Configure Metric Alert

Metric alert watches **numbers** (metrics), like CPU usage, and sends alert if value crosses limit.

Example:

Alert if **CPU usage is more than 70% for 5 minutes**.

Step-by-step:

1. **Go to Azure Portal**
   https://portal.azure.com

2. **Search for "Virtual Machines"**
   Pick a VM that you want to monitor.

3. In the left menu, click on **"Alerts" > "+ New Alert Rule"**

4. Under **Scope**
   Confirm the correct VM is selected.

5. Under **Condition**, click **"Add condition"**

6. Select **"Percentage CPU"** as the signal.

7. Under **Configure signal logic**:

   - Condition: **Greater than**
   - Threshold value: **70**
   - Aggregation type: **Average**
   - Period: **5 minutes**

8. Click **Done**

9. Under **Action Group**, click **"Create action group"**

   - Name: `CPUAlertActionGroup`

- Email or SMS: Enter your email to get the alert
- Save it

10. Under **Alert rule details**
    - Alert rule name: `HighCPUAlert`
    - Severity: **3 (Informational)** or **2 (Warning)**
11. Click **Create alert rule**

✅ Testing Metric Alert:

1. On your VM, run a script or workload that increases CPU.
    - Use a tool like CPU stress in Linux or open many browser tabs in Windows.
2. Wait 5-10 minutes.
3. Check your email — you'll get an alert when CPU goes above 70%.

2️⃣ Configure Activity Log Alert

Activity log alert is triggered when someone **makes changes in Azure**, like deleting a VM, updating a resource, or disabling a security setting.

Example:

Alert when someone **deletes a Resource Group**.

Step-by-step:

1. Go to Azure Portal
   Search for **"Monitor"** and click it.
2. Go to **"Alerts" > "+ New Alert Rule"**

3. Under **Scope**:
    - Click **“Select scope”**, choose the **subscription** you want to monitor.
4. Under **Condition**, click **“Add condition”**
5. Choose **“Delete Resource Group (Administrative)”**
    - If not listed, search for **“Delete”**, then choose the right activity.
6. Click **Done**
7. Under **Action Group**:
    - Use an existing action group or create a new one (like above).
8. Alert rule name: `DeleteRGAlert`
   Severity: **2 (Warning)**
9. Click **Create alert rule**

✅ Testing Activity Log Alert:

1. Go to Azure → create a test Resource Group (e.g., `RG-TestAlert`)
2. Delete that Resource Group.
3. Wait a few minutes, then check your email — you’ll get an alert.

3️⃣ Configure Log Search Alert

Log search alert is used with **Log Analytics**. It watches for logs that match a **query**.

Example:

Alert when someone gets **“Failed RDP login”** on a VM.

Step-by-step:

1. Make sure your VM is sending logs to a **Log Analytics Workspace**

   If not:

   - Go to the VM → Monitoring → **Diagnostic settings**
   - Click **“Add diagnostic setting”**
   - Choose **Send to Log Analytics**
   - Select or create a **workspace**

2. Go to Azure Portal → Search for **“Log Analytics workspaces”**
3. Open your workspace → Click **Logs**
4. Use this query for failed logins:
   SecurityEvent

   | where EventID == 4625

   | where AccountType == "User"

1. Click **“New Alert Rule”** on top
2. Set condition:
   - When **results > 0** in last **5 minutes**
3. Add action group (email, etc.)
4. Alert name: `FailedRDPLoginAlert`
   Severity: **2 (Warning)**
5. Click **Create**

✅ Testing Log Search Alert:

1. Try to RDP into your VM with wrong password (just once or twice)
2. Wait 5-10 minutes
3. You'll receive an alert for failed login attempt.

🔐 As an Azure Cloud Security Engineer, why are these alerts important?

Alert Type	What It Protects You From
Metric Alert	System performance issues, possible DoS attacks
Activity Log Alert	Unauthorized or risky changes in environment

Log Search Alert	Security threats like brute-force, malware behavior