Activity Log Alert (Portal)

(LAB-300-01A-02)

Part A: Create Action Group

An action group is a collection of notification preferences defined by the owner of an Azure subscription. Azure Monitor and Service Health alerts use action groups to notify users that an alert has been triggered.

1. From Azure portal, go to **Monitor**, select **Alerts**
2. Click **Manage action** at the top of the Alerts window
   Under action group, you will be required to fill in specific information regarding your group whom to send alert, including:

   a. Action group name: Provide action group name **mydemogroup**

   b. Short name: Provide short name **mydemogroup**

   c. Subscription: Select default subscription

   d. Resource group: Leave the default resource group

   e. Action name: Provide action name **myalertgroup**

      Under action type, dropdown select "***email/sms/push/voice***", it will open new window

   f. Under Email/SMS/Push/Voice, provide the following details:

      i. Email: Provide your **email id**

      ii. SMS: Select country code & provide your **mobile no**.

      iii. Leave other details as default & Press **Ok**

   g. Press **Ok**

   h. You will also be received email & SMS of the alert

Part B: Create Alert

3. Under Alerts, click **+New alert rule** at the top of the Alerts window

4. The **Create rule** window appears.

    a. Click on **Select** under **resources**. Under Define Alert condition alert, use Filter by subscription / Filter by resource type and select the resource or resource group from the list displayed.

        i. **Filter by subscription**: Dropdown & select **Default subscription**

        ii. **Filter by resource type**: Dropdown & select **Network security groups**

        iii. Under **resource** select your network security group **myDemoNSG01**

        iv. Leave all the settings as default & click on **Done**

    b. Click on **Add** under **conditions**. Under Configure signal logic, configure the following:

        i. Signal type: Dropdown & select **Activity log**

        ii. Monitor service: Dropdown & select **Activity Log – Administrative**

        iii. Under signal name, select **Create or Update Network Security Group**

        iv. Dropdown & select **Informational** event level under **Alert logic**

        v. Leave other settings as default & select **Done**

    c. Click **Add** under **actions**.

        i. Select **mydemogroup** & click on **Add**

d. In Alert details, provide the following details:

   i. Alert rule name: **Changes in NSG resource**

   ii. Action: **Alert due to changes performed in NSG resource**

   iii. Save alert to resource group: **myRG-300-01-01**

5. Click on **Create alert rule**

Part C: Change rules in NSG

6. Go to left side on click on **Resource group**

7. Select **myRG-300-01-01**
   Note: In the resource group you can see the myDemoNSG01

8. Open the **myDemoNSG01**

9. Select **Inbound security rules** under settings

10. Select **+ Add**

11. Leave all the settings as default & press **Add**

Note: Wait for few mnts., before alert get fired

Part D: Check Alert

12. From Azure portal, go to **Monitor**, select Alerts. Here you will see the fired alerts

13. You will also be received email & SMS of the alert