Azure Activity Log event schema

09/30/2020 • 25 minutes to read • +6

In this article

The Azure Activity log provides insight into any subscription-level events that have occurred in Azure. This article describes Activity log categories and the schema for each.

The schema will vary depending on how you access the log:

- The schemas described in this article are when you access the Activity log from the REST API. This is also the schema used when you select the **JSON** option when viewing an event in the Azure portal.
- See the final section Schema from storage account and event hubs for the schema when you use a diagnostic setting to send the Activity log to Azure Storage or Azure Event Hubs.
- See Azure Monitor data reference for the schema when you use a diagnostic setting to send the Activity log to a Log Analytics workspace.

Severity Level

Each entry in the activity log has a severity level. Severity level can have one of the following values:

Severity	Description
Critical	Events that demand the immediate attention of a system administrator. May indicate that an application or system has failed or stopped responding.
Error	Events that indicate a problem, but do not require immediate attention.
Warning	Events that provide forewarning of potential problems, although not an actual error. Indicate that a resource is not in an ideal state and may degrade later into showing errors or critical events.
Informational	Events that pass noncritical information to the administrator. Similar to a note that says: "For your information".

The devlopers of each resource provider choose the severity levels of their resource entries. As a result, the actual severity to you can vary depending on how your application is built. For example, items that are "critical" to a particular resource taken in isloation may not be as important as "errors" in a resource type that is central to your Azure application. Be sure to consider this fact when deciding what events to alert on.

Categories

Each event in the Activity Log has a particular category that are described in the following table. See the sections below for more detail on each category and its schema when you access the Activity log from the portal, PowerShell, CLI, and REST API. The schema is different when you stream the Activity log to storage or Event Hubs. A mapping of the properties to the resource logs schema is provided in the last section of the article.

Category	Description
Administrative	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*. 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 Azure role-based

Category	Description
	access control in a subscription.
Service Health	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 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.
Resource Health	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 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*.
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.

Administrative category

This category contains the record of all create, update, delete, and action operations performed through Resource Manager. Examples of the types of events you would see in this category include "create virtual machine" and "delete network security group" 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. The Administrative category also includes any changes to Azure role-based access control in a subscription.

Sample event

JSON

Copy

```
{
    "authorization": {
        "action": "Microsoft.Network/networkSecurityGroups/write",
        "scope": "/subscriptions/<subscription ID>/resourcegroups
/myResourceGroup/providers/Microsoft.Network/networkSecurityGroups/myNSG"
    },
    "caller": "rob@contoso.com",
    "channels": "Operation",
    "claims": {
        "aud": "https://management.core.windows.net/",
        "iss": "https://sts.windows.net/1114444b-7467-4144-a616-
e3a5d63e147b/",
        "iat": "1234567890",
        "nbf": "1234567890",
        "exp": "1234567890",
        "_claim_names": "{\"groups\":\"src1\"}",
        "_claim_sources": "{\"src1\":{\"endpoint
\":\"https://graph.microsoft.com/1114444b-7467-4144-a616-e3a5d63e147b/users
/f409edeb-4d29-44b5-9763-ee9348ad91bb/getMemberObjects\"}}",
        "http://schemas.microsoft.com/claims/authnclassreference": "1",
        "aio": "A3GgTJdwK4vy7Fa7l6DgJC2mI0GX44tML385OpU1Q+z+jaPnFMwB",
        "http://schemas.microsoft.com/claims/authnmethodsreferences":
"rsa,mfa",
        "appid": "355249ed-15d9-460d-8481-84026b065942",
        "appidacr": "2",
        "http://schemas.microsoft.com/2012/01/devicecontext/claims/identi-
fier": "10845a4d-ffa4-4b61-a3b4-e57b9b31cdb5",
        "e_exp": "262800",
        "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname":
"Robertson",
        "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname":
"Rob",
        "ipaddr": "111.111.1.111",
        "name": "Rob Robertson",
        "http://schemas.microsoft.com/identity/claims/objectidentifier": "f409edeb-4d29-44b5-9763-ee9348ad91bb",
        "onprem_sid": "S-1-5-21-4837261184-168309720-1886587427-18514304",
        "puid": "18247BBD84827C6D",
        "http://schemas.microsoft.com/identity/claims/scope": "user_impersonation",
        "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier": "b-24Jf94A3FH2sHWVIFqO3-RSJEiv24Jnif3gj7s",
        "http://schemas.microsoft.com/identity/claims/tenantid": "1114444b-7467-4144-a616-e3a5d63e147b",
        "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name": "rob@contoso.com",
        "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn": "rob@contoso.com",
        "uti": "IdP3SUJGtkGlt7dDQVRPAA",
        "ver": "1.0"
    },
    "correlationId": "b5768deb-836b-41cc-803e-3f4de2f9e40b",
    "eventDataId": "d0d36f97-b29c-4cd9-9d3d-ea2b92af3e9d",
    "eventName": {
        "value": "EndRequest",
        "localizedValue": "End request"
    },
    "category": {
        "value": "Administrative",
        "localizedValue": "Administrative"
    },
    "eventTimestamp": "2018-01-29T20:42:31.3810679Z",
    "id": "/subscriptions/<subscription ID>/resourcegroups/myResourceGroup/providers/Microsoft.Network/networkSecurityGroups/myNSG/events/d0d36f97-b29c-4cd9-9d3d-ea2b92af3e9d/ticks/636528553513810679",
    "level": "Informational",
    "operationId": "04e575f8-48d0-4c43-a8b3-78c4eb01d287",
    "operationName": {
        "value": "Microsoft.Network/networkSecurityGroups/write",
        "localizedValue": "Microsoft.Network/networkSecurityGroups/write"
    },
    "resourceGroupName": "myResourceGroup",
    "resourceProviderName": {
        "value": "Microsoft.Network",
        "localizedValue": "Microsoft.Network"
    },
    "resourceType": {
        "value": "Microsoft.Network/networkSecurityGroups",
        "localizedValue": "Microsoft.Network/networkSecurityGroups"
    },
    "resourceId": "/subscriptions/<subscription ID>/resourcegroups/myResourceGroup/providers/Microsoft.Network/networkSecurityGroups/myNSG",
    "status": {
        "value": "Succeeded",
        "localizedValue": "Succeeded"
    },
    "subStatus": {
        "value": "",
        "localizedValue": ""
    },
    "submissionTimestamp": "2018-01-29T20:42:50.0724829Z",
    "subscriptionId": "<subscription ID>",
    "properties": {
        "statusCode": "Created",
        "serviceRequestId": "a4c11dbd-697e-47c5-9663-12362307157d",
        "responseBody": "",
        "requestbody": ""
    },
    "relatedEvents": []
}
```

Property descriptions

Element Name	Description
authorization	Blob of Azure RBAC properties of the event. Usually includes the “action”, “role” and “scope” properties.
caller	Email address of the user who has performed the operation, UPN claim, or SPN claim based on availability.
channels	One of the following values: “Admin”, “Operation”
claims	The JWT token used by Active Directory to authenticate the user or application to perform this operation in Resource Manager.
correlationId	Usually a GUID in the string format. Events that share a correlationId belong to the same uber action.
description	Static text description of an event.
eventDataId	Unique identifier of an event.
eventName	Friendly name of the Administrative event.

Element Name	Description
category	Always "Administrative"
httpRequest	Blob describing the Http Request. Usually includes the “clientRequestId”, “clientIpAddress” and “method” (HTTP method. For example, PUT).
level	Level of the event. One of the following values: “Critical”, “Error”, “Warning”, and “Informational”
resourceGroupName	Name of the resource group for the impacted resource.
resourceProviderName	Name of the resource provider for the impacted resource
resourceType	The type of resource that was affected by an Administrative event.
resourceId	Resource ID of the impacted resource.
operationId	A GUID shared among the events that correspond to a single operation.
operationName	Name of the operation.
properties	Set of `<Key, Value>` pairs (that is, a Dictionary) describing the details of the event.
status	String describing the status of the operation. Some common values are: Started, In Progress, Succeeded, Failed, Active, Resolved.
subStatus	Usually the HTTP status code of the corresponding REST call, but can also include other strings describing a substatus, such as these common values: OK (HTTP Status Code: 200), Created (HTTP Status Code: 201), Accepted (HTTP Status Code: 202), No Content (HTTP Status Code: 204), Bad Request (HTTP Status Code: 400), Not Found (HTTP Status Code: 404), Conflict (HTTP Status Code: 409), Internal Server Error (HTTP Status Code: 500), Service Unavailable (HTTP Status Code: 503), Gateway Timeout (HTTP Status Code: 504).
eventTimestamp	Timestamp when the event was generated by the Azure service processing the request corresponding the event.

Element Name	Description
submissionTimestamp	Timestamp when the event became available for querying.
subscriptionId	Azure Subscription ID.

Service health category

This category contains the record of any service health incidents that have occurred in Azure. An example of the type of event you would see in this category is "SQL Azure in East US is experiencing downtime." Service health events come in five varieties: Action Required, Assisted Recovery, Incident, Maintenance, Information, or Security, and only appear if you have a resource in the subscription that would be impacted by the event.

Sample event

JSON Copy

```json
{
  "channels": "Admin",
  "correlationId": "c550176b-8f52-4380-bdc5-36c1b59d3a44",
  "description": "Active: Network Infrastructure - UK South",
  "eventDataId": "c5bc4514-6642-2be3-453e-c6a67841b073",
  "eventName": {
      "value": null
  },
  "category": {
      "value": "ServiceHealth",
      "localizedValue": "Service Health"
  },
  "eventTimestamp": "2017-07-20T23:30:14.8022297Z",
  "id": "/subscriptions/<subscription ID>/events/c5bc4514-6642-2be3-453e-
c6a67841b073/ticks/636361902148022297",
  "level": "Warning",
  "operationName": {
      "value": "Microsoft.ServiceHealth/incident/action",
      "localizedValue": "Microsoft.ServiceHealth/incident/action"
  },
  "resourceProviderName": {
      "value": null
  },
  "resourceType": {
      "value": null,
      "localizedValue": ""
  },
  "resourceId": "/subscriptions/<subscription ID>",
  "status": {
      "value": "Active",
      "localizedValue": "Active"
  },
  "subStatus": {
      "value": null
  },
  "submissionTimestamp": "2017-07-20T23:30:34.7431946Z",
  "subscriptionId": "<subscription ID>",
  "properties": {
    "title": "Network Infrastructure - UK South",
    "service": "Service Fabric",
    "region": "UK South",
    "communication": "Starting at approximately 21:41 UTC on 20 Jul 2017, a subset of customers in UK South may experience degraded performance, connectivity drops or timeouts when accessing their Azure resources hosted in this region. Engineers are investigating underlying Network Infrastructure issues in this region. Impacted services may include, but are not limited to App Services, Automation, Service Bus, Log Analytics, Key Vault, SQL Database, Service Fabric, Event Hubs, Stream Analytics, Azure Data Movement, API Management, and Azure Cognitive Search. Multiple engineering teams are engaged in multiple workflows to mitigate the impact. The next update will be provided in 60 minutes, or as events warrant.",
    "incidentType": "Incident",
    "trackingId": "NA0F-BJG",
    "impactStartTime": "2017-07-20T21:41:00.0000000Z",
    "impactedServices": "[{\"ImpactedRegions\":[{\"RegionName\":\"UK South\"}],\"ServiceName\":\"Service Fabric\"}]",
    "defaultLanguageTitle": "Network Infrastructure - UK South",
    "defaultLanguageContent": "Starting at approximately 21:41 UTC on 20 Jul 2017, a subset of customers in UK South may experience degraded performance, connectivity drops or timeouts when accessing their Azure resources hosted in this region. Engineers are investigating underlying Network Infrastructure issues in this region. Impacted services may include, but are not limited to App Services, Automation, Service Bus, Log Analytics, Key Vault, SQL Database, Service Fabric, Event Hubs, Stream Analytics, Azure Data Movement, API Management, and Azure Cognitive Search. Multiple engineering teams are engaged in multiple workflows to mitigate the impact. The next update will be provided in 60 minutes, or as events warrant.",
    "stage": "Active",
    "communicationId": "636361902146035247",
    "version": "0.1.1"
  }
}
```

Refer to the service health notifications article for documentation about the values in the properties.

Resource health category

This category contains the record of any resource health events that have occurred to your Azure resources. An example of the type of event you would see in this category is "Virtual Machine health status changed to unavailable." 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.

Sample event

JSON Copy

```json
{
    "channels": "Admin, Operation",
    "correlationId": "28f1bfae-56d3-7urb-bff4-194d261248e9",
    "description": "",
    "eventDataId": "a80024e1-883d-37ur-8b01-7591a1befccb",
    "eventName": {
        "value": "",
        "localizedValue": ""
    },
    "category": {
        "value": "ResourceHealth",
        "localizedValue": "Resource Health"
    },
    "eventTimestamp": "2018-09-04T15:33:43.65Z",
    "id": "/subscriptions/<subscription ID>/resourceGroups/<resource
group>/providers/Microsoft.Compute/virtualMachines/<resource name>/events
/a80024e1-883d-42a5-8b01-7591a1befccb/ticks/636716720236500000",
    "level": "Critical",
    "operationId": "",
    "operationName": {
        "value": "Microsoft.Resourcehealth/healthevent/Activated/action",
        "localizedValue": "Health Event Activated"
    },
    "resourceGroupName": "<resource group>",
    "resourceProviderName": {
        "value": "Microsoft.Resourcehealth/healthevent/action",
        "localizedValue": "Microsoft.Resourcehealth/healthevent/action"
    },
    "resourceType": {
        "value": "Microsoft.Compute/virtualMachines",
        "localizedValue": "Microsoft.Compute/virtualMachines"
    },
    "resourceId": "/subscriptions/<subscription ID>/resourceGroups/<resource group>/providers/Microsoft.Compute/virtualMachines/<resource name>",
    "status": {
        "value": "Active",
        "localizedValue": "Active"
    },
    "subStatus": {
        "value": "",
        "localizedValue": ""
    },
    "submissionTimestamp": "2018-09-04T15:36:24.2240867Z",
    "subscriptionId": "<subscription ID>",
    "properties": {
        "stage": "Active",
        "title": "Virtual Machine health status changed to unavailable",
        "details": "Virtual machine has experienced an unexpected event",
        "healthStatus": "Unavailable",
        "healthEventType": "Downtime",
        "healthEventCause": "PlatformInitiated",
        "healthEventCategory": "Unplanned"
    },
    "relatedEvents": []
}
```

Property descriptions

Element Name	Description
channels	Always “Admin, Operation”
correlationId	A GUID in the string format.
description	Static text description of the alert event.
eventDataId	Unique identifier of the alert event.
category	Always "ResourceHealth"
eventTimestamp	Timestamp when the event was generated by the Azure service processing the request corresponding the event.

Element Name	Description
level	Level of the event. One of the following values: “Critical”, ”Error”, ”Warning”, ”Informational”, and ”Verbose”
operationId	A GUID shared among the events that correspond to a single operation.
operationName	Name of the operation.
resourceGroupName	Name of the resource group that contains the resource.
resourceProviderName	Always "Microsoft.Resourcehealth/healthevent/action".
resourceType	The type of resource that was affected by a Resource Health event.
resourceId	Name of the resource ID for the impacted resource.
status	String describing the status of the health event. Values can be: Active, Resolved, InProgress, Updated.
subStatus	Usually null for alerts.
submissionTimestamp	Timestamp when the event became available for querying.
subscriptionId	Azure Subscription ID.
properties	Set of `<Key, Value>` pairs (that is, a Dictionary) describing the details of the event.
properties.title	A user-friendly string that describes the health status of the resource.
properties.details	A user-friendly string that describes further details about the event.
properties.currentHealthStatus	The current health status of the resource. One of the following values: "Available", "Unavailable", "Degraded", and "Unknown".

Element Name	Description
properties.previousHealthStatus	The previous health status of the resource. One of the following values: "Available", "Unavailable", "Degraded", and "Unknown".
properties.type	A description of the type of resource health event.
properties.cause	A description of the cause of the resource health event. Either "UserInitiated" and "PlatformInitiated".

Alert category

This category contains the record of all activations of classic Azure alerts. An example of the type of event you would see in this category is "CPU % on myVM has been over 80 for the past 5 minutes." A variety of Azure systems have an alerting concept -- you can define a rule of some sort and receive a notification when conditions match that rule. Each time a supported Azure alert type 'activates,' or the conditions are met to generate a notification, a record of the activation is also pushed to this category of the Activity Log.

Sample event

JSON Copy

```json
{
  "caller": "Microsoft.Insights/alertRules",
  "channels": "Admin, Operation",
  "claims": {
    "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/spn":
"Microsoft.Insights/alertRules"
  },
  "correlationId": "/subscriptions/<subscription ID>/resourceGroups
/myResourceGroup/providers/microsoft.insights/alertrules/myalert/incidents
/L3N1YnNjcmlwdGlvbnMvZGY2MDJjOWMtN2FhMC00MDdkLWE2ZmItZWIyMGM4YmQxMTkyL3Jlc29
1cmNlR3JvdXBzL0NzbUV2ZW50RE9HRk9PRC1XZXN0VVMvcHJvdmlkZXJzL21pY3Jvc29mdC5pbnN
pZ2h0cy9hbGVydHJ1bGVzL215YWxlcnQwNjM2MzYyMjU4NTM1MjIxOTIw",
  "description": "'Disk read LessThan 100000 ([Count]) in the last 5 min-
utes' has been resolved for CloudService: myResourceGroup/Production
/Event.BackgroundJobsWorker.razzle (myResourceGroup)",
  "eventDataId": "149d4baf-53dc-4cf4-9e29-17de37405cd9",
  "eventName": {
    "value": "Alert",
    "localizedValue": "Alert"
  },
  "category": {
    "value": "Alert",
    "localizedValue": "Alert"
  },
  "id": "/subscriptions/<subscription ID>/resourceGroups/myResourceGroup
/providers/Microsoft.ClassicCompute/domainNames/myResourceGroup/slots
/Production/roles/Event.BackgroundJobsWorker.razzle/events/149d4baf-
53dc-4cf4-9e29-17de37405cd9/ticks/636362258535221920",
  "level": "Informational",
  "resourceGroupName": "myResourceGroup",
  "resourceProviderName": {
    "value": "Microsoft.ClassicCompute",
    "localizedValue": "Microsoft.ClassicCompute"
  },
  "resourceId": "/subscriptions/<subscription ID>/resourceGroups
/myResourceGroup/providers/Microsoft.ClassicCompute/domainNames
/myResourceGroup/slots/Production/roles/Event.BackgroundJobsWorker.razzle",
  "resourceType": {
    "value": "Microsoft.ClassicCompute/domainNames/slots/roles",
    "localizedValue": "Microsoft.ClassicCompute/domainNames/slots/roles"
  },
  "operationId": "/subscriptions/<subscription ID>/resourceGroups
/myResourceGroup/providers/microsoft.insights/alertrules/myalert/incidents
/L3N1YnNjcmlwdGlvbnMvZGY2MDJjOWMtN2FhMC00MDdkLWE2ZmItZWIyMGM4YmQxMTkyL3Jlc29
1cmNlR3JvdXBzL0NzbUV2ZW50RE9HRk9PRC1XZXN0VVMvcHJvdmlkZXJzL21pY3Jvc29mdC5pbnN
pZ2h0cy9hbGVydHJ1bGVzL215YWxlcnQwNjM2MzYyMjU4NTM1MjIxOTIw",
  "operationName": {
    "value": "Microsoft.Insights/AlertRules/Resolved/Action",
    "localizedValue": "Microsoft.Insights/AlertRules/Resolved/Action"
  },
  "properties": {
    "RuleUri": "/subscriptions/<subscription ID>/resourceGroups
/myResourceGroup/providers/microsoft.insights/alertrules/myalert",
    "RuleName": "myalert",
    "RuleDescription": "",
    "Threshold": "100000",
    "WindowSizeInMinutes": "5",
    "Aggregation": "Average",
    "Operator": "LessThan",
    "MetricName": "Disk read",
    "MetricUnit": "Count"
  },
  "status": {
    "value": "Resolved",
    "localizedValue": "Resolved"
  },
  "subStatus": {
    "value": null
  },
  "eventTimestamp": "2017-07-21T09:24:13.522192Z",
  "submissionTimestamp": "2017-07-21T09:24:15.6578651Z",
  "subscriptionId": "<subscription ID>"
}
```

Property descriptions

Element Name	Description
caller	Always Microsoft.Insights/alertRules
channels	Always “Admin, Operation”
claims	JSON blob with the SPN (service principal name), or resource type, of the alert engine.
correlationId	A GUID in the string format.
description	Static text description of the alert event.
eventDataId	Unique identifier of the alert event.
category	Always "Alert"
level	Level of the event. One of the following values: “Critical”, “Error”, “Warning”, and “Informational”
resourceGroupName	Name of the resource group for the impacted resource if it is a metric alert. For other alert types, it is the name of the resource group that contains the alert itself.
resourceProviderName	Name of the resource provider for the impacted resource if it is a metric alert. For other alert types, it is the name of the resource provider for the alert itself.
resourceId	Name of the resource ID for the impacted resource if it is a metric alert. For other alert types, it is the resource ID of the alert resource itself.

Element Name	Description
operationId	A GUID shared among the events that correspond to a single operation.
operationName	Name of the operation.
properties	Set of `<Key, Value>` pairs (that is, a Dictionary) describing the details of the event.
status	String describing the status of the operation. Some common values are: Started, In Progress, Succeeded, Failed, Active, Resolved.
subStatus	Usually null for alerts.
eventTimestamp	Timestamp when the event was generated by the Azure service processing the request corresponding the event.
submissionTimestamp	Timestamp when the event became available for querying.
subscriptionId	Azure Subscription ID.

Properties field per alert type

The properties field will contain different values depending on the source of the alert event. Two common alert event providers are Activity Log alerts and metric alerts.

Properties for Activity Log alerts

Element Name	Description
properties.subscriptionId	The subscription ID from the activity log event which caused this activity log alert rule to be activated.
properties.eventDataId	The event data ID from the activity log event which caused this activity log alert rule to be activated.
properties.resourceGroup	The resource group from the activity log event which caused this activity log alert rule to be activated.

Element Name	Description
properties.resourceId	The resource ID from the activity log event which caused this activity log alert rule to be activated.
properties.eventTimestamp	The event timestamp of the activity log event which caused this activity log alert rule to be activated.
properties.operationName	The operation name from the activity log event which caused this activity log alert rule to be activated.
properties.status	The status from the activity log event which caused this activity log alert rule to be activated.

Properties for metric alerts

Element Name	Description
properties.RuleUri	Resource ID of the metric alert rule itself.
properties.RuleName	The name of the metric alert rule.
properties.RuleDescription	The description of the metric alert rule (as defined in the alert rule).
properties.Threshold	The threshold value used in the evaluation of the metric alert rule.
properties.WindowSizeInMinutes	The window size used in the evaluation of the metric alert rule.
properties.Aggregation	The aggregation type defined in the metric alert rule.
properties.Operator	The conditional operator used in the evaluation of the metric alert rule.
properties.MetricName	The metric name of the metric used in the evaluation of the metric alert rule.

Element Name	Description
properties.MetricUnit	The metric unit for the metric used in the evaluation of the metric alert rule.

Autoscale category

This category 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 the type of event you would see in this category is "Autoscale scale up action failed." Using autoscale, you can automatically scale out or scale in the number of instances in a supported resource type based on time of day and/or load (metric) data using an autoscale setting. When the conditions are met to scale up or down, the start and succeeded or failed events will be recorded in this category.

Sample event

JSON

Copy

```json
{
  "caller": "Microsoft.Insights/autoscaleSettings",
  "channels": "Admin, Operation",
  "claims": {
    "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/spn":
"Microsoft.Insights/autoscaleSettings"
  },
  "correlationId": "fc6a7ff5-ff68-4bb7-81b4-3629212d03d0",
  "description": "The autoscale engine attempting to scale resource '/sub-
scriptions/<subscription ID>/resourceGroups/myResourceGroup/providers
/Microsoft.ClassicCompute/domainNames/myResourceGroup/slots/Production/roles
/myResource' from 3 instances count to 2 instances count.",
  "eventDataId": "a5b92075-1de9-42f1-b52e-6f3e4945a7c7",
  "eventName": {
    "value": "AutoscaleAction",
    "localizedValue": "AutoscaleAction"
  },
  "category": {
    "value": "Autoscale",
    "localizedValue": "Autoscale"
  },
  "id": "/subscriptions/<subscription ID>/resourceGroups/myResourceGroup
/providers/microsoft.insights/autoscalesettings/myResourceGroup-Production-
myResource-myResourceGroup/events/a5b92075-1de9-42f1-b52e-6f3e4945a7c7/ticks
/636361956518681572",
  "level": "Informational",
  "resourceGroupName": "myResourceGroup",
  "resourceProviderName": {
    "value": "microsoft.insights",
    "localizedValue": "microsoft.insights"
  },
  "resourceId": "/subscriptions/<subscription ID>/resourceGroups
/myResourceGroup/providers/microsoft.insights/autoscalesettings
/myResourceGroup-Production-myResource-myResourceGroup",
  "resourceType": {
    "value": "microsoft.insights/autoscalesettings",
    "localizedValue": "microsoft.insights/autoscalesettings"
  },
  "operationId": "fc6a7ff5-ff68-4bb7-81b4-3629212d03d0",
  "operationName": {
    "value": "Microsoft.Insights/AutoscaleSettings/Scaledown/Action",
    "localizedValue": "Microsoft.Insights/AutoscaleSettings/Scaledown
/Action"
  },
  "properties": {
    "Description": "The autoscale engine attempting to scale resource '/sub-
scriptions/<subscription ID>/resourceGroups/myResourceGroup/providers
/Microsoft.ClassicCompute/domainNames/myResourceGroup/slots/Production/roles
/myResource' from 3 instances count to 2 instances count.",
    "ResourceName": "/subscriptions/<subscription ID>/resourceGroups
/myResourceGroup/providers/Microsoft.ClassicCompute/domainNames
/myResourceGroup/slots/Production/roles/myResource",
    "OldInstancesCount": "3",
    "NewInstancesCount": "2",
    "LastScaleActionTime": "Fri, 21 Jul 2017 01:00:51 GMT"
  },
  "status": {
    "value": "Succeeded",
    "localizedValue": "Succeeded"
  },
  "subStatus": {
    "value": null
  },
  "eventTimestamp": "2017-07-21T01:00:51.8681572Z",
  "submissionTimestamp": "2017-07-21T01:00:52.3008754Z",
  "subscriptionId": "<subscription ID>"
}
```

Property descriptions

Element Name	Description
caller	Always Microsoft.Insights/autoscaleSettings
channels	Always “Admin, Operation”
claims	JSON blob with the SPN (service principal name), or resource type, of the autoscale engine.
correlationId	A GUID in the string format.
description	Static text description of the autoscale event.
eventDataId	Unique identifier of the autoscale event.
level	Level of the event. One of the following values: “Critical”, “Error”, “Warning”, and “Informational”
resourceGroupName	Name of the resource group for the autoscale setting.
resourceProviderName	Name of the resource provider for the autoscale setting.
resourceId	Resource ID of the autoscale setting.
operationId	A GUID shared among the events that correspond to a single operation.
operationName	Name of the operation.
properties	Set of `<Key, Value>` pairs (that is, a Dictionary) describing the details of the event.
properties.Description	Detailed description of what the autoscale engine was doing.
properties.ResourceName	Resource ID of the impacted resource (the resource on which the scale action was being performed)
properties.OldInstancesCount	The number of instances before the autoscale action took effect.

Element Name	Description
properties.NewInstancesCount	The number of instances after the autoscale action took effect.
properties.LastScaleActionTime	The timestamp of when the autoscale action occurred.
status	String describing the status of the operation. Some common values are: Started, In Progress, Succeeded, Failed, Active, Resolved.
subStatus	Usually null for autoscale.
eventTimestamp	Timestamp when the event was generated by the Azure service processing the request corresponding the event.
submissionTimestamp	Timestamp when the event became available for querying.
subscriptionId	Azure Subscription ID.

Security category

This category contains the record any alerts generated by Azure Security Center. An example of the type of event you would see in this category is "Suspicious double extension file executed."

Sample event

JSON Copy

```json
{
    "channels": "Operation",
    "correlationId": "965d6c6a-a790-4a7e-8e9a-41771b3fbc38",
    "description": "Suspicious double extension file executed. Machine logs
indicate an execution of a process with a suspicious double extension.\r
\nThis extension may trick users into thinking files are safe to be opened
and might indicate the presence of malware on the system.",
    "eventDataId": "965d6c6a-a790-4a7e-8e9a-41771b3fbc38",
    "eventName": {
        "value": "Suspicious double extension file executed",
        "localizedValue": "Suspicious double extension file executed"
    },
    "category": {
        "value": "Security",
        "localizedValue": "Security"
    },
    "eventTimestamp": "2017-10-18T06:02:18.6179339Z",
    "id": "/subscriptions/<subscription ID>/providers/Microsoft.Security/locations/centralus/alerts/965d6c6a-a790-4a7e-8e9a-41771b3fbc38/events/965d6c6a-a790-4a7e-8e9a-41771b3fbc38/ticks/636439033386179339",
    "level": "Informational",
    "operationId": "965d6c6a-a790-4a7e-8e9a-41771b3fbc38",
    "operationName": {
        "value": "Microsoft.Security/locations/alerts/activate/action",
        "localizedValue": "Microsoft.Security/locations/alerts/activate/action"
    },
    "resourceGroupName": "myResourceGroup",
    "resourceProviderName": {
        "value": "Microsoft.Security",
        "localizedValue": "Microsoft.Security"
    },
    "resourceType": {
        "value": "Microsoft.Security/locations/alerts",
        "localizedValue": "Microsoft.Security/locations/alerts"
    },
    "resourceId": "/subscriptions/<subscription ID>/providers/Microsoft.Security/locations/centralus/alerts/2518939942613820660_a48f8653-3fc6-4166-9f19-914f030a13d3",
    "status": {
        "value": "Active",
        "localizedValue": "Active"
    },
    "subStatus": {
        "value": null
    },
    "submissionTimestamp": "2017-10-18T06:02:52.2176969Z",
    "subscriptionId": "<subscription ID>",
    "properties": {
        "accountLogonId": "0x2r4",
        "commandLine": "c:\\mydirectory\\doubleetension.pdf.exe",
        "domainName": "hpc",
        "parentProcess": "unknown",
        "parentProcess id": "0",
        "processId": "6988",
        "processName": "c:\\mydirectory\\doubleetension.pdf.exe",
        "userName": "myUser",
        "UserSID": "S-3-2-12",
        "ActionTaken": "Detected",
        "Severity": "High"
    },
    "relatedEvents": []
}
```

Property descriptions

Element Name	Description
channels	Always “Operation”
correlationId	A GUID in the string format.
description	Static text description of the security event.
eventDataId	Unique identifier of the security event.
eventName	Friendly name of the security event.
category	Always "Security"
ID	Unique resource identifier of the security event.
level	Level of the event. One of the following values: “Critical”, “Error”, “Warning”, or “Informational”
resourceGroupName	Name of the resource group for the resource.
resourceProviderName	Name of the resource provider for Azure Security Center. Always "Microsoft.Security".
resourceType	The type of resource that generated the security event, such as "Microsoft.Security/locations/alerts"
resourceId	Resource ID of the security alert.
operationId	A GUID shared among the events that correspond to a single operation.
operationName	Name of the operation.

Element Name	Description
properties	Set of `<Key, Value>` pairs (that is, a Dictionary) describing the details of the event. These properties will vary depending on the type of security alert. See this page for a description of the types of alerts that come from Security Center.
properties.Severity	The severity level. Possible values are "High," "Medium," or "Low."
status	String describing the status of the operation. Some common values are: Started, In Progress, Succeeded, Failed, Active, Resolved.
subStatus	Usually null for security events.
eventTimestamp	Timestamp when the event was generated by the Azure service processing the request corresponding the event.
submissionTimestamp	Timestamp when the event became available for querying.
subscriptionId	Azure Subscription ID.

Recommendation category

This category contains the record of any new recommendations that are generated for your services. An example of a recommendation would be "Use availability sets for improved fault tolerance." There are four types of Recommendation events that can be generated: High Availability, Performance, Security, and Cost Optimization.

Sample event

JSON

```json
{
    "channels": "Operation",
    "correlationId": "92481dfd-c5bf-4752-b0d6-0ecddaa64776",
    "description": "The action was successful.",
    "eventDataId": "06cb0e44-111b-47c7-a4f2-aa3ee320c9c5",
    "eventName": {
        "value": "",
        "localizedValue": ""
    },
    "category": {
        "value": "Recommendation",
        "localizedValue": "Recommendation"
    },
    "eventTimestamp": "2018-06-07T21:30:42.976919Z",
    "id": "/SUBSCRIPTIONS/<Subscription ID>/RESOURCEGROUPS/MYRESOURCEGROUP
/PROVIDERS/MICROSOFT.COMPUTE/VIRTUALMACHINES/MYVM/events/06cb0e44-111b-47c7-
a4f2-aa3ee320c9c5/ticks/636640038429769190",
    "level": "Informational",
    "operationId": "",
    "operationName": {
        "value": "Microsoft.Advisor/generateRecommendations/action",
        "localizedValue": "Microsoft.Advisor/generateRecommendations/action"
    },
    "resourceGroupName": "MYRESOURCEGROUP",
    "resourceProviderName": {
        "value": "MICROSOFT.COMPUTE",
        "localizedValue": "MICROSOFT.COMPUTE"
    },
    "resourceType": {
        "value": "MICROSOFT.COMPUTE/virtualmachines",
        "localizedValue": "MICROSOFT.COMPUTE/virtualmachines"
    },
    "resourceId": "/SUBSCRIPTIONS/<Subscription ID>/RESOURCEGROUPS
/MYRESOURCEGROUP/PROVIDERS/MICROSOFT.COMPUTE/VIRTUALMACHINES/MYVM",
    "status": {
        "value": "Active",
        "localizedValue": "Active"
    },
    "subStatus": {
        "value": "",
        "localizedValue": ""
    },
    "submissionTimestamp": "2018-06-07T21:30:42.976919Z",
    "subscriptionId": "<Subscription ID>",
    "properties": {
        "recommendationSchemaVersion": "1.0",
        "recommendationCategory": "Security",
        "recommendationImpact": "High",
        "recommendationRisk": "None"
    },
    "relatedEvents": []
}
```

Property descriptions

Element Name	Description
channels	Always “Operation”
correlationId	A GUID in the string format.
description	Static text description of the recommendation event
eventDataId	Unique identifier of the recommendation event.
category	Always "Recommendation"
ID	Unique resource identifier of the recommendation event.
level	Level of the event. One of the following values: “Critical”, “Error”, “Warning”, or “Informational”
operationName	Name of the operation. Always "Microsoft.Advisor/generateRecommendations/action"
resourceGroupName	Name of the resource group for the resource.
resourceProviderName	Name of the resource provider for the resource that this recommendation applies to, such as "MICROSOFT.COMPUTE"
resourceType	Name of the resource type for the resource that this recommendation applies to, such as "MICROSOFT.COMPUTE/virtualmachines"
resourceId	Resource ID of the resource that the recommendation applies to
status	Always "Active"
submissionTimestamp	Timestamp when the event became available for querying.

Element Name	Description
subscriptionId	Azure Subscription ID.
properties	Set of `<Key, Value>` pairs (that is, a Dictionary) describing the details of the recommendation.
properties.recommendationSchemaVersion	Schema version of the recommendation properties published in the Activity Log entry
properties.recommendationCategory	Category of the recommendation. Possible values are "High Availability", "Performance", "Security", and "Cost"
properties.recommendationImpact	Impact of the recommendation. Possible values are "High", "Medium", "Low"
properties.recommendationRisk	Risk of the recommendation. Possible values are "Error", "Warning", "None"

Policy category

This category contains records of all effect action operations performed by Azure Policy. Examples of the types of events you would see in this category include *Audit* and *Deny*. Every action taken by Policy is modeled as an operation on a resource.

Sample Policy event

JSON Copy

```json
{
    "authorization": {
        "action": "Microsoft.Resources/checkPolicyCompliance/read",
        "scope": "/subscriptions/<subscriptionID>"
    },
    "caller": "33a68b9d-63ce-484c-a97e-94aef4c89648",
    "channels": "Operation",
    "claims": {
        "aud": "https://management.azure.com/",
        "iss": "https://sts.windows.net/1114444b-7467-4144-a616-e3a5d63e147b/",
        "iat": "1234567890",
        "nbf": "1234567890",
        "exp": "1234567890",
        "aio": "A3GgTJdwK4vy7Fa7l6DgJC2mI0GX44tML385OpU1Q+z+jaPnFMwB",
        "appid": "1d78a85d-813d-46f0-b496-dd72f50a3ec0",
        "appidacr": "2",
        "http://schemas.microsoft.com/identity/claims/identityprovider": "https://sts.windows.net/1114444b-7467-4144-a616-e3a5d63e147b/",
        "http://schemas.microsoft.com/identity/claims/objectidentifier": "f409edeb-4d29-44b5-9763-ee9348ad91bb",
        "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier": "b-24Jf94A3FH2sHWVIFqO3-RSJEiv24Jnif3gj7s",
        "http://schemas.microsoft.com/identity/claims/tenantid": "1114444b-7467-4144-a616-e3a5d63e147b",
        "uti": "IdP3SUJGtkGlt7dDQVRPAA",
        "ver": "1.0"
    },
    "correlationId": "b5768deb-836b-41cc-803e-3f4de2f9e40b",
    "description": "",
    "eventDataId": "d0d36f97-b29c-4cd9-9d3d-ea2b92af3e9d",
    "eventName": {
        "value": "EndRequest",
        "localizedValue": "End request"
    },
    "category": {
        "value": "Policy",
        "localizedValue": "Policy"
    },
    "eventTimestamp": "2019-01-15T13:19:56.1227642Z",
    "id": "/subscriptions/<subscriptionID>/resourceGroups/myResourceGroup/providers/Microsoft.Sql/servers/contososqlpolicy/events/13bbf75f-36d5-4e66-b693-725267ff21ce/ticks/636831551961227642",
    "level": "Warning",
    "operationId": "04e575f8-48d0-4c43-a8b3-78c4eb01d287",
    "operationName": {
        "value": "Microsoft.Authorization/policies/audit/action",
        "localizedValue": "Microsoft.Authorization/policies/audit/action"
    },
    "resourceGroupName": "myResourceGroup",
    "resourceProviderName": {
        "value": "Microsoft.Sql",
        "localizedValue": "Microsoft SQL"
    },
    "resourceType": {
        "value": "Microsoft.Resources/checkPolicyCompliance",
        "localizedValue": "Microsoft.Resources/checkPolicyCompliance"
    },
    "resourceId": "/subscriptions/<subscriptionID>/resourceGroups/myResourceGroup/providers/Microsoft.Sql/servers/contososqlpolicy",
    "status": {
        "value": "Succeeded",
        "localizedValue": "Succeeded"
    },
    "subStatus": {
        "value": "",
        "localizedValue": ""
    },
    "submissionTimestamp": "2019-01-15T13:20:17.1077672Z",
    "subscriptionId": "<subscriptionID>",
    "properties": {
        "isComplianceCheck": "True",
        "resourceLocation": "westus2",
        "ancestors": "72f988bf-86f1-41af-91ab-2d7cd011db47",
        "policies": "[{\"policyDefinitionId\":\"/subscriptions
/<subscriptionID>/providers/Microsoft.
            Authorization/policyDefinitions/5775cdd5-d3d3-47bf-bc55-
bb8b61746506/\",\"policyDefiniti
            onName\":\"5775cdd5-d3d3-47bf-bc55-bb8b61746506
\",\"policyDefinitionEffect\":\"Deny\",\"
            policyAssignmentId\":\"/subscriptions/<subscriptionID>/providers
/Microsoft.Authorization
            /policyAssignments/991a69402a6c484cb0f9b673
/\",\"policyAssignmentName\":\"991a69402a6c48
            4cb0f9b673\",\"policyAssignmentScope\":\"/subscriptions
/<subscriptionID>\",\"policyAssig
            nmentParameters\":{}}]"
    },
    "relatedEvents": []
}
```

Policy event property descriptions

Element Name	Description
authorization	Array of Azure RBAC properties of the event. For new resources, this is the action and scope of the request that triggered evaluation. For existing resources, the action is "Microsoft.Resources/checkPolicyCompliance/read".
caller	For new resources, the identity that initiated a deployment. For existing resources, the GUID of the Microsoft Azure Policy Insights RP.
channels	Policy events use only the "Operation" channel.

Element Name	Description
claims	The JWT token used by Active Directory to authenticate the user or application to perform this operation in Resource Manager.
correlationId	Usually a GUID in the string format. Events that share a correlationId belong to the same uber action.
description	This field is blank for Policy events.
eventDataId	Unique identifier of an event.
eventName	Either "BeginRequest" or "EndRequest". "BeginRequest" is used for delayed auditIfNotExists and deployIfNotExists evaluations and when a deployIfNotExists effect starts a template deployment. All other operations return "EndRequest".
category	Declares the activity log event as belonging to "Policy".
eventTimestamp	Timestamp when the event was generated by the Azure service processing the request corresponding the event.
ID	Unique identifier of the event on the specific resource.
level	Level of the event. Audit uses "Warning" and Deny uses "Error". An auditIfNotExists or deployIfNotExists error can generate "Warning" or "Error" depending on severity. All other Policy events use "Informational".
operationId	A GUID shared among the events that correspond to a single operation.
operationName	Name of the operation and directly correlates to the Policy effect.
resourceGroupName	Name of the resource group for the evaluated resource.
resourceProviderName	Name of the resource provider for the evaluated resource.

Element Name	Description
resourceType	For new resources, it is the type being evaluated. For existing resources, returns "Microsoft.Resources/checkPolicyCompliance".
resourceId	Resource ID of the evaluated resource.
status	String describing the status of the Policy evaluation result. Most Policy evaluations return "Succeeded", but a Deny effect returns "Failed". Errors in auditIfNotExists or deployIfNotExists also return "Failed".
subStatus	Field is blank for Policy events.
submissionTimestamp	Timestamp when the event became available for querying.
subscriptionId	Azure Subscription ID.
properties.isComplianceCheck	Returns "False" when a new resource is deployed or an existing resource's Resource Manager properties are updated. All other evaluation triggers result in "True".
properties.resourceLocation	The Azure region of the resource being evaluated.
properties.ancestors	A comma-separated list of parent management groups ordered from direct parent to farthest grandparent.
properties.policies	Includes details about the policy definition, assignment, effect, and parameters that this Policy evaluation is a result of.
relatedEvents	This field is blank for Policy events.

Schema from storage account and event hubs

When streaming the Azure Activity log to a storage account or event hub, the data follows the resource log schema. The table below provides a mapping of properties from the above schemas to the resource logs schema.

ⓘ **Important**

The format of Activity log data written to a storage account changed to JSON Lines on Nov. 1st, 2018. See **Prepare for format change to Azure Monitor resource logs archived to a storage account** for details on this format change.

Resource logs schema property	Activity Log REST API schema property	Notes
time	eventTimestamp	
resourceId	resourceId	subscriptionId, resourceType, resourceGroupName are all inferred from the resourceId.
operationName	operationName.value	
category	Part of operation name	Breakout of the operation type - "Write"/"Delete" /"Action"
resultType	status.value	
resultSignature	substatus.value	
resultDescription	description	
durationMs	N/A	Always 0
callerIpAddress	httpRequest.clientIpAddress	
correlationId	correlationId	
identity	claims and authorization properties	
Level	Level	
location	N/A	Location of where the event was processed. *This is not the location of the resource, but*

Resource logs schema property	Activity Log REST API schema property	Notes
		rather where the event was processed. This property will be removed in a future update.
Properties	properties.eventProperties	
properties.eventCategory	category	If properties.eventCategory is not present, category is "Administrative"
properties.eventName	eventName	
properties.operationId	operationId	
properties.eventProperties	properties	

Following is an example of an event using this schema..

JSON Copy

```json
{
    "records": [
        {
            "time": "2019-01-21T22:14:26.9792776Z",
            "resourceId": "/subscriptions/s1/resourceGroups/MSSupportGroup
/providers/microsoft.support/supporttickets/115012112305841",
            "operationName": "microsoft.support/supporttickets/write",
            "category": "Write",
            "resultType": "Success",
            "resultSignature": "Succeeded.Created",
            "durationMs": 2826,
            "callerIpAddress": "111.111.111.11",
            "correlationId": "c776f9f4-36e5-4e0e-809b-c9b3c3fb62a8",
            "identity": {
                "authorization": {
                    "scope": "/subscriptions/s1/resourceGroups
/MSSupportGroup/providers/microsoft.support/supporttickets/115012112305841",
                    "action": "microsoft.support/supporttickets/write",
                    "evidence": {
                        "role": "Subscription Admin"
                    }
                },
                "claims": {
                    "aud": "https://management.core.windows.net/",
                    "iss": "https://sts.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/",
                    "iat": "1421876371",
                    "nbf": "1421876371",
                    "exp": "1421880271",
                    "ver": "1.0",
                    "http://schemas.microsoft.com/identity/claims/tenantid": "00000000-0000-0000-0000-000000000000",
                    "http://schemas.microsoft.com/claims/authnmethodsreferences": "pwd",
                    "http://schemas.microsoft.com/identity/claims/objectidentifier": "2468adf0-8211-44e3-95xq-85137af64708",
                    "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn": "admin@contoso.com",
                    "puid": "20030000801A118C",
                    "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier": "9vckmEGF7zDKk1YzIY8k0t1_EAPaXoeHyPRn6f413zM",
                    "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname": "John",
                    "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname": "Smith",
                    "name": "John Smith",
                    "groups": "cacfe77c-e058-4712-83qw-f9b08849fd60,7f71d11d-4c41-4b23-99d2-d32ce7aa621c,31522864-0578-4ea0-9gdc-e66cc564d18c",
                    "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name": " admin@contoso.com",
                    "appid": "c44b4083-3bq0-49c1-b47d-974e53cbdf3c",
                    "appidacr": "2",
                    "http://schemas.microsoft.com/identity/claims/scope": "user_impersonation",
                    "http://schemas.microsoft.com/claims/authnclassreference": "1"
                }
            },
            "level": "Information",
            "location": "global",
            "properties": {
                "statusCode": "Created",
                "serviceRequestId": "50d5cddb-8ca0-47ad-9b80-6cde2207f97c"
            }
        }
    ]
}
```

Next steps

- Learn more about the Activity Log
- Create a diagnostic setting to send Activity Log to Log Analytics workspace, Azure storage, or event hubs

Is this page helpful?

👍 Yes 👎 No