Windows PowerShell Get-Help on Cmdlet 'Get-AzPolicyEvent'

PS:\>Get-HELP Get-AzPolicyEvent -Full

NAME

Get-AzPolicyEvent

SYNOPSIS

Gets policy evaluation events generated as resources are created or updated.

SYNTAX

Get-AzPolicyEvent [-Apply <System.String>] [-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] [-Filter <System.String>] [-From <System.DateTime>] -ManagementGroupName <System.String> [-OrderBy <System.String>] [-Select <System.String>] [-To <System.DateTime>] [-Top <System.Int32>] [<CommonParameters>]

Get-AzPolicyEvent [-Apply <System.String>] [-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] [-Filter <System.String>] [-From <System.DateTime>] [-OrderBy <System.String>] -PolicyAssignmentName <System.String> [-Select <System.String>] [-SubscriptionId <System.String>] [-To <System.DateTime>] [-Top <System.Int32>] [<CommonParameters>]

Get-AzPolicyEvent [-Apply <System.String>] [-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] [-Filter <System.String>] [-From <System.DateTime>] [-OrderBy <System.String>] -PolicyAssignmentName <System.String> -ResourceGroupName <System.String> [-Select <System.String>] [-SubscriptionId <System.String>] [-To <System.DateTime>] [-Top <System.Int32>] [<CommonParameters>]

Get-AzPolicyEvent [-Apply <System.String>] [-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] [-Filter <System.String>] [-From <System.DateTime>] [-OrderBy <System.String>] -PolicyDefinitionName <System.String> [-Select <System.String>] [-SubscriptionId <System.String>] [-To <System.DateTime>] [-Top <System.Int32>] [<CommonParameters>]

Get-AzPolicyEvent [-Apply <System.String>] [-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] [-Filter <System.String>] [-From <System.DateTime>] [-OrderBy <System.String>] -PolicySetDefinitionName <System.String> [-Select <System.String>] [-SubscriptionId <System.String>] [-To <System.DateTime>] [-Top <System.Int32>] [<CommonParameters>]

Get-AzPolicyEvent [-Apply <System.String>] [-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] [-Filter <System.String>] [-From <System.DateTime>] [-OrderBy <System.String>] -ResourceGroupName <System.String> [-Select <System.String>] [-SubscriptionId <System.String>] [-To <System.DateTime>] [-Top <System.Int32>] [<CommonParameters>]

Get-AzPolicyEvent [-Apply <System.String>] [-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] [-Filter <System.String>] [-From <System.DateTime>] [-OrderBy <System.String>] -ResourceId <System.String> [-Select <System.String>] [-To <System.DateTime>] [-Top <System.Int32>] [<CommonParameters>]

Get-AzPolicyEvent [-Apply <System.String>] [-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] [-Filter

<System.String>] [-From <System.DateTime>] [-OrderBy <System.String>] [-Select <System.String>] [-SubscriptionId <System.String>] [-To <System.DateTime>] [-Top
<System.Int32>] [<CommonParameters>]

DESCRIPTION

Gets policy evaluation events generated as resources are created or updated. Policy event records can be queried at various scopes based on the time interval
specified (defaults to last day). Results can be filtered, grouped, and group aggregations can be computed.

PARAMETERS

-Apply <System.String>

Apply expression for aggregations using OData notation.

Required? false
Position? named
Default value None
Accept pipeline input? False
Accept wildcard characters? false

-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>

The credentials, account, tenant, and subscription used for communication with Azure.

Required? false
Position? named
Default value None
Accept pipeline input? False
Accept wildcard characters? false

-Filter <System.String>

Filter expression using OData notation.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-From <System.DateTime>

ISO 8601 formatted timestamp specifying the start time of the interval to query. When not specified, defaults to 'To' parameter value minus 1 day.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-ManagementGroupName <System.String>

Management group name.

Required? true

Position? named

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-OrderBy <System.String>

Ordering expression using OData notation. One or more comma-separated column names with an optional 'desc' (the default) or 'asc'.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-PolicyAssignmentName <System.String>

Policy assignment name.

Required? true

Position? named

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-PolicyDefinitionName <System.String>

Policy definition name.

Required? true

Position? named

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-PolicySetDefinitionName <System.String>

Policy set definition name.

Required? true

Position? named

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-ResourceGroupName <System.String>

Resource group name.

Required? true

Position? named

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-ResourceId <System.String>

Resource ID.

Required? true

Position? named

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-Select <System.String>

Select expression using OData notation. One or more comma-separated column names. Limits the columns on each record to just those requested.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-SubscriptionId <System.String>

Subscription ID.

Required? false

Position? named

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-To <System.DateTime>

ISO 8601 formatted timestamp specifying the end time of the interval to query. When not specified, defaults to time of request.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-Top <System.Int32>

Maximum number of records to return.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

<CommonParameters>

This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer, PipelineVariable, and OutVariable. For more information, see about_CommonParameters (https:/go.microsoft.com/fwlink/?LinkID=113216).

INPUTS

System.String

OUTPUTS

Microsoft.Azure.Commands.PolicyInsights.Models.PolicyEvent

NOTES

-- Example 1: Get policy events in current subscription scope --

Get-AzPolicyEvent

Gets policy event records generated in the last day for all resources within the subscription in current session context.

Example 2: Get policy events in the specified subscription scope

Get-AzPolicyEvent -SubscriptionId "fff10b27-fff3-fff5-fff8-fffbe01e86a5"

Gets policy event records generated in the last day for all resources within the specified subscription.

---- Example 3: Get policy events in management group scope ----

Get-AzPolicyEvent -ManagementGroupName "myManagementGroup"

Gets policy event records generated in the last day for all resources within the specified management group.

Example 4: Get policy events in resource group scope in current subscription

Get-AzPolicyEvent -ResourceGroupName "myResourceGroup"

Gets policy event records generated in the last day for all resources within the specified resource group (in the

subscription in current session context).

Example 5: Get policy events in resource group scope in the specified subscription

Get-AzPolicyEvent -SubscriptionId "fff10b27-fff3-fff5-fff8-fffbe01e86a5" -ResourceGroupName "myResourceGroup"

Gets policy event records generated in the last day for all resources within the specified resource group (in the specified subscription).

--------- Example 6: Get policy events for a resource ---------

Get-AzPolicyEvent -ResourceId

"/subscriptions/fff10b27-fff3-fff5-fff8-fffbe01e86a5/resourceGroups/myResourceGroup/providers/Microsoft.EventHub/namespaces/myns1/eventhubs/eh1/consumergroups/cg1"

Gets policy event records generated in the last day for the specified resource.

Example 7: Get policy events for a policy set definition in current subscription

Get-AzPolicyEvent -PolicySetDefinitionName "fff58873-fff8-fff5-fffc-fffbe7c9d697"

Gets policy event records generated in the last day for all resources (within the tenant in current session context) effected by the specified policy set definition
(that exists in the subscription in current session context).

Example 8: Get policy events for a policy set definition in the specified subscription

Get-AzPolicyEvent -SubscriptionId "fff10b27-fff3-fff5-fff8-fffbe01e86a5" -PolicySetDefinitionName

"fff58873-fff8-fff5-fffc-fffbe7c9d697"

Gets policy event records generated in the last day for all resources (within the tenant in current session context) effected by the specified policy set definition
(that exists in the specified subscription).

Example 9: Get policy events for a policy definition in current subscription

Get-AzPolicyEvent -PolicyDefinitionName "fff58873-fff8-fff5-fffc-fffbe7c9d697"

Gets policy event records generated in the last day for all resources (within the tenant in current session context) effected by the specified policy definition (that
exists in the subscription in current session context).

Example 10: Get policy events for a policy definition in the specified subscription

Get-AzPolicyEvent -SubscriptionId "fff10b27-fff3-fff5-fff8-fffbe01e86a5" -PolicyDefinitionName "fff58873-fff8-fff5-fffc-fffbe7c9d697"

Gets policy event records generated in the last day for all resources (within the tenant in current session context) effected by the specified policy definition (that
exists in the specified subscription).

Example 11: Get policy events for a policy assignment in current subscription

Get-AzPolicyEvent -PolicyAssignmentName "ddd8ef92e3714a5ea3d208c1"

Gets policy event records generated in the last day for all resources (within the tenant in current session context) effected by the specified policy assignment (that
exists in the subscription in current session context).

Example 12: Get policy events for a policy assignment in the specified subscription

Get-AzPolicyEvent -SubscriptionId "fff10b27-fff3-fff5-fff8-fffbe01e86a5" -PolicyAssignmentName "ddd8ef92e3714a5ea3d208c1"

Gets policy event records generated in the last day for all resources (within the tenant in current session context) effected by the specified policy assignment (that
exists in the specified subscription).

Example 13: Get policy events for a policy assignment in the specified resource group in the current subscription

Get-AzPolicyEvent -ResourceGroupName "myResourceGroup" -PolicyAssignmentName "ddd8ef92e3714a5ea3d208c1"

Gets policy event records generated in the last day for all resources (within the tenant in current session context) effected by the specified policy assignment (that
exists in the resource group in the subscription in current session context).

Example 14: Get policy events in current subscription scope, with OrderBy, Top and Select query options

Get-AzPolicyEvent -OrderBy "Timestamp desc, PolicyAssignmentName asc" -Top 5 -Select "Timestamp, ResourceId, PolicyAssignmentId, PolicySetDefinitionId,
PolicyDefinitionId"

Gets policy event records generated in the last day for all resources within the subscription in current session context. The command orders the results by timestamp
and policy assignment name properties, and takes only top 5 of those listed in that order. It also selects to list only a subset of the columns for each record.

Example 15: Get policy events in current subscription scope, with From and To query options

```
Get-AzPolicyEvent -From "2018-03-08 00:00:00Z" -To "2018-03-15 00:00:00Z"
```

Gets policy event records generated within the date range specified for all resources within the subscription in current session context.

Example 16: Get policy events in current subscription scope, with Filter query option

```
Get-AzPolicyEvent -Filter "(PolicyDefinitionAction eq 'deny' or PolicyDefinitionAction eq 'audit') and ResourceLocation ne 'eastus'"
```

Gets policy event records generated in the last day for all resources within the subscription in current session context. The command limits the results returned by
filtering based on policy definition action (includes deny or audit actions) and resource location (excludes eastus location).

Example 17: Get policy events in current subscription scope, with Apply specifying row count aggregation

```
Get-AzPolicyEvent -Apply "aggregate(`$count as NumberOfRecords)"
```

Gets the number of policy event records generated in the last day for all resources within the subscription in current session context. The command returns the count
of the policy event records only, which is returned inside AdditionalProperties property.

Example 18: Get policy events in current subscription scope, with Apply specifying grouping with aggregation

```
Get-AzPolicyEvent -Filter "PolicyDefinitionAction eq 'audit' or PolicyDefinitionAction eq 'deny'" -Apply "groupby((PolicyAssignmentId, PolicyDefinitionId,
PolicyDefinitionAction, ResourceId), aggregate(`$count as NumEvents))" -OrderBy "NumEvents desc" -Top 5
```

Gets policy event records generated in the last day for all resources within the subscription in current session context. The command limits the results returned by

filtering based on policy definition action (includes only audit and deny events). It groups the results based on policy assignment, policy definition, policy

definition action, and resource id, and computes the number of records in each group, which is returned inside AdditionalProperties property. It orders the results by

the count aggregation in descending order, and takes only top 5 of those listed in that order.

Example 19: Get policy events in current subscription scope, with Apply specifying grouping without aggregation

```
Get-AzPolicyEvent -Filter "PolicyDefinitionAction eq 'audit' or PolicyDefinitionAction eq 'deny'" -Apply "groupby((ResourceId))"
```

Gets policy event records generated in the last day for all resources within the subscription in current session context. The command limits the results returned by

filtering based on policy definition action (includes only audit and deny events). It groups the results based on resource id. This generates the list of all

resources within the subscription that generated a policy event for at least one audit or deny policy.

Example 20: Get policy events in current subscription scope, with Apply specifying multiple groupings

```
Get-AzPolicyEvent -Filter "PolicyDefinitionAction eq 'deny'" -Apply "groupby((PolicyAssignmentId, PolicyDefinitionId, ResourceId))/groupby((PolicyAssignmentId,
PolicyDefinitionId), aggregate(`$count as NumDeniedResources))" -OrderBy "NumDeniedResources desc" -Top 5
```

Gets policy event records generated in the last day for all resources within the subscription in current session context. The command limits the results returned by

filtering based on policy definition action (includes only deny events). It groups the results first based on policy assignment, policy definition, and resource id.

Then, it further groups the results of this grouping with the same properties except for resource id, and computes the number of records in each of these groups,

which is returned inside AdditionalProperties property. It orders the results by the count aggregation in descending order, and takes only top 5 of those listed in

that order. This generates the top 5 deny policies with the most number of denied resources.

RELATED LINKS

Online Version: https://learn.microsoft.com/powershell/module/az.policyinsights/get-azpolicyevent