# Lab 11 - Implement Monitoring

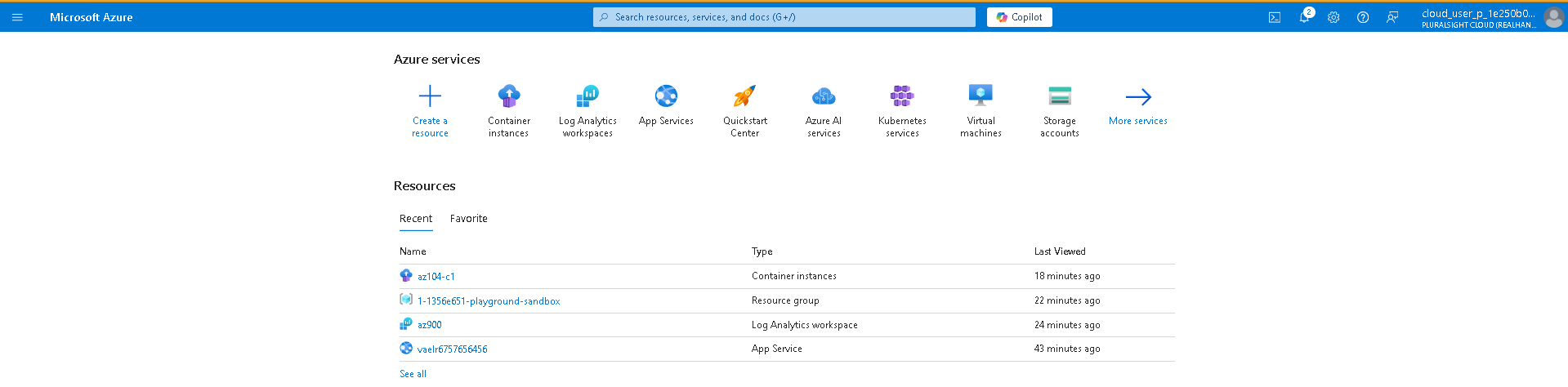
Made by Valeriy Manuilyk <3

## Task 1: Use a template to provision an infrastructure

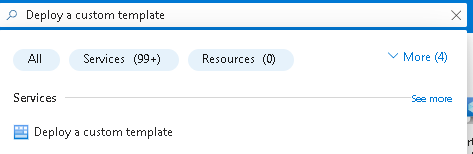
1.Download the ****\Allfiles\Lab11\az104-11-vm-template.json**** lab files to your computer.



2.Sign in to the ****Azure portal**** - https://portal.azure.com



3.From the Azure portal, search for and select Deploy a custom template.



1. On the custom deployment page, select ****Build you own template in the editor****

5.On the edit template page, select ****Load file****.

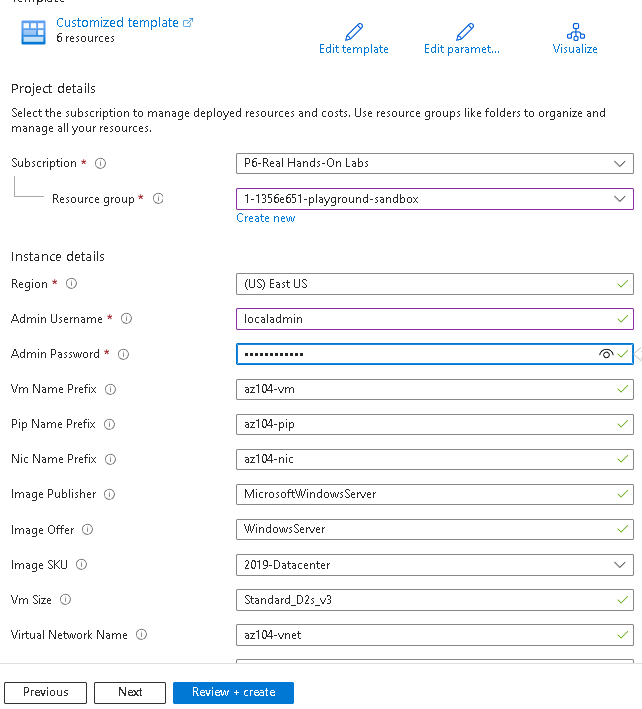
6.Locate and select the ****\Allfiles\Labs11\az104-11-vm-template.json**** file and select ****Open****.



7.Select ****Save****.

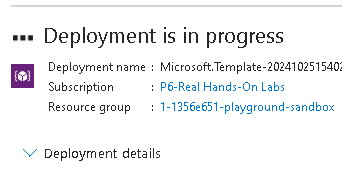


8.Use the following information to complete the custom deployment fields, leaving all other fields with their default values:

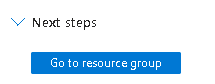


9.Select ****Review + Create****, then select ****Create****.

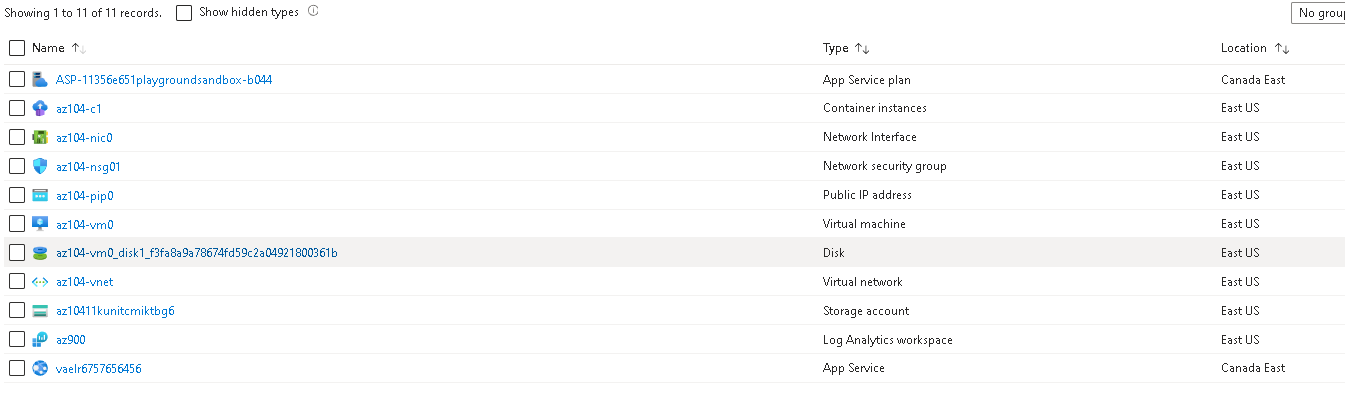




10.Wait for the deployment to finish, then click ****Go to resource group****.

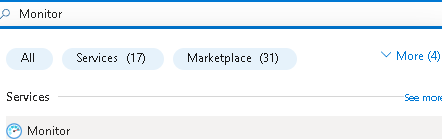


11.Review what resources were deployed. There should be one virtual network with one virtual machine.



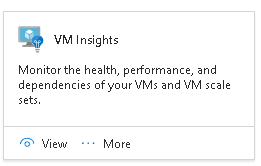
****Configure Azure Monitor for virtual machines (this will be used in the last task)****

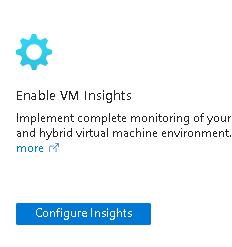
1.In the portal, search for and select ****Monitor****.



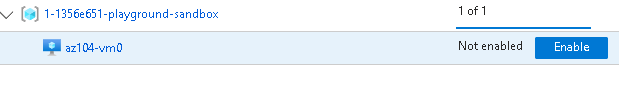
2.Take a minute to review all the insights, detection, triage, and diagnosis tools that are available.

3.Select ****View**** in the ****VM Insights**** box, and then select ****Configure Insights****.

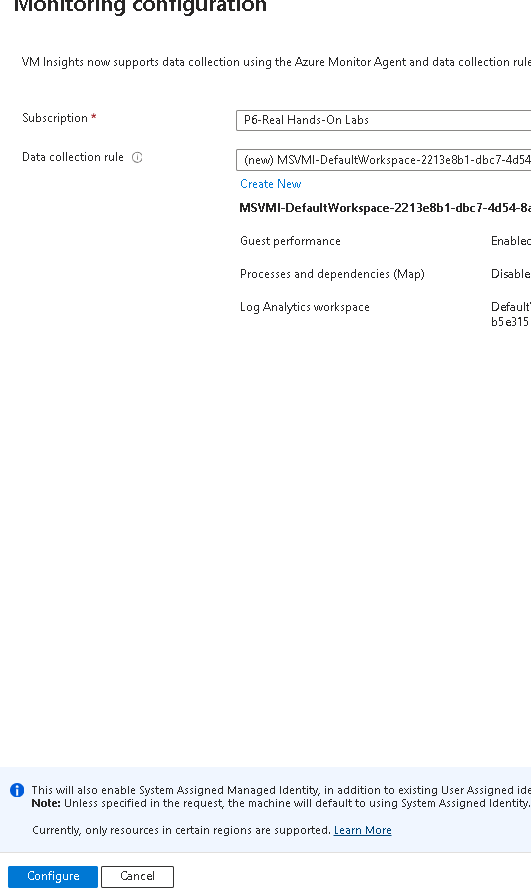




4.Select your virtual machine, and then ****Enable**** (twice).



5.Take the defaults for subscription and data collection rules, then select ****Configure****.

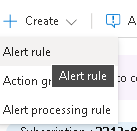


## Task 2: Create an alert

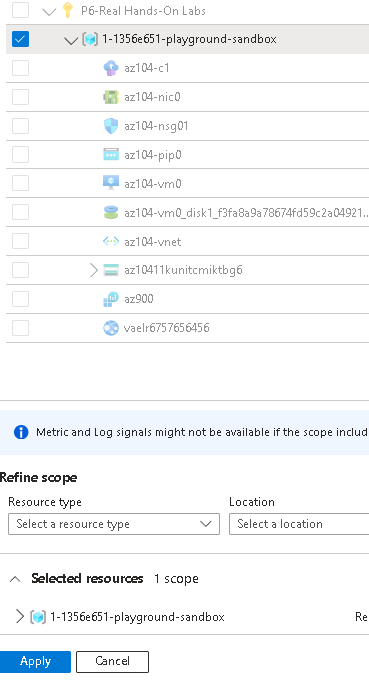
1.Continue on the ****Monitor**** page , select ****Alerts****.



2.Select ****Create +**** and select ****Alert rule****.



3.Select the box for the resource group, then select ****Apply****. This alert will apply to any virtual machines in the resource group. Alternatively, you could just specify one particular machine.



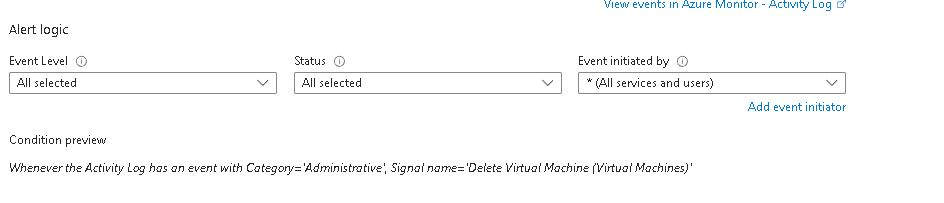
4.Select the ****Condition**** tab and then select the ****See all signals**** link.



5.Search for and select ****Delete Virtual Machine (Virtual Machines)****. Notice the other built-in signals. Select ****Apply****

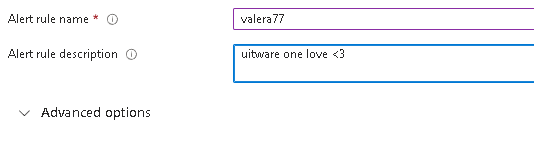


6.In the ****Alert logic**** area (scroll down), review the ****Event level**** selections. Leave the default of ****All selected****.

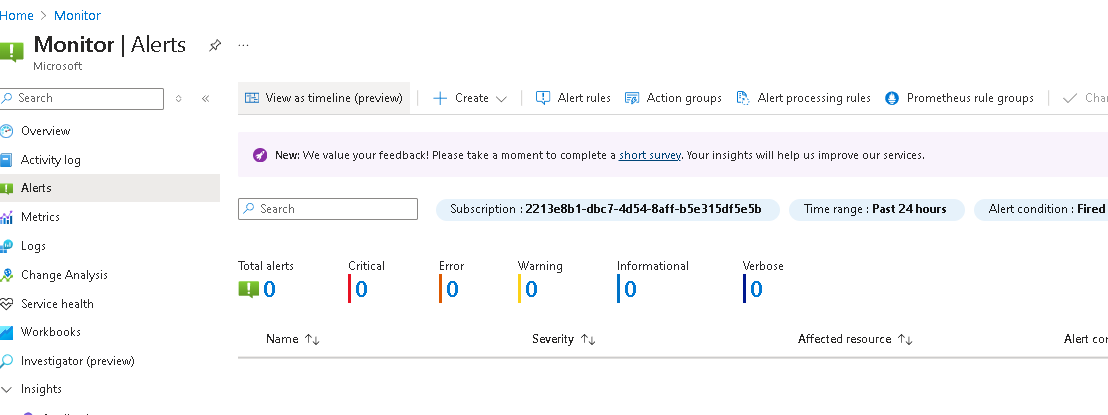


7.Review the ****Status**** selections. Leave the default of ****All selected****.

8.Leave the ****Create an alert rule**** pane open for the next task.

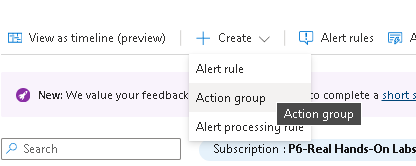




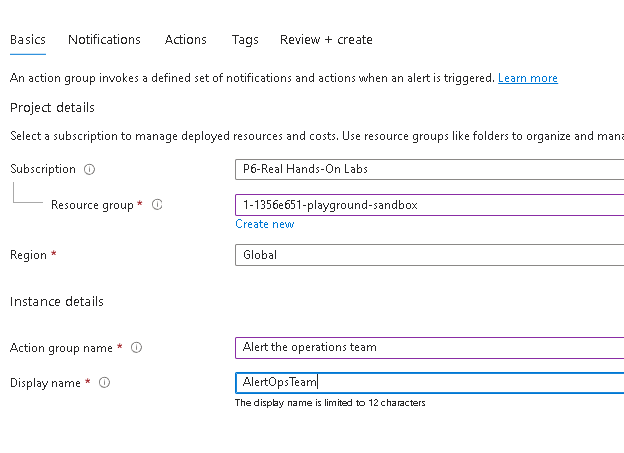


## Task 3: Configure action group notifications

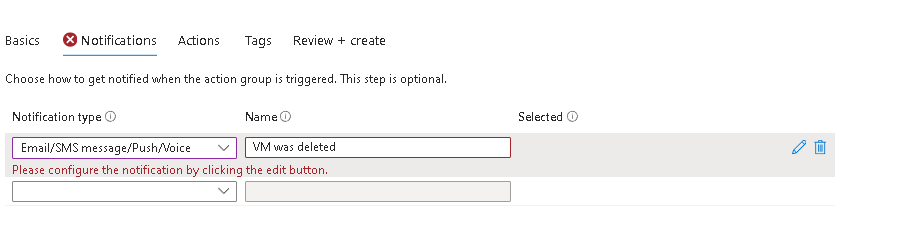
1.Continue working on your alert. Select ****Next: Actions****, and then select ****Create action group****.



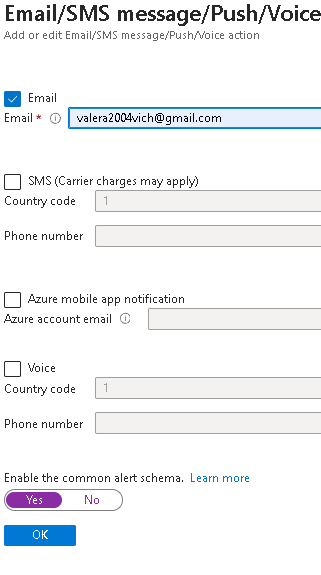
2.On the ****Basics**** tab, enter the following values for each setting.



3.Select ****Next: Notifications**** and enter the following values for each setting.



4.Select ****Email****, and in the ****Email**** box, enter your email address, and then select ****OK****.



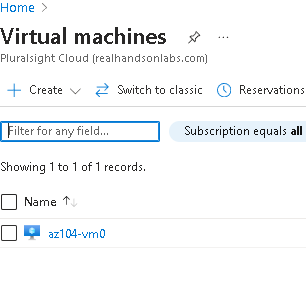
5.Once the action group is created move to the ****Next: Details**** tab and enter the following values for each setting.

6.Select ****Review + create**** to validate your input, then select ****Create****.

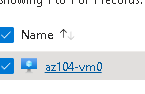


## Task 4: Trigger an alert and confirm it is working

1.In the portal, search for and select ****Virtual machines****.



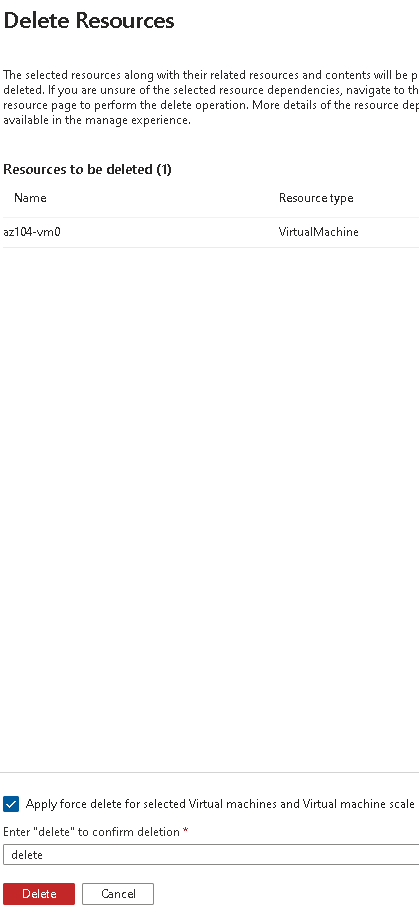
2.Check the box for the ****az104-vm0**** virtual machine.

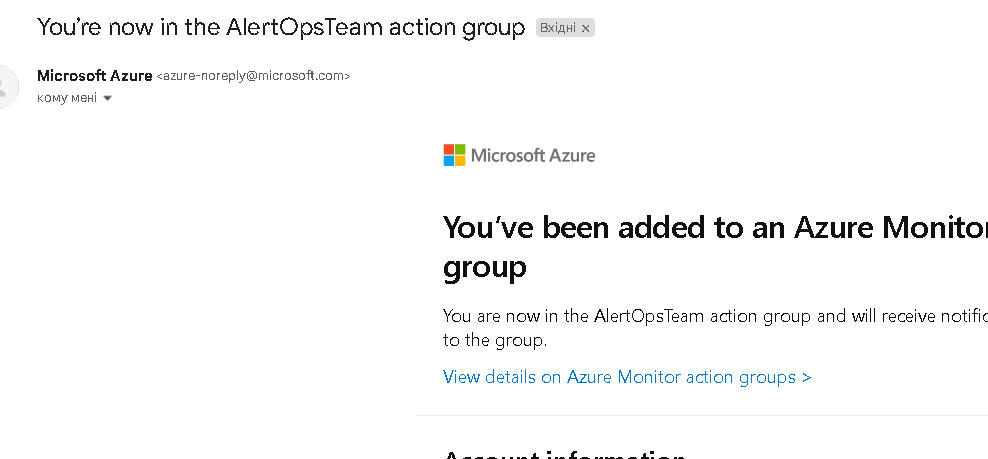


3.Select ****Delete**** from the menu bar.

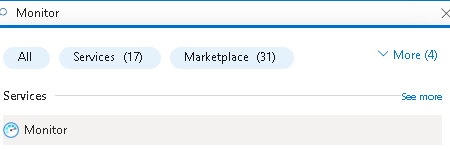
4.Check the box for ****Apply force delete****. Enter delete to confirm and then select ****Delete****.

5.In the title bar, select the ****Notifications**** icon and wait until ****vm0**** is successfully deleted.



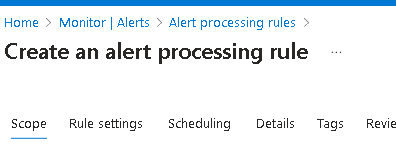


7.On the Azure portal resource menu, select ****Monitor****, and then select ****Alerts**** in the menu on the left.

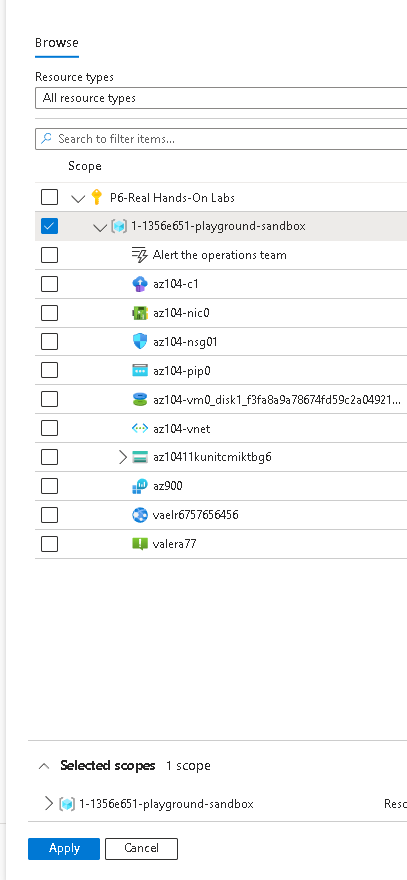


## Task 5: Configure an alert processing rule

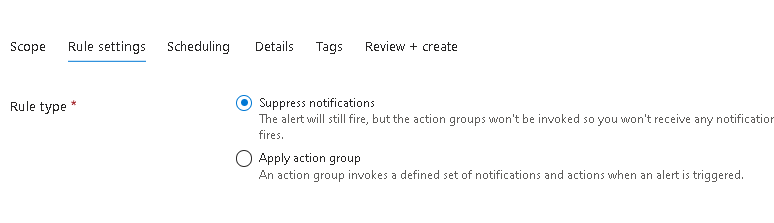
1.Continue in the ****Alerts**** blade, select ****Alert processing rules**** and then ****+ Create****.



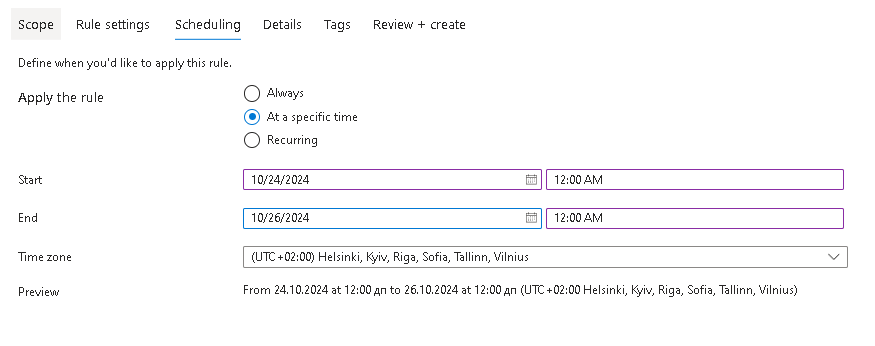
2.Select your ****resource group****, then select ****Apply****.



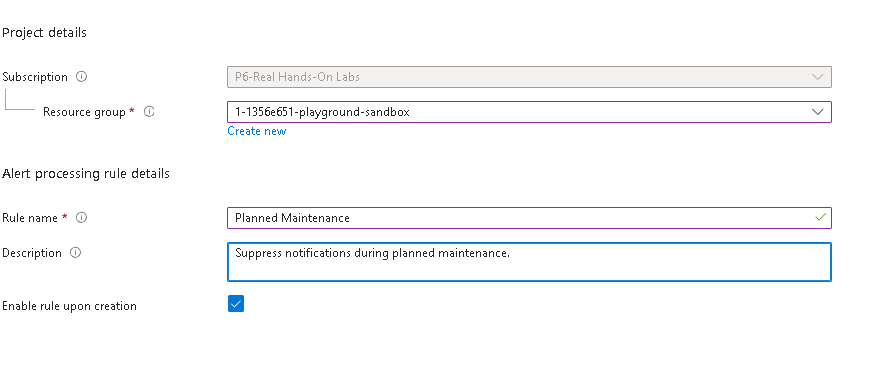
3.Select ****Next: Rule settings****, then select ****Suppress notifications****.



4.Select ****Next: Scheduling****.

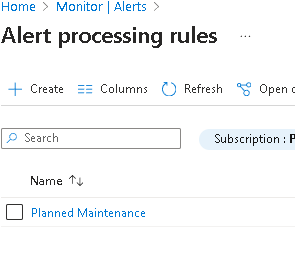


5.Select ****Next: Details**** and enter these settings:



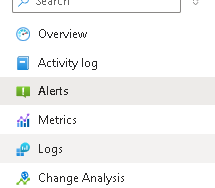
6.Select ****Review + create**** to validate your input, then select ****Create****.



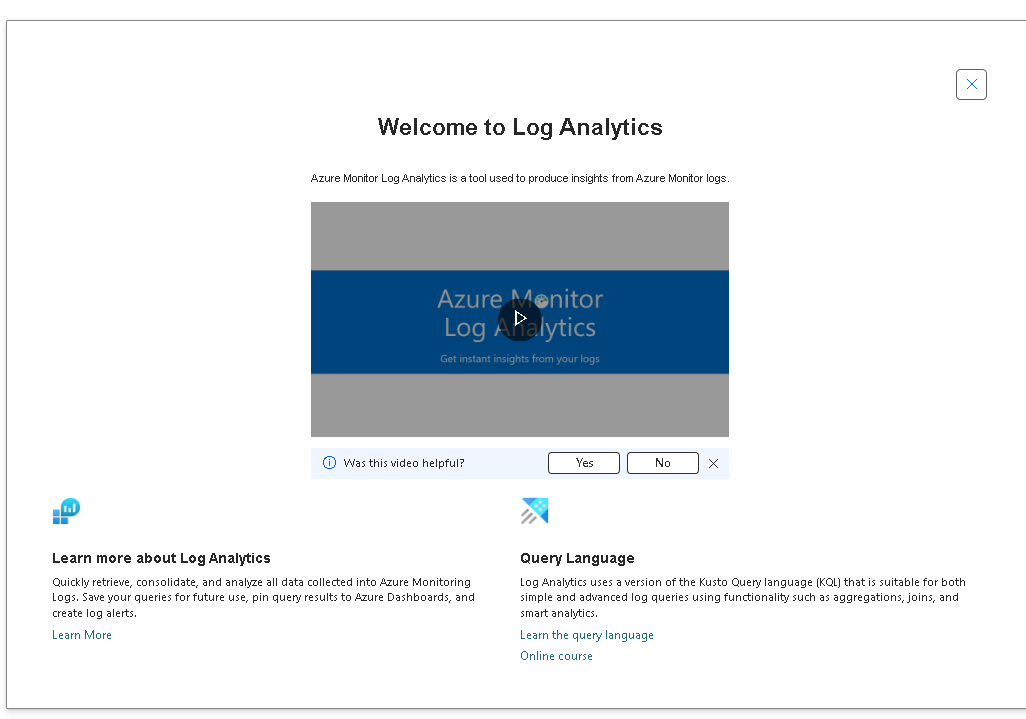


## Task 6: Use Azure Monitor log queries

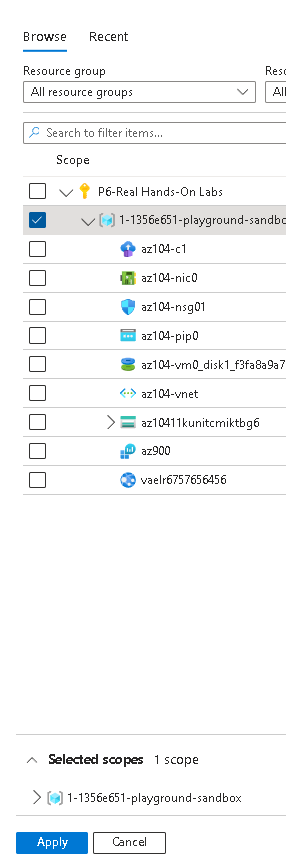
1.In the Azure portal, search for and select Monitor blade, click ****Logs****



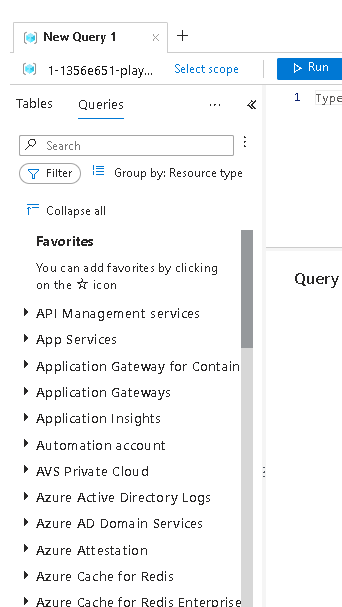
2.If necessary close the splash screen.



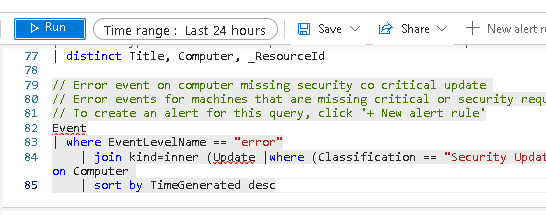
3.Select a scope, your ****resource group****. Select ****Apply****.



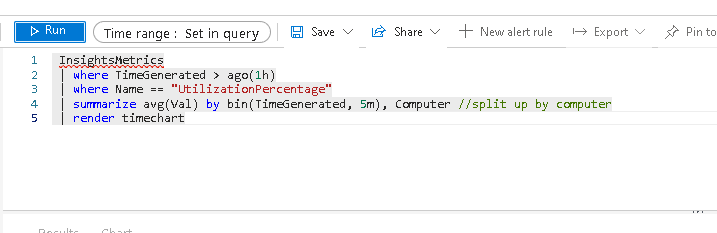
4.In the ****Queries**** tab, select ****Virtual machines**** (left pane).



11.Review the queries that are available. ****Run**** (hover over the query) the ****Count heartbeats**** query.



12.Replace the query with this one, and then click ****Run****. Review the resulting chart.



**Conclusion:**

Alerts help you detect and address issues before users notice there might be a problem with your infrastructure or application.

You can alert on any metric or log data source in the Azure Monitor data platform.

An alert rule monitors your data and captures a signal that indicates something is happening on the specified resource.

An alert is triggered if the conditions of the alert rule are met. Several actions (email, SMS, push, voice) can be triggered.

Action groups include individuals that should be notified of an alert.