Netsurion®
Powering Secure and Agile Networks

How-To Guide

Configuring Microsoft Defender to Forward Logs to EventTracker

Publication Date:

April 4, 2022

Abstract

This guide provides instructions to retrieve the **Microsoft Defender** events via the Azure Event Hub and then configure the **Azure function app** to forward the logs to EventTracker. After EventTracker receives the logs from the Event Hub, the reports, dashboard, alerts, and saved searches can be configured.

Scope

The configuration details in this guide are consistent with EventTracker version 9.3 and later and Microsoft Defender for Endpoint.

Audience

The Administrators who are assigned the task to monitor the **Microsoft Defender** events using EventTracker.

Table of Contents

1. Overview

Microsoft 365 Defender is a unified pre- and post-breach enterprise defense suite that natively coordinates detection, prevention, investigation, and response across endpoints, identities, email, and applications to provide integrated protection against sophisticated attacks.

EventTracker helps to monitor events from the Microsoft Defender for Endpoint. Its dashboard and reports will help you track, alert information, and alert evidence which in turn help to detect file-less attacks, backdoor drops, and virus/malware.

2. Prerequisites

- An Azure Subscription and a user who is a global administrator.
- Azure Resource group.
- EventTracker Manager public IP address.
- Download Azure integration package from ETS_Microsoft_Defender_Forwarder.zip

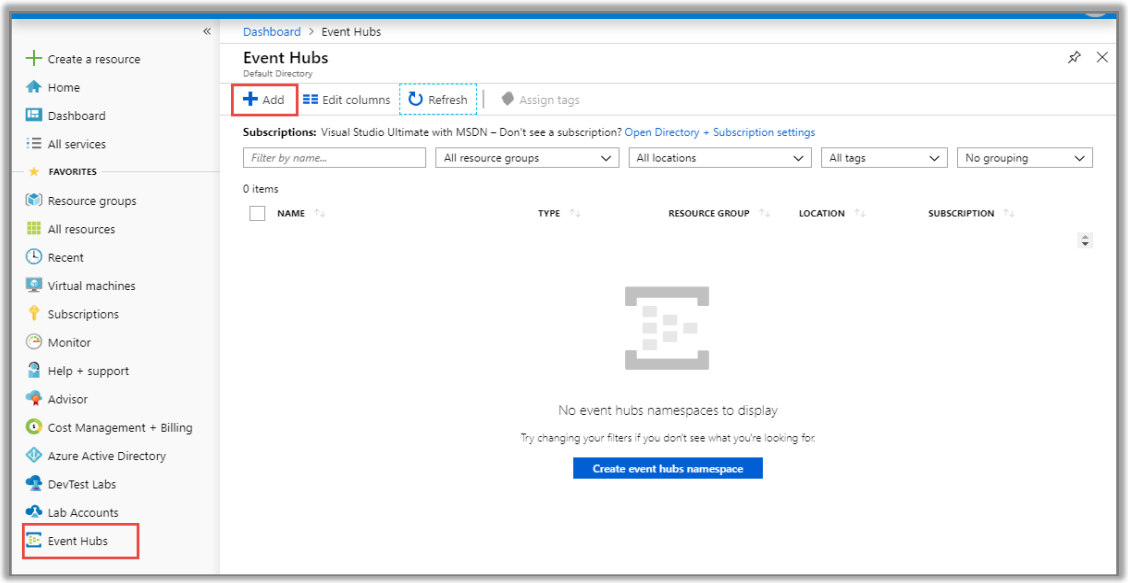
3. Configuring Event hub to Forward Logs to EventTracker

Microsoft Defender can be integrated with EventTracker by streaming the logs to the Azure Event Hub, and from Azure Event Hub to EventTracker.

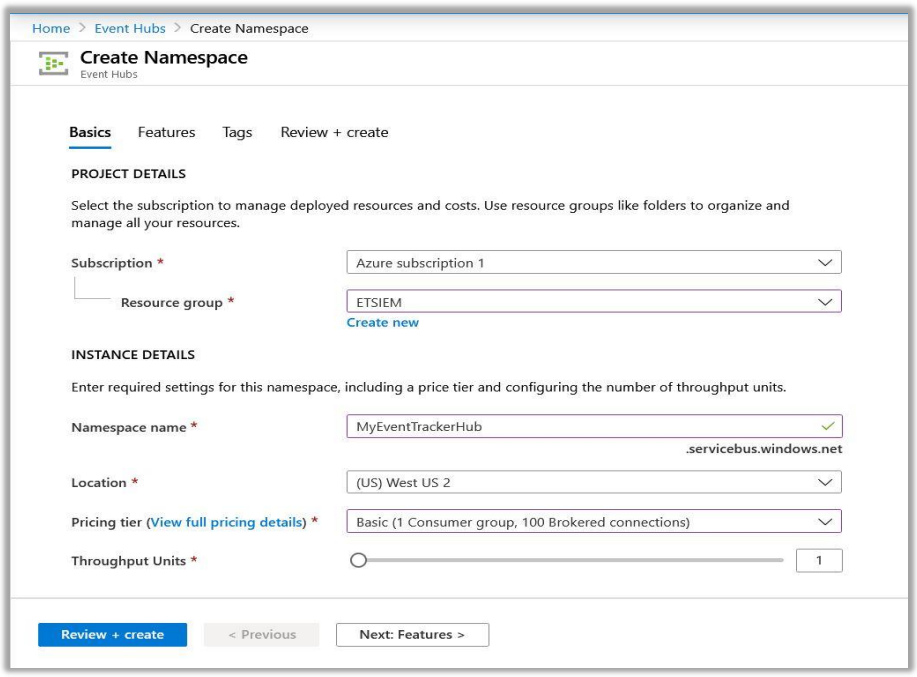
3.1 Creating an Event Hubs namespace and an Event Hub

The Event Hubs namespace contains one or more Event Hubs. The configured Azure services create Event Hub in these namespaces to store activities and diagnostics logs.

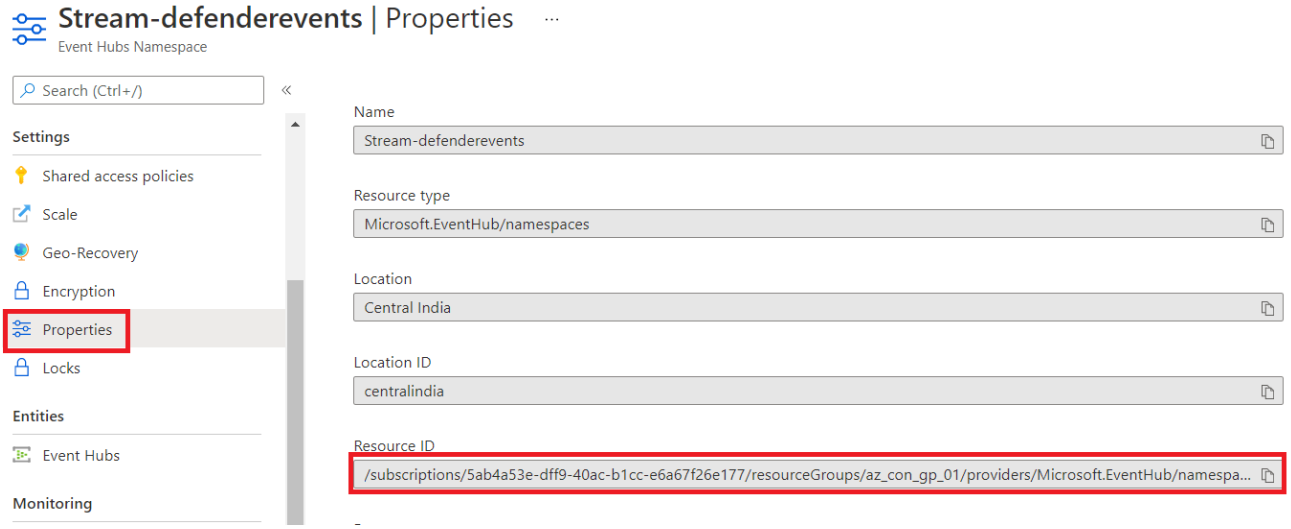
1. Login to portal.azure.com
2. Navigate to **All services > Event Hubs > Add.**



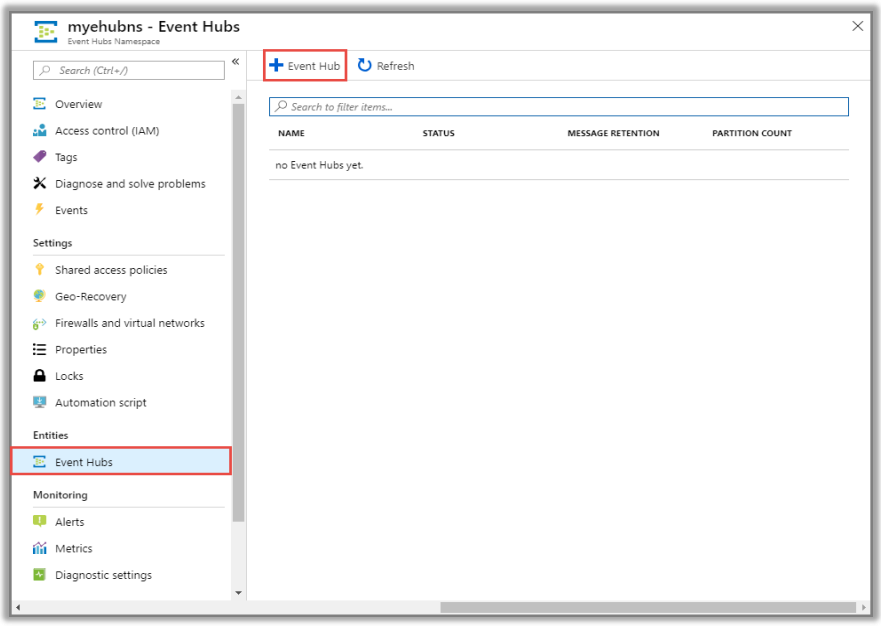
3. Create a namespace. Provide a **Namespace Name**, e.g. **MyEventTrackerHub**, Resource group, and any other settings -> **Review + Create**.
   Recommendation: Create and choose Resource group Name with "EventTracker". It would give a better picture of the billing for the services.



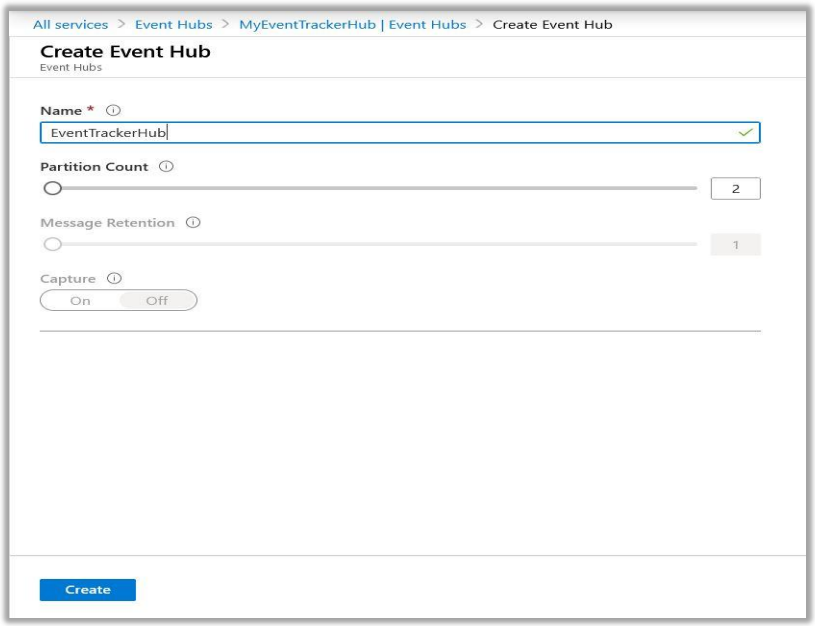
4. On the Event Hubs namespace page, Click **Properties** under **Settings** on the left panel and copy the **Resource ID** value, Which will be used in further steps (4.1 step 3)



5. On the Event Hubs namespace page, select **Event Hubs** on the left menu. At the top of the window, click **+ Event Hub**.



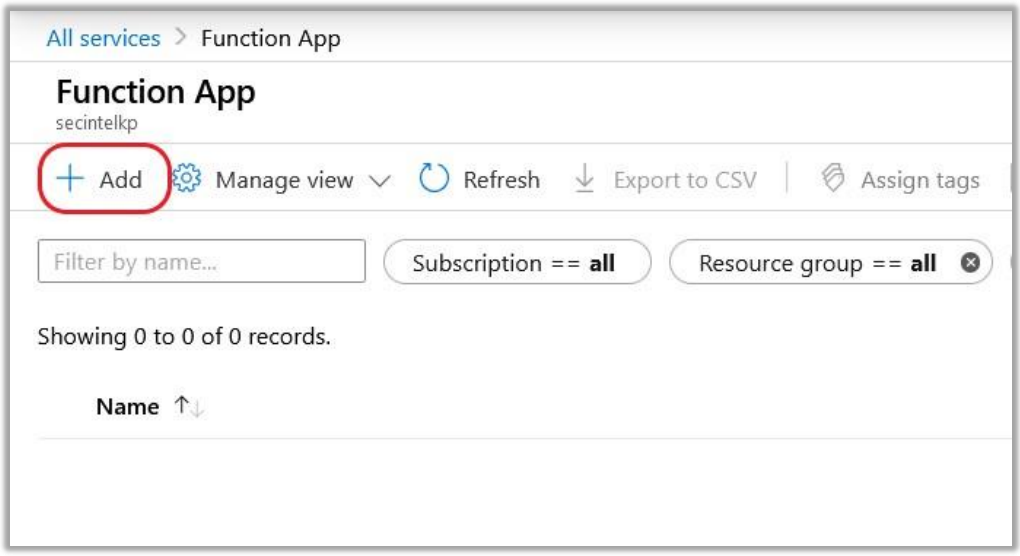
6. Type a name for your Event Hub and provide the EventHub name, partition count based on your environment, **Copy** the Event Hub name which will be used in further steps (4.1 Step 3), and then click **Create**.



3.2 Configuring Azure Function app to forward data to EventTracker

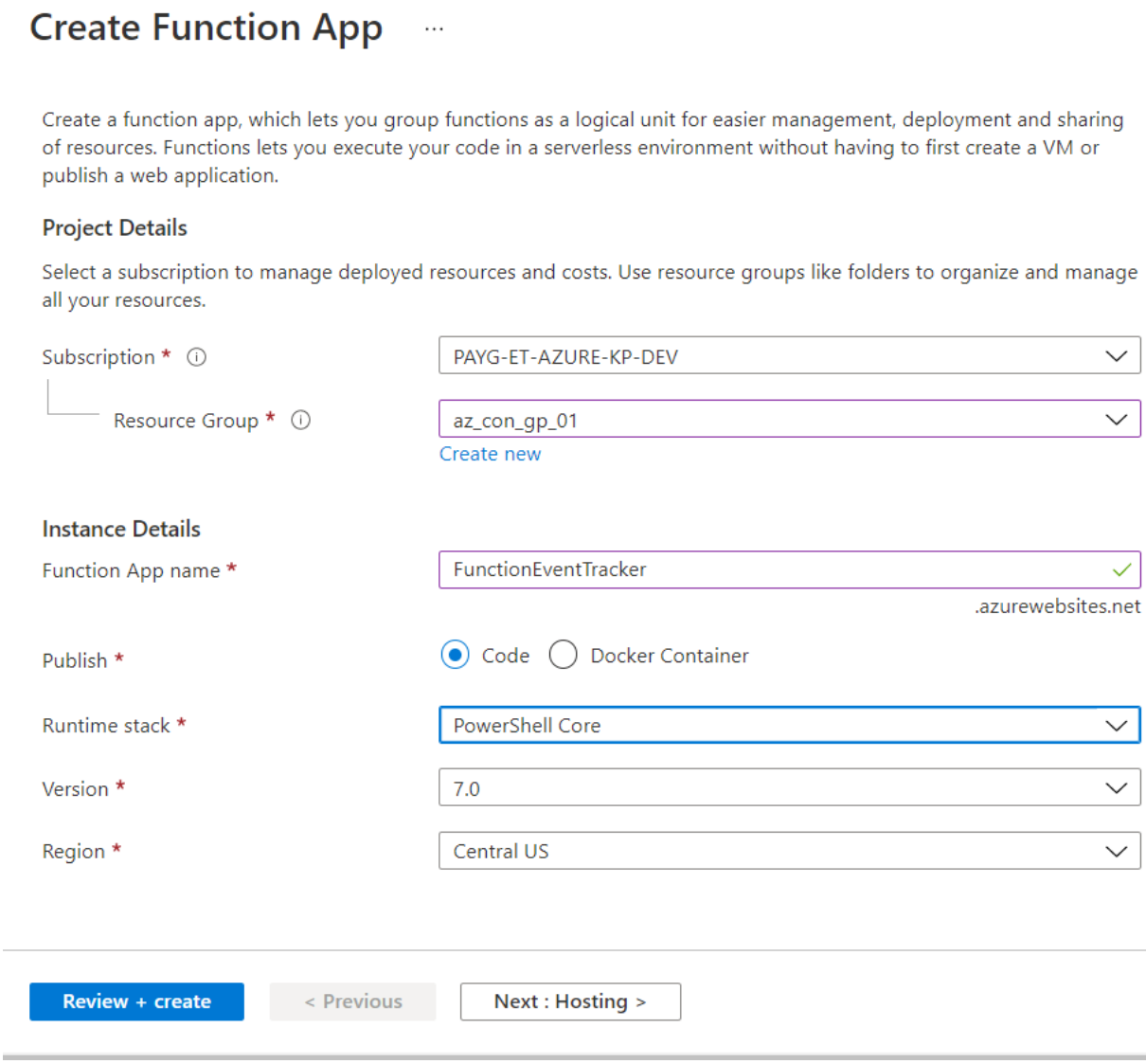
Azure Functions is a solution for easily running small pieces of code, or **functions**, in the cloud. For more details on the function app overview and cost, refer to the link.

1. Navigate to **All Services > Function App** and click the **+ Add** button.

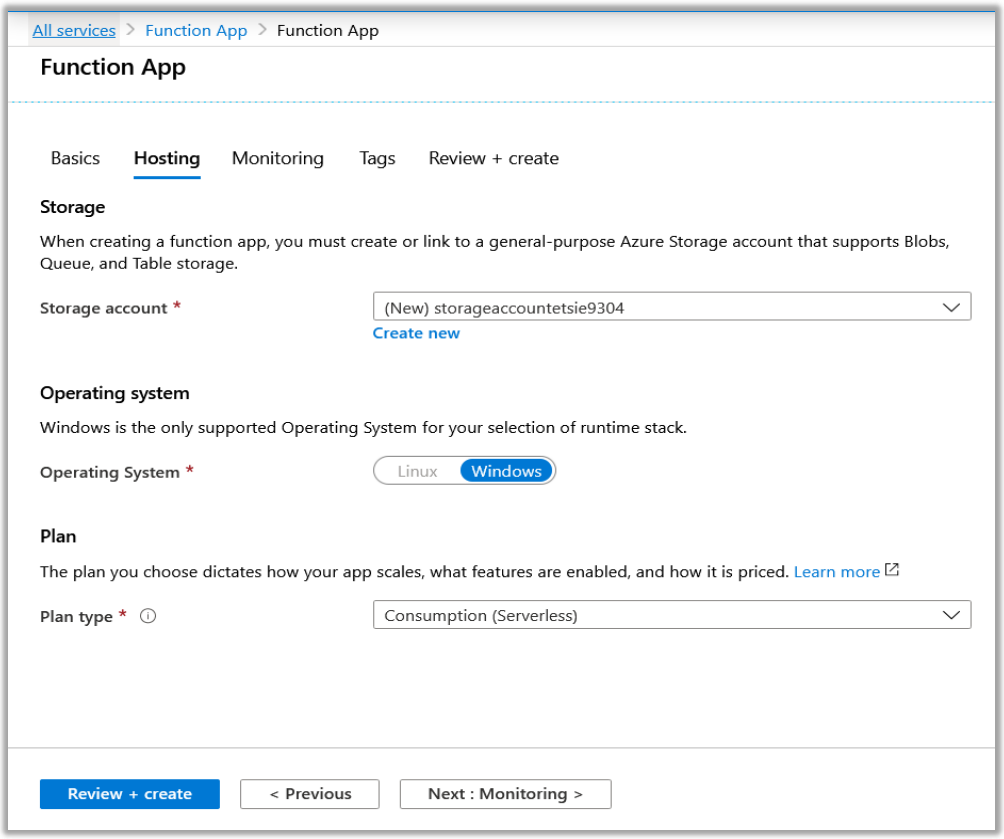


2. In the configure function app window,
   - In **Project Details**, select the desired subscription and **Resource Group**.
   - In **Instance Details**:
     - Provide a **function app name**, like **FunctionEventTracker**.
     - Select **Code** in **Publish** option.
     - In **Runtime stack**, select **PowerShell Core**.
     - Select the appropriate **region.**

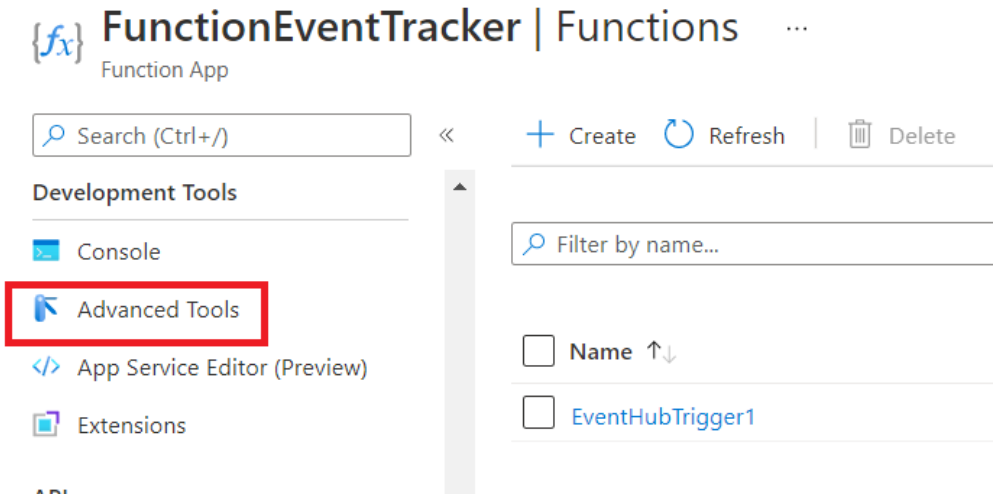
Recommendation: Create and choose Resource group Name with "EventTracker". It would give a better picture of the billing for the services.



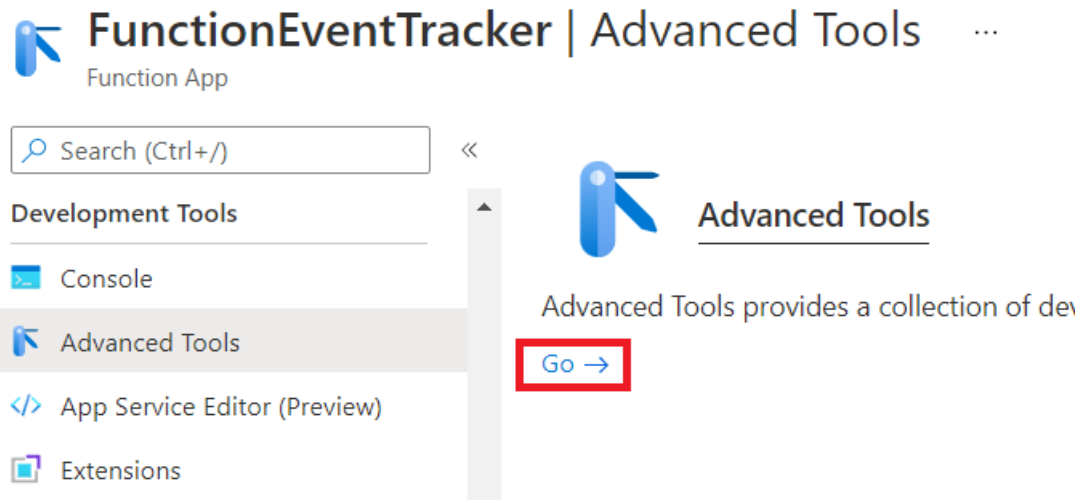
3. Click **Next: Hosting**.
   - Under Storage Section, select your storage account.
   - Under the Operating system, select Windows.
   - Under Plan, choose a plan of your choice.



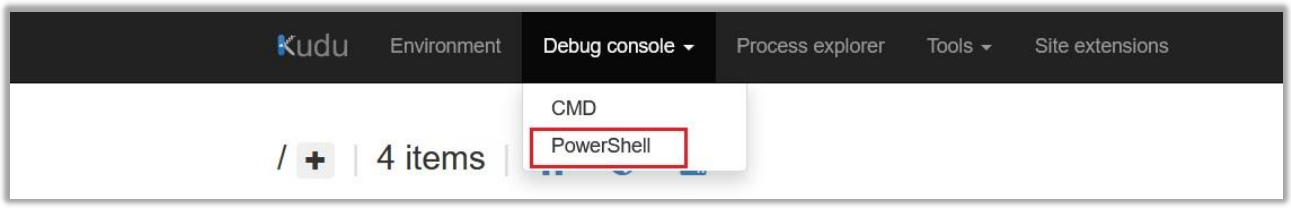
4. Click **Review + Create**.
5. After the **Function** app is created, navigate to All services > Function App > FunctionEventTracker to do further configuration and click on Advanced **tools** under **Development** Tools.



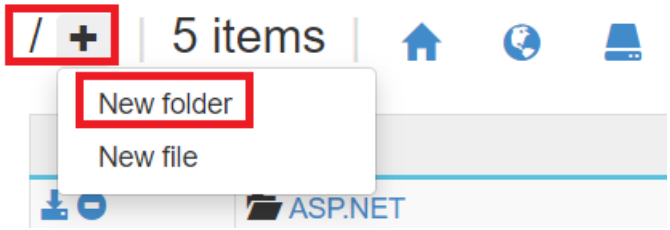
6. Click **Go** and provide Azure credentials.



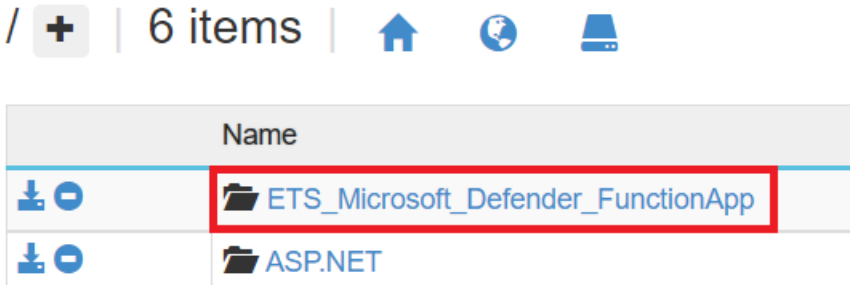
7. A new browser window opens. Select **PowerShell** from **Debug console** menu.



8. Click on + and click on **New folder** provide a folder name such as **ETS_Microsoft_Defender_FunctionApp**.

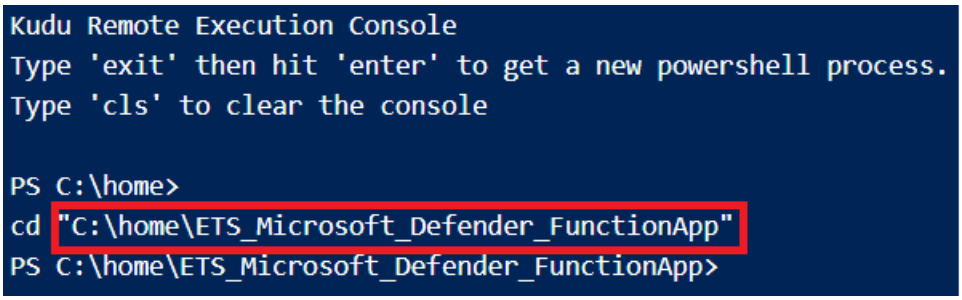


9. Click on folder which was created on last step

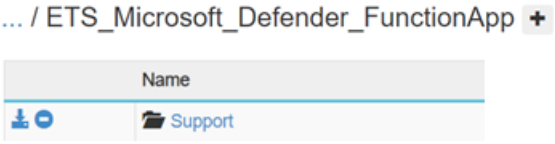


10. Copy the Base path as shown below, which will be used in the future step (step 21)

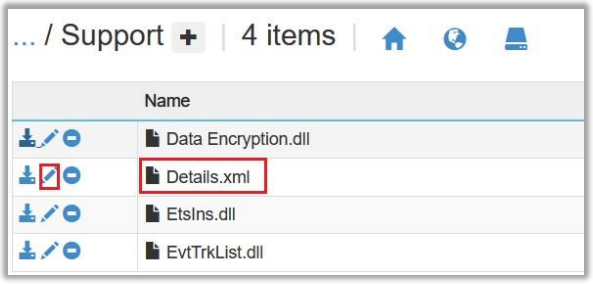
    (Example path: - **C:\home\ETS_Microsoft_Defender_FunctionApp)**



11. Drag and drop the **Support** folder (as received in the integration package) to create a folder. A new **Support** folder is added.



12. Navigate to the **Support/** folder and click on the **Edit** button for the **Details.xml** file.

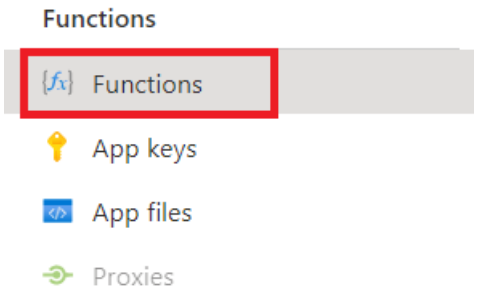


13. Here,
    - In line number 9, **mgr_name**, provide the EventTracker Manager hostname.
    - In line no. 10, **mgr_port**, enter the EventTracker Manager port number, e.g., 14505.
    - In line number 11, **mgr_ip**, provide the EventTracker Manager public IP address.
    - In line number 13, **org_name**, provide your organization name and org_name can only contain A-Z, a-z, 0-9, and Under score(_).

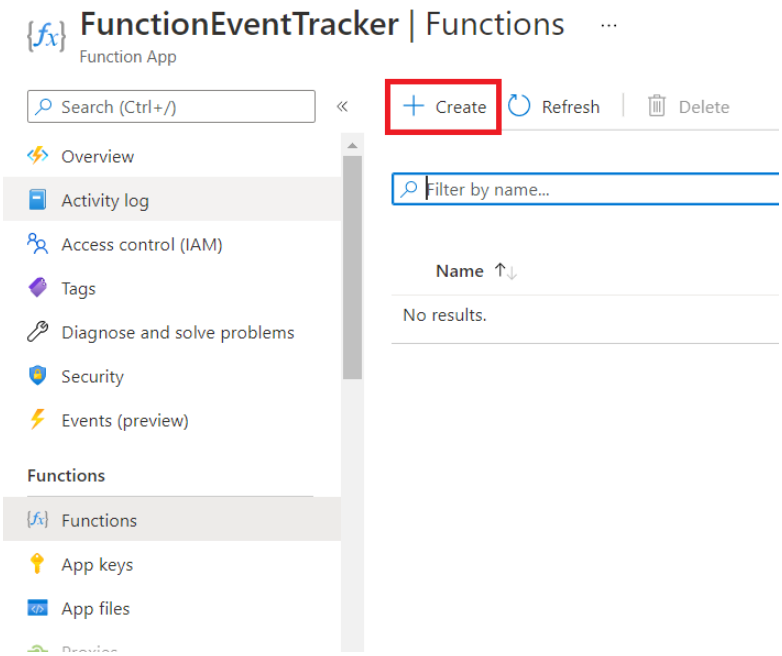
```
<Objs version="1.1.0.1"
    xmlns="http://schemas.microsoft.com/powershell/2004/04">
    <Obj RefId="0">
        <TN RefId="0">
            <T>System.Management.Automation.PSCustomObject</T>
            <T>System.Object</T>
        </TN>
        <MS>
            <S N="mgr_name">ET.CONTOSO.LOCAL</S> <!-- Replace with EventTracker manager name. e.g., ET.CONTOSO.LOCAL -->
            <S N="mgr_port">14505</S> <!-- Replace with EventTracker manager port. e.g., 14505 -->
            <S N="mgr_IP">198.17.23.198</S> <!-- Replace with EventTracker manager public IP address. e.g., 198.17.23.198 -->
            <S N="sys_ip">127.0.0.1</S>
            <S N="org_name">EventTracker</S> <!-- Replace with Organization Name. e.g., EventTracker -->
        </MS>

    </Obj>
</Objs>
```

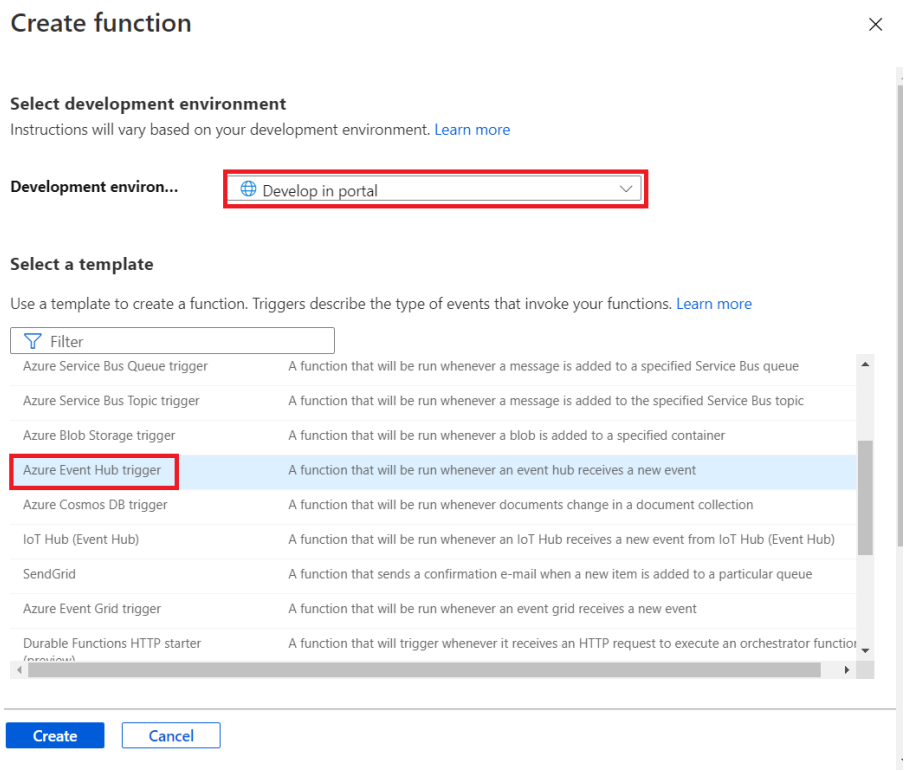
14. Click **Save**.
15. Come back to the Function APP tab (navigate to All services > Function App > FunctionEventTracker) to do further configuration and click **Functions** under Functions.



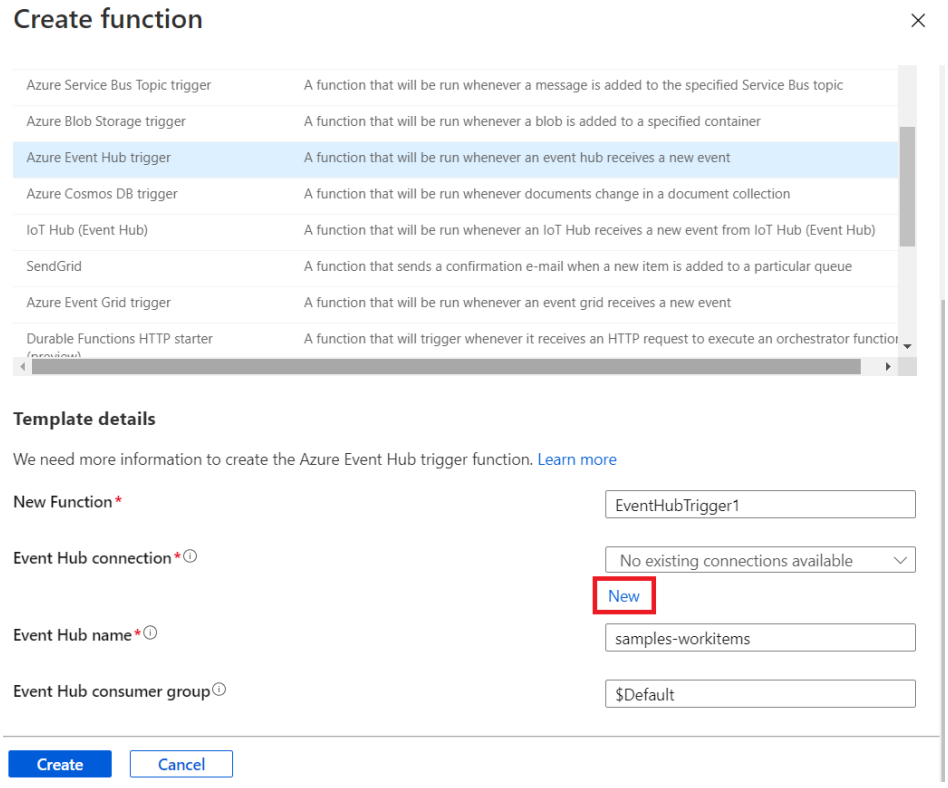
16. Click **Create.**



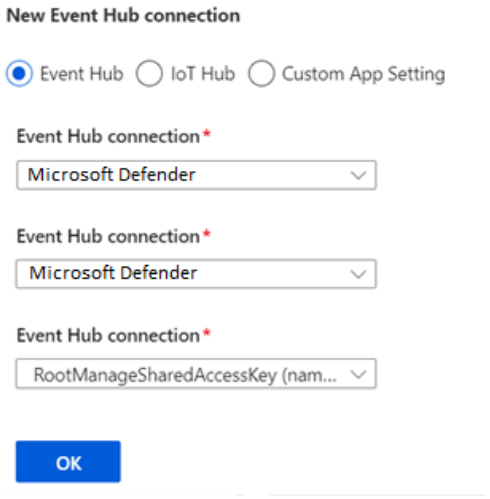
17. Select the **Develop in portal** option and click the **Azure Event Hub trigger.**



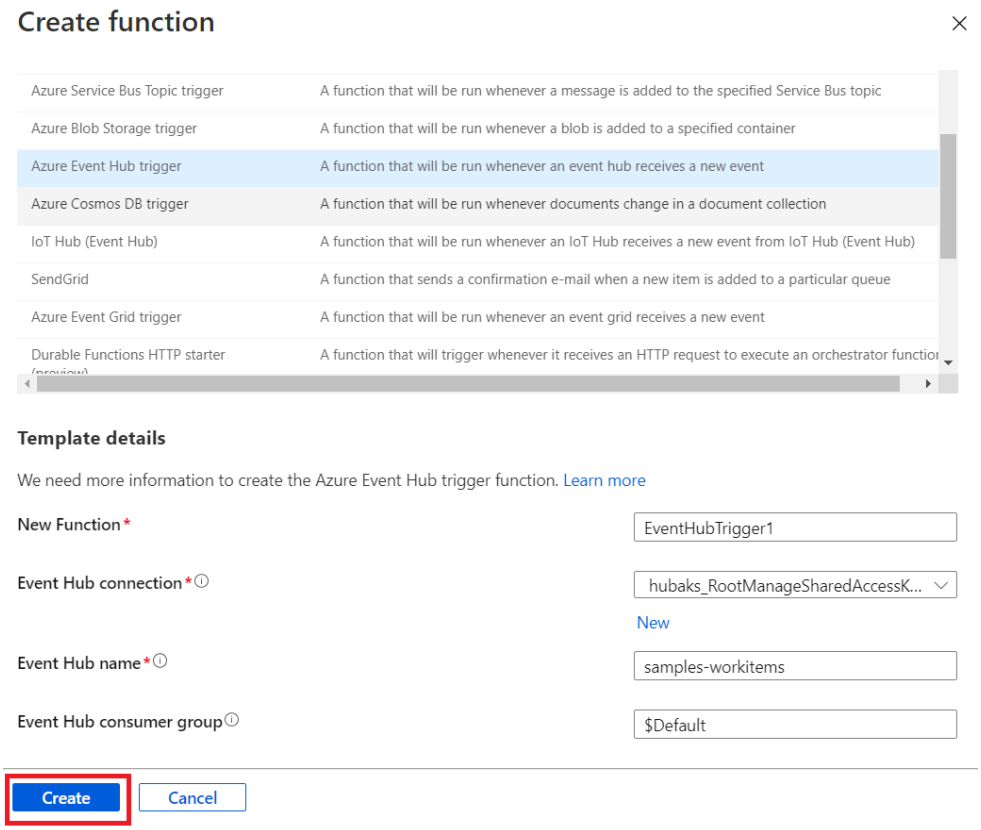
18. In the Event Hub connection, click **New**.



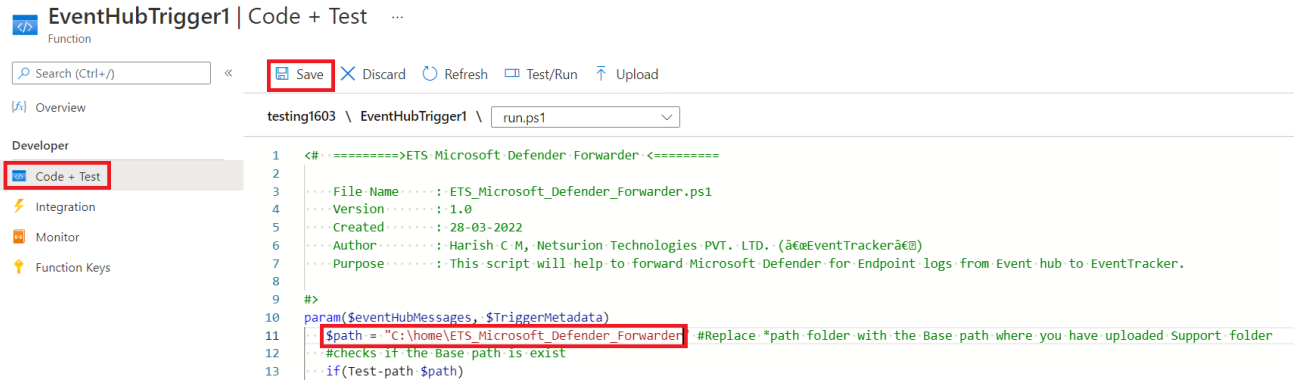
19. Let Azure populate the available Event Hub namespace and Event Hub. Select the desired ones and click **Ok.**



20. Click **Create**.



21. Click **Code+Test** and copy the contents of **ETS_Microsoft_Defender_forwarder.ps1** (as received in the integration package) and paste it into the given **run.ps1** window in the Azure function app portal and replace the path which was copied on **step 10** (Example path: - C:\home\ETS_Azure_FunctionApp) and click **Save.**

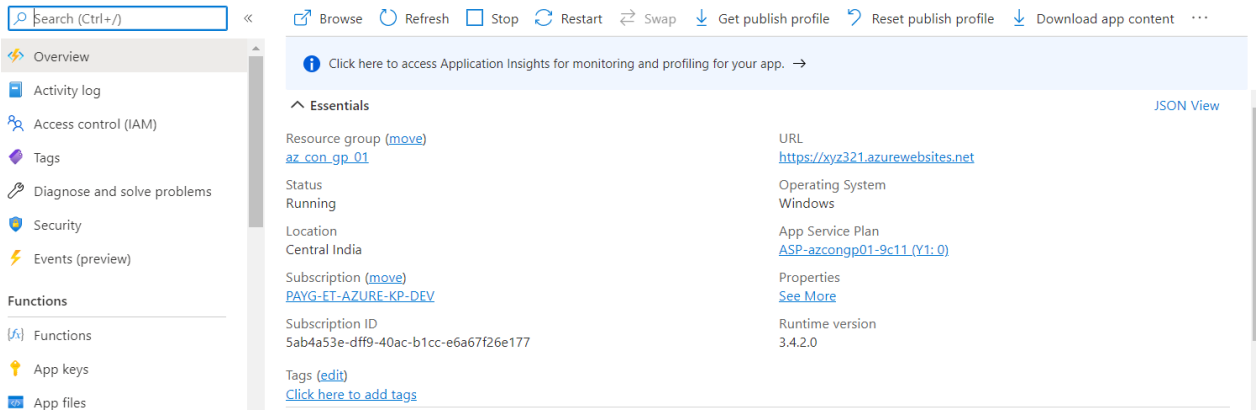


3.3 Cost Management

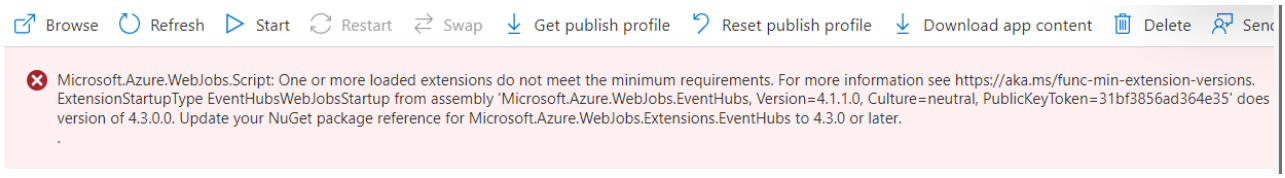
- The below-mentioned services are charged by Microsoft based on usage.
  - Function App
    Click here Function-App-price-tier to know more on pricing details.
  - Event Hub
    Click here Event-Hub-price-tier to know more on pricing details.

3.4 Verifying Function App

- Once the Function App is deployed, follow the below-mentioned steps to verify the deployment.
  1. Login to https://portal.azure.com/
  2. Search for Function App service.
  3. Click on created Function App.
  4. On successful deployment the screen would look as shown below.

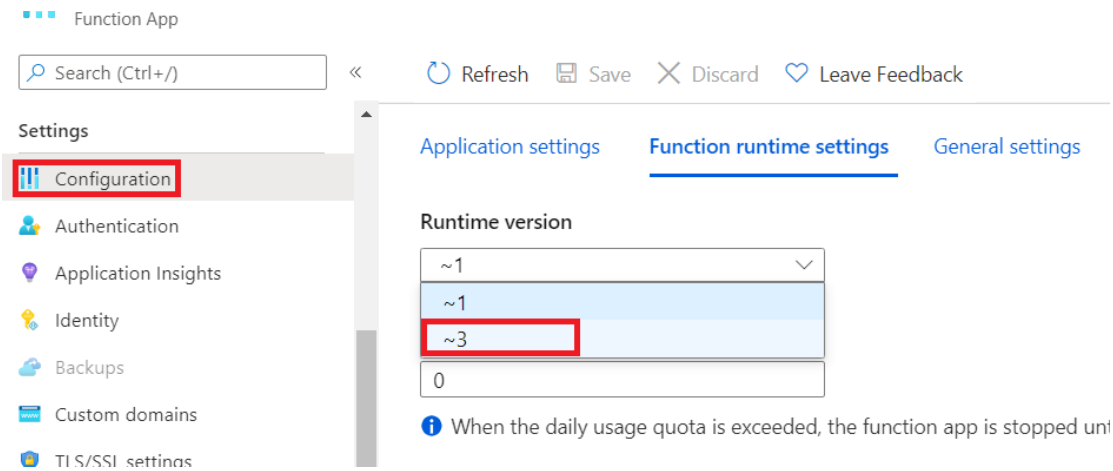


- Sometimes due to the mismatch of the extension package one could see below-mentioned error. Below are the steps provided to remediate the issue.



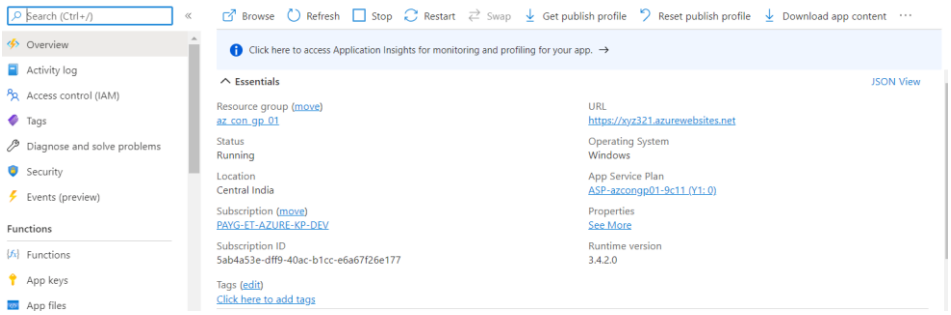
- To check the extension bundle.
  1. Click on **App files** under the Function section in the left pane of the function App home page
  2. Choose **host.json** from the dropdown
  3. Modify the version details in the JSON file to **"version": "[2.*, 3.0.0)"**
  4. Click **Save.**

- To check the Function App run time version.
  1. Click on **Configuration** under Settings in the left pane of the function App home page.
  2. Click on **Function runtime settings.**
  3. Choose Runtime version to **~3** from the dropdown.
  4. Click **Save.**



- Click on the **Overview** in the left pane to go to the **Function App** home page.

  Now the home page should not be showing the earlier error message as shown below.



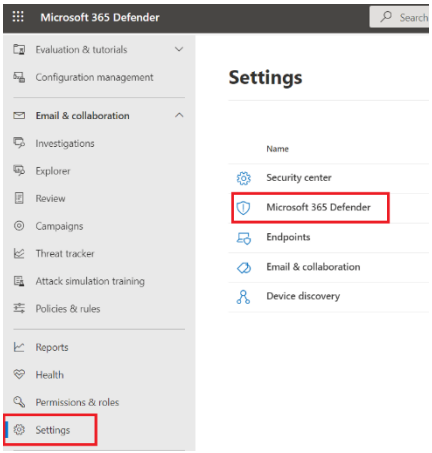
4. Configuring Microsoft Defender to Forward Logs to Event hub

Microsoft Defender for Endpoint can be integrated with EventTracker by streaming the logs to the Azure Event Hub, and from Azure Event Hub to EventTracker.

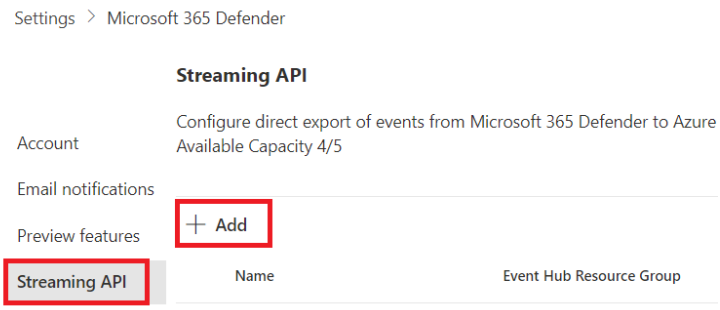
4.1 Configuring Microsoft Defender to stream events to Event Hub

Login to security.microsoft.com using the admin account and create an event hub namespace, if not created.

1. Click on **Settings** on the left panel and click **Microsoft 365 Defender.**

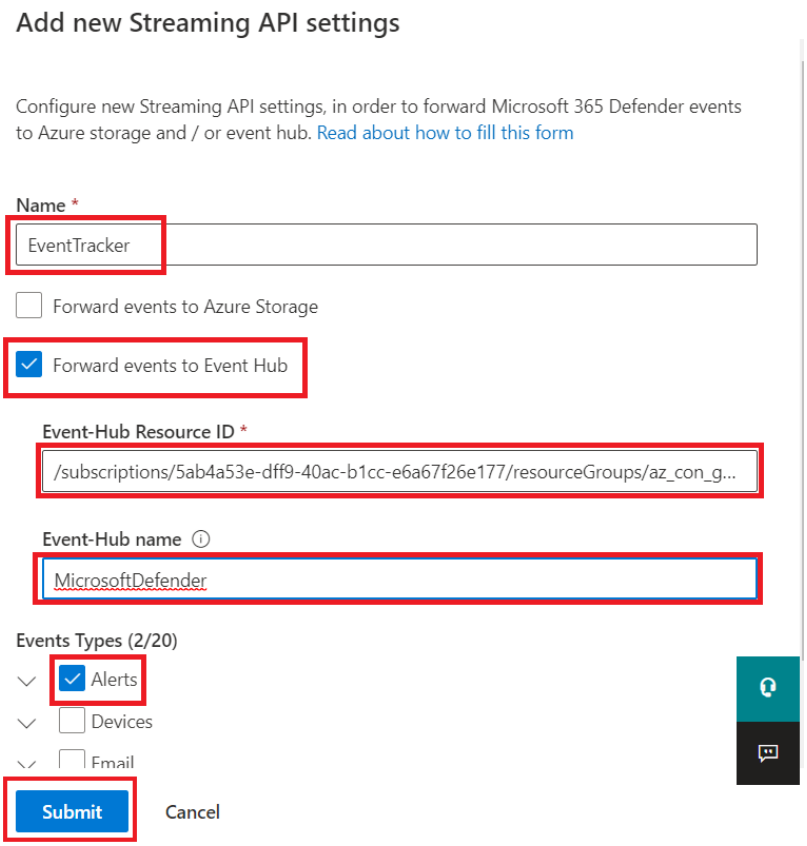


2. Click **Streaming API** and Click on **+Add.**

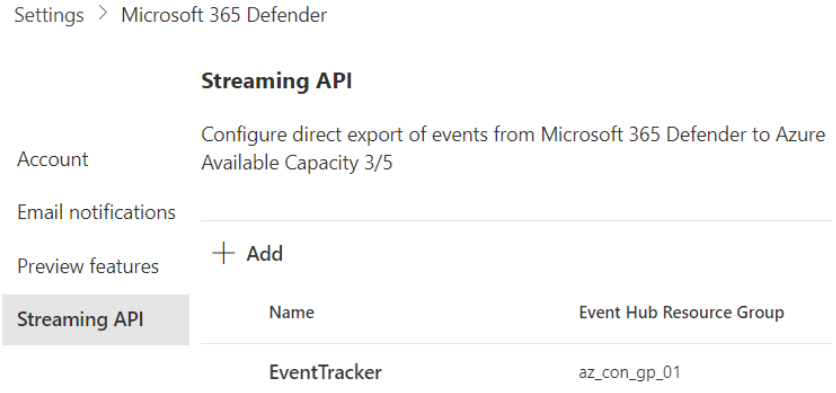


3. Configure Stream API.

- Fill Name like **EventTracker.**
- Check the box **Forward event to Azure Storage.**
- **Paste** Event-Hub Resource ID (Copied on 3.1 step 4).
- **Paste** Event-Hub name (Copied on 3.1 step 6).
- Check the box **Alerts** under **Events Types.**
- Click **Submit.**



4. After successful configuration the following screen display.



About Netsurion

Flexibility and security within the IT environment are two of the most important factors driving business today. Netsurion's managed cybersecurity platforms enable companies to deliver on both. Netsurion Managed Threat Protection combines our ISO-certified security operations center (SOC) with our own award-winning cybersecurity platform to better predict, prevent, detect, and respond to threats against your business. Netsurion Secure Edge Networking delivers our purpose-built edge networking platform with flexible managed services to multi-location businesses that need optimized network security, agility, resilience, and compliance for all branch locations. Whether you need technology with a guiding hand or a complete outsourcing solution, Netsurion has the model to help drive your business forward. To learn more visit netsurion.com or follow us on Twitter or LinkedIn.

Contact Us

Corporate Headquarters

Netsurion
Trade Centre South
100 W. Cypress Creek Rd
Suite 530
Fort Lauderdale, FL 33309

Contact Numbers

EventTracker Enterprise SOC: 877-333-1433 (Option 2)
EventTracker Enterprise for MSPs SOC: 877-333-1433 (Option 3)
EventTracker Essentials SOC: 877-333-1433 (Option 4)
EventTracker Software Support: 877-333-1433 (Option 5)
https://www.netsurion.com/eventtracker-support