Table of contents

Create and manage action groups in the Azure portal

Article

01/23/2023

16 minutes to read

18 contributors Feedback

In this article

When Azure Monitor data indicates that there might be a problem with your infrastructure or application, an alert is triggered. Azure Monitor, Azure Service Health, and Azure Advisor then use action groups to notify users about the alert and take an action. An action group is a collection of notification preferences that are defined by the owner of an Azure subscription.

This article shows you how to create and manage action groups in the Azure portal. Depending on your requirements, you can configure various alerts to use the same action group or different action groups.

Each action is made up of the following properties:

Type : The notification that's sent or action that's performed. Examples include sending a voice call, SMS, or email. You can also trigger various types of automated actions. For detailed information about notification and action types, see Action-specific information, later in this article.

: The notification that's sent or action that's performed. Examples include sending a voice call, SMS, or email. You can also trigger various types of automated actions. For detailed information about notification and action types, see Action-specific information, later in this article. Name : A unique identifier within the action group.

: A unique identifier within the action group. Details: The corresponding details that vary by type.

For information about how to use Azure Resource Manager templates to configure action groups, see Action group Resource Manager templates.

An action group is a global service, so there's no dependency on a specific Azure region. Requests from clients can be processed by action group services in any region. For instance, if one region of the action group service is down, the traffic is automatically routed and processed by other regions. As a global service, an action group helps provide a disaster recovery solution.

P

Create an action group by using the Azure portal

Go to the Azure portal. Search for and select Monitor. The Monitor pane consolidates all your monitoring settings and data in one view. Select Alerts, and then select Action groups. Select Create. Enter information as explained in the following sections.

Configure basic action group settings

Under Project details Select values for Subscription and Resource group .

Select the region Option Behavior Global The action groups service decides where to store the action group. The action group is persisted in at least two regions to ensure regional resiliency. Processing of actions may be done in any geographic region.

Voice, SMS and email actions performed as the result of service health alerts are resilient to Azure live-site-incidents. Regional The action group is stored within the selected region. The action group is zone-redundant. Processing of actions is performed within the region.Use this option if you want to ensure that the processing of your action group is performed within a specific geographic boundary. The action group is saved in the subscription, region and resource group that you select. Under Instance details, enter values for Action group name and Display name. The display name is used in place of a full action group name when the group is used to send notifications.

Configure notifications

To open the Notifications tab, select Next: Notifications. Alternately, at the top of the page, select the Notifications tab. Define a list of notifications to send when an alert is triggered. Provide the following information for each notification: Notification type : Select the type of notification that you want to send. The available options are: Email Azure Resource Manager Role : Send an email to users who are assigned to certain subscription-level Azure Resource Manager roles. Email/SMS message/Push/Voice : Send various notification types to specific recipients.

Name : Enter a unique name for the notification.

Details : Based on the selected notification type, enter an email address, phone number, or other information.

Common alert schema: You can choose to turn on the common alert schema, which provides the advantage of having a single extensible and unified alert payload across all the alert services in Monitor. For more information about this schema, see Common alert schema. Select OK.

Configure actions

To open the Actions tab, select Next: Actions. Alternately, at the top of the page, select the Actions tab. Define a list of actions to trigger when an alert is triggered. Provide the following information for each action: Action type : Select from the following types of actions: An Azure Automation runbook An Azure Functions function A notification that's sent to Azure Event Hubs A notification that's sent to an IT service management (ITSM) tool An Azure Logic Apps workflow A secure webhook A webhook

Name : Enter a unique name for the action.

Details : Enter appropriate information for your selected action type. For instance, you might enter a webhook URI, the name of an Azure app, an ITSM connection, or an Automation runbook. For an ITSM action, also enter values for Work item and other fields that your ITSM tool requires.

Common alert schema: You can choose to turn on the common alert schema, which provides the advantage of having a single extensible and unified alert payload across all the alert services in Monitor. For more information about this schema, see Common alert schema.

Create the action group

If you'd like to assign a key-value pair to the action group, select Next: Tags or the Tags tab. Otherwise, skip this step. By using tags, you can categorize your Azure resources. Tags are available for all Azure resources, resource groups, and subscriptions. To review your settings, select Review + create. This step quickly checks your inputs to

make sure you've entered all required information. If there are issues, they're reported here. After you've reviewed the settings, select Create to create the action group.

Note When you configure an action to notify a person by email or SMS, they receive a confirmation indicating that they have been added to the action group.

Test an action group in the Azure portal (preview)

When you create or update an action group in the Azure portal, you can test the action group.

Define an action, as described in the previous few sections. Then select Review + create.

Note If you are editing an already exisitng action group, you must save changes to the action group before testing.

On the page that lists the information that you entered, select Test action group. Select a sample type and the notification and action types that you want to test. Then select Test. If you close the window or select Back to test setup while the test is running, the test is stopped, and you don't get test results. When the test is complete, a test status of either Success or Failed appears. If the test failed and you'd like to get more information, select View details.

You can use the information in the Error details section to understand the issue. Then you can edit, save changes, and test the action group again.

When you run a test and select a notification type, you get a message with "Test" in the subject. The tests provide a way to check that your action group works as expected before you enable it in a production environment. All the details and links in test email notifications are from a sample reference set.

Azure Resource Manager role membership requirements

The following table describes the role membership requirements that are needed for the test actions functionality:

User's role membership Existing action group Existing resource group and new action group New resource group and new action group Subscription contributor Supported Supported Supported Resource group contributor Supported Supported Not applicable Action group resource contributor Supported Not applicable Not applicable Azure Monitor contributor Supported Supported Not applicable Custom role Supported Supported Not applicable

Manage your action groups

After you create an action group, you can view it in the portal:

From the Monitor page, select Alerts. Select Manage actions. Select the action group that you want to manage. You can: Add, edit, or remove actions.

Delete the action group.

Action-specific information

The following sections provide information about the various actions and notifications that you can configure in an action group.

Note To check numeric limits on each type of action or notification, see Subscription service limits for monitoring.

Automation runbook

To check limits on Automation runbook payloads, see Automation limits.

You may have a limited number of runbook actions per action group.

Azure app push notifications

To enable push notifications to the Azure mobile app, provide the email address that you use as your account ID when you configure the Azure mobile app. For more information about the Azure mobile app, see Get the Azure mobile app.

You might have a limited number of Azure app actions per action group.

Email

Ensure that your email filtering and any malware/spam prevention services are configured appropriately. Emails are sent from the following email addresses:

azure-noreply@microsoft.com

azureemail-noreply@microsoft.com

alerts-noreply@mail.windowsazure.com

You may have a limited number of email actions per action group. For information about rate limits, see Rate limiting for voice, SMS, emails, Azure App push notifications, and webhook posts.

Email Azure Resource Manager role

When you use this type of notification, you can send email to the members of a subscription's role. Email is only sent to Azure Active Directory (Azure AD) user members of the role. Email isn't sent to Azure AD groups or service principals.

A notification email is sent only to the primary email address.

If your primary email doesn't receive notifications, take the following steps:

In the Azure portal, go to Active Directory. On the left, select All users. On the right, a list of users appears. Select the user whose primary email you'd like to review. In the user profile, look under Contact info for an Email value. If it's blank: At the top of the page, select Edit. Enter an email address. At the top of the page, select Save.

You may have a limited number of email actions per action group. To check which limits apply to your situation, see Rate limiting for voice, SMS, emails, Azure App push notifications, and webhook posts.

When you set up the Azure Resource Manager role:

Assign an entity of type "User" to the role. Make the assignment at the subscription level. Make sure an email address is configured for the user in their Azure AD profile.

Note It can take up to 24 hours for a customer to start receiving notifications after they add a new Azure Resource Manager role to their subscription.

Event Hubs

An Event Hubs action publishes notifications to Event Hubs. For more information about Event Hubs, see Azure Event Hubsâ€”A big data streaming platform and event ingestion service. You can subscribe to the alert notification stream from your event receiver.

Functions

An action that uses Functions calls an existing HTTP trigger endpoint in Functions. For more information about Functions, see Azure Functions. To handle a request, your endpoint must handle the HTTP POST verb.

When you define the function action, the function's HTTP trigger endpoint and access key are saved in the action definition, for example, https://azfunctionurl.azurewebsites.net/api/httptrigger?code= . If you change the access key for the function, you need to remove and recreate the function action in the action group.

You may have a limited number of function actions per action group.

Note The function must have access to the storage account. If not, no keys will be available and the function URI will not be accessible.

ITSM

An ITSM action requires an ITSM connection. To learn how to create an ITSM connection, see ITSM integration.

You might have a limited number of ITSM actions per action group.

Logic Apps

You may have a limited number of Logic Apps actions per action group.

Secure webhook

When you use a secure webhook action, you must use Azure AD to secure the connection between your action group and your protected web API, which is your webhook endpoint.

The secure webhook Action authenticates to the protected API using a Service Principal instance in the AD tenant of the "AZNS AAD Webhook" AAD Application. To make the action group work, this AAD Webhook Service Principal needs to be added as member of a role on the target AAD application that grants access to the target endpoint.

For an overview of Azure AD applications and service principals, see Microsoft identity platform (v2.0) overview. Follow these steps to take advantage of the secure webhook functionality.

Note Basic authentication is not supported for SecureWebhook. To use basic authentication you must use Webhook.

Note If you use the webhook action, your target webhook endpoint needs to be able to process the various JSON payloads that different alert sources emit. If the webhook endpoint expects a specific schema, for example, the Microsoft Teams schema, use the Logic Apps action to transform the alert schema to meet the target webhook's expectations.

Create an Azure AD application for your protected web API. For detailed information, see Protected web API: App registration. Configure your protected API to be called by a daemon app, and expose application permissions, not delegated permissions. For more information about these permissions, see If your web API is called by a service or

daemon app. Note Configure your protected web API to accept V2.0 access tokens. For detailed information about this setting, see Azure Active Directory app manifest. To enable the action group to use your Azure AD application, use the PowerShell script that follows this procedure. Note You must be assigned the Azure AD Application Administrator role to run this script. Modify the PowerShell script's Connect-AzureAD call to use your Azure AD tenant ID. Modify the PowerShell script's $myAzureADApplicationObjectId variable to use the Object ID of your Azure AD application. Run the modified script. Note The service principle needs to be assigned an owner role of the Azure AD application to be able to create or modify the secure webhook action in the action group. Configure the secure webhook action. Copy the $myApp.ObjectId value that's in the script. In the webhook action definition, in the Object Id box, enter the value that you copied.

Secure webhook PowerShell script

Connect-AzureAD -TenantId "" # Define your Azure AD application's ObjectId. $myAzureADApplicationObjectId = "" # Define the action group Azure AD AppId. $actionGroupsAppId = "461e8683-5575-4561-ac7f-899cc907d62a" # Define the name of the new role that gets added to your Azure AD application. $actionGroupRoleName = "ActionGroupsSecureWebhook" # Create an application role with the given name and description. Function CreateAppRole([string] $Name, [string] $Description) { $appRole = New-Object Microsoft.Open.AzureAD.Model.AppRole $appRole.AllowedMemberTypes = New-Object System.Collections.Generic.List[string] $appRole.AllowedMemberTypes.Add("Application"); $appRole.DisplayName = $Name $appRole.Id = New-Guid $appRole.IsEnabled = $true $appRole.Description = $Description $appRole.Value = $Name; return $appRole } # Get your Azure AD application, its roles, and its service principal. $myApp = Get-AzureADApplication -ObjectId $myAzureADApplicationObjectId $myAppRoles = $myApp.AppRoles $actionGroupsSP = Get-AzureADServicePrincipal -Filter ("appId eq '" + $actionGroupsAppId + "'") Write-Host "App Roles before addition of new role.." Write-Host $myAppRoles # Create the role if it doesn't exist. if ($myAppRoles -match "ActionGroupsSecureWebhook") { Write-Host "The Action Group role is already defined.`n" } else { $myServicePrincipal = Get-AzureADServicePrincipal -Filter ("appId eq '" + $myApp.AppId + "'") # Add the new role to the Azure AD application. $newRole = CreateAppRole -Name $actionGroupRoleName -Description "This is a role for Action Group to join" $myAppRoles.Add($newRole) Set-AzureADApplication -ObjectId $myApp.ObjectId -AppRoles $myAppRoles } # Create the service principal if it doesn't exist. if ($actionGroupsSP -match "AzNS AAD Webhook") { Write-Host "The Service principal is already defined.`n" } else { # Create a service principal for the action group Azure AD application and add it to the role. $actionGroupsSP = New-AzureADServicePrincipal -AppId $actionGroupsAppId } New-AzureADServiceAppRoleAssignment -Id $myApp.AppRoles[0].Id -ResourceId $myServicePrincipal.ObjectId -ObjectId $actionGroupsSP.ObjectId -PrincipalId

$actionGroupsSP.ObjectId Write-Host "My Azure AD Application (ObjectId): " + $myApp.ObjectId Write-Host "My Azure AD Application's Roles" Write-Host $myApp.AppRoles

SMS

For information about rate limits, see Rate limiting for voice, SMS, emails, Azure App push notifications, and webhook posts.

For important information about using SMS notifications in action groups, see SMS alert behavior in action groups.

You might have a limited number of SMS actions per action group.

Note If you can't select your country/region code in the Azure portal, SMS isn't supported for your country/region. If your country/region code isn't available, you can vote to have your country/region added at Share your ideas. In the meantime, as a workaround, configure your action group to call a webhook to a third-party SMS provider that offers support in your country/region.

For information about pricing for supported countries/regions, see Azure Monitor pricing.

Countries with SMS notification support

Country code Country 61 Australia 43 Austria 32 Belgium 55 Brazil 1 Canada 56 Chile 86 China 420 Czech Republic 45 Denmark 372 Estonia 358 Finland 33 France 49 Germany 852 Hong Kong 91 India 353 Ireland 972 Israel 39 Italy 81 Japan 352 Luxembourg 60 Malaysia 52 Mexico 31 Netherlands 64 New Zealand 47 Norway 351 Portugal 1 Puerto Rico 40 Romania 7 Russia 65 Singapore 27 South Africa 82 South Korea 34 Spain 41 Switzerland 886 Taiwan 971 UAE 44 United Kingdom 1 United States

Voice

For important information about rate limits, see Rate limiting for voice, SMS, emails, Azure App push notifications, and webhook posts.

You might have a limited number of voice actions per action group.

Note If you can't select your country/region code in the Azure portal, voice calls aren't supported for your country/region. If your country/region code isn't available, you can vote to have your country/region added at Share your ideas. In the meantime, as a workaround, configure your action group to call a webhook to a third-party voice call provider that offers support in your country/region. The only country code that action groups currently support for voice notification is +1 for the United States.

For information about pricing for supported countries/regions, see Azure Monitor pricing.

Webhook

Note If you use the webhook action, your target webhook endpoint needs to be able to process the various JSON payloads that different alert sources emit. If the webhook endpoint expects a specific schema, for example, the Microsoft Teams schema, use the Logic Apps action to transform the alert schema to meet the target webhook's expectations.

Webhook action groups use the following rules:

A webhook call is attempted at most three times.

The first call waits 10 seconds for a response.

Between the first and second call it waits 20 seconds for a response.

Between the second and third call it waits 40 seconds for a response.

The call is retried if any of the following conditions are met: A response isn't received within the timeout period. One of the following HTTP status codes is returned: 408, 429, 503, 504 or TaskCancellationException. If any one of the above errors is encountered an additonal 5 seconds wait for the response.

If three attempts to call the webhook fail, no action group calls the endpoint for 15 minutes.

210.00155555556

For source IP address ranges, see Action group IP addresses.

Next steps

Reference

Strategies and Tactics of Behavioral Research

Magic Mom, Magic Dad: 18 cartoons to help parents avoid tantrums: Thirty years of research turned into simple cartoons to help parents with young children (ages 2-5) avoid temper tantrums.