O'REILLY®

Azure Governance and Compliance

Introduction

Reza Salehi

Cloud Consultant and Trainer

Azure Governance and Compliance

- Governance
- Azure Policy (overview, definition, effect, exemption, remediation)
- Assigning Azure Policies
- Azure Policy Initiative
- Common use cases (PCI DSS, HITRUST/HIPPA, SOC2)

Course Repository

https://github.com/zaalion/oreilly-policy-governance

Governance

Azure Governance

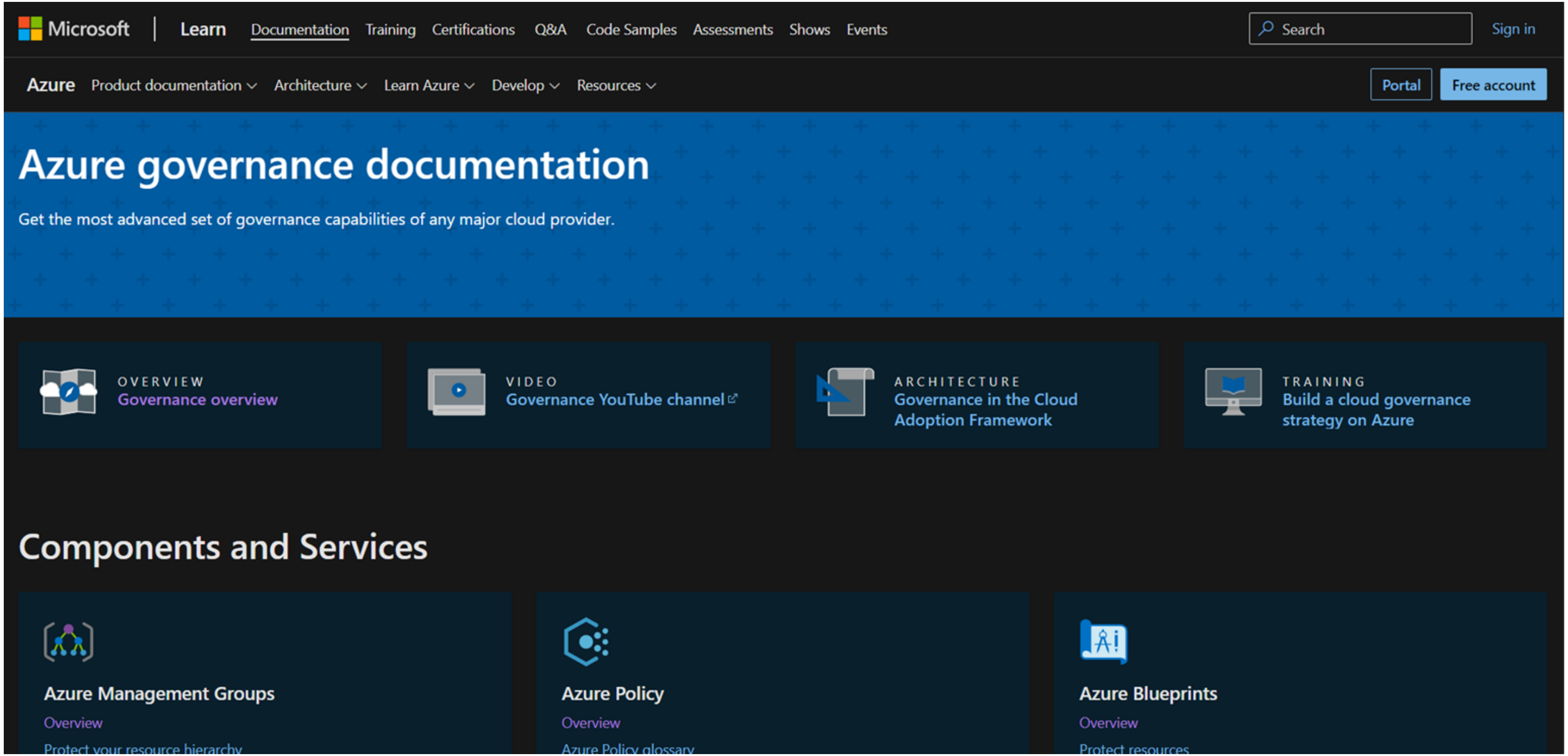
“Governance provides mechanisms and processes to maintain control over your applications and resources in Azure.”

https://learn.microsoft.com/en-us/azure/governance/azure-management#govern

Azure Governance

- Enforce company standards
- Ensure security best practices are followed
- Comply with government and industry standards

https://learn.microsoft.com/en-us/azure/governance/azure-management#govern



Azure governance documentation

Get the most advanced set of governance capabilities of any major cloud provider.

OVERVIEW
Governance overview

VIDEO
Governance YouTube channel

ARCHITECTURE
Governance in the Cloud Adoption Framework

TRAINING
Build a cloud governance strategy on Azure

Components and Services

Azure Management Groups
Overview
Protect your resource hierarchy

Azure Policy
Overview
Azure Policy glossary

Azure Blueprints
Overview
Protect resources

https://learn.microsoft.com/en-us/azure/governance/

Azure Compliance

“Comply with legal or regulatory standards, start here to learn about compliance in Azure.”

https://learn.microsoft.com/en-us/azure/governance/azure-management#govern

Enforcing Compliance Commitments

Azure Compliance

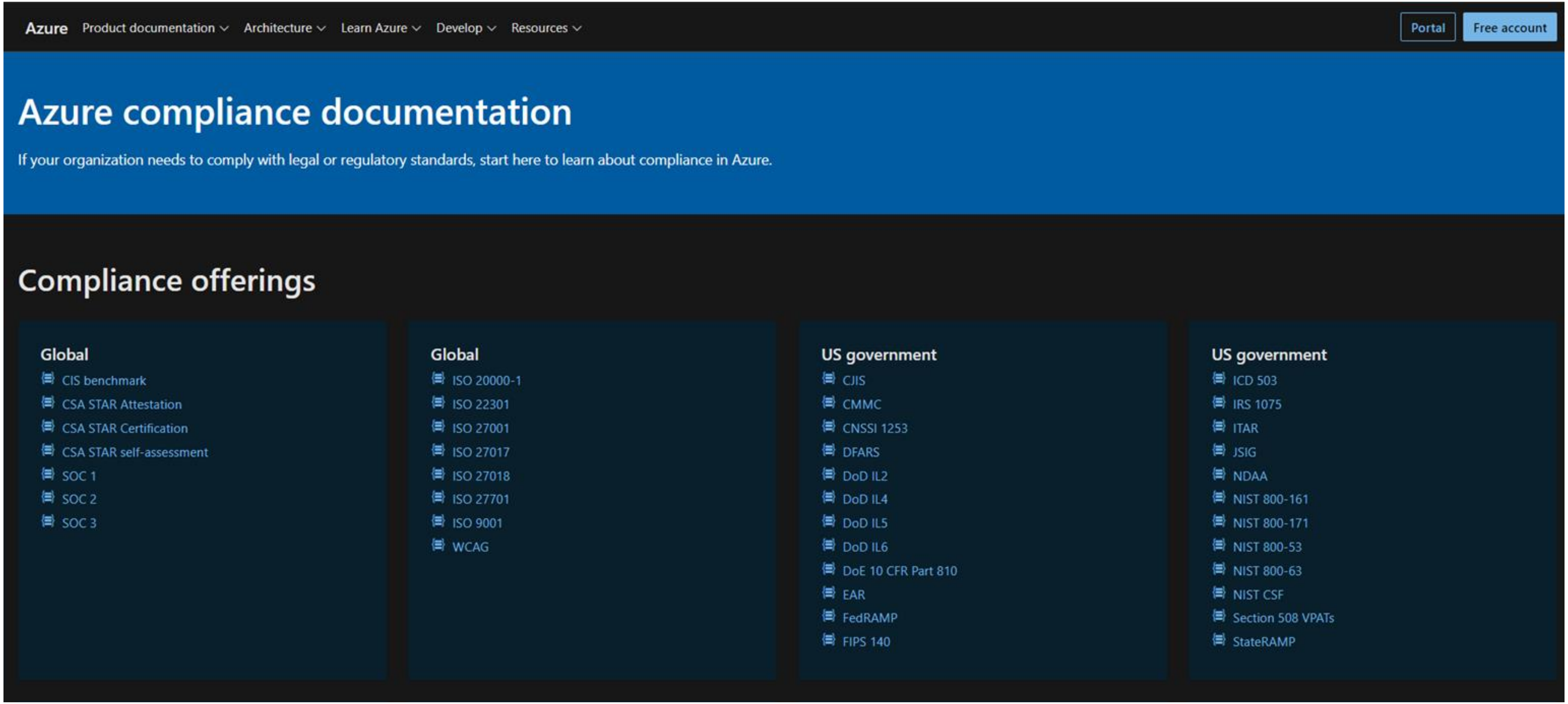
- Global
- US government
- Financial services
- Healthcare and life sciences
- Automotive, education, energy, media, and telecommunication

https://learn.microsoft.com/en-us/azure/governance/azure-management#govern

Azure Compliance

- Regional - Americas
- Regional - Asia Pacific
- Regional - EMEA

https://learn.microsoft.com/en-us/azure/governance/azure-management#govern



Azure compliance documentation

If your organization needs to comply with legal or regulatory standards, start here to learn about compliance in Azure.

Compliance offerings

Global

- CIS benchmark
- CSA STAR Attestation
- CSA STAR Certification
- CSA STAR self-assessment
- SOC 1
- SOC 2
- SOC 3

Global

- ISO 20000-1
- ISO 22301
- ISO 27001
- ISO 27017
- ISO 27018
- ISO 27701
- ISO 9001
- WCAG

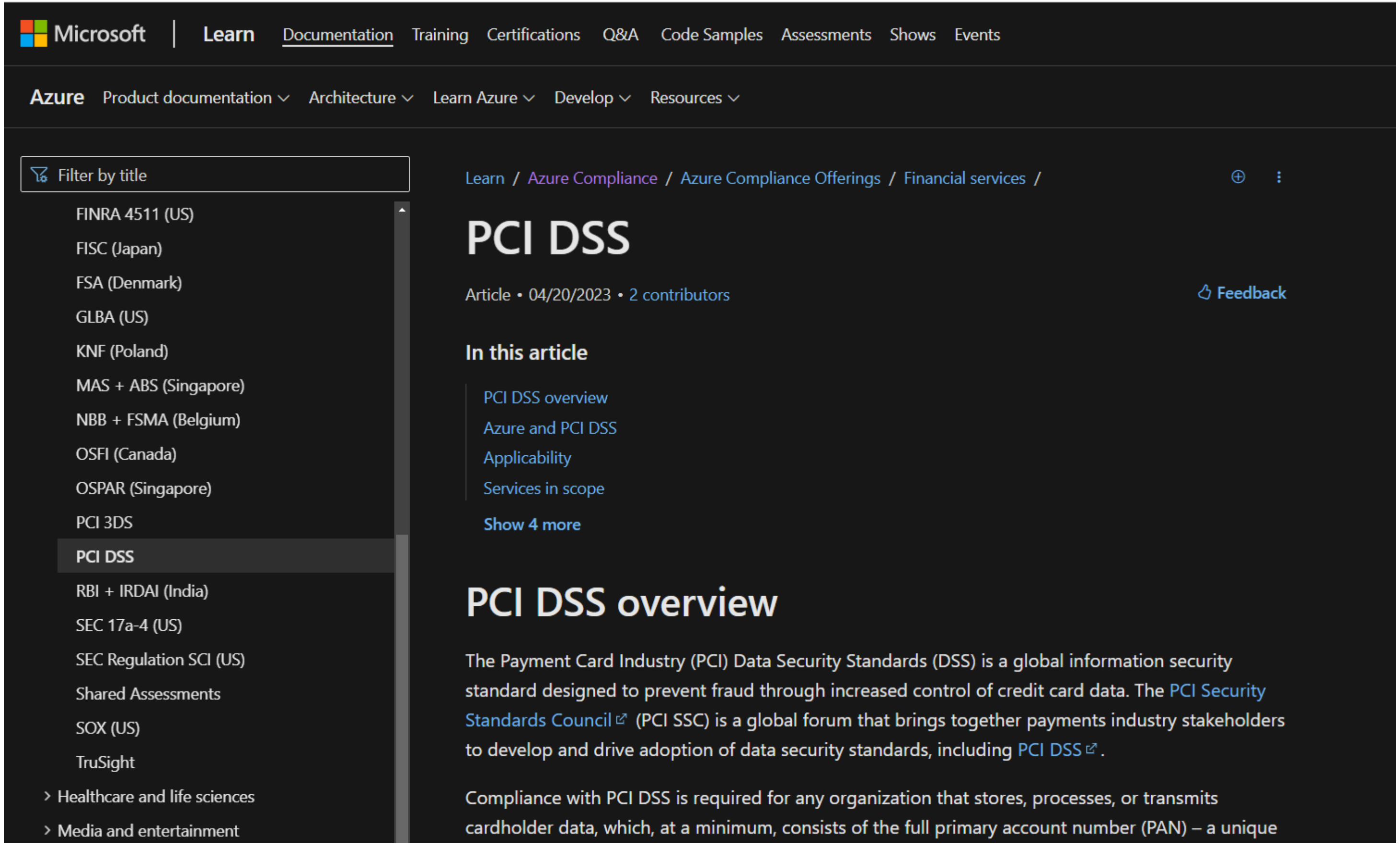
US government

- CJIS
- CMMC
- CNSSI 1253
- DFARS
- DoD IL2
- DoD IL4
- DoD IL5
- DoD IL6
- DoE 10 CFR Part 810
- EAR
- FedRAMP
- FIPS 140

US government

- ICD 503
- IRS 1075
- ITAR
- JSIG
- NDAA
- NIST 800-161
- NIST 800-171
- NIST 800-53
- NIST 800-63
- NIST CSF
- Section 508 VPATs
- StateRAMP

https://learn.microsoft.com/en-us/azure/compliance/



PCI DSS

Article • 04/20/2023 • 2 contributors

In this article

- PCI DSS overview
- Azure and PCI DSS
- Applicability
- Services in scope

Show 4 more

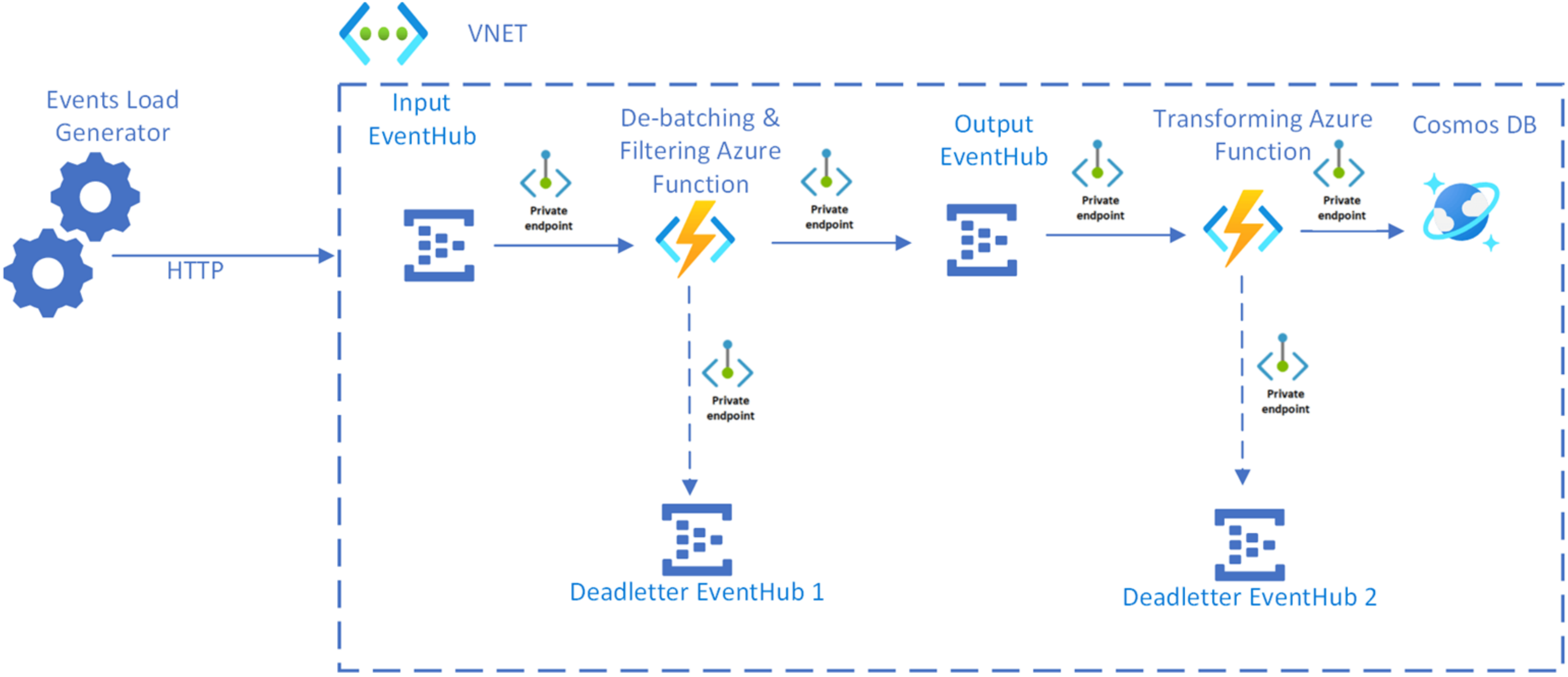
PCI DSS overview

The Payment Card Industry (PCI) Data Security Standards (DSS) is a global information security standard designed to prevent fraud through increased control of credit card data. The PCI Security Standards Council (PCI SSC) is a global forum that brings together payments industry stakeholders to develop and drive adoption of data security standards, including PCI DSS.

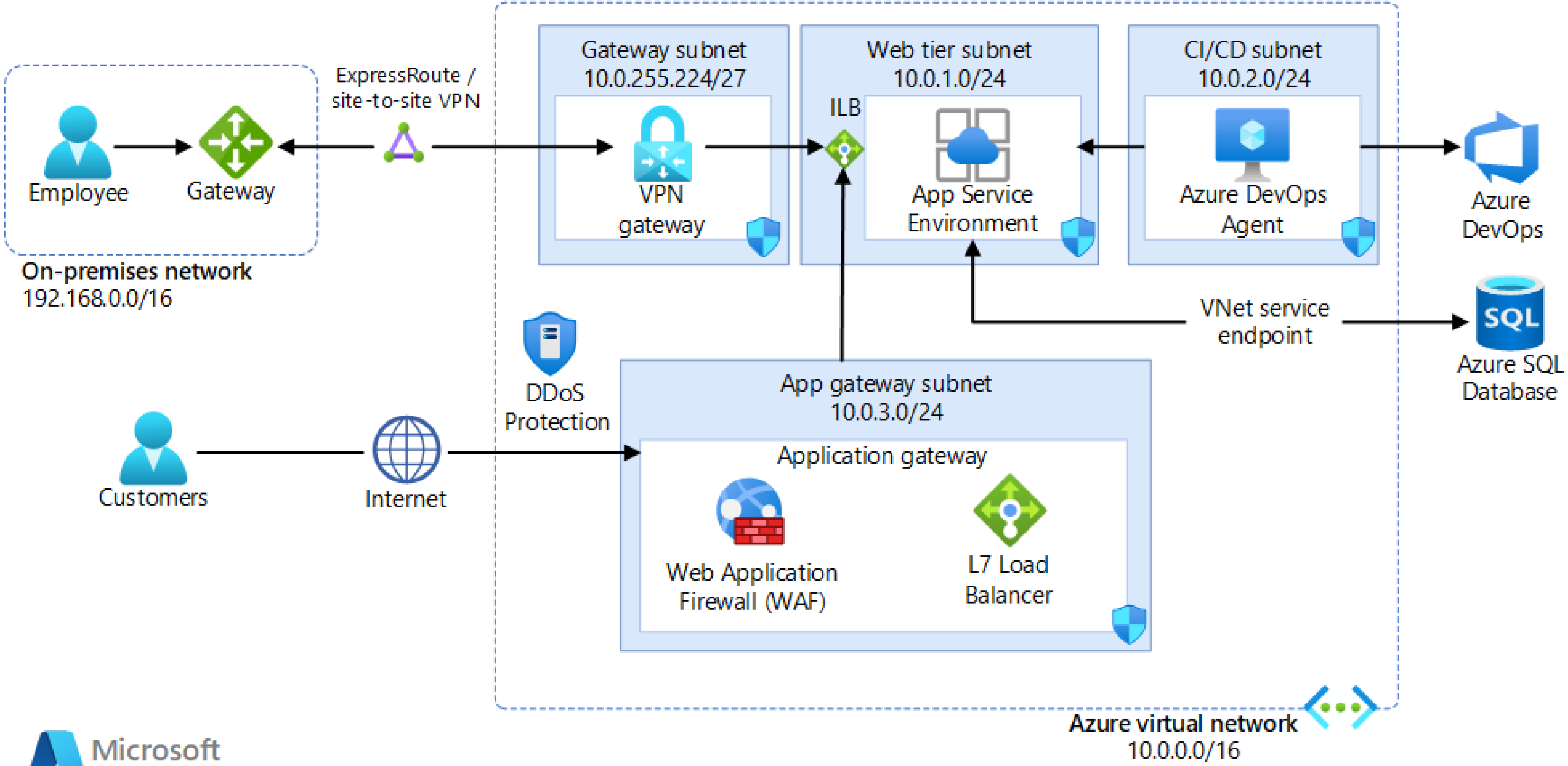
Compliance with PCI DSS is required for any organization that stores, processes, or transmits cardholder data, which, at a minimum, consists of the full primary account number (PAN) – a unique

https://learn.microsoft.com/en-us/azure/compliance/offerings/offering-pci-dss

Enforcing Azure Best Practices

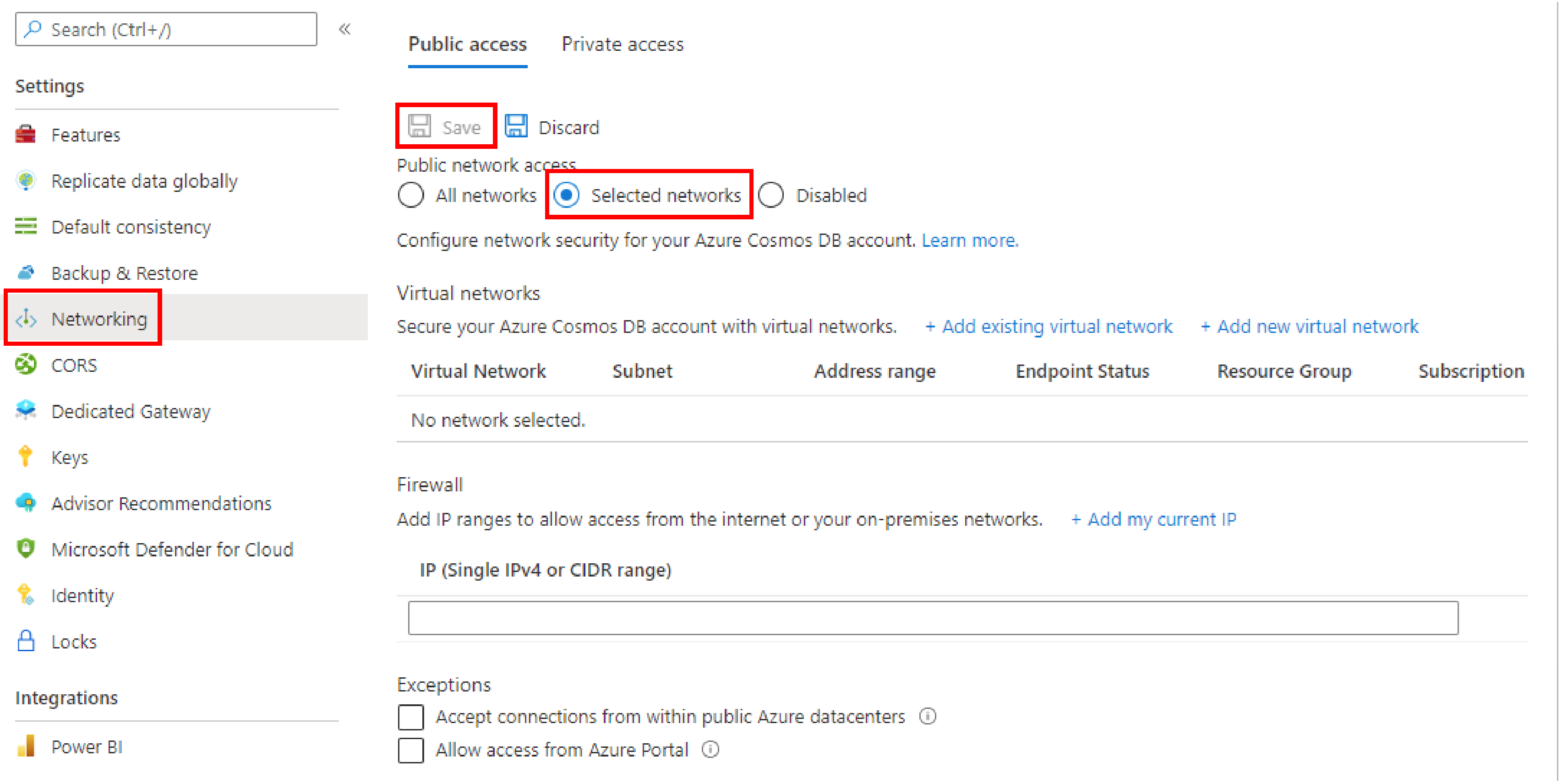


https://learn.microsoft.com/en-us/azure/architecture/solution-ideas/articles/serverless-event-processing-private-link



Microsoft Azure

https://learn.microsoft.com/en-us/azure/architecture/example-scenario/apps/fully-managed-secure-apps



Public network access

○ All networks ● Selected networks ○ Disabled

Configure network security for your Azure Cosmos DB account. Learn more.

Virtual networks

Secure your Azure Cosmos DB account with virtual networks. + Add existing virtual network + Add new virtual network

Virtual Network	Subnet	Address range	Endpoint Status	Resource Group	Subscription
No network selected.					

Firewall

Add IP ranges to allow access from the internet or your on-premises networks. + Add my current IP

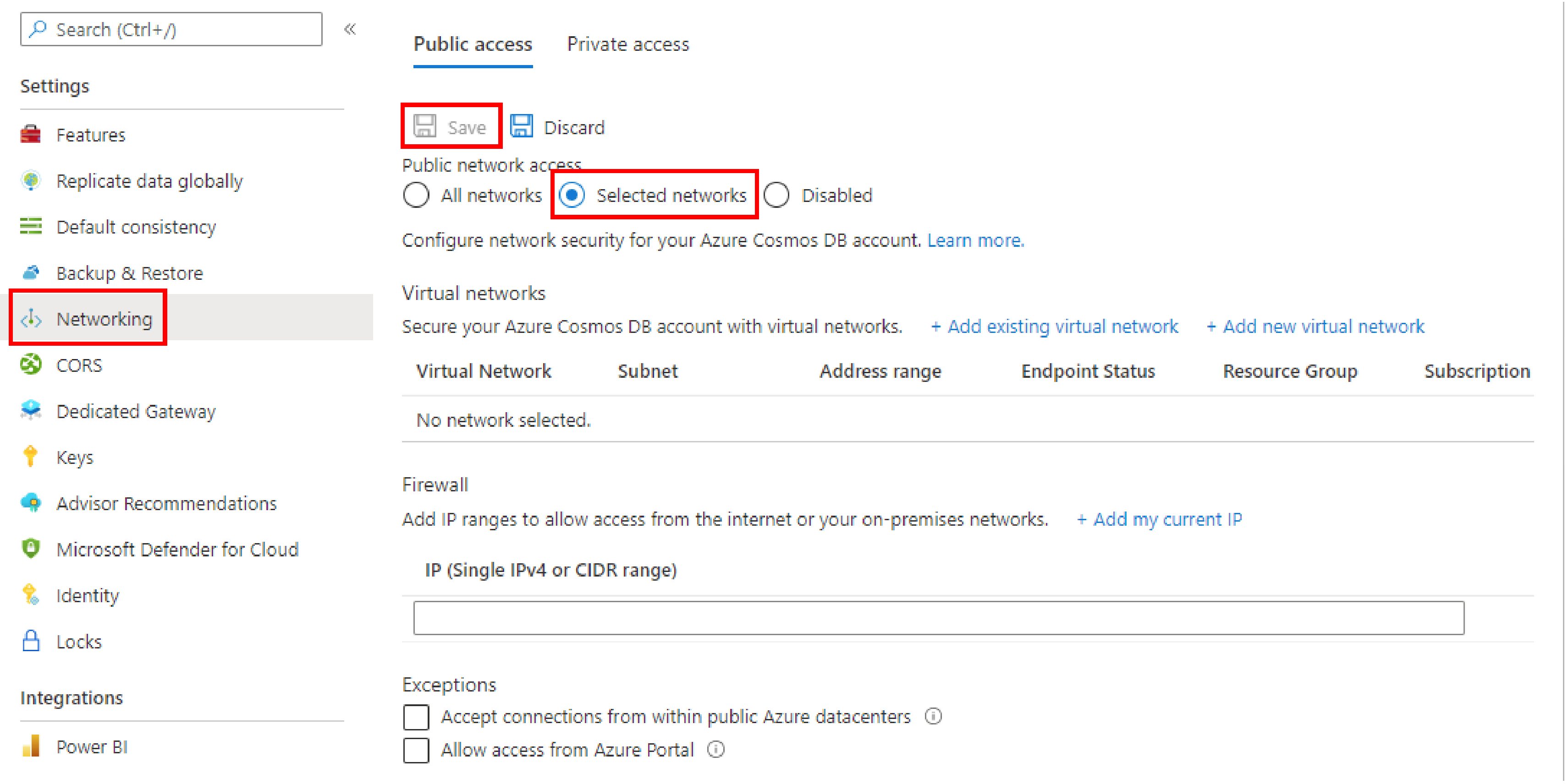
IP (Single IPv4 or CIDR range)

Exceptions

□ Accept connections from within public Azure datacenters ⓘ

□ Allow access from Azure Portal ⓘ

https://learn.microsoft.com/en-us/azure/cosmos-db/how-to-configure-firewall



Settings

- Features
- Replicate data globally
- Default consistency
- Backup & Restore
- Networking
- CORS
- Dedicated Gateway
- Keys
- Advisor Recommendations
- Microsoft Defender for Cloud
- Identity
- Locks

Integrations

- Power BI

Public access | Private access

Save | Discard

Public network access

○ All networks ● Selected networks ○ Disabled

Configure network security for your Azure Cosmos DB account. Learn more.

Virtual networks

Secure your Azure Cosmos DB account with virtual networks. + Add existing virtual network + Add new virtual network

Virtual Network	Subnet	Address range	Endpoint Status	Resource Group	Subscription
No network selected.					

Firewall

Add IP ranges to allow access from the internet or your on-premises networks. + Add my current IP

IP (Single IPv4 or CIDR range)

Exceptions

□ Accept connections from within public Azure datacenters ⓘ

□ Allow access from Azure Portal ⓘ

https://learn.microsoft.com/en-us/azure/cosmos-db/how-to-configure-firewall

Azure Best Practices

https://learn.microsoft.com/en-us/azure/governance/azure-management#govern

Azure Policy

Azure Policy

Azure Policy helps to **govern** your Azure resources and meet the compliance requirements.

https://docs.microsoft.com/en-us/azure/governance/policy/overview

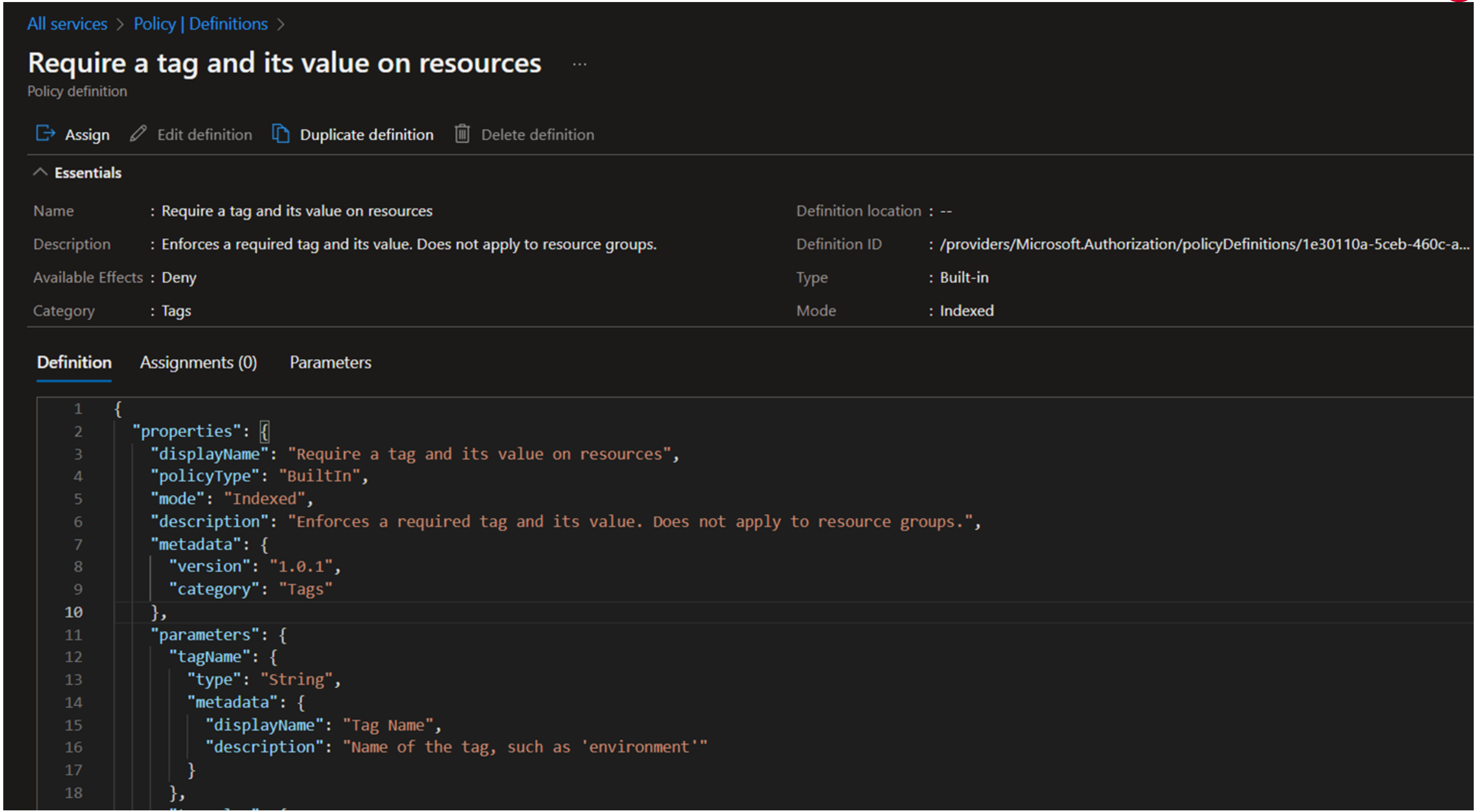
Azure Policy

- Enforce organizational standards
- Assess compliance at-scale
- Several built-in policy definitions
- Create your own custom policy definition

https://docs.microsoft.com/en-us/azure/governance/policy/overview

Azure Best Practices

https://learn.microsoft.com/en-us/azure/governance/azure-management#govern



Require a tag and its value on resources

Policy definition

Name : Require a tag and its value on resources

Description : Enforces a required tag and its value. Does not apply to resource groups.

Available Effects : Deny

Category : Tags

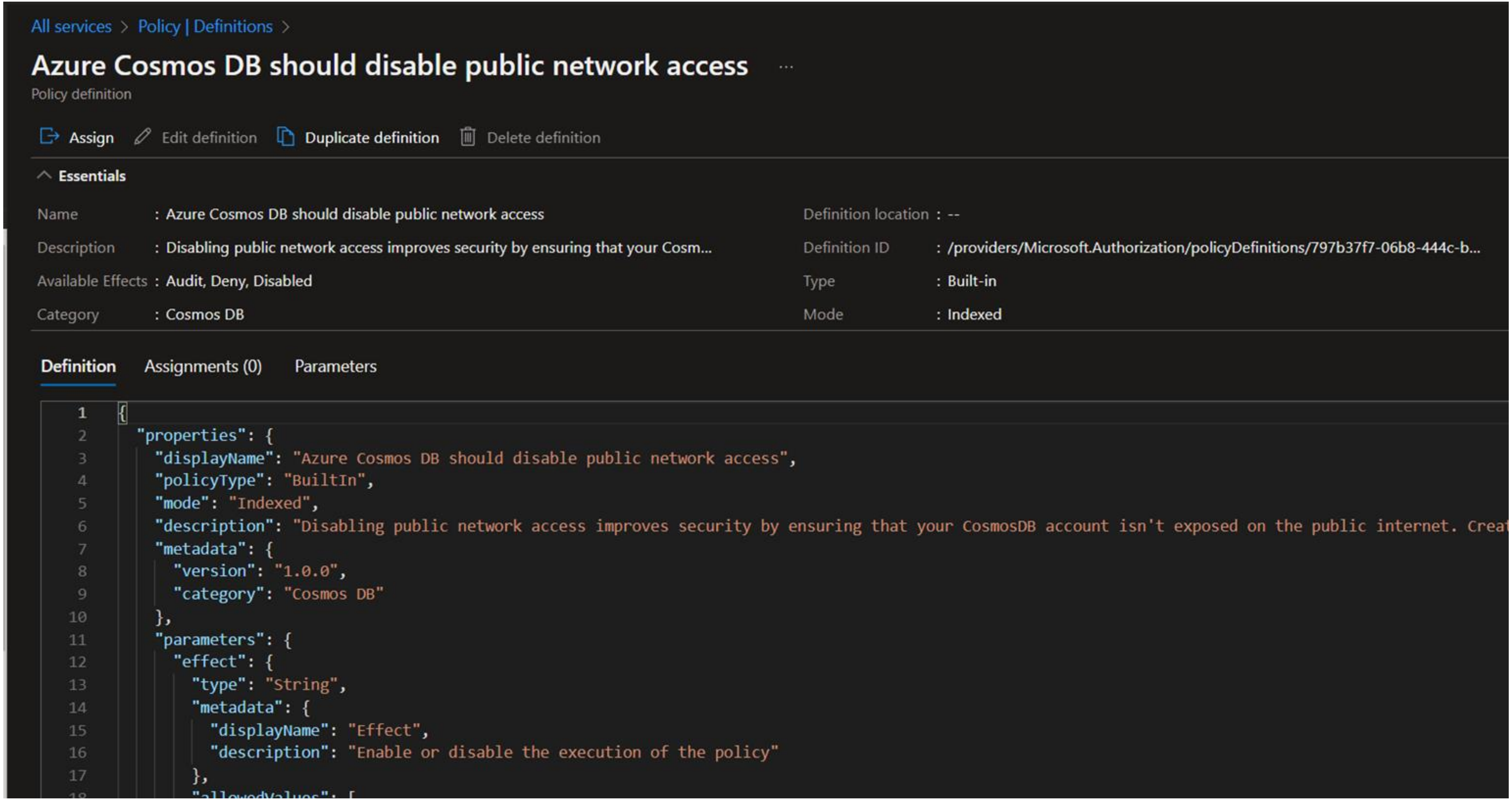
Definition location : --

Definition ID : /providers/Microsoft.Authorization/policyDefinitions/1e30110a-5ceb-460c-a...

Type : Built-in

Mode : Indexed

```
{
  "properties": {
    "displayName": "Require a tag and its value on resources",
    "policyType": "BuiltIn",
    "mode": "Indexed",
    "description": "Enforces a required tag and its value. Does not apply to resource groups.",
    "metadata": {
      "version": "1.0.1",
      "category": "Tags"
    },
    "parameters": {
      "tagName": {
        "type": "String",
        "metadata": {
          "displayName": "Tag Name",
          "description": "Name of the tag, such as 'environment'"
        }
      },
```



All services > Policy | Definitions >

Azure Cosmos DB should disable public network access ...

Policy definition

Essentials

Name : Azure Cosmos DB should disable public network access

Description : Disabling public network access improves security by ensuring that your Cosm...

Available Effects : Audit, Deny, Disabled

Category : Cosmos DB

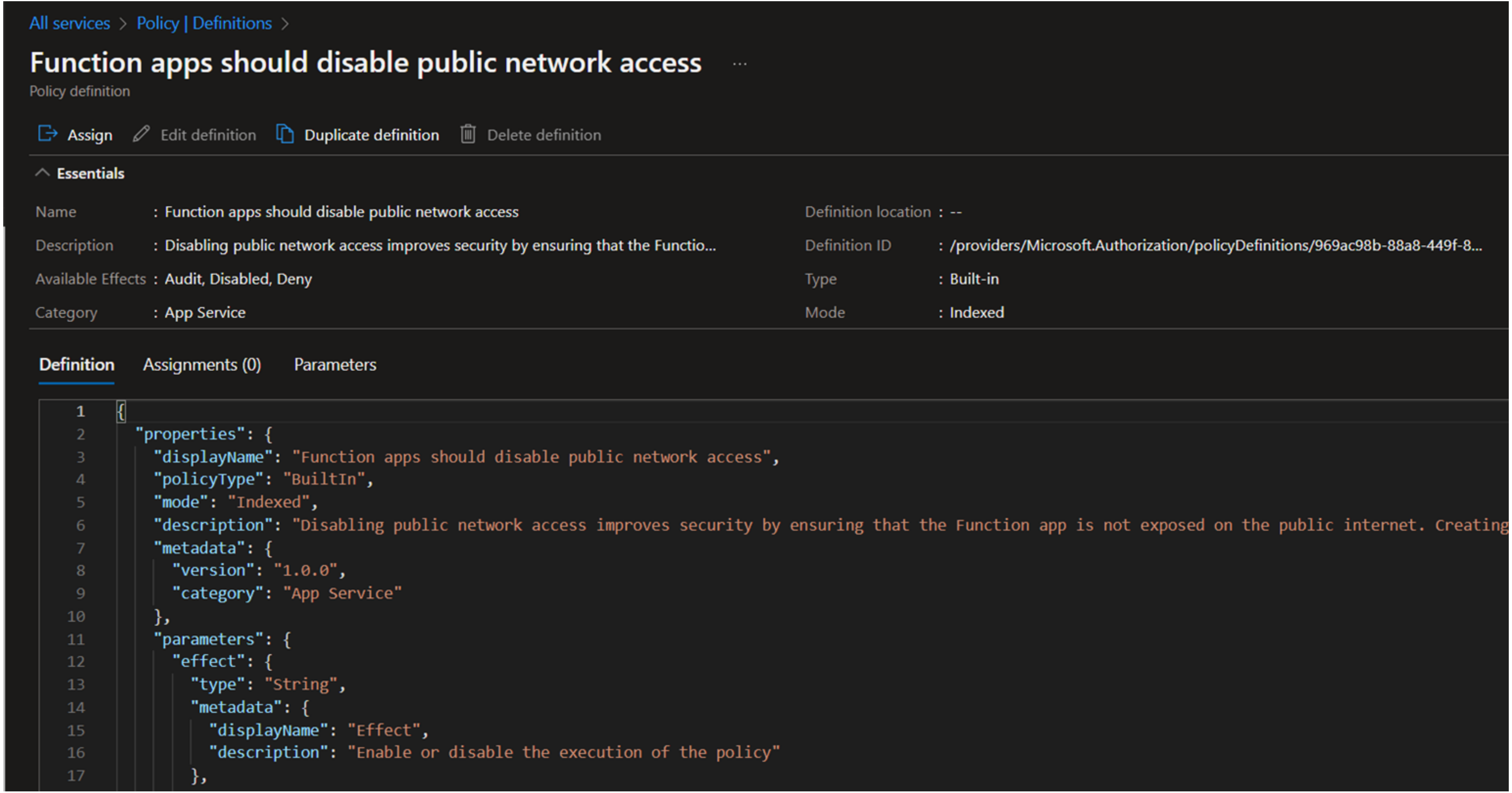
Definition location : --

Definition ID : /providers/Microsoft.Authorization/policyDefinitions/797b37f7-06b8-444c-b...

Type : Built-in

Mode : Indexed

```
{
  "properties": {
    "displayName": "Azure Cosmos DB should disable public network access",
    "policyType": "BuiltIn",
    "mode": "Indexed",
    "description": "Disabling public network access improves security by ensuring that your CosmosDB account isn't exposed on the public internet. Creat
    "metadata": {
      "version": "1.0.0",
      "category": "Cosmos DB"
    },
    "parameters": {
      "effect": {
        "type": "String",
        "metadata": {
          "displayName": "Effect",
          "description": "Enable or disable the execution of the policy"
        },
        "allowedValues": [
```

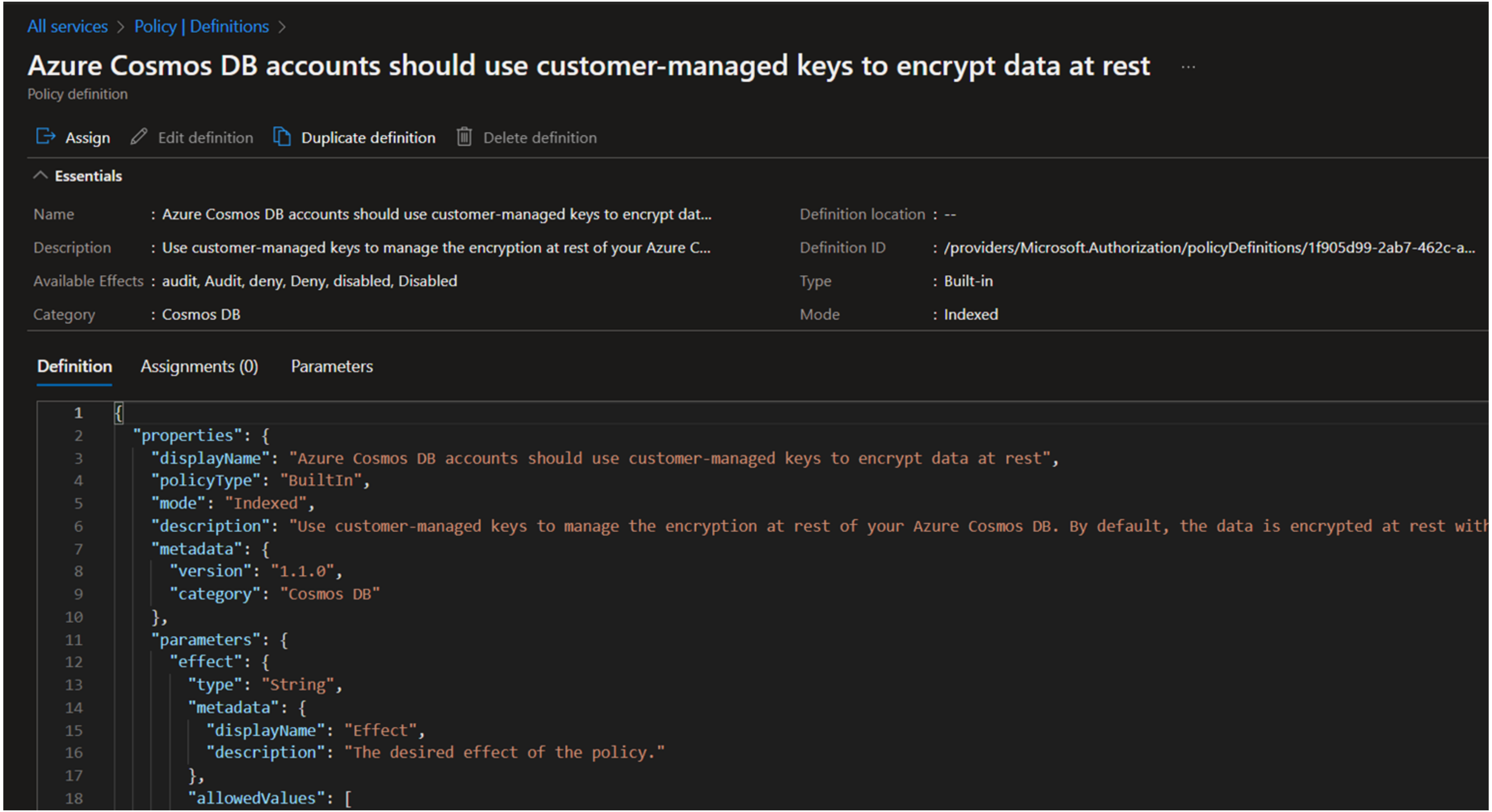


Function apps should disable public network access

Policy definition

Name	: Function apps should disable public network access	Definition location	: --
Description	: Disabling public network access improves security by ensuring that the Functio...	Definition ID	: /providers/Microsoft.Authorization/policyDefinitions/969ac98b-88a8-449f-8...
Available Effects	: Audit, Disabled, Deny	Type	: Built-in
Category	: App Service	Mode	: Indexed

```
{
  "properties": {
    "displayName": "Function apps should disable public network access",
    "policyType": "BuiltIn",
    "mode": "Indexed",
    "description": "Disabling public network access improves security by ensuring that the Function app is not exposed on the public internet. Creating
    "metadata": {
      "version": "1.0.0",
      "category": "App Service"
    },
    "parameters": {
      "effect": {
        "type": "String",
        "metadata": {
          "displayName": "Effect",
          "description": "Enable or disable the execution of the policy"
        },
```



All services > Policy | Definitions >

Azure Cosmos DB accounts should use customer-managed keys to encrypt data at rest

Policy definition

Essentials

Name	: Azure Cosmos DB accounts should use customer-managed keys to encrypt dat...
Description	: Use customer-managed keys to manage the encryption at rest of your Azure C...
Available Effects	: audit, Audit, deny, Deny, disabled, Disabled
Category	: Cosmos DB
Definition location	: --
Definition ID	: /providers/Microsoft.Authorization/policyDefinitions/1f905d99-2ab7-462c-a...
Type	: Built-in
Mode	: Indexed

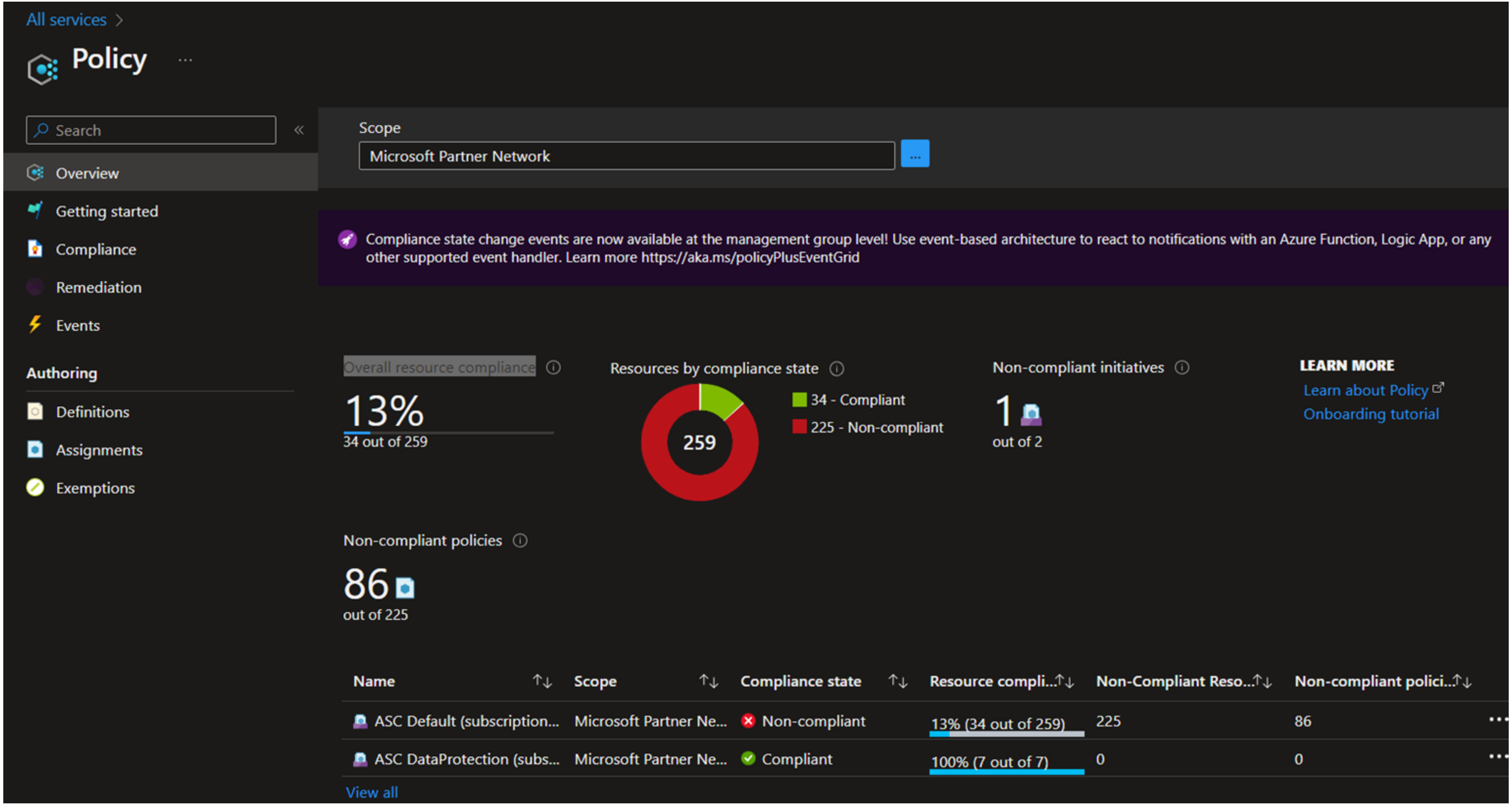
```
{
  "properties": {
    "displayName": "Azure Cosmos DB accounts should use customer-managed keys to encrypt data at rest",
    "policyType": "BuiltIn",
    "mode": "Indexed",
    "description": "Use customer-managed keys to manage the encryption at rest of your Azure Cosmos DB. By default, the data is encrypted at rest with
    "metadata": {
      "version": "1.1.0",
      "category": "Cosmos DB"
    },
    "parameters": {
      "effect": {
        "type": "String",
        "metadata": {
          "displayName": "Effect",
          "description": "The desired effect of the policy."
        },
        "allowedValues": [
```

Azure Policy Overview Portal

Azure Policy Overview

- Resources by compliance state
- Overall resource compliance
- Non-compliant initiatives
- Non-compliant policies

https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Overview



All services >

Policy ···

Search

- Overview
- Getting started
- Compliance
- Remediation
- Events

Authoring

- Definitions
- Assignments
- Exemptions

Scope

Microsoft Partner Network ...

Compliance state change events are now available at the management group level! Use event-based architecture to react to notifications with an Azure Function, Logic App, or any other supported event handler. Learn more https://aka.ms/policyPlusEventGrid

Overall resource compliance ⓘ

13%

34 out of 259

Resources by compliance state ⓘ

259

🟩 34 - Compliant

🟥 225 - Non-compliant

Non-compliant initiatives ⓘ

1

out of 2

LEARN MORE

Learn about Policy

Onboarding tutorial

Non-compliant policies ⓘ

86

out of 225

Name ↑↓	Scope ↑↓	Compliance state ↑↓	Resource compli...↑↓	Non-Compliant Reso...↑↓	Non-compliant polici...↑↓
ASC Default (subscription...	Microsoft Partner Ne...	✗ Non-compliant	13% (34 out of 259)	225	86
ASC DataProtection (subs...	Microsoft Partner Ne...	✓ Compliant	100% (7 out of 7)	0	0

View all

Azure Policy Definition Structure

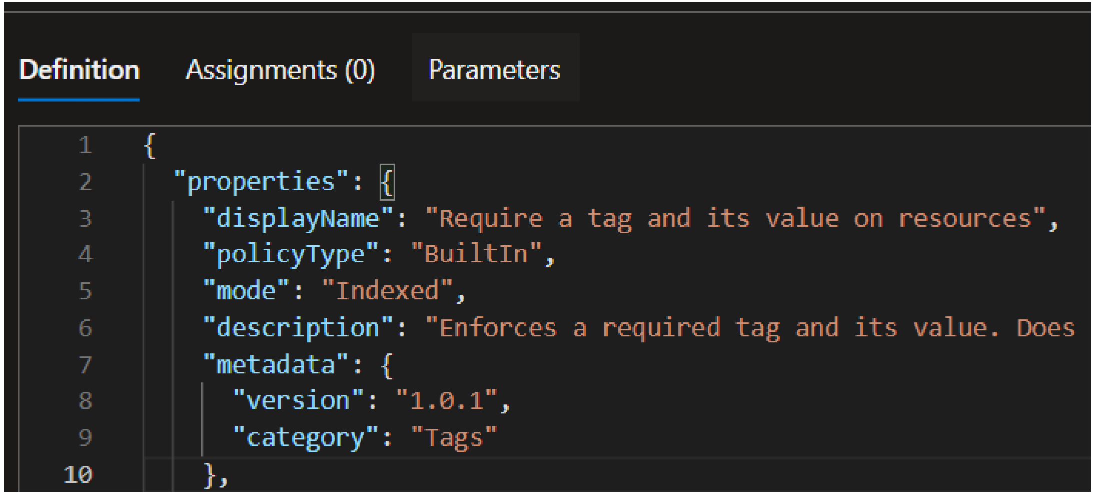
Azure Policy Definition Structure

- Type
- Display name, description
- Mode
- Metadata
- Parameters
- Policy rule (logical evaluation, effect)

https://learn.microsoft.com/en-us/azure/governance/policy/concepts/definition-structure

Azure Policy Definition: Display Name

User-friendly name

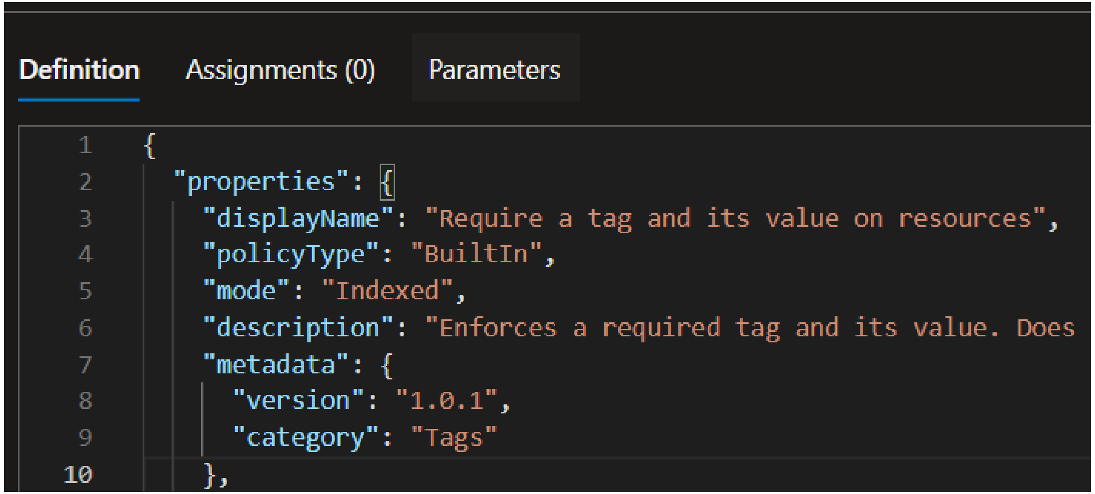


```
{
  "properties": {
    "displayName": "Require a tag and its value on resources",
    "policyType": "BuiltIn",
    "mode": "Indexed",
    "description": "Enforces a required tag and its value. Does
    "metadata": {
      "version": "1.0.1",
      "category": "Tags"
    },
```

https://learn.microsoft.com/en-us/azure/governance/policy/concepts/definition-structure

Azure Policy Definition: Description

User-friendly description

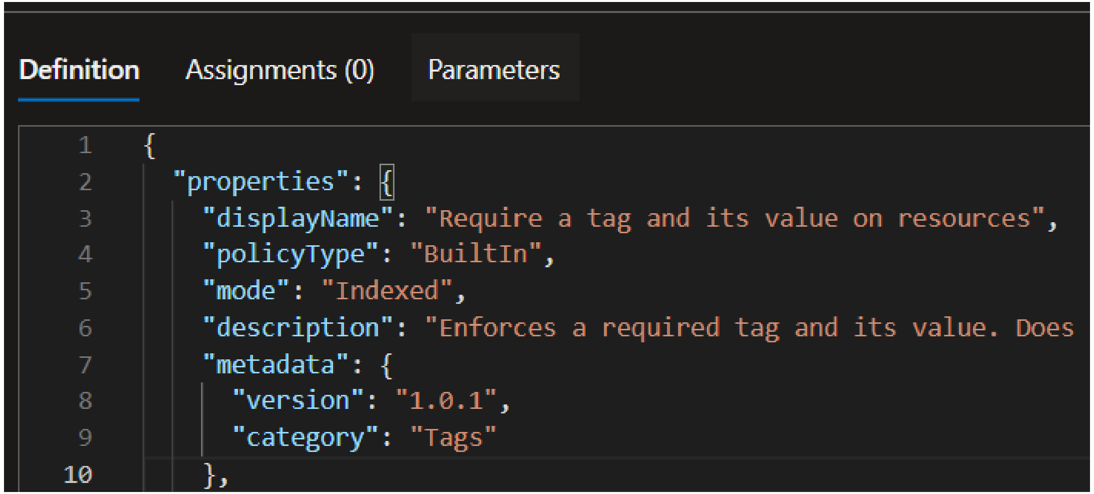


```
{
  "properties": {
    "displayName": "Require a tag and its value on resources",
    "policyType": "BuiltIn",
    "mode": "Indexed",
    "description": "Enforces a required tag and its value. Does
    "metadata": {
      "version": "1.0.1",
      "category": "Tags"
    },
```

https://learn.microsoft.com/en-us/azure/governance/policy/concepts/definition-structure

Azure Policy Definition: Type

- Built-in
- Custom
- Static

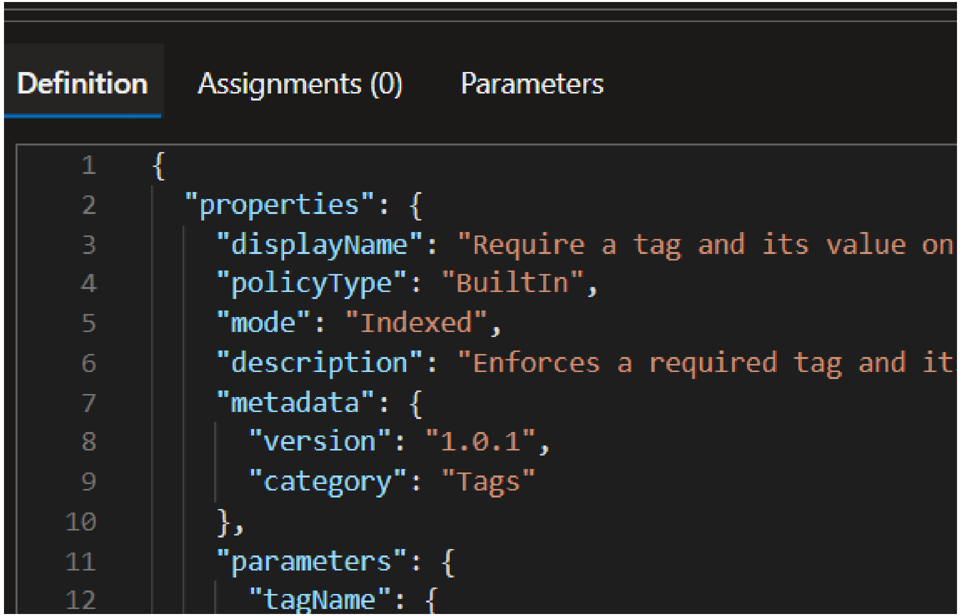


```
{
  "properties": {
    "displayName": "Require a tag and its value on resources",
    "policyType": "BuiltIn",
    "mode": "Indexed",
    "description": "Enforces a required tag and its value. Does
    "metadata": {
      "version": "1.0.1",
      "category": "Tags"
    },
```

https://learn.microsoft.com/en-us/azure/governance/policy/concepts/definition-structure

Azure Policy Definition: Metadata

- Optional property
- 1024 characters

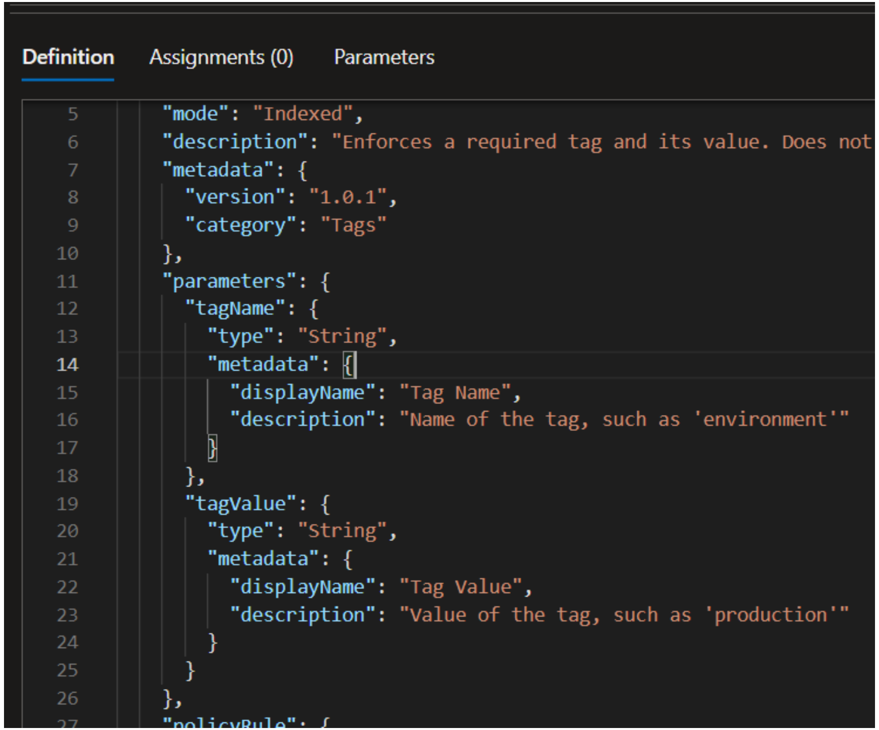


```
{
  "properties": {
    "displayName": "Require a tag and its value on
    "policyType": "BuiltIn",
    "mode": "Indexed",
    "description": "Enforces a required tag and it
    "metadata": {
      "version": "1.0.1",
      "category": "Tags"
    },
    "parameters": {
      "tagName": {
```

https://learn.microsoft.com/en-us/azure/governance/policy/concepts/definition-structure

Azure Policy Definition: Parameters

- Policy parameters
- Tag name/value
- Region/location
- Etc.

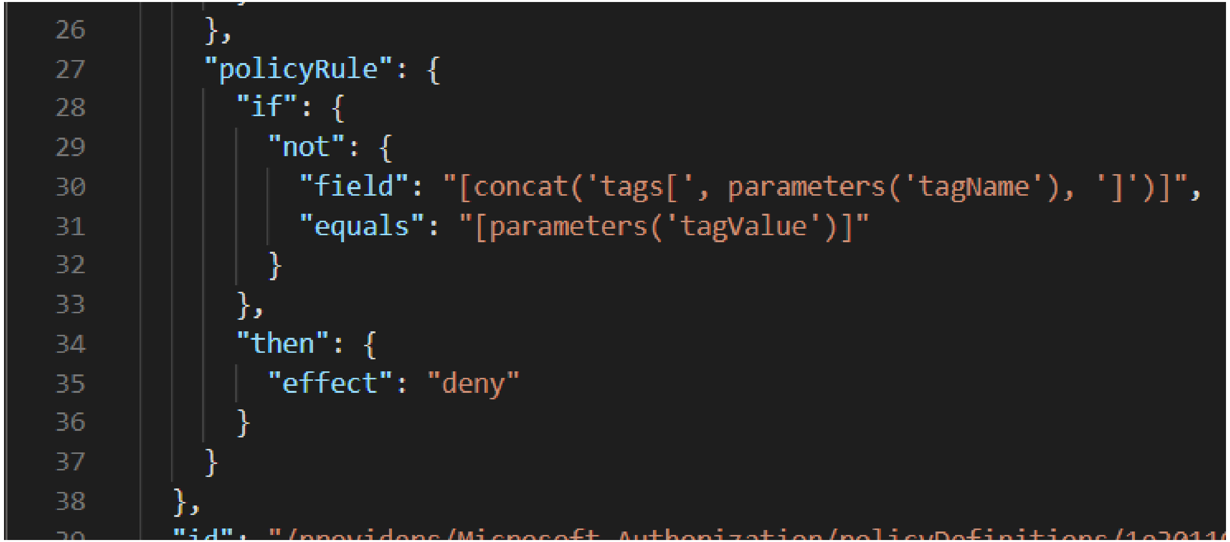


```
  "mode": "Indexed",
  "description": "Enforces a required tag and its value. Does not
  "metadata": {
    "version": "1.0.1",
    "category": "Tags"
  },
  "parameters": {
    "tagName": {
      "type": "String",
      "metadata": {
        "displayName": "Tag Name",
        "description": "Name of the tag, such as 'environment'"
      }
    },
    "tagValue": {
      "type": "String",
      "metadata": {
        "displayName": "Tag Value",
        "description": "Value of the tag, such as 'production'"
      }
    }
  },
  "policyRule": {
```

https://learn.microsoft.com/en-us/azure/governance/policy/concepts/definition-structure

Azure Policy Definition: Rule

- Rule
- Effect



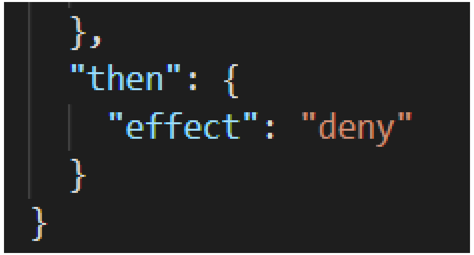
```
    },
    "policyRule": {
      "if": {
        "not": {
          "field": "[concat('tags[', parameters('tagName'), ']')]",
          "equals": "[parameters('tagValue')]"
        }
      },
      "then": {
        "effect": "deny"
      }
    }
  },
  "id": "/providers/Microsoft.Authorization/policyDefinitions/1e3011
```

https://learn.microsoft.com/en-us/azure/governance/policy/concepts/definition-structure

Azure Policy Effect

Azure Policy Effect

- Deny
- Modify
- DeployIfNotExists
- Append
- Audit
- AuditIfNotExists
- Disabled

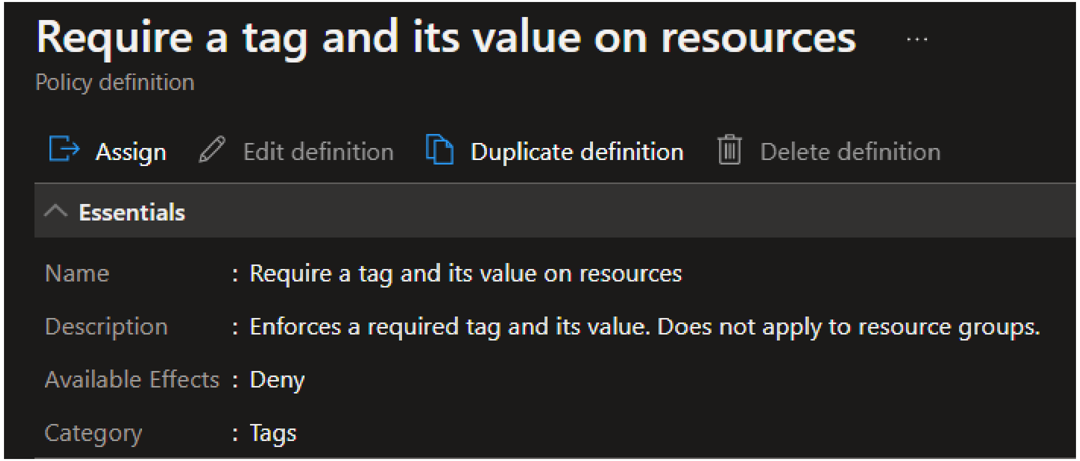


```
  },
  "then": {
    "effect": "deny"
  }
}
```

https://learn.microsoft.com/en-us/azure/governance/policy/concepts/definition-structure

Azure Policy Effect: Deny

- Generates an event in the activity log
- Fails the request



Require a tag and its value on resources

Policy definition

Name : Require a tag and its value on resources

Description : Enforces a required tag and its value. Does not apply to resource groups.

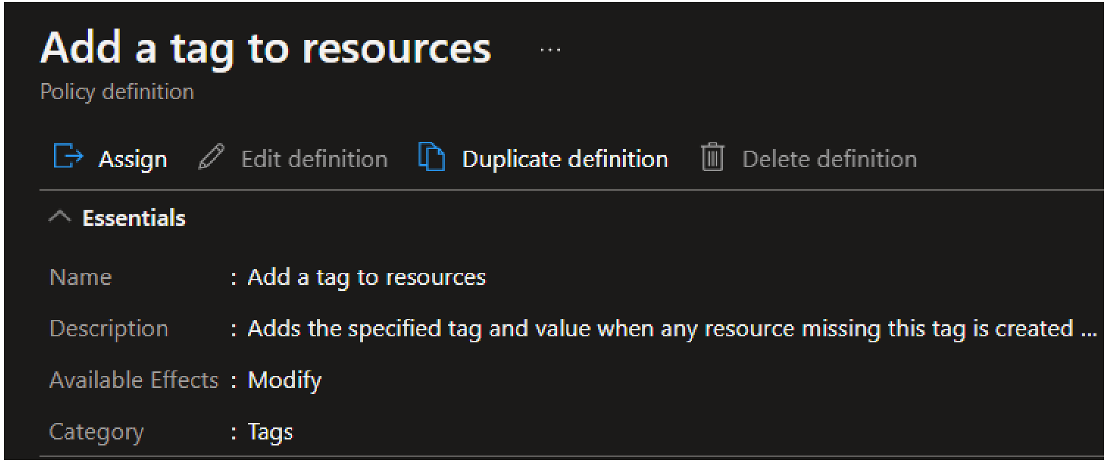
Available Effects : Deny

Category : Tags

https://learn.microsoft.com/en-us/azure/governance/policy/concepts/definition-structure

Azure Policy Effect: Modify

- Adds, updates, or removes the defined set of fields in the request



Name : Add a tag to resources

Description : Adds the specified tag and value when any resource missing this tag is created ...

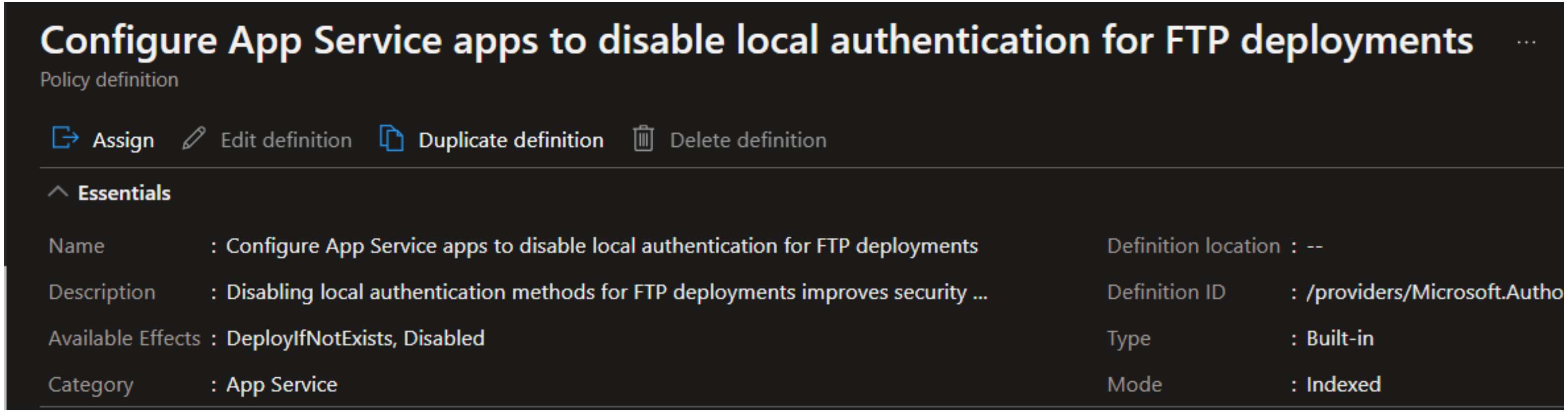
Available Effects : Modify

Category : Tags

https://learn.microsoft.com/en-us/azure/governance/policy/concepts/definition-structure

Azure Policy Effect: DeployIfNotExists

- Deploys a related resource if it doesn't already exist



Configure App Service apps to disable local authentication for FTP deployments

Policy definition

Name : Configure App Service apps to disable local authentication for FTP deployments

Description : Disabling local authentication methods for FTP deployments improves security ...

Available Effects : DeployIfNotExists, Disabled

Category : App Service

Definition location : --

Definition ID : /providers/Microsoft.Autho

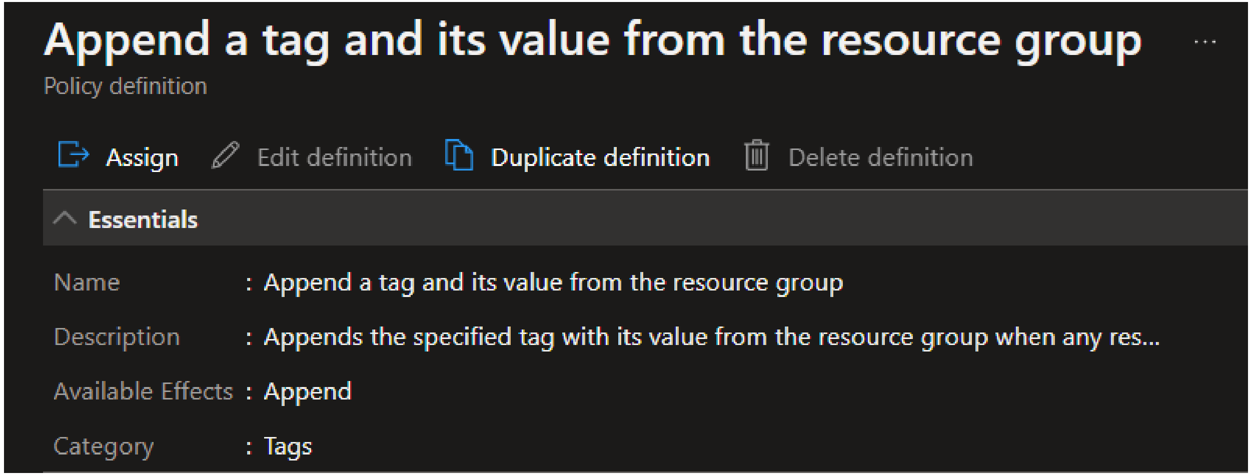
Type : Built-in

Mode : Indexed

https://learn.microsoft.com/en-us/azure/governance/policy/concepts/definition-structure

Azure Policy Effect: Append

- Adds the defined set of fields to the request



Append a tag and its value from the resource group

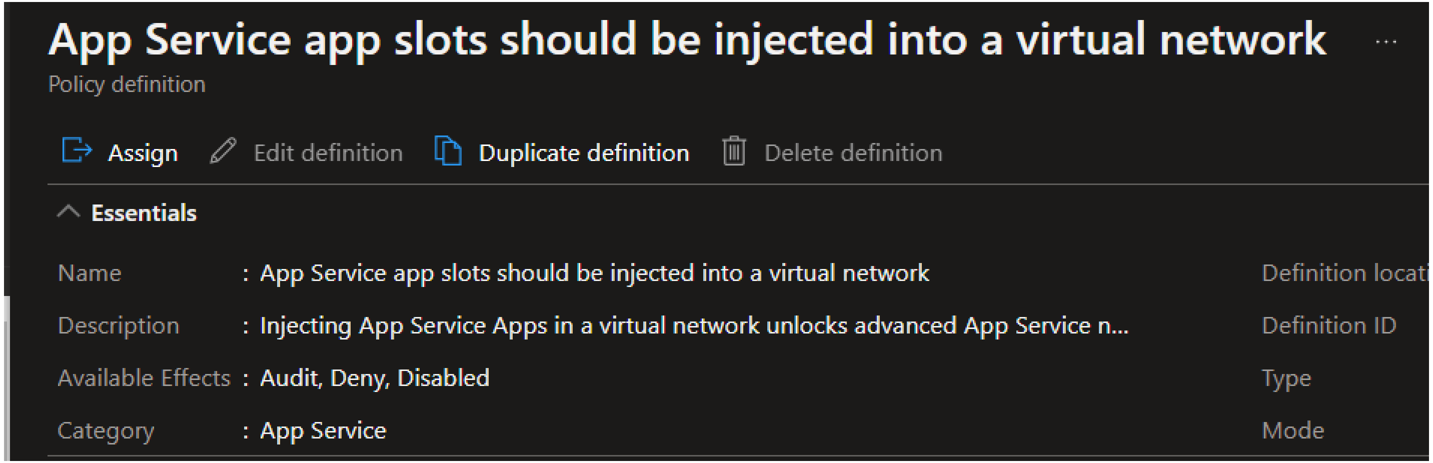
Policy definition

Name	: Append a tag and its value from the resource group
Description	: Appends the specified tag with its value from the resource group when any res...
Available Effects	: Append
Category	: Tags

https://learn.microsoft.com/en-us/azure/governance/policy/concepts/definition-structure

Azure Policy Effect: Audit

- Generates a warning event in activity log but doesn't fail the request



App Service app slots should be injected into a virtual network ···

Policy definition

Name : App Service app slots should be injected into a virtual network

Description : Injecting App Service Apps in a virtual network unlocks advanced App Service n...

Available Effects : Audit, Deny, Disabled

Category : App Service

Definition locati

Definition ID

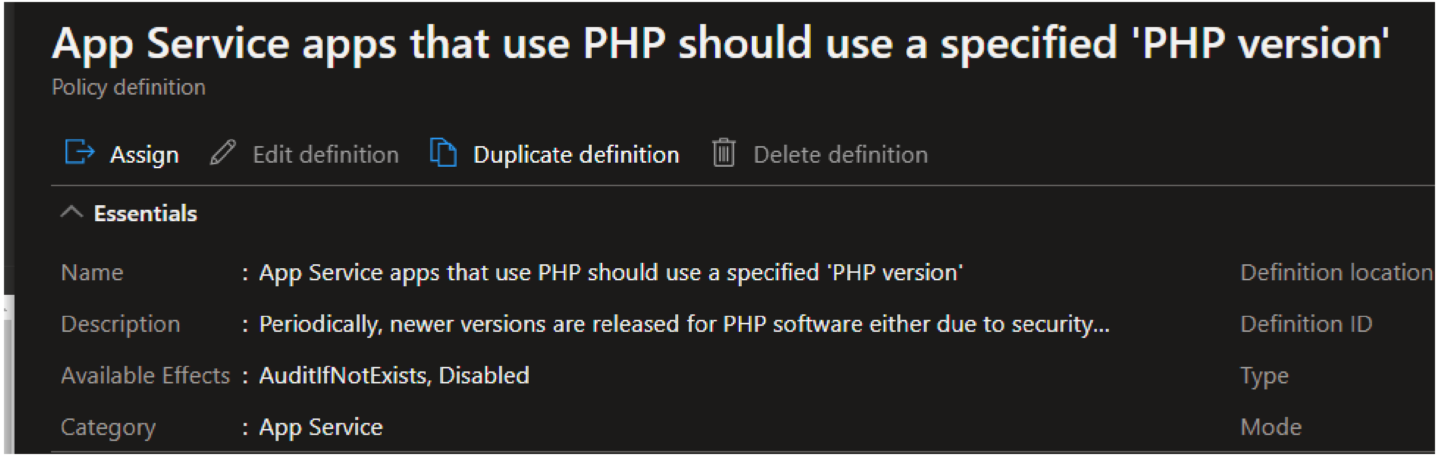
Type

Mode

https://learn.microsoft.com/en-us/azure/governance/policy/concepts/definition-structure

Azure Policy Effect: AuditIfNotExists

- Generates a warning event in activity log if a related resource doesn't exist



App Service apps that use PHP should use a specified 'PHP version'

Policy definition

Essentials

Name : App Service apps that use PHP should use a specified 'PHP version'

Description : Periodically, newer versions are released for PHP software either due to security...

Available Effects : AuditIfNotExists, Disabled

Category : App Service

Definition location

Definition ID

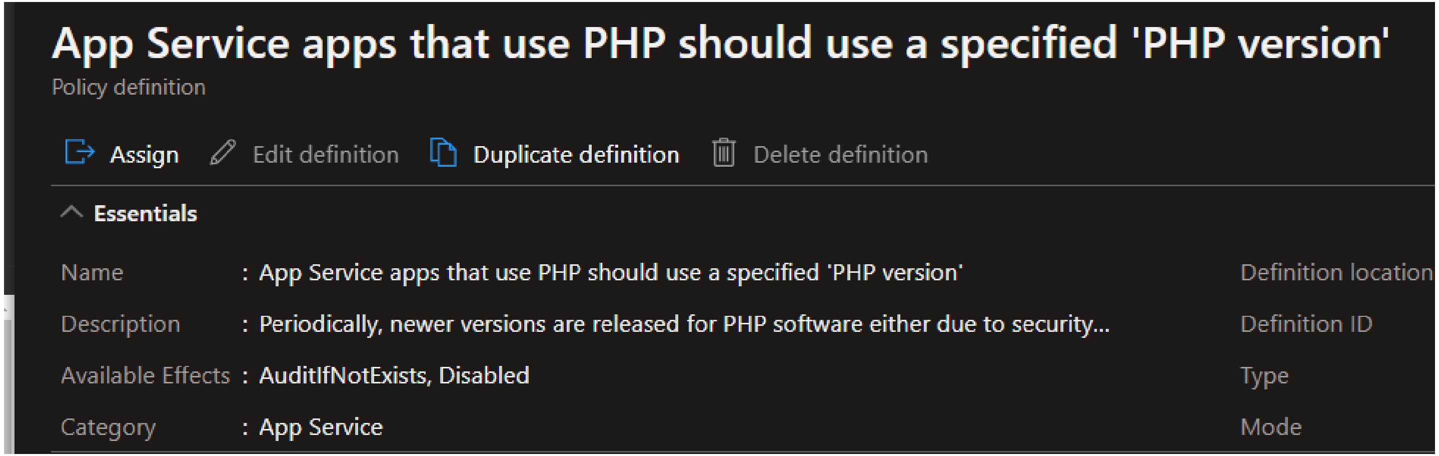
Type

Mode

https://learn.microsoft.com/en-us/azure/governance/policy/concepts/definition-structure

Azure Policy Effect: Disabled

- Doesn't evaluate resources for compliance to the policy rule



App Service apps that use PHP should use a specified 'PHP version'

Policy definition

Name	: App Service apps that use PHP should use a specified 'PHP version'	Definition location
Description	: Periodically, newer versions are released for PHP software either due to security...	Definition ID
Available Effects	: AuditIfNotExists, Disabled	Type
Category	: App Service	Mode

https://learn.microsoft.com/en-us/azure/governance/policy/concepts/definition-structure

General Built-in Policy Definitions

Azure Built-in Policies

- General
- Resource-specific
- Look into built-in policies before creating your own!

https://learn.microsoft.com/en-us/azure/governance/policy/samples/built-in-policies

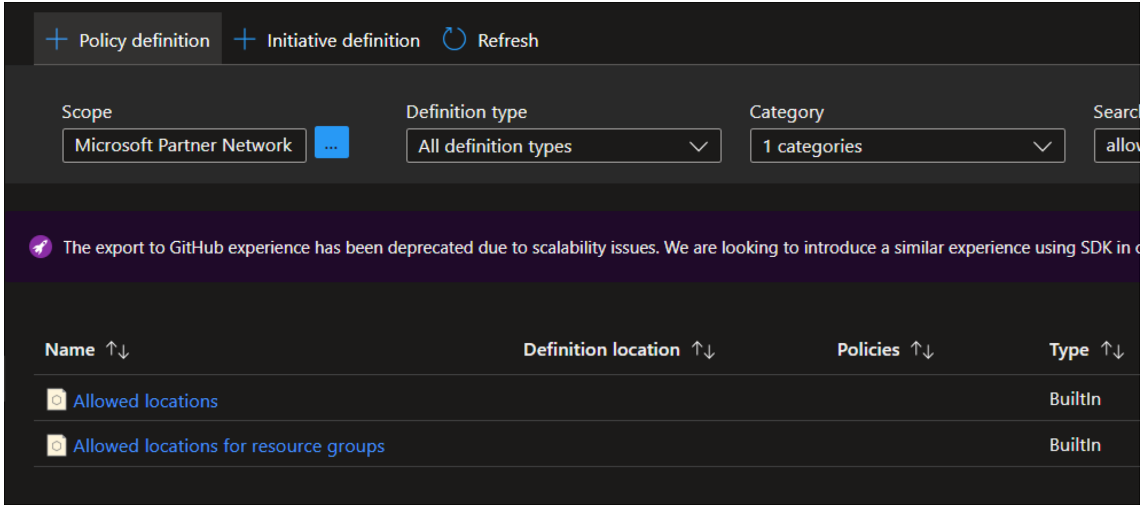
General Built-in Policy Definitions

- Allowed locations
- Allowed locations for resource groups
- Allowed resource types
- Not allowed resource types
- Audit resource location matches resource group location
- Audit usage of custom RBAC roles

https://learn.microsoft.com/en-us/azure/governance/policy/samples/built-in-policies#general

Allowed Locations

- Enforce data residency (data localization) laws
- EU (GDPR)
- Australia
- Canada
- Indonesia
- Russia



Scope: Microsoft Partner Network ...

Definition type: All definition types

Category: 1 categories

Searc allo

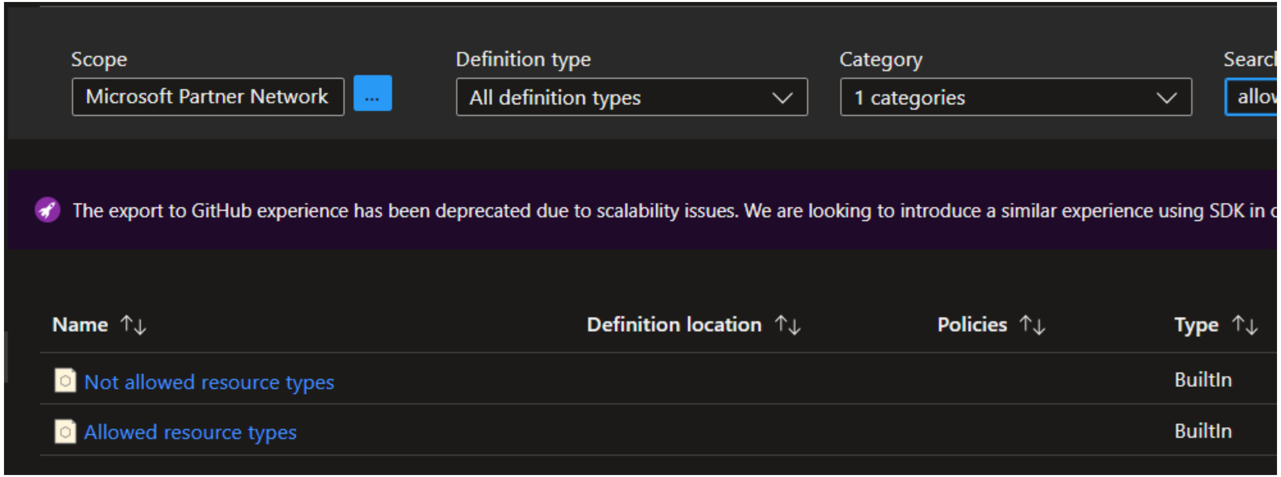
The export to GitHub experience has been deprecated due to scalability issues. We are looking to introduce a similar experience using SDK in c

Name ↑↓	Definition location ↑↓	Policies ↑↓	Type ↑↓
Allowed locations			BuiltIn
Allowed locations for resource groups			BuiltIn

https://learn.microsoft.com/en-us/azure/governance/policy/samples/built-in-policies#general

Allowed Resource Types

- Enforce company best practices
- Save costs



Scope: Microsoft Partner Network

Definition type: All definition types

Category: 1 categories

Searc: allov

The export to GitHub experience has been deprecated due to scalability issues. We are looking to introduce a similar experience using SDK in c

Name ↑↓	Definition location ↑↓	Policies ↑↓	Type ↑↓
Not allowed resource types			BuiltIn
Allowed resource types			BuiltIn

https://learn.microsoft.com/en-us/azure/governance/policy/samples/built-in-policies#general

Resource-specific Built-in Policy Definitions

Resource-specific Built-in Policy Definitions

API Management

App Service

Azure Databricks

Bot Service

Cognitive Services

Compute

Cosmos DB

Key Vault

Network

Service Bus

SQL

Storage

Tags

https://learn.microsoft.com/en-us/azure/governance/policy/samples/built-in-policies

Azure Storage Account

- Storage account keys should not be expired
- Storage accounts should restrict network access
- Secure transfer to storage accounts should be enabled
- Storage Accounts should use a virtual network service endpoint
- Configure your Storage account public access to be disallowed
- …

https://learn.microsoft.com/en-us/azure/governance/policy/samples/built-in-policies#storage

Azure App Service

- App Service apps should disable public network access
- App Service apps should use managed identity
- Azure Defender for App Service should be enabled
- App Service apps should use a virtual network service endpoint
- Configure App Service apps to disable local authentication for FTP deployments
- …

https://learn.microsoft.com/en-us/azure/governance/policy/samples/built-in-policies#app-service

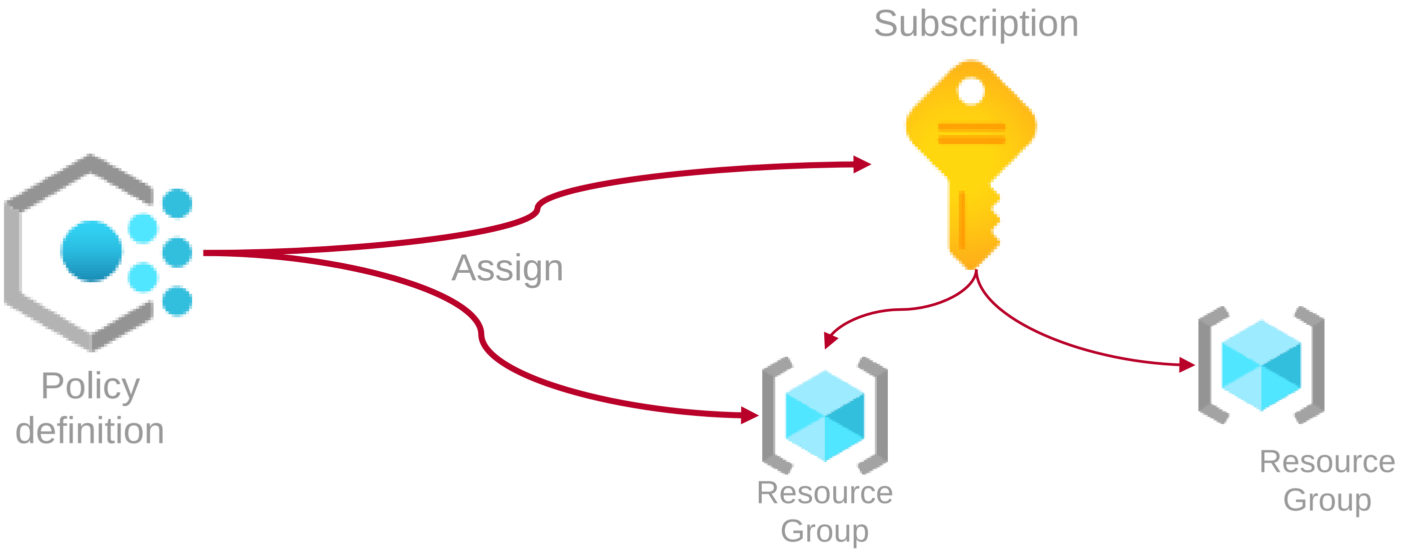
Azure Key Vault

- Key vaults should have deletion protection enabled
- Azure Defender for Key Vault should be enabled
- Key vaults should have soft delete enabled
- Azure Key Vault should have firewall enabled
- Configure Azure Key Vaults with private endpoints
- …

https://learn.microsoft.com/en-us/azure/governance/policy/samples/built-in-policies#key-vault

Assigning a Built-in Policy Definition

Assigning a Built-in Policy Definition



https://learn.microsoft.com/en-us/azure/governance/policy/concepts/definition-structure

Policy Assignment

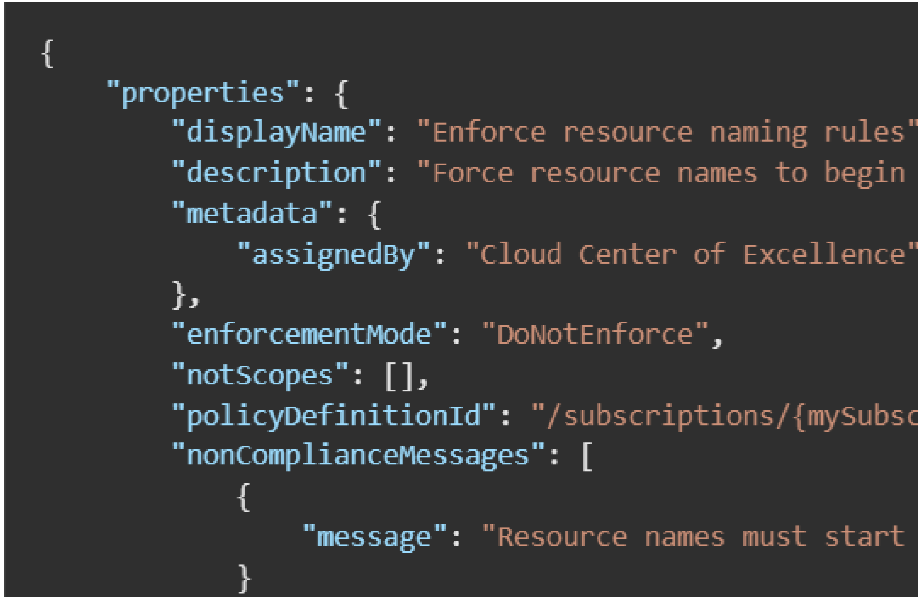
- display name
- description
- metadata
- enforcement mode

- excluded scopes
- policy definition
- non-compliance messages
- parameters
- identity

https://learn.microsoft.com/en-us/azure/governance/policy/concepts/assignment-structure

Policy Assignment: Enforcement Mode

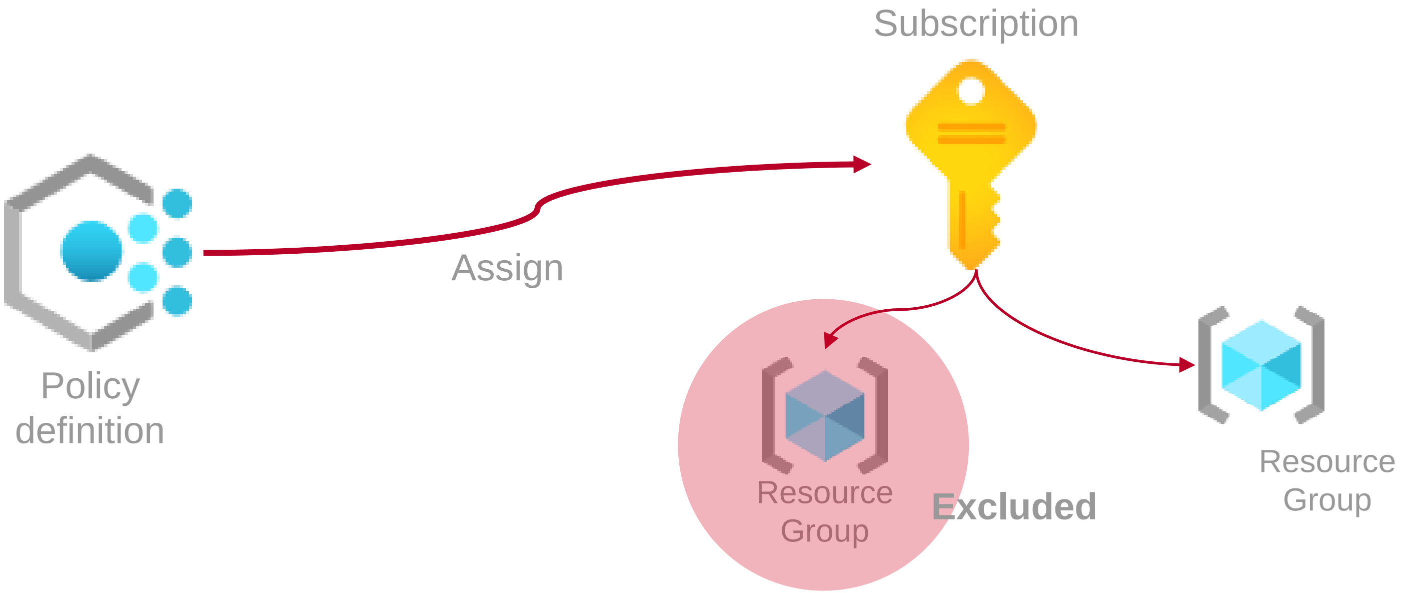
- Default
- DoNotEnforce



```
{
    "properties": {
        "displayName": "Enforce resource naming rules"
        "description": "Force resource names to begin
        "metadata": {
            "assignedBy": "Cloud Center of Excellence"
        },
        "enforcementMode": "DoNotEnforce",
        "notScopes": [],
        "policyDefinitionId": "/subscriptions/{mySubsc
        "nonComplianceMessages": [
            {
                "message": "Resource names must start
            }
```

https://learn.microsoft.com/en-us/azure/governance/policy/concepts/assignment-structure#enforcement-mode

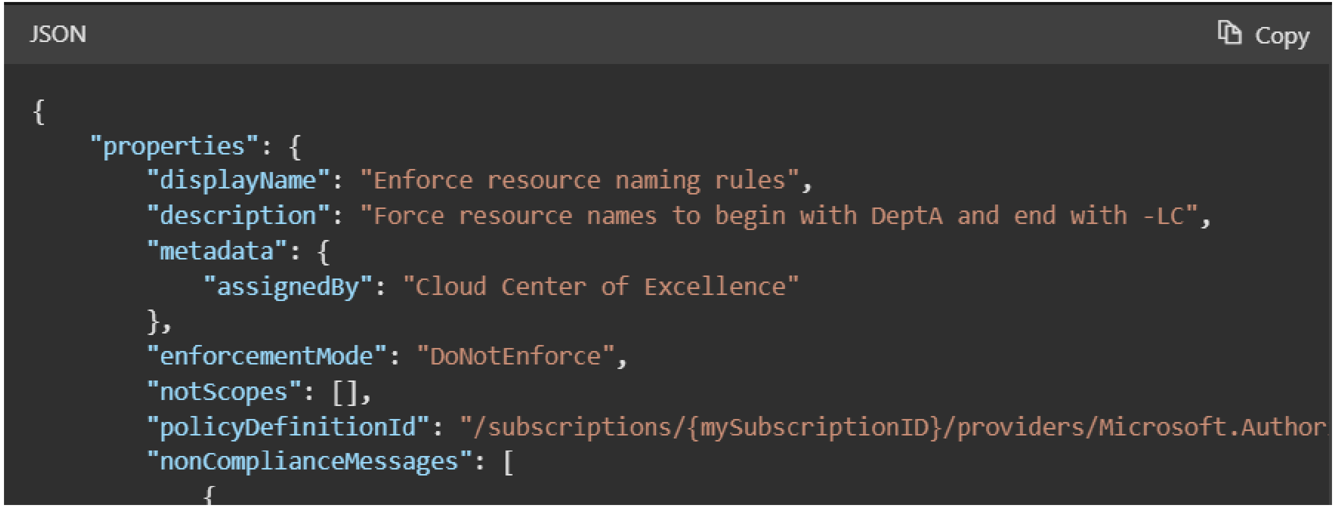
Policy Assignment: Excluded Scopes



https://learn.microsoft.com/en-us/azure/governance/policy/concepts/assignment-structure#enforcement-mode

Policy Assignment: Policy Definition

- The policy to assign

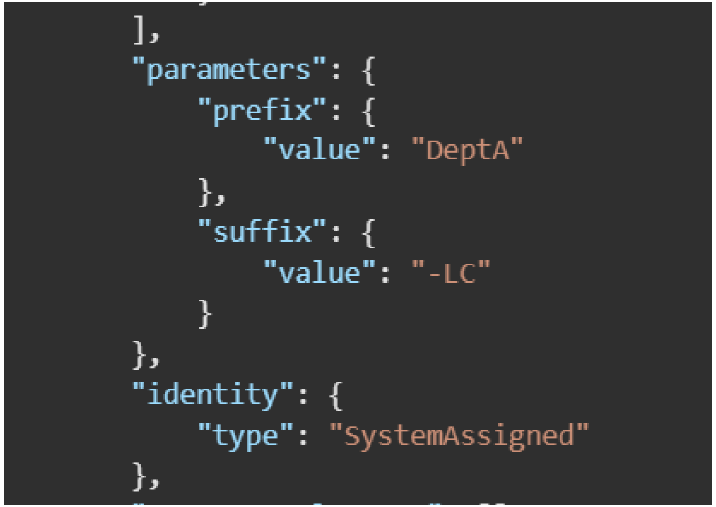


```json
{
    "properties": {
        "displayName": "Enforce resource naming rules",
        "description": "Force resource names to begin with DeptA and end with -LC",
        "metadata": {
            "assignedBy": "Cloud Center of Excellence"
        },
        "enforcementMode": "DoNotEnforce",
        "notScopes": [],
        "policyDefinitionId": "/subscriptions/{mySubscriptionID}/providers/Microsoft.Author
        "nonComplianceMessages": [
            {
```

https://learn.microsoft.com/en-us/azure/governance/policy/concepts/assignment-structure#policy-definition-id

Policy Assignment: Parameters

- Assignment parameters (location, tag name, etc.)

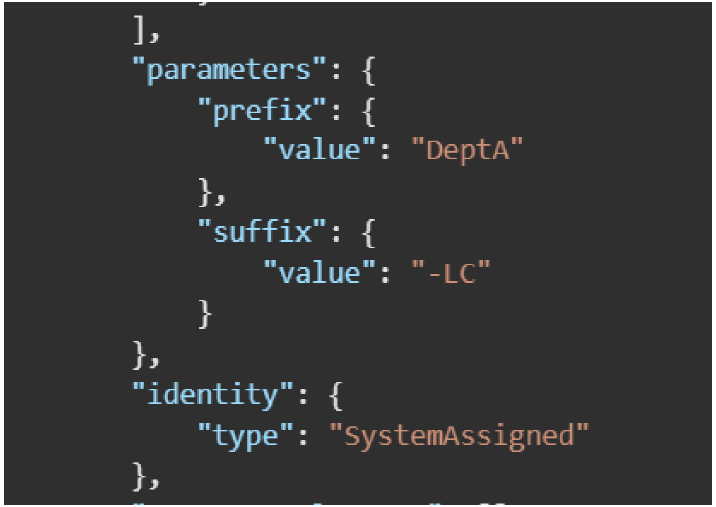


```
],
"parameters": {
    "prefix": {
        "value": "DeptA"
    },
    "suffix": {
        "value": "-LC"
    }
},
"identity": {
    "type": "SystemAssigned"
},
```

https://learn.microsoft.com/en-us/azure/governance/policy/concepts/assignment-structure#parameters

Policy Assignment: Identity

- For policy assignments with effect set to deployIfNotExist or modify.

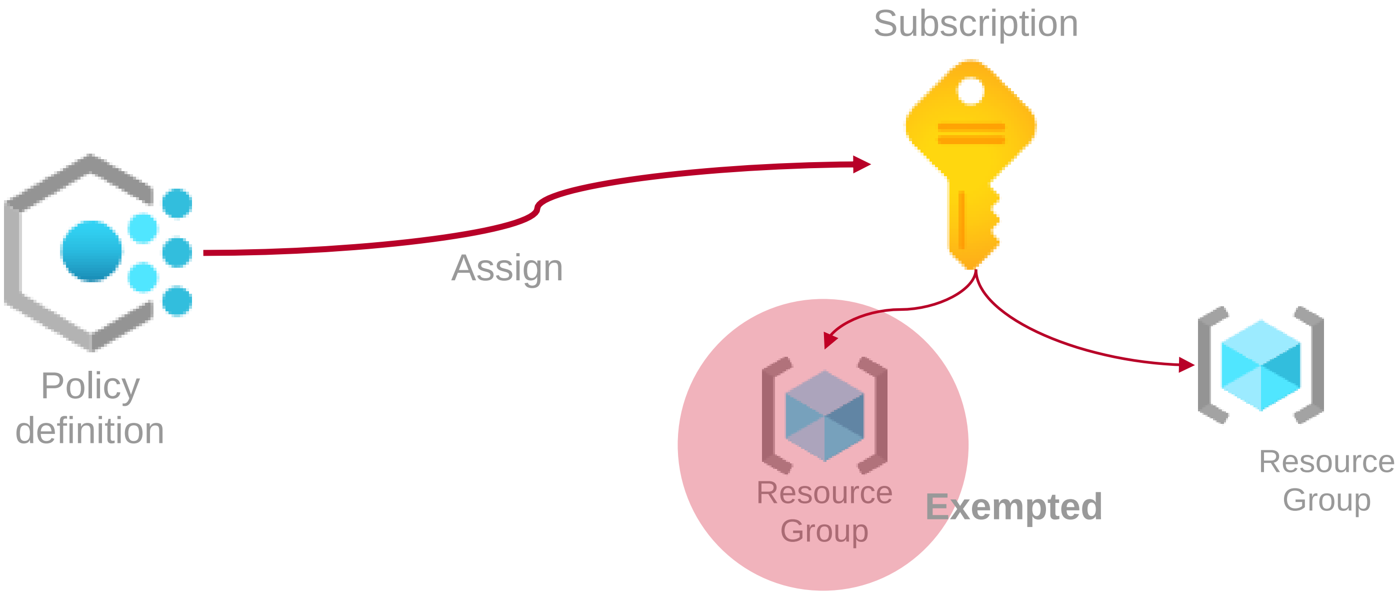


```
],
"parameters": {
    "prefix": {
        "value": "DeptA"
    },
    "suffix": {
        "value": "-LC"
    }
},
"identity": {
    "type": "SystemAssigned"
},
```

https://learn.microsoft.com/en-us/azure/governance/policy/concepts/assignment-structure#identity

Policy Exemption

Policy Exemption



https://learn.microsoft.com/en-us/azure/governance/policy/concepts/assignment-structure#enforcement-mode

Policy Exemption

- Like **exclusions**, “a policy **exemption** can also be used skip the evaluation of a resource.“

https://learn.microsoft.com/en-us/azure/governance/policy/tutorials/create-and-manage#remove-a-non-compliant-or-denied-resource-from-the-scope-with-an-exclusion

Policy Exemption

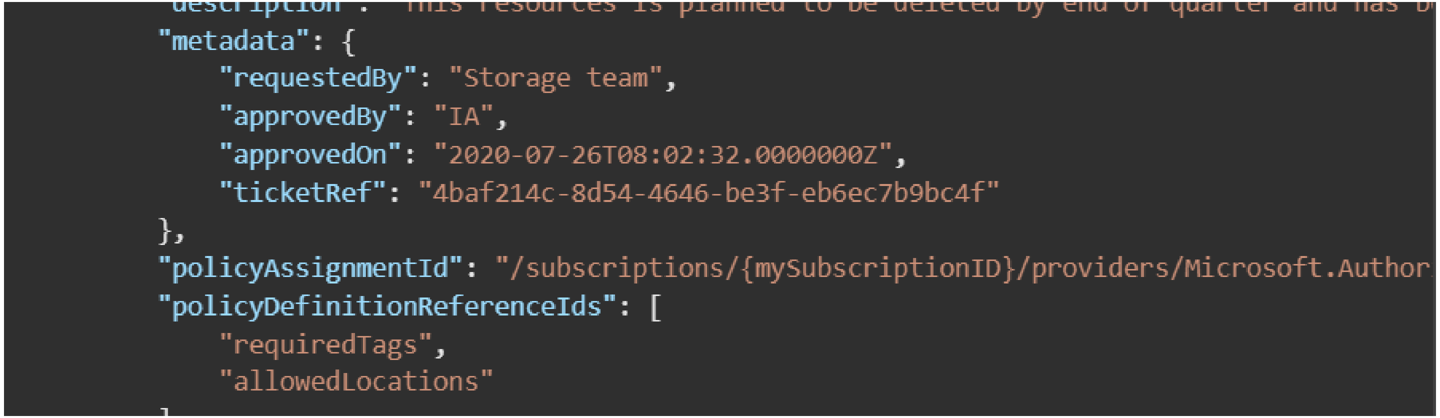
- display name
- description
- metadata
- policy assignment

- policy definitions within an initiative
- exemption category
- expiration

https://learn.microsoft.com/en-us/azure/governance/policy/concepts/exemption-structure

Policy Exemption: Policy Assignment

- Assignment name

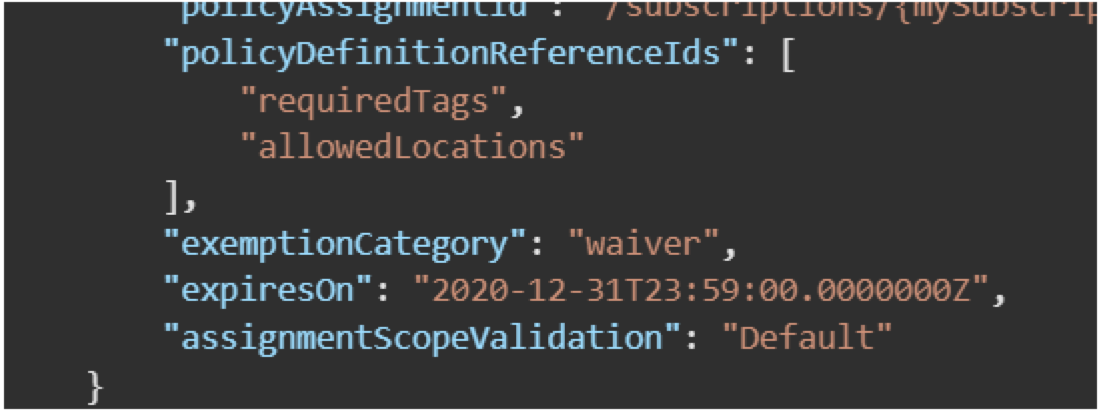


```
    "description": "This resources is planned to be deleted by end of quarter and has b
    "metadata": {
        "requestedBy": "Storage team",
        "approvedBy": "IA",
        "approvedOn": "2020-07-26T08:02:32.0000000Z",
        "ticketRef": "4baf214c-8d54-4646-be3f-eb6ec7b9bc4f"
    },
    "policyAssignmentId": "/subscriptions/{mySubscriptionID}/providers/Microsoft.Author
    "policyDefinitionReferenceIds": [
        "requiredTags",
        "allowedLocations"
    ]
```

https://learn.microsoft.com/en-us/azure/governance/policy/concepts/exemption-structure#policy-assignment-id

Policy Exemption: Exemption Category

- Mitigated: “the policy intent is met through another method”
- Waiver: the resource is non-compliant

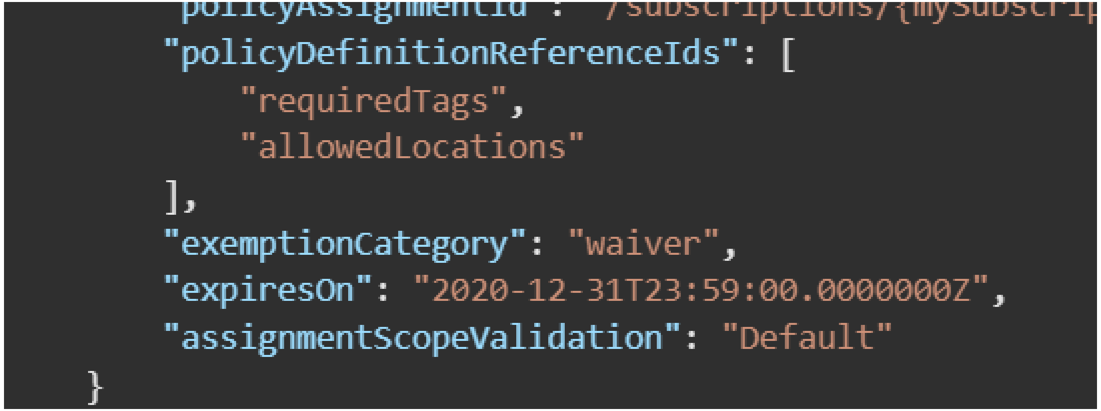


```
        "policyAssignmentId": "/subscriptions/{mySubscrip
        "policyDefinitionReferenceIds": [
            "requiredTags",
            "allowedLocations"
        ],
        "exemptionCategory": "waiver",
        "expiresOn": "2020-12-31T23:59:00.0000000Z",
        "assignmentScopeValidation": "Default"
    }
```

https://learn.microsoft.com/en-us/azure/governance/policy/concepts/exemption-structure#exemption-category

Policy Exemption: Expiration

- **expiresOn** property: when a resource (hierarchy) exemption expires.

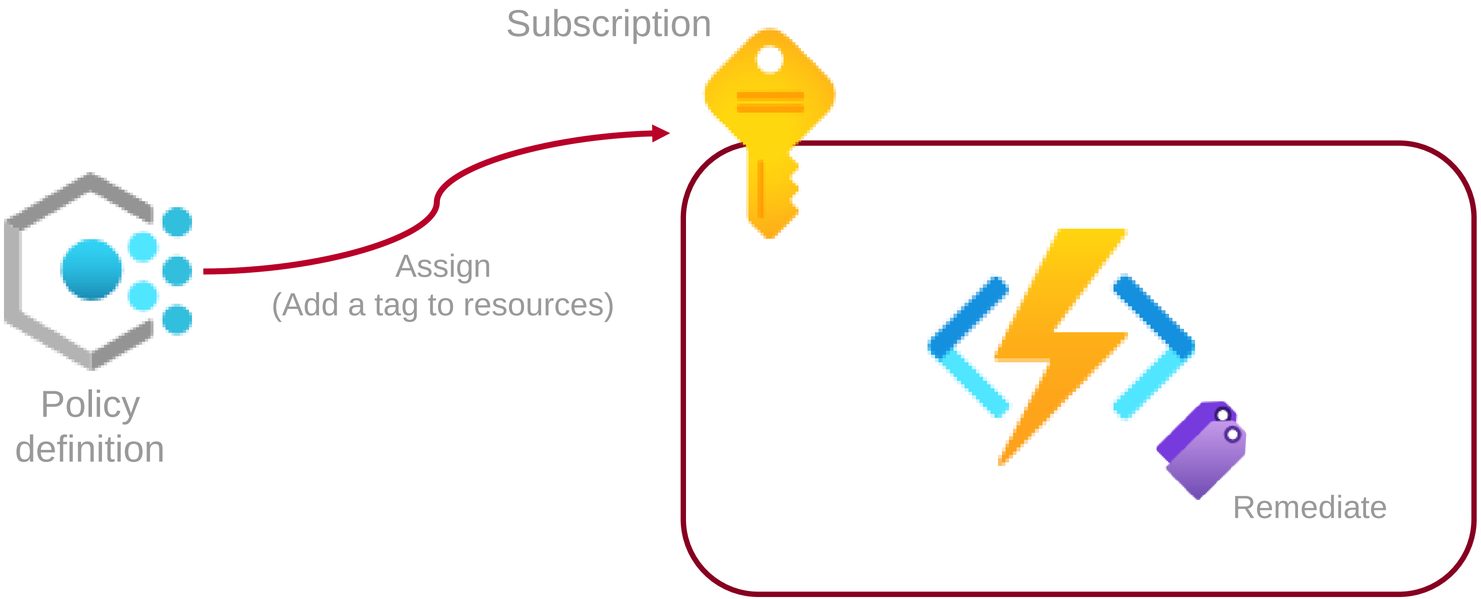


```
        "policyAssignmentId": "/subscriptions/{mySubscrip
        "policyDefinitionReferenceIds": [
            "requiredTags",
            "allowedLocations"
        ],
        "exemptionCategory": "waiver",
        "expiresOn": "2020-12-31T23:59:00.0000000Z",
        "assignmentScopeValidation": "Default"
    }
```

https://learn.microsoft.com/en-us/azure/governance/policy/concepts/exemption-structure#expiration

Remediation

Remediate Non-compliant Resources



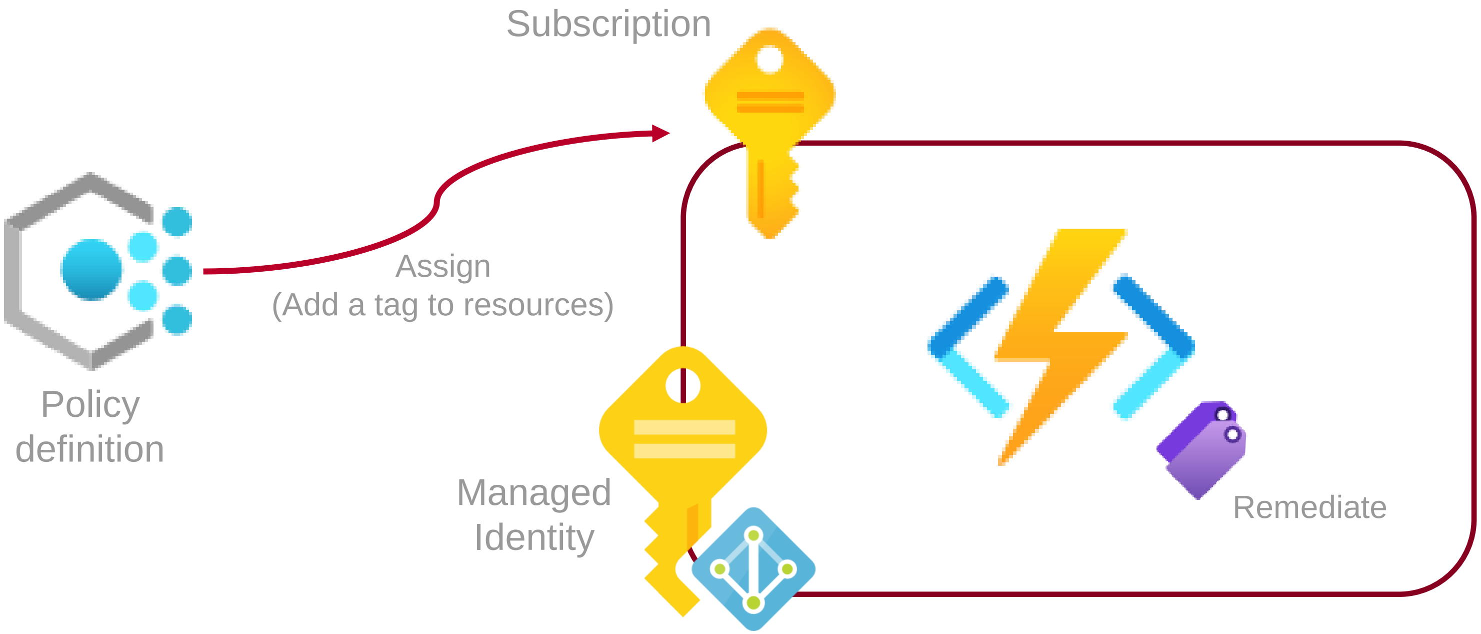
https://learn.microsoft.com/en-us/azure/governance/policy/how-to/remediate-resources

Remediate Non-compliant Resources

“Resources that are non-compliant to policies with **deployIfNotExists** or **modify** effects, can be put into a compliant state through Remediation.”

https://learn.microsoft.com/en-us/azure/governance/policy/how-to/remediate-resources

Remediate Non-compliant Resources



https://learn.microsoft.com/en-us/azure/governance/policy/how-to/remediate-resources

Remediate Non-compliant Resources

1. Policy definition effect should be **modify** or **deployIfNotExists**
2. Create a managed identity
3. Give needed permissions to the managed identity
4. Create the remediation task with the managed identity
5. Monitor the remediation task progress

https://learn.microsoft.com/en-us/azure/governance/policy/how-to/remediate-resources

Creating a Custom Policy Definition

Azure Policies

- General (built-in)
- Resource-specific (built-in)
- Create your own custom policy

https://learn.microsoft.com/en-us/azure/governance/policy/samples/built-in-policies

Custom Policy Definitions

- A custom policy definition allows you to define your own rules for using Azure.

https://learn.microsoft.com/en-us/azure/governance/policy/tutorials/create-custom-policy-definition

Custom Policy Definitions

- Security practices
- Cost management
- Organization-specific rules (naming, tagging, etc.)

https://learn.microsoft.com/en-us/azure/governance/policy/tutorials/create-custom-policy-definition

Azure Policy Definition Structure

- Type
- Display name, description
- Mode
- Metadata
- Parameters
- Policy rule (logical evaluation, effect)

https://learn.microsoft.com/en-us/azure/governance/policy/concepts/definition-structure

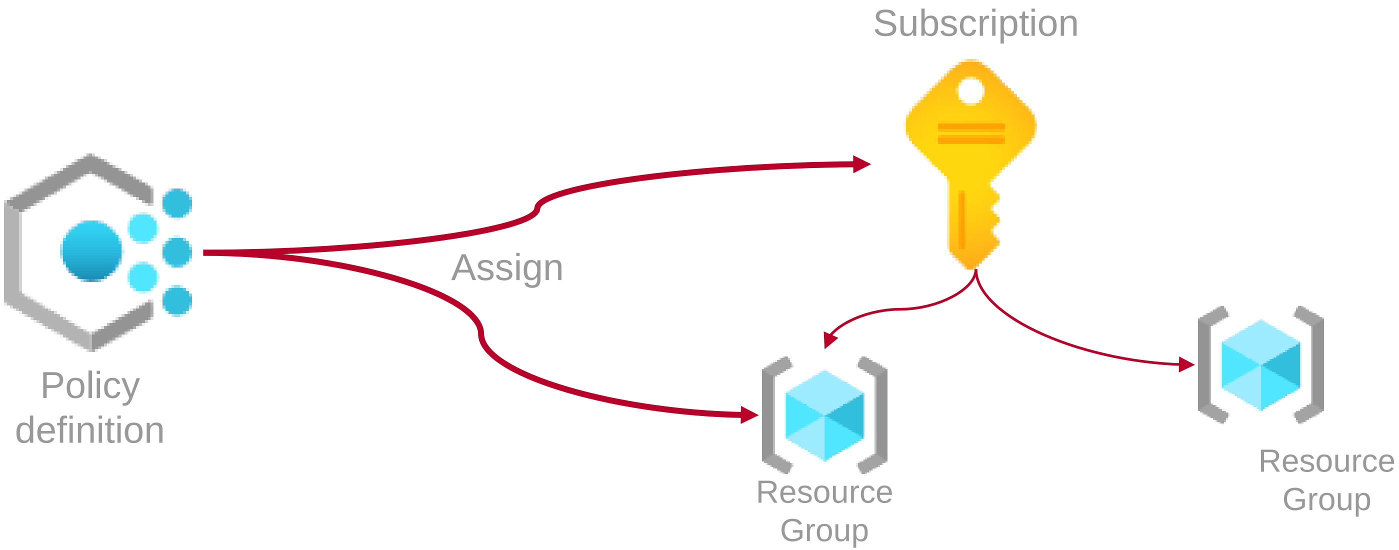
Creating Your Custom Policy Definition

1. Identify requirements
2. Determine resource properties
3. Determine the effect to use
4. Compose the definition

https://learn.microsoft.com/en-us/azure/governance/policy/tutorials/create-custom-policy-definition

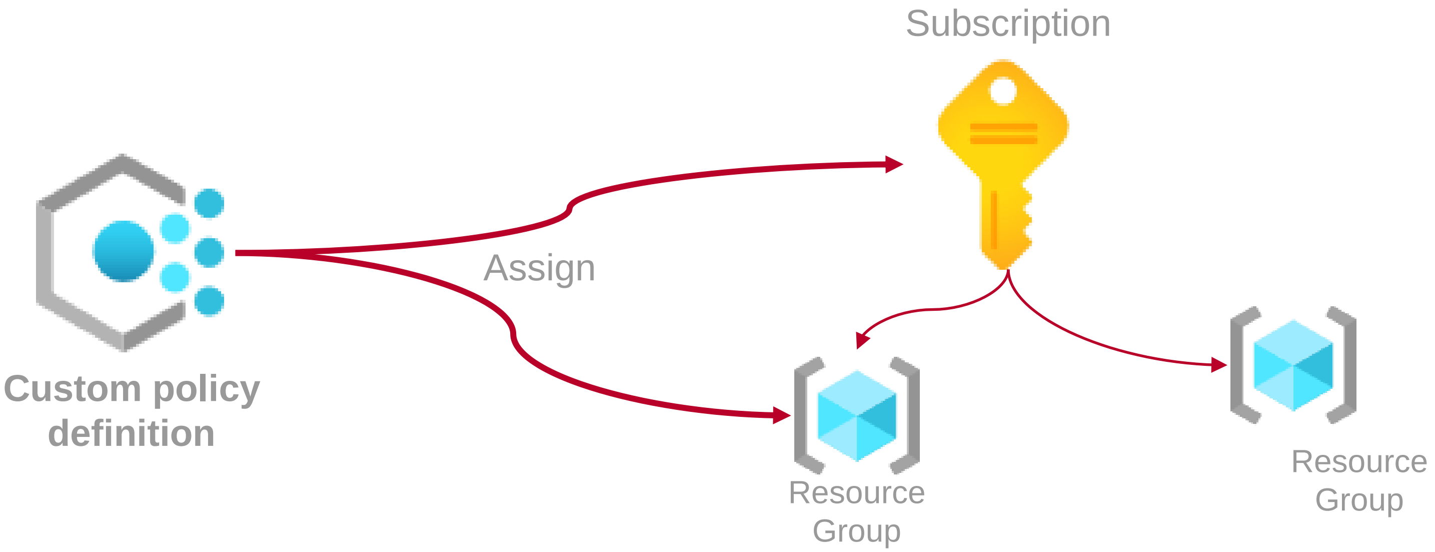
Assigning a Custom Policy Definition

Assigning a Built-in Policy Definition



https://learn.microsoft.com/en-us/azure/governance/policy/concepts/definition-structure

Assigning a Built-in Policy Definition



https://learn.microsoft.com/en-us/azure/governance/policy/concepts/definition-structure

Policy Assignment

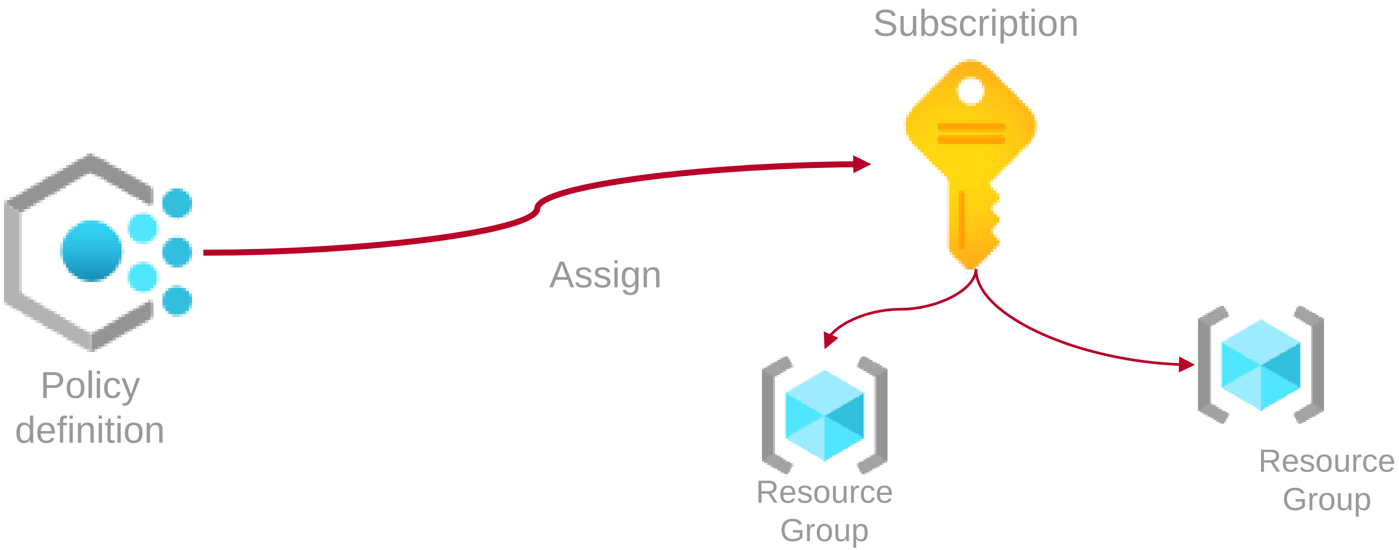
- display name
- description
- metadata
- enforcement mode

- excluded scopes
- **policy definition**
- non-compliance messages
- parameters
- identity

https://learn.microsoft.com/en-us/azure/governance/policy/concepts/assignment-structure

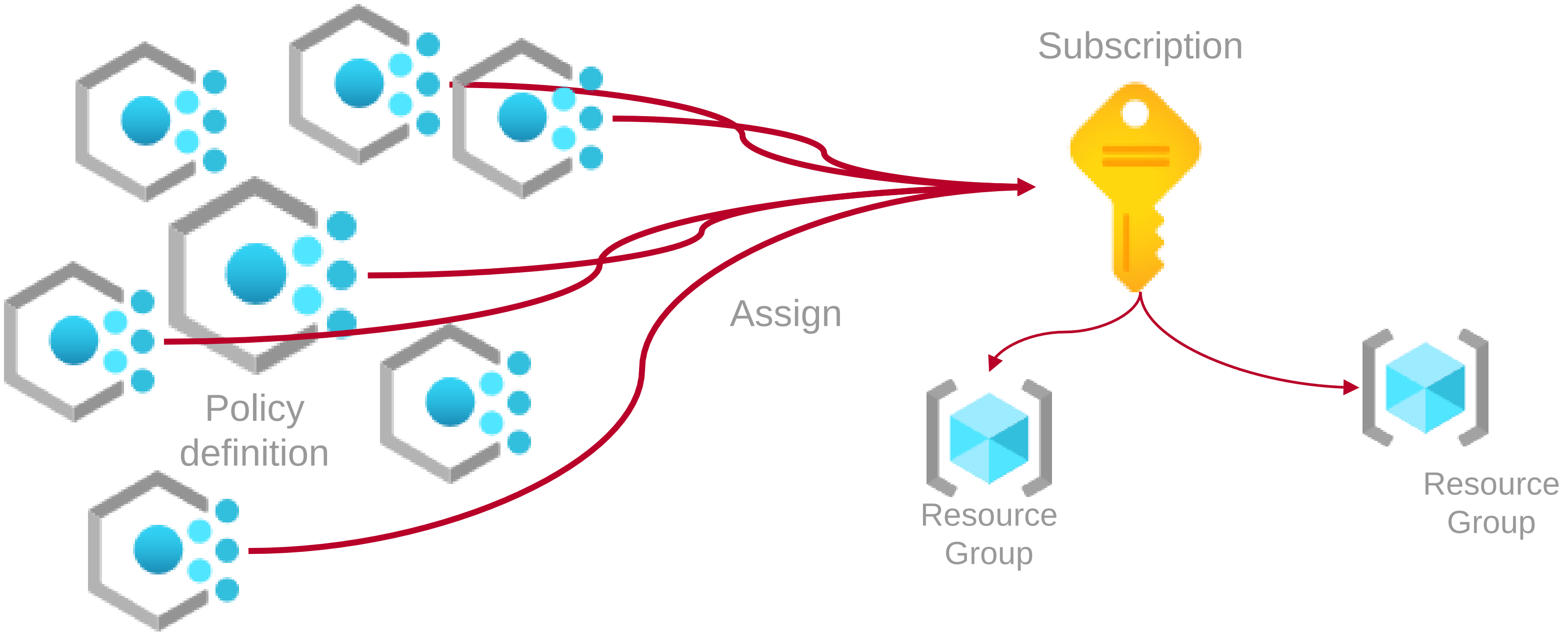
Azure Policy Initiative

Assigning a Built-in Policy Definition



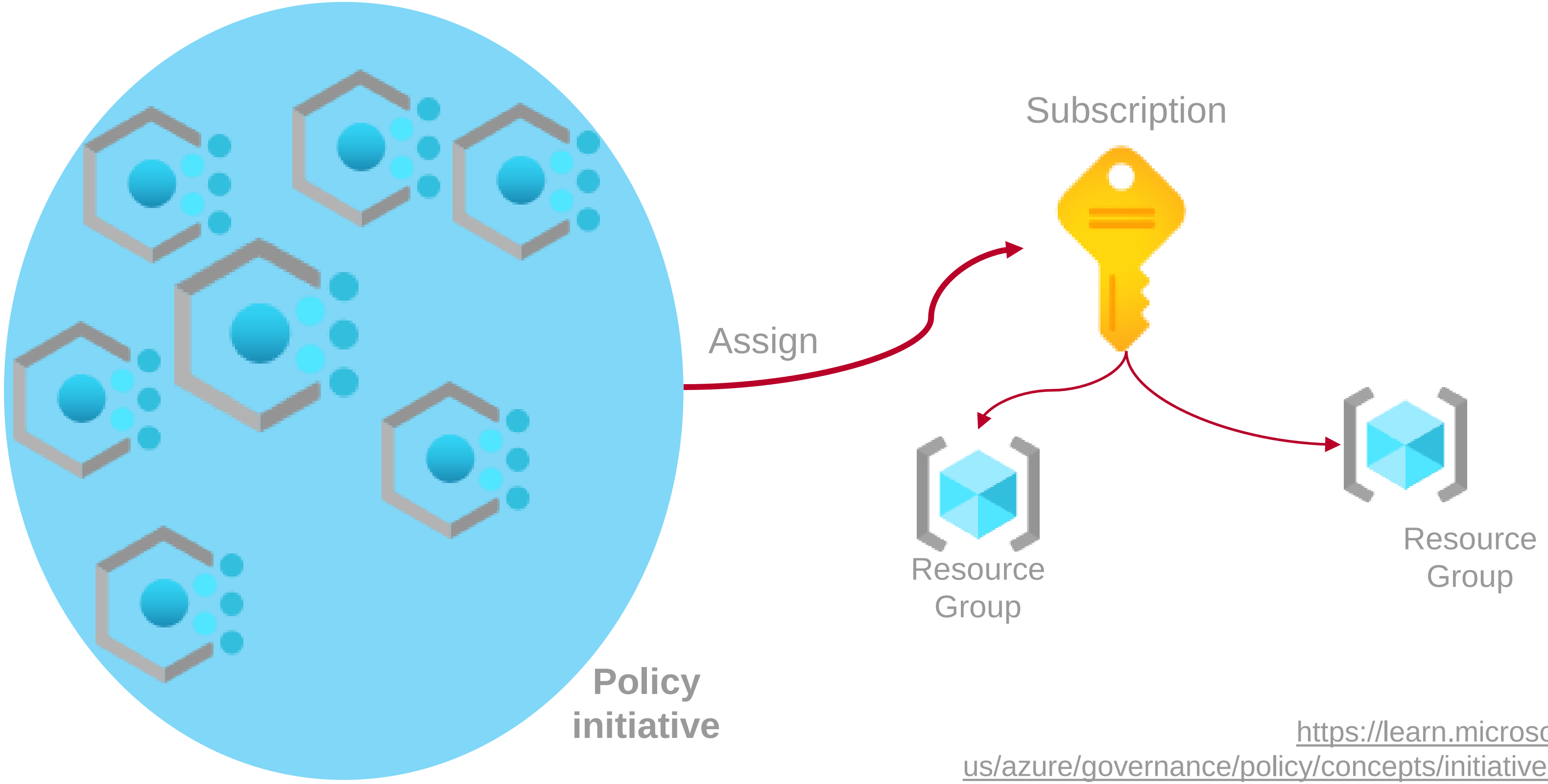
https://learn.microsoft.com/en-us/azure/governance/policy/concepts/definition-structure

Assigning a Built-in Policy Definition



https://learn.microsoft.com/en-us/azure/governance/policy/concepts/definition-structure

Assigning a Built-in Policy Definition



https://learn.microsoft.com/en-us/azure/governance/policy/concepts/initiative-definition-structure

Azure Policy Initiative

- display name
- description
- metadata
- policy assignment
- policy definitions

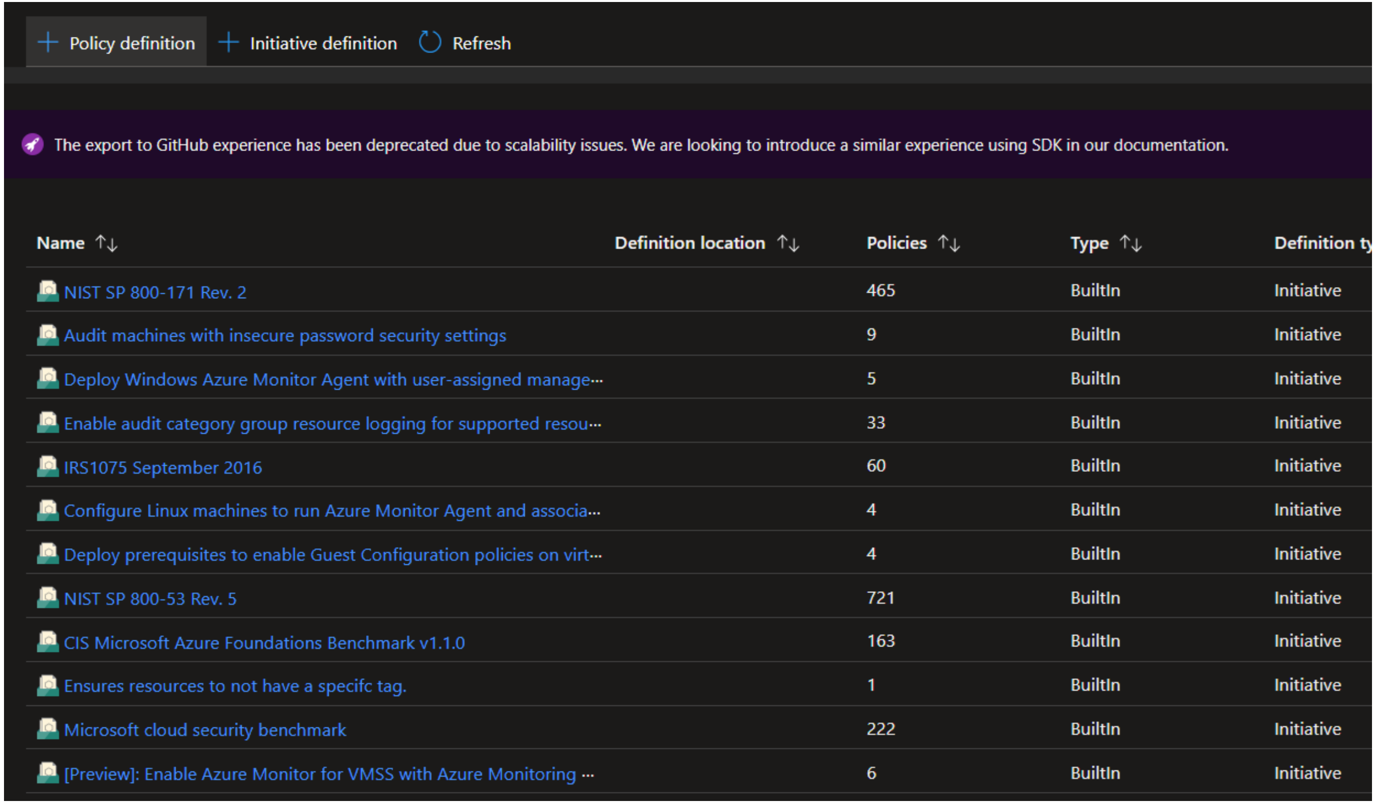
https://learn.microsoft.com/en-us/azure/governance/policy/concepts/initiative-definition-structure

Azure Policy Initiative

- Built-in
- Custom

https://learn.microsoft.com/en-us/azure/governance/policy/concepts/initiative-definition-structure

Built-in Azure Policy Initiatives



The export to GitHub experience has been deprecated due to scalability issues. We are looking to introduce a similar experience using SDK in our documentation.

Name ↑↓	Definition location ↑↓	Policies ↑↓	Type ↑↓	Definition ty
NIST SP 800-171 Rev. 2		465	BuiltIn	Initiative
Audit machines with insecure password security settings		9	BuiltIn	Initiative
Deploy Windows Azure Monitor Agent with user-assigned manage...		5	BuiltIn	Initiative
Enable audit category group resource logging for supported resou...		33	BuiltIn	Initiative
IRS1075 September 2016		60	BuiltIn	Initiative
Configure Linux machines to run Azure Monitor Agent and associa...		4	BuiltIn	Initiative
Deploy prerequisites to enable Guest Configuration policies on virt...		4	BuiltIn	Initiative
NIST SP 800-53 Rev. 5		721	BuiltIn	Initiative
CIS Microsoft Azure Foundations Benchmark v1.1.0		163	BuiltIn	Initiative
Ensures resources to not have a specifc tag.		1	BuiltIn	Initiative
Microsoft cloud security benchmark		222	BuiltIn	Initiative
[Preview]: Enable Azure Monitor for VMSS with Azure Monitoring ...		6	BuiltIn	Initiative

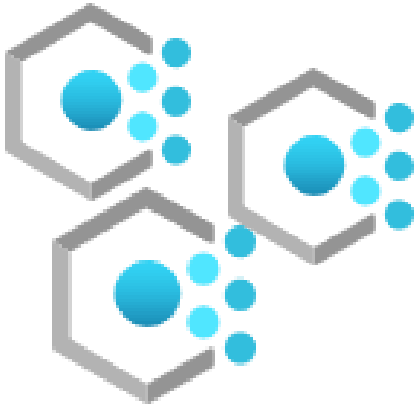
Built-in Azure Policy Initiatives

- SOC 2 Type 2
- HITRUST/HIPAA
- PCI DSS v4
- ISO 27001:2013
- NIST SP 800-53 Rev. 5
- CMMC Level 3
- More…

https://learn.microsoft.com/en-us/azure/governance/policy/samples/built-in-initiatives

Custom Azure Policy Initiatives

- A custom initiative definition allows you to define your own rules for using Azure.



https://learn.microsoft.com/en-us/azure/defender-for-cloud/custom-security-policies?pivots=azure-portal

PCI DSS

HITRUST/HIPAA

SOC 2

Course Repository

https://github.com/zaalion/oreilly-policy-governance

Thank you!

Reza Salehi

@zaalion