# **Condition:** **Resource Group Deletion**

**Condition**

**Description:**

* A Resource Group provides a way to monitor, control access, provision and manage billing for collections of assets that are required to run an application, or used by a client or company department. They are automatically created for virtual machines, databases, and other assets, no matter how they are added to the cloud fabric.
* You have access to *Monitoring* and *Alert rules* for all the assets combined, and the ability to control role-based access to assets in the group, which is one of the most valuable reasons to use resource groups.
* Azure Resource Manager (ARM) is the technology that works behind the scenes so that you can administer assets using these logical containers.

**Impact:** Deletion of a Resource Group may result in deletion of all the child (nested) resources, and it also affects the user who are using assets inside resource group for performing their activity.

**Criticality:** Critical

**Frequency:** 15 Minutes

**Trigger Details**

**Trigger Condition:** Alert will be triggered if a “**Microsoft.Resources/subscriptions/resourcegroups /delete**” operation is succeeded.

**Method to capture trigger point:**

* REST API can be used to capture the activity logs on the subscription and filter the ‘Resource Group’ delete events.
* REST API URI is as mentioned below:

https://management.azure.com/subscriptions/{subscriptionId}/providers/microsoft.insights/eventtypes/management/values?api-version=2015-04-01&$filter

**$filter**: Reduces the set of data collected. This argument is required and it also requires at least the start date/time for events to be captured. This argument

**Example:**

<https://management.azure.com/subscriptions/61e103f4-57ec-4f6a-a2f5-df2a28f98d19/providers/microsoft.insights/eventtypes/management/values?api-version=2015-04-01&eventTimestamp> ge '01/23/2020 05:00:00’ and resourceProvider eq 'Microsoft.Resources'

* Reference link:

<https://docs.microsoft.com/en-us/rest/api/monitor/activitylogs/list>

* Alert will be triggered if **“operationName”** value is **“Microsoft.Resources/subscriptions/resourcegroups/delete”** **AND** **“status”** value is **“Succeeded”**.

**Sample Output from API:**

"authorization": {

"action": "Microsoft.Resources/subscriptions/resourceGroups/delete",

"scope": "/subscriptions/61e103f4-57ec-4f6a-a2f5-df2a28f98d19/resourceGroups/practicegroup"

},

"caller": "akshi.srivastava@continuum.net",

"channels": "Operation",

"claims": {

"aud": "https://management.core.windows.net/",

"iss": "https://sts.windows.net/c40ed5d6-e0e3-4d79-830c-7991f33a7c8e/",

"iat": "1579762110",

"nbf": "1579762110",

"exp": "1579766010",

"http://schemas.microsoft.com/claims/authnclassreference": "1",

"aio": "AVQAq/8OAAAAByvLNAmA87OuTF7nxuc5JgX3SsdwF3Q1Y3sNRjzpe+A20WasFHwsgMFQGoo0cAex770LJvEsxRwSWbFRmcfoRxYDBMyCOw0MbsHsvRtMxMg=",

"http://schemas.microsoft.com/claims/authnmethodsreferences": "pwd,mfa",

"appid": "c44b4083-3bb0-49c1-b47d-974e53cbdf3c",

"appidacr": "2",

"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname": "Srivastava",

"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname": "Akshi",

"groups": "5b26fef6-37df-49c1-ac28-3f2c5d9a92fc",

"ipaddr": "14.141.10.220",

"name": "Akshi Srivastava",

"http://schemas.microsoft.com/identity/claims/objectidentifier": "b05b67a1-b710-4b11-bc69-23ee20de1d2f",

"onprem\_sid": "S-1-5-21-1958057136-1394578505-252747866-9909",

"puid": "100320004A1D2F4C",

"http://schemas.microsoft.com/identity/claims/scope": "user\_impersonation",

"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier": "IIaWrr87mxJLBDT6TBcxsyWHYEICwqw9FnYWRRyX-UI",

"http://schemas.microsoft.com/identity/claims/tenantid": "c40ed5d6-e0e3-4d79-830c-7991f33a7c8e",

"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name": "akshi.srivastava@continuum.net",

"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn": "akshi.srivastava@continuum.net",

"uti": "zTR-n9iclE659Dd32y9CAA",

"ver": "1.0"

},

"correlationId": "dcef7c67-d512-4b47-8911-7611904efa98",

"description": "",

"eventDataId": "2064bd49-50e5-4fe2-9468-b03a57b9a356",

"eventName": {

"value": "EndRequest",

"localizedValue": "EndRequest"

},

"category": {

"value": "Administrative",

"localizedValue": "Administrative"

},

"id": "/subscriptions/61e103f4-57ec-4f6a-a2f5-df2a28f98d19/resourcegroups/practicegroup/events/2064bd49-50e5-4fe2-9468-b03a57b9a356/ticks/637153601517769604",

"level": "Informational",

"resourceGroupName": "practicegroup",

"resourceProviderName": {

"value": "Microsoft.Resources",

"localizedValue": "Microsoft.Resources"

},

"resourceId": "/subscriptions/61e103f4-57ec-4f6a-a2f5-df2a28f98d19/resourcegroups/practicegroup",

"resourceType": {

"value": "Microsoft.Resources/subscriptions/resourceGroups",

"localizedValue": "Microsoft.Resources/subscriptions/resourceGroups"

},

"operationId": "80a47e9a-2a33-4e7c-9c02-eb4b564d60de",

"operationName": {

"value": "Microsoft.Resources/subscriptions/resourcegroups/delete",

"localizedValue": "Microsoft.Resources/subscriptions/resourcegroups/delete"

},

"properties": {

"statusCode": "OK"

},

"status": {

"value": "Succeeded",

"localizedValue": "Succeeded"

},

"subStatus": {

"value": "",

"localizedValue": ""

},

"eventTimestamp": "2020-01-23T07:09:11.7769604Z",

"submissionTimestamp": "2020-01-23T07:10:32.1286063Z",

"subscriptionId": "61e103f4-57ec-4f6a-a2f5-df2a28f98d19",

"tenantId": "c40ed5d6-e0e3-4d79-830c-7991f33a7c8e"

},

**Alert Details**

**Alert Category:** Resource Group

**Details required along with Alert:**

1. Subscription ID
2. Resource Group Name (Name from resourceId).
3. Account Name performing the action (caller).
4. Event time stamp (eventTimestamp).