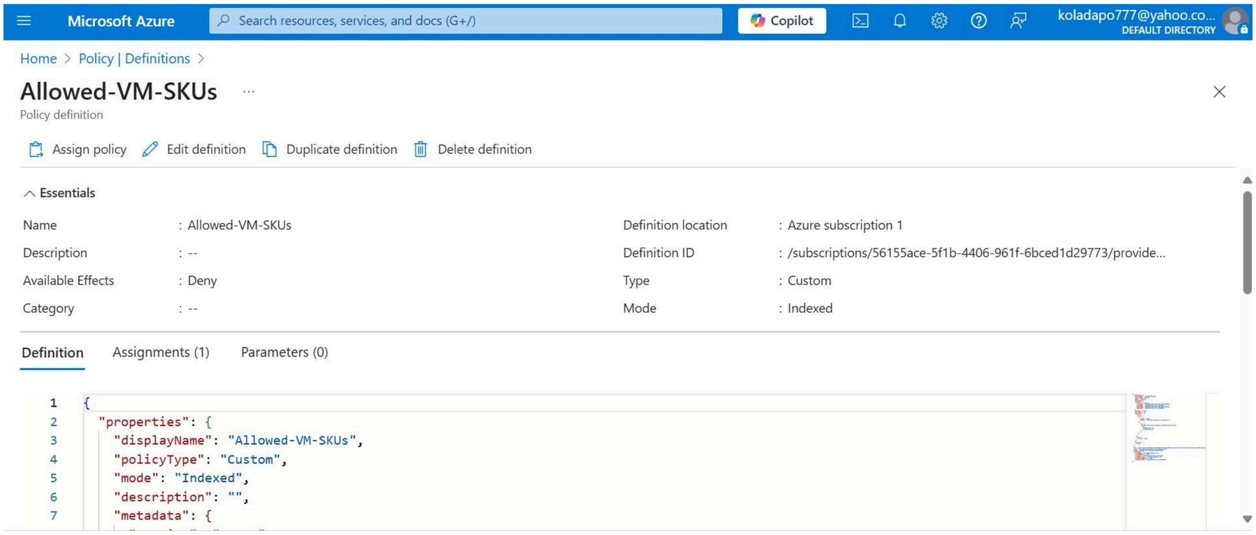
Project Summary Report: Implementing Governance with Azure Policy

From the outset, my objective for this project was clear: to implement and validate governance using Azure Policy, specifically focusing on restricting Virtual Machine SKUs. This involved understanding key Azure Policy components, creating and assigning a custom policy, and rigorously testing its enforcement in real-world scenarios.

My prerequisites included having an Azure account with appropriate permissions and a dedicated resource group for testing.

Key Accomplishments & Findings:

1. **Azure Policy Fundamentals:** I successfully familiarised myself with the core components of Azure Policy, including policy definitions, assignments, and initiatives. I also explored various built-in policies to understand their structure and capabilities.
2. **Custom Policy Creation and Assignment:** I designed and implemented a custom Azure Policy definition named "Allowed-VM-SKUs." This policy was configured to explicitly **deny** the creation of any Virtual Machines with SKUs other than `Standard_D2s_v3` and `Standard_D4s_v3`. I then assigned this policy to my designated test resource group, setting its effect to "deny."



Allowed-VM-SKUs

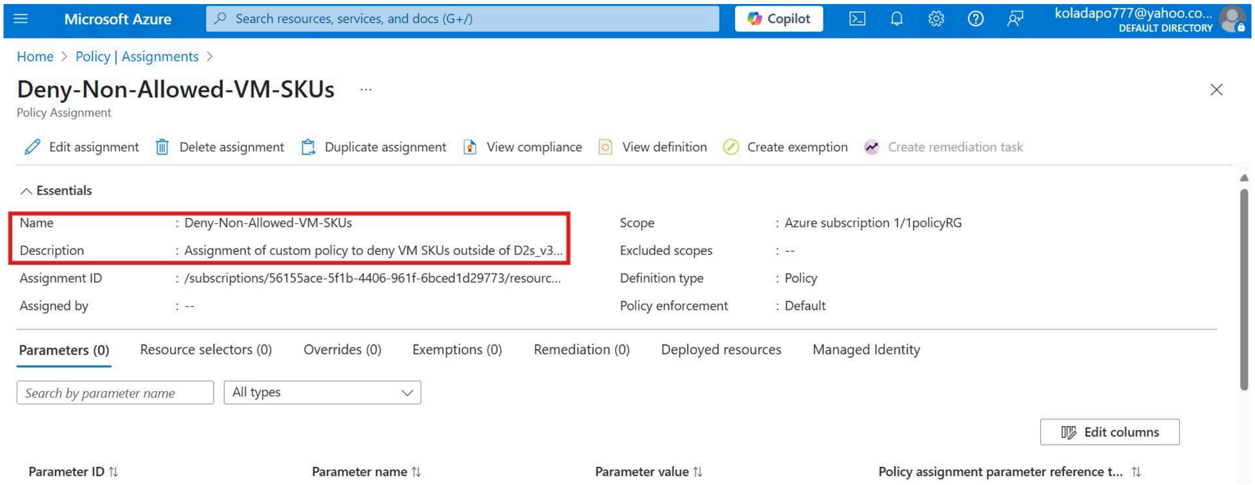
Policy definition

Essentials

Name	: Allowed-VM-SKUs	Definition location	: Azure subscription 1
Description	: --	Definition ID	: /subscriptions/56155ace-5f1b-4406-961f-6bced1d29773/provide...
Available Effects	: Deny	Type	: Custom
Category	: --	Mode	: Indexed

```
{
  "properties": {
    "displayName": "Allowed-VM-SKUs",
    "policyType": "Custom",
    "mode": "Indexed",
    "description": "",
    "metadata": {
```

Screenshot of Policy Definition validates the creation on the Azure Portal



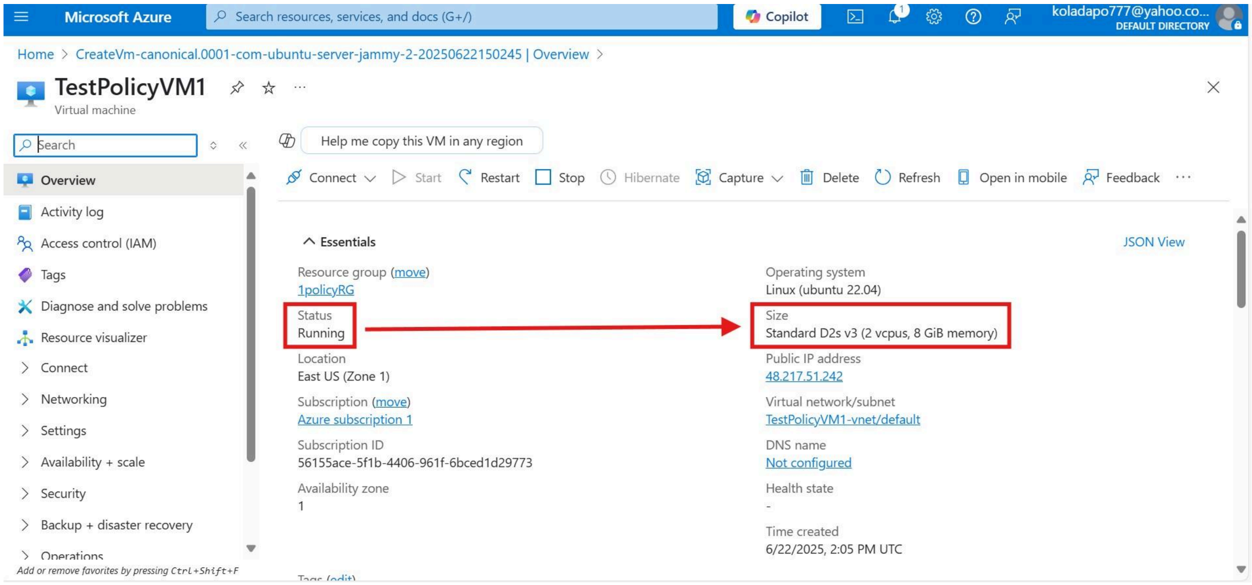
Deny-Non-Allowed-VM-SKUs

Policy Assignment

Name : Deny-Non-Allowed-VM-SKUs
Description : Assignment of custom policy to deny VM SKUs outside of D2s_v3...
Assignment ID : /subscriptions/56155ace-5f1b-4406-961f-6bced1d29773/resourc...
Assigned by : --
Scope : Azure subscription 1/1policyRG
Excluded scopes : --
Definition type : Policy
Policy enforcement : Default

Screenshot of Policy Assignment in Azure Portal

3. **Validation of Policy Enforcement (Task 3):** This was a critical phase that yielded clear results:
    - **Compliant Deployment:** I successfully deployed a Virtual Machine using the `Standard_D2s_v3` SKU. This confirmed that the policy correctly permitted resources that adhered to its rules.



TestPolicyVM1

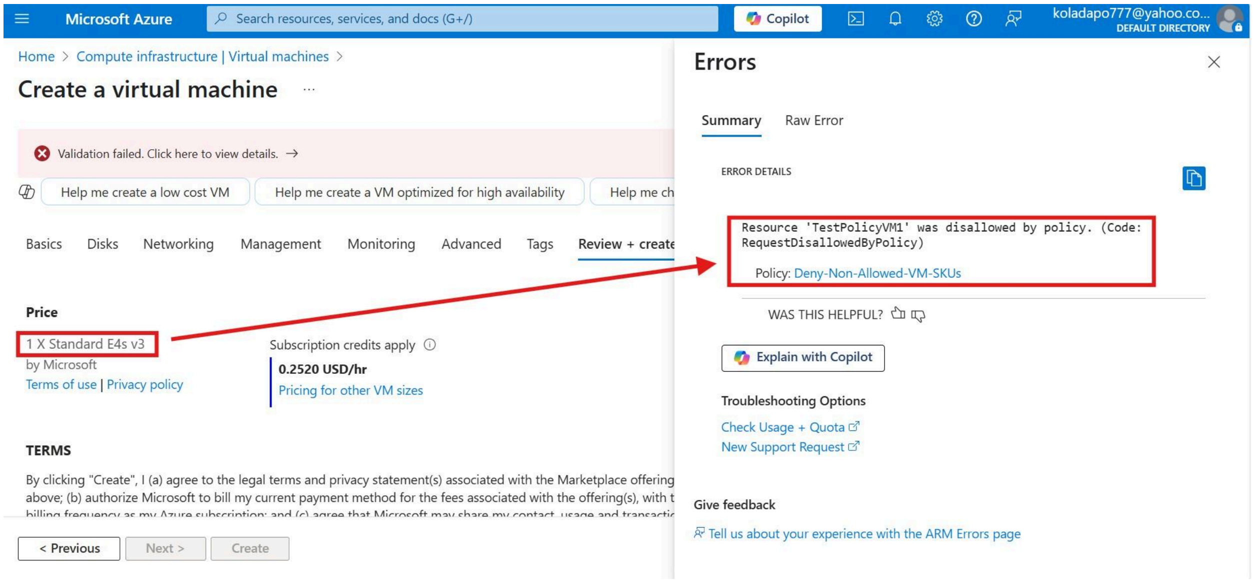
Virtual machine

Resource group (move)
1policyRG
Status
Running
Location
East US (Zone 1)
Subscription (move)
Azure subscription 1
Subscription ID
56155ace-5f1b-4406-961f-6bced1d29773
Availability zone
1

Operating system
Linux (ubuntu 22.04)
Size
Standard D2s v3 (2 vcpus, 8 GiB memory)
Public IP address
48.217.51.242
Virtual network/subnet
TestPolicyVM1-vnet/default
DNS name
Not configured
Health state
-
Time created
6/22/2025, 2:05 PM UTC

Screenshot of Successful Compliant VM SKU size Deployment (Standard D2s_v3)

  - **Non-Compliant Deployment Denial:** When I attempted to deploy a Virtual Machine with the `Standard_E4s_v3` SKU (which is not in the allowed list), the deployment was explicitly **denied** by the Azure Policy. This was a definitive validation of the policy's effectiveness in enforcing the desired governance.



Create a virtual machine

Validation failed. Click here to view details. →

Price

1 X Standard E4s v3
by Microsoft
Terms of use | Privacy policy

Subscription credits apply

0.2520 USD/hr
Pricing for other VM sizes

TERMS

By clicking "Create", I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace offering above; (b) authorize Microsoft to bill my current payment method for the fees associated with the offering(s), with t billing frequency as my Azure subscription; and (c) agree that Microsoft may share my contact, usage and transactio

Errors

ERROR DETAILS

```
Resource 'TestPolicyVM1' was disallowed by policy. (Code:
RequestDisallowedByPolicy)
```

Policy: Deny-Non-Allowed-VM-SKUs

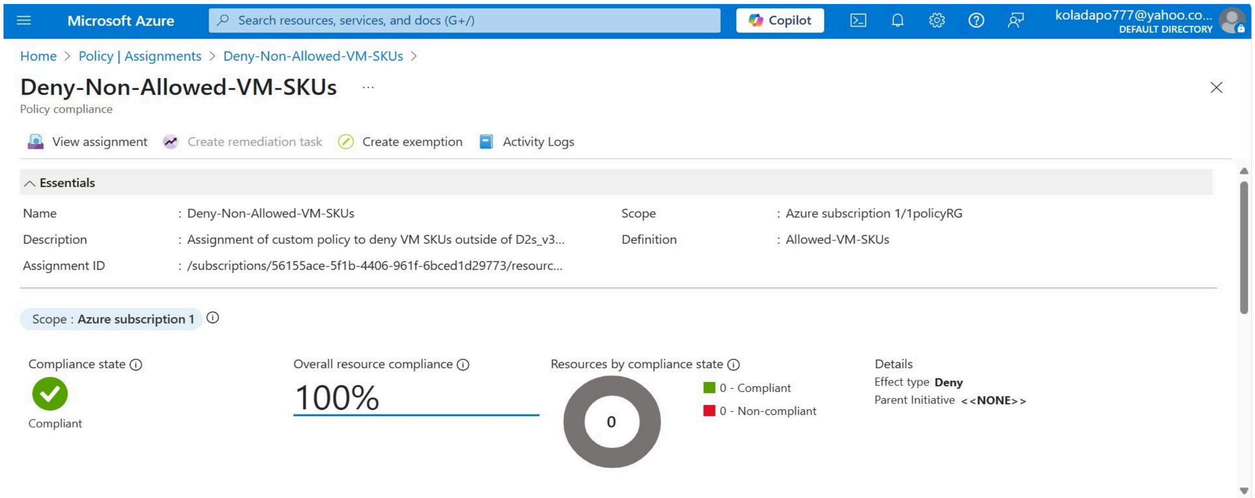
Troubleshooting Options

Give feedback

Tell us about your experience with the ARM Errors page

Screenshot of failed non-compliant VM SKU size (Standard E4s_v3)

4. **Compliance Status:** The Azure Policy compliance dashboard for my assignment showed a "100% Compliant" status with "0 Non-compliant" resources. This is the expected outcome for a `Deny` policy, as it prevents non-compliant resources from being provisioned in the first place, thus maintaining a compliant state.



Deny-Non-Allowed-VM-SKUs

Policy compliance

Name	: Deny-Non-Allowed-VM-SKUs	Scope	: Azure subscription 1/1policyRG
Description	: Assignment of custom policy to deny VM SKUs outside of D2s_v3...	Definition	: Allowed-VM-SKUs
Assignment ID	: /subscriptions/56155ace-5f1b-4406-961f-6bced1d29773/resourc...		

Scope : Azure subscription 1

Compliance state
Compliant

Overall resource compliance
100%

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

Details
Effect type Deny
Parent Initiative <<NONE>>

Screenshot of Policy Compliant Status

This project successfully demonstrated the implementation and real-world effectiveness of Azure Policy in enforcing organisational standards regarding VM SKU usage. The experience provided valuable insights into policy definition, assignment, validation, and crucial troubleshooting aspects related to Azure's global infrastructure.

<u>Deeper Insights and Real-World Applications of Azure Policy Findings</u>

The successful implementation of the VM SKU restriction policy offers several deeper insights into the practical application of Azure Policy in a real-world cloud environment.

Deeper Insight and Analysis:

1. **Beyond Simple Control: Proactive Guardrails & Post-Deployment Denial:** My experience showed that Azure Policy isn't just about reactive auditing; its `Deny` effect acts as a powerful guardrail. In my testing within 'East US', non-compliant resources were consistently blocked *during* the actual deployment validation process. This highlights that Policy consistently prevents non-compliant resources by denying the creation request, thereby significantly reducing human error and forcing adherence to standards *before* resources are fully provisioned.
2. **Holistic Governance View:** The crucial realisation about regional availability and subscription quotas highlighted that effective Azure governance extends beyond just policy rules. Policies must be designed and applied with a keen understanding of other Azure service limitations and subscription configurations. A policy might technically allow a resource, but if the underlying region or quota doesn't support it, the deployment will still fail. This emphasises the need for a holistic view, where policy, regional planning, and quota management are all interconnected aspects of a robust governance strategy.
3. **Nuance in Immediate Feedback Loops:** During the project, specifically when testing in 'East US', I observed that resources that violated the policy were *not* proactively greyed out in the portal. Instead, the denial consistently occurred during the deployment validation phase. This indicates that while Azure Policy ensures consistent enforcement by blocking non-compliant deployments, the immediate visual feedback in the portal can vary. Regardless of the UI presentation, the policy's core function of blocking non-compliant deployments remained consistently effective, shifting the enforcement to the deployment validation step if not reflected visually beforehand.

<u>Real-World Applications and Potential Use Cases</u>:

The findings from this specific VM SKU restriction project are highly transferable to a multitude of real-world Azure governance challenges:

- **Cost Management:**

    - **Use Case:** Preventing the deployment of overly expensive VM SKUs or high-tier storage accounts.
    - **Insight:** Policies can enforce cost-effective choices across compute, storage, and networking, ensuring budget adherence.
- **Security Baselines:**
    - **Use Case:** Mandating encryption for all storage accounts or databases; enforcing specific network security group (NSG) rules; requiring HTTPS for web applications.
    - **Insight:** Policies can ensure a foundational security posture automatically, reducing the attack surface.
- **Regulatory Compliance (e.g., GDPR, HIPAA):**
    - **Use Case:** Restricting data residency to specific geographic regions, ensuring specific tags are applied for data classification, and mandating logging and monitoring configurations.
    - **Insight:** Azure Policy provides a programmatic way to enforce controls required by various regulatory frameworks, simplifying compliance audits.
- **Resource Consistency and Tagging:**
    - **Use Case:** Requiring specific tags (e.g., 'Environment', 'CostCenter', 'Owner') on all resources; enforcing naming conventions for resources and resource groups.
    - **Insight:** Essential for clear resource organisation, cost allocation, and simplified management at scale. The `Append` and `Modify` effects of policy are particularly useful here.
- **Network Security:**
    - **Use Case:** Only allowing specific Virtual Network (VNet) ranges to be created, restricting public IP addresses, and enforcing the use of Azure Private Link.
    - **Insight:** Policies can build a strong network perimeter by controlling what can be deployed and how it connects.
- **Disaster Recovery (DR) and High Availability (HA):**
    - **Use Case:** Requiring virtual machines to be deployed within Availability Sets or Availability Zones; enforcing data replication strategies.
    - **Insight:** Policies can help ensure that critical applications are designed and deployed with the necessary resilience from the start.

In conclusion, my experience highlights that Azure Policy is a foundational tool for any organisation looking to achieve robust, scalable, and automated governance in their cloud estate. It empowers cloud teams to define guardrails that ensure security, compliance, cost efficiency, and operational consistency across their entire Azure footprint.