Barracuda Web Application Firewall Integration with Microsoft Azure Sentinel

https://campus.barracuda.com/doc/96011804/

Microsoft Azure Sentinel is a scalable, cloud-native security information event management (SIEM) and security orchestration automated response (SOAR) solution that does the following:

- Provides intelligent security analytics at cloud scale for your enterprise.
- Collects log information from all devices and applications, both on-premises and in multiple clouds.
- Analyzes the data and detects threats quickly with artificial intelligence (AI).

For more information about Azure Sentinel, see Microsoft Documentation.

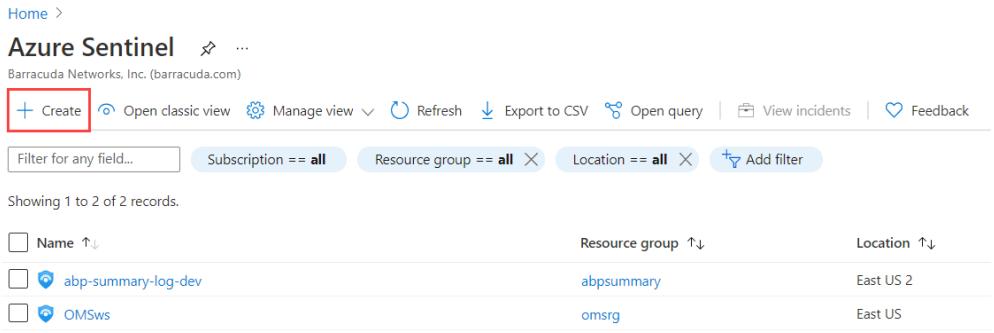
Barracuda Web Application Firewall (WAF) integration allows you to easily connect your Barracuda Networks logs with Azure Sentinel to view dashboards, create custom alerts, and improve investigation. This integration provides greater insight into the organization's network and improves your security operation capabilities.

Prerequisites

- Create a Log Analytics workspace using the Barracuda Web Application Firewall ARM template. See Creating a Workspace Using the ARM Template.

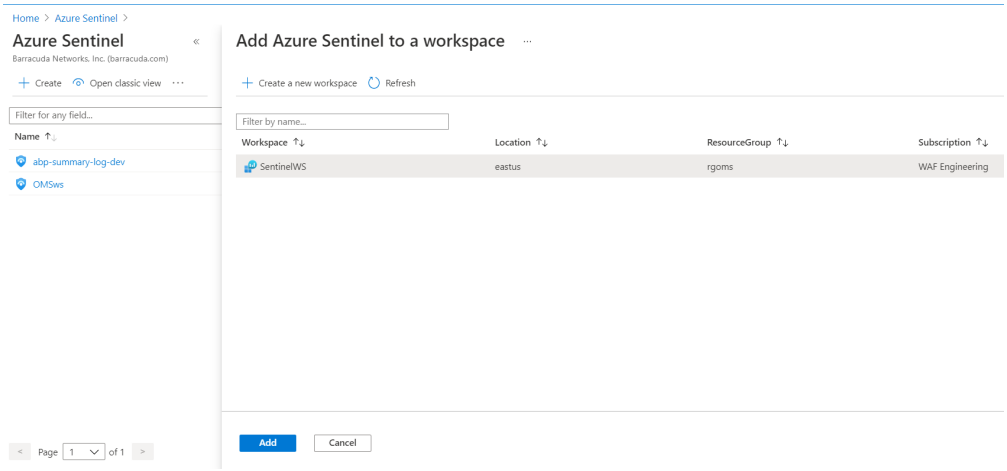
Integrate Barracuda Web Application Firewall with Azure Sentinel

1. Go to the **Azure Sentinel** page and click **Create**.

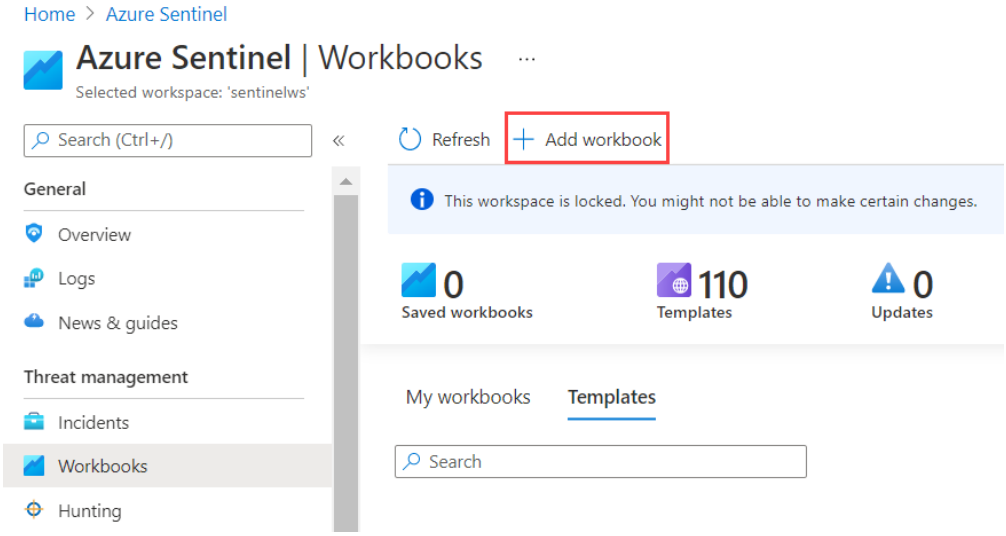


2. On the **Add Azure Sentinel to a workspace** page, select the workspace you created and click

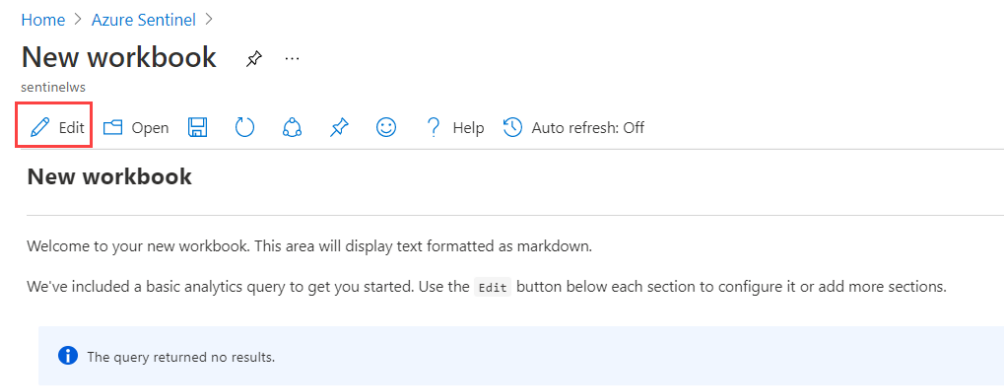
Add.



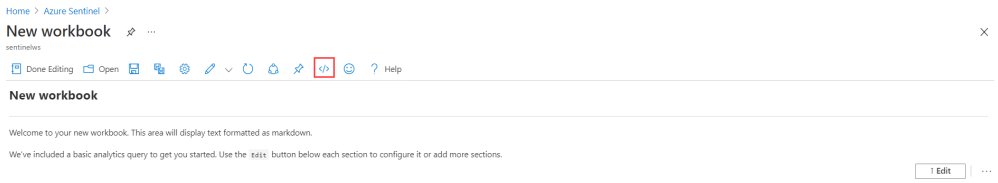
3. On the **Azure Sentinel** page, click on **Workbooks** under **Threat Management** and then click **Add workbook**.



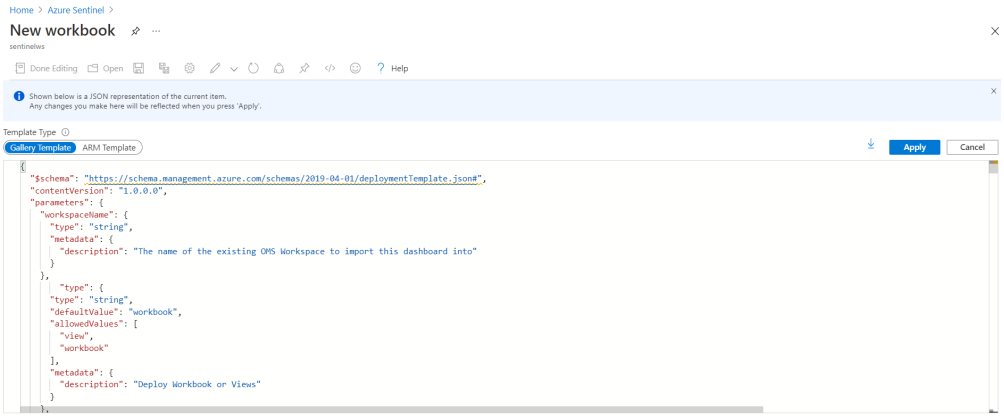
4. On the **New workbook** page, click **Edit**.



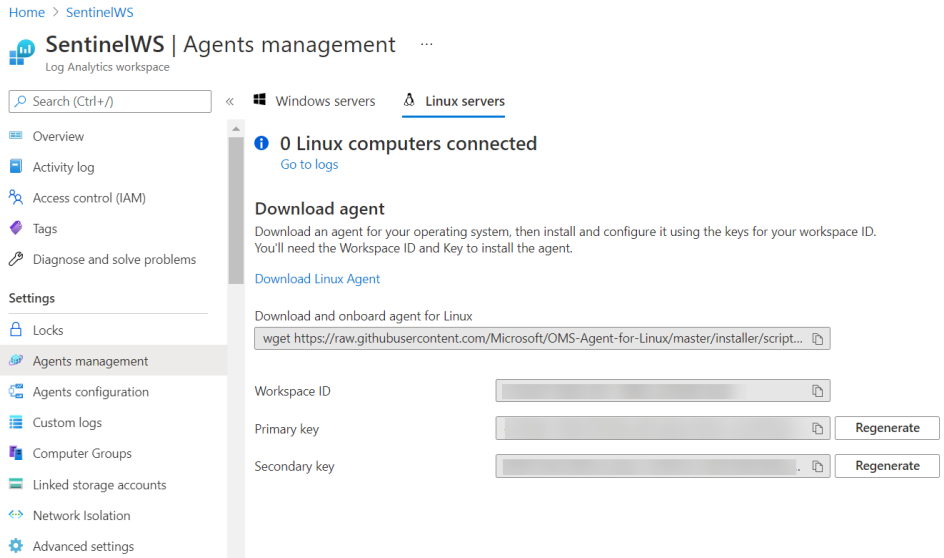
5. On the Edit page, click **Advanced Editor** (**</>**).



6. On the Editor page:
    1. Select the **Template Type** as **Gallery Template**.
    2. Clear the text area.
    3. Copy and paste the Barracuda ARM Template. The Sentinel workbook template is available on GitHub.
    4. Click **Apply** and click **Save**.



7. Go to the workspace you created and click **Agents Management** under **Settings**.
8. In the left panel, click **Linux servers** and note down the **Workspace ID**, **Primary key** and **Secondary key** details.



9. On the Barracuda Web Application Firewall web interface:
    1. Go to the **ADVANCED > Export Logs** page.
    2. In the **External Log Servers** section, click **Add Log Server** and add the Microsoft Azure Log Analytics server details. See Configure the Barracuda Web Application Firewall to Integrate with the Log Analytics Server and Export Logs.
10. You can now see the event logs and graphs displayed on Azure Sentinel.

Figures

1. Azure_Sentinel.png
2. Add_Azure_Sentinel.png
3. Add_Workbook.png
4. New_workbook.png
5. Edit_workbook.png
6. Template.png
7. Agents Management.png