Policies creation

Table of contents

- RBAC vs policy
- Types of policies
- policy assignment
- Policy enforcement
- exclusions (not scope)
- policy limits
- Blueprints

- denial effect (not allowed a resource to be created if not compliant).
- audit effect (allowed a resource to be created with a warning message).
  - shows non compliant resources in ⟹ *compliance / policy name / activity logs*.

RBAC vs policy

RBAC	Policy
Controlling the permissions, the actions that I can take on certain scopes and certain resources.	Those guard rails to control the types of resour we can use, type of configurations we're allowed have

---

- ! Question
- How can i use azure policy to really enforce those requirements we have?

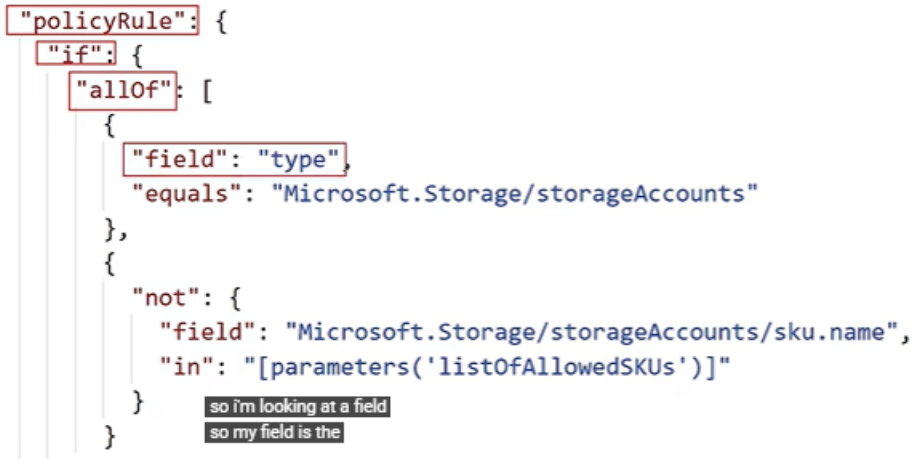
- Arc enabled Infrastructure. what it does is, it takes the azure control plane and takes it to other clouds, it takes it on premises.
- There are aspects of it that will also apply to these arc enabled resources.
- so don't think of this as only azure resources because **arc enablement extends that azure control plane elsewhere, all these azure policies gonna apply there as well** .
- so when i think about azure policy it is a **json format** and the goal is i'm going to create this structure so i'm going to think about.

- this json document and i can do many different types of things i might say hey
  - i want to restrict to certain locations,
  - i want certain tag values,
  - i only want to use this type of skew
    there's a whole set of different things i can do

---

policies

1. Properties
2. definition location
3. parameters
4. Policy rule



- allof - &
- anyOf - ||
- not - !
- if condition
- then effect
  - disabled (will not evaluated)
  - append/modify (adding to an array / add, replace, remove tags or properties)
  - deny (based on the condition, deny it)
  - audit (let it happen, track the compliance)
  - audit if not exist
  - deploy if not exist (execute a template, to perform some remediation to make something right)

Types of policies

1. built-in
2. custom
3. static

---

policy assignment

assigning that particular policy to a level of hierarchy and that policy can be inherited to the lower levels.

Policy enforcement

1. enabled
2. disabled

- think of disabled as *what-if* mode.

---

exclusions (not scope)

exclude that policy to a particular

- sub
- res grp
- res

---

policy limits

exclusions limit - 400 exclusions

definitions - an *entry of Scope*
management group or
subscription.

assignments and exemptions - an *entry of Scope*
management group,
subscription,
resource group, or
individual resource.

Maximum count of Azure Policy objects

There's a maximum count for each object type for Azure Policy. For definitions, an entry of *Scope* means the management group or subscription. For assignments and exemptions, an entry of *Scope* means the management group, subscription, resource group, or individual resource.

Where	What	Maximum count
Scope	Policy definitions	500
Scope	Initiative definitions	200
Tenant	Initiative definitions	2,500
Scope	Policy or initiative assignments	200
Scope	Exemptions	1000
Policy definition	Parameters	20
Initiative definition	Policies	1000
Initiative definition	Parameters	400
Policy or initiative assignments	Exclusions (notScopes)	400
Policy rule	Nested conditionals	512
Remediation task	Resources	50,000
Policy definition, initiative, or assignment request body	Bytes	1,048,576

Object type	Maximum count	Scope
Policy definitions	500	Management group or subscription
Initiative definitions	200	Management group, subscription, or tenant
Policy or initiative assignments	200	Management group, subscription, resource gro or individual resource
Exemptions	1000	Management group, subscription, resource gro or individual resource
Policy definition parameters	20	Policy definition
Initiative definition policies	1000	Initiative definition
Initiative definition parameters	400	Initiative definition
Policy or initiative assignment exclusions (notScopes)	400	Policy or initiative assignment
Policy rule nested conditionals	512	Policy rule
Remediation task resources	50,000	Policy definition, initiative, or assignment request body
Request body size (bytes)	1,048,576	Policy definition, initiative, or assignment request body

---

Blueprints

Blueprints used to combine resource groups and arm templates and RBAC and policies