

 tajamar.	Máster en Ingeniería MultiCloud, DevOps y Seguridad.
AZURE LAB #7	

Administración de Azure Storage

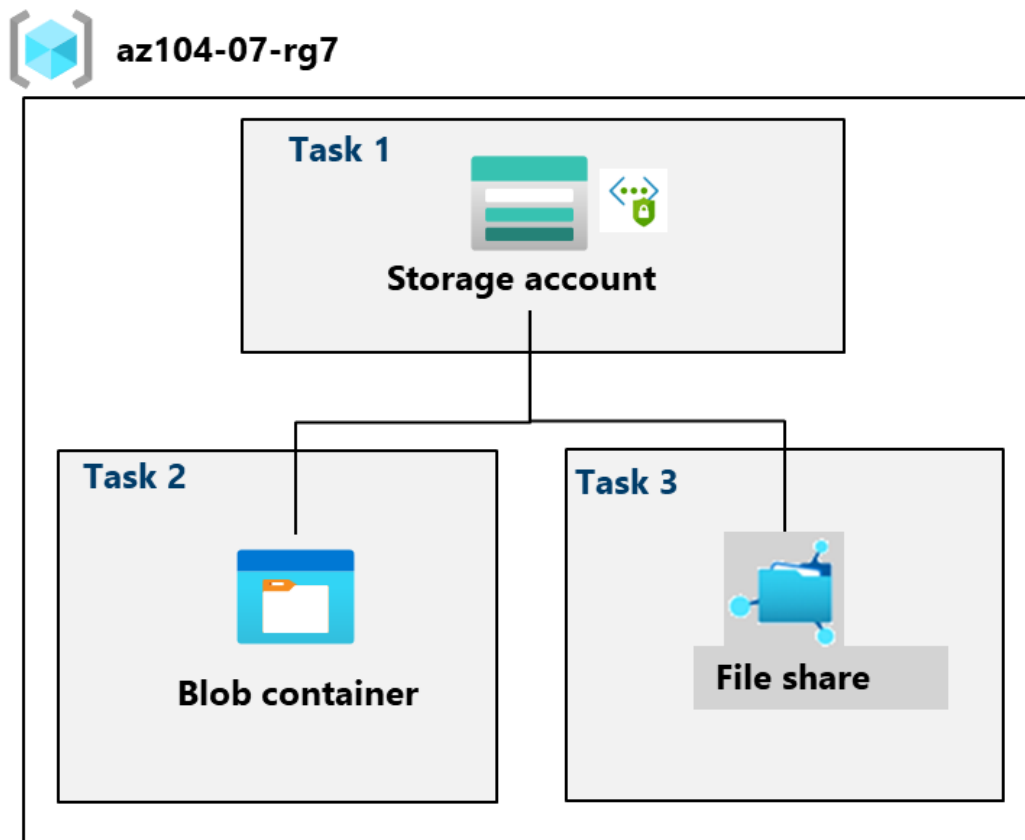
 tajamar.	Máster en Ingeniería MultiCloud, DevOps y Seguridad.
AZURE LAB #7	


Contenido

Esquema del laboratorio	3
Crear y configurar una cuenta de almacenamiento.	4
Creación y configuración del almacenamiento de blobs seguro	10
Configuración de Azure file storage.	14

	Máster en Ingeniería MultiCloud, DevOps y Seguridad.
AZURE LAB #7	

Esquema del laboratorio



	Máster en Ingeniería MultiCloud, DevOps y Seguridad.
AZURE LAB #7	

Crear y configurar una cuenta de almacenamiento.

Home > Storage center | Blob Storage >

Create a storage account

Basics Advanced Networking Data protection Encryption Tags Review + create

Azure Storage is a Microsoft-managed service providing cloud storage that is highly available, secure, durable, scalable, and redundant. Azure Storage includes Azure Blobs (objects), Azure Data Lake Storage Gen2, Azure Files, Azure Queues, and Azure Tables. The cost of your storage account depends on the usage and the options you choose below. [Learn more about Azure storage accounts](#)

Project details

Select the subscription in which to create the new storage account. Choose a new or existing resource group to organize and manage your storage account together with other resources.

Subscription * Azure for Students

Resource group * az104-rg7 [Create new](#)

Instance details

Storage account name * ① saraul1

Region * ① (Europe) Germany West Central [Deploy to an Azure Extended Zone](#)

Preferred storage type Choose preferred storage type

① This helps us provide relevant guidance. It doesn't restrict your storage to this resource type. [Learn more](#)

Performance * ①

☒ Standard: Recommended for most scenarios (general-purpose v2 account)

☐ Premium: Recommended for scenarios that require low latency.

Redundancy * ①


Geo-redundant storage (GRS)

☐ Make read access to data available in the event of regional unavailability.

☐ Geo priority replication guarantees Blob storage data is geo-replicated within 15 minutes.

Previous Next Review + create

Comienzo creando la cuenta de almacenamiento, la región de la cuenta la he tenido que poner Alemania ya que España no permite Geo-redundant storage de momento.

	Máster en Ingeniería MultiCloud, DevOps y Seguridad.
AZURE LAB #7	

Home > Storage center | Blob Storage >

Create a storage account

Basics Advanced **Networking** Data protection Encryption Tags Review + create

Public access

Access your resource from anywhere through a public network.

Note: Allowing access to your resource through a public network increases security risk. [Learn more](#)

Public network access *

- ☐ Enable
Allow inbound and outbound access with the option to restrict select inbound access using resource access configurations for this resource.
- ☒ **Disable**
Restrict inbound access while allowing outbound access.
- ☐ Secure by perimeter (Most restricted)
Restrict inbound and outbound access using a network security perimeter. Secure by perimeter offers the greatest level of inbound and outbound restriction to secure your resource.

Public network access scope

- ☐ Enable from all networks
- ☐ Enable from selected virtual networks and IP addresses

Private endpoint

Create a private endpoint to allow a private connection to this resource. Additional private endpoint connections can be created within the storage account or private link center.


+ Add private endpoint

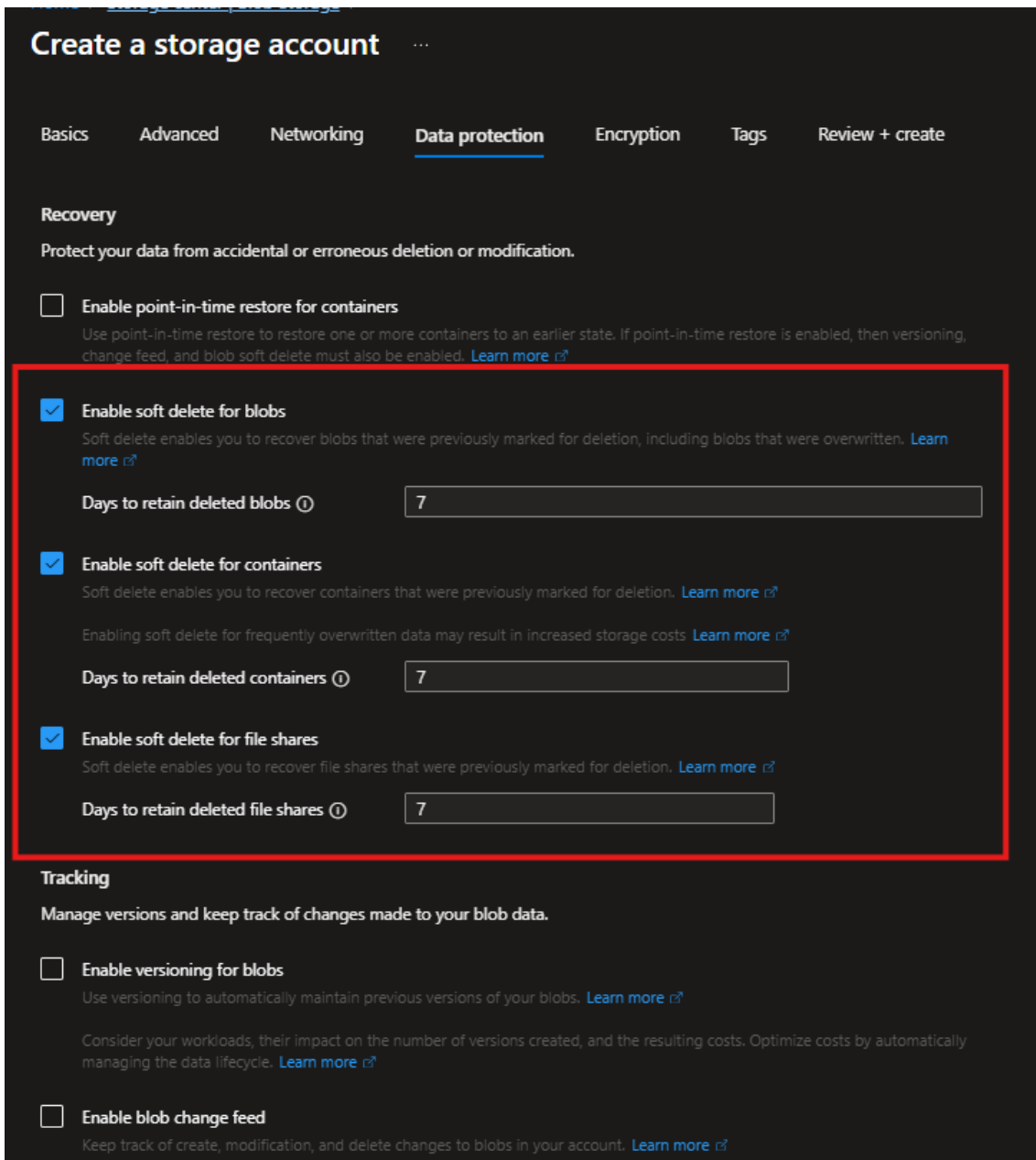
Name	Subscription	Resource g...	Region	Target sub-...	Subnet	Private DN...
Click on add to create a private endpoint						

Network routing

Previous Next **Review + create**

El ajuste "Disable" para el acceso a la red pública (Public Network Access) en una cuenta de Azure Storage es una configuración crítica de seguridad que restringe completamente el tráfico de entrada (inbound) proveniente de cualquier red pública, incluyendo internet.

	Máster en Ingeniería MultiCloud, DevOps y Seguridad.
AZURE LAB #7	



Create a storage account

Basics Advanced Networking **Data protection** Encryption Tags Review + create

Recovery

Protect your data from accidental or erroneous deletion or modification.

☐ Enable point-in-time restore for containers
Use point-in-time restore to restore one or more containers to an earlier state. If point-in-time restore is enabled, then versioning, change feed, and blob soft delete must also be enabled. [Learn more](#)

☒ Enable soft delete for blobs
Soft delete enables you to recover blobs that were previously marked for deletion, including blobs that were overwritten. [Learn more](#)
Days to retain deleted blobs ①

☒ Enable soft delete for containers
Soft delete enables you to recover containers that were previously marked for deletion. [Learn more](#)
Enabling soft delete for frequently overwritten data may result in increased storage costs. [Learn more](#)
Days to retain deleted containers ①

☒ Enable soft delete for file shares
Soft delete enables you to recover file shares that were previously marked for deletion. [Learn more](#)
Days to retain deleted file shares ①

Tracking

Manage versions and keep track of changes made to your blob data.


☐ Enable versioning for blobs
Use versioning to automatically maintain previous versions of your blobs. [Learn more](#)
Consider your workloads, their impact on the number of versions created, and the resulting costs. Optimize costs by automatically managing the data lifecycle. [Learn more](#)

☐ Enable blob change feed
Keep track of create, modification, and delete changes to blobs in your account. [Learn more](#)

Esta sección se centra en configurar las características de recuperación y control de versiones para proteger los datos de tu cuenta de almacenamiento contra eliminaciones accidentales o errores.

Soft Delete (Eliminación Blanda):

- Propósito: La eliminación blanda evita la pérdida permanente de datos cuando un usuario o una aplicación realiza una operación de borrado.

	Máster en Ingeniería MultiCloud, DevOps y Seguridad.
AZURE LAB #7	

- Funcionamiento: Cuando se elimina un elemento, este permanece en un estado recuperable durante un período de tiempo definido.

✓ Your deployment is complete

Deployment name: saraul1_1764924175512 Start time: 5/12/2025, 9:43:00
 Subscriptions: Azure for Students Correlation ID: 33b9aee2-e7cf-4cc5-bc2e-b53b9ee2123
 Resource group: az104-rg7

Deployment details

Resource	Type	Status	Operation details
✓ saraul1/default	Microsoft.Storage/storageAccounts/fileservices	OK	Operation details
✓ saraul1/default	Microsoft.Storage/storageAccounts/blobServices	OK	Operation details
✓ saraul1	Microsoft.Storage/storageAccounts	OK	Operation details

Next steps

[Go to resource](#)

Give feedback

[Tell us about your experience with deployment](#)

Creo la cuenta de almacenamiento.

Public network access

Configure what inbound access is enabled through this resource's public endpoint. [Learn more](#)

Public network access

☒ Enable
Allow inbound and outbound access with the option to restrict select inbound access using resource access configurations for this resource.

☐ Disable
Restrict inbound access while allowing outbound access.

☐ Secured by perimeter (Most restricted)
Restrict inbound and outbound access using a network security perimeter. Secure by perimeter offers the greatest level of inbound and outbound restriction to secure your resource.

⚠ Enabling public network access will make this resource available publicly. Unless public access is required, consider using the most restricted access configurations. [Learn more](#)

Public network access scope

☐ Enable from all networks

☒ Enable from selected networks

Virtual Networks

Allow select virtual networks to connect to your resource using service endpoints. [Learn more](#)

+ Add a virtual network

Virtual Network	Subnet	Address Range	Endpoint Status	Resource Group	Subscription
<p>IPv4 Addresses</p> <p>Allow select public internet IP addresses to access your resource. Learn more</p> <p><input checked="" type="checkbox"/> 95.124.167.181 🔗</p> <p><input type="text" value=""/></p> <p>(IPv4 address or CIDR)</p>					

Resource instances


Specify resource instances that will have access to your storage account based on their system-assigned managed identity. [Learn more](#)

Accedo al recurso > networking

Permite tanto el tráfico de entrada como de salida a través del endpoint público de la cuenta de almacenamiento. Sin embargo, permite que las restricciones definidas en la sección "Public network access scope" se apliquen.

2. Alcance del Acceso a la Red Pública: "Enable from selected networks"

La opción marcada en el segundo recuadro rojo es "Enable from selected networks" (Habilitar desde redes seleccionadas).

	Máster en Ingeniería MultiCloud, DevOps y Seguridad.
AZURE LAB #7	

Propósito: Esta opción restringe el acceso a la cuenta de almacenamiento sólo a las redes y direcciones IP que se especifiquen.

saraul1 | Redundancy

Storage account

Search

Save Discard Prepare for failover Refresh Give feedback

Resource visualizer

Data storage

Containers

File shares

Queues

Tables

Security + networking

Networking

Front Door and CDN

Access keys

Shared access signature

Encryption

Microsoft Defender for Cloud

Data management

Storage Actions

Redundancy

Data protection

Object replication

Blob inventory

Static website

Lifecycle management

Azure AI Search

Settings

Monitoring

Monitoring (classic)

Automation

Azure Storage redundancy copies your data so that it is protected from transient hardware failures, network or power outages, and natural disasters. If an outage renders the primary endpoint unavailable, then you can initiate a failover to the secondary endpoint to rapidly restore write access to your data. [Learn more.](#)

Redundancy

Geo-redundant storage (GRS)

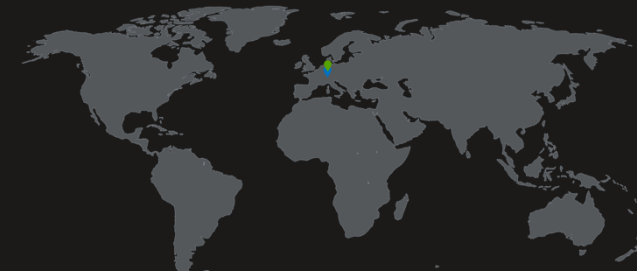
Need help with changing redundancy setting? [Help with Copilot](#)

Geo priority replication (Blob only) ☐

Last failover time -

Storage endpoints [View all](#)


Location	Data center type	Status	Failover
Germany West Central	Primary	Available	-
Germany North	Secondary	Available	-



Primary location

Secondary location

Miramos donde se estará replicando la cuenta de almacenamiento.

	Máster en Ingeniería MultiCloud, DevOps y Seguridad.
AZURE LAB #7	

Home > saraul1 | Lifecycle management >

Add a rule ...

✓ Details 2 Base blobs

Lifecycle management uses your rules to automatically move blobs to cooler tiers or to delete them. If you create multiple rules, the associated actions must be implemented in tier order (from hot to cool storage, then archive, then deletion).

If

Base blobs were *

☒ Last modified
☐ Created

More than (days ago) *


30

Then

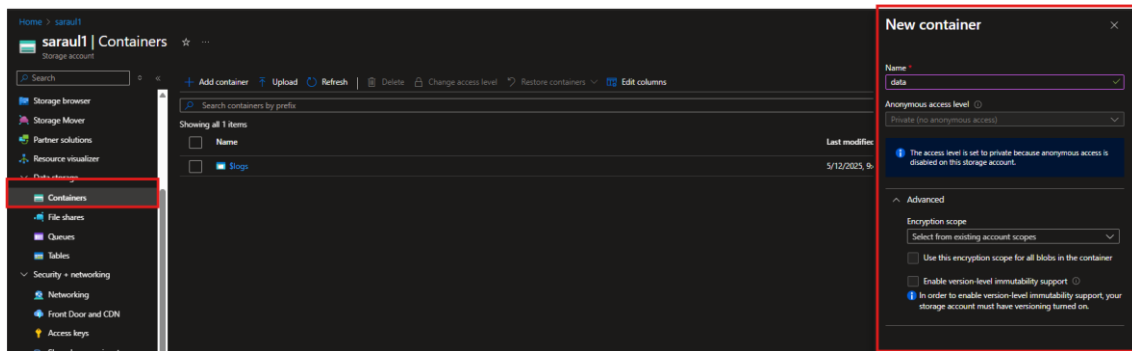
Move to cool storage

+ Add conditions

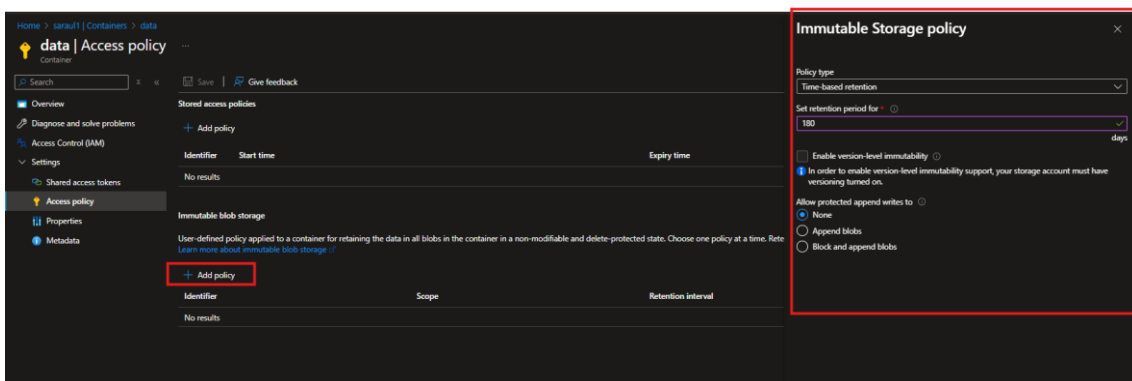
Configuro una regla para que los blobs se muevan a cool tier cuando no se han tocado en más de 30 días.

	Máster en Ingeniería MultiCloud, DevOps y Seguridad.
AZURE LAB #7	

Creación y configuración del almacenamiento de blobs seguro



Dentro de containers creo un nuevo contenedor.




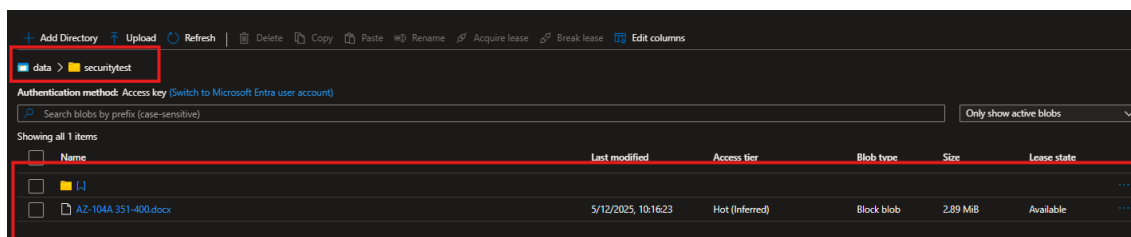
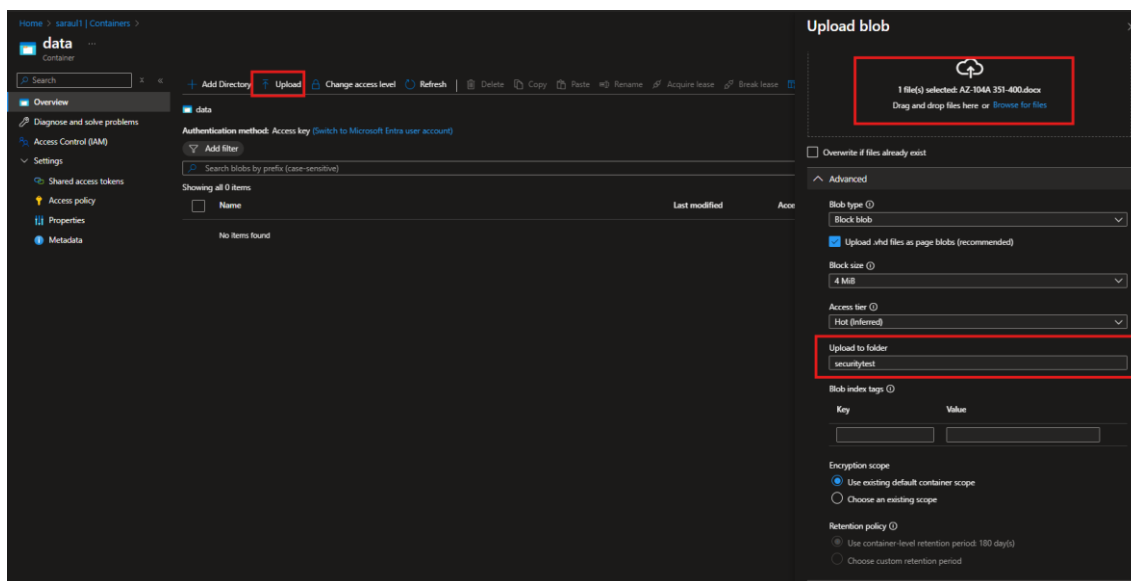
Esta configuración asegura que los datos, una vez escritos en el contenedor, no puedan ser modificados ni eliminados por un período de tiempo predefinido. Esto se conoce a menudo como "Write Once, Read Many" (WORM).

Tipo y Duración de la Política

Tipo de Política: Se ha seleccionado "Time-based retention" (Retención basada en el tiempo). Esto significa que la inmutabilidad de los blobs se mantendrá durante una duración específica.

Período de Retención: Se ha configurado en 180 días. Durante 180 días después de que un blob se escriba en este contenedor, nadie, ni siquiera un administrador con permisos completos, podrá borrar o sobrescribir ese blob. Una vez transcurridos los 180 días, el blob puede ser eliminado.

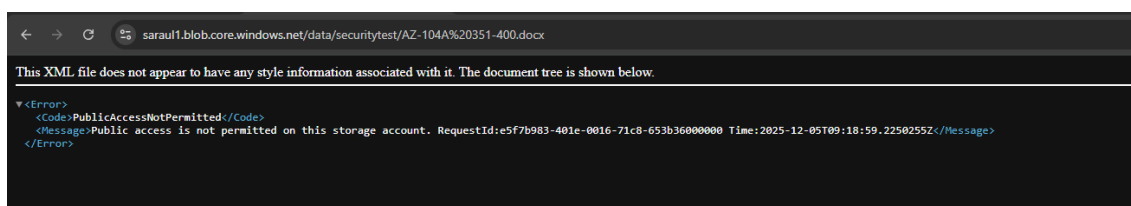
	Máster en Ingeniería MultiCloud, DevOps y Seguridad.
AZURE LAB #7	




Tipo de Blob: Está seleccionado Block blob (Blob en bloque), el tipo más común para archivos generales, como documentos, imágenes o videos.

Upload to folder: Se ha especificado un "directorio virtual" llamado securitytest.

Encryption Scope: Permite elegir si se usa la clave de cifrado por defecto del contenedor o una clave personalizada.



Como he configurado el acceso a privado no puede acceder desde el buscador cualquier persona.

	Máster en Ingeniería MultiCloud, DevOps y Seguridad.
AZURE LAB #7	

securitytest/AZ-104A 351-400.docx

Blob

Save
 Discard
 Download
 Refresh
 Delete

Overview Versions Snapshots Edit Generate SAS

A shared access signature (SAS) is a URI that grants restricted access to an Azure Storage blob. Use it when you want to grant access without sharing your storage account key. [Learn more about creating an account SAS](#)

Signing method
☒ Account key ☐ User delegation key

Signing key ⓘ
 Key 1

Stored access policy
 None

Permissions * ⓘ
 Read

Start and expiry date/time ⓘ

Start
 04/12/2025 10:05:57
 (UTC+01:00) Brussels, Copenhagen, Madrid, Paris


Expiry
 06/12/2025 18:20:57
 (UTC+01:00) Brussels, Copenhagen, Madrid, Paris

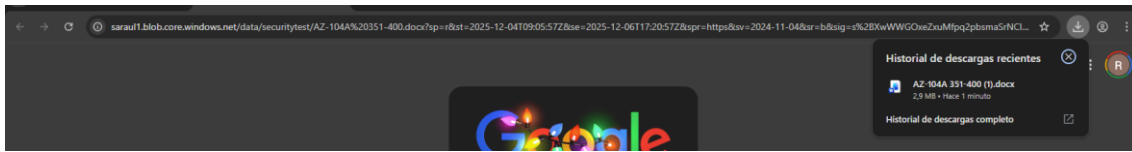
Allowed IP addresses ⓘ
 for example, 168.1.5.65 or 168.1.5.65-168.1.5.65

Allowed protocols ⓘ
☒ HTTPS only ☐ HTTPS and HTTP


Generate SAS token and URL

La configuración define la generación de una SAS a nivel de Blob firmada con la clave de la cuenta (el método de firma más potente) para conceder acceso de solo lectura al documento. La SAS es válida por un período muy limitado de tiempo y solo se permite el acceso a través de HTTPS, pero no está restringida por dirección IP y no utiliza una política de acceso almacenada, lo que exige mayor vigilancia sobre su caducidad y distribución.

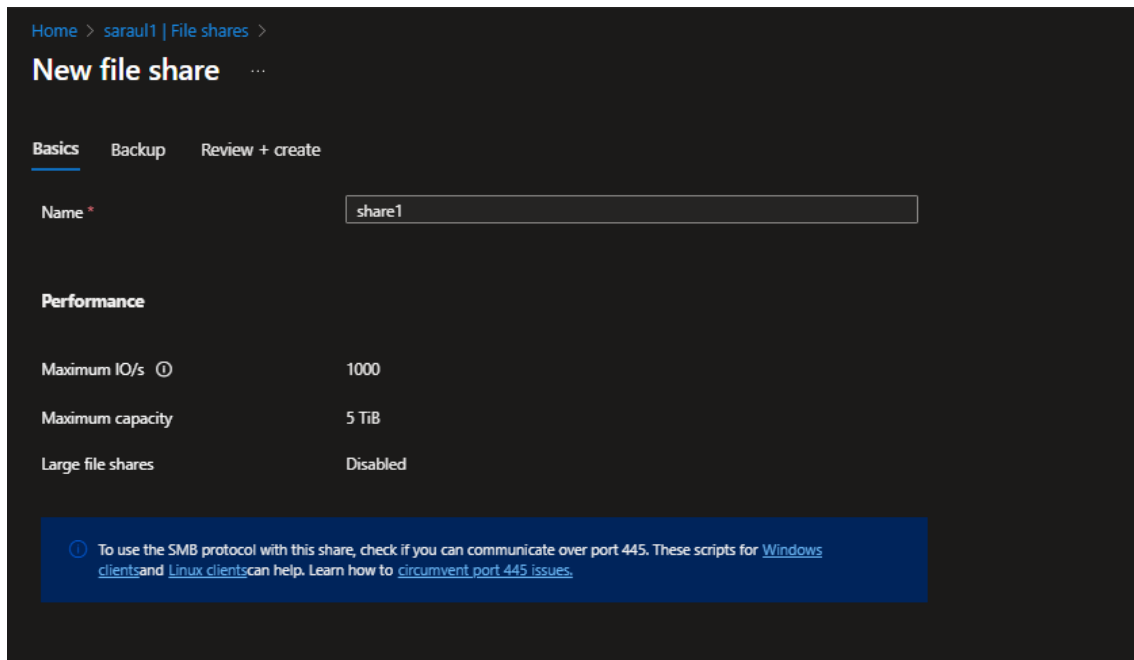
	Máster en Ingeniería MultiCloud, DevOps y Seguridad.
AZURE LAB #7	



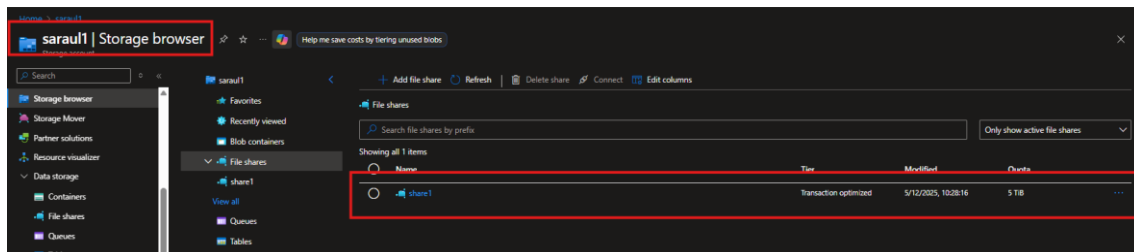
Al momento de copiar la url del sas generado se me descarga el archivo Word que he subido al container.

	Máster en Ingeniería MultiCloud, DevOps y Seguridad.
AZURE LAB #7	

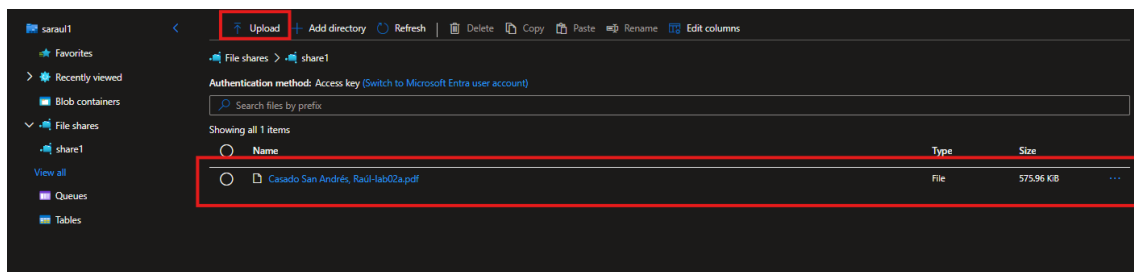
Configuración de Azure file storage.




Dentro de la cuenta de almacenamiento accedes a file shares y creamos uno nuevo.

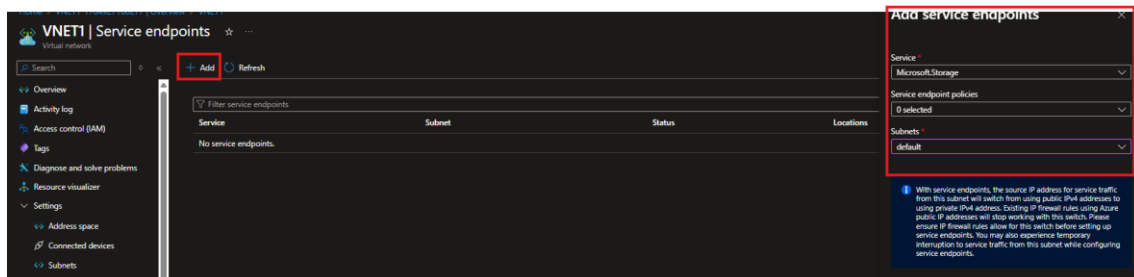


Comprobamos que he creado el file share.



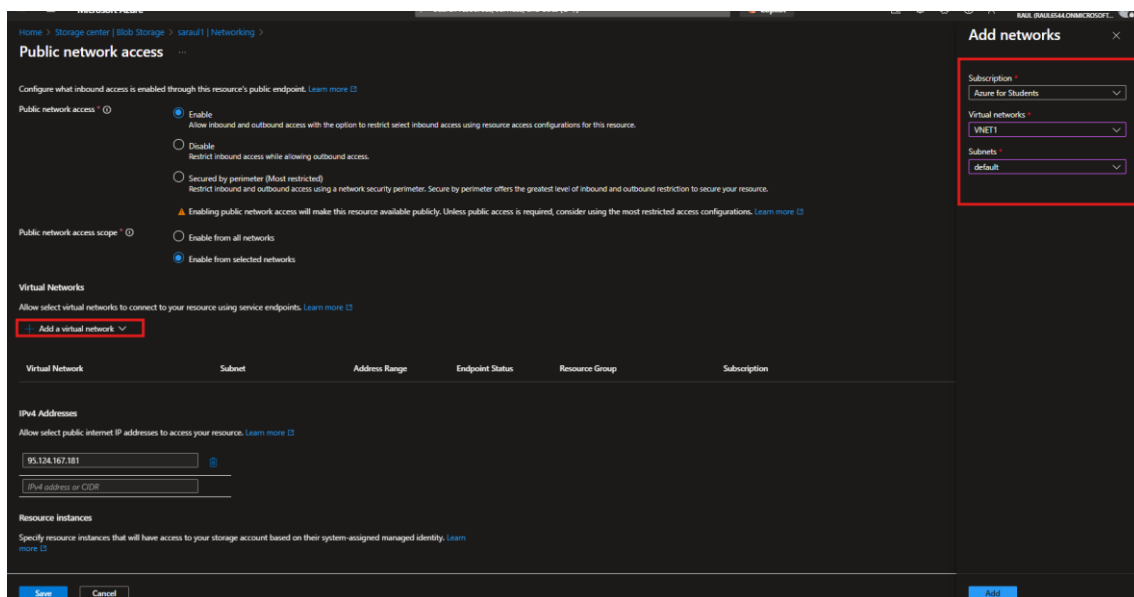
Subo un archivo de prueba.

	Máster en Ingeniería MultiCloud, DevOps y Seguridad.
AZURE LAB #7	




Creo una nueva red virtual, dentro de su configuración accedo a service endpoints donde creo uno nuevo para las cuentas de almacenamiento de la subred por defecto.

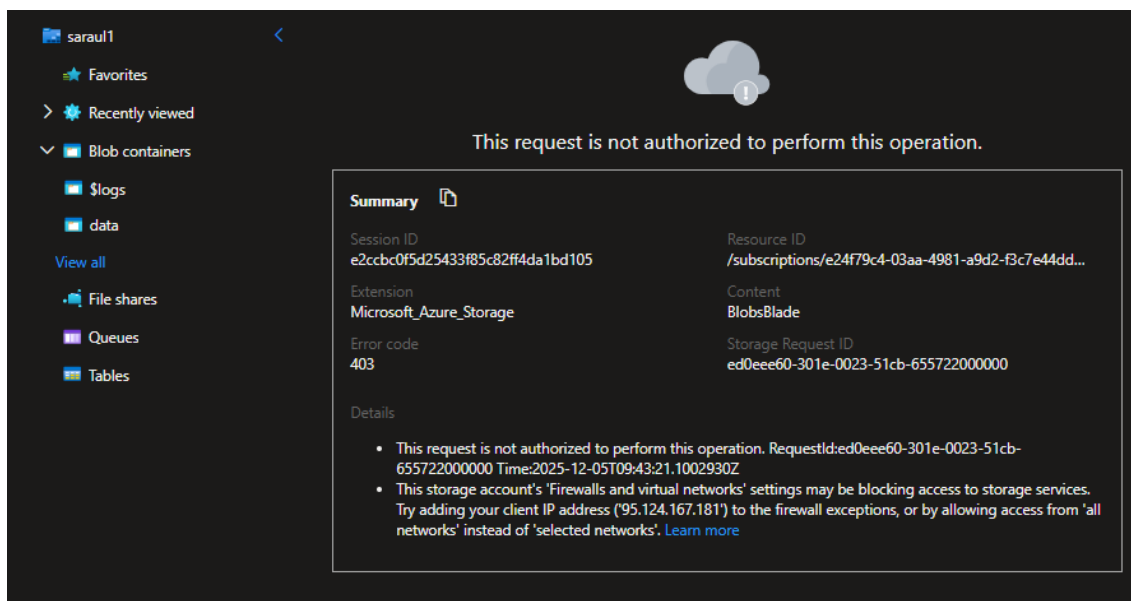
El servicio lo he tenido que cambiar a Microsoft.Storage.Global para que funcione al añadir el service endpoint a la configuración de red virtual de la cuenta de almacenamiento.



Añado la red virtual para dar acceso únicamente mediante la red virtual.

Borro mi ip pública de mi equipo.


	Máster en Ingeniería MultiCloud, DevOps y Seguridad.
AZURE LAB #7	



Al intentar acceder para ver los recursos dentro de mi container me produce un error ya que intento acceder mediante la ip de mi equipo y no con la red virtual.

Acción: Al configurar el Firewall de la cuenta de almacenamiento en "Enable from selected networks" y eliminar mi dirección IP pública (últimos pasos), el endpoint público de la cuenta de almacenamiento deja de ser accesible desde Internet en general.

Utilidad: Esto reduce drásticamente la superficie de ataque. Ningún atacante o usuario no autorizado fuera de mi red de Azure puede intentar conectarse a la cuenta, ni siquiera para probar la autenticación (como la clave de cuenta o SAS).

	Máster en Ingeniería MultiCloud, DevOps y Seguridad.
AZURE LAB #7	

2. Uso de Service Endpoints (Conexión Privada en la Red Troncal)

Acción: El paso clave es habilitar el Service Endpoint para Microsoft.Storage en el subnet default de vnet1.

Utilidad: Un Service Endpoint dirige el tráfico de salida desde tu VNet (vnet1) hacia el servicio de almacenamiento directamente a través de la red troncal (backbone) de Microsoft Azure, en lugar de a través de Internet.

Mejora de la seguridad: El tráfico nunca abandona la red segura de Microsoft.

Mejora del rendimiento: La ruta es optimizada y dedicada.

Conservación de ancho de banda: No se incurre en costos de ancho de banda de salida de Internet.