Windows PowerShell Get-Help on Cmdlet 'New-AzActivityLogAlert'

PS:\>Get-HELP New-AzActivityLogAlert -Full

NAME

New-AzActivityLogAlert

SYNOPSIS

Create a new Activity Log Alert rule or update an existing one.

SYNTAX

New-AzActivityLogAlert -Name <String> -ResourceGroupName <String> [-SubscriptionId <String>] -Action <IActionGroup[]> -Condition <IAlertRuleAnyOfOrLeafCondition[]>

-Location <String> -Scope <String[]> [-Description <String>] [-Enabled <Boolean>] [-Tag <Hashtable>] [-DefaultProfile <PSObject>] [-Break] [-HttpPipelineAppend

<SendAsyncStep[]>] [-HttpPipelinePrepend <SendAsyncStep[]>] [-Proxy <Uri>] [-ProxyCredential <PSCredential>] [-ProxyUseDefaultCredentials] [-WhatIf] [-Confirm]

[<CommonParameters>]

DESCRIPTION

Create a new Activity Log Alert rule or update an existing one.

PARAMETERS

-Name <String>

The name of the Activity Log Alert rule.

Required? true

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-ResourceGroupName <String>

The name of the resource group.

The name is case insensitive.

Required? true

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-SubscriptionId <String>

The ID of the target subscription.

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-Action <IActionGroup[]>

The list of the Action Groups.

To construct, see NOTES section for ACTIONGROUP properties and create a hash table.

To construct, see NOTES section for ACTION properties and create a hash table.

Required? true

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-Condition <IAlertRuleAnyOfOrLeafCondition[]>

The list of Activity Log Alert rule conditions.

To construct, see NOTES section for CONDITIONALLOF properties and create a hash table.

To construct, see NOTES section for CONDITION properties and create a hash table.

Required? true

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-Location <String>

The location of the resource.

Since Azure Activity Log Alerts is a global service, the location of the rules should always be 'global'.

Required? true

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-Scope <String[]>

A list of resource IDs that will be used as prefixes.

The alert will only apply to Activity Log events with resource IDs that fall under one of these prefixes.

This list must include at least one item.

Required? true

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-Description <String>

A description of this Activity Log Alert rule.

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-Enabled <Boolean>

Indicates whether this Activity Log Alert rule is enabled.

If an Activity Log Alert rule is not enabled, then none of its actions will be activated.

Required? false

Position? named

Default value False

Accept pipeline input? false

Accept wildcard characters? false

-Tag <Hashtable>

The tags of the resource.

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-DefaultProfile <PSObject>

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

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-Break [<SwitchParameter>]

Wait for .NET debugger to attach

Required? false

Position? named

Default value False

Accept pipeline input? false

Accept wildcard characters? false

-HttpPipelineAppend <SendAsyncStep[]>

SendAsync Pipeline Steps to be appended to the front of the pipeline

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-HttpPipelinePrepend <SendAsyncStep[]>

SendAsync Pipeline Steps to be prepended to the front of the pipeline

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-Proxy <Uri>

The URI for the proxy server to use

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-ProxyCredential <PSCredential>

Credentials for a proxy server to use for the remote call

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-ProxyUseDefaultCredentials [<SwitchParameter>]

Use the default credentials for the proxy

Required? false

Position? named

Default value False

Accept pipeline input? false

Accept wildcard characters? false

-WhatIf [<SwitchParameter>]

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-Confirm [<SwitchParameter>]

Required? false

Position? named

Default value

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

OUTPUTS

Microsoft.Azure.PowerShell.Cmdlets.Monitor.ActivityLogAlert.Models.Api20201001.IActivityLogAlertResource

NOTES

COMPLEX PARAMETER PROPERTIES

To create the parameters described below, construct a hash table containing the appropriate properties. For

information on hash tables, run Get-Help
about_Hash_Tables.

ACTION <IActionGroup[]>: The list of the Action Groups. To construct, see NOTES section for ACTIONGROUP properties and create a hash table.

Id <String>: The resource ID of the Action Group. This cannot be null or empty.

[WebhookProperty <IActionGroupWebhookProperties>]: the dictionary of custom properties to include with the post operation. These data are appended to the
webhook payload.

[(Any) <String>]: This indicates any property can be added to this object.

CONDITION <IAlertRuleAnyOfOrLeafCondition[]>: The list of Activity Log Alert rule conditions. To construct, see NOTES section for CONDITIONALLOF properties and
create a hash table.

[ContainsAny <String[]>]: The value of the event's field will be compared to the values in this array (case-insensitive) to determine if the condition is met.

[Equal <String>]: The value of the event's field will be compared to this value (case-insensitive) to determine if the condition is met.

[Field <String>]: The name of the Activity Log event's field that this condition will examine. The possible values for this field are
(case-insensitive): 'resourceId', 'category', 'caller', 'level', 'operationName', 'resourceGroup', 'resourceProvider', 'status', 'subStatus', 'resourceType', or
anything beginning with 'properties'.

[AnyOf <IAlertRuleLeafCondition[]>]: An Activity Log Alert rule condition that is met when at least one of its member leaf conditions are met.

[ContainsAny <String[]>]: The value of the event's field will be compared to the values in this array (case-insensitive) to determine if the condition is met.

[Equal <String>]: The value of the event's field will be compared to this value (case-insensitive) to determine if the condition is met.

[Field <String>]: The name of the Activity Log event's field that this condition will examine. The possible values for this field are
(case-insensitive): 'resourceId', 'category', 'caller', 'level', 'operationName', 'resourceGroup', 'resourceProvider', 'status', 'subStatus', 'resourceType', or

anything beginning with 'properties'.

---------- EXAMPLE 1 ----------

PS C:\>$scope = "/subscriptions/"+(Get-AzContext).Subscription.ID

$actiongroup=New-AzActivityLogAlertActionGroupObject -Id $ActionGroupResourceId -WebhookProperty @{"sampleWebhookProperty"="SamplePropertyValue"}

$condition1=New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -Equal Administrative -Field category

$condition2=New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -Equal Error -Field level

$any1=New-AzActivityLogAlertAlertRuleLeafConditionObject -Field properties.incidentType -Equal Maintenance

$any2=New-AzActivityLogAlertAlertRuleLeafConditionObject -Field properties.incidentType -Equal Incident

$condition3=New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -AnyOf $any1,$any2

New-AzActivityLogAlert -Name $AlertName -ResourceGroupName $ResourceGroupName -Action $actiongroup -Condition @($condition1,$condition2,$condition3) -Location global

-Scope $scope

RELATED LINKS

https://learn.microsoft.com/powershell/module/az.monitor/new-azactivitylogalert