# **Condition:** **Virtual Machine Deleted**

**Condition**

**Description:**

* An Azure VM gives you the flexibility of virtualization without having to buy and maintain the physical hardware that runs it. However, you still need to maintain the VM by performing tasks, such as configuring, patching, and installing the software that runs on it.
* Each of these virtual machines provides its own virtual hardware which includes CPUs, memory, hard drives, network interfaces and other such devices.

**Impact:** Deletion of a VM may result in downtime of the applications running on the VM, and also affect the user activities that are being performed on the VM.

**Criticality:** Critical

**Frequency:** 15 Minutes

**Trigger Details**

**Trigger Condition:** Alert will be triggered if a “**Microsoft.Compute/virtualMachines/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 VM 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.

**Example:**

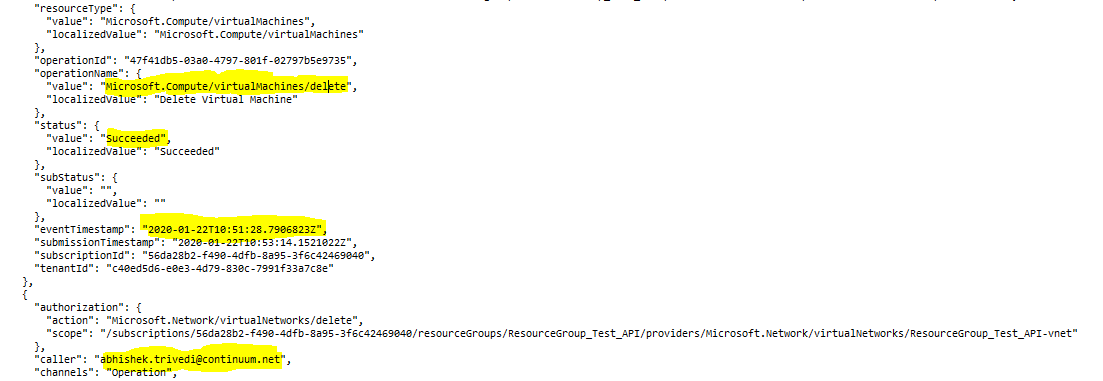
https://management.azure.com/subscriptions/56da28b2-f490-4dfb-8a95-3f6c42469040/providers/microsoft.insights/eventtypes/management/values?api-version=2015-04-01&eventTimestamp ge '01/20/2020 12:55:35' and resourceProvider eq 'Microsoft.Compute'

* Reference link:

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

* Alert will be triggered if **“operationName"** value is **"Microsoft.Compute/virtualMachines/delete”** **AND** **“status”** value is **“Succeeded”**.

**Sample Output from API:**



**Alert Details**

**Alert Category:** Virtual Machines

**Details required along with Alert:**

1. Subscription ID
2. Name of the VM.
3. Resource Group Name.
4. Account Name performing the action (caller).
5. Event time stamp.