AQUILA - Azure Logs Integration

The **Azure Logs integration** enables you to collect logs from specific Azure services such as:

- **Microsoft Entra ID** (Sign-in, Audit, Identity Protection, Provisioning logs)
- **Azure Spring Apps**
- **Azure Firewall**
- **Microsoft Graph Activity**
- **Activity and Platform logs**
- Additional supported Azure services

Example Use Cases

- **Brute force sign-in detection**: Collect **Microsoft Entra ID sign-in logs** and configure an alert in the Observability Logs app to notify you if failed sign-in attempts exceed a defined threshold.
- **Capacity planning**: Collect **Azure Activity logs** to track when virtual machines fail to start due to quota limits, helping plan resource scaling.

Data Streams

The Azure Logs integration collects **log data streams** from the following sources:

- Activity Logs
- Platform Logs
- Microsoft Entra ID Logs (Sign-in, Audit, Identity Protection, Provisioning)
- Microsoft Graph Activity Logs
- Azure Spring Apps Logs

Logs provide a complete record of events that occur in your Azure environment, allowing you to detect threats, troubleshoot issues, and plan capacity.

Azure Setup Prerequisites

To successfully forward Azure logs, you will need:

1. **Diagnostic Settings**
   - Configure diagnostic settings in Azure to export metrics and logs from source services (e.g., Entra ID, Activity Logs).
   - Logs must be sent to a supported destination for analysis and storage.
2. **Event Hubs**

- One or more **Event Hubs** to temporarily store and stream logs exported by Azure services.
- Log Collector will use Event Hubs as the ingestion point.

3. **Storage Account Container**
   - A **Storage Account container** to store checkpoint information about logs consumed by Log Collector.
   - This ensures logs are ingested reliably without duplication or loss.

Step 1: Create an Event Hub for Microsoft Entra ID Logs

1. **Go to Azure Portal > Event Hubs > Create Namespace**
   - Select **Resource Group** or create a new one.
   - Choose a **Region** and a **Pricing Tier (Standard or Premium)**.
   - Click **Review + Create** → **Create**.
2. **Create an Event Hub** inside the namespace
   - Navigate to the **Namespace** → Click **+ Event Hub**.
   - Set **Name**: entra-id-logs (Example)
   - Set **Partitions**: At least **2** (for redundancy).
   - Click **Create**.
3. **Create a Consumer Group (Optional)**
   - Go to **Event Hub > Consumer Groups**.
   - Add a new group (e.g., aquila-agent-group).
4. **Generate Connection String**
   - Navigate to **Event Hubs Namespace > Shared Access Policies**.
   - Click **+ Add Policy**.
   - Set Name: AquilaAgentPolicy.
   - Select **"Listen"** permission.
   - Copy **Primary Connection String** (used in the next steps).

Step 2: Enable Diagnostic Settings for Microsoft Entra ID

1. **Go to Azure Portal > Microsoft Entra ID**.
2. Navigate to **Monitoring > Diagnostic Settings**.
3. Click **+ Add Diagnostic Setting** and configure:
   - **Name**: entra-logs-to-aquila
   - **Log Categories**:
     -Sign-in logs
     -Audit logs
     -Identity Protection logs
     -Provisioning logs
   - **Destination**: Select **Event Hubs**.
   - **Choose the Event Hub Namespace** created earlier.
   - **Select the Event Hub (entra-id-logs)**.
   - Click **Save**.

Step 3: Configure Azure Storage for Checkpointing

1. **Create a Storage Account**
   - Navigate to **Azure Portal > Storage Accounts > Create**.
   - Select **Resource Group** (same as Event Hub).
   - Set **Storage Account Name**:
   - **Disable Hierarchical Namespace** and **Enable TLS 1.2**.
   - Click **Create**.
2. **Create a Blob Container**
   - Open the **Storage Account > Containers**.
   - Click **+ Container**.
   - Set **Name**:
   - Set **Public Access Level**: Private.
3. **Copy Storage Account Keys**
   - Go to **Storage Account > Access Keys**.
   - Copy **Storage Account Name & Key** for integration configuration.

> **Please saved and provide this values to AQUILA Support Team.**

- **Event Hub Name**:
- **Consumer Group**:
- **Event Hub Connection String**:
- **Storage Account Name**:
- **Storage Account Key**:
- **Storage Container Name**:
- **Resource Manager Endpoint(optional)**:

---

*If you need further assistance, kindly contact **support@cytechint.com** for prompt assistance and guidance.*

Revision #3
Created 5 February 2025 06:30:43 by Richmond Abella
Updated 10 November 2025 09:13:52 by Richmond Abella