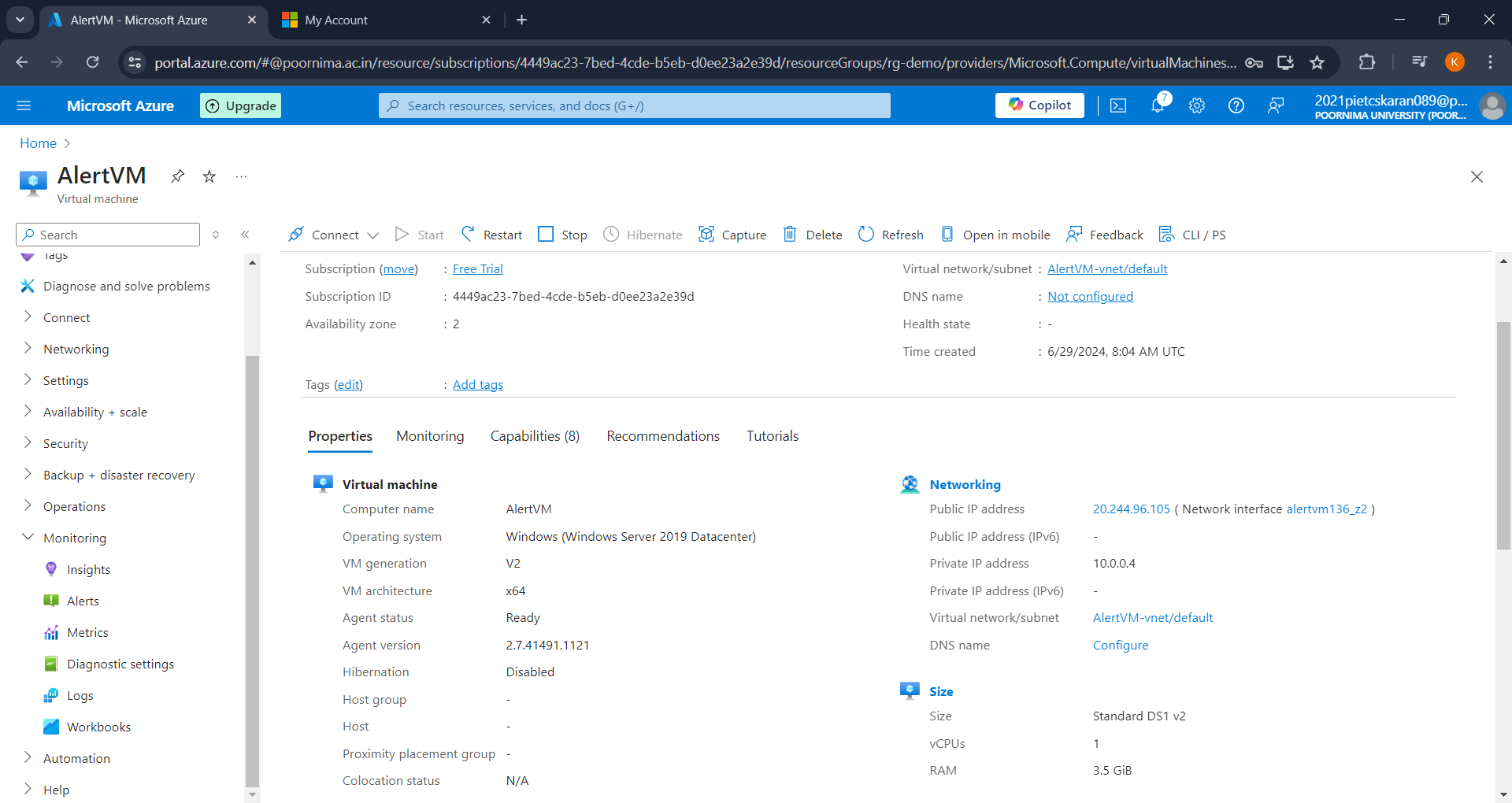
1. **Create a Memory Alert for Virtual machines Configure Alerts/thresholds /Action groups on the resources Database monitoring**

**Ans:**

* **Creating a virtual machine.**

1. Click on "Create a resource" > "Compute" > "Virtual Machine".
2. Configure Basic Settings:
3. Provide the necessary information such as subscription, resource group, VM name, region, image, size, and authentication type (username and password or SSH key).
4. After configuring the necessary settings (disks, networking, management), go to the "Review + create" tab, review all configurations, and click "Create" to start the deployment process.

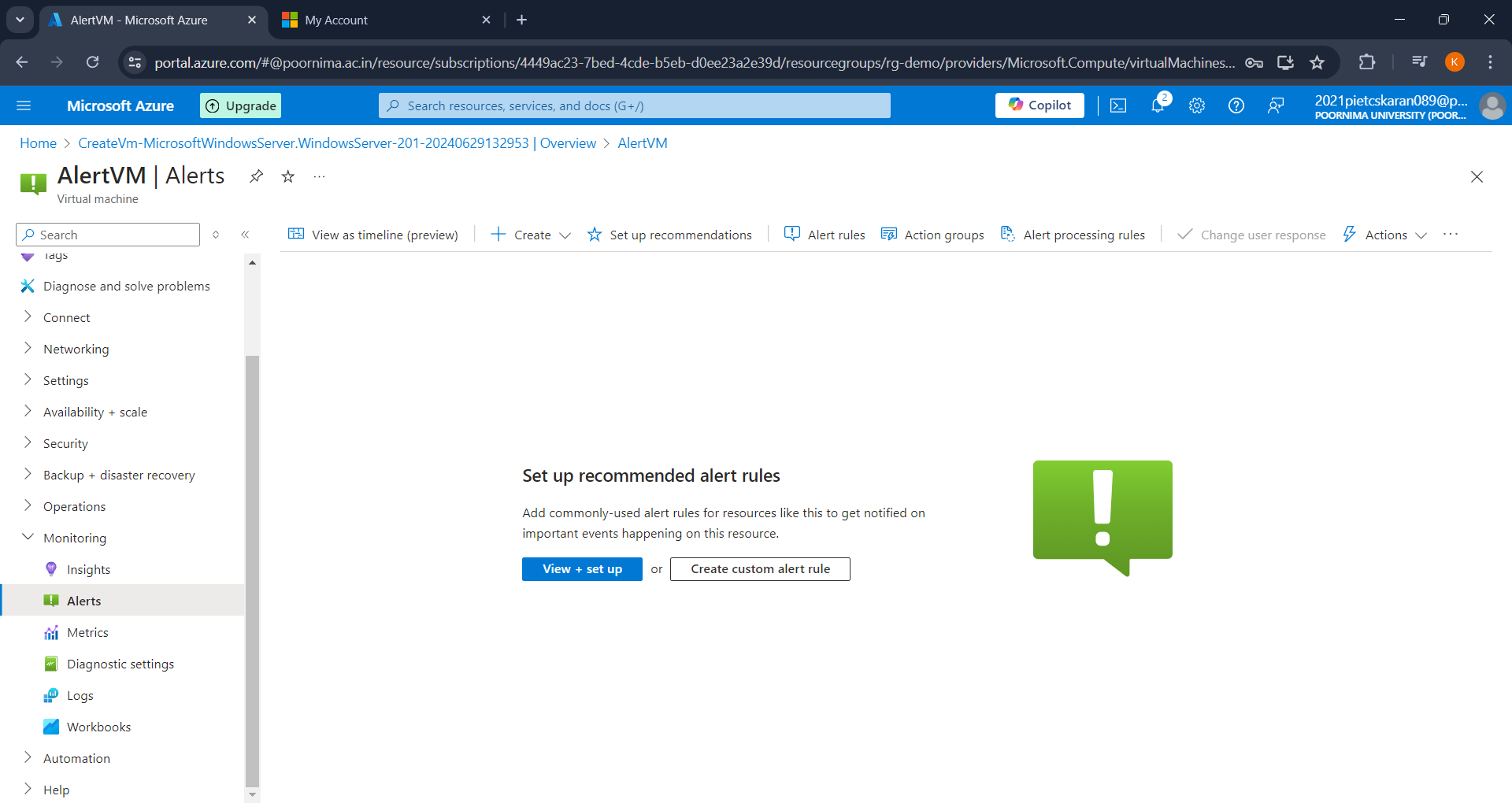


* **Configure Memory Alerts for Virtual Machines**
* Step 1: Set Up Monitoring

1. Go to the Azure portal.
2. Navigate to the virtual machine you want to monitor.
3. In the left-hand menu, select "Monitoring" > "Insights".

* Step 2: Create an Alert Rule

1. Under the "Alerts" section, click on "Alert rules".
2. Click on "New alert rule".
3. Define the scope by selecting the specific virtual machine.
4. Choose a condition:
5. Click on "Add condition".
6. Select the signal type. For memory usage, you might need to look for metrics such as "Available memory" or "Memory % Committed Bytes In Use".
7. Configure the condition settings (e.g., threshold value).
8. Define the action:
9. Click on "Add action group".
10. Create a new action group or select an existing one.
11. Add actions such as email, SMS, webhook, or Azure Function.
12. Define the alert details (name, description, severity).
13. Review and create the alert rule.Create a new Public IP Address or select an existing one.

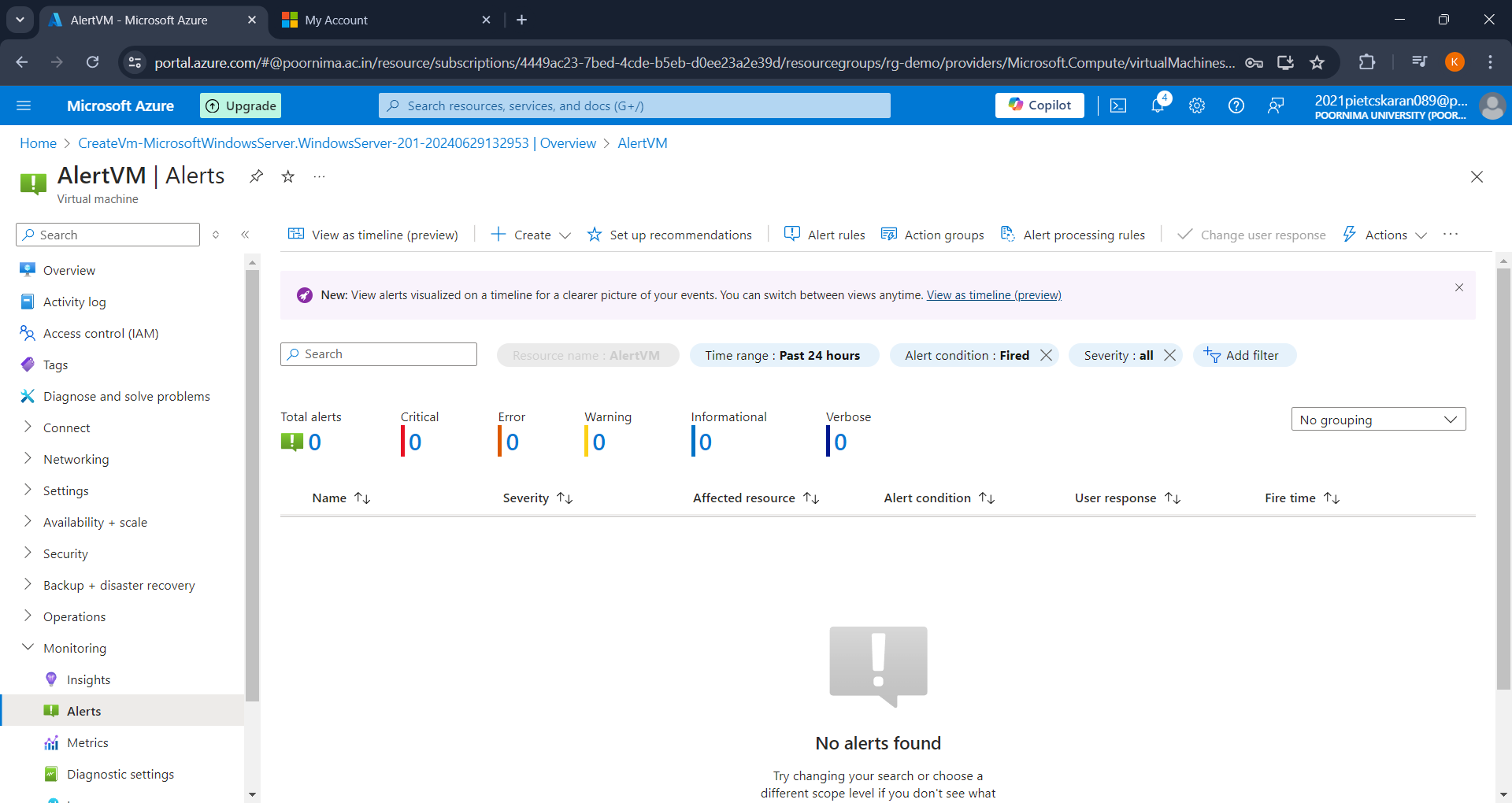


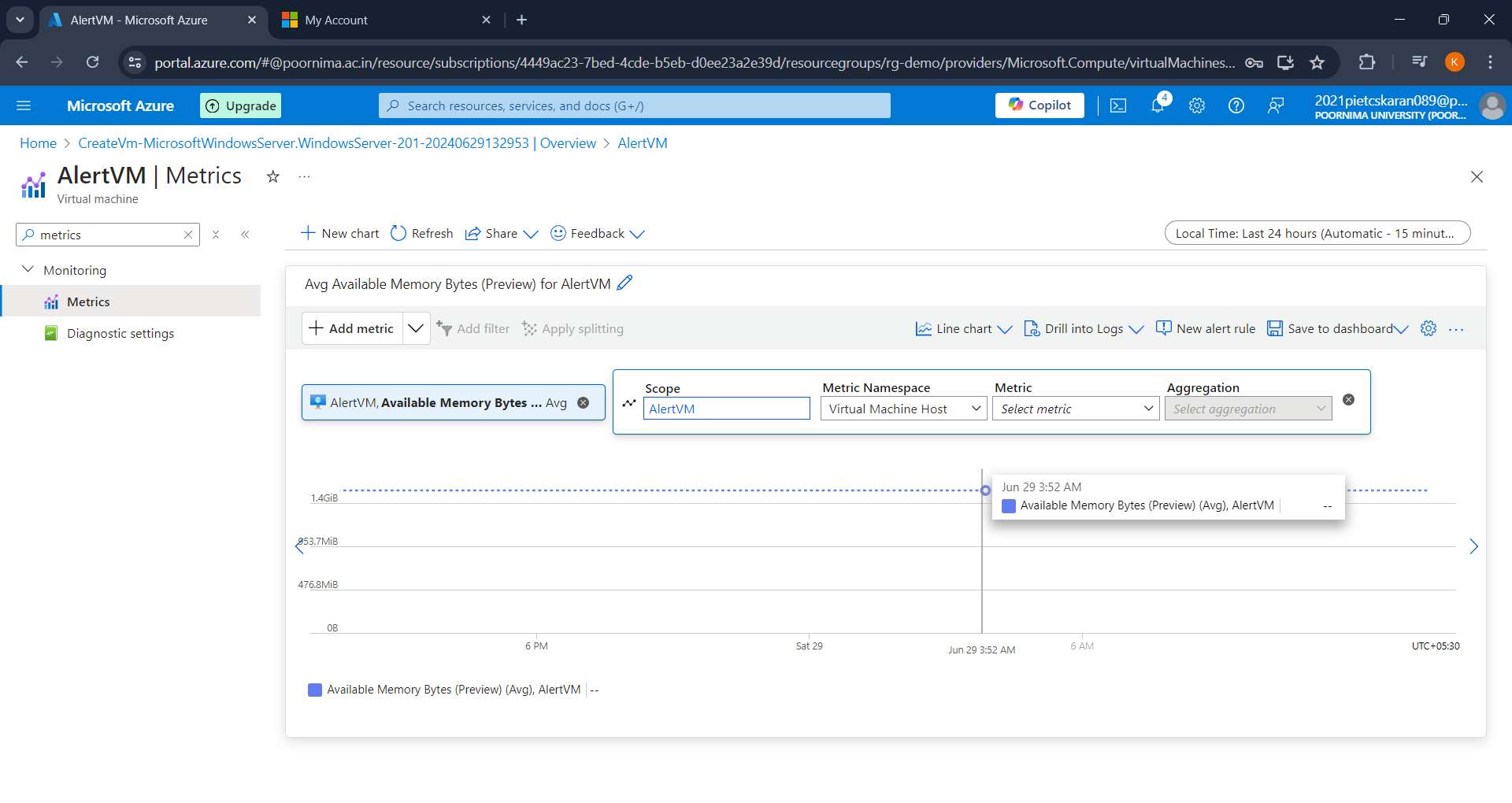
* **Configure Alerts/Thresholds**
* Step 1: Define Metrics and Thresholds

1. Go to the "Metrics" section of your resource.
2. Select the metrics you want to monitor (e.g., CPU usage, Disk I/O, Memory usage).
3. Set thresholds for these metrics based on your requirements.

* Step 2: Create Alert RulesClick Add a backend pool.

1. Navigate to "Alerts" > "Alert rules".
2. Click on "New alert rule".
3. Follow the same steps as mentioned above to configure the scope, conditions, actions, and details.





* **Set Up Action Groups**

1. Navigate to "Alerts" > "Manage actions".
2. Click on "Add action group".
3. Fill in the necessary details (action group name, short name).
4. Add the necessary actions (e.g., email, SMS, webhook).
5. Assign the action group to the alert rules you created.

* **Database Monitoring**
* Step 1: Enable Diagnostics

1. Go to the Azure portal.
2. Navigate to your database resource.
3. In the left-hand menu, select "Diagnostic settings".
4. Enable diagnostics and select the logs and metrics you want to collect.

* Step 2: Set Up Alerts

1. Go to "Alerts" > "Alert rules".
2. Click on "New alert rule".
3. Define the scope by selecting the database.
4. Choose a condition:
5. Click on "Add condition".
6. Select the appropriate signal type (e.g., DTU percentage, Deadlocks, CPU percentage).
7. Configure the condition settings.
8. Define the action:
9. Click on "Add action group".
10. Create a new action group or select an existing one.
11. Add necessary actions.
12. Define the alert details (name, description, severity).
13. Review and create the alert rule.

