

## Load Balancing For Clustered Barracuda Web Application Firewall Instances in the New Microsoft Azure Management Portal

<https://campus.barracuda.com/doc/49057819/>

This guide will walk you through the steps to load balance traffic across multiple instances of the Barracuda Web Application Firewall deployed in the new Microsoft Azure Management Portal.

In Microsoft Azure, you can create services using the **WAN IP Address** of the Barracuda Web Application Firewall.

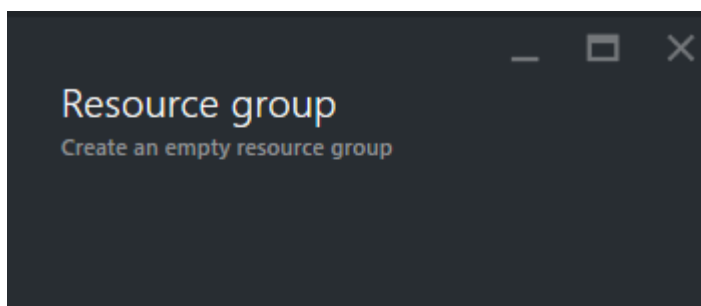
### Configuring a Load-Balanced Set Using the Azure Resource Manager Model

Follow the steps below to configure a load-balanced set using the Resource Manager model in the new Microsoft Azure Management Portal:

- [Step 1. Create a Resource Group](#)
- [Step 2. Create a Load Balancer for the Resource Group](#)
- [Step 3. Create an Availability Set for the Resource Group](#)
- [Step 4. Deploy and Provision the Barracuda Web Application Firewall VM\(s\) Using the Resource Manager](#)
- [Step 5. Configure the Barracuda Web Application Firewall VMs and Add them to the Cluster Setup](#)
- [Step 6. Add the Clustered Barracuda Web Application Firewall Instances to the Load Balance Set](#)

#### Step 1. Create a Resource Group

1. Log into the [Microsoft Azure Management Portal](#).
2. Click **Resource groups** on the left panel.
3. In the **Resource groups** page, click **Add** and specify values for the following:
  - **Resource group name:** Enter a name for the resource group.
  - **Subscription:** Select the subscription from the drop-down list.
  - **Resource group location:** Select the location for the resource group.
  - Click **Create**.



\* Resource group name

WAF-RG1



\* Subscription

 ▼

\* Resource group location

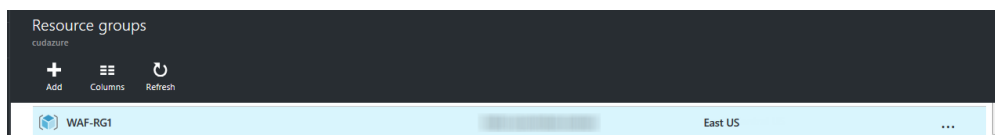
East US



☐ Pin to dashboard

Create

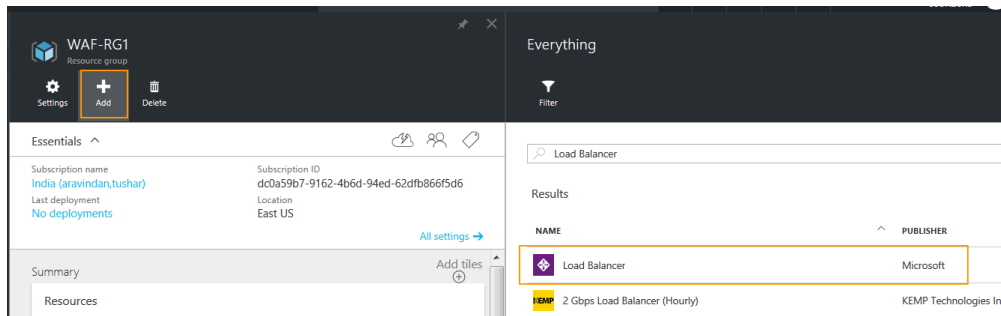
- The created resource group gets displayed in the **Resource groups** list.



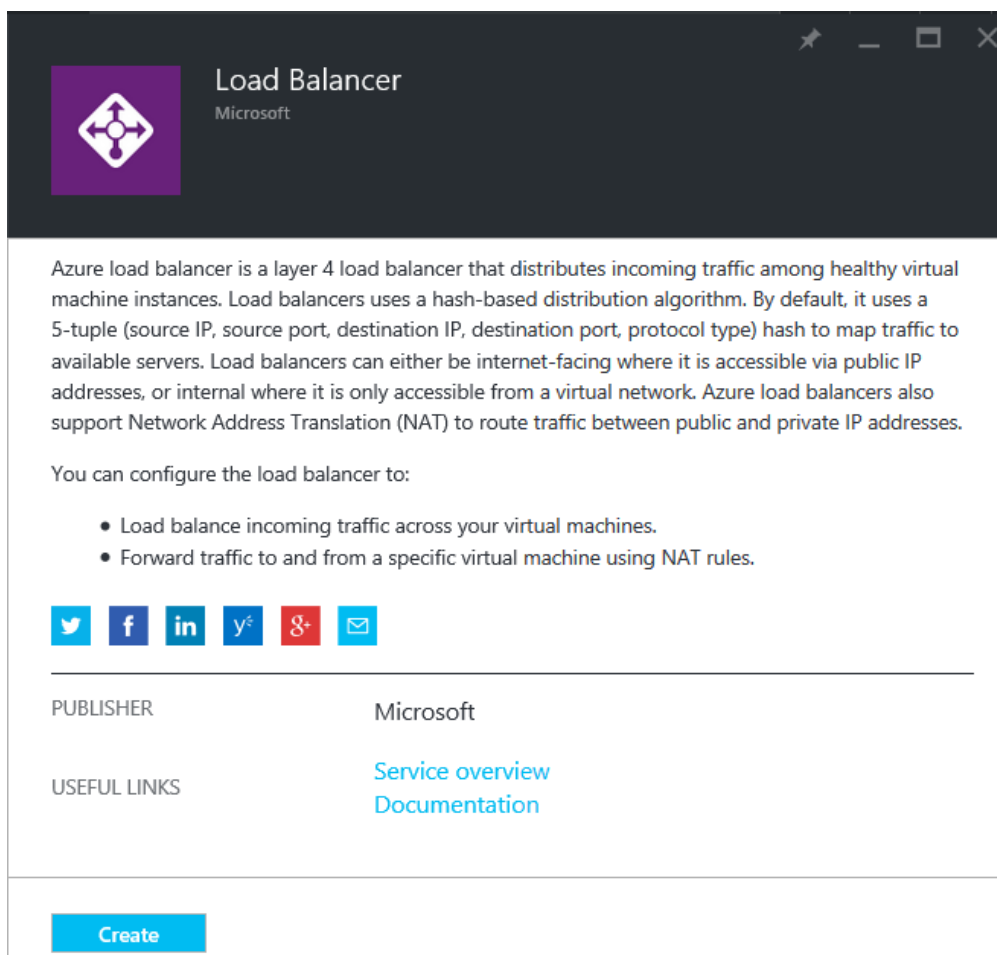
## Step 2. Create a Load Balancer for the Resource Group

- In the [Microsoft Azure Management Portal](#), click **Resource groups** on the left panel.

2. In the **Resource group** list, locate and click on the resource group created in [Step 1. Create a Resource Group](#).
3. Click **Add** in the **Resource group** page, and enter Load Balancer in the search field.
4. In the search results, select the Microsoft **Load Balancer**.



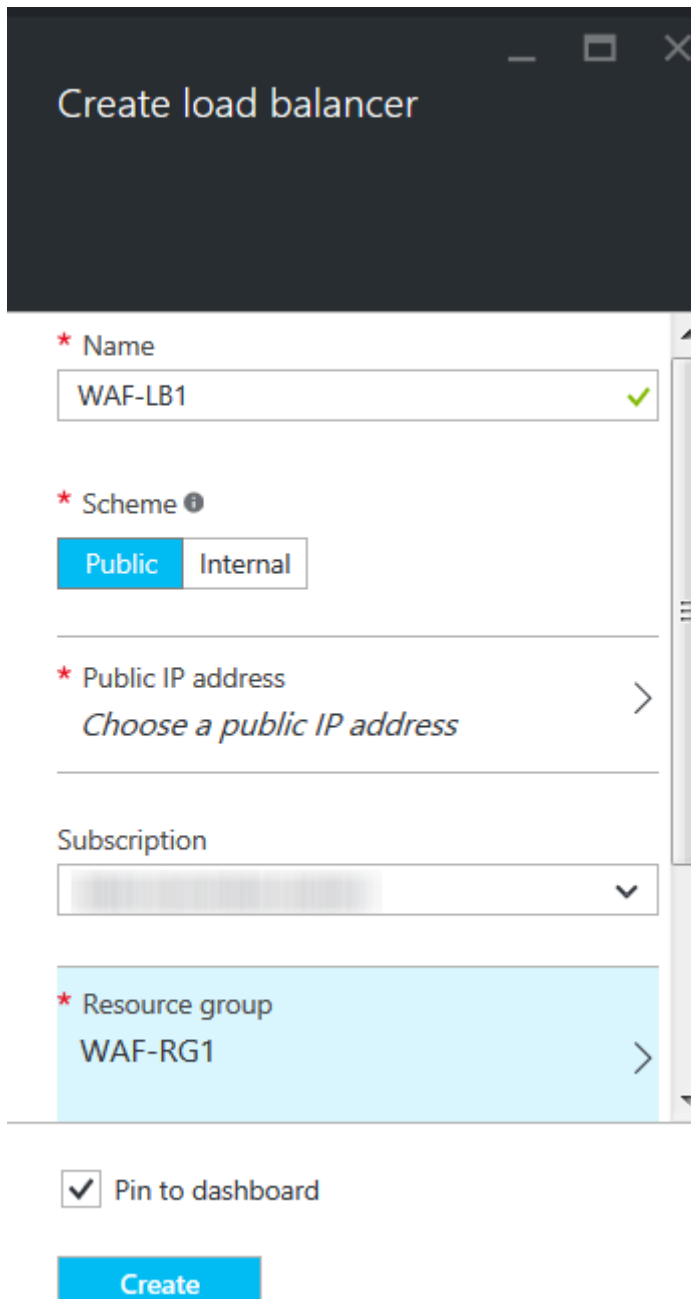
5. Click **Create**.



6. On the **Create load balancer** page, specify values for the following:
  - **Name:** Enter a name for the load balancer.
  - **Scheme:** Select **Public**.
  - **Public IP address:** Assign a new public IP address, or select a public IP address from the existing list.

- **Subscription:** Select the subscription where you want to deploy the load balancer.
- **Resource group:** Select the resource group created in [Step 1. Create a Resource Group](#).
- **Location:** Select a location for the load balancer. Note: Ensure that the location of the resource group and the load balancer is same.

7. Click **Create**.



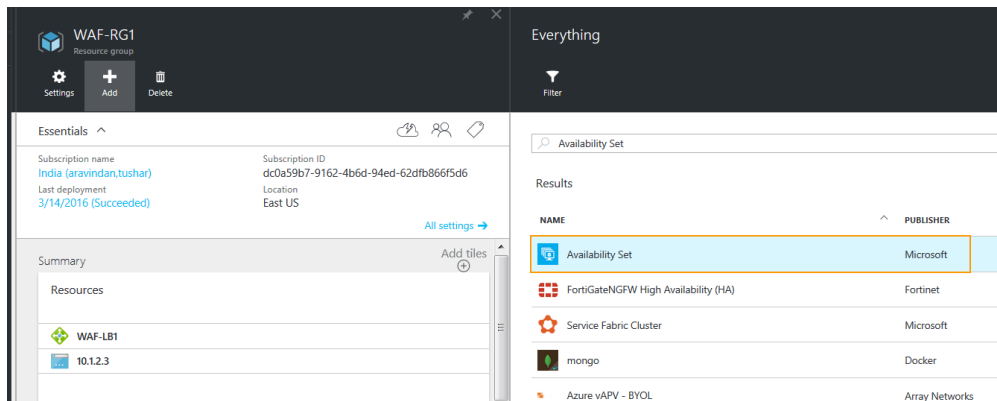
The screenshot shows the 'Create load balancer' form in the Azure portal. The form has a dark header with the title 'Create load balancer'. Below the header, there are several fields and options:

- Name:** A text input field containing 'WAF-LB1' with a green checkmark icon to its right.
- Scheme:** A section with a red asterisk and an information icon. It contains two buttons: 'Public' (highlighted in blue) and 'Internal'.
- Public IP address:** A section with a red asterisk. It contains the text 'Choose a public IP address' and a right-pointing chevron icon.
- Subscription:** A dropdown menu with a right-pointing chevron icon.
- Resource group:** A section with a red asterisk. It contains the text 'WAF-RG1' and a right-pointing chevron icon.

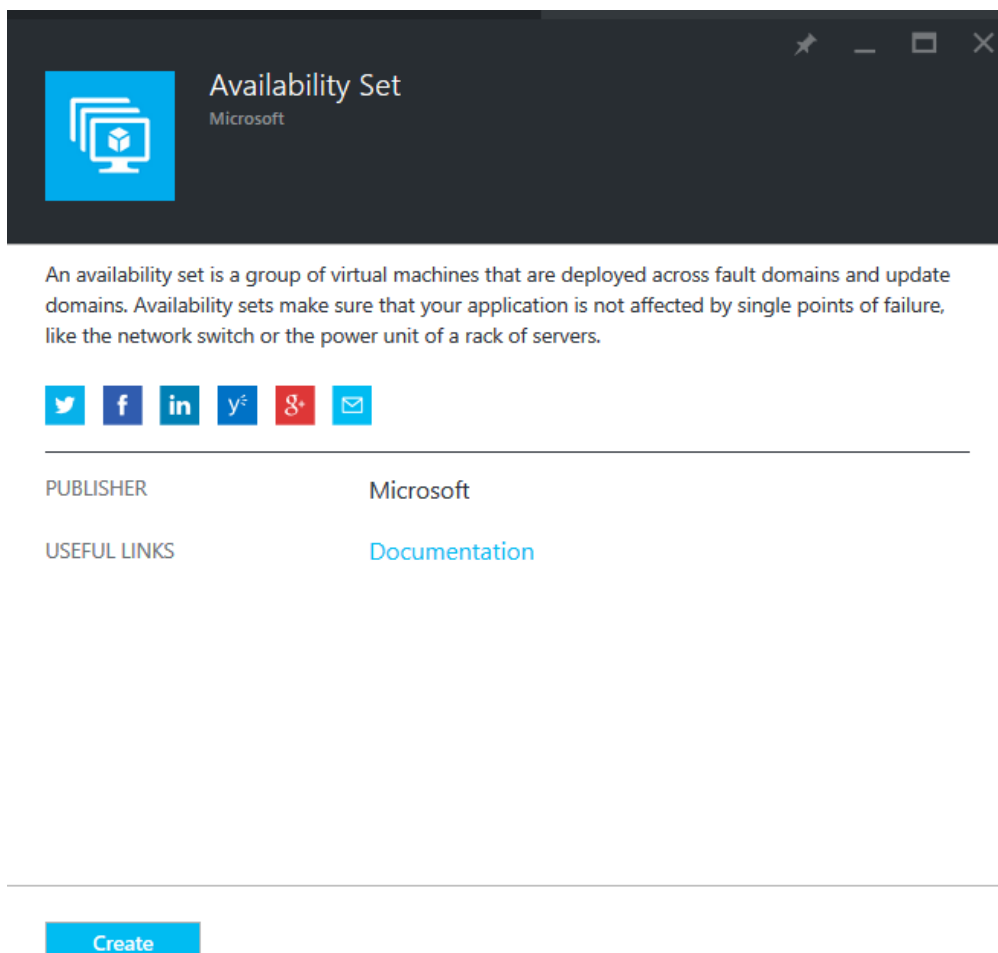
At the bottom of the form, there is a checkbox labeled 'Pin to dashboard' which is checked. Below this is a blue 'Create' button.

### Step 3. Create an Availability Set for the Resource Group

1. In the [Microsoft Azure Management Portal](#), click **Resource groups** on the left panel.
2. In the **Resource group** list, locate and click on the resource group created in [Step 1. Create a Resource Group](#) from the existing **Resource group** list.
3. Click **Add** in the **Resource group** page, and enter Availability Set in the search field.
4. In the search results, select the Microsoft **Availability Set**.



5. Click **Create**.



6. In the **Create availability set** page, specify values for the following:
  - **Name:** Enter a name for the availability set.

- **Fault domains:** Use the default value.
- **Update domains:** Use the default value.

The availability set should contain at least two "Fault" and "Update" domains; otherwise, both WAFs may be impacted by maintenance at the same time. Also, ensure that this is left at Microsoft defaults.

To learn more about the availability zone in an Azure region, see

<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/tutorial-availability-sets> and

<https://docs.microsoft.com/en-us/azure/virtual-machines/linux/manage-availability>

- **Subscription:** Select the subscription where you want to deploy the availability set.
- **Resource group:** Select the resource group created in [Step 1. Create a Resource Group](#) from the existing **Resource group** list.
- **Location:** Select a location for the availability set. Note: Ensure that the location of the resource group and the availability set is same.

7. Click **Create**.

## Create availability set

\* Name  
WAF-AS1 ✓

Fault domains ⓘ  
 2

Update domains ⓘ  
 5

Subscription

\* Resource group  
 WAF-RG1 >  
[New](#)

Location

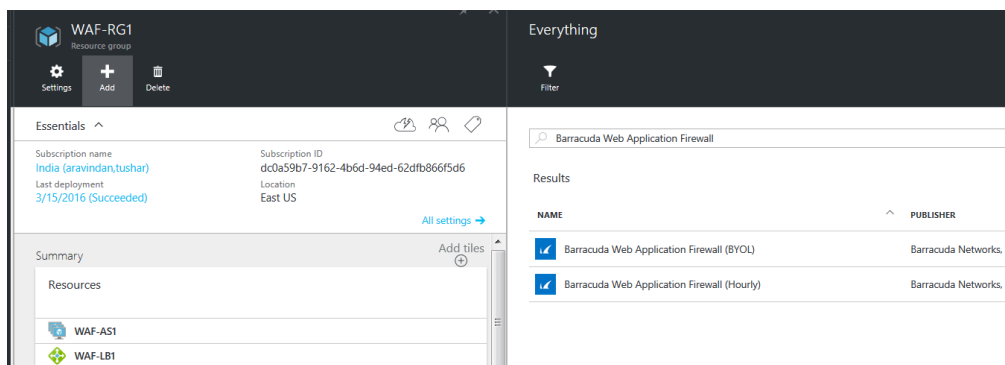
Create

## Step 4. Deploy and Provision the Barracuda Web Application Firewall VM(s) Using the Resource Manager

To load balance the traffic between the Barracuda Web Application Firewall virtual machines (VMs), deploy and provision the Barracuda Web Application Firewall instances in the resource group created in [Step 1. Create a Resource Group](#) (which includes load balancer and availability set created in [Step 2. Create a Load Balancer for the Resource Group](#) and [Step 3. Create an Availability Set for the Resource Group](#) respectively). Perform the following steps to deploy and provision the Barracuda Web Application Firewall VMs:

The Barracuda Web Application Firewall instances deployed in Microsoft Azure are assigned with a public IP address through which they can be accessed. If the deployed instances are configured behind an Azure Load Balancer, the public IP addresses assigned to the instances before being associated with the Azure Load Balancer will continue to work as earlier.

1. In the [Microsoft Azure Management Portal](#), click **Resource groups** on the left panel.
2. In the **Resource group** list, locate and click on the resource group created in [Step 1. Create a Resource Group](#).
3. Click **Add** in the **Resource group** page, and enter Barracuda Web Application Firewall for Azure in the search field.
4. In the search results, select Barracuda Web Application Firewall for Azure (**BYOL** or **Hourly** as per your requirement).



5. Follow the steps mentioned in the [Deploying and Provisioning the Barracuda Web Application Firewall Using Resource Manager in the New Microsoft Azure Portal](#) article to deploy the Barracuda Web Application Firewall VM. When deploying the Barracuda Web Application Firewall VM, ensure that you do the following:
  1. Select the resource group created in [Step 1. Create a Resource Group](#) from the existing resource group list.
  2. Select the same location as that of the resource group created in [Step 1. Create a Resource Group](#).
  3. Select the availability set created in [Step 3. Add an Availability Set to the Resource Group](#) from the existing **Availability set** list.
6. Repeat Step 5 to deploy multiple Barracuda Web Application Firewall VMs into the same load balance set.

If you have deployed the Barracuda Web Application Firewall VM(s) with the “Bring Your Own License (BYOL)” option, license the VM(s) by following the steps mentioned under "Licensing the Barracuda Web Application Firewall on Microsoft Azure" in the [Barracuda Web Application Firewall Quick Start Guide – Microsoft Azure](#) article.

If the Barracuda Web Application Firewall VM(s) is deployed with the “Hourly” option, the VM(s) is



licensed automatically.

---

## Step 5. Configure the Barracuda Web Application Firewall VMs and Add Them to the Cluster Setup

---

1. Log into the Barracuda Web Application Firewall web interface using the public IP address of the VM with port 8000 (for HTTP), or using only the public IP address (for HTTPS).
2. Verify the configuration on the **BASIC > IP Configuration** page, and change the system password on the **BASIC > Administration** page. For more information, see the "Verify Configuration and Change the Password" section in the [Barracuda Web Application Firewall Quick Start Guide - Microsoft Azure](#).
3. Perform the cluster by following the steps mentioned under "Step 2. Set Up a High Availability Environment with the Barracuda Web Application Firewall" in the [Configuring a Load-Balanced Set Using the Classic Model](#) section.
4. Repeat Step 3 to add the remaining Barracuda Web Application Firewall VMs into the cluster setup.


Ensure the endpoints are opened on all the Barracuda Web Application Firewalls for the applications/services created.

---

## Step 6 - Add the Clustered Barracuda Web Application Firewall Instances to the Load Balance Set

---

1. In the [Microsoft Azure Management Portal](#), click **Browse** at the bottom of the screen on the left panel and select **Load Balancers**.









## Load Balancer

Microsoft

Azure load balancer is a layer 4 load balancer that distributes incoming traffic among healthy virtual machine instances. Load balancers uses a hash-based distribution algorithm. By default, it uses a 5-tuple (source IP, source port, destination IP, destination port, protocol type) hash to map traffic to available servers. Load balancers can either be internet-facing where it is accessible via public IP addresses, or internal where it is only accessible from a virtual network. Azure load balancers also support Network Address Translation (NAT) to route traffic between public and private IP addresses.

You can configure the load balancer to:

- Load balance incoming traffic across your virtual machines.
- Forward traffic to and from a specific virtual machine using NAT rules.

---

PUBLISHER

Microsoft

USEFUL LINKS




[Service overview](#)  
[Documentation](#)

---


Create

- On the **Load balancers** page, select the load balancer created in [Step 2. Add a Load Balancer to the Resource Group](#).
- On the **Settings** page, select **Probes**.



load balancers

NAME	
arafeb-LB-NGF	...
arafeb-LB-WAF	...
asc-ubuntu-waf	...
WAF-LB1	...



**WAF-LB1**  
 Load balancer

Essentials

Resource group

WAF-RG1

Location

East US

Subscription name

Subscription ID

Protocol/port

-

Backend pool

-

Probe

-

NAT rules

0 inbound

IP address

- (10.1.2.3)

All settings →

Settings

WAF-LB1

Search settings

SUPPORT & TROUBLESHOOTING

Audit logs

>

GENERAL

Properties

>

Load balancing rules

>

Probes

>

IP address

>

Backend pools

>

Inbound NAT rules

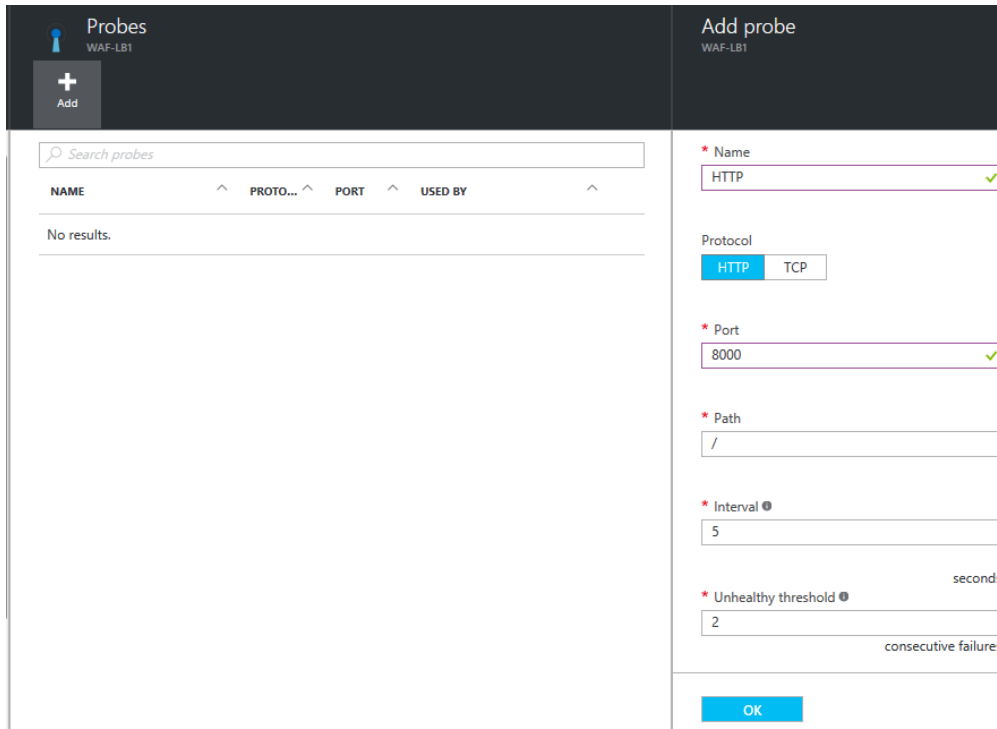
>

- On the **Probes** page, click **Add** and specify values for the following in the **Add probe** page:
  - **Name:** Enter a name for the probe.
  - **Protocol:** Select **HTTP**.
  - **Port:** Enter **8000**.
  - **Interval:** Enter the interval time (in seconds) between probes sent by the Microsoft Azure to the Barracuda Web Application Firewall virtual machine to determine the health status.

**Note:** It is recommended to keep the default values.

- **Unhealthy threshold:** Enter the number of probe failures that are allowed before marking the virtual machine as unhealthy. Note: It is recommended to keep the default values.

5. Click **OK**.



6. On the **Settings** page, click **Backend pools**.

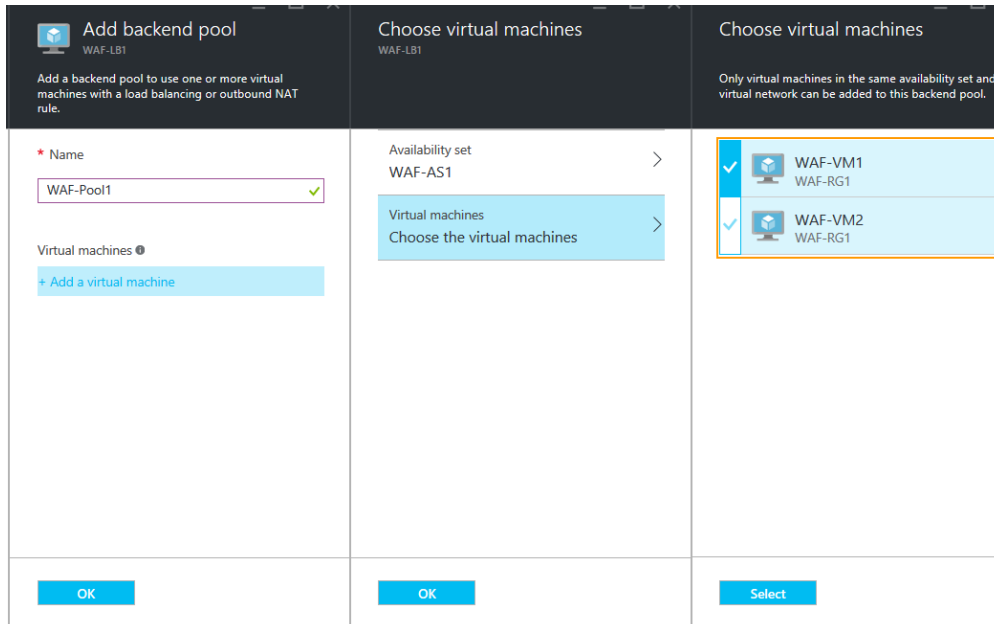
7. On the **Backend address pools** page, click **Add**.

8. On the **Add backend pool** page:

1. **Name:** Enter a name for the backend pool.
2. **Virtual machines:** Click **Add a virtual machine**.

9. On the **Choose virtual machines** page:

1. Click **Availability set** and select the availability set created in [Step 3. Create an Availability Set for the Resource Group](#).
2. Click **Virtual machines**, select the Barracuda Web Application Firewall VMs you added in [Step 5. Configure the Barracuda Web Application Firewall VMs and Add them to the Cluster Setup](#) on the **Choose virtual machines** page, and click **Select**.



The screenshot shows three panels in the Azure portal:

- Add backend pool (WAF-LB1):**
  - Name: WAF-Pool1 (with a green checkmark)
  - Virtual machines: + Add a virtual machine
  - OK button
- Choose virtual machines (WAF-LB1):**
  - Availability set: WAF-AS1
  - Virtual machines: Choose the virtual machines
  - OK button
- Choose virtual machines:**
  - Only virtual machines in the same availability set and virtual network can be added to this backend pool.
  - Selected VMs: WAF-VM1 (WAF-RG1) and WAF-VM2 (WAF-RG1), both with checkmarks.
  - Select button

10. Click **OK** on the **Choose virtual machines** page, and on the **Add backend pool** page.
11. On the **Settings** page, click **Load balancing rules**.
12. On the **Load balancing rules** page, click **Add** and specify values for the following in the **Add load balancing rule** page:
  - **Name:** Enter a name for the load balancing rule.
  - **Protocol:** Select TCP.
  - **Port:** Enter the port on which you want to receive the traffic on the Load Balancer to load balance the traffic between the Barracuda Web Application Firewall.
  - **Backend port:** Enter the port on the Barracuda Web Application Firewall to which you want to distribute the traffic.
  - **Backend pool:** Select the backend pool created in Step 7 in the [Step 6. Add the Clustered Barracuda Web Application Firewall Instances to the Load Balance Set](#) section.
  - **Probe:** Select the probe created in Step 4 in the [Step 6. Add the Clustered Barracuda Web Application Firewall Instances to the Load Balance Set](#) section.
  - **Session persistence:** Select the persistence as per your requirement.
  - **Idle timeout (minutes):** Keep the default value.
  - **Floating IP (direct server return):** Select *Disabled*.
13. Click **OK**.

Now, any requests coming to the load balancer public IP address/DNS configured in Step 6.c in the [Step 2. Create a Load Balancer for the Resource Group](#) section will be distributed between the specified Barracuda Web Application Firewalls.

## Configuring a Load-Balanced Set Using the Classic Model

Follow the steps below to configure a load-balanced set using the Classic model in the new Microsoft Azure Management Portal:

- [Step 1. Deploy the Barracuda Web Application Firewall Instances in Microsoft Azure](#)
- [Step 2. Set Up a High Availability Environment With the Barracuda Web Application Firewall](#)
- [Step 3. Set Up Load Balancing on the First Barracuda Web Application Firewall Instance](#)
- [Step 4. Add Other Barracuda Web Application Firewall Instances to the Load-Balanced Set](#)

## Step 1. Deploy the Barracuda Web Application Firewall Instances in Microsoft Azure

1. Follow the steps in [Deploying and Provisioning the Barracuda Web Application Firewall in the New Microsoft Azure Management Portal](#). To license and configure your virtual machine, continue with [Barracuda Web Application Firewall Quick Start Guide - Microsoft Azure](#). In these instructions, the newly configured virtual machine is called Barracuda-WAF1.
2. Verify that Barracuda-WAF1 is accessible through port 8000 (for HTTP) and port 8443 (for HTTPS).
3. Add new ports for HTTP and HTTPS to Barracuda-WAF1 in **ENDPOINTS** (for example, port 8001 for HTTP and port 8444 for HTTPS).
4. In the web interface of Barracuda-WAF1, do the following:
  1. Enter the HTTP port number you configured in Step 3 into **Web Interface HTTP Port** under **Web Interface Settings** on the **BASIC > Administration** page.
  2. Enter the HTTPS port number you configured in Step 3 into **Web Interface HTTPS/SSL Port** on the **ADVANCED > Secure Administration** page.
5. Verify that you can access Barracuda-WAF1 using the HTTP and HTTPS ports specified in Step 4a. and 4b. .
6. In Microsoft Azure, delete port 8000 and port 8443 from the listed **ENDPOINTS** for Barracuda-WAF1.
7. To deploy another Barracuda Web Application Firewall (called Barracuda-WAF2) in Microsoft Azure, follow the instructions in the [Deploying and Provisioning the Barracuda Web Application Firewall in the New Microsoft Azure Management Portal](#) article.

When you configure the **CLOUD SERVICE DNS NAME**, choose the **CLOUD SERVICE DNS NAME** of Barracuda-WAF1 from the **CLOUD SERVICE** list.

When the second Barracuda Web Application Firewall instance is added to the same **CLOUD SERVICE** to set up load balancing between clustered Barracuda Web Application Firewall, Microsoft Azure may add a random high port as **ENDPOINTS** for **Public Port** instead of adding 8000 and 8443 ports. In this case, do the following:

- Access the second Barracuda Web Application Firewall web interface using the random high port, as the high port **ENDPOINTS** added in **Public Port** are NATed with the configured Private Port's **ENDPOINTS**.

**OR**

- Edit the high port and configure desired ports (i.e. port 8000 and 8443) in the **ENDPOINTS** for the deployed VM before accessing.

8. Continue with [Barracuda Web Application Firewall Quick Start Guide - Microsoft Azure](#) to license and configure your virtual machine.
9. By default, the Barracuda-WAF2 is configured with port 8000 (for HTTP) and port 8443 (for HTTPS).

Now, Barracuda-WAF1 is accessible through port 8001 for HTTP and port 8444 for HTTPS, and Barracuda-WAF2 is accessible through port 8000 for HTTP and port 8443 for HTTPS.

## Step 2. Set Up a High Availability Environment With the Barracuda Web Application Firewall

Follow these steps to cluster your Barracuda Web Application Firewall virtual machines in Microsoft Azure:

The Barracuda Web Application Firewall virtual machines should all be deployed in the same **CLOUD SERVICE** for High Availability in Microsoft Azure.

1. Install each system and ensure that each Barracuda Web Application Firewall is running the same firmware version. Each Barracuda Web Application Firewall in a cluster must have the same model number and firmware version.
2. Make a backup of each Barracuda Web Application Firewall configuration.
3. No processes should be running on any virtual machine when you link them together. To be sure, go to the **ADVANCED > Task Manager** page of each Barracuda Web Application Firewall and verify that no processes are running.
4. From the **ADVANCED > High Availability** page of Barracuda-WAF1, enter a **Cluster Shared Secret** password, and click **Save**.
5. From the **ADVANCED > High Availability** page of Barracuda-WAF2, do the following:
  1. Enter the same **Cluster Shared Secret** password, and click **Save**. Both units in a cluster must have the same Cluster Shared Secret to communicate with each other.
  2. In the **Clustered Systems** section, enter the WAN IP address of Barracuda-WAF1, and click **Join Cluster**. *Make sure that the join cluster task is not cancelled when the join is in progress.*
6. On each Barracuda Web Application Firewall, refresh the **ADVANCED > High Availability** page, and verify the following:
  1. Each system's Hostname, serial number and WAN IP address appears in the **Clustered Systems** list.
  2. The identity of the system (Self or Peer) displays in the **Type** field.
  3. The **Status** is green for all virtual machines in the cluster.
7. View the **Cluster Status** from the **BASIC > Dashboard** page, under **Performance Statistics**.

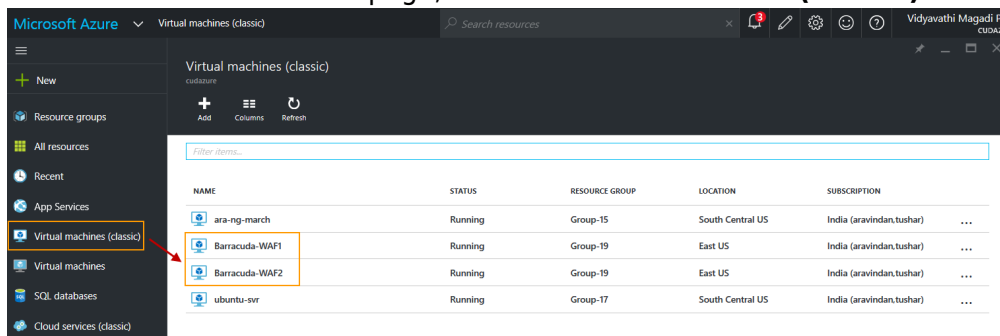
To add more units to the existing cluster, repeat Steps 1 to 5.a. and then do the following:

- From the **ADVANCED > High Availability** page of the Barracuda Web Application Firewall you are adding to the cluster, enter the WAN IP address of any system in the cluster in the **Peer IP Address** field and click **Join Cluster**. Verify that the following occurs:

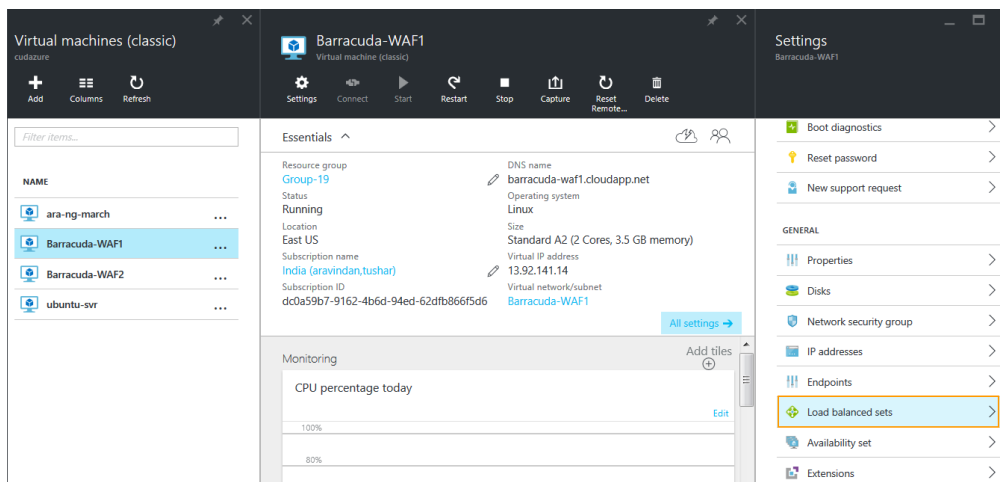
- The configuration of the cluster automatically propagates to the newly added system.
- The new unit information propagates to all other units in the cluster.

### Step 3. Set Up Load Balancing on the First Barracuda Web Application Firewall Instance

1. Log into the [Microsoft Azure Management Portal](#).
2. On the **Microsoft Azure Home** page, select **Virtual machines (classic)** on the left panel.

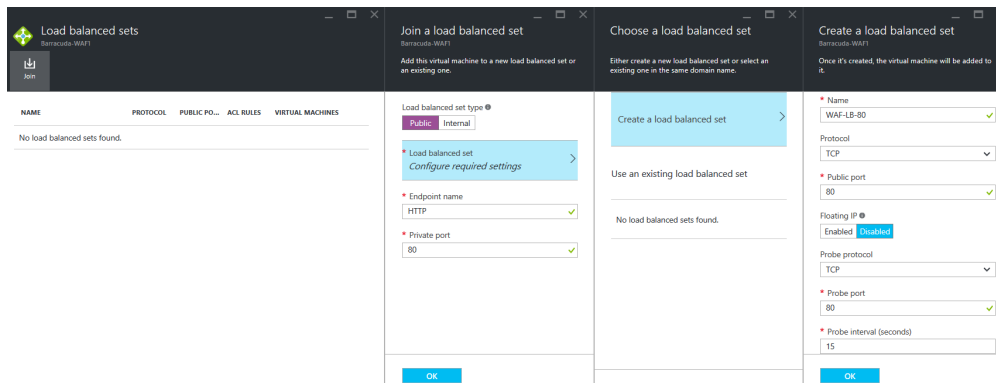


3. On the **Virtual machines (classic)** page, select *Barracuda-WAF1*.
4. In the **Essentials** section, click **All Settings**, and select **Load balanced sets**.

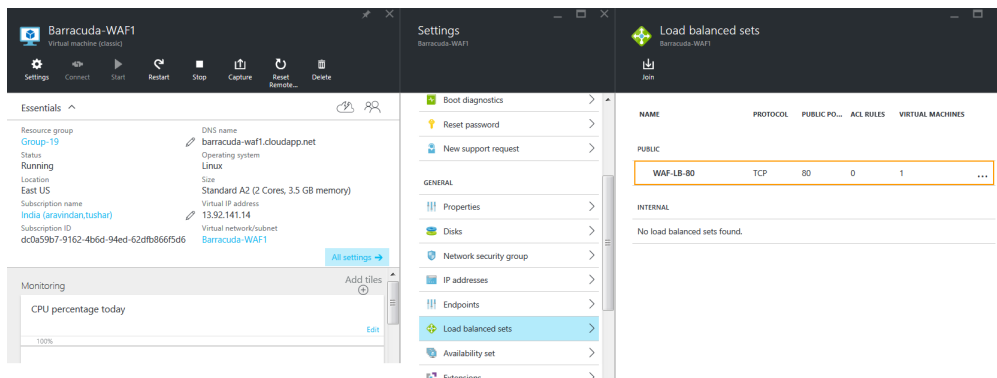


5. On the **Load balanced sets** page, click **Join** and specify values for the following fields in the **Join a load balanced set** page:
  - Set the **Load balanced set type** to **Public**
  - **Endpoint Name:** Enter a name for the endpoint. **Example:** HTTP
  - **Private Port:** Enter the internal port that should listen to traffic on the endpoint. **Example:** 80.
  - Click **Load balanced set Configure required settings**, and select **Create a load balanced set**.
6. On the **Create a load balanced set** page, specify values for the following fields:
  - **Name:** Enter a name for the load-balanced set. **Example:** WAF-LB-80
  - **Protocol:** Select **TCP** from the list.

- **Public Port:** Enter the port number of the service you are load balancing. **Example:** Port 80 for HTTP traffic.
- Set **Floating IP** to **Disabled**.
- Select the **Protocol** to be used for probing, enter values for **Port**, **Interval (seconds)** and **Number of retries** as required, and click **OK**.



- Now, click **OK** under **Join a load balanced set**. This will create the load balanced set and join it to *Barracuda-WAF1*.
- Click **OK** to set up the load-balanced set.



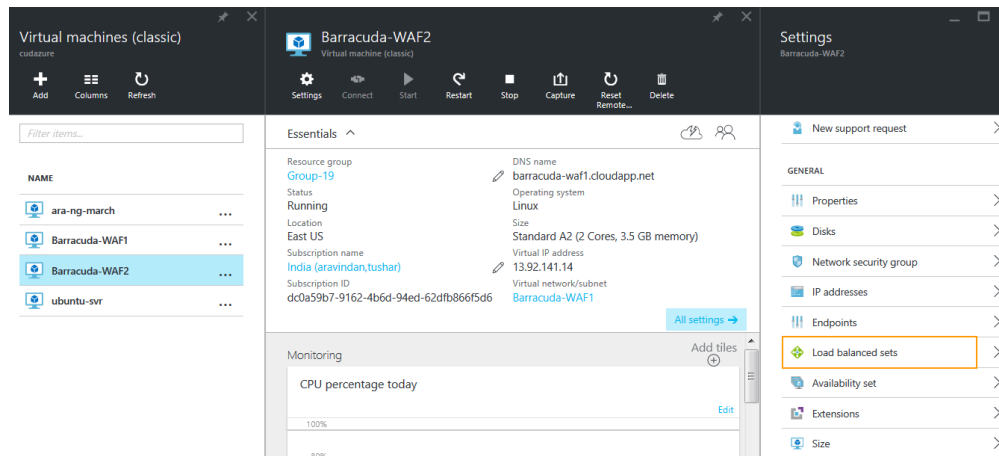
- Repeat the process to add more ports to the load-balanced set.

## Step 4. Add Other Barracuda Web Application Firewall Instances to the Load-Balanced Set

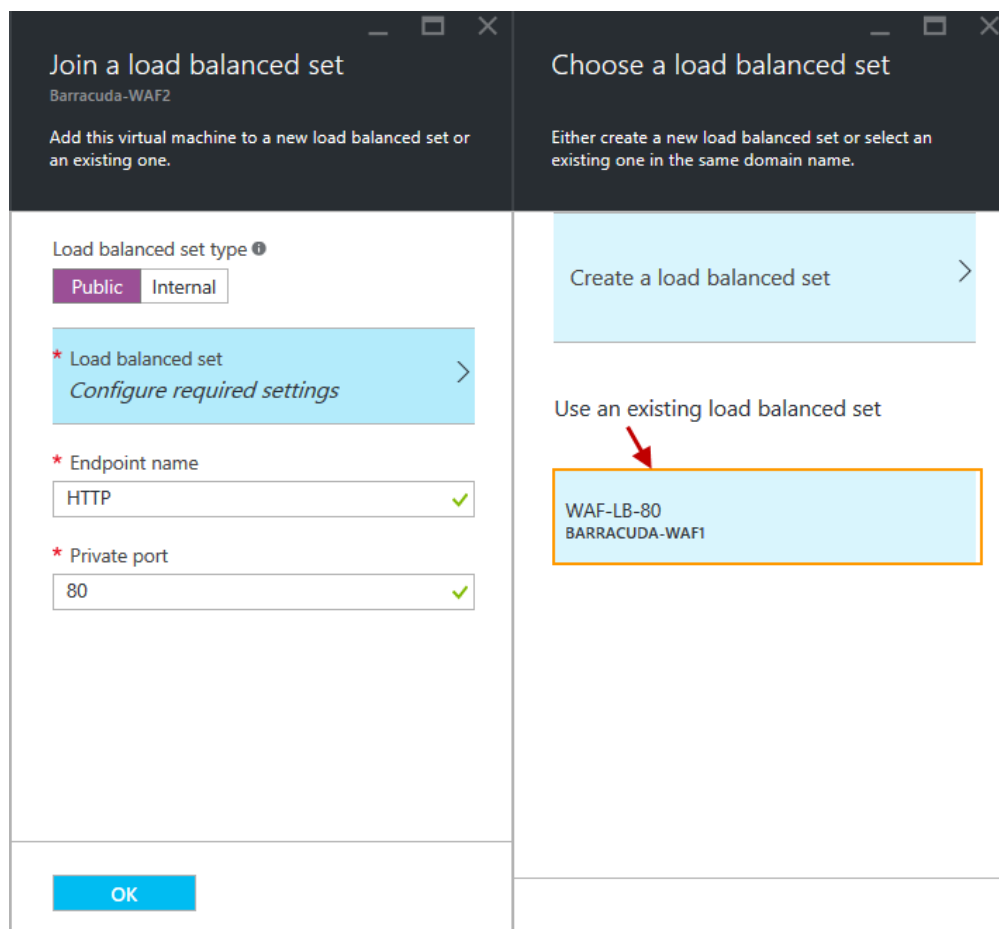
After you create the load-balanced set for Barracuda-WAF1, add other Barracuda Web Application Firewall virtual machines to the set. Example: Barracuda-WAF2

- Log into the [Microsoft Azure Management Portal](#).
- On the **Microsoft Azure Home** page, select **Virtual machines (classic)** on the left panel.
- On the **Virtual machines (classic)** page, select *Barracuda-WAF2*.
- In the **Essentials** section, click **All Settings**, and select **Load balanced sets**.

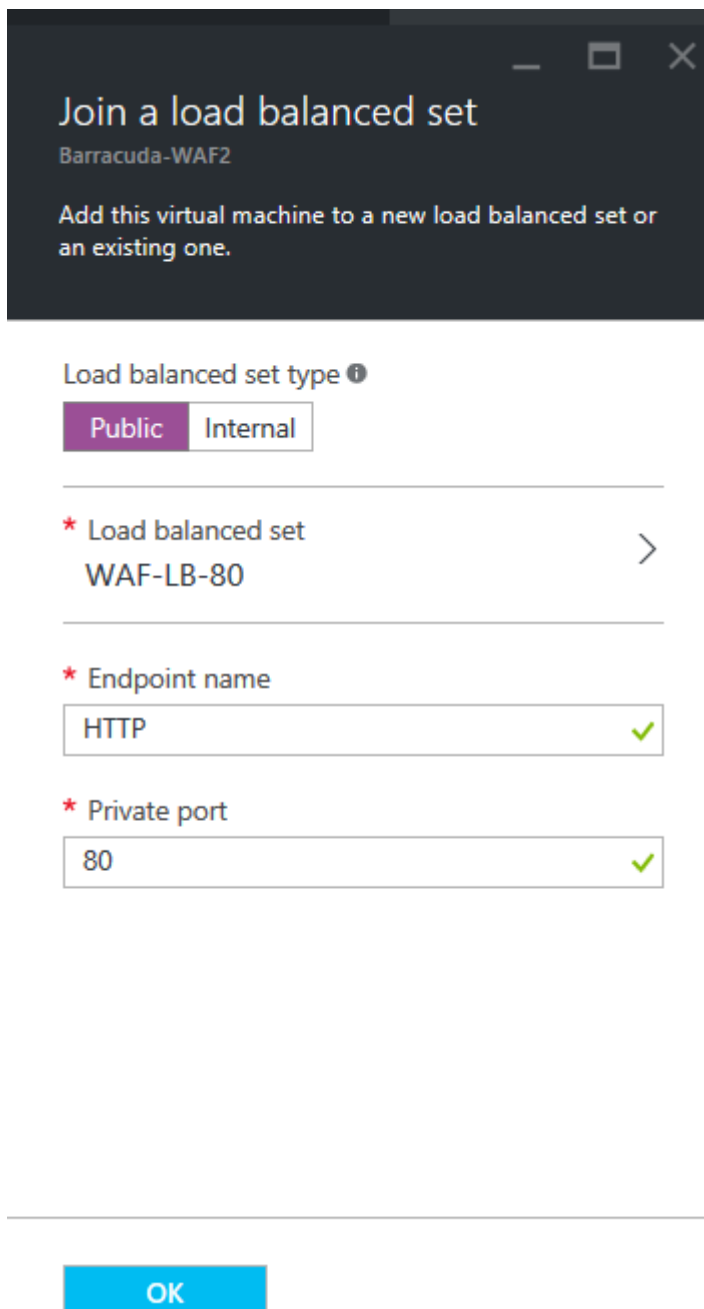




5. On the **Load balanced sets** page, click **Join** and specify values for the following fields in the **Join a load balanced set** page:
  - Set the **Load balanced set type** to **Public**.
  - Click **Load balanced set Configure required settings**.
6. On the **Choose a load balanced set** page, select the load-balanced set you created in Step 6 under [Step 3. Set Up Load Balancing on the First Barracuda Web Application Firewall Instance](#).



7. On the **Join a load balanced set** page, you will see the load-balanced set associated with the *Barracuda-WAF2* instance.



Join a load balanced set

Barracuda-WAF2

Add this virtual machine to a new load balanced set or an existing one.

Load balanced set type ⓘ

Public Internal

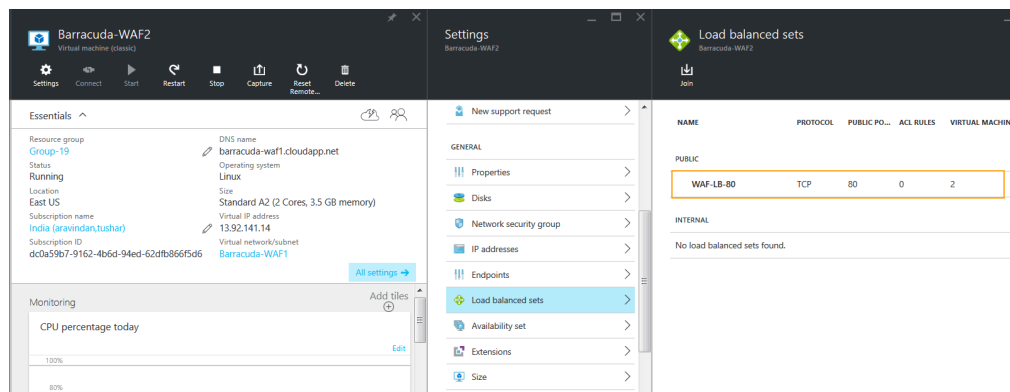
\* Load balanced set  
WAF-LB-80 >

\* Endpoint name  
HTTP ✓

\* Private port  
80 ✓

OK

8. Click **OK** to add the *Barracuda-WAF2* instance to the load-balanced set.



9. Repeat the process to add more Barracuda Web Application Firewall virtual machines to the load-balanced set.

## Figures

1. Creating Resource Group.png
2. Resource Group List.png
3. Adding Load Balancer.png
4. Load Balancer.png
5. Creating LB.png
6. Adding Availability Set.png
7. Availability Set.png
8. doc1image.png
9. BWAF instance.png
10. Load Balancer.png
11. Configuring LB.png
12. Add a probe.png
13. Select VMs.png
14. VMs\_classic.png
15. WAF1\_LB\_Sets.png
16. Configuring\_LB\_Set\_for\_WAF1.png
17. WAF1\_LB\_Set\_Joined.png
18. WAF2\_LB\_Sets.png
19. Configuring\_LB\_Set\_for\_WAF2.png
20. Join\_LB\_Set.png
21. LB\_Set\_Joined.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.