**Automated Infra Healing System: Design and Workflow**

**Objective:**

To automate the process of healing servers based on connectivity issues detected from SCOM alerts fetched from Kibana.

The process involves:

* Fetching alerts from Kibana every 5 minutes.
* Storing alerts in a tracker to identify recurring issues within the last 24 hours.
* Triggering automatic healing actions such as escalation emails or server reboots based on the number of alerts in the last 24 hours.

**1. Fetching Alerts from Kibana:**

Every 5 minutes, the system fetches alerts from Kibana related to the event "**Failed to Connect to Computer**" from SCOM.

**Kibana Query Details:**

* **Alert Name:** "**Failed to Connect to Computer**"
* **Source:** SCOM
* **Time Frame:** The query is set to fetch alerts that have occurred within the last 5 min.

The query checks for the specific event "Failed to Connect to Computer" and retrieves information on the hostname or server name associated with the alert. This step ensures that only relevant and **active critical alerts** are fetched.

**2. Storing Alerts in an Alert Tracker:**

Once alerts are fetched, the system tracks each alert with its timestamp in an alert\_tracker file, a JSON-based storage solution. This allows for persistent tracking of each server's alerts over time.

**Alert Tracker Logic:**

* The tracker stores alerts for each server, including the timestamp of when each alert occurred.
* The system checks if a server has had more than 2 alerts in the last 24 hours. If yes, it escalates the issue via email.

The tracker ensures that only servers with multiple alerts are considered for escalation or automated healing.

**3. Escalation Process:**

If the same server has received more than **2 alerts** within the last 24 hours, an **escalation email** is sent to the EMS team, informing them of the recurring issue.

**Escalation Email Details:**

* **Subject:** "Escalation: Multiple Connectivity Alerts for [Server\_Name]"
* **Body:** "The server [Server\_Name] has triggered multiple connectivity alerts within the last 24 hours and requires manual intervention Auto Healing Failed."

The email uses the **SMTP** server to send the message to the EMS team, ensuring that critical issues are escalated for manual resolution.

**4. Automated Healing Based on Connectivity Checks:**

If the server has **2 or fewer alerts** in the last 24 hours, the system performs a set of automated checks to determine if the server is still reachable. These checks are:

* **Ping Check**: The system pings the server to check its network connectivity.
* **RDP (Remote Desktop Protocol) Check**: The system checks if RDP (for Windows servers) is accessible.
* **SSH Check**: The system checks if SSH (for Linux servers) is accessible.

**Healing Conditions:**

* **If both RDP and SSH fail**:
  + The system considers the server unreachable and performs a **reboot action** through **SCVMM (System Center Virtual Machine Manager)** using PowerShell commands.
* **If either RDP, or SSH succeeds**:
  + No action is taken; the server is considered online.

**5. Rebooting the Server via SCVMM:**

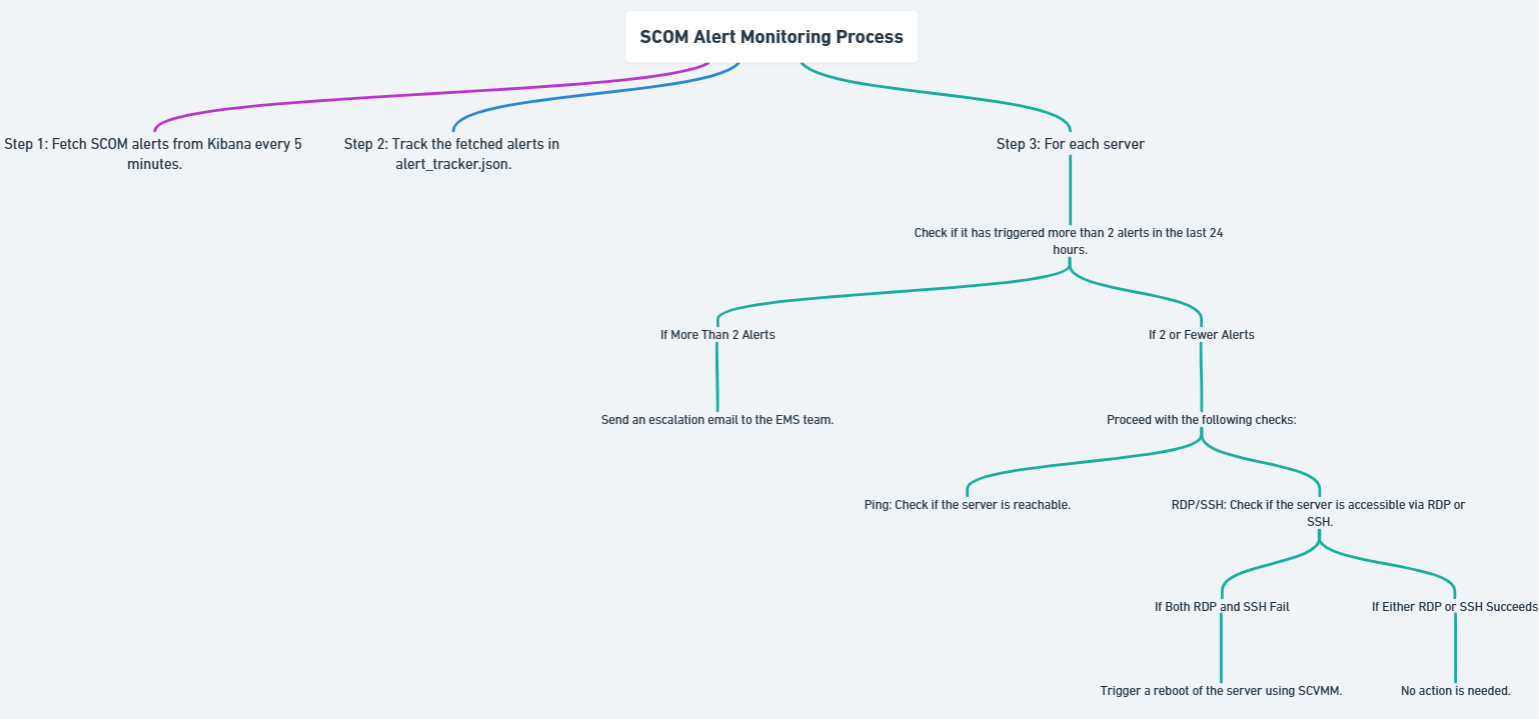
If the server is unreachable (both RDP&SSH fail), the system proceeds with rebooting the server using SCVMM.

**SCVMM Reboot Process:**

* The system uses a PowerShell command to trigger a reboot on the target server:
* The system checks if the reboot command is successful, and logs any errors if the reboot fails.

**6. Workflow Summary:**

* **Step 1:** Fetch SCOM alerts from Kibana every 5 minutes.
* **Step 2:** Track the fetched alerts in alert\_tracker.json.
* **Step 3:** For each server, check if it has triggered more than 2 alerts in the last 24 hours.
  + **If More Than 2 Alerts:** Send an **escalation email** to the EMS team.
  + **If 2 or Fewer Alerts:** Proceed with the following checks:
    - **Ping**: Check if the server is reachable.
    - **RDP/SSH**: Check if the server is accessible via RDP or SSH.
  + **If Both RDP and SSH Fail:** Trigger a **reboot** of the server using SCVMM.
  + **If Either RDP or SSH Succeeds:** No action is needed.



**7. Technology Stack:**

* **Kibana**: For fetching SCOM alerts.
* **Elasticsearch**: To query the alerts from the Kibana index.
* **Ping3**: For performing the ping check.
* **Python**: For scripting the entire automation process.
* **SCVMM**: For managing and rebooting the virtual machines.
* **SMTP Server**: For sending the escalation emails to the EMS team.

**Conclusion:**

This system automates the healing process for servers that are facing connectivity issues, either by escalating the issue to the EMS team or by rebooting the server. It reduces manual intervention and improves the response time to server outages, ensuring that critical systems are addressed promptly.