

Név: Péter Bence Gábor

Neptun kód: X89O8X

Tantárgy: Korszerű hálózati alkalmazások

Fontos: Ügyeljen arra, hogy az elnevezésekben használja saját Neptun kódját azonosításra. Csak azok a képernyőképek fogadhatók el, amelyek **teljes képernyőről készülnek**, és a látható elnevezések közül **legalább egy tartalmazza a Neptun kódot**.

Feladatok:

1. Mutassa be szövegesen a Role-Based Access control működését. Mutasson be pár alapvető role-hoz tartozó jogosultságokat. Készítsen legalább három eltérő jogosultsági körrel rendelkező felhasználót és mutassa be a folyamatot képernyőképek segítségével.
2. Készítsen egy Azure Allowed Locations policy-t egy kiválasztott régióra. Dokumentálja a létrehozását és az eredményt képernyőképek segítségével.
3. Mutassa be szövegesen az Azure AD Privileged Identity Management működését. Hogyan kell konfigurálni ilyen felhasználókat? Mutassa be ezt a folyamatot képernyőképek segítségével.

1. Feladat:

A Role-Based Access Control (RBAC) egy olyan hozzáférés-kezelési modell, amely lehetővé teszi a felhasználók számára, hogy különböző jogosultságokkal rendelkezzenek a rendszerhez való hozzáféréshez. Az RBAC modell egy adatbázist és egy szabálykészletet használ a jogosultságok meghatározására.

Az RBAC modellben az egyes felhasználók különböző szerepkörökbe tartoznak, amelyek jogosultságokat határoznak meg a rendszerben való tevékenységeikhez. Az egyes szerepkörökhöz különböző jogosultságok vannak rendelve, és a felhasználók csak az adott szerepkör által meghatározott jogosultságokkal rendelkeznek.

Az RBAC modellben a felhasználók és a szerepkörök közötti kapcsolatot meghatározó szabálykészletet általában az adminisztrátorok állítják össze. Az adminisztrátorok hozzárendelhetik a felhasználókat az adott szerepkörökhöz, és módosíthatják a szerepkörök által meghatározott jogosultságokat.

Az RBAC modellben az egyes jogosultságokat általában műveletekhez vagy erőforrásokhoz kapcsolják, például a fájl megnyitása, az adatbázisban való keresés vagy az adminisztrátori beállítások módosítása. Az RBAC modell lehetővé teszi az adminisztrátorok számára, hogy finomhangolják a jogosultságokat, hogy a felhasználók csak a számukra szükséges erőforrásokhoz férjenek hozzá, és csak a számukra szükséges műveleteket végezhessek el.

Az RBAC modell előnyei közé tartozik az egyszerű kezelhetőség, a biztonságosabb hozzáférés-kezelés és az egységes hozzáférési irányítás. Az RBAC modell általában nagyobb rendszerekben alkalmazható, ahol a felhasználók száma és a rendszerhez való hozzáférési jogok bonyolultsága magas.

Workspaces Applications Apr 27 10:05 PM

Users - Microsoft Azure

Home Széchenyi István Egyetem | Users

Users

Search

+ New user Download users Bulk operations Refresh Manage view Delete Per-user MFA Preview features Got feedback?

Want to switch back to the legacy users list experience? Click here to leave the preview.

11,391 users found

Display name	User principal name	User type	On-premises sy...	Identities	Company name	Creation type
a.akos2000est	a.akos2000est@gmail.co...	Guest	No	MicrosoftAccount		Invitation
a.h.murtada	a.h.murtada@gmail.com#f...	Guest	No	laeaze.onmicrosoft.com		Invitation
A00271362	A00271362_student.at@e...	Guest	No	laeaze.onmicrosoft.com		Invitation
a00302948	a00302948_student.at@e...	Guest	No	laeaze.onmicrosoft.com		Invitation
a16302	a16302_akos@ca.p@EX...	Guest	No	laeaze.onmicrosoft.com		Invitation
Abdoh Adam Laido	abdoh.adam.laido@hallg...	Member	No	laeaze.onmicrosoft.com		
Abel Ester	abel.ester@hallgato.cse.hu	Member	No	laeaze.onmicrosoft.com		
Abbas Ameen	abbas.ameen@hallgato.s...	Member	No	laeaze.onmicrosoft.com		
Abdul Rahman Younes Al-Ditba	abdul.rahman.younes.al.d...	Member	No	laeaze.onmicrosoft.com		
Abdulmalik Kamila	abdulmalik.kamila@hallg...	Member	No	laeaze.onmicrosoft.com		
Abu Hasan Muhiham	abu.hasan.muhiham@hallg...	Member	No	laeaze.onmicrosoft.com		
Abonyi Balazs	abonyi.balazs@hallgato.s...	Member	No	laeaze.onmicrosoft.com		
Abonyi Györfő	abonyi.gyoszi@hallgato.s...	Member	No	laeaze.onmicrosoft.com		
Abonyi László	abonyi.laszlo@hallgato.s...	Member	No	laeaze.onmicrosoft.com		
Abonyi Reka Edit	abonyi.reka.edit@hallgat...	Member	No	laeaze.onmicrosoft.com		
Abou Saad Rastef	abou.saad.rafa@hallgat...	Member	No	laeaze.onmicrosoft.com		
Aboulagag Safwan	aboulagag.safwan@hal...	Member	No	laeaze.onmicrosoft.com		
Abraham Andree	abraham.andree@hallgat...	Member	No	laeaze.onmicrosoft.com		
Abraham Andree	abraham.andree@hallgat...	Member	No	laeaze.onmicrosoft.com		
Abraham Attia	abraham.attia@hallgato.s...	Member	No	laeaze.onmicrosoft.com		
Abraham Kitts	abraham.kitts@hallgato.s...	Member	No	laeaze.onmicrosoft.com		
Abraham Lilian Aliza	abraham.lilian.aliza@hallg...	Member	No	laeaze.onmicrosoft.com		
Abraham Mate	abraham.mate@hallgato.s...	Member	No	laeaze.onmicrosoft.com		
Abraham Parik	abraham.parik@hallgato.s...	Member	No	laeaze.onmicrosoft.com		
Abraham Peter	abraham.peter@hallgato.s...	Member	No	laeaze.onmicrosoft.com		
Abraham Rebeka	abraham.rebeka@hallgat...	Member	No	laeaze.onmicrosoft.com		
Abraham Tibor	abraham.tibor@hallgato.s...	Member	No	laeaze.onmicrosoft.com		
academics	academics_g@ca.p@EX...	Guest	No	laeaze.onmicrosoft.com		Invitation

Workspaces Applications Apr 27 10:09 PM

Create a tenant - Microsoft Azure

Home Széchenyi István Egyetem | Overview Manage tenants

Create a tenant

Azure Active Directory

Basics Configuration Review + create

Directory details

Configure your new directory

Organization name * X99GBX-org

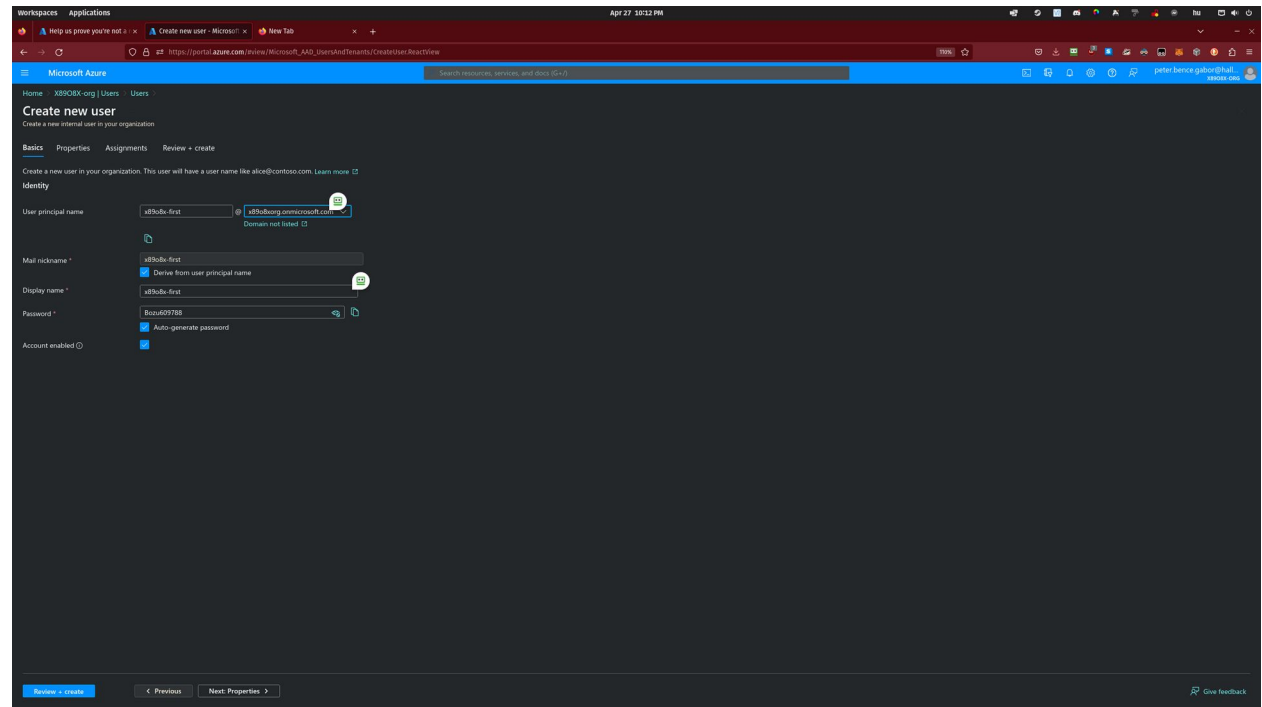
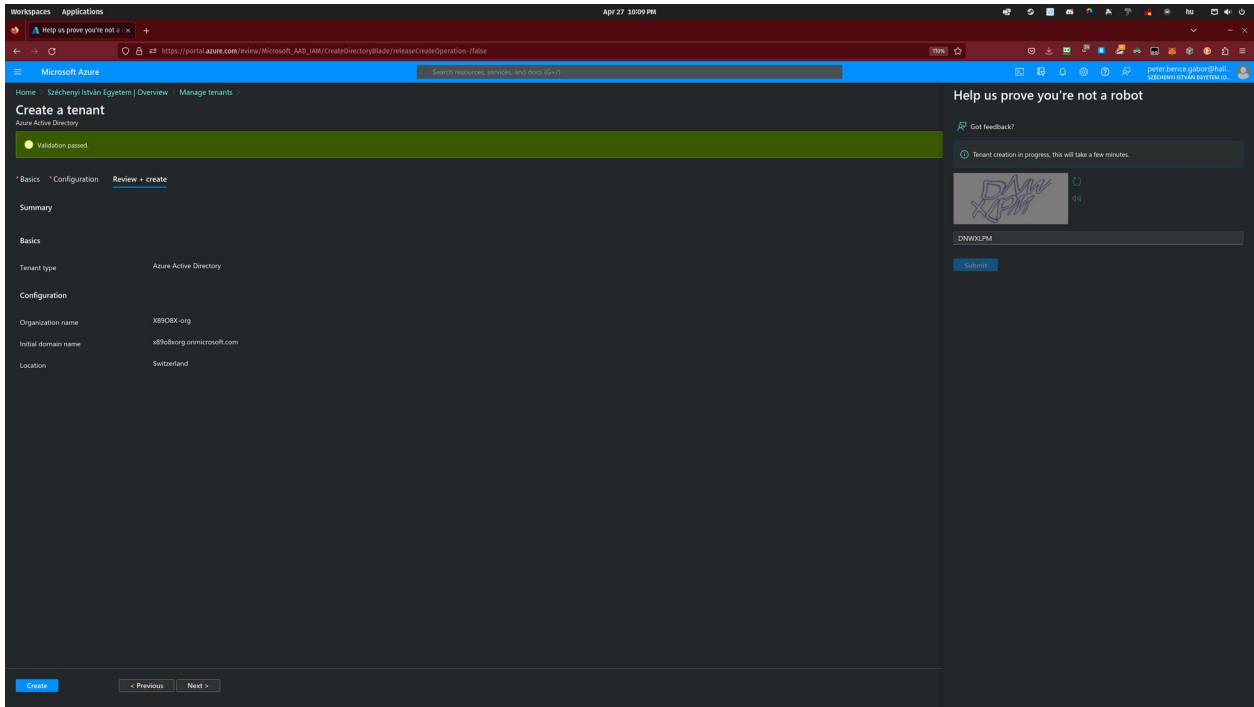
Initial domain name * x99b.org ✓

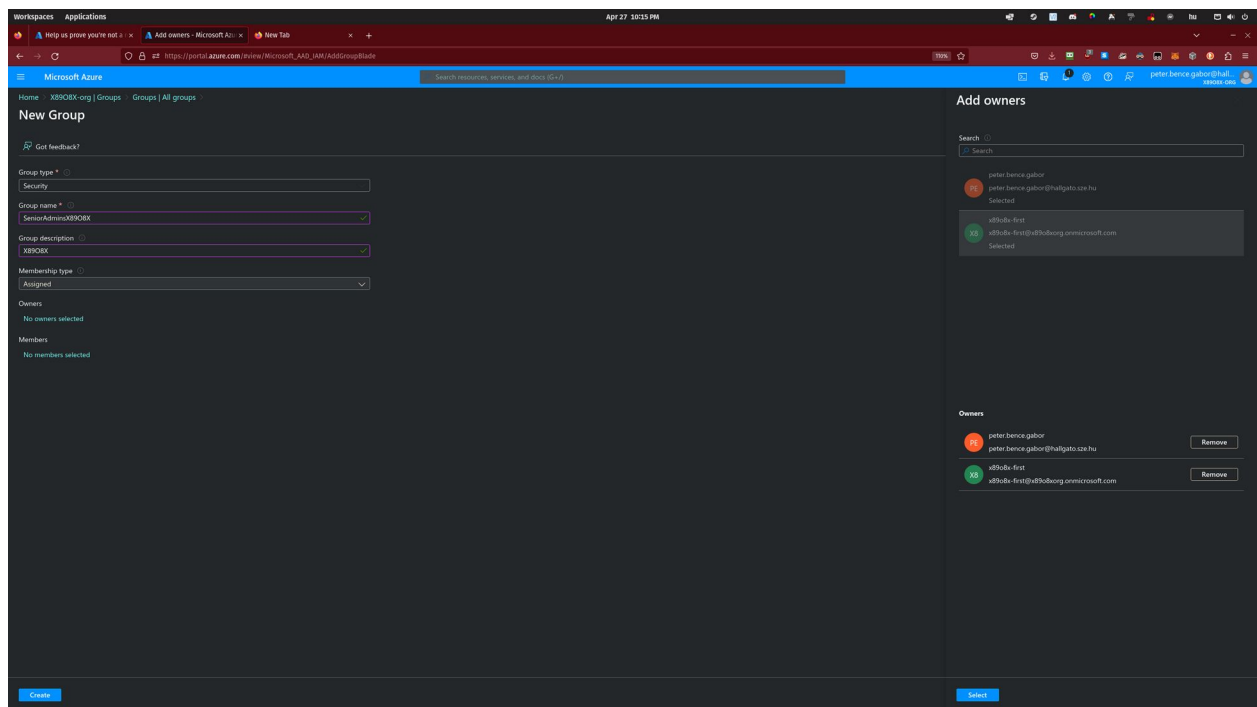
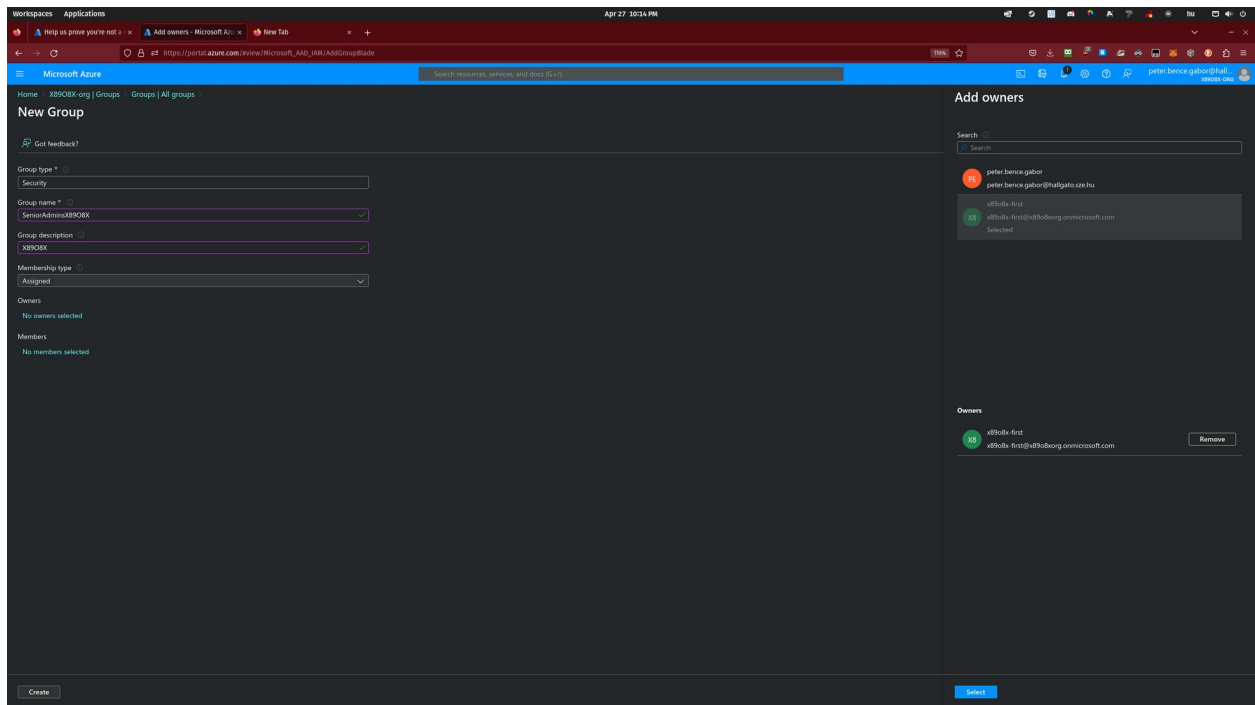
Location Switzerland

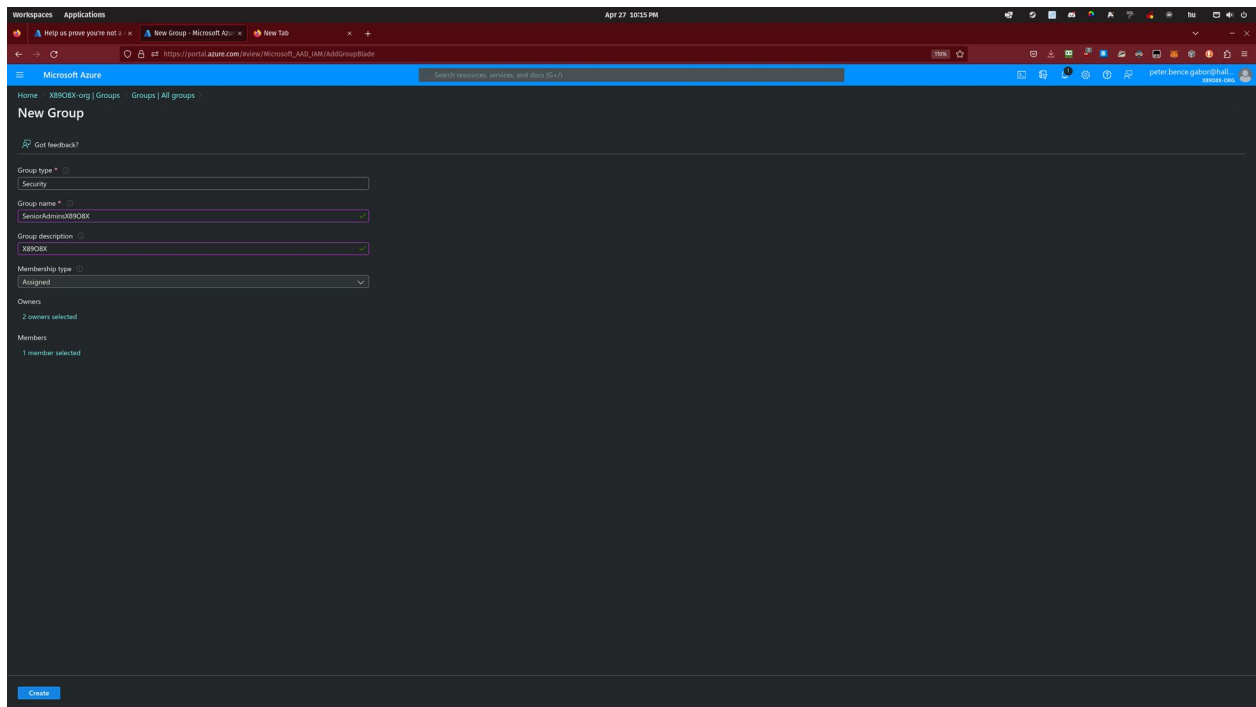
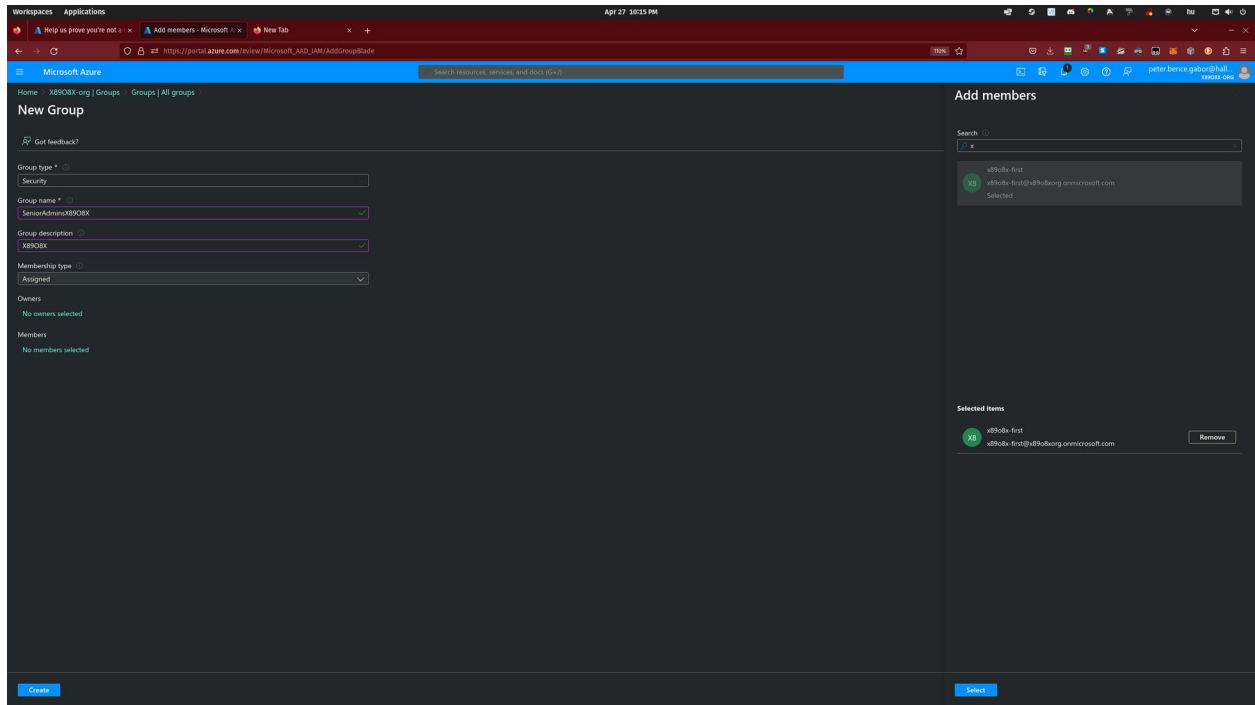
Geographic location: Europe

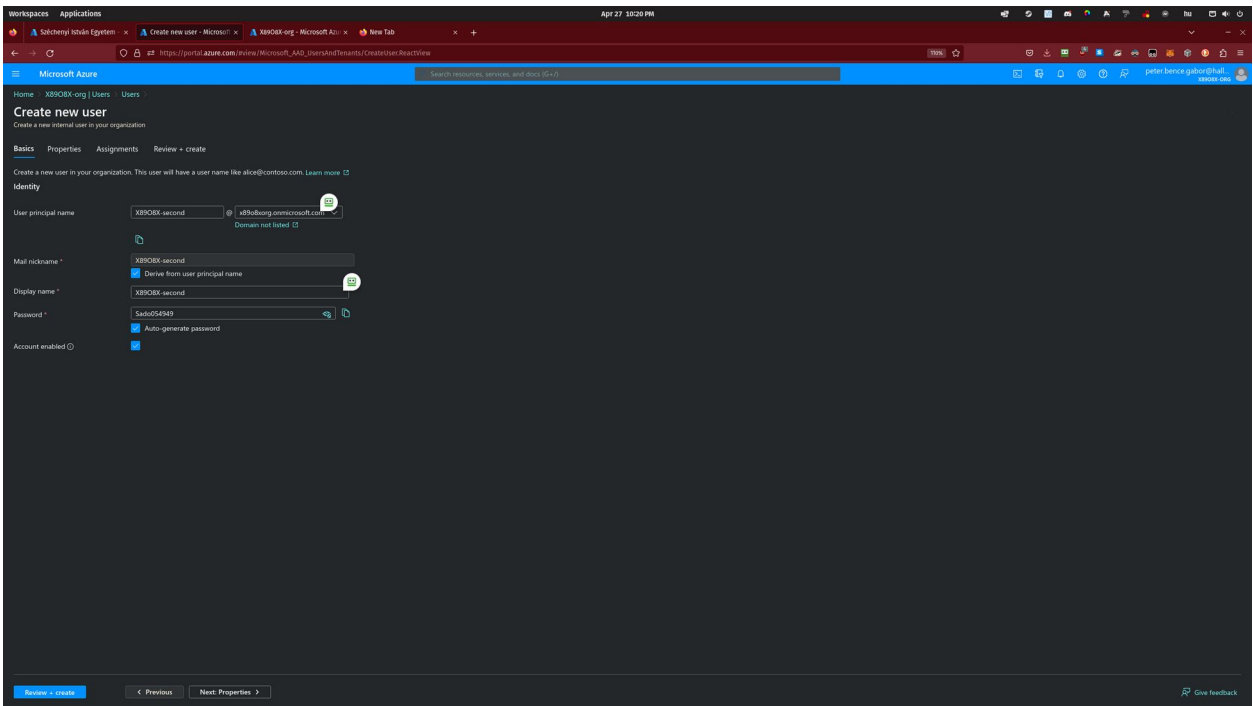
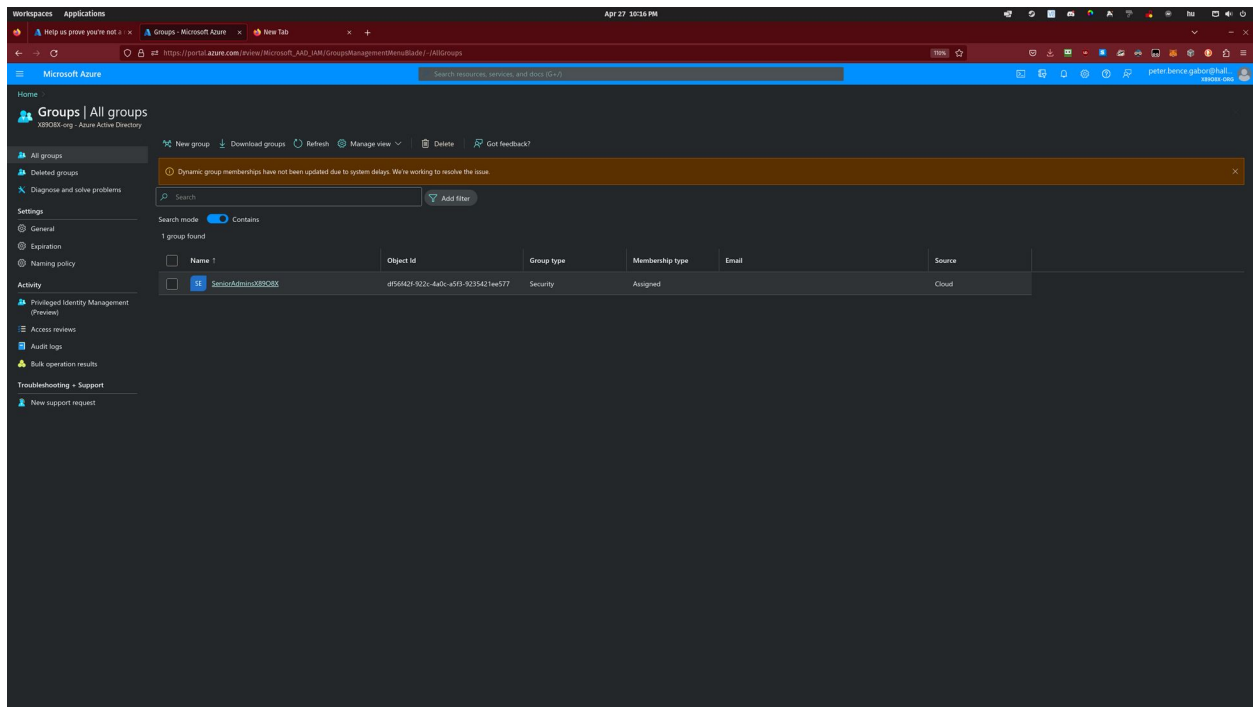
The location selected above will determine the geographic location where Azure Active Directory (Azure AD) will store your Core Store data only. To determine where Microsoft will store or process your Azure AD data, see Azure AD Data residency.

Review + create Previous Next Review + create









Workspaces Applications Apr 27 10:21 PM

Sikcheryi Ishan Egetem Users - Microsoft Azure XBOIX.org - Microsoft Azure New Tab

Microsoft Azure Search resources, services, and docs (Go)

Home XBOIX.org | Users

Users

Search

+ New user Download users Bulk operations Refresh Manage view Delete Per-user MFA Preview features Get feedback?

Want to switch back to the legacy users list experience? Click here to leave the preview.

Search Add filter

3 users found

<input type="checkbox"/>	Display name	User principal name	User type	On-premises ty...	Identities	Company name	Creation type
<input type="checkbox"/>	peter bence gabor	peter.bence.gabor_hallgat...	Member	No	ExternalAzureAD		
<input type="checkbox"/>	XB	xbludu-first@xbluduorg...	Member	No	xbluduorg.onmicrosoft.com		
<input type="checkbox"/>	XB	XBOIX-second@xbludu...	Member	No	xbluduorg.onmicrosoft.com		

Manage

- All users (preview)
- Audit logs
- Sign-in logs
- Diagnose and solve problems
- Deleted users (preview)
- Password reset
- User settings
- Bulk operation results
- Troubleshooting + Support
- New support request

https://portal.azure.com/blade/Microsoft_AAD_UsersAndTenants/UserProfileBlade?userId=7baa9e6c-5238-4e6d-9767-05c72e070228

Workspaces Application Apr 27 10:21 PM

Sikcheryi Ishan Egetem Add members - Microsoft Azure XBOIX.org - Microsoft Azure New Tab

Microsoft Azure Search resources, services, and docs (Go)

Home XBOIX.org | Groups Groups | All groups

New Group

Get feedback?

Group type * Security

Group name * JuniorAdminXBOIX

Group description JuniorAdminXBOIX

Membership type Assigned

Owners

No owners selected

Members

No members selected

Add members

Search

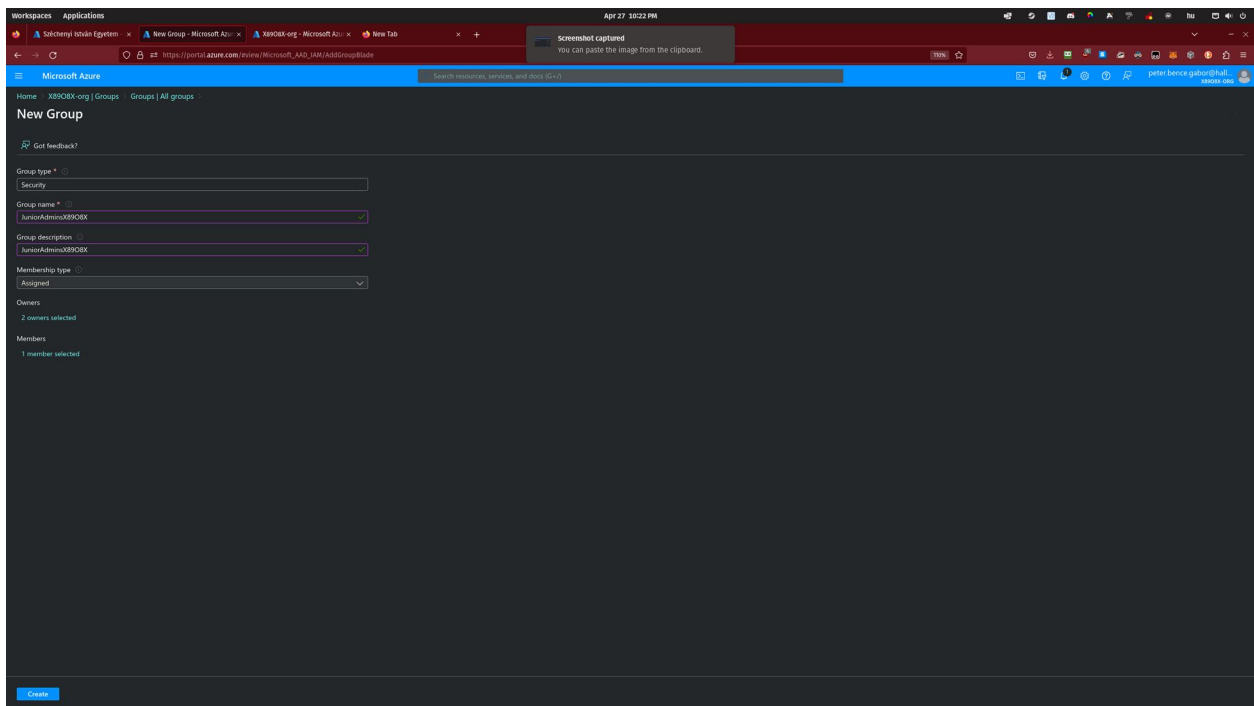
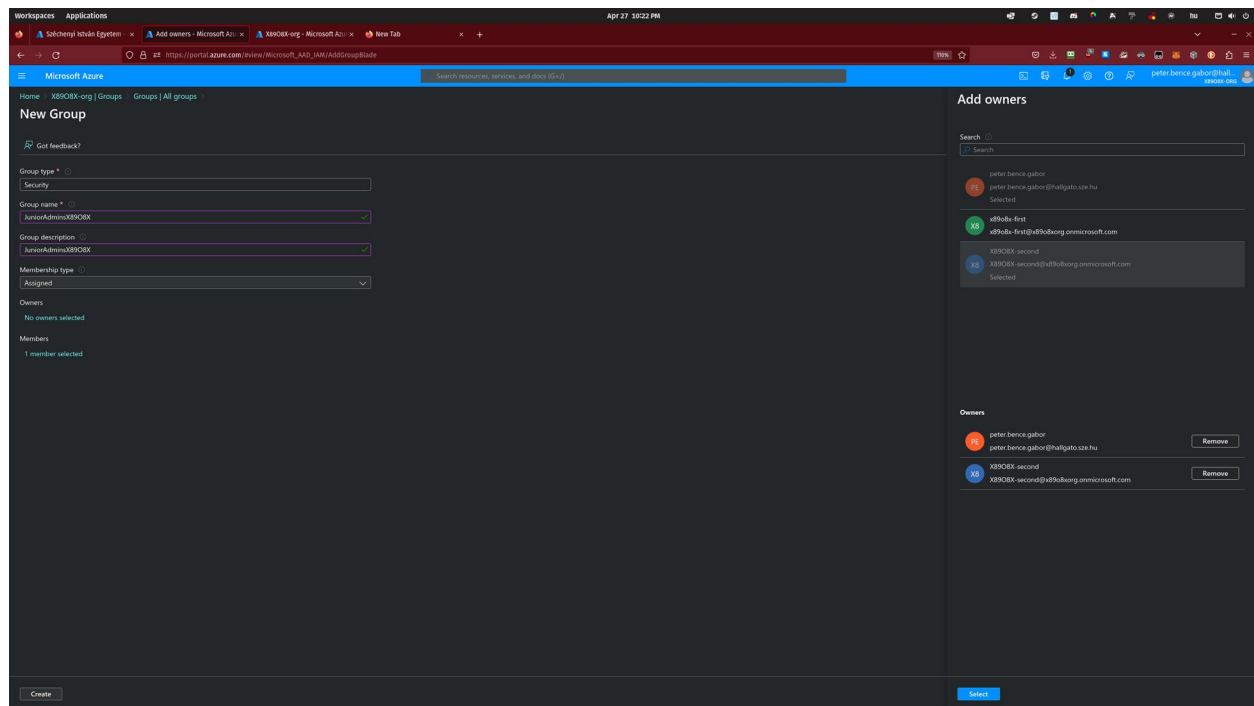
XB

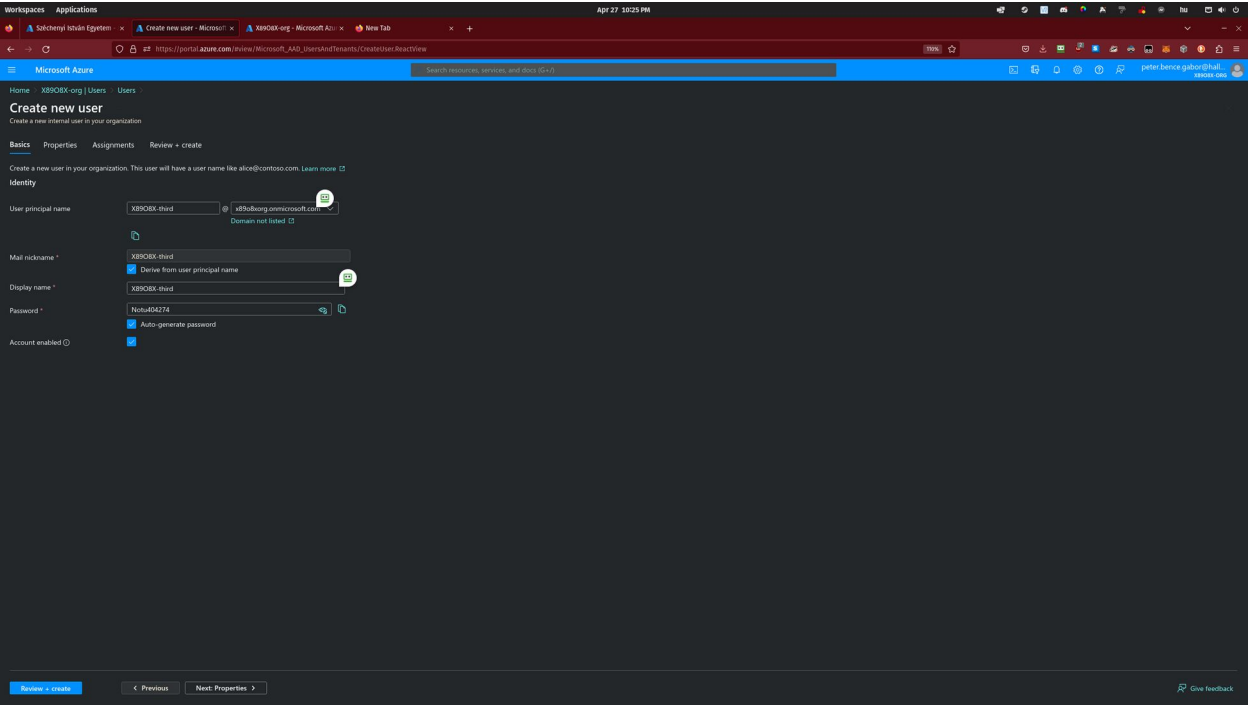
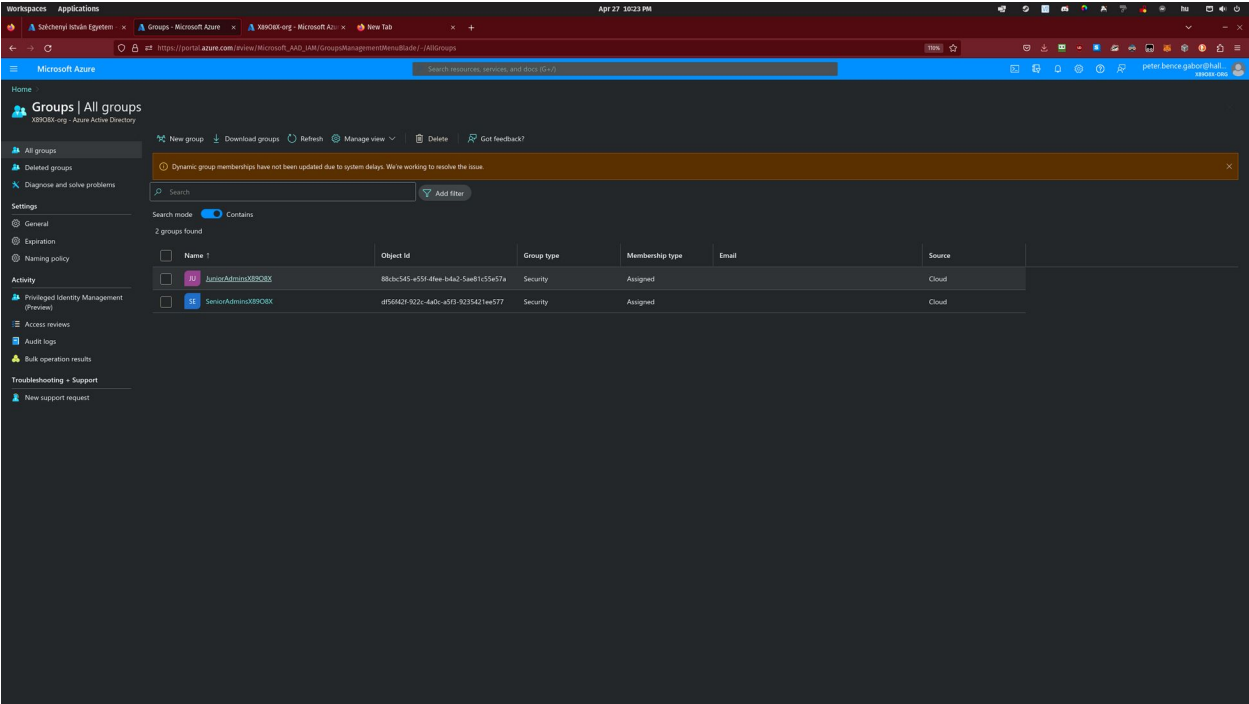
- SeniorAdminXBOIX
- xbludu-first
- xbludu-first@xbluduorg.onmicrosoft.com
- XBOIX-second
- XBOIX-second@xbluduorg.onmicrosoft.com

Selected items

- XBOIX-second
- XBOIX-second@xbluduorg.onmicrosoft.com

Create Select





WorkspacesApplications

Apr 27 10:26 PM

Szűchenyi István Egyetem xCreate new user - Microsoft Azure xXB9OEX-org - Microsoft Azure xNew Tab x

https://portal.azure.com/enlive/Microsoft_AAD_UsersAndGroups/Groups/ReactView

Microsoft Azure

Search resources, services, and docs (Ctrl+K)

Home > XB9OEX-org | Users > Users

Create new user

Create a new internal user in your organization

BasicsPropertiesAssignmentsReview + create

Basics

User principal nameXB9OEX-third@b9b9org.onmicrosoft.com

Display nameXB9OEX-third

Mail nicknameXB9OEX-third

PasswordNaduA0A2T4

Account enabledYes

Properties

User typeMember

Assignments

Administrative units

Groups

Roles

Create< PreviousNext >

Give feedback

Save to RoboForm?

Report an issue

AzureXB9OEX-third

Never for this siteNot NowSave

WorkspacesApplications

Apr 27 10:26 PM

Szűchenyi István Egyetem xNew Group - Microsoft Azure xXB9OEX-org - Microsoft Azure xNew Tab x

https://portal.azure.com/enlive/Microsoft_AAD_UsersAndGroups/Groups

Microsoft Azure

Search resources, services, and docs (Ctrl+K)

Home > XB9OEX-org | Groups > Groups | All groups

New Group

Get feedback?

Group type *Microsoft 365

Group name *ServiceDeskXB9OEX

Group email address *ServiceDeskXB9OEX

Group descriptionServiceDesk

Membership typeAssigned

☒ Use group sensitivity labels in Azure Active Directory to classify and protect Microsoft 365 groups. [Learn more about assigning sensitivity labels in AAD.](#)

Owners

No owners selected

Members

No members selected

Create

Workspaces Applications Apr 27 10:28 PM

ServiceDeskX8908X | Members

Overview

Manage

Properties

Members

Owners

Roles and administrators

Administrative units

Group memberships

Applications

Licenses

Azure role assignments

Activity

Privileged Identity Management (Preview)

Access reviews

Audit logs

Bulk operation results

Troubleshooting + Support

New support request

Direct members All members

Search by name

Add filters

Name	Type	Email
No members have been found		

Add members

Search

Search

peter.bence.gabor
peter.bence.gabor@talgato.sze.hu

XB
xb@bdc-1st@bdc.org.onmicrosoft.com

XB
XB@BDC-second@bdc.org.onmicrosoft.com

XB
XB@BDC-third@bdc.org.onmicrosoft.com

Selected items

XB
XB@BDC-third@bdc.org.onmicrosoft.com

Remove

Select

Workspaces Applications Apr 27 10:29 PM

ServiceDeskX8908X | Members

Overview

Manage

Properties

Members

Owners

Roles and administrators

Administrative units

Group memberships

Applications

Licenses

Azure role assignments

Activity

Privileged Identity Management (Preview)

Access reviews

Audit logs

Bulk operation results

Troubleshooting + Support

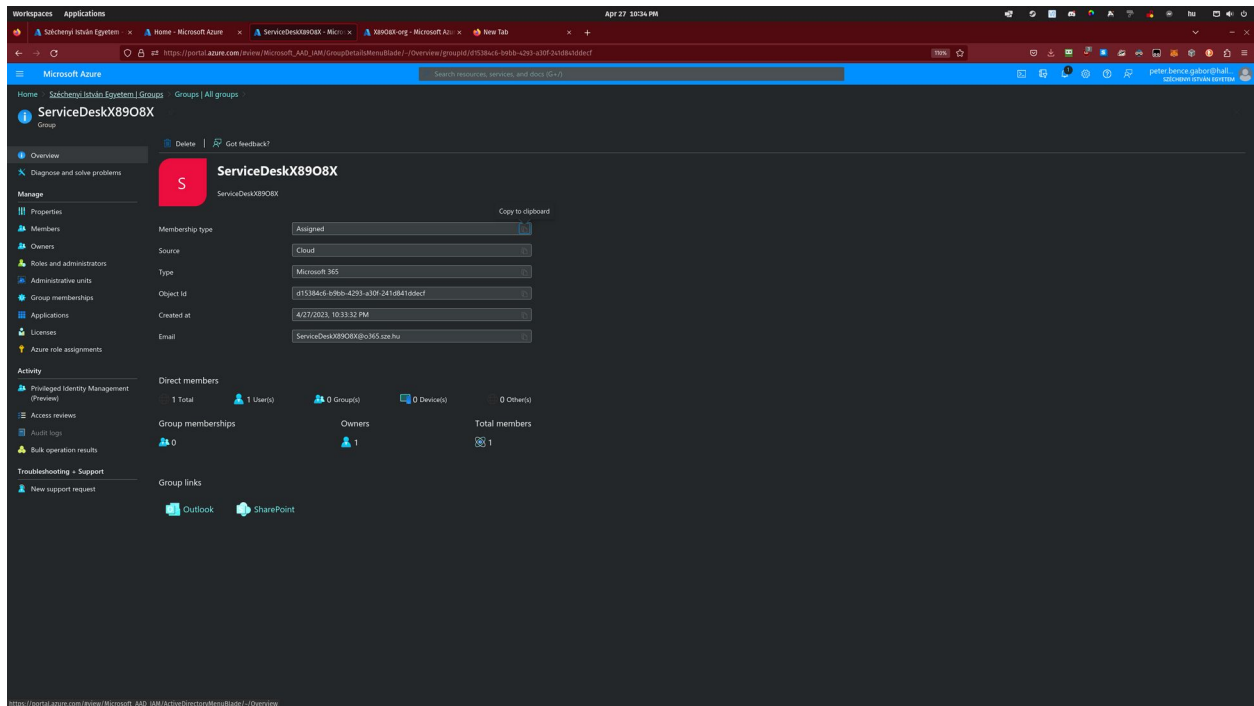
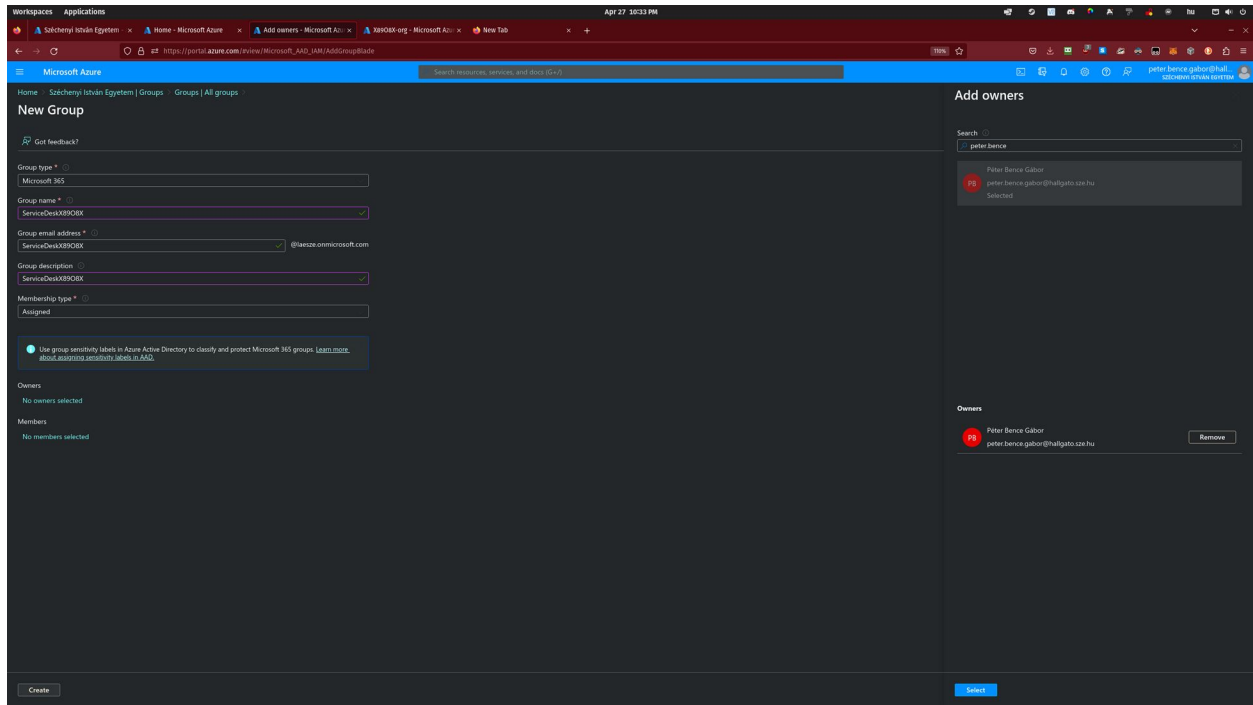
New support request

Direct members All members

Search by name

Add filters

Name	Type	Email	User type
XB XB@BDC-third	User		Member



WorkspacesApplications

Apr 27 10:36 PM

Home - Resource groups - AZLAB_X86X86 | Access control (IAM)

Search resources, services, and docs (Ctrl)

100%

petre.sereja.gabur@full-stechenyl-stvlas.ro

Add role assignment

RoleMembersReview + assign

A role definition is a collection of permissions. You can use the built-in roles or you can create your own custom roles. Learn more

Search by role name, description, or IDType: AllCategory: AllAssignment type: All

Name	Description	Privileged	Type	Category	Details
Owner	Grants full access to manage all resources, including the ability to assign roles in Azure RBAC.	Privileged	Built-in role	General	View
Contributor	Grants full access to manage all resources, but does not allow you to assign roles in Azure RBAC, manage assignments in Azure Blueprints, or share image galleries.	Privileged	Built-in role	General	View
Reader	View all resources, but does not allow you to make any changes.		Built-in role	General	View
Access Review Operator Service Role	Lets you grant Access Review System app permissions to discover and revoke access as needed by the access review process.		Built-in role	None	View
AcrDelete	acr delete		Built-in role	Containers	View
AcrImageSigner	acr image signer		Built-in role	Containers	View
AcrPull	acr pull		Built-in role	Containers	View
AcrPush	acr push		Built-in role	Containers	View
AcrQuarantineReader	acr quarantine data reader		Built-in role	Containers	View
AcrQuarantineWriter	acr quarantine data writer		Built-in role	Containers	View
AgFood Platform Sensor Partner Contributor	Provides contribute access to manage sensor related entities in AgFood Platform Service		Built-in role	None	View
AgFood Platform Service Admin	Provides admin access to AgFood Platform Service		Built-in role	AI + Machine Learning	View
AgFood Platform Service Contributor	Provides contribute access to AgFood Platform Service		Built-in role	AI + Machine Learning	View
AgFood Platform Service Reader	Provides read access to AgFood Platform Service		Built-in role	AI + Machine Learning	View
AnyBuild Builder	Basic user role for AnyBuild. This role allows listing of agent information and execution of remote build capabilities.		Built-in role	None	View
API Management Developer Portal Content Editor	Can customize the developer portal, edit its content, and publish it.		Built-in role	None	View
API Management Service Contributor	Can manage service and the APIs		Built-in role	Integration	View
API Management Service Operator Role	Can manage service but not the APIs		Built-in role	Integration	View
API Management Service Reader Role	Read-only access to service and APIs		Built-in role	Integration	View
API Management Service Workspace API Developer	Has read access to tags and products and write access to allow assigning APIs to products, assigning tags to products and APIs. This role should be assigned on the service scope.		Built-in role	None	View
API Management Service Workspace API Developer Manager	Has the same access as API Management Service Workspace API Developer as well as read access to users and write access to allow assigning users to groups. This role should be assigned on th...		Built-in role	None	View
API Management Workspace API Developer	Has read access to entities in the workspace and read and write access to entities for editing APIs. This role should be assigned on the workspace scope.		Built-in role	None	View
API Management Workspace API Product Manager	Has read access to entities in the workspace and read and write access to entities for publishing APIs. This role should be assigned on the workspace scope.		Built-in role	None	View
API Management Workspace Contributor	Can manage the workspace and view, but not modify its members. This role should be assigned on the workspace scope.		Built-in role	None	View
API Management Workspace Reader	Has read-only access to entities in the workspace. This role should be assigned on the workspace scope.		Built-in role	None	View
App Compliance Automation Administrator	App Compliance Automation Administrator Role		Built-in role	None	View
App Compliance Automation Developer	App Compliance Automation Developer Role		Built-in role	None	View

Review + assignPreviousNext

Feedback

WorkspacesApplications

Apr 27 10:36 PM

Home - Resource groups - AZLAB_X86X86 | Access control (IAM)

Search resources, services, and docs (Ctrl)

100%

petre.sereja.gabur@full-stechenyl-stvlas.ro

Add role assignment

RoleMembersReview + assign

A role definition is a collection of permissions. You can use the built-in roles or you can create your own custom roles. Learn more

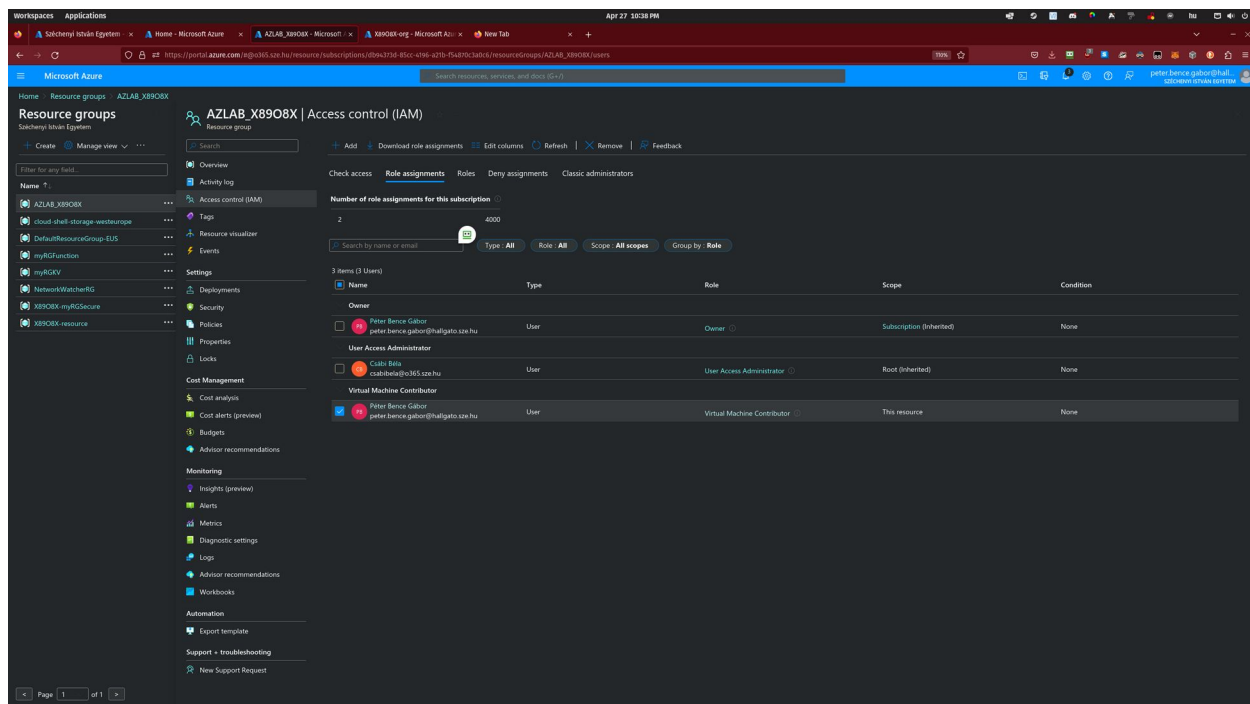
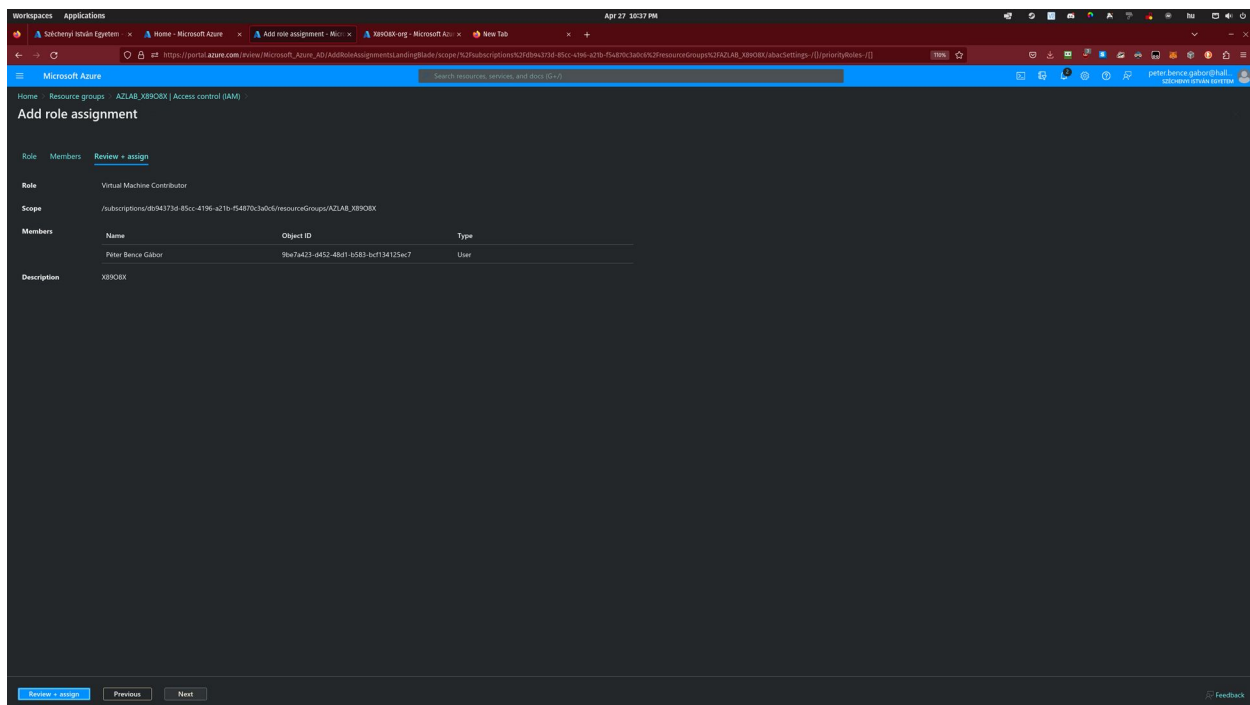
Virtual Machine ConType: AllCategory: AllAssignment type: All

Name	Description	Privileged	Type	Category	Details
Classic Virtual Machine Contributor	Lets you manage classic virtual machines, but not access to them, and not the virtual network or storage account they're connected to.		Built-in role	Compute	View
Desktop Virtualization Power On Contributor	This role is in preview and subject to change. Provide permission to the Azure Virtual Desktop Resource Provider to start virtual machines.		Built-in role	None	View
Desktop Virtualization Power On Off Contributor	This role is in preview and subject to change. Provide permission to the Azure Virtual Desktop Resource Provider to start and stop virtual machines.		Built-in role	None	View
Desktop Virtualization Virtual Machine Contributor	This role is in preview and subject to change. Provide permission to the Azure Virtual Desktop Resource Provider to create, delete, update, start, and stop virtual machines.		Built-in role	None	View
DevTest Lets User	Lets you connect, start, restart, and shutdown your virtual machines in your Azure DevTest Labs.		Built-in role	DevOps	View
Virtual Machine Contributor	Lets you manage virtual machines, but not access to them, and not the virtual network or storage account they're connected to.		Built-in role	Compute	View
Virtual Machine Local User Login	View Virtual Machines in the portal and login as a local user configured on the acs server		Built-in role	None	View
Windows365NetworkInterfaceContributor	Create NICs and join it to virtual machine in another tenant. This role is used in Windows365 scenarios.		Built-in role	None	View

< PreviousPage 1 of 1Next >

Review + assignPreviousNext

Feedback



Workspaces Applications Apr 27 10:38 PM

Home Resource groups AZLAB_X8908X

Resource groups

Sakcheryi Ishán Egiyem

Create Manage view

Filter for any field:

- AZLAB_X8908X
- cloud-shell-storage-westusmpc
- DefaultResourceGroup-EUS
- myGFunction
- myGKV
- NetworkWatcherRG
- X8908X-myGSecure
- X8908X-resource

Search

Overview

Access control (IAM)

Tags

Resource visualizer

Events

Settings

Deployments

Security

Policies

Properties

Locks

Cost Management

Cost analysis

Cost alerts (preview)

Budgets

Advisor recommendations

Monitoring

Insights (preview)

Alerts

Metrics

Diagnostic settings

Logs

Advisor recommendations

Workbooks

Automation

Export template

Support + troubleshooting

New Support Request

AZLAB_X8908X | Access control (IAM)

Resource group

Check access Role assignments Roles Deny assignments Classic administrators

Number of role assignments for this subscription

2 4000

Search by name or email

Type: All Role: All Scope: All scopes

3 items (3 Users)

Name	Type
Owner	
Peter Bence Gabor peter.bence.gabor@halgato.sze.hu	User
User Access Administrator	
Csiki Balázs csikibalazs365@sze.hu	User
Virtual Machine Contributor	
Peter Bence Gabor peter.bence.gabor@halgato.sze.hu	User

Virtual Machine Contributor

Built-in role

Permissions JSON Assignments

Description: Lets you manage virtual machines, but not access to them, and not the virtual network or storage account they're connected to.

Search permissions

Actions DataActions

Showing 334 of 334 permissions

Type	Permissions	Description
Microsoft.Authorization		
Read	Get administrator	Reads the administrators for the subscription.
Read	Get administrator operation statuses	Gets the administrator operation statuses of the subscription.
Read	Get deny assignment	Get information about a deny assignment.
Read	Read the information about diagnostic settings categories	Get the information about diagnostic settings categories
Read	Get information about diagnostics settings	Read the information about diagnostics settings
Read	Get Role eligibility schedule instance	Gets the role eligibility schedule instances at given scope.
Read	Get management locks	Gets locks at the specified scope
Read	Get operations	Gets the list of operations
Read	List permissions	Lists all the permissions the caller has at a given scope.
Read	Get policy assignment	Get information about a policy assignment.
Read	Get Private Link Association	Get information about private link association.
Read	Get Resource Management Private Link	Get information about resource management private link.
Read	Get Private Endpoint Connection	Get information about private endpoint connection.
Read	Get Private Endpoint Connection Proxy	Get information about private endpoint connection proxy.
Read	Get policy definition	Get information about a policy definition.
Read	Get policy exemption	Get information about a policy exemption.
Read	Get policy set definition	Get information about a policy set definition.
Read	Get operations for resource providers	Get operations for all resource providers which can be used in role definitions.
Read	Get role assignment	Get information about a role assignment.
Read	Get Role assignment schedule	Gets the role assignment schedules at given scope.
Read	Get Role assignment schedule instance	Gets the role assignment schedule instances at given scope.
Read	Get Role assignment schedule request	Gets the role assignment schedule requests at given scope.
Read	Get role definition	Get information about a role definition.
Read	Get Role eligibility schedule	Gets the role eligibility schedules at given scope.

Workspaces Applications Apr 27 10:39 PM

Home X8908X-rg | Roles and administrators Roles and administrators | All roles Application Developer

Application Developer | Assignments

All roles

Diagnose and solve problems

Manage

Assignments

Description

Activity

Bulk operation results

Troubleshooting + Support

New support request

Add assignments Remove assignments Download assignments Refresh Manage in PIM Get feedback?

You can also assign built-in roles to groups now. [Learn More](#)

Search

Search by name Type

All

Name	Username	Type
No role assignments found		

Add assignments

Search

Search

- peter.bence.gabor peter.bence.gabor@halgato.sze.hu
- x8908x-first x8908x-first@x8908x.onmicrosoft.com Selected
- x8908x-second x8908x-second@x8908x.onmicrosoft.com
- x8908x-third x8908x-third@x8908x.onmicrosoft.com

Selected items

- x8908x-first x8908x-first@x8908x.onmicrosoft.com Remove

Add

Workspaces Applications Apr 27 10:40 PM

Microsoft Azure Search resources, services, and docs (v2)

Home XBOX-org | Roles and administrators Roles and administrators | All roles Application Administrator

Application Administrator | Assignments

All roles

Diagnose and solve problems

Manage

- Assignments
- Description
- Activity
- Bulk operation results
- Troubleshooting + Support
- New support request

+ Add assignments X Remove assignments Download assignments Refresh Manage in PIM Get feedback?

You can also assign built-in roles to groups now. [Learn More](#)

Search Search by name Type All

Name	UserName	Type
No role assignments found		

Add assignments

Search

Selected

- peter.bence.gabor peter.bence.gabor@halgato.sze.hu
- af9bde-first af9bde-first@af9bdeorg.onmicrosoft.com
- XBOX-second XBOX-second@af9bdeorg.onmicrosoft.com
- XBOX-third XBOX-third@af9bdeorg.onmicrosoft.com

Selected items

- af9bde-first af9bde-first@af9bdeorg.onmicrosoft.com Remove

Add

Workspaces Applications Apr 27 10:40 PM

Microsoft Azure Search resources, services, and docs (v2)

Home XBOX-org | Roles and administrators Roles and administrators | All roles Attack Payload Author

Attack Payload Author | Assignments

All roles

Diagnose and solve problems

Manage

- Assignments
- Description
- Activity
- Bulk operation results
- Troubleshooting + Support
- New support request

+ Add assignments X Remove assignments Download assignments Refresh Manage in PIM Get feedback?

You can also assign built-in roles to groups now. [Learn More](#)

Search Search by name Type All

Name	UserName	Type
No role assignments found		

Add assignments

Search

Selected

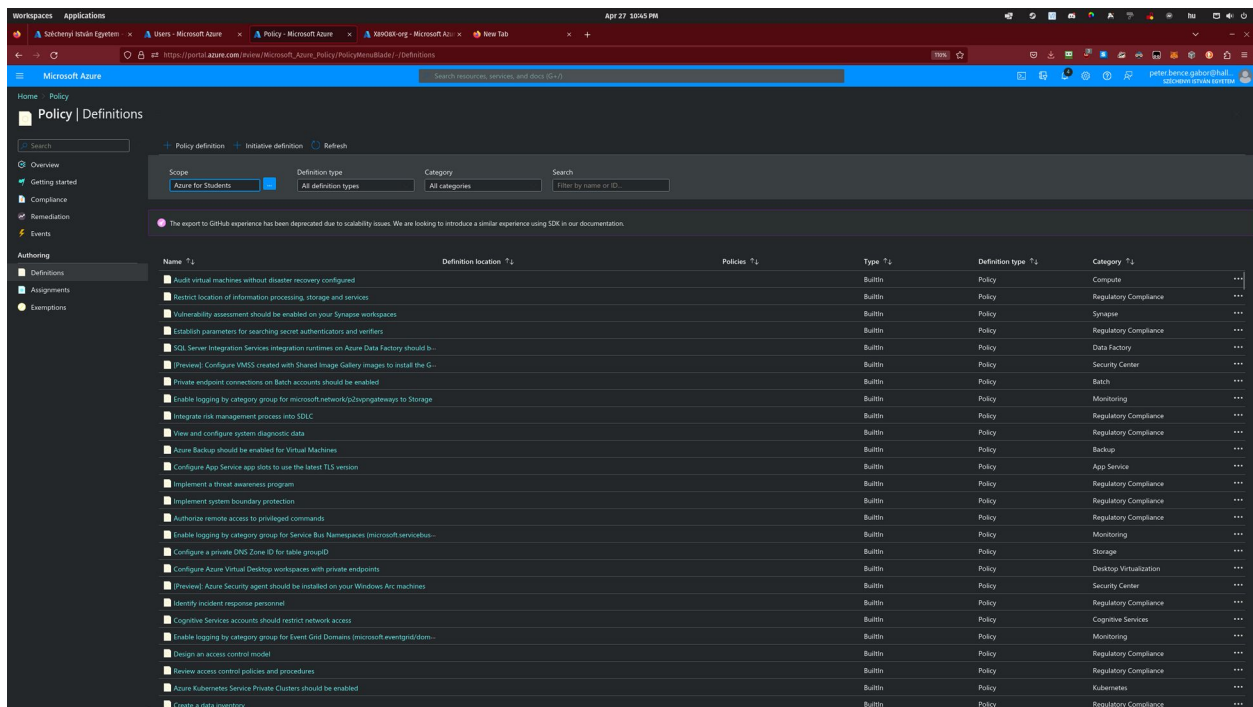
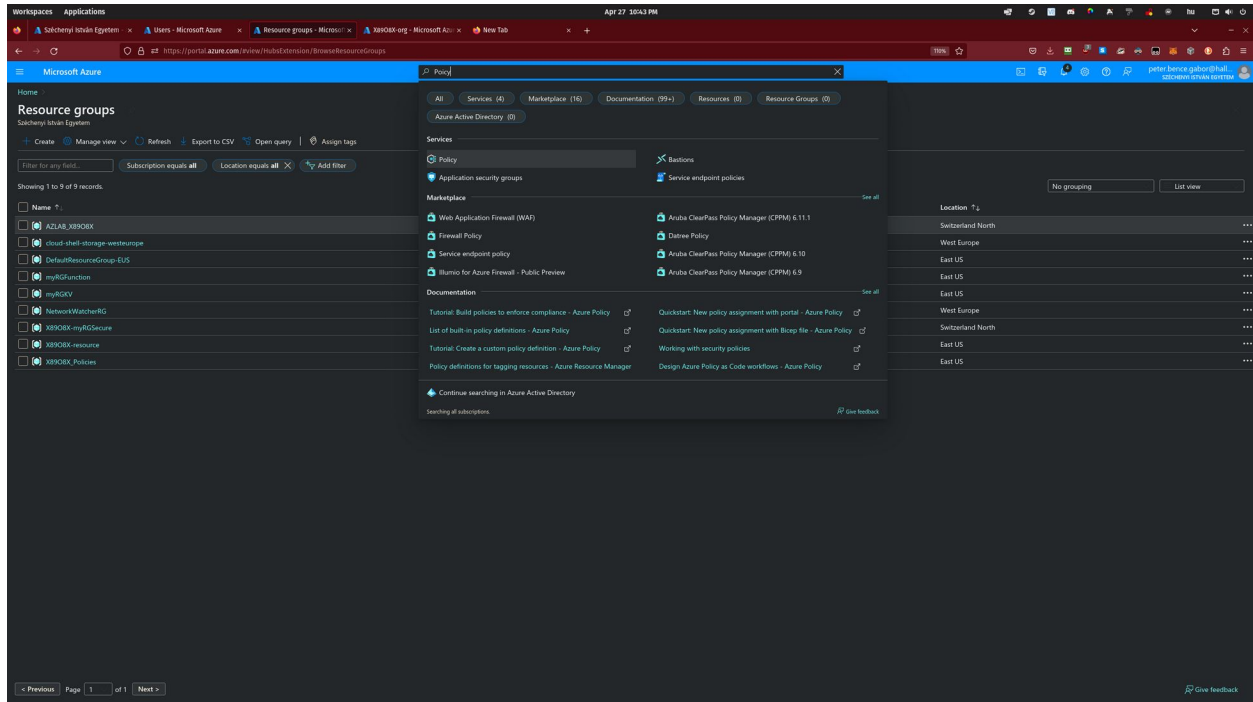
- peter.bence.gabor peter.bence.gabor@halgato.sze.hu
- af9bde-first af9bde-first@af9bdeorg.onmicrosoft.com
- XBOX-second XBOX-second@af9bdeorg.onmicrosoft.com
- XBOX-third XBOX-third@af9bdeorg.onmicrosoft.com

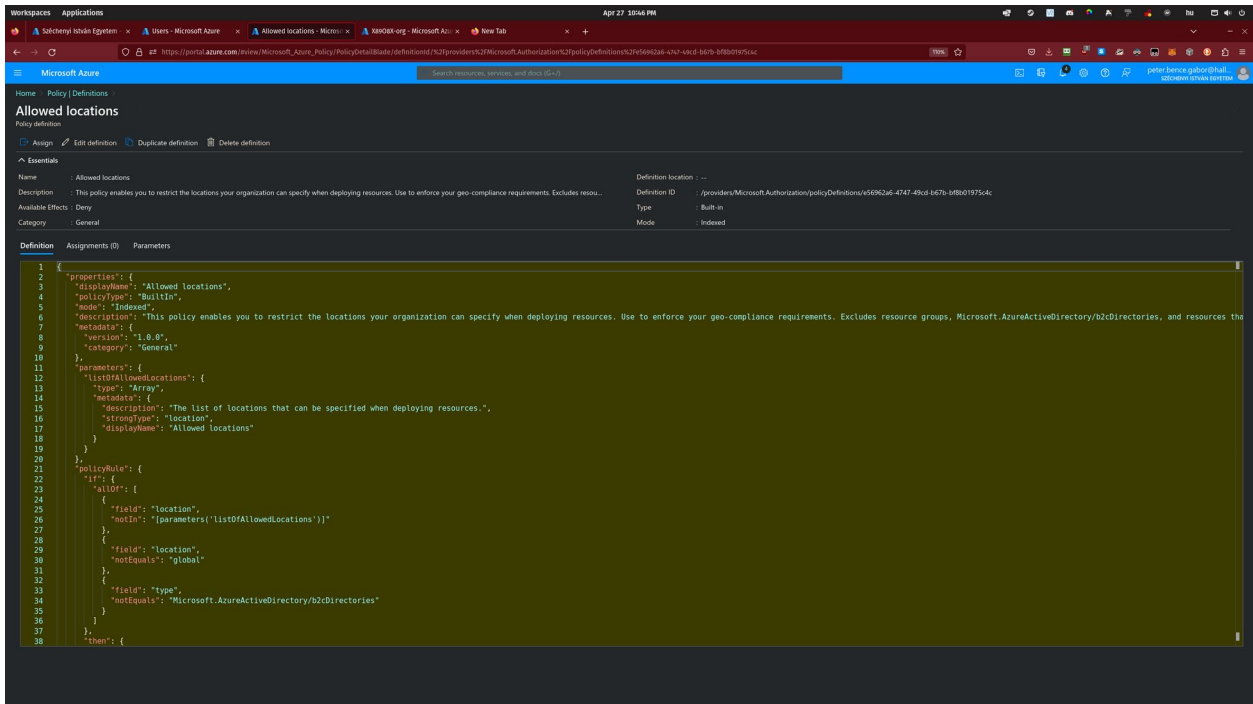
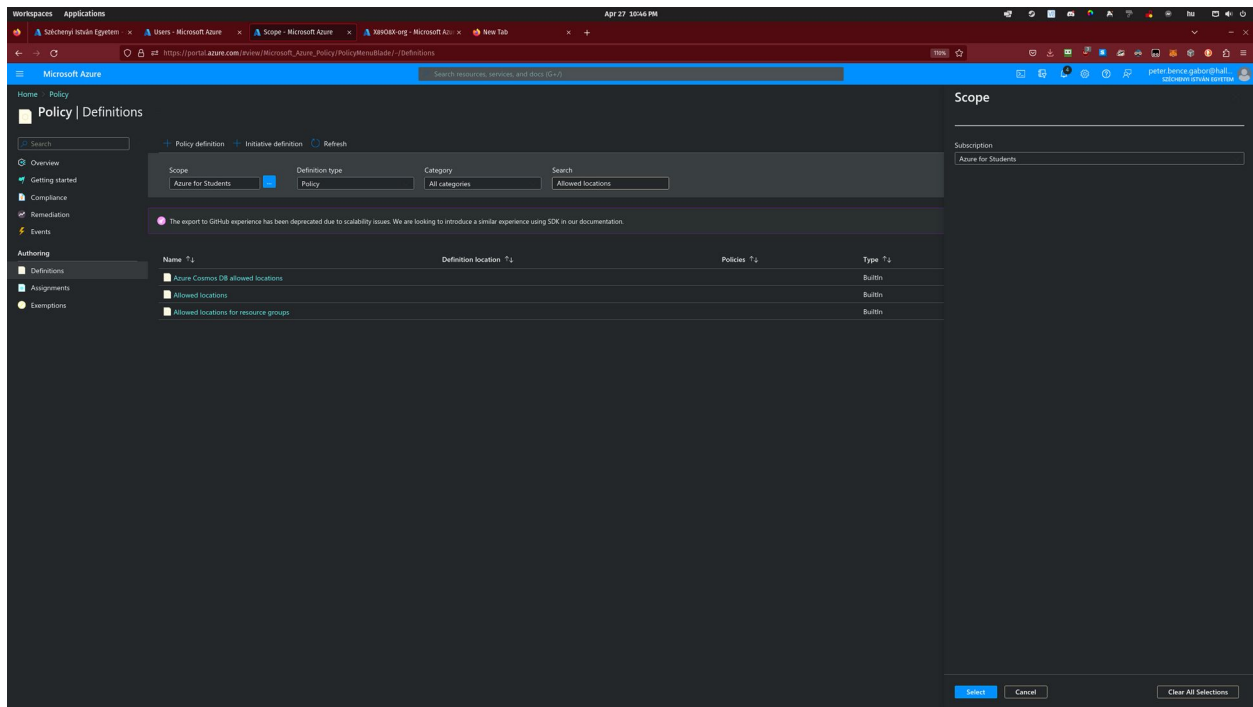
Selected items

- XBOX-second XBOX-second@af9bdeorg.onmicrosoft.com Remove

Add

2. Feladat





WorkspacesApplications

Apr 27, 10:47 PM

Sakcheryl Ishak EgietemUsers - Microsoft AzureAllowed locations - Micro...XRDQ88.org - Microsoft Az...New Tab

https://portal.azure.com/review/Microsoft_Azure_Policy/CreateAssignmentBladeV2/assignMode-/?definitionId/%2Fproviders%2FMicrosoft.Authorization%2FpolicyDefinitions%2Fcd69b2ac-43e2-48d2-b6b5-bf8b07095c4c

Microsoft AzureSearch resources, services, and docs from

HomePolicyDefinitionsAllowed locationsAssign policy

BasicsAdvancedParametersRemediationNon-compliance messagesReview + create

Scope

ScopeLearn more about setting the scope *

Exclusions

Optimally select resources to exclude from the policy assignment.

Basics

Policy definition

Allowed locations

Assignment name *

Allowed locations

Description

Policy enforcement

EnabledDisabled

Assigned by

Review + createCancelPreviousNext

WorkspacesApplications

Apr 27, 10:40 PM

Sakcheryl Ishak EgietemUsers - Microsoft AzureAllowed locations - Micro...XRDQ88.org - Microsoft Az...New Tab

https://portal.azure.com/review/Microsoft_Azure_Policy/CreateAssignmentBladeV2/assignMode-/?definitionId/%2Fproviders%2FMicrosoft.Authorization%2FpolicyDefinitions%2Fcd69b2ac-43e2-48d2-b6b5-bf8b07095c4c

Microsoft AzureSearch resources, services, and docs from

HomePolicyDefinitionsAllowed locationsAssign policy

BasicsAdvancedParametersRemediationNon-compliance messagesReview + create

Search by parameter name

Only show parameters that need input or review

Allowed locations *

Switzerland

Sw

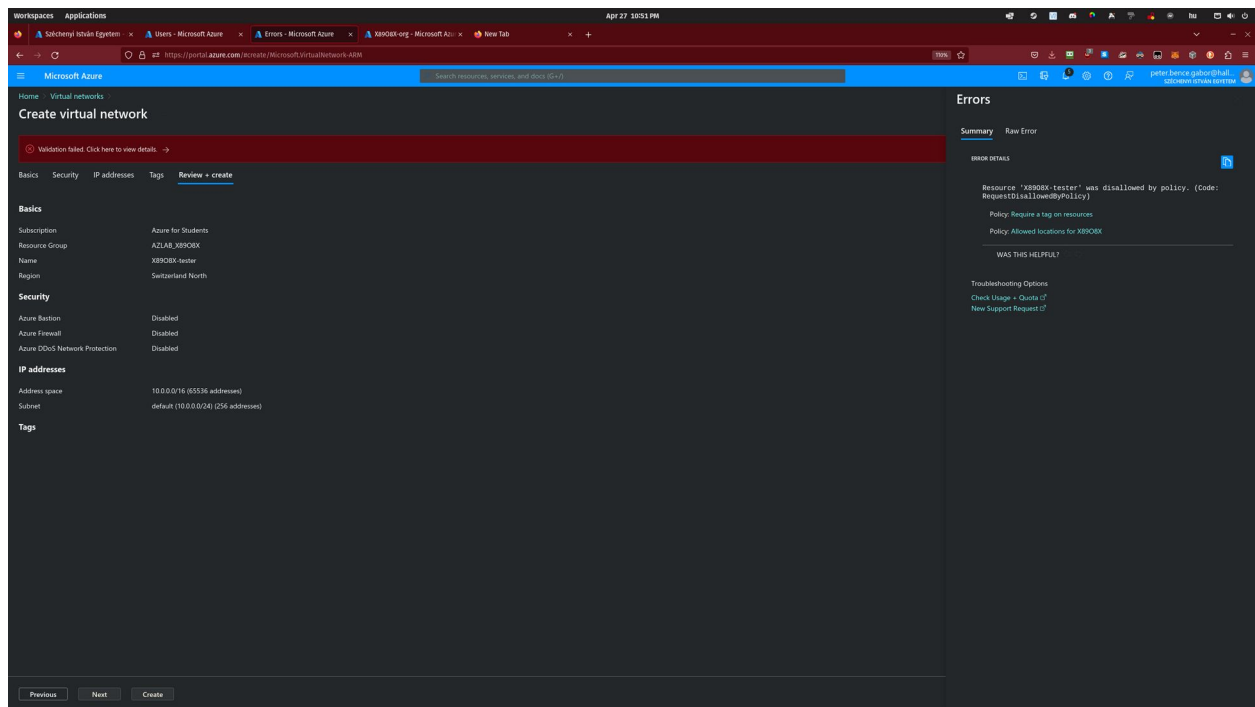
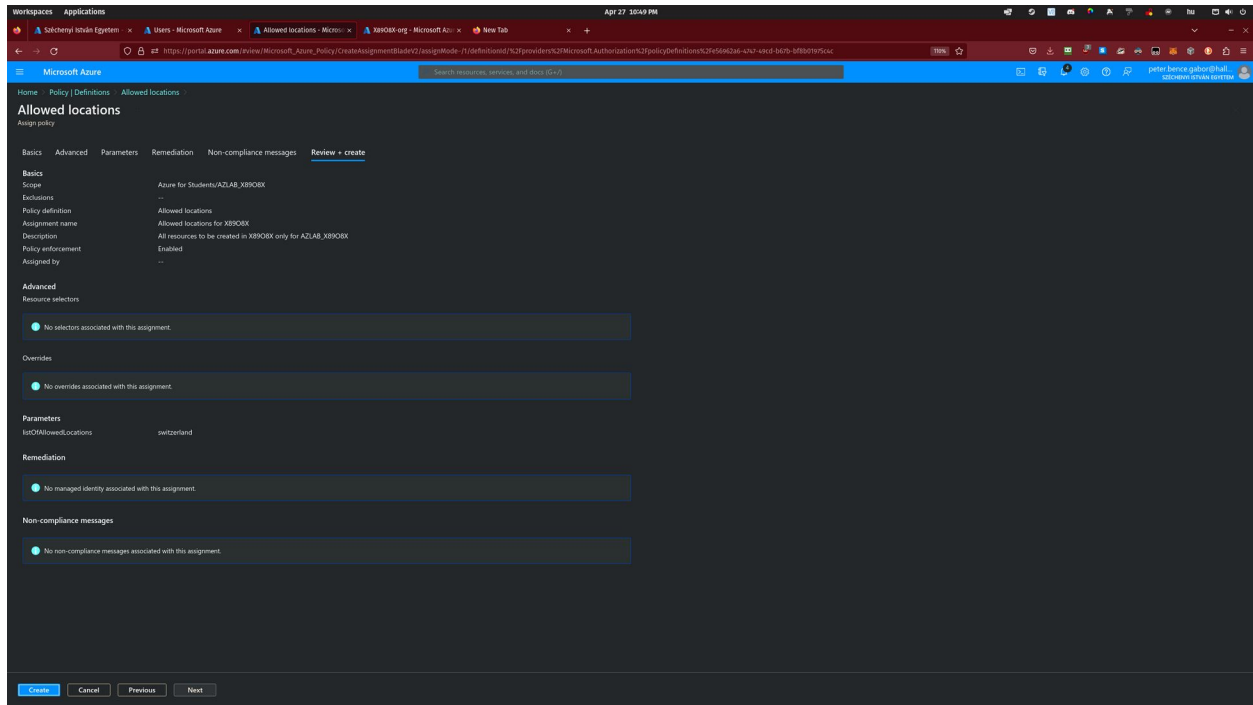
☐ Sweden Central

☒ Switzerland

☐ Switzerland North

☐ Switzerland West

Review + createCancelPreviousNext



3. Feladat:

Az Azure AD Privileged Identity Management (PIM) egy olyan Azure felhőszolgáltatás, amely lehetővé teszi a felhasználók számára, hogy hatékonyabban kezeljék a rendszerben található magas kockázatú fiókokat és az azokhoz kapcsolódó jogosultságokat. Az Azure AD PIM segítségével a felhasználók azonosíthatják és kezelhetik azokat a felhasználói fiókokat, amelyekhez magas szintű jogosultságok kapcsolódnak.

Az Azure AD PIM modellje szerint a felhasználók magas kockázatú jogosultságokhoz hozzáférését csak akkor engedélyezi a rendszer, ha az adott jogosultság tényleges használatra kerül. Ez az elv az ún. "just-in-time" (JIT) hozzáférés-kezelést jelenti, amely lehetővé teszi a felhasználók számára, hogy csak akkor kapjanak hozzáférést a szükséges jogosultságokhoz, amikor valóban szükség van rájuk.

Az Azure AD PIM segítségével a rendszergazdák biztonságos módon kezelhetik az Azure fiókokat és az azokhoz kapcsolódó jogosultságokat. A rendszergazdák beállíthatják a JIT hozzáférési politikákat, meghatározhatják, hogy kiknek és mikor engedélyezik a magas kockázatú jogosultságokat, és rögzíthetik az adott hozzáféréseket.

Az Azure AD PIM segítségével az Azure fiókok ellenőrzése és auditeálása is egyszerűbbé válik. Az Azure AD PIM segítségével az adminisztrátorok nyomon követhetik az Azure fiókok hozzáféréseit és jogosultságait, rögzíthetik a hozzáféréseket, és ellenőrizhetik a rendszerbiztonsági eseményeket.

Az Azure AD PIM előnyei közé tartozik az erős biztonsági védelem, a JIT hozzáférés-kezelés, a könnyű felhasználói fiókkezelés és az Azure rendszereinek nagyobb biztonsága. Az Azure AD PIM használata általában nagyobb méretű és összetett rendszerekben ajánlott, ahol magas kockázatú felhasználói fiókok és jogosultságok vannak jelen.

