Custom Azure RBAC Role for Key Vault Secrets Access

Assign precise read-only access to secrets in Azure Key Vault using custom roles

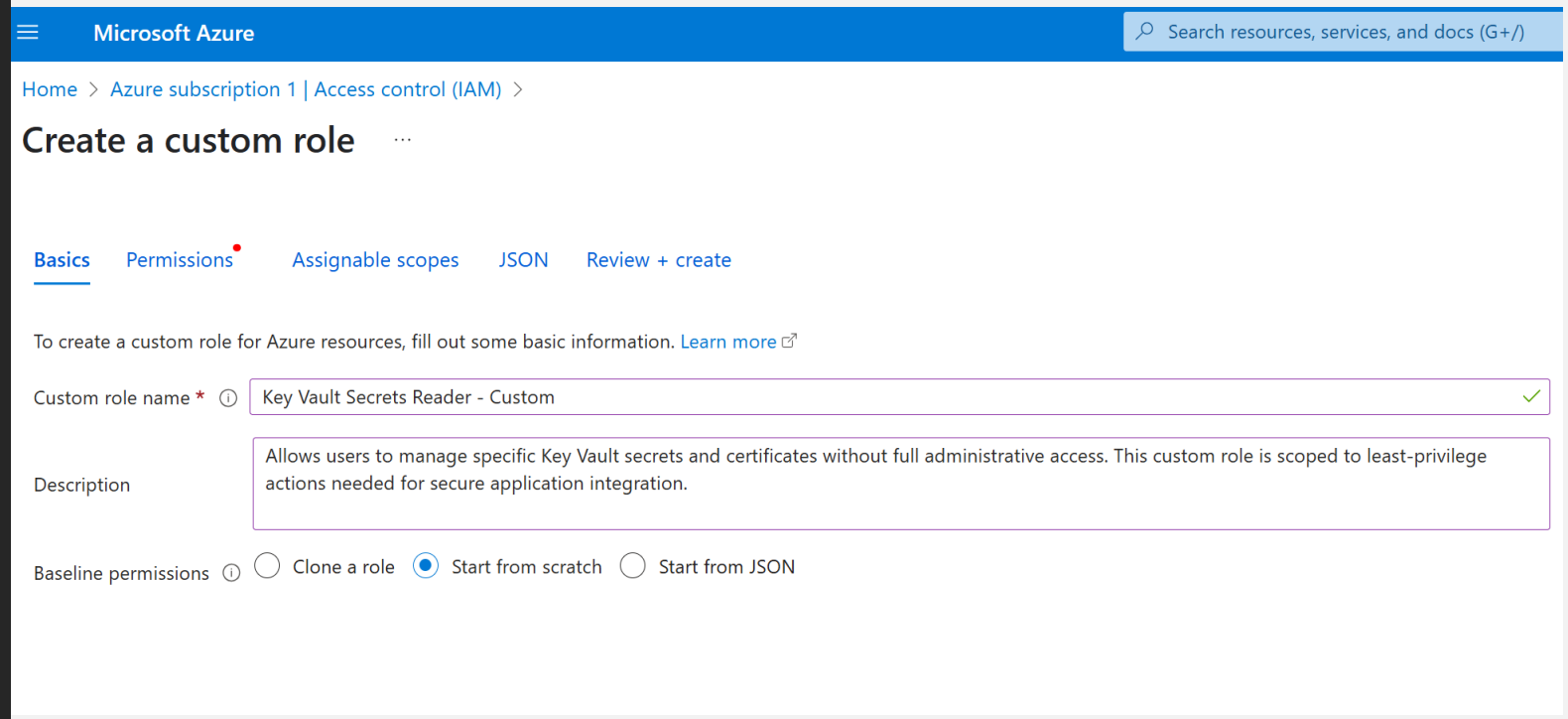
#PerparimLabs #AzureSecurity #EntraRBAC

Why Create a Custom Role for Azure Key Vault?

- **Built-in roles** like ***Reader*** or ***Contributor*** may grant more permissions than needed
- Custom roles allow precise control — e.g., **read-only access to secrets**
- Helps enforce **least privilege** and **segregation of duties**
- Applies across **RBAC-supported scopes** (subscription, resource group, or vault level)

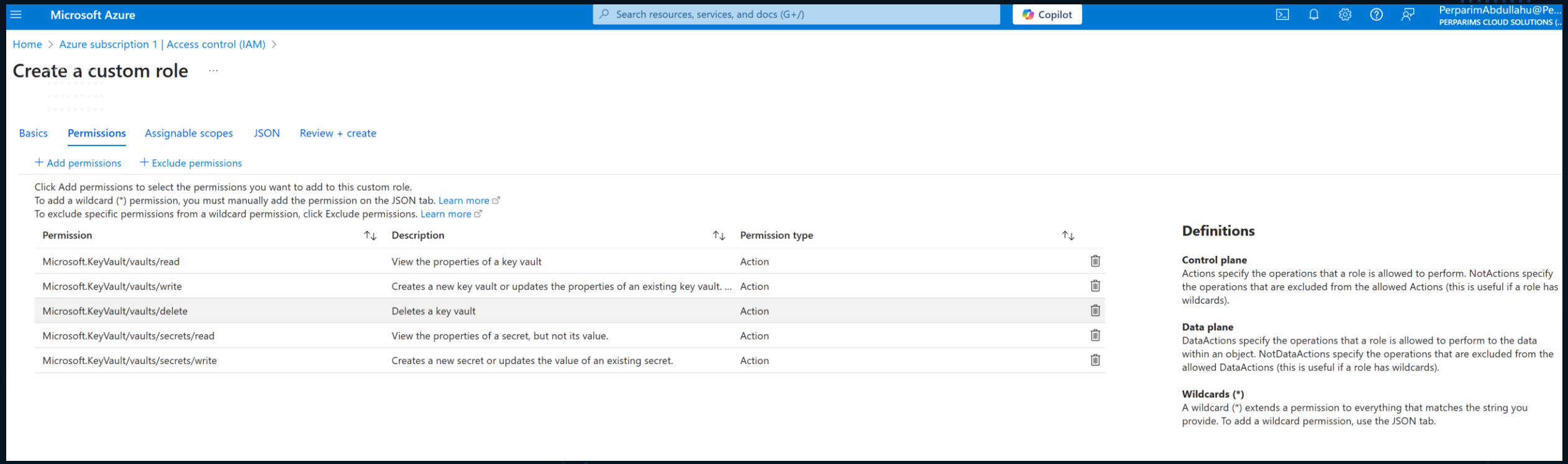
#RBAC #LeastPrivilege #AzureKeyVault

Create a Custom Role for Azure Key Vault



- Navigate to **Subscriptions** > select your subscription
- Go to **Access Control (IAM)** > click **+ Add** → **Add Custom Role**
- Choose ***Start from scratch*** and give your role a name *(e.g., "Key Vault Secrets Reader - Custom")*
- Optionally, add a **description** for clarity

#AzureRBAC #CustomRole #KeyVaultAccess



Define Permissions for the Custom Role

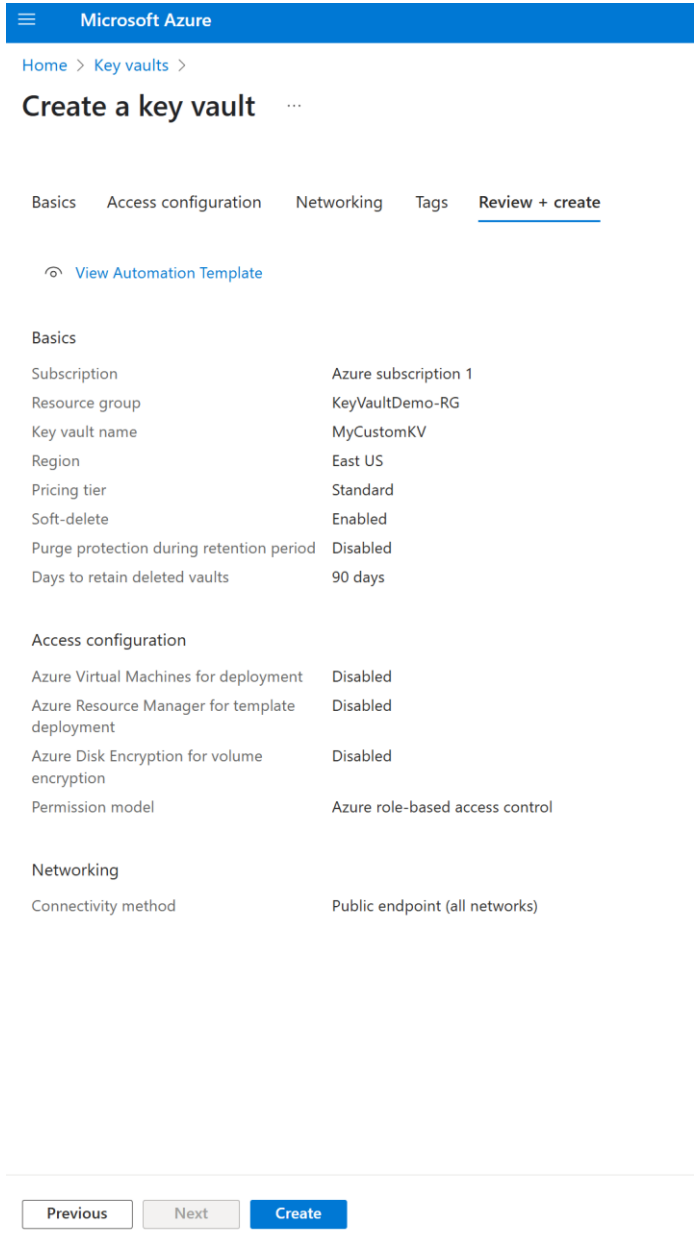
- In the **Permissions** tab, click **+ Add permissions**
- Use the search bar to find:
  - Microsoft.KeyVault/vaults/* – full Key Vault permissions
  - Or specific actions like secrets/read, secrets/list
- Select only the permissions your role requires
- Click **Add** to confirm selection

#LeastPrivilege #CustomRBAC #AzureKeyVault

Create a New Azure Key Vault

- Go to **portal.azure.com**
- Search for **Key Vaults** in the top search bar
- Click **+ Create**
- Fill in:
- **Resource Group:** (e.g., KeyVaultDemo-RG)
- **Key Vault Name:** (e.g., MyCustomKV)
- **Region:** East US or your preferred one
- **Pricing Tier:** Standard (or Premium if needed)
- **Access Configuration:** Choose **Azure Role-Based Access Control (RBAC)**
- Click **Review + Create** → **Create**

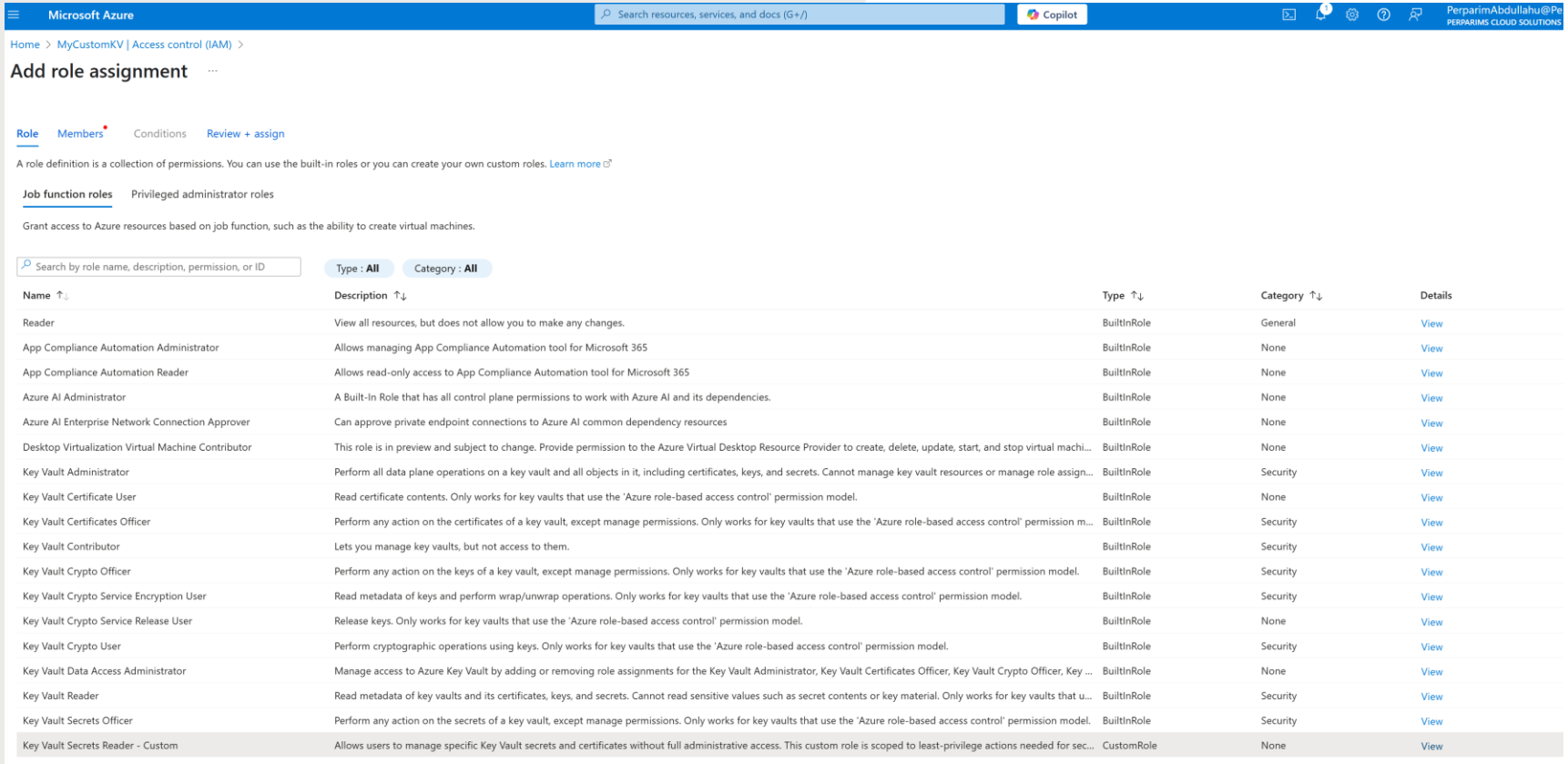
🔐 *Choosing Azure Role-Based Access Control lets us use the custom role we created earlier.*

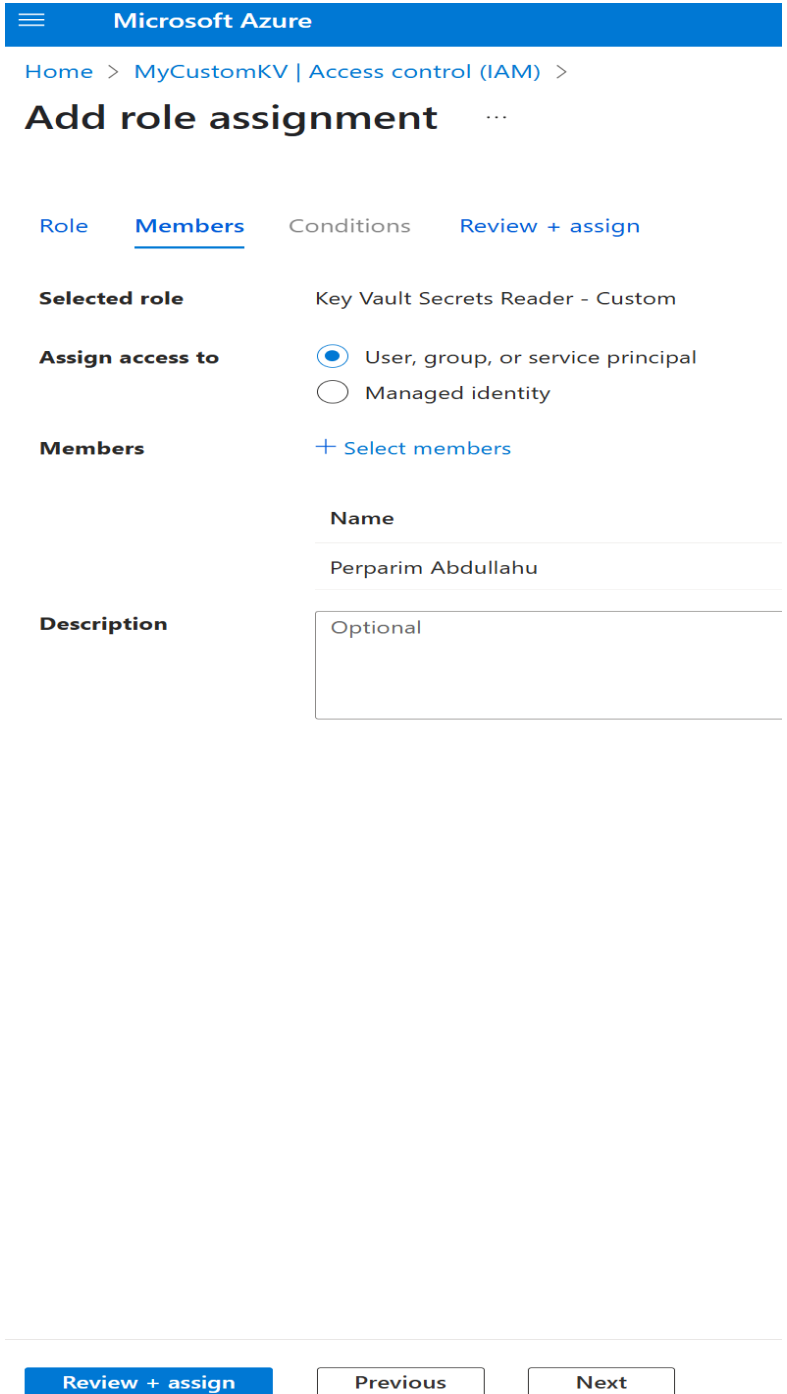


#AzureKeyVault #AccessManagement #RBACSecurity

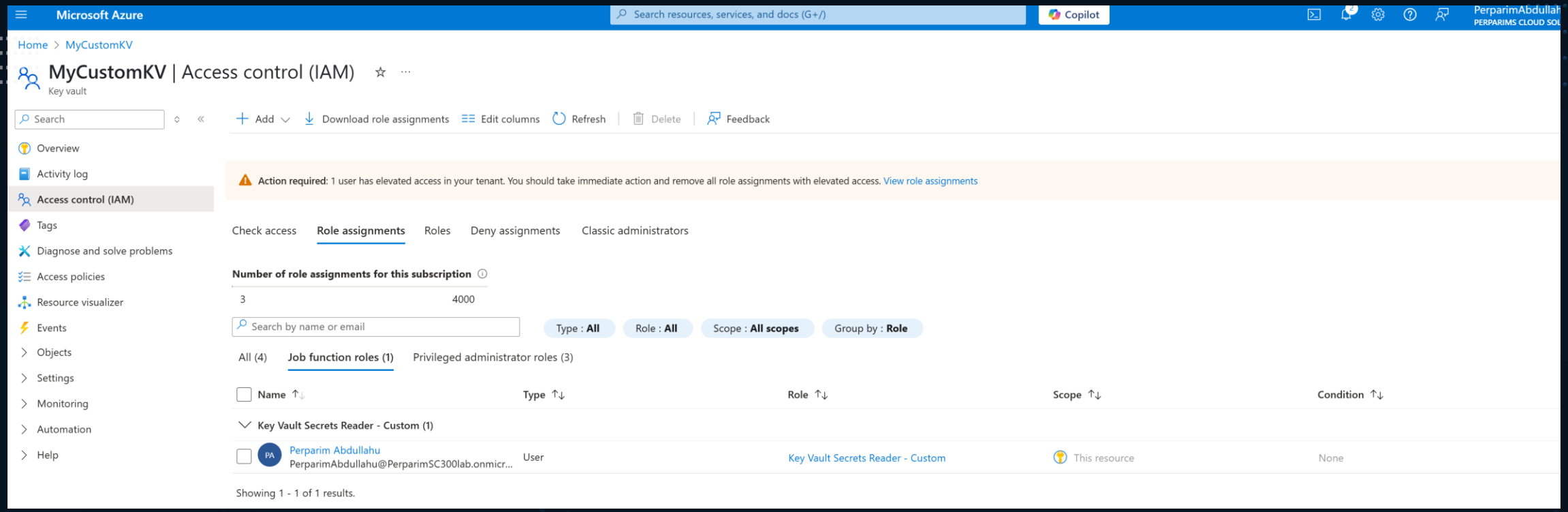
Assign Custom Role to a User via IAM

- Go to the **Key Vault** you just created
- On the left blade, click **Access control (IAM)**
- Click **+ Add** → **Add role assignment**
- In the Role dropdown, search and select your **custom role** (e.g., Key Vault Secrets Reader - Custom)
- Click **Next**
- Under Members, choose a **User, Group, or Service Principal**
- Select the member and click **Next** → **Review + assign**





#RoleAssignment #AzureSecurity #IAMControl



Confirm Custom Role Assignment

- Go back to the **Key Vault → Access control (IAM)**
- Click **Role assignments** tab
- Confirm that the **custom role** is assigned to your user
- Click your user to view **permissions inherited from the custom role**
- Optional: Try accessing Key Vault items (e.g., Secrets) to test the effective permission
- If your role included secrets/list, confirm visibility
- If secrets/get, confirm value access

🔍 *Use "Check access" if you want to validate permissions for a specific user.*

#VerifyAccess #RBACinAction #AzureKeyVaultLab

Key Takeaways from the Lab

- ✅ Created a **custom Azure RBAC role** for granular Key Vault access
- ✅ Selected only required permissions (e.g., secrets/list, secrets/get) — following **least privilege** principle
- ✅ Assigned the role at the **Key Vault scope** via IAM blade
- ✅ Verified access by confirming role assignment and testing access
- 💼 This setup mirrors real-world scenarios where teams need **controlled access to secrets** without granting full admin rights

#AzureLabs #CustomRBAC #AccessControl
#KeyVaultSecurity