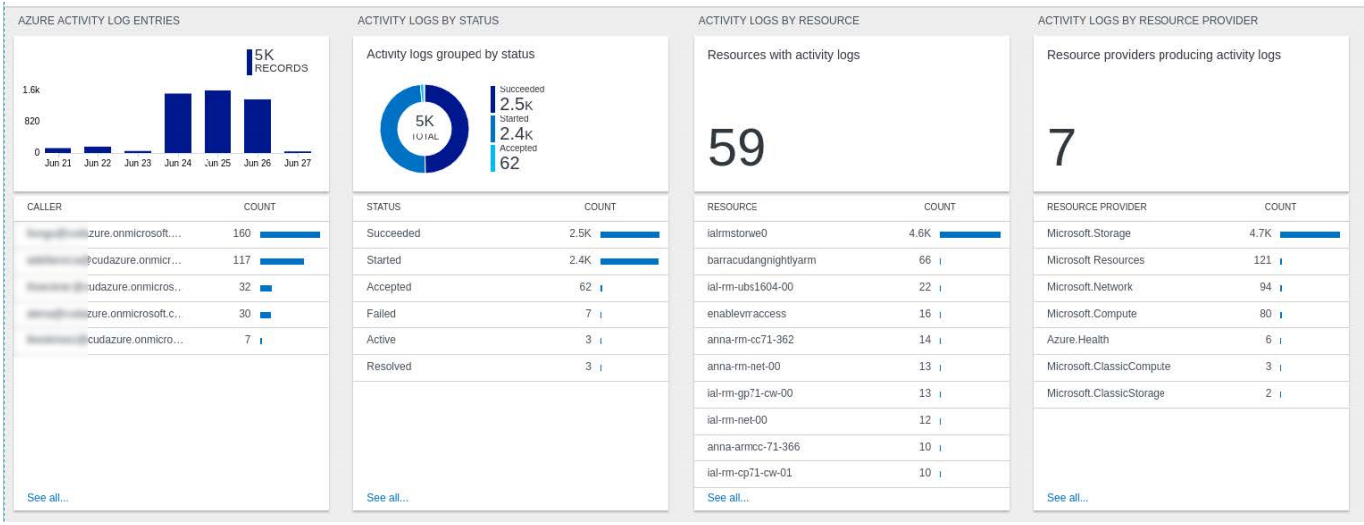
How to Configure Azure OMS Log Streaming

https://campus.barracuda.com/doc/73719773/

To stream log data and custom metrics from your firewall to Microsoft OMS in Azure, you must connect the firewall VM to your OMS workspace and configure syslog streaming on the firewall to send the syslog stream to Azure OMS. For streaming logs to Azure OMS using the CEF format, you must configure Microsoft OMS Security instead of Microsoft OMS as the streaming destination. On the Azure side, the virtual machines are connected to the OMS workspace. All selected log files are then streamed to Azure OMS, where they can be stored, analyzed, or processed.

To stream log data from the same source to multiple destinations, you must assign these multiple destinations to that single log source in the Logdata Stream configuration.



Custom VPN Metrics

- Client-to-site VPN tunnels
- SSL VPN clients
- Site-to-site VPN tunnels up
- Site-to-site VPN tunnels down

Custom System Metrics

- Load
- Used memory
- Protected IPs

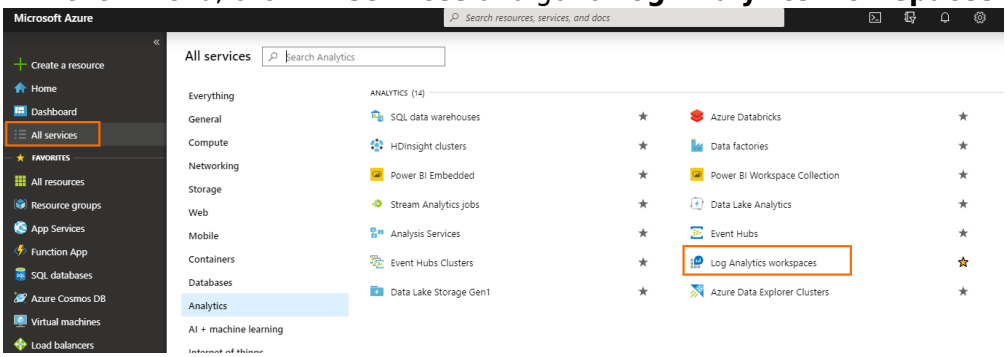
Custom Firewall Metrics

- Bytes in
- Bytes out
- Bytes total
- Packets in
- Packets out
- Packets total
- Connections dropped
- IPS Hits
- Forwarding Connections new
- Forwarding Connections total
- Connections new
- Connections total
- Connections blocked
- Connections failed

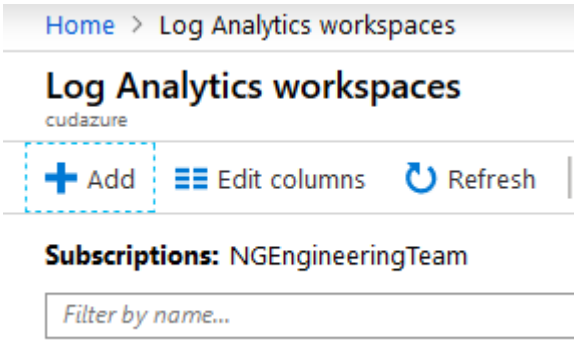
Configure OMS log streaming before managing your firewall via the Control Center.

Step 1. Create Log Analytics Workspace

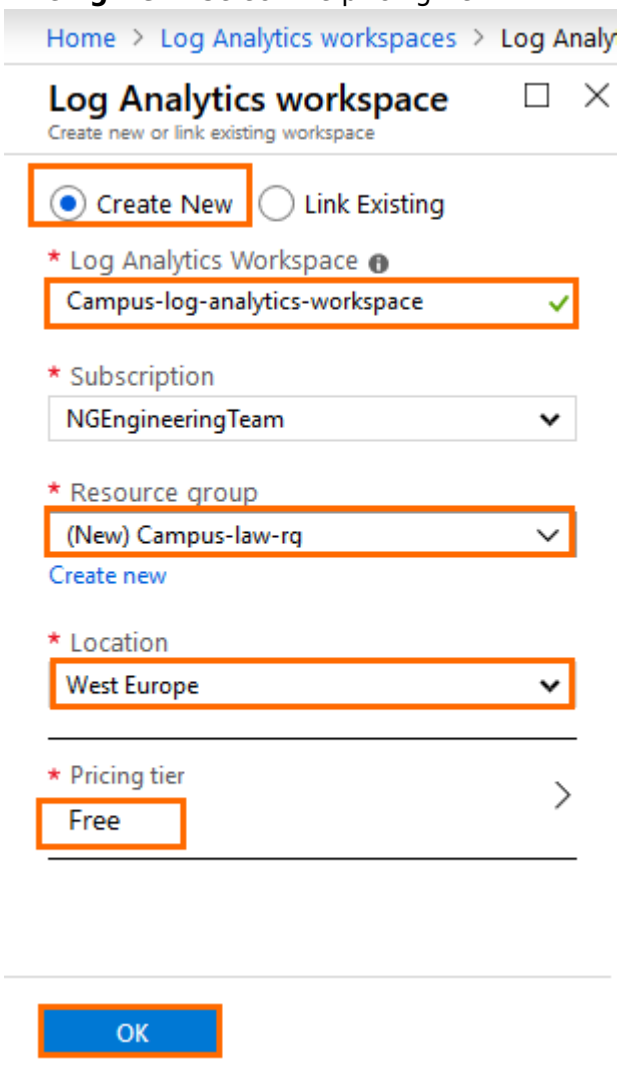
1. Log into the Azure portal: https://portal.azure.com
2. In the left menu, click **All services** and go to **Log Analytics workspaces**.



3. In the **Log Analytics workspaces** blade, click **Add**.

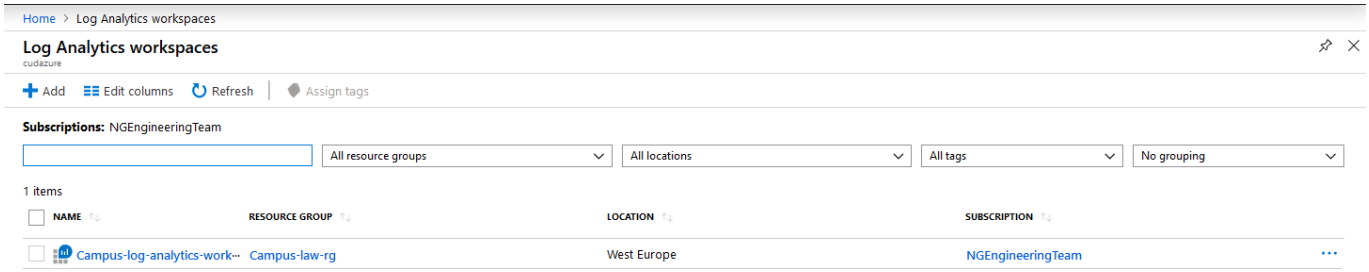


4. In the **Log Analytics workspaces** blade:
   - Select **Create New**.
   - **Log Analytics workspace** – Enter a name for the Log Analytics workspace.
   - **Resource Group** – Select an existing resource group, or create a new dedicated resource group for your workspace.
   - **Location** – Select the geographical location where the data for your workspace will be stored.
   - **Pricing tier** – Select the pricing tier.



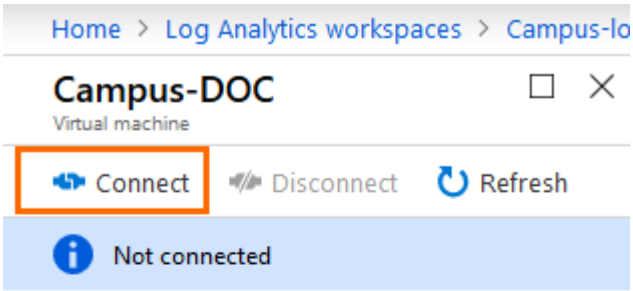
5. Click **OK**.

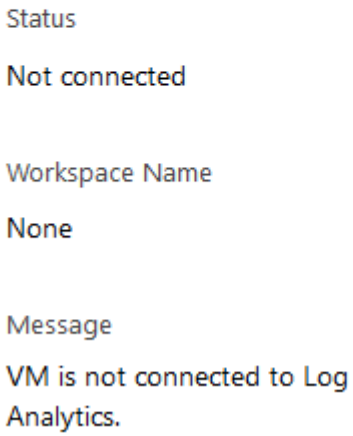
Click **Refresh** in the **Log Analytics workspaces** blade to display the new Log Analytics workspace.



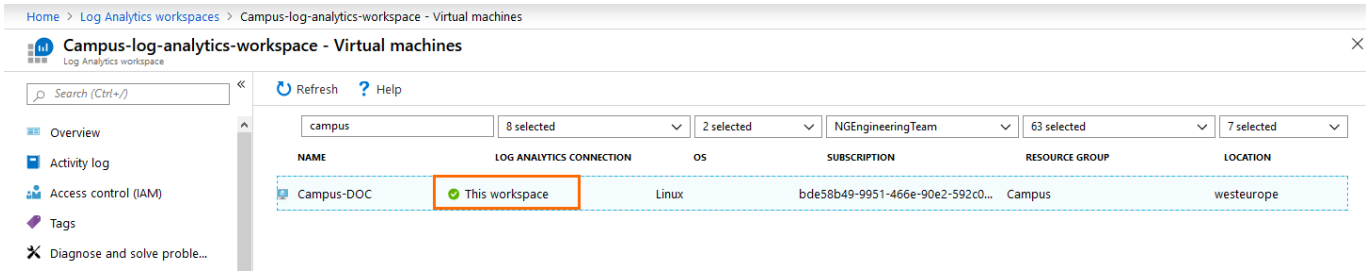
Step 2. Connect Virtual Machines to the Log Analytics Workspace

1. Log into the Azure portal: https://portal.azure.com.
2. In the left menu, click **All Services** and go to **Log Analytics workspaces**.
3. In the **Log Analytics workspaces** blade, click the workspace created in Step 1.
4. In the **Workspace Data Sources** section, click **Virtual machines**.
5. Enter the name of your CloudGen Firewall virtual machine that you want to connect to the workspace.
6. Click the entry of your virtual machine.
7. Click **Connect**.





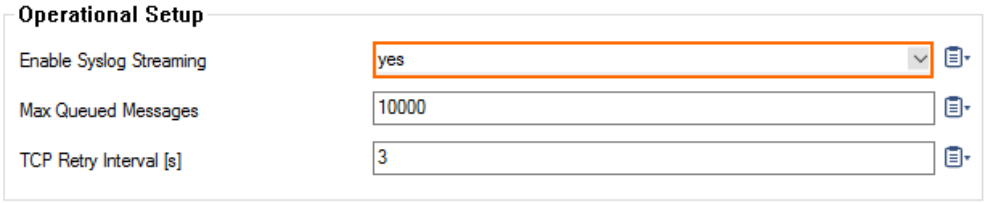
It may take a couple of minutes for the extension to be installed on the firewall.



Step 3. Enable the Syslog Streaming on the Firewall VM

Enable syslog streaming on the firewall.

1. Go to **CONFIGURATION >Configuration Tree> Box > Infrastructure Services > Syslog Streaming** .
2. Click **Lock**.
3. Set **Enable Syslog Streaming** to **yes**.



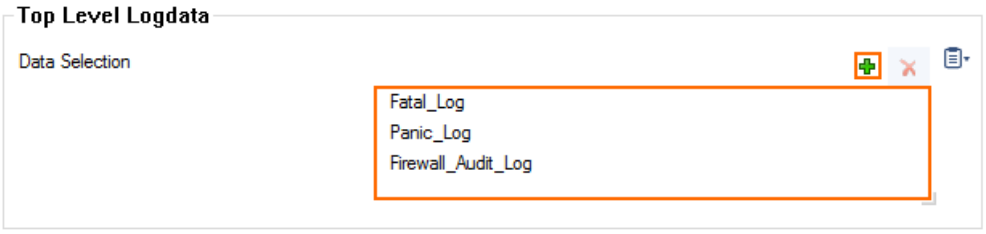
4. Click **Send Changes** and **Activate**.

Step 4. Configure Logdata Filters

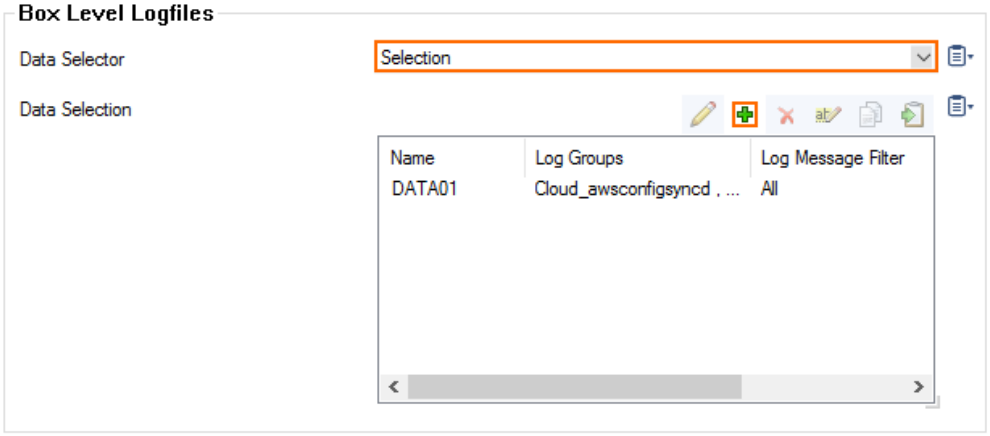
Define profiles specifying the log file types to be transferred / streamed. Log files are classified into top level, box level, and service level log data sources.

1. Go to **CONFIGURATION >Configuration Tree> Box > Infrastructure Services > Syslog Streaming** .
2. In the left menu, select **Logdata Filters** .
3. Click **Lock**.
4. In the **Filters** table, click **+** to add a new filter. The **Filters** window opens.
5. Enter a **Name**.
6. Click **OK**.
7. In the **Data Selection** table, add t he **Top Level Logdata** log files to be streamed. You can select:
    - **Fatal_log**

- **Firewall_Audit_Log** – The firewall audit log must be enabled and configured, and **Audit Delivery** must be set to **Syslog Proxy**. For more information, see How to Enable the Firewall Audit Log Service. Alternatively, the firewall audit log can also be streamed as a part of the firewall service logs.
- **Panic_log**



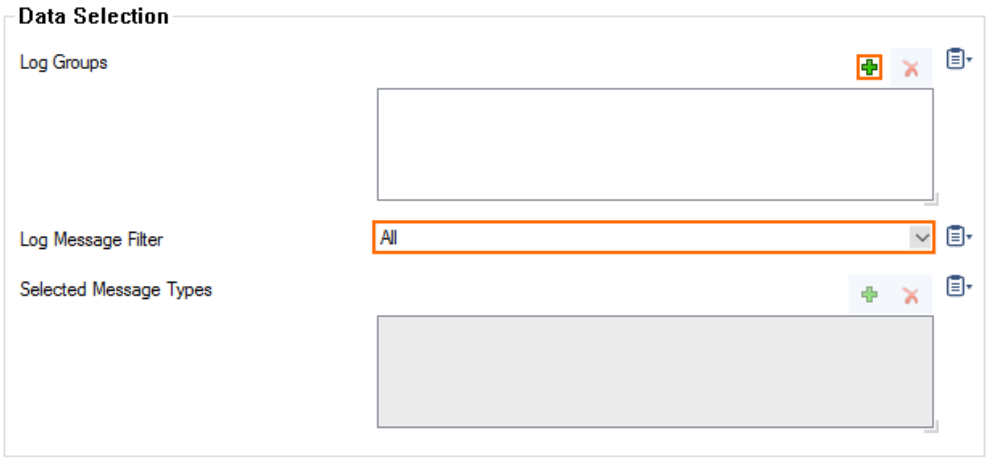
8. Configure the **Affected Box Logdata** filters:
   1. From the **Data Selector** list, select which files for this category are streamed:
      - **All** – All box level logs are streamed.
      - **None** – Box level logs are not streamed.
      - **Selection** – Only box level log files defined in the **Data Selection** list are streamed.



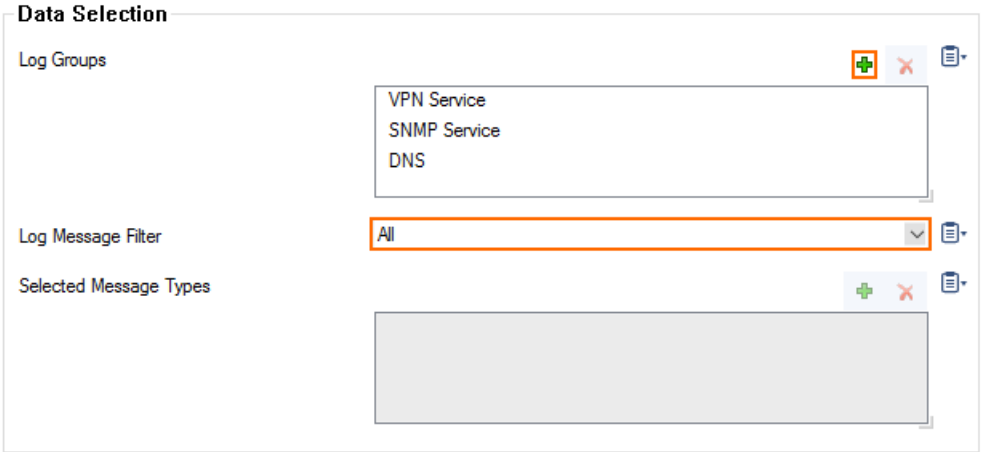
   2. (**Selection** only) Click **+** to add custom filters to the **Data Selection** table.
      1. In the **Log Groups** table, click **+**.
      2. (only for **Microsoft OMS** and standard syslog streaming) From **Log Groups**, select the box level log files, or select **Other** to enter a **user defined log group pattern** to stream log files matching this pattern.
      3. (optional for **Microsoft OMS Security** and logfile streaming using CEF) From **Log Groups**, select **Firewall-Activity-Only** and **Firewall-Threat-Only**.

      4. (optional) From the **Log Message Filter** list, select the message types from the log group that is streamed.

5. (**Selection** only) In the **Selected Messages Types** table, click **+** to add message types.
6. Click **OK**.



9. Configure the **Affected Service Logdata** filters:
   1. From the **Data Selector** list, select which files for this category are streamed:
      - **All** – All service logs are streamed.
      - **None** – Service level logs are not streamed.
      - **Selection** – Only service level log files defined in the **Data Selection** list are streamed.
   2. (**Selection** only) Click **+** to add custom filters to the **Data Selection** table.
      1. In the **Log Groups** table, click **+**.
      2. Select the box level log files, or select **Other** to enter a **user defined log group pattern** to stream log files matching this pattern.
      3. (optional) From the **Log Message Filter** list, select the message types from the log group that are streamed.
      4. (**Selection** only) In the **Selected Messages Types** table, click **+** to add message types.
      5. Click **OK**.

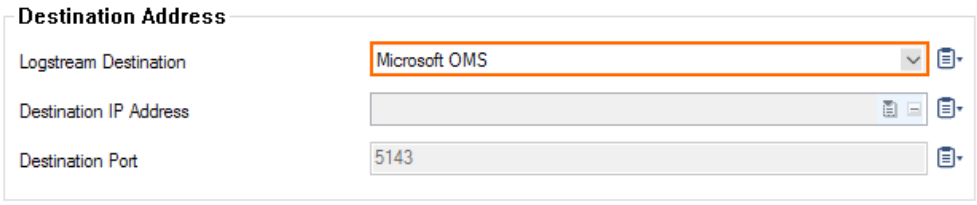


10. Click **Send Changes** and **Activate** .

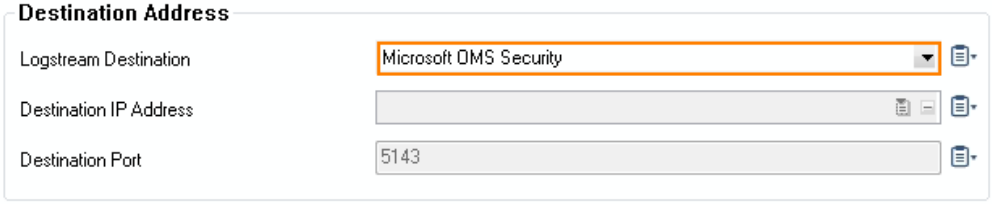
Step 5. Configure Microsoft OMS as the Logstream Destination

Configure the firewall to send the syslog stream to OMS.

1. Go to **CONFIGURATION >Configuration Tree> Box > Infrastructure Services > Syslog Streaming** .
2. In the left menu, select **Logstream Destinations** .
3. Click **Lock**.
4. In the **Destinations** table, click **+** to add a new filter. The **Destinations** window opens.
5. Enter a **Name**.
6. Click **OK**.
7. (only for **Microsoft OMS** and standard syslog streaming) From the **Logstream Destination** list, select **Microsoft OMS**.



8. (optional for **Microsoft OMS Security** and logfile streaming using CEF) From the **Logstream Destination** list, select **Microsoft OMS Security**.



9. Click **OK**.
10. Click **Send Changes** and **Activate**.

Step 6. Configure the Logdata Streams to Microsoft OMS

Combine the logdata filters and logstream destination to a logdata stream.

1. Go to **CONFIGURATION >Configuration Tree> Box > Infrastructure Services > Syslog Streaming** .
2. In the left menu, select **Logdata Streams** .
3. Click **Lock**.
4. In the **Streams** table, click **+** to add a new syslog stream. The **Streams** window opens.
5. Enter a **Name**.
6. Click **OK**.
7. Set **Active Stream** to **yes**.

8. In the **Log Destinations** table, click **+** and select the logstream destination configured in Step 5.
9. In the **Log Filters** table, click **+** and select the logdata filter configured in Step 4. Choose either OMS or OMS Security as your log destination.

10. Click **OK**.
11. Click **Send Changes** and **Activate**.

All logs covered by the logdata filter are now streamed to Azure OMS. It might take some time for logs to be displayed in the OMS portal.

Figures

1. oms.png
2. all_services_log.png
3. add_log_a_w.png
4. create_law2.png
5. display_law.png
6. connect_vm.png
7. law_cgf_status.png
8. oms_08.png
9. oms_09.png
10. oms_10.png
11. conf_oms_sec.png
12. oms_11.png
13. oms_12.png
14. oms_13.png
15. select_dest_oms_security_via_cef.png
16. oms_14.png