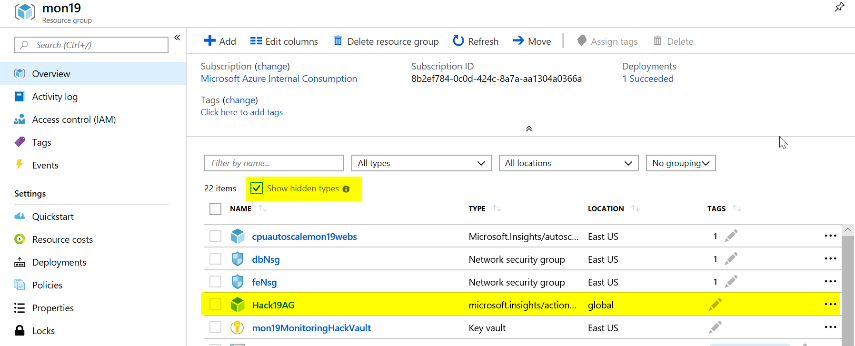
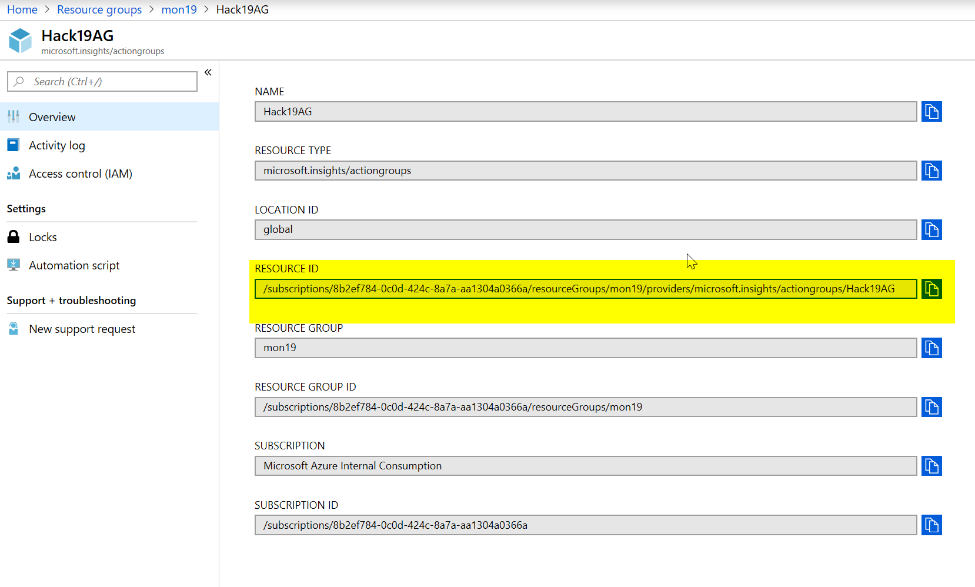
* Update the parameters file and deployment script for the GenerateAlertRules.json template located in the AlertTemplates folder
  + Add the names of your VMs and ResouceId for your Action Group

To find the ResourceId for your Action group navigate to the Resource Group where you are stored the action group and make sure to check off “Show hidden types”.



Click on your Action Group and copy the ResourceId



Then update the deployAlertRules.parameters.json file as it shows below.

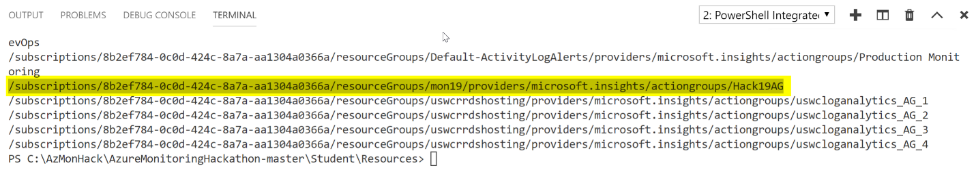
Or

In the deployAlertRulesTemplates.ps1 script update the resourcegroup and run the first few lines then run the code to get the Azure Monitor Action Group

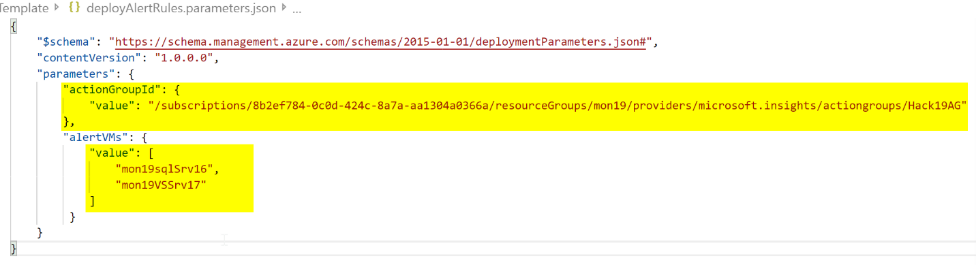
#Get Azure Monitor Action Group

Get-AzureRmResource -ResourceType 'Microsoft.Insights/actiongroups' | Select-Object Name, ResourceId

Copy and paste the resource Id for the Action Group you would like to use.



Save the parameters file and update the deployAlertRulesTemplate.ps1 file with the name of your Resource Group (and save it).



* Deploy the GenerateAlertRules.json template using the sample PowerShell script (deployAlertRulesTemplate.ps1) or create a Bash script (look at the example from the initial deployment)

#Update Path to files as needed

#Update the parameters file with the names of your VMs and the ResourceId of your Action Group (use command above to find ResourceId)

$template=".\AlertsTemplate\GenerateAlertRules.json"

$para=".\AlertsTemplate\deployAlertRules.parameters.json"

$job = 'job.' + ((Get-Date).ToUniversalTime()).tostring("MMddyy.HHmm")

New-AzureRmResourceGroupDeployment `

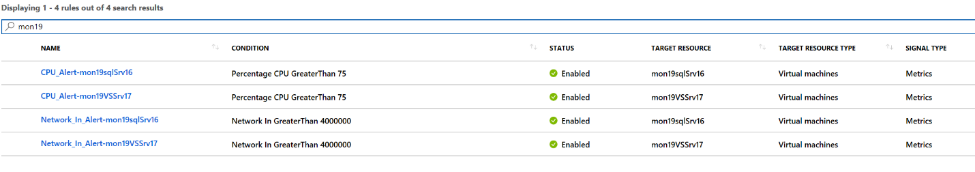
-Name $job `

-ResourceGroupName $rg.ResourceGroupName `

-TemplateFile $template `

-TemplateParameterFile $para

* Verify you have new Monitor Alert Rules in the Portal or from the command line (sample command is in the deployment script)



* Modify the GenerateAlertsRules.json to include “Disk Write Operations/Sec” and set a threshold of 10  
  **Tip:** Go here to view the list of metrics available by resource type - <https://docs.microsoft.com/en-us/azure/monitoring-and-diagnostics/monitoring-supported-metrics#microsoftcomputevirtualmachines>

Use this link to see the ARM schema - <https://docs.microsoft.com/en-us/rest/api/monitor/metricalerts/update>

{

"type": "Microsoft.Insights/metricAlerts",

"name": "[concat('Disk\_Write\_Alert','-',parameters('alertVMs')[copyIndex()])]",

"copy": {

"name": "iterator",

"count": "[length(parameters('alertVMs'))]"

},

"apiVersion": "2018-03-01",

"location": "global",

"tags": {},

"scale": null,

"properties": {

"description": "Disk Write metric has detected a large amount of disk operations",

"severity": "[parameters('alertSeverity')]",

"enabled": "[parameters('isEnabled')]",

"scopes": [

"[resourceId('Microsoft.Compute/virtualMachines', parameters('alertVMs')[copyIndex()])]"

],

"evaluationFrequency": "PT5M",

"windowSize": "PT5M",

"criteria": {

"odata.type": "Microsoft.Azure.Monitor.SingleResourceMultipleMetricCriteria",

"allOf": [

{

"name": "MetricDiskWriteOper",

"metricName": "Disk Write Operations/Sec",

"dimensions": [],

"operator": "GreaterThan",

"threshold": 10,

"timeAggregation": "Average"

}

]

},

"actions": [

{

"actionGroupId": "[parameters('actionGroupId')]",

"webHookProperties": {}

}

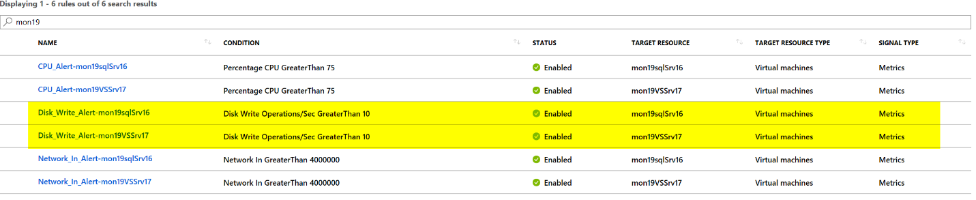
]

},

"dependsOn": []

},

* Rerun your template and verify your new Alert Rules are created for each of your VMs



* First team to me a screenshot of the new Alert Rules wins the challenge!!