

Guide for setting up Azure Policy Rule Set for private DNS zones

Preparation – Clone Github Repository

Import Github Repo

Create a new repository

A repository contains all project files, including the revision history. Already have a

[Import a repository.](#)

Import your project to GitHub

Import all the files, including the revision history, from another version control system.

Your old repository's clone URL

`https://github.com/starbuckscoffee/azurepolicy`

Learn more about the types of [supported VCS](#).

starbuckscoffee/azurepolicy

Your new repository details

[Single sign-on](#) to see more options for organizations within the Microsoft Open Source enterprise.

Owner *

Repository Name *



/ azurepolicy



Privacy



Public

Anyone on the internet can see this repository. You choose who can commit.



Private

You choose who can see and commit to this repository.

[i](#) You are creating a public repository in the higotodemo organization.

Cancel

Begin import

higotodemo/azurepolicy

✓ Importing complete! Your new repository [higotodemo/azurepolicy](#) is ready.

Preparation – Enable GitHub Actions

The screenshot shows the GitHub repository settings interface. At the top, the navigation bar includes 'Projects', 'Wiki', 'Security', 'Insights', and 'Settings'. The 'Settings' tab is selected and highlighted with a red box. On the left sidebar, the 'Actions' tab is selected and highlighted with a red box. Below the sidebar, the 'Actions permissions' section is visible. The first option, 'Allow all actions and reusable workflows', is selected with a radio button and highlighted with a red box. Red arrows indicate the navigation path from the 'Settings' tab to the 'Actions' tab and then to the 'Allow all actions and reusable workflows' option. A 'Save' button is located at the bottom right of the settings area.

Projects Wiki Security Insights Settings

General

Access

Collaborators and teams

Moderation options

Code and automation

Branches

Tags

Actions

General

Actions permissions

☒ **Allow all actions and reusable workflows**
Any action or reusable workflow can be used, regardless of who authored it or where it is defined.

☐ **Disable actions**
The Actions tab is hidden and no workflows can run.

☐ **Allow higotodemo actions and reusable workflows**
Any action or reusable workflow defined in a repository within higotodemo can be used.

☐ **Allow higotodemo, and select non-higotodemo, actions and reusable workflows**
Any action or reusable workflow that matches the specified criteria, plus those defined in a repository [more about allowing specific actions and reusable workflows to run.](#)

Save

Preparation – Generate Service Principal

Create yet another Service Principal

```
az ad sp create-for-rbac --name "__your_SP_name" --role owner --scopes /subscriptions/__yourSubscriptionId --sdk-auth
```

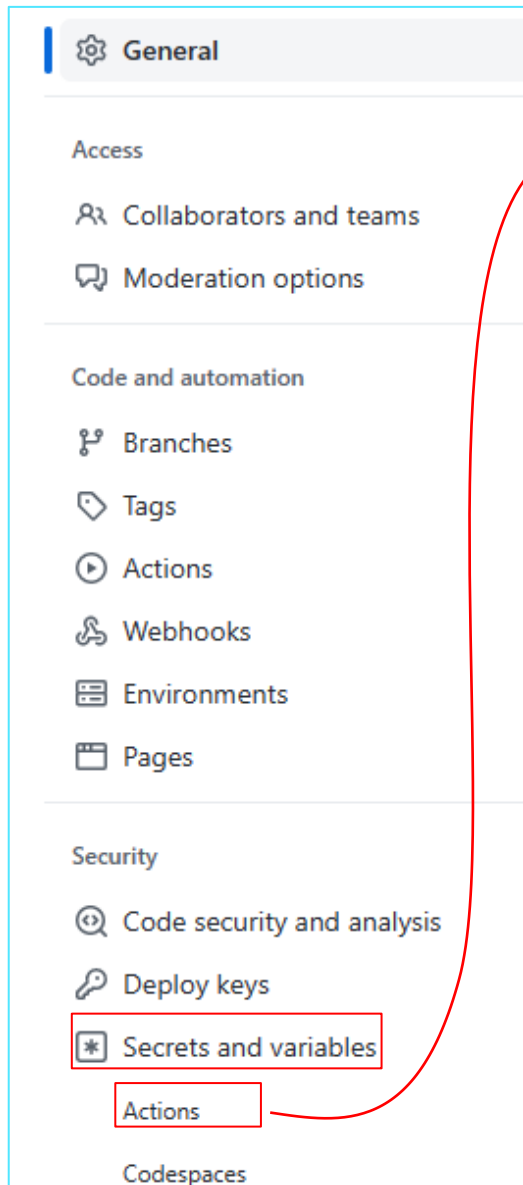
```
Windows PowerShell
C:\Program Files (x86)\Micros

higoto@DESKTOP-ADVJRJA:~/actions-runner$ az ad sp create-for-rbac --name "AadApp4VSenderprise" --role contri
butor --scopes /subscriptions/340954be-b2b0-423b-9784-dbcaa0fb8107/resourceGroups/VSEJpnEastVnetRg --sdk-a
uth
Option '--sdk-auth' has been deprecated and will be removed in a future release.
Creating 'contributor' role assignment under scope '/subscriptions/340954be-b2b0-423b-9784-dbcaa0fb8107/reso
urceGroups/VSEJpnEastVnetRg'
The output includes credentials that you must protect. Be sure that you do not include these credentials in
your code or check the credentials into your source control. For more information, see https://aka.ms/azadsp
-cli
{
  "clientId": "397fa0a3-d19c-4503-93cd-b0b6ef75d1ed",
  "clientSecret": "5qr0Q-mqC50gXVdpatf-jajehHkId-1KjrsEaqbRK",
  "subscriptionId": "340954be-b2b0-423b-9784-dbcaa0fb8107",
  "tenantId": "bfa4e849-059a-4b98-8756-944872678dc8",
  "activeDirectoryEndpointUrl": "https://login.microsoftonline.com",
  "resourceManagerEndpointUrl": "https://management.azure.com/",
  "activeDirectoryGraphResourceId": "https://graph.windows.net/",
  "sqlManagementEndpointUrl": "https://management.core.windows.net:8443/",
  "galleryEndpointUrl": "https://gallery.azure.com/",
  "managementEndpointUrl": "https://management.core.windows.net/"
}
higoto@DESKTOP-ADVJRJA:~/actions-runner$
```

Create JSON file

```
{
  "clientId": "xxxxxxxxxxxxxxxx",
  "clientSecret": "#####",
  "tenantId": "your tennant Id",
  "subscriptionId": "your subscription Id"
}
```

Preparation – Set Github Secrets



The screenshot shows the 'Actions secrets / New secret' form. The 'Name' field is filled with 'AZURE_CREDENTIALS'. The 'Secret' field contains a JSON object for an Azure Service Principal. A red box highlights the 'Add secret' button at the bottom. A red arrow points from the 'New repository secret' button in the top section to the 'Name' field. Another red arrow points from the 'Secret' field to the 'Add secret' button. A red dashed arrow points from the 'AZURE_CREDENTIALS' name to the corresponding secret name in the reference file on the right.

Secrets Variables

Actions secrets

New repository secret

Actions secrets / New secret

Name *

AZURE_CREDENTIALS

Secret *

Azure Service Principal

```
{
  "clientId": "xxxxxxxxxxxx",
  "clientSecret": "#####",
  "tenantId": "your tennant Id",
  "subscriptionId": "your subscription Id"
}
```

Add secret

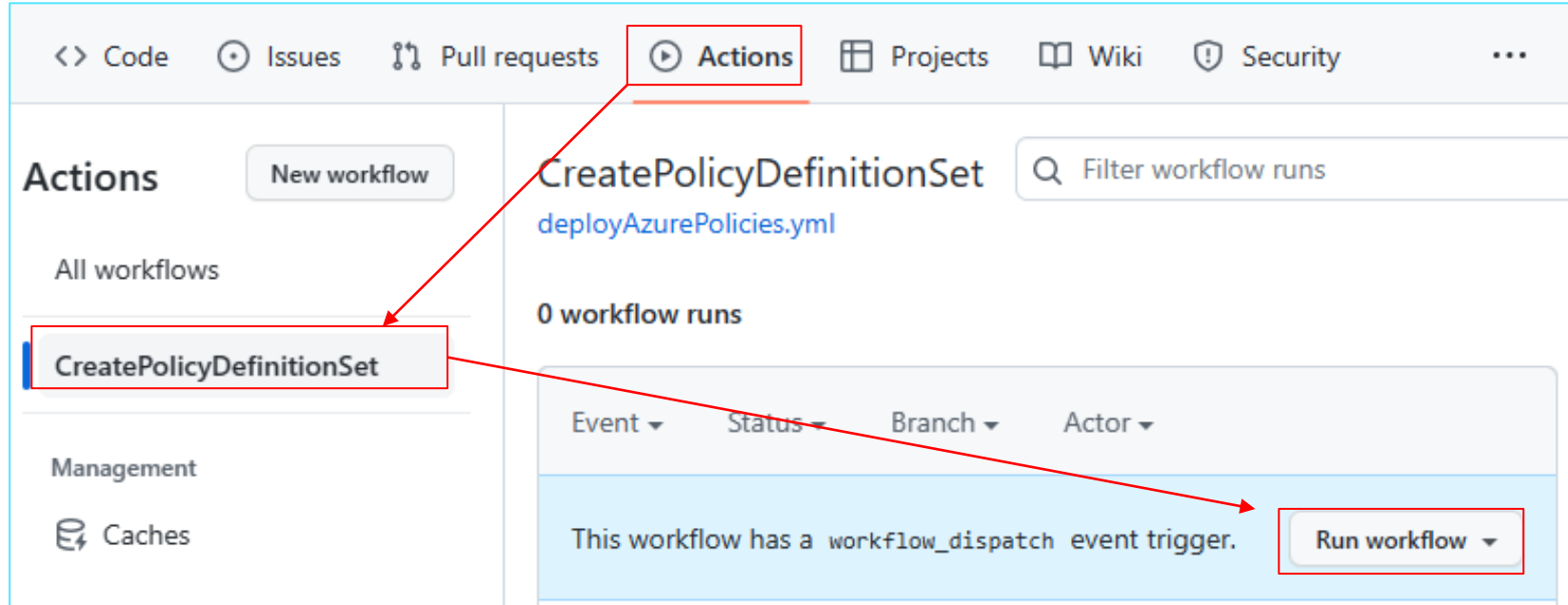
Reference File

azurepolicy/.github/workflows/deployAzurePolicies.yml

```
1 on: [workflow_dispatch]
2
3 name: CreatePolicyDefinitionSet
4
5 jobs:
6   deploy-azure-policy:
7     runs-on: ubuntu-latest
8     steps:
9       - name: Checkout
10        uses: actions/checkout@v2
11       - name: Login to Azure
12        uses: azure/login@v1
13        with:
14          creds: ${secrets.AZURE_CREDENTIALS}
15          allow-no-subscriptions: true
16       - name: Create or Update Azure Policies
17        run: |
18          cd 0_7
19          chmod 755 deployPolicies.sh
20          ./deployPolicies.sh
21       - name: Create or Update Azure Policy Set
22        run: |
23          cd 0_7
24          pwd
25          chmod 755 deployPolicySetInitiative.sh
26          ./deployPolicySetInitiative.sh
```

← See Prev. Slide

Preparation – Run GitHub Action Workflow



Assign Azure Policy Set

Azure Portal → Policy

Policy

Policy definition Initiative definition Export definitions Refresh

Search

Overview

Getting started

Compliance

Remediation

Events

Authoring

Definitions

Assignments

Exemptions

Scope: Visual Studio Enterprise

Definition type: All definition types

Category: 1 categories

Search: Filter by name or

Now export your definitions to GitHub and manage them using actions!

Select all

PrivateDnsZoneGroupId

Name ↑↓	Definition location ↑↓	Policies ↑↓	Type ↑↓	Definit... ↑↓	Category ↑↓
Create_Private_Endpoint_Resource_for_ADX_groupId_cluster	Visual Studio Enterprise		Custom	Policy	PrivateDnsZoneGroupId
Create_Private_Endpoint_Resource_for_ContainerRegistry_groupId_re...	Visual Studio Enterprise		Custom	Policy	PrivateDnsZoneGroupId
Create_Private_Endpoint_Resource_for_CosmosCassandra_groupId_C...	Visual Studio Enterprise		Custom	Policy	PrivateDnsZoneGroupId
Create_Private_Endpoint_Resource_for_CosmosGremlin_groupId_Gre...	Visual Studio Enterprise		Custom	Policy	PrivateDnsZoneGroupId
Create_Private_Endpoint_Resource_for_CosmosMongo_groupId_Mon...	Visual Studio Enterprise		Custom	Policy	PrivateDnsZoneGroupId
Create_Private_Endpoint_Resource_for_WebPubSub_groupId_WebPu...	Visual Studio Enterprise		Custom	Policy	PrivateDnsZoneGroupId
PolicySet_Create_private_endpoint_resources_from_multiple_groupIds	Visual Studio Enterprise	26	Custom	Initiative	PrivateDnsZoneGroupId

Filter rules by Category

Scroll down

Next Slide...

Assign Azure Policy Set

[Home](#) > [Policy | Definitions](#) >

PolicySet_Create_private_endpoint_resources_from_multiple_groupIds ...

Initiative Definition

[Assign](#) [Edit initiative](#) [Duplicate initiative](#) [Delete initiative](#) [Export initiative](#)

^ Essentials

Name : PolicySet_Create_private_endpoint_resources_from_multiple_g

Description : --

Category : PrivateDnsZoneGroupId

Basics Advanced Parameters **Remediation** Non-compliance messages Review + create

By default, this assignment will only take effect on newly created resources. Existing resources can be updated via a remediation task. For deployIfNotExists policies, the remediation task will deploy the specified template. For modify policies, the remediation task will update the resources.

☒ Create a remediation task ⓘ

Policy to remediate

Create_Private_Endpoint_Resource_for_Storage_groupId_blob - (Create_Private_Endpoint_Resource_for_Storage_groupId_blob)

Managed Identity

Policies with the deployIfNotExists and modify effect types need the ability to deploy resources and edit tags on existing resources. You can choose between an existing user assigned managed identity or creating a system assigned managed identity. [Learn more about Managed Identity.](#)

☒ Create a Managed Identity ⓘ

Type of Managed Identity ⓘ

☒ System assigned managed identity ☐ User assigned managed identity

System assigned identity location *

Japan East

Assign Azure Policy Set

The screenshot shows the 'Assign Azure Policy Set' wizard in the Azure portal. The 'Non-compliance messages' tab is active, showing a text area for the 'Default non-compliance message' and a table for 'Policy specific messages'. The 'Review + create' tab is also visible, showing the policy details. Red arrows highlight the 'Default non-compliance message' field, the 'Policy specific messages' table, and the 'Create' button.

Non-compliance messages

Non-compliance messages help users understand why a resource is not compliant with the policy. The message will be displayed w in the evaluation details of any non-compliant resource.

Default non-compliance message ⓘ

YOUR NON COMPLIANCE MESSAGE

Policy specific messages

Search by name or reference ID

Edit message for selected policies

<input checked="" type="checkbox"/>	POLICY DEFINITION	REFERENCE ID
<input checked="" type="checkbox"/>	Create_Private_Endpoint_Resource_for_Storage_groupId_b...	Create_Private...
<input checked="" type="checkbox"/>	Create_Private_Endpoint_Resource_for_ContainerRegistry_...	Create_Private...
<input checked="" type="checkbox"/>	Create_Private_Endpoint_Resource_for_DeviceProvisioning...	Create_Private...

Review + create

Basics

Scope: Visual Studio Enterprise

Exclusions: --

Policy definition: PolicySet_Create_private_endpoint_resources_from_multiple_groupIds

Assignment name: PolicySet_Create_private_endpoint_resources_from_multiple_groupIds

Description: --

Policy enforcement: Enabled

Assigned by: Hisashi Goto

Advanced

Resource selectors

Create Cancel Previous Next

Verify Assigned Azure Policy Set

The screenshot displays the Azure Policy 'Policy | Assignments' page. On the left, the 'Assignments' tab is selected in the 'Authoring' section. The main area shows a single assignment named 'PolicySet_Create_private_endpoint_resources_from_multiple_groupIds'. A red box highlights the 'Parameters (33)' tab, which contains a table of parameters. A red arrow points from the 'Assignments' tab to the assignment name, and another red arrow points from the assignment name to the 'Parameters' tab. A dashed blue box highlights the 'Parameter value' column, with a label 'Private DNS zones' pointing to it.

Home > Policy

Policy | Assignments

Search << Assign policy >>

- Overview
- Getting started
- Compliance
- Remediation
- Events

Now create custom non-compliance

Total Assignments 1

Assignment name ↑↓

PolicySet_Create_private_endpoint_resources_from_multiple_groupIds

PolicySet_Create_private_endpoint_resources_from_multiple_groupIds

Policy Assignment

Edit Delete Duplicate View compliance View definition Create exemption Create Remediation Task

Essentials

Name : PolicySet_Create_private_endpoint_resources_from_multiple_groupIds

Description : --

Assignment ID : /subscriptions/340954be-b2b0-423b-9784-dbcaa0fb8107/providers/Microsoft.Authorization/policyAssignments/bfacdfbee3ae49b9...

Parameters (33) Resource selectors (0) Overrides (0) Exemptions (0) Remediation (1) Deployed resources (0) Manage

Search by parameter name All types

Parameter ID	Parameter name	Parameter value
Create_Private_Endpoint_Resource...	StorageBlob	"privatelink.blob.core.windows.net"
Create_Private_Endpoint_Resource...	ContainerRegistry	"privatelink.azurecr.io"
Create_Private_Endpoint_Resource...	DeviceProvisioningService	"privatelink.azurecr.io"

Private DNS zones

Reference : Assign Azure Policy Set -- Parameters

For your reference:

The image shows the 'Parameters' tab of the 'PolicySet_Create_private_endpoint_resources_from_multiple_g' assignment initiative. The 'Parameters' tab is selected, and the checkbox 'Only show parameters that need input or review' is checked. Below this, there are four parameters: 'StorageBlob', 'ContainerRegistry', 'DeviceProvisioningService', and 'DigitalTwin'. The 'ContainerRegistry' parameter is highlighted with a red box and a red arrow pointing to the 'ContainerRegistry' dialog box. The dialog box shows the 'Subscription' as 'Visual Studio Enterprise' and the 'privateDnsZones' list. A red arrow points from the 'privateDnsZones' dropdown in the dialog to the 'ContainerRegistry' parameter in the main page. A yellow callout box with the text 'You can pick up your private DNS zones manually..' points to the list of private DNS zones in the dialog. The list includes: 'privatelink.azure-devices.net', 'privatelink.blob.core.windows.net', 'privatelink.servicebus.windows.net', and 'privatelink.vaultcore.azure.net'. The 'Select' button is highlighted in blue.

PolicySet_Create_private_endpoint_resources_from_multiple_g

Assign initiative

Basics Advanced **Parameters** Remediation Non-compliance messages

Search by para... ☒ Only show parameters that need input or review

Check Off

StorageBlob *

ContainerRegistry *

DeviceProvisioningService *

DigitalTwin *

ContainerRegistry

Subscription

Visual Studio Enterprise

privateDnsZones

privatelink.azure-devices.net

privatelink.blob.core.windows.net

privatelink.servicebus.windows.net


privatelink.vaultcore.azure.net

You can pick up your private DNS zones manually..

Select Cancel

Reference : Customize Policy Set






Click Azure Policy Initiative

 PolicySet_Create_private_endpoint_resources_from_multiple_groupIds

Visual Studio Enterprise26

PolicySet_Create_private_endpoint_resources_from_multiple_groupIds

Initiative Definition

 Assign  Edit initiative  Duplicate initiative  Delete initiative  Export initiative

^ Essentials

Basics **Policies** Groups Initiative parameters Policy parameters Review + save

Add one or more policies to this initiative. Reference ID can be used as a friendly display name but must be unique within the initiative.







Add policy definition(s)

Add selected policies to a group

26 policies are not part of any group

Search by name or referen...

Group : 1 selected

<input type="checkbox"/>	POLICY DEFINITION	REFERENCE ID	GROUP	
<input type="checkbox"/>	 Create_Private_Endpoint_Resource_for_Stor...	Create_Private_Endpoint_Reso...	0 groups	
<input type="checkbox"/>	 Create_Private_Endpoint_Resource_for_Cont...	Create_Private_Endpoint_Reso...	0 groups	
<input type="checkbox"/>	 Create_Private_Endpoint_Resource_for_Devi...	Create_Private_Endpoint_Reso...	0 groups	


Review + save

Cancel

Previous

Next

Remove Unused private DNS zone



- View policy definition
- Edit Reference ID
- Edit Groups
- Remove policy



Thank you