

## Reprovision Virtual Machines Deployed in a Public Cloud

<https://campus.barracuda.com/doc/68362024/>

The Barracuda Web Application Firewall virtual machines deployed on Microsoft Azure/Amazon Web Services can be reprovisioned using the web interface WebConsConf.

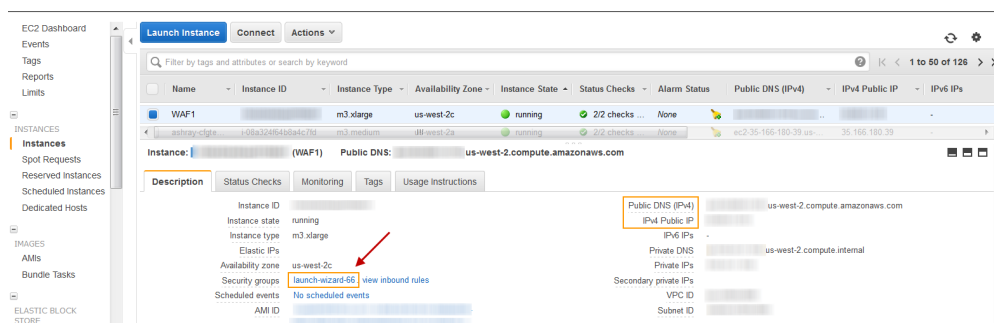
### Prerequisites

The Barracuda Web Application Firewall virtual machine:

- Should have Internet access to reach the Barracuda servers on port 80 and 443.
- Should not be clustered with other Barracuda Web Application Firewall virtual machine(s).
- Should have port 42832 opened in the Network Security Group on Microsoft Azure or Security Group on Amazon Web Services. (Refer to the sections mentioned below.)
  - [Configuring the WebConsConf Port for the Barracuda Web Application Firewall VM on Amazon Web Services](#)
  - [Configuring the WebConsConf Port for the Barracuda Web Application Firewall VM on Microsoft Azure](#)

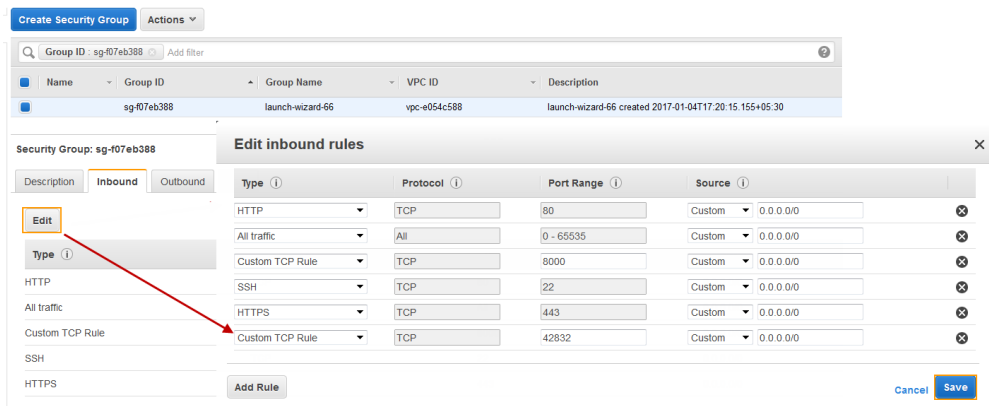
### Configuring the WebConsConf Port for the Barracuda Web Application Firewall VM on Amazon Web Services

1. Log into the [EC2 Management Console](#).
2. From the EC2 dashboard, select **Instances** under **INSTANCES**.
3. Select the instance that needs reprovisioning from the instances table.
4. Click on the security group in the **Description** tab. Also, note down the **Public DNS (IPv4)** or **IPv4 Public IP**.



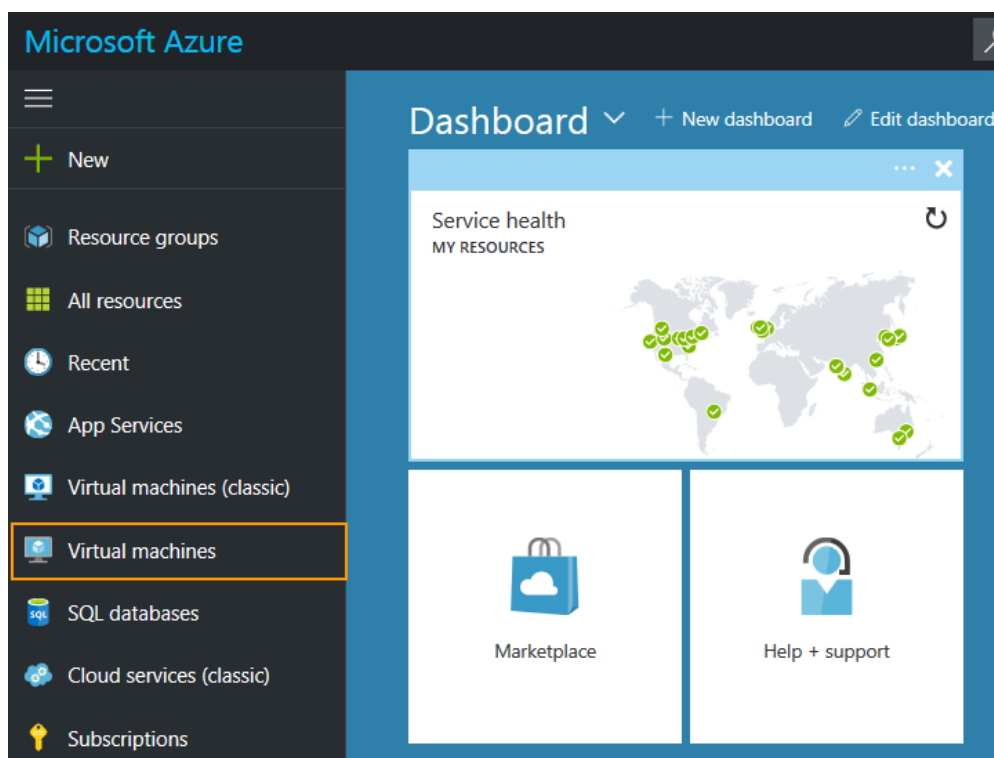
5. In the Security Group page, select the **Inbound** tab and click **Edit**.
6. In the **Edit inbound rules** window, click **Add Rule** and do the following:
  1. **Type** - Select **Custom TCP Rule**.
  2. **Port Range** - Specify **42832**.

3. **Source** – Enter 0.0.0.0/0
7. Click **Save**.

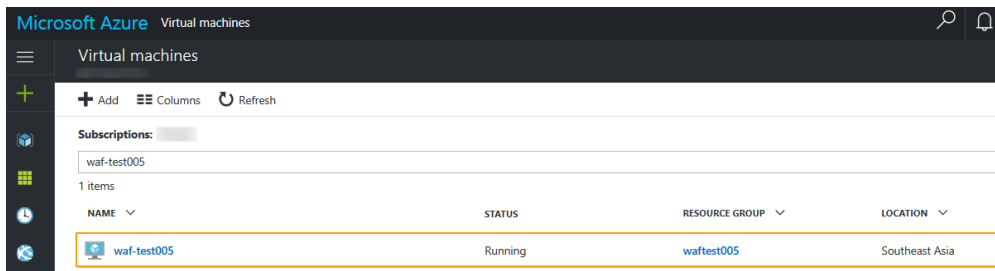


## Configuring the WebConsConf Port for the Barracuda Web Application Firewall VM on Microsoft Azure

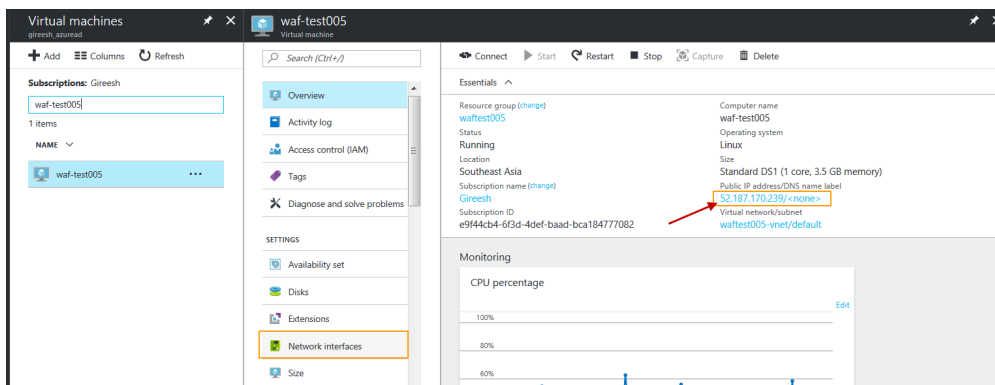
1. Log into the [Microsoft Azure Management Portal](#).
2. Click **Virtual machines** on the left panel.



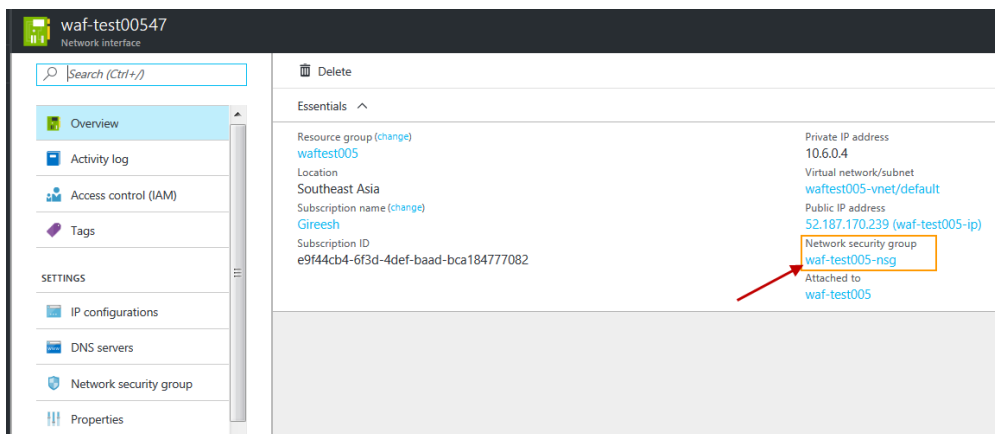
3. In the **Virtual machines** page, locate the virtual machine that you want to reprovision.



4. Click on the instance, and select **Network Interfaces**. Also, write down the **Public IP address/DNS server label** of the Barracuda Web Application Firewall instance.



5. Click on the network interface, and select the **Network security group** associated with the interface.



6. In the **Network security group** page, click on the icon next to **Inbound security rules**.

Delete

Essentials ^

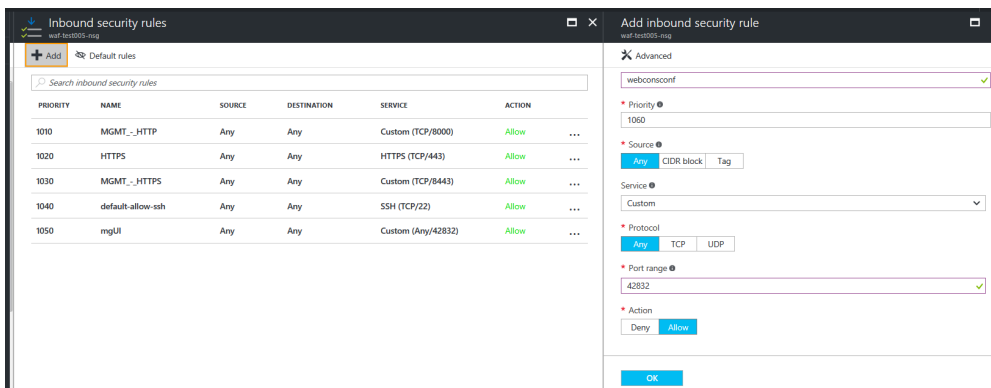
Resource group [\(change\)](#)  
[waftest005](#)  
 Location  
 Southeast Asia  
 Subscription name [\(change\)](#)  
[Gireesh](#)  
 Subscription ID  
 e9f44cb4-6f3d-4def-baad-bca184777082

Security rules  
 5 inbound, 0 outbound  
 Associated with  
 0 subnets, 1 network interfaces

**5 Inbound security rules**

PRIORITY	NAME	SOURCE	DESTINATION	SERVICE	ACTION
1010	MGMT_-_HTTP	Any	Any	Custom (TCP/8000)	Allow
1020	HTTPS	Any	Any	HTTPS (TCP/443)	Allow
1030	MGMT_-_HTTPS	Any	Any	Custom (TCP/8443)	Allow
1040	default-allow-ssh	Any	Any	SSH (TCP/22)	Allow
1050	mgUI	Any	Any	Custom (Any/42832)	Allow

7. In the **Inbound security rules** page, click **Add**.
8. In the **Add Inbound security rule** page, do the following:
  1. **Advanced** - Enter a name.
  2. **Priority** - Set the priority order for the rule.
  3. **Source** - Any
  4. **Service** - Custom
  5. **Protocol** - Any
  6. **Port range** - 42832
  7. **Action** - Allow
9. Click **OK**.



Inbound security rules

waftest005-nag

+ Add Default rules

Search inbound security rules

PRIORITY	NAME	SOURCE	DESTINATION	SERVICE	ACTION
1010	MGMT_-_HTTP	Any	Any	Custom (TCP/8000)	Allow
1020	HTTPS	Any	Any	HTTPS (TCP/443)	Allow
1030	MGMT_-_HTTPS	Any	Any	Custom (TCP/8443)	Allow
1040	default-allow-ssh	Any	Any	SSH (TCP/22)	Allow
1050	mgUI	Any	Any	Custom (Any/42832)	Allow

Add inbound security rule

waftest005-nag

Advanced

webconconf

\* Priority 1060

\* Source Any CIDR block Tag

Service Custom

\* Protocol Any TCP UDP

\* Port range 42832

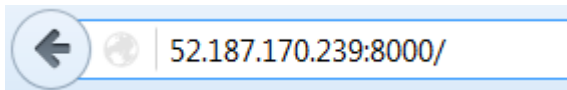
\* Action Deny Allow

OK

## Reprovisioning the Barracuda Web Application Firewall Virtual Machine Deployed on Microsoft Azure/Amazon Web Services

Perform the steps below to reprovision the Barracuda Web Application Firewall virtual machine (VM):

1. Open a web browser, and enter the public IP address followed by the port written down in the section "Configuring the WebConsConf Port for the Barracuda Web Application Firewall VM on Microsoft Azure/Amazon Web Services".



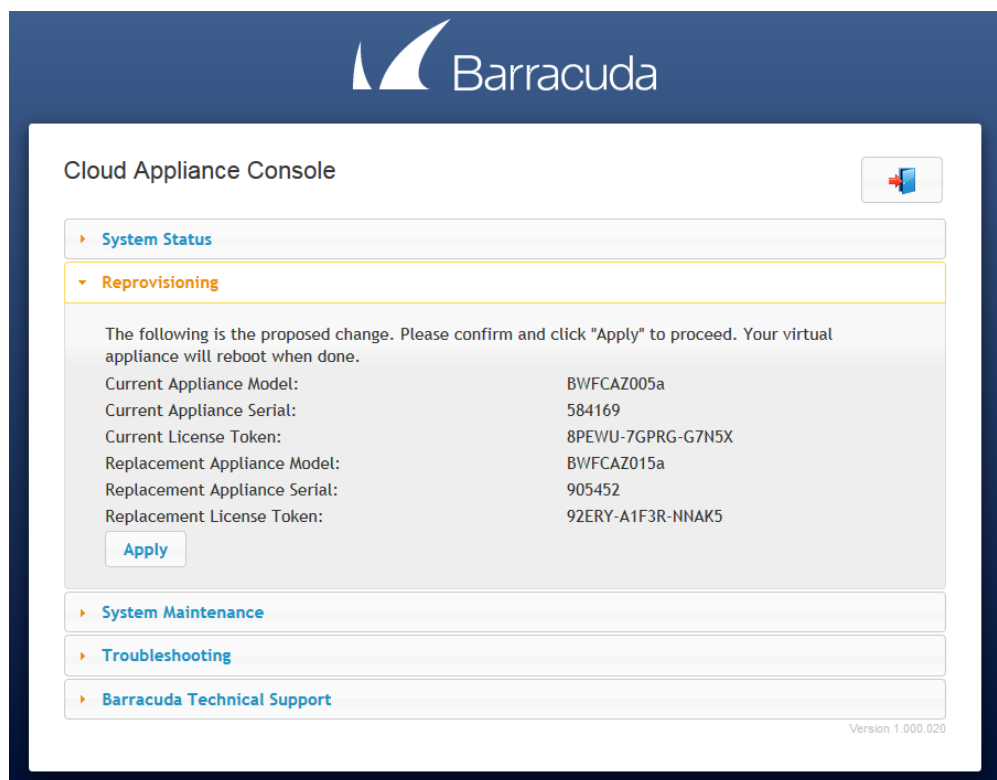
2. Log into the Barracuda Web Application Firewall web interface using your credentials.
3. Go to the **NETWORKS > ACL** page, **Auto Created System ACLs** section, and confirm that the WebConsConf rule is created with port 42832.
4. Now, open another web browser and enter the public IP address written down in Step 4, followed by the WebConsConf port (42832).
5. Log into the Cloud Appliance Console using your admin user credentials.



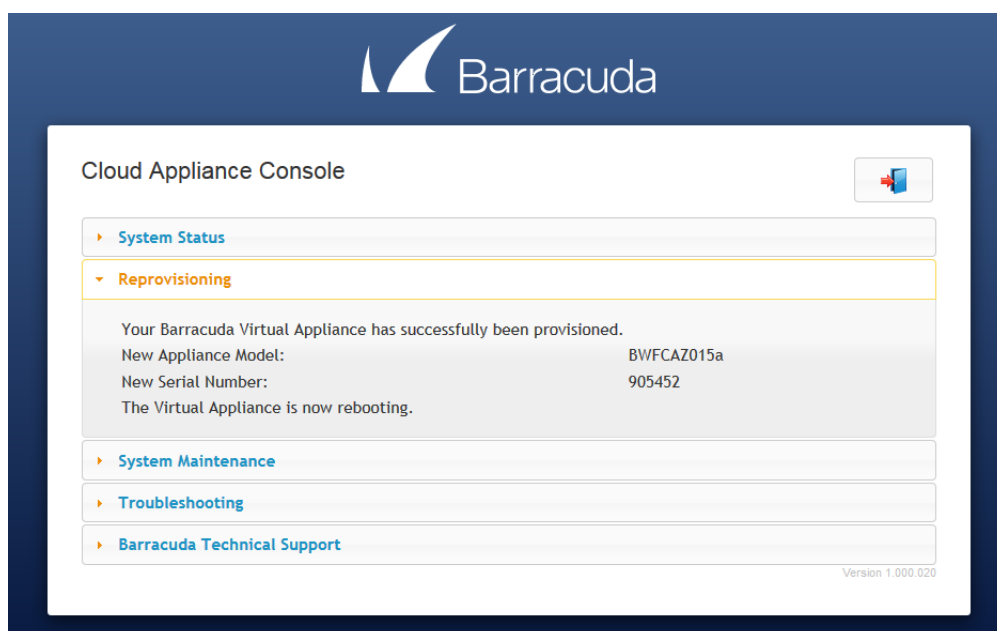
6. In the **Cloud Appliance Console** page, click **Reprovisioning** and do the following:
  1. Enter the new license key in the **Replacement License Token** text box.
  2. Click **Download**.




3. After the download is complete, click **Apply**.



7. The Barracuda Web Application Firewall virtual appliance is provisioned with the new model and serial number.



8. The virtual appliance reboots with the new serial number and the selected model.



The image shows the Barracuda Cloud Appliance Console interface. At the top, there is a blue header with the Barracuda logo. Below the header, the main content area is white and contains a sidebar on the left with navigation links: System Status, Reprovisioning, System Maintenance, Troubleshooting, and Barracuda Technical Support. The Reprovisioning section is currently selected and expanded, showing details about the current appliance model (BWFAZ015a), serial number (905452), and license token (92ERY-A1F3R-NNAK5). It also includes a text box for entering a replacement license token and a Download button. A small icon of a server with a plus sign is visible in the top right corner of the console area.

**Barracuda**

Cloud Appliance Console

System Status

Reprovisioning

Current Appliance Model: BWFAZ015a  
Current Appliance Serial: 905452  
Current License Token: 92ERY-A1F3R-NNAK5

This form will allow you to reprovision your Barracuda Virtual Appliance. Enter a new license token and click "Download" to proceed. Once the new license bundle is retrieved, you will see a confirmation message.

Replacement License Token:

Download

System Maintenance

Troubleshooting

Barracuda Technical Support

Version 1.000.020

## Figures

1. Instance.png
2. Security\_Group\_1.png
3. Virtual\_Machine.png
4. WAF\_VM.png
5. Network\_Interface\_Public\_IP.png
6. Network\_Security\_Group.png
7. Inbound\_security\_rules.png
8. Add\_Inbound\_Sec\_Rules.png
9. Public\_IP\_Address.png
10. Cloud\_Appliance\_Console.png
11. New\_Token.png
12. Reprovisioning\_Completed.png
13. Instance\_with\_New\_Serial\_Number.png
14. Reprovisioned\_With\_New\_Serial\_No.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.