# **Condition: Remove user permission from Azure resources**

**Condition**

**Description:**

* **What is Access control (IAM)?**

Access control (IAM) is the blade that use to assign roles. It's also known as identity and access management and appears in several locations in the Azure portal.

* **Who needs access?**

Who refers to a user, group, service principal, or managed identity. This is also called a *security principal*.

* **What role do they need?**

Permissions are grouped together into roles. You can select from a list of several [built-in roles](https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles) or you use your own custom roles.

* **Where do they need access?**

Where refers to the set of resources that the access applies to. Where can be a management group, subscription, resource group, or a single resource such as a storage account. This is called the *scope*.

* **Why need to Monitor Access Control:**

If any unauthorised user received permission on any Azure resource. Then particular user can make changes under that resource as per permission assigned.

**Impact:** With deletion of role assignment for a user, all permissions will be removed that a user has with respect to that role to access azure resources.

**Criticality:** Critical

**Frequency:** 15 Minutes

**Trigger Details**

**Trigger Condition:** Alert will be triggered if **“Microsoft.Authorization/roleAssignments/delete**” operation is succeeded.

**Method to capture trigger point:**

* REST API can be used to capture the activity logs either on the subscription level or on the resource level.
* 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}](https://management.azure.com/subscriptions/%7bsubscriptionId%7d/providers/microsoft.insights/eventtypes/management/values?api-version=2015-04-01&$filter=%7b$filter%7d)

**$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

&$filter=eventTimestamp ge '2015-01-21T20:00:00Z' and eventTimestamp le '2015-01-23T20:00:00Z'

* Reference link:

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

* Alert will be triggered if **“operationName”** value is **“Microsoft.Authorization/roleAssignments/delete”** **AND** **“status”** value is **“Succeeded”**.

Pull the Resource details (scope from where permissions are removed to access) like Virtual machine, NSG, storage account name etc. with the help of resourceId. In below sample API example, subscription id is the scope for which permission is removed.

**Sample Output from API:**

{

"authorization": {

"action": "Microsoft.Authorization/roleAssignments/delete",

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

},

"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": "1580982601",

"nbf": "1580982601",

"exp": "1580986501",

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

"aio": "AVQAq/8OAAAAoUqOStYHBFhk9yz5Grtu+i6PGw0pPP/8g6fUFXb+FHVYnog/79ts1LjGKpuKyOjGDQ2Il/GpiNto16xOcOCFnsbCvhmgZUp6QdgZhOsbjn8=",

"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": "unmzvSNoeE27mmN\_8jAMAA",

"ver": "1.0"

},

"correlationId": "1d2b21f2-b1a6-4e59-be88-ce244de7356d",

"description": "",

"eventDataId": "67d51db0-db9a-4de4-978d-b4acb2f55a34",

"eventName": {

"value": "EndRequest",

"localizedValue": "End request"

},

"category": {

"value": "Administrative",

"localizedValue": "Administrative"

},

"httpRequest": {

"clientRequestId": "b0b471a1-085d-4e9d-86ce-f6db89275007",

"clientIpAddress": "125.22.49.114",

"method": "DELETE"

},

"id": "/subscriptions/61e103f4-57ec-4f6a-a2f5-df2a28f98d19/providers/Microsoft.Authorization/roleAssignments/be743b46-bd5b-4b40-aeb9-8ba2aed69186/events/67d51db0-db9a-4de4-978d-b4acb2f55a34/ticks/637165806063015472",

"level": "Informational",

"resourceProviderName": {

"value": "Microsoft.Authorization",

"localizedValue": "Microsoft.Authorization"

},

"resourceId": "/subscriptions/61e103f4-57ec-4f6a-a2f5-df2a28f98d19/providers/Microsoft.Authorization/roleAssignments/be743b46-bd5b-4b40-aeb9-8ba2aed69186",

"resourceType": {

"value": "Microsoft.Authorization/roleAssignments",

"localizedValue": "Microsoft.Authorization/roleAssignments"

},

"operationId": "b9df9c03-1c5e-464c-8de5-12a99cddf349",

"operationName": {

"value": "Microsoft.Authorization/roleAssignments/delete",

"localizedValue": "Delete role assignment"

},

"properties": {

"statusCode": "OK",

"serviceRequestId": "af05c202-dd3b-4cf9-8ec8-7e3530da786d",

"responseBody": "{\"properties\":{\"roleDefinitionId\":\"/subscriptions/61e103f4-57ec-4f6a-a2f5-df2a28f98d19/providers/Microsoft.Authorization/roleDefinitions/b7e6dc6d-f1e8-4753-8033-0f276bb0955b\",\"principalId\":\"5c250555-5af4-4d7c-8c9f-ad9e2538a632\",\"principalType\":\"User\",\"scope\":\"/subscriptions/61e103f4-57ec-4f6a-a2f5-df2a28f98d19\",\"createdOn\":\"2020-02-06T07:17:10.8353392Z\",\"updatedOn\":\"2020-02-06T07:17:10.8353392Z\",\"createdBy\":\"b05b67a1-b710-4b11-bc69-23ee20de1d2f\",\"updatedBy\":\"b05b67a1-b710-4b11-bc69-23ee20de1d2f\"},\"id\":\"/subscriptions/61e103f4-57ec-4f6a-a2f5-df2a28f98d19/providers/Microsoft.Authorization/roleAssignments/be743b46-bd5b-4b40-aeb9-8ba2aed69186\",\"type\":\"Microsoft.Authorization/roleAssignments\",\"name\":\"be743b46-bd5b-4b40-aeb9-8ba2aed69186\"}"

},

"status": {

"value": "Succeeded",

"localizedValue": "Succeeded"

},

"subStatus": {

"value": "OK",

"localizedValue": "OK (HTTP Status Code: 200)"

},

"eventTimestamp": "2020-02-06T10:10:06.3015472Z",

"submissionTimestamp": "2020-02-06T10:12:05.2085682Z",

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

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

},

**Alert Details**

**Alert Category:** Security

**Details required along with Alert:**

1. Subscription ID
2. Account Name performing the action (caller).
3. Resource for which alert generated (resourceId).
4. Event time stamp (eventTimestamp).