Session Recording

https://campus.barracuda.com/doc/104369220/

Session recording is a troubleshooting tool that enables you to capture the live traffic i.e. the HTTP requests and HTTP responses from a specified client IP address to an application configured on WAF-As-A-Service. This feature is useful to debug traffic related problems, especially with HTTPS applications.

When configured and started, the Barracuda WAF-as-a-Service enables session recording on all traffic processing instances (Barracuda managed containers or custom containers) that are active for the last 60 seconds and serving traffic to the backend server.

Steps to Configure Session Recording

1. Go to the **RESOURCES** tab.
2. In the left panel, scroll down and expand **TROUBLESHOOTING**.
3. Select **Session Recording**.
4. On the Session Recording page, specify values for the following:
    1. **Application**: Click the drop-down list and select the application for which you want to capture the sessions.
    2. **Client-IP**: Specify the client IP address for which you want to enable the requests/responses to be captured. The session recording captures the requests/responses coming from the specified client IP.
    3. **Port**: Specify the port number associated with the client IP.
    4. **Recording Request**: Select the checkbox to enable requests to the application to be captured. Set the maximum request size limit to be captured during a session.
    5. **Recording Response**: Select the checkbox to enable responses to the application to be captured. Set the maximum response size limit to be captured during a session.

        You can capture only requests or responses, or both by enabling/disabling the **Recording Request** and **Recording Response** checkboxes. Ensure at least one option is selected before you start the recording.
    6. **Number of requests to record**: Specify the maximum number of requests to be captured during a session.
    7. **Content type to record**: Specify the content types that needs to be captured in the requests and/or responses during a session.
    8. Click **Start recording**.

After the session recording is stopped, the captured files can be downloaded as follows:

- All files are collected in a ZIP file and the **Download** option is available in the web interface.
- **Custom Container-based deployments**: The files are copied to the storage location specified in the environment variables of the deployment definition YAML file.

Use a text editor or an XML parser to open the downloaded file and check the request(s) and response(s) from the client and the server respectively.

-- When a new session is captured for the same application, the previous session is overwritten by the new session.

-- Session Recording should be started during a debugging window and stopped immediately after capturing the required information. It is not recommended to leave it running for a long time

Session Recording in Custom Containers

For session recording to work with custom container deployments, storage location (AWS S3 or Azure blob) is a mandatory parameter to be specified as a part of the deployment definition YAML file.

1. Follow the steps mentioned in Deploying WAF-as-a-Service Security Module as a Container on On-Premises Kubernetes Cluster to deploy the custom container.
2. After **Step 6. Download the YAML file**, edit the YAML file to include the following:
    1. Specify the storage location of the custom container in the respective environment variables:
       TROUBLESHOOTING_STORAGE_TYPE : "AWS"
       TROUBLESHOOTING_AWS_ACCESS_KEY_ID : ""
       TROUBLESHOOTING_AWS_SECRET_ACCESS_KEY : "
       TROUBLESHOOTING_AWS_BUCKET : ""

       TROUBLESHOOTING_STORAGE_TYPE : "AZURE"
       TROUBLESHOOTING_AZURE_CONNECTION_STR : ""
       TROUBLESHOOTING_AZURE_CONTAINER_NAME : ""
3. Save and deploy the container.

Storage Environment Variables

To add Azure storage details, specify values for the following environment variables:

TROUBLESHOOTING_STORAGE_TYPE: "AZURE"

- **TROUBLESHOOTING_AZURE_CONNECTION_STR**: Specify the connection string of the Azure blob storage account.

- **TROUBLESHOOTING_AZURE_CONTAINER_NAME**: Specify the name of the blob container where you want to upload the session recording files.

Connection strings are the credentials to authenticate to the Azure storage account. The Barracuda WAF-as-a-Service uses the specified connection string to authenticate to Azure and upload the captured session recording files to a folder in the specified blob.

To add AWS storage details, specify values for the following environment variables:

TROUBLESHOOTING_STORAGE_TYPE: "AWS"

- **TROUBLESHOOTING_AWS_ACCESS_KEY_ID**: Specify the AWS access key associated with the Identity and Access Management (IAM) user.
- **TROUBLESHOOTING_AWS_SECRET_ACCESS_KEY**: Specify the AWS secret access key (password) associated with the access key.
- **TROUBLESHOOTING_AWS_BUCKET**: Specify the name of the S3 bucket on AWS.

Access keys are the credentials to authenticate to Amazon Web services. The Barracuda WAF-as-a-Service uses the specified access key ID and secret access key to authenticate to AWS and upload the captured session recording files to a folder in the specified S3 bucket.

Example for Azure Storage Type

-----BEGIN RSA PRIVATE KEY-----
MIIEowIBhUBXi5ArPcc6YQopxY0lxFEMuJ+jT6p6mKKSdmNoOoHsjxCP8fh5vVl4KIKfpZCi
MM0jlX+5cYM+SyjzG5wwoDvBWRGWw+jFQBQ/VSECgYBLJdTV6lVMeELrwdUPFrPL
H9sqT5UU24Ky/Xzpwk7CGVXIqCP0yBXwG7V1j6wtm4kPzOOGxJZp4sPUL+InfbqW
-----END RSA PRIVATE KEY-----
#BARRACUDA_SERVER_CA: NONE
DEVICEHUB_AUTH_KEY : “secret_key”
TROUBLESHOOTING_STORAGE_TYPE : “AZURE”
TROUBLESHOOTING_AZURE_CONTAINER_NAME : “container1”
TROUBLESHOOTING_AZURE_CONNECTION_STR :
“DefaultEndpointsProtocol=https;AccountName=containername;AccountKey=ABCD1234ghjk==/MS.net”

Example for AWS Storage Type

-----BEGIN RSA PRIVATE KEY-----

```
    MIIEowIBhUBXi5ArPcc6YQopxY0lxFEMuJ+jT6p6mKKSdmNoOoHsjxCP8fh5vVl4KIKfpZCi
    MM0jlX+5cYM+SyjzG5wwoDvBWRGWw+jFQBQ/VSECgYBLJdTV6lVMeELrwdUPFrPL
    H9sqT5UU24Ky/Xzpwk7CGVXIqCP0yBXwG7V1j6wtm4kPzOOGxJZp4sPUL+InfbqW
    -----END RSA PRIVATE KEY-----
#BARRACUDA_SERVER_CA: NONE
DEVICEHUB_AUTH_KEY : “secret_key”
TROUBLESHOOTING_STORAGE_TYPE : “AWS”
TROUBLESHOOTING_AWS_ACCESS_KEY_ID : “DEFJKLOUYHGBGNMJ”
TROUBLESHOOTING_AWS_SECRET_ACCESS_KEY : “KLJYTR6OLPIJUxcd8ZSDEregM”
TROUBLESHOOTING_AWS_BUCKET : “bucket1”
```

-- Currently, only AWS and Azure storage options are available for custom containers.
-- Ensure that you specify the storage location in the deployment definition YAML file before initiating the session recording for the application.