😊 Monitoring Alerts

Azure Monitor is a comprehensive monitoring solution offered by Microsoft Azure, designed to provide insights into the performance and health of applications and resources deployed on Azure. It helps users to gain visibility into their cloud environment, identify issues, and take proactive measures to ensure optimal performance and availability.

Azure Monitor offers a variety of features, including:

1. **Metrics:** Azure Monitor collects and analyzes performance metrics from various Azure services, allowing users to monitor the health and performance of their applications and resources in real-time. These metrics can include CPU usage, memory usage, network traffic, and more.
2. **Logs:** Azure Monitor collects log data from Azure resources and applications, as well as custom log data from sources such as virtual machines and containers. It provides powerful querying capabilities and integration with Azure Resource Graph for advanced analytics and troubleshooting.
3. **Alerts:** Users can set up alerts based on metrics and log data to notify them of issues or anomalies in their Azure environment. Azure Monitor supports alerting through various channels, including email, SMS, webhook, and integration with services like Azure Logic Apps and Azure Functions.
4. **Dashboards:** Azure Monitor allows users to create custom dashboards to visualize and analyze monitoring data from their Azure environment. Dashboards can include metrics, logs, and other monitoring insights, providing a centralized view of application performance and health.
5. **Application Insights:** Integrated with Azure Monitor, Application Insights provides application performance monitoring (APM) capabilities, including request tracking, dependency tracking, and performance profiling. It helps developers identify and diagnose issues in their applications, leading to improved reliability and user experience.
6. **Service Health:** Azure Monitor provides insights into the health and availability of Azure services and regions through the Azure Service Health dashboard. Users can stay informed about service incidents, planned maintenance, and other service-related events that may impact their applications.

Overall, Azure Monitor offers a comprehensive set of tools and capabilities for monitoring and managing Azure resources and applications, helping organizations to optimize performance, ensure reliability, and deliver a great user experience.

😄 Use cases of Azure Monitor:

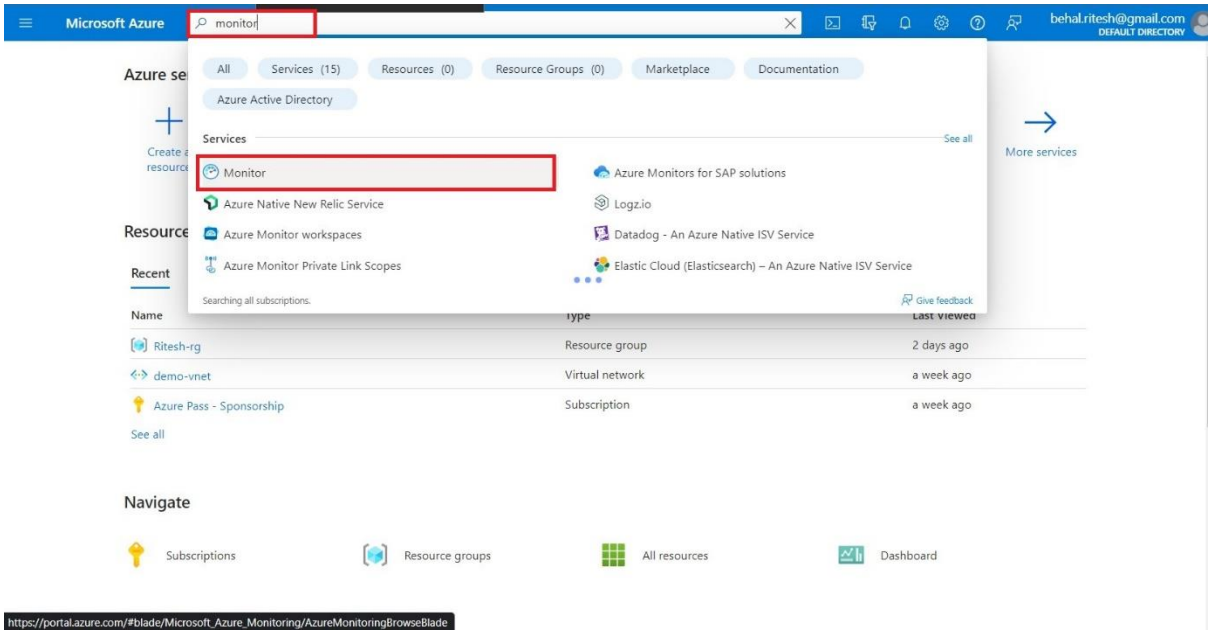
Azure Monitor can be utilized across various scenarios and use cases to monitor, diagnose, and optimize the performance and health of applications and resources deployed on Azure. Here are some common use cases:

1. **Infrastructure Monitoring:** Azure Monitor enables monitoring of Azure infrastructure components such as virtual machines, virtual networks, storage accounts, and Azure Kubernetes Service (AKS) clusters. Users can track metrics like CPU usage, memory utilization, disk I/O, and network traffic to ensure the optimal performance and availability of their infrastructure resources.
2. **Application Performance Monitoring (APM):** With Application Insights, a component of Azure Monitor, developers can monitor the performance and usage of their applications. They can track metrics related to response times, request rates, error rates, and dependencies (such as database queries and external API calls) to identify performance bottlenecks, troubleshoot issues, and optimize application performance.
3. **Log Analytics:** Azure Monitor's Log Analytics feature allows users to collect, analyze, and visualize log data from Azure resources, applications, and custom sources. Organizations can centralize log data from various sources, perform advanced analytics and correlation, and gain insights into application behavior, security events, and operational issues.
4. **Alerting and Notification:** Azure Monitor enables users to set up alerts based on predefined conditions or custom queries for metrics and log data. For example, users can configure alerts for CPU utilization exceeding a threshold, application errors reaching a certain rate, or security events matching specific patterns. Alerts can be sent via email, SMS, or integrated with other Azure services like Azure Functions or Azure Logic Apps for automated remediation.
5. **Auto-scaling:** By leveraging Azure Monitor metrics, organizations can implement auto-scaling strategies to dynamically adjust the capacity of their Azure resources based on workload demands. For instance, they can configure auto-scaling rules to increase the number of virtual machine instances or scale out Azure Kubernetes Service (AKS) clusters during peak traffic periods and scale in during low-traffic periods, ensuring optimal resource utilization and cost efficiency.
6. **Security Monitoring and Compliance:** Azure Monitor helps organizations enhance their security posture by monitoring for security-related events and compliance violations. By analyzing security logs and leveraging Azure Security Center integration, users can detect suspicious activities, respond to security incidents, and ensure compliance with regulatory requirements such as GDPR, HIPAA, and PCI DSS.
7. **Service Level Agreement (SLA) Monitoring:** Azure Monitor provides insights into the availability and performance of Azure services, allowing users to monitor compliance with service-level agreements (SLAs). Users can track service health and uptime, identify service interruptions, and analyze historical data to assess SLA adherence and plan for service reliability improvements.

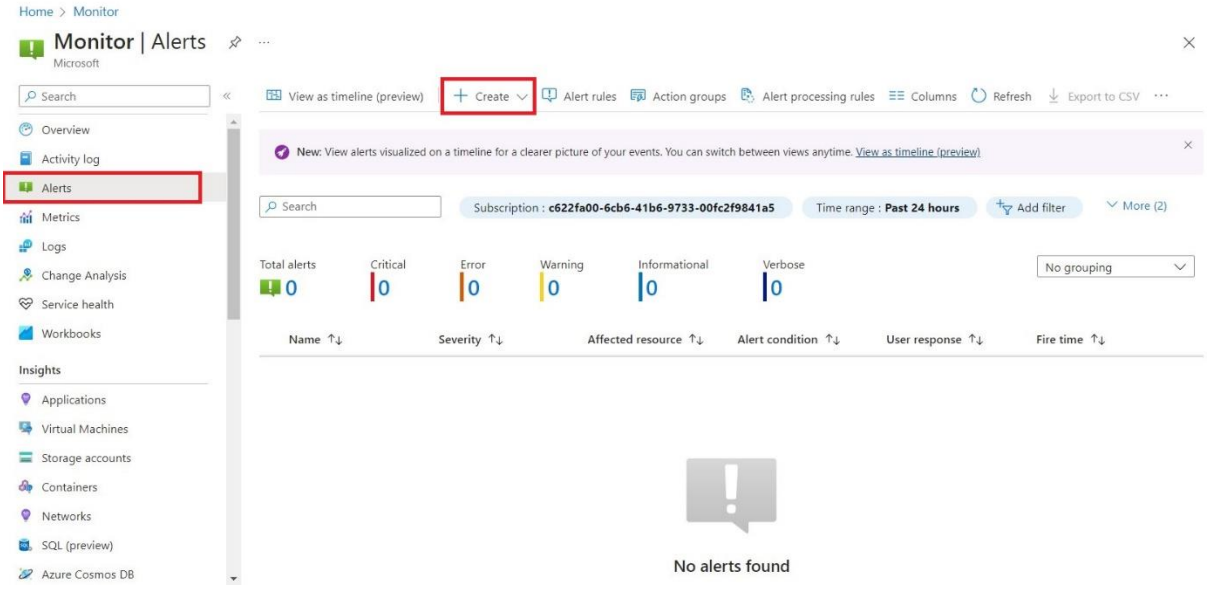
In this lab walkthrough, we are setting up monitoring alerts using Azure Monitor. The end goal is to create an alert rule that notifies us when certain conditions are met, such as network traffic exceeding a threshold on a virtual machine. By following the provided steps, users can configure the alert rule, create an action group for notifications, and receive alerts via email when the specified conditions are triggered. This helps in proactively identifying and addressing issues in Azure resources, ensuring optimal performance and availability.

😄 To begin with the Lab:

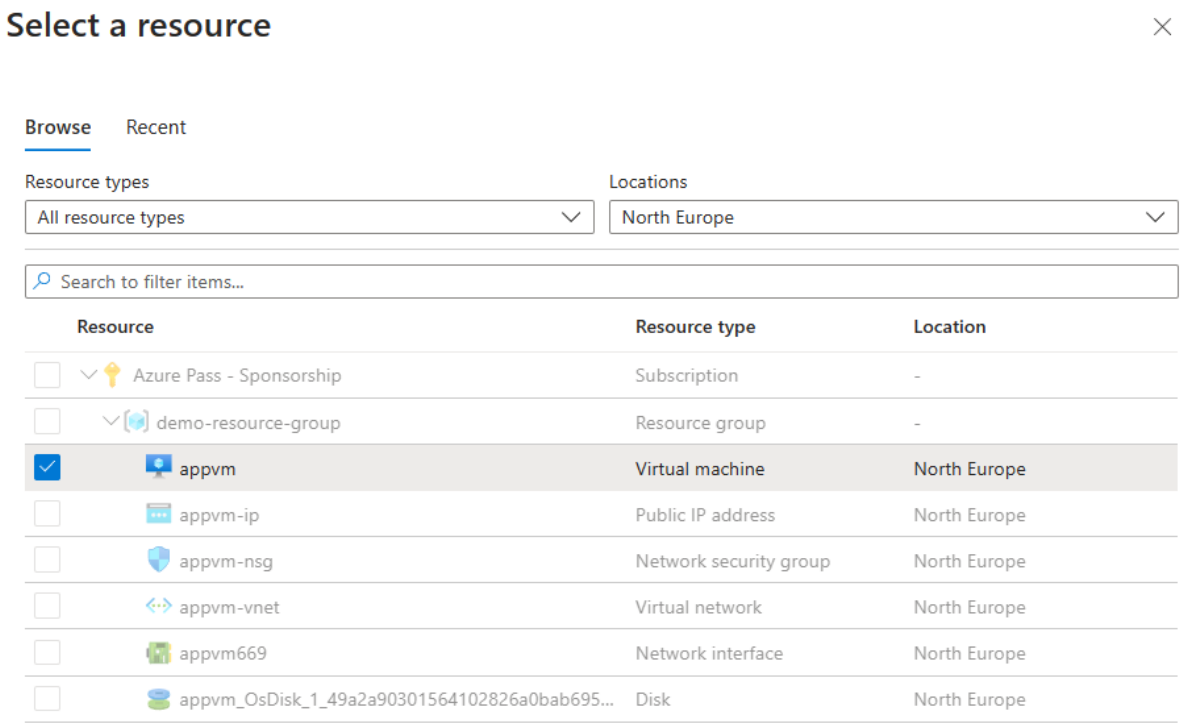
1. The prerequisites for this lab are that you should have some resources such as a windows virtual machine or a storage account but windows VM is much preferred.
2. In your Azure Portal search for Monitor and navigate to it.



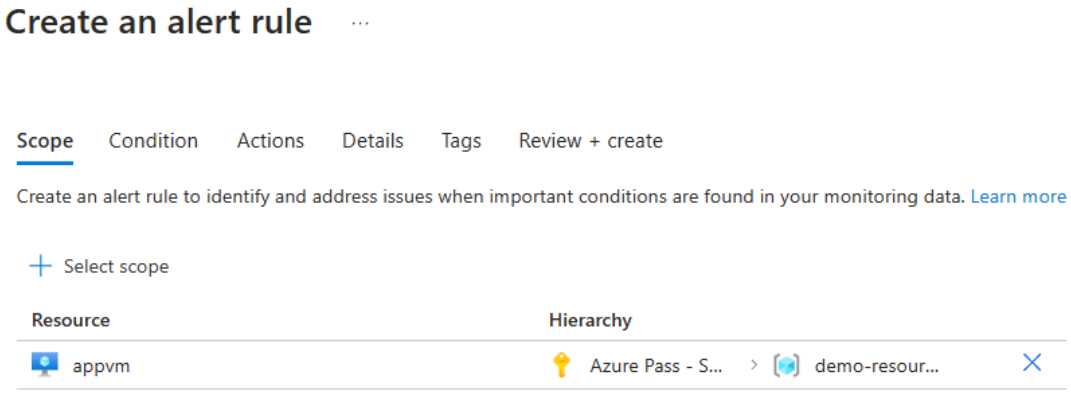
3. Choose “Alerts” from the left blade within the Azure Monitor window. Click on Create then choose to create alert rule.



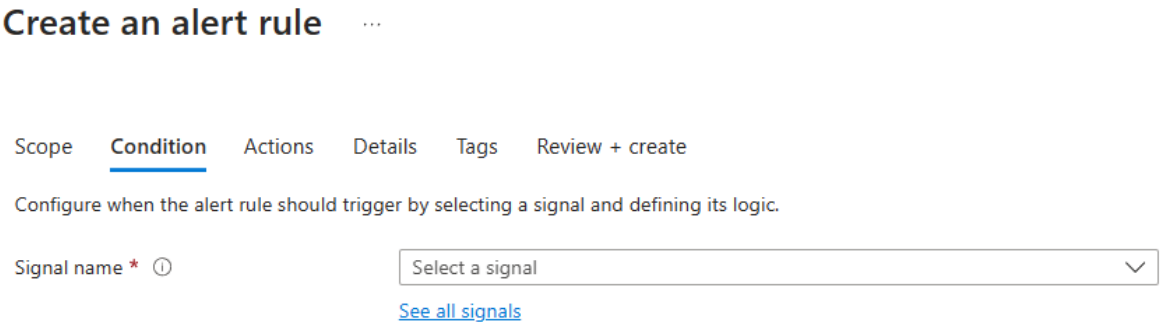
4. Now you need to expand the resources in your resource group and choose your Virtual machine. Then click on apply.



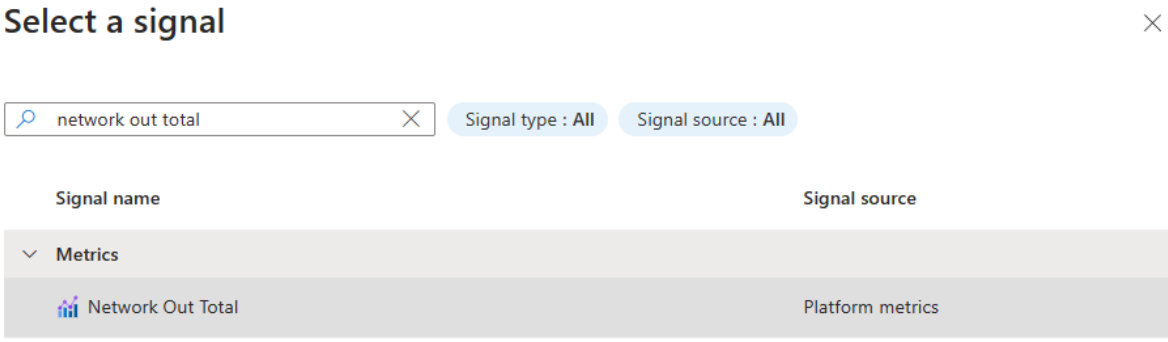
5. So, we created our scope, and now we have to move forward.



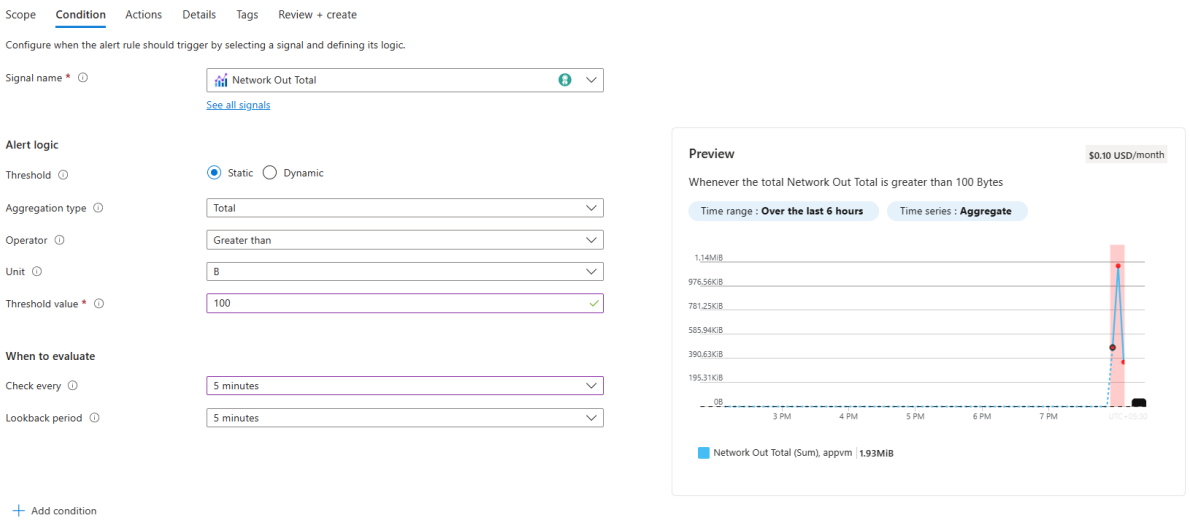
6. Now in the in the condition we need to click on see all signals.



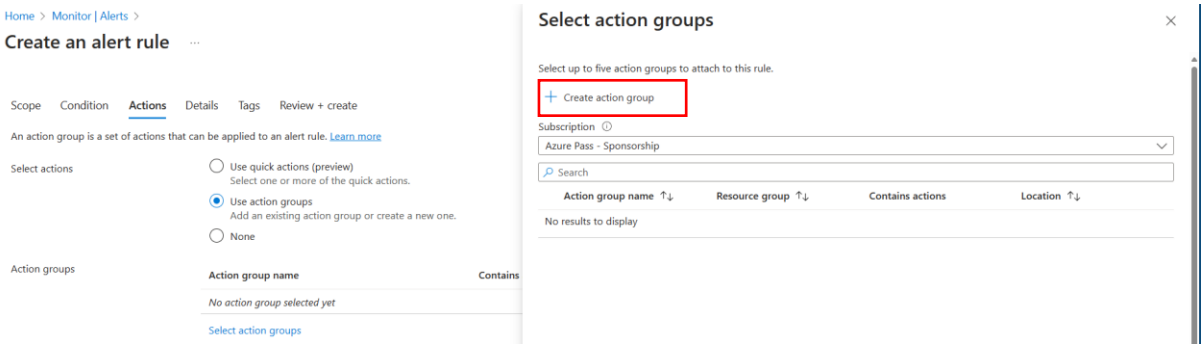
7. Then you need to search for network out total and choose it then click on apply.



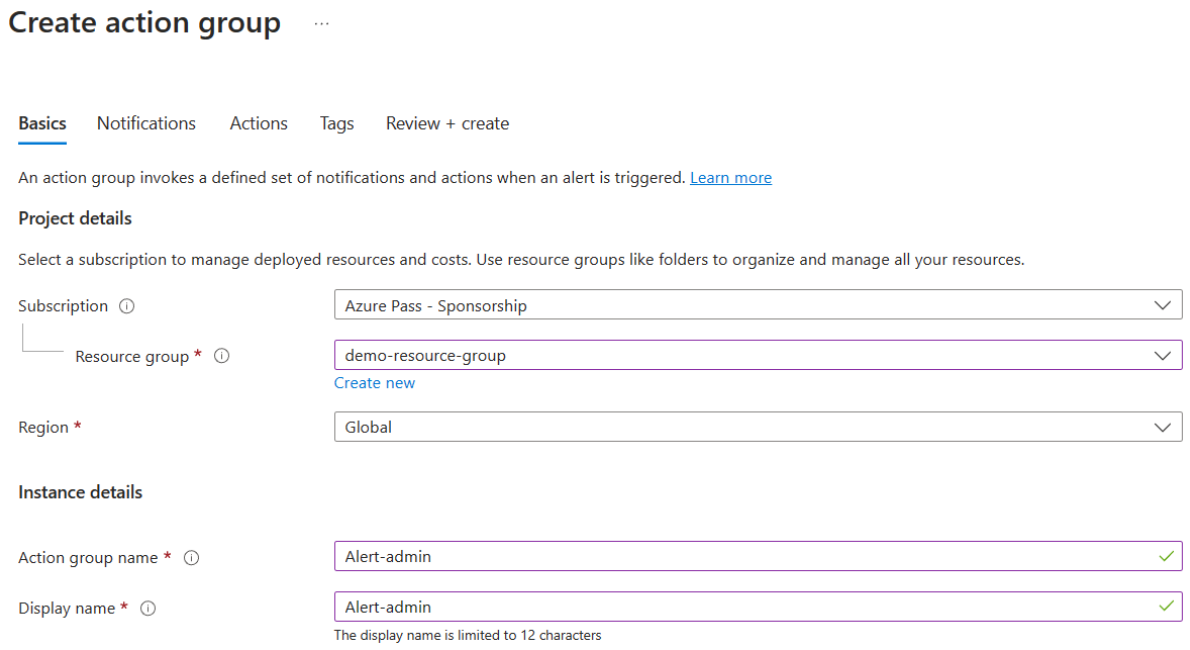
8. Now you will see that you have options to set the condition as per your wish and this is also providing with a graph which you can see down below.
9. Now choose the same settings as shown below and move forward.



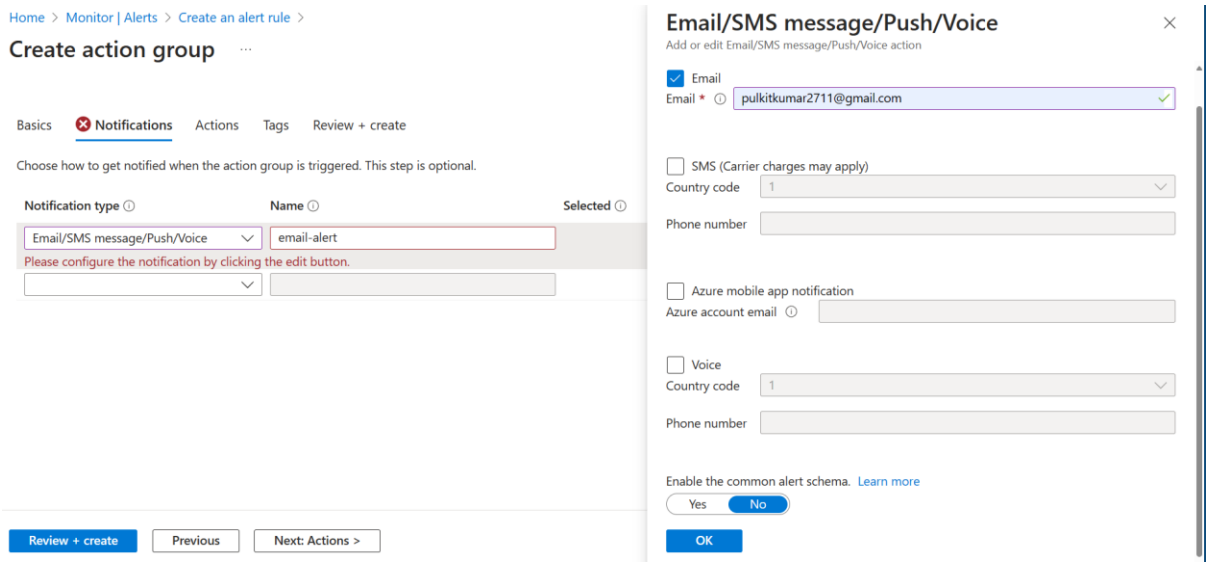
10. On the next page it will ask you to create action groups. So you need to click on create action group.



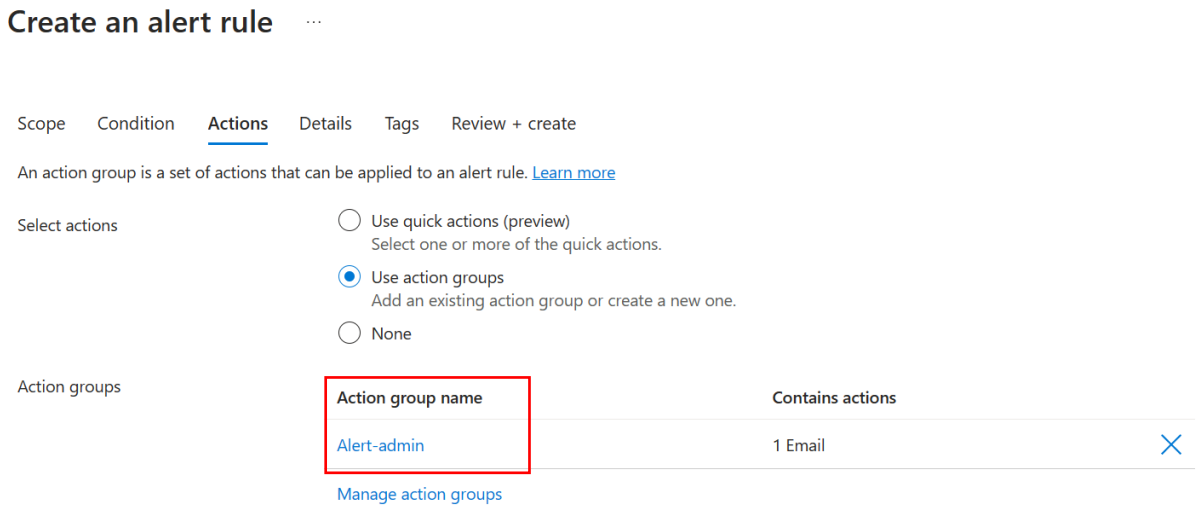
11. Then while creating an action group you need to choose your resource group and then give it a name.



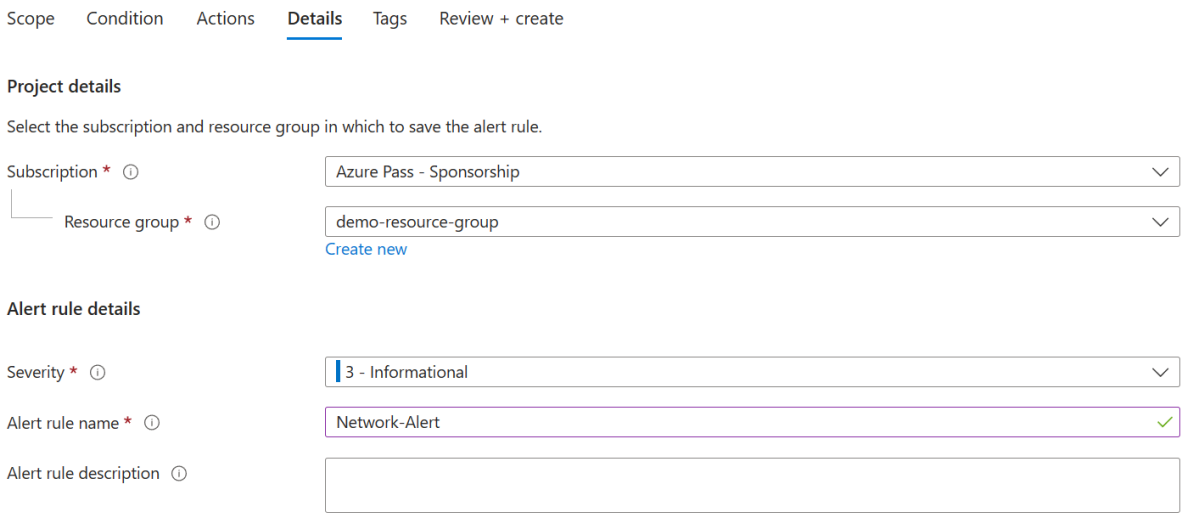
12. Now in the notification you need to choose email and then give your email then click on OK.
13. Then just move to review page and create your action group.



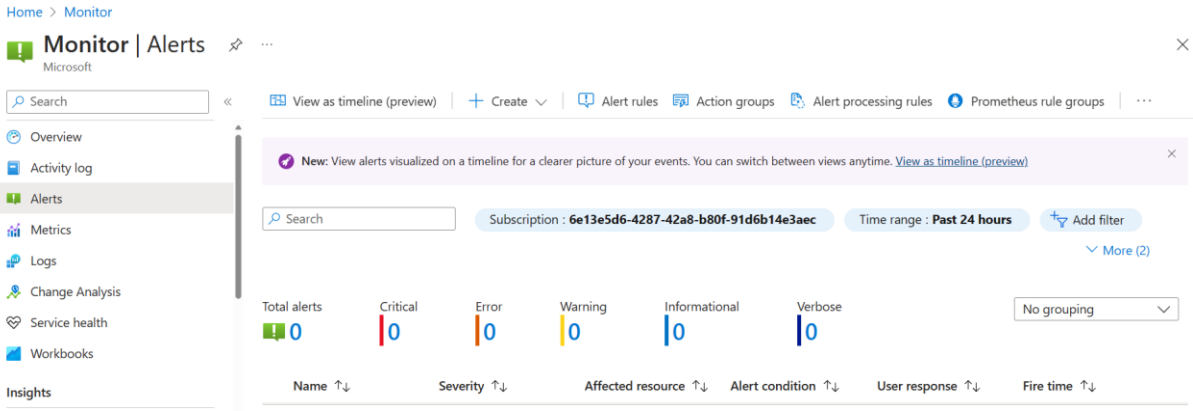
14. Here what you're doing is we're just creating something known as the action group. This is when we're (indistinct) back onto the creation of the alert group. The action group is separate. You've gone ahead and created the action group. The action group defines what needs to be done when the alert is triggered and now this action group has been added onto this alert rule. Go onto next for the details.



15. Then in the details give the alert rule name and move to review page and create your alert.



16. You just have created an alert it won't show anything until after 5 minutes. So just wait for some time.



17. Also if you go check the email that you have provided Microsoft also sends you the email that you have been added to the action group.

Microsoft Azure

You've been added to an Azure Monitor action group

You are now in the Alert-admin action group and will receive notifications sent to the group.

View details on Azure Monitor action groups >

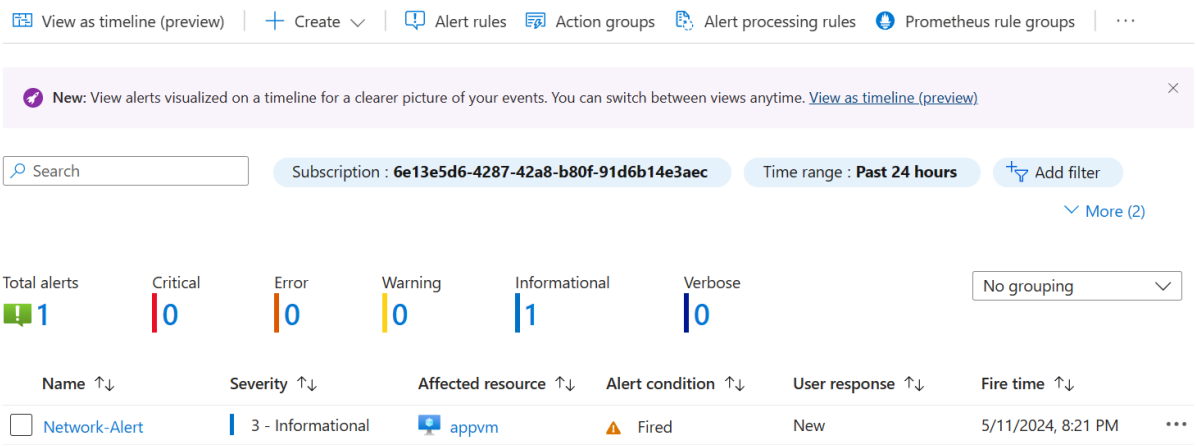
Account information

Subscription ID: 6E13E5D6-4287-42A8-B80F-91D6B14E3AEC

Resource group name: demo-resource-group

Action group name: Alert-admin

18. After 5 minutes we got an alert if you couldn't see this just refresh the page. .



19. Also we got an email regarding our alert.

⚠ Your Azure Monitor alert was triggered

Azure monitor alert rule Network-Alert was triggered for appvm at May 11, 2024 14:51 UTC.

Rule ID	/subscriptions/6e13e5d6-4287-42a8-b80f-91d6b14e3aec/resourceGroups/demo-resource-group/providers/microsoft.insights/metricAlerts/Network-Alert View Rule >
Resource ID	/subscriptions/6e13e5d6-4287-42a8-b80f-91d6b14e3aec/resourceGroups/demo-resource-group/providers/Microsoft.Compute/virtualMachines/appvm View Resource >

Alert Activated Because:

Metric name	Network Out Total
Metric namespace	virtualMachines/appvm
Dimensions	ResourceId = c4f0e9e0-ada0-49a4-84c9-aa3a90df06ec
Time Aggregation	Total
Period	Over the last 5 mins
Value	252778