Microsoft.Network/networkSecurityGroups",
    "apiVersion": "2016-03-30",
    "name": "[variables('networkSecurityGroupName')]",
    "location": "[parameters('location')]",
    "properties": {
      "securityRules": []
    }
  },
  {
    "type": "Microsoft.Network/networkInterfaces",
    "apiVersion": "2015-05-01-preview",
    "name": "[parameters('nicName')]",
    "location": "[parameters('location')]",
    "properties": {
      "ipConfigurations": [
        {
          "name": "ipconfig1",
          "properties": {
            "privateIPAllocationMethod": "Static",
            "privateIpAddress": "[parameters('privateIpAddress')]",
            "subnet": {
              "id": "[variables('subnetRef')]"
            }
          }
        }
      ]
    }
  },
  {
    "type": "Microsoft.Compute/virtualMachines",
    "apiVersion": "2015-05-01-preview",
    "name": "[parameters('vmName')]",
    "location": "[parameters('location')]",
    "dependsOn": [
      "[concat('Microsoft.Storage/storageAccounts/', parameters('storageAccountName'))]",
      "[parameters('nicName')]"
    ],
    "properties": {
      "hardwareProfile": {
        "vmSize": "[parameters('vmSize')]"
      },
      "osProfile": {
        "computername": "[parameters('vmName')]",
        "adminUsername": "[parameters('adminUsername')]",
        "adminPassword": "[parameters('adminPassword')]"
      },
      "storageProfile": {
        "imageReference": {
          "publisher": "[parameters('imagePublisher')]",
          "offer": "[parameters('imageOffer')]",

```

```

        "sku": "[parameters('imageSKU')]",
        "version": "latest"
    },
    "osDisk": {
        "name": "osdisk",
        "vhd": {
            "uri": "[concat('http://',parameters('storageAccountName'),'.blob.',parameters('storageAccountDomain'),'/vhds/', 'osdisk', '.vhd')]"
        },
        "caching": "ReadWrite",
        "createOption": "FromImage"
    }
},
"networkProfile": {
    "networkInterfaces": [
        {
            "id": "[resourceId('Microsoft.Network/networkInterfaces',parameters('nicName'))]"
        }
    ]
}
}
]
}

```

Pasos siguientes

En este artículo, ha conocido la administración de grupos de back-end de Azure Load Balancer y ha aprendido a configurar un grupo de back-end mediante una combinación de dirección IP y red virtual.

Más información sobre [Azure Load Balancer](#).

Azure Load Balancer con el conjunto de escalado de máquinas virtuales de Azure

23/09/2020 • 3 minutes to read • [Edit Online](#)

Al trabajar con conjuntos de escalado de máquinas virtuales y el equilibrador de carga, debe tener en cuenta las pautas siguientes:

Enrutamiento de puerto y reglas NAT de entrada:

- Después de crear el conjunto de escalado, no se puede modificar el puerto de back-end para una regla de equilibrio de carga que se usa en un sondeo de estado del equilibrador de carga. Para cambiar el puerto, puede quitar el sondeo de estado mediante la actualización del conjunto de escalado de máquinas virtuales de Azure, actualizar el puerto y, a continuación, volver a configurar el sondeo de estado.
- Al usar el conjunto de escalado de máquinas virtuales en el grupo de back-end del equilibrador de carga, las reglas NAT de entrada predeterminadas se crean automáticamente.

Grupo NAT de entrada:

- Cada conjunto de escalado de máquinas virtuales debe tener al menos un grupo NAT de entrada.
- El grupo NAT de entrada es una colección de reglas NAT de entrada. Un grupo NAT de entrada no puede admitir varios conjuntos de escalado de máquinas virtuales.
- Para eliminar un grupo de NAT de un conjunto de escalado de máquinas virtuales existente, primero debe quitar el grupo de NAT del conjunto de escalado. A continuación se muestra un ejemplo completo que usa la CLI:

```
az vmss update
  --resource-group MyResourceGroup
  --name MyVMSS
  --remove
virtualMachineProfile.networkProfile.networkInterfaceConfigurations[0].ipConfigurations[0].loadBalancerInboundNatPools
az vmss update-instances
  --instance-ids *
  --resource-group MyResourceGroup
  --name MyVMSS
az network lb inbound-nat-pool delete
  --resource-group MyResourceGroup
  --lb-name MyLoadBalancer
  --name MyNatPool
```

Reglas de equilibrio de carga:

- Al usar el conjunto de escalado de máquinas virtuales en el grupo de back-end del equilibrador de carga, la regla de equilibrio de carga predeterminada se crea automáticamente.

Reglas de salida:

- A fin de crear una regla de salida para un grupo de back-end al que ya se hace referencia mediante una regla de equilibrio de carga, primero debe marcar "**Crear reglas de salida implícitas**" como **No** en el portal cuando se crea la regla de equilibrio de carga de entrada.

Add load balancing rule

myLoadBalancer

Name *

myLoadBalancingRule ✓

IP Version *

☒ IPv4 ☐ IPv6

Frontend IP address * ⓘ

52.143.93.25 (LoadBalancerFrontEnd) ▼

Protocol

☒ TCP ☐ UDP

Port *

80

Backend port * ⓘ

80

Backend pool ⓘ

myBackendPool ▼

Health probe ⓘ

myHealthProbe (TCP:80) ▼

Session persistence ⓘ

None ▼

Idle timeout (minutes) ⓘ



4

TCP reset

☒ Disabled ☐ Enabled

Floating IP (direct server return) ⓘ

☒ Disabled ☐ Enabled

Create implicit outbound rules ⓘ

☐ Yes ☒ No

OK

Los siguientes métodos se pueden usar para implementar un conjunto de escalado de máquinas virtuales con una instancia existente de Azure Load Balancer.

- [Configuración de un conjunto de escalado de máquinas virtuales con una instancia existente de Azure Load Balancer mediante Azure Portal](#)
- [Configuración de un conjunto de escalado de máquinas virtuales con una instancia existente de Azure Load Balancer mediante Azure PowerShell.](#)
- [Configuración de un conjunto de escalado de máquinas virtuales con una instancia existente de Azure Load Balancer mediante la CLI de Azure.](#)

Configuración de un conjunto de escalado de máquinas virtuales con una instancia existente de Azure Load Balancer mediante Azure Portal

23/09/2020 • 4 minutes to read • [Edit Online](#)

En este artículo, aprenderá a configurar un conjunto de escalado de máquinas virtuales con una instancia existente de Azure Load Balancer.

Prerrequisitos

- Suscripción a Azure.
- Un equilibrador de carga de SKU estándar existente en la suscripción donde se implementará el conjunto de escalado de máquinas virtuales.
- Una instancia de Azure Virtual Network para el conjunto de escalado de máquinas virtuales.

Inicio de sesión en Azure Portal

Inicie sesión en Azure Portal en <https://portal.azure.com>.

Implementación de un conjunto de escalado de máquinas virtuales con un equilibrador de carga existente

En esta sección, creará un conjunto de escalado de máquinas virtuales en Azure Portal con un equilibrador de carga de Azure existente.

NOTE

En los pasos siguientes se supone que se ha implementado previamente una red virtual denominada **myVNet** y un equilibrador de carga de Azure denominado **myLoadBalancer**.

1. En la parte superior izquierda de la pantalla, haga clic en **Crear un recurso** > **Proceso** > **Conjunto de escalado de máquinas virtuales** o busque **Conjunto de escalado de máquinas virtuales** en la búsqueda de Marketplace.
2. Seleccione **Crear**.
3. En **Creación de un conjunto de escalado de máquinas virtuales**, escriba o seleccione esta información en la pestaña **Conceptos básicos**:

CONFIGURACIÓN	VALUE
Detalles del proyecto	
Subscription	Selección de su suscripción a Azure
Grupo de recursos	Seleccione Crear nuevo , escriba myResourceGroup , seleccione Aceptar o seleccione un grupo de recursos existente.

CONFIGURACIÓN	VALUE
Detalles del conjunto de escalado	
Nombre del conjunto de escalado de máquinas virtuales	Escriba myVMSS .
Region	Seleccione Este de EE. UU. 2 .
Zona de disponibilidad	Seleccione Ninguno .
Detalles de instancia	
Imagen	Seleccione Ubuntu Server 18.04 LTS .
Instancia de Azure Spot	Seleccione No .
Size	Deje el valor predeterminado.
Cuenta de administrador	
Tipo de autenticación	Seleccione Contraseña .
Nombre de usuario	Escriba el nombre de usuario de administrador.
Contraseña	Escriba la contraseña del administrador.
Confirmar contraseña	Escriba de nuevo la contraseña del administrador.

Create a virtual machine scale set

×

Basics

Disks

Networking

Scaling

Management

Health

Advanced

Tags

Review + create

Azure virtual machine scale sets let you create and manage a group of load balanced VMs. The number of VM instances can automatically increase or decrease in response to demand or a defined schedule. Scale sets provide high availability to your applications, and allow you to centrally manage, configure, and update a large number of VMs.

[Learn more about virtual machine scale sets](#)

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *

Contoso Subscription

▼

Resource group *

myResourceGroup

▼

[Create new](#)

Scale set details

Virtual machine scale set name *

myVMSS

✓

Region *

(US) East US

▼

Availability zone ⓘ

None

▼

Instance details

Image * ⓘ

Ubuntu Server 18.04 LTS

▼

[Browse all public and private images](#)

Azure Spot instance ⓘ

☐ Yes
 ☒ No

Size * ⓘ

Standard D2s v3

2 vcpus, 8 GiB memory

[Change size](#)

Administrator account

Authentication type ⓘ

☒ Password
 ☐ SSH public key

Username * ⓘ

youradminuser

✓

Password * ⓘ

👁

Confirm password * ⓘ

👁

Review + create

< Previous

Next : Disks >

4. Seleccione la pestaña **Redes**.

5. Escriba o seleccione esta información en la pestaña **Redes**:

CONFIGURACIÓN	VALUE
Configuración de redes virtuales	
Virtual network	Seleccione myVNet o la red virtual existente.

CONFIGURACIÓN	VALUE
Equilibrio de carga	
Usar un equilibrador de carga	Seleccione Sí .
Configuración de equilibrio de carga	
Opciones de equilibrio de carga	Seleccione el equilibrador de carga de Azure .
Seleccionar un equilibrador de carga	Seleccione myLoadBalancer o el equilibrador de carga existente.
Seleccionar un grupo de back-end	Seleccione myBackendPool o el grupo de back-end existente.

Create a virtual machine scale set

×

Basics

Disks

Networking

Scaling

Management

Health

Advanced

Tags

Review + create

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution. [Learn more about VMSS networking](#)

Virtual network configuration

Azure Virtual Network (VNet) enables many types of Azure resources to securely communicate with each other, the internet, and on-premises networks. [Learn more about VNets](#)

Virtual network *

myVNet

Create virtual network

Manage selected virtual network

Network interface

A network interface enables an Azure virtual machine to communicate with internet, Azure, and on-premises resources. A VM can have one or more network interfaces.

+ Create new nic

🗑 Delete

<input type="checkbox"/>	NAME	CREATE PUBLI...	SUBNET	NETWORK SECU...	ACCELERATED N...
<input type="checkbox"/>	myVNet-nic01	No	mySubnet (10.0.0.0/24)	Basic	Off

Load balancing

You can place this virtual machine scale set in the backend pool of an existing Azure load balancing solution. [Learn more](#)

Use a load balancer

☒ Yes
 ☐ No

Load balancing settings

- Application Gateway** is an HTTP/HTTPS web traffic load balancer with URL-based routing, SSL termination, session persistence, and web application firewall. [Learn more about Application Gateway](#)
- Azure Load Balancer** supports all TCP/UDP network traffic, port-forwarding, and outbound flows. [Learn more about Azure Load Balancer](#)

Load balancing options *

Azure load balancer

Select a load balancer *

myLoadBalancer

Create new

Select a backend pool *

myBackendPool

Create new

Review + create

< Previous

Next : Scaling >

- Seleccione la pestaña **Administración**.
- En la pestaña **Administración**, establezca **Diagnósticos de arranque** en **Desactivado**.
- Seleccione el botón azul **Revisar y Crear**.
- Revise la configuración y seleccione el botón **Crear**.

Pasos siguientes

En este artículo, implementó un conjunto de escalado de máquinas virtuales con una instancia existente de Azure Load Balancer. Para obtener más información sobre los conjuntos de escalado de máquinas virtuales y el

equilibrador de carga, consulte:

- [¿Qué es Azure Load Balancer?](#)
- [¿Qué son los conjuntos de escalado de máquinas virtuales?](#)

Configuración de un conjunto de escalado de máquinas virtuales con una instancia existente de Azure Load Balancer mediante Azure PowerShell

23/09/2020 • 5 minutes to read • [Edit Online](#)

En este artículo, aprenderá a configurar un conjunto de escalado de máquinas virtuales con una instancia existente de Azure Load Balancer.




Prerrequisitos

- Suscripción a Azure.
- Un equilibrador de carga de SKU estándar existente en la suscripción donde se implementará el conjunto de escalado de máquinas virtuales.
- Una instancia de Azure Virtual Network para el conjunto de escalado de máquinas virtuales.

Uso de Azure Cloud Shell

En Azure se hospeda Azure Cloud Shell, un entorno de shell interactivo que puede utilizar mediante el explorador. Puede usar Bash o PowerShell con Cloud Shell para trabajar con los servicios de Azure. Puede usar los comandos preinstalados de Cloud Shell para ejecutar el código de este artículo sin tener que instalar nada en su entorno local.

Para iniciar Azure Cloud Shell:

OPCIÓN	EJEMPLO O VÍNCULO
Seleccione Pruébelo en la esquina superior derecha de un bloque de código. Solo con seleccionar Pruébelo no se copia automáticamente el código en Cloud Shell.	
Vaya a https://shell.azure.com o seleccione el botón Iniciar Cloud Shell para abrir Cloud Shell en el explorador.	
Seleccione el botón Cloud Shell en la barra de menús de la esquina superior derecha de Azure Portal .	

Para ejecutar el código de este artículo en Azure Cloud Shell:

1. Inicie Cloud Shell.
2. Seleccione el botón **Copiar** de un bloque de código para copiar el código.
3. Pegue el código en la sesión de Cloud Shell. Para ello, seleccione **Ctrl+Mayús+V** en Windows y Linux, o bien seleccione **Cmd+Mayús+V** en macOS.
4. Seleccione **Entrar** para ejecutar el código.

NOTE

Este artículo se ha actualizado para usar el nuevo módulo Az de Azure PowerShell. Aún puede usar el módulo de AzureRM que continuará recibiendo correcciones de errores hasta diciembre de 2020 como mínimo. Para más información acerca del nuevo módulo Az y la compatibilidad con AzureRM, consulte [Introducing the new Azure PowerShell Az module](#) (Presentación del nuevo módulo Az de Azure PowerShell). Para obtener instrucciones sobre la instalación del módulo Az, consulte [Instalación de Azure PowerShell](#).

Inicio de sesión en la CLI de Azure

Inicie sesión en Azure.

```
Connect-AzAccount
```

Implementación de un conjunto de escalado de máquinas virtuales con un equilibrador de carga existente

Reemplace los valores entre corchetes por los nombres de los recursos en la configuración.

```
$rsg = <resource-group>
$loc = <location>
$vms = <vm-scale-set-name>
$vnt = <virtual-network>
$sub = <subnet-name>
$lbn = <load-balancer-name>
$pol = <upgrade-policy-mode>

$lb = Get-AzLoadBalancer -ResourceGroupName $rsg -Name $lbn

New-AzVmss -ResourceGroupName $rsg -Location $loc -VMScaleSetName $vms -VirtualNetworkName $vnt -SubnetName $sub -LoadBalancerName $lb -UpgradePolicyMode $pol
```

En el ejemplo siguiente se implementa un conjunto de escalado de máquinas virtuales con:

- Un conjunto de escalado de máquinas virtuales denominado **myVMSS**
- Una instancia de Azure Load Balancer denominada **myLoadBalancer**
- Un grupo de back-end de equilibradores de carga denominado **myBackendPool**
- Una instancia de Azure Virtual Network denominada **myVnet**
- Una subred denominada **mySubnet**
- Un grupo de recursos denominado **myResourceGroup**

```
$rsg = "myResourceGroup"
$loc = "East US 2"
$vms = "myVMSS"
$vnt = "myVnet"
$sub = "mySubnet"
$pol = "Automatic"
$lbn = "myLoadBalancer"

$lb = Get-AzLoadBalancer -ResourceGroupName $rsg -Name $lbn

New-AzVmss -ResourceGroupName $rsg -Location $loc -VMSSetName $vms -VirtualNetworkName $vnt -SubnetName $sub -LoadBalancerName $lb -UpgradePolicyMode $pol
```

NOTE

Después de crear el conjunto de escalado, no se puede modificar el puerto de back-end para una regla de equilibrio de carga que se usa en un sondeo de estado del equilibrador de carga. Para cambiar el puerto, puede quitar el sondeo de estado mediante la actualización del conjunto de escalado de máquinas virtuales de Azure, actualizar el puerto y, a continuación, volver a configurar el sondeo de estado.

Pasos siguientes

En este artículo, implementó un conjunto de escalado de máquinas virtuales con una instancia existente de Azure Load Balancer. Para obtener más información sobre los conjuntos de escalado de máquinas virtuales y el equilibrador de carga, consulte:

- [¿Qué es Azure Load Balancer?](#)
- [¿Qué son los conjuntos de escalado de máquinas virtuales?](#)

Configuración de un conjunto de escalado de máquinas virtuales con una instancia existente de Azure Load Balancer mediante la CLI de Azure

23/09/2020 • 5 minutes to read • [Edit Online](#)

En este artículo, aprenderá a configurar un conjunto de escalado de máquinas virtuales con una instancia existente de Azure Load Balancer.




Prerrequisitos

- Suscripción a Azure.
- Un equilibrador de carga de SKU estándar existente en la suscripción donde se implementará el conjunto de escalado de máquinas virtuales.
- Una instancia de Azure Virtual Network para el conjunto de escalado de máquinas virtuales.

Uso de Azure Cloud Shell

En Azure se hospeda Azure Cloud Shell, un entorno de shell interactivo que puede utilizar mediante el explorador. Puede usar Bash o PowerShell con Cloud Shell para trabajar con los servicios de Azure. Puede usar los comandos preinstalados de Cloud Shell para ejecutar el código de este artículo sin tener que instalar nada en su entorno local.

Para iniciar Azure Cloud Shell:

OPCIÓN	EJEMPLO O VÍNCULO
Seleccione Pruébelo en la esquina superior derecha de un bloque de código. Solo con seleccionar Pruébelo no se copia automáticamente el código en Cloud Shell.	
Vaya a https://shell.azure.com o seleccione el botón Iniciar Cloud Shell para abrir Cloud Shell en el explorador.	
Seleccione el botón Cloud Shell en la barra de menús de la esquina superior derecha de Azure Portal .	

Para ejecutar el código de este artículo en Azure Cloud Shell:

1. Inicie Cloud Shell.
2. Seleccione el botón **Copiar** de un bloque de código para copiar el código.
3. Pegue el código en la sesión de Cloud Shell. Para ello, seleccione **Ctrl+Mayús+V** en Windows y Linux, o bien seleccione **Cmd+Mayús+V** en macOS.
4. Seleccione **Entrar** para ejecutar el código.

Si decide usar la CLI localmente, para este artículo es preciso que tenga instalada la versión 2.0.28 o posterior de la CLI de Azure. Para encontrar la versión, ejecute `az --version`. Si necesita instalarla o actualizarla, consulte [Instalación de la CLI de Azure 2.0](#).

Inicio de sesión en la CLI de Azure

Inicie sesión en Azure.

```
az login
```

Implementación de un conjunto de escalado de máquinas virtuales con un equilibrador de carga existente

Reemplace los valores entre corchetes por los nombres de los recursos en la configuración.

```
az vmss create \
  --resource-group <resource-group> \
  --name <vmss-name> \
  --image <your-image> \
  --admin-username <admin-username> \
  --generate-ssh-keys \
  --upgrade-policy-mode Automatic \
  --instance-count 3 \
  --vnet-name <virtual-network-name> \
  --subnet <subnet-name> \
  --lb <load-balancer-name> \
  --backend-pool-name <backend-pool-name>
```

En el ejemplo siguiente se implementa un conjunto de escalado de máquinas virtuales con:

- Un conjunto de escalado de máquinas virtuales denominado **myVMSS**
- Una instancia de Azure Load Balancer denominada **myLoadBalancer**
- Un grupo de back-end de equilibradores de carga denominado **myBackendPool**
- Una instancia de Azure Virtual Network denominada **myVnet**
- Una subred denominada **mySubnet**
- Un grupo de recursos denominado **myResourceGroup**
- Imagen del servidor Ubuntu para el conjunto de escalado de máquinas virtuales

```
az vmss create \
  --resource-group myResourceGroup \
  --name myVMSS \
  --image Canonical:UbuntuServer:18.04-LTS:latest \
  --admin-username adminuser \
  --generate-ssh-keys \
  --upgrade-policy-mode Automatic \
  --instance-count 3 \
  --vnet-name myVnet \
  --subnet mySubnet \
  --lb myLoadBalancer \
  --backend-pool-name myBackendPool
```

NOTE

Después de crear el conjunto de escalado, no se puede modificar el puerto de back-end para una regla de equilibrio de carga que se usa en un sondeo de estado del equilibrador de carga. Para cambiar el puerto, puede quitar el sondeo de estado mediante la actualización del conjunto de escalado de máquinas virtuales de Azure, actualizar el puerto y, a continuación, volver a configurar el sondeo de estado.

Pasos siguientes

En este artículo, implementó un conjunto de escalado de máquinas virtuales con una instancia existente de Azure Load Balancer. Para obtener más información sobre los conjuntos de escalado de máquinas virtuales y el equilibrador de carga, consulte:

- [¿Qué es Azure Load Balancer?](#)
- [¿Qué son los conjuntos de escalado de máquinas virtuales?](#)

Actualización de Azure Load Balancer público

23/09/2020 • 11 minutes to read • [Edit Online](#)

[Azure Standard Load Balancer](#) ofrece un amplio conjunto de funcionalidades y alta disponibilidad gracias a la redundancia de zona. Para más información acerca de la SKU de Load Balancer, consulte la [tabla de comparación](#).

Hay tres fases en una actualización:

1. Migración de la configuración
2. Incorporación de máquinas virtuales a los grupos de back-end de Standard Load Balancer

Este artículo trata sobre la migración de la configuración. La incorporación de máquinas virtuales a los grupos de back-end puede variar en función de su entorno específico, pero [se proporcionan](#) algunas recomendaciones generales de alto nivel.

Información general sobre la actualización

Existe un script de Azure PowerShell que hace lo siguiente:

- Crea una instancia de Load Balancer con una SKU estándar en el grupo de recursos y la ubicación que especifique.
- Copia perfectamente las configuraciones de Load Balancer de SKU básica en la instancia de Standard Load Balancer recién creada.
- Crea una regla de salida predeterminada que permite la conectividad saliente.

Advertencias y limitaciones

- El script solo admite la actualización de Public Load Balancer. En el caso de la actualización interna de la instancia básica de Load Balancer, puede encontrar instrucciones en [esta página](#).
- Standard Load Balancer tiene una nueva dirección pública. No es posible trasladar las direcciones IP asociadas a las instancias de Basic Load Balancer existentes sin problemas a las instancias de Standard Load Balancer, ya que tienen diferentes SKU.
- Si se crea la instancia de Standard Load Balancer en una región diferente, no podrá asociar las máquinas virtuales existentes de la región antigua a la instancia de Standard Load Balancer recién creada. Para solucionar esta limitación, asegúrese de crear una nueva máquina virtual en la nueva región.
- Si Load Balancer no tiene ninguna configuración de IP de front-end ni grupo de back-end, es probable que se produzca un error al ejecutar el script. Asegúrese de que no están vacíos

Descarga del script

Descargue el script de migración de la [Galería de PowerShell](#).

Uso del script

Dispone de dos opciones en función de sus preferencias y de la configuración del entorno de PowerShell local:

- Si no tiene instalados los módulos de Azure Az, o si no le importa desinstalarlos, la mejor alternativa es usar la opción `Install-Script` para ejecutar el script.
- Si necesita conservar los módulos de Azure Az, lo mejor es que descargue el script y lo ejecute directamente.

Para determinar si tiene instalados los módulos de Azure Az, ejecute `Get-InstalledModule -Name az`. Si no ve ningún módulo de Az instalado, puede usar el método `Install-Script`.

Instalación con el método Install-Script

Para usar esta opción, los módulos de Azure Az no deben estar instalados en el equipo. En caso de que lo estén, el comando siguiente mostrará un error. Puede desinstalar los módulos de Azure Az o usar la otra opción para descargar manualmente el script y ejecutarlo.

Ejecute el script con el siguiente comando:

```
Install-Script -Name AzurePublicLBUpgrade
```

Este comando también instala los módulos de Az necesarios.

Instalación directamente con el script

Si tiene instalados algunos módulos de Azure Az y no puede desinstalarlos (o no le interesa hacerlo), puede descargar manualmente el script mediante la pestaña **Descarga manual** en el vínculo de descarga del script. El script se descarga como un archivo nupkg sin procesar. Para instalar el script desde este archivo nupkg, consulte [Descarga manual del paquete](#).

Para ejecutar el script:

1. Use `Connect-AzAccount` para conectarse a Azure.
2. Use `Import-Module Az` para importar los módulos de Az.
3. Examine los parámetros obligatorios:
 - **oldRgName: [String]: Required:** es el grupo de recursos de la instancia existente de Basic Load Balancer que desea actualizar. Para encontrar este valor de cadena, vaya a Azure Portal, seleccione el origen Basic Load Balancer y haga clic en la sección **Información general** del equilibrador de carga. El grupo de recursos se encuentra en esa página.
 - **oldLBName: [String]: Required:** es el nombre de la instancia de Basic Load Balancer que desea actualizar.
 - **newrgName: [String]: Required:** es el grupo de recursos en el que se creará la instancia de Standard Load Balancer. Puede tratarse de un nuevo grupo de recursos o de uno ya existente. Si elige un grupo de recursos existente, tenga en cuenta que el nombre de la instancia de Load Balancer debe ser único dentro del grupo de recursos.
 - **newlocation: [String]: Required:** es la ubicación en la que se creará la instancia de Standard Load Balancer. Se recomienda heredar la misma ubicación de la instancia elegida de Basic Load Balancer para la instancia de Standard Load Balancer para una mejor asociación con otros recursos existentes.
 - **newLBName: [String]: Required:** es el nombre de la instancia de Standard Load Balancer que se va a crear.
4. Ejecute el script con los parámetros adecuados. Podría tardar entre cinco y siete minutos en finalizar.

Ejemplo

```
AzurePublicLBUpgrade.ps1 -oldRgName "test_publicUpgrade_rg" -oldLBName "LBForPublic" -newrgName  
"test_userInput3_rg" -newlocation "centralus" -newLbName "LBForUpgrade"
```

Incorporación de máquinas virtuales a los grupos de back-end de Standard Load Balancer

En primer lugar, asegúrese de que el script ha creado correctamente una instancia de Standard Public Load Balancer con la configuración exacta migrada a partir de la instancia de Basic Public Load Balancer. Puede comprobarlo desde Azure Portal.

Asegúrese de que envía una pequeña cantidad de tráfico mediante Standard Load Balancer como una prueba manual.

Estos son algunos escenarios en los que puede agregar máquinas virtuales a los grupos de back-end de la

instancia de Standard Public Load Balancer recién creada y cómo se pueden configurar y nuestras recomendaciones para cada uno de ellos:

- **Traslado de las máquinas virtuales existentes desde los grupos de back-end de las instancias antiguas de Basic Public Load Balancer a los grupos de back-end de la instancia de Standard Public Load Balancer recién creada.**
 1. Para realizar las tareas de esta guía de inicio rápido, inicie sesión en [Azure Portal](#).
 2. Seleccione **Todos los recursos** en el menú de la izquierda y, a continuación, seleccione la **instancia recién creada de Standard Load Balancer** de la lista de recursos.
 3. En **Configuración**, seleccione **Grupos de back-end**.
 4. Seleccione el grupo de back-end que coincida con el grupo de back-end de Basic Load Balancer y seleccione el valor siguiente:
 - **Máquina virtual:** Despliegue y seleccione las máquinas virtuales del grupo de back-end coincidente de la instancia de Basic Load Balancer.
 1. Seleccione **Guardar**.

NOTE

En el caso de las máquinas virtuales que tienen direcciones IP públicas, deberá crear direcciones IP estándar primero en aquellos casos en los que no se garantice la misma dirección IP. Desasocie las máquinas virtuales de las direcciones IP básicas y asíócielas con las direcciones IP estándar recién creadas. A continuación, podrá seguir las instrucciones para agregar máquinas virtuales al grupo de back-end de Standard Load Balancer.

- **Creación de nuevas máquinas virtuales para agregarlas a los grupos de back-end de la instancia de Standard Public Load Balancer recién creada.**
 - [Aquí](#) encontrará más instrucciones sobre cómo crear una máquina virtual y cómo asociarla con Standard Load Balancer.

Creación de una regla de salida para la conexión de salida

Siga las [instrucciones](#) para crear una regla de salida para poder:

- Definir la NAT de salida desde cero.
- Escalar y ajustar el comportamiento de la NAT de salida existente.

Preguntas frecuentes

¿Hay alguna limitación en el script de Azure PowerShell para migrar la configuración de v1 a v2?

Sí. Consulte [Advertencias y limitaciones](#).

¿Puede el script de Azure PowerShell cambiar el tráfico de la instancia de Basic Load Balancer a la instancia de Standard Load Balancer recién creada?

No. El script de Azure PowerShell solo migra la configuración. Usted es el responsable de realizar y controlar la migración real del tráfico.

Se han producido algunos problemas al usar este script. ¿Cómo puedo obtener ayuda?

Puede enviar un correo electrónico a slbupgradesupport@microsoft.com, abrir una incidencia con el Soporte técnico de Azure o hacer ambas cosas.

Pasos siguientes

[Más información sobre Load Balancer estándar](#)

Actualización de Azure Load Balancer interno sin necesidad de conexión de salida

23/09/2020 • 9 minutes to read • [Edit Online](#)

[Azure Standard Load Balancer](#) ofrece un amplio conjunto de funcionalidades y alta disponibilidad gracias a la redundancia de zona. Para más información acerca de la SKU de Load Balancer, consulte la [tabla de comparación](#).

En este artículo se presenta un script de PowerShell que crea una instancia de Standard Load Balancer con la misma configuración que la instancia básica de Load Balancer junto con la migración del tráfico desde la instancia básica hasta la estándar.

Información general sobre la actualización

Existe un script de Azure PowerShell que hace lo siguiente:

- Crea una instancia de Load Balancer interno de SKU estándar en la ubicación que se especifique. Tenga en cuenta que la instancia de Standard Load Balancer interno no proporciona ninguna [conexión de salida](#).
- Copia perfectamente las configuraciones de Load Balancer de la SKU básica en la instancia de Standard Load Balancer recién creada.
- Mueve sin problemas las direcciones IP privadas de la instancia básica de Load Balancer a la instancia de Standard Load Balancer recién creada.
- Mueve sin problemas las máquinas virtuales del grupo de back-end de la instancia básica de Load Balancer al grupo de back-end de Standard Load Balancer.

Advertencias y limitaciones

- El script solo admite la actualización de Load Balancer interno si no se requiere ninguna conexión de salida. Si necesita [conexión de salida](#) para alguna de las máquinas virtuales, vea esta [página](#) para obtener instrucciones.
- La instancia de Load Balancer básica debe estar en el mismo grupo de recursos que las NIC y VM de back-end.
- Si se crea la instancia de Standard Load Balancer en una región diferente, no podrá asociar las máquinas virtuales existentes de la región antigua a la instancia de Standard Load Balancer recién creada. Para solucionar esta limitación, asegúrese de crear una nueva máquina virtual en la nueva región.
- Si Load Balancer no tiene ninguna configuración de IP de front-end ni grupo de back-end, es probable que se produzca un error al ejecutar el script. Asegúrese de que no están vacíos.

Cambio del método de asignación de IP a Estática para la configuración de IP de front-end (ignore este paso si ya es estática)

1. Seleccione **Todos los servicios** en el menú de la izquierda, **Todos los recursos** y, después, en la lista de recursos, su instancia básica de Load Balancer.
2. En **Configuración**, seleccione **Configuración de IP de front-end** y seleccione la primera configuración de IP de front-end.
3. Para **Asignación**, seleccione **Estática**.
4. Repita el paso 3 para todas las configuraciones de IP de front-end de la instancia básica de Load Balancer.

Descarga del script

Descargue el script de migración de la [Galería de PowerShell](#).

Uso del script

Dispone de dos opciones en función de sus preferencias y de la configuración del entorno de PowerShell local:

- Si no tiene instalados los módulos de Azure Az, o si no le importa desinstalarlos, la mejor alternativa es usar la opción `Install-Script` para ejecutar el script.
- Si necesita conservar los módulos de Azure Az, lo mejor es que descargue el script y lo ejecute directamente.

Para determinar si tiene instalados los módulos de Azure Az, ejecute `Get-InstalledModule -Name az`. Si no ve ningún módulo de Az instalado, puede usar el método `Install-Script`.

Instalación con el método Install-Script

Para usar esta opción, los módulos de Azure Az no deben estar instalados en el equipo. En caso de que lo estén, el comando siguiente mostrará un error. Puede desinstalar los módulos de Azure Az o usar la otra opción para descargar manualmente el script y ejecutarlo.

Ejecute el script con el siguiente comando:

```
Install-Script -Name AzureILBUpgrade
```

Este comando también instala los módulos de Az necesarios.

Instalación directamente con el script

Si tiene instalados algunos módulos de Azure Az y no puede desinstalarlos (o no le interesa hacerlo), puede descargar manualmente el script mediante la pestaña **Descarga manual** en el vínculo de descarga del script. El script se descarga como un archivo nupkg sin procesar. Para instalar el script desde este archivo nupkg, consulte [Descarga manual del paquete](#).

Para ejecutar el script:

1. Use `Connect-AzAccount` para conectarse a Azure.
2. Use `Import-Module Az` para importar los módulos de Az.
3. Examine los parámetros obligatorios:
 - **rgName: [String]: Required:** es el grupo de recursos de la instancia existente de Basic Load Balancer y la nueva instancia de Standard Load Balancer. Para encontrar este valor de cadena, vaya a Azure Portal, seleccione el origen Basic Load Balancer y haga clic en la sección **Información general** del equilibrador de carga. El grupo de recursos se encuentra en esa página.
 - **oldLBName: [String]: Required:** es el nombre de la instancia de Basic Load Balancer que desea actualizar.
 - **newlocation: [String]: Required:** es la ubicación en la que se creará la instancia de Standard Load Balancer. Se recomienda heredar la misma ubicación de la instancia elegida de Basic Load Balancer para la instancia de Standard Load Balancer para una mejor asociación con otros recursos existentes.
 - **newLBName: [String]: Required:** es el nombre de la instancia de Standard Load Balancer que se va a crear.
4. Ejecute el script con los parámetros adecuados. Podría tardar entre cinco y siete minutos en finalizar.

Ejemplo

```
AzureILBUpgrade.ps1 -rgName "test_InternalUpgrade_rg" -oldLBName "LBForInternal" -newlocation  
"centralus" -newLbName "LBForUpgrade"
```

Preguntas frecuentes

¿Hay alguna limitación en el script de Azure PowerShell para migrar la configuración de v1 a v2?

Sí. Consulte [Advertencias y limitaciones](#).

¿Puede el script de Azure PowerShell cambiar el tráfico de la instancia de Basic Load Balancer a la instancia de Standard Load Balancer recién creada?

Sí, lo migra. Si quiere migrar el tráfico de forma personal, use [este script](#) que no mueve las máquinas virtuales automáticamente.

Se han producido algunos problemas al usar este script. ¿Cómo puedo obtener ayuda?

Puede enviar un correo electrónico a slbupgradesupport@microsoft.com, abrir una incidencia con el Soporte técnico de Azure o hacer ambas cosas.

Pasos siguientes

[Más información sobre Load Balancer estándar](#)

Actualización de Azure Load Balancer interno con necesidad de conexión de salida

23/09/2020 • 12 minutes to read • [Edit Online](#)

[Azure Standard Load Balancer](#) ofrece un amplio conjunto de funcionalidades y alta disponibilidad gracias a la redundancia de zona. Para más información acerca de la SKU de Load Balancer, consulte la [tabla de comparación](#). Dado que Standard Load Balancer interno no proporciona conexión de salida, se ofrece una solución para crear una instancia de Standard Public Load Balancer en su lugar.

Hay cuatro fases en una actualización:

1. Migrar la configuración a Standard Public Load Balancer
2. Agregar máquinas virtuales a los grupos de back-end de Standard Public Load Balancer
3. Configurar reglas de NSG para la subred o las máquinas virtuales que deben evitar Internet

Este artículo trata sobre la migración de la configuración. La incorporación de máquinas virtuales a los grupos de back-end puede variar en función de su entorno específico, pero [se proporcionan](#) algunas recomendaciones generales de alto nivel.

Información general sobre la actualización

Existe un script de Azure PowerShell que hace lo siguiente:

- Crea una instancia de Public Load Balancer de SKU estándar en el grupo de recursos y la ubicación que se especifique.
- Copia perfectamente las configuraciones de la instancia de Load Balancer interno de SKU básica en la instancia de Standard Public Load Balancer recién creada.
- Crea una regla de salida que permite la conectividad de salida.

Advertencias y limitaciones

- El script admite la actualización de Load Balancer interno si se requiere conexión de salida. Si no es necesaria una conexión de salida para ninguna de las máquinas virtuales, vea [esta página](#) para obtener un procedimiento recomendado.
- Standard Load Balancer tiene una nueva dirección pública. No es posible trasladar sin problemas las direcciones IP asociadas a la instancia existente de Basic Load Balancer interno a Standard Public Load Balancer, ya que tienen diferentes SKU.
- Si se crea la instancia de Standard Load Balancer en una región diferente, no podrá asociar las máquinas virtuales existentes de la región antigua a la instancia de Standard Load Balancer recién creada. Para solucionar esta limitación, asegúrese de crear una nueva máquina virtual en la nueva región.
- Si Load Balancer no tiene ninguna configuración de IP de front-end ni grupo de back-end, es probable que se produzca un error al ejecutar el script. Asegúrese de que no están vacíos.

Descarga del script

Descargue el script de migración de la [Galería de PowerShell](#).

Uso del script

Dispone de dos opciones en función de sus preferencias y de la configuración del entorno de PowerShell local:

- Si no tiene instalados los módulos de Azure Az, o si no le importa desinstalarlos, la mejor alternativa es usar la opción `Install-Script` para ejecutar el script.
- Si necesita conservar los módulos de Azure Az, lo mejor es que descargue el script y lo ejecute directamente.

Para determinar si tiene instalados los módulos de Azure Az, ejecute `Get-InstalledModule -Name az`. Si no ve ningún módulo de Az instalado, puede usar el método `Install-Script`.

Instalación con el método Install-Script

Para usar esta opción, los módulos de Azure Az no deben estar instalados en el equipo. En caso de que lo estén, el comando siguiente mostrará un error. Puede desinstalar los módulos de Azure Az o usar la otra opción para descargar manualmente el script y ejecutarlo.

Ejecute el script con el siguiente comando:

```
Install-Script -Name AzurePublicLBUpgrade
```

Este comando también instala los módulos de Az necesarios.

Instalación directamente con el script

Si tiene instalados algunos módulos de Azure Az y no puede desinstalarlos (o no le interesa hacerlo), puede descargar manualmente el script mediante la pestaña **Descarga manual** en el vínculo de descarga del script. El script se descarga como un archivo nupkg sin procesar. Para instalar el script desde este archivo nupkg, consulte [Descarga manual del paquete](#).

Para ejecutar el script:

1. Use `Connect-AzAccount` para conectarse a Azure.
2. Use `Import-Module Az` para importar los módulos de Az.
3. Examine los parámetros obligatorios:
 - **oldRgName: [String]: Required:** es el grupo de recursos de la instancia existente de Basic Load Balancer que desea actualizar. Para encontrar este valor de cadena, vaya a Azure Portal, seleccione el origen Basic Load Balancer y haga clic en la sección **Información general** del equilibrador de carga. El grupo de recursos se encuentra en esa página.
 - **oldLBName: [String]: Required:** es el nombre de la instancia de Basic Load Balancer que desea actualizar.
 - **newrgName: [String]: Required:** es el grupo de recursos en el que se creará la instancia de Standard Load Balancer. Puede tratarse de un nuevo grupo de recursos o de uno ya existente. Si elige un grupo de recursos existente, tenga en cuenta que el nombre de la instancia de Load Balancer debe ser único dentro del grupo de recursos.
 - **newlocation: [String]: Required:** es la ubicación en la que se creará la instancia de Standard Load Balancer. Se recomienda heredar la misma ubicación de la instancia elegida de Basic Load Balancer para una mejor asociación con otros recursos existentes.
 - **newLBName: [String]: Required:** es el nombre de la instancia de Standard Load Balancer que se va a crear.
4. Ejecute el script con los parámetros adecuados. Podría tardar entre cinco y siete minutos en finalizar.

Ejemplo

```
AzurePublicLBUpgrade.ps1 -oldRgName "test_publicUpgrade_rg" -oldLBName "LBForPublic" -newrgName "test_userInput3_rg" -newlocation "centralus" -newLbName "LBForUpgrade"
```

Incorporación de máquinas virtuales a los grupos de back-end de Standard Load Balancer

En primer lugar, asegúrese de que el script ha creado correctamente una instancia de Standard Public Load Balancer con la configuración exacta migrada a partir de la instancia de Basic Public Load Balancer. Puede comprobarlo desde Azure Portal.

Asegúrese de que envía una pequeña cantidad de tráfico mediante Standard Load Balancer como una prueba manual.

Estos son algunos escenarios en los que puede agregar máquinas virtuales a los grupos de back-end de la instancia de Standard Public Load Balancer recién creada y cómo se pueden configurar y nuestras recomendaciones para cada uno de ellos:

- **Traslado de las máquinas virtuales existentes desde los grupos de back-end de las instancias antiguas de Basic Public Load Balancer a los grupos de back-end de la instancia de Standard Public Load Balancer recién creada.**

1. Para realizar las tareas de esta guía de inicio rápido, inicie sesión en [Azure Portal](#).
2. Seleccione **Todos los recursos** en el menú de la izquierda y, a continuación, seleccione la **instancia recién creada de Standard Load Balancer** de la lista de recursos.
3. En **Configuración**, seleccione **Grupos de back-end**.
4. Seleccione el grupo de back-end que coincida con el grupo de back-end de Basic Load Balancer y seleccione el valor siguiente:
 - **Máquina virtual:** Despliegue y seleccione las máquinas virtuales del grupo de back-end coincidente de la instancia de Basic Load Balancer.
1. Seleccione **Guardar**.

NOTE

En el caso de las máquinas virtuales que tienen direcciones IP públicas, deberá crear direcciones IP estándar primero en aquellos casos en los que no se garantice la misma dirección IP. Desasocie las máquinas virtuales de las direcciones IP básicas y asócielas con las direcciones IP estándar recién creadas. A continuación, podrá seguir las instrucciones para agregar máquinas virtuales al grupo de back-end de Standard Load Balancer.

- **Creación de nuevas máquinas virtuales para agregarlas a los grupos de back-end de la instancia de Standard Public Load Balancer recién creada.**
 - [Aquí](#) encontrará más instrucciones sobre cómo crear una máquina virtual y cómo asociarla con Standard Load Balancer.

Creación de una regla de salida para la conexión de salida

Siga las [instrucciones](#) para crear una regla de salida para poder:

- Definir la NAT de salida desde cero.
- Escalar y ajustar el comportamiento de la NAT de salida existente.

Creación de reglas de NSG para las máquinas virtuales a fin de evitar la comunicación en Internet

Si quiere evitar que el tráfico de Internet llegue a las máquinas virtuales, puede crear una [regla de NSG](#) en la interfaz de red de las máquinas virtuales.

Preguntas frecuentes

¿Hay alguna limitación en el script de Azure PowerShell para migrar la configuración de v1 a v2?

Sí. Consulte [Advertencias y limitaciones](#).

¿Puede el script de Azure PowerShell cambiar el tráfico de la instancia de Basic Load Balancer a la instancia de Standard Load Balancer recién creada?

No. El script de Azure PowerShell solo migra la configuración. Usted es el responsable de realizar y controlar la migración real del tráfico.

Se han producido algunos problemas al usar este script. ¿Cómo puedo obtener ayuda?

Puede enviar un correo electrónico a slbupgradesupport@microsoft.com, abrir una incidencia con el Soporte técnico de Azure o hacer ambas cosas.

Pasos siguientes

[Más información sobre Load Balancer estándar](#)

Modificación de la configuración de tiempo de espera de inactividad de TCP para Azure Load Balancer

23/09/2020 • 7 minutes to read • [Edit Online](#)




NOTE

Este artículo se ha actualizado para usar el nuevo módulo Az de Azure PowerShell. Aún puede usar el módulo de AzureRM que continuará recibiendo correcciones de errores hasta diciembre de 2020 como mínimo. Para más información acerca del nuevo módulo Az y la compatibilidad con AzureRM, consulte [Introducing the new Azure PowerShell Az module](#) (Presentación del nuevo módulo Az de Azure PowerShell). Para obtener instrucciones sobre la instalación del módulo Az, consulte [Instalación de Azure PowerShell](#).

Uso de Azure Cloud Shell

En Azure se hospeda Azure Cloud Shell, un entorno de shell interactivo que puede utilizar mediante el explorador. Puede usar Bash o PowerShell con Cloud Shell para trabajar con los servicios de Azure. Puede usar los comandos preinstalados de Cloud Shell para ejecutar el código de este artículo sin tener que instalar nada en su entorno local.

Para iniciar Azure Cloud Shell:

OPCIÓN	EJEMPLO O VÍNCULO
Seleccione Pruébalo en la esquina superior derecha de un bloque de código. Solo con seleccionar Pruébalo no se copia automáticamente el código en Cloud Shell.	
Vaya a https://shell.azure.com o seleccione el botón Iniciar Cloud Shell para abrir Cloud Shell en el explorador.	
Seleccione el botón Cloud Shell en la barra de menús de la esquina superior derecha de Azure Portal .	

Para ejecutar el código de este artículo en Azure Cloud Shell:

1. Inicie Cloud Shell.
2. Seleccione el botón **Copiar** de un bloque de código para copiar el código.
3. Pegue el código en la sesión de Cloud Shell. Para ello, seleccione **Ctrl+Mayús+V** en Windows y Linux, o bien seleccione **Cmd+Mayús+V** en macOS.
4. Seleccione **Entrar** para ejecutar el código.

Si decide instalar y usar PowerShell de forma local, para realizar los pasos de este artículo necesita la versión 5.4.1 del módulo de Azure PowerShell o cualquier versión posterior. Ejecute `Get-Module -ListAvailable Az` para buscar la versión instalada. Si necesita actualizarla, consulte [Instalación del módulo de Azure PowerShell](#). Si PowerShell se ejecuta localmente, también debe ejecutar `Connect-AzAccount` para crear una conexión con Azure.

Tiempo de espera de inactividad de TCP

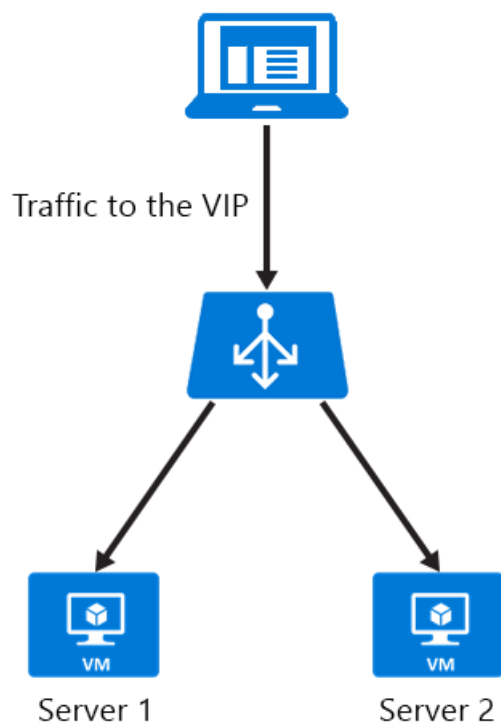
Azure Load Balancer tiene una configuración de tiempo de espera de inactividad de 4 a 30 minutos. De forma predeterminada, se establece en 4 minutos. Si un período de inactividad es mayor que el valor de tiempo de espera, no hay ninguna garantía de que todavía exista la sesión TCP o HTTP entre el cliente y el servicio en la nube.

Cuando se cierra la conexión, la aplicación cliente puede recibir el mensaje de error siguiente: "The underlying connection was closed: A connection that was expected to be kept alive was closed by the server" (Se ha terminado la conexión: El servidor cerró una conexión que se esperaba estuviera activa).

Una práctica común es usar TCP Keep-alive. Esta práctica mantiene la conexión activa durante un periodo más largo. Para obtener más información, consulte estos [ejemplos de .NET](#). Con Keep-alive habilitado, los paquetes se envían durante los periodos de inactividad en la conexión. Los paquetes de Keep-alive garantizan que no se alcance el valor de tiempo de espera de inactividad y la conexión se mantenga durante un largo período.

La configuración funciona solo para conexiones entrantes. Para evitar la pérdida de la conexión, configure el TCP keep-alive con un intervalo menor que el valor de tiempo de espera de inactividad o aumentar el valor de tiempo de espera de inactividad. Para admitir estos escenarios, se agregó compatibilidad con un tiempo de espera de inactividad configurable.

TCP keep-alive funciona en escenarios donde la batería no supone una restricción. No se recomienda para aplicaciones móviles. El uso de TCP Keep-alive desde una aplicación móvil puede agotarla batería del dispositivo más rápidamente.



Las secciones siguientes describen cómo cambiar la configuración de tiempo de espera de inactividad para los recursos de IP pública y equilibrador de carga.

NOTE

El tiempo de espera de inactividad de TCP no afecta a las reglas de equilibrio de carga en el protocolo UDP.

Configuración del tiempo de espera de TCP para la IP pública a nivel de instancia en 15 minutos

```
$publicIP = Get-AzPublicIpAddress -Name MyPublicIP -ResourceGroupName MyResourceGroup
$publicIP.IdleTimeoutInMinutes = "15"
Set-AzPublicIpAddress -PublicIpAddress $publicIP
```

`IdleTimeoutInMinutes` es opcional. Si no se establece, el tiempo de espera predeterminado es de 4 minutos. El intervalo de tiempo de espera aceptable está entre 4 y 30 minutos.

Establecimiento del tiempo de espera de TCP en una regla de carga equilibrada en 15 minutos

Para establecer el tiempo de espera de inactividad de un equilibrador de carga, se establece el valor de "IdleTimeoutInMinutes" en la regla de carga equilibrada. Por ejemplo:

```
$lb = Get-AzLoadBalancer -Name "MyLoadBalancer" -ResourceGroup "MyResourceGroup"
$lb | Set-AzLoadBalancerRuleConfig -Name myLBrule -IdleTimeoutInMinutes 15
```

Pasos siguientes

[Información general sobre el equilibrador de carga interno](#)

[Introducción a la creación de un equilibrador de carga orientado a Internet](#)

[Configuración de un modo de distribución del equilibrador de carga](#)

Configuración del modo de distribución de Azure Load Balancer

23/09/2020 • 12 minutes to read • [Edit Online](#)

NOTE

Este artículo se ha actualizado para usar el nuevo módulo Az de Azure PowerShell. Aún puede usar el módulo de AzureRM que continuará recibiendo correcciones de errores hasta diciembre de 2020 como mínimo. Para más información acerca del nuevo módulo Az y la compatibilidad con AzureRM, consulte [Introducing the new Azure PowerShell Az module](#) (Presentación del nuevo módulo Az de Azure PowerShell). Para obtener instrucciones sobre la instalación del módulo Az, consulte [Instalación de Azure PowerShell](#).

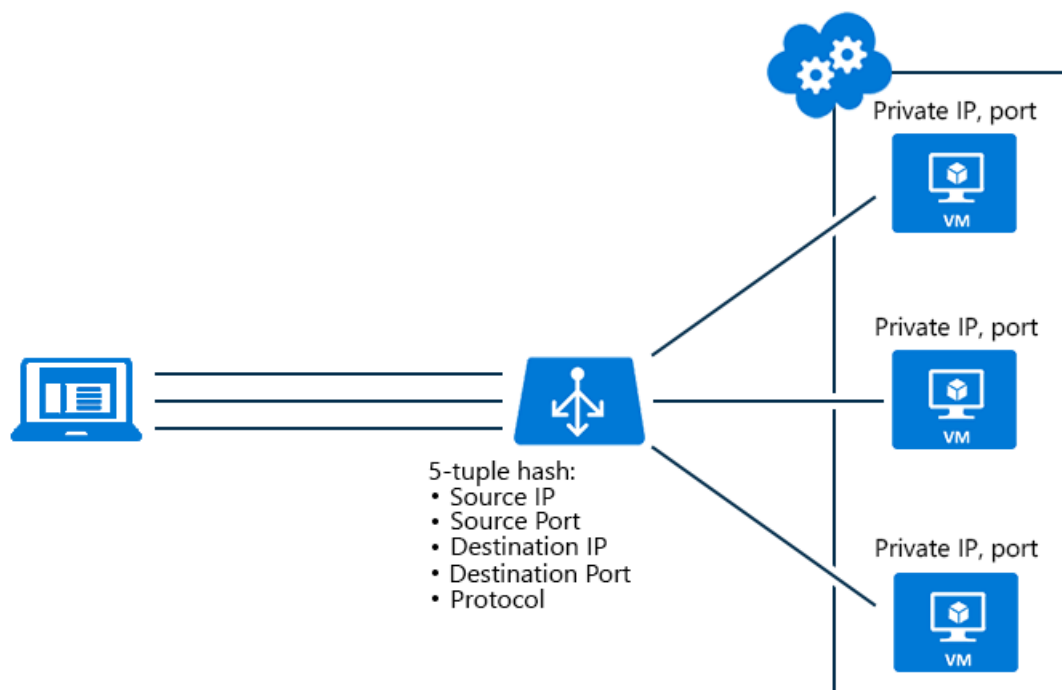
Distribución basada en hash

El modo de distribución predeterminado para Azure Load Balancer es un hash de tupla de cinco elementos.

La tupla consta de:

- IP de origen
- Puerto de origen
- IP de destino
- Puerto de destino
- Tipo de protocolo

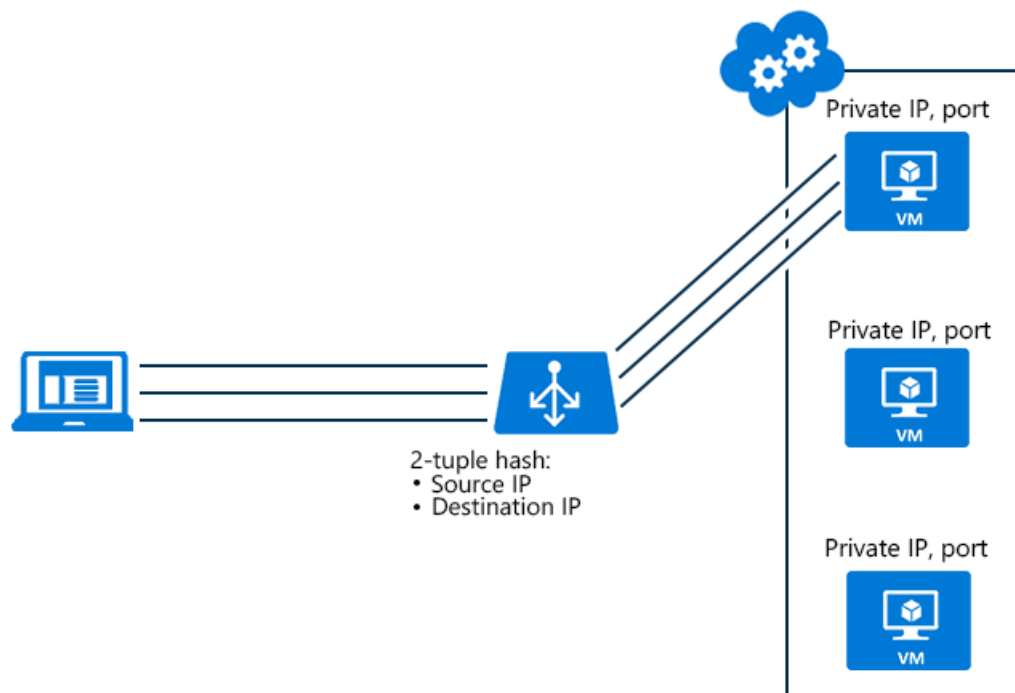
El hash se utiliza para asignar el tráfico a los servidores disponibles. El algoritmo solo proporciona adherencia dentro de una sesión de transporte. Los paquetes que se encuentran en la misma sesión se dirigen a la misma dirección IP del centro de datos tras el punto de conexión con equilibrio de carga. Cuando el cliente inicia una nueva sesión desde la misma IP de origen, el puerto de origen cambia y provoca que el tráfico vaya hacia otro punto de conexión del centro de datos.



Modo de afinidad de IP de origen

El equilibrador de carga también se puede configurar mediante el modo de distribución de afinidad de IP de origen. Este modo de distribución también se conoce como afinidad de la sesión o afinidad de IP del cliente. El modo utiliza un hash de tupla de dos elementos (IP de origen e IP de destino) o de tres elementos (IP de origen, IP de destino y tipo de protocolo) para asignar el tráfico a los servidores disponibles. Mediante el uso de la afinidad de la IP de origen, las conexiones que se han iniciado desde el mismo equipo cliente van al mismo punto de conexión del centro de datos.

En la figura siguiente, se ilustra la configuración de tupla de dos elementos. Observe cómo la tupla de dos elementos se ejecuta a través del equilibrador de carga en la máquina virtual 1 (VM1). A continuación, VM2 y VM3 realizan una copia de seguridad de VM1.



El modo de afinidad de IP de origen resuelve una incompatibilidad entre Azure Load Balancer y la Puerta de enlace de Escritorio remoto (RD Gateway). Al utilizar este modo, puede crear una granja de servidores de Puerta de enlace de Escritorio remoto en un solo servicio en la nube.

Otro escenario de caso de uso es la carga de elementos multimedia. La carga de datos tiene lugar a través de UDP, pero el plano de control se consigue mediante TCP:

- Un cliente inicia una sesión TCP en la dirección pública de carga equilibrada y se le dirige a una DIP específica. El canal se mantiene activo para supervisar el estado de conexión.
- Se inicia una nueva sesión UDP desde el mismo equipo cliente al mismo punto de conexión público de carga equilibrada. La conexión se dirige al mismo punto de conexión DIP que la conexión TCP anterior. La carga de elementos multimedia se puede ejecutar a alto rendimiento al tiempo que mantiene un canal de control a través de TCP.

NOTE

Cuando un conjunto de carga equilibrada cambia al quitar o agregar una máquina virtual, la distribución de las solicitudes de cliente se vuelve a calcular. No puede depender de nuevas conexiones desde clientes existentes para terminar en el mismo servidor. Además, el uso del modo de distribución de afinidad de IP de origen puede ocasionar una distribución desigual del tráfico. Los clientes que se ejecutan detrás de servidores proxy pueden considerarse como una sola aplicación cliente.

Configuración de la afinidad de IP de origen

Portal de Azure

Para cambiar la configuración del modo de distribución, modifique la regla de equilibrio de carga en el portal.

1. Inicie sesión en Azure Portal y busque el grupo de recursos que contiene el equilibrador de carga que desea cambiar. Para ello, debe hacer clic en **Grupos de recursos**.
2. En la pantalla de información general del equilibrador de carga, haga clic en **Reglas de equilibrio de carga en Configuración**.
3. En la pantalla de reglas de equilibrio de carga, haga clic en la regla de equilibrio de carga para la que desee cambiar el modo de distribución.
4. En la regla, para cambiar el modo de distribución hay que cambiar el cuadro desplegable **Persistencia de la sesión**. Están disponibles las siguientes opciones:
 - **Ninguno (basado en hash)** : especifica que cualquier máquina virtual puede controlar las solicitudes sucesivas del mismo cliente.
 - **IP de cliente (dos tuplas de afinidad de IP de origen)** : especifica que la misma máquina virtual controlará las solicitudes sucesivas de la misma dirección IP de cliente.
 - **IP de cliente y protocolo (tres tuplas de afinidad de IP de origen)** : especifica que la misma máquina virtual controlará las solicitudes sucesivas de la combinación de la misma dirección IP de cliente y protocolo.
5. Elija el modo de distribución y haga clic en **Guardar**.

Azure PowerShell

En máquinas virtuales implementadas con Resource Manager, use PowerShell para cambiar la configuración de distribución del equilibrador de carga en una regla de equilibrio de carga existente. El siguiente comando actualiza el modo de distribución:

```
$lb = Get-AzLoadBalancer -Name MyLb -ResourceGroupName MyLbRg
$lb.LoadBalancingRules[0].LoadDistribution = 'sourceIp'
Set-AzLoadBalancer -LoadBalancer $lb
```

En máquinas virtuales clásicas, use Azure PowerShell para cambiar la configuración de distribución. Agregue un punto de conexión de Azure a una máquina virtual y configure el modo de distribución del equilibrador de carga:

```
Get-AzureVM -ServiceName mySvc -Name MyVM1 | Add-AzureEndpoint -Name HttpIn -Protocol TCP -PublicPort 80 -
LocalPort 8080 -LoadBalancerDistribution sourceIP | Update-AzureVM
```

Establezca el valor del elemento `LoadBalancerDistribution` para la cantidad necesaria de equilibrio de carga. Especifique `sourceIP` para el equilibrio de carga con tupla de dos elementos (IP de origen e IP de destino). Especifique `sourceIPProtocol` para el equilibrio de carga con tupla de tres elementos (IP de origen, IP de destino y tipo de protocolo). Especifique `none` para el comportamiento predeterminado de equilibrio de carga con tupla de cinco elementos.

Recupere una configuración de modo de distribución del equilibrador de carga de punto de extremo mediante estos valores:

```
PS C:\> Get-AzureVM -ServiceName MyService -Name MyVM | Get-AzureEndpoint
```

```
VERBOSE: 6:43:50 PM - Completed Operation: Get Deployment
LBSetName : MyLoadBalancedSet
LocalPort : 80
Name : HTTP
Port : 80
Protocol : tcp
Vip : 65.52.xxx.xxx
ProbePath :
ProbePort : 80
ProbeProtocol : tcp
ProbeIntervalInSeconds : 15
ProbeTimeoutInSeconds : 31
EnableDirectServerReturn : False
Acl : {}
InternalLoadBalancerName :
IdleTimeoutInMinutes : 15
LoadBalancerDistribution : sourceIP
```

Cuando el elemento `LoadBalancerDistribution` no está presente, Azure Load Balancer usa el algoritmo de tupla de cinco elementos predeterminado.

Configuración del modo de distribución en un conjunto de puntos de conexión de carga equilibrada

Cuando los puntos de conexión forman parte de un conjunto de puntos de conexión de carga equilibrada, el modo de distribución debe configurarse en el conjunto de puntos de conexión de carga equilibrada:

```
Set-AzureLoadBalancedEndpoint -ServiceName MyService -LBSetName LBSet1 -Protocol TCP -LocalPort 80 -
ProbeProtocolTCP -ProbePort 8080 -LoadBalancerDistribution sourceIP
```

Configuración del modo de distribución para puntos de conexión de Cloud Services

Utilice el SDK de Azure para .NET 2.5 para actualizar el servicio en la nube. Los valores del punto de conexión para Cloud Services se establecen en el archivo .csdef. Para actualizar el modo de distribución del equilibrador de carga para una implementación de Cloud Services, se requiere una actualización de la implementación.

Este es un ejemplo de los cambios de .csdef para la configuración de extremo:

```
<WorkerRole name="worker-role-name" vmsize="worker-role-size" enableNativeCodeExecution="[true|false]">
  <Endpoints>
    <InputEndpoint name="input-endpoint-name" protocol="[http|https|tcp|udp]" localPort="local-port-number"
port="port-number" certificate="certificate-name" loadBalancerProbe="load-balancer-probe-name"
loadBalancerDistribution="sourceIP" />
  </Endpoints>
</WorkerRole>
<NetworkConfiguration>
  <VirtualNetworkSite name="VNet"/>
  <AddressAssignments>
<InstanceAddress roleName="VMRolePersisted">
  <PublicIPs>
    <PublicIP name="public-ip-name" idleTimeoutInMinutes="timeout-in-minutes"/>
  </PublicIPs>
</InstanceAddress>
  </AddressAssignments>
</NetworkConfiguration>
```

Ejemplo de API

En el ejemplo siguiente se muestra cómo volver a configurar el modo de distribución del equilibrador de carga para un conjunto específico de carga equilibrada en una implementación.

Cambiar el modo de distribución para un conjunto de carga equilibrada implementado

Utilice el modelo de implementación clásica de Azure para cambiar una configuración de implementación existente. Agregue el `x-ms-version` encabezado y establezca el valor en la versión 2014-09-01 o posterior.

Solicitud

```
POST https://management.core.windows.net/<subscription-id>/services/hostedservices/<cloudservice-name>/deployments/<deployment-name>?comp=UpdateLbSet    x-ms-version: 2014-09-01
Content-Type: application/xml
```

```
<LoadBalancedEndpointList xmlns="http://schemas.microsoft.com/windowsazure"
xmlns:i="https://www.w3.org/2001/XMLSchema-instance">
  <InputEndpoint>
    <LoadBalancedEndpointSetName> endpoint-set-name </LoadBalancedEndpointSetName>
    <LocalPort> local-port-number </LocalPort>
    <Port> external-port-number </Port>
    <LoadBalancerProbe>
      <Port> port-assigned-to-probe </Port>
      <Protocol> probe-protocol </Protocol>
      <IntervalInSeconds> interval-of-probe </IntervalInSeconds>
      <TimeoutInSeconds> timeout-for-probe </TimeoutInSeconds>
    </LoadBalancerProbe>
    <Protocol> endpoint-protocol </Protocol>
    <EnableDirectServerReturn> enable-direct-server-return </EnableDirectServerReturn>
    <IdleTimeoutInMinutes>idle-time-out</IdleTimeoutInMinutes>
    <LoadBalancerDistribution>sourceIP</LoadBalancerDistribution>
  </InputEndpoint>
</LoadBalancedEndpointList>
```

Como se ha descrito anteriormente, establezca el elemento `LoadBalancerDistribution` en `sourceIP` para la afinidad con tupla de dos elementos, `sourceIPProtocol` para la afinidad con tupla de tres elementos o `none` para los casos sin afinidad (afinidad con tupla de cinco elementos).

Response

```
HTTP/1.1 202 Accepted
Cache-Control: no-cache
Content-Length: 0
Server: 1.0.6198.146 (rd_rdfc_stable.141015-1306) Microsoft-HTTPAPI/2.0
x-ms-servedbyregion: ussouth2
x-ms-request-id: 9c7bda3e67c621a6b57096323069f7af
Date: Thu, 16 Oct 2014 22:49:21 GMT
```

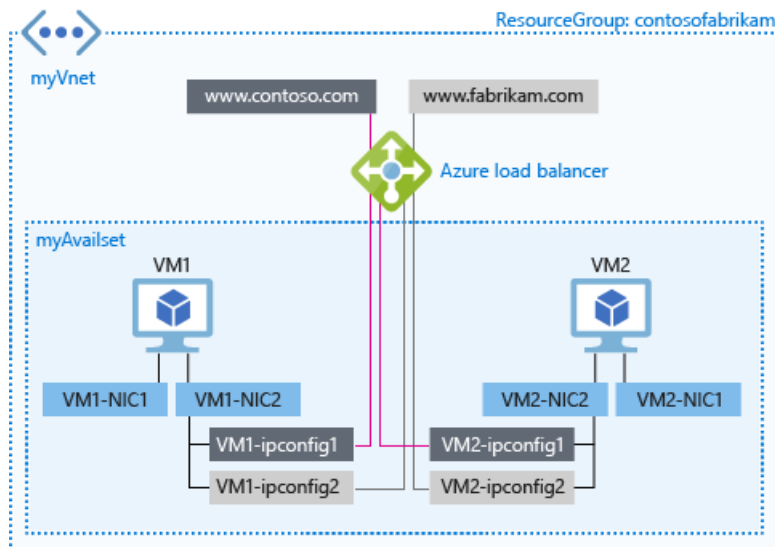
Pasos siguientes

- [Información general sobre el equilibrador de carga interno de Azure](#)
- [Introducción a la configuración de un equilibrador de carga accesible desde Internet](#)
- [Configuración de opciones de tiempo de espera de inactividad de TCP para el equilibrador de carga](#)

Equilibrio de carga en varias configuraciones de IP mediante Azure Portal

23/09/2020 • 13 minutes to read • [Edit Online](#)

En este artículo, le mostraremos cómo usar Azure Load Balancer con varias direcciones IP en un controlador de interfaz de red secundario (NIC). En el siguiente diagrama se ilustra nuestro escenario:



En nuestro escenario, usamos la siguiente configuración:

- Dos máquinas virtuales (VM) que ejecutan Windows.
- Cada máquina virtual tiene un NIC principal y otro secundario.
- Cada NIC secundario tiene dos configuraciones IP.
- Cada máquina virtual hospeda dos sitios web: contoso.com y fabrikam.com.
- Cada uno de los sitios web está enlazado a una configuración de IP en el NIC secundario.
- Azure Load Balancer se utiliza para exponer dos direcciones IP de servidor front-end, una para cada sitio web. Las direcciones de servidor front-end se utilizan para distribuir el tráfico a la configuración IP correspondiente para cada sitio web.
- Se usa el mismo número de puerto para las direcciones IP de servidor front-end y las de grupo back-end.

Prerequisites

En nuestro ejemplo de escenario se da por supuesto que tiene un grupo de recursos denominado **contosofabrikam** con la siguiente configuración:

- El grupo de recursos incluye una red virtual denominada **myVNet**.
- La red **myVNet** incluye dos máquinas virtuales con el nombre **VM1** y **VM2**.
- VM1 y VM2 están en el mismo conjunto de disponibilidad, denominado **myAvailabilitySet**.
- VM1 y VM2 tienen un NIC principal con los nombres **VM1NIC1** y **VM2NIC1**, respectivamente.
- VM1 y VM2 tienen un NIC secundaria con los nombres **VM1NIC2** y **VM2NIC2**, respectivamente.

Para más información sobre la creación de máquinas virtuales con varios NIC, vea [Creación de una máquina virtual con varios NIC mediante PowerShell](#).

Equilibrio de carga en varias configuraciones de IP

Complete los pasos siguientes para reproducir el escenario que se describe en este artículo.

Paso 1: Configuración de los NIC secundarios

Para cada máquina virtual de la red virtual, agregue la configuración de IP para el NIC secundario:

1. Vaya a Azure Portal: <https://portal.azure.com>. Inicie sesión con su cuenta de Azure.
2. En la parte superior izquierda de la pantalla, seleccione el icono **Grupo de recursos**. A continuación, seleccione el grupo de recursos donde se encuentran las máquinas virtuales (por ejemplo, **contosofabrikam**). En el panel **Grupos de recursos** se muestran todos los recursos y los NIC para las máquinas virtuales.
3. Agregue al NIC secundario de cada máquina virtual la configuración de IP:
 - a. Seleccione el NIC secundario que desee configurar.
 - b. Seleccione **Configuraciones IP**. En el siguiente panel, cerca de la parte superior, seleccione **Agregar**.
 - c. En **Agregar configuración IP**, agregue una segunda configuración de IP al NIC:
 - a. Escriba un nombre para la configuración de IP secundaria. (Por ejemplo, para VM1 y VM2, asigne a las configuraciones de IP los nombres **VM1NIC2-ipconfig2** y **VM2NIC2-ipconfig2** respectivamente).
 - b. Para **Dirección IP privada**, en la configuración **Asignación**, seleccione **Estática**.
 - c. Seleccione **Aceptar**.

Cuando haya finalizado la segunda configuración de IP para el NIC secundario, se muestra en **Configuraciones de IP** del NIC en cuestión.

Paso 2: Creación del equilibrador de carga

Creación del equilibrador de carga para la configuración:

1. Vaya a Azure Portal: <https://portal.azure.com>. Inicie sesión con su cuenta de Azure.
2. En la parte superior izquierda de la pantalla, seleccione **Crear un recurso** > **Redes** > **Load Balancer**. A continuación, seleccione **Crear**.
3. En **Crear equilibrador de carga**, escriba un nombre para el equilibrador de carga. En este escenario, usamos el nombre **mylb**.
4. En **Dirección IP pública**, cree una nueva dirección IP pública denominada **PublicIP1**.
5. En **Grupo de recursos**, seleccione el grupo de recursos existente de sus máquinas virtuales (por ejemplo, **contosofabrikam**). Seleccione la ubicación para implementar el equilibrador de carga y, luego, seleccione **Aceptar**.

El equilibrador de carga comienza a realizar la implementación. La implementación puede tardar unos minutos en completarse. Una vez completada la implementación, el equilibrador de carga se muestra como un recurso en el grupo de recursos.

Paso 3: Configuración del grupo de direcciones IP de servidor front-end

Para cada sitio web (contoso.com y fabrikam.com), configure el grupo de direcciones IP de servidor front-end en el equilibrador de carga:

1. En el portal, seleccione **Más servicios**. En el cuadro de filtro, escriba **Dirección IP pública** y, a

continuación, seleccione **Direcciones IP públicas**. En el siguiente panel, cerca de la parte superior, seleccione **Agregar**.

2. Configure dos direcciones IP públicas (**PublicIP1** y **PublicIP2**) para ambos sitios web (contoso.com y fabrikam):
 - a. Escriba un nombre para la dirección IP de servidor front-end.
 - b. En **Grupo de recursos**, seleccione el grupo de recursos existente de sus máquinas virtuales (por ejemplo, **contosofabrikam**).
 - c. Para **Ubicación**, seleccione la misma ubicación que la de las máquinas virtuales.
 - d. Seleccione **Aceptar**.

Una vez creadas las direcciones IP públicas, se muestran en las **direcciones IP públicas**.

3. En el portal, seleccione **Más servicios**. En el cuadro de filtro, escriba **load balancer** y, luego, seleccione **Load Balancer**.
4. Seleccione el equilibrador de carga (**mylb**) al que desea agregar el grupo de direcciones IP de servidor front-end.
5. En **Configuración**, seleccione **Configuración de direcciones IP de front-end**. En el siguiente panel, cerca de la parte superior, seleccione **Agregar**.
6. Escriba un nombre para la dirección IP de servidor front-end (por ejemplo, **contosofe** o **fabrikamfe**).
7. Seleccione **Dirección IP**. En **Elegir dirección IP pública**, seleccione las direcciones IP para servidor front-end (**PublicIP1** o **PublicIP2**).
8. Cree la segunda dirección IP de servidor front-end repitiendo desde el [paso 3](#) hasta el [paso 7](#) en esta sección.

Después de configurar el grupo de servidores front-end, las direcciones IP se muestran en la configuración **Configuración de direcciones IP de front-end** del equilibrador de carga.

Paso 4: Configuración del grupo de servidores back-end

Para cada sitio web (contoso.com y fabrikam.com), configure el grupo de direcciones de servidores back-end en el equilibrador de carga:

1. En el portal, seleccione **Más servicios**. En el cuadro de filtro, escriba **load balancer** y, luego, seleccione **Load Balancer**.
2. Seleccione el equilibrador de carga (**mylb**) al que va a agregar el grupo de servidores back-end.
3. En **Configuración**, seleccione **Grupos de back-end**. Escriba un nombre para el grupo de servidores back-end (por ejemplo, **contosopool** o **fabrikampool**). En el siguiente panel, cerca de la parte superior, seleccione **Agregar**.
4. En **Asociado a**, seleccione **Conjunto de disponibilidad**.
5. En **Conjunto de disponibilidad**, seleccione **myAvailset**.
6. Agregue las configuraciones de IP de la red de destino para ambas máquinas virtuales:

Add backend pool
myloadbalancer

* Name
Contosopool ✓

IP version
IPv4 IPv6

Associated to
Availability set

Availability set
ContosoAvailset
number of virtual machines: 2

Target network IP configurations
Only VMs within the current availability set can be chosen. Once a VM is chosen, you can select a network IP configuration related to it.

Virtual machine: ContosoVM1 Network IP configuration: ContosoVM1Nic2/ipconfigtest (192.168.2.5)	🗑️
--	----

* Target virtual machine
ContosoVM2
size: Standard_DS2_v2, network interfaces: 2

* Network IP configuration
ipconfigtest (192.168.4.5)

+ Add a target network IP configuration

OK

- En **Máquina virtual de destino**, seleccione la máquina virtual que desea agregar al grupo de servidores back-end (por ejemplo, **VM1** o **VM2**).
- En **Configuración IP de red**, seleccione la configuración de IP del NIC secundario de la máquina virtual que seleccionó en el paso anterior (por ejemplo **VM1NIC2-ipconfig2** o **VM2NIC2-ipconfig2**).

7. Seleccione **Aceptar**.

Después de configurar el grupo de servidores back-end, las direcciones se muestran en la configuración **Grupo back-end** del equilibrador de carga.

Paso 5: Configuración del sondeo de mantenimiento

Configuración de un sondeo de estado para el equilibrador de carga:

- En el portal, seleccione **Más servicios**. En el cuadro de filtro, escriba **load balancer** y, luego, seleccione **Load Balancer**.
- Seleccione el equilibrador de carga (**mylb**) al que desee agregar el sondeo de mantenimiento.
- En **Configuración**, seleccione **Sondeo de estado**. En el siguiente panel, cerca de la parte superior, seleccione **Agregar**.
- Escriba un nombre para el sondeo de estado (por ejemplo, **HTTP**). Seleccione **Aceptar**.

Paso 6: Configuración de las reglas de equilibrio de carga

Para cada sitio web (contoso.com y fabrikam.com), configure las reglas de equilibrio de carga:

- En **Configuración**, seleccione **Reglas de equilibrio de carga**. En el siguiente panel, cerca de la parte superior, seleccione **Agregar**.
- En **Nombre**, escriba un nombre para la regla de equilibrio de carga (por ejemplo, **HTTPc** para contoso.com,

o HTTPf para fabrikam.com).

3. En **Dirección IP de front-end**, seleccione la dirección IP de servidor front-end creada previamente (por ejemplo **contosofo** o **fabrikamfe**).
4. En **Puerto y Puerto back-end**, mantenga el valor predeterminado de **80**.
5. En **IP flotante (Direct Server Return)** , seleccione **Deshabilitado**.
6. Seleccione **Aceptar**.
7. Cree la segunda regla del equilibrador de carga repitiendo el [paso 1](#) hasta el [paso 6](#) en esta sección.

Una vez configuradas las reglas, se muestran en el equilibrador de carga la configuración de **reglas de equilibrio de carga**.

Paso 7: Configuración de los registros DNS

Como último paso, configure los registros de recursos de DNS para que apunten a las direcciones IP de servidor front-end respectivas para el equilibrador de carga. Puede hospedar los dominios en Azure DNS. Para más información sobre el uso de Azure DNS con Load Balancer, consulte [Uso de Azure DNS con otros servicios de Azure](#).

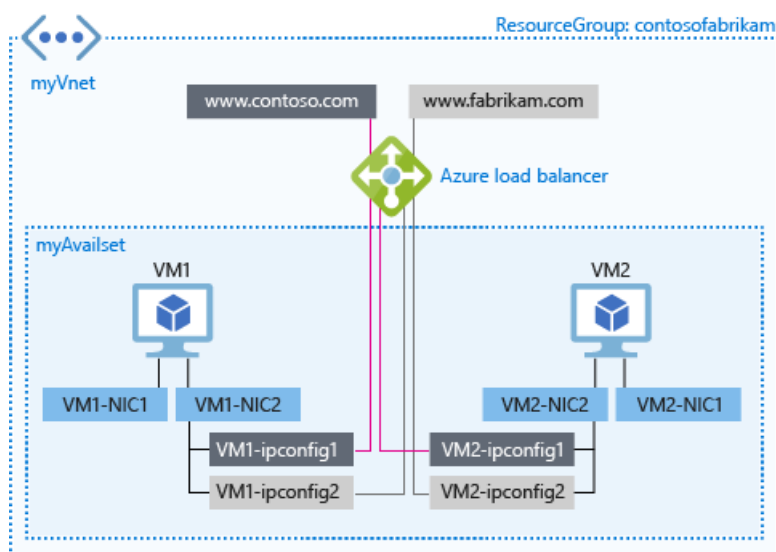
Pasos siguientes

- Aprenda más sobre cómo combinar servicios de equilibrio de carga en Azure en [Uso de servicios de equilibrio de carga de Azure](#).
- Obtenga información sobre cómo usar diferentes tipos de registros para administrar y solucionar los problemas del equilibrador de carga en [Registros de Azure Monitor para Azure Load Balancer](#).

Equilibrio de carga en configuraciones de varias IP mediante la CLI de Azure

23/09/2020 • 6 minutes to read • [Edit Online](#)

En este artículo, se explica cómo se utiliza Azure Load Balancer con varias direcciones IP en una interfaz de red secundaria (NIC). En este escenario, tenemos dos máquinas virtuales que ejecutan Windows. Cada una de ellas cuenta con una NIC principal y otra secundaria. Cada NIC secundario tiene dos configuraciones IP. Cada máquina virtual hospeda dos sitios web: contoso.com y fabrikam.com. Cada uno de los sitios web está enlazado a una de las configuraciones de IP de la NIC secundaria. Usamos Azure Load Balancer para exponer dos direcciones IP front-end, una por cada sitio web, que van a distribuir el tráfico a la configuración de IP correspondiente del sitio web. En este escenario, se utiliza el mismo número de puerto en los dos front-end, así como en las dos direcciones IP del grupo de back-end.



Pasos para equilibrar la carga en varias configuraciones de IP

Para reproducir el escenario que se describe en este artículo, siga los pasos que se describen a continuación:

1. [Instale y configure la CLI de Azure](#) siguiendo los pasos que se describen en el artículo vinculado e inicie sesión en la cuenta de Azure.
2. [Cree un grupo de recursos](#) llamado *contosofabrikam*, tal y como se describe a continuación:

```
az group create contosofabrikam westcentralus
```

3. [Cree un conjunto de disponibilidad](#) para las dos máquinas virtuales. En este caso, utilice el siguiente comando:

```
az vm availability-set create --resource-group contosofabrikam --location westcentralus --name myAvailabilitySet
```

4. [Cree una red virtual](#) llamada *myVNet* y una subred denominada *mySubnet*.

```
az network vnet create --resource-group contosofabrikam --name myVnet --address-prefixes 10.0.0.0/16 --location westcentralus --subnet-name MySubnet --subnet-prefix 10.0.0.0/24
```

5. Cree un equilibrador de carga llamado *mylb*.

```
az network lb create --resource-group contosofabrikam --location westcentralus --name mylb
```

6. Cree dos direcciones IP públicas dinámicas para las configuraciones de IP de front-end del equilibrador de carga:

```
az network public-ip create --resource-group contosofabrikam --location westcentralus --name PublicIp1 --domain-name-label contoso --allocation-method Dynamic

az network public-ip create --resource-group contosofabrikam --location westcentralus --name PublicIp2 --domain-name-label fabrikam --allocation-method Dynamic
```

7. Cree las dos configuraciones de IP de front-tend: *contosofe* y *fabrikamfe*, respectivamente:

```
az network lb frontend-ip create --resource-group contosofabrikam --lb-name mylb --public-ip-name PublicIp1 --name contosofe
az network lb frontend-ip create --resource-group contosofabrikam --lb-name mylb --public-ip-name PublicIp2 --name fabrikamfe
```

8. Cree los grupos de direcciones del back-end: *contosopool* y *fabrikampool*, un [sondeo](#): - *HTTP*, y las reglas de equilibrado de carga: *HTTPc* y *HTTPf*.

```
az network lb address-pool create --resource-group contosofabrikam --lb-name mylb --name contosopool
azure network lb address-pool create --resource-group contosofabrikam --lb-name mylb --name fabrikampool

az network lb probe create --resource-group contosofabrikam --lb-name mylb --name HTTP --protocol "http" --interval 15 --count 2 --path index.html

az network lb rule create --resource-group contosofabrikam --lb-name mylb --name HTTPc --protocol tcp --probe-name http --frontend-port 5000 --backend-port 5000 --frontend-ip-name contosofe --backend-address-pool-name contosopool
az network lb rule create --resource-group contosofabrikam --lb-name mylb --name HTTPf --protocol tcp --probe-name http --frontend-port 5000 --backend-port 5000 --frontend-ip-name fabrikamfe --backend-address-pool-name fabrikampool
```

9. Ejecute el comando siguiente para [comprobar que el equilibrador de carga](#) se creó correctamente:

```
az network lb show --resource-group contosofabrikam --name mylb
```

10. Cree una dirección IP pública: *myPublicIp*, y una [cuenta de almacenamiento](#): *mystorageaccount1*, para la primera máquina virtual (VM1), tal y como se muestra a continuación:

```
az network public-ip create --resource-group contosofabrikam --location westcentralus --name myPublicIP --domain-name-label mypublicdns345 --allocation-method Dynamic

az storage account create --location westcentralus --resource-group contosofabrikam --kind Storage --sku-name GRS mystorageaccount1
```

11. Cree las interfaces de red para VM1 y agregue una segunda configuración de IP, *VM1-ipconfig2*, y cree la

VM tal como se describe a continuación:

```
az network nic create --resource-group contosofabrikam --location westcentralus --subnet-vnet-name myVnet --subnet-name mySubnet --name VM1Nic1 --ip-config-name NIC1-ipconfig1
az network nic create --resource-group contosofabrikam --location westcentralus --subnet-vnet-name myVnet --subnet-name mySubnet --name VM1Nic2 --ip-config-name VM1-ipconfig1 --public-ip-name myPublicIP --lb-address-pool-ids "/subscriptions/<your subscription ID>/resourceGroups/contosofabrikam/providers/Microsoft.Network/loadBalancers/mylb/backendAddressPools/contosopool"
az network nic ip-config create --resource-group contosofabrikam --nic-name VM1Nic2 --name VM1-ipconfig2 --lb-address-pool-ids "/subscriptions/<your subscription ID>/resourceGroups/contosofabrikam/providers/Microsoft.Network/loadBalancers/mylb/backendAddressPools/fabrikampool"
az vm create --resource-group contosofabrikam --name VM1 --location westcentralus --os-type linux --nic-names VM1Nic1,VM1Nic2 --vnet-name VNet1 --vnet-subnet-name Subnet1 --availability-set myAvailabilitySet --vm-size Standard_DS3_v2 --storage-account-name mystorageaccount1 --image-urn canonical:UbuntuServer:16.04.0-LTS:latest --admin-username <your username> --admin-password <your password>
```

12. Repita los pasos 10 y 11 con la segunda máquina virtual:

```
az network public-ip create --resource-group contosofabrikam --location westcentralus --name myPublicIP2 --domain-name-label mypublicdns785 --allocation-method Dynamic
az storage account create --location westcentralus --resource-group contosofabrikam --kind Storage --sku-name GRS mystorageaccount2
az network nic create --resource-group contosofabrikam --location westcentralus --subnet-vnet-name myVnet --subnet-name mySubnet --name VM2Nic1
az network nic create --resource-group contosofabrikam --location westcentralus --subnet-vnet-name myVnet --subnet-name mySubnet --name VM2Nic2 --ip-config-name VM2-ipconfig1 --public-ip-name myPublicIP2 --lb-address-pool-ids "/subscriptions/<your subscription ID>/resourceGroups/contosofabrikam/providers/Microsoft.Network/loadBalancers/mylb/backendAddressPools/contosopool"
az network nic ip-config create --resource-group contosofabrikam --nic-name VM2Nic2 --name VM2-ipconfig2 --lb-address-pool-ids "/subscriptions/<your subscription ID>/resourceGroups/contosofabrikam/providers/Microsoft.Network/loadBalancers/mylb/backendAddressPools/fabrikampool"
az vm create --resource-group contosofabrikam --name VM2 --location westcentralus --os-type linux --nic-names VM2Nic1,VM2Nic2 --vnet-name VNet1 --vnet-subnet-name Subnet1 --availability-set myAvailabilitySet --vm-size Standard_DS3_v2 --storage-account-name mystorageaccount2 --image-urn canonical:UbuntuServer:16.04.0-LTS:latest --admin-username <your username> --admin-password <your password>
```

13. Por último, debe configurar los registros de recursos DNS para que apunten a la dirección IP de front-end correspondiente del equilibrador de carga. Puede hospedar los dominios en Azure DNS. Para más información sobre el uso de Azure DNS con Load Balancer, consulte [Uso de Azure DNS con otros servicios de Azure](#).

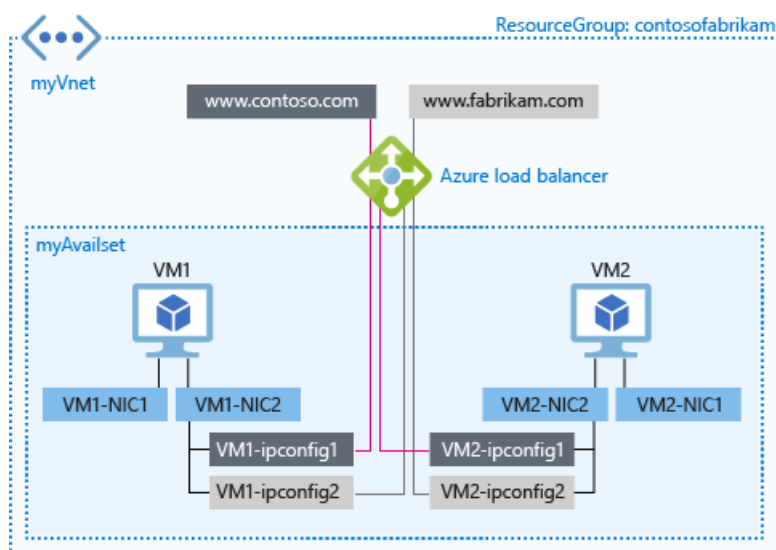
Pasos siguientes

- Aprenda más sobre cómo combinar servicios de equilibrio de carga en Azure en [Uso de servicios de equilibrio de carga de Azure](#).
- Aprenda a usar diferentes tipos de registros en Azure para administrar el equilibrador de carga y solucionar sus problemas en [Análisis de registros para Azure Load Balancer](#).

Equilibrio de carga en varias configuraciones de IP mediante PowerShell

23/09/2020 • 7 minutes to read • [Edit Online](#)

En este artículo, se explica cómo se utiliza Azure Load Balancer con varias direcciones IP en una interfaz de red secundaria (NIC). En este escenario, tenemos dos máquinas virtuales que ejecutan Windows. Cada una de ellas cuenta con una NIC principal y otra secundaria. Cada NIC secundario tiene dos configuraciones IP. Cada máquina virtual hospeda dos sitios web: contoso.com y fabrikam.com. Cada uno de los sitios web está enlazado a una de las configuraciones de IP de la NIC secundaria. Usamos Azure Load Balancer para exponer dos direcciones IP front-end, una por cada sitio web, que van a distribuir el tráfico a la configuración de IP correspondiente del sitio web. En este escenario, se utiliza el mismo número de puerto en los dos front-end, así como en las dos direcciones IP del grupo de back-end.



NOTE

Este artículo se ha actualizado para usar el nuevo módulo Az de Azure PowerShell. Aún puede usar el módulo de AzureRM que continuará recibiendo correcciones de errores hasta diciembre de 2020 como mínimo. Para más información acerca del nuevo módulo Az y la compatibilidad con AzureRM, consulte [Introducing the new Azure PowerShell Az module](#) (Presentación del nuevo módulo Az de Azure PowerShell). Para obtener instrucciones sobre la instalación del módulo Az, consulte [Instalación de Azure PowerShell](#).

Pasos para equilibrar la carga en varias configuraciones de IP

Siga estos pasos para reproducir el escenario que se describe en este artículo:

1. Instale Azure PowerShell. Consulte [Cómo instalar y configurar Azure PowerShell](#) para obtener más información sobre cómo instalar la versión más reciente de Azure PowerShell, seleccionar la suscripción que quiere usar e iniciar sesión en su cuenta.
2. Cree un grupo de recursos con el siguiente comando:

```
$location = "westcentralus".  
$myResourceGroup = "contosofabrikam"
```

Para más información, consulte el [Paso 2: Creación de un grupo de recursos](#).

3. Cree un conjunto de disponibilidad que contenga sus máquinas virtuales. En este caso, utilice el siguiente comando:

```
New-AzAvailabilitySet -ResourceGroupName "contosofabrikam" -Name "myAvailset" -Location "West Central US"
```

4. Siga las instrucciones de los pasos 3 a 5 del artículo [Creación de una máquina virtual Windows](#) para preparar la creación de una máquina virtual con una sola NIC. Realice el paso 6.1 y use el siguiente código en lugar del paso 6.2:

```
$availset = Get-AzAvailabilitySet -ResourceGroupName "contosofabrikam" -Name "myAvailset"
New-AzVMConfig -VMName "VM1" -VMSize "Standard_DS1_v2" -AvailabilitySetId $availset.Id
```

Después, complete los pasos 6.3 a 6.8 de [Creación de una máquina virtual Windows](#).

5. Agregue una segunda configuración de IP a cada una de las máquinas virtuales. Siga las instrucciones del artículo [Asignación de varias direcciones IP a máquinas virtuales](#). Use las opciones de configuración siguientes:

```
$NicName = "VM1-NIC2"
$RgName = "contosofabrikam"
$NicLocation = "West Central US"
$IPConfigName4 = "VM1-ipconfig2"
$Subnet1 = Get-AzVirtualNetworkSubnetConfig -Name "mySubnet" -VirtualNetwork $myVnet
```

Para los fines de este tutorial, no es necesario asociar las configuraciones de IP secundarias a direcciones IP públicas. Edite el comando para quitar la parte pública de la asociación de IP.

6. Complete de nuevo los pasos 4 a 6 de este artículo para VM2. Al hacerlo, asegúrese de reemplazar el nombre de la máquina virtual por VM2. Tenga en cuenta que no es necesario crear una red virtual para la segunda máquina virtual. Según sus necesidades de uso, puede crear o no una nueva subred.
7. Cree dos direcciones IP públicas y almacénelas en las variables correspondientes, tal y como se muestra:

```
$publicIP1 = New-AzPublicIpAddress -Name PublicIp1 -ResourceGroupName contosofabrikam -Location 'West Central US' -AllocationMethod Dynamic -DomainNameLabel contoso
$publicIP2 = New-AzPublicIpAddress -Name PublicIp2 -ResourceGroupName contosofabrikam -Location 'West Central US' -AllocationMethod Dynamic -DomainNameLabel fabrikam

$publicIP1 = Get-AzPublicIpAddress -Name PublicIp1 -ResourceGroupName contosofabrikam
$publicIP2 = Get-AzPublicIpAddress -Name PublicIp2 -ResourceGroupName contosofabrikam
```

8. Cree dos configuraciones de IP de front-end:

```
$frontendIP1 = New-AzLoadBalancerFrontendIpConfig -Name contosoFE -PublicIpAddress $publicIP1
$frontendIP2 = New-AzLoadBalancerFrontendIpConfig -Name fabrikamFE -PublicIpAddress $publicIP2
```

9. Cree los grupos de direcciones de back-end, un sondeo y las reglas de equilibrio de carga:

```
$beaddresspool1 = New-AzLoadBalancerBackendAddressPoolConfig -Name contosopool
$beaddresspool2 = New-AzLoadBalancerBackendAddressPoolConfig -Name fabrikampool

$healthProbe = New-AzLoadBalancerProbeConfig -Name HTTP -RequestPath 'index.html' -Protocol http -Port
80 -IntervalInSeconds 15 -ProbeCount 2

$lbrule1 = New-AzLoadBalancerRuleConfig -Name HTTPc -FrontendIpConfiguration $frontendIP1 -
BackendAddressPool $beaddresspool1 -Probe $healthprobe -Protocol Tcp -FrontendPort 80 -BackendPort 80
$lbrule2 = New-AzLoadBalancerRuleConfig -Name HTTPf -FrontendIpConfiguration $frontendIP2 -
BackendAddressPool $beaddresspool2 -Probe $healthprobe -Protocol Tcp -FrontendPort 80 -BackendPort 80
```

10. Una vez que tenga estos recursos creados, cree el equilibrador de carga:

```
$mylb = New-AzLoadBalancer -ResourceGroupName contosofabrikam -Name mylb -Location 'West Central US' -
FrontendIpConfiguration $frontendIP1 -LoadBalancingRule $lbrule -BackendAddressPool $beaddresspool -
Probe $healthProbe
```

11. Agregue el segundo grupo de direcciones de back-end y la configuración de IP de front-end al equilibrador de carga recién creado:

```
$mylb = Get-AzLoadBalancer -Name "mylb" -ResourceGroupName $myResourceGroup | Add-
AzLoadBalancerBackendAddressPoolConfig -Name fabrikampool | Set-AzLoadBalancer

$mylb | Add-AzLoadBalancerFrontendIpConfig -Name fabrikamfe -PublicIpAddress $publicIP2 | Set-
AzLoadBalancer

Add-AzLoadBalancerRuleConfig -Name HTTP -LoadBalancer $mylb -FrontendIpConfiguration $frontendIP2 -
BackendAddressPool $beaddresspool2 -Probe $healthProbe -Protocol Tcp -FrontendPort 80 -BackendPort 80 |
Set-AzLoadBalancer
```

12. Los siguientes comandos obtienen las NIC y agregan ambas configuraciones de IP de cada NIC secundaria al grupo de direcciones de back-end del equilibrador de carga:

```
$nic1 = Get-AzNetworkInterface -Name "VM1-NIC2" -ResourceGroupName "MyResourcegroup";
$nic2 = Get-AzNetworkInterface -Name "VM2-NIC2" -ResourceGroupName "MyResourcegroup";

$nic1.IpConfigurations[0].LoadBalancerBackendAddressPools.Add($mylb.BackendAddressPools[0]);
$nic1.IpConfigurations[1].LoadBalancerBackendAddressPools.Add($mylb.BackendAddressPools[1]);
$nic2.IpConfigurations[0].LoadBalancerBackendAddressPools.Add($mylb.BackendAddressPools[0]);
$nic2.IpConfigurations[1].LoadBalancerBackendAddressPools.Add($mylb.BackendAddressPools[1]);

$mylb = $mylb | Set-AzLoadBalancer

$nic1 | Set-AzNetworkInterface
$nic2 | Set-AzNetworkInterface
```

13. Por último, debe configurar los registros de recursos DNS para que apunten a la dirección IP de front-end correspondiente del equilibrador de carga. Puede hospedar los dominios en Azure DNS. Para más información sobre el uso de Azure DNS con Load Balancer, consulte [Uso de Azure DNS con otros servicios de Azure](#).

Pasos siguientes

- Aprenda más sobre cómo combinar servicios de equilibrio de carga en Azure en [Uso de servicios de equilibrio de carga de Azure](#).
- Obtenga información sobre cómo usar diferentes tipos de registros en Azure para administrar y solucionar los problemas del equilibrador de carga en [Registros de Azure Monitor para Azure Load Balancer](#).

Traslado de un equilibrador de carga externo a otra región mediante Azure Portal

23/09/2020 • 20 minutes to read • [Edit Online](#)

Hay varios escenarios en los que quizá quiera trasladar un equilibrador de carga externo de una región a otra. Por ejemplo, puede que quiera crear otro equilibrador de carga externo con la misma configuración para realizar pruebas. También es posible que quiera trasladar un equilibrador de carga externo a otra región como parte del planeamiento para la recuperación ante desastres.

En un sentido literal, no se puede trasladar un equilibrador de carga externo de Azure de una región a otra. Aunque se puede usar una plantilla de Azure Resource Manager para exportar la configuración y dirección IP pública actuales de un equilibrador de carga externo. Después, puede preparar el recurso para otra región al exportar el equilibrador de carga y la dirección IP pública a una plantilla, modificar los parámetros para que coincidan con la región de destino y, a continuación, implementar la plantilla en la nueva región. Para más información sobre Resource Manager y sus plantillas, consulte [Exportación de grupos de recursos a plantillas](#).

Prerequisitos

- Asegúrese de que el equilibrador de carga externo de Azure se encuentra en la región de Azure desde la que va a realizar el traslado.
- Los equilibradores de carga externos de Azure no se pueden trasladar entre regiones. Tendrá que asociar el nuevo equilibrador de carga a los recursos de la región de destino.
- Deberá tener asignado el rol de colaborador de red u otro superior para exportar la configuración de un equilibrador de carga externo e implementar una plantilla para crear un equilibrador de carga externo en otra región.
- Identifique el diseño de red de origen y todos los recursos que está usando actualmente. Este diseño incluye, entre otros, equilibradores de carga, grupos de seguridad de red (NSG), direcciones IP públicas y redes virtuales.
- Compruebe que la suscripción a Azure permite crear equilibradores de carga externos en la región de destino. Para habilitar la cuota necesaria, póngase en contacto con el soporte técnico.
- Asegúrese de que la suscripción tiene suficientes recursos para admitir la adición de equilibradores de carga. Vea [Límites, cuotas y restricciones de suscripción y servicios de Microsoft Azure](#).

Preparación y traslado

En los procedimientos siguientes se muestra cómo preparar el equilibrador de carga externo para el traslado mediante una plantilla de Resource Manager y cómo trasladar la configuración del equilibrador de carga externo a la región de destino mediante Azure Portal. En primer lugar, debe exportar la configuración de IP pública del equilibrador de carga externo.

NOTE

Este artículo se ha actualizado para usar el nuevo módulo Az de Azure PowerShell. Aún puede usar el módulo de AzureRM que continuará recibiendo correcciones de errores hasta diciembre de 2020 como mínimo. Para más información acerca del nuevo módulo Az y la compatibilidad con AzureRM, consulte [Introducing the new Azure PowerShell Az module](#) (Presentación del nuevo módulo Az de Azure PowerShell). Para obtener instrucciones sobre la instalación del módulo Az, consulte [Instalación de Azure PowerShell](#).

Exportación de la plantilla de la dirección IP pública e implementación desde el portal

1. Inicie sesión en [Azure Portal](#) y después seleccione **Grupos de recursos**.
2. Busque el grupo de recursos que contiene la dirección IP pública de origen y selecciónelo.
3. Seleccione **Configuración** > **Exportar plantilla**.
4. Seleccione **Implementar** en **Exportar plantilla**.
5. Seleccione **PLANTILLA** > **Editar parámetros** para abrir el archivo parameters.json en el editor en línea.
6. Para editar el parámetro del nombre de la dirección IP pública, cambie la propiedad **value** en **parameters** del nombre de la dirección IP pública de origen al nombre de la dirección IP pública de destino. Escriba el nombre entre comillas.

```
{
  "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentParameters.json#",
  "contentVersion": "1.0.0.0",
  "parameters": {
    "publicIPAddresses_myVM1pubIP_name": {
      "value": "<target-publicip-name>"
    }
  }
}
```

Seleccione **Guardar** en el editor.

7. Seleccione **PLANTILLA** > **Editar plantilla** para abrir el archivo template.json en el editor en línea.
8. Para editar la región de destino a la que se va a trasladar la dirección IP pública, cambie la propiedad **location** en **resources**:

```

"resources": [
  {
    "type": "Microsoft.Network/publicIPAddresses",
    "apiVersion": "2019-06-01",
    "name": "[parameters('publicIPAddresses_myPubIP_name')]",
    "location": "<target-region>",
    "sku": {
      "name": "Basic",
      "tier": "Regional"
    },
    "properties": {
      "provisioningState": "Succeeded",
      "resourceGuid": "7549a8f1-80c2-481a-a073-018f5b0b69be",
      "ipAddress": "52.177.6.204",
      "publicIPAddressVersion": "IPv4",
      "publicIPAllocationMethod": "Dynamic",
      "idleTimeoutInMinutes": 4,
      "ipTags": []
    }
  }
]

```

Para obtener los códigos de ubicación de la región, consulte [Ubicaciones de Azure](#). El código de una región es el nombre de la región sin espacios. Por ejemplo, el código de Centro de EE. UU. es **centralus**.

9. También puede cambiar otros parámetros de la plantilla si quiere o tiene que hacerlo, según sus requisitos:

- **SKU.** Puede cambiar la SKU de la dirección IP pública de la configuración de estándar a básica o viceversa modificando la propiedad **name** en **sku** en el archivo `template.json`:

```

"resources": [
  {
    "type": "Microsoft.Network/publicIPAddresses",
    "apiVersion": "2019-06-01",
    "name": "[parameters('publicIPAddresses_myPubIP_name')]",
    "location": "<target-region>",
    "sku": {
      "name": "Basic",
      "tier": "Regional"
    },
  },
]

```

Para obtener información sobre las diferencias entre las IP públicas de la SKU básica y estándar, consulte [Creación, modificación o eliminación de una dirección IP pública](#).

- **Método de asignación de IP pública y Tiempo de espera de inactividad.** Puede cambiar el método de asignación de IP pública cambiando la propiedad **publicIPAllocationMethod** de **Dynamic** a **Static** o de **Static** a **Dynamic**. Puede cambiar el tiempo de espera de inactividad cambiando la propiedad **idleTimeoutInMinutes** al valor deseado. El valor predeterminado es **4**.


```

"resources": [
{
  "type": "Microsoft.Network/publicIPAddresses",
  "apiVersion": "2019-06-01",
  "name": "[parameters('publicIPAddresses_myPubIP_name')]",
  "location": "<target-region>",
  "sku": {
    "name": "Basic",
    "tier": "Regional"
  },
  "properties": {
    "provisioningState": "Succeeded",
    "resourceGuid": "7549a8f1-80c2-481a-a073-018f5b0b69be",
    "ipAddress": "52.177.6.204",
    "publicIPAddressVersion": "IPv4",
    "publicIPAllocationMethod": "Dynamic",
    "idleTimeoutInMinutes": 4,
    "ipTags": []
  }
},

```

Para obtener información sobre los métodos de asignación y los valores de tiempo de espera de inactividad, consulte [Creación, modificación o eliminación de una dirección IP pública](#).

10. Seleccione **Guardar** en el editor en línea.
11. Seleccione **ASPECTOS BÁSICOS > Suscripción** para elegir la suscripción donde se implementará la dirección IP pública de destino.
12. Seleccione **ASPECTOS BÁSICOS > Grupo de recursos** para elegir el grupo de recursos donde se implementará la dirección IP pública de destino. Puede seleccionar **Crear nuevo** para crear un grupo de recursos para la dirección IP pública de destino. Asegúrese de que el nombre no sea el mismo que el del grupo de recursos de origen de la dirección IP pública de origen existente.
13. Compruebe que **ASPECTOS BÁSICOS > Ubicación** está establecido en la ubicación de destino en la que quiere que se implemente la dirección IP pública.
14. En **CONFIGURACIÓN**, compruebe que el nombre coincide con el nombre que especificó anteriormente en el editor de parámetros.
15. Active la casilla **TÉRMINOS Y CONDICIONES**.
16. Seleccione **Comprar** para implementar la dirección IP pública de destino.
17. Si tiene otra dirección IP pública que se usa como NAT de salida del equilibrador de carga que se traslada, repita los pasos anteriores para exportar e implementar la segunda dirección IP pública de salida en la región de destino.

Exportación de la plantilla del equilibrador de carga externo e implementación del equilibrador de carga desde Azure Portal

1. Inicie sesión en [Azure Portal](#) y después seleccione **Grupos de recursos**.
2. Busque el grupo de recursos que contiene el equilibrador de carga externo de origen y selecciónelo.
3. Seleccione **Configuración > Exportar plantilla**.
4. Seleccione **Implementar** en **Exportar plantilla**.
5. Seleccione **PLANTILLA > Editar parámetros** para abrir el archivo parameters.json en el editor en línea.
6. Para modificar el parámetro del nombre del equilibrador de carga externo, cambie la propiedad **value** del nombre del equilibrador de carga externo de origen por el nombre del equilibrador de carga externo de destino. Escriba el nombre entre comillas.

```

"$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentParameters.json#",
"contentVersion": "1.0.0.0",
"parameters": {
  "loadBalancers_myLoadbalancer_ext_name": {
    "value": "<target-external-lb-name>"
  },
  "publicIPAddresses_myPubIP_in_externalid": {
    "value": "<target-publicIP-resource-ID>"
  },
}

```

7. Para modificar el valor de la dirección IP pública de destino que trasladó en los pasos anteriores, debe obtener primero el identificador de recurso y luego pegarlo en el archivo parameters.json. Para obtener el identificador realice lo siguiente:

- En otra pestaña o ventana del explorador, inicie sesión en [Azure Portal](#) y seleccione **Grupos de recursos**.
- Busque el grupo de recursos de destino que contiene la IP pública que trasladó en los pasos anteriores. Selecciónelo.
- Seleccione **Configuración > Propiedades**.
- En la hoja de la derecha, resalte **Id. de recurso** y cópielo en el Portapapeles. También puede seleccionar **Copiar al Portapapeles** a la derecha de la ruta de acceso del **Id. de recurso**.
- Pegue el identificador de recurso en la propiedad **value** del editor **Editar parámetros** que está abierto en la otra ventana o pestaña del explorador:

```

```json
"$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentParameters.json#",
"contentVersion": "1.0.0.0",
"parameters": {
 "loadBalancers_myLoadbalancer_ext_name": {
 "value": "<target-external-lb-name>"
 },
 "publicIPAddresses_myPubIP_in_externalid": {
 "value": "<target-publicIP-resource-ID>"
 },
}

```

- Seleccione **Guardar** en el editor en línea.
8. Si ha configurado reglas de salida y NAT de salida para el equilibrador de carga, verá una tercera entrada en este archivo para el identificador externo de la IP pública de salida. Repita los pasos anteriores en la región **target** para obtener el identificador de la dirección IP pública de salida. Péguelo en el archivo parameters.json:

```

"$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
"contentVersion": "1.0.0.0",
"parameters": {
 "loadBalancers_myLoadbalancer_ext_name": {
 "value": "<target-external-lb-name>",
 },
 "publicIPAddresses_myPubIP_in_externalid": {
 "value": "<target-publicIP-resource-ID>",
 },
 "publicIPAddresses_myPubIP_out_externalid": {
 "defaultValue": "<target-publicIP-outbound-resource-ID>",
 }
},

```

9. Seleccione **PLANTILLA > Editar plantilla** para abrir el archivo template.json en el editor en línea.
10. Para editar la región de destino a la que se va a trasladar la configuración del equilibrador de carga externo, cambie la propiedad **location** en **resources** del archivo template.json:

```

"resources": [
 {
 "type": "Microsoft.Network/loadBalancers",
 "apiVersion": "2019-06-01",
 "name": "[parameters('loadBalancers_myLoadBalancer_name')]",
 "location": "<target-external-lb-region>",
 "sku": {
 "name": "Standard",
 "tier": "Regional"
 }
 },

```

11. Para obtener los códigos de ubicación de la región, consulte [Ubicaciones de Azure](#). El código de una región es el nombre de la región sin espacios. Por ejemplo, el código de Centro de EE. UU. es **centralus**.
12. También puede cambiar otros parámetros de la plantilla si quiere o tiene que hacerlo, según sus requisitos:
  - **SKU**. Puede cambiar la SKU del equilibrador de carga externo de la configuración de estándar a básica o viceversa modificando la propiedad **name** en **sku** en el archivo template.json:

```

"resources": [
 {
 "type": "Microsoft.Network/loadBalancers",
 "apiVersion": "2019-06-01",
 "name": "[parameters('loadBalancers_myLoadBalancer_name')]",
 "location": "<target-external-lb-region>",
 "sku": {
 "name": "Standard",
 "tier": "Regional"
 }
 },

```

Para obtener información sobre las diferencias entre los equilibradores de carga de la SKU básica y estándar, consulte [Introducción a Azure Standard Load Balancer](#).

- **Reglas de equilibrio de carga**. Puede agregar o quitar reglas de equilibrio de carga de la configuración agregando o quitando entradas en la sección **loadBalancingRules** del archivo template.json:

```

"loadBalancingRules": [
 {
 "name": "myInboundRule",
 "etag": "W/\"39e5e9cd-2d6d-491f-83cf-b37a259d86b6\"",
 "properties": {
 "provisioningState": "Succeeded",
 "frontendIPConfiguration": {
 "id": "[concat(resourceId('Microsoft.Network/loadBalancers',
parameters('loadBalancers_myLoadBalancer_name')),
'/frontendIPConfigurations/myfrontendIPinbound')]"
 },
 "frontendPort": 80,
 "backendPort": 80,
 "enableFloatingIP": false,
 "idleTimeoutInMinutes": 4,
 "protocol": "Tcp",
 "enableTcpReset": false,
 "loadDistribution": "Default",
 "disableOutboundSnat": true,
 "backendAddressPool": {
 "id": "[concat(resourceId('Microsoft.Network/loadBalancers',
parameters('loadBalancers_myLoadBalancer_name')), '/backendAddressPools/myBEPoolInbound')]"
 },
 "probe": {
 "id": "[concat(resourceId('Microsoft.Network/loadBalancers',
parameters('loadBalancers_myLoadBalancer_name')), '/probes/myHTTPProbe')]"
 }
 }
 }
]

```

Para obtener información sobre las reglas de equilibrio de carga, consulte [¿Qué es Azure Load Balancer?](#)

- **Sondeos.** Puede agregar o quitar sondeos del equilibrador de carga en la configuración agregando o quitando entradas en la sección **probes** del archivo template.json:

```

"probes": [
 {
 "name": "myHTTPProbe",
 "etag": "W/\"39e5e9cd-2d6d-491f-83cf-b37a259d86b6\"",
 "properties": {
 "provisioningState": "Succeeded",
 "protocol": "Http",
 "port": 80,
 "requestPath": "/",
 "intervalInSeconds": 15,
 "numberOfProbes": 2
 }
 }
],

```

Para más información, consulte [Sondeos de estado de Load Balancer](#).

- **Reglas NAT de entrada.** Puede agregar o quitar reglas NAT de entrada del equilibrador de carga agregando o quitando entradas en la sección **inboundNatRules** del archivo template.json:

```

"inboundNatRules": [
 {
 "name": "myInboundNATRule",
 "etag": "W/\"39e5e9cd-2d6d-491f-83cf-b37a259d86b6\"",
 "properties": {
 "provisioningState": "Succeeded",
 "frontendIPConfiguration": {
 "id": "[concat(resourceId('Microsoft.Network/loadBalancers',
parameters('loadBalancers_myLoadBalancer_name')),
'/frontendIPConfigurations/myfrontendIPinbound')]"
 },
 "frontendPort": 4422,
 "backendPort": 3389,
 "enableFloatingIP": false,
 "idleTimeoutInMinutes": 4,
 "protocol": "Tcp",
 "enableTcpReset": false
 }
 }
]

```

Para completar la adición o eliminación de una regla NAT de entrada, esta debe agregarse o quitarse como propiedad **type** al final del archivo template.json:

```

{
 "type": "Microsoft.Network/loadBalancers/inboundNatRules",
 "apiVersion": "2019-06-01",
 "name": "[concat(parameters('loadBalancers_myLoadBalancer_name'), '/myInboundNATRule')]",
 "dependsOn": [
 "[resourceId('Microsoft.Network/loadBalancers',
parameters('loadBalancers_myLoadBalancer_name'))]"
],
 "properties": {
 "provisioningState": "Succeeded",
 "frontendIPConfiguration": {
 "id": "[concat(resourceId('Microsoft.Network/loadBalancers',
parameters('loadBalancers_myLoadBalancer_name')),
'/frontendIPConfigurations/myfrontendIPinbound')]"
 },
 "frontendPort": 4422,
 "backendPort": 3389,
 "enableFloatingIP": false,
 "idleTimeoutInMinutes": 4,
 "protocol": "Tcp",
 "enableTcpReset": false
 }
}

```

Para obtener información sobre las reglas NAT de entrada, consulte [¿Qué es Azure Load Balancer?](#)

- **Reglas de salida.** Puede agregar o quitar reglas de salida de la configuración editando la propiedad **outboundRules** en el archivo template.json:

```

"outboundRules": [
 {
 "name": "myOutboundRule",
 "etag": "W/\"39e5e9cd-2d6d-491f-83cf-b37a259d86b6\"",
 "properties": {
 "provisioningState": "Succeeded",
 "allocatedOutboundPorts": 10000,
 "protocol": "All",
 "enableTcpReset": false,
 "idleTimeoutInMinutes": 15,
 "backendAddressPool": {
 "id": "[concat(resourceId('Microsoft.Network/loadBalancers',
parameters('loadBalancers_myLoadBalancer_name')), '/backendAddressPools/myBEPoolOutbound')]"
 },
 "frontendIPConfigurations": [
 {
 "id": "[concat(resourceId('Microsoft.Network/loadBalancers',
parameters('loadBalancers_myLoadBalancer_name')),
'/frontendIPConfigurations/myFrontendIPOutbound')]"
 }
]
 }
 }
]

```

Para más información, consulte [Reglas de salida de Load Balancer](#).

13. Seleccione **Guardar** en el editor en línea.
14. Seleccione **ASPECTOS BÁSICOS > Suscripción** para elegir la suscripción en la que se implementará el equilibrador de carga externo de destino.
15. Seleccione **ASPECTOS BÁSICOS > Grupo de recursos** para elegir el grupo de recursos en el que se implementará el equilibrador de carga de destino. Puede seleccionar **Crear nuevo** para crear un grupo de recursos para el equilibrador de carga externo de destino. También puede elegir el grupo de recursos existente que creó anteriormente para la dirección IP pública. Asegúrese de que el nombre no es el mismo que el del grupo de recursos de origen del equilibrador de carga externo de origen existente.
16. Compruebe que **ASPECTOS BÁSICOS > Ubicación** está establecido en la ubicación de destino en la que quiere implementar el equilibrador de carga externo.
17. En **CONFIGURACIÓN**, compruebe que el nombre coincide con el nombre que especificó anteriormente en el editor de parámetros. Compruebe que los identificadores de recursos estén especificados para todas las direcciones IP públicas en la configuración.
18. Active la casilla **TÉRMINOS Y CONDICIONES**.
19. Seleccione **Comprar** para implementar la dirección IP pública de destino.

## Discard (Descartar)

Si quiere descartar la dirección IP pública de destino y el equilibrador de carga externo, elimine el grupo de recursos que los contiene. Para ello, en el portal, seleccione el grupo de recursos en el panel y, luego, **Eliminar** en la parte superior de la página de información general.

## Limpieza

Para confirmar los cambios y completar el traslado de la dirección IP pública y el equilibrador de carga externo, elimine la dirección IP pública de origen y el equilibrador de carga externo o el grupo de recursos. Para ello, en el portal, seleccione ese grupo de recursos en el panel y luego seleccione **Eliminar** en la parte superior de cada

página.

## Pasos siguientes

En este tutorial, ha migrado un equilibrador de carga externo de Azure de una región a otra y ha limpiado los recursos de origen. Para más información sobre el traslado de recursos entre regiones y la recuperación ante desastres en Azure, consulte:

- [Traslado de los recursos a un nuevo grupo de recursos o a una nueva suscripción](#)
- [Traslado de máquinas virtuales de Azure a otra región](#)

# Traslado de un equilibrador de carga externo de Azure a otra región mediante Azure PowerShell

23/09/2020 • 19 minutes to read • [Edit Online](#)

Hay varios escenarios en los que quizá quiera trasladar su equilibrador de carga externo actual de una región a otra. Por ejemplo, puede que quiera crear un equilibrador de carga externo con la misma configuración para realizar pruebas. También puede que quiera trasladar un equilibrador de carga externo a otra región como parte del planeamiento para la recuperación ante desastres.

Los equilibradores de carga externos de Azure no se pueden trasladar de una región a otra. Sin embargo, puede usar una plantilla de Azure Resource Manager para exportar la configuración y dirección IP pública actuales de un equilibrador de carga externo. Después, puede preparar el recurso para otra región al exportar el equilibrador de carga y la dirección IP pública a una plantilla, modificar los parámetros para que coincidan con la región de destino y, a continuación, implementar la plantilla en la nueva región. Para más información sobre Resource Manager y sus plantillas, consulte [Exportación de grupos de recursos a plantillas](#).

## Requisitos previos

- Asegúrese de que el equilibrador de carga externo de Azure se encuentra en la región de Azure desde la que va a realizar el traslado.
- Los equilibradores de carga externos de Azure no se pueden trasladar entre regiones. Tendrá que asociar el nuevo equilibrador de carga a los recursos de la región de destino.
- Necesitará contar con el rol de colaborador de red u otro superior para exportar la configuración de un equilibrador de carga externo e implementar una plantilla para crear un equilibrador de carga externo en otra región.
- Identifique el diseño de red de origen y todos los recursos que está usando actualmente. Este diseño incluye, entre otros, equilibradores de carga, grupos de seguridad de red (NSG), direcciones IP públicas y redes virtuales.
- Compruebe que la suscripción a Azure permite crear equilibradores de carga externos en la región de destino que se usa. Para habilitar la cuota necesaria, póngase en contacto con el soporte técnico.
- Asegúrese de que la suscripción tiene suficientes recursos para admitir la adición de equilibradores de carga para este proceso. Vea [Límites, cuotas y restricciones de suscripción y servicios de Microsoft Azure](#)

## Preparación y traslado

En los pasos siguientes se muestra cómo preparar el equilibrador de carga externo para el traslado mediante una plantilla de Resource Manager y cómo trasladar la configuración del equilibrador de carga externo a la región de destino mediante Azure PowerShell. Como parte de este proceso, debe incluirse y crearse la configuración de la dirección IP pública del equilibrador de carga externo antes de trasladarlo.



## NOTE

Este artículo se ha actualizado para usar el nuevo módulo Az de Azure PowerShell. Aún puede usar el módulo de AzureRM que continuará recibiendo correcciones de errores hasta diciembre de 2020 como mínimo. Para más información acerca del nuevo módulo Az y la compatibilidad con AzureRM, consulte [Introducing the new Azure PowerShell Az module](#) (Presentación del nuevo módulo Az de Azure PowerShell). Para obtener instrucciones sobre la instalación del módulo Az, consulte [Instalación de Azure PowerShell](#).

## Exportación de la plantilla de la dirección IP pública e implementación desde Azure PowerShell

1. Inicie sesión en la suscripción a Azure con el comando [Connect-AzAccount](#) y siga las instrucciones de la pantalla:

```
Connect-AzAccount
```

2. Obtenga el Id. de recurso de la dirección IP pública que quiere trasladar a la región de destino y colóquelo en una variable mediante [Get-AzPublicIpAddress](#):

```
$sourcePubIPID = (Get-AzPublicIpAddress -Name <source-public-ip-name> -ResourceGroupName <source-resource-group-name>).Id
```

3. Exporte la IP pública de origen a un archivo .json en el directorio donde se ejecuta el comando [Export-AzResourceGroup](#):

```
Export-AzResourceGroup -ResourceGroupName <source-resource-group-name> -Resource $sourceVNETID -IncludeParameterDefaultValue
```

4. El nombre del archivo descargado se asignará en función del grupo de recursos desde el que se exportó el recurso. Busque el archivo que se exportó con el comando denominado **<resource-group-name>.json** y ábralo en el editor que prefiera:

```
notepad.exe <source-resource-group-name>.json
```

5. Para editar el parámetro del nombre de la dirección IP pública, cambie el valor **defaultValue** de la propiedad del nombre de la IP pública de origen por el nombre de la dirección IP pública de destino. Asegúrese de que el nombre se encuentra entre comillas:

```
{
 "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
 "contentVersion": "1.0.0.0",
 "parameters": {
 "publicIPAddresses_myVM1pubIP_name": {
 "defaultValue": "<target-publicip-name>",
 "type": "String"
 }
 }
}
```

6. Para editar la región de destino a la que se va a trasladar la dirección IP pública, cambie la propiedad **location** en resources:

```

"resources": [
 {
 "type": "Microsoft.Network/publicIPAddresses",
 "apiVersion": "2019-06-01",
 "name": "[parameters('publicIPAddresses_myPubIP_name')]",
 "location": "<target-region>",
 "sku": {
 "name": "Basic",
 "tier": "Regional"
 },
 "properties": {
 "provisioningState": "Succeeded",
 "resourceGuid": "7549a8f1-80c2-481a-a073-018f5b0b69be",
 "ipAddress": "52.177.6.204",
 "publicIPAddressVersion": "IPv4",
 "publicIPAllocationMethod": "Dynamic",
 "idleTimeoutInMinutes": 4,
 "ipTags": []
 }
 }
]

```

7. Para obtener los códigos de ubicación de la región, puede usar el cmdlet Azure PowerShell [Get-AzLocation](#) al ejecutar el siguiente comando:

```
Get-AzLocation | format-table
```

8. También puede cambiar otros parámetros de la plantilla si así lo desea; son opcionales según sus requisitos:

- **SKU:** puede cambiar la SKU de la dirección IP pública de la configuración de estándar a básica o viceversa modificando la propiedad **sku > name** en el archivo **<resource-group-name>.json**:

```

"resources": [
 {
 "type": "Microsoft.Network/publicIPAddresses",
 "apiVersion": "2019-06-01",
 "name": "[parameters('publicIPAddresses_myPubIP_name')]",
 "location": "<target-region>",
 "sku": {
 "name": "Basic",
 "tier": "Regional"
 },
 },
]

```

Para más información sobre las diferencias entre las IP públicas de la SKU básica y estándar, consulte [Creación, modificación o eliminación de una dirección IP pública](#).

- **Método de asignación de IP pública y tiempo de espera de inactividad:** puede cambiar estas dos opciones en la plantilla si cambia la propiedad **publicIPAllocationMethod** de **Dynamic** a **Static** o bien de **Static** a **Dynamic**. El tiempo de espera de inactividad se puede cambiar modificando la propiedad **idleTimeoutInMinutes** con la cantidad deseada. El valor predeterminado es **4**:

```
"resources": [
 {
 "type": "Microsoft.Network/publicIPAddresses",
 "apiVersion": "2019-06-01",
 "name": "[parameters('publicIPAddresses_myPubIP_name')]",
 "location": "<target-region>",
 "sku": {
 "name": "Basic",
 "tier": "Regional"
 },
 "properties": {
 "provisioningState": "Succeeded",
 "resourceGuid": "7549a8f1-80c2-481a-a073-018f5b0b69be",
 "ipAddress": "52.177.6.204",
 "publicIPAddressVersion": "IPv4",
 "publicIPAllocationMethod": "Dynamic",
 "idleTimeoutInMinutes": 4,
 "ipTags": []
 }
 }
]
```

Para más información sobre los métodos de asignación y los valores de tiempo de espera de inactividad, consulte [Creación, modificación o eliminación de una dirección IP pública](#).

9. Guarde el archivo **<resource-group-name>.json**.
10. Cree un grupo de recursos en la región de destino para la dirección IP pública de destino que se va a implementar mediante [New-AzResourceGroup](#).

```
New-AzResourceGroup -Name <target-resource-group-name> -location <target-region>
```

11. Implemente el archivo **<resource-group-name>.json** editado en el grupo de recursos que creó en el paso anterior mediante [New-AzResourceGroupDeployment](#):

```
New-AzResourceGroupDeployment -ResourceGroupName <target-resource-group-name> -TemplateFile <source-resource-group-name>.json
```

12. Para comprobar que los recursos se crearon en la región de destino, use los comandos [Get-AzResourceGroup](#) y [Get-AzPublicIpAddress](#):

```
Get-AzResourceGroup -Name <target-resource-group-name>
```

```
Get-AzPublicIpAddress -Name <target-publicip-name> -ResourceGroupName <target-resource-group-name>
```

## Exportación de la plantilla del equilibrador de carga externo e implementación desde Azure PowerShell

1. Inicie sesión en la suscripción a Azure con el comando [Connect-AzAccount](#) y siga las instrucciones de la pantalla:

```
Connect-AzAccount
```

- Obtenga el identificador del recurso del equilibrador de carga externo que quiere trasladar a la región de destino y colóquelo en una variable mediante [Get-AzLoadBalancer](#):

```
$sourceExtLBID = (Get-AzLoadBalancer -Name <source-external-lb-name> -ResourceGroupName <source-resource-group-name>).Id
```

- Exporte la configuración del equilibrador de carga externo de origen a un archivo .json en el directorio donde se ejecuta el comando [Export-AzResourceGroup](#):

```
Export-AzResourceGroup -ResourceGroupName <source-resource-group-name> -Resource $sourceExtLBID -IncludeParameterDefaultValue
```

- El nombre del archivo descargado se asignará en función del grupo de recursos desde el que se exportó el recurso. Busque el archivo que se exportó con el comando denominado **<resource-group-name>.json** y ábralo en el editor que prefiera:

```
notepad.exe <source-resource-group-name>.json
```

- Para editar el parámetro del nombre del equilibrador de carga externo, cambie la propiedad **defaultValue** del nombre del equilibrador de carga externo de origen por el nombre del equilibrador de carga externo de destino. Asegúrese de que el nombre se encuentra entre comillas:

```
"$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
"contentVersion": "1.0.0.0",
"parameters": {
 "loadBalancers_myLoadbalancer_ext_name": {
 "defaultValue": "<target-external-lb-name>",
 "type": "String"
 },
 "publicIPAddresses_myPubIP_in_externalid": {
 "defaultValue": "<target-publicIP-resource-ID>",
 "type": "String"
 },
}
```

- Para modificar el valor de la dirección IP pública de destino que se ha trasladado antes, primero debe obtener el identificador de recurso y, a continuación, copiarlo y pegarlo en el archivo **<resource-group-name>.json**. Para obtener el identificador, use [Get-AzPublicIPAddress](#):

```
$targetPubIPID = (Get-AzPublicIPAddress -Name <target-public-ip-name> -ResourceGroupName <target-resource-group-name>).Id
```

Escriba la variable y presione ENTRAR para mostrar el identificador del recurso. Resalte la ruta de acceso del identificador y cópiela en el portapapeles:

```
PS C:\> $targetPubIPID
/subscriptions/7668d659-17fc-4ffd-85ba-9de61fe977e8/resourceGroups/myResourceGroupLB-
Move/providers/Microsoft.Network/publicIPAddresses/myPubIP-in-move
```

- En el archivo **<resource-group-name>.json**, pegue el **identificador del recurso** de la variable en lugar del valor **defaultValue** en el segundo parámetro del identificador externo de la IP pública y, después, asegúrese de escribir la ruta de acceso entre comillas:

```

"$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
"contentVersion": "1.0.0.0",
"parameters": {
 "loadBalancers_myLoadbalancer_ext_name": {
 "defaultValue": "<target-external-lb-name>",
 "type": "String"
 },
 "publicIPAddresses_myPubIP_in_externalid": {
 "defaultValue": "<target-publicIP-resource-ID>",
 "type": "String"
 },
}

```

8. Si ha configurado las reglas de salida y NAT de salida para el equilibrador de carga, en este archivo habrá una tercera entrada para el identificador externo de la IP pública saliente. Repita los pasos anteriores en la **región de destino** para obtener el identificador de la dirección IP pública de salida y pegue esa entrada en el archivo **<resource-group-name>.json**:

```

"$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
"contentVersion": "1.0.0.0",
"parameters": {
 "loadBalancers_myLoadbalancer_ext_name": {
 "defaultValue": "<target-external-lb-name>",
 "type": "String"
 },
 "publicIPAddresses_myPubIP_in_externalid": {
 "defaultValue": "<target-publicIP-resource-ID>",
 "type": "String"
 },
 "publicIPAddresses_myPubIP_out_externalid": {
 "defaultValue": "<target-publicIP-outbound-resource-ID>",
 "type": "String"
 },
}

```

9. Para editar la región de destino a la que se va a trasladar la configuración del equilibrador de carga externo, cambie la propiedad **location** en **resources** del archivo **<resource-group-name>.json**:

```

"resources": [
 {
 "type": "Microsoft.Network/loadBalancers",
 "apiVersion": "2019-06-01",
 "name": "[parameters('loadBalancers_myLoadBalancer_name')]",
 "location": "<target-external-lb-region>",
 "sku": {
 "name": "Standard",
 "tier": "Regional"
 },
 },
]

```

10. Para obtener los códigos de ubicación de la región, puede usar el cmdlet Azure PowerShell [Get-AzLocation](#) al ejecutar el siguiente comando:

```
Get-AzLocation | format-table
```

11. También puede cambiar otros parámetros de la plantilla si así lo desea; son opcionales según sus requisitos:

- **SKU**: puede cambiar la SKU del equilibrador de carga externo en la configuración del nivel estándar al

básico o viceversa si modifica la propiedad `sku > name` en el archivo `<resource-group-name>.json`:

```
"resources": [
{
 "type": "Microsoft.Network/loadBalancers",
 "apiVersion": "2019-06-01",
 "name": "[parameters('loadBalancers_myLoadBalancer_name')]",
 "location": "<target-external-lb-region>",
 "sku": {
 "name": "Standard",
 "tier": "Regional"
 },
},
```

Para más información sobre las diferencias entre los equilibradores de carga de la SKU básica y estándar, consulte [Introducción a Azure Standard Load Balancer](#).

- **Reglas de equilibrio de carga:** puede agregar o quitar reglas de equilibrio de carga en la configuración agregando o quitando entradas en la sección `loadBalancingRules` del archivo `<resource-group-name>.json`:

```
"loadBalancingRules": [
 {
 "name": "myInboundRule",
 "etag": "W/\"39e5e9cd-2d6d-491f-83cf-b37a259d86b6\"",
 "properties": {
 "provisioningState": "Succeeded",
 "frontendIPConfiguration": {
 "id": "[concat(resourceId('Microsoft.Network/loadBalancers',
parameters('loadBalancers_myLoadBalancer_name')),
'/frontendIPConfigurations/myfrontendIPinbound')]"
 },
 "frontendPort": 80,
 "backendPort": 80,
 "enableFloatingIP": false,
 "idleTimeoutInMinutes": 4,
 "protocol": "Tcp",
 "enableTcpReset": false,
 "loadDistribution": "Default",
 "disableOutboundSnat": true,
 "backendAddressPool": {
 "id": "[concat(resourceId('Microsoft.Network/loadBalancers',
parameters('loadBalancers_myLoadBalancer_name')), '/backendAddressPools/myBEPoolInbound')]"
 },
 "probe": {
 "id": "[concat(resourceId('Microsoft.Network/loadBalancers',
parameters('loadBalancers_myLoadBalancer_name')), '/probes/myHTTPProbe')]"
 }
 }
 }
]
```

Para más información sobre las reglas de equilibrio de carga, consulte [¿Qué es Azure Load Balancer?](#)

- **Sondeos:** puede agregar o quitar sondeos para el equilibrador de carga en la configuración agregando o quitando entradas en la sección `probes` del archivo `<resource-group-name>.json` :

```

"probes": [
 {
 "name": "myHTTPProbe",
 "etag": "W/\"39e5e9cd-2d6d-491f-83cf-b37a259d86b6\"",
 "properties": {
 "provisioningState": "Succeeded",
 "protocol": "Http",
 "port": 80,
 "requestPath": "/",
 "intervalInSeconds": 15,
 "numberOfProbes": 2
 }
 }
],

```

Para más información sobre los sondeos de estado de Azure Load Balancer, consulte [Sondeos de estado de Load Balancer](#).

- **Reglas NAT de entrada:** puede agregar o quitar reglas NAT de entrada para el equilibrador de carga agregando o quitando entradas en la sección `inboundNatRules` del archivo `<resource-group-name>.json` :

```

"inboundNatRules": [
 {
 "name": "myInboundNATRule",
 "etag": "W/\"39e5e9cd-2d6d-491f-83cf-b37a259d86b6\"",
 "properties": {
 "provisioningState": "Succeeded",
 "frontendIPConfiguration": {
 "id": "[concat(resourceId('Microsoft.Network/loadBalancers',
parameters('loadBalancers_myLoadBalancer_name')),
'/frontendIPConfigurations/myfrontendIPinbound')]"
 },
 "frontendPort": 4422,
 "backendPort": 3389,
 "enableFloatingIP": false,
 "idleTimeoutInMinutes": 4,
 "protocol": "Tcp",
 "enableTcpReset": false
 }
 }
]

```

Para completar la adición o eliminación de una regla NAT de entrada, esta debe agregarse o quitarse como propiedad `type` al final del archivo `<resource-group-name>.json`:

```
{
 "type": "Microsoft.Network/loadBalancers/inboundNatRules",
 "apiVersion": "2019-06-01",
 "name": "[concat(parameters('loadBalancers_myLoadBalancer_name'), '/myInboundNATRule')]",
 "dependsOn": [
 "[resourceId('Microsoft.Network/loadBalancers',
parameters('loadBalancers_myLoadBalancer_name'))]"
],
 "properties": {
 "provisioningState": "Succeeded",
 "frontendIPConfiguration": {
 "id": "[concat(resourceId('Microsoft.Network/loadBalancers',
parameters('loadBalancers_myLoadBalancer_name')),
'/frontendIPConfigurations/myfrontendIPinbound')]"
 },
 "frontendPort": 4422,
 "backendPort": 3389,
 "enableFloatingIP": false,
 "idleTimeoutInMinutes": 4,
 "protocol": "Tcp",
 "enableTcpReset": false
 }
}
```

Para más información sobre las reglas NAT de entrada, consulte [¿Qué es Azure Load Balancer?](#)

- **Reglas de salida:** puede agregar o quitar reglas de salida en la configuración mediante la edición de la propiedad **outboundRules** en el archivo **<resource-group-name>.json** :

```
"outboundRules": [
 {
 "name": "myOutboundRule",
 "etag": "W/\"39e5e9cd-2d6d-491f-83cf-b37a259d86b6\"",
 "properties": {
 "provisioningState": "Succeeded",
 "allocatedOutboundPorts": 10000,
 "protocol": "All",
 "enableTcpReset": false,
 "idleTimeoutInMinutes": 15,
 "backendAddressPool": {
 "id": "[concat(resourceId('Microsoft.Network/loadBalancers',
parameters('loadBalancers_myLoadBalancer_name')), '/backendAddressPools/myBEPoolOutbound')]"
 },
 "frontendIPConfigurations": [
 {
 "id": "[concat(resourceId('Microsoft.Network/loadBalancers',
parameters('loadBalancers_myLoadBalancer_name')),
'/frontendIPConfigurations/myfrontendIPOutbound')]"
 }
]
 }
 }
]
```

Para más información sobre las reglas de salida, consulte [Reglas de salida de Load Balancer](#).

12. Guarde el archivo **<resource-group-name>.json**.
13. Cree un grupo de recursos en la región de destino para el equilibrador de carga externo de destino que se va a implementar mediante [New-AzResourceGroup](#). El grupo de recursos existente anterior también se puede reutilizar como parte de este proceso:



```
New-AzResourceGroup -Name <target-resource-group-name> -location <target-region>
```

14. Implemente el archivo **<resource-group-name>.json** editado en el grupo de recursos que creó en el paso anterior mediante [New-AzResourceGroupDeployment](#):

```
New-AzResourceGroupDeployment -ResourceGroupName <target-resource-group-name> -TemplateFile <source-resource-group-name>.json
```

15. Para comprobar que los recursos se crearon en la región de destino, use los comandos [Get-AzResourceGroup](#) y [Get-AzLoadBalancer](#):

```
Get-AzResourceGroup -Name <target-resource-group-name>
```

```
Get-AzLoadBalancer -Name <target-publicip-name> -ResourceGroupName <target-resource-group-name>
```

## Discard (Descartar)

Después de la implementación, si quiere empezar de nuevo o descartar la IP pública y el equilibrador de carga en el destino, elimine el grupo de recursos que se creó en el destino y se eliminará la IP pública y el equilibrador de carga trasladados. Para quitar el grupo de recursos, use [Remove-AzResourceGroup](#):

```
Remove-AzResourceGroup -Name <resource-group-name>
```

## Limpieza

Para confirmar los cambios y completar el traslado del NSG, elimine el NSG o el grupo de recursos de origen mediante [Remove-AzResourceGroup](#) o [Remove-AzPublicIpAddress](#) y [Remove-AzLoadBalancer](#)

```
Remove-AzResourceGroup -Name <resource-group-name>
```

```
Remove-AzLoadBalancer -name <load-balancer> -ResourceGroupName <resource-group-name>
```

```
Remove-AzPublicIpAddress -Name <public-ip> -ResourceGroupName <resource-group-name>
```

## Pasos siguientes

En este tutorial, ha movido un grupo de seguridad de red de Azure de una región a otra y ha limpiado los recursos de origen. Para obtener más información sobre cómo trasladar recursos entre regiones y la recuperación ante

desastres en Azure, consulte:

- [Traslado de los recursos a un nuevo grupo de recursos o a una nueva suscripción](#)
- [Traslado de máquinas virtuales de Azure a otra región](#)

# Traslado de equilibradores de carga internos de Azure a otra región mediante Azure Portal

23/09/2020 • 20 minutes to read • [Edit Online](#)

Hay varios escenarios en los que quizá quiera trasladar su equilibrador de carga interno actual de una región a otra. Por ejemplo, puede que quiera crear un equilibrador de carga interno con la misma configuración para realizar pruebas. También puede que quiera trasladar un equilibrador de carga interno a otra región como parte del planeamiento para la recuperación ante desastres.

Los equilibradores de carga internos de Azure no se pueden trasladar de una región a otra. Sin embargo, puede usar una plantilla de Azure Resource Manager para exportar la configuración y la red virtual actuales de un equilibrador de carga interno. Después, puede preparar el recurso para otra región al exportar el equilibrador de carga y la red virtual a una plantilla, modificar los parámetros para que coincidan con la región de destino y, a continuación, implementar la plantilla en la nueva región. Para más información sobre Resource Manager y las plantillas, consulte [Inicio rápido: Creación e implementación de plantillas de Azure Resource Manager mediante Azure Portal](#).

## Prerrequisitos

- Asegúrese de que el equilibrador de carga interno de Azure se encuentra en la región de Azure desde la que va a realizar el traslado.
- Los equilibradores de carga internos de Azure no se pueden trasladar entre regiones. Tendrá que asociar el nuevo equilibrador de carga a los recursos de la región de destino.
- Necesitará contar con el rol de colaborador de red u otro superior para exportar la configuración de un equilibrador de carga interno e implementar una plantilla para crear un equilibrador de carga interno en otra región.
- Identifique el diseño de red de origen y todos los recursos que está usando actualmente. Este diseño incluye, pero no se limita a los equilibradores de carga, los grupos de seguridad de red, las máquinas virtuales y las redes virtuales.
- Compruebe que su suscripción a Azure permite crear equilibradores de carga internos en la región de destino que se usa. Para habilitar la cuota necesaria, póngase en contacto con el soporte técnico.
- Asegúrese de que la suscripción tiene suficientes recursos para admitir la adición de equilibradores de carga para este proceso. Vea [Límites, cuotas y restricciones de suscripción y servicios de Microsoft Azure](#)

## Preparación y traslado

En los pasos siguientes se muestra cómo preparar el equilibrador de carga interno para el traslado mediante una plantilla de Resource Manager y cómo trasladar la configuración del equilibrador de carga interno a la región de destino mediante Azure Portal. Como parte de este proceso, la configuración de la red virtual del equilibrador de carga interno debe incluirse y debe crearse antes de trasladar el equilibrador de carga interno.

## NOTE

Este artículo se ha actualizado para usar el nuevo módulo Az de Azure PowerShell. Aún puede usar el módulo de AzureRM que continuará recibiendo correcciones de errores hasta diciembre de 2020 como mínimo. Para más información acerca del nuevo módulo Az y la compatibilidad con AzureRM, consulte [Introducing the new Azure PowerShell Az module](#) (Presentación del nuevo módulo Az de Azure PowerShell). Para obtener instrucciones sobre la instalación del módulo Az, consulte [Instalación de Azure PowerShell](#).

## Exportación de la plantilla de red virtual e implementación desde Azure Portal

1. Inicie sesión en [Azure Portal](#) > Grupos de recursos.
2. Seleccione el grupo de recursos que contiene la red virtual de origen y haga clic en él.
3. Seleccione > Configuración > Exportar plantilla.
4. En la hoja Exportar plantilla, elija Implementar.
5. Haga clic en PLANTILLA > Editar parámetros para abrir el archivo **parameters.json** en el editor en línea.
6. Para editar el parámetro correspondiente al nombre de la red virtual, cambie la propiedad **value** de **parameters**:

```
{
 "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentParameters.json#",
 "contentVersion": "1.0.0.0",
 "parameters": {
 "virtualNetworks_myVNET1_name": {
 "value": "<target-virtual-network-name>"
 }
 }
}
```

7. Cambie el valor de nombre de la red virtual de origen en el editor por un nombre de su elección para la red virtual de destino. Asegúrese de escribir el nombre entre comillas.
8. Haga clic en Guardar en el editor.
9. Haga clic en Plantilla > Editar plantilla para abrir el archivo **template.json** en el editor en línea.
10. Para editar la región de destino a la que se va a trasladar la red virtual, cambie la propiedad **location** en **resources**:

```
"resources": [
 {
 "type": "Microsoft.Network/virtualNetworks",
 "apiVersion": "2019-06-01",
 "name": "[parameters('virtualNetworks_myVNET1_name')]",
 "location": "<target-region>",
 "properties": {
 "provisioningState": "Succeeded",
 "resourceGuid": "6e2652be-35ac-4e68-8c70-621b9ec87dcb",
 "addressSpace": {
 "addressPrefixes": [
 "10.0.0.0/16"
]
 }
 }
 },
]
```

11. Para obtener los códigos de ubicación de la región, consulte [Ubicaciones de Azure](#). El código de una región es el nombre de la región sin espacios, **Centro de EE. UU. = centralus**.
12. Si quiere, también puede cambiar otros parámetros del archivo **template.json**. Estos son opcionales según sus necesidades:
  - **Espacio de direcciones:** el espacio de direcciones de la red virtual se puede modificar antes de guardar al editar la sección **resources** > **addressSpace** y cambiar la propiedad **addressPrefixes** en el archivo **template.json**:

```
"resources": [
 {
 "type": "Microsoft.Network/virtualNetworks",
 "apiVersion": "2019-06-01",
 "name": "[parameters('virtualNetworks_myVNET1_name')]",
 "location": "<target-region",
 "properties": {
 "provisioningState": "Succeeded",
 "resourceGuid": "6e2652be-35ac-4e68-8c70-621b9ec87dcb",
 "addressSpace": {
 "addressPrefixes": [
 "10.0.0.0/16"
]
 },
 },
],
]
```

- **Subred:** es posible modificar o realizar adiciones al nombre de subred y al espacio de direcciones de subred si edita la sección **subnets** del archivo **template.json**. El nombre de la subred se puede cambiar si modifica la propiedad **name**. El espacio de direcciones de subred se puede cambiar si modifica la propiedad **addressPrefix** en el archivo **template.json**:

```
"subnets": [
 {
 "name": "subnet-1",
 "etag": "W/\"d9f6e6d6-2c15-4f7c-b01f-bed40f748dea\"",
 "properties": {
 "provisioningState": "Succeeded",
 "addressPrefix": "10.0.0.0/24",
 "delegations": [],
 "privateEndpointNetworkPolicies": "Enabled",
 "privateLinkServiceNetworkPolicies": "Enabled"
 },
 },
 {
 "name": "GatewaySubnet",
 "etag": "W/\"d9f6e6d6-2c15-4f7c-b01f-bed40f748dea\"",
 "properties": {
 "provisioningState": "Succeeded",
 "addressPrefix": "10.0.1.0/29",
 "serviceEndpoints": [],
 "delegations": [],
 "privateEndpointNetworkPolicies": "Enabled",
 "privateLinkServiceNetworkPolicies": "Enabled"
 },
 },
]
```

Para cambiar el prefijo de dirección, debe editar el archivo **template.json** en dos lugares; primero en la sección mencionada anteriormente y después en la sección **type** a continuación. Cambie la propiedad **addressPrefix** para que coincida con la anterior:

```

"type": "Microsoft.Network/virtualNetworks/subnets",
"apiVersion": "2019-06-01",
"name": "[concat(parameters('virtualNetworks_myVNET1_name'), '/GatewaySubnet')]",
"dependsOn": [
 "[resourceId('Microsoft.Network/virtualNetworks',
parameters('virtualNetworks_myVNET1_name'))]"
],
"properties": {
 "provisioningState": "Succeeded",
 "addressPrefix": "10.0.1.0/29",
 "serviceEndpoints": [],
 "delegations": [],
 "privateEndpointNetworkPolicies": "Enabled",
 "privateLinkServiceNetworkPolicies": "Enabled"
}
},
{
 "type": "Microsoft.Network/virtualNetworks/subnets",
 "apiVersion": "2019-06-01",
 "name": "[concat(parameters('virtualNetworks_myVNET1_name'), '/subnet-1')]",
 "dependsOn": [
 "[resourceId('Microsoft.Network/virtualNetworks',
parameters('virtualNetworks_myVNET1_name'))]"
],
 "properties": {
 "provisioningState": "Succeeded",
 "addressPrefix": "10.0.0.0/24",
 "delegations": [],
 "privateEndpointNetworkPolicies": "Enabled",
 "privateLinkServiceNetworkPolicies": "Enabled"
 }
}
]

```

13. Haga clic en **Guardar** en el editor en línea.
14. Haga clic en **BÁSICO > Suscripción** para elegir la suscripción en la que se implementará la red virtual de destino.
15. Haga clic en **BÁSICO > Grupo de recursos** para elegir el grupo de recursos en el que se implementará la red virtual de destino. Puede hacer clic en **Crear nuevo** para crear un nuevo grupo de recursos para la red virtual de destino. Asegúrese de que el nombre no es el mismo que el del grupo de recursos de origen de la red virtual existente.
16. Compruebe que **BÁSICO > Ubicación** está establecido en la ubicación de destino en la que quiere implementar la red virtual.
17. En **CONFIGURACIÓN**, compruebe que el nombre coincide con el nombre que especificó en el editor de parámetros anterior.
18. Marque la casilla en **TÉRMINOS Y CONDICIONES**.
19. Haga clic en el botón **Comprar** para implementar la red virtual de destino.

### **Exportación de la plantilla del equilibrador de carga interno e implementación desde Azure PowerShell**

1. Inicie sesión en [Azure Portal](#) > **Grupos de recursos**.
2. Seleccione el grupo de recursos que contiene el equilibrador de carga interno de origen y haga clic en él.
3. Seleccione > **Configuración** > **Exportar plantilla**.
4. En la hoja **Exportar plantilla**, elija **Implementar**.

5. Haga clic en **PLANTILLA > Editar parámetros** para abrir el archivo **parameters.json** en el editor en línea.
6. Para editar el parámetro del nombre del equilibrador de carga interno, cambie la propiedad **defaultValue** del nombre del equilibrador de carga interno de origen por el nombre del equilibrador de carga interno de destino. Asegúrese de que el nombre se encuentra entre comillas:

```
"$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
"contentVersion": "1.0.0.0",
"parameters": {
 "loadBalancers_myLoadBalancer_name": {
 "defaultValue": "<target-internal-lb-name>",
 "type": "String"
 },
 "virtualNetworks_myVNET2_internalid": {
 "defaultValue": "<target-vnet-resource-ID>",
 "type": "String"
 }
}
```

7. Para editar el valor de la red virtual de destino que se traslado anteriormente, primero debe obtener el Id. de recurso y después copiarlo y pegarlo en el archivo **parameters.json**. Para obtener el identificador realice lo siguiente:
  - a. Inicie sesión en [Azure Portal](#) > **Grupos de recursos** en otra pestaña o ventana del explorador.
  - b. Busque el grupo de recursos de destino que contiene la red virtual trasladada en los pasos anteriores y haga clic en él.
  - c. Seleccione **Configuración > Propiedades**.
  - d. En la hoja de la derecha, resalte **Id. de recurso** y cópielo en el Portapapeles. También puede hacer clic en el botón **Copiar en el Portapapeles** a la derecha de la ruta de acceso del **Id. de recurso**.
  - e. Pegue el Id. de recurso en la propiedad **defaultValue** del editor **Editar parámetros** que abrió en otra ventana o pestaña del explorador:

```
"$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
"contentVersion": "1.0.0.0",
"parameters": {
 "loadBalancers_myLoadBalancer_name": {
 "defaultValue": "<target-internal-lb-name>",
 "type": "String"
 },
 "virtualNetworks_myVNET2_internalid": {
 "defaultValue": "<target-vnet-resource-ID>",
 "type": "String"
 }
}
```

- f. Haga clic en **Guardar** en el editor en línea.
8. Haga clic en **Plantilla > Editar plantilla** para abrir el archivo **template.json** en el editor en línea.
9. Para editar la región de destino a la que se va a trasladar la configuración del equilibrador de carga interno, cambie la propiedad **location** en **resources** del archivo **template.json**:

```
"resources": [
 {
 "type": "Microsoft.Network/loadBalancers",
 "apiVersion": "2019-06-01",
 "name": "[parameters('loadBalancers_myLoadBalancer_name')]",
 "location": "<target-internal-lb-region>",
 "sku": {
 "name": "Standard",
 "tier": "Regional"
 }
 },

```

10. Para obtener los códigos de ubicación de la región, consulte [Ubicaciones de Azure](#). El código de una región es el nombre de la región sin espacios, **Centro de EE. UU.** = **centralus**.

11. También puede cambiar otros parámetros de la plantilla si así lo desea; son opcionales según sus requisitos:

- **SKU:** puede cambiar la SKU del equilibrador de carga interno en la configuración del nivel estándar al básico o viceversa si modifica la propiedad **sku > name** en el archivo **template.json**:

```
"resources": [
 {
 "type": "Microsoft.Network/loadBalancers",
 "apiVersion": "2019-06-01",
 "name": "[parameters('loadBalancers_myLoadBalancer_name')]",
 "location": "<target-internal-lb-region>",
 "sku": {
 "name": "Standard",
 "tier": "Regional"
 }
 },

```

Para más información sobre las diferencias entre los equilibradores de carga de la SKU básica y estándar, consulte [Introducción a Azure Standard Load Balancer](#).

- **Reglas de equilibrio de carga:** puede agregar o quitar reglas de equilibrio de carga en la configuración agregando o quitando entradas en la sección **loadBalancingRules** del archivo **template.json**:



```

"loadBalancingRules": [
 {
 "name": "myInboundRule",
 "etag": "W/\"39e5e9cd-2d6d-491f-83cf-b37a259d86b6\"",
 "properties": {
 "provisioningState": "Succeeded",
 "frontendIPConfiguration": {
 "id": "[concat(resourceId('Microsoft.Network/loadBalancers',
parameters('loadBalancers_myLoadBalancer_name')),
'/frontendIPConfigurations/myfrontendIPinbound')]"
 },
 "frontendPort": 80,
 "backendPort": 80,
 "enableFloatingIP": false,
 "idleTimeoutInMinutes": 4,
 "protocol": "Tcp",
 "enableTcpReset": false,
 "loadDistribution": "Default",
 "disableOutboundSnat": true,
 "backendAddressPool": {
 "id": "[concat(resourceId('Microsoft.Network/loadBalancers',
parameters('loadBalancers_myLoadBalancer_name')), '/backendAddressPools/myBEPoolInbound')]"
 },
 "probe": {
 "id": "[concat(resourceId('Microsoft.Network/loadBalancers',
parameters('loadBalancers_myLoadBalancer_name')), '/probes/myHTTPProbe')]"
 }
 }
 }
]

```

Para más información sobre las reglas de equilibrio de carga, consulte [¿Qué es Azure Load Balancer?](#)

- **Sondeos:** puede agregar o quitar sondeos para el equilibrador de carga en la configuración agregando o quitando entradas en la sección **probes** del archivo **template.json**:

```

"probes": [
 {
 "name": "myHTTPProbe",
 "etag": "W/\"39e5e9cd-2d6d-491f-83cf-b37a259d86b6\"",
 "properties": {
 "provisioningState": "Succeeded",
 "protocol": "Http",
 "port": 80,
 "requestPath": "/",
 "intervalInSeconds": 15,
 "numberOfProbes": 2
 }
 }
],

```

Para más información sobre los sondeos de estado de Azure Load Balancer, consulte [Sondeos de estado de Load Balancer](#).

- **Reglas NAT de entrada:** puede agregar o quitar reglas NAT de entrada para el equilibrador de carga agregando o quitando entradas en la sección **inboundNatRules** del archivo **template.json**:

```

"inboundNatRules": [
 {
 "name": "myInboundNATRule",
 "etag": "W/\"39e5e9cd-2d6d-491f-83cf-b37a259d86b6\"",
 "properties": {
 "provisioningState": "Succeeded",
 "frontendIPConfiguration": {
 "id": "[concat(resourceId('Microsoft.Network/loadBalancers',
parameters('loadBalancers_myLoadBalancer_name')),
'/frontendIPConfigurations/myfrontendIPinbound')]"
 },
 "frontendPort": 4422,
 "backendPort": 3389,
 "enableFloatingIP": false,
 "idleTimeoutInMinutes": 4,
 "protocol": "Tcp",
 "enableTcpReset": false
 }
 }
]

```

Para completar la adición o eliminación de una regla NAT de entrada, esta debe agregarse o quitarse como una propiedad **type** al final del archivo **template.json**:

```

{
 "type": "Microsoft.Network/loadBalancers/inboundNatRules",
 "apiVersion": "2019-06-01",
 "name": "[concat(parameters('loadBalancers_myLoadBalancer_name'), '/myInboundNATRule')]",
 "dependsOn": [
 "[resourceId('Microsoft.Network/loadBalancers',
parameters('loadBalancers_myLoadBalancer_name'))]"
],
 "properties": {
 "provisioningState": "Succeeded",
 "frontendIPConfiguration": {
 "id": "[concat(resourceId('Microsoft.Network/loadBalancers',
parameters('loadBalancers_myLoadBalancer_name')),
'/frontendIPConfigurations/myfrontendIPinbound')]"
 },
 "frontendPort": 4422,
 "backendPort": 3389,
 "enableFloatingIP": false,
 "idleTimeoutInMinutes": 4,
 "protocol": "Tcp",
 "enableTcpReset": false
 }
}

```

Para más información sobre las reglas NAT de entrada, consulte [¿Qué es Azure Load Balancer?](#)

12. Haga clic en **Guardar** en el editor en línea.
13. Haga clic en **BÁSICO > Suscripción** para elegir la suscripción en la que se implementará el equilibrador de carga interno de destino.
14. Haga clic en **BÁSICO > Grupo de recursos** para elegir el grupo de recursos en el que se implementará el equilibrador de carga de destino. Puede hacer clic en **Crear nuevo** para crear un nuevo grupo de recursos para el equilibrador de carga interno de destino o puede elegir el grupo de recursos existente que se creó anteriormente para la red virtual. Asegúrese de que el nombre no es el mismo que el del grupo de recursos de origen del equilibrador de carga interno de origen existente.
15. Compruebe que **BÁSICO > Ubicación** está establecido en la ubicación de destino en la que quiere

implementar el equilibrador de carga interno.

16. En **CONFIGURACIÓN**, compruebe que el nombre coincide con el nombre que especificó en el editor de parámetros anterior. Compruebe que los Id. de recursos estén especificados para todas las redes virtuales en la configuración.
17. Marque la casilla en **TÉRMINOS Y CONDICIONES**.
18. Haga clic en el botón **Comprar** para implementar la red virtual de destino.

## Discard (Descartar)

Si quiere descartar la red virtual de destino y el equilibrador de carga interno, elimine el grupo de recursos que contiene la red virtual de destino y el equilibrador de carga interno. Para ello, en el portal, seleccione el grupo de recursos en el panel y, luego, **Eliminar** en la parte superior de la página de información general.

## Limpieza

Para confirmar los cambios y completar el traslado de la red virtual y el equilibrador de carga interno, elimine la red virtual de origen y el equilibrador de carga interno o el grupo de recursos. Para ello, seleccione la red virtual y el equilibrador de carga interno o grupo de recursos desde el panel en el portal y seleccione **Eliminar** en la parte superior de cada página.

## Pasos siguientes

En este tutorial, migró un equilibrador de carga interno de Azure de una región a otra y limpió los recursos de origen. Para obtener más información sobre cómo trasladar recursos entre regiones y la recuperación ante desastres en Azure, consulte:

- [Traslado de los recursos a un nuevo grupo de recursos o a una nueva suscripción](#)
- [Traslado de máquinas virtuales de Azure a otra región](#)

# Traslado de un equilibrador de carga interno de Azure a otra región mediante PowerShell

23/09/2020 • 18 minutes to read • [Edit Online](#)

Hay varios escenarios en los que quizá quiera trasladar su equilibrador de carga interno actual de una región a otra. Por ejemplo, puede que quiera crear un equilibrador de carga interno con la misma configuración para realizar pruebas. También puede que quiera trasladar un equilibrador de carga interno a otra región como parte del planeamiento para la recuperación ante desastres.

Los equilibradores de carga internos de Azure no se pueden trasladar de una región a otra. Sin embargo, puede usar una plantilla de Azure Resource Manager para exportar la configuración y la red virtual actuales de un equilibrador de carga interno. Después, puede preparar el recurso para otra región al exportar el equilibrador de carga y la red virtual a una plantilla, modificar los parámetros para que coincidan con la región de destino y, a continuación, implementar la plantilla en la nueva región. Para más información sobre Resource Manager y sus plantillas, consulte [Exportación de grupos de recursos a plantillas](#).

## Requisitos previos

- Asegúrese de que el equilibrador de carga interno de Azure se encuentra en la región de Azure desde la que va a realizar el traslado.
- Los equilibradores de carga internos de Azure no se pueden trasladar entre regiones. Tendrá que asociar el nuevo equilibrador de carga a los recursos de la región de destino.
- Necesitará contar con el rol de colaborador de red u otro superior para exportar la configuración de un equilibrador de carga interno e implementar una plantilla para crear un equilibrador de carga interno en otra región.
- Identifique el diseño de red de origen y todos los recursos que está usando actualmente. Este diseño incluye, pero no se limita a los equilibradores de carga, los grupos de seguridad de red, las máquinas virtuales y las redes virtuales.
- Compruebe que su suscripción a Azure permite crear equilibradores de carga internos en la región de destino que se usa. Para habilitar la cuota necesaria, póngase en contacto con el soporte técnico.
- Asegúrese de que la suscripción tiene suficientes recursos para admitir la adición de equilibradores de carga para este proceso. Vea [Límites, cuotas y restricciones de suscripción y servicios de Microsoft Azure](#)

## Preparación y traslado

En los pasos siguientes se muestra cómo preparar el equilibrador de carga interno para el traslado mediante una plantilla de Resource Manager y cómo trasladar la configuración del equilibrador de carga interno a la región de destino mediante Azure PowerShell. Como parte de este proceso, la configuración de la red virtual del equilibrador de carga interno debe incluirse y debe crearse antes de trasladar el equilibrador de carga interno.

## NOTE

Este artículo se ha actualizado para usar el nuevo módulo Az de Azure PowerShell. Aún puede usar el módulo de AzureRM que continuará recibiendo correcciones de errores hasta diciembre de 2020 como mínimo. Para más información acerca del nuevo módulo Az y la compatibilidad con AzureRM, consulte [Introducing the new Azure PowerShell Az module](#) (Presentación del nuevo módulo Az de Azure PowerShell). Para obtener instrucciones sobre la instalación del módulo Az, consulte [Instalación de Azure PowerShell](#).

## Exportación de la plantilla de red virtual e implementación desde Azure PowerShell

1. Inicie sesión en la suscripción a Azure con el comando [Connect-AzAccount](#) y siga las instrucciones de la pantalla:

```
Connect-AzAccount
```

2. Obtenga el identificador de recurso de la red virtual que quiere trasladar a la región de destino y colóquelo en una variable mediante [Get-AzVirtualNetwork](#):

```
$sourceVNETID = (Get-AzVirtualNetwork -Name <source-virtual-network-name> -ResourceGroupName <source-resource-group-name>).Id
```

3. Exporte la red virtual de origen a un archivo json en el directorio donde se ejecuta el comando [Export-AzResourceGroup](#):

```
Export-AzResourceGroup -ResourceGroupName <source-resource-group-name> -Resource $sourceVNETID -IncludeParameterDefaultValue
```

4. El nombre del archivo descargado se asignará en función del grupo de recursos desde el que se exportó el recurso. Busque el archivo que se exportó con el comando denominado **<resource-group-name>.json** y ábralo en el editor que prefiera:

```
notepad.exe <source-resource-group-name>.json
```

5. Para editar el parámetro del nombre de la red virtual, cambie la propiedad **defaultValue** del nombre de la red virtual de origen por el nombre de la red virtual de destino y asegúrese de que el nombre esté entre comillas:

```
{
 "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentmyResourceGroupVNET.json#",
 "contentVersion": "1.0.0.0",
 "parameters": {
 "virtualNetworks_myVNET1_name": {
 "defaultValue": "<target-virtual-network-name>",
 "type": "String"
 }
 }
}
```

6. Para editar la región de destino a la que se va a trasladar la red virtual, cambie la propiedad **location** en **resources**:

```
"resources": [
 {
 "type": "Microsoft.Network/virtualNetworks",
 "apiVersion": "2019-06-01",
 "name": "[parameters('virtualNetworks_myVNET1_name')]",
 "location": "<target-region>",
 "properties": {
 "provisioningState": "Succeeded",
 "resourceGuid": "6e2652be-35ac-4e68-8c70-621b9ec87dcb",
 "addressSpace": {
 "addressPrefixes": [
 "10.0.0.0/16"
]
 }
 }
 },

```

7. Para obtener los códigos de ubicación de la región, puede usar el cmdlet Azure PowerShell [Get-AzLocation](#) al ejecutar el siguiente comando:

```
Get-AzLocation | format-table
```

8. Si quiere, también puede cambiar otros parámetros del archivo **<resource-group-name>.json**. Estos son opcionales según sus necesidades:

- **Espacio de direcciones:** el espacio de direcciones de la red virtual se puede modificar antes de guardar al editar la sección **resources** > **addressSpace** y cambiar la propiedad **addressPrefixes** en el archivo **<resource-group-name>.json**:

```
"resources": [
 {
 "type": "Microsoft.Network/virtualNetworks",
 "apiVersion": "2019-06-01",
 "name": "[parameters('virtualNetworks_myVNET1_name')]",
 "location": "<target-region>",
 "properties": {
 "provisioningState": "Succeeded",
 "resourceGuid": "6e2652be-35ac-4e68-8c70-621b9ec87dcb",
 "addressSpace": {
 "addressPrefixes": [
 "10.0.0.0/16"
]
 }
 }
 },

```

- **Subred:** es posible modificar o realizar adiciones al nombre de subred y al espacio de direcciones de subred si edita la sección **subnets** del archivo **<resource-group-name>.json**. El nombre de la subred se puede cambiar si modifica la propiedad **name**. El espacio de direcciones de subred se puede cambiar si modifica la propiedad **addressPrefix** en el archivo **<resource-group-name>.json**:

```

"subnets": [
 {
 "name": "subnet-1",
 "etag": "W/\"d9f6e6d6-2c15-4f7c-b01f-bed40f748dea\"",
 "properties": {
 "provisioningState": "Succeeded",
 "addressPrefix": "10.0.0/24",
 "delegations": [],
 "privateEndpointNetworkPolicies": "Enabled",
 "privateLinkServiceNetworkPolicies": "Enabled"
 }
 },
 {
 "name": "GatewaySubnet",
 "etag": "W/\"d9f6e6d6-2c15-4f7c-b01f-bed40f748dea\"",
 "properties": {
 "provisioningState": "Succeeded",
 "addressPrefix": "10.0.1.0/29",
 "serviceEndpoints": [],
 "delegations": [],
 "privateEndpointNetworkPolicies": "Enabled",
 "privateLinkServiceNetworkPolicies": "Enabled"
 }
 }
]

```

Para cambiar el prefijo de dirección, debe editar el archivo `<resource-group-name>.json` en dos lugares; primero en la sección mencionada anteriormente y después en la sección **type** a continuación. Cambie la propiedad **addressPrefix** para que coincida con la anterior:

```

"type": "Microsoft.Network/virtualNetworks/subnets",
"apiVersion": "2019-06-01",
"name": "[concat(parameters('virtualNetworks_myVNET1_name'), '/GatewaySubnet')]",
"dependsOn": [
 "[resourceId('Microsoft.Network/virtualNetworks',
parameters('virtualNetworks_myVNET1_name'))]"
],
"properties": {
 "provisioningState": "Succeeded",
 "addressPrefix": "10.0.1.0/29",
 "serviceEndpoints": [],
 "delegations": [],
 "privateEndpointNetworkPolicies": "Enabled",
 "privateLinkServiceNetworkPolicies": "Enabled"
}
},
{
 "type": "Microsoft.Network/virtualNetworks/subnets",
 "apiVersion": "2019-06-01",
 "name": "[concat(parameters('virtualNetworks_myVNET1_name'), '/subnet-1')]",
 "dependsOn": [
 "[resourceId('Microsoft.Network/virtualNetworks',
parameters('virtualNetworks_myVNET1_name'))]"
],
 "properties": {
 "provisioningState": "Succeeded",
 "addressPrefix": "10.0.0.0/24",
 "delegations": [],
 "privateEndpointNetworkPolicies": "Enabled",
 "privateLinkServiceNetworkPolicies": "Enabled"
 }
}
]

```

9. Guarde el archivo `<resource-group-name>.json`.
10. Cree un grupo de recursos en la región de destino para la red virtual de destino que se va a implementar mediante [New-AzResourceGroup](#).

```
New-AzResourceGroup -Name <target-resource-group-name> -location <target-region>
```

11. Implemente el archivo `<resource-group-name>.json` editado en el grupo de recursos que creó en el paso anterior mediante [New-AzResourceGroupDeployment](#):

```
New-AzResourceGroupDeployment -ResourceGroupName <target-resource-group-name> -TemplateFile <source-resource-group-name>.json
```

12. Para comprobar que los recursos se crearon en la región de destino, use los comandos [Get-AzResourceGroup](#) y [Get-AzVirtualNetwork](#):

```
Get-AzResourceGroup -Name <target-resource-group-name>
```

```
Get-AzVirtualNetwork -Name <target-virtual-network-name> -ResourceGroupName <target-resource-group-name>
```

### Exportación de la plantilla del equilibrador de carga interno e implementación desde Azure PowerShell

1. Inicie sesión en la suscripción a Azure con el comando [Connect-AzAccount](#) y siga las instrucciones de la pantalla:

```
Connect-AzAccount
```

2. Obtenga el identificador del recurso del equilibrador de carga interno que quiere trasladar a la región de destino y colóquelo en una variable mediante [Get-AzLoadBalancer](#):

```
$sourceIntLBID = (Get-AzLoadBalancer -Name <source-internal-lb-name> -ResourceGroupName <source-resource-group-name>).Id
```

3. Exporte la configuración del equilibrador de carga interno de origen a un archivo json en el directorio donde se ejecuta el comando [Export-AzResourceGroup](#):

```
Export-AzResourceGroup -ResourceGroupName <source-resource-group-name> -Resource $sourceIntLBID -IncludeParameterDefaultValue
```

4. El nombre del archivo descargado se asignará en función del grupo de recursos desde el que se exportó el recurso. Busque el archivo que se exportó con el comando denominado `<resource-group-name>.json` y ábralo en el editor que prefiera:

```
notepad.exe <source-resource-group-name>.json
```



5. Para editar el parámetro del nombre del equilibrador de carga interno, cambie la propiedad **defaultValue** del nombre del equilibrador de carga interno de origen por el nombre del equilibrador de carga interno de destino. Asegúrese de que el nombre se encuentra entre comillas:

```
"$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
"contentVersion": "1.0.0.0",
"parameters": {
 "loadBalancers_myLoadBalancer_name": {
 "defaultValue": "<target-external-lb-name>",
 "type": "String"
 },
 "virtualNetworks_myVNET2_externalid": {
 "defaultValue": "<target-vnet-resource-ID>",
 "type": "String"
 }
}
```

6. Para editar el valor de la red virtual de destino que se traslado anteriormente, primero debe obtener el Id. de recurso y después copiarlo y pegarlo en el archivo **<resource-group-name>.json**. Para obtener el identificador, use [Get-AzVirtualNetwork](#):

```
$targetVNETID = (Get-AzVirtualNetwork -Name <target-vnet-name> -ResourceGroupName <target-resource-group-name>).Id
```

Escriba la variable y presione ENTRAR para mostrar el identificador del recurso. Resalte la ruta de acceso del identificador y cópiela en el portapapeles:

```
PS C:\> $targetVNETID
/subscriptions/7668d659-17fc-4ffd-85ba-9de61fe977e8/resourceGroups/myResourceGroupVNET-
Move/providers/Microsoft.Network/virtualNetworks/myVNET2-Move
```

7. En el archivo **<resource-group-name>.json**, pegue el **identificador del recurso** de la variable en lugar del valor **defaultValue** en el segundo parámetro del identificador de la red virtual de destino y asegúrese de escribir la ruta de acceso entre comillas:

```
"$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
"contentVersion": "1.0.0.0",
"parameters": {
 "loadBalancers_myLoadBalancer_name": {
 "defaultValue": "<target-external-lb-name>",
 "type": "String"
 },
 "virtualNetworks_myVNET2_externalid": {
 "defaultValue": "<target-vnet-resource-ID>",
 "type": "String"
 }
}
```

8. Para editar la región de destino a la que se va a trasladar la configuración del equilibrador de carga interno, cambie la propiedad **location** en **resources** del archivo **<resource-group-name>.json**:

```
"resources": [
 {
 "type": "Microsoft.Network/loadBalancers",
 "apiVersion": "2019-06-01",
 "name": "[parameters('loadBalancers_myLoadBalancer_name')]",
 "location": "<target-internal-lb-region>",
 "sku": {
 "name": "Standard",
 "tier": "Regional"
 }
 },

```

9. Para obtener los códigos de ubicación de la región, puede usar el cmdlet Azure PowerShell [Get-AzLocation](#) al ejecutar el siguiente comando:

```
Get-AzLocation | format-table
```

10. También puede cambiar otros parámetros de la plantilla si así lo desea; son opcionales según sus requisitos:

- **SKU:** puede cambiar la SKU del equilibrador de carga interno en la configuración del nivel estándar al básico o viceversa si modifica la propiedad **sku > name** en el archivo **<resource-group-name>.json**:

```
"resources": [
 {
 "type": "Microsoft.Network/loadBalancers",
 "apiVersion": "2019-06-01",
 "name": "[parameters('loadBalancers_myLoadBalancer_name')]",
 "location": "<target-internal-lb-region>",
 "sku": {
 "name": "Standard",
 "tier": "Regional"
 }
 },

```

Para más información sobre las diferencias entre los equilibradores de carga de la SKU básica y estándar, consulte [Introducción a Azure Standard Load Balancer](#).

- **Reglas de equilibrio de carga:** puede agregar o quitar reglas de equilibrio de carga en la configuración agregando o quitando entradas en la sección **loadBalancingRules** del archivo **<resource-group-name>.json**:

```

"loadBalancingRules": [
 {
 "name": "myInboundRule",
 "etag": "W/\"39e5e9cd-2d6d-491f-83cf-b37a259d86b6\"",
 "properties": {
 "provisioningState": "Succeeded",
 "frontendIPConfiguration": {
 "id": "[concat(resourceId('Microsoft.Network/loadBalancers',
parameters('loadBalancers_myLoadBalancer_name')),
'/frontendIPConfigurations/myfrontendIPinbound')]"
 },
 "frontendPort": 80,
 "backendPort": 80,
 "enableFloatingIP": false,
 "idleTimeoutInMinutes": 4,
 "protocol": "Tcp",
 "enableTcpReset": false,
 "loadDistribution": "Default",
 "disableOutboundSnat": true,
 "backendAddressPool": {
 "id": "[concat(resourceId('Microsoft.Network/loadBalancers',
parameters('loadBalancers_myLoadBalancer_name')), '/backendAddressPools/myBEPoolInbound')]"
 },
 "probe": {
 "id": "[concat(resourceId('Microsoft.Network/loadBalancers',
parameters('loadBalancers_myLoadBalancer_name')), '/probes/myHTTPProbe')]"
 }
 }
 }
]

```

Para más información sobre las reglas de equilibrio de carga, consulte [¿Qué es Azure Load Balancer?](#)

- **Sondeos:** puede agregar o quitar sondeos para el equilibrador de carga en la configuración agregando o quitando entradas en la sección **probes** del archivo **<resource-group-name>.json**:

```

"probes": [
 {
 "name": "myHTTPProbe",
 "etag": "W/\"39e5e9cd-2d6d-491f-83cf-b37a259d86b6\"",
 "properties": {
 "provisioningState": "Succeeded",
 "protocol": "Http",
 "port": 80,
 "requestPath": "/",
 "intervalInSeconds": 15,
 "numberOfProbes": 2
 }
 }
],

```

Para más información sobre los sondeos de estado de Azure Load Balancer, consulte [Sondeos de estado de Load Balancer](#).

- **Reglas NAT de entrada:** puede agregar o quitar reglas NAT de entrada para el equilibrador de carga agregando o quitando entradas en la sección **inboundNatRules** del archivo **<resource-group-name>.json**:

```

"inboundNatRules": [
 {
 "name": "myInboundNATRule",
 "etag": "W/\"39e5e9cd-2d6d-491f-83cf-b37a259d86b6\"",
 "properties": {
 "provisioningState": "Succeeded",
 "frontendIPConfiguration": {
 "id": "[concat(resourceId('Microsoft.Network/loadBalancers',
parameters('loadBalancers_myLoadBalancer_name')),
'/frontendIPConfigurations/myfrontendIPinbound')]"
 },
 "frontendPort": 4422,
 "backendPort": 3389,
 "enableFloatingIP": false,
 "idleTimeoutInMinutes": 4,
 "protocol": "Tcp",
 "enableTcpReset": false
 }
 }
]

```

Para completar la adición o eliminación de una regla NAT de entrada, esta debe agregarse o quitarse como propiedad **type** al final del archivo **<resource-group-name>.json**:

```

{
 "type": "Microsoft.Network/loadBalancers/inboundNatRules",
 "apiVersion": "2019-06-01",
 "name": "[concat(parameters('loadBalancers_myLoadBalancer_name'), '/myInboundNATRule')]",
 "dependsOn": [
 "[resourceId('Microsoft.Network/loadBalancers',
parameters('loadBalancers_myLoadBalancer_name'))]"
],
 "properties": {
 "provisioningState": "Succeeded",
 "frontendIPConfiguration": {
 "id": "[concat(resourceId('Microsoft.Network/loadBalancers',
parameters('loadBalancers_myLoadBalancer_name')),
'/frontendIPConfigurations/myfrontendIPinbound')]"
 },
 "frontendPort": 4422,
 "backendPort": 3389,
 "enableFloatingIP": false,
 "idleTimeoutInMinutes": 4,
 "protocol": "Tcp",
 "enableTcpReset": false
 }
}

```

Para más información sobre las reglas NAT de entrada, consulte [¿Qué es Azure Load Balancer?](#)

11. Guarde el archivo **<resource-group-name>.json**.
12. Cree un grupo de recursos en la región de destino para el equilibrador de carga interno de destino que se va a implementar mediante [New-AzResourceGroup](#). El grupo de recursos existente anterior también se puede reutilizar como parte de este proceso:

```
New-AzResourceGroup -Name <target-resource-group-name> -location <target-region>
```

13. Implemente el archivo **<resource-group-name>.json** editado en el grupo de recursos que creó en el paso anterior mediante [New-AzResourceGroupDeployment](#):

```
New-AzResourceGroupDeployment -ResourceGroupName <target-resource-group-name> -TemplateFile <source-resource-group-name>.json
```

14. Para comprobar que los recursos se crearon en la región de destino, use los comandos [Get-AzResourceGroup](#) y [Get-AzLoadBalancer](#):

```
Get-AzResourceGroup -Name <target-resource-group-name>
```

```
Get-AzLoadBalancer -Name <target-publicip-name> -ResourceGroupName <target-resource-group-name>
```

## Discard (Descartar)

Después de la implementación, si quiere empezar de nuevo o descartar la red virtual y el equilibrador de carga en el destino, elimine el grupo de recursos que se creó en el destino y se eliminará la red virtual y el equilibrador de carga trasladados. Para quitar el grupo de recursos, use [Remove-AzResourceGroup](#):

```
Remove-AzResourceGroup -Name <resource-group-name>
```

## Limpieza

Para confirmar los cambios y completar el traslado del NSG, elimine el NSG o el grupo de recursos de origen mediante [Remove-AzResourceGroup](#) o [Remove-AzVirtualNetwork](#) y [Remove-AzLoadBalancer](#)

```
Remove-AzResourceGroup -Name <resource-group-name>
```

```
Remove-AzLoadBalancer -name <load-balancer> -ResourceGroupName <resource-group-name>
```

```
Remove-AzVirtualNetwork -Name <virtual-network-name> -ResourceGroupName <resource-group-name>
```

## Pasos siguientes

En este tutorial, migró un equilibrador de carga interno de Azure de una región a otra y limpió los recursos de origen. Para obtener más información sobre cómo trasladar recursos entre regiones y la recuperación ante desastres en Azure, consulte:

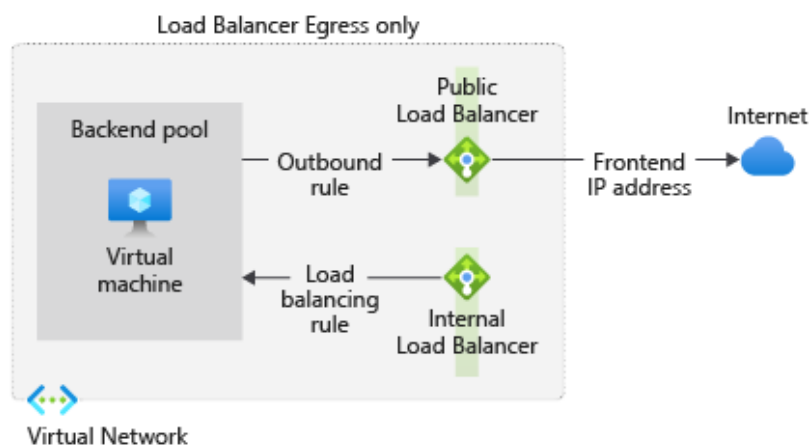
- [Traslado de los recursos a un nuevo grupo de recursos o a una nueva suscripción](#)
- [Traslado de máquinas virtuales de Azure a otra región](#)

# Configuración del equilibrador de carga solo de salida

23/09/2020 • 13 minutes to read • [Edit Online](#)

Use una combinación de equilibradores de carga estándar internos y externos para crear conectividad de salida para las máquinas virtuales situadas detrás de un equilibrador de carga interno.

Esta configuración proporciona NAT de salida en los escenarios de equilibradores de carga internos, lo que produce una configuración de "solo salida" para el grupo de back-end.



*Ilustración: Configuración de un equilibrador de carga solo de salida*

Esto son los pasos que se deben realizar:

1. Crear una red virtual con un host bastión.
2. Crear una máquina virtual solo con una dirección IP privada.
3. Crear equilibradores de carga estándar internos y públicos.
4. Agregar grupos de back-end a ambos equilibradores de carga y colocar la máquina virtual en cada grupo.
5. Conectarse a la máquina virtual a través del host bastión y:
  - a. Probar la conectividad de salida.
  - b. Configurar una regla de salida en el equilibrador de carga público.
  - c. Probar de nuevo la conectividad de salida.

## Creación de la red virtual y la máquina virtual

Cree una red virtual con dos subredes:

- Subred principal
- Subred bastión

Cree una máquina virtual en la nueva red virtual.

### Crear la red virtual

1. [Inicie sesión](#) en Azure Portal.
2. En la parte superior izquierda de la pantalla, seleccione **Crear un recurso** > **Redes** > **Red virtual** o busque **Red virtual** en el cuadro de búsqueda.
3. En **Crear red virtual**, escriba o seleccione esta información en la pestaña **Conceptos básicos**:

CONFIGURACIÓN	VALOR
<b>Detalles del proyecto</b>	
Suscripción	Selección de su suscripción a Azure
Grupo de recursos	Seleccione <b>Crear nuevo</b> . Escriba <b>myResourceGroupLB</b> . Seleccione <b>Aceptar</b> .
<b>Detalles de instancia</b>	
Nombre	Escriba <b>myVNet</b> .
Region	Seleccione <b>Este de EE. UU. 2</b> .

4. Seleccione la pestaña **Direcciones IP** o el botón **Siguiente: Direcciones IP** situado en la parte inferior de la página.

5. En la pestaña **Direcciones IP**, especifique esta información:

CONFIGURACIÓN	VALUE
Espacio de direcciones IPv4	Escriba <b>10.1.0.0/16</b> .

6. En **Nombre de subred**, seleccione la palabra **predeterminada**.

7. En **Editar subred**, especifique esta información:

CONFIGURACIÓN	VALUE
Nombre de subred	Escriba <b>myBackendSubnet</b> .
Intervalo de direcciones de subred	Escriba <b>10.1.0.0/24</b> .

8. Seleccione **Guardar**.

9. Seleccione la pestaña **Seguridad**.

10. En **BastionHost**, seleccione **Habilitar**. Escriba esta información:

CONFIGURACIÓN	VALUE
Nombre del bastión	Escriba <b>myBastionHost</b> .
Espacio de direcciones de AzureBastionSubnet	Escriba <b>10.1.1.0/24</b> .
Dirección IP pública	Seleccione <b>Crear nuevo</b> . En <b>Nombre</b> , escriba <b>myBastionIP</b> . Seleccione <b>Aceptar</b> .

11. Seleccione la pestaña **Revisar y crear** o el botón **Revisar y crear**.

12. Seleccione **Crear**.

## Creación de una máquina virtual

1. En la parte superior izquierda de Azure Portal, seleccione **Crear un recurso** > **Proceso** > **Máquina virtual**.

2. En **Crear una máquina virtual**, escriba o seleccione los valores en la pestaña **Básico**:

CONFIGURACIÓN	VALUE
<b>Detalles del proyecto</b>	
Suscripción	Selección de su suscripción a Azure
Grupo de recursos	Seleccione <b>myResourceGroupLB</b> .
<b>Detalles de instancia</b>	
Nombre de la máquina virtual	Escriba <b>myVM</b> .
Region	Seleccione <b>Este de EE. UU. 2</b> .
Opciones de disponibilidad	Seleccione <b>No se requiere redundancia de la infraestructura</b>
Imagen	Seleccione <b>Windows Server 2019 Datacenter</b> .
Instancia de Azure Spot	Seleccione <b>No</b> .
Size	Elija el tamaño de la máquina virtual o acepte la configuración predeterminada.
<b>Cuenta de administrador</b>	
Nombre de usuario	Escriba un nombre de usuario.
Contraseña	Escriba una contraseña.
Confirmar contraseña	Vuelva a escribir la contraseña.
<b>Reglas de puerto de entrada</b>	
Puertos de entrada públicos	Seleccione <b>Allow selected ports</b> (Permitir puertos seleccionados).
Selección de puertos de entrada	Seleccione <b>RDP (3389)</b> .

3. Seleccione la pestaña **Redes** o seleccione **Siguiente: Discos** y, después, **Siguiente: Redes**.

4. En la pestaña **Redes**, seleccione o escriba:

CONFIGURACIÓN	VALUE
<b>Interfaz de red</b>	
Virtual network	<b>myVNet</b>



CONFIGURACIÓN	VALUE
Subnet	myBackendSubnet
Dirección IP pública	Seleccione <b>Ninguno</b> .
Grupo de seguridad de red de NIC	Seleccione <b>Ninguno</b> .
¿Quiere colocar esta máquina virtual detrás de una solución de equilibrio de carga existente?	Seleccione <b>No</b> .

5. Seleccione la pestaña **Administración** o seleccione **Siguiente > Administración**.

6. En la pestaña **Administración**, seleccione o escriba:

CONFIGURACIÓN	VALUE
Supervisión	
Diagnósticos de arranque	Seleccione <b>Desactivado</b> .

7. Seleccione **Revisar + crear**.

8. Revise la configuración y, a continuación, seleccione **Crear**.

## Creación de equilibradores de carga y prueba de la conectividad

Use Azure Portal para crear los siguientes elementos:

- Equilibrador de carga interno
- Equilibrador de carga público

Agregue la máquina virtual creada al grupo de back-end de cada uno. A continuación, realizará una configuración para permitir solo la conectividad saliente desde la máquina virtual, que probará antes y después.

### Creación del equilibrador de carga interno

1. En la parte superior izquierda de la pantalla, seleccione **Crear un recurso > Redes > Load Balancer**.
2. En la pestaña **Conceptos básicos** de la página **Crear equilibrador de carga**, escriba o seleccione la siguiente información:

CONFIGURACIÓN	VALUE
Suscripción	Seleccione su suscripción.
Resource group	Seleccione <b>myResourceGroupLB</b> , que creó en el paso anterior.
Nombre	Escriba <b>myInternalLoadBalancer</b> .
Region	Seleccione <b>Este de EE. UU. 2</b> .
Tipo	seleccione <b>Interno</b> .
SKU	Seleccione <b>Estándar</b> .

CONFIGURACIÓN	VALUE
Virtual network	Seleccione <b>myVNet</b> , que creó en el paso anterior.
Subnet	Seleccione <b>myBackendSubnet</b> , que creó en el paso anterior.
Asignación de dirección IP	seleccione <b>Dinámico</b> .

3. Acepte los valores predeterminados en los demás valores y seleccione **Revisar y crear**.

4. En la pestaña **Revisar + crear**, seleccione **Crear**.

### Creación de un equilibrador de carga público

1. En la parte superior izquierda de la pantalla, seleccione **Crear un recurso > Redes > Load Balancer**.

2. En la pestaña **Conceptos básicos** de la página **Crear equilibrador de carga**, escriba o seleccione la siguiente información:

CONFIGURACIÓN	VALUE
Suscripción	Seleccione su suscripción.
Resource group	Seleccione <b>Crear nuevo</b> y escriba <b>MyResourceGroupLB</b> en el cuadro de texto.
Nombre	Escriba <b>myPublicLoadBalancer</b> .
Region	Seleccione <b>Este de EE. UU. 2</b> .
Tipo	Seleccione <b>Público</b> .
SKU	Seleccione <b>Estándar</b> .
Dirección IP pública	Seleccione <b>Crear nuevo</b> .
Nombre de la dirección IP pública	Escriba <b>myFrontendIP</b> en el cuadro de texto.
Zona de disponibilidad	Seleccione <b>Con redundancia de zona</b> .
Adición de una dirección IPv6 pública	así que seleccione <b>No</b> .

3. Acepte los valores predeterminados en los demás valores y seleccione **Revisar y crear**.

4. En la pestaña **Revisar + crear**, seleccione **Crear**.

### Creación de un grupo de direcciones de back-end interno

Cree el grupo de direcciones de back-end **myInternalBackendPool**:

1. Seleccione **Todos los servicios** en el menú de la izquierda, elija **Todos los recursos** y, después, seleccione **myLoadBalancer** en la lista de recursos.

2. En **Configuración**, seleccione **Grupos de back-end** y, a continuación, seleccione **Agregar**.

3. En la página **Add a backend pool** (Agregar un grupo de back-end), escriba **myBackendPool** como nombre del grupo de back-end.

4. En **Red virtual**, seleccione **myVNet**.
5. En **Máquinas virtuales**, seleccione **Agregar** y elija **myVM**.
6. Seleccione **Agregar**.

#### Creación de un grupo de direcciones de back-end público

Cree el grupo de direcciones de back-end **myPublicBackendPool**:

1. Seleccione **Todos los servicios** en el menú de la izquierda, elija **Todos los recursos** y, después, seleccione **myPublicLoadBalancer** en la lista de recursos.
2. En **Configuración**, seleccione **Grupos de back-end** y, a continuación, seleccione **Agregar**.
3. En la página **Add a backend pool** (Agregar un grupo de back-end), escriba **myPublicBackEndPool** como nombre del grupo de back-end.
4. En **Red virtual**, seleccione **myVNet**.
5. En **Máquinas virtuales**, seleccione **Agregar** y elija **myVM**.
6. Seleccione **Agregar**.

#### Prueba de la conectividad antes de la regla de salida

1. Seleccione **Todos los servicios** en el menú de la izquierda, elija **Todos los recursos** y, en la lista de recursos, seleccione **myVM**, que se encuentra en el grupo de recursos **myResourceGroupLB**.
2. En la página **Información general**, seleccione **Conectar** y, luego, **Bastion**.
3. Escriba el nombre de usuario y la contraseña especificados durante la creación de la máquina virtual.
4. Seleccione **Conectar**.
5. Abra Internet Explorer.
6. Escriba <https://whatsmyip.org> en la barra de direcciones.
7. Se producirá un error en la conexión. De forma predeterminada, el equilibrador de carga público estándar **no permite el tráfico saliente sin una regla de salida definida**.

#### Creación de una regla de salida del equilibrador de carga público

1. Seleccione **Todos los servicios** en el menú de la izquierda, elija **Todos los recursos** y, después, seleccione **myPublicLoadBalancer** en la lista de recursos.
2. En **Configuración**, seleccione **Reglas de salida** y, a continuación, seleccione **Agregar**.
3. Use estos valores para configurar las reglas de salida:

CONFIGURACIÓN	VALUE	
Nombre	Escriba <b>myOutboundRule</b> .	
Dirección IP del front-end	Seleccione <b>LoadBalancerFrontEnd</b> .	
Tiempo de espera de inactividad (minutos)	Mueva el control deslizante a <b>15 minutos</b> .	
Restablecimiento de TCP	Seleccione <b>Habilitado</b> .	
Grupo back-end	Seleccione <b>myPublicBackendPool</b> .	

CONFIGURACIÓN	VALUE	
Asignación de puertos: > Asignación de puertos	Seleccione <b>Use the default number of outbound ports</b> (Usar el número predeterminado de puertos de salida).	

4. Seleccione **Agregar**.

### Prueba de la conectividad después de la regla de salida

1. Seleccione **Todos los servicios** en el menú de la izquierda, elija **Todos los recursos** y, en la lista de recursos, seleccione **myVM**, que se encuentra en el grupo de recursos **myResourceGroupLB**.
2. En la página **Información general**, seleccione **Conectar** y, luego, **Bastion**.
3. Escriba el nombre de usuario y la contraseña especificados durante la creación de la máquina virtual.
4. Seleccione **Conectar**.
5. Abra Internet Explorer.
6. Escriba <https://whatsmyip.org> en la barra de direcciones.
7. La conexión funcionará correctamente.
8. La dirección IP mostrada debe ser la dirección IP de front-end de **myPublicLoadBalancer**.

## Limpieza de recursos

Cuando no los necesite, elimine el grupo de recursos, los equilibradores de carga, la máquina virtual y todos los recursos relacionados.

Para ello, seleccione el grupo de recursos **myResourceGroupLB** y, luego, elija **Eliminar**.

## Pasos siguientes

En este tutorial, se ha creado una configuración de "solo salida" con una combinación de equilibradores de carga públicos e internos.

Esta configuración permite equilibrar la carga del tráfico interno entrante en el grupo de back-end y, al mismo tiempo, evitar las conexiones entrantes públicas.

- Más información sobre [Azure Load Balancer](#).
- Aprenda sobre las [conexiones salientes en Azure](#).
- [Preguntas frecuentes sobre Load Balancer](#).
- Más información sobre [Azure Bastion](#).

# Solución de problemas de Azure Load Balancer

23/09/2020 • 23 minutes to read • [Edit Online](#)

En esta página se proporcionan soluciones de problemas para preguntas frecuentes sobre Azure Load Balancer Estándar y Básico. Para más información sobre Load Balancer Estándar, consulte [Introducción a Azure Load Balancer Estándar \(versión preliminar\)](#).

Cuando el equilibrador de carga no tenga conectividad, los síntomas más comunes son los siguientes:

- Las máquinas virtuales detrás del equilibrador de carga no responden a los sondeos de estado
- Las máquinas virtuales detrás del equilibrador de carga no responden al tráfico del puerto configurado

Cuando los clientes externos a las VM de back-end pasan a través del equilibrador de carga, se usará la dirección IP de los clientes para la comunicación. Asegúrese de que la dirección IP de los clientes se agregue a la lista de permitidos de NSG.

## Síntoma: Las máquinas virtuales detrás del equilibrador de carga no responden a los sondeos de estado

Para que los servidores back-end participen en el conjunto del equilibrador de carga, deben pasar la comprobación del sondeo. Para más información sobre los sondeos de estado, consulte [Descripción de los sondeos del equilibrador de carga](#).

Es posible que las máquinas virtuales del grupo de back-end del equilibrador de carga no responda a los sondeos por alguno de los motivos siguientes:

- Que una máquina virtual del grupo de back-end del equilibrador de carga esté dañada
- Que una máquina virtual del grupo de back-end del equilibrador de carga no escuche en el puerto de sondeo
- Que el firewall o un grupo de seguridad de red esté bloqueando el puerto de las máquinas virtuales del grupo de back-end del equilibrador de carga
- Otros errores de configuración del equilibrador de carga

### Causa 1: Que una máquina virtual del grupo de back-end del equilibrador de carga esté dañada

#### Validación y resolución

Para resolver este problema, inicie sesión en las máquinas virtuales participantes, compruebe si el estado de la máquina virtual es correcto y responde a **PsPing** o **TCPing** de otra máquina virtual del grupo. Si la máquina virtual está dañada o no responde al sondeo, debe corregir el problema y reparar la máquina virtual para que pueda volver a participar en el equilibrio de carga.

### Causa 2: Que una máquina virtual del grupo de back-end del equilibrador de carga no escuche en el puerto de sondeo

Si la máquina virtual está correcta, pero no responde al sondeo, una razón podría ser que el puerto de sondeo no esté abierto en la máquina virtual participante o que esta no escuche en ese puerto.

#### Validación y resolución

1. Inicie sesión en la máquina virtual de back-end.
2. Abra un símbolo del sistema y ejecute el siguiente comando para validar que existe una aplicación de escucha en el puerto de sondeo:  
`netstat -an`
3. Si el estado del puerto no aparece como **LISTENING** (ESCUCHANDO), configure el puerto correcto.

4. Como alternativa, seleccione otro puerto que aparezca como **LISTENING** (ESCUCHANDO) y actualice en consecuencia la configuración del equilibrador de carga.

### **Causa 3: Que el firewall o un grupo de seguridad de red esté bloqueando el puerto de las VM del grupo de back-end del equilibrador de carga**

Si el firewall de la máquina virtual está bloqueando el puerto de sondeo, o uno o varios grupos de seguridad de red configurados en la subred o en la máquina virtual no permite que el sondeo alcance el puerto, la máquina virtual no puede responder al sondeo de estado.

#### **Validación y resolución**

- Si el firewall está habilitado, compruebe si está configurado para permitir el puerto de sondeo. De lo contrario, configure el firewall para permitir el tráfico en el puerto de sondeo y pruebe de nuevo.
- En la lista de grupos de seguridad de red, compruebe si el tráfico entrante o saliente del puerto de sondeo tiene interferencias.
- Además, compruebe si hay una regla de grupos de seguridad de red **Deny All** en la NIC de la máquina virtual o la subred que tenga una prioridad mayor que la regla predeterminada que permite los sondeos de equilibrio de carga y tráfico (los grupos de seguridad de red deben permitir la dirección IP del equilibrador de carga 168.63.129.16).
- Si cualquiera de estas reglas bloquea el tráfico del sondeo, elimine y vuelva a configurar las reglas para permitirlo.
- Pruebe si la máquina virtual ahora responde a los sondeos de estado.

### **Causa 4: Otros errores de configuración del equilibrador de carga**

Si parece que los motivos anteriores se han validado y resuelto correctamente, y aun así la máquina virtual de back-end sigue sin responder al sondeo de estado, compruebe manualmente la conectividad y recopile algunos seguimientos para entenderla.

#### **Validación y resolución**

- Use **Psping** de una de las otras máquinas virtuales dentro de la red virtual para probar la respuesta del puerto de sondeo (ejemplo: `.\psping.exe -t 10.0.0.4:3389`) y registre los resultados.
- Use **TCPing** de una de las otras máquinas virtuales dentro de la red virtual para probar la respuesta del puerto de sondeo (ejemplo: `.\tcping.exe 10.0.0.4 3389`) y registre los resultados.
- Si no se recibe respuesta con estas pruebas de ping:
  - Ejecute un seguimiento Netsh en la máquina virtual del grupo de back-end de destino y en otra máquina virtual de prueba de la misma red virtual simultáneamente. Ahora, ejecute una prueba de PsPing durante algún tiempo, recopile seguimientos de red y detenga la prueba.
  - Analizar la captura de red y observe si hay paquetes entrantes y salientes relacionados con la consulta de ping.
    - Si no se observan paquetes entrantes se observan en la máquina virtual del grupo de back-end, puede haber grupos de seguridad de red o una configuración incorrecta de UDR que bloquee el tráfico.
    - Si no se observan paquetes salientes en la máquina virtual del grupo de back-end, la máquina virtual podría tener otros problemas ajenos (por ejemplo, que la aplicación bloquee el puerto de sondeo).
  - Compruebe si los paquetes de sondeo se fuerzan a otro destino (probablemente mediante la configuración de UDR) antes de alcanzar el equilibrador de carga. Esto puede hacer que el tráfico nunca alcance la máquina virtual de back-end.
- Cambiar el tipo de sondeo (por ejemplo, de HTTP a TCP) y configure el puerto correspondiente en las ACL de los grupos de seguridad de red y firewall para comprobar si el problema está relacionado con la configuración de respuesta del sondeo. Para más información acerca de la configuración del sondeo de estado, consulte [Endpoint Load Balancing health probe configuration](#) (Configuración del sondeo de estado en el punto de conexión del

equilibrador de carga).

## Síntoma: Las VM detrás del equilibrador de carga no responden al tráfico del puerto de datos configurado

Si una máquina virtual del grupo de back-end aparece como correcta y responde a los sondeos de estado, pero aun así no participa en el equilibrio de carga o no responde al tráfico de datos, puede deberse a alguno de los motivos siguientes:

- Que una máquina virtual del grupo de back-end del equilibrador de carga no escuche en el puerto de datos
- Que un grupo de seguridad de red esté bloqueando el puerto de la máquina virtual del grupo de back-end del equilibrador de carga
- Que se acceda al equilibrador de carga desde la misma máquina virtual y NIC
- Que se acceda al front-end del equilibrador de carga en Internet desde la máquina virtual del grupo de back-end del equilibrador de carga participante

### Causa 1: Que una VM del grupo de back-end del equilibrador de carga no escuche en el puerto de datos

Si una máquina virtual no responde al tráfico de datos, puede deberse a que el puerto de destino no esté abierto en la máquina virtual participante, o a que la máquina virtual no escuche en ese puerto.

#### Validación y resolución

1. Inicie sesión en la máquina virtual de back-end.
2. Abra un símbolo del sistema y ejecute el siguiente comando para validar que existe una aplicación de escucha en el puerto de datos: `netstat -an`
3. Si el puerto no aparece con el estado "LISTENING" (ESCUCHANDO), configure el puerto de escucha
4. Si el puerto está marcado como Listening (Escuchando), compruebe si hay problemas en la aplicación de destino de ese puerto.

### Causa 2: Que un grupo de seguridad de red esté bloqueando el puerto de la máquina virtual del grupo de back-end del equilibrador de carga

Si uno o varios grupos de seguridad de red configurados en la subred o en la máquina virtual bloquean la dirección IP de origen o el puerto, la máquina virtual no puede responder.

En el caso del equilibrador de carga público, la dirección IP de los clientes de Internet se usará para la comunicación entre los clientes y las VM de back-end del equilibrador de carga. Asegúrese de que la dirección IP de los clientes esté permitida en el grupo de seguridad de red de la VM de back-end.

1. Enumere los grupos de seguridad de red configurados en la máquina virtual de back-end. Para más información, consulte [Administración de los grupos de seguridad de red](#).
2. En la lista de grupos de seguridad de red, compruebe si:
  - el tráfico entrante o saliente del puerto de datos tiene interferencias.
  - hay una regla de grupos de seguridad de red **Deny All** en la NIC de la máquina virtual o la subred que tenga una prioridad mayor que la regla predeterminada que permite los sondeos del equilibrador de carga y de tráfico (los grupos de seguridad de red deben permitir la dirección IP del equilibrador de carga 168.63.129.16, que es el puerto de sondeo)
3. Si cualquiera de estas reglas bloquea el tráfico, elimine y vuelva a configurar las reglas para permitir el tráfico de datos.
4. Pruebe si la máquina virtual ahora responde a los sondeos de estado.

### Causa 3: Acceso al equilibrador de carga desde la misma VM e interfaz de red

Que la aplicación hospedada en la máquina virtual de back-end del equilibrador de carga intente acceder a otra aplicación que se hospeda en la misma máquina virtual de back-end a través de la misma interfaz de red es un escenario incompatible y producirá un error.

**Resolución:** Este problema se puede resolver por una de las siguientes vías:

- Configure las máquinas virtuales del grupo de back-end por separado para cada aplicación.
- Configure la aplicación en máquinas virtuales de NIC doble para que cada aplicación use su propia interfaz de red y dirección IP.

#### **Causa 4: Acceso al front-end del equilibrador de carga interno desde la VM del grupo de back-end del equilibrador de carga participante**

Si se configura un equilibrador de carga interno dentro de una red virtual y una de las máquinas virtuales de back-end participantes intenta acceder al front-end de este, pueden producirse errores al asignar el flujo a la máquina virtual original. No se admite este escenario.

**Solución:** hay varias maneras para desbloquear este escenario, incluido el uso de un proxy. Evalúe Application Gateway u otros proxys de terceros (por ejemplo, nginx o haproxy). Para más información acerca de Application Gateway, consulte [Introducción a Application Gateway](#)

**Detalles:** los equilibradores de carga internos no traducen las conexiones de salida que se originan en el front-end de un equilibrador de carga interno, porque ambos están en un espacio de direcciones IP privadas. Los equilibradores de carga públicos proporcionan [conexiones salientes](#) desde direcciones IP privadas dentro de la red virtual a direcciones IP públicas. En el caso de los equilibradores de carga internos, este enfoque evita el agotamiento del puerto SNAT potencial en un espacio de direcciones IP interno único, donde no se requiere traducción.

Un efecto secundario es que si un flujo de salida de una máquina virtual del grupo de servidores back-end intenta un flujo hacia el front-end del Load Balancer interno en su grupo y se asigna a sí mismo, las dos piernas del flujo no coinciden. Dado que no coinciden, se produce un error en el flujo. El flujo se realiza correctamente si el flujo no se ha asignado a la misma máquina virtual del grupo de servidores back-end que creó el flujo al front-end.

Cuando el flujo se vuelve a asignar a sí mismo, el flujo de salida parece originarse desde la máquina virtual hasta el front-end y el flujo de entrada correspondiente parece provenir de la máquina virtual. Desde el punto de vista del sistema operativo invitado, las partes entrantes y salientes del mismo flujo no coinciden dentro de la máquina virtual. La pila TCP no reconocerá estas mitades del mismo flujo como parte del mismo flujo. El origen y el destino no coinciden. Cuando el flujo se asigna a cualquier otra máquina virtual del grupo de back-end, las mitades del flujo coinciden y la máquina virtual puede responder al flujo.

El síntoma de este escenario es el tiempo de espera de conexión intermitente cuando el flujo vuelve al mismo back-end que originó el flujo. Las soluciones alternativas comunes incluyen la inserción de una capa de proxy detrás del Load Balancer interno y el uso de reglas de estilo de Direct Server Return (DSR). Para más información, consulte [Varios front-ends para Azure Load Balancer](#).

Puede combinar una Load Balancer interna con cualquier proxy de terceros o usar el [Application Gateway](#) interno para escenarios de proxy con HTTP/HTTPS. Aunque podría usar un Load Balancer público para mitigar este problema, el escenario resultante es propenso a [agotamiento de SNAT](#). Evite este segundo enfoque a menos que se administre con cuidado.

**Síntoma:** No se puede cambiar el puerto de back-end para la regla de LB existente para un equilibrador de carga con un conjunto de escalado de máquinas virtuales implementado en el grupo de servidores back-end.

**Causa:** no se puede modificar el puerto de back-end para una regla de equilibrio de carga que usa un sondeo de estado para el equilibrador de carga al que el conjunto de escalado de máquinas virtuales hace referencia.

**Resolución:** para cambiar el puerto, puede quitar el sondeo de estado mediante la actualización del conjunto de escalado de máquinas virtuales, actualizar el puerto y, a continuación, volver a configurar el sondeo de estado.



**Síntoma:** El tráfico pequeño sigue pasando a través del equilibrador de carga después de quitar las VM del grupo de back-end del equilibrador de carga.

**Causa:** Las VM que se quitan del grupo de back-end ya no deben recibir tráfico. La pequeña cantidad de tráfico de red podría estar relacionada con el almacenamiento, DNS y otras funciones de Azure.

Para comprobarlo, puede realizar un seguimiento de red. El FQDN que se usa para las cuentas de almacenamiento de blobs se muestra en las propiedades de cada cuenta de almacenamiento. Desde una máquina virtual dentro de la suscripción de Azure, puede realizar una nslookup para determinar la dirección IP de Azure asignada a esa cuenta de almacenamiento.

## Capturas de red adicionales

Si decide abrir un caso de soporte técnico, recopile la información siguiente para una resolución más rápida. Elija una sola máquina virtual de back-end para realizar las pruebas siguientes:

- Use Psping de una de las máquinas virtuales de back-end de la red virtual para probar la respuesta del puerto de sondeo (ejemplo: psping 10.0.0.4:3389) y registre los resultados.
- Si no se recibe respuesta con estas pruebas de ping, ejecute un seguimiento Netsh simultáneo en la máquina virtual de back-end y la máquina virtual de prueba de la red virtual mientras ejecuta PsPing y detenga el seguimiento Netsh.

## Pasos siguientes

Si los pasos anteriores no resuelven el problema, abra una [incidencia de soporte técnico](#).

# Solución de errores comunes de implementación de Azure con Azure Load Balancer

23/09/2020 • 6 minutes to read • [Edit Online](#)

En este artículo se describen algunos errores comunes de implementación de Azure Load Balancer y se proporciona información sobre cómo resolverlos. Si busca información sobre un código de error y esa información no se proporciona en este artículo, háganoslo saber. En la parte inferior de esta página, puede dejar comentarios. Se realiza un seguimiento de los comentarios con problemas de GitHub.

## Códigos de error

CÓDIGO DE ERROR	DETALLES Y MITIGACIÓN
DifferentSkuLoadBalancersAndPublicIpAddressNotAllowed	Las SKU de la IP pública y de Load Balancer deben coincidir. Asegúrese de que las SKU de la IP pública y de Azure Load Balancer coincidan. Se recomienda usar SKU estándar para cargas de trabajo de producción. Más información sobre las <a href="#">diferencias en las SKU</a>
DifferentSkuLoadBalancerAndPublicIpAddressNotAllowedInVMSS	Los conjuntos de escalado de máquinas virtuales usan Basic Load Balancer de forma predeterminada cuando no se especifica la SKU o se implementa sin direcciones IP públicas estándar. Vuelva a implementar el conjunto de escalado de máquinas virtuales con direcciones IP públicas estándar en las instancias individuales para asegurarse de que ha seleccionado Standard Load Balancer, o simplemente seleccione un equilibrador de carga estándar al implementar el conjunto de escalado de máquinas virtuales en Azure Portal.
MaxAvailabilitySetsInLoadBalancerReached	El grupo de back-end de un equilibrador de carga puede contener como máximo 150 conjuntos de disponibilidad. Si no tiene conjuntos de disponibilidad definidos explícitamente para las máquinas virtuales en el grupo de back-end, cada máquina virtual individual entra en su propio conjunto de disponibilidad. Por lo tanto, la implementación de 150 máquinas virtuales independientes implicaría que tendría 150 conjuntos de disponibilidad, lo que alcanza el límite. Puede implementar un conjunto de disponibilidad y agregarle más máquinas virtuales como solución alternativa.
NetworkInterfaceAndLoadBalancerAreInDifferentAvailabilitySets	En el caso del equilibrador de carga de la SKU básica, la interfaz de red y el equilibrador de carga deben estar en el mismo conjunto de disponibilidad.
RulesOfSameLoadBalancerTypeUseSameBackendPortProtocolAndIPConfig	Un conjunto de escalado de máquinas virtuales solo puede hacer referencia a una regla en un tipo de equilibrador de carga determinado (interno, público) con el mismo puerto de back-end y protocolo. Actualice la regla para cambiar esta creación de regla duplicada.

CÓDIGO DE ERROR	DETALLES Y MITIGACIÓN
RulesOfSameLoadBalancerTypeUseSameBackendPortProtocolAndVmssIPConfig	Un conjunto de escalado de máquinas virtuales solo puede hacer referencia a una regla en un tipo de equilibrador de carga determinado (interno, público) con el mismo puerto de back-end y protocolo. Actualice los parámetros de la regla para cambiar esta creación de regla duplicada.
AnotherInternalLoadBalancerExists	Solo puede tener un equilibrador de carga de tipo interno que haga referencia al mismo conjunto de interfaces de red o máquinas virtuales en el back-end del equilibrador de carga. Actualice la implementación para asegurarse de que está creando solo una instancia de Load Balancer del mismo tipo.
CannotUseInactiveHealthProbe	No puede tener un sondeo que no lo use ninguna regla configurada para el mantenimiento del conjunto de escalado de máquinas virtuales. Asegúrese de que el sondeo que se está configurando se use activamente.
VMScaleSetCannotUseMultipleLoadBalancersOfSameType	No puede tener varios equilibradores de carga del mismo tipo (interno, público). Puede tener un equilibrador de carga público interno como máximo.
VMScaleSetCannotReferenceLoadbalancerWhenLargeScaleOrCrossAZ	No se admite Basic Load Balancer para conjuntos de escalado de máquinas virtuales de múltiples ubicaciones o para el conjunto de escalado de máquinas virtuales de varias zonas de disponibilidad. Use Standard Load Balancer en su lugar.
MarketplacePurchaseEligibilityFailed	Cambie a la cuenta administrativa correcta para habilitar las compras debido a que la suscripción es una suscripción EA. Puede leer más <a href="#">aquí</a> .
ResourceDeploymentFailure	<p>Si el equilibrador de carga está en un estado de error, siga estos pasos para recuperarlo de dicho estado:</p> <ol style="list-style-type: none"> <li>1. Vaya a <a href="https://resources.azure.com">https://resources.azure.com</a> e inicie sesión con las credenciales de Azure Portal.</li> <li>2. Seleccione <b>Lectura o escritura</b>.</li> <li>3. A la izquierda, expanda <b>Suscripciones</b> y, a continuación, expanda la suscripción con la instancia de Load Balancer que se va a actualizar.</li> <li>4. Expanda <b>ResourceGroups</b> y, a continuación, expanda el grupo de recursos con la instancia de Load Balancer que se va a actualizar.</li> <li>5. Seleccione <b>Microsoft.Network &gt; LoadBalancers</b> y, a continuación, seleccione la instancia de Load Balancer que se va a actualizar, <b>LoadBalancer_1</b>.</li> <li>6. En la página para mostrar de <b>LoadBalancer_1</b>, seleccione <b>GET &gt; Editar</b>.</li> <li>7. Actualice el valor de <b>ProvisioningState</b> de <b>Incorrecto</b> a <b>Correcto</b>.</li> <li>8. Seleccione <b>PUT</b>.</li> </ol>

## Pasos siguientes

- Consulte la [tabla de comparación de SKU](#) de Azure Load Balancer
- Más información sobre los [límites de Azure Load Balancer](#).

# Solución de errores de conexiones salientes

23/09/2020 • 14 minutes to read • [Edit Online](#)

Este artículo está diseñado para proporcionar soluciones a los problemas habituales que pueden producirse con conexiones salientes de una instancia de Azure Load Balancer. La mayoría de los problemas con la conectividad saliente que experimentan los clientes se deben al agotamiento de puertos SNAT y a tiempos de espera de conexión agotados que generan pérdida de paquetes. En este artículo se proporcionan los pasos para mitigar cada uno de estos problemas.

## Administración del agotamiento de puertos SNAT (PAT)

Los [puertos efímeros](#) usados para [PAT](#) son un recurso agotable, como se describe en [Máquina virtual independiente sin una dirección IP pública](#) y [Máquina virtual de carga equilibrada sin dirección IP pública](#). Puede supervisar el uso de puertos efímeros y compararlos con su asignación actual para determinar la probabilidad o confirmar el agotamiento de SNAT mediante [esta guía](#).

Si sabe que se van a iniciar muchas conexiones TCP o UDP salientes a la misma dirección IP y puerto de destino, y observa errores en las conexiones salientes, o el soporte técnico está avisando del agotamiento de los puertos SNAT ([puertos efímeros](#) asignados previamente usados por [PAT](#)), dispone de varias opciones generales para mitigar este problema. Revise estas opciones y vea cuál está disponible y resulta mejor para su escenario. Es posible que una o varias de ellas puedan ayudar a administrar este escenario.

Si tiene problemas para entender el comportamiento de las conexiones de salida, puede usar las estadísticas de pila IP (netstat). O bien, puede ser útil observar el comportamiento de la conexión mediante capturas de paquetes. Estas capturas de paquetes se pueden realizar en el sistema operativo invitado de la instancia o se puede usar [Network Watcher para la captura de paquetes](#).

## Asignación manual de puertos SNAT para maximizar puertos SNAT por máquina virtual

Como se define en los [puertos preasignados](#), el equilibrador de carga asignará automáticamente los puertos según el número de máquinas virtuales en el back-end. De forma predeterminada, esto se hace con cautela para garantizar la escalabilidad. Si conoce el número máximo de máquinas virtuales que tendrá en el back-end, puede asignar manualmente puertos SNAT en cada regla de salida. Por ejemplo, si sabe que va a tener un máximo de 10 máquinas virtuales, puede asignar 6400 puertos SNAT por máquina virtual en lugar del valor predeterminado 1024.

## Modificación de la aplicación para reutilizar las conexiones

Puede reducir la demanda de puertos efímeros utilizados para SNAT mediante la reutilización de conexiones en la aplicación. Esta es especialmente importante para protocolos como HTTP/1.1, en los que la reutilización de las conexiones es la opción predeterminada. Y, a su vez, se pueden beneficiar otros protocolos que usan HTTP como transporte (por ejemplo, REST).

La reutilización es siempre preferible a conexiones individuales atómicas para cada solicitud. La reutilización tiene como resultado transacciones TCP muy eficientes y con un mayor rendimiento.

## Modificación de la aplicación para usar la agrupación de conexiones

Puede emplear un esquema de agrupación de conexiones en la aplicación, donde las solicitudes se distribuyan

internamente a través de un conjunto fijo de conexiones (cada una reutilizada siempre que sea posible). Este esquema limita el número de puertos efímeros en uso y crea un entorno más predecible. También puede aumentar el rendimiento de las solicitudes al permitir varias operaciones simultáneas cuando una sola conexión bloquea la respuesta de una operación.

La agrupación de conexiones puede existir ya en el marco de trabajo que se use para desarrollar la aplicación o su configuración. Se puede combinar la agrupación de conexiones con la reutilización de conexiones. Así, sus múltiples conexiones consumen un número fijo y predecible de puertos para la misma dirección IP y el mismo puerto de destino. Las solicitudes también se benefician del uso eficiente de transacciones TCP que reducen la latencia y la utilización de recursos. Las transacciones UDP también pueden beneficiarse, dado que administrar el número de flujos de UDP puede evitar, a su vez, condiciones de administración del agotamiento de los puertos SNAT.

## Modificación de la aplicación para utilizar lógica de reintento menos agresiva

Cuando se agotan los [puertos efímeros asignados previamente](#) usados para [PAT](#) o se producen errores de la aplicación, los reintentos agresivos o por fuerza bruta sin lógica de retroceso y decadencia causan que se produzca el agotamiento o su persistencia. Puede reducir la demanda de puertos efímeros mediante el uso de una lógica de reintento menos agresiva.

Los puertos efímeros tienen un tiempo de inactividad de 4 minutos (no ajustable). Si los reintentos son demasiado agresivos, el agotamiento no tiene ninguna oportunidad de solucionarlo por sí mismo. Por lo tanto, una parte fundamental del diseño es considerar cómo y con qué frecuencia la aplicación vuelve a intentar las transacciones.

## Asignación de una IP pública a cada máquina virtual

La asignación de una dirección IP pública cambia el escenario a [IP pública a una máquina virtual](#). Todos los puertos efímeros de la dirección IP pública que se usan para cada máquina virtual están disponibles para la máquina virtual. (En contraste con los escenarios donde los puertos efímeros de una dirección IP pública se comparten con todas las máquinas virtuales asociadas al grupo back-end respectivo). Existen ventajas e inconvenientes que deben considerarse, como el costo adicional de las direcciones IP públicas y el posible impacto de la creación de listas de permitidos con un gran número de direcciones IP individuales.

### NOTE

Esta opción no está disponible para roles de trabajo web.

## Uso de varios servidores front-end

Cuando se usa Load Balancer estándar público, se asignan [varias direcciones IP de servidor front-end para las conexiones salientes](#) y [se multiplica el número de puertos SNAT disponibles](#). Cree una configuración de IP de servidor front-end, una regla y el grupo de servidores back-end para desencadenar la programación de SNAT para la dirección IP pública del servidor front-end. La regla no tiene que funcionar y no es necesario que el sondeo de estado sea correcto. Si usa varios servidores front-end para la entrada también (en lugar de simplemente para la salida), debe usar además sondeos de estado personalizados para garantizar la confiabilidad.

### NOTE

En la mayoría de los casos, el agotamiento de puertos SNAT indica que el diseño es incorrecto. Asegúrese de saber por qué está agotando los puertos antes de usar más servidores front-end para agregar puertos SNAT. Puede estar enmascarando un problema que podría provocar un error más adelante.

# Escalado horizontal

Los [puertos preasignados](#) se asignan según el tamaño del grupo de back-end y se agrupan en niveles para minimizar la interrupción cuando algunos de los puertos tengan que reasignarse para alojar el siguiente nivel de tamaño superior de grupo de back-end. Podría tener la opción de aumentar la utilización de puertos SNAT para un front-end determinado si ajusta el grupo de back-end al tamaño máximo de un nivel determinado. Tenga en cuenta que la asignación de puertos predeterminada es necesaria para que la aplicación se escale horizontalmente de forma eficaz sin que haya riesgo de agotamiento de SNAT.

Por ejemplo, dos máquinas virtuales en el grupo back-end tendrían 1024 puertos SNAT disponibles por cada configuración de IP, lo que permite un total de 2048 puertos SNAT para la implementación. Si la implementación fuera a aumentarse hasta 50 máquinas virtuales, incluso si el número de puertos preasignados permanece constante por máquina virtual, se puede utilizar un total de 51 200 (50 x 1024) puertos SNAT por la implementación. Si quiere escalar horizontalmente la implementación, compruebe el número de [puertos preasignados](#) por cada nivel para asegurarse de adaptar el escalado horizontal al máximo del nivel correspondiente. En el ejemplo anterior, si hubiera elegido escalar horizontalmente a 51 en lugar de a 50 instancias, avanzaría al nivel siguiente y terminaría con menos puertos SNAT por VM, así como en total.

Si se escala horizontalmente al siguiente nivel de grupo de back-end de mayor tamaño, algunas de las conexiones salientes podrían agotar el tiempo de espera si hubiera que reasignar los puertos. Si solo usa algunos de los puertos SNAT, no importa si se escala horizontalmente al siguiente mayor tamaño de grupo de back-end. La mitad de los puertos existentes se volverá a asignar cada vez que cambie al siguiente nivel de grupo de back-end. Si no quiere que suceda esto, tendrá que adaptar la implementación al tamaño del nivel. O bien, asegúrese de que la aplicación puede detectar y volver a intentar según se requiera. Las conexiones persistentes de TCP pueden ayudar a detectar cuándo dejan de funcionar los puertos SNAT por una reasignación.

## Uso de conexiones persistentes para restablecer el tiempo de espera de inactividad saliente

Las conexiones salientes tienen un tiempo de espera de inactividad de 4 minutos. Este tiempo de espera se ajusta desde [Reglas de salida](#). Pero también puede usar conexiones persistentes de transporte (por ejemplo, TCP) o de capa de aplicación para actualizar un flujo de inactividad y restablecer este tiempo de espera de inactividad en caso necesario.

Al utilizar conexiones persistentes de TCP, es suficiente con habilitarlas en un lado de la conexión. Por ejemplo, es suficiente habilitarlas solo en el servidor para restablecer el temporizador de inactividad del flujo y no se necesita para ambos lados en conexiones persistentes de TCP iniciadas. Existen conceptos similares existen para la capa de aplicación, incluidas las configuraciones de cliente/servidor de base de datos. Compruebe el lado del servidor para ver qué opciones existen para las conexiones persistentes específicas de la aplicación.

## Pasos siguientes

Siempre buscamos mejorar la experiencia de nuestros clientes. Si tiene problemas con la conectividad saliente que no aparecen o no se resuelven en este artículo, envíe sus comentarios a través de GitHub desde la parte inferior de la página y abordaremos sus comentarios lo antes posible.

# Solución de problemas de disponibilidad de front-end y back-end y de mantenimiento de recursos

23/09/2020 • 11 minutes to read • [Edit Online](#)

Este artículo sirve de guía para investigar los problemas que afectan a la disponibilidad de la IP de front-end y los recursos de back-end del equilibrador de carga.

## Acerca de las métricas que se van a usar

Las dos métricas que se van a usar son la *disponibilidad de la ruta de acceso de datos* y el *estado de sondeo de mantenimiento*, y es importante comprender su significado para obtener información correcta.

## Disponibilidad de la ruta de acceso de datos

La métrica de disponibilidad de la ruta de acceso de datos se genera mediante un ping de TCP cada 25 segundos en todos los puertos de front-end que tienen configuradas reglas NAT de entrada y de equilibrio de carga. Después, este ping de TCP se enrutará a cualquiera de las instancias de back-end correctas (comprobadas). Si el servicio recibe una respuesta al ping, se considera un éxito y la suma de la métrica se iterará una vez, en caso de que se produzca un error, no se iterará. El recuento de esta métrica es 1/100 del total de pings de TCP por período de muestra. Por lo tanto, debemos considerar el promedio, que mostrará el promedio de suma/recuento para el período de tiempo. La métrica de disponibilidad de la ruta de acceso de datos agregada por promedio nos ofrece un porcentaje de tasa de éxito para los pings de TCP en la dirección IP:puerto de front-end para cada una de las reglas NAT de entrada y de equilibrio de carga.

## Estado del sondeo de mantenimiento

La métrica de estado del sondeo de mantenimiento se genera mediante un ping del protocolo definido en el sondeo de estado. Este ping se envía a cada instancia del grupo de back-end y del puerto definido en el sondeo de estado. En el caso de sondeos HTTP y HTTPS, un ping correcto requiere una respuesta HTTP 200 Correcto, mientras que en los sondeos TCP, cualquier respuesta se considera correcta. Los errores o éxitos consecutivos de cada sondeo determinan si una instancia de back-end es correcta y puede recibir tráfico para las reglas de equilibrio de carga a las que el grupo de back-end está asignado. De manera similar al caso de la disponibilidad de la ruta de acceso de datos, usamos la agregación de promedio, que nos indica el promedio de pings correctos y totales durante el intervalo de muestreo. Este valor del estado de sondeo de mantenimiento indica el estado del back-end en aislamiento del equilibrador de carga, mediante el sondeo de las instancias de back-end sin enviar tráfico a través del front-end.

### IMPORTANT

El estado de sondeo de mantenimiento se muestra cada minuto. Esto puede dar lugar a fluctuaciones menores en un valor que, en otro caso, sería constante. Por ejemplo, si hay dos instancias de back-end, una sondeada como correcta y otra como incorrecta, el servicio de sondeo de estado puede capturar 7 muestras para la instancia correcta y 6 para la instancia incorrecta. Esto hará que un valor 50, previamente constante, se muestre como 46,15 para un intervalo de un minuto.

## Diagnóstico de equilibradores de carga degradados y no disponibles

Como se describe en el [artículo sobre el mantenimiento de los recursos](#), un equilibrador de carga degradado es aquel que muestra entre el 25 % y el 90 % de disponibilidad de la ruta de acceso de datos, y un equilibrador de

carga no disponible es el que tiene menos del 25 % de disponibilidad de la ruta de acceso de datos, durante un período de dos minutos. Se pueden seguir estos mismos pasos para investigar los errores observados en cualquier estado de sondeo de mantenimiento o alertas de disponibilidad de ruta de acceso de datos que haya configurado. Exploraremos el caso en el que comprobamos el mantenimiento de los recursos y encontramos que el equilibrador de carga tiene una disponibilidad de la ruta de acceso de datos del 0 %; es decir, nuestro servicio está inactivo.

En primer lugar, vamos a la vista de métricas detalladas de nuestra hoja de información del equilibrador de carga. Puede hacerlo a través de la hoja de recursos del equilibrador de carga o el vínculo del mensaje de mantenimiento de los recursos. Después, vaya a la pestaña de disponibilidad de front-end y back-end y revise una ventana de treinta minutos del período de tiempo en el que se produjo el estado de degradación o de no disponibilidad. Si vemos que la disponibilidad de la ruta de acceso a los datos ha sido del 0 %, sabemos que hay un problema que impide el tráfico para todas nuestras reglas NAT de entrada y de equilibrio de carga, y se puede ver cuánto tiempo ha durado este impacto.

Lo siguiente que necesitamos mirar es nuestra métrica de estado de sondeo de mantenimiento para determinar si la ruta de acceso a los datos no está disponible porque no tenemos instancias de back-end correctas para atender el tráfico. Si tenemos al menos una instancia de back-end correcta para todas nuestras reglas de equilibrio de carga y de entrada, sabemos que no es nuestra configuración la causa de que las rutas de acceso de datos no estén disponibles. Este escenario puede indicar un problema de la plataforma Azure, aunque es poco frecuente, pero no debe preocuparse, ya que se envía una alerta automatizada a nuestro equipo para resolver rápidamente todos los problemas de la plataforma.

## Diagnóstico de errores de sondeo de estado

Supongamos que comprobamos el estado de sondeo de mantenimiento y encontramos que todas las instancias aparecen como incorrectas. Esto explica por qué nuestra ruta de acceso a datos no está disponible, ya que el tráfico no tiene ninguna instancia a la que ir. Debemos recorrer la siguiente lista de comprobación para descartar los errores de configuración comunes:

- Compruebe el uso de CPU de los recursos para comprobar si las instancias son realmente correctas.
  - Puede comprobar esto.
- Si se usa una comprobación de sondeo HTTP o HTTPS, si la aplicación es correcta y responde.
  - Valide si es funcional accediendo directamente a las aplicaciones a través de la dirección IP privada o la dirección IP pública de nivel de instancia asociada a la instancia de back-end.
- Revise los grupos de seguridad de red que se aplican a nuestros recursos de back-end. Asegúrese de que no hay ninguna regla con una prioridad mayor que AllowAzureLoadBalancerInBound, lo que bloquearía el sondeo de estado.
  - Para ello, visite la hoja de redes de las máquinas virtuales de back-end o Virtual Machine Scale Sets
  - Si existe este problema de NSG, mueva la regla de permiso existente o cree una nueva regla de prioridad alta para permitir el tráfico de AzureLoadBalancer.
- Compruebe el sistema operativo. Asegúrese de que las máquinas virtuales están escuchando en el puerto de sondeo y revise las reglas de firewall del sistema operativo para asegurarse de que no estén bloqueando el tráfico de sondeo procedente de la dirección IP 168.63.129.16.
  - Puede comprobar los puertos de escucha ejecutando netstat -a en el símbolo del sistema de Windows o netstat-l en un terminal de Linux.
- No coloque una máquina virtual NVA de firewall en el grupo de back-end del equilibrador de carga, use [rutas definidas por el usuario](#) para enrutar el tráfico a las instancias de back-end a través del firewall.
- Asegúrese de que usa el protocolo correcto, si usa HTTP para sondear un puerto que escucha una aplicación que no es HTTP, se producirá un error en el sondeo.

Si ha recorrido esta lista de comprobación y todavía se producen errores de sondeo de estado, puede haber problemas de plataforma poco frecuentes que afecten al servicio de sondeo para las instancias. En este caso, Azure le respaldará. Se envía una alerta automatizada a nuestro equipo para resolver rápidamente todos los problemas



de la plataforma.

## Pasos siguientes

- [Más información sobre los sondeos de estado de Azure Load Balancer](#)
- [Más información sobre las métricas de Azure Load Balancer](#)

# Preguntas frecuentes sobre Load Balancer

23/09/2020 • 9 minutes to read • [Edit Online](#)

## ¿Qué tipos de Load Balancer existen?

Equilibradores de carga internos que equilibran el tráfico dentro de una red virtual y equilibradores de carga externos que equilibran el tráfico hacia y desde un punto de conexión conectado a Internet. Para más información, consulte [Tipos de Load Balancer](#).

Para ambos tipos, Azure ofrece una SKU básica y una SKU estándar que tienen diferentes capacidades funcionales, de rendimiento, de seguridad y de seguimiento de estado. Estas diferencias se explican en el artículo [Comparación de SKU](#).

## ¿Cómo puedo actualizar de la versión Basic de Load Balancer a la versión Standard?

Consulte el artículo [Actualización de Basic a Standard](#) para obtener una secuencia de comandos automatizada e instrucciones sobre la actualización de una SKU de Load Balancer.

## ¿Cuáles son las diferentes opciones de equilibrio de carga en Azure?

Consulte la [Guía de tecnología de Load Balancer](#) para conocer los servicios de equilibrio de carga disponibles y los usos recomendados para cada uno.

## ¿Dónde puedo encontrar plantillas de Resource Manager para Load Balancer?

Consulte la [lista de plantillas de inicio rápido de Azure Load Balancer](#) para conocer las plantillas de Resource Manager de las implementaciones comunes.

## ¿En qué se diferencian las reglas NAT de entrada de las reglas de equilibrio de carga?

Las reglas NAT se usan para especificar un recurso de back-end al que enrutar el tráfico. Por ejemplo, la configuración de un puerto de equilibrador de carga específico para enviar el tráfico RDP a una máquina virtual específica. Las reglas de equilibrio de carga se usan para especificar un grupo de recursos de back-end para enrutar el tráfico y equilibrar la carga en cada instancia. Por ejemplo, una regla de equilibrador de carga puede enrutar los paquetes TCP en el puerto 80 del equilibrador de carga en un grupo de servidores web.

## ¿Qué es la IP 168.63.129.16?

La dirección IP virtual para el host etiquetada como equilibrador de carga de la infraestructura de Azure en la que se originan los sondeos del estado de Azure. Al configurar las instancias de back-end, deben permitir que el tráfico procedente de esta dirección IP responda correctamente a los sondeos de estado. Esta regla no interactúa con el acceso al front-end de Load Balancer. Si no usa Azure Load Balancer, puede anular esta regla. [Aquí](#) encontrará más información sobre las etiquetas de servicio.

## ¿Puedo usar el emparejamiento de VNET global con Load Balancer

## básico?

No. Load Balancer básico no admite el emparejamiento de VNET global. En su lugar, puede usar Standard Load Balancer. Consulte el artículo de [actualización de básico a Standard](#) para una actualización sin problemas.

## ¿Cómo puedo descubrir la dirección IP pública que usa una máquina virtual de Azure?

Hay muchas maneras de determinar la dirección IP de origen público de una conexión saliente. OpenDNS proporciona un servicio que puede mostrar la dirección IP pública de la máquina virtual. Mediante el comando nslookup, puede enviar una consulta DNS del nombre myip.opendns.com para la resolución de OpenDNS. El servicio devuelve la dirección IP de origen que se usó para enviar la consulta. Si ejecuta la siguiente consulta desde la máquina virtual, la respuesta es la dirección IP pública que se usa para esa máquina virtual:

```
nslookup myip.opendns.com resolver1.opendns.com
```

## ¿Cómo funcionan las conexiones a Azure Storage en la misma región?

La conectividad saliente a través de los escenarios anteriores no es necesaria para conectarse al almacenamiento en la misma región que la máquina virtual. Si no quiere que pase esto, use grupos de seguridad de red (NSG) como se explicó anteriormente. Para la conectividad con el almacenamiento en otras regiones, se requiere conectividad de salida. Tenga en cuenta que, al conectarse al almacenamiento desde una máquina virtual en la misma región, la dirección IP de origen en los registros de diagnóstico de almacenamiento será una dirección de proveedor interna y no la dirección IP pública de la máquina virtual. Si desea restringir el acceso a la cuenta de almacenamiento a las máquinas virtuales de una o varias subredes de Virtual Network en la misma región, use [Virtual Network los puntos de conexión de servicio](#) y no la dirección IP pública al configurar el firewall de la cuenta de almacenamiento. Una vez configurados los puntos de conexión de servicio, verá la dirección IP privada de su instancia de Virtual Network en los registros de diagnóstico de almacenamiento y no la dirección interna del proveedor.

## ¿Cuáles son los procedimientos recomendados con respecto a la conectividad de salida?

Standard Load Balancer y la IP pública estándar presentan capacidades nuevas y comportamientos diferentes en la conectividad saliente. No son lo mismo que las SKU de nivel Básico. Si quiere conectividad saliente al trabajar con las SKU de nivel Estándar, debe definir las direcciones IP públicas estándar o con la instancia pública de Load Balancer estándar. Esto incluye establecer conectividad saliente cuando se usa una instancia interna de Standard Load Balancer. Se recomienda que use siempre las reglas de salida en una instancia pública de Load Balancer estándar. Esto significa que cuando se usa una instancia interna de Standard Load Balancer, es necesario seguir los pasos para establecer la conectividad saliente para las máquinas virtuales en el grupo de back-end si se quiere contar con conectividad saliente. En el contexto de la conectividad saliente, una máquina virtual independiente, todas las máquinas virtuales de un conjunto de disponibilidad y todas las instancias de VMSS se comportan como un grupo. Es decir que, si una máquina virtual en un conjunto de disponibilidad está asociada con una SKU de nivel Estándar, todas las instancias de máquina virtual dentro de dicho conjunto de disponibilidad ahora siguen las mismas reglas que están asociadas con la SKU de nivel Estándar, incluso si una instancia individual no está directamente asociada con ella. Este comportamiento también se observa en el caso de una máquina virtual independiente con varias tarjetas de interfaz de red conectadas a un equilibrador de carga. Si una NIC se agrega como independiente, tendrá el mismo comportamiento. Revise cuidadosamente todo el documento para entender los conceptos generales, consulte [Standard Load Balancer](#) para conocer las diferencias entre las SKU y consulte las [reglas de salida](#). Al usar las reglas de salida, obtiene un control avanzado de todos los aspectos de la conectividad saliente.

## Pasos siguientes

Si su pregunta no aparece en la lista anterior, envíe sus comentarios sobre esta página junto con su pregunta. Esto creará un problema de GitHub para que el equipo del producto se asegure de que las preguntas de todos nuestros valiosos clientes se respondan.