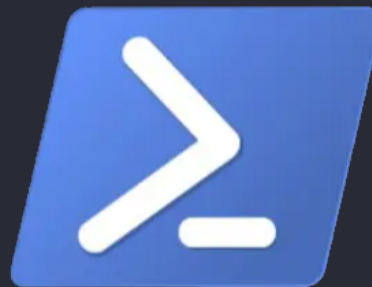


GlobalBao > azure-policy-as-code > x_PolicyMgmt > GetPolicyIDs.ps1 > ...

```
1 #####
2 # Description: Queries built-in Azure Policy resources (policies/policysets), builds a hashtable object with the results, and exports to JSON for consumption via Bicep.
3 # Note1: Excluded policies: 'Static' (type), 'Deprecated' (Metadata.deprecated), and 'Preview' (Metadata.preview)
4 # Note2: This script is modified from Justin Grote's original input as mentioned here: https://github.com/Azure/bicep/issues/1895
5 #####
6
7 # Define folder path for exported JSON files
8 $FilePath = 'C:\Temp'
9
10 # Authenticate to Azure and return all subscription IDs you have access to
11 Login-AzAccount
12 Get-AzSubscription
13
14 # Create object for policy results
15 [ScriptBlock]$PolicyNameResolver = {
16     --- $baseDisplayName = $PSItem.properties.displayName -replace '[^\s\w]', ''
17     --- $category = $PSItem.properties.metadata.category -replace '\s', ''
18     --- $name = (Get-Culture).TextInfo.ToTitleCase($baseDisplayName) -replace '\s', ''
19     --- $category + "_" + $name
20 }
21
22 # Query policy definitions and build hashtable
23 $policies = Get-AzPolicyDefinition |
24     --- Where-Object {$_.properties.PolicyType -match 'BuiltIn' -and $_.properties.Metadata.deprecated -ne 'True' -and $_.properties.Metadata.preview -ne 'True'} |
25     --- Select-Object @{N='Name';E=$PolicyNameResolver}, PolicyDefinitionId |
26     --- Sort-Object Name |
27     --- Foreach-Object {
28         --- "{0}": "{1}" -f $_.Name, $_.PolicyDefinitionId
29     --- }
30
31 # Export policy definition results to JSON
32 ConvertTo-Json -InputObject $policies -Depth 10 | Out-File $FilePath\builtin_policy_definitions.json
33
34 # Query policyset definitions and build hashtable
35 $policysets = Get-AzPolicySetDefinition |
36     --- Where-Object {$_.properties.PolicyType -match 'BuiltIn' -and $_.properties.Metadata.deprecated -ne 'True' -and $_.properties.Metadata.preview -ne 'True'} |
37     --- Select-Object @{N='Name';E=$PolicyNameResolver}, PolicySetDefinitionId |
38     --- Sort-Object Name |
39     --- Foreach-Object {
40         --- "{0}": "{1}" -f $_.Name, $_.PolicySetDefinitionId
41     --- }
42
43 # Export policyset definition results to JSON
44 ConvertTo-Json -InputObject $policysets -Depth 10 | Out-File $FilePath\builtin_policyset_definitions.json
```



1 - BUILD POLICY ID LIBRARY

```
1
2 "APIforFHIR_AzureAPIForFHIRShouldUseACustomermanagedKeyToEncryptDataAtRest": "/providers/Microsoft.Authorization/policyDefinitions/051cba44-2429-45b9-9649-46cec11c7119",
3 "APIforFHIR_AzureAPIForFHIRShouldUsePrivateLink": "/providers/Microsoft.Authorization/policyDefinitions/1ee56206-5dd1-42ab-b02d-8aae8b1634ce",
4 "APIforFHIR_CORSShouldNotAllowEveryDomainToAccessYourAPIForFHIR": "/providers/Microsoft.Authorization/policyDefinitions/0fea8f8a-4169-495d-8307-30ec335f387d",
5 "APIManagement_APIManagementServiceShouldUseASKUThatSupportsVirtualNetworks": "/providers/Microsoft.Authorization/policyDefinitions/73ef9241-5d81-4cd4-b483-8443d1730fe5",
6 "APIManagement_APIManagementServicesShouldDisablePublicNetworkAccess": "/providers/Microsoft.Authorization/policyDefinitions/df73bd95-24da-4a4f-96b9-4e8b94b402bd",
7 "APIManagement_APIManagementServicesShouldUseAVirtualNetwork": "/providers/Microsoft.Authorization/policyDefinitions/ef619a2c-cc4d-4d03-b2ba-8c94a834d85b",
8 "APIManagement_ConfigureAPIManagementServicesToDisablePublicNetworkAccess": "/providers/Microsoft.Authorization/policyDefinitions/7ca8c8ac-3a6e-493d-99ba-c5fa35347ff2",
9 "AppConfiguration_AppConfigurationShouldDisablePublicNetworkAccess": "/providers/Microsoft.Authorization/policyDefinitions/3d9f5e4c-9947-4579-9539-2a7695fbc187",
10 "AppConfiguration_AppConfigurationShouldUseACustomermanagedKey": "/providers/Microsoft.Authorization/policyDefinitions/967a4b4b-2da9-43c1-b7d0-f98d0d74d0b1",
11 "AppConfiguration_AppConfigurationShouldUseASKUThatSupportsPrivateLink": "/providers/Microsoft.Authorization/policyDefinitions/89c8a434-18f0-402c-8147-630a8dea54e0",
12 "AppConfiguration_AppConfigurationShouldUsePrivateLink": "/providers/Microsoft.Authorization/policyDefinitions/ca610c1d-041c-4332-9d88-7ed3094967c7",
13 "AppConfiguration_AppConfigurationStoresShouldHaveLocalAuthenticationMethodsDisabled": "/providers/Microsoft.Authorization/policyDefinitions/b08ab3ca-1062-4db3-8803-ee9cae605d6",
14 "AppConfiguration_ConfigureAppConfigurationStoresToDisableLocalAuthenticationMethods": "/providers/Microsoft.Authorization/policyDefinitions/72bc14af-4ab8-43af-b4e4-38e7983f9a1f",
15 "AppConfiguration_ConfigureAppConfigurationToDisablePublicNetworkAccess": "/providers/Microsoft.Authorization/policyDefinitions/73290fa2-dfa7-4bbb-945d-a5e23b75df2c",
16 "AppConfiguration_ConfigurePrivateDNSZonesForPrivateEndpointsConnectedToAppConfiguration": "/providers/Microsoft.Authorization/policyDefinitions/7a860e27-9ca2-4fc6-822d-c2d248c300df",
17 "AppConfiguration_ConfigurePrivateEndpointsForAppConfiguration": "/providers/Microsoft.Authorization/policyDefinitions/614ffa75-862c-456e-ad8b-eea1b0844b07",
18 "AppPlatform_AzureSpringCloudShouldUseNetworkInjection": "/providers/Microsoft.Authorization/policyDefinitions/af35e2a4-ef96-44e7-a9ae-853dd97032c4",
19 "AppService_APIAppShouldOnlyBeAccessibleOverHTTPS": "/providers/Microsoft.Authorization/policyDefinitions/b7ddfbd9-1260-477d-91fd-98bd9be789a6",
20 "AppService_APIAppsShouldUseAnAzureFileShareForItsContentDirectory": "/providers/Microsoft.Authorization/policyDefinitions/324c7761-08db-4474-9661-d1039abc92ee",
21 "AppService_AppServiceAppsShouldBeInjectedIntoAVirtualNetwork": "/providers/Microsoft.Authorization/policyDefinitions/72d04c29-f87d-4575-9731-419ff16a2757",
22 "AppService_AppServiceAppsShouldEnableOutboundNonrfc1918TrafficToAzureVirtualNetwork": "/providers/Microsoft.Authorization/policyDefinitions/33228571-70a4-4fa1-8ca1-26d0aba8d6ef",
23 "AppService_AppServiceAppsShouldUseASKUThatSupportsPrivateLink": "/providers/Microsoft.Authorization/policyDefinitions/546fe8d2-368d-4029-a418-6af48a7f61e5",
24 "AppService_AppServiceEnvironmentAppsShouldNotBeReachableOverPublicInternet": "/providers/Microsoft.Authorization/policyDefinitions/2d048aca-6479-4923-88f5-e2ac295d9af3",
25 "AppService_AppServiceEnvironmentShouldBeConfiguredWithStrongestTLCipherSuites": "/providers/Microsoft.Authorization/policyDefinitions/817dcf37-e83d-4999-a472-644eada2ea1e",
26 "AppService_AppServiceEnvironmentShouldBeProvisionedWithLatestVersions": "/providers/Microsoft.Authorization/policyDefinitions/eb4d34ab-0929-491c-bbf3-61e13da19f9a",
27 "AppService_AppServiceEnvironmentShouldDisableTLS10And11": "/providers/Microsoft.Authorization/policyDefinitions/d6545c6b-dd9d-4265-91e6-0b451e2f1c50",
28 "AppService_AppServiceEnvironmentShouldEnableInternalEncryption": "/providers/Microsoft.Authorization/policyDefinitions/fb74e86f-d351-4b8d-b034-93da7391c01f",
29 "AppService_AppServiceShouldHaveLocalAuthenticationMethodsDisabledForFTPDeployments": "/providers/Microsoft.Authorization/policyDefinitions/871b205b-57cf-4e1e-a234-492616998bf7",
30 "AppService_AppServiceShouldHaveLocalAuthenticationMethodsDisabledForSCMSiteDeployments": "/providers/Microsoft.Authorization/policyDefinitions/aede300b-d67f-480a-ae26-4b3dfb1a1fdc",
31 "AppService_AppServiceShouldUsePrivateLink": "/providers/Microsoft.Authorization/policyDefinitions/687aa49d-0982-40f8-bf6b-66d1da97a04b",
32 "AppService_AppServiceSlotsShouldHaveLocalAuthenticationMethodsDisabledForFTPDeployments": "/providers/Microsoft.Authorization/policyDefinitions/ec71c0bc-6a45-4b1f-9587-80dc83e6898c",
33 "AppService_AppServiceSlotsShouldHaveLocalAuthenticationMethodsDisabledForSCMSiteDeployments": "/providers/Microsoft.Authorization/policyDefinitions/847ef871-e2fe-4e6e-907e-4adbf71de5cf",
34 "AppService_AppServicesShouldDisablePublicNetworkAccess": "/providers/Microsoft.Authorization/policyDefinitions/63a0ac64-5d5f-4569-8a3d-df67cc1ce9d7",
35 "AppService_AuthenticationShouldBeEnabledOnYourAPIApp": "/providers/Microsoft.Authorization/policyDefinitions/c4ebc54a-46e1-481a-bee2-d4411e95d828",
36 "AppService_AuthenticationShouldBeEnabledOnYourFunctionApp": "/providers/Microsoft.Authorization/policyDefinitions/c75248c1-ea1d-4a9c-8fc9-29a6aab5da8",
37 "AppService_AuthenticationShouldBeEnabledOnYourWebApp": "/providers/Microsoft.Authorization/policyDefinitions/95bccee9-a7f8-4bec-9ee9-62c3473701fc",
38 "AppService_ConfigureAppServiceSlotsToDisableLocalAuthenticationForFTPDeployments": "/providers/Microsoft.Authorization/policyDefinitions/f493116f-3b7f-4ab3-bf80-0c2af35e46c2",
39 "AppService_ConfigureAppServiceSlotsToDisableLocalAuthenticationForSCMSites": "/providers/Microsoft.Authorization/policyDefinitions/2c034a29-2a5f-4857-b120-f800fe5549ae",
40 "AppService_ConfigureAppServicesToDisablePublicNetworkAccess": "/providers/Microsoft.Authorization/policyDefinitions/81dff7c0-4020-4b58-955d-c076a2136b56",
41 "AppService_ConfigureAppServicesToUsePrivateDNSZones": "/providers/Microsoft.Authorization/policyDefinitions/b318f84a-b872-429b-ac6d-a01b96814452",
42 "AppService_ConfigureAppServiceToDisableLocalAuthenticationForSCMSites": "/providers/Microsoft.Authorization/policyD
43 "AppService_ConfigureAppServiceToDisableLocalAuthenticationOnFTPDeployments": "/providers/Microsoft.Authorization/po
44 "AppService_CORSShouldNotAllowEveryResourceToAccessYourAPIApp": "/providers/Microsoft.Authorization/policyDefinitio
45 "AppService_CORSShouldNotAllowEveryResourceToAccessYourFunctionApps": "/providers/Microsoft.Authorization/policyDefi
46 "AppService_CORSShouldNotAllowEveryResourceToAccessYourWebApplications": "/providers/Microsoft.Authorization/policyD
47 "AppService_DiagnosticLogsInAppServicesShouldBeEnabled": "/providers/Microsoft.Authorization/policyDefinitions/b607c
48 "AppService_EnsureAPIAppHasClientCertificatesIncomingClientCertificatesSetToOn": "/providers/Microsoft.Authorization
49 "AppService_EnsureThatHTTPVersionIsTheLatestIfUsedToRunTheAPIApp": "/providers/Microsoft.Authorization/policyDefinit
50 "AppService_EnsureThatHTTPVersionIsTheLatestIfUsedToRunTheFunctionApp": "/providers/Microsoft.Authorization/policyDe
51 "AppService_EnsureThatHTTPVersionIsTheLatestIfUsedToRunTheWebApp": "/providers/Microsoft.Authorization/policyDefinit
52 "AppService_EnsureThatJavaVersionIsTheLatestIfUsedAsAPartOfTheAPIApp": "/providers/Microsoft.Authorization/policyDefinitio
```



```
1 targetScope = 'managementGroup'
2
3 // PARAMETERS
4 param policySource string = 'Bicep'
5 param policyCategory string = 'Custom'
6 param customPolicies object
7
8 // VARIABLES
9 var builtinPolicies = json(loadTextContent('./builtin_policy_definitions.json'))
10
11 // CUSTOM POLICYSETS
12 resource iam_governance 'Microsoft.Authorization/policySetDefinitions@2020-09-01' = {
13   name: 'iam_governance'
14   properties: {
15     policyType: 'Custom'
16     displayName: 'IAM Governance Initiative'
17     description: 'Identity & Access Management Governance Initiative via ${policySource}'
18     metadata: {
19       category: policyCategory
20       source: policySource
21       version: '1.0.0'
22     }
23   }
24   parameters: {}
25 }
26
27 policyDefinitions: [
28   {
29     policyDefinitionId: builtinPolicies.General_AuditUsageOfCustomRBACRules
30     policyDefinitionReferenceId: 'General_AuditUsageOfCustomRBACRules'
31     parameters: {
32       effect: {
33         value: '[parameters(\`effect\`)]'
34       }
35     }
36   }
37   {
38     policyDefinitionId: builtinPolicies.General_CustomSubscriptionOwnerRolesShouldNotExist
39     policyDefinitionReferenceId: 'General_CustomSubscriptionOwnerRolesShouldNotExist'
40     parameters: {
41       effect: {
42         value: '[parameters(\`effect\`)]'
43       }
44     }
45   }
46 ]
```



2 - LOAD POLICY ID LIBRARY AND USE IN POLICYSETS

General_AuditUsageOfCustomRBACRules: '/providers/Microsoft.Authorization/policyDefinitions/a451c1ef-c6ca-483d-87ed-f49761e3ffb5'