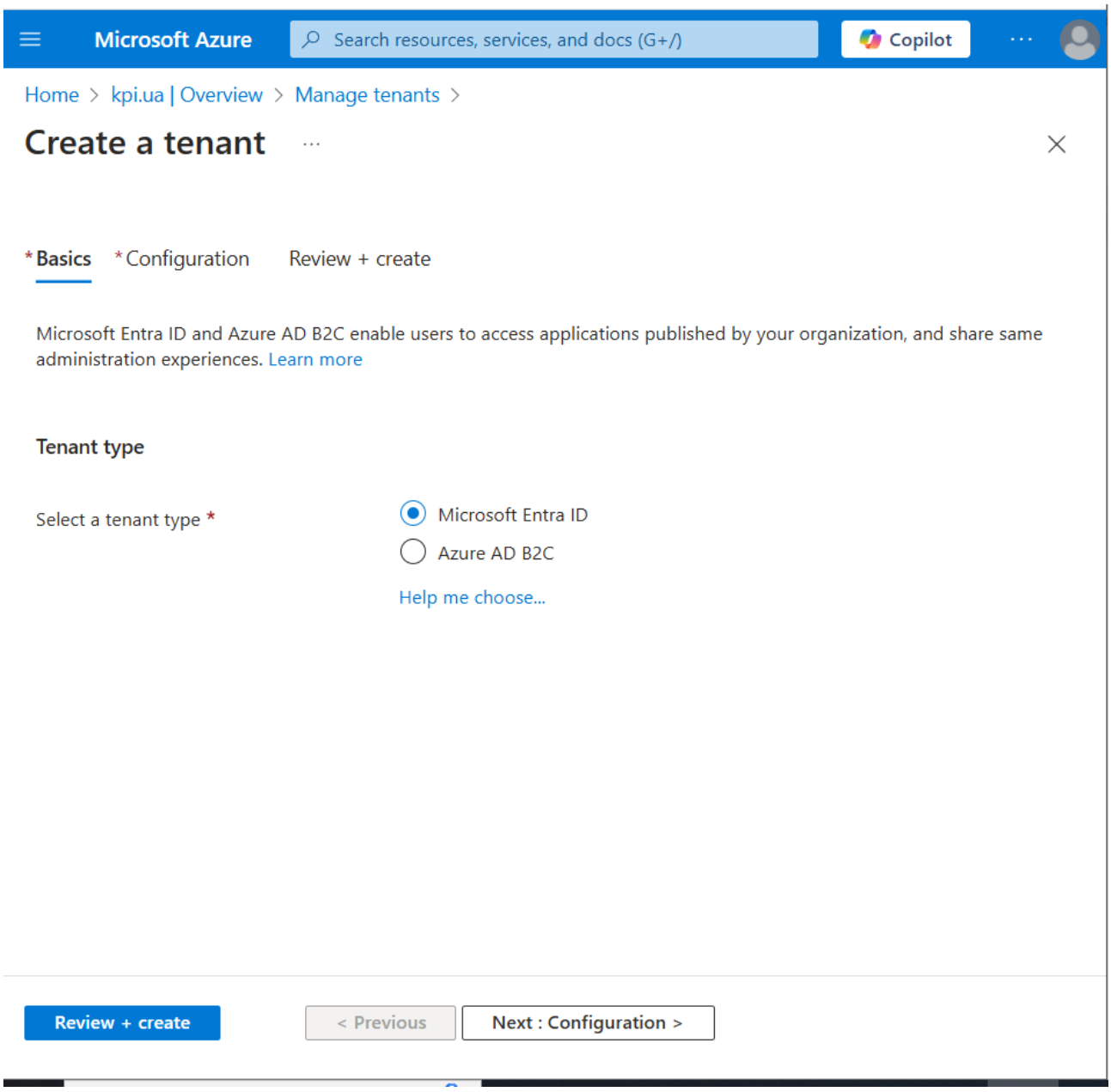
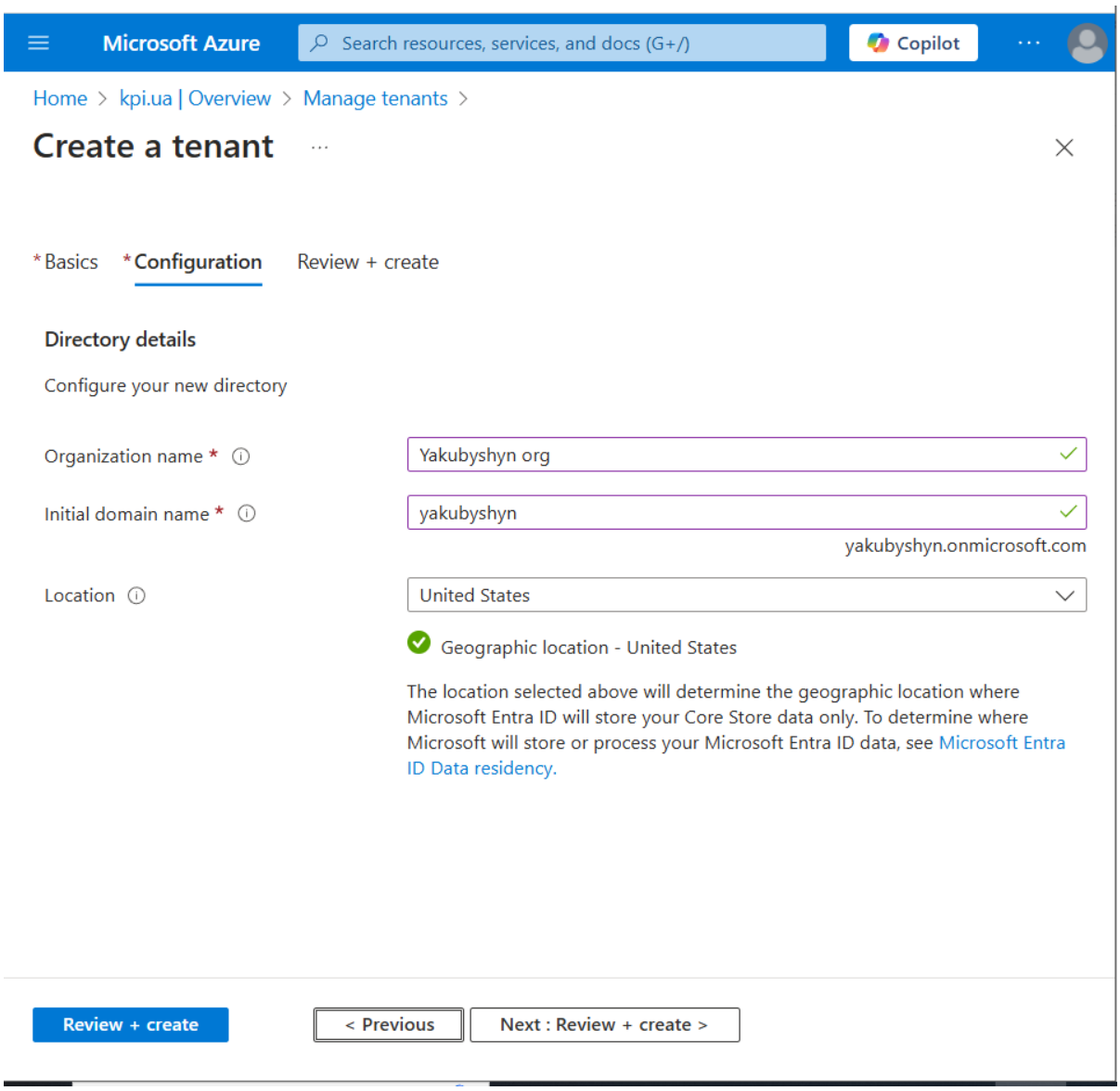
Yakubyshyn Anatolii

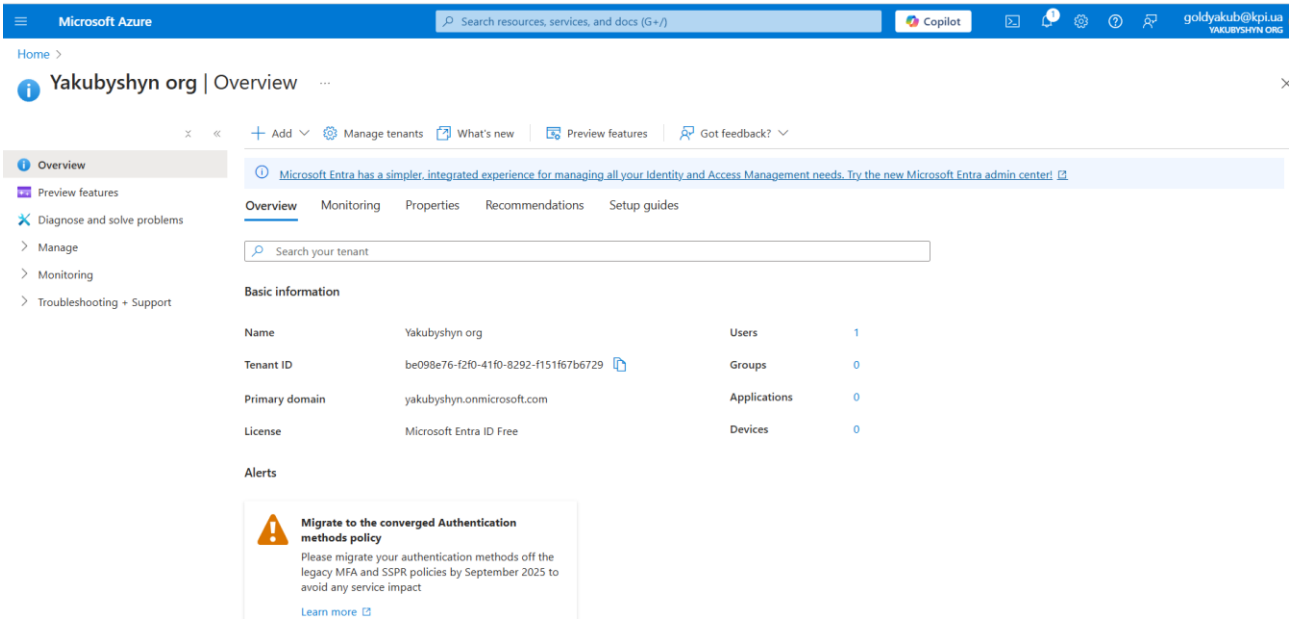
Practical Task 1*: Introduction to Microsoft Entra ID*

Create a new Microsoft Entra ID tenant.

In Manage tenants I have found create a tenant

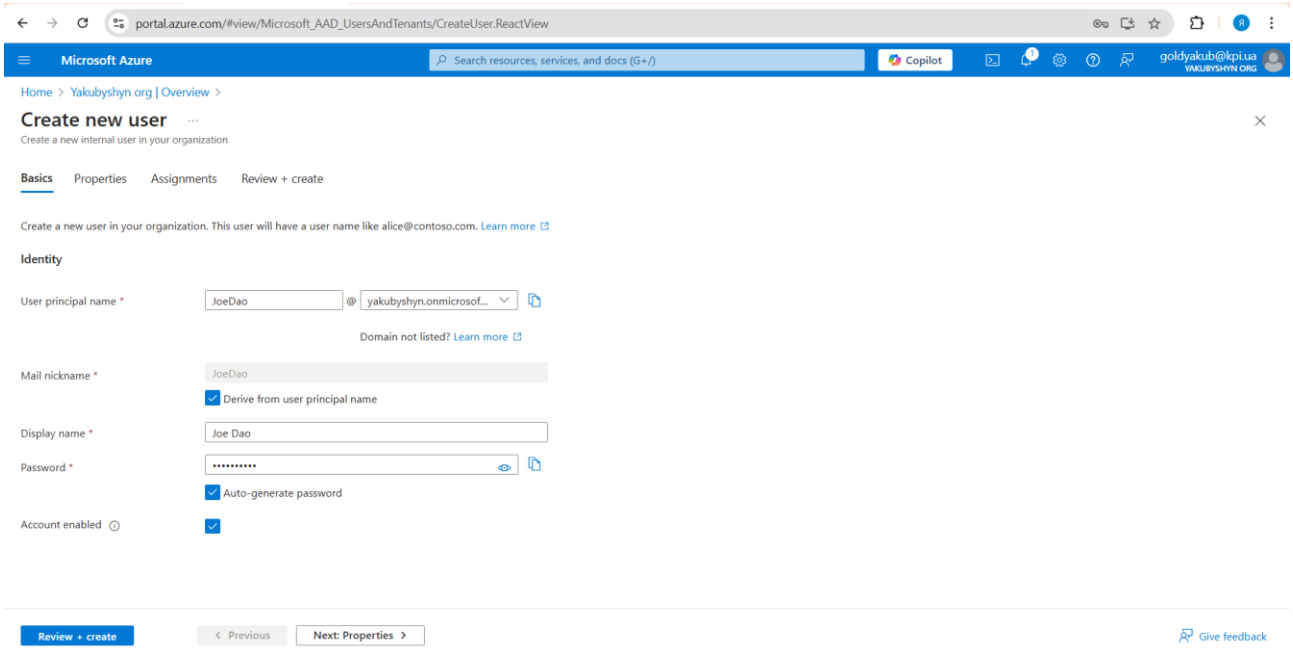


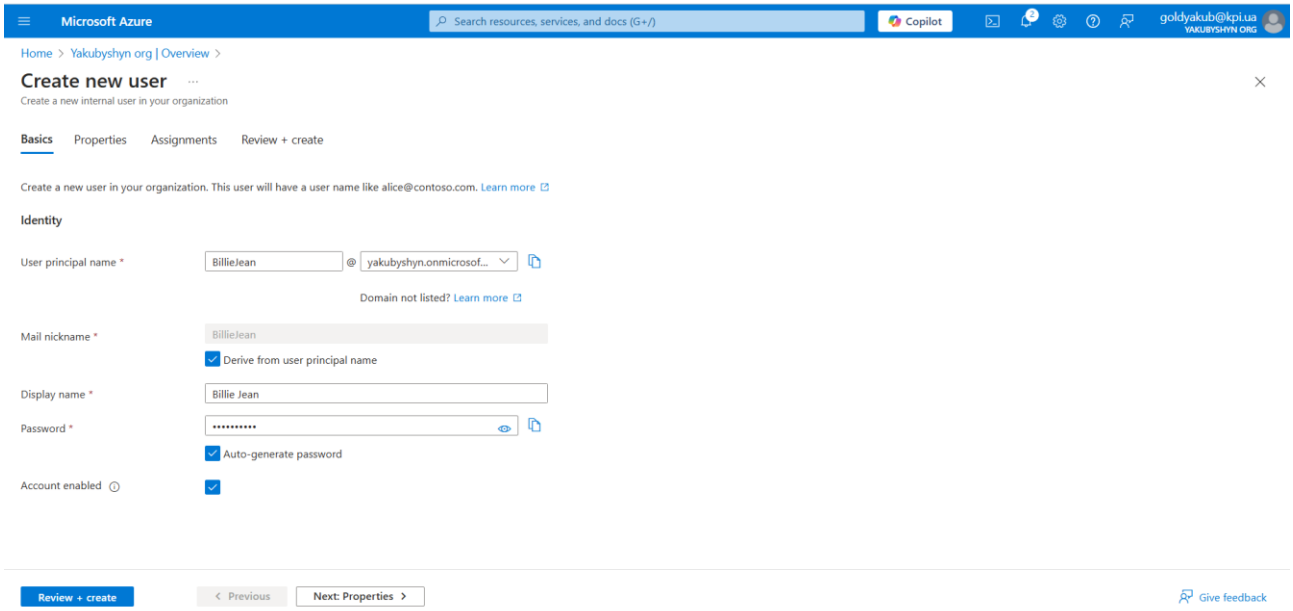




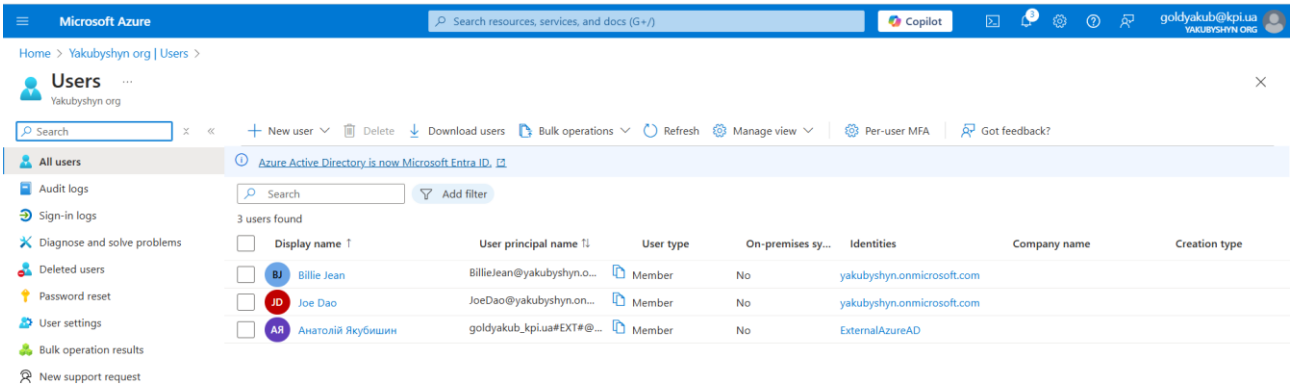
Tenant was created successfully

2. Add at least two users to the directory.



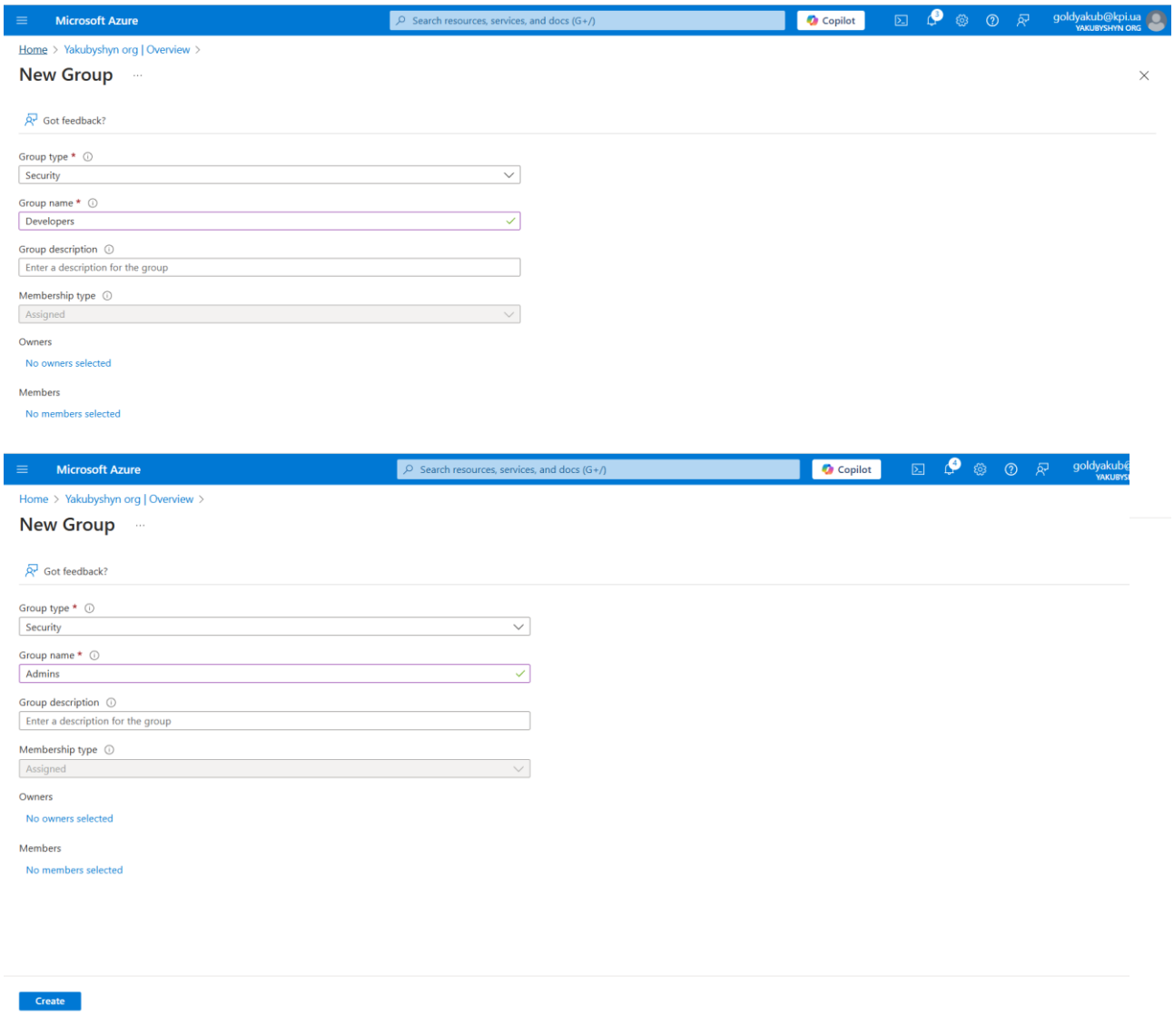


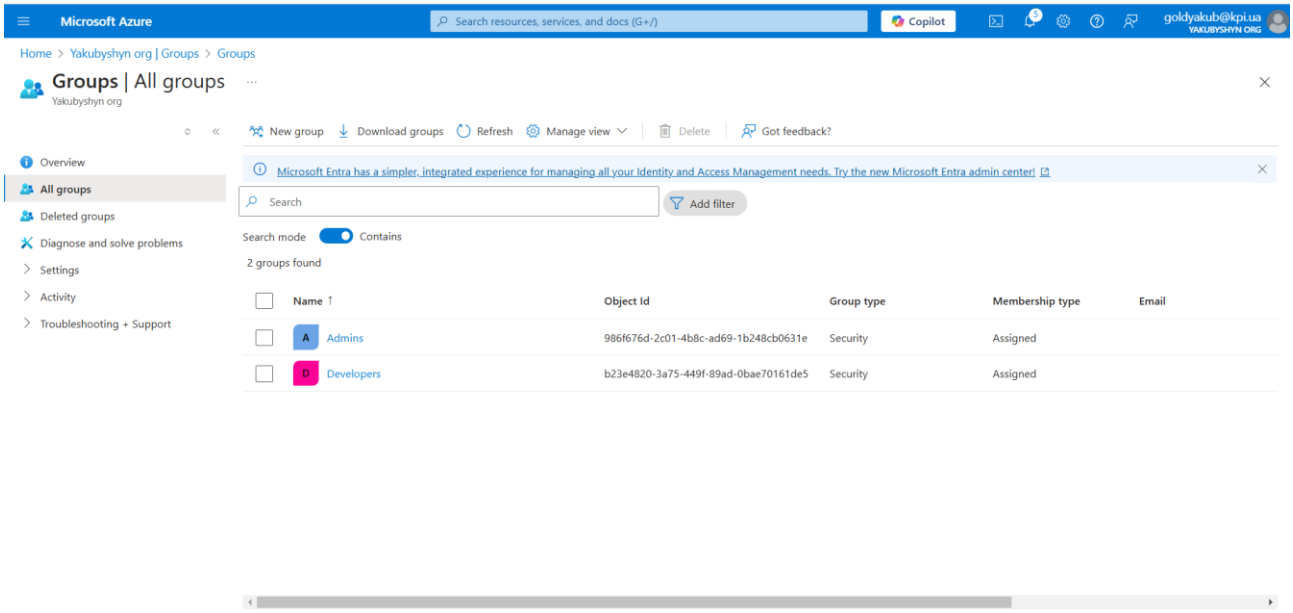
I left default options everywhere and just clicked Next



users page

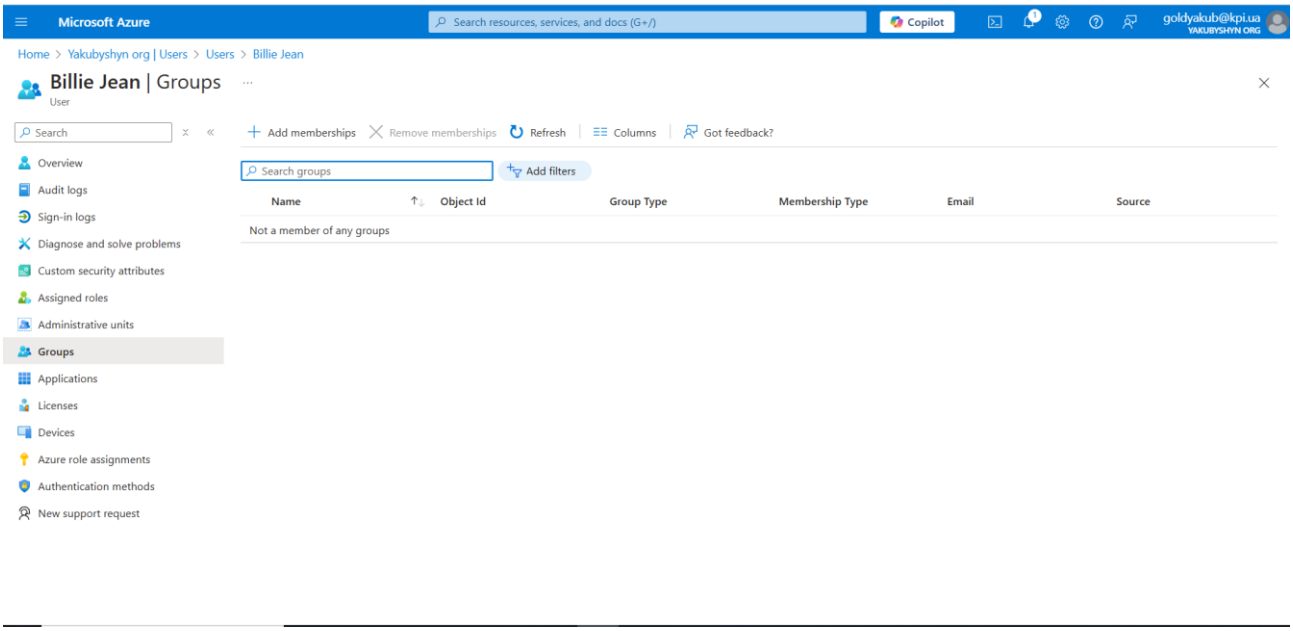
3. Create two groups named Developers and Admins.



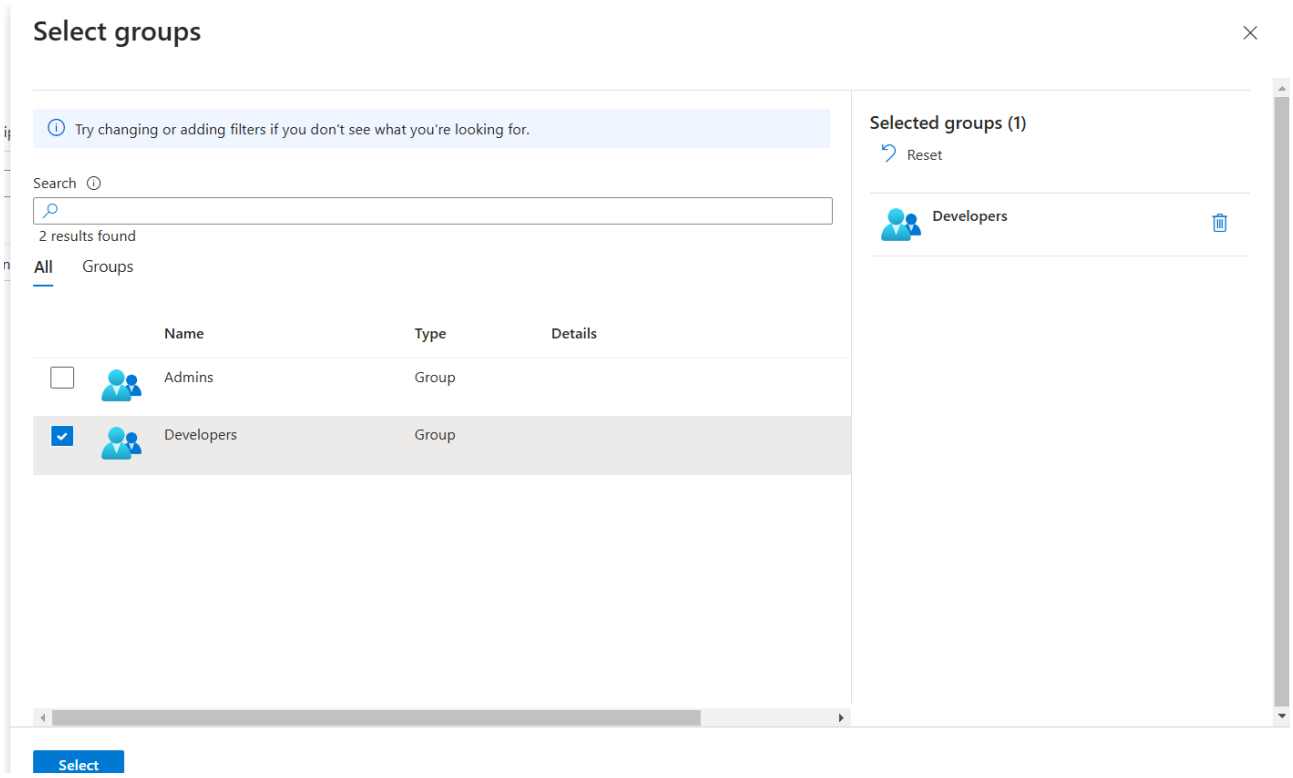


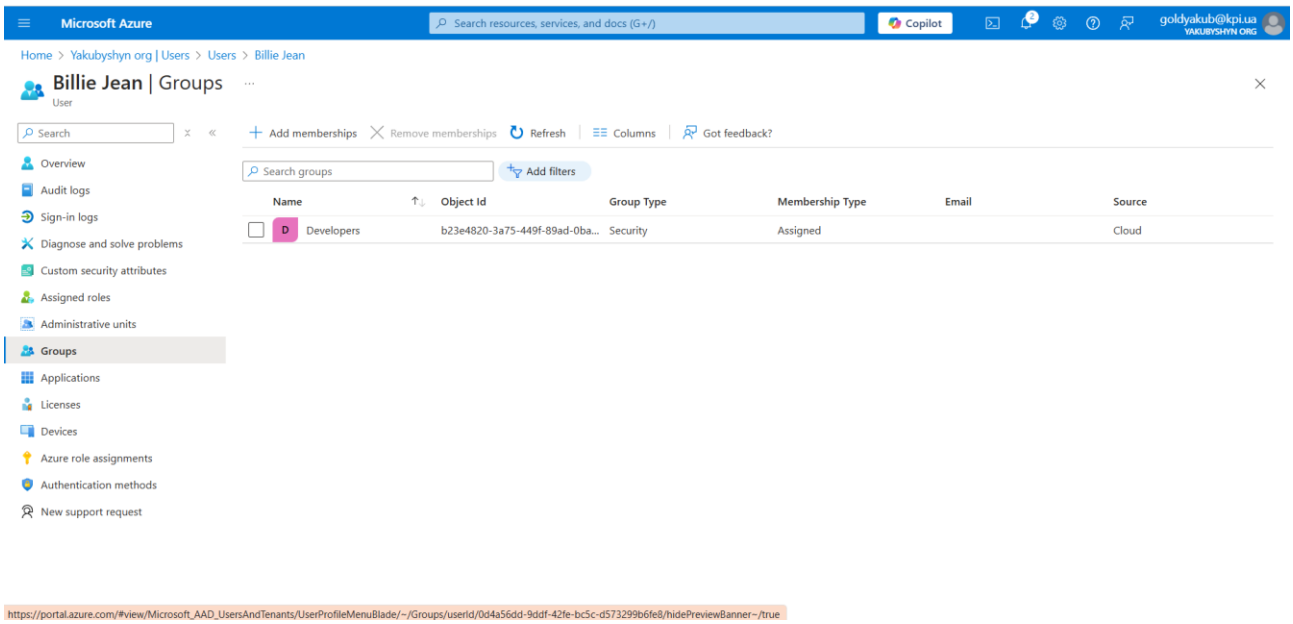
All groups page

4. Assign the users to appropriate groups.

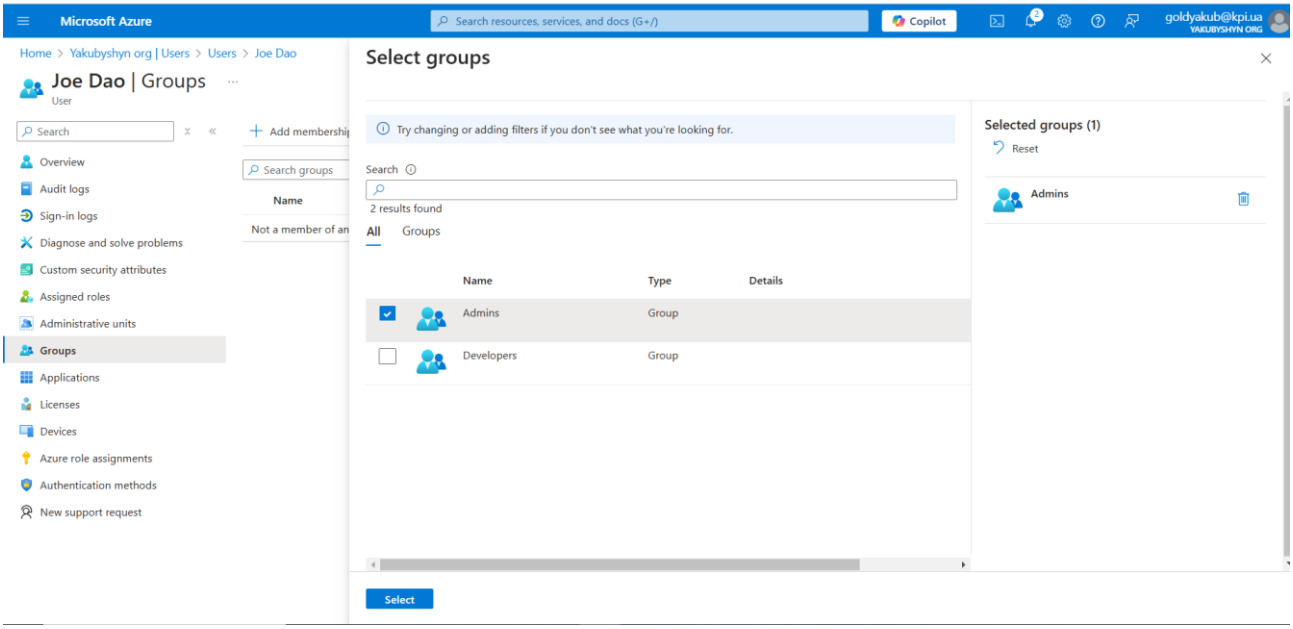


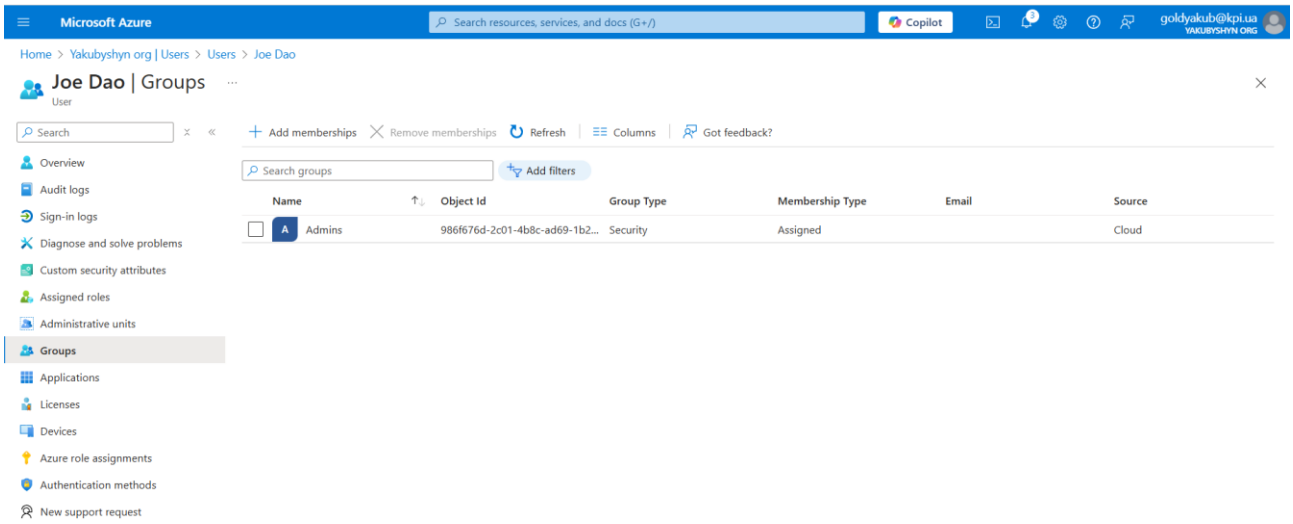
Clicking add memberships





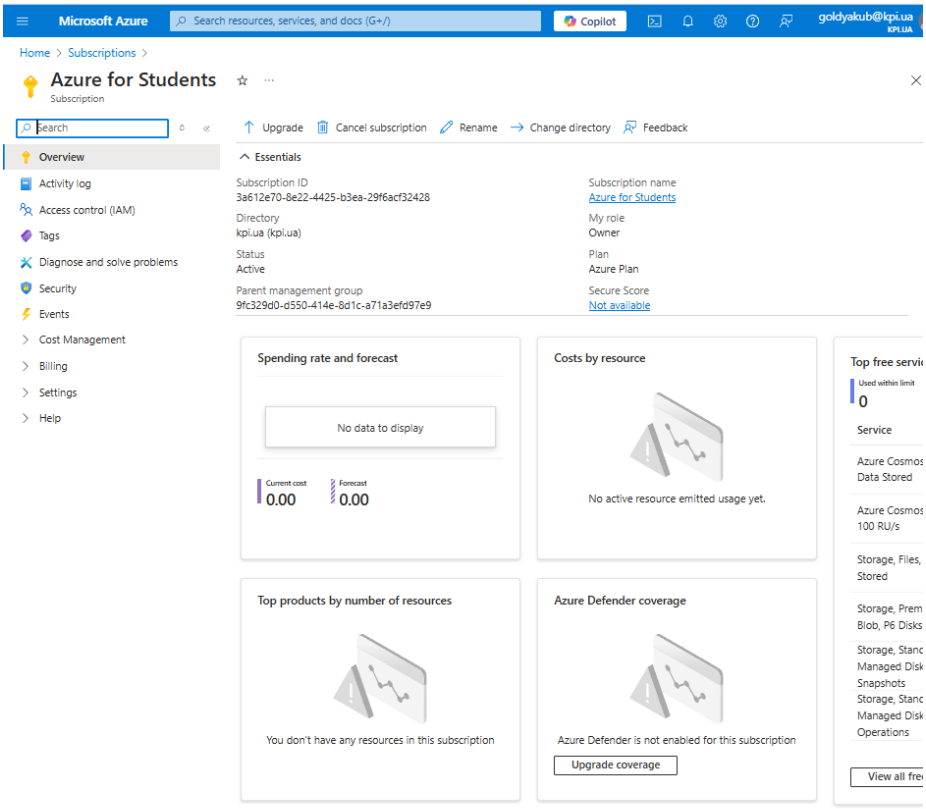
https://portal.azure.com/#view/Microsoft_AAD_UsersAndTenants/UserProfileMenuBlade/~/Groups/userId/0d4a56dd-9ddf-42fe-bc5c-d573299b6fe8/hidePreviewBanner~/true



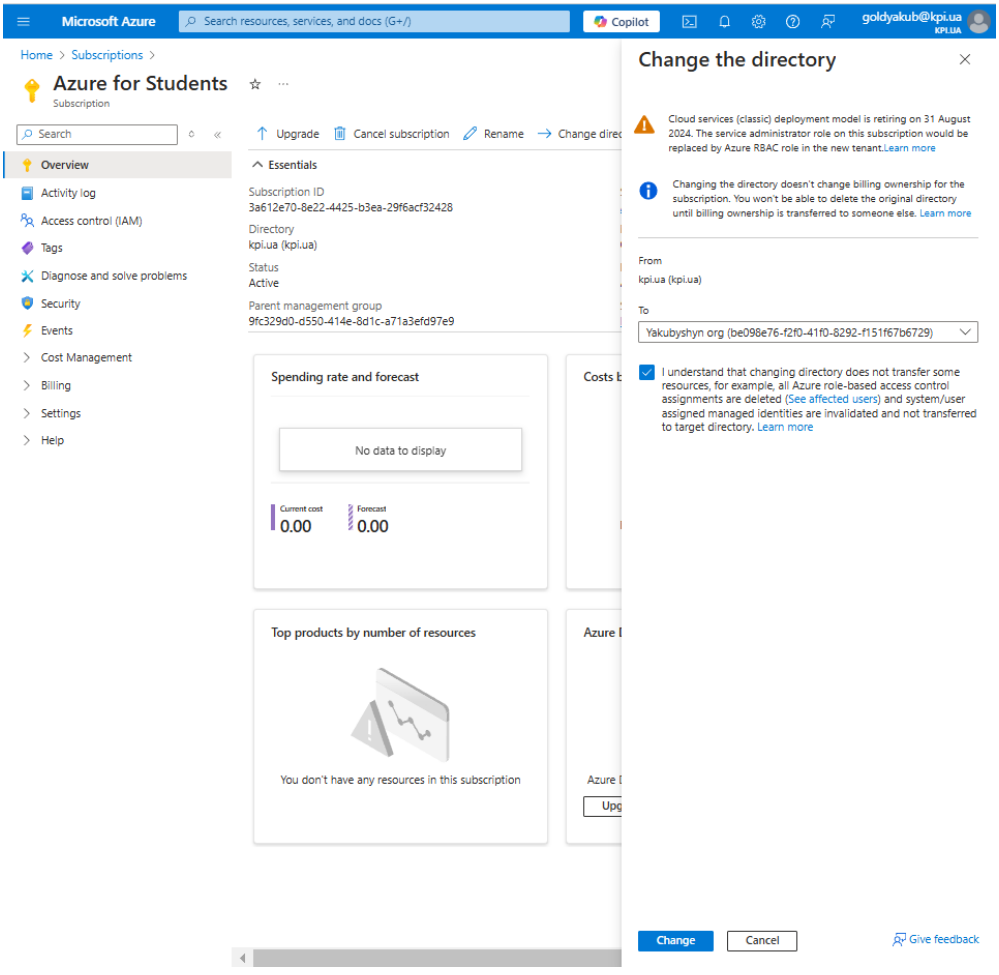


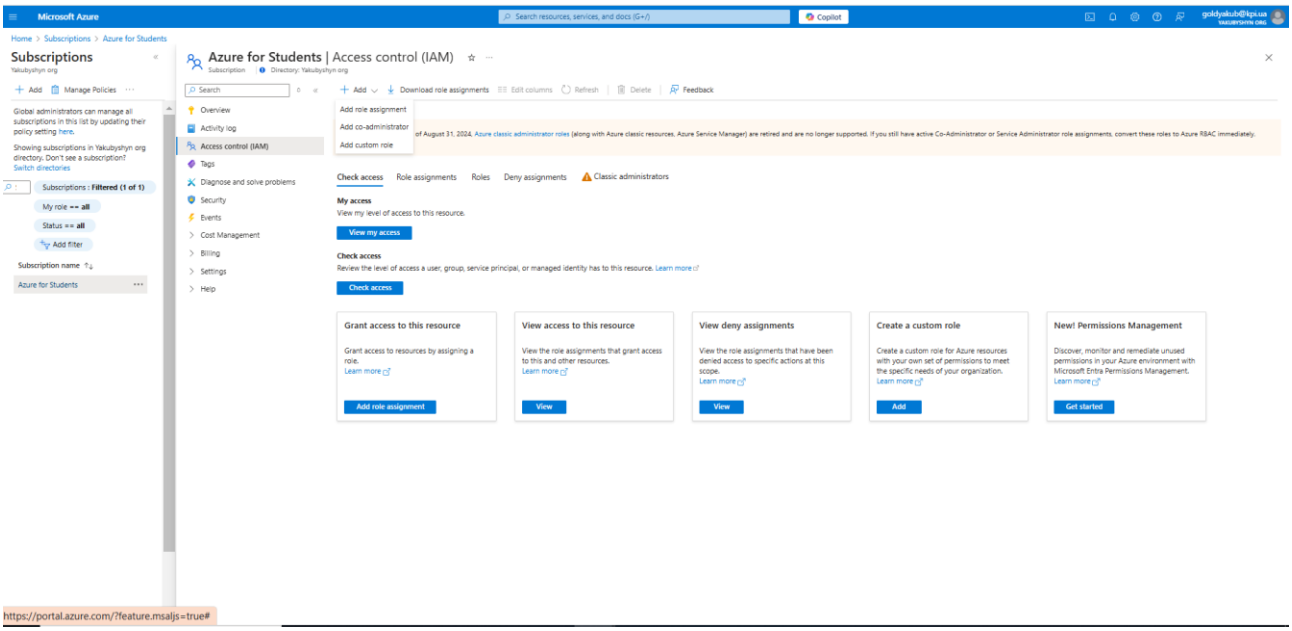
5. Assign the Global Reader role to the Admins group.

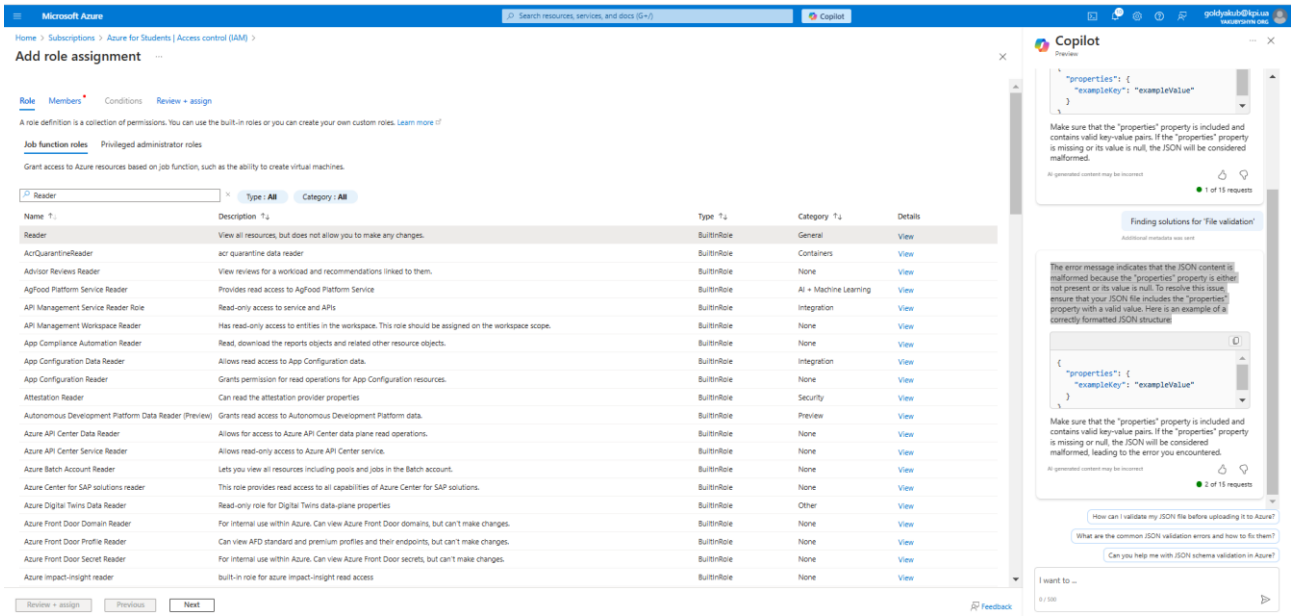
Firstly, I need to transfer subscription to a new tenant.

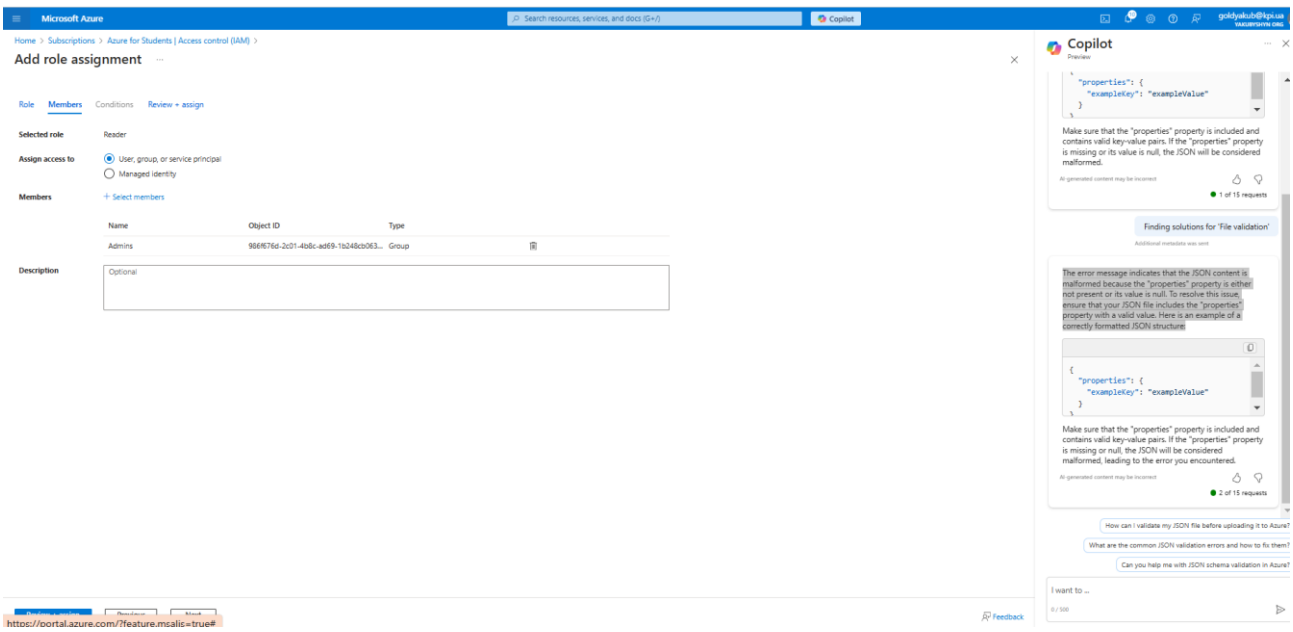


Click change directory

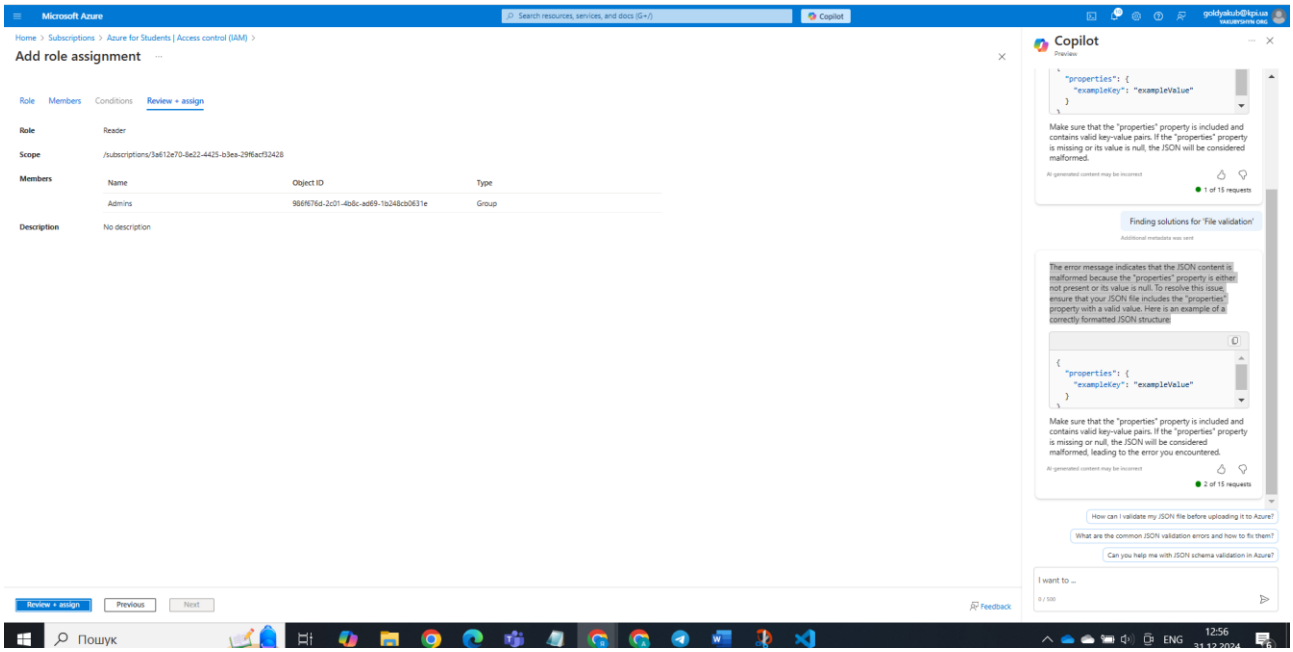


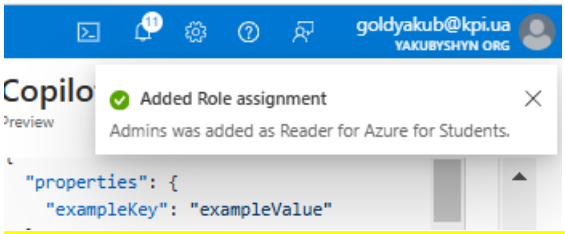

Microsoft Azure
Subscriptions
Azure for Students | Access control (IAM)
Add role assignment
Add co-administrator
Add custom role
Check access
Role assignments
Roles
Deny assignments
Classic administrators
Grant access to this resource
View access to this resource
View deny assignments
Create a custom role
New! Permissions Management
https://portal.azure.com/?feature.msaljs=true#


Microsoft Azure
Add role assignment
Role
Members
Conditions
Review + assign
Job function roles
Privileged administrator roles
Copilot
Finding solutions for 'File validation'
I want to ...

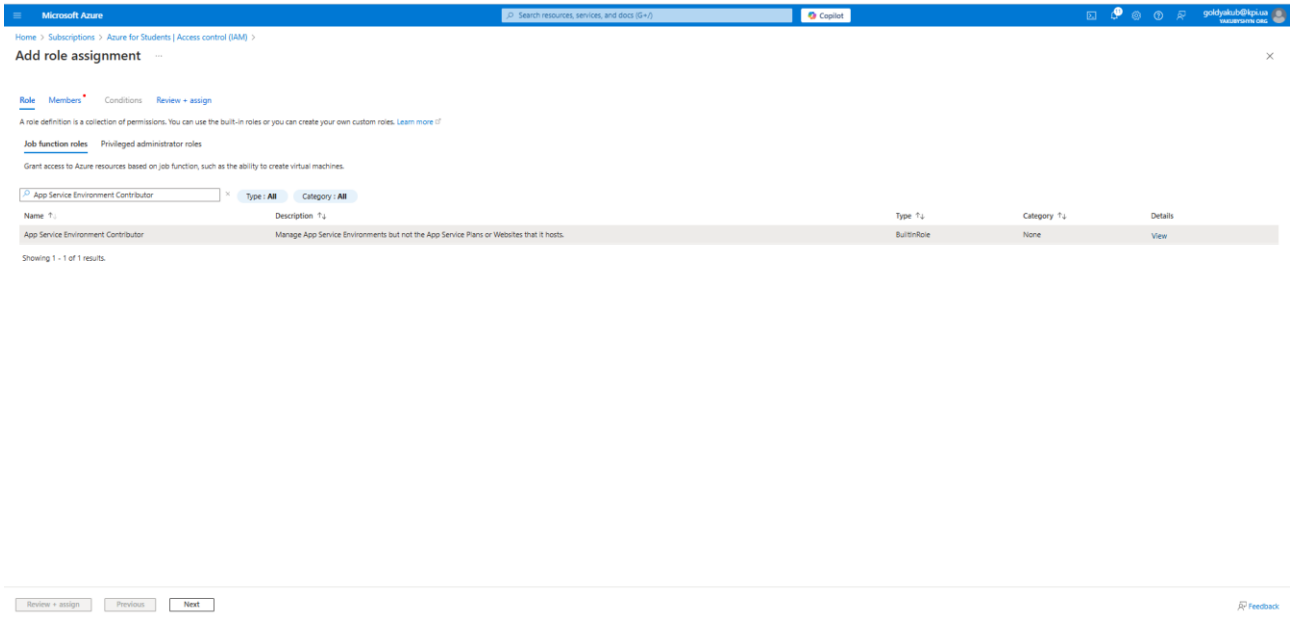

Microsoft Azure
Add role assignment
Role
Members
Conditions
Review + assign
Selected role
Reader
Assign access to
Members
Description
Copilot
Finding solutions for 'File validation'
I want to ...
https://portal.azure.com/?feature.msaljs=true#

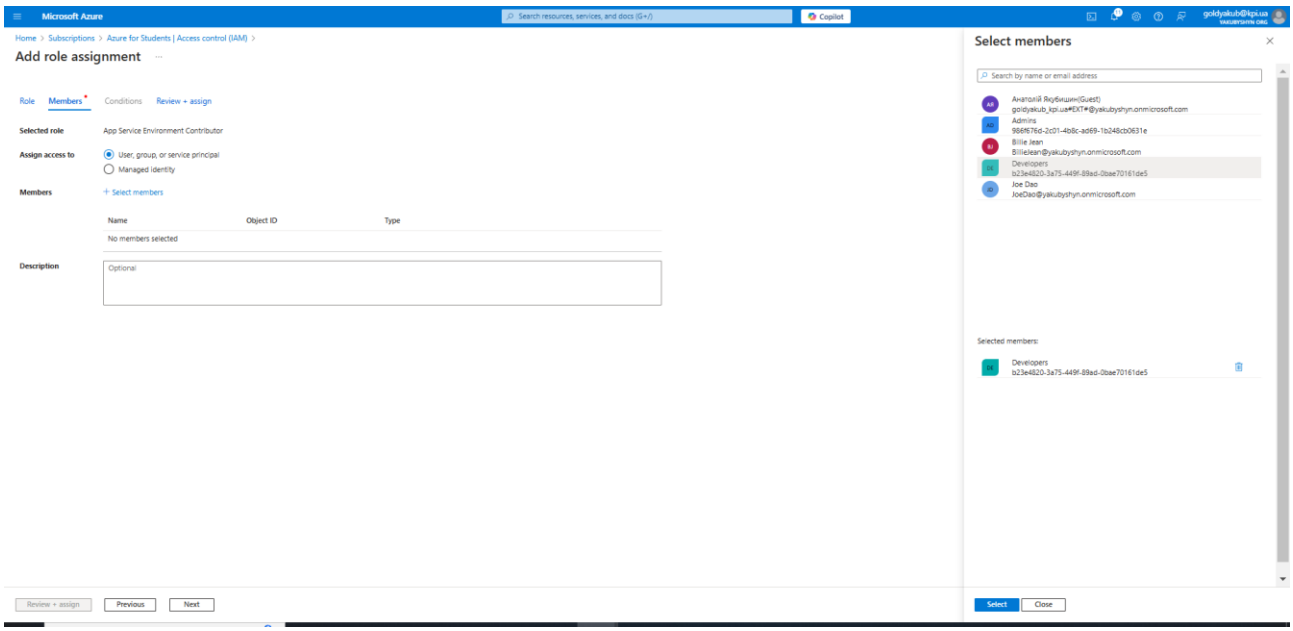
After that I clicked review and assign

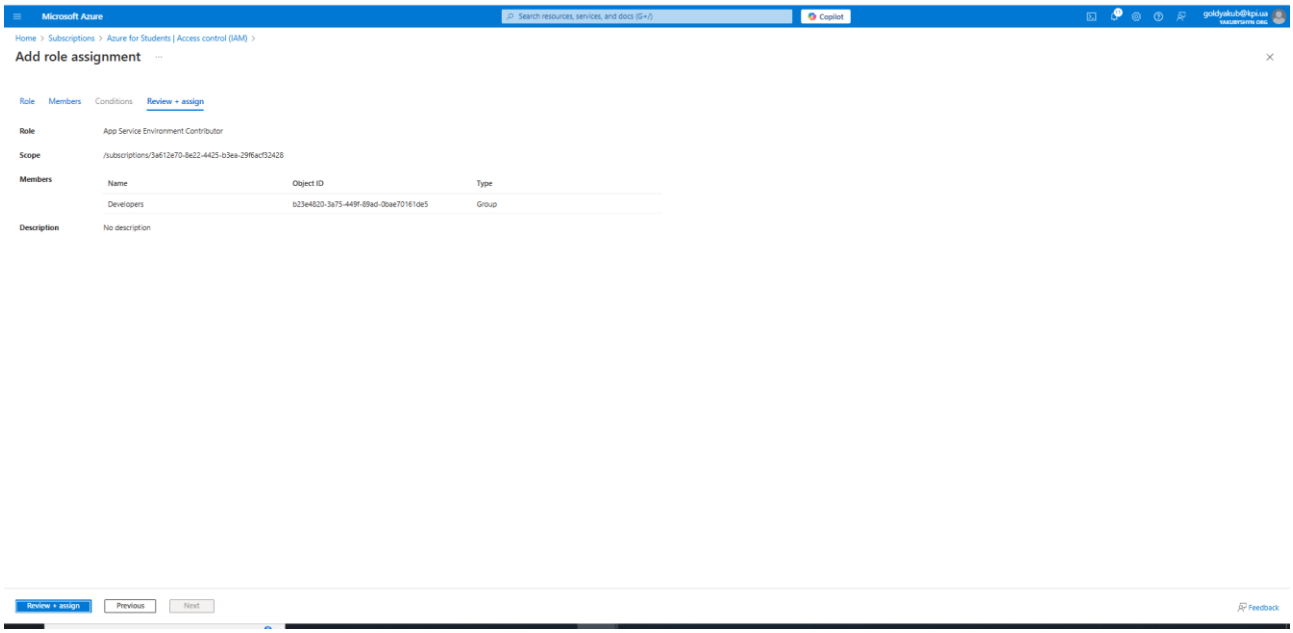


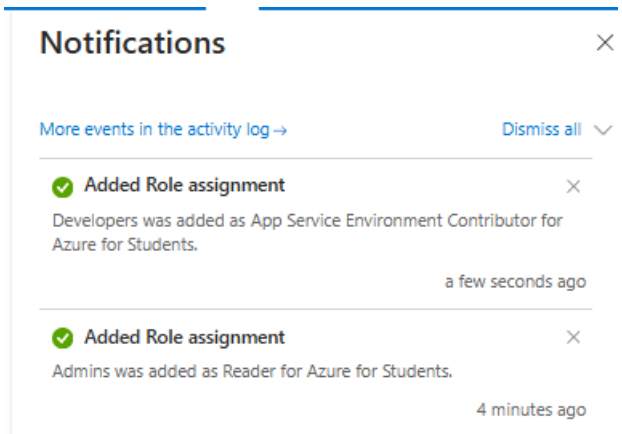


6. Assign the Application Developer role to the Developers group

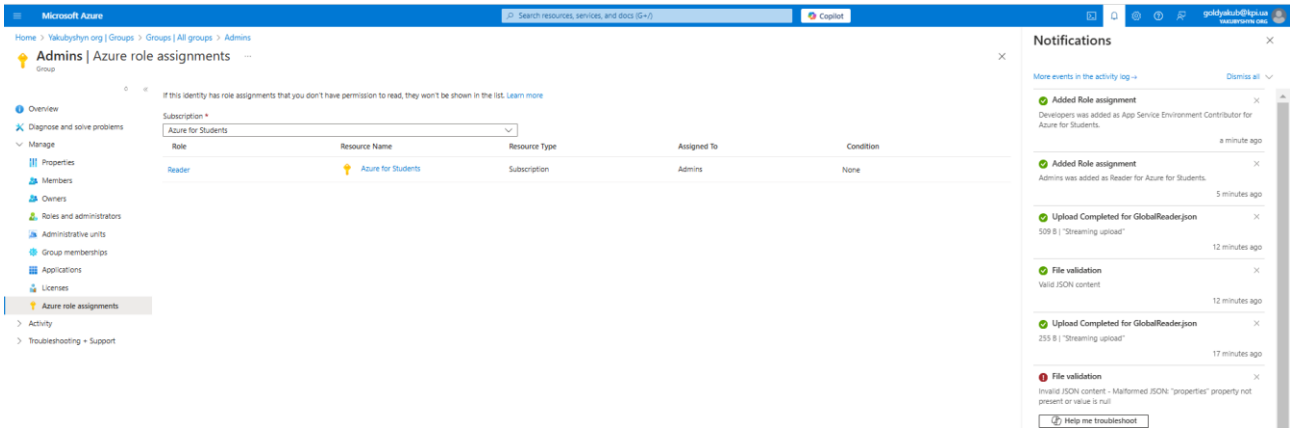


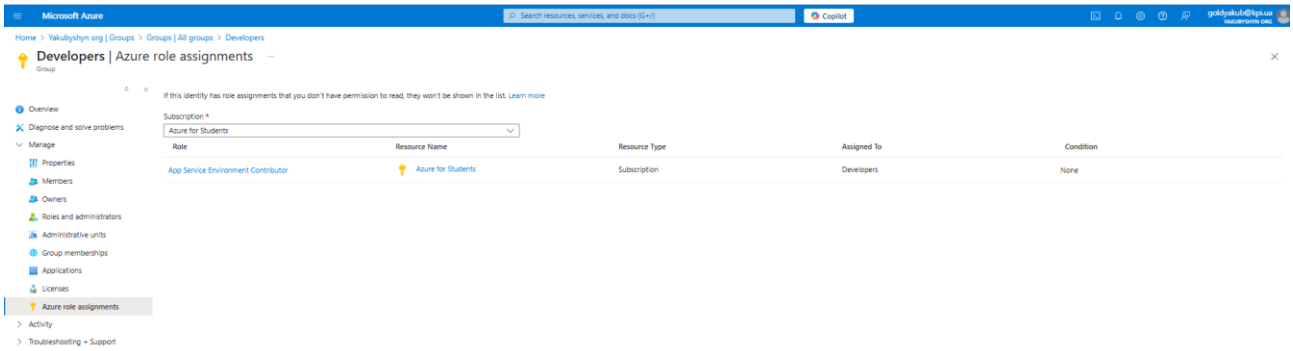

Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > Subscriptions > Azure for Students | Access control (IAM) >
Add role assignment
Role
Members
Conditions
Review + assign
Selected role
App Service Environment Contributor
Assign access to
User, group, or service principal
Managed identity
Members
+ Select members
Name
Object ID
Type
No members selected
Description
Optional
Review + assign
Previous
Next
Select members
Search by name or email address
Admins
Billie Jean
BillieJean@yakubyshyn.onmicrosoft.com
Developers
b23e4820-3a75-449f-89ad-0bae70161de5
Joe Dao
JoeDao@yakubyshyn.onmicrosoft.com
Selected members:
Developers
b23e4820-3a75-449f-89ad-0bae70161de5
Select
Close


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > Subscriptions > Azure for Students | Access control (IAM) >
Add role assignment
Role
Members
Conditions
Review + assign
Role
App Service Environment Contributor
Scope
/subscriptions/3a612e70-8e22-4425-b3ea-29f6acf32428
Members
Name
Object ID
Type
Developers
b23e4820-3a75-449f-89ad-0bae70161de5
Group
Description
No description
Review + assign
Previous
Next
Feedback


Notifications
More events in the activity log →
Dismiss all
Added Role assignment
Developers was added as App Service Environment Contributor for Azure for Students.
a few seconds ago
Added Role assignment
Admins was added as Reader for Azure for Students.
4 minutes ago

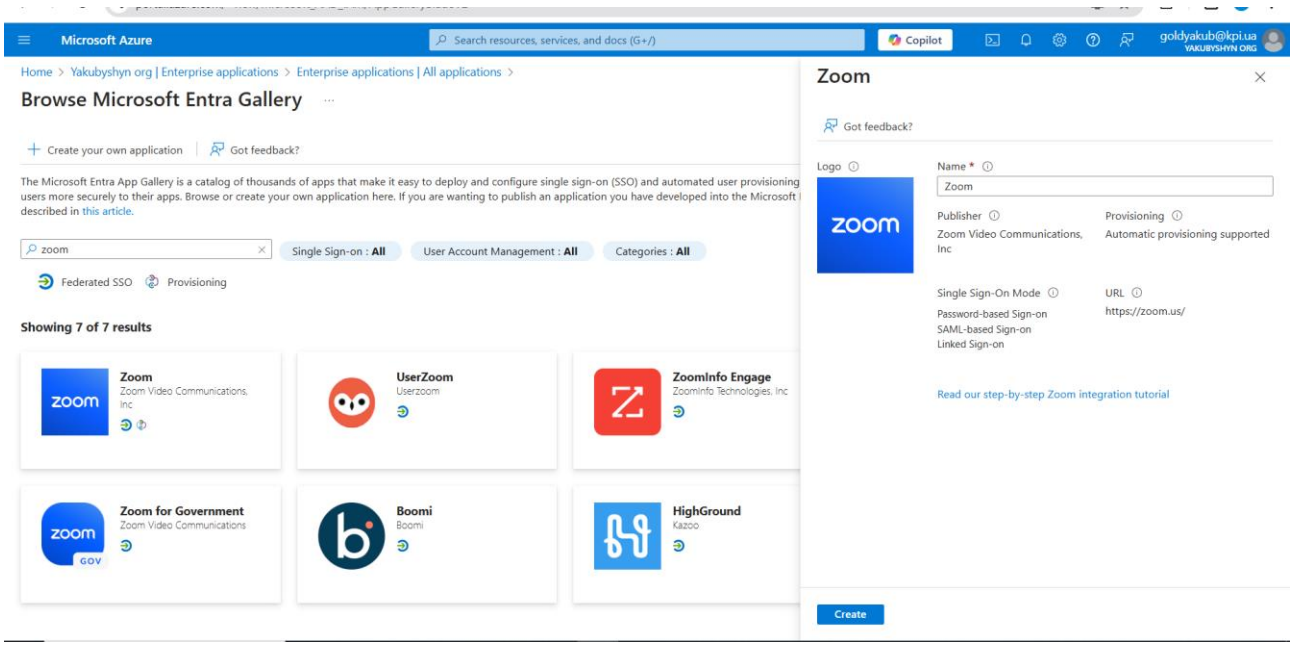
7. Verify that the role assignments function as expected for both groups.



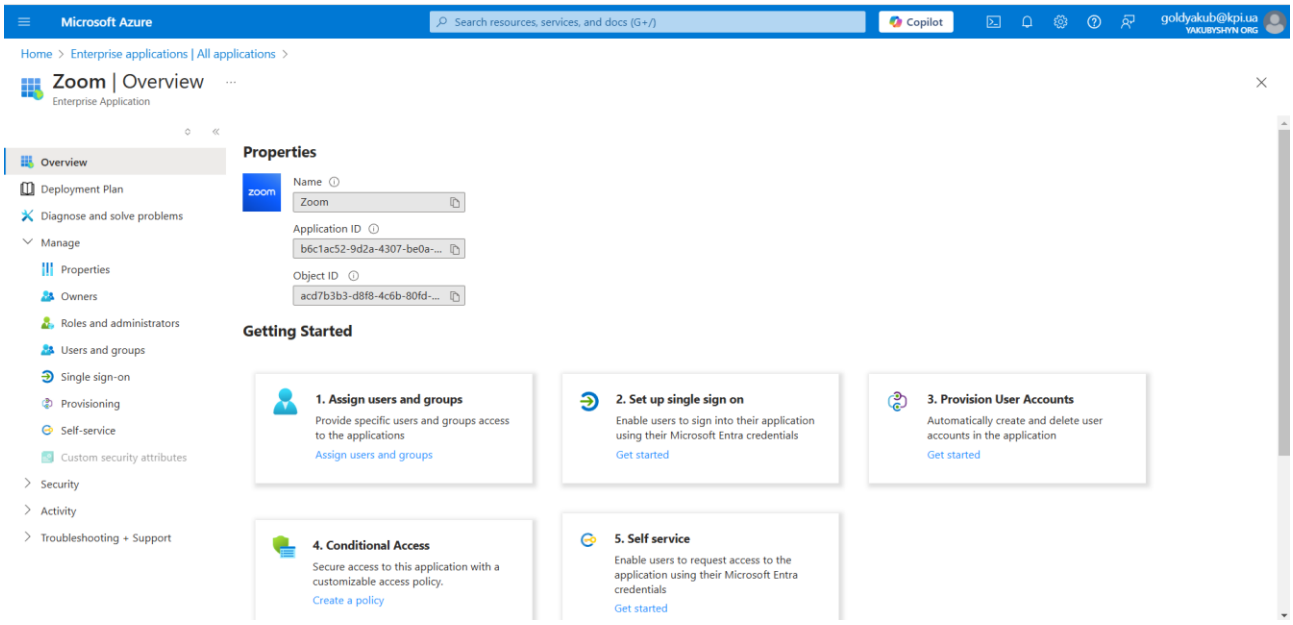


Practical Task 2: *Enabling Single Sign-On (SSO) and Multi-Factor Authentication (MFA)*

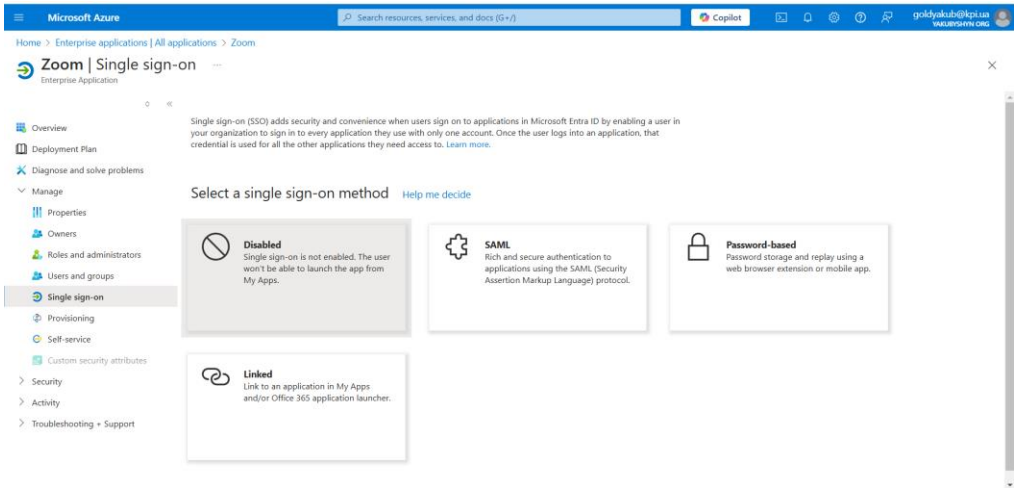
1. Enable Single Sign-On (SSO) for your Microsoft Entra ID tenant



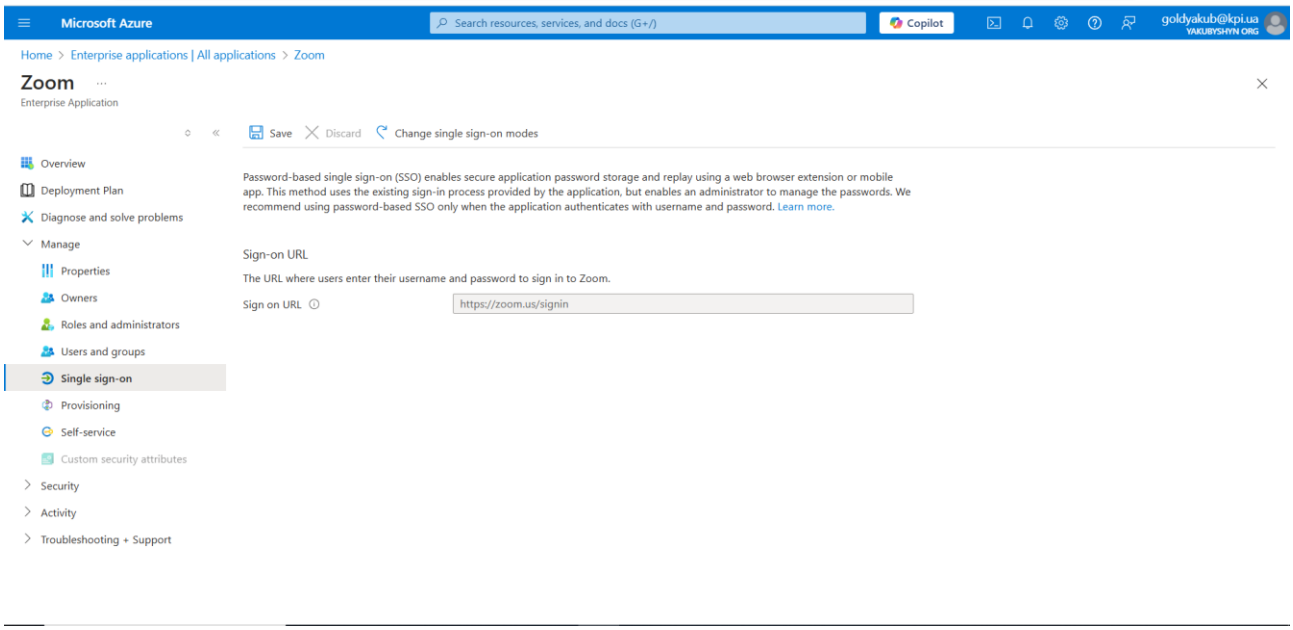
Create zoom app

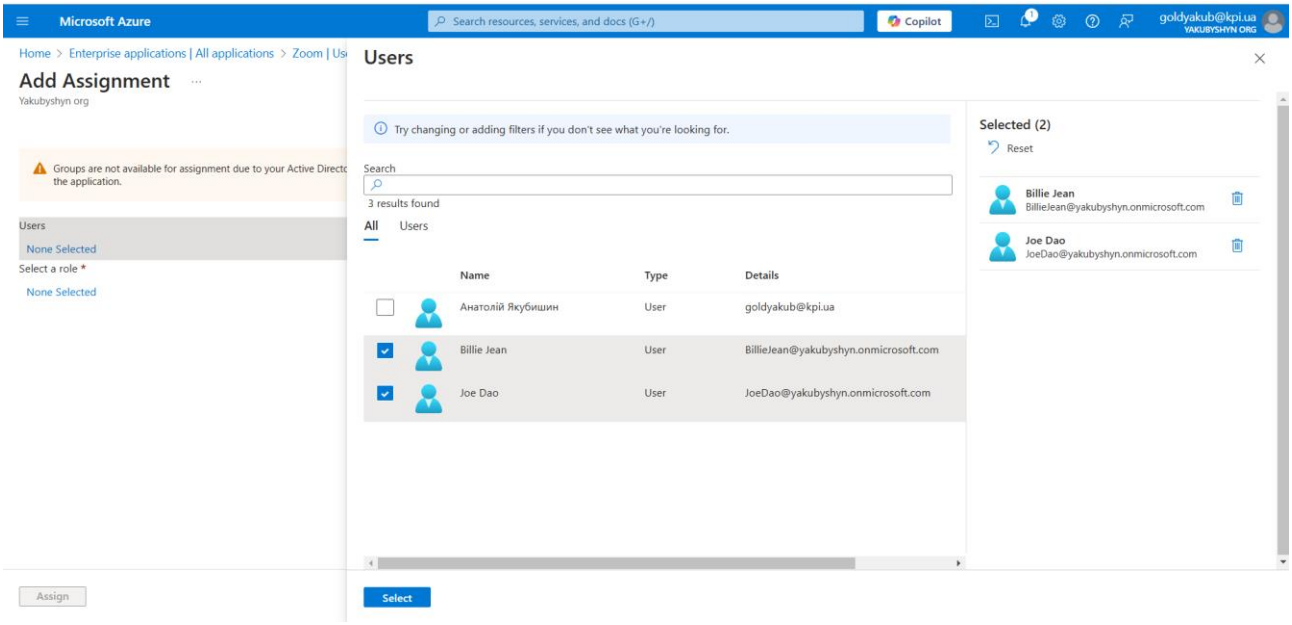


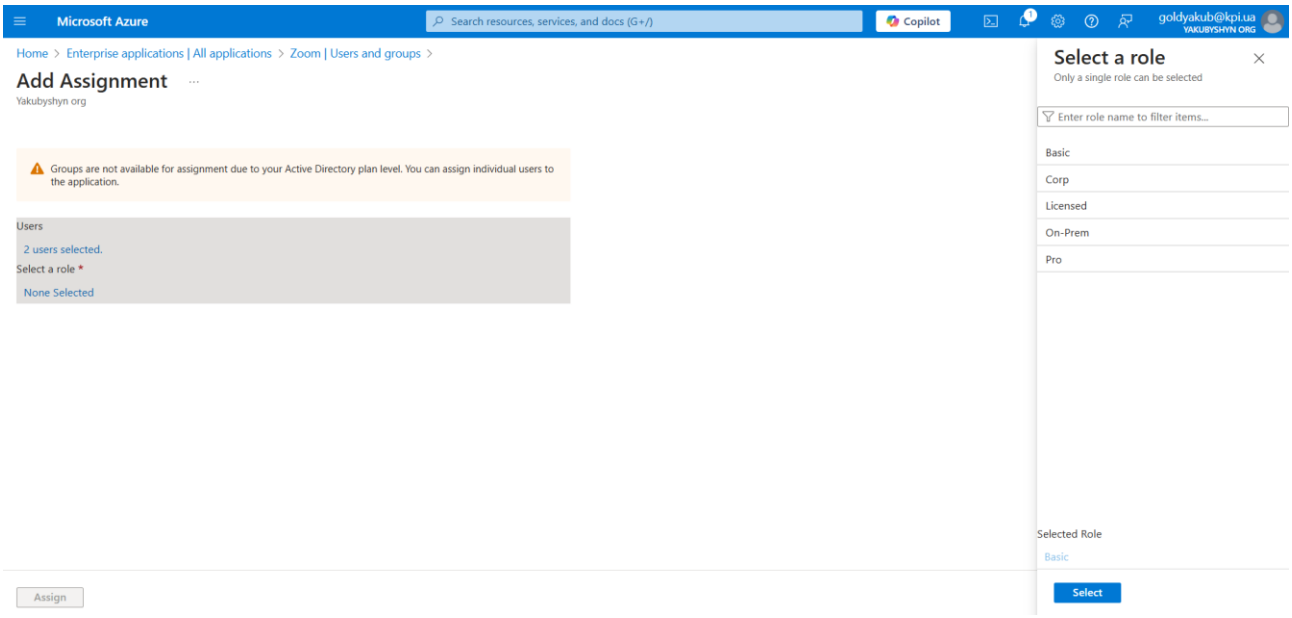
Setup single sign on

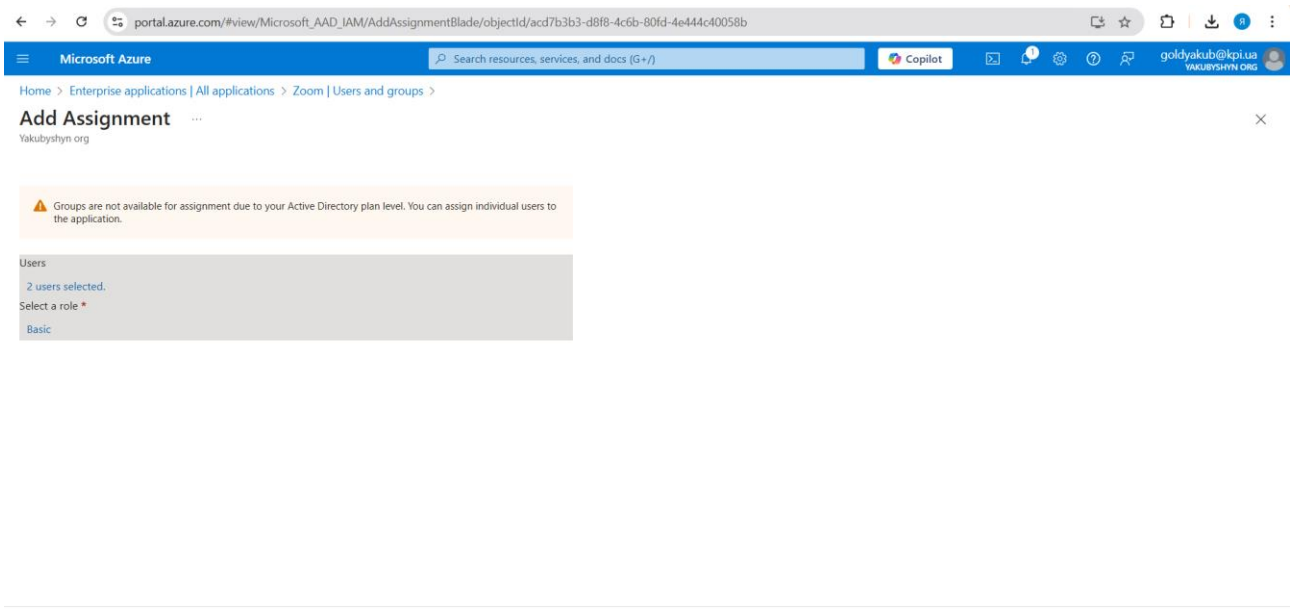


Password-based



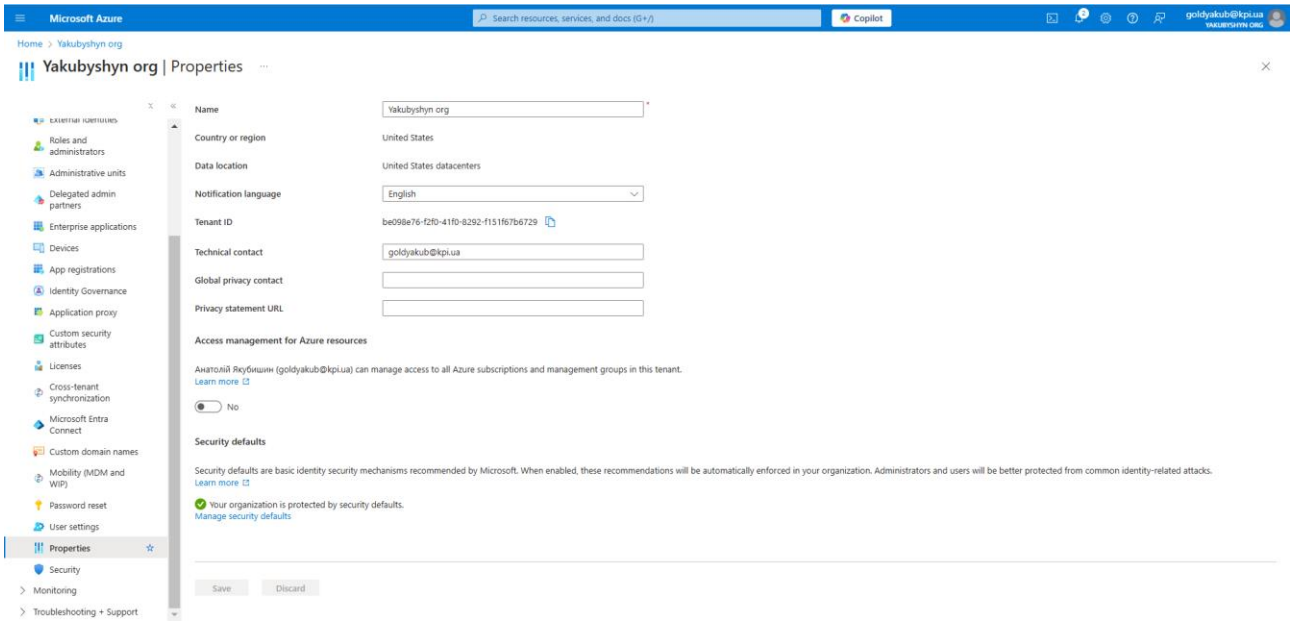

Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
goldyakub@kpi.ua
YAKUBYSHYN ORG
Home > Enterprise applications | All applications > Zoom | Us
Add Assignment
Yakubyshyn org
Groups are not available for assignment due to your Active Directo
the application.
Users
None Selected
Select a role *
None Selected
Assign
Users
Try changing or adding filters if you don't see what you're looking for.
Search
3 results found
All
Users
Name
Type
Details
Анатолій Якубишин
User
goldyakub@kpi.ua
Billie Jean
User
BillieJean@yakubyshyn.onmicrosoft.com
Joe Dao
User
JoeDao@yakubyshyn.onmicrosoft.com
Selected (2)
Reset
Billie Jean
BillieJean@yakubyshyn.onmicrosoft.com
Joe Dao
JoeDao@yakubyshyn.onmicrosoft.com
Select

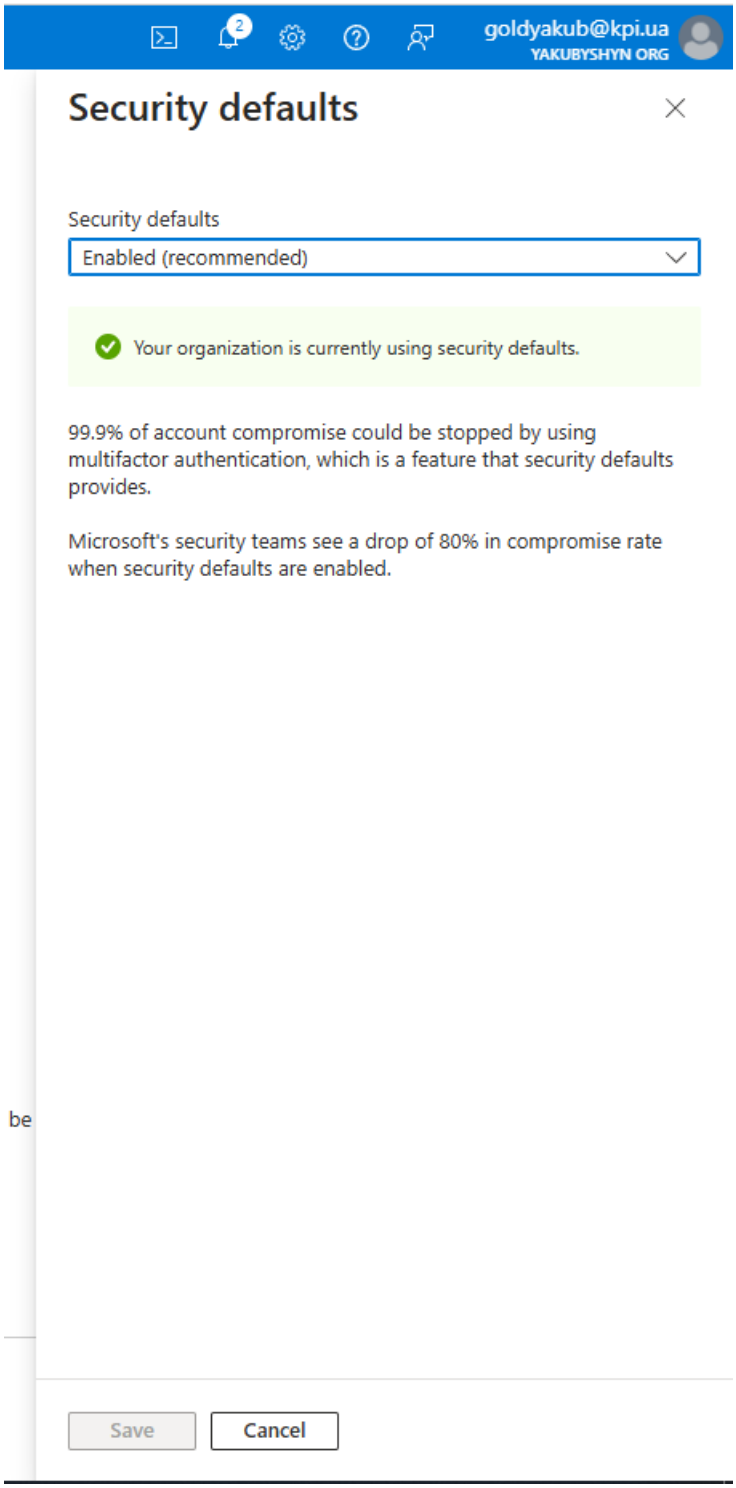

Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
goldyakub@kpi.ua
YAKUBYSHYN ORG
Home > Enterprise applications | All applications > Zoom | Users and groups >
Add Assignment
Yakubyshyn org
Groups are not available for assignment due to your Active Directory plan level. You can assign individual users to the application.
Users
2 users selected.
Select a role *
None Selected
Assign
Select a role
Only a single role can be selected
Enter role name to filter items...
Basic
Corp
Licensed
On-Prem
Pro
Selected Role
Basic
Select



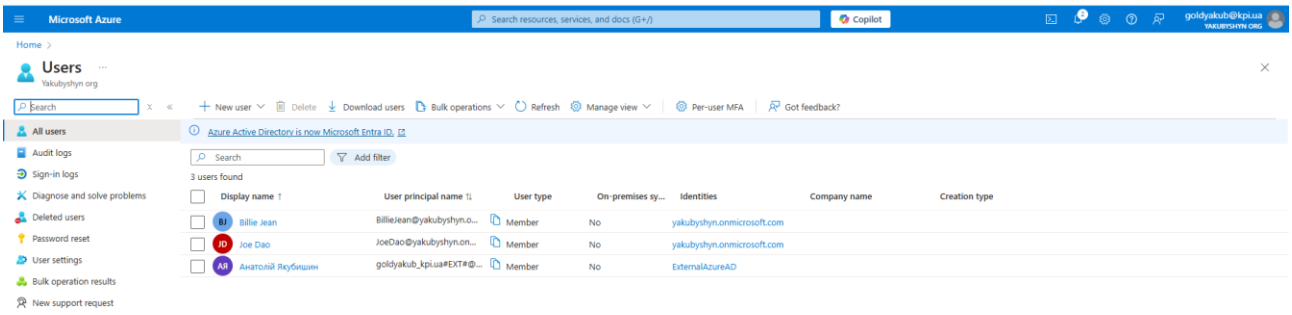
2. Enforce Multi-Factor Authentication (MFA) for all users in the directory.
3. Configure conditional access policies to require MFA for high-risk sign-ins.

Because I don't have *Microsoft Entra ID Premium*. I am doing some workaround

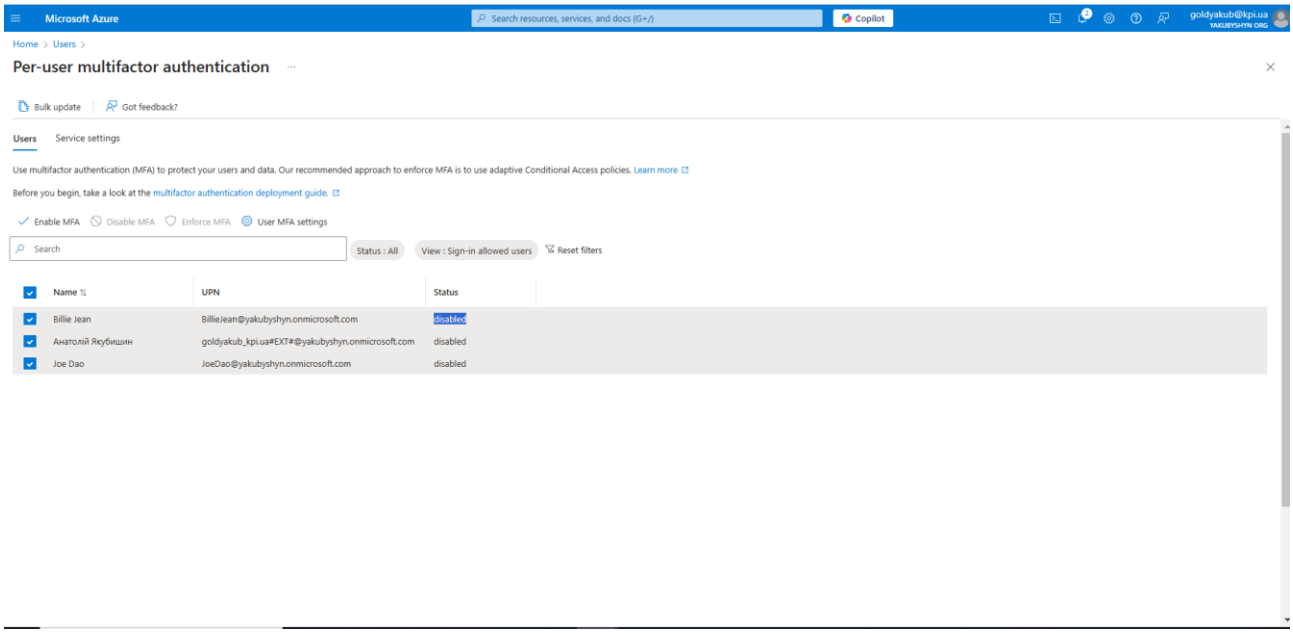




Enabled security defaults to use MFA



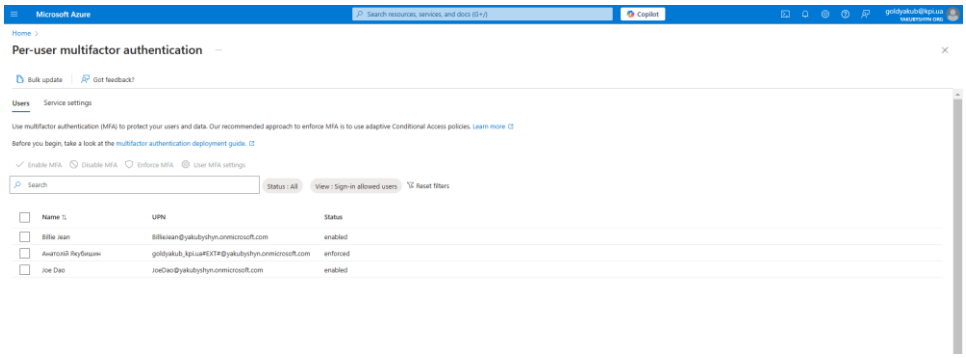
click per user MFA



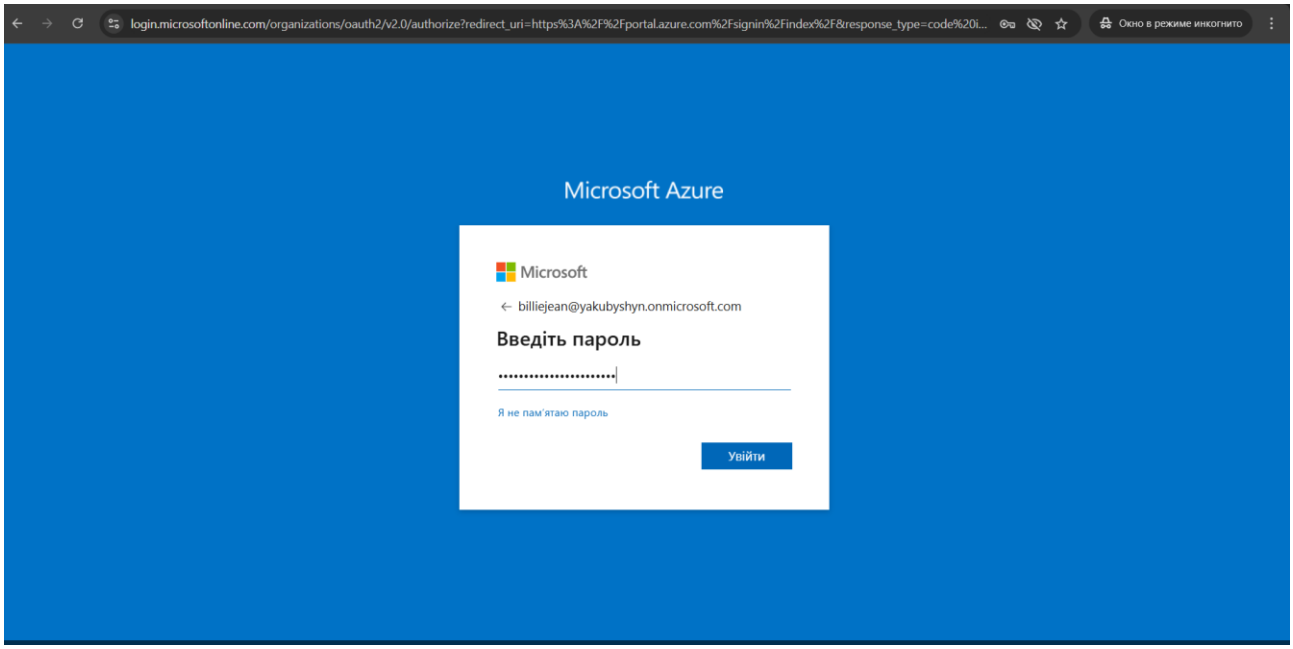
Click enable MFA

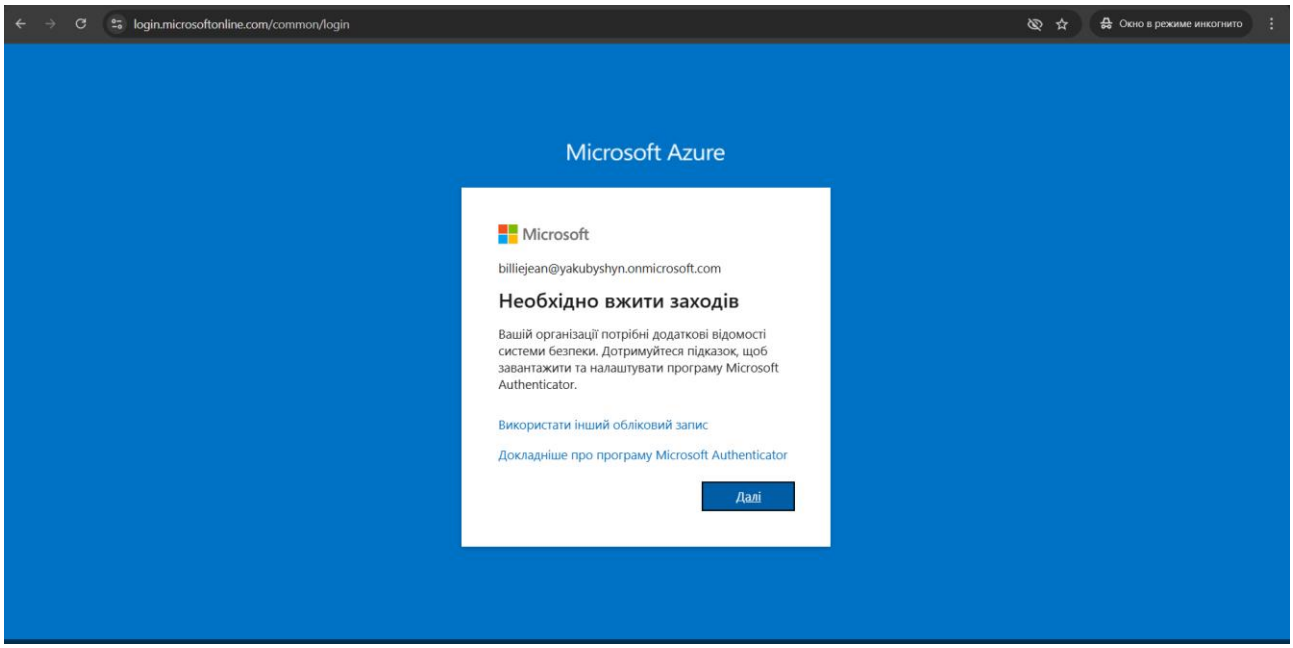
Azure after refresh forced me to add MFA to my root account.

In result I have:



4. Verify that SSO and MFA settings are correctly applied for the users.

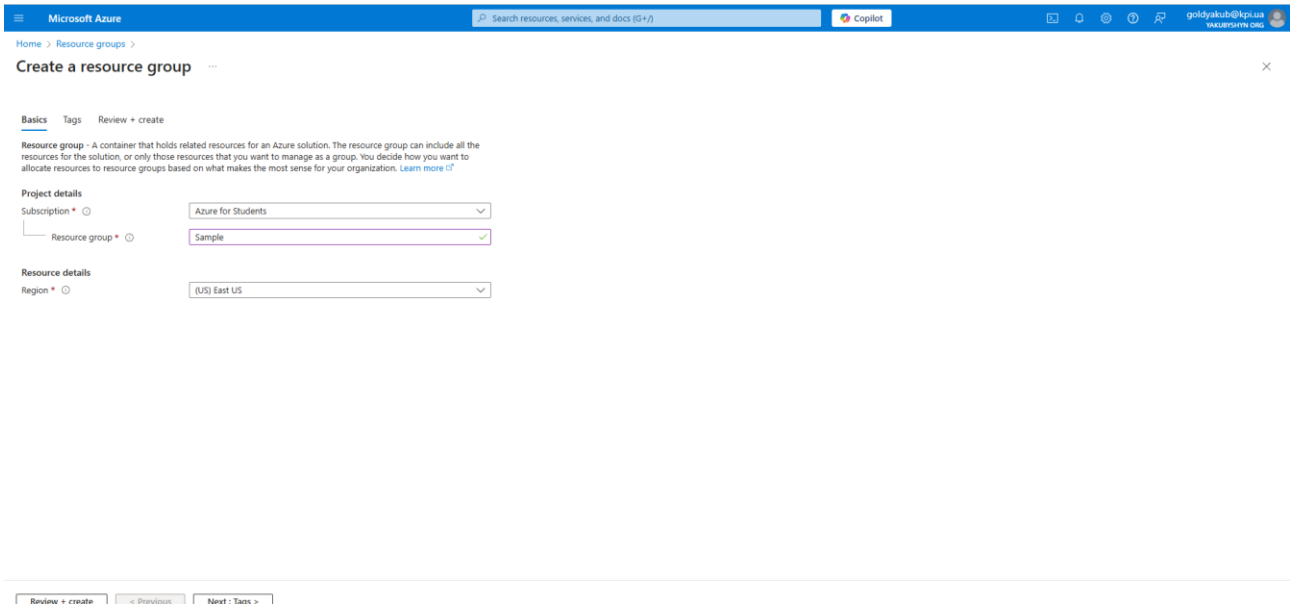




As a result, we see that MFA enforced for users (it is needed to add MS Authenticator).

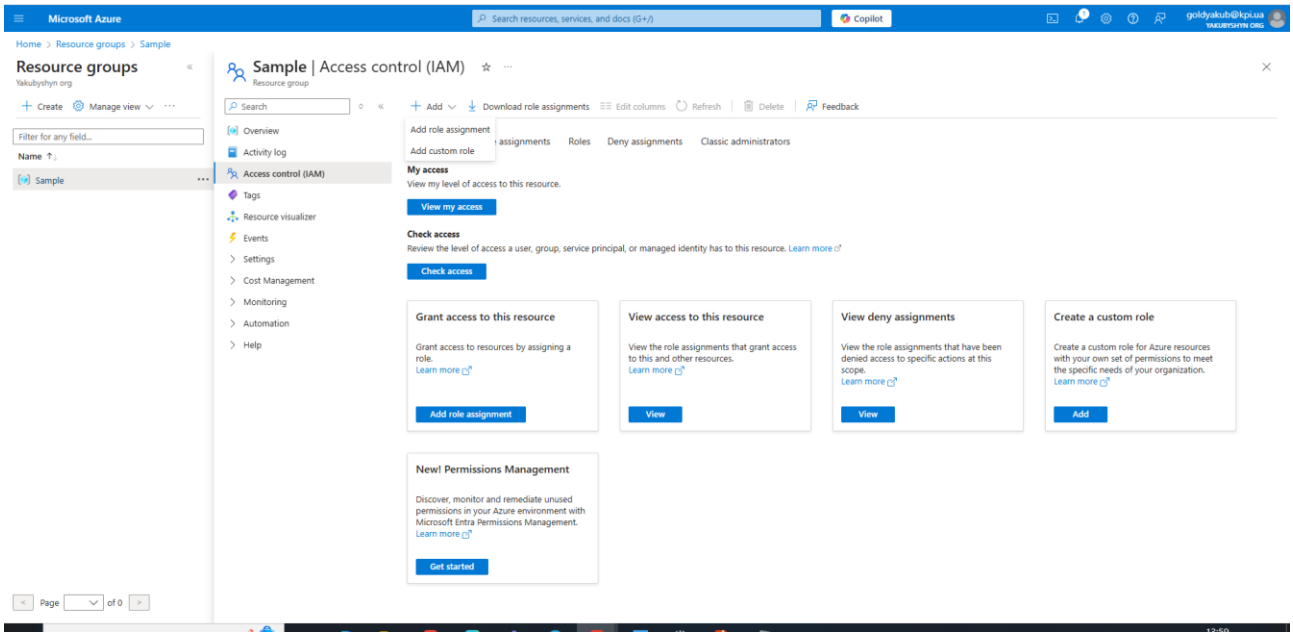
Practical Task 3: *Implementing Role-Based Access Control (RBAC)*

Implement Role-Based Access Control (RBAC) in Azure to manage access to resources based on roles and ensure fine-grained access management.

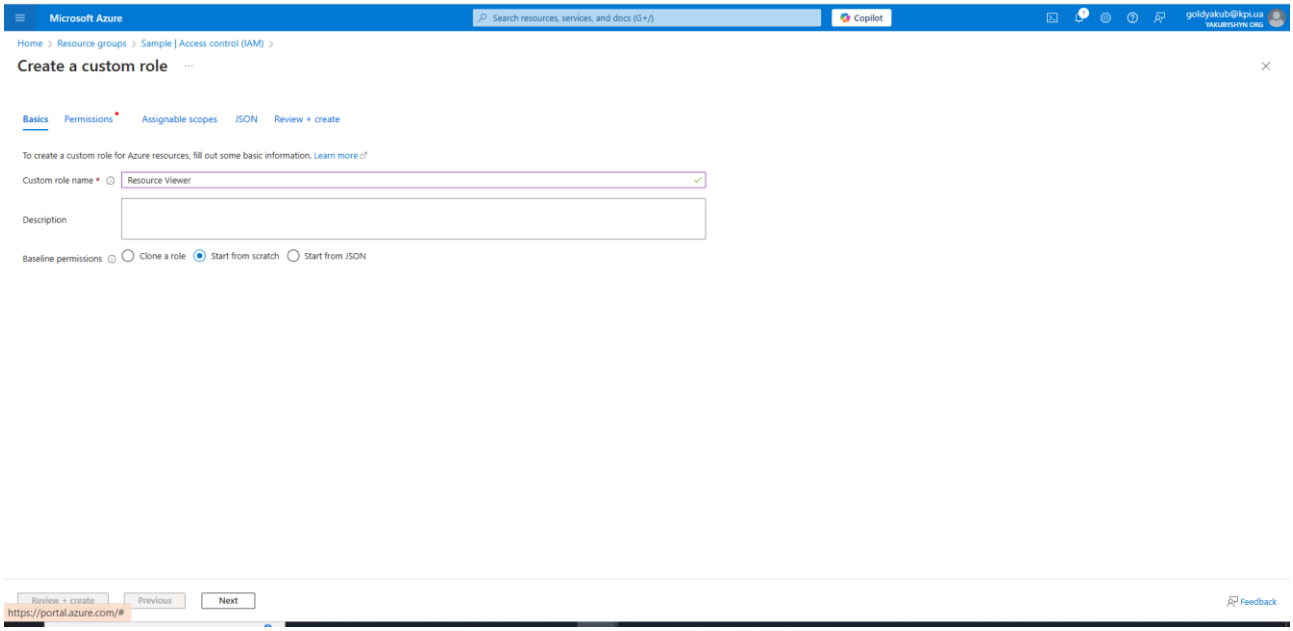


Created ‘Sample’ resource group to proceed with tasks.

1. Create a custom role named Resource Viewer with read-only permissions for a specific resource group.

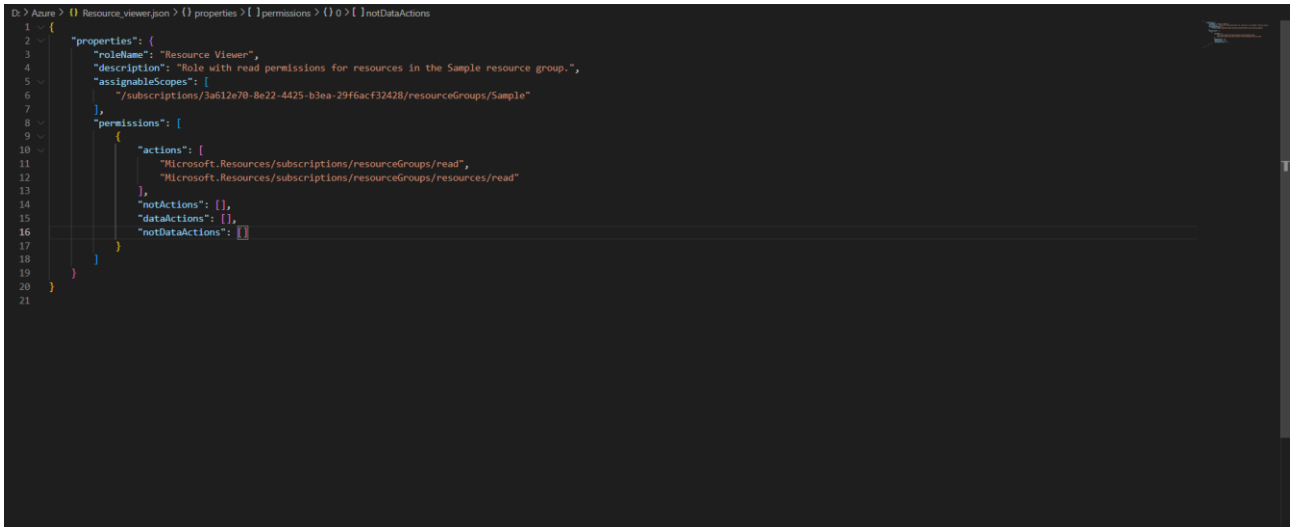


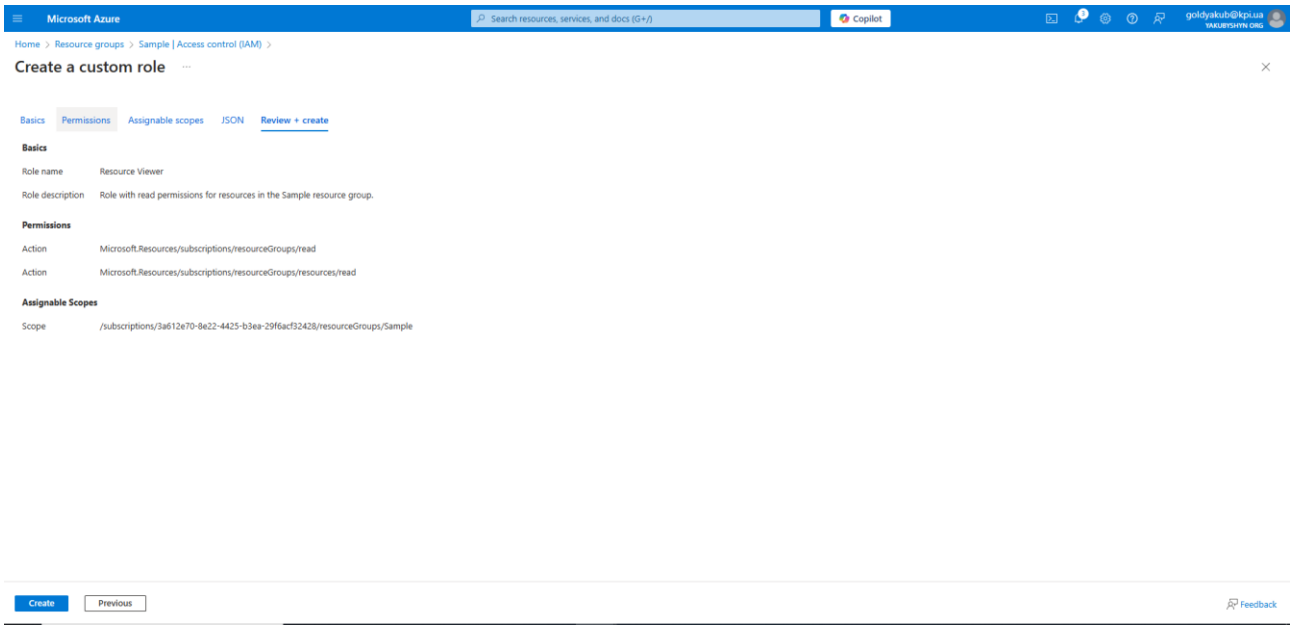
Click add custom role



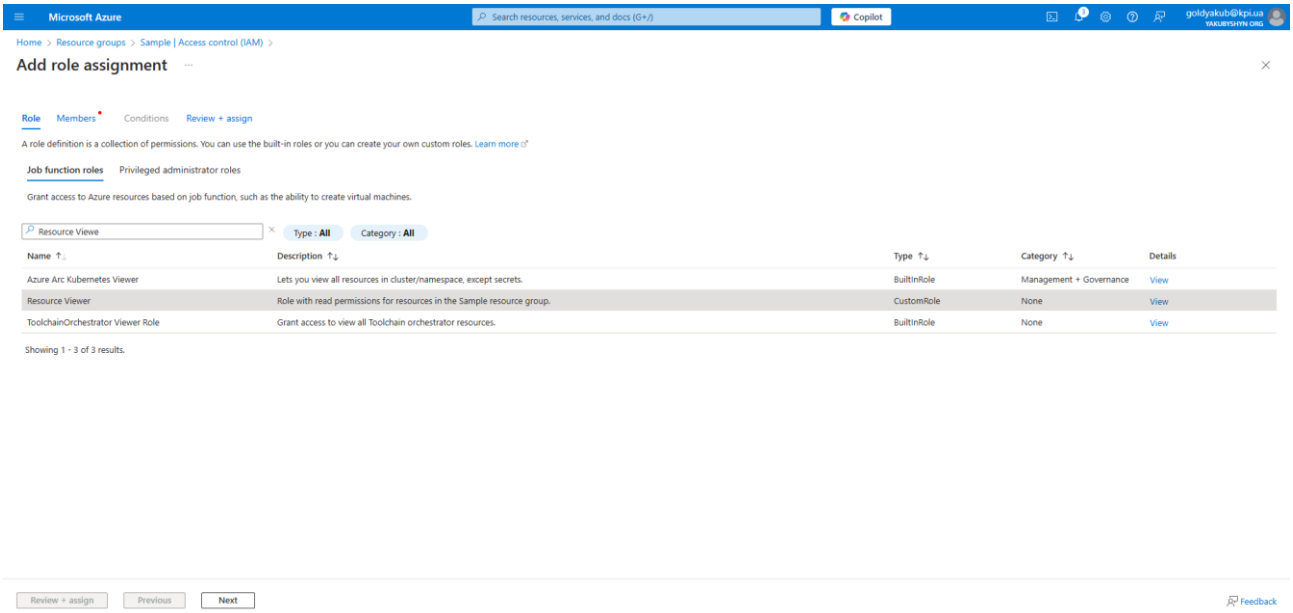
Gave a name

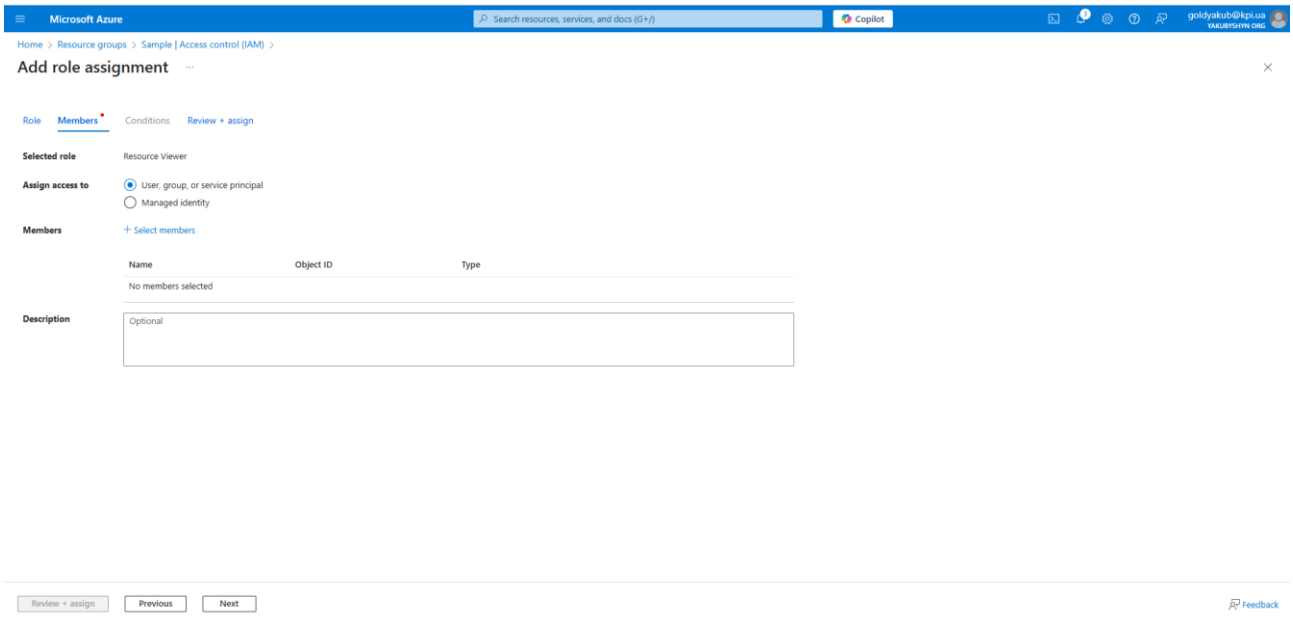
Clicked Start from JSON

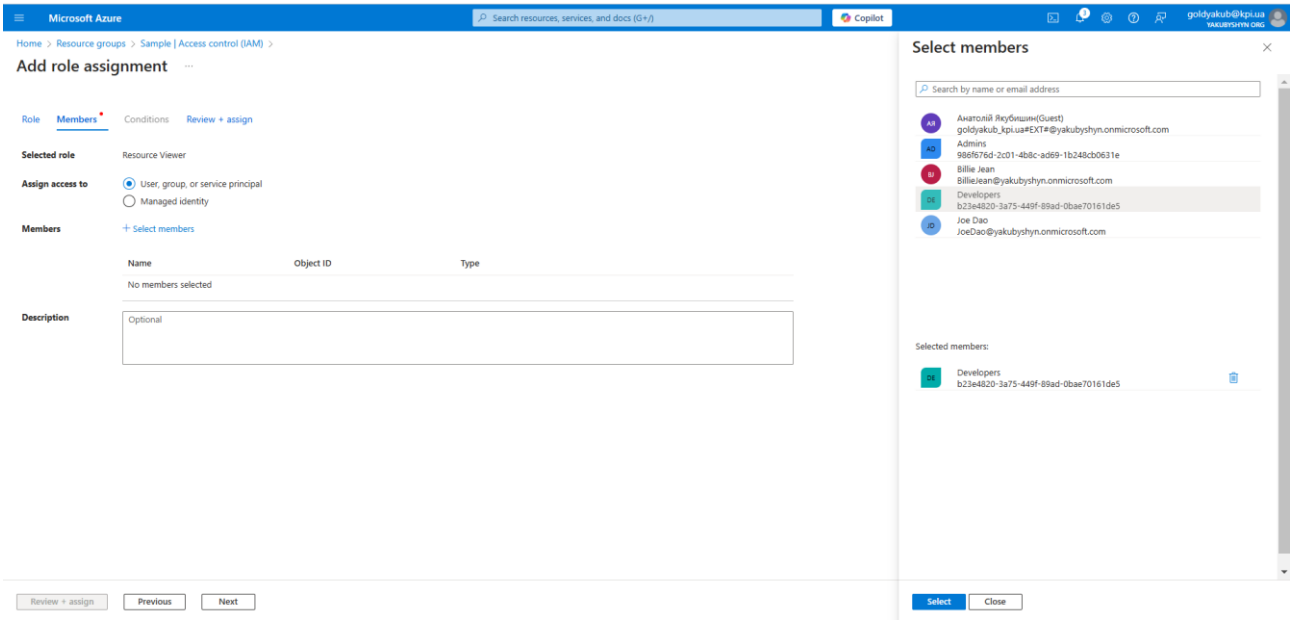


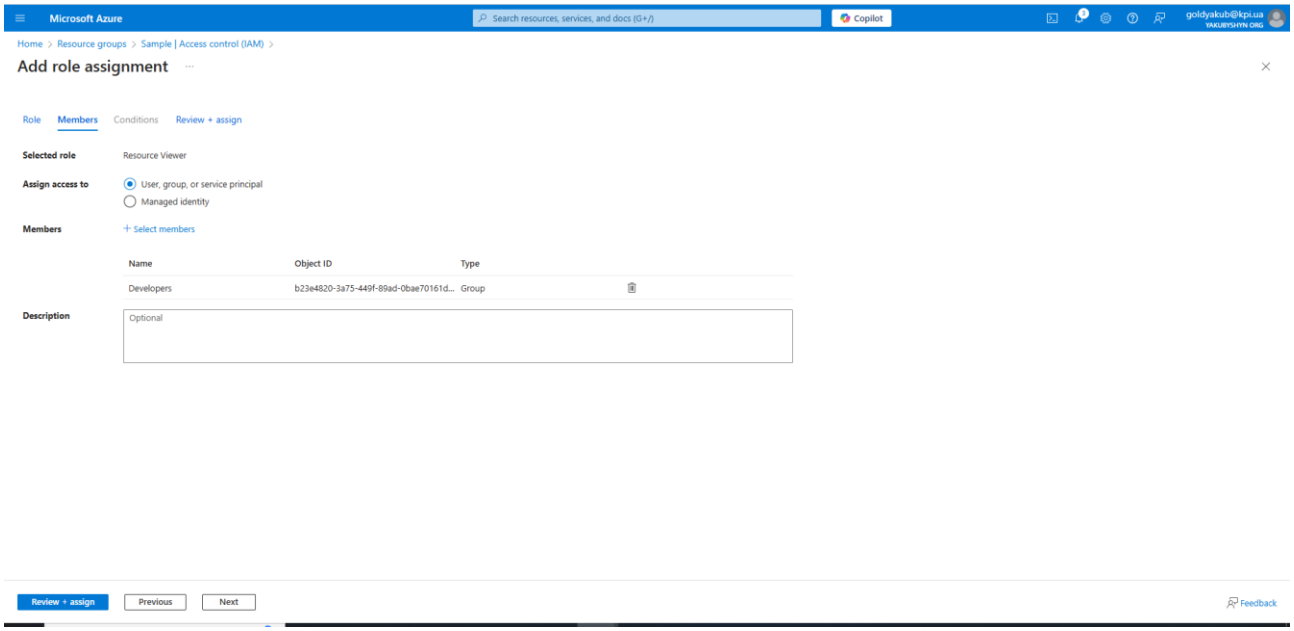


2. Assign the Resource Viewer role to the Developers group created earlier



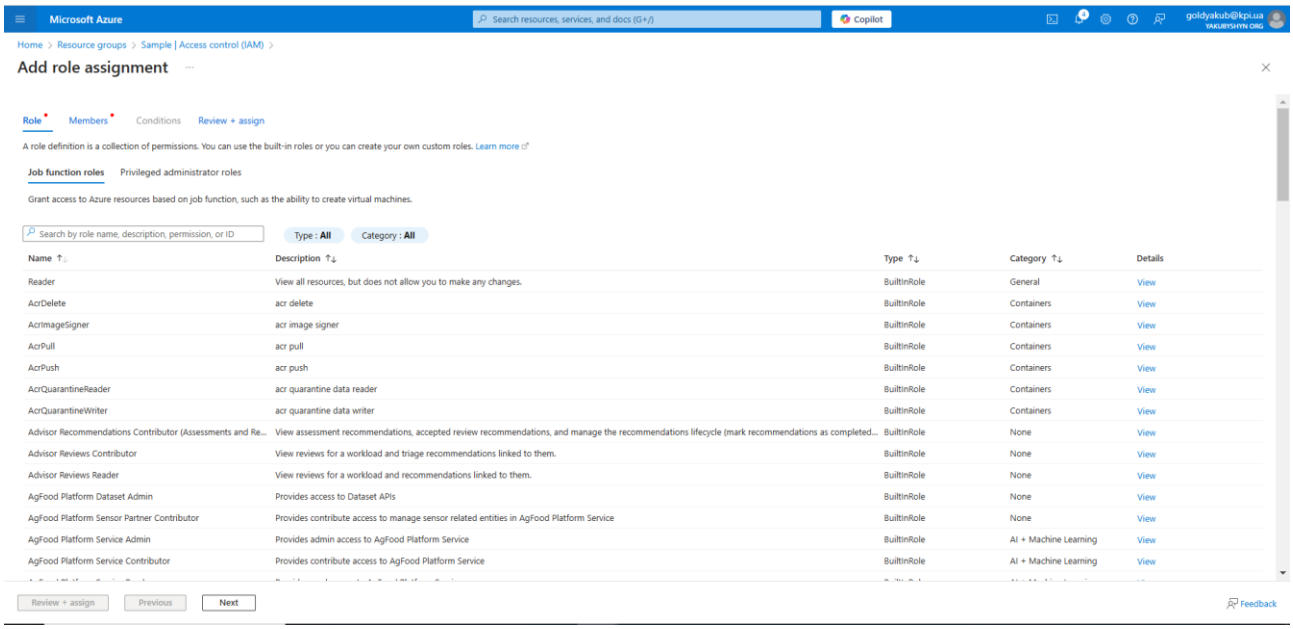


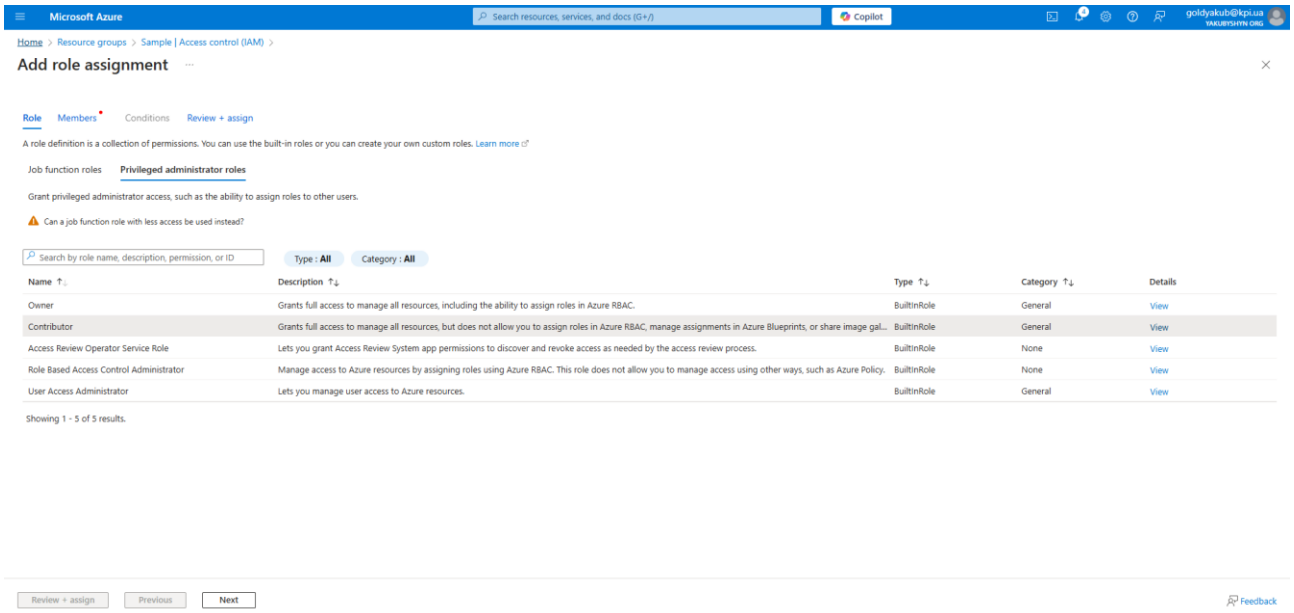


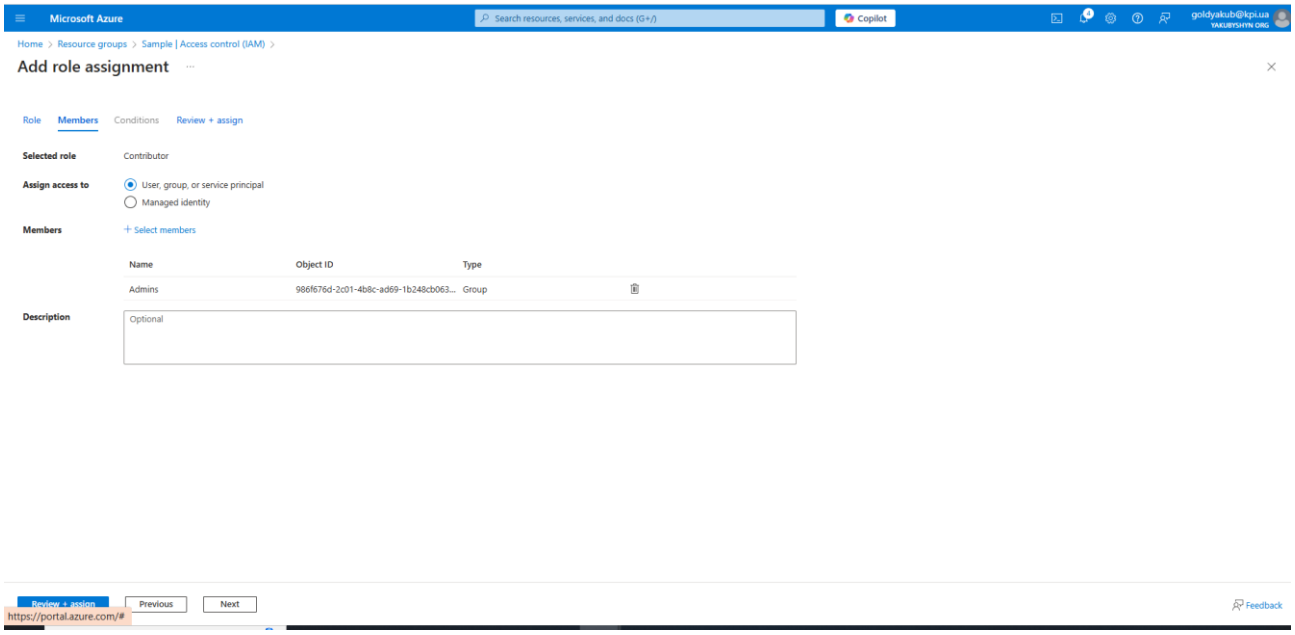


Click Review + assign

3. Assign the built-in **Contributor** role to the Admins group for the same resource group

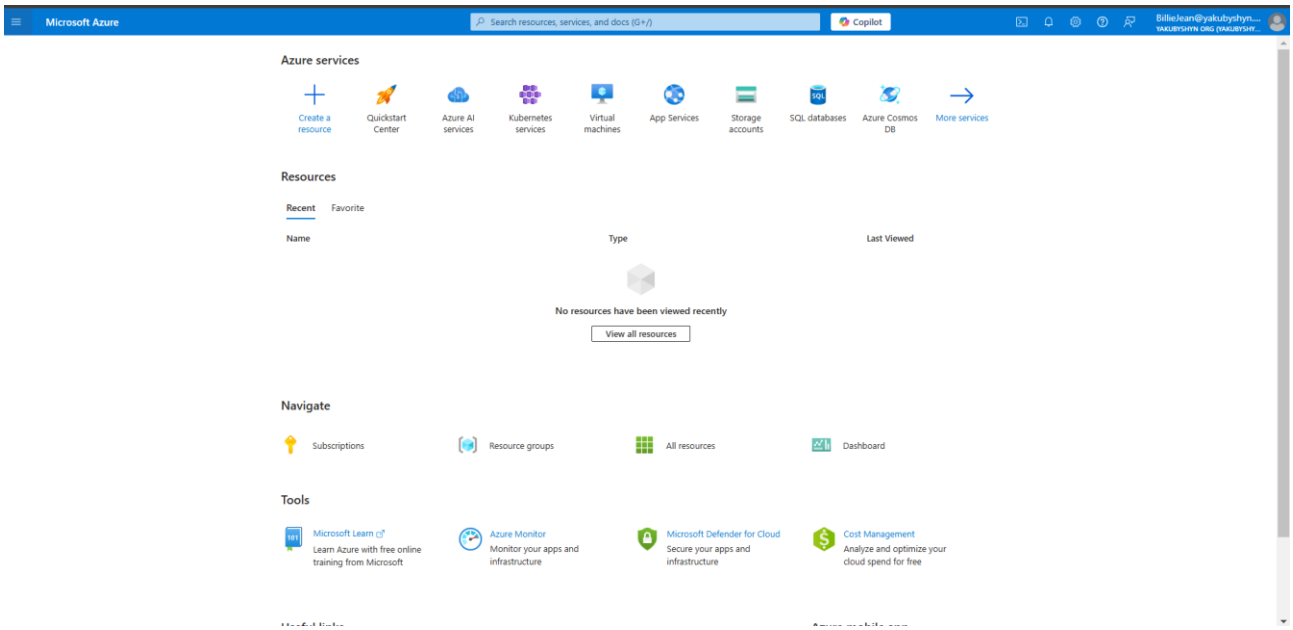




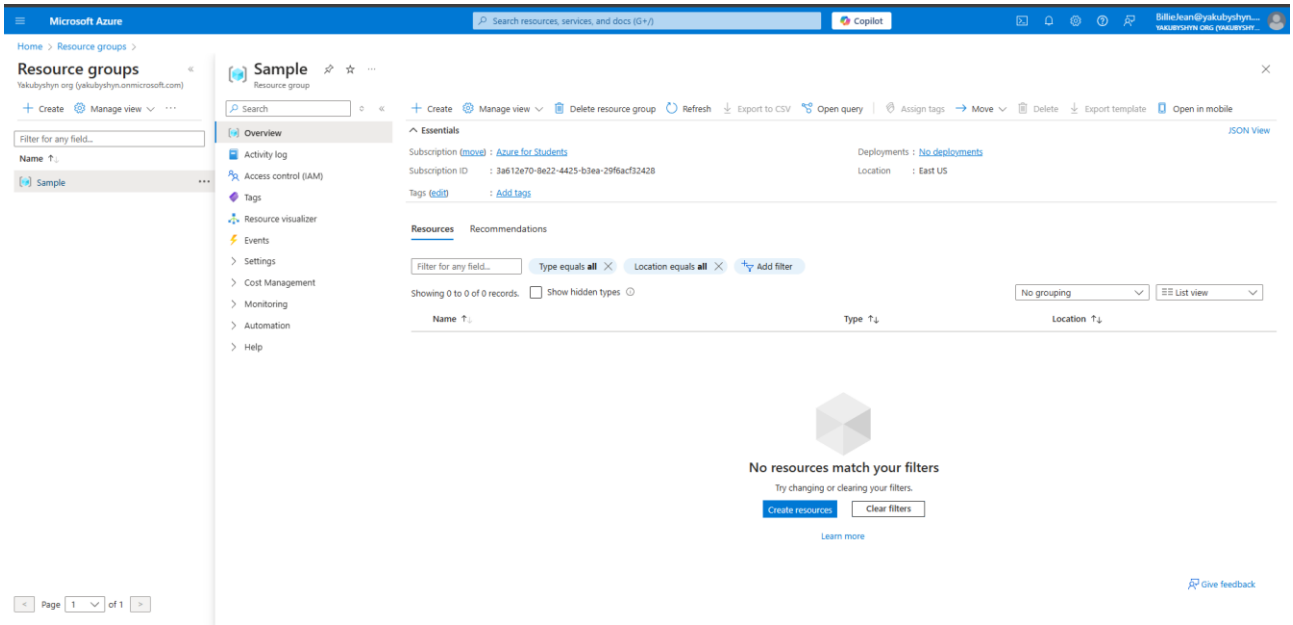


Then Review + assign

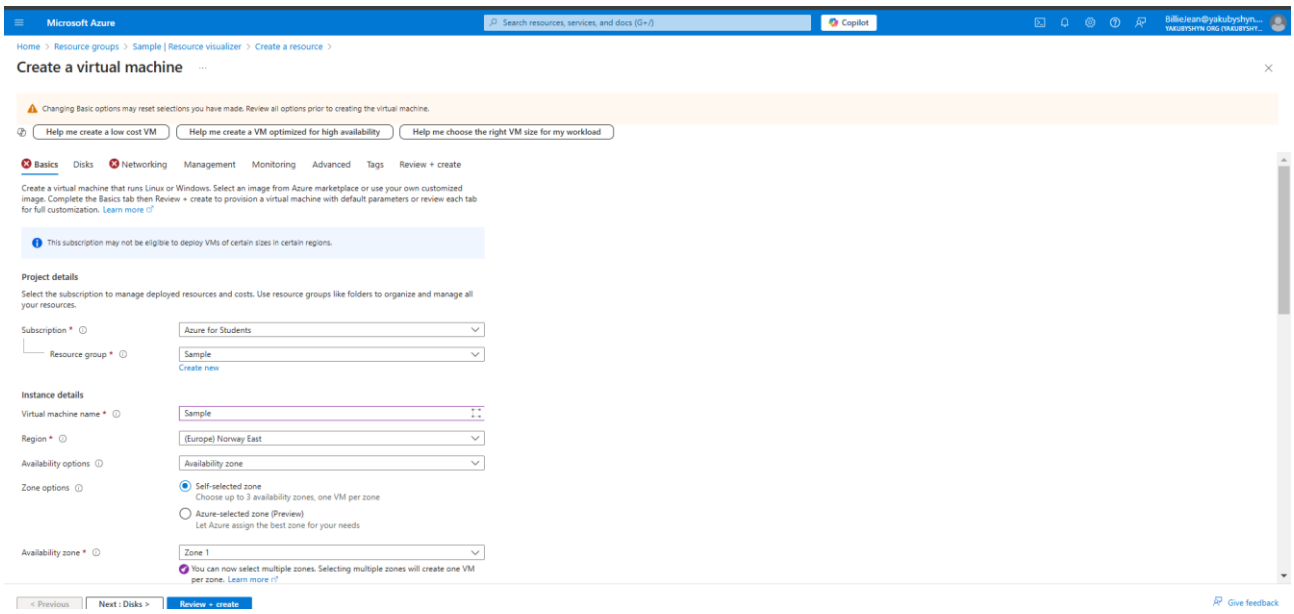
4. Verify that members of the Developers group have only read access and members of the Admins group have full access to the resource group

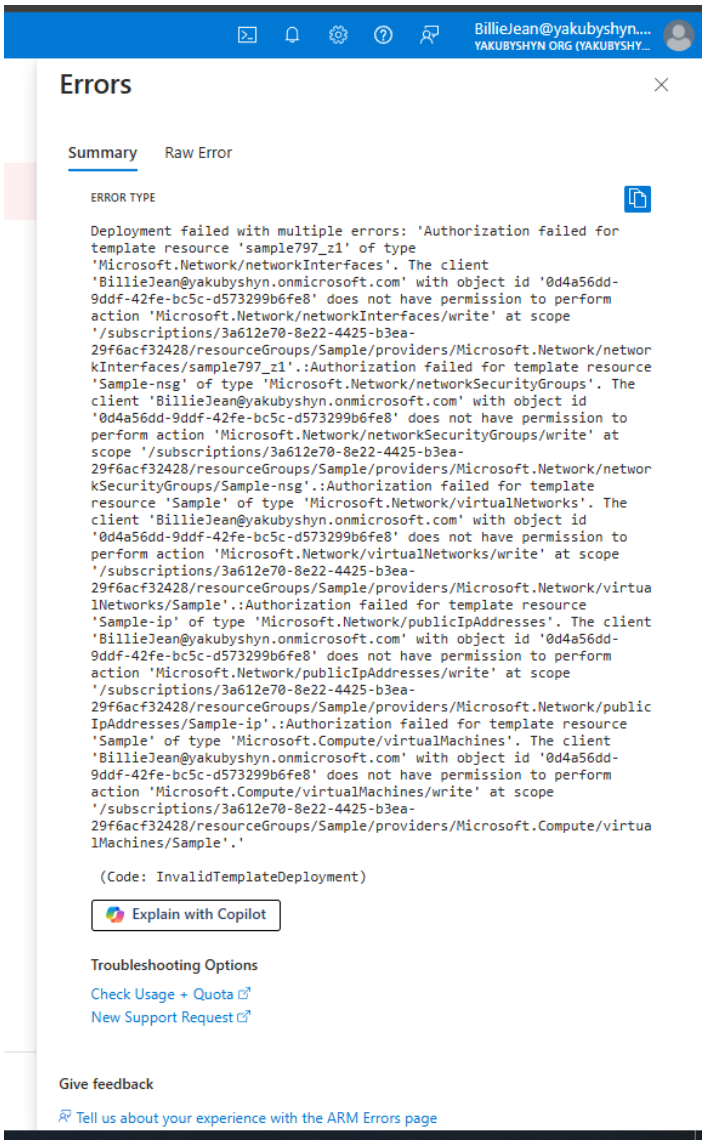


Logged in as Developer

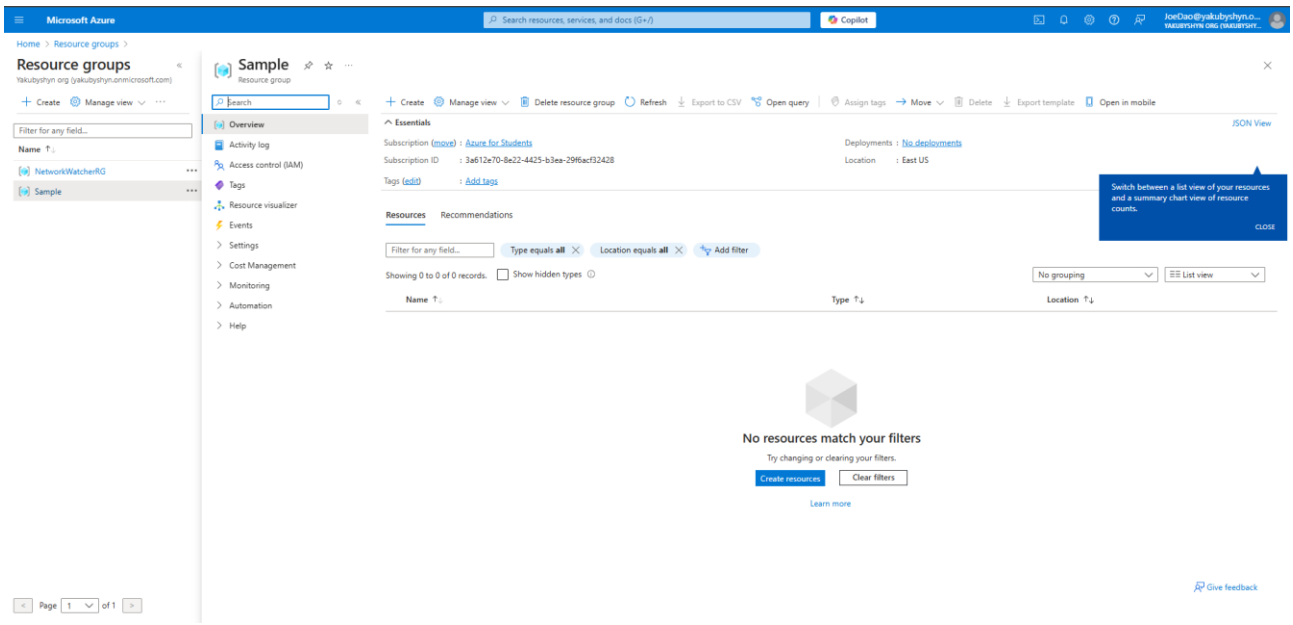


Switched to a ‘Sample’ Resource group

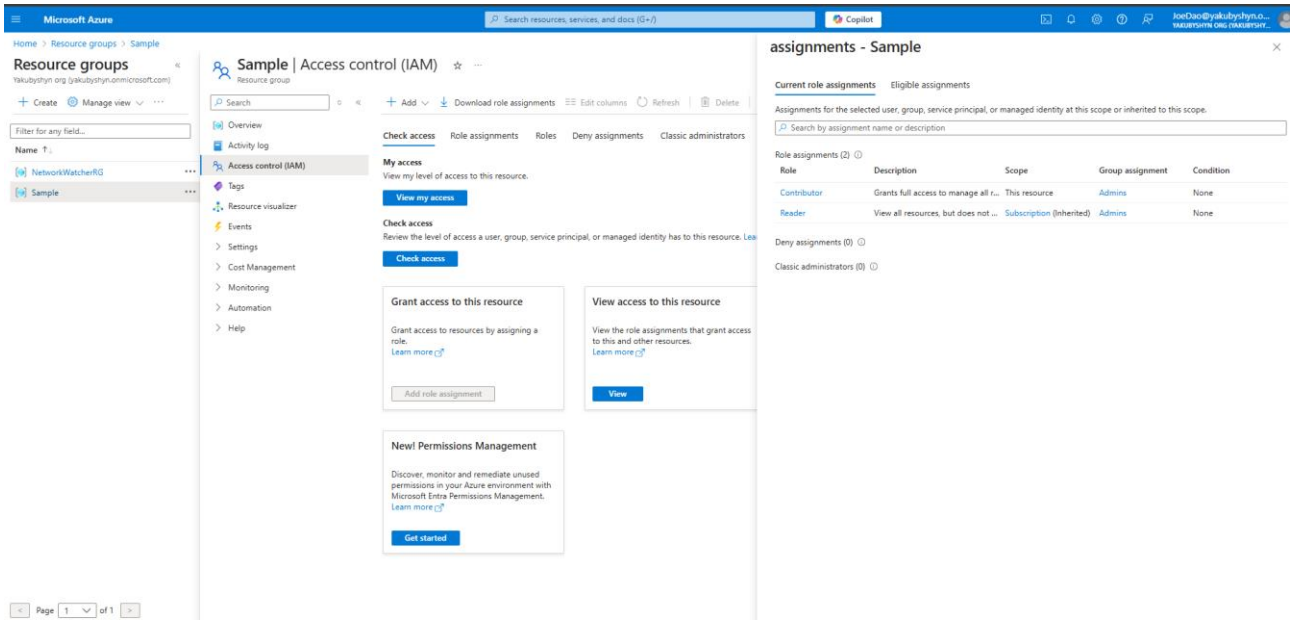

Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > Resource groups > Sample | Resource visualizer > Create a resource >
Create a virtual machine
Changing Basic options may reset selections you have made. Review all options prior to creating the virtual machine.
Help me create a low cost VM
Help me create a VM optimized for high availability
Help me choose the right VM size for my workload
Basics
Disks
Networking
Management
Monitoring
Advanced
Tags
Review + create
Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. Learn more
This subscription may not be eligible to deploy VMs of certain sizes in certain regions.
Project details
Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.
Subscription *
Azure for Students
Resource group *
Sample
Create new
Instance details
Virtual machine name *
Sample
Region *
(Europe) Norway East
Availability options
Availability zone
Zone options
Self-selected zone
Choose up to 3 availability zones, one VM per zone
Azure-selected zone (Preview)
Let Azure assign the best zone for your needs
Availability zone *
Zone 1
You can now select multiple zones. Selecting multiple zones will create one VM per zone. Learn more
< Previous
Next : Disks >
Review + create
Give feedback


BillieJean@yakubyshyn....
YAKUBYSHYN ORG (YAKUBYSHY...
Errors
Summary
Raw Error
ERROR TYPE
Deployment failed with multiple errors: 'Authorization failed for template resource 'sample797_z1' of type 'Microsoft.Network/networkInterfaces'. The client 'BillieJean@yakubyshyn.onmicrosoft.com' with object id '0d4a56dd-9ddf-42fe-bc5c-d573299b6fe8' does not have permission to perform action 'Microsoft.Network/networkInterfaces/write' at scope '/subscriptions/3a612e70-8e22-4425-b3ea-29f6acf32428/resourceGroups/Sample/providers/Microsoft.Network/networkInterfaces/sample797_z1'.:Authorization failed for template resource 'Sample-nsg' of type 'Microsoft.Network/networkSecurityGroups'. The client 'BillieJean@yakubyshyn.onmicrosoft.com' with object id '0d4a56dd-9ddf-42fe-bc5c-d573299b6fe8' does not have permission to perform action 'Microsoft.Network/networkSecurityGroups/write' at scope '/subscriptions/3a612e70-8e22-4425-b3ea-29f6acf32428/resourceGroups/Sample/providers/Microsoft.Network/networkSecurityGroups/Sample-nsg'.:Authorization failed for template resource 'Sample' of type 'Microsoft.Network/virtualNetworks'. The client 'BillieJean@yakubyshyn.onmicrosoft.com' with object id '0d4a56dd-9ddf-42fe-bc5c-d573299b6fe8' does not have permission to perform action 'Microsoft.Network/virtualNetworks/write' at scope '/subscriptions/3a612e70-8e22-4425-b3ea-29f6acf32428/resourceGroups/Sample/providers/Microsoft.Network/virtualNetworks/Sample'.:Authorization failed for template resource 'Sample-ip' of type 'Microsoft.Network/publicIpAddresses'. The client 'BillieJean@yakubyshyn.onmicrosoft.com' with object id '0d4a56dd-9ddf-42fe-bc5c-d573299b6fe8' does not have permission to perform action 'Microsoft.Network/publicIpAddresses/write' at scope '/subscriptions/3a612e70-8e22-4425-b3ea-29f6acf32428/resourceGroups/Sample/providers/Microsoft.Network/publicIpAddresses/Sample-ip'.:Authorization failed for template resource 'Sample' of type 'Microsoft.Compute/virtualMachines'. The client 'BillieJean@yakubyshyn.onmicrosoft.com' with object id '0d4a56dd-9ddf-42fe-bc5c-d573299b6fe8' does not have permission to perform action 'Microsoft.Compute/virtualMachines/write' at scope '/subscriptions/3a612e70-8e22-4425-b3ea-29f6acf32428/resourceGroups/Sample/providers/Microsoft.Compute/virtualMachines/Sample'.'
(Code: InvalidTemplateDeployment)
Explain with Copilot
Troubleshooting Options
Check Usage + Quota
New Support Request
Give feedback
Tell us about your experience with the ARM Errors page

As expected



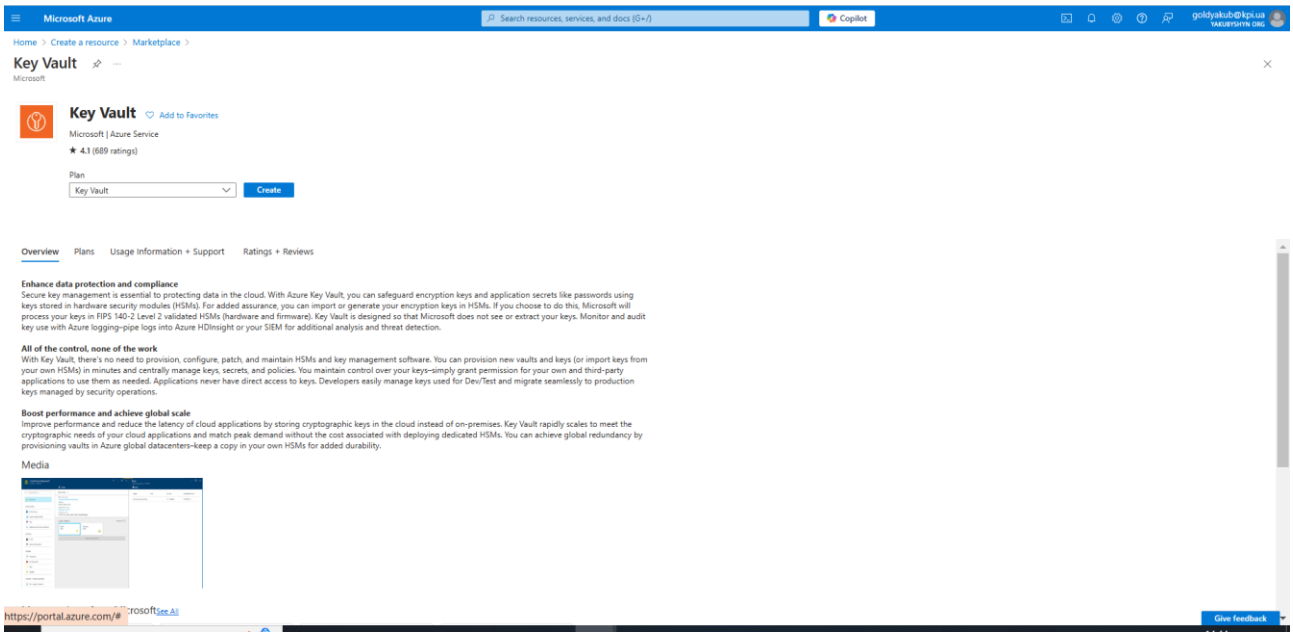
Logged in as an Admin

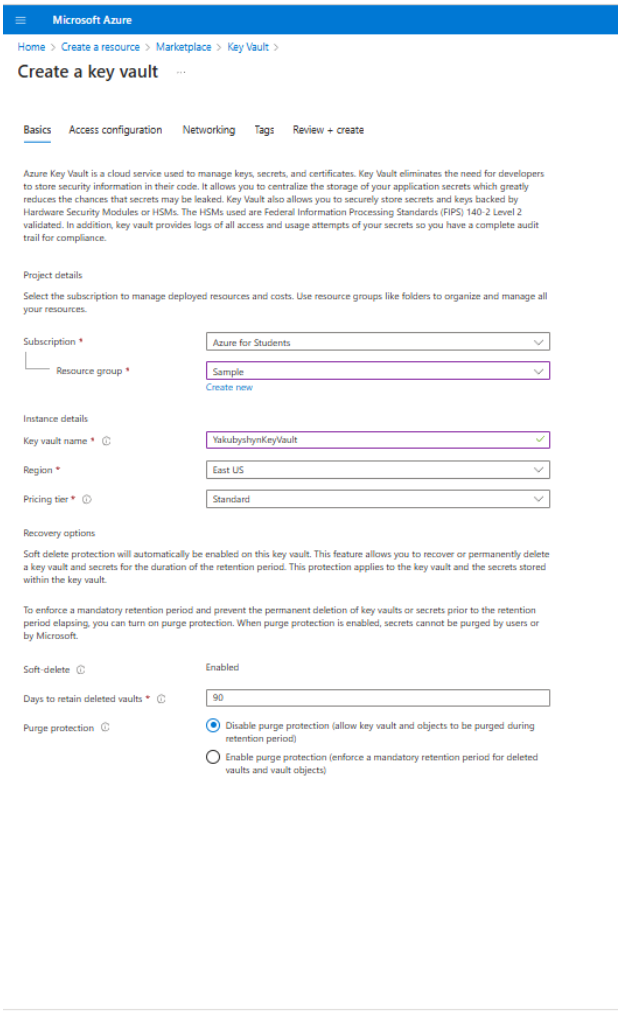


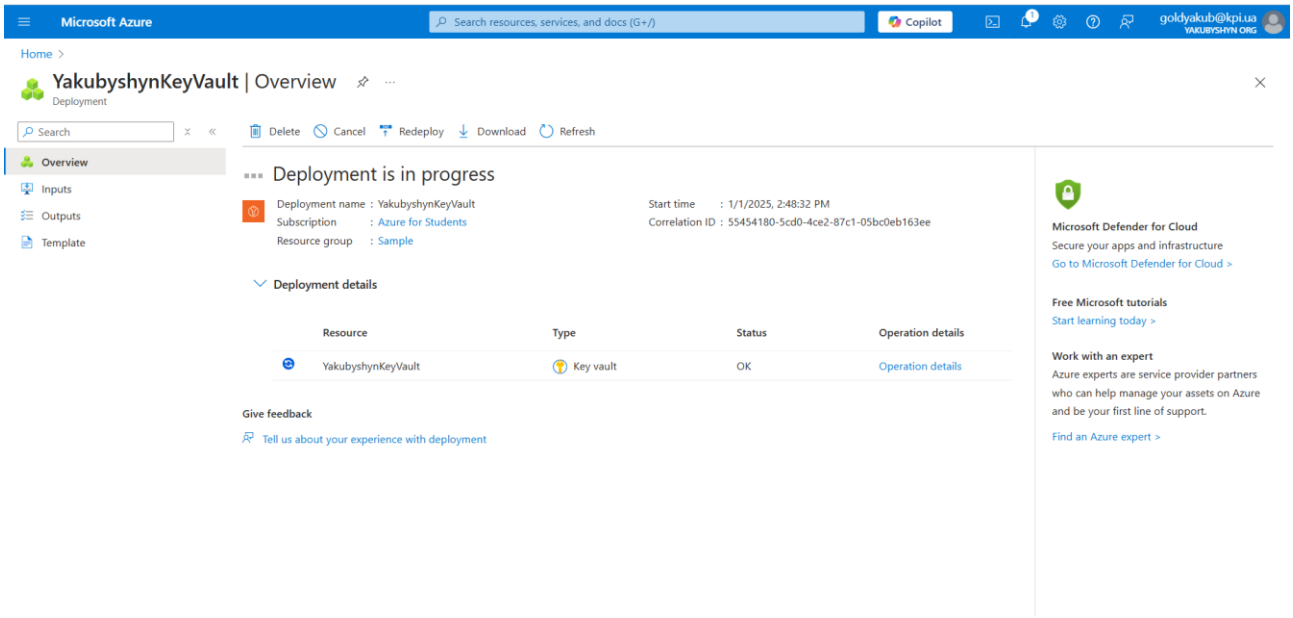
Practical Task 4: *Securing Sensitive Information with Azure Key Vault*

Set up Azure Key Vault to securely store and manage sensitive information such as keys, secrets, and certificates.

1. *Create a new Azure Key Vault in your subscription.*



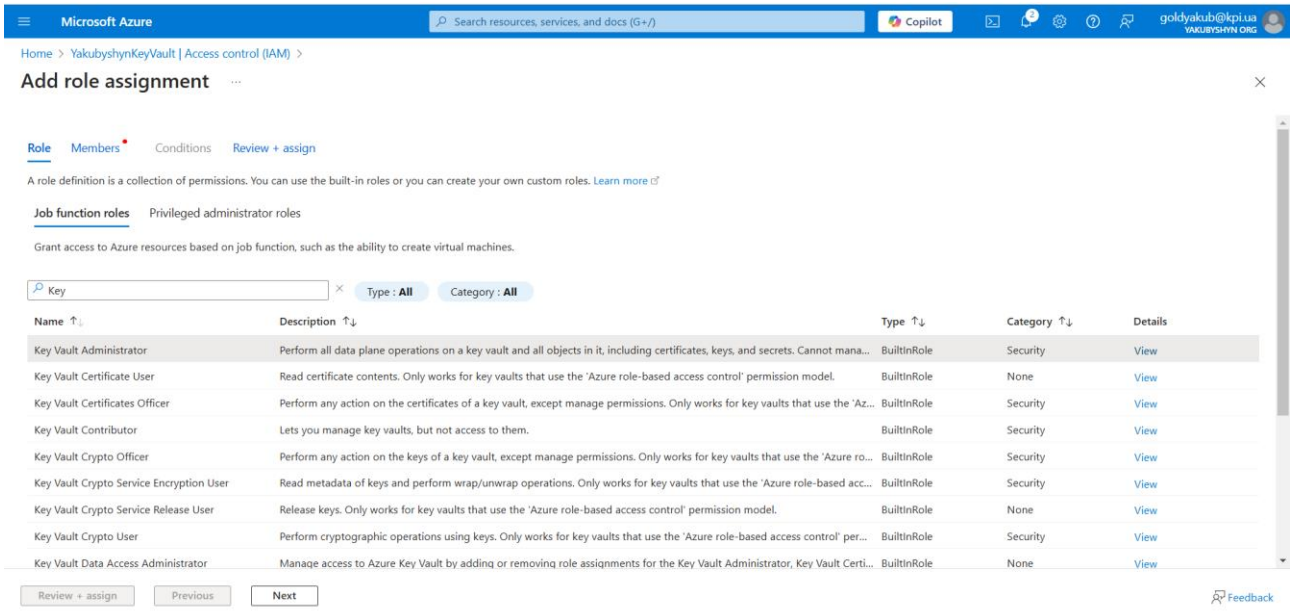

Microsoft Azure
Home > Create a resource > Marketplace > Key Vault >
Create a key vault
Basics
Access configuration
Networking
Tags
Review + create
Azure Key Vault is a cloud service used to manage keys, secrets, and certificates. Key Vault eliminates the need for developers to store security information in their code. It allows you to centralize the storage of your application secrets which greatly reduces the chances that secrets may be leaked. Key Vault also allows you to securely store secrets and keys backed by Hardware Security Modules or HSMs. The HSMs used are Federal Information Processing Standards (FIPS) 140-2 Level 2 validated. In addition, key vault provides logs of all access and usage attempts of your secrets so you have a complete audit trail for compliance.
Project details
Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.
Subscription *
Azure for Students
Resource group *
Sample
Create new
Instance details
Key vault name *
YakubyshynKeyVault
Region *
East US
Pricing tier *
Standard
Recovery options
Soft delete protection will automatically be enabled on this key vault. This feature allows you to recover or permanently delete a key vault and secrets for the duration of the retention period. This protection applies to the key vault and the secrets stored within the key vault.
To enforce a mandatory retention period and prevent the permanent deletion of key vaults or secrets prior to the retention period elapsing, you can turn on purge protection. When purge protection is enabled, secrets cannot be purged by users or by Microsoft.
Soft-delete
Enabled
Days to retain deleted vaults *
90
Purge protection
Disable purge protection (allow key vault and objects to be purged during retention period)
Enable purge protection (enforce a mandatory retention period for deleted vaults and vault objects)
Previous
Next
Review + create

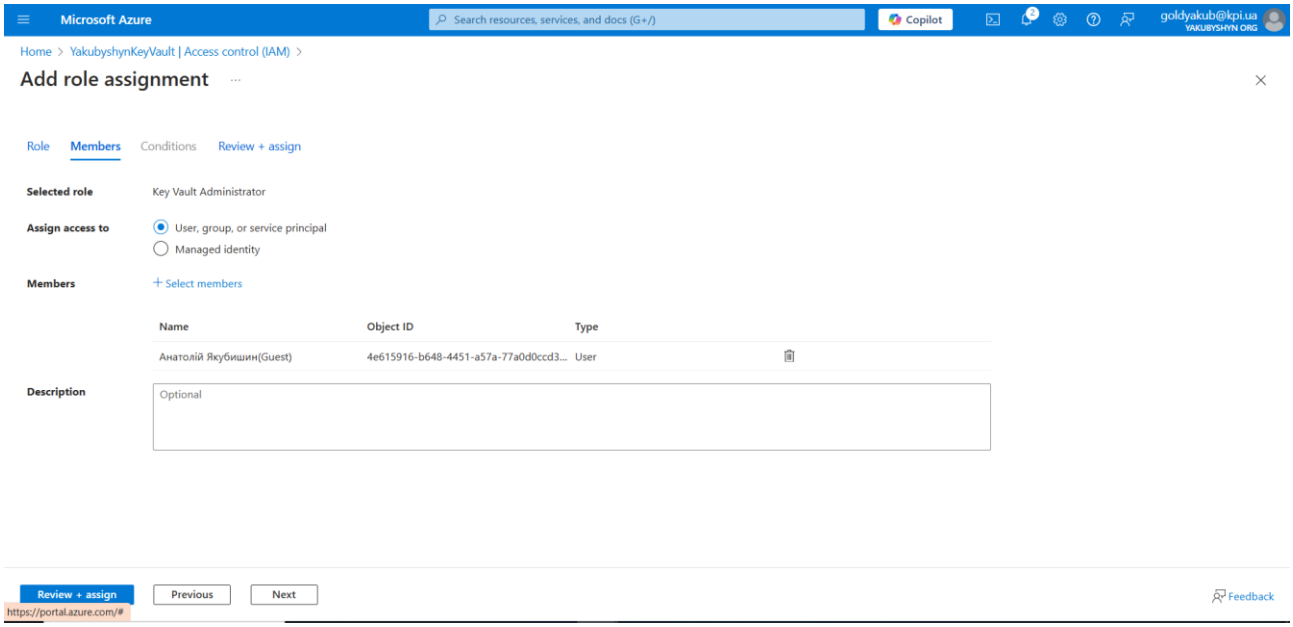

Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
goldyakub@kpi.ua
YAKUBYSHYN ORG
Home >
YakubyshynKeyVault | Overview
Deployment
Search
Overview
Inputs
Outputs
Template
Delete
Cancel
Redeploy
Download
Refresh
Deployment is in progress
Deployment name : YakubyshynKeyVault
Subscription : Azure for Students
Resource group : Sample
Start time : 1/1/2025, 2:48:32 PM
Correlation ID : 55454180-5cd0-4ce2-87c1-05bc0eb163ee
Deployment details
Resource
Type
Status
Operation details
YakubyshynKeyVault
Key vault
OK
Operation details
Give feedback
Tell us about your experience with deployment
Microsoft Defender for Cloud
Secure your apps and infrastructure
Go to Microsoft Defender for Cloud >
Free Microsoft tutorials
Start learning today >
Work with an expert
Azure experts are service provider partners who can help manage your assets on Azure and be your first line of support.
Find an Azure expert >

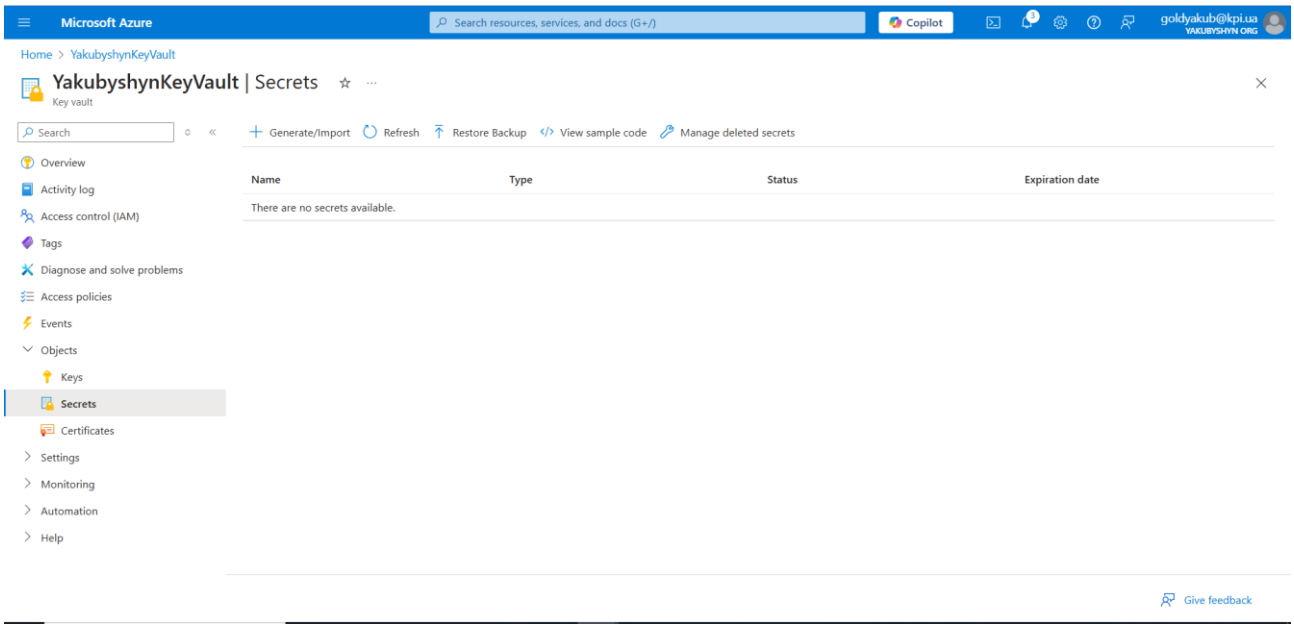
2. Add a secret to the Key Vault (e.g., a database connection string).

Before doing this, it is needed to assign myself as the "Key Vault Administrator" role

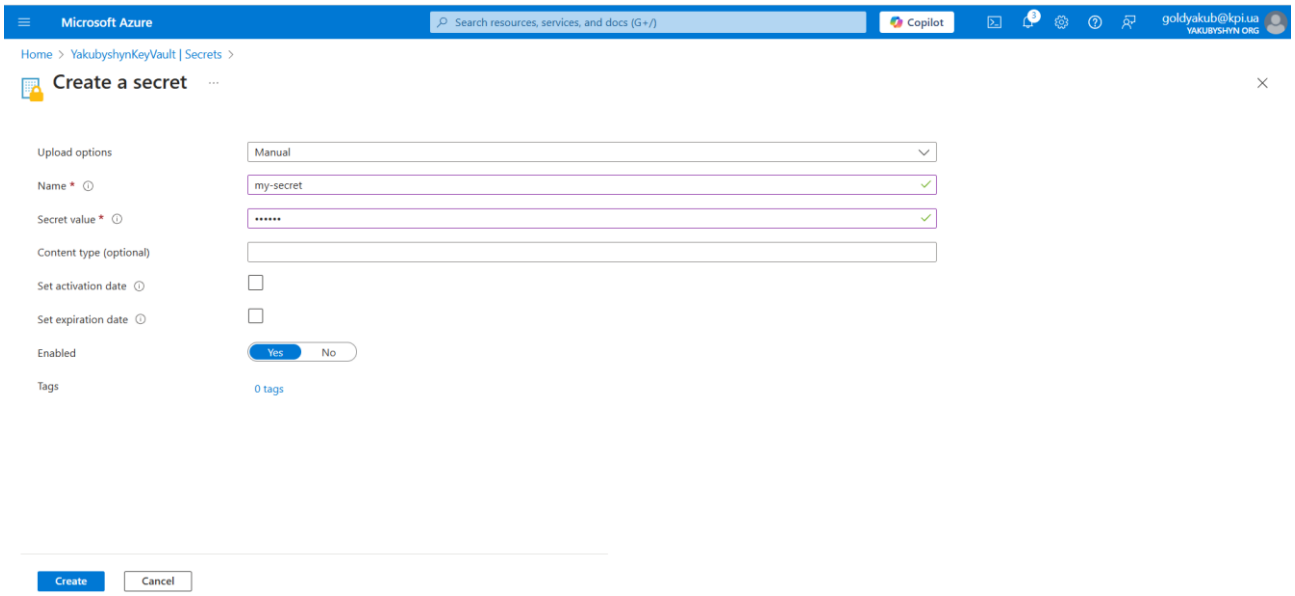
(https://learn.microsoft.com/en-us/answers/questions/1370440/azure-keyvault-the-operation-is-not-allowed-by-rba)



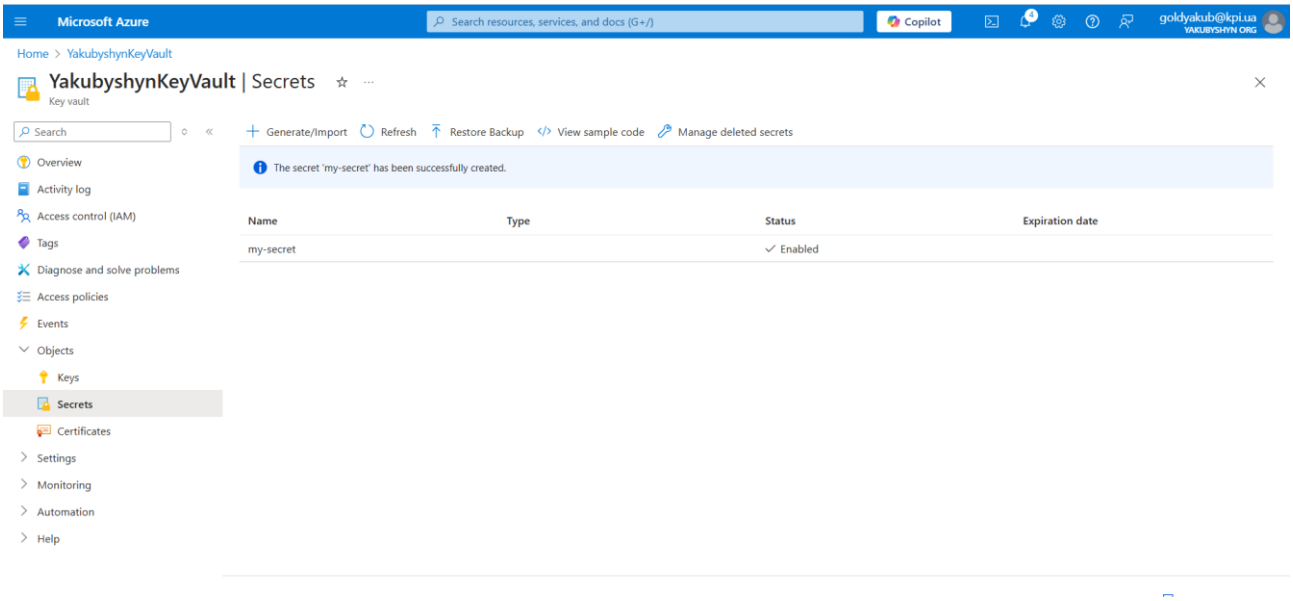




Then click Generate/Import

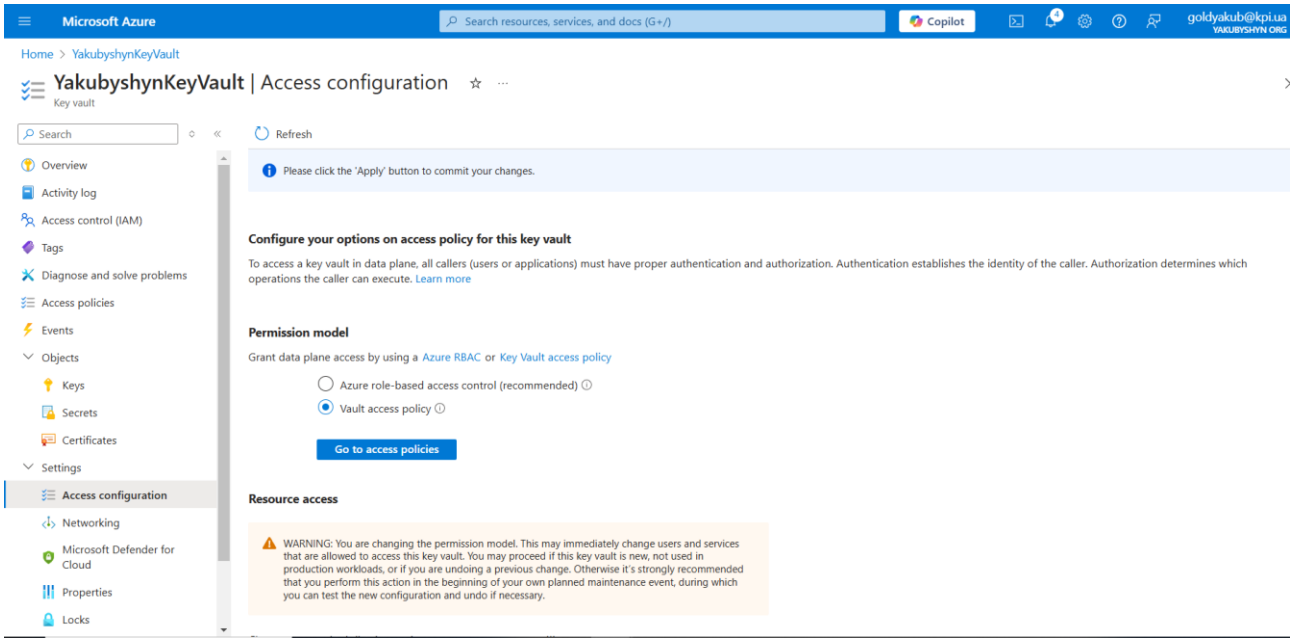


Then click Create

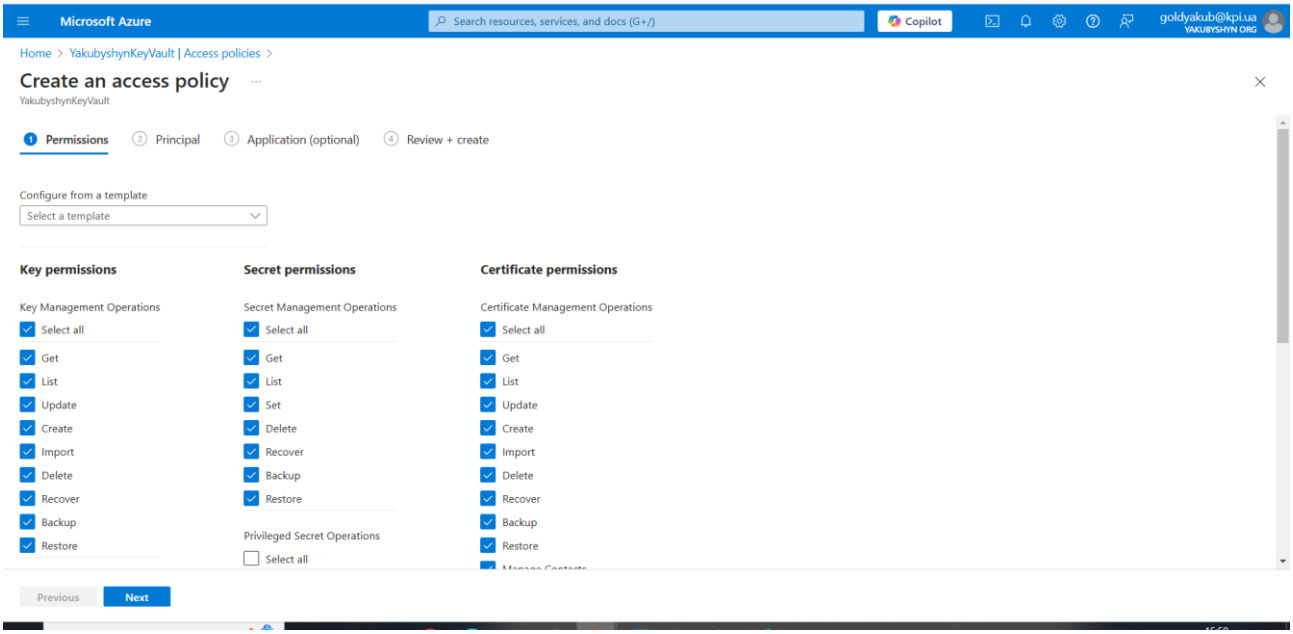


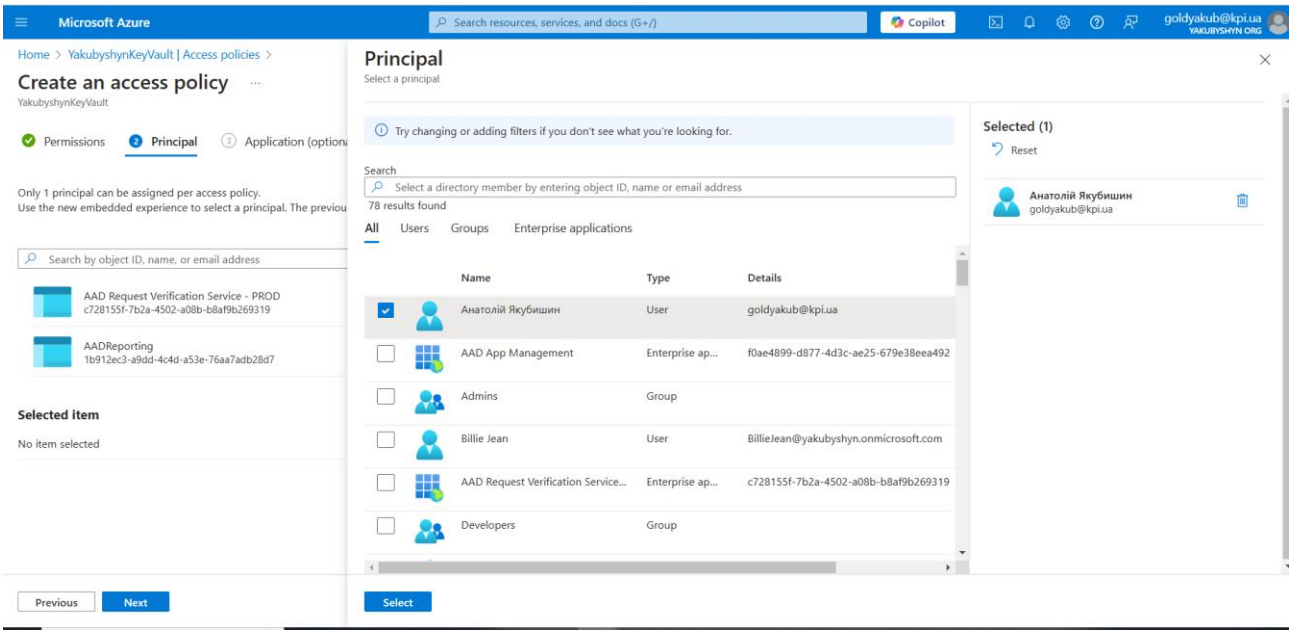
3. Set access policies to grant the Application Developer role (assigned to the Developers group) permission to retrieve secrets from the Key Vault.

Settings->Access configuration-> vault Access policy

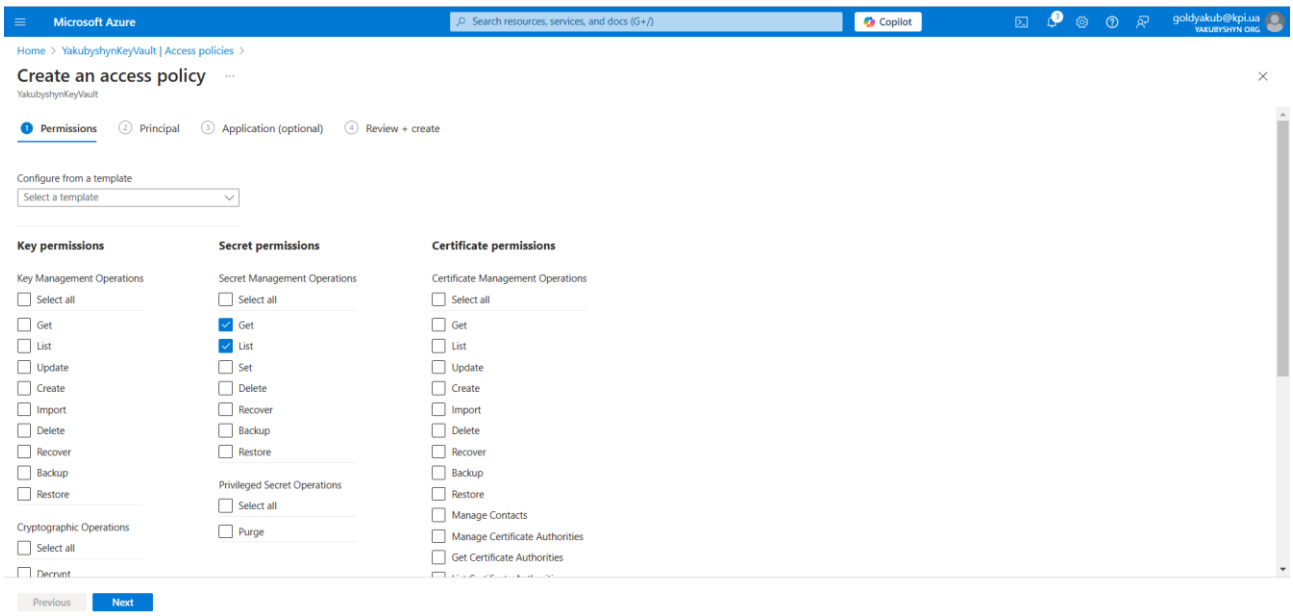


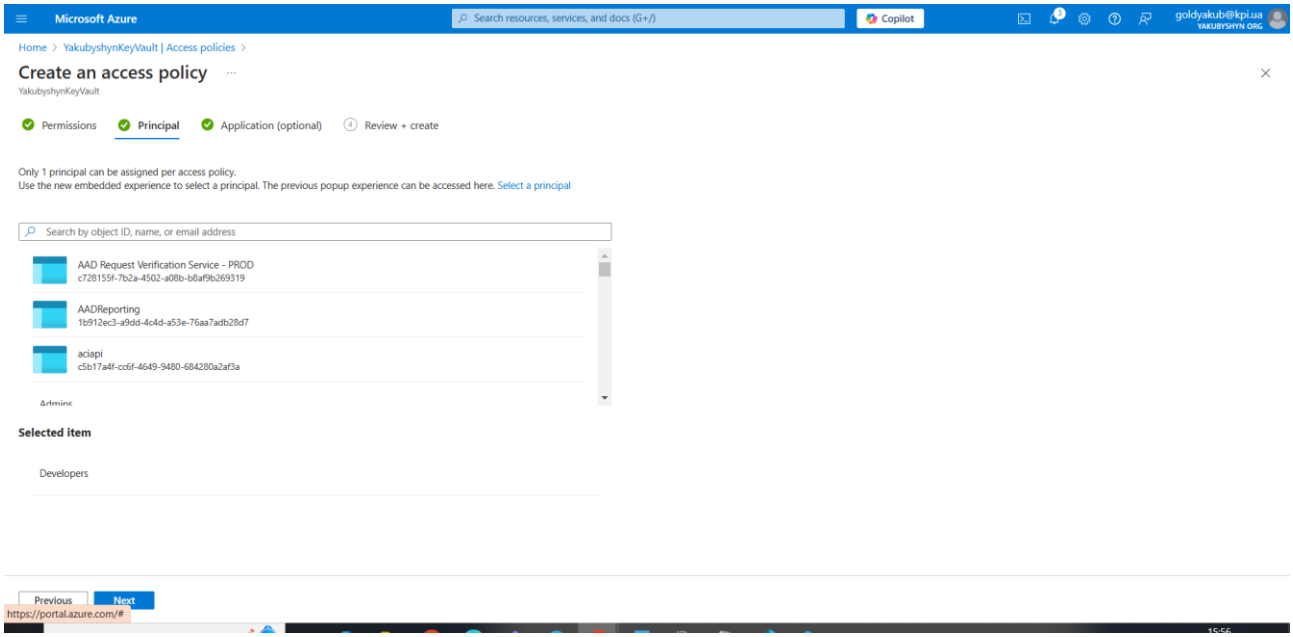
Update for main user

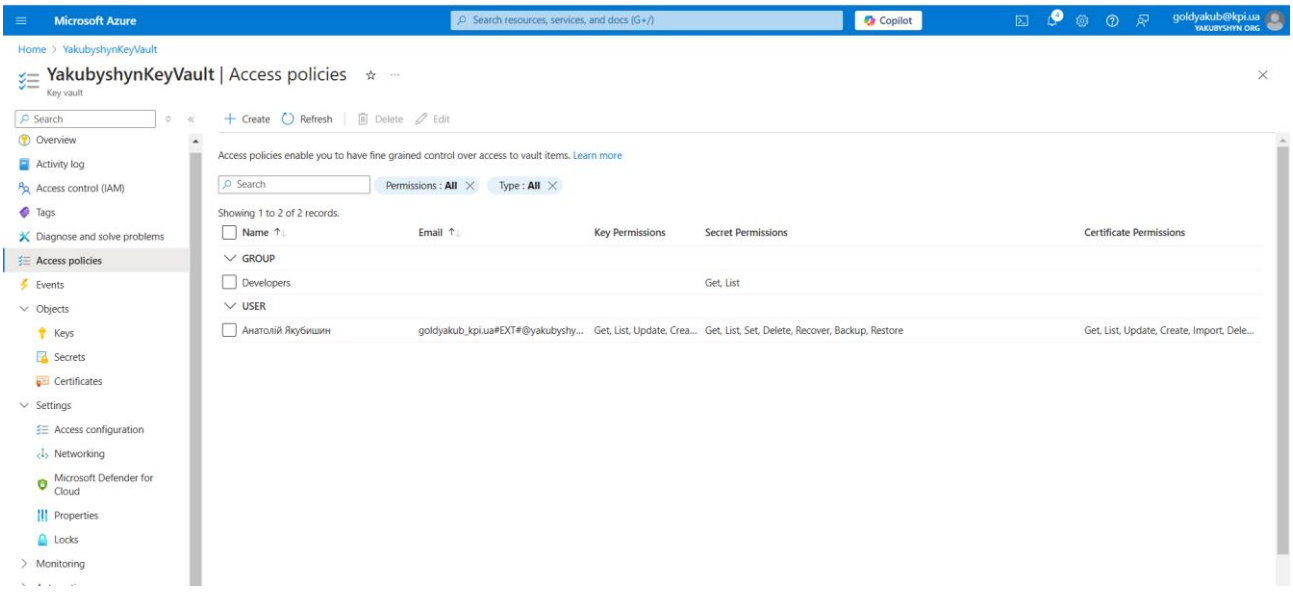


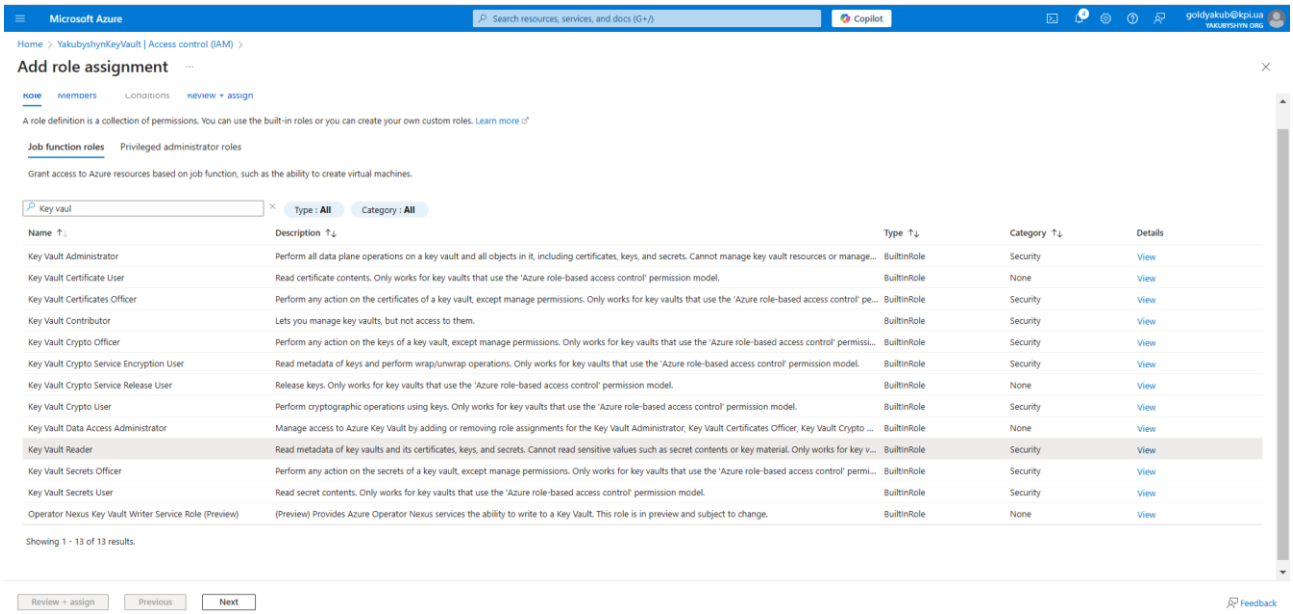


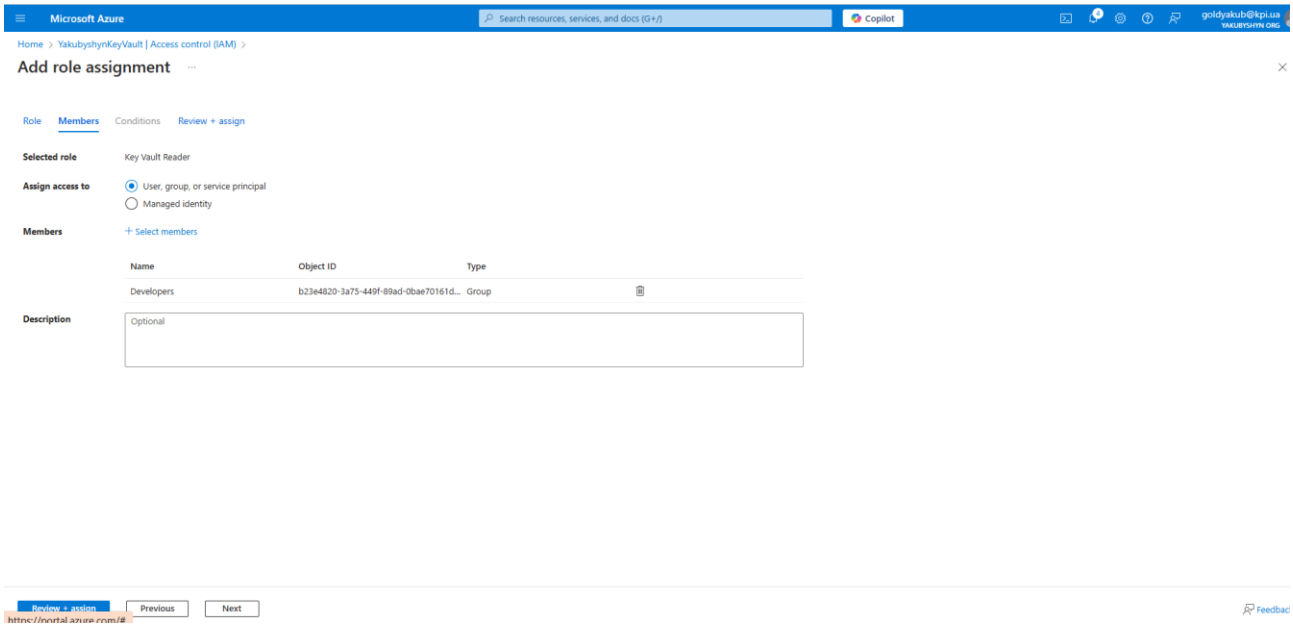
Then next, next review and create


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
goldyakub@kpi.ua
YAKUBYSHYN ORG
Home > YakubyshynKeyVault | Access policies >
Create an access policy
YakubyshynKeyVault
Permissions
Principal
Application (optional)
Review + create
Configure from a template
Select a template
Key permissions
Key Management Operations
Select all
Get
List
Update
Create
Import
Delete
Recover
Backup
Restore
Cryptographic Operations
Select all
Decrypt
Secret permissions
Secret Management Operations
Select all
Get
List
Set
Delete
Recover
Backup
Restore
Privileged Secret Operations
Select all
Purge
Certificate permissions
Certificate Management Operations
Select all
Get
List
Update
Create
Import
Delete
Recover
Backup
Restore
Manage Contacts
Manage Certificate Authorities
Get Certificate Authorities
Previous
Next

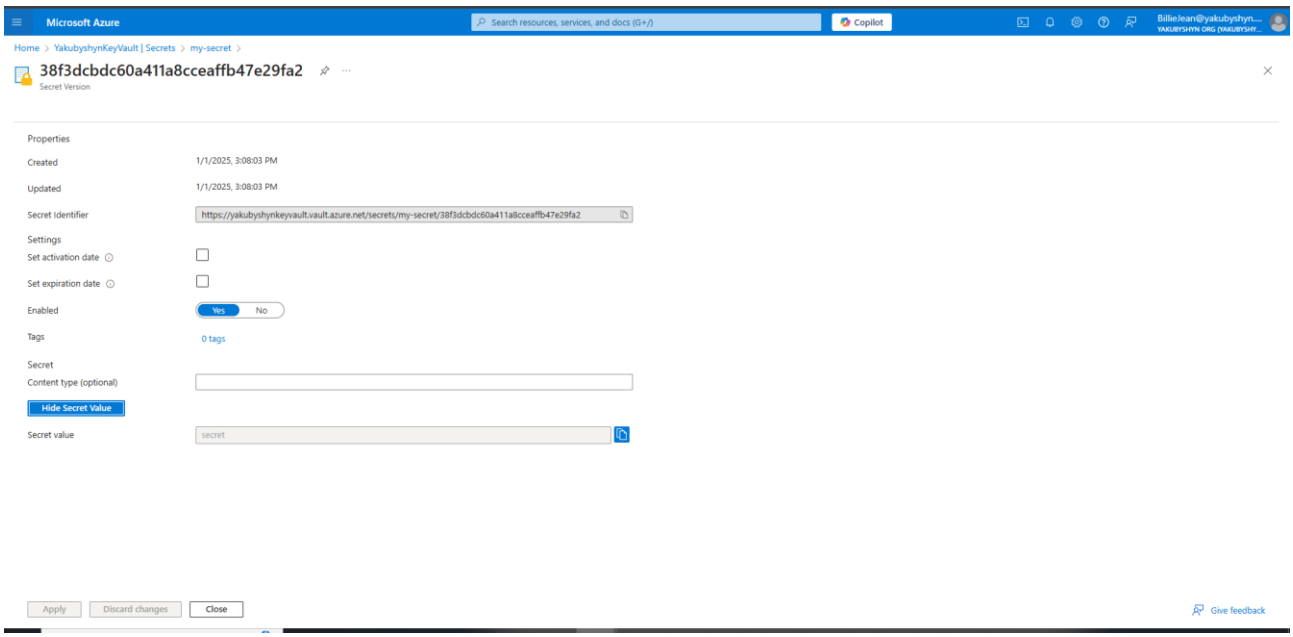

Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
goldyakub@kpi.ua
YAKUBYSHYN ORG
Home > YakubyshynKeyVault | Access policies >
Create an access policy
YakubyshynKeyVault
Permissions
Principal
Application (optional)
Review + create
Only 1 principal can be assigned per access policy.
Use the new embedded experience to select a principal. The previous popup experience can be accessed here. Select a principal
Search by object ID, name, or email address
AAD Request Verification Service - PROD
c728155f-7b2a-4502-a08b-b8af9b269319
AADReporting
1b912ec3-a9dd-4c4d-a53e-76aa7adb28d7
aciapi
c5b17a4f-cc6f-4649-9480-684280a2af3a
Selected item
Developers
Previous
Next


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
goldyakub@kpi.ua
YAKUBYSHYN ORG
Home > YakubyshynKeyVault
YakubyshynKeyVault | Access policies
Key vault
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Access policies
Events
Objects
Keys
Secrets
Certificates
Settings
Access configuration
Networking
Microsoft Defender for Cloud
Properties
Locks
Monitoring
Create
Refresh
Delete
Edit
Access policies enable you to have fine grained control over access to vault items. Learn more
Search
Permissions : All
Type : All
Showing 1 to 2 of 2 records.
Name
Email
Key Permissions
Secret Permissions
Certificate Permissions
GROUP
Developers
Get, List
USER
Анатолій Якубишин
goldyakub_kpi.ua#EXT#@yakubyshy...
Get, List, Update, Crea...
Get, List, Set, Delete, Recover, Backup, Restore
Get, List, Update, Create, Import, Dele...

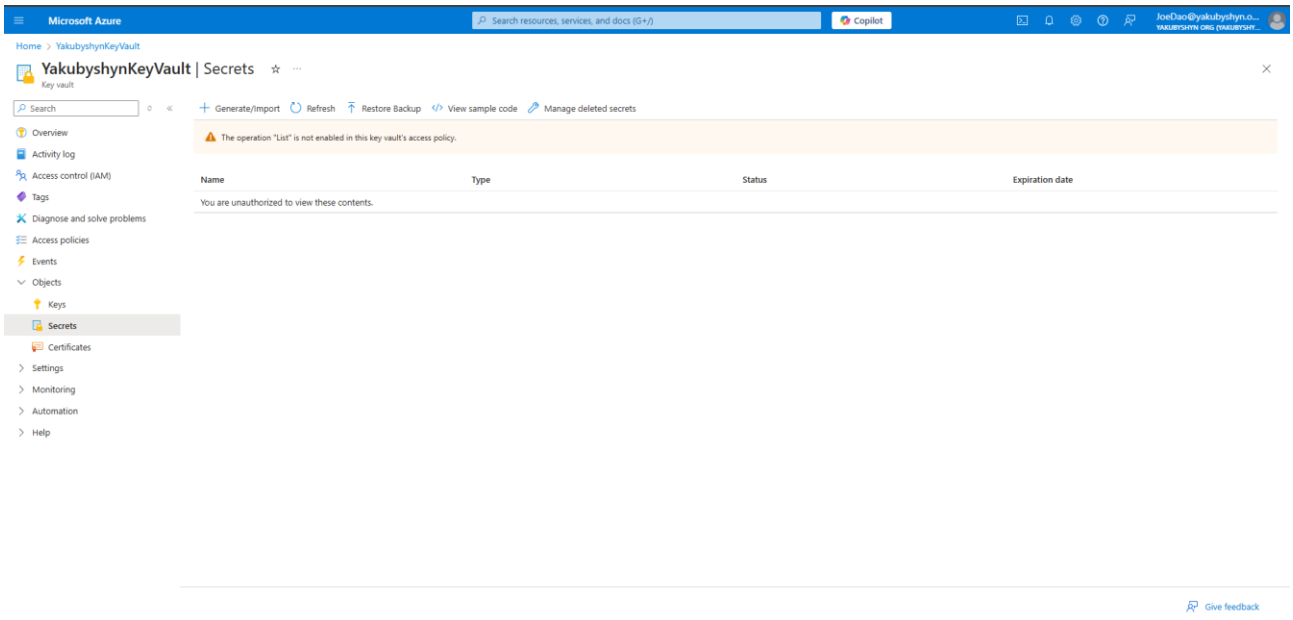




4. Verify that only members of the Developers group can access the stored secret.



Developer (Billie Jean) can see secret content

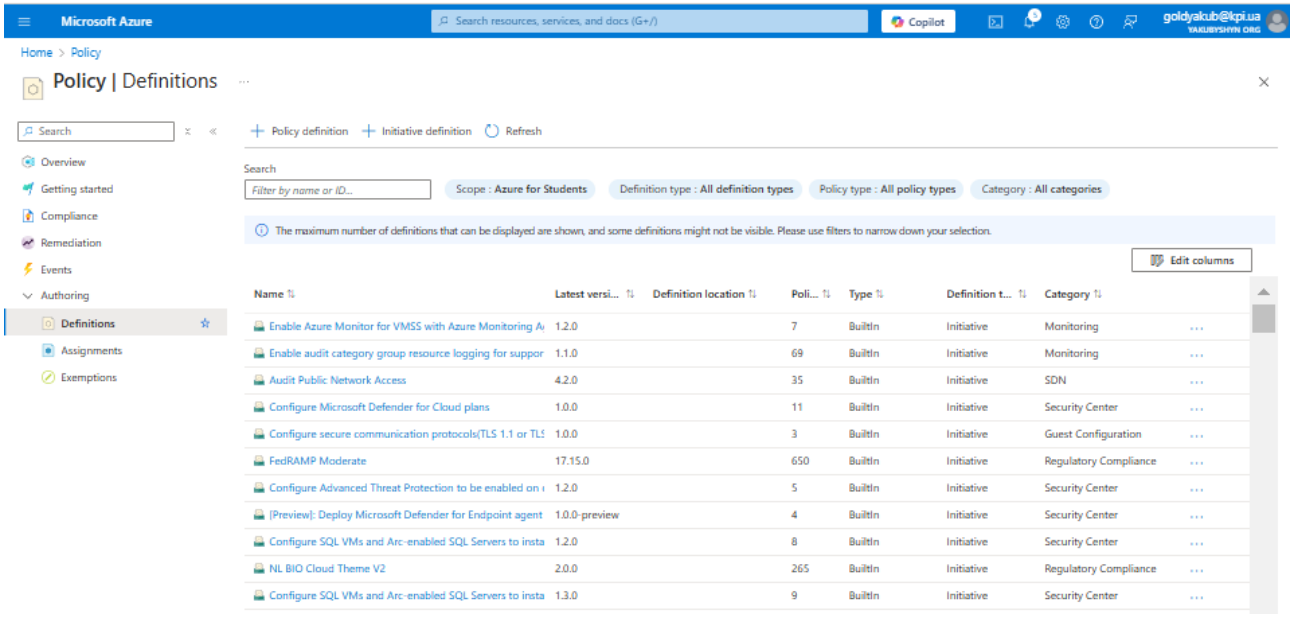


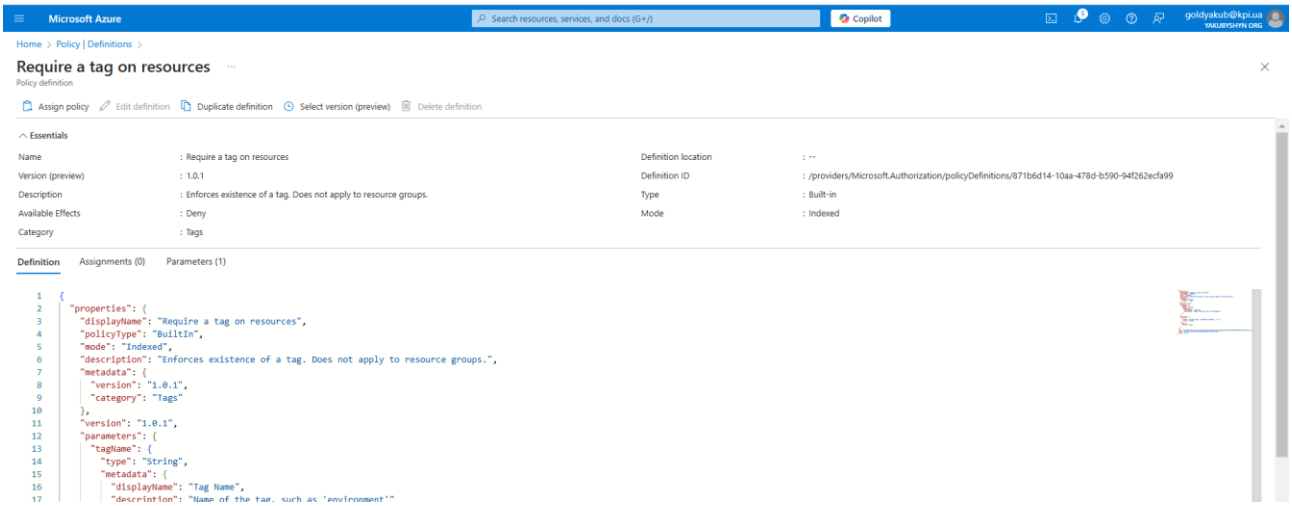
Admins even can’t list secrets

Practical Task 5: *Creating and Assigning Basic Azure Policies*

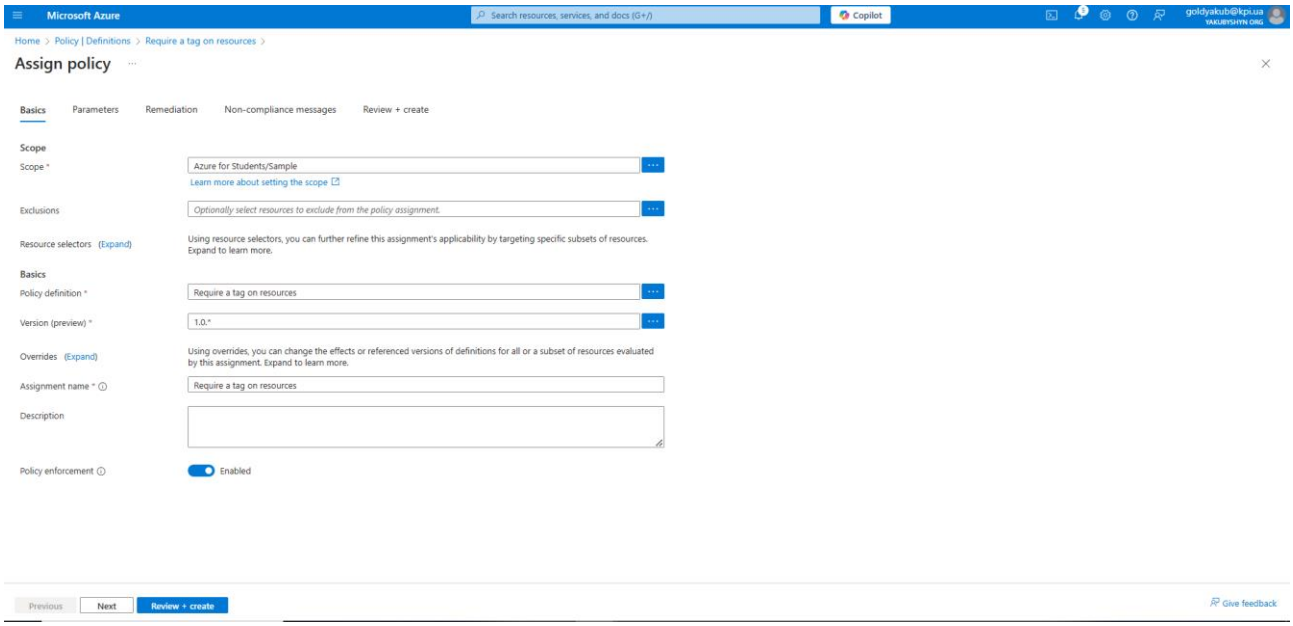
Define and assign Azure Policies to enforce compliance with organizational standards for resource management.

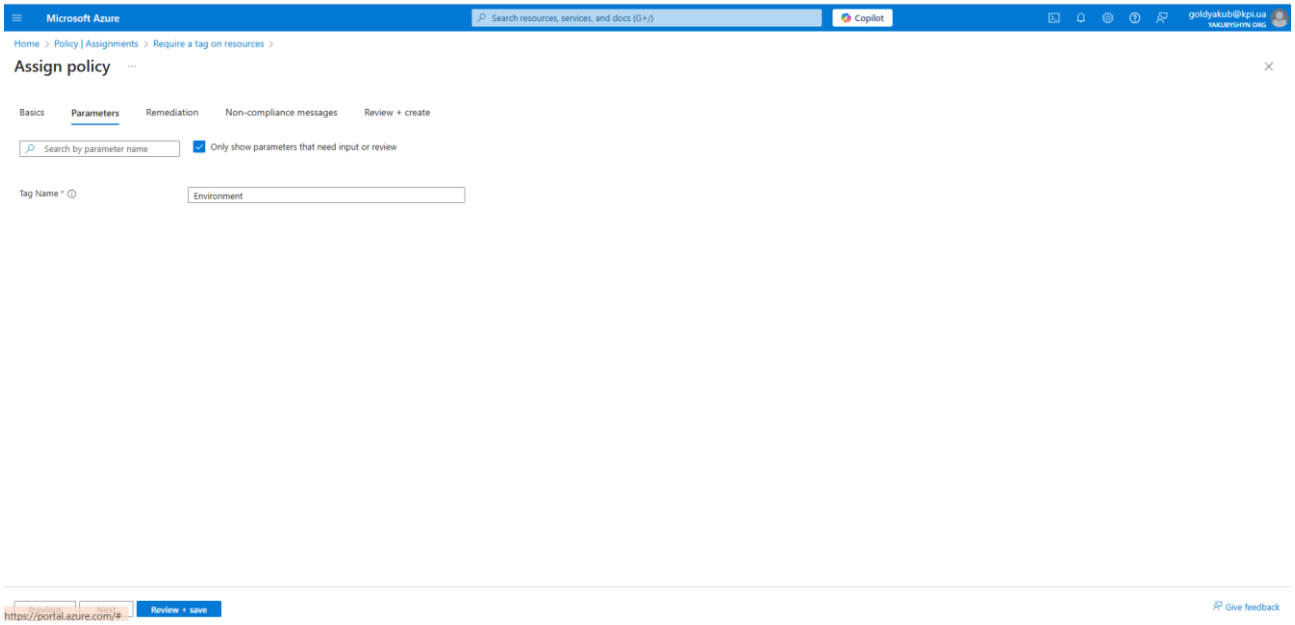
1. Create an Azure Policy to enforce tagging for all newly created resources with a specific tag (e.g., Environment: Development).

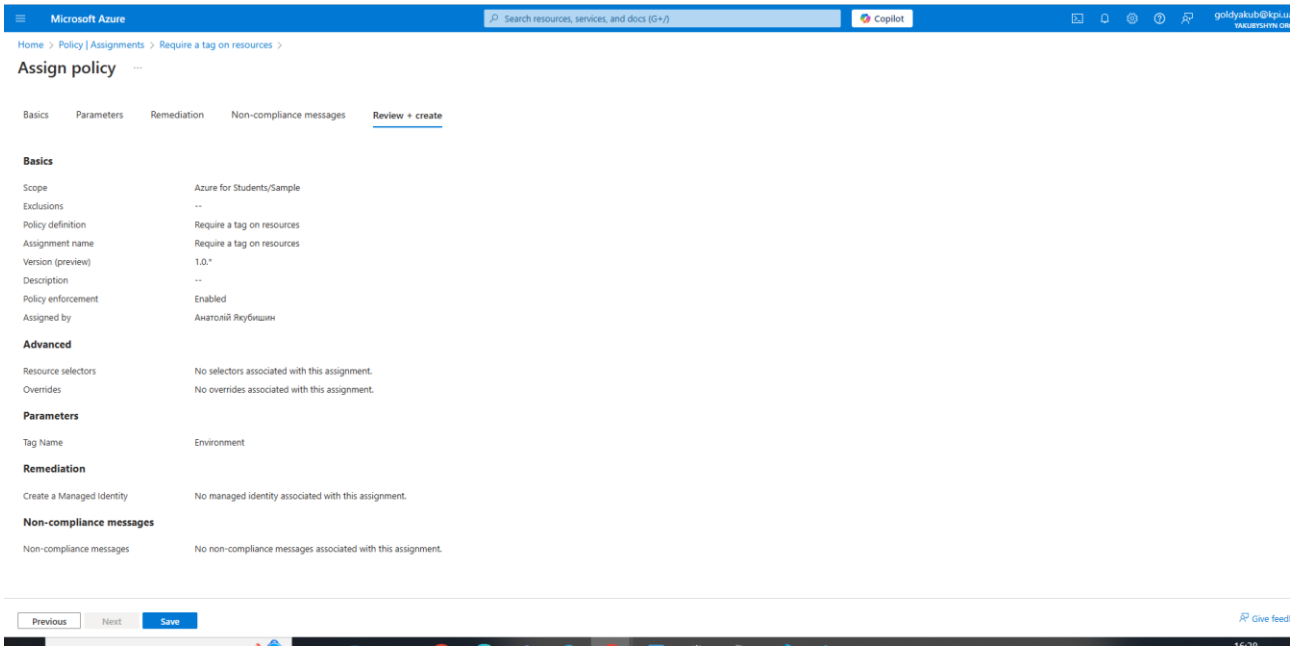


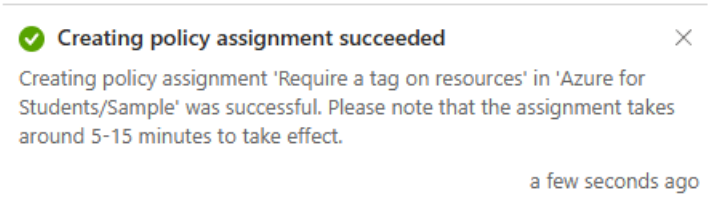


2. Assign the policy to a resource group.

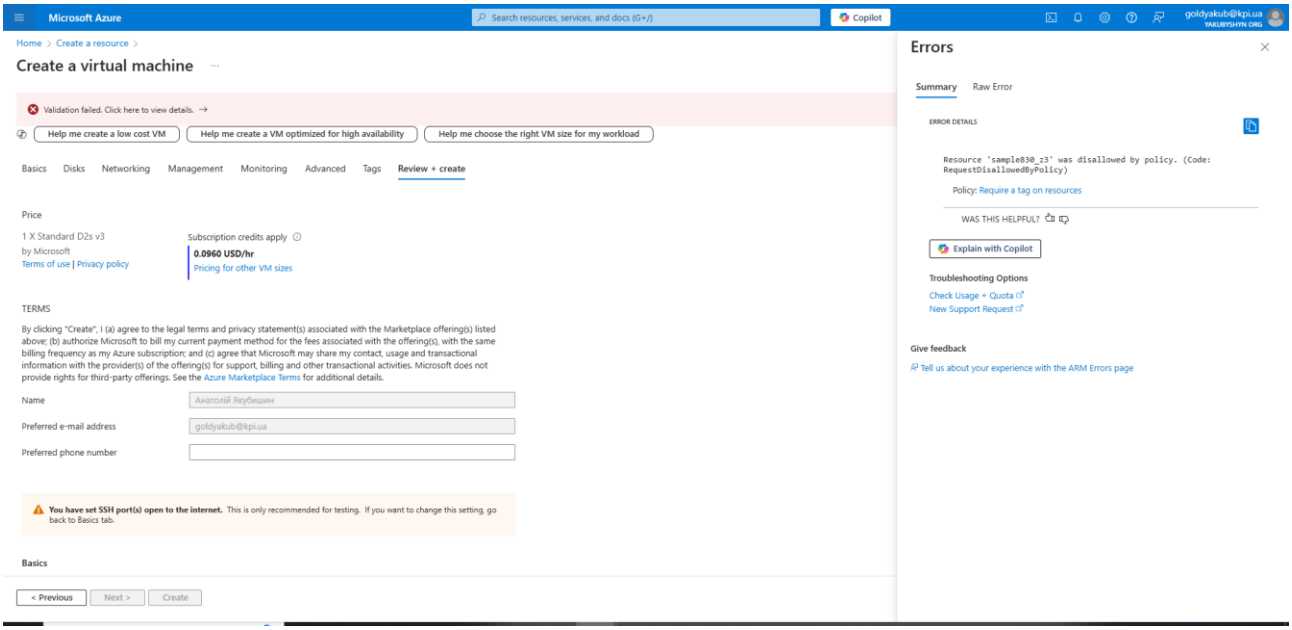


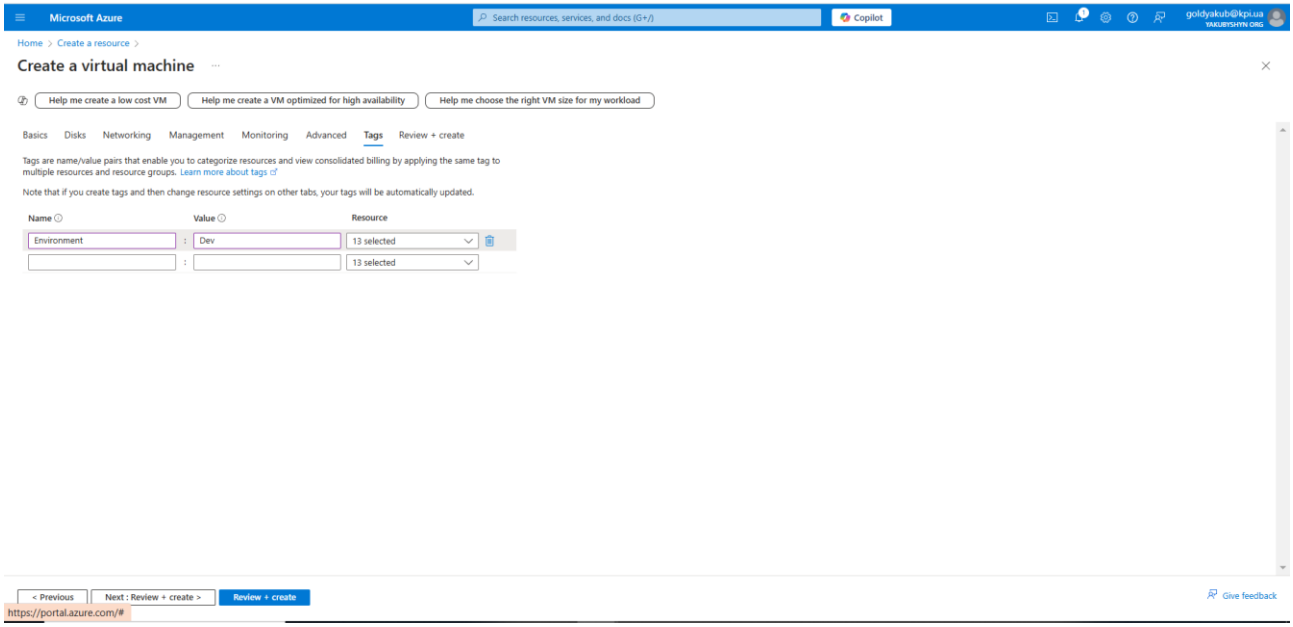



Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > Policy | Assignments > Require a tag on resources >
Assign policy
Basics
Parameters
Remediation
Non-compliance messages
Review + create
Basics
Scope
Azure for Students/Sample
Exclusions
--
Policy definition
Require a tag on resources
Assignment name
Require a tag on resources
Version (preview)
1.0.*
Description
--
Policy enforcement
Enabled
Assigned by
Анатолій Якубишин
Advanced
Resource selectors
No selectors associated with this assignment.
Overrides
No overrides associated with this assignment.
Parameters
Tag Name
Environment
Remediation
Create a Managed Identity
No managed identity associated with this assignment.
Non-compliance messages
Non-compliance messages
No non-compliance messages associated with this assignment.
Previous
Next
Save

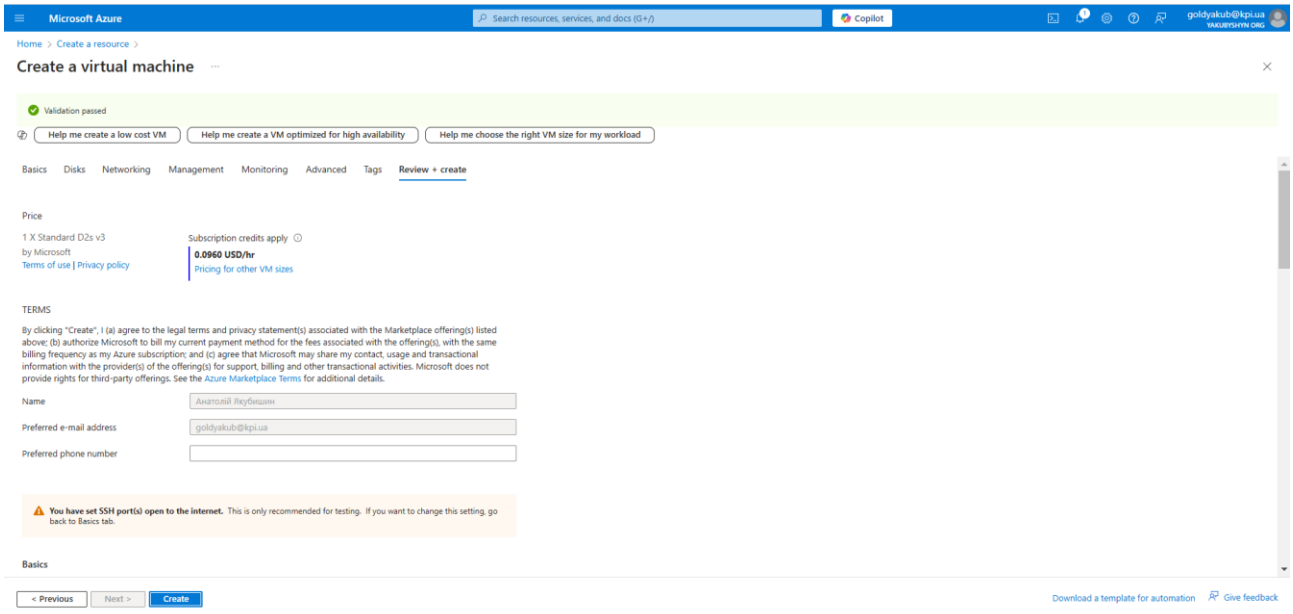

Creating policy assignment succeeded
Creating policy assignment 'Require a tag on resources' in 'Azure for Students/Sample' was successful. Please note that the assignment takes around 5-15 minutes to take effect.
a few seconds ago

3. Verify that any new resource created in the resource group without the required tag is marked as non-compliant.

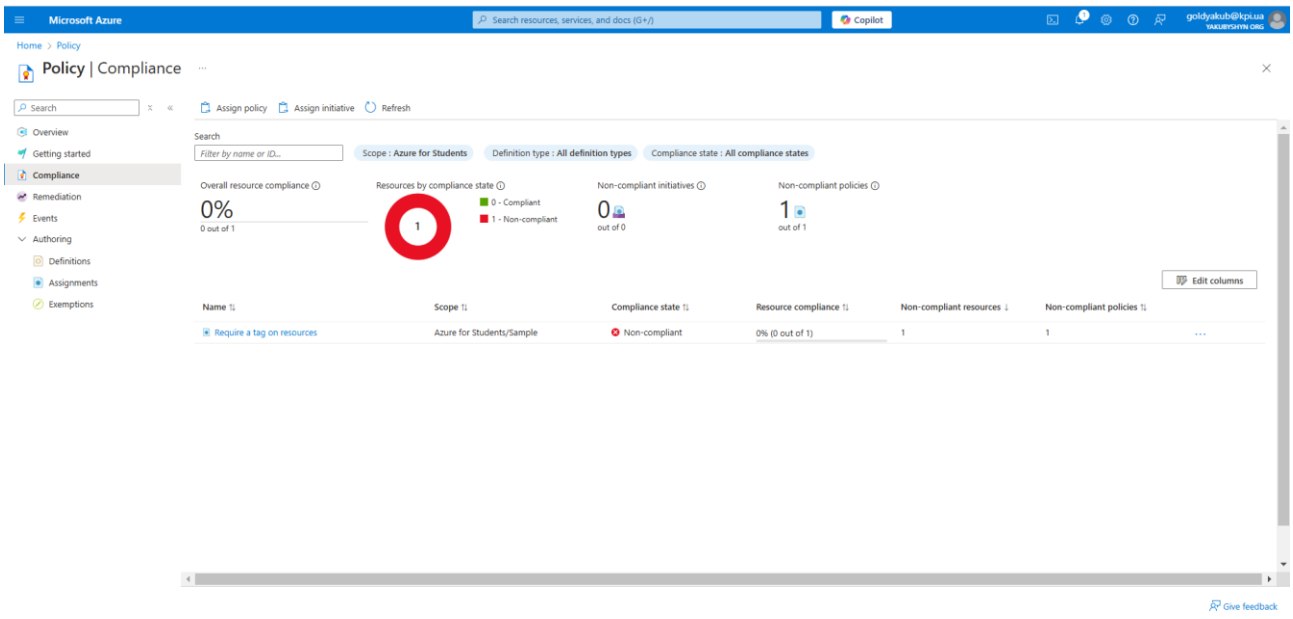


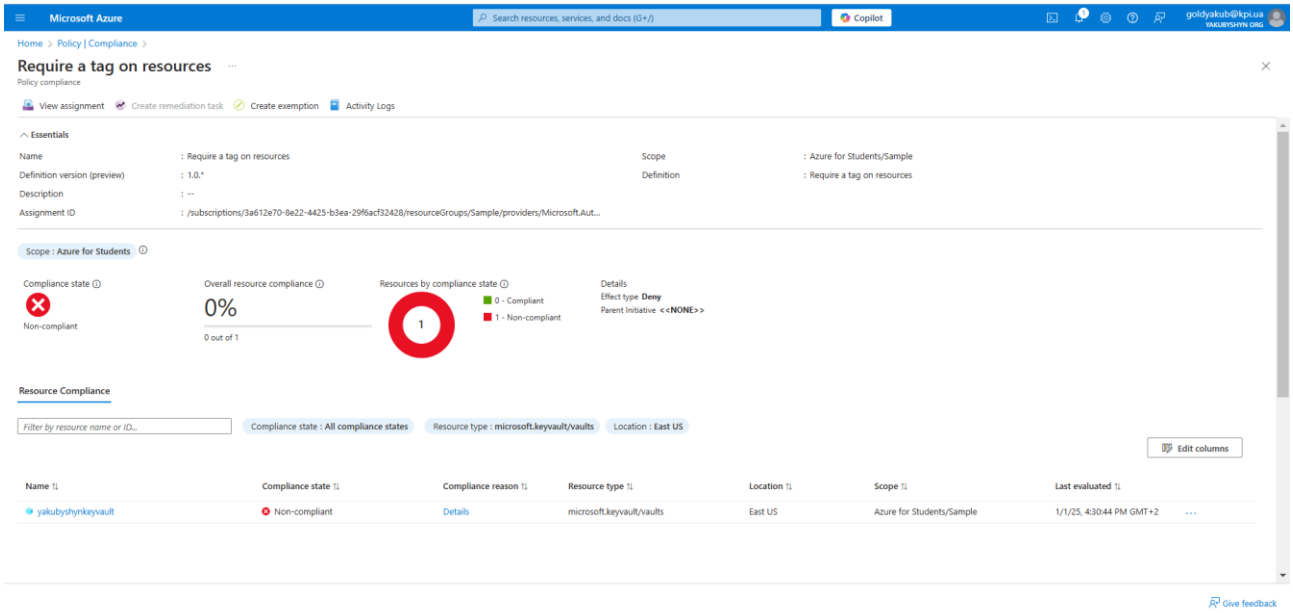


https://portal.azure.com/#



4. Review and document the compliance status of the resource group.



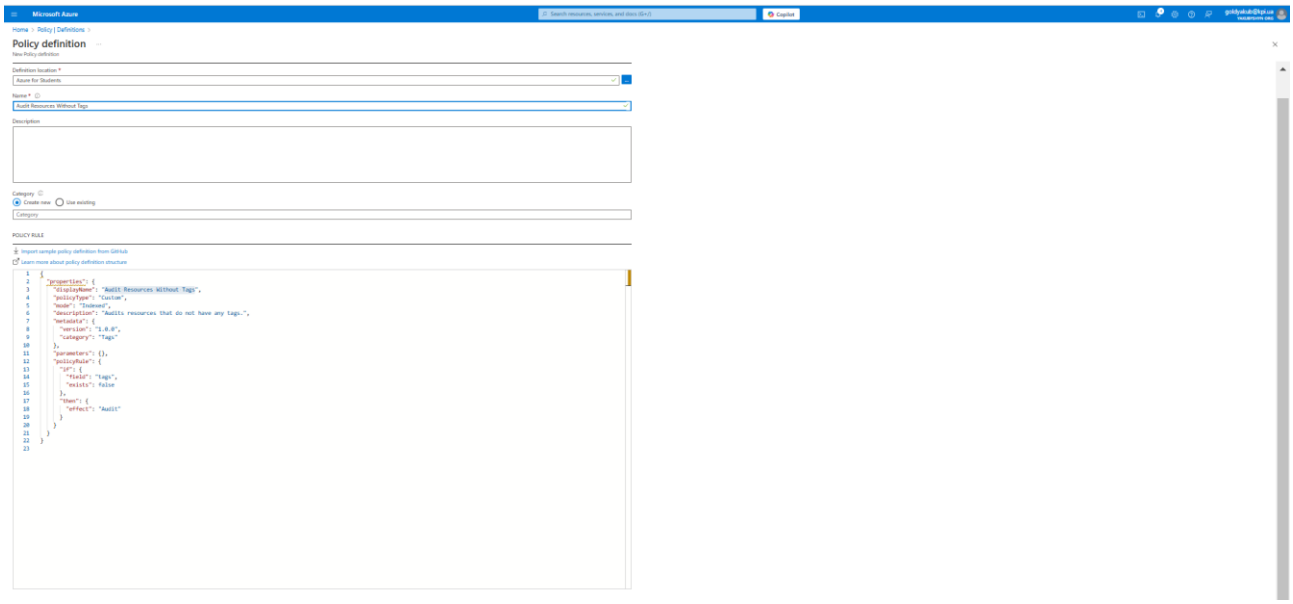


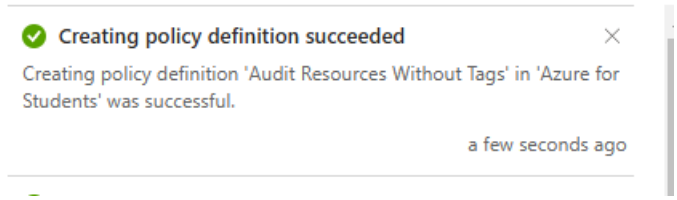
As expected (because was created before this policy)

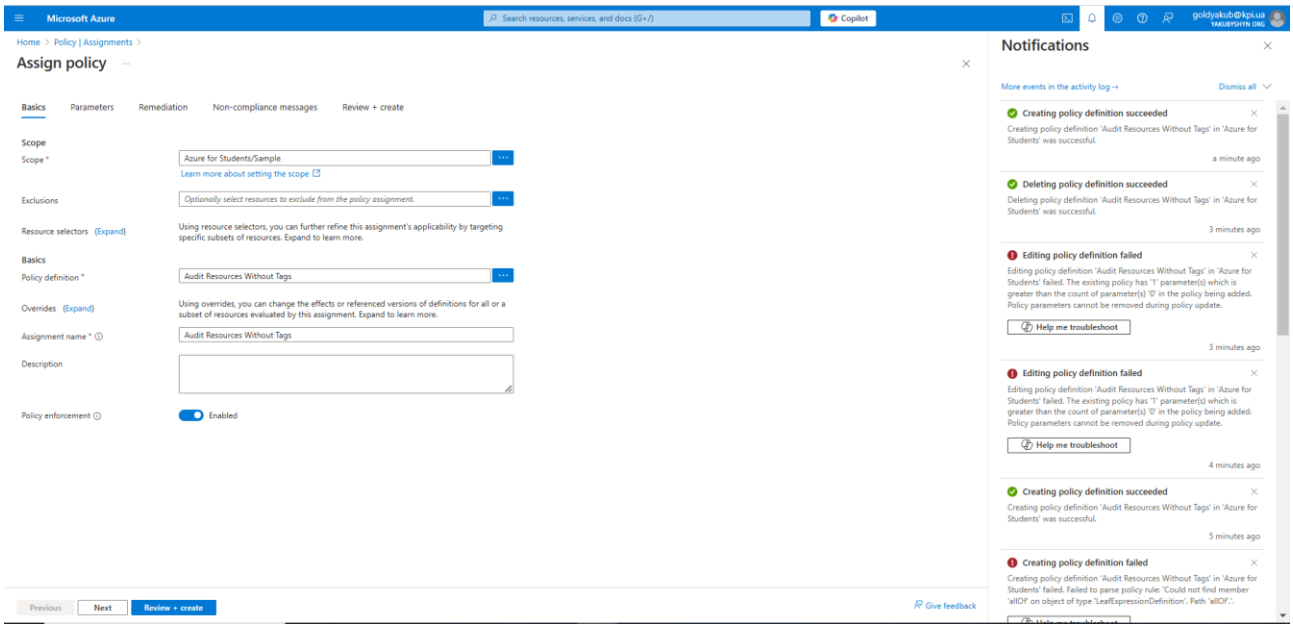
Practical Task 6: *Using Policy Effects to Enforce Compliance Configure Azure Policies with different policy effects to enforce compliance and manage resources according to organizational standards.*

1. Create a policy with the Audit effect to monitor and log untagged resources within a resource group.

```
{
  "properties": {
    "displayName": "Audit Resources Without Tags",
    "policyType": "Custom",
    "mode": "Indexed",
    "description": "Audits resources that do not have any tags.",
    "metadata": {
      "version": "1.0.0",
      "category": "Tags"
    },
    "parameters": {},
    "policyRule": {
      "if": {
        "field": "tags",
        "exists": false
      },
      "then": {
        "effect": "Audit"
      }
    }
  }
}
```

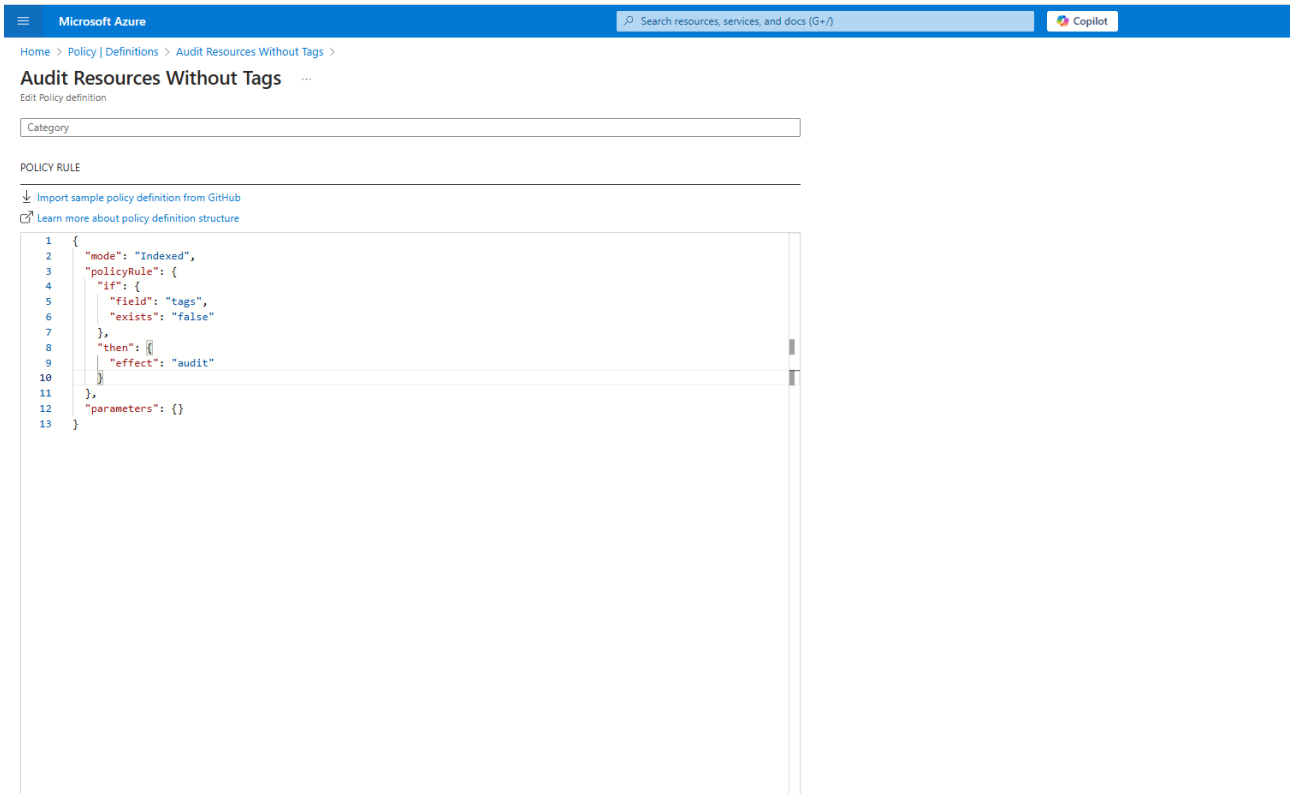






Review+create -> create

Made a mistake in policy definition



Corrected version

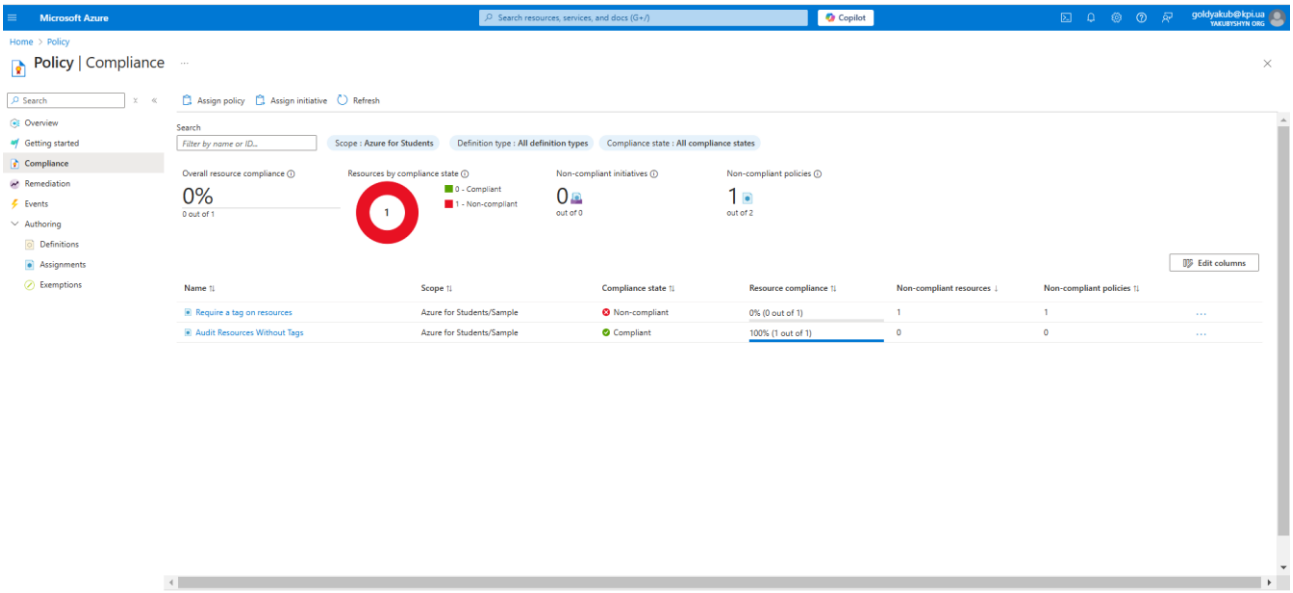
https://techcommunity.microsoft.com/discussions/azuregovernance/azure-policy---find-ressources-without-tags/3289179

changed exists “false” to exists “true” to see as non-complient

```
"policyRule": {
      "if": {
        "field": "tags",
        "exists": "true"
      },
      "then": {
        "effect": "audit"
      }
    },
    "versions": [
      "1.0.0"
    ]
  },
```

But then changed back because complient is expected status

IF paremeter exists is ‘false’



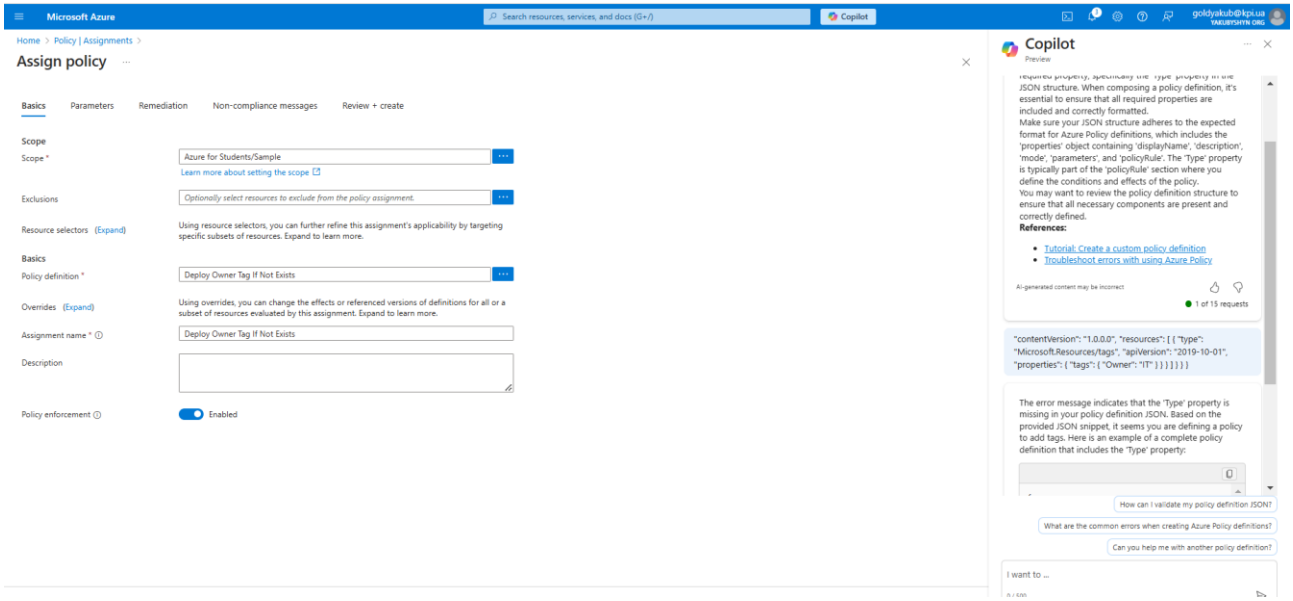
As a result (false) as it should be

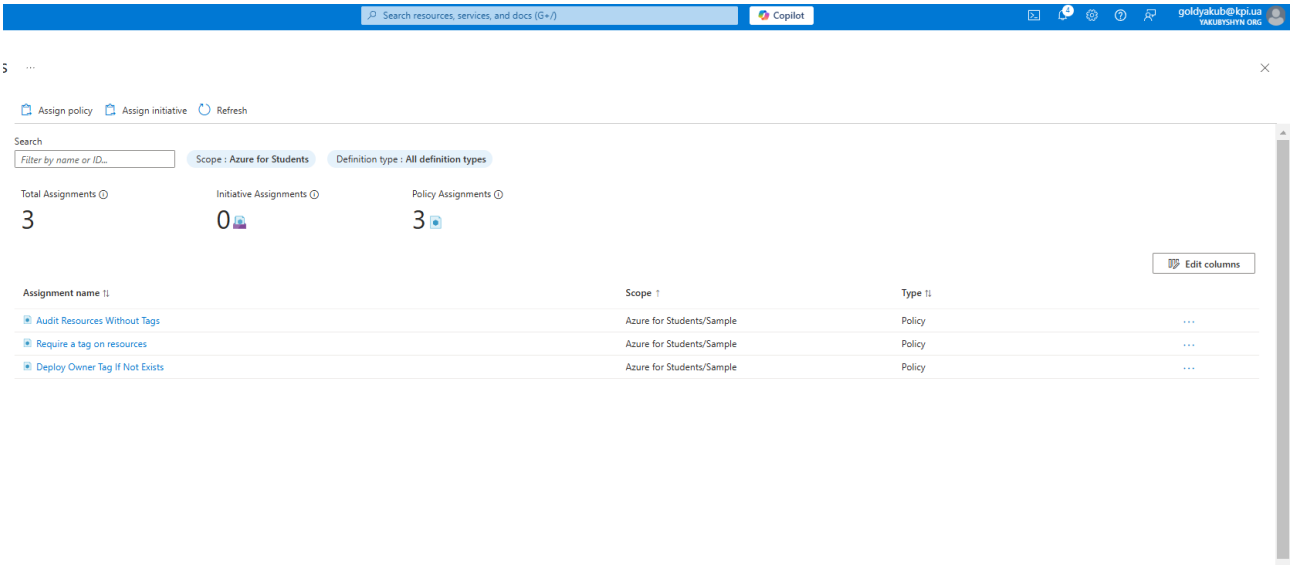
2. Create a policy with the DeployIfNotExists effect to automatically add a specific tag (Owner: IT) to any newly created resource.

```
{
  "mode": "Indexed",
  "policyRule": {
    "if": {
      "field": "tags.Owner",
      "exists": "false"
    },
```

```
    "then": {
      "effect": "deployIfNotExists",
      "details": {
        "type": "Microsoft.Resources/tags",
        "deployment": {
          "properties": {
            "mode": "Incremental",
            "template": {
              "$schema": "https://schema.management.azure.com/schemas/2019-04-
01/deploymentTemplate.json#",
              "contentVersion": "1.0.0.0",
              "resources": [
                {
                  "type": "Microsoft.Resources/tags",
                  "apiVersion": "2019-10-01",
                  "properties": {
                    "tags": {
                      "Owner": "IT"
                    }
                  }
                }
              ]
            }
          }
        }
      }
    },
    "parameters": {}
}
```

Then I assigned policy:





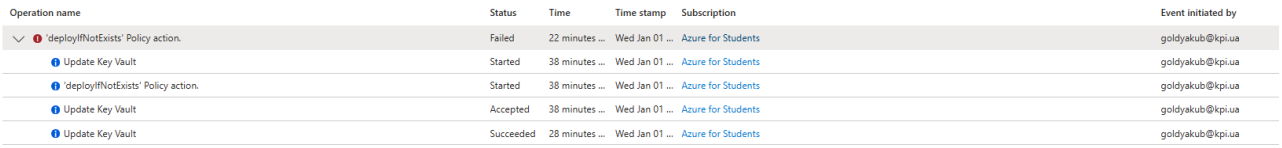
3. Assign these policies to a resource group and verify their behavior by:

   Creating a resource without a tag and checking the compliance logs.

   Creating a resource to validate the automatic tag deployment

(Created extra Azure Key Vaults)

It doesn't work



`. The request to retrieve resources of type 'Microsoft.Resources/tags' failed with HTTP status code`

I don't see `'Microsoft.Resources/tags'`

In my student subscription

It is possible to do this task using *modify effect*

https://learn.microsoft.com/en-us/azure/governance/policy/tutorials/govern-tags

```
{
  "mode": "Indexed",
  "policyRule": {
    "if": {
      "field": "tags.Owner",
```

```
      "exists": "false"
    },
    "then": {
      "effect": "modify",

      "details": {
         "roleDefinitionIds": [
        "/providers/microsoft.authorization/roleDefinitions/b24988ac-6180-42a0-
ab88-20f7382dd24c"
      ],
        "operations": [
          {
            "operation": "add",
            "field": "tags.Owner",
            "value": "IT"
          }
        ]
      }
    }
  },
  "parameters": {}
}
```

Assigned this policy

Created vault with name ‘TestingVaultTolia’

I haven’t added Owner tag. But it was added automatically.