Azure Policy

Memi Lavi
www.memilavi.com

Azure Policy

- Enforcing organizational standards and compliance at scale is not simple
- Quite important in the cloud
- Role-based access helps a little, but not enough

Azure Policy

- Examples:
  - All VMs should be built on a specific region
  - Only specific types of VM are allowed to be built
  - Tags must be specified on all resources in the resource group
  - App Services should only be accessible over HTTPS

Azure Policy

- Azure Policy is the mechanism for that
- It allows:
  - Defining policies
  - Assigning the policies to scopes (Subscription, Resource Group, specific resource)
- Is free (aside from auditing guest machines)

Azure Policy Evaluation

- Policies are evaluated:
    - When a resource is created / updated / deleted in a scope
    - When a new policy is assigned to a scope
    - When a policy is updated
    - Once every 24 hours (compliance evaluation cycle)

Azure Policy Outcome

- As a result of a non-compliant resource:
  - Resource change is denied
  - Resource change is logged
  - Resource is altered before the change
  - Resource is altered after the change
  - Related resources are deployed

Azure Policy Concepts

Definition → The policy definition: What is allowed, and to what resources (eg. Only specific VM sizes can be built)

Initiative → Logical grouping of definitions. (eg. VM definitions)

Assignment → Assigning the definition or initiative to a scope (Subscription, Resource Group, individual resource)

Effect → What is the outcome regarding non-compliant resource

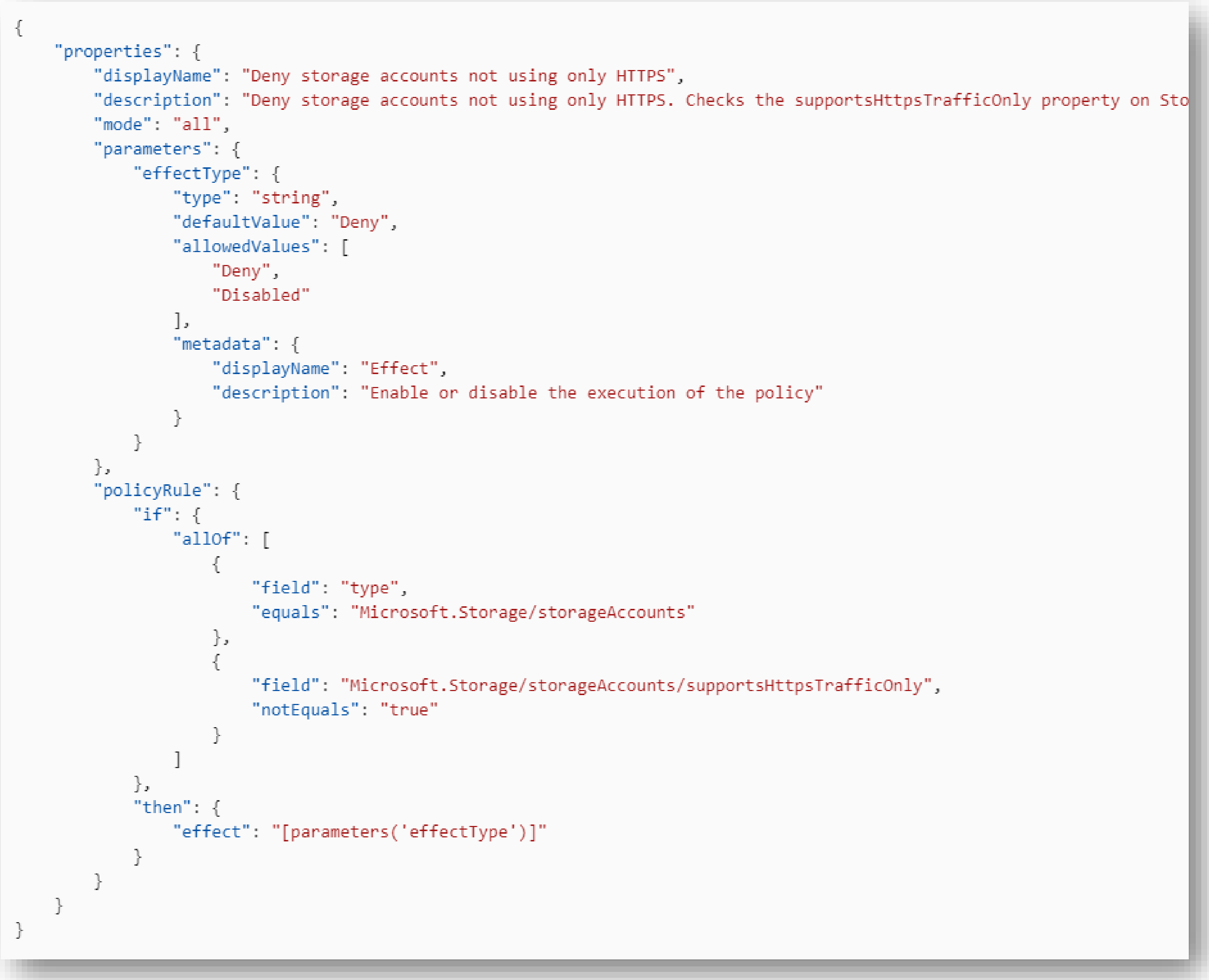
Custom Policies

- So far we’ve used built-in policies
- You can create your own if there isn’t one that satisfies your needs
- Look very closely at existing definitions and sample, you might find what you’re looking for

Custom Policies Authoring

- Policy Definitions are JSON-based documents
- Describe the various properties of the policy, and the rule

Custom Policy Example



```
{
    "properties": {
        "displayName": "Deny storage accounts not using only HTTPS",
        "description": "Deny storage accounts not using only HTTPS. Checks the supportsHttpsTrafficOnly property on Sto
        "mode": "all",
        "parameters": {
            "effectType": {
                "type": "string",
                "defaultValue": "Deny",
                "allowedValues": [
                    "Deny",
                    "Disabled"
                ],
                "metadata": {
                    "displayName": "Effect",
                    "description": "Enable or disable the execution of the policy"
                }
            }
        },
        "policyRule": {
            "if": {
                "allOf": [
                    {
                        "field": "type",
                        "equals": "Microsoft.Storage/storageAccounts"
                    },
                    {
                        "field": "Microsoft.Storage/storageAccounts/supportsHttpsTrafficOnly",
                        "notEquals": "true"
                    }
                ]
            },
            "then": {
                "effect": "[parameters('effectType')]"
            }
        }
    }
}
```