Create a Container Deployment File

https://campus.barracuda.com/doc/98208763/

You must deploy your container before your application can go live. A wizard will help you create the YAML file WAF-as-a-Service uses to deploy your container.

1. Go to the **Resources** tab. Click **WAF Containers > Container Management**.
2. Find your container in the table and click the three dots in the **Action** column.
3. Click the **Deploy** option to open the **Container Deployment** wizard.

Container Deployment Infrastructure

Select the infrastructure that will host your container and click **Continue**.

- Currently only Kubernetes is supported for *automatic* deployment – meaning these steps are creating a configuration file that is compatible with Kubernetes.
- Other container infrastructures are supported, but will likely require a different format or different environment variables. It may be helpful to look through the file created here before deploying with another infrastructure.

Private Key for Container Deployment

Select a method to add the private key you generated. See Create Your Own Container Key if you need to generate a new one.

- We recommend inserting the key directly into the deployment (YAML) file created by this wizard. You can also choose to upload or paste the key here.

Click **Continue** to go to the **Advanced Settings**.

Container Deployment Advanced Settings

1. Select a **Datapath Version**. See Managing the datapath for more information.
2. Select the **Config Token** to be used with this deployment. If you are unsure when to use, select **Token 1**. See Rotating Container Config Tokens for more about using and rotating **Config Tokens** .
3. Choose whether or not to include **Virus Scanning** with this deployment.
   If you do not add **Virus Scanning** with your container deployment, the **App Profiles**

component will still show it as an option. Selecting **Virus Scanning** there will not enable scanning. However, it can be added later by modifying and redeploying the container.

4. Click **Continue.**

Container Troubleshooting Options

Select the desired **Troubleshooting** options.

- **Disable diagnostic log collection** – Clicking this box will prevent diagnostic and deployment data from being sent to Barracuda and will make it more difficult for Barracuda to diagnose any potential problems. If you allow this data to go to Barracuda it is encrypted and only available to necessary support personnel.
- **Do not send Access Logs and Firewall Logs to WAF-as-a-Service** – Selecting this prevents container traffic from being sent to Barracuda.

  Access Logs and Firewall Logs are an important troubleshooting tool. If you do not send them to Barracuda, you must use the Log Export component to configure your own Log Servers to receive logs directly from the WAF Container. Without logs, neither you nor Barracuda will be able to troubleshoot your configuration.

- **Disable handling of Scheduled Events when deployed on Microsoft Azure** – This only applies to containers hosted in Microsoft Azure. All others should leave this box unchecked. Azure will perform maintenance events that will interrupt container operations. Clicking this box enables fluid handling of these events.

Choose one of the following **Support Tunnel** options. A support tunnel provides a way for Barracuda Support to access your WAF-as-a-Service deployment.

- **Disabled** – The support tunnel will be completely disabled. Barracuda Support will not be able to troubleshoot issues on your container.
- **Enabled** – The tunnel will always be open.
- **Allow tunnel to be opened remotely through the WAF-as-a-Service UI or API** – The tunnel can be opened and closed by the administrator.
- **Allow tunnel to be opened only through a local kubectl command** – The support tunnel cannot be opened through the WAF-as-a-Service UI. This is the most secure option.

Choose a **Core Dump Collection** option. A core dump is information collected about the container and WAF-as-a-Service's state in the rare instance that a crash occurs.

- **Disable** – Core dumps cannot be collected. Barracuda will not be able to troubleshoot problems.
- **Enable** – Core dumps are collected by default.
- **Allow collection to be enabled remotely through the WAF-as-a-Service UI or API** – The administrator can enable core dump collecting through the UI.

- **Allow collection to be enabled only through a local kubectl command** – This is the most secure collection option.

  Corefiles may contain parts of plaintext from your requests or responses. Disable this setting if your application transfers data that cannot be sent to third parties according to regulations.
  If you deploy other (non-WAF) containers to the same cluster, their corefiles will also be sent to Barracuda. Barracuda will never open corefiles that are not from the WAF container.

Click **Continue** to generate the deployment file.

See Deploying your Own Container to learn how to deploy the container in your infrastructure.