Deploying the Barracuda Web Application Firewall Virtual Machine Scale Sets (VMSS) - BYOL Instance in Microsoft Azure

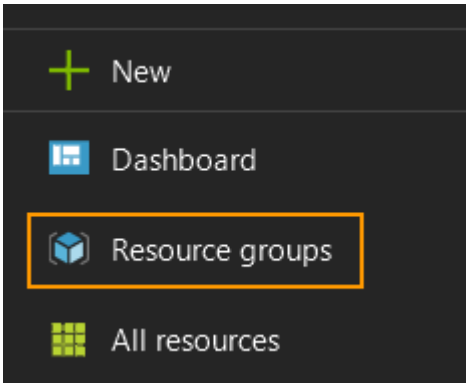
https://campus.barracuda.com/doc/75694304/

Before proceeding with deploying the Barracuda Web Application Firewall VMSS, do the following:

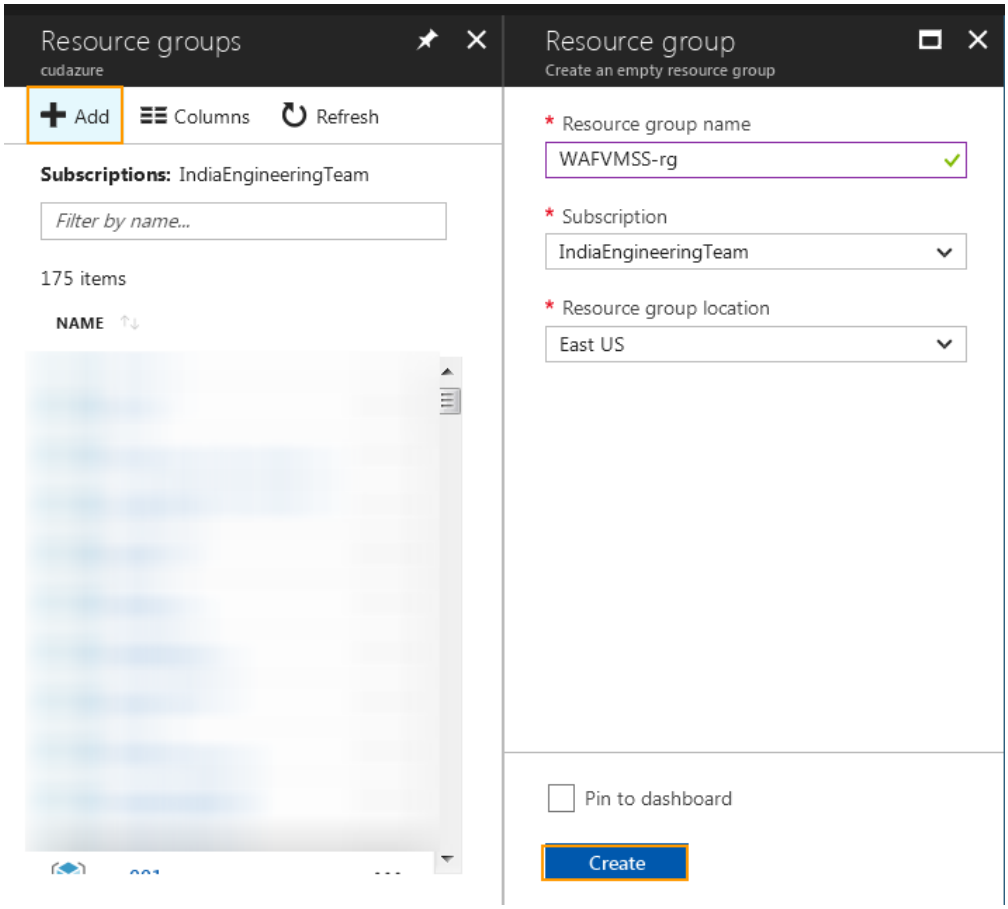
Step 1. Create a Resource Group

To create a resource group, perform the following steps:

1. Log into the Microsoft Azure Portal.
2. Click **Resource groups** in the left panel.



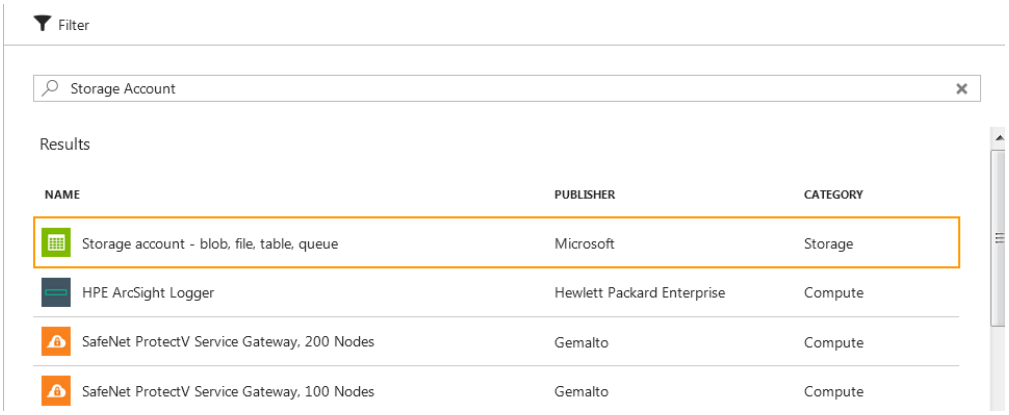
3. In the **Resource groups** page, click **Add** and specify values for the following:
    1. **Resource group name**: Enter a name for the resource group.
    2. **Subscription**: Select the subscription in which you want to create the resource group.
    3. **Resource group location**: Select a location for the resource group.
    4. Click **Create**.



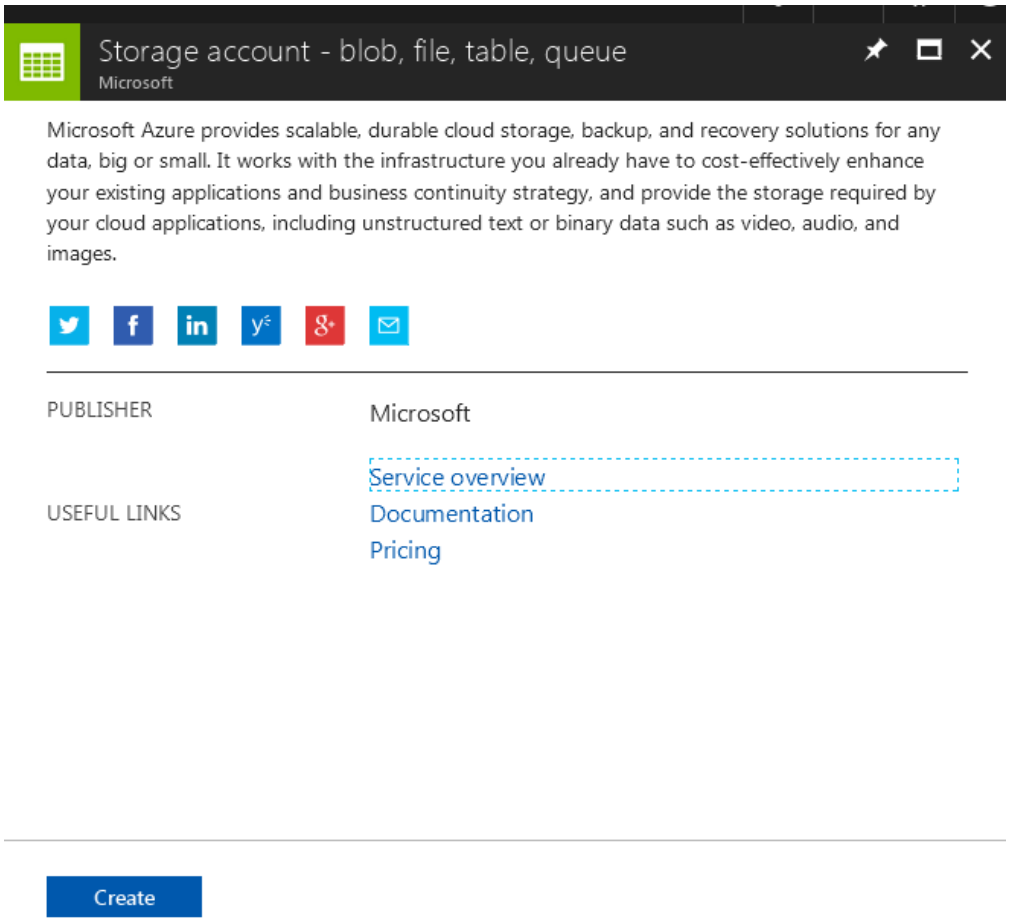
Step 2. Create a Storage Account

Perform the following steps to create a storage account:

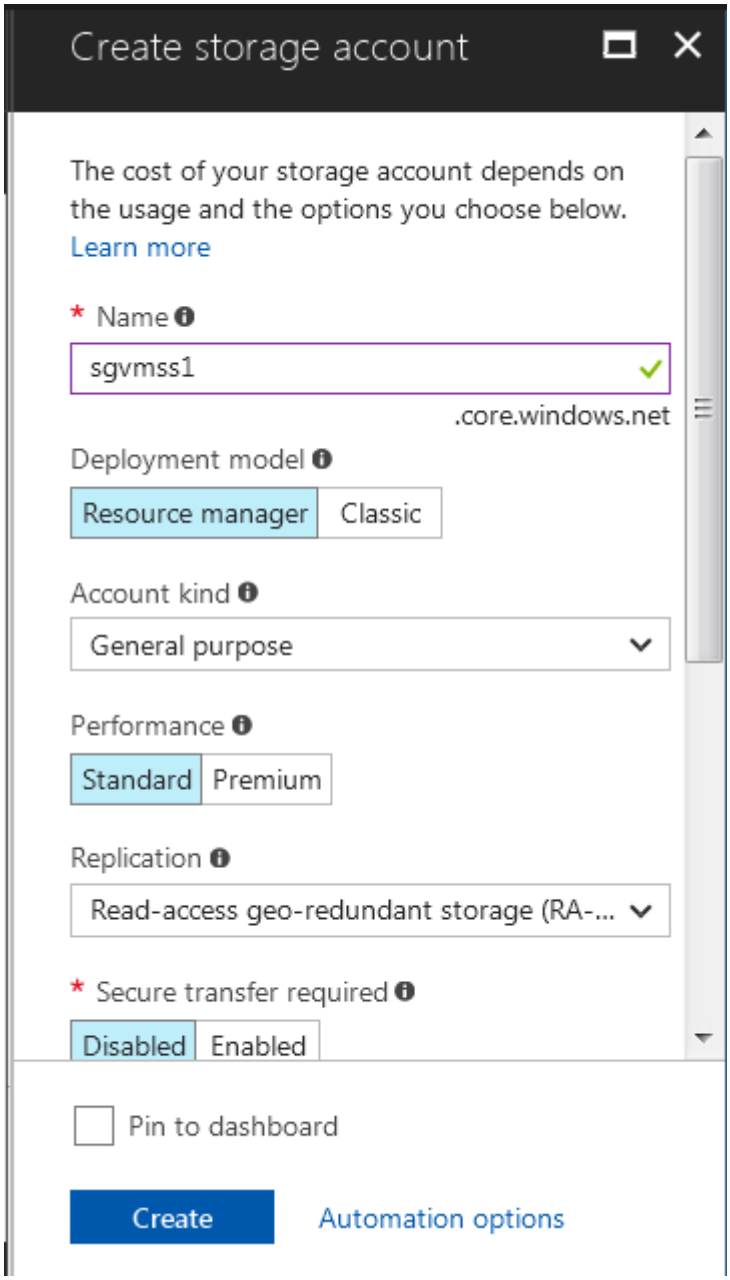
1. Log into the Microsoft Azure Portal.
2. Click **New** in the left panel, and type *Storage Account* in the **Search** field.
3. In the search results, select **Microsoft Storage account**.



4. In the **Storage account – blob, file, table, queue** page, click **Create**.



5. In the **Create storage account** page:
    1. **Name**: Enter a name for the storage account.
    2. **Deployment model**: Ensure the deployment model is set to **Resource Manager**.
    3. **Account kind**: Select the type of storage account that needs to be created. **Default**: General purpose
    4. **Performance**: Select the performance tier as required.
    5. **Replication**: Select the replication option for the storage account.
    6. **Secure transfer required**: Select **Enabled** if you want to transfer the data into or out of storage account. Default: Disabled.
    7. **Subscription**: Select the subscription in which you want to create the storage account. **Note**: Ensure that the subscription for the storage account and the resource group is same.
    8. **Resource group**: Select the resource group created in **Step 1. Create a Resource Group**.
    9. **Location**: Select the location for the storage account. **Note**: Ensure that the location for the storage account and the resource group is same.
    10. Click **Create**.



Step 3. Create and upload license file

Perform the following steps to create and upload a license file:

Create a container

1. Click the storage account that you have created.
2. Click **Blobs**.
3. Click **+Container** under Blob service.
4. **Name**: Enter a name for the container.

> The container name must be lowercase and must start with a letter or a number. They must contain only letters, numbers, and the dash (-) character.

5. **Public access level**: Set the level of public access to the container. The default level is **Private (no anonymous access)** and it is recommended to use the default level.
6. Click **OK** to create the container.

Create a License file

A license file contains licenses that can be used. This file should be created in the valid JSON format and should be saved in the name "*barracuda-byol-license-list.json*".

1. Open notepad or any text editor. Type the licenses in the format illustrated below.

```
{
    "licenses" :
        [
            "4TG2E-xxxxx-xxxxx",
            "AXA40-xxxxx-xxxxx",
            "B3544-xxxxx-xxxxx",
            "35E3R-xxxxx-xxxxx",
            "T3AF7-xxxxx-xxxxx"
        ]
}
```

> It is recommended that you validate the JSON file using JSONLint or any other online validator before uploading the license file. The created WAF instances might fail during provisioning if the JSON file is not valid.

2. Save the license file. Note that you save the file with the name "*barracuda-byol-license-list.json*" as mentioned earlier.

Upload the license file

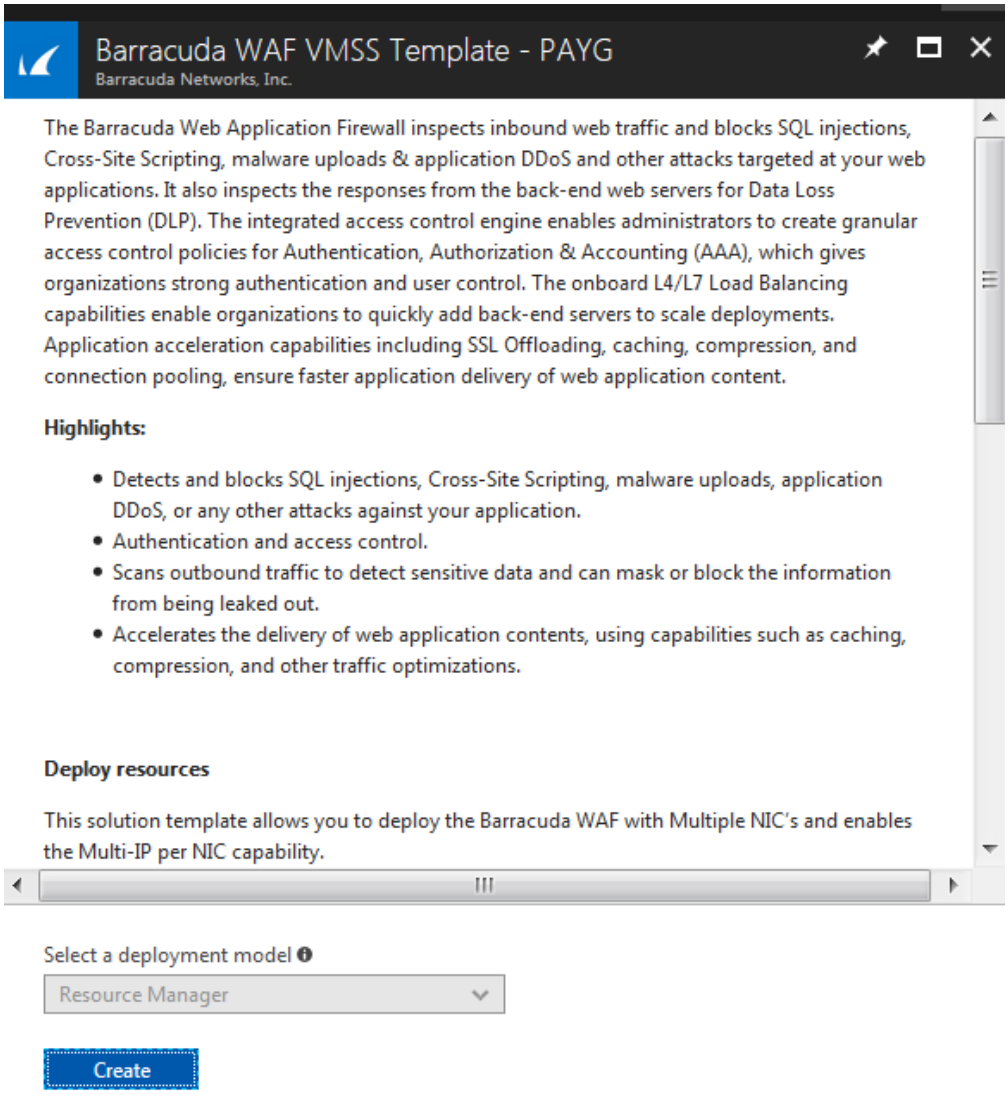
1. To upload a license file, select the container you created.
2. Click **Upload**.
3. In the right pane, click the browse button and then select the license file you created.
4. Click **Upload** to upload the license file to the container.

Deploying the Barracuda Web Application Firewall VMSS

Perform the following steps to deploy the Barracuda Web Application Firewall VMSS instance:

1. Log into the Microsoft Azure Portal.
2. Click **Marketplace** at the bottom of the screen.
3. In the **Everything** page, type *Barracuda WAF VMSS Template* in the **Search** text field.
4. In the search results, select **Barracuda WAF VMSS Template - BYOL.**

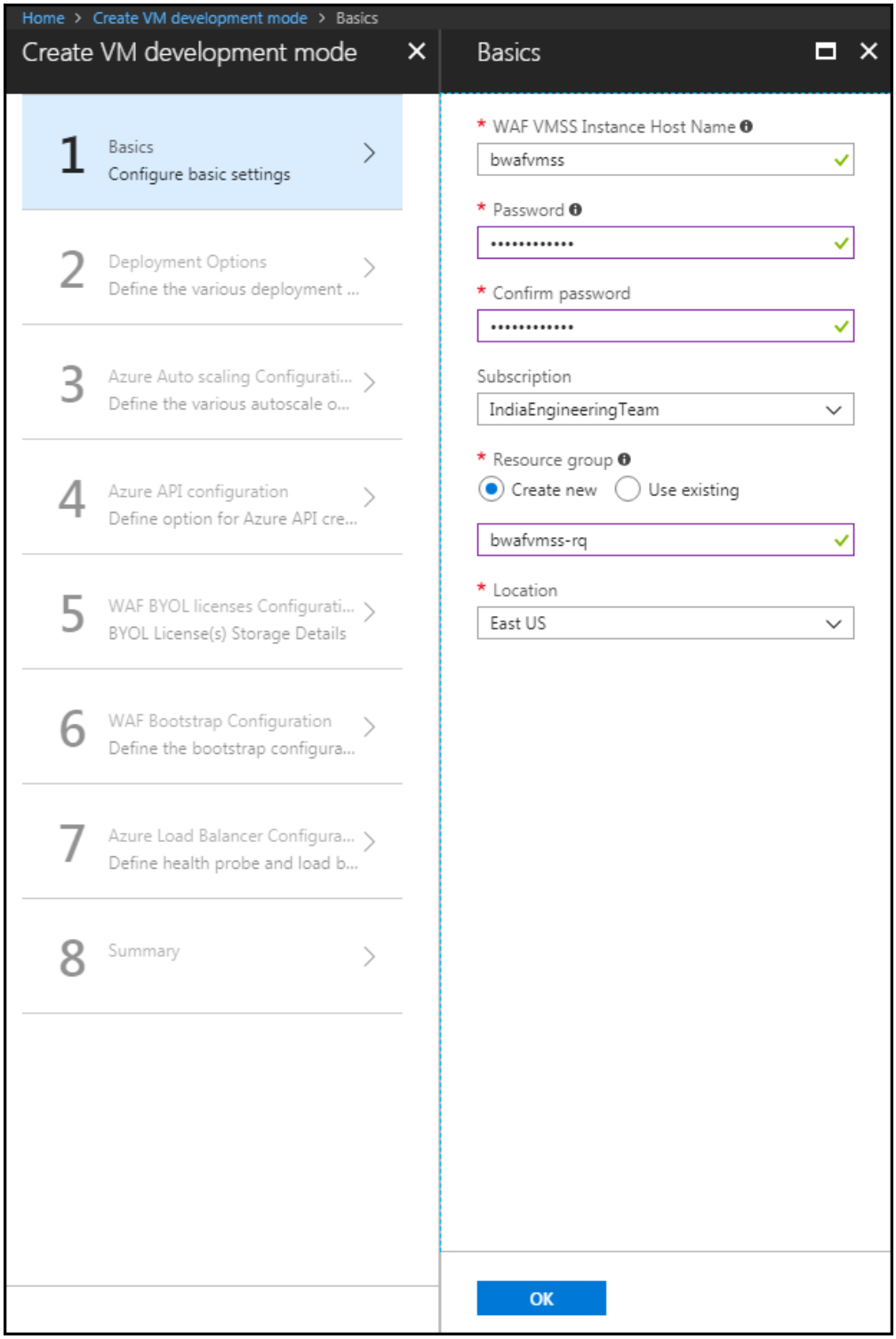
5. In the **Barracuda WAF VMSS Template - BYOL** page:
    1. Read the product overview.
    2. Click **Create**.



6. In the **Create Barracuda WAF VMSS Template - BYOL > 1 Basics** page:
    1. **Barracuda Web Application Firewall Virtual Machine Scale Set Name**: Enter a name for the Barracuda Web Application Firewall VMSS.
    2. **Password**: Enter a password for authentication. This will be your password to access

the Barracuda Web Application Firewall web interface.

3. **Confirm Password**: Re-enter the password for confirmation.
4. **Billing Method**: Select **Bring your own License (BYOL)** form the drop-down list as your billing method.
5. **Firmware Version**: From the drop-down list, select the firmware version on which your instance is deployed.
6. **Subscription**: Select the subscription from the drop-down list.
7. **Resource group**: Create a new resource group or select a resource group that is empty from the existing **Resource group** list.
8. **Location**: Select a location for the Barracuda Web Application Firewall VMSS.
9. Click **OK**.



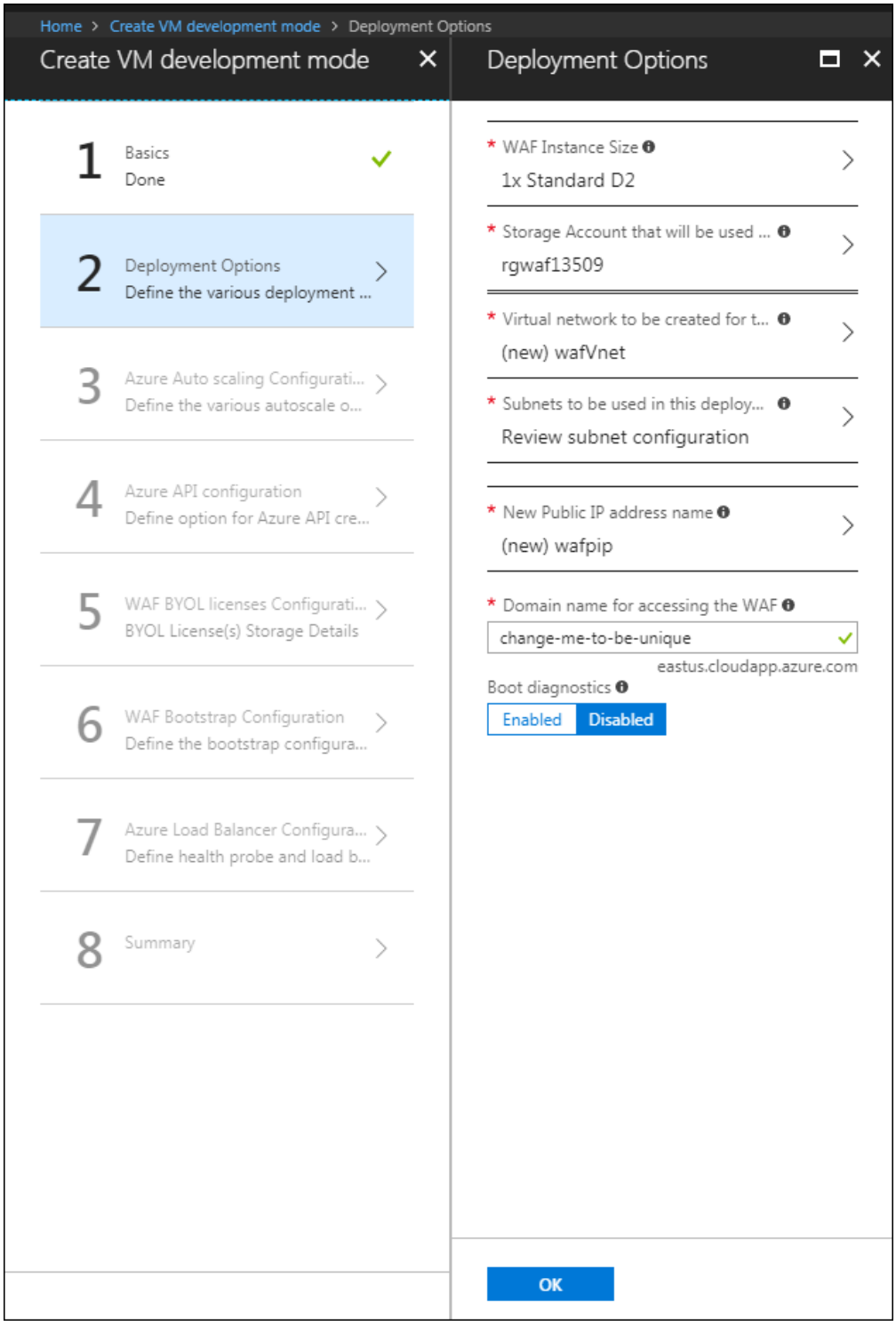
7. In the **Create Barracuda WAF VMSS Template - BYOL > 2 Deployment Options** page:
    1. **Barracuda Web Application Firewall Instance Size**: Select a size for the instance.
    2. **Storage Account**: Create a new storage account or select a storage account from the existing **Storage account** list.

        The storage account should be in the same region where the Barracuda Web Application Firewall VMSS instance needs to be deployed.
    3. **Virtual network**: Create a new virtual network, or select a virtual network from the

existing **Virtual network** list in which you want to deploy the Barracuda Web Application Firewall VMSS.

4. **Subnets**: Review the subnet configuration and modify if required.
5. **New Public IP address name**: Enter a name for the public IP address associated with the Barracuda Web Application Firewall Firewall VMSS.
6. **Domain name for accessing the Barracuda Web Application Firewall**: Enter the domain for the Barracuda Web Application Firewall VMSS.
7. **Boot diagnostics**: When **Enabled**, the boot up debug logs gets saved in the specified storage account.
8. **Specify storage account where license file is stored** : Enter the name of the storage account where your license file is stored.

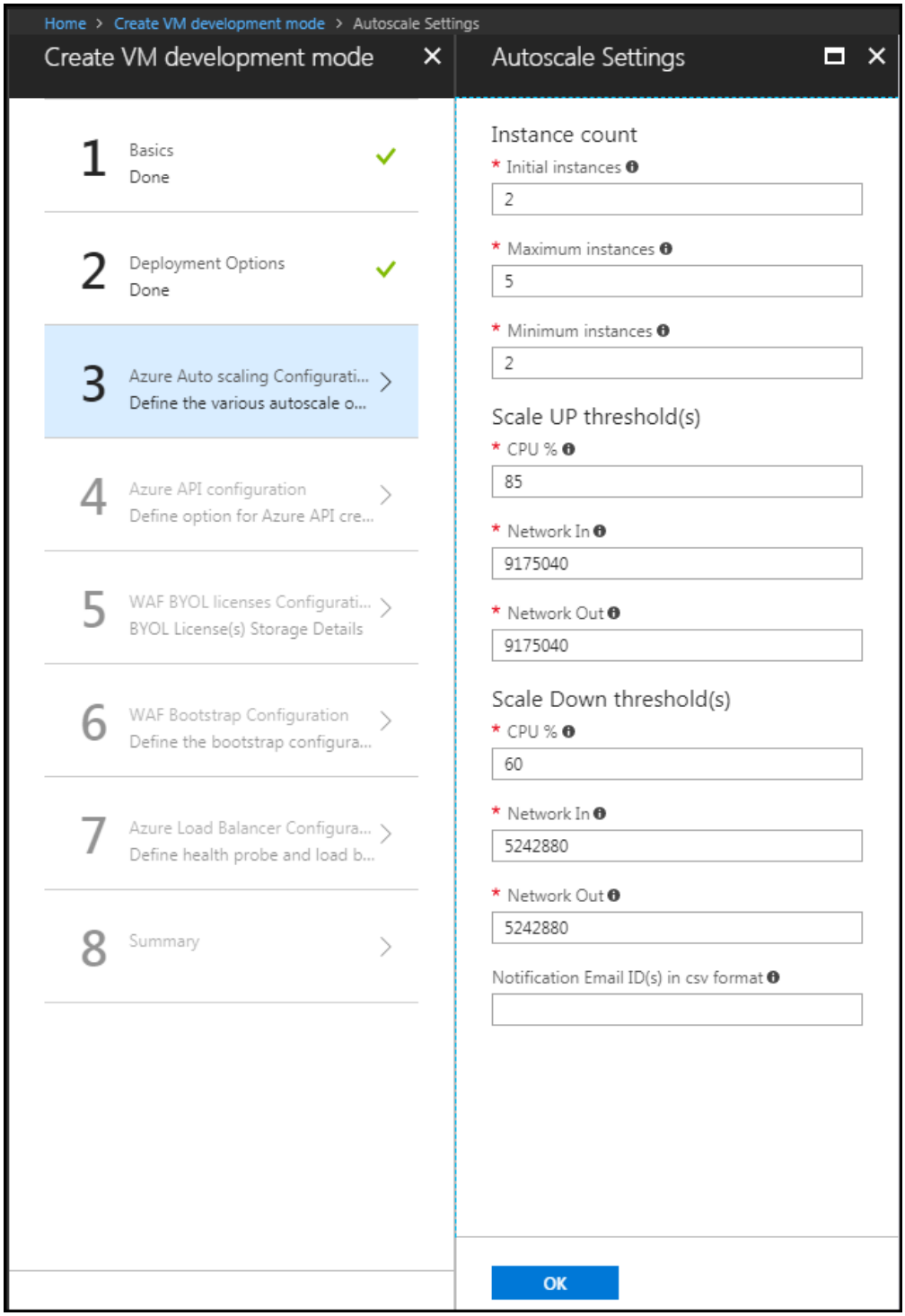
   Ensure that the license file is created in the valid JSON format and named as "*barracuda-byol-license-list.json".* Refer to *Step 3. Create and upload license file* to know more about the license key and how to generate and upload them.
9. **License Storage Account Key** : Enter the account key for your storage account. The key is available in the path - " **Storage account" > Access keys > Key1, Key2** You are provided with two access keys so that you can maintain connections using one key while regenerating the other.
10. **License Storage Blob Name** : Enter the path of the storage Blob where the license file is stored.
11. Click **OK**.



8. In the **Create Barracuda WAF VMSS Template - BYOL > 3 Azure Auto Scaling Configuration** page:
    1. **Instance Count**
        1. **Initial Instances**: Enter the number of instances to be deployed initially to serve the traffic. **Default**: 2
        2. **Maximum Instances**: Enter the maximum number of instances to be scaled up to handle the traffic when required. **Default**: 5

3. **Minimum Instances**: Enter the minimum number of instances to be scaled down when the traffic less. **Default**: 2
   - Ensure that the **Minimum Instances** are lesser than or same as the **Initial Instances**.
   - If the **Initial Instances** value is less than the **Minimum Instances**, the deployment of instances will fail.
4. **Overprovisioning**: When set to **Enable**, the VMSS spins up more number of virtual machines than what is required to handle the traffic.

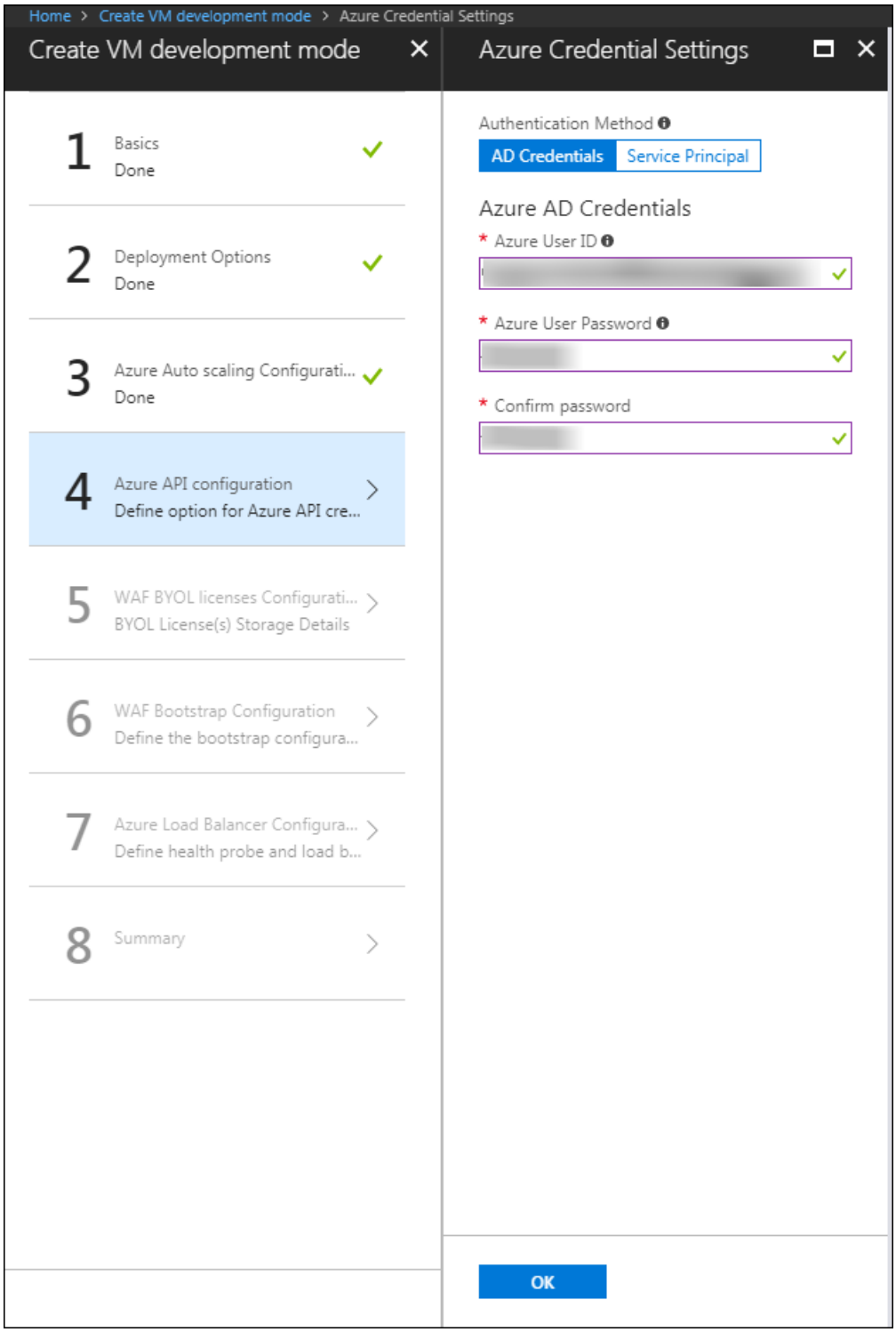
2. **Scale Up Thresholds**
   1. **CPU%**: Enter the scale up threshold for CPU utilization. **Default**: 85%
   2. **Network In**: Enter the scale up threshold for NetworkIn throughput. **Default**: 9175040
   3. **Network Out**: Enter the scale up threshold for NetworkOut throughput. **Default**: 9175040
3. **Scale Down Thresholds**
   1. **CPU%**: Enter the scale down threshold for SPU utilization. **Default**: 60%
   2. **Network In**: Enter the scale down threshold for NetworkIn throughput. **Default**: 5242880
   3. **Network Out**: Enter the scale down threshold for NetworkOut throughput. **Default**: 5242880
4. **Notification Email ID(s) in CSV Format**: Enter the email address to which the auto scaling event notification emails needs to be sent.
5. Click **OK**.



9. In the **Create Barracuda WAF VMSS Template - BYOL > 4 Azure API Configuration** page:
10. **Authentication Method**: Select the authentication method to authenticate to Azure Active Directory (AAD).
    1. **Azure AD Credentials**
        1. **Azure User ID**: Enter the user name to authenticate to the AAD.
        2. **Azure User Password**: Enter the password associated with user.
        3. **Confirm Password**: Re-enter the password to confirm.
    2. **Azure Service Principal**

1. **Client ID**: Enter the ID of the application in AAD.
2. **Tenant ID**: Enter the ID of the Active Directory tenant.
3. **Azure Secret Key**: Enter the secret key generated.

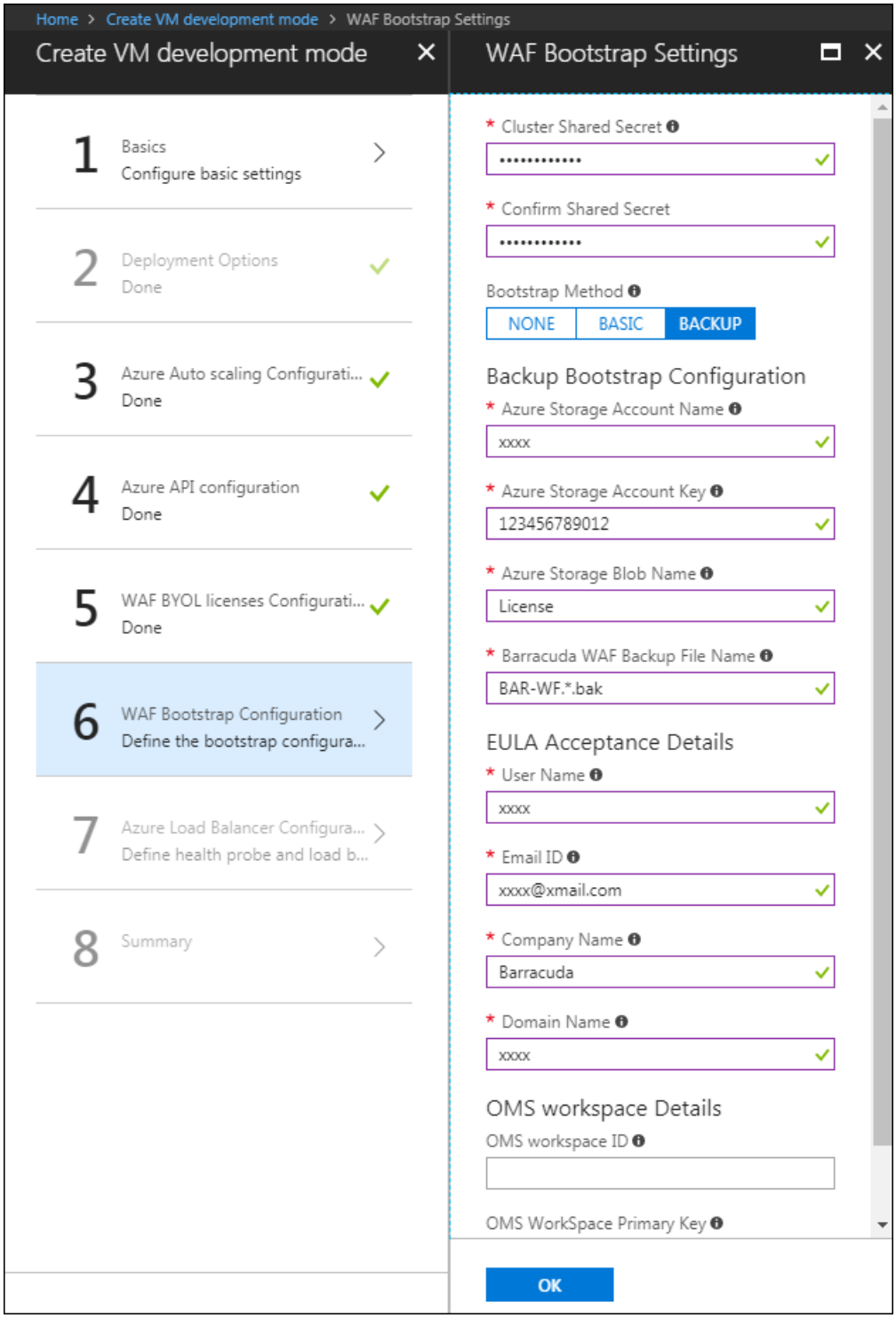
3. Click **OK**.



12. In the **Create Barracuda WAF VMSS Template - BYOL > 5 Barracuda Web Application Firewall Bootstrap Settings** page.
    1. **Cluster Shared Secret**: Enter a password to be used by the Barracuda Web Application

Firewall instances in the VMSS group.

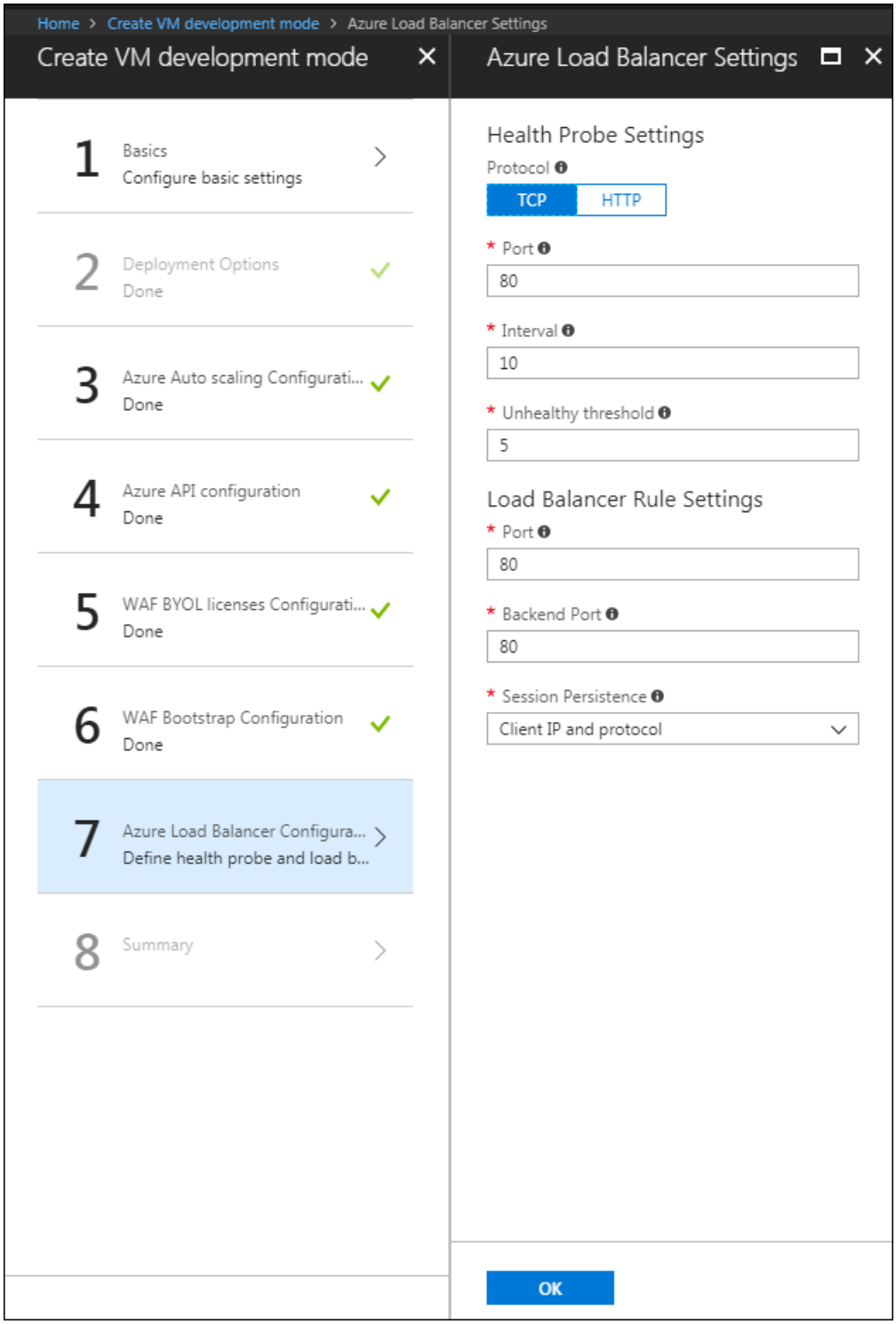
2. **Confirm Shared Secret**: Re-type the shared secret password.
3. **Bootstrap Method**: Select the method (**NONE, BASIC** or **BACKUP**) for bootstrapping.
4. **Basic Bootstrap Configuration**
    1. **WAF Service Name**: Enter a name for the service that needs to be created on the Barracuda Web Application Firewall instances.
    2. **WAF Service Port**: Enter the port number on which the service is listening to.
    3. **Backend Servers (IP:PORT)**: Enter the IP address of the server followed by the port that needs to be protected by the Barracuda Web Application Firewall. Use comma (,) as a separator to specify multiple server IP addresses.
5. **Backup Bootstrap Configuration**
    1. **Azure Storage Account Name**: Enter the name of the storage account.
    2. **Azure Storage Account Key**: Enter the key of the storage account.
    3. **Azure Storage Blob Name**: Enter the name of the blob configured in the storage account.
    4. **Type of Backup file**: Select the type of the backup file that you want to use for bootstrapping the instances.
    1. **Barracuda Web Application Firewall Backup file Name**: Enter the name of the backup file.
6. **OMS Workspace Details**
    1. **OMS Workspace Primary Key**: Enter the primary key of the OMS server.
    2. **OMS Workspace Primary Key**: Enter the primary key of the OMS server.
7. Click **OK**.



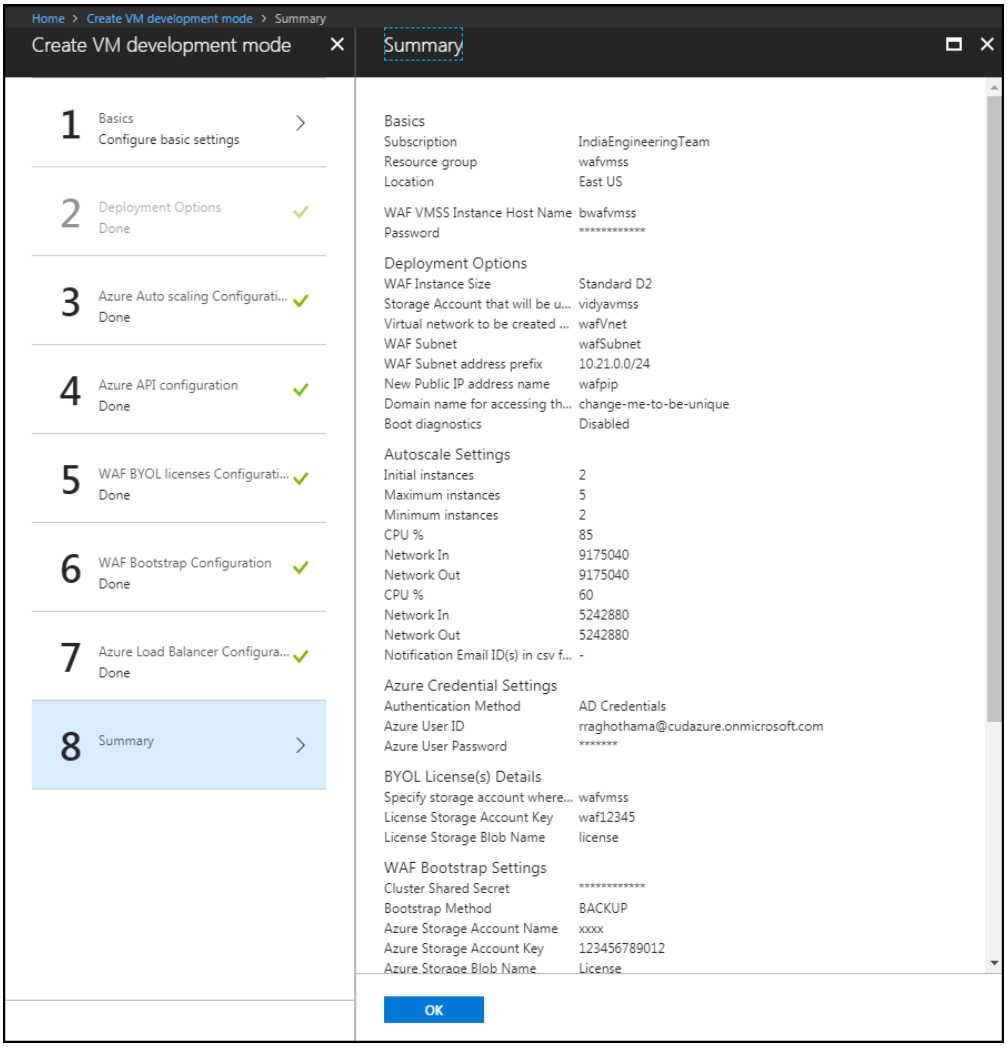
13. In the **Create Barracuda WAF VMSS Template - BYOL > 6 Azure Load Balancer Configuration** page:
    1. **Health Probe Settings**
        1. **Protocol**: Select **TCP** or **HTTP**. It is recommended to use the **TCP** protocol.
        2. **Port**: Enter the port to be used when probing the instance.
        3. **Interval**: Enter the interval time to probe the instance.
        4. **Unhealthy threshold**: Enter how many attempts can fail before the backend instance is marked as unhealthy.

2. **Load Balancer Rule Settings**
    1. **Port**: Enter the port on which the load balancer is listening.
    2. **Backend Port**: Enter the port on which the Barracuda Web Application Firewall is listening.
    3. **Session Persistence**: Select the persistence type.
3. **EULA Acceptance Details**
    1. **User Name**: Enter your user name.
    2. **Email ID**: Enter your Email address.
    3. **Company Name**: Enter your company name.
    4. **Domain Name**: Enter the domain name.

1. Click **OK**.



14. In the **Create Barracuda WAF VMSS Template - BYOL > 7 Summary** page, verify the values you entered and click **OK**.



Recommendations

- If the license file "*barracuda-byol-license-process.dat*" which was generated by the previous stack is present in blob storage, then free licenses may not be available. This can lead to provisioning failures.
- It is advised not to delete or modify the "*barracuda-byol-license-process.dat*" license file when the VMSS stack is in **Running** state. It can lead to provisioning/clustering failures.
- In scenarios, when you deploy an additional VMSS stack, it is recommended to use a different blob path for storing the "*barracuda-byol-license-list.json*" license file.

Figures