View and retrieve Azure Activity log events

To view contributors to this article access the link below

https://docs.microsoft.com/en-us/azure/azure-monitor/platform/activity-log-view

In this article

1. Azure portal
2. Categories in the Activity log
3. View change history

The Azure Activity Log provides insight into subscription-level events that have occurred in Azure. This article provides details on different methods for viewing and retrieving Activity Log events.

Azure portal

View the Activity Log for all resources from the **Monitor** menu in the Azure portal. View the Activity Log for a particular resource from the **Activity Log** option in that resource's menu.

You can filter Activity Log events by the following fields:

- **Timespan**: The start and end time for events.
- **Category**: The event category as described in [Categories in the Activity Log](#).
- **Subscription**: One or more Azure subscription names.
- **Resource group**: One or more resource groups within the selected subscriptions.
- **Resource (name)**: - The name of a specific resource.
- **Resource type**: The type of resource, for example *Microsoft.Compute/virtualmachines*.

- **Operation name** - The name of an Azure Resource Manager operation, for example *Microsoft.SQL/servers/Write*.
- **Severity**: The severity level of the event. Available values are *Informational*, *Warning*, *Error*, *Critical*.
- **Event initiated by**: The user who performed the operation.
- **Open search**: Open text search box that searches for that string across all fields in all events.

Categories in the Activity log

Each event in the Activity Log has a particular category that are described in the following table. For full details on the schemata of these categories, see [Azure Activity Log event schema](#).

Table 1

Category	Description
	Contains the record of all create, update, delete, and action operations performed through Resource Manager. Examples of Administrative events include *create virtual machine* and *delete network security group*.
Administrative	Every action taken by a user or application using Resource Manager is modeled as an operation on a particular resource type. If the operation type is *Write*, *Delete*, or *Action*, the records of both the start and success or fail of that operation are recorded in the Administrative category. Administrative events also include any changes to role-based access control in a subscription.
	Contains the record of any service health incidents that have occurred in Azure. An example of a Service Health event *SQL Azure in East US is experiencing downtime*.
Service Health	Service Health events come in Six varieties: *Action Required*, *Assisted Recovery*, *Incident*, *Maintenance*, *Information*, or *Security*. These events are only created if you have a resource in the subscription that would be impacted by the event.
	Contains the record of any resource health events that have occurred to your Azure resources. An example of a Resource Health event is *Virtual Machine health status changed to unavailable*.
Resource Health	Resource Health events can represent one of four health statuses: *Available*, *Unavailable*, *Degraded*, and *Unknown*. Additionally, Resource Health events can be categorized as being *Platform Initiated* or *User Initiated*.
Alert	Contains the record of activations for Azure alerts. An example of an Alert event is *CPU % on myVM has been over 80 for the past 5 minutes*.
Autoscale	Contains the record of any events related to the operation of the autoscale engine based on any autoscale settings you have defined in your subscription. An example of an Autoscale event is *Autoscale scale up action failed*.

Table 1

Category	Description
Recommendation	Contains recommendation events from Azure Advisor.
Security	Contains the record of any alerts generated by Azure Security Center. An example of a Security event is *Suspicious double extension file executed*.
Policy	Contains records of all effect action operations performed by Azure Policy. Examples of Policy events include *Audit* and *Deny*. Every action taken by Policy is modeled as an operation on a resource.

View change history

When reviewing the Activity Log, it can help to see what changes happened during that event time. You can view this information with **Change history**. Select an event from the Activity Log you want to look deeper into. Select the **Change history (Preview)** tab to view any associated changes with that event.

Activity log

≣≣ Edit columns   ↻ Refresh   ⬆ Export to Event Hub

🔍 Search   ✕

(Management Group : **None**)   (Subscription : **2 selected**

First 88 items.

OPERATION NAME

▶ ℹ Create or Update Virtual Machine

⚠ Audit

▶ ℹ AuditIfNotExists

▶ ℹ AuditIfNotExists

If there are any associated changes with the event, you'll see a list of changes that you can select. This opens up the **Change history (Preview)** page. On this page you see the changes to the resource. As you can see from the following example, we are able to see not only that the VM changed sizes, but what the previous VM size was before the change and what it was changed to.

Change history (Preview)

⬡ View resource   ↗ View resource schema   ▤ Activity log

Resource name : WindowsVM1

Resource group : Default-Web-CentralUS

Selected change log	The following
Selected change log	
Tue, 4/23/2019, 5:05:19 PM	1 {
	2
(Timespan : **Last week**)	3
	4
CHANGE DETECTION TIME	5
	6
Tue, 4/23/2019, 5:05:19 PM	7
	8
Mon, 4/22/2019, 2:37:17 PM	9
	10
Wed, 4/17/2019, 9:49:18 PM	11
	12 –
	13
	14
	15