

Azure Data Lake Role Based Access Control (RBAC) y Access Control List (ACL)

Quiero explicar el Control de acceso basado en roles (Role based access control [RBAC]). Ahora, sabemos que Azure Active Directory es nuestro Identity provider, así que aquí, podemos crear usuarios y el usuario puede realmente iniciar sesión en nuestra cuenta de Azure. Ahora, digamos que definimos un usuario en Azure Active Directory. Ahora, este usuario puede iniciar sesión en nuestra cuenta Azure, básicamente tener acceso a nuestra suscripción Azure. Pero inicialmente, no tendrá ningún permiso para acceder a los recursos que se definen como parte de la suscripción. Tendremos que darle acceso explícitamente a través de algo conocido como "Role based access control (RBAC)". Así que si tenemos una cuenta de almacenamiento, si tenemos una Azure Data Lake Gen2 storage account, si queremos que tengan acceso a esa cuenta de almacenamiento, lo primero que tenemos que hacer es dar acceso a través de "Role based access control".

<https://learn.microsoft.com/es-es/azure/role-based-access-control/built-in-roles>

El control de acceso basado en rol de Azure (Azure RBAC) tiene varios roles integrados de Azure que se pueden asignar a usuarios, grupos, entidades de servicio e identidades administradas. Las asignaciones de roles sirven para controlar el acceso a los recursos de Azure. Si los roles integrados no satisfacen las necesidades específicas de la organización, puede crear roles personalizados de Azure propios.

En la tabla siguiente se proporciona una breve descripción de cada rol integrado. Haga clic en el nombre del rol para ver la lista de **Actions**, **NotActions**, **DataActions** y **NotDataActions** para cada rol.

Rol integrado	Descripción	id
General		
Colaborador	Concede acceso completo para administrar todos los recursos, pero no le permite asignar roles en Azure RBAC, administrar asignaciones en Azure Blueprints ni compartir galerías de imágenes.	b24988ac-6180-42a0-ab88-20f7382dd24c
Contributor		
Propietario	Permite conceder acceso total para administrar todos los recursos, incluida la posibilidad de asignar roles en Azure RBAC.	8e3af657-a8ff-443c-a75c-2fe8c4bcb635
Owner		
Lector	Permite ver todos los recursos, pero no realizar ningún cambio.	acdd72a7-3385-48ef-bd42-f606fba81ae7
Reader		
Administrador de acceso de usuario	Permite administrar el acceso de usuario a los recursos de Azure.	18d7d88d-d35e-4fb5-a5c3-7773c20a72d9
User Access Administrator		

Vamos a ejemplificarlo creando un nuevo usuario en Azure Active Directory

The screenshot shows the Microsoft Azure portal interface. At the top, the header includes the Microsoft Azure logo, a search bar, and the user's email address (techsup1000@gmail.com). The left-hand navigation pane is visible, with the 'Users' option under the 'Manage' section highlighted by a red rectangular box. The main content area displays the 'Default Directory | Overview' page for the 'Default Directory' tenant. This page includes tabs for 'Overview', 'Monitoring', and 'Tutorials'. Below the tabs is a search bar for the tenant. The 'Basic information' section lists several details: Name (Default Directory), Tenant ID (5f5f1c90-abac-4ebe-88d7-0f3d121f967e), Primary domain (techsup1000gmail.onmicrosoft.com), License (Azure AD Premium P2), Users (12), and Groups (7).

Microsoft Azure Search resources, services, and docs (G+/)

techsup1000@gmail.com
DEFAULT DIRECTORY (TECHSUP1000)

Dashboard > Default Directory >

Users | All users (Preview)

Default Directory - Azure Active Directory

+ New user + New guest user Bulk operations Refresh Reset password

This page includes previews available for your evaluation. View previews

Search users Add filters

12 users found

	Name	User principal n...	User type	Directory synced	Identity issi
<input type="checkbox"/>	9f4a5dde-728...	techsup1000_gmail.c...	Member	No	techsup100
<input type="checkbox"/>	admin	admin@cloud-work-...	Member	No	techsup100
<input type="checkbox"/>	admin	admin@cloudportal...	Member	No	techsup100
<input type="checkbox"/>	domainusrA	domainusrA@cloud-...	Member	Yes	techsup100
<input type="checkbox"/>	domainusrB	domainusrB@cloud-...	Member	Yes	techsup100
<input type="checkbox"/>	ITuserA	ITuserA@cloud-work...	Member	Yes	techsup100
<input type="checkbox"/>	newsq1	newsq1@techsup100...	Member	No	techsup100
<input type="checkbox"/>	On-Premises ...	Sync_ADCONNECT_0...	Member	Yes	techsup100

Microsoft Azure Search resources, services, and docs (G+/)

techsup1000@gmail.com
DEFAULT DIRECTORY (TECHSUP1000)

Dashboard > Default Directory > Users >

New user

Default Directory

Got feedback?

☒ **Create user**

Create a new user in your organization.
This user will have a user name like
alice@techsup1000gmail.onmicrosoft.com.
[I want to create users in bulk](#)

☐ **Invite user**

Invite a new guest user to
collaborate with your organization.
The user will be emailed an
invitation they can accept in order
to begin collaborating.
[I want to invite guest users in bulk](#)

[Help me decide](#)

Microsoft Azure

Search resources, services, and docs (G+ /)

6

?

techsup1000@gmail.com
DEFAULT DIRECTORY (TECHSUP1...

>>


Dashboard > Default Directory > Users >

New user ...

Default Directory

Got feedback?

Identity

User name * ⓘ
datalake ✓ @ techsup1000gmail.onmic... ▼ 
The domain name I need isn't shown here

Name * ⓘ
datalake ✓

First name

Last name

Microsoft Azure

Search resources, services, and docs (G+ /)

6

?

techsup1000@gmail.com
DEFAULT DIRECTORY (TECHSUP1...

>>

Dashboard > Default Directory > Users >

New user ...

Default Directory

Got feedback?

Last name

Password

☐ Auto-generate password
☒ Let me create the password

Initial password * ⓘ
.....

Microsoft Azure Search resources, services, and docs (G+/)

techsup1000@gmail.com
DEFAULT DIRECTORY (TECHSUP1...

Dashboard > Default Directory > Users >

New user

Default Directory

Got feedback?

Groups and roles

Groups 0 groups selected

Roles User

Settings

Block sign in Yes No

Usage location

Job info

Create

Microsoft Azure Search resources, services, and docs (G+/)

techsup1000@gmail.com
DEFAULT DIRECTORY (TECHSUP1...

Dashboard > Default Directory >

Users | All users (Preview)

Default Directory - Azure Active Directory

Successfully created user
Successfully created user datalake. 3:57 PM

+ New user + New guest user Bulk operations Refresh Reset password

This page includes previews available for your evaluation. View previews

Search: datalake 1 user found

Name	User principal n...	User type	Directory synced	Identity issue
<input type="checkbox"/> datalake	datalake@techsup10...	Member	No	techsup1000g

Microsoft Azure Search resources, services, and docs (G+/)

techsup1000@gmail.com
DEFAULT DIRECTORY (TECHSUP1...

Dashboard > Default Directory > Users > datalake

datalake | Profile

User

Edit Reset password Revoke sessions Delete Refresh Got feedback?

Manage

Profile

Assigned roles

Administrative units

Groups

Applications

datalake

datalake@techsup1000gmail.onmicrosoft.com

User Sign-ins

DA

Si ingresamos a Azure con la cuenta del nuevo usuario, veremos que no podemos visualizar ningún recurso de la suscripción.

The screenshot shows the Microsoft Azure portal home page. The top navigation bar includes the Microsoft Azure logo, a search bar, and user information for 'datalake@techsup1000...'. The main content area features a 'Welcome to Azure!' message and a 'Default Directory' dropdown menu. The dropdown menu is open, showing options like 'Azure Staging techsup1000@gmail.com' and 'Sign in with a different account'. Below the welcome message, there are three cards: 'Start with an Azure free trial', 'Manage Azure Active Directory', and 'Access student benefits'. The URL at the bottom of the browser window is: `https://portal.azure.com/Account/SwitchTo?ru=https%3A%2F%2Fportal.azure.com%2F%23blade%2F%2FBrowseAll&login_hint=techsup1000%40gmail.com`

Nuevamente, ingresamos con la cuenta **admin** y seguimos los siguientes pasos para crear un RBAC

The screenshot shows the Microsoft Azure portal interface for a storage account named 'datalake2000'. The left sidebar contains a navigation menu with options like 'Overview', 'Activity log', 'Tags', 'Diagnose and solve problems', 'Access Control (IAM)', 'Data migration', 'Events', 'Storage Explorer (preview)', 'Data storage', 'Containers', and 'File shares'. The 'Access Control (IAM)' option is highlighted with a red box. The main content area displays the 'Access Control (IAM)' page for 'datalake2000 | Access Control (IAM)'. The page has a search bar and a '+ Add' button, which is also highlighted with a red box. Below the search bar, there are tabs for 'Check access', 'Role assignments', 'Roles', 'Roles (Classic)', and 'Deny assignments'. The 'Check access' tab is selected. The page shows sections for 'My access', 'Check access', and 'Grant access to this resource'. The 'Grant access to this resource' section includes a button 'Add role assignment (Preview)' and a link 'Use the classic experience'. The 'View access to this resource' section is also visible.

Microsoft Azure Search resources, services, and docs (G+)

techsup1000@gmail.com
DEFAULT DIRECTORY (TECHSUP1...

Dashboard > datalake2000

datalake2000 | Access Control (IAM)

Storage account

Search (Ctrl+)

Overview
Activity log
Tags
Diagnose and solve problems
Access Control (IAM)
Data migration
Events
Storage Explorer (preview)

Data storage
Containers
File shares

+ Add Download role assignments Edit columns Refresh Remove

Add role assignment
Add role assignment (Preview)
Add co-administrator
View my level of access to this resource.
View my access

Check access
Review the level of access a user, group, service principal, or managed identity has to this resource. [Learn more](#)

Find
User, group, or service principal
Search by name or email address

Grant access to this resource
Grant access to resources by assigning a role.
Add role assignment (Preview)
Use the classic experience [Learn more](#)

View access to this resource
View the role assignments that grant access to this and other resources.

Microsoft Azure Search resources, services, and docs (G+)

techsup1000@gmail.com
DEFAULT DIRECTORY (TECHSUP1...

Dashboard > datalake2000

datalake2000 | Access Control (IAM)

Storage account

Search (Ctrl+)

Overview
Activity log
Tags
Diagnose and solve problems
Access Control (IAM)
Data migration
Events
Storage Explorer (preview)

Data storage
Containers
File shares
Queues
Tables

+ Add Download role assignments

Check access Role assignments Roles

My access
View my level of access to this resource.
View my access

Check access
Review the level of access a user, group, service principal, or managed identity has to this resource. [Learn more](#)

Find
User, group, or service principal
Search by name or email address

Add role assignment

Role
Reader

Assign access to
User, group, or service principal

Select
datalake

No users, groups, or service principals found.

Selected members:

data lake
datalake@techsup1000gmail.onmicro... [Remove](#)

Save Discard

Ahora si volvemos a logearnos con el nuevo usuario podremos ver nuestra Azure Data Lake Storage account. Esto es posible porque hemos dado el control de acceso basado en roles (Role based access control) a esta cuenta de almacenamiento.

Microsoft Azure

Search resources, services, and docs (G+)

datalake@techsup1000...
DEFAULT DIRECTORY (TECHSUP1...

Home > All resources >

datalake2000
Storage account

Search (Ctrl+/)

Activity log

Tags

Diagnose and solve problems

Access Control (IAM)

Data migration

Events

Storage Explorer (preview)

Data storage

Containers

File shares

Queues

Tables

Open in Explorer Delete Move Refresh Feedback

Microsoft recommends upgrading to the new alerts platform to ensure no interruptions in your alerts. Classic alerts will be retired starting in 2021. Upgrade to the new alerts platform. [Learn more](#)

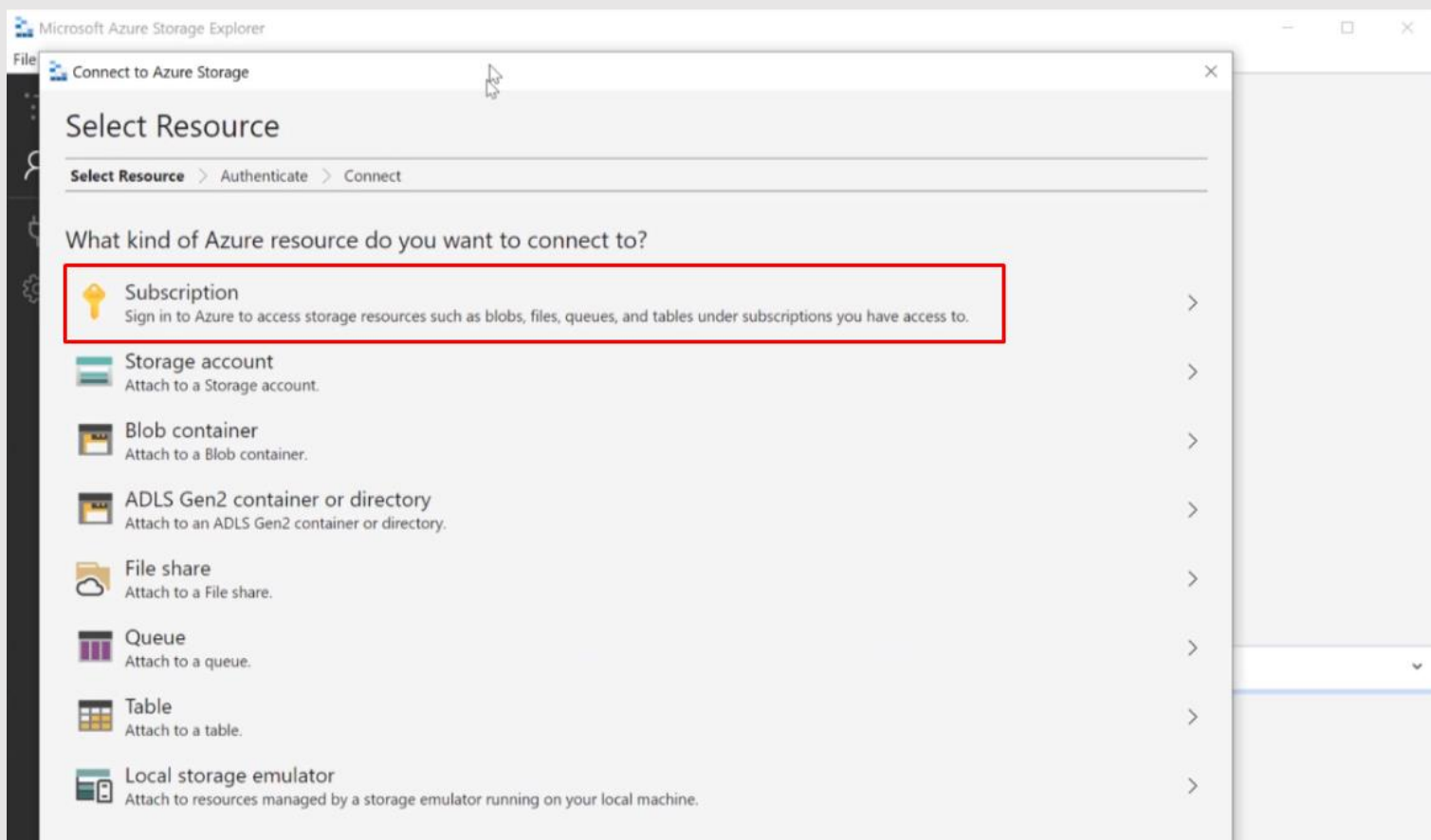
Essentials JSON View

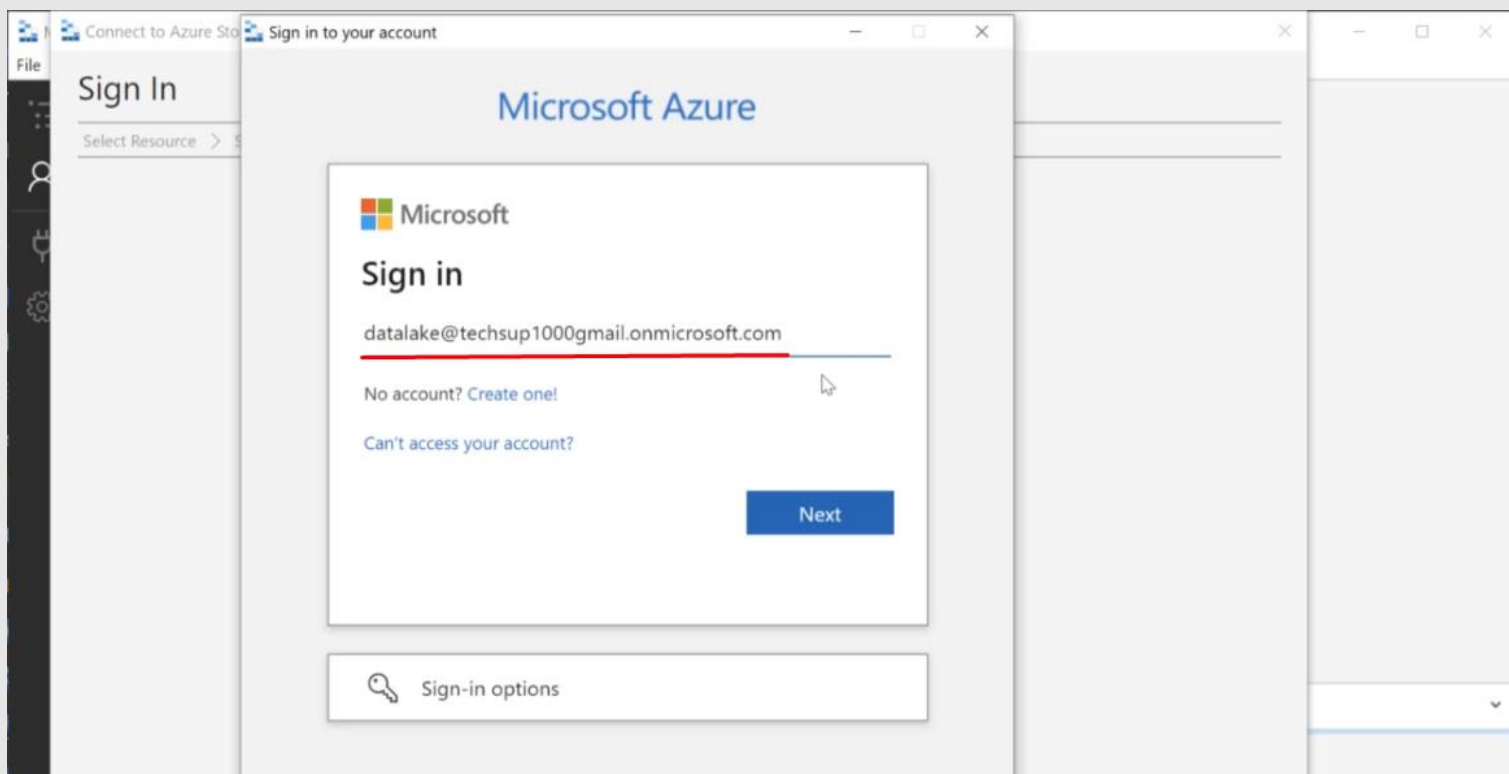
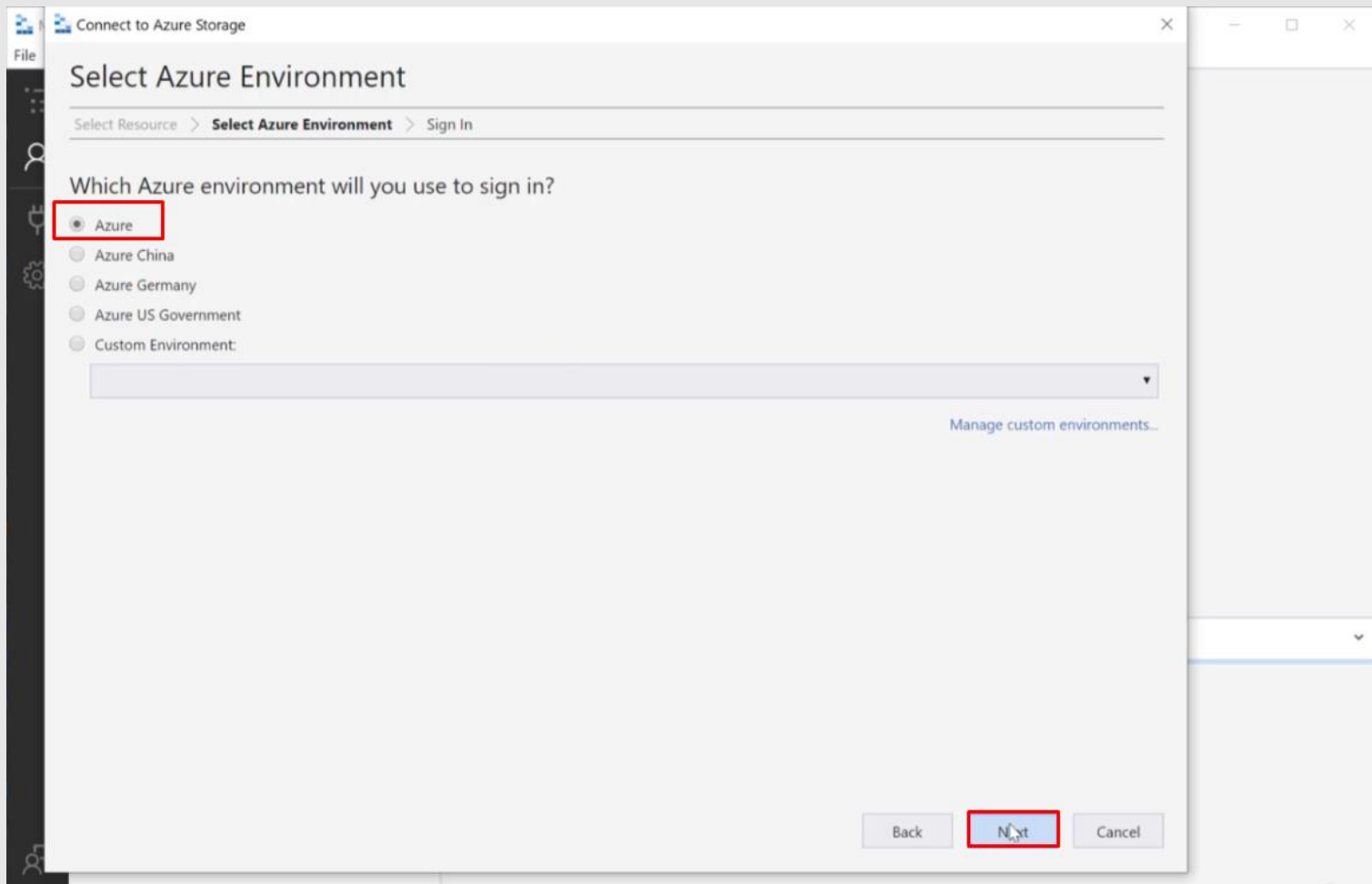
Resource group (change)	Performance/Access tier
data-grp	Standard/Hot
Location	Replication
North Europe	Locally-redundant storage (LRS)
Subscription (change)	Account kind
Test Environment	StorageV2 (general purpose v2)
Subscription ID	Provisioning state
20c6eec9-2d80-4700-b0f6-4fde579a8783	Succeeded
Disk state	Created
Available	7/1/2021, 10:54:09 PM
Tags (change)	

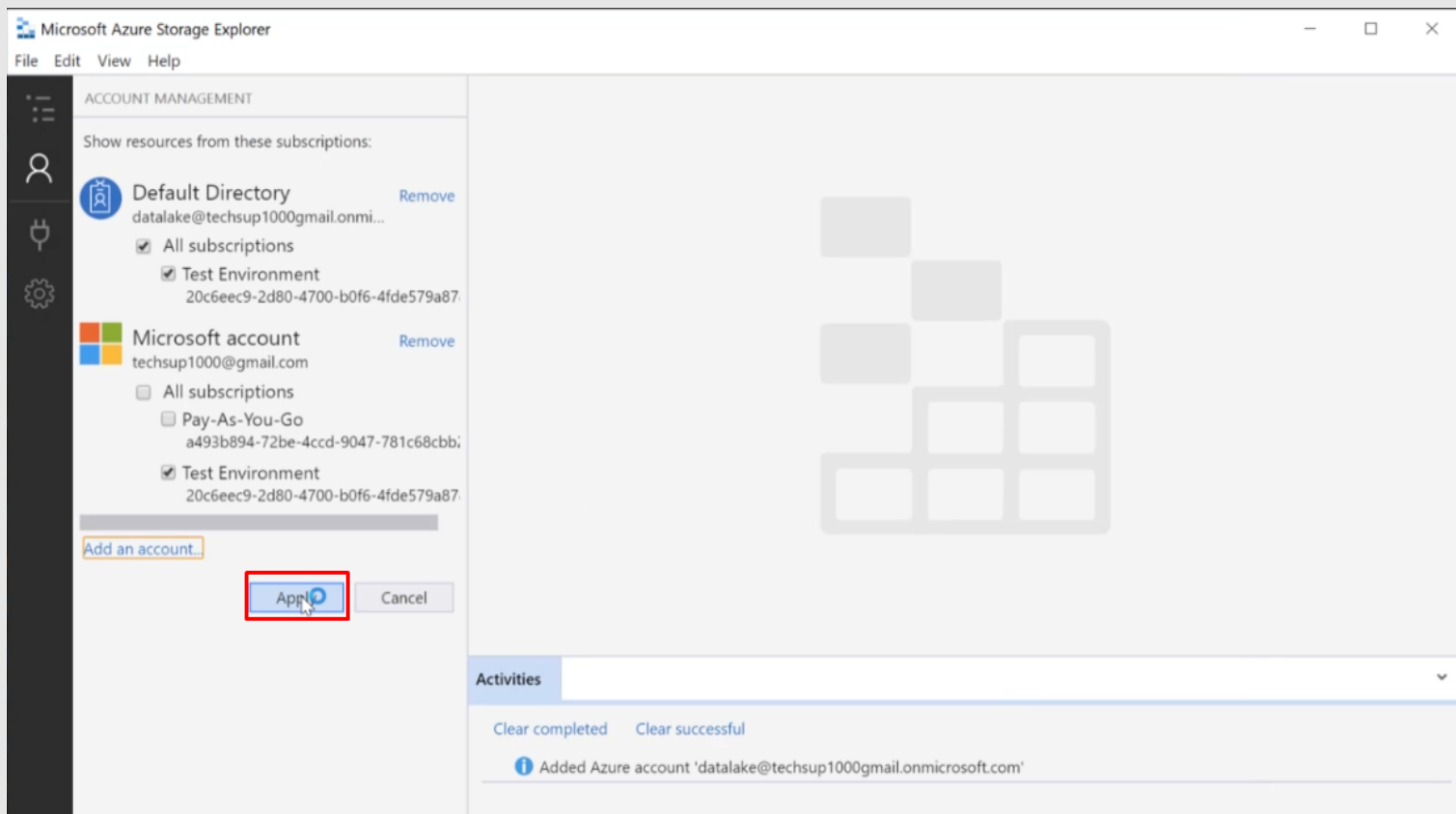
Access Control List (ACL)

Vimos que a nuestro nuevo usuario en Azure Active Directory le otorgamos un Rol de lector “Reader” para que pueda visualizar nuestro Azure Data Lake Storage. Sin embargo, aun nos falta otorgarle permisos para que pueda visualizar y leer los objetos que se encuentran dentro de la cuenta de almacenamiento. Estos permisos son manejados por ACL.

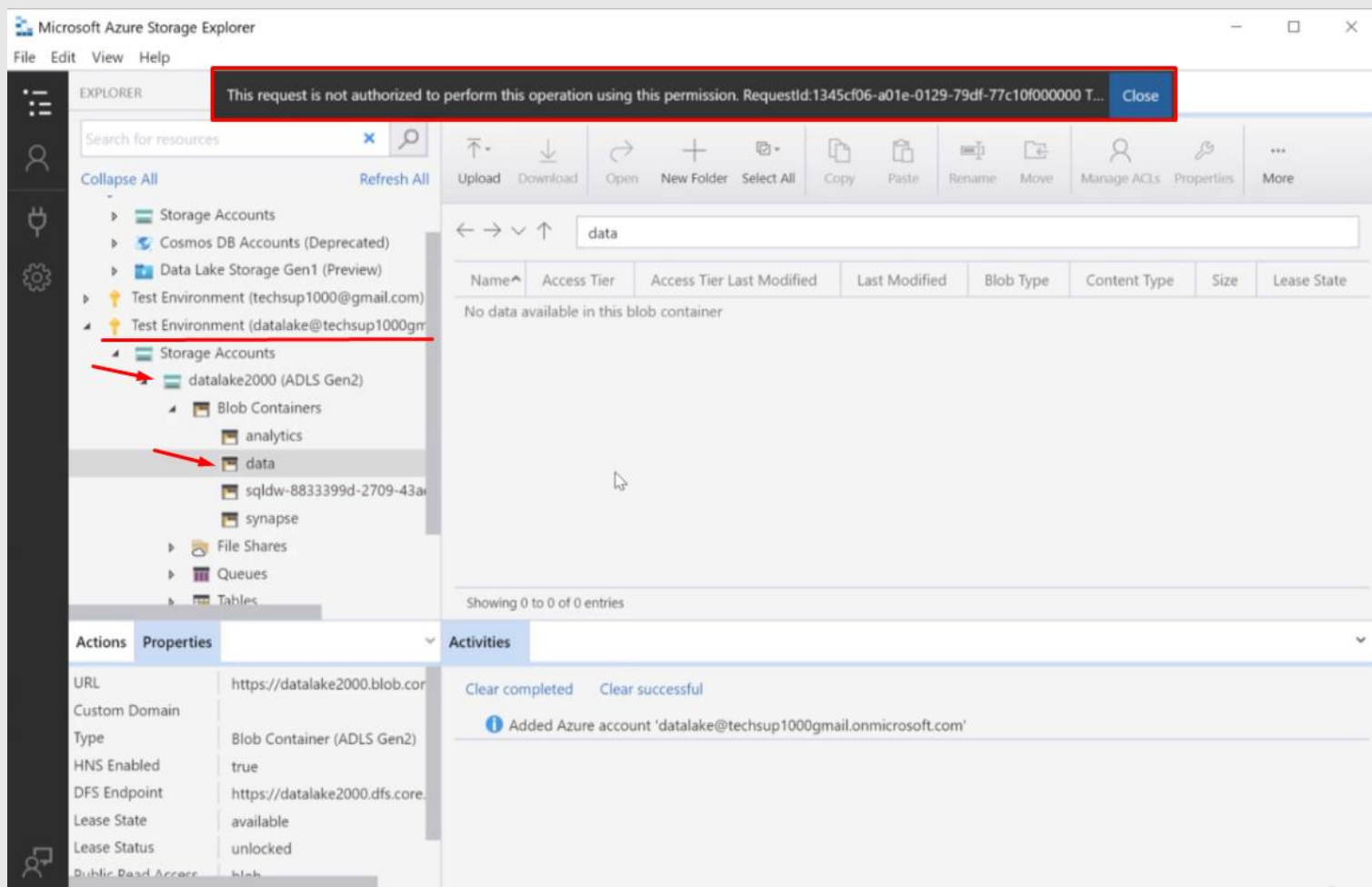
Si ingresamos con la cuenta del nuevo usuario utilizando Azure Storage Explorer







Como comentamos anteriormente, vemos que el usuario no tiene acceso a los objetos dentro del Azure Data Lake Storage



Microsoft Azure Search resources, services, and docs (G+)

techsup1000@gmail.com
DEFAULT DIRECTORY (TECHSUP1...

Dashboard > Storage accounts > datalake2000

datalake2000 | Access Control (IAM)

Storage account

Search (Ctrl+)

+ Add Download role assignments Edit columns Refresh Remove

Overview
Activity log
Tags
Diagnose and solve problems
Access Control (IAM)
Data migration
Events
Storage Explorer (preview)

Data storage
Containers
File shares

Add role assignment
Add role assignment (review)
Add co-administrator
View my level of access to this resource.
View my access

Check access
Review the level of access a user, group, service principal, or managed identity has to this resource. [Learn more](#)

Find
User, group, or service principal
Search by name or email address

Grant access to this resource
Grant access to resources by assigning a role.
Add role assignment (Preview)
Use the classic experience [Learn more](#)

View access to this resource
View the role assignments that grant access to this and other resources.

Microsoft Azure Search resources, services, and docs (G+)

techsup1000@gmail.com
DEFAULT DIRECTORY (TECHSUP1...

Dashboard > Storage accounts > datalake2000

datalake2000 | Access Control (IAM)

Storage account

Search (Ctrl+)

+ Add Download role assignments

Check access Role assignments Roles

My access
View my level of access to this resource.
View my access

Check access
Review the level of access a user, group, service principal, or managed identity has to this resource. [Learn more](#)

Find
User, group, or service principal
Search by name or email address

Add role assignment

Role
Storage Blob Data Reader

Assign access to
User, group, or service principal

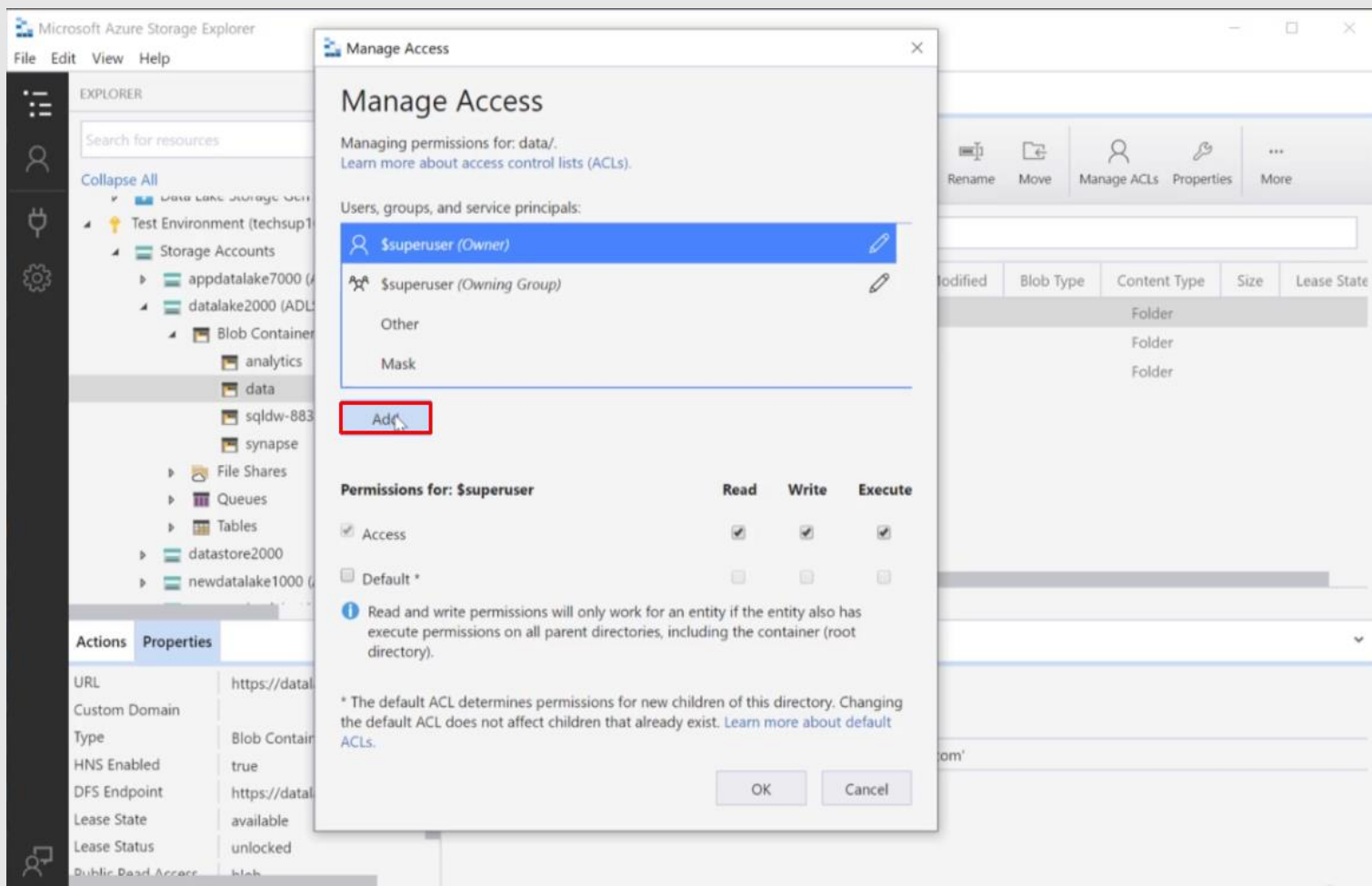
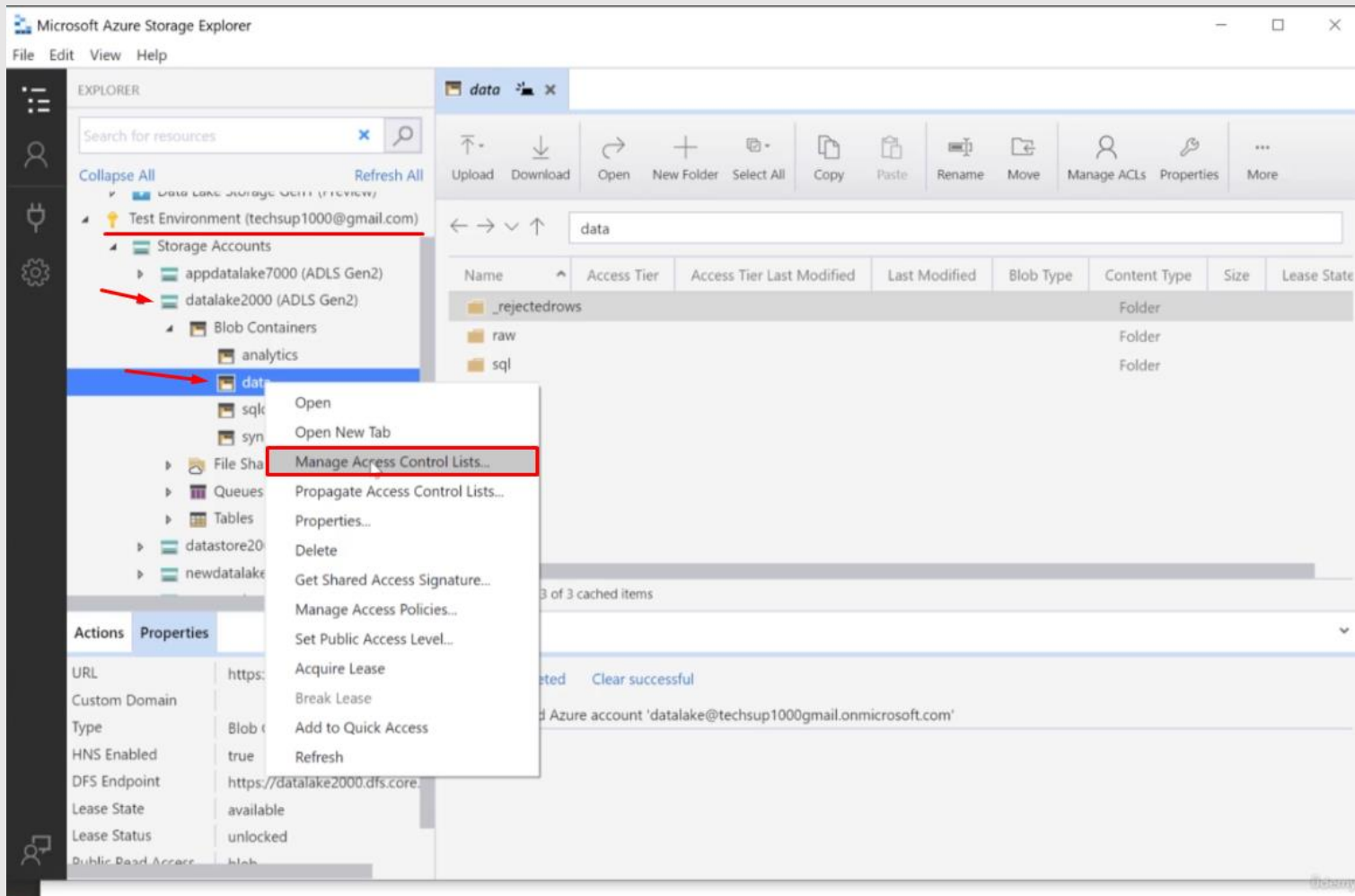
Select
datalake

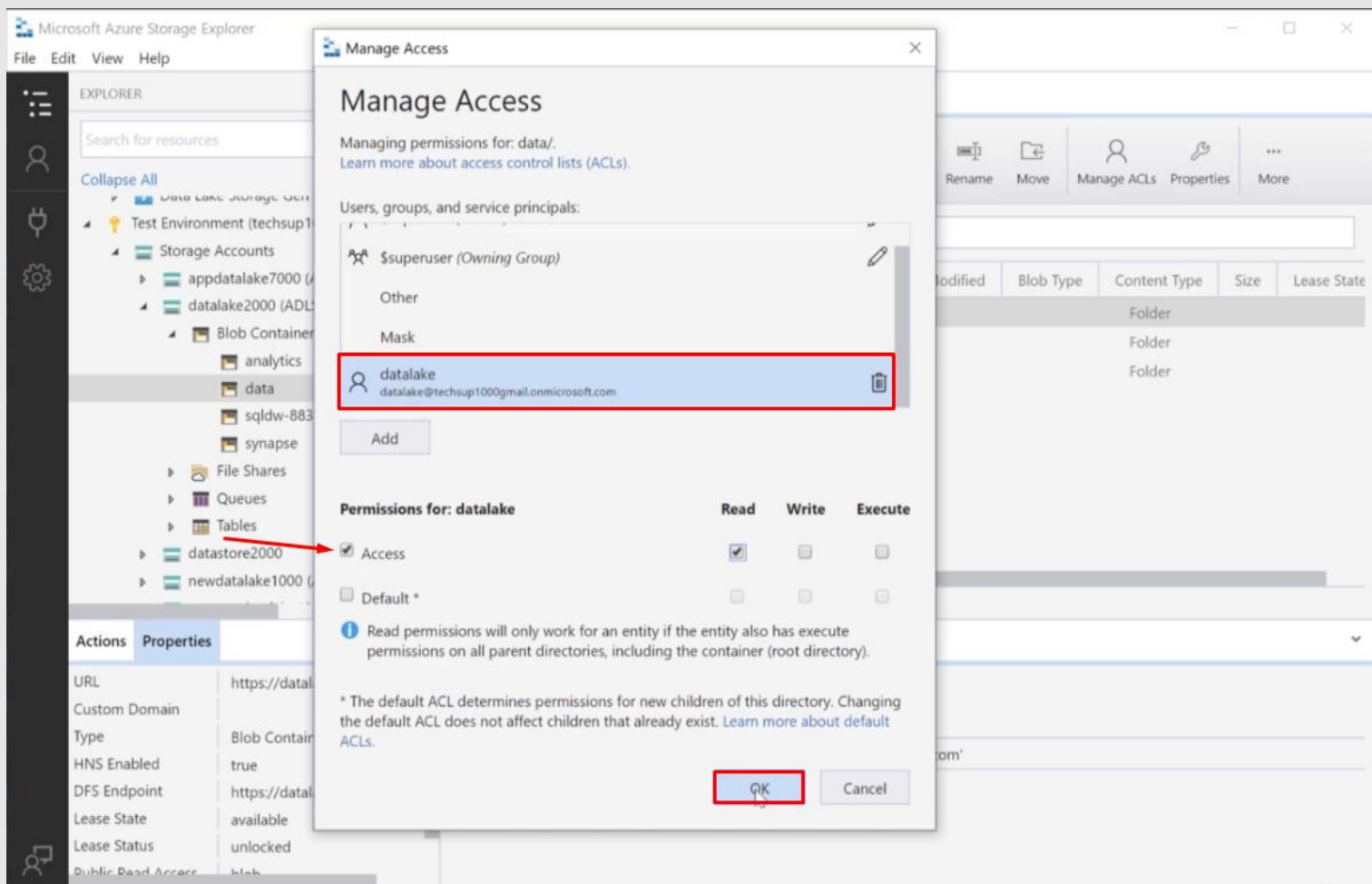
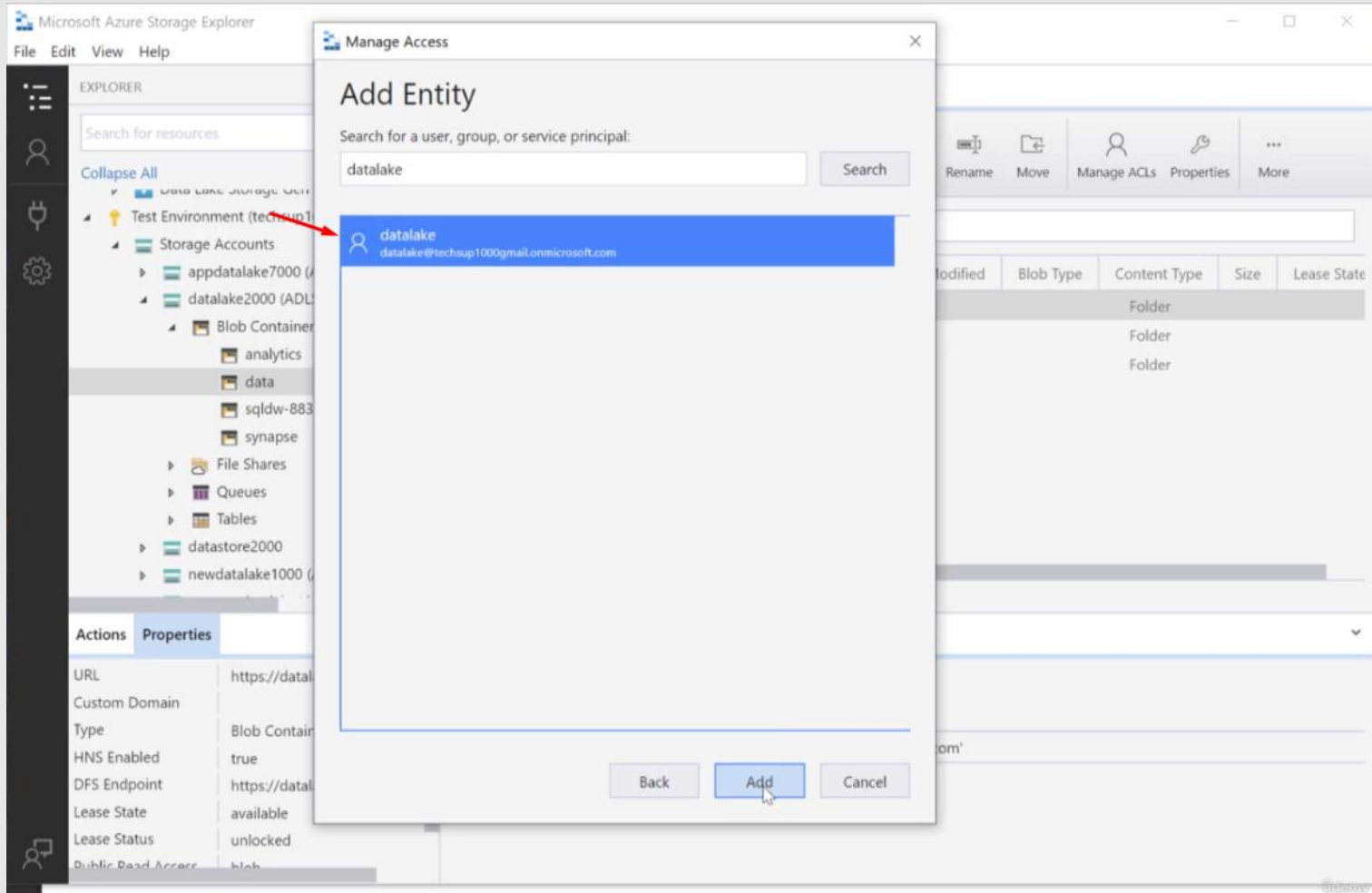
No users, groups, or service principals found.

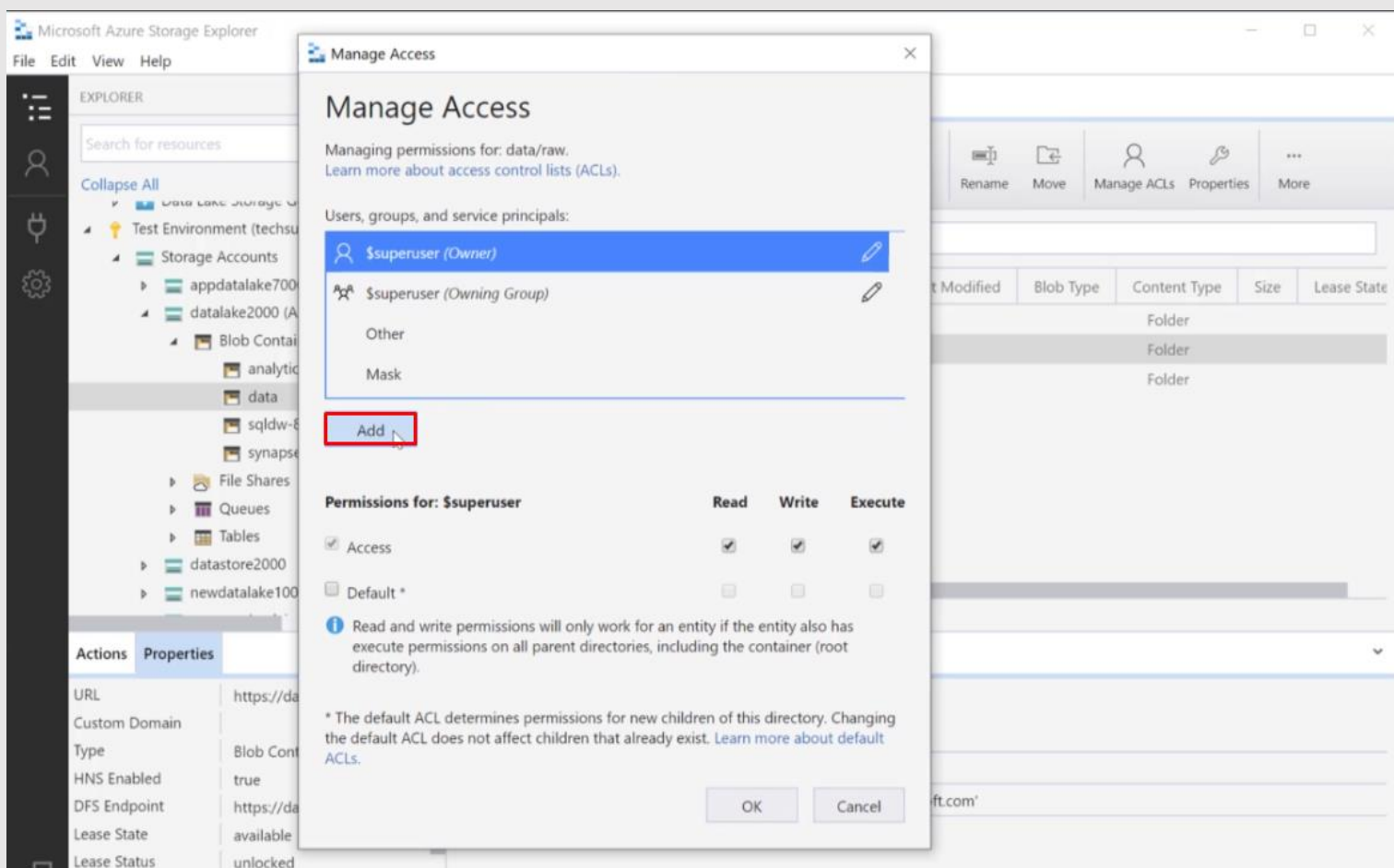
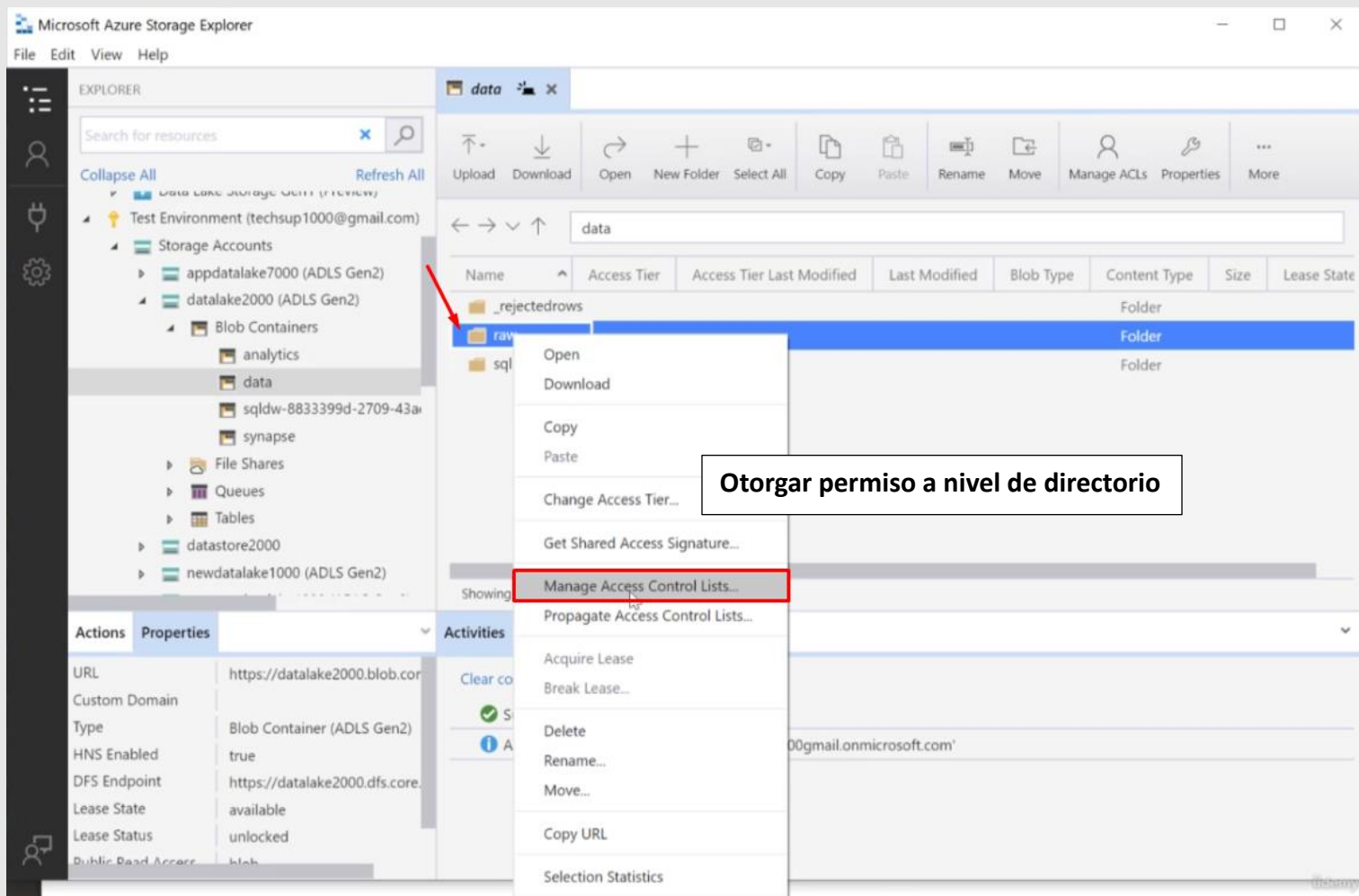
Selected members:

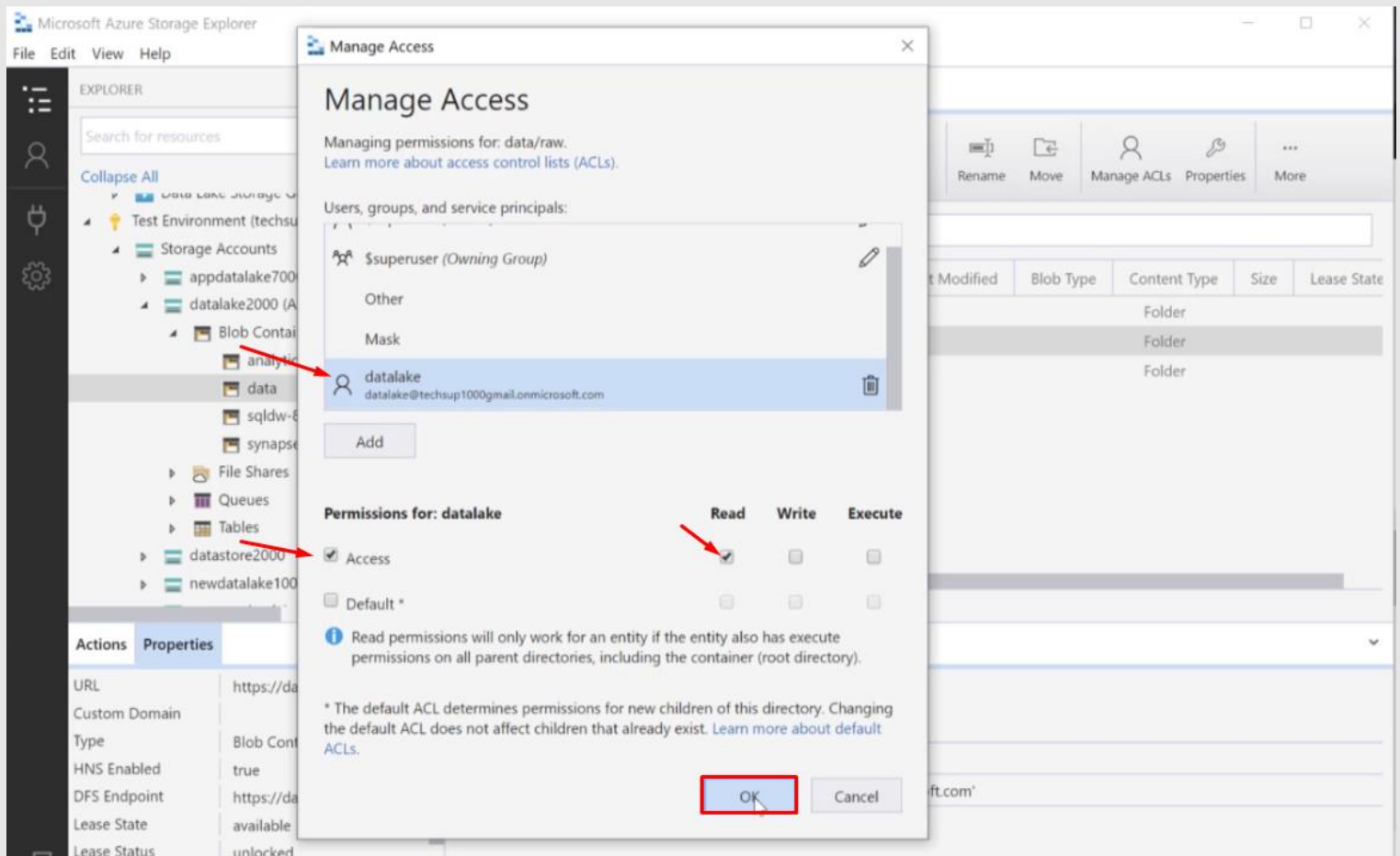
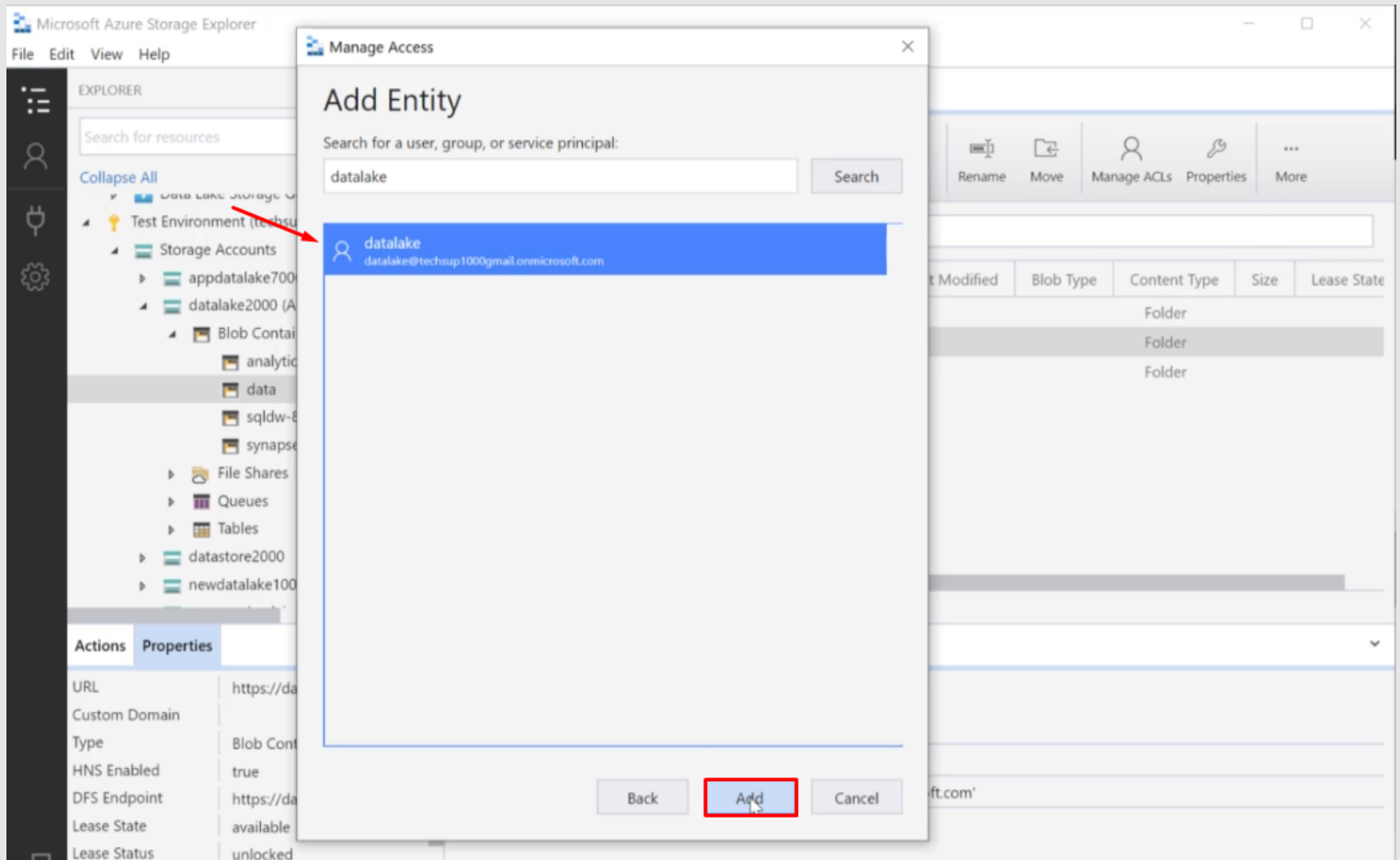
data lake
data lake@techsup1000gmail.onmicro... Remove

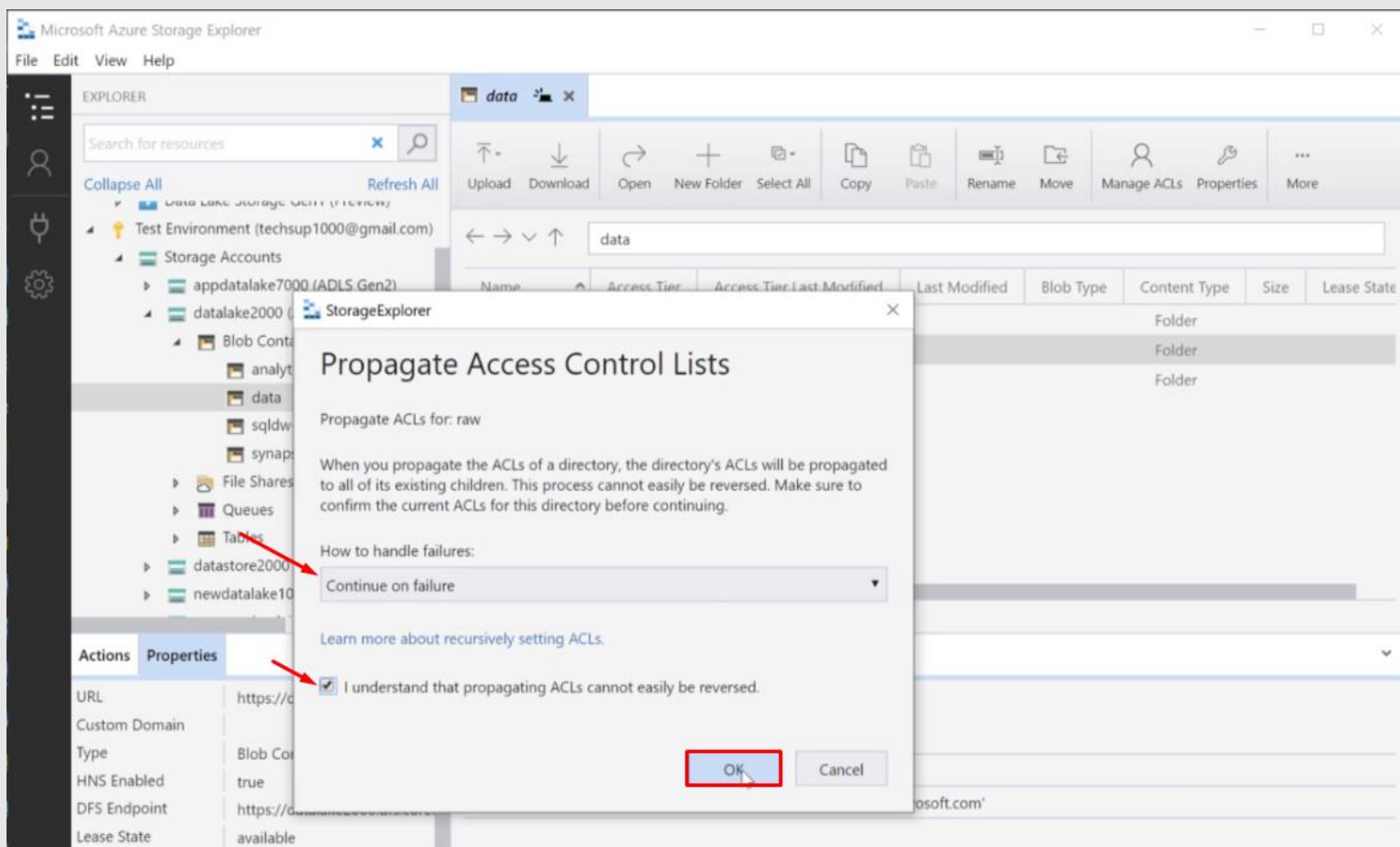
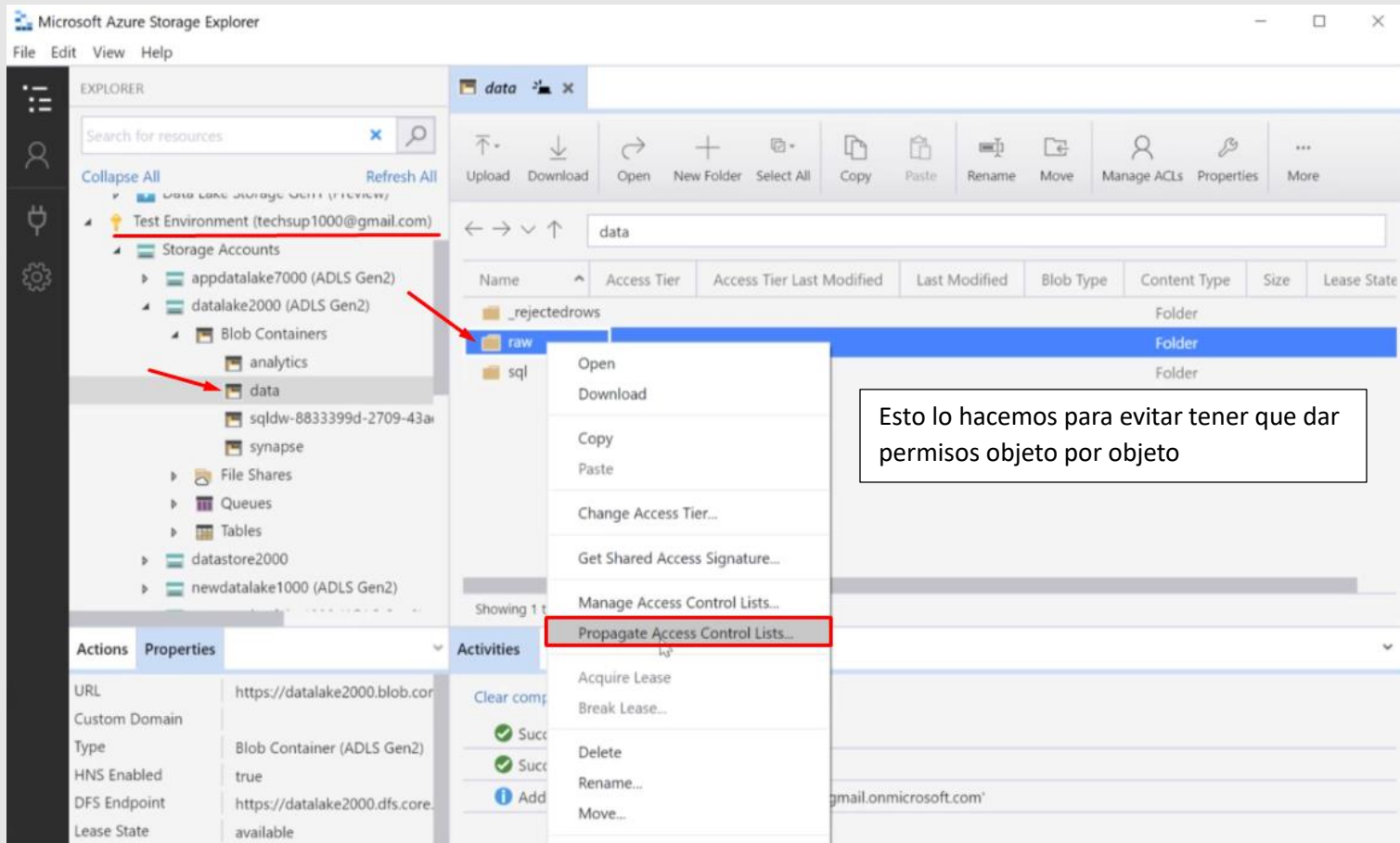
Save Discard











Podemos ver que ahora el nuevo usuario tiene acceso a todos los objetos

The screenshot displays the Microsoft Azure Storage Explorer interface. On the left, the 'EXPLORER' pane shows the hierarchy: 'Test Environment (datalake@techsup1000gr)' > 'Storage Accounts' > 'datalake2000 (ADLS Gen2)' > 'Blob Containers' > 'data'. A red arrow points to the 'data' container. The main pane shows the contents of the 'data' container, with a sub-path 'data > raw' selected. A red box highlights the following table of items:

Name	Access Tier	Access Tier Last Modified	Last Modified	Blob Type	Content Type	Size
customer					Folder	
newparquet					Folder	
nginx					Folder	
parquet					Folder	
Log.csv	Hot (inferred)		7/4/2021, 5:09:29 PM	Block Blob	application/octet-stream	
log.json	Hot (inferred)		7/7/2021, 5:10:33 PM	Block Blob	application/octet-stream	
Log_original.csv	Hot (inferred)		7/7/2021, 8:34:15 AM	Block Blob	application/octet-stream	
product.csv	Hot (inferred)		7/6/2021, 8:49:33 PM	Block Blob	application/octet-stream	
PT1H.json	Hot (inferred)		7/2/2021, 4:00:49 PM	Block Blob	application/json	

Below the table, it says 'Showing 1 to 9 of 9 cached items'. The bottom pane shows the 'Activities' section with the following messages:

- Clear completed Clear successful
- Successfully propagated ACLs of 'raw', directories changed: 5, files changed: 12.
- Successfully saved permissions for 'data/raw'
- Successfully saved permissions for 'data/'
- Added Azure account 'datalake@techsup1000gmail.onmicrosoft.com'