AKS Governance with Azure Policy

Agenda

Azure Policy

AKS Azure Policy Add-on

AKS Policy to manage AKS clusters

Azure Policy

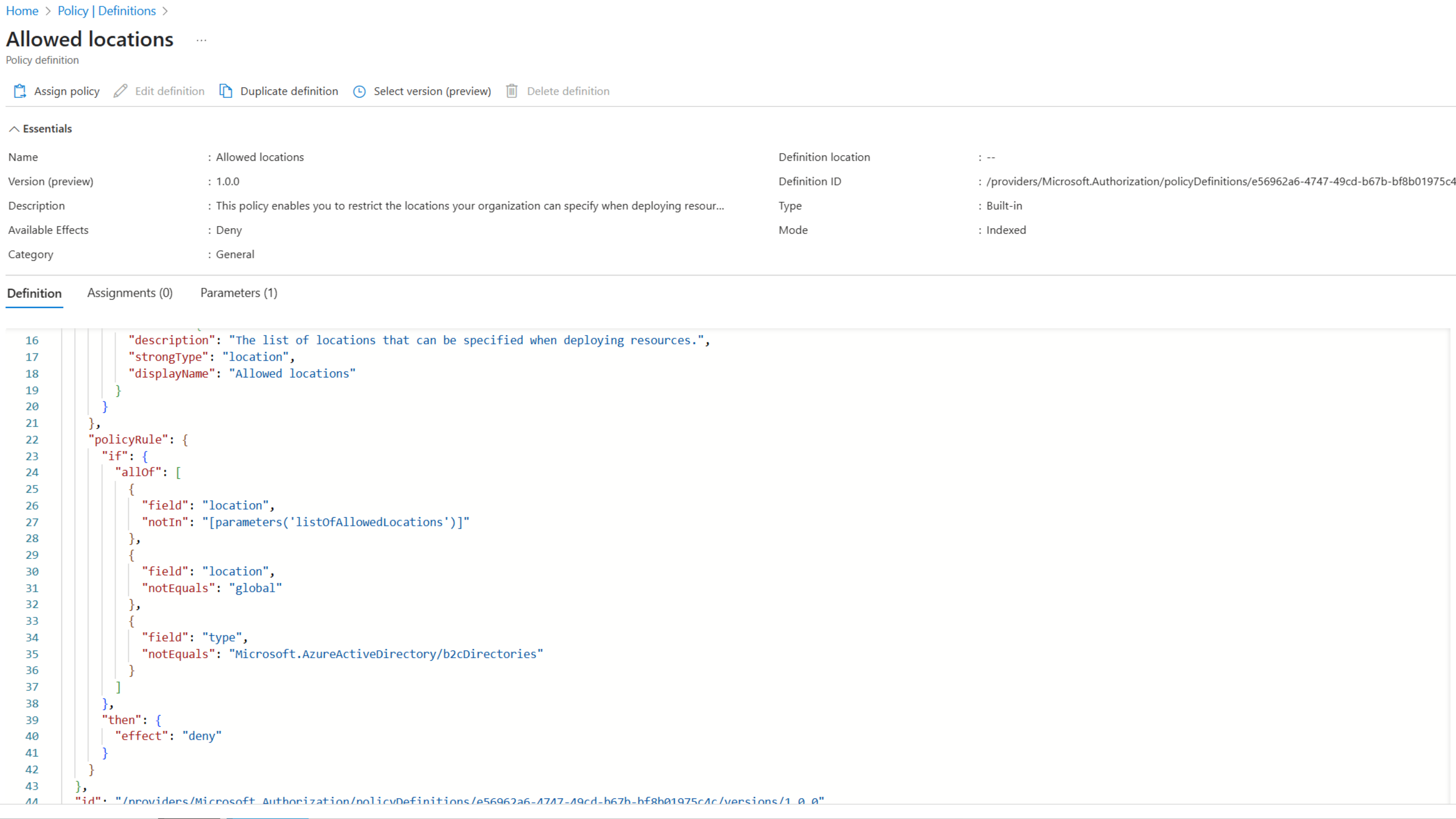
Set of rules to automatically enforce organizational standards

Ensure compliance and security over entire tenant

Unify solutions

How Azure Policies work

Define policies, e.g. only allow resources in West Europe or specific VM SKUs



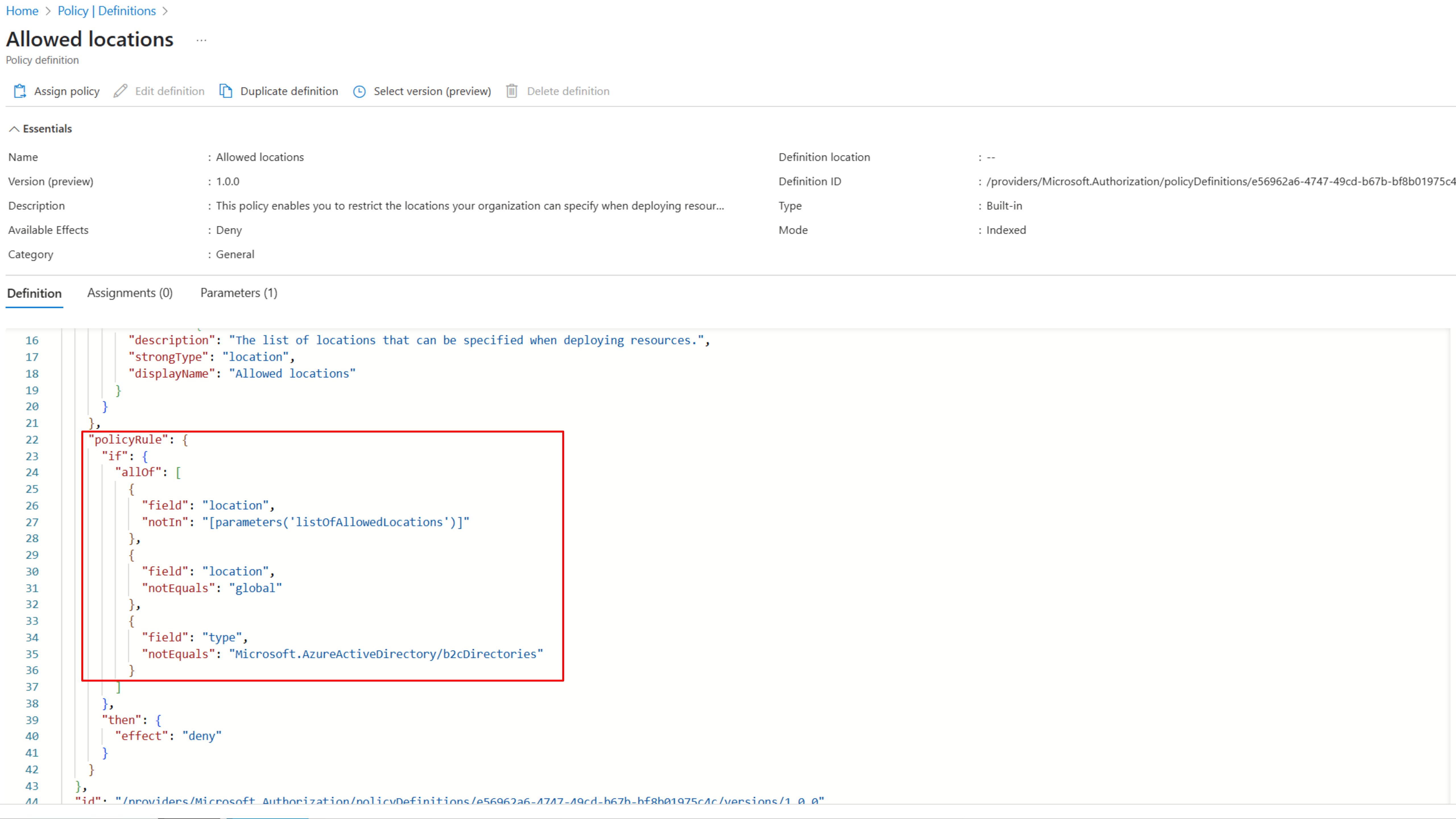
Allowed locations

Policy definition

Essentials

Name	: Allowed locations	Definition location	: --
Version (preview)	: 1.0.0	Definition ID	: /providers/Microsoft.Authorization/policyDefinitions/e56962a6-4747-49cd-b67b-bf8b01975c4
Description	: This policy enables you to restrict the locations your organization can specify when deploying resour...	Type	: Built-in
Available Effects	: Deny	Mode	: Indexed
Category	: General		

```
          "description": "The list of locations that can be specified when deploying resources.",
          "strongType": "location",
          "displayName": "Allowed locations"
        }
      }
    },
    "policyRule": {
      "if": {
        "allOf": [
          {
            "field": "location",
            "notIn": "[parameters('listOfAllowedLocations')]"
          },
          {
            "field": "location",
            "notEquals": "global"
          },
          {
            "field": "type",
            "notEquals": "Microsoft.AzureActiveDirectory/b2cDirectories"
          }
        ]
      },
      "then": {
        "effect": "deny"
      }
    }
  },
  "id": "/providers/Microsoft.Authorization/policyDefinitions/e56962a6-4747-49cd-b67b-bf8b01975c4c/versions/1.0.0"
```



Home > Policy | Definitions >

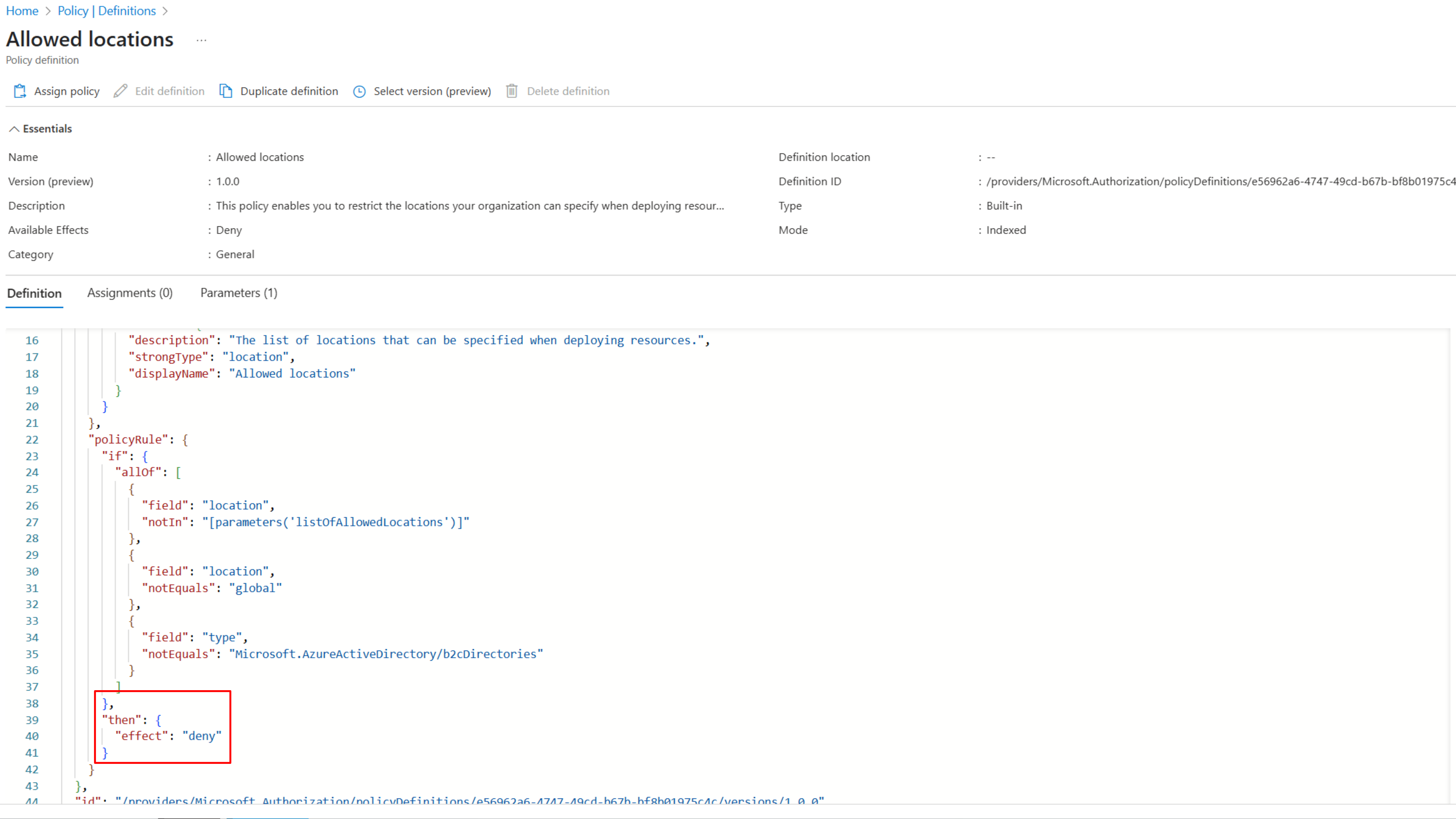
Allowed locations

Policy definition

Essentials

Name	: Allowed locations	Definition location	: --
Version (preview)	: 1.0.0	Definition ID	: /providers/Microsoft.Authorization/policyDefinitions/e56962a6-4747-49cd-b67b-bf8b01975c4
Description	: This policy enables you to restrict the locations your organization can specify when deploying resour...	Type	: Built-in
Available Effects	: Deny	Mode	: Indexed
Category	: General		

```
          "description": "The list of locations that can be specified when deploying resources.",
          "strongType": "location",
          "displayName": "Allowed locations"
        }
      }
    },
    "policyRule": {
      "if": {
        "allOf": [
          {
            "field": "location",
            "notIn": "[parameters('listOfAllowedLocations')]"
          },
          {
            "field": "location",
            "notEquals": "global"
          },
          {
            "field": "type",
            "notEquals": "Microsoft.AzureActiveDirectory/b2cDirectories"
          }
        ]
      },
      "then": {
        "effect": "deny"
      }
    }
  },
  "id": "/providers/Microsoft.Authorization/policyDefinitions/e56962a6-4747-49cd-b67b-bf8b01975c4c/versions/1.0.0"
```



Home > Policy | Definitions >

Allowed locations

Policy definition

Essentials

Name	: Allowed locations	Definition location	: --
Version (preview)	: 1.0.0	Definition ID	: /providers/Microsoft.Authorization/policyDefinitions/e56962a6-4747-49cd-b67b-bf8b01975c4
Description	: This policy enables you to restrict the locations your organization can specify when deploying resour...	Type	: Built-in
Available Effects	: Deny	Mode	: Indexed
Category	: General		

```
          "description": "The list of locations that can be specified when deploying resources.",
          "strongType": "location",
          "displayName": "Allowed locations"
        }
      }
    },
    "policyRule": {
      "if": {
        "allOf": [
          {
            "field": "location",
            "notIn": "[parameters('listOfAllowedLocations')]"
          },
          {
            "field": "location",
            "notEquals": "global"
          },
          {
            "field": "type",
            "notEquals": "Microsoft.AzureActiveDirectory/b2cDirectories"
          }
        ]
      },
      "then": {
        "effect": "deny"
      }
    }
  },
  "id": "/providers/Microsoft.Authorization/policyDefinitions/e56962a6-4747-49cd-b67b-bf8b01975c4c/versions/1.0.0"
```

How Azure Policies work

Define policies, e.g. only allow resources in West Europe or specific VM SKUs

Assign policy to MG, subscription or RG

Automated checks

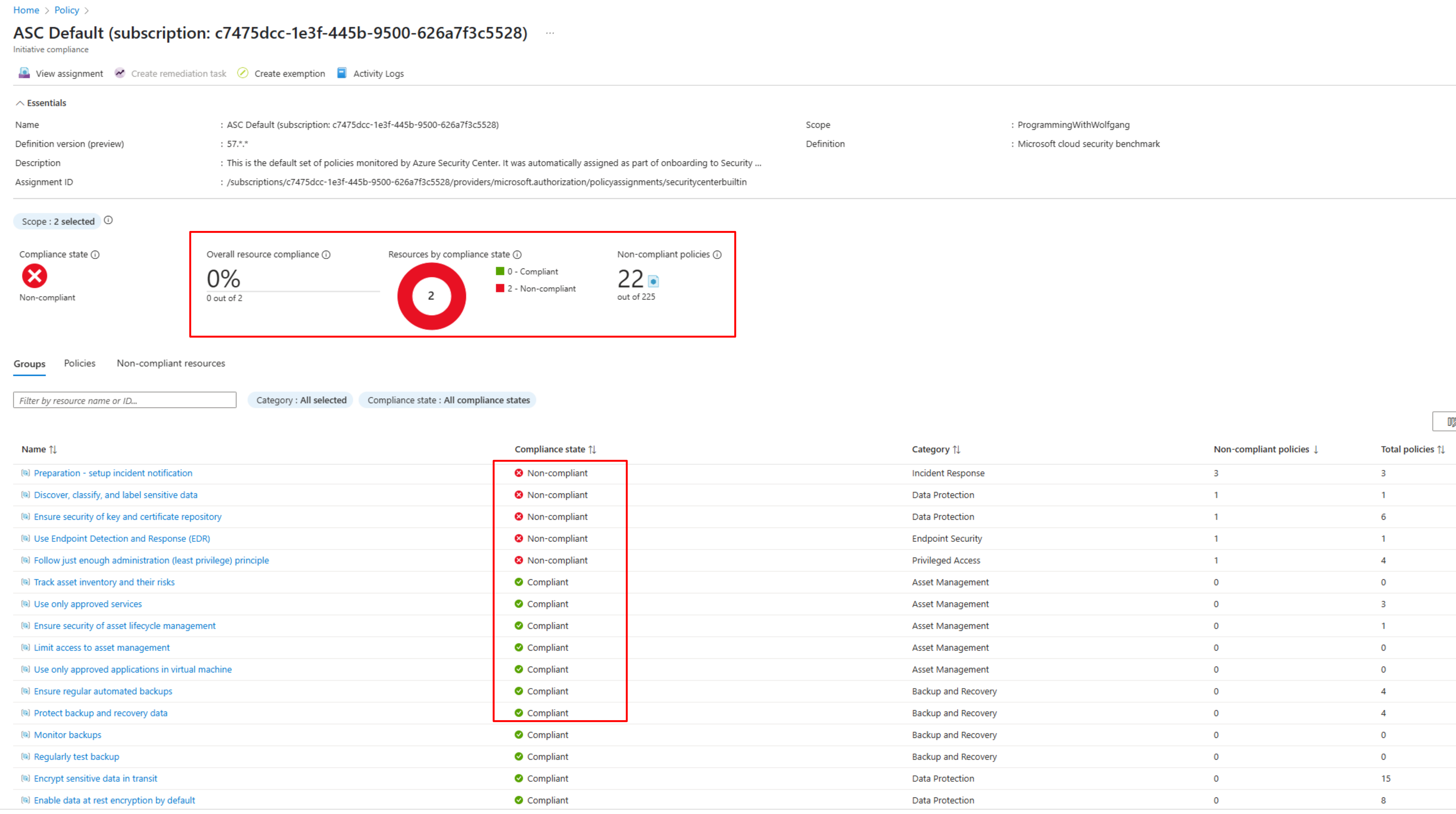
Azure Policy Use Cases

Audit existing resources

Prevent future non-compliance

Automate remediation

Centralized dashboard and control



Home > Policy >

ASC Default (subscription: c7475dcc-1e3f-445b-9500-626a7f3c5528) ···

Initiative compliance

Essentials

Name	: ASC Default (subscription: c7475dcc-1e3f-445b-9500-626a7f3c5528)	Scope	: ProgrammingWithWolfgang
Definition version (preview)	: 57.*.*	Definition	: Microsoft cloud security benchmark
Description	: This is the default set of policies monitored by Azure Security Center. It was automatically assigned as part of onboarding to Security ...		
Assignment ID	: /subscriptions/c7475dcc-1e3f-445b-9500-626a7f3c5528/providers/microsoft.authorization/policyassignments/securitycenterbuiltin		

Scope : 2 selected

Compliance state
Non-compliant

Overall resource compliance
0%
0 out of 2

Resources by compliance state
2
🟩 0 - Compliant
🟥 2 - Non-compliant

Non-compliant policies
22
out of 225

Groups
Policies
Non-compliant resources
Filter by resource name or ID...
Category : All selected
Compliance state : All compliance states

Name ↑↓	Compliance state ↑↓	Category ↑↓	Non-compliant policies ↓	Total policies ↑↓
Preparation - setup incident notification	Non-compliant	Incident Response	3	3
Discover, classify, and label sensitive data	Non-compliant	Data Protection	1	1
Ensure security of key and certificate repository	Non-compliant	Data Protection	1	6
Use Endpoint Detection and Response (EDR)	Non-compliant	Endpoint Security	1	1
Follow just enough administration (least privilege) principle	Non-compliant	Privileged Access	1	4
Track asset inventory and their risks	Compliant	Asset Management	0	0
Use only approved services	Compliant	Asset Management	0	3
Ensure security of asset lifecycle management	Compliant	Asset Management	0	1
Limit access to asset management	Compliant	Asset Management	0	0
Use only approved applications in virtual machine	Compliant	Asset Management	0	0
Ensure regular automated backups	Compliant	Backup and Recovery	0	4
Protect backup and recovery data	Compliant	Backup and Recovery	0	4
Monitor backups	Compliant	Backup and Recovery	0	0
Regularly test backup	Compliant	Backup and Recovery	0	0
Encrypt sensitive data in transit	Compliant	Data Protection	0	15
Enable data at rest encryption by default	Compliant	Data Protection	0	8

Azure Policy with AKS

Manage resources inside cluster → Azure Policy Add-on for AKS

Manage Cluster → Azure Policy