

# Azure Integration - Microsoft Entra ID Logs

## 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., `elastic-agent-group`).
  4. **Generate Connection String**
    - Navigate to **Event Hubs Namespace > Shared Access Policies**.
    - Click **+ Add Policy**.
    - Set Name: `ElasticAgentPolicy`.
    - 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-elastic`
  - **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:** `elasticstorageentra`.
- **Disable Hierarchical Namespace** and **Enable TLS 1.2**.
- Click **Create**.

### 2. Create a Blob Container

- Open the **Storage Account > Containers**.
- Click **+ Container**.
- Set **Name:** `entra-checkpoints`.
- Set **Public Access Level:** Private.

### 3. Copy Storage Account Keys

- Go to **Storage Account > Access Keys**.
  - Copy **Storage Account Name & Key** for Elastic configuration.
- 

## Step 4: Configure Elastic Agent in Kibana

### 1. Go to Kibana > Fleet > Integrations.

### 2. Click **Azure Logs > Add Integration**.

### 3. Configure the integration:

- **Event Hub Name:** `entra-id-logs`
- **Consumer Group:** `$Default` (or `elastic-agent-group`)
- **Event Hub Connection String:** *(Paste the copied string)*
- **Storage Account Name:** `elasticstorageentra`
- **Storage Account Key:** *(Paste the copied key)*
- **Storage Container Name:** `entra-checkpoints`
- **Resource Manager Endpoint:** Default ( `https://management.azure.com/` )

### 4. Click **Save & Deploy**.

---

## Step 5: Verify Logs in Kibana

### 1. Go to Kibana > Discover.

### 2. Select the index pattern:

`logs-azure.entra_id-*`

### 3. Apply filters to view:

- Failed Sign-ins
  - Unauthorized Access Attempts
  - Privileged Account Changes
4. Create **Alerts & Dashboards** to track suspicious activity.
- 

# Summary

**Microsoft Entra ID Logs → Azure Event Hub → Elastic → Kibana**

**Create Event Hub & Consumer Group**

**Enable Diagnostic Settings for Microsoft Entra ID**

**Set Up Azure Storage for Checkpoints**

**Configure Elastic Agent in Kibana**

**Monitor Logs & Create Alerts in Kibana**

---

Revision #1

Created 5 February 2025 06:30:43 by Richmond Abella

Updated 5 February 2025 08:01:23 by Richmond Abella