

Viktor Gazdag | Cloud Village | DefCon 32

# 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, DefCon31 Cloud Village, DoD C

# 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



# PROPERTIES & ALIAS

- Policy Alias and Resource Property and Modifiable
- Resourcetype



# PROPERTIES & ALIAS

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



# wucpittest2

Storage account



Overview

Properties

Monitoring

Capabilities (7)

Recommendations (0)

Tutorials

Tools + SDKs

```
"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"
},
```

## service

hierarchical namespace

Disabled

blob access tier

Hot

anonymous access

Disabled



## Security

Require secure transfer for REST API operations

Disabled

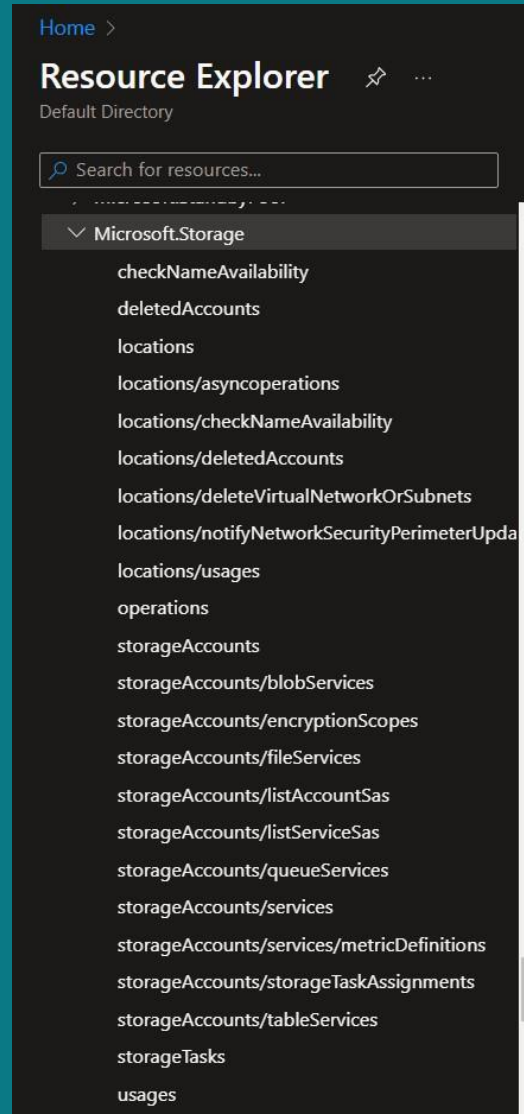
Storage account key access

Enabled

```
"policyRule": {
  "if": {
    "allof": [
      {
        "field": "type",
        "equals": "Microsoft.Storage/storageAccounts"
      },
      {
        "anyOf": [
          {
            "allof": [
              {
                "value": "[requestContext().apiVersion]",
                "less": "2019-04-01"
              },
              {
                "field": "Microsoft.Storage/storageAccounts/supportsHttpsTrafficOnly",
                "exists": "false"
              }
            ]
          },
          {
            "field": "Microsoft.Storage/storageAccounts/supportsHttpsTrafficOnly",
            "equals": "false"
          }
        ]
      }
    ]
  }
}
```

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

Microsoft Entra ID is the successor to Azure Active Directory (AAD), offering a unified identity and access management solution across Microsoft and third-party applications.

Entra ID provides enhanced security features, including Conditional Access, Multi-Factor Authentication (MFA), and Privileged Identity Management (PIM), alongside core identity management capabilities like user and group management.

While Azure AD was primarily designed for managing identities within the Azure ecosystem, Entra ID offers a broader, cloud-native identity platform that integrates seamlessly with various Microsoft and non-Microsoft services.

Entra ID also introduces new features like Passwordless Authentication and Self-Service Password Reset, aiming to improve user experience and security. The transition from Azure AD to Entra ID represents Microsoft's commitment to a more integrated and secure identity management framework.

For organizations already using Azure AD, the migration to Entra ID is a gradual process, allowing them to leverage the new features and security enhancements while maintaining compatibility with existing applications and workflows.

Entra ID's unified architecture simplifies identity management across the organization, providing a single source of truth for user identities and access permissions, ultimately leading to improved security and operational efficiency.

As Microsoft continues to evolve its cloud ecosystem, Entra ID is positioned as the central hub for identity management, ensuring secure and seamless access to critical resources for users and applications alike.

Organizations looking to optimize their identity management strategy should consider the benefits of Entra ID, including enhanced security, improved user experience, and the ability to manage identities across a diverse range of cloud and on-premise environments.

The transition to Entra ID is a strategic move towards a more secure and integrated identity management solution, enabling organizations to better protect their digital assets and streamline their access management processes.

# 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](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 }
```

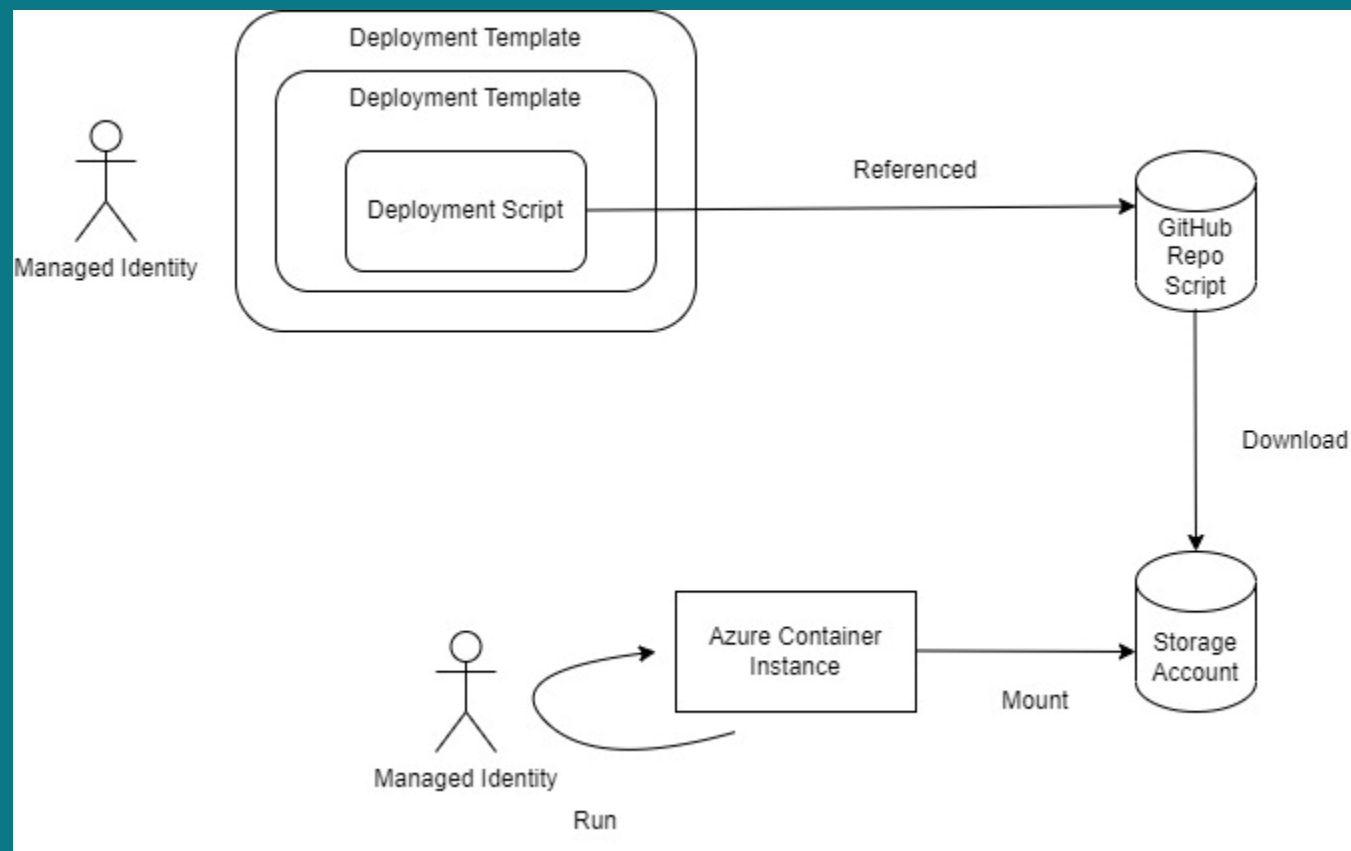
# PROOF OF CONCEPT

- 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](#)

**i** 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

Ti... : Tue Jul 30 2024 00:00:00 GMT+0100 (British Summer Ti... [Add Filter](#)

21 items.

Operation name	Status	Time	Time stamp	Subscription	Event initiated by	Resource type
> <b>i</b> Delete Container Group	Succeeded	28 minutes ...	Tue Jul 30 2...	DFCVT	managed_identity	Microsoft.ContainerInstance/containerGroups
> <b>i</b> Update User Assigned Identity Create	Succeeded	29 minutes ...	Tue Jul 30 2...	DFCVT	managed_identity	Microsoft.ManagedIdentity/userAssignedIdent...
> <b>i</b> Update User Assigned Identity Create	Succeeded	29 minutes ...	Tue Jul 30 2...	DFCVT	managed_identity	Microsoft.ManagedIdentity/userAssignedIdent...
> <b>i</b> Create role assignment	Succeeded	38 minutes ...	Tue Jul 30 2...	DFCVT	managed_identity	Microsoft.Authorization/roleAssignments
> <b>i</b> Create role assignment	Succeeded	38 minutes ...	Tue Jul 30 2...	DFCVT	managed_identity	Microsoft.Authorization/roleAssignments
> <b>i</b> Create role assignment	Succeeded	38 minutes ...	Tue Jul 30 2...	DFCVT	managed_identity	Microsoft.Authorization/roleAssignments
> <b>i</b> Update Storage Account Create	Succeeded	39 minutes ...	Tue Jul 30 2...	DFCVT	managed_identity	Microsoft.Storage/storageAccounts
> <b>i</b> Update Storage Account Create	Succeeded	40 minutes ...	Tue Jul 30 2...	DFCVT	managed_identity	Microsoft.Storage/storageAccounts
> <b>i</b> Create role assignment	Succeeded	59 minutes ...	Tue Jul 30 2...	DFCVT	cybernewbie1337@gmail...	Microsoft.Authorization/roleAssignments
> <b>i</b> Create policy assignment	Succeeded	59 minutes ...	Tue Jul 30 2...	DFCVT	cybernewbie1337@gmail...	Microsoft.Authorization/policyAssignments
> <b>i</b> Create policy definition	Succeeded	an hour ago	Tue Jul 30 2...	DFCVT	cybernewbie1337@gmail...	Microsoft.Authorization/policyDefinitions

# AZURE AUDIT LOG

## Create role assignment

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

[+ New alert rule](#)

Summary

JSON

Change 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"/> |  <b>[..]</b>             |
| <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/resourcegroupoft.ManagedIdentity/userAs"]
mi_wucpi2	Included Updat...		"AccountEnabled, AppPrincServicePrincipalName, CredManagedIdentityResourceId"
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](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-lab8d0634bb2>

# 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/@vladimirtul/elevating-privileges-through-azure-policy-872298cf673f>

# QUESTIONS

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